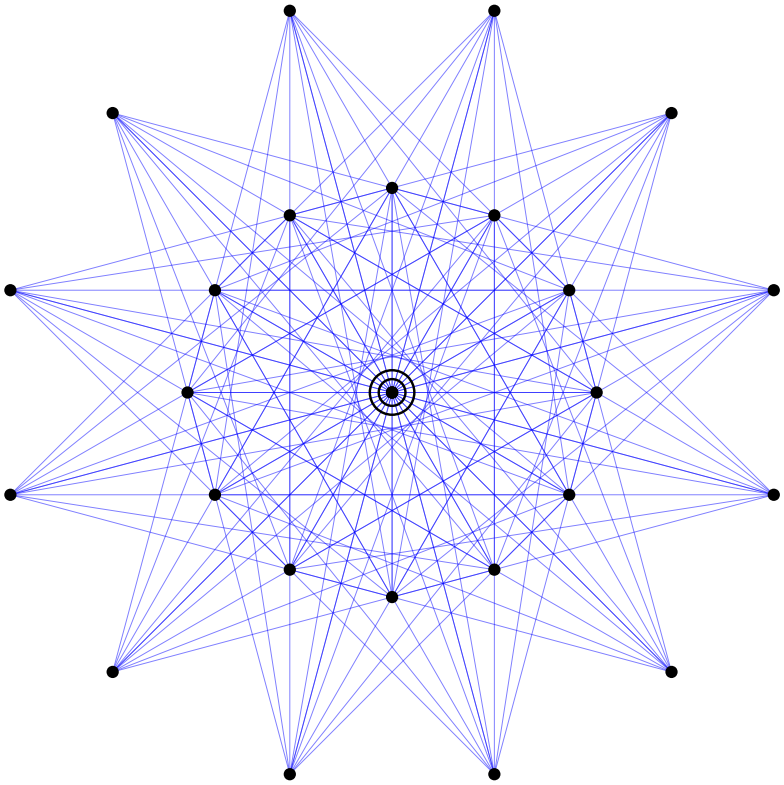
Albert algebras over commutative rings

The last frontier of Jordan systems

Preliminary version dated February 20, 2025

Skip Garibaldi, Holger P. Petersson and Michel L. Racine

Frontispiece



A projection into the plane of a graph whose vertices represent the 27 lines on a cubic surface, where two vertices are joined by an edge if the lines intersect. Three of the vertices (which are distinct in the true graph) all have the same image, the central vertex in the picture, which we have represented as a dot with two surrounding rings.

Contents

Preface

Albert algebras stand at a crossroads of subjects. They are useful for understanding exceptional Lie and algebraic groups and symmetric domains. They also stand out in their own natural context of non-associative algebras. Just as their more famous relative, the octonions, are the unique sort of simple alternative algebra that is not associative, Albert algebras are the unique sort of simple Jordan algebra that are not derived in a natural way from an associative algebra. These two attributes single out Albert algebras for special study.

In the present volume, such a study will be undertaken over arbitrary commutative rings. Despite the exceptional status enjoyed by Albert algebras within the general theory of Jordan algebras, they share a number of remarkable features with a wider class of Jordan algebras called Freudenthal algebras[1], which will therefore be included in our study, on an almost equal footing with Albert algebras. From a methodological point of view, Albert algebras cannot be properly understood without bringing octonion algebras into play. We will do so by regarding them as the most conspicuous class of examples in the theory of composition algebras over commutative rings, a subject of interest in its own right that will be presented here almost from scratch.

Albert algebras in context

Albert algebras, which (over fields) used to be called exceptional simple Jordan algebras in the past, are a class of exotic algebraic structures that, in spite of being confined to spaces of dimension 27, have an amazing potential for profound applications in various branches of mathematics. Here are a few striking examples.

Jordan algebras. Albert algebras made their first appearance in 1934 when Jordan[2], von Neumann and Wigner [148] proposed an algebraic formalism for quantum mechanics by developing a structure theory for what later would be called *formally real* (nowadays *euclidean*) Jordan algebras. Over a field F of characteristic not two, a *Jordan algebra* is defined as a (non-associative) F-algebra (i.e., an F-vector space equipped with a bilinear product xy, subject

[1] Hans Freudenthal (1905–1990).
[2] Pascual Jordan (1902–1980), see [57] for some biographical information.

to no further restrictions) that is commutative and satisfies what, under some mild hypotheses, turns out to be the minimal identity of degree at most 4 not implied by the commutative law (see 27.2): the *Jordan identity*

$$x(y(xx)) = (xy)(xx).$$

Standard examples of Jordan algebras arise as follows: given any associative algebra A over F, one endows the underlying vector space with a new multiplication, the *symmetric product*, defined by

$$x \bullet y := \frac{1}{2}(xy + yx), \tag{1}$$

and one checks that the resulting (commutative) algebra, denoted by A^+, is in fact a Jordan algebra. If a Jordan algebra is isomorphic to a subalgebra of A^+, for some associative algebra A, it is said to be *special*, otherwise *exceptional*.

In the course of their investigation, Jordan, von Neumann, and Wigner came across the 27-dimensional commutative real algebra $\mathrm{Her}_3(\mathbb{O})$ of 3-by-3 hermitian matrices with entries in the Graves-Cayley octonions $\mathbb{O}$ (a certain 8-dimensional real division algebra with involution, see §1 below) under the symmetric matrix product (1) and asked whether it is a Jordan algebra, and whether it is exceptional. Both questions were answered affirmatively by Albert[3] in [3], an immediate follow-up to [148]. The two papers may thus be regarded as the birth certificate of Albert algebras. Albert algebras in general may then be defined, very roughly, as twisted versions of $\mathrm{Her}_3(\mathbb{O}) \otimes_{\mathbb{R}} \mathbb{C}$, the complexification of $\mathrm{Her}_3(\mathbb{O})$. Over appropriate fields of characteristic not 2, Albert [8, 10] proved the existence of division exceptional Jordan algebras and, in a sense, obtained them all. In view of this remarkable achievement, and of the preceding ones, it is appropriate that simple exceptional Jordan algebras are called *Albert algebras*.

The role played by Albert algebras in Jordan theory is not confined to the set-up described above. On the contrary, thanks to their exceptional character, they take up a distinguished position within the general hierarchy of Jordan algebras, and this did not change after McCrimmon [181] invented quadratic Jordan algebras in the 1960s, which allowed the study of Jordan algebras over arbitrary commutative rings. The crowning achievement of this study is the McCrimmon-Zelmanov structure theory [191] of prime Jordan algebras without finiteness conditions, culminating in the conclusion that Albert algebras over fields of arbitrary characteristic are precisely the simple exceptional Jordan algebras (again no finiteness conditions are imposed). This is in striking

[3] A. Adrian Albert (1905–1972), see [139] or [12] for biographical information.

analogy to Kleinfeld's theorem 13.10 that octonion algebras over fields are precisely the simple alternative algebras that are not associative.

The connection between Albert algebras and octonion algebras is more than just an analogy. Not only can one use octonion algebras to construct Albert algebras as described in 5.5 and 39.19 (a), one can go the other way as well: Any Albert algebra, division or not, over a field determines an octonion algebra over that field, see 41.8, 41.25(iii) and Exc. 46.23.

Exceptional groups and Lie algebras. Albert algebras are tightly connected with semi-simple algebraic groups and Lie algebras, particularly those of exceptional type F_4, E_6, E_7 or D_4. An in-depth study of this connection will be carried out in Chapters VIII and IX below. One of the fundamental results in this context says that assigning to any Albert algebra its automorphism group (viewed as a group scheme) gives a bijection between isomorphism classes of Albert algebras and isomorphism classes of semi-simple group schemes of type F_4. Originally due to Hijikata [118] over fields of characteristic not 2 or 3, this result is extended here in 55.5 to arbitrary base rings. There is a somewhat weaker connection with groups of type E_6, in that the isomorphism group of the cubic norm on an Albert algebra is a simply connected semisimple affine group scheme of type E_6, see 58.2. Similar statements hold also for Lie algebras. For the reader interested in studying semisimple groups of types F_4 and E_6 that are not split, it can be a useful technique to re-state the problem as one about Albert algebras. This view is pursued for groups over a base field in [160, 268, 270]. Here we do the same but in the more general setting of an arbitrary base ring.

There is a distinguished connection between Albert algebras and Lie algebras. More generally, there are numerous relationships between Jordan algebras on the one hand and Lie algebras and semisimple affine group schemes on the other, such as from a grading as in [171, 80] or the Tits[4]-Kantor-Koecher construction or by the Freudenthal-Tits Magic Square, which is related to dual pairs in the sense of Howe [278]. As a specific example, the approach via grading gives a way to construct groups of type E_7 from Albert algebras, as explained in [138] or [95]. We do not pursue these constructions here. The existence of all of these connections was nicely expressed in [187]: "*if you open up a Lie algebra and look inside, 9 times out of 10 there is a Jordan algebra ... which makes it tick*."

Moufang and Tits polygons. Moufang n-gons ($n \geq 3$) are certain bipartite graphs of diameter n and girth $2n$ arising naturally in Tits's theory of spherical buildings [280, 281]. They have been enumerated completely by Tits-Weiss

[4] Jacques Tits (1930–2021), see [294] or [247] for biographical information.

[283]. As a first important step it is shown that Moufang n-gons exist only for $n = 3, 4, 6, 8$ [283, Thm. 17.1]. In the present context, the case $n = 6$ of Moufang hexagons is particularly interesting since [283, Thm. 17.5] yields a bijective correspondence between Moufang hexagons and Freudenthal division algebras, which in turn had been enumerated earlier by Petersson-Racine [225]. This correspondence can be modified to include arbitrary Freudenthal algebras if one is willing to relax the defining conditions of Moufang polygons, which will lead to the notion of a Tits polygon. See Mühlherr-Weiss [201] for details.

Bounded symmetric domains. The theory of bounded symmetric domains, i.e., of bounded domains in complex affine n-space such that every point p allows an automorphism of the domain having order 2 and p as an isolated fixed point, was initiated by E. Cartan [44] and culminated in their complete classification. The final classification list contains two exceptional types, in dimension 27 and 16, respectively. Both are intimately tied up with Albert algebras. A concise description of the 27-dimensional exceptional bounded symmetric domain in terms of Albert algebras may be found in U. Hirzebruch [120], while in order to achieve the same for the 16-dimensional one, Albert algebras must be viewed through the lens of Jordan pairs, see Loos [171, 172] or [68].

Severi varieties [169]. Freudenthal algebras over a field exist in dimensions 1, 3, 6, 9, 15 and, finally (the Albert case), 27. Let $X \subseteq \mathbb{P}^N$ be a smooth complex projective variety of dimension n, not contained in any hyperplane. Given any point $p \in \mathbb{P}^N \setminus X$, the projection from p defines a morphism

$$\pi_p \colon X \longrightarrow \mathbb{P}^{N-1},$$

and one may ask under what conditions the map π_p, for generic p, is a closed immersion. Zak [297] has shown that this is always the case for $n > \frac{2}{3}(N-2)$ and answered the question of what happens on the boundary $n = \frac{2}{3}(N-2)$. More precisely, he classified what he called *Severi varieties*, i.e., varieties X as above such that $n = \frac{2}{3}(N-2)$ and the projection π_p for generic $p \in \mathbb{P}^N \setminus X$ is always a closed immersion. It turns out that, up to projective equivalence, there are exactly four Severi varieties, of dimension $n = 2, 4, 8, 16$, respectively. Moreover, they may be described concisely as the projective varieties of rank-one elements in complex Freudenthal algebras of dimension at least 6. In the Albert case, one obtains the famous E_6-variety of dimension 16. See Theorem 41.29 for more on rank-one elements and §58 for more on E_6.

The 27 lines on a cubic surface. A celebrated theorem of 19th century algebraic geometry, due to Cayley and Salmon, says that there are exactly 27 lines

on any (smooth) cubic surface in projective 3-space over the complexes, and that the incidence relation among these lines does not depend on the cubic surface chosen, see for example [117]. To say the same thing differently, if you create a graph with vertices the lines on the surface and edges joining lines that are incident, you get the graph depicted in the frontispiece of this book, regardless of the surface you start with. This result is intimately connected with the (unique) Albert algebra over the complex numbers.

In one direction, given a cubic surface, one defines a vector space J with a basis identified with the lines on the surface. One can define a cubic form on J with signs chosen according to tritangent planes [77], from which one obtains a multiplication on J that is unique up to isotopy and which makes J an Albert algebra. In the other direction, given an Albert algebra J, the group of linear transformations preserving its (cubic) norm form is a semisimple affine group scheme of type E_6 as explained in 58.2. This leads to an identification of a basis of J with the 27 lines. Neher [202, II, §5] interprets the elements of J corresponding to the lines as quantities called tripotents (generalizing the notion of an idempotent) endowed, among other things, with an orthogonality relation. For more on the correspondences between Jordan algebras and the 27 lines, a good place to start is [179, §3].

About this book

This book was stimulated by new developments in the theory of Albert algebras over a field and grew out of surveys on the subject presented by subsets of the authors at Oberwolfach and published as [227], a 2004 survey [218], lectures at the universities of Artois and Ottawa in 2012, and a 2019 survey [220]. The aim of those surveys was to fill a gap in the literature: for fields of characteristic 2, the best reference on Jordan algebras may be [140], which focuses on the McCrimmon theory, whereas there was a lack of good references covering the specific properties of Albert algebras.

Why over commutative rings and not fields? Our original interest was to write a book on Albert algebras over a field including also fields of characteristic 2. That required writing in the language of quadratic Jordan algebras as explained above. Surprisingly, once this more powerful machinery has been brought to bear, it is very little extra work to consider algebras over an arbitrary ring instead of merely a field. (This observation is less surprising in view of the McCrimmon-Zelmanov structure theory already mentioned.) Hence our decision to write a book about Albert algebras over rings.

Remarks on prerequisites. We aim to make the presentation at a level ac-

cessible to graduate students in mathematics. Towards that goal, in most of the book we prove everything we use that is not already in standard reference books such as Bourbaki's *Algebra* [28, 29] and *Commutative Algebra* [27]. We also provide references to the Stacks Project [271] because it is so convenient and free. In the final two chapters, on Lie algebras and group schemes respectively, the presentation requires more background and we expand our scope of references in order to control the length of the presentation.

Exercises. There are more than 300 exercises contained in the book. They are intended to serve the didactic principle of active learning and to provide the reader with important additional material complementing the main text. Solutions to the exercises are available online as [96].

Plan of the book

Authors writing a monograph on a topic as versatile as Albert algebras in the most general setting are faced with a serious difficulty: it takes a considerable amount of time before the principal object of study can be properly defined. In the present case, the notion of an Albert algebra over an arbitrary commutative ring appears for the first time only on page 403. In order to mitigate the unpleasant side-effect of our approach and, also, to have early on motivating examples at our disposal, we start out with an introductory chapter (Chap. I) where the principal characters of the book (octonions and Albert algebras) are presented in the more familiar surroundings of the field $\mathbb{R}$ of real numbers and the ring $\mathbb{Z}$ of rational integers. This has the additional advantage of following rather closely the historical development of the subject (stretching back into the 19th century), and of providing a first motivation for the study of quadratic Jordan algebras. We describe in detail the Hurwitz quaternions [127] and the Dickson-Coxeter octonions [56, 64] over the integers, which in turn give rise to our first encounter with Albert algebras over $\mathbb{Z}$.

Researchers working on non-associative algebras over commutative rings often ignore properties of the underlying modules by simply treating them as a black box. In Chap. II we proceed differently and not only introduce the standard vocabulary of non-associative algebras over commutative rings (§§7, 8) but also recall two of the most important technical ingredients utilized in the present volume: scalar extensions (or base change) and (finitely generated) projective modules (§9). Standard properties of involutions (§10) and quadratic maps (§11) are also recalled before we conclude the chapter with a short introduction into Roby's theory [249] of polynomial laws (§12).

In Chap. III we make an excursion into alternative algebras over commutative rings. We prove Artin's theorem (14.5) and study in greater detail McCrimmon's theory of homotopes (§15), which gets short shrift in many texts on alternative algebras.

Chapter IV is devoted to the study of composition algebras over a commutative ring k, which we carry out within the more general framework of what we call conic algebras (called quadratic algebras or algebras of degree 2 by other authors). We present the Cayley-Dickson construction in this general setting (§18) and define composition k-algebras, basically, as unital non-associative algebras over k that are projective as k-modules and allow a non-singular quadratic form permitting composition (19.5). We then use the Cayley-Dickson construction to obtain first examples of octonion algebras and to derive first structure theorems for composition algebras over arbitrary commutative rings. Specializing, it is shown that all composition algebras of rank $r > 1$ over an LG ring[5] arise from an appropriate quadratic étale algebra by an at most two-fold application of the Cayley-Dickson construction. Another technique of producing examples of octonion algebras using ternary hermitian spaces is presented in §21. It immediately leads to the notion of a split composition algebra (21.19) and here, in particular, to the split octonions of Zorn vector matrices (21.18). After an excursion into reduced composition algebras (§22), we proceed to address the norm equivalence problem in §23, which asks whether composition algebras are classified by their norms and has an affirmative answer when working over an LG ring (Theorem 23.5) but not in general (Gille's theorem 23.9). Section 24 is devoted to an elementary tour de force through the theory of affine (group) schemes, which will be used in §26 to split arbitrary composition algebras by faithfully flat extensions, even by étale covers.

In Chap. V, we develop from scratch the elementary theory of (quadratic) Jordan algebras over commutative rings, confining ourselves to what is absolutely indispensable for the intended applications. Over fields of characteristic not 2, or over commutative rings in which 2 is invertible, this theory is well documented in book form (Jacobson [136] or McCrimmon [190]). The sole justification for the present chapter derives from the fact that the only systematic account of quadratic Jordan algebras, in the Jacobson lecture notes [137, 140], is becoming less and less accessible.

Inspired by McCrimmon [183], we take up the study of cubic norm structures and cubic Jordan algebras in Chap. VI. Our approach is distinguished by its precision (in that it works for the first time with a precise concept of a cubic form) and by its generality (in that the underlying modules are nearly

[5] LG rings are defined in 11.20. Every semi-local ring is an LG ring, and so is the ring of all algebraic integers.

arbitrary). The only concession we allow ourselves to make is the assumption that the base point of a cubic norm structure, i.e., the unit element of the corresponding cubic Jordan algebra, is unimodular, which holds automatically if the underlying module is projective. This assumption has the advantage of guaranteeing the validity of certain identities (e.g., that the norm of a cubic norm structure permits Jordan composition) which fail in McCrimmon's original setting (Exc. 34.28). The foundations of the theory will be laid out in §§33, 34, which in particular clarify the connection between cubic Jordan algebras and cubic alternative ones (34.12). In §35 we will be concerned with a general elementary principle of building up "big" cubic norm structures out of "smaller" ones. This principle, which will play a crucial role in the two Tits constructions later on, is based on a number of important identities that will also be the subject of this section. Section 36 is devoted to the study of cubic Jordan matrix algebras, providing the reader with examples of cubic Jordan algebras that are as explicit as one could possibly hope for. The construction of cubic Jordan matrix algebras will be formalized in a peculiar way making sure that it commutes with arbitrary base change. In §37 we turn to the important concept of elementary idempotents, which are the analogue in cubic Jordan algebras of absolutely primitive idempotents in finite-dimensional linear Jordan algebras over fields of characteristic not 2. We use elementary idempotents to present a special version of the Jacobson Co-ordinatization Theorem 37.17, whose proof will be provided at the end of the section. In §38 we draw the connection to Loos's theory [174] of generically algebraic Jordan algebras over commutative rings, allowing us to talk, in an ad-hoc manner, about Jordan algebras of degree 3 as a subclass of cubic Jordan algebras. This paves the way for our introduction of Freudenthal algebras in §39, where we use (and prove) Racine's enumeration theorem for semi-simple cubic Jordan algebras over fields to show that Freudenthal algebras exist only in ranks 1, 3, 6, 9, 15, and 27, with those of rank 27 being (finally!) referred to as Albert algebras. We define the notion of a split Freudenthal algebra and prove, pretty much in the spirit of what we have done for composition algebras in §26, that all Freudenthal algebras are split by some faithfully flat extension, though not always by an étale cover. After having investigated isotopies, norm similarities and isomorphisms in §40, with an important characterization of isotopes in Jordan matrix algebras over LG rings (Thm. 40.10) as its central result, we proceed in §41 to study reduced Freudenthal algebras over fields by exhibiting various classifying quadratic form invariants.

When it comes to exhibiting specific examples of cubic Jordan algebras not derived from hermitian matrices with entries in a composition algebra, the two Tits constructions are the method of choice. A new approach to these construc-

tions, a first outline of which may be found in [220, §§8–10], will be described in Chap. VII. In analogy to the Cayley-Dickson construction of composition algebras, the classical version of the first Tits construction [183, Thm. 6], [226, Thm. 3.5] has a cubic associative algebra as well as an invertible scalar in the base ring as input and produces a cubic Jordan algebra as output. The second Tits construction [183, Thm. 7], [226, Thm. 3.4], being a twisted version of the first, starts out from a cubic associative algebra with involution of the second kind and an "admissible scalar" as input to produce again a cubic Jordan algebra as output.

By contrast, the approach adopted here has been initiated by Faulkner's remarkable observation [75] that the first Tits construction survives in the more general setting of cubic *alternative* algebras rather than cubic associative ones. In fact, as we will be able to make abundantly clear, cubic alternative algebras are the natural habitat of the two Tits constructions. In order to derive the most important properties of the first Tits construction, we rely on the concept of a Kummer element 42.8 and its important characterization 42.16. Using this concept, we can show, for example, that, given a cubic Jordan algebra J and a Kummer element of J relative to some regular cubic Jordan subalgebra J_0 of J, there exists a cubic alternative algebra A such that $J_0 = A^{(+)}$ and J arises from A as well as some invertible scalar in the base ring by means of the first Tits construction. Our approach to the second Tits construction is based on isotopy involutions (43.2) rather than ordinary ones and on the concept of an étale element (44.8). Étale elements have the advantage of being available in abundance over an infinite field once we know they exist over the algebraic closure. This elementary observation plays a crucial role in the proof of Cor. 45.12, which says that over an LG ring all Albert algebras arise from the second Tits construction.

The chapter concludes in §46 with an application of the preceding results to mostly finite-dimensional cubic Jordan division algebras over fields. We show in particular that they are either (the Jordan algebras of) purely inseparable field extensions of characteristic 3 and exponent at most 1 or Freudenthal algebras of dimension 1, 3, 9 or 27 (46.8). In each of these dimensions, we construct examples over appropriate fields and, as a counter point, conclude the section by showing that over the "standard" fields ($\mathbb{C}$, $\mathbb{R}$, finite, local and global ones), Albert division algebras do not exist.

In the Cartan-Killing classification of finite-dimensional simple Lie algebras over an algebraically closed field of characteristic 0, there are infinite families and a few *exceptional* ones. Albert algebras over a field are the only *exceptional* simple Jordan algebras. While octonion algebras over fields were not called exceptional alternative algebras, they could well have been in view of

Kleinfeld's theorem. One could therefore argue that this book is a study of exceptional objects over rings. After studying derivation algebras of octonion algebras over rings, Chapter VIII describes various Lie algebras associated with a Jordan algebra J, the structure Lie algebra, and the algebra of derivations. Particular attention is paid to the case when J is an Albert algebra. While we try to work over a general ring, the results over fields, in particular over fields of characteristic 2 or 3, make clear some limitations.

Chapter IX is about group schemes and their relationships with Albert algebras and other sorts of algebras studied in the rest of the book. It describes the automorphism groups in the language of semisimple group schemes from SGA3 [101]. We describe faithfully flat descent and non-abelian cohomology in §54 and use it to prove correspondences between algebras and group schemes in §55. Section 56 departs temporarily from the main theme of the chapter to give an important example of an Albert algebra over the integers that is constructed by interpreting clever computations from Elkies-Gross [71] as concerning an isotopy. This eventually leads to a classification of Albert algebras over $\mathbb{Z}$ in §57. The problem of classifying such algebras was viewed as an open question until the development of this book, which led to the paper [95] containing a cosmetically different solution. The proof relies on various results from the literature and is a substantial deviation from our general goal of proving everything we use that is not in Bourbaki. In a final section, §58, we prove some connections of Albert algebras with groups of type E_6.

Acknowledgments

Many mathematicians deserve thanks for their helpful comments on this text, including Aravind Asok, Asher Auel, Peter Brühne, Jürgen Elstrodt, Detlev Hoffmann, Bruce Hunt, John Voight, and Torben Wiedemann. We are also grateful to Brian Conrad whose perspicacious remarks stimulated results in this book and the related paper [95]; Ryan Dahn for discussions concerning the history of Jordan; Catherine Garibaldi for contributing Figure 2a(ii); Bob Guralnick for his enthusiastic support; and Katie Leach and Arman Chowdhury at Cambridge University Press for their assistance. This text reflects our debt to various people who have influenced our way of thinking about mathematics over the course of years, including Alberto Elduque, Ottmar Loos, Erhard Neher, Markus Rost, J-P. Serre, and Adrian Wadsworth.

Finally, the people who most deserve our thanks are our families. Skip Garibaldi is grateful to his wife, Julia, and his children, for their support and encouragement and the gift of many weekend mornings without which his con-

tributions to this book would not have been possible. Holger P. Petersson would like to express his most profound gratitude to his wife, Bärbel, without whose love, patience, advice and unwavering support and encouragement, stretching over a period of more than twenty years, his contributions to this volume would never have come into being. Michel Racine would like to thank his wife Lise for her patience and encouragement through the years.

Conclusion

We hope this introduction has whetted your appetite for Albert algebras, dear reader. We have spent decades studying them and are delighted to have this opportunity to share what we have learned with you.

Notation and conventions

In this book, rings have a multiplication that is associative but possibly not commutative. Every ring R has a 1, which we sometimes denote 1_R, and every homomorphism of rings $\phi\colon R \to S$ satisfies $\phi(1_R) = 1_S$. (This definition of ring agrees with the one in Bourbaki [28, §I.8.1].) The set with one element has a unique ring structure, and we call it the *zero ring*; it is the terminal object in the category of rings. The set of integers, $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, denoted $\mathbb{Z}$, is a commutative ring; it is the initial object in the category of rings.

Most of the action in this volume takes place over an arbitrary commutative ring, usually denoted by k. Unadorned tensor products are always to be taken over k. Fields are denoted by capital letters, like $F, K, L, \ldots$.

We write k^n for a free module of rank n over k, usually identified with n-by-1 column vectors, and we write u^{T} for the transpose of a matrix or vector u. With this convention, for $u, v \in k^n$, $u^{\mathsf{T}}v$ is an element of k (commonly called the dot product of u and v) and uv^{T} is an n-by-n matrix. We write $\mathbf{1}_n$ for the n-by-n identity matrix.

Let M be a k-module. A *bilinear form* b on M is a k-linear map $b\colon M \otimes M \to k$. Equivalently, it is a function $M \times M \to k$ that is linear in each of the copies of M. This definition naturally extends to a notion of *multilinear form*, i.e., a k-linear function $M \otimes M \otimes \cdots \otimes M \to k$, see [28, §II.3.9]. A multilinear form is *alternating* if it vanishes on every simple tensor with two slots that agree, i.e., of the form $\cdots \otimes m \otimes \cdots \otimes m \otimes \cdots$ for some $m \in M$.

We provide a table of some of the notation used in this book.

$\mathbb{N}$	the set of non-negative integers: $0, 1, 2, \ldots$
$\mathrm{Mat}_n(k)$	the set of n-by-n matrices with entries in the ring k
$\mathrm{diag}(\gamma_1, \ldots, \gamma_n)$	the diagonal matrix in $\mathrm{Mat}_n(k)$ with diagonal entries $\gamma_1, \ldots, \gamma_n$
$\mathrm{GL}_n(k)$	the group of invertible elements of $\mathrm{Mat}_n(k)$
$\mathcal{S}_m$	the symmetric group on m letters
□	when written at the end of a theorem or corollary, indicates that the proof was already given or a reference is provided instead of a proof
–	placeholder for an unspecified argument to a function or functor
1°, 2°, ...	subdivisions of a proof, used to indicate the logical structure to the reader

I

Prologue: the ancient protagonists

Prominent specimens of the protagonists of the present volume will be introduced here not only over the field $\mathbb{R}$ of real numbers but also over the ring $\mathbb{Z}$ of rational integers. The results we obtain or at least sketch along the way will serve as a motivation for the systematic study we intend to carry out in the subsequent chapters of the book.

1 The Graves-Cayley octonions

At practically the same time, William R. Hamilton (1843), John T. Graves (1843) and Arthur Cayley (1845) discovered what are arguably the most important non-commutative, or even non-associative, real division algebras: the Hamiltonian quaternions and the Graves-Cayley octonions. It is particularly the latter, with their ability to co-ordinatize the euclidean Albert algebra (cf. 5.5 below), that deserve our attention. We begin with a brief digression into elementary linear algebra.

1.1 The cross product in 3-space. We regard complex column 3-space $\mathbb{C}^3$ as a *right* vector space over the field $\mathbb{C}$ of complex numbers in the natural way. It carries the canonical hermitian inner product

$$\mathbb{C}^3 \times \mathbb{C}^3 \longrightarrow \mathbb{C}, \quad (u, v) \longmapsto \bar{u}^{\mathsf{T}} v,$$

with respect to which the unit vectors $e_i \in \mathbb{C}^3$, $1 \leq i \leq 3$, form an orthonormal basis; we write $u \mapsto \|u\|$ for the corresponding hermitian norm on $\mathbb{C}^3$. Recall that the *cross* (or *vector*) *product* on $\mathbb{C}^3$ can be defined by the formula

$$(u \times v)^{\mathsf{T}} w = \det(u, v, w) \qquad (u, v, w \in \mathbb{C}^3). \tag{1}$$

The cross product is complex linear in each variable and $u, v \in \mathbb{C}^3$ are linearly dependent if and only if $u \times v = 0$; in particular, the cross product is *alternating*, i.e., $u \times u = 0$ for all $u \in \mathbb{C}^3$. Moreover, (1) implies that the expression $(u \times v)^{\mathsf{T}} w$ remains invariant under cyclic permutations of its arguments. The cross product of the unit vectors is determined by the formula

$$e_i \times e_j = e_l \quad \text{for } (ijl) \in \{(123), (231), (312)\}. \tag{2}$$

The specification of the indices i, j, l in this formula will henceforth be expressed by saying that it holds *for all cyclic permutations* (ijl) *of* (123). Finally, the cross product satisfies the *Grassmann identity*

$$(u \times v) \times w = vw^{\mathsf{T}}u - uw^{\mathsf{T}}v = w \times (v \times u) \tag{3}$$

for all $u, v, w \in \mathbb{C}^3$, which immediately implies the *Jacobi identity*

$$(u \times v) \times w + (v \times w) \times u + (w \times u) \times v = 0. \tag{4}$$

1.2 Real algebras. A detailed dictionary of non-associative algebras will be presented in 7.1 below. For the time being, it suffices to define a *real algebra* as a vector space A over the field $\mathbb{R}$ of real numbers together with an $\mathbb{R}$-bilinear product $(x, y) \mapsto xy$ from $A \times A$ to A that need neither be associative nor commutative. Nor will A in general admit an identity element, but if it does, i.e., if there exists an element $e \in A$ (necessarily unique) such that $ex = x = xe$ for all $x \in A$, the algebra is said to be *unital*. A sub-vector space of A stable under multiplication is called a *subalgebra*; it is a real algebra in its own right. We speak of a *unital subalgebra* B of a unital algebra A if $B \subseteq A$ is a subalgebra containing the identity element of A. For $X, Y \subseteq A$, we denote by XY the additive subgroup of A generated by all products xy, $x \in X$, $y \in Y$; we always write $X^2 := XX$ and $Xy := X\{y\}$, $xY := \{x\}Y$ for all $x, y \in A$. If A and B are real algebras, we define a *homomorphism* from A to B as a linear map $h\colon A \to B$ preserving products: $h(xy) = h(x)h(y)$ for all $x, y \in A$. A real algebra A is said to be a *division algebra* if $A \neq \{0\}$ and for all $u, v \in A$, $u \neq 0$, the equations $ux = v$ and $yu = v$ can be solved uniquely in A; if A has finite dimension (as a vector space over $\mathbb{R}$), this is equivalent to the absence of zero divisors: for all $a, b \in A$, the equation $ab = 0$ implies $a = 0$ or $b = 0$.

Now suppose A is a finite-dimensional real algebra and let $(e_i)_{1 \le i \le n}$ be a basis of A over $\mathbb{R}$. Then there is a unique family $(\gamma_{ijl})_{1 \le i,j,l \le n}$ of real numbers such that

$$e_j e_l = \sum_{i=1}^{n} \gamma_{ijl} e_i \qquad (1 \le j, l \le n). \tag{1}$$

The γ_{ijl} are called the *structure constants* of A relative to the basis chosen; they determine the multiplication of A uniquely. But note that different bases of the same algebra may have vastly different structure constants. Given a finite-dimensional real algebra, it sometimes helps to look for a basis with a particularly simple set of structure constants. If A and B are two real algebras of the same finite dimension, with bases $(e_i)_{1 \le i \le n}$ and $(d_i)_{1 \le i \le n}$, respectively, then the linear bijection $h\colon A \to B$ sending e_i to d_i for $1 \le i \le n$ is easily seen to be an

isomorphism of real algebras if and only if the family of structure constants of A relative to (e_i) is the same as the family of structure constants of B relative to (d_i).

1.3 Real quadratic maps. A map $Q\colon V \to W$ between finite-dimensional real vector spaces V, W is said to be *quadratic* if it is homogeneous of degree 2, so $Q(\alpha v) = \alpha^2 Q(v)$ for all $\alpha \in \mathbb{R}$, $v \in V$, and the map

$$DQ\colon V \times V \longrightarrow W, \quad (v_1, v_2) \longmapsto Q(v_1 + v_2) - Q(v_1) - Q(v_2), \tag{1}$$

is (symmetric) bilinear. In this case, we call DQ the *bilinearization* or *polar map* of Q. We mostly write $Q(v_1, v_2) := DQ(v_1, v_2)$ if there is no danger of confusion.

For example, given a finite-dimensional real algebra A, the *squaring*

$$\mathrm{sq}\colon A \longrightarrow A, \quad x \longmapsto x^2, \tag{2}$$

is a quadratic map with bilinearization given by

$$\mathrm{sq}(x, y) = D\,\mathrm{sq}(x, y) = xy + yx \tag{3}$$

for all $x, y \in A$.

Recall that a real quadratic *form*, i.e., a quadratic map $q\colon V \to \mathbb{R}$, is *positive* (resp. *negative*) *definite* if $q(v) > 0$ (resp. < 0) for all non-zero elements $v \in V$.

1.4 Real euclidean vector spaces. By a *real euclidean vector space* we mean a real vector space V together with a symmetric bilinear form $\sigma\colon V \times V \to \mathbb{R}$ which is *positive definite* in the sense that $\sigma(v, v) > 0$ for all non-zero elements $v \in V$. We then refer to σ as the *euclidean scalar product* of (V, σ) and define the corresponding *euclidean norm* as the map $\|\cdot\|\colon V \to \mathbb{R}$ given by $\|v\| := \sqrt{\sigma(v, v)}$ for all $v \in V$.

1.5 Defining the Graves-Cayley octonions. We may view

$$\mathbb{O} := \mathbb{C} \times \mathbb{C}^3$$

as a *real* vector space of dimension 8 whose elements have the form (a, u), $a \in \mathbb{C}$, $u \in \mathbb{C}^3$. Following Zorn [299, p. 401], we make $\mathbb{O}$ into a real algebra by the multiplication

$$(a, u)(b, v) := (ab - \bar{u}^{\mathsf{T}} v, v\bar{a} + ub + \bar{u} \times \bar{v}) \qquad (a, b \in \mathbb{C},\ u, v \in \mathbb{C}^3). \tag{1}$$

This algebra, also denoted by $\mathbb{O}$, is called the algebra of *Graves-Cayley octonions*. It has an identity element furnished by

$$1_{\mathbb{O}} := (1, 0) \tag{2}$$

but is neither commutative nor associative. For example, $i \in \mathbb{C}$ being the imaginary unit, an easy computation shows

$$((0,e_1)(0,e_2))(0,e_3 i) = (-i,0) = -(0,e_1)((0,e_2)(0,e_3 i)).$$

1.6 Norm, trace and conjugation. The map $n_{\mathbb{O}} \colon \mathbb{O} \to \mathbb{R}$ defined by

$$n_{\mathbb{O}}((a,u)) := \bar{a}a + \bar{u}^{\mathsf{T}}u = |a|^2 + \bar{u}^{\mathsf{T}}u \qquad (a \in \mathbb{C},\ u \in \mathbb{C}^3) \tag{1}$$

is called the *norm* of $\mathbb{O}$ and satisfies $n_{\mathbb{O}}(1_{\mathbb{O}}) = 1$. It is a positive definite real quadratic form whose bilinearization may be written as

$$n_{\mathbb{O}}(x,y) = \bar{a}b + \bar{b}a + \bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u = 2\,\mathrm{Re}(\bar{a}b + \bar{u}^{\mathsf{T}}v) \tag{2}$$

for $x = (a,u)$, $y = (b,v)$, $a,b \in \mathbb{C}$, $u,v \in \mathbb{C}^3$ and hence gives rise, in the sense of 1.4, to a euclidean scalar product on $\mathbb{O}$ defined by

$$\langle x,y\rangle := \frac{1}{2}n_{\mathbb{O}}(x,y) = \mathrm{Re}(\bar{a}b + \bar{u}^{\mathsf{T}}v), \tag{3}$$

making $\mathbb{O}$ into a real euclidean vector space with the corresponding euclidean norm

$$\|x\| := \sqrt{\langle x,x\rangle} = \sqrt{n_{\mathbb{O}}(x)} = \sqrt{|a|^2 + \|u\|^2}. \tag{4}$$

While Definition (3) is the standard way of introducing a euclidean scalar product in the present set-up, expression (2) is important in a more general context when working over commutative rings where $\frac{1}{2}$ is not available.

The norm of $\mathbb{O}$ as defined in (1) canonically induces the *trace* of $\mathbb{O}$, i.e., the linear form $t_{\mathbb{O}} \colon \mathbb{O} \to \mathbb{R}$ defined by

$$t_{\mathbb{O}}(x) := n_{\mathbb{O}}(1_{\mathbb{O}}, x) = 2\,\mathrm{Re}(a) = a + \bar{a}, \tag{5}$$

and the conjugation of $\mathbb{O}$, i.e., the linear map

$$\iota_{\mathbb{O}} \colon \mathbb{O} \longrightarrow \mathbb{O}, \quad x \longmapsto \bar{x} := t_{\mathbb{O}}(x)1_{\mathbb{O}} - x, \tag{6}$$

which obviously satisfies

$$\overline{(a,u)} = (\bar{a},-u) \qquad (a \in \mathbb{C},\ u \in \mathbb{C}^3), \tag{7}$$

leaves the norm invariant:

$$n_{\mathbb{O}}(\bar{x}) = n_{\mathbb{O}}(x) \qquad (x \in \mathbb{O}), \tag{8}$$

and has period 2: $\bar{\bar{x}} = x$ for all $x \in \mathbb{O}$. We view

$$\mathbb{O}^0 := \mathrm{Ker}(t_{\mathbb{O}}) = \{x \in \mathbb{O} \mid \bar{x} = -x\} = (i\mathbb{R}) \times \mathbb{C}^3 \tag{9}$$

as a euclidean subspace of $\mathbb{O}$. For $a \in \mathbb{C}$, $u \in \mathbb{C}^3$, we use (1.5.1) to compute

$$(a,u)^2 = (a^2 - \bar{u}^{\mathsf{T}}u, 2\operatorname{Re}(a)u) = 2\operatorname{Re}(a)(a,u) - (|a|^2 + \|u\|^2)(1,0),$$

so by (1), (5) every element $x \in \mathbb{O}$ satisfies the quadratic equation

$$x^2 - t_{\mathbb{O}}(x)x + n_{\mathbb{O}}(x)1_{\mathbb{O}} = 0. \tag{10}$$

Combining this with (6), we conclude

$$x\bar{x} = n_{\mathbb{O}}(x)1_{\mathbb{O}} = \bar{x}x, \quad x + \bar{x} = t_{\mathbb{O}}(x)1_{\mathbb{O}}. \tag{11}$$

Moreover, replacing x by $x + y$, expanding and collecting mixed terms in (10), we conclude (see also (1.3.3))

$$x \circ y := xy + yx = t_{\mathbb{O}}(x)y + t_{\mathbb{O}}(y)x - n_{\mathbb{O}}(x,y)1_{\mathbb{O}}. \tag{12}$$

The process of passing from (10) to (12) will be encountered quite frequently in the present work and is called *linearization*. We also note

$$n_{\mathbb{O}}(x,\bar{y}) = t_{\mathbb{O}}(xy) = n_{\mathbb{O}}(\bar{x},y) \tag{13}$$

for $x = (a,u)$, $y = (b,v)$, $a,b \in \mathbb{C}$, $u,v \in \mathbb{C}^3$ since (1.5.1), (5), 2 yield

$$t_{\mathbb{O}}(xy) = 2\operatorname{Re}(\bar{a}b - \bar{u}^{\mathsf{T}}v) = n_{\mathbb{O}}((\bar{a},-u),(b.v)) = n_{\mathbb{O}}(\bar{x},y),$$

hence the second equation of (13), while the first now follows from (8) linearized.

1.7 Alternativity. As we have seen in 1.5, the algebra of Graves-Cayley octonions is not associative. On the other hand, it follows from Exc. 1.16 below that it is *alternative*: the *associator* $[x,y,z] := (xy)z - x(yz)$ is an alternating (trilinear) function of its arguments $x,y,z \in \mathbb{O}$. In particular, the identities

$$x^2y = x(xy), \quad (xy)x = x(yx), \quad (yx)x = yx^2$$

hold in all of $\mathbb{O}$. Alternative algebras are an important generalization of associative algebras and will be studied more systematically, under a much broader perspective, in later portions of the book, see particularly Chap. III below. We speak of a *properly* alternative algebra if it is alternative but *not* associative.

1.8 Theorem. *The Graves-Cayley octonions form an eight-dimensional properly alternative real division algebra, and the norm of* $\mathbb{O}$ permits composition: $n_{\mathbb{O}}(xy) = n_{\mathbb{O}}(x)n_{\mathbb{O}}(y)$ *for all* $x,y \in \mathbb{O}$.

Proof As we have seen, the real algebra $\mathbb{O}$ is alternative (1.7) but not associative (1.5). It remains to show that the positive definite quadratic form $n_{\mathbb{O}}$

permits composition since this immediately implies that $\mathbb{O}$ has no zero divisors, hence is a division algebra (1.2). Accordingly, let $x = (a, u)$, $y = (b, v)$, $a, b \in \mathbb{C}$, $u, v \in \mathbb{C}^3$. Then (1.5.1), (1.6.1) yield

$$\begin{aligned} n_{\mathbb{O}}(xy) &= n_{\mathbb{O}}((ab - \bar{u}^{\mathsf{T}}v, v\bar{a} + ub + \bar{u} \times \bar{v})) \\ &= (\bar{a}\bar{b} - \bar{v}^{\mathsf{T}}u)(ab - \bar{u}^{\mathsf{T}}v) + (\bar{v}^{\mathsf{T}}a + \bar{u}^{\mathsf{T}}\bar{b} + (u \times v)^{\mathsf{T}})(v\bar{a} + ub + \bar{u} \times \bar{v}) \\ &= \bar{a}a\bar{b}b - \bar{a}\bar{b}\bar{u}^{\mathsf{T}}v - \bar{v}^{\mathsf{T}}uab + \bar{v}^{\mathsf{T}}u\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}va\bar{a} + \bar{v}^{\mathsf{T}}uab + \bar{v}^{\mathsf{T}}(\bar{u} \times \bar{v})a \\ &\quad + \bar{u}^{\mathsf{T}}v\bar{a}\bar{b} + \bar{u}^{\mathsf{T}}u\bar{b}b + \bar{u}^{\mathsf{T}}(\bar{u} \times \bar{v})\bar{b} + (u \times v)^{\mathsf{T}}(v\bar{a} + ub + \bar{u} \times \bar{v}). \end{aligned}$$

Observing (1.1.1), we obtain $\bar{v}^{\mathsf{T}}(\bar{u} \times \bar{v}) = \bar{u}^{\mathsf{T}}(\bar{u} \times \bar{v}) = (u \times v)^{\mathsf{T}}v = (u \times v)^{\mathsf{T}}u = 0$, while (1.1.1) combined with the Grassmann identity (1.1.3) implies

$$(u \times v)^{\mathsf{T}}(\bar{u} \times \bar{v}) = \bar{v}^{\mathsf{T}}((u \times v) \times \bar{u}) = \bar{v}^{\mathsf{T}}v\bar{u}^{\mathsf{T}}u - \bar{v}^{\mathsf{T}}u\bar{u}^{\mathsf{T}}v.$$

Hence the preceding displayed formula reduces to

$$n_{\mathbb{O}}(xy) = \bar{a}a\bar{b}b + \bar{a}a\bar{v}^{\mathsf{T}}v + \bar{u}^{\mathsf{T}}u\bar{b}b + \bar{u}^{\mathsf{T}}u\bar{v}^{\mathsf{T}}v = n_{\mathbb{O}}(x)n_{\mathbb{O}}(y),$$

as claimed. □

1.9 Remark. The composition formula $n_{\mathbb{O}}(xy) = n_{\mathbb{O}}(x)n_{\mathbb{O}}(y)$ is bi-quadratic in $x, y \in \mathbb{O}$ and by (repeated) linearization yields

$$\begin{aligned} n_{\mathbb{O}}(x_1y, x_2y) &= n_{\mathbb{O}}(x_1, x_2)n_{\mathbb{O}}(y), \\ n_{\mathbb{O}}(xy_1, xy_2) &= n_{\mathbb{O}}(x)n_{\mathbb{O}}(y_1, y_2), \\ n_{\mathbb{O}}(x_1y_1, x_2y_2) + n_{\mathbb{O}}(x_1y_2, x_2y_1) &= n_{\mathbb{O}}(x_1, x_2)n_{\mathbb{O}}(y_1, y_2) \end{aligned}$$

for all $x, y, x_1, x_2, y_1, y_2 \in \mathbb{O}$.

1.10 Inversion formula. Given $x \neq 0$ in $\mathbb{O}$, Theorem 1.8 yields unique elements $y, z \in \mathbb{O}$ such that $xy = zx = 1_{\mathbb{O}}$. In fact, by (1.6.11), we necessarily have

$$y = z = x^{-1} := \frac{1}{n_{\mathbb{O}}(x)}\bar{x}.$$

We call x^{-1} the *inverse* of x in $\mathbb{O}$

1.11 The Hamiltonian quaternions. The subspace $\mathbb{H} := \mathbb{R} \times \mathbb{R}^3$ of $\mathbb{O}$ is actually a subalgebra since

$$(\alpha, u)(\beta, v) = (\alpha\beta - u^{\mathsf{T}}v, \alpha v + \beta u + u \times v). \qquad (\alpha, \beta \in \mathbb{R},\ u, v \in \mathbb{R}^3) \qquad (1)$$

This algebra is called the algebra of *Hamiltonian quaternions*. It contains an identity element since $1_{\mathbb{H}} := 1_{\mathbb{O}} \in \mathbb{H}$. Note that the Hamiltonian quaternions

can be defined directly, without recourse to the Graves-Cayley octonions, by the product (1) on the real vector space $\mathbb{R} \times \mathbb{R}^3$. Moreover, the vectors

$$1_{\mathbb{H}} := 1_{\mathbb{O}}, \quad \mathbf{i} := (0, e_1), \quad \mathbf{j} := (0, e_2), \quad \mathbf{k} := (0, e_3) \tag{2}$$

form a basis of $\mathbb{H}$ over $\mathbb{R}$ in which $1_{\mathbb{H}}$ acts as a two-sided identity element and, by (1) combined with (1.1.2),

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1_{\mathbb{H}}, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}. \tag{3}$$

Thus we have obtained a basis of the Hamiltonian quaternions with a particularly simple family of structure constants (cf. 1.2). We will see in Cor. 1.12 below that the Hamiltoniam quaternions are associative. Hence (3) may be written more concisely as

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1_{\mathbb{H}}. \tag{4}$$

Restricting the norm, trace, conjugation of $\mathbb{O}$ to $\mathbb{H}$, we obtain what we call the *norm, trace, conjugation of* $\mathbb{H}$, denoted by $n_{\mathbb{H}}$, $t_{\mathbb{H}}$, $\iota_{\mathbb{H}}$, respectively, which enjoy the same algebraic properties we have derived for the Graves-Cayley octonions in 1.6. By the same token, $\mathbb{H}$ may also be viewed canonically as a real euclidean vector space. Consulting Thm. 1.8, we now obtain the following result.

1.12 Corollary. *The Hamiltonian quaternions* $\mathbb{H}$ *form an associative but not commutative real division algebra of dimension four, and the norm of* $\mathbb{H}$ *permits composition:* $n_{\mathbb{H}}(xy) = n_{\mathbb{H}}(x)n_{\mathbb{H}}(y)$ *for all* $x, y \in \mathbb{H}$.

Proof The only statement demanding a proof is the assertion that $\mathbb{H}$ is associative. But this can either be verified directly, or follows immediately from Exc. 1.16 combined with the Jacobi identity (1.1.4). □

1.13 Vista: spatial rotations. The Hamiltonian quaternions are widely used today to represent the attitude of a rigid body such as a spacecraft [166] or smart phone (e.g., via the class `CMAttitude` in the Apple iPhone API) and perhaps even a toothbrush [128].

The aim is to keep track of how the rigid body has rotated relative to some known starting orientation, represented by an element g in the group SO(3) of rotations of $\mathbb{R}^3$ about the origin. In earlier systems, g was represented using "Euler angles", which capture how much the body has rotated along three different axes, such as pitch, roll, and yaw. However, that approach suffers from various challenges.

The quaternionic approach is by keeping track of a *versor*, i.e., a quaternion $v \in \mathbb{H}$ with norm 1. It follows from 1.10 that the set V of versors is a

group. The conjugation action of the group V on the trace zero quaternions, $\mathbb{R}^3$, gives a surjective group homomorphism $V \to \mathrm{SO}(3)$ by Exercise 1.20, and one records a preimage v of g rather than g itself. This approach avoids some of the challenges of Euler angles (e.g., "gimbal lock") and makes it easy to smoothly interpolate between different attitudes by interpolating between versors, see, for example, [177, 58].

1.14 Vista: classifying real algebras. A famous theorem says that a finite-dimensional unital real algebra A endowed with a positive-definite quadratic from $n\colon A \to \mathbb{R}$ that permits composition is isomorphic to $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$. We prove this result in 23.13 below. There are many ways to go about proving this result: [198] and [38] provide recent and particularly elementary approaches, whereas §4 of [161] provides a proof that generalizes and is more in line with the historical development.

Varying the hypotheses somewhat leads to similar-sounding conclusions that can require very different techniques. One variation ignores the quadratic form and instead requires A to be alternative. It turns out that this seeming extra generality does not result in any additional algebras, see Exc. 19.30.

Another variation only asks for A to be a division algebra. It takes just a few lines to explicitly describe all the possibilities when $\dim A = 1$, so assume $\dim A > 1$. Exercise 1.15 shows that $\dim A$ is even. With a little topology, one can show that $\dim A$ must be a power of 2, see [124] or [119]. With a lot more work, the Bott-Milnor-Kervaire theorem [26, 150] says that A must have dimension 1, 2, 4, or 8. This relies on deep algebraic topology, and it is closely related to the fact that the only spheres that are parallelizable are those of dimension 0, 1, 3, or 7.

Within dimensions 2, 4, and 8, there is a whole zoo of division algebras. The 2-dimensional ones are classified in the sense that there is a short list of distinct isomorphism classes, albeit infinitely many since the entries in the list involve a parameter that can take uncountably many different values, see [125] and [66]. For the 4-dimensional or 8-dimensional division algebras, a dimension counting argument from "algebraic geography" shows that those algebras break up into uncountably many equivalence classes not just up to isomorphism but even up to a weaker equivalence relation known as isotopy, see [210, §5].

Later in this book, we will return to the notion of isotopy in slightly different contexts in sections 15 and 31.

Exercises

1.15. Suppose A is a finite-dimensional real division algebra. Prove that $\dim A$ is even or 1.

1.16. *The associator of* $\mathbb{O}$ (McCrimmon). The deviation of a real algebra A from being associative is measured by its *associator* $[x, y, z] := (xy)z - x(yz)$ for $x, y, z \in A$. Prove for $i = 1, 2, 3$ and $x_i := (a_i, u_i) \in \mathbb{O}$, $a_i \in \mathbb{C}$, $u_i \in \mathbb{C}^3$, that

$$[x_1, x_2, x_3] = \Big(\overline{\det(u_1, u_2, u_3)} - \det(u_1, u_2, u_3), \sum ((u_i \times u_j) \times \bar{u}_k + (\bar{u}_i \times \bar{u}_j)(a_k - \bar{a}_k))\Big),$$

where the sum on the right is extended over all cyclic permutations (ijk) of (123). Conclude that the associator of $\mathbb{O}$ is an alternating (trilinear) function of its arguments.

1.17. Prove without recourse to properties of the norm that $\mathbb{O}$ is a division algebra.

1.18. *Norm, trace and conjugation under the product of* $\mathbb{O}$.

(a) Prove that the conjugation of $\mathbb{O}$ is an (algebra) *involution*, i.e., not only $\bar{\bar{x}} = x$ but also $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in \mathbb{O}$.

(b) Show that trace and norm of $\mathbb{O}$ satisfy

$$t_{\mathbb{O}}(xy) = t_{\mathbb{O}}(yx), \quad t_{\mathbb{O}}((xy)z) = t_{\mathbb{O}}(x(yz)), \quad n_{\mathbb{O}}(x, z\bar{y}) = n_{\mathbb{O}}(xy, z) = n_{\mathbb{O}}(y, \bar{x}z)$$

for all $x, y, z \in \mathbb{O}$.

(c) Prove $x(\bar{x}y) = n_{\mathbb{O}}(x)y = (yx)\bar{x}$ and $xyx := (xy)x = x(yx) = n_{\mathbb{O}}(x, \bar{y})x - n_{\mathbb{O}}(x)\bar{y}$ for all $x, y \in \mathbb{O}$.

1.19. *The Moufang identities.* We will see later (cf. 13.3) that the Moufang identities

$$x(y(xz)) = (xyx)z, \quad (xy)(zx) = x(yz)x, \quad ((zx)y)x = z(xyx)$$

(cf. Exc. 1.18 (c) for a parentheses-saving notation) hold in arbitrary alternative algebras. Give a direct proof for the alternative algebra $\mathbb{O}$ by reducing to the case $y, z \in \{0\} \times \mathbb{C}^3$ and using as well as proving the *cross product identity*

$$(u \times v)w^{\mathsf{T}} + (v \times w)u^{\mathsf{T}} + (w \times u)v^{\mathsf{T}} = \det(u, v, w)\mathbf{1}_3 \tag{1}$$

for all $u, v, w \in \mathbb{C}^3$.

1.20. View $\mathbb{R}^3$ as the subspace of trace zero elements of $\mathbb{H}$ as in 1.11.

(a) For an angle θ and unit vector $u \in \mathbb{R}^3$, verify that $v = (\cos(\theta/2), \sin(\theta/2)u)$ is a versor, i.e., $n_{\mathbb{H}}(v) = 1$. Verify that all versors are of this form.

(b) For $s \in \mathbb{R}^3$, verify that

$$vsv^{-1} = s\cos\theta + (u \times s)\sin\theta + u(u \cdot s)(1 - \cos\theta). \tag{1}$$

Remark. Rodrigues' Rotation Formula says that the right side of (1) is the vector obtained from s by applying the rotation of $\mathbb{R}^3$ around the axis u through the angle θ. So by (b), the map $s \mapsto vsv^{-1}$ is in SO(3) and by (a) we find a group homomorphism $V \to \mathrm{SO}(3)$ of the group of versors to SO(3). Moreover, part (b) says that it is surjective, because every element of SO(3) is a rotation about some axis u by some angle θ by Euler's Rotation Theorem.

2 Cartan-Schouten bases

In 1.11 we have exhibited a basis for the Hamiltonian quaternions with a particularly simple family of structure constants. In this section, we will pursue the same objective for the Graves-Cayley octonions. Due to their higher dimension and the lack of associativity, however, matters will be not quite as simple as in the quaternionic case.

2.1 Defining Cartan-Schouten bases (Cartan-Schouten [45])**.** We define a *Cartan-Schouten basis* of $\mathbb{O}$ as a basis consisting of the identity element $1_{\mathbb{O}}$ and additional vectors $u_1, \dots, u_7 \in \mathbb{O}$ such that the following two conditions are fulfilled, for all $r = 1, \dots, 7$:

$$u_r^2 = -1_{\mathbb{O}}, \tag{1}$$

$$u_{r+i}u_{r+3i} = u_r = -u_{r+3i}u_{r+i} \qquad (i = 1, 2, 4), \tag{2}$$

where the indices in (2) are to be reduced mod 7. We then put $u_0 := 1_{\mathbb{O}}$, allowing us to write Cartan-Schouten bases as $(u_r)_{0 \le r \le 7}$. By (1) and (1.6.10), we have $t_{\mathbb{O}}(u_r) = 0$, hence $u_r \in \mathbb{O}^0$, for $1 \le r \le 7$. The conscientious reader may wonder whether equations (1), (2) really define a multiplication table for the basis chosen, i.e., whether all possible products between the basis vectors are well defined and uniquely determined by the preceding conditions. That this is indeed the case will be settled affirmatively in Exc. 2.7 below. We also note by Exc. 2.8 that Cartan-Schouten bases are orthonormal relative to the inner product $\langle x, y \rangle$ of (1.6.3). Finally, as an illustration of the connection between structure constants and isomorphisms explained in 1.2, we conclude from (1) and (2) that the linear map $\varphi\colon \mathbb{O} \to \mathbb{O}$ defined by $\varphi(u_r) = u_{r+1}$ ($1 \le r \le 7$, indices mod 7) is an automorphism of $\mathbb{O}$ having order 7.

2.2 Proposition. *Cartan-Schouten bases of* $\mathbb{O}$ *exist.*

Proof Let (u_1, u_2) be a pair of ortho-normal vectors in the seven-dimensional euclidean vector space $\mathbb{O}^0$. Then (1.6.13) yields

$$t_{\mathbb{O}}(u_1u_2) = n_{\mathbb{O}}(\bar{u}_1, u_2) = -n_{\mathbb{O}}(u_1, u_2) = 0,$$

hence $u_1u_2 \in \mathbb{O}^0$. Now let $u_3 \in \mathbb{O}^0$ be an orthonormal vector that is perpendicular to u_1, u_2, and u_1u_2. Then Exc. 2.8 shows that $u_0 = 1_{\mathbb{O}}, u_1, u_2, u_3, u_r := u_{r-3}u_{r-2}$ ($4 \le r \le 7$) make up a Cartan-Schouten basis of $\mathbb{O}$. □

There is a remarkable interplay between Cartan-Schouten bases and projective planes that provides a first glimpse at the profound connection between non-associative algebras and geometry; for more on this fascinating topic, we refer the reader to Faulkner [78]. Here we only sketch some details.

2.3 Incidence geometries. An *incidence geometry* consists of

(i) two disjoint sets $\mathcal{P}$, whose elements are called *points*, and $\mathcal{L}$, whose elements are called *lines*,
(ii) a relation between points and lines, i.e., a subset $I \subseteq \mathcal{P} \times \mathcal{L}$.

If $P \in \mathcal{P}$, $\ell \in \mathcal{L}$ satisfy $(P, \ell) \in I$, we say P is *incident to* ℓ (or P *lies on* ℓ, or ℓ *passes through* P). If several points all lie on a single line, they are said to be *collinear*.

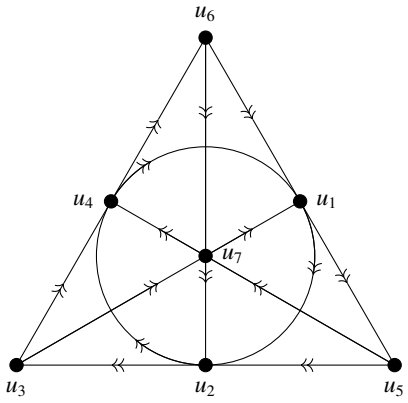
2.4 Projective planes. An incidence geometry as in 2.3 is called a *projective plane* if

(i) any two distinct points lie on a unique line,
(ii) any two distinct lines pass through a unique point,
(iii) there are four points no three of which are collinear.

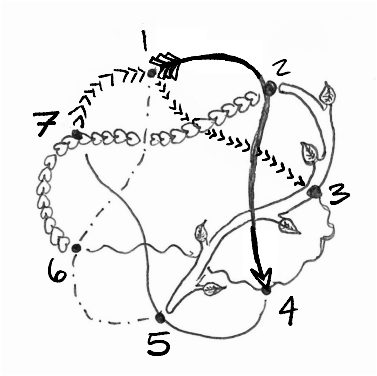
Important examples are provided by $\mathbb{P}^2(F)$, the projective plane of a field F: its points (resp. lines) are defined as the one-(resp. two-)dimensional subspaces of (three-dimensional column space) F^3 over F, and a point P is said to be incident with a line ℓ if $P \subseteq \ell$. Working with the canonical scalar product $(x, y) \mapsto x^{\mathsf{T}} y$ on F^3, it is clear that P (resp. ℓ) $\subseteq F^3$ is a point (resp. a line) if and only if $P^\perp$ (resp. $\ell^\perp$) $\subseteq F^3$ is a line (resp. a point), and P is incident to ℓ if and only if $\ell^\perp$ is incident to $P^\perp$. In particular, over a finite field F, there are as many points as there are lines in $\mathbb{P}^2(F)$.

2.5 The Fano plane and Cartan-Schouten bases. The *Fano plane* is the projective plane $\mathbb{P}^2(\mathbb{F}_2)$, where $\mathbb{F}_2$ stands for the field with two elements. The points of this geometry have the form $\{0, x\}$ with $0 \neq x \in \mathbb{F}_2^3$, hence identify canonically with the seven elements of $\mathbb{F}_2^3 \setminus \{0\}$, while the lines of this geometry have the form $\{0, x, y, x + y\}$, where $x, y \in \mathbb{F}_2^3 \setminus \{0\}$ are distinct points. Hence each line, of which there are seven by what we have seen in 2.4, consists of three points (besides 0) that are permuted cyclically under addition.

In the standard visualization of the Fano plane (see Fig. 2a(i)), its seven lines are represented by (i) the three sides, (ii) the three medians, and (iii) the inner circle of an equilateral triangle, while its seven points are located and numbered as shown. The entire picture fits into a directed graph whose nodes agree with the points of the Fano plane and give rise to subdivisions of the seven lines, yielding fifteen edges directed in the way indicated; for an artist's rendition of the Fano plane, see Fig. 2a(ii). The key feature of this construction is that one can use it to recover the Graves-Cayley octonions on the free *real* vector space generated by the nodes u_r, $1 \leq r \leq 7$, and an additional element u_0. In order to accomplish this, it suffices to define a multiplication on the



(i) A typical presentation.



(ii) An artist's presentation.

Figure 2a Two visualizations of the Fano plane.

basis vectors that enjoys the characteristic properties (2.1.1), (2.1.2) of Cartan-Schouten bases. We do so by setting $u_0 u_r := u_r =: u_r u_0$ for $0 \le r \le 7$, $u_r^2 = -u_0$ for $1 \le r \le 7$, and by defining $u_r u_s$ for $1 \le r, s \le 7$, $r \ne s$, in the following way: let u_t, $1 \le t \le 7$, be the third point on the line containing u_r and u_s. If, after an appropriate cyclic permutation of the indices r, s, t, the orientation of the edge joining u_r and u_s leads from u_r to u_s (resp. from u_s to u_r), we put $u_r u_s := u_t$ (resp. $u_r u_s := -u_t$). Then (2.1.1) holds by definition, while (2.1.2) can be verified in a straightforward manner.

We remark that these multiplication rules can alternatively be expressed in terms of Kirkman's $(7, 3, 1)$ block design, see [151] or [37] or [237], the last of which also contains alternative illustrations of the Fano plane.

2.6 Symmetries of the Graves-Cayley octonions. One of the most important features of the Graves-Cayley octonions is the fact that, in spite of their non-associative character, they have lots of symmetries. More specifically, we consider their automorphism group, denoted by $\mathrm{Aut}(\mathbb{O})$ and defined as the set of bijective linear maps $\varphi\colon \mathbb{O} \to \mathbb{O}$ satisfying $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in \mathbb{O}$; it is obviously a subgroup of $\mathrm{GL}(\mathbb{O})$, the full linear group of the real vector space $\mathbb{O}$. We know from Exc. 2.9 below that $\mathrm{Aut}(\mathbb{O})$ canonically embeds as a closed subgroup into the orthogonal group $\mathrm{O}(\mathbb{O}^0) \cong \mathrm{O}_7(\mathbb{R})$ of the euclidean vector space $\mathbb{O}^0$, a compact real Lie group of dimension 21, and hence is a compact real Lie group in its own right [51, Cor. of Prop. IV.XIV.2]. Our claim

that $\mathbb{O}$ has lots of symmetries will now be corroborated by the formula

$$\dim(\mathrm{Aut}(\mathbb{O})) = 14. \tag{1}$$

At this stage, we will not be able to give a rigorous proof of this formula; instead, we will confine ourselves to a naive dimension count making the formula intuitively plausible.

First of all, the automorphism group of $\mathbb{O}$ acts simply transitively on the set of Cartan-Schouten bases of $\mathbb{O}$. Each Cartan-Schouten basis, in turn, by Exc. 2.8 below, is completely determined by an element of

$$X^0 := \{(u_1, u_2, u_3) \in X \mid \langle u_1 u_2, u_3\rangle = 0\}, \tag{2}$$

where X stands for the set of orthonormal systems of length 3 in the euclidean vector space $\mathbb{O}^0 \cong \mathbb{R}^7$. Thus we have $\dim(\mathrm{Aut}(\mathbb{O})) = \dim(X^0)$. On the other hand, the orthogonal group $\mathrm{O}_7(\mathbb{R})$ acts transitively on X, and for the first three unit vectors $e_1, e_2, e_3 \in \mathbb{R}^7$, the isotropy group of $(e_1, e_2, e_3) \in X$ identifies canonically with $\mathrm{O}_4(\mathbb{R})$. Hence

$$\dim(X) = \dim(\mathrm{O}_7(\mathbb{R})) - \dim(\mathrm{O}_4(\mathbb{R})) = \frac{7\cdot 6}{2} - \frac{4\cdot 3}{2} = 21 - 6 = 15.$$

But (2) shows that X^0 is a "hypersurface" in X, which gives

$$\dim(\mathrm{Aut}(\mathbb{O})) = \dim(X^0) = \dim(X) - 1 = 14,$$

as claimed in (1).

Exercises

2.7. Put $M := \{r \in \mathbb{Z} \mid 1 \le r \le 7\} \times \{1, 2, 4\}$ and show for $s, t \in \mathbb{Z}$, $1 \le s, t \le 7$, that $s \ne t$ if and only if either there is a unique element $(r, i) \in M$ satisfying $r + i \equiv s \bmod 7$ and $r + 3i \equiv t \bmod 7$, or there is a unique element $(r, i) \in M$ satisfying $r + 3i \equiv s \bmod 7$ and $r + i \equiv t \bmod 7$.

2.8. *Characterization of Cartan-Schouten bases.* Prove for a family $(u_r)_{0\le r\le 7}$ of elements in $\mathbb{O}$ that the following conditions are equivalent.

(i) $(u_r)_{0\le r\le 7}$ is a Cartan-Schouten basis of $\mathbb{O}$.

(ii) $u_0 = 1_{\mathbb{O}}$ and

$$u_r^2 = -1_{\mathbb{O}} = (u_r u_{r+1})u_{r+3} = u_r(u_{r+1}u_{r+3}) \quad (1 \le r \le 7, \text{ indices mod } 7). \tag{1}$$

(iii) $u_0 = 1_{\mathbb{O}}$, and $(u_r)_{1\le r\le 7}$ is a basis of $\mathbb{O}^0$ such that $\|u_r\| = 1$ for $1 \le r \le 7$ and

$$u_{r+i}u_{r+3i} = u_r \qquad (1 \le r \le 7,\ i = 1, 2, 4, \text{ indices mod } 7). \tag{2}$$

(iv) $u_0 = 1_{\mathbb{O}}$, and (u_1, u_2, u_3) is an orthonormal system in the euclidean vector space $\mathbb{O}^0$ such that

$$n_{\mathbb{O}}(u_1u_2, u_3) = 0, \quad u_r = u_{r-3}u_{r-2} \qquad (4 \le r \le 7). \tag{3}$$

In this case, $(u_r)_{0\le r\le 7}$ is an orthonormal basis of $\mathbb{O}$ (relative to the inner product $\langle x, y\rangle$ of (1.5.3)).

2.9. *The algebra* $\mathbb{O}^+$. The real vector space $\mathbb{O}$ becomes a commutative real algebra $\mathbb{O}^+$ under the multiplication

$$x \cdot y := \frac{1}{2} x \circ y = \frac{1}{2} t_{\mathbb{O}}(x)y + \frac{1}{2} t_{\mathbb{O}}(y)x - \frac{1}{2} n_{\mathbb{O}}(x, y)1_{\mathbb{O}} \qquad (x, y \in \mathbb{O})$$

with identity element $1_{\mathbb{O}^+} := 1_{\mathbb{O}}$. Show that $\mathrm{Aut}(\mathbb{O}) \subseteq \mathrm{Aut}(\mathbb{O}^+)$ is a closed subgroup and that the assignment $\varphi \mapsto \varphi|_{\mathbb{O}^0}$ determines a topological isomorphism from $\mathrm{Aut}(\mathbb{O}^+)$ onto $\mathrm{O}(\mathbb{O}^0)$.

3 Unital subalgebras of $\mathbb{O}$ and their $\mathbb{Z}$-structures

The Graves-Cayley octonions, and the Hamiltonian quaternions as well, derive a considerable amount of their significance from the profound connections with seemingly unrelated topics in other areas of mathematics and physics. One of these connections pertains to the arithmetic theory of quadratic forms. Without striving for completeness or maximum generality, it will be briefly touched upon in the next two sections. Our results, incomplete as they are, underscore the need for an understanding of quaternion and octonion algebras not just over fields but, in fact, over arbitrary commutative rings.

3.1 The general set-up. (a) Throughout this section, we fix a real vector space V of finite dimension n and assume most of the time, but not always, that V is equipped with a positive definite quadratic form $q\colon V \to \mathbb{R}$. Speaking of (V, q) as a positive definite real quadratic space under these circumstances, we may and always will regard V as a euclidean vector space with the scalar product $\langle x, y\rangle := \frac{1}{2} q(x, y)$ and denote the associated euclidean norm by $\|x\| = \sqrt{\langle x, x\rangle} = \sqrt{q(x)}$, for all $x, y \in V$.

(b) We also denote by $\mathbb{D}$ one of the unital subalgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$ of $\mathbb{O}$. Via restriction, $\mathbb{D}$ inherits from $\mathbb{O}$ the data norm, trace, bilinearized norm and conjugation, denoted by $n_{\mathbb{D}}$, $t_{\mathbb{D}}$, $Dn_{\mathbb{D}}$, $\iota_{\mathbb{D}}$, respectively, that mutatis mutandis enjoy the various properties assembled in 1.6 for the Graves-Cayley octonions. These properties will be freely used here without further ado. In particular, $n_{\mathbb{D}}\colon \mathbb{D} \to \mathbb{R}$ is a positive definite quadratic form permitting composition, and $(\mathbb{D}, n_{\mathbb{D}})$ is a positive definite real quadratic space as in (a), allowing us to regard $\mathbb{D}$ as a euclidean subspace of $\mathbb{O}$ in a natural way.

3.2 Algebras over $\mathbb{Z}$ and $\mathbb{Q}$. There is nothing special about the base field $\mathbb{R}$ in the definition of an algebra. It may be replaced by any commutative associative

ring of scalars, a point of view adopted systematically in the remainder of the book. For example, we may pass to the field $\mathbb{Q}$ of rational numbers or the ring $\mathbb{Z}$ of integers: by a $\mathbb{Q}$-*algebra* (resp., a $\mathbb{Z}$-*algebra*) we mean a $\mathbb{Q}$-vector space (resp., an additive abelian group) A together with a $\mathbb{Q}$-bilinear (resp., a bi-additive) map from $A \times A$ to A. The conventions of 1.2 carry over to this modified setting virtually without change. Any real algebra may be viewed as a $\mathbb{Q}$-algebra (resp., a $\mathbb{Z}$-algebra) by *restriction of scalars*: rather than allowing scalar multiplication by arbitrary real numbers, one does so only by elements of $\mathbb{Q}$ (resp. $\mathbb{Z}$).

3.3 Power-associative algebras and the minimum polynomial. Let A be a finite-dimensional unital algebra over K, where either $K = \mathbb{R}$ or $K = \mathbb{Q}$. Powers of $x \in A$ with integer exponents ≥ 0 are defined inductively by $x^0 := 1_A$, $x^{n+1} := xx^n$ for $n \in \mathbb{N}$. We say A is *power-associative* if $x^{m+n} = x^m x^n$ for all $x \in A$, $m, n \in \mathbb{N}$, equivalently, if

$$K[x] := \sum_{n \in \mathbb{N}} Kx^n \subseteq A \tag{1}$$

is a unital commutative associative subalgebra, for all $x \in A$. When this holds, it makes sense to talk about the *minimum* (or *minimal*) *polynomial* of x (over K) in its capacity as an element of $K[x]$. It will be denoted by μ_x, or μ_x^K to indicate dependence on K, and is the unique monic polynomial in $K[\mathbf{t}]$ that generates the ideal of all polynomials in $K[\mathbf{t}]$ killing x.

The preceding considerations apply in particular to $K = \mathbb{R}$ and the real algebra $\mathbb{D}$; indeed, $\mathbb{D}$ is power-associative since, for $x \in \mathbb{D}$, we may invoke (1.6.10) to conclude that $\mathbb{R}[x] = \mathbb{R}1_{\mathbb{D}} + \mathbb{R}x \subseteq \mathbb{D}$ is a unital commutative associative subalgebra of dimension at most 2. Moreover, again by (1.6.10),

$$\mu_x = \mathbf{t}^2 - t_{\mathbb{D}}(x)\mathbf{t} + n_{\mathbb{D}}(x) \quad \Longleftrightarrow \quad x \notin \mathbb{R}1_{\mathbb{D}}, \tag{2}$$

while, of course, $\mu_{\alpha 1_{\mathbb{D}}} = \mathbf{t} - \alpha$ for $\alpha \in \mathbb{R}$.

3.4 Integral elements. Let A be a finite-dimensional unital power-associative algebra over $K = \mathbb{R}$ or $K = \mathbb{Q}$. An element $x \in A$ is said to be *integral* if $f(x) = 0$ for some monic polynomial $f \in \mathbb{Z}[\mathbf{t}]$. For example, x is integral if its minimal polynomial has integral coefficients. The converse of this also holds in important special cases.

3.5 Proposition. *Let A be a finite-dimensional unital power-associative algebra over $\mathbb{Q}$ and $x \in A$. Then the following conditions are equivalent.*

(i) *x is integral.*

(ii) *$\mathbb{Z}[x] := \sum_{n \in \mathbb{N}} \mathbb{Z}x^n$ is a finitely generated abelian group.*

(iii) $\mu_x \in \mathbb{Z}[\mathbf{t}]$.

Proof (i) $\Leftrightarrow$ (ii). Apply Bourbaki [27, V, §1, Thm. 1] or [271, Tag 052I] to $A := \mathbb{Z}$, $R := \mathbb{Z}[x]$.

(iii) $\Rightarrow$ (i). Clear.

(i) $\Rightarrow$ (iii). Apply [27, V, §1, Cor. of Prop. 11] to $A := \mathbb{Z}$, $K := \mathbb{Q}$, $K' := \mathbb{Q}[x]$ to conclude that the coefficients of $\mu_x \in \mathbb{Q}[\mathbf{t}]$ are integral over $\mathbb{Z}$. Hence (iii) holds since $\mathbb{Z}$ is integrally closed. □

3.6 Integral quadratic lattices and $\mathbb{Z}$-structures. (a) A subset $L \subseteq V$ is called a *lattice* in V if there exists a basis $(e_1, \dots, e_n)$ of V (as a real vector space) which is *associated with* L in the sense that

$$L = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n.$$

Then L is a free abelian group of rank n, and $\mathbb{Q}L := \mathbb{Q}e_1 \oplus \cdots \oplus \mathbb{Q}e_n$ is an n-dimensional vector space over $\mathbb{Q}$.

(b) By an *integral quadratic lattice* in (V, q) (or simply in V, the quadratic form q being understood) we mean a lattice $L \subseteq V$ such that $q(L) \subseteq \mathbb{Z}$, which after linearization implies $q(x, y) \in \mathbb{Z}$ for all $x, y \in L$.

(c) Let A be a finite-dimensional unital $\mathbb{R}$-algebra. A lattice L in A is said to be *unital* if $1_A \in L$. Note in particular that a unital integral quadratic lattice $L \subseteq \mathbb{D}$ satisfies $t_{\mathbb{D}}(L) \subseteq \mathbb{Z}$ and is stable under conjugation; in particular, the minimum polynomial of $x \in L$ by (3.3.2) has integer coefficients, so L consists entirely of integral elements.

(d) Let A be a finite-dimensional unital $\mathbb{R}$-algebra. By a $\mathbb{Z}$-*structure* of A we mean a unital lattice $M \subseteq A$ that is closed under multiplication ($M^2 \subseteq M$). $\mathbb{Z}$-structures $M \subseteq A$ are, in particular, unital $\mathbb{Z}$-algebras, more precisely, $\mathbb{Z}$-subalgebras of A. Note further that $\mathbb{Q}M$ is a unital $\mathbb{Q}$-subalgebra of A.

3.7 Lemma. *Let $L \subseteq V$ be a lattice. A family of elements in $\mathbb{Q}L$ that is linearly independent over $\mathbb{Q}$ is so over $\mathbb{R}$.*

Proof Let $(e_1, \dots, e_n)$ be a basis of V associated with L. If $x_1, \dots, x_m \in \mathbb{Q}L$ are linearly independent over $\mathbb{Q}$, they can be extended to a $\mathbb{Q}$-basis $(x_1, \dots, x_n)$ of $\mathbb{Q}L$. This implies $x_j = \sum_{i=1}^n \alpha_{ij} e_i$ for $1 \le j \le n$ and some matrix $(\alpha_{ij}) \in \mathrm{GL}_n(\mathbb{Q}) \subset \mathrm{GL}_n(\mathbb{R})$. Thus $(x_1, \dots, x_n)$ is an $\mathbb{R}$-basis of V, forcing $x_1, \dots, x_m$ to be linearly independent over $\mathbb{R}$. □

3.8 Proposition. *Let A be a finite-dimensional unital power-associative real algebra, L a unital lattice in A such that $\mathbb{Q}L \subseteq A$ is a subalgebra over $\mathbb{Q}$. Then*

$\mu_x^{\mathbb{R}} = \mu_x^{\mathbb{Q}}$ for all $x \in \mathbb{Q}L$, so the minimum polynomial of x over $\mathbb{R}$ agrees with the minimum polynomial of x over $\mathbb{Q}$. In particular, it belongs to $\mathbb{Q}[\mathbf{t}]$.

Proof By definition, $\mu_x^{\mathbb{R}}$ divides $\mu_x^{\mathbb{Q}}$ over $\mathbb{R}$. But both are monic polynomials in $\mathbb{R}[\mathbf{t}]$ of the same degree, by Lemma 3.7. Hence $\mu_x^{\mathbb{R}} = \mu_x^{\mathbb{Q}}$. □

3.9 Corollary. *Every $\mathbb{Z}$-structure M of $\mathbb{D}$ is a unital integral quadratic lattice.*

Proof Unitality being part of the definition, it remains to show $n_{\mathbb{D}}(x) \in \mathbb{Z}$ for all $x \in M$. First of all, $\mathbb{Q}M$ is a finite-dimensional unital power-associative $\mathbb{Q}$-algebra containing x, and μ_x as given in 3.3 is the minimum polynomial of x over $\mathbb{Q}$ (Prop. 3.8). On the other hand, let $\mathbb{Z}[x] = \sum_{n\geq 0} \mathbb{Z}x^n$ be the unital subalgebra of M generated by x. Since M is finitely generated as a $\mathbb{Z}$-module, so is $\mathbb{Z}[x] \subseteq M$. Thus x is integral over $\mathbb{Z}$ (Proposition 3.5). By Proposition 3.5 again and (3.3.2), this implies $n_{\mathbb{D}}(x) \in \mathbb{Z}$, as claimed. □

3.10 Basis transitions. If $E = (e_1, \dots, e_n)$ is an ordered basis of V, then so is $E^S = (e'_1, \dots, e'_n)$, $e'_j := \sum_{i=1}^n s_{ij} e_i$, $1 \leq j \leq n$, for any invertible real n-by-n matrix $S = (s_{ij})$. In this way, $\mathrm{GL}_n(\mathbb{R})$ acts on the set of bases of V from the right in a *simply transitive* manner, so any two bases E, E' of V allow a unique $S \in \mathrm{GL}_n(\mathbb{R})$ such that $E^S = E'$. We call S the *transition matrix* from E to E'.

Let $E := (e_1, \dots, e_n)$ be an $\mathbb{R}$-basis of V. Then we write

$$Dq(E) := \big(q(e_i, e_j)\big)_{1\leq i,j\leq n} \in \mathrm{Mat}_n(\mathbb{R}) \tag{1}$$

for the matrix of the symmetric bilinear form $Dq\colon V \times V \to \mathbb{R}$ relative to the basis E. Along with Dq, the matrix $Dq(E)$ is also positive definite. Given $S \in \mathrm{GL}_n(\mathbb{R})$, it is well known and easily checked that

$$Dq(E^S) = S^{\mathsf{T}} Dq(E) S. \tag{2}$$

If L is an integral quadratic lattice in V and the basis E is associated with L, then the positive definite matrix $Dq(E)$ has integral coefficients and its diagonal entries are even.

3.11 Proposition. *Let $L \subseteq V$ be an integral quadratic lattice and E an $\mathbb{R}$-basis of V that is associated with L. Then*

$$\det(L) := \det\big(Dq(E)\big)$$

is a positive integer that only depends on L and not on the basis chosen.

Proof Since $Dq(E)$ belongs to $\mathrm{Mat}_n(\mathbb{Z})$, its determinant is an integer, which must be positive since $Dq(E)$ is positive definite. The transition matrix from

E to another basis E' of V associated with L not only has integral coefficients but is also unimodular, i.e., has determinant ± 1. Now (3.10.2) shows $\det(Dq(E')) = \det(Dq(E))$. □

3.12 The discriminant. Let L be an integral quadratic lattice of V. The quantity $\det(L)$ exhibited in Proposition 3.11 is called the *determinant* of L; it is a positive integer. Following Kneser [156, 10.1, p. 43], on the other hand, the non-zero (possibly negative) integer

$$\operatorname{disc}(L) := (-1)^{\lfloor \frac{n}{2} \rfloor} \det(L)$$

is called the *discriminant* of L. By a *unimodular* integral quadratic lattice of V we mean an integral quadratic lattice of discriminant ± 1.

3.13 Proposition. *Let $L' \subseteq L$ be integral quadratic lattices of V. Then L/L' is finite and* $\operatorname{disc}(L') = [L : L']^2 \operatorname{disc}(L)$.

Proof Let E (resp. E') be an $\mathbb{R}$-basis of V associated with L (resp. L') and S the transition matrix from E to E'. Then $S \in \mathrm{Mat}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{R})$, and the Elementary Divisor Theorem [141, Thm. 3.8] implies that there exist $P, Q \in \mathrm{GL}_n(\mathbb{Z})$ and a chain of successive non-zero integral divisors $d_1 | \cdots | d_n$ satisfying $S = P \operatorname{diag}(d_1, \ldots, d_n) Q$. Replacing E' by E'^T, $T := Q^{-1}$, and E by E^P, we may assume $S = \operatorname{diag}(d_1, \ldots, d_n)$. With $E = (e_1, \ldots, e_n)$ this implies $E' = E^S = (d_1 e_1, \ldots, d_n e_n)$, and

$$L/L' \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})$$

is finite of order $\prod_{i=1}^n |d_i|$. On the other hand, applying Proposition 3.11 and (3.10.2), we conclude

$$\begin{aligned} \operatorname{disc}(L') &= (-1)^{\lfloor \frac{n}{2} \rfloor} \det\left(Dq(E^S)\right) = (-1)^{\lfloor \frac{n}{2} \rfloor} \Big(\prod_{i=1}^n d_i\Big)^2 \det\left(Dq(E)\right) \\ &= [L : L']^2 \operatorname{disc}(L), \end{aligned}$$

as claimed. □

3.14 Corollary. *A unimodular integral quadratic lattice of V is maximal in the sense that it is not contained in any other integral quadratic lattice of V.* □

3.15 Remark. The preceding observations apply in particular to $\mathbb{Z}$-structures of $\mathbb{D}$. For example, a $\mathbb{Z}$-structure of $\mathbb{D}$ that is unimodular (as an integral quadratic lattice) is maximal as an integral quadratic lattice by Corollary 3.14, hence as a $\mathbb{Z}$-structure as well (Cor. 3.9).

3.16 Examples. Let M be a $\mathbb{Z}$-structure and E an orthonormal basis of $\mathbb{D}$ (as a euclidean real vector space). If E is associated with M, then (3.10.1) shows $Dn_{\mathbb{D}}(E) = 2 \cdot \mathbf{1}_r$, $r := \dim_{\mathbb{R}}(\mathbb{D})$, and we conclude

$$\operatorname{disc}(M) = (-1)^{\lfloor \frac{r}{2} \rfloor} 2^r. \tag{1}$$

We now consider a number of specific cases.

(a) By Exc. 3.19 below, $M := \mathbb{Z}$ is the unique $\mathbb{Z}$-structure of $\mathbb{D} := \mathbb{R}$, and we have $\operatorname{disc}(\mathbb{Z}) = 2$.

(b) The *Gaussian integers* $\operatorname{Ga}(\mathbb{C}) := \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ are a $\mathbb{Z}$-structure of $\mathbb{D} := \mathbb{C}$, and we have $\operatorname{disc}(\operatorname{Ga}(\mathbb{C})) = -2^2 = -4$. The Gaussian integers are the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ [203, Thm. 1.5]. Hence Corollary 3.9 shows that they form a maximal $\mathbb{Z}$-structure.

(c) In (1.11.1) we have exhibited an orthonormal basis $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ of $\mathbb{D} := \mathbb{H}$, with structure constants by (1.11.3) equal to ± 1. Thus

$$\operatorname{Ga}(\mathbb{H}) := \mathbb{Z}1_{\mathbb{H}} \oplus \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus \mathbb{Z}\mathbf{k} \tag{2}$$

is a $\mathbb{Z}$-structure of $\mathbb{H}$ having discriminant $\operatorname{disc}(\operatorname{Ga}(\mathbb{H})) = 2^4 = 16$. We call $\operatorname{Ga}(\mathbb{H})$ the *Gaussian integers* of $\mathbb{H}$. (Some authors call $\operatorname{Ga}(\mathbb{H})$ the Lipschitz quaternions.)

(d) Let $E = (u_r)_{0 \le r \le 7}$ be a Cartan-Schouten basis of $\mathbb{D} := \mathbb{O}$. From Exc. 2.8 we deduce that E is an orthonormal basis of $\mathbb{O}$, while (2.1.1), (2.1.2) show that the corresponding structure constants are ± 1. Hence

$$\operatorname{Ga}(\mathbb{O}) := \operatorname{Ga}_E(\mathbb{O}) := \bigoplus_{r=0}^{7} \mathbb{Z}u_r \tag{3}$$

is a $\mathbb{Z}$-structure of $\mathbb{O}$ having discriminant $\operatorname{disc}(\operatorname{Ga}(\mathbb{O})) = 2^8 = 256$. We call $\operatorname{Ga}(\mathbb{O})$ the *Gaussian integers* of $\mathbb{O}$ relative to E.

Exercises

3.17. Prove for an additive subgroup $L \subseteq V$ that the following conditions are equivalent.

(i) L is a lattice.
(ii) L spans V as a real vector space and is a free abelian group of rank at most $\dim_{\mathbb{R}}(V)$.
(iii) There are lattices $L_0, L_1 \subseteq V$ such that $L_0 \subseteq L \subseteq L_1$.

3.18. Let M be a $\mathbb{Z}$-structure of $\mathbb{D}$. Show that there exists an additive subgroup of $\mathbb{D}$ properly containing M that is free of finite rank and closed under multiplication but *not* a $\mathbb{Z}$-structure of $\mathbb{D}$.

3.19. Let M be a $\mathbb{Z}$-structure of $\mathbb{D}$. Prove $M \cap \mathbb{R} = \mathbb{Z}$. (*Hint*: Note that M is a discrete additive subgroup of $\mathbb{D}$ under the natural topology and that the non-zero discrete additive subgroups of $\mathbb{R}$ have the form $\mathbb{Z}v$ for some non-zero element $v \in \mathbb{R}$.)

4 Maximal quaternionic and octonionic $\mathbb{Z}$-structures

Contrary to the Gaussian integers in $\mathbb{C}$, their simple-minded analogues in $\mathbb{H}$ and $\mathbb{O}$ (cf. 3.16 (c),(d)) are *not* maximal $\mathbb{Z}$-structures. In fact, they will be enlarged to maximal ones in the present section.

4.1 Towards the Hurwitz $\mathbb{Z}$-structure of $\mathbb{H}$. Starting out from the orthonormal basis $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ of $\mathbb{H}$ exhibited in (1.11.2), we put

$$\mathbf{h} := \frac{1}{2}(1_{\mathbb{H}} + \mathbf{i} + \mathbf{j} + \mathbf{k}) \in \mathbb{H} \tag{1}$$

and note

$$n_{\mathbb{H}}(\mathbf{h}) = t_{\mathbb{H}}(\mathbf{h}) = n_{\mathbb{H}}(\mathbf{i}, \mathbf{h}) = n_{\mathbb{H}}(\mathbf{j}, \mathbf{h}) = n_{\mathbb{H}}(\mathbf{k}, \mathbf{h}) = 1. \tag{2}$$

After an obvious identification, we can realize the complex numbers via

$$\mathbb{C} := \mathbb{R}[\mathbf{i}] = \mathbb{R}1_{\mathbb{H}} \oplus \mathbb{R}\mathbf{i} \tag{3}$$

as a subalgebra of $\mathbb{H}$, which satisfies the relation

$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}\mathbf{h} \tag{4}$$

as a direct sum of subspaces. To see this, it suffices to show that the sum on the right of (4) is direct, so let $u, v \in \mathbb{C}$ and suppose $u = v\mathbf{h}$. If $v \neq 0$, then $\mathbf{h} = v^{-1}u \in \mathbb{C}$, a contradiction. Thus $u = v = 0$, as desired. Note that

$$\mathrm{Ga}(\mathbb{C}) = \mathbb{Z}[\mathbf{i}] = \mathbb{Z}1_{\mathbb{H}} \oplus \mathbb{Z}\mathbf{i} \tag{5}$$

after the identification carried out in (3).

4.2 Theorem (Hurwitz [127])**.** *With the notation and assumptions of 4.1,*

$$\mathrm{Hur}(\mathbb{H}) := \mathrm{Ga}(\mathbb{C}) \oplus \mathrm{Ga}(\mathbb{C})\mathbf{h} \tag{1}$$

is a $\mathbb{Z}$-structure and a maximal integral quadratic lattice of $\mathbb{H}$, called its $\mathbb{Z}$-structure of (or simply the) Hurwitz quaternions. $\mathrm{Hur}(\mathbb{H})$ *contains the Gaussian integers of $\mathbb{H}$ as a sub-$\mathbb{Z}$-structure and has discriminant* 4*:*

$$\mathrm{Ga}(\mathbb{H}) \subseteq \mathrm{Hur}(\mathbb{H}), \quad \mathrm{disc}\,(\mathrm{Hur}(\mathbb{H})) = 4. \tag{2}$$

Moreover, $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{h}, \mathbf{ih})$ *and* $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{h})$ *are $\mathbb{R}$-bases of $\mathbb{H}$ that are both associated with* $\mathrm{Hur}(\mathbb{H})$.

Proof Since $\mathbb{H}$ is a division algebra by Corollary 1.12, the map $\mathbb{H} \to \mathbb{H}$, $x \mapsto x\mathbf{h}$, is bijective. Combining (4.1.4), (4.1.5) with (1), we therefore conclude that $M := \mathrm{Hur}(\mathbb{H}) \subseteq \mathbb{H}$ is a unital lattice and that $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{h}, \mathbf{ih})$ is an $\mathbb{R}$-basis of $\mathbb{H}$ associated with M.

Next we prove that M is closed under multiplication. Let $u \in \mathrm{Ga}(\mathbb{C})$. Then (1.6.12) implies $u\mathbf{h} + \mathbf{h}u = t_{\mathbb{H}}(u)\mathbf{h} + t_{\mathbb{H}}(\mathbf{h})u - n_{\mathbb{H}}(u, \mathbf{h})1_{\mathbb{H}}$, where the coefficients of the linear combination on the right by (4.1.2) are all integers. Hence $M = \mathrm{Ga}(\mathbb{C}) \oplus \mathbf{h}\,\mathrm{Ga}(\mathbb{C})$. We conclude $\mathrm{Ga}(\mathbb{C})\mathbf{h}\,\mathrm{Ga}(\mathbb{C}) \subseteq \mathrm{Ga}(\mathbb{C})^2 + \mathrm{Ga}(\mathbb{C})^2\mathbf{h} = M$, and (1.6.10), (4.1.2) imply

$$\begin{aligned}\mathrm{Ga}(\mathbb{C})\mathbf{h}\,\mathrm{Ga}(\mathbb{C})\mathbf{h} \subseteq M\mathbf{h} &= \mathrm{Ga}(\mathbb{C})\mathbf{h} + \mathrm{Ga}(\mathbb{C})\mathbf{h}^2 \\ &= \mathrm{Ga}(\mathbb{C})\mathbf{h} + \mathrm{Ga}(\mathbb{C})(\mathbf{h} - 1_{\mathbb{H}}) \subseteq \mathrm{Ga}(\mathbb{C}) \oplus \mathrm{Ga}(\mathbb{C})\mathbf{h} = M.\end{aligned}$$

Thus M is indeed multiplicatively closed and hence a $\mathbb{Z}$-structure of $\mathbb{H}$. Since

$$\mathbf{ih} = \frac{1}{2}(\mathbf{i} - 1_{\mathbb{H}} + \mathbf{k} - \mathbf{j}) = -(1_{\mathbb{H}} + \mathbf{j} - \mathbf{h}),$$

we see that $E := (1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{h})$ is another $\mathbb{R}$-basis of $\mathbb{H}$ associated with M. In particular, $\mathrm{Ga}(\mathbb{H}) \subseteq M$ (since $\mathbf{k} = 2\mathbf{h} - 1_{\mathbb{H}} - \mathbf{i} - \mathbf{j}$) and

$$Dn_{\mathbb{H}}(E) = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$

Subtracting the arithmetic mean of the first two rows from the fourth, we conclude

$$\mathrm{disc}(M) = \det \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = 4 \cdot (2 - 1) = 4.$$

(Alternately, note that $\mathrm{Hur}(\mathbb{H})/\mathrm{Ga}(\mathbb{H}) = \mathbb{Z}/2$, so by Prop. 3.13,

$$16 = \mathrm{disc}\,\mathrm{Ga}(\mathbb{H}) = 2^2\,\mathrm{disc}(\mathrm{Hur}(\mathbb{H})),$$

yielding $\mathrm{disc}(\mathrm{Hur}(\mathbb{H})) = 4$.) It remains to show that M is a maximal integral quadratic lattice of $\mathbb{H}$, which we leave as an exercise (Exc. 4.9). □

4.3 Remark. The Hurwitz quaternions are endowed with a rich arithmetic structure that has been investigated extensively in the literature. For example, it is possible to derive Jacobi's famous formula [129], [130, pp. 238-9] for the number of ways a positive integer can be expressed as a sum of four (integral) squares in a purely arithmetic fashion by appealing to properties of

the Hurwitz quaternions [127, p. 335]. The reader may consult Brandt [35] or Conway-Smith [55, Ch. 5] for further details on the subject. There are also profound connections with the theory of automorphic forms, cf. Krieg [164] for a systematic and essentially self-contained study of this topic.

In the second part of the present section, we will imitate our approach to the Hurwitz quaternions on the octonionic level. This will lead us to a $\mathbb{Z}$-structure of $\mathbb{O}$ that is not only maximal but even, remarkably, a unimodular integral quadratic lattice.

4.4 Towards the Dickson-Coxeter octonions. In 1.11, we have defined the Hamiltonian quaternions $\mathbb{H}$ explicitly as a unital subalgebra of $\mathbb{O}$. For our subsequent considerations, it will be important to select a different realization of this kind, depending on the choice of a Cartan-Schouten basis $E = (u_r)_{0\leq r\leq 7}$ of $\mathbb{O}$ that will remain fixed throughout the rest of this section. Recall from Exc. 2.8 that E is an orthonormal basis of $\mathbb{O}$ obeying the multiplication rules (2.1.2) which may be conveniently read off from Fig. 2a on page 12.

In particular, we have the relations $u_1u_2 = u_4$, $u_2u_4 = u_1$, $u_4u_1 = u_2$, which show that the Hamiltonian quaternions may also be identified via

$$\mathbb{H} = \mathbb{R}1_{\mathbb{O}} \oplus \mathbb{R}u_1 \oplus \mathbb{R}u_2 \oplus \mathbb{R}u_4 \tag{1}$$

as a unital subalgebra of $\mathbb{O}$ under the matching $1_{\mathbb{H}} = 1_{\mathbb{O}}$, $\mathbf{i} = u_1$, $\mathbf{j} = u_2$, $\mathbf{k} = u_4$. This obviously implies

$$\mathrm{Ga}(\mathbb{H}) = \mathbb{Z}1_{\mathbb{O}} \oplus \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \mathbb{Z}u_4 \tag{2}$$

for the Gaussian integers of $\mathbb{H}$. We now put

$$\mathbf{p} := \frac{1}{2}(1_{\mathbb{O}} + u_1 + u_2 + u_3) \in \mathbb{O} \tag{3}$$

and note

$$u_1\mathbf{p} = \frac{1}{2}(-1_{\mathbb{O}} + u_1 + u_4 + u_7), \tag{4}$$

$$u_2\mathbf{p} = \frac{1}{2}(-1_{\mathbb{O}} + u_2 - u_4 + u_5), \tag{5}$$

$$u_3\mathbf{p} = \frac{1}{2}(-1_{\mathbb{O}} + u_3 - u_5 - u_7), \tag{6}$$

$$u_4\mathbf{p} = \frac{1}{2}(-u_1 + u_2 + u_4 - u_6) \tag{7}$$

as well as

$$n_{\mathbb{O}}(\mathbf{p}) = t_{\mathbb{O}}(\mathbf{p}) = n_{\mathbb{O}}(u_1, \mathbf{p}) = n_{\mathbb{O}}(u_2, \mathbf{p}) = n_{\mathbb{O}}(u_3, \mathbf{p}) = 1, \quad n_{\mathbb{O}}(u_4, \mathbf{p}) = 0. \tag{8}$$

We also claim

$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H}\mathbf{p}, \tag{9}$$

which will follow once we have shown that the sum on the right is direct. Indeed, suppose $u = v\mathbf{p} \neq 0$ for some $u, v \in \mathbb{H}$. Then Exc. 1.18 (c) yields $n_{\mathbb{O}}(v)\mathbf{p} = \bar{v}(v\mathbf{p}) = \bar{v}u \in \mathbb{H}$, hence $\mathbf{p} \in \mathbb{H}$, a contradiction to (1), (3).

4.5 Theorem (Dickson [64], Coxeter [56])**.** *With the notation and assumptions of 4.4,*

$$\mathrm{DiCo}(\mathbb{O}) := \mathrm{DiCo}_E(\mathbb{O}) := \mathrm{Ga}(\mathbb{H}) \oplus \mathrm{Ga}(\mathbb{H})\mathbf{p} \tag{1}$$

is a $\mathbb{Z}$-structure and a positive definite unimodular integral quadratic lattice of $\mathbb{O}$, called its $\mathbb{Z}$-structure of (or simply the) Dickson-Coxeter octonions *(relative to E).* $\mathrm{DiCo}(\mathbb{O})$ *contains the Gaussian integers of $\mathbb{O}$ as a sub-$\mathbb{Z}$-structure, and*

$$E' := (1_{\mathbb{O}}, u_1, u_2, u_4, \mathbf{p}, u_1\mathbf{p}, u_2\mathbf{p}, u_4\mathbf{p}) \tag{2}$$

is an $\mathbb{R}$-basis of $\mathbb{O}$ associated with $\mathrm{DiCo}(\mathbb{O})$.

Proof From (4.4.9) and (1) we deduce that $M := \mathrm{DiCo}(\mathbb{O})$ is a unital lattice in $\mathbb{O}$ and E' as defined in (2) is an $\mathbb{R}$-basis of $\mathbb{O}$ associated with M.

Now we show that the lattice M is integral quadratic. Indeed, from (4.4.8) we obtain $n_{\mathbb{O}}(\mathrm{Ga}(\mathbb{H}), \mathbf{p}) \subseteq \mathbb{Z}$. But then, given $u, v \in \mathrm{Ga}(\mathbb{H})$, we may apply Exc. 1.18 (c) as well as Thm. 1.8 and (4.4.3) to conclude

$$n_{\mathbb{O}}(u + v\mathbf{p}) = n_{\mathbb{O}}(u) + n_{\mathbb{O}}(u, v\mathbf{p}) + n_{\mathbb{O}}(v\mathbf{p}) = n_{\mathbb{O}}(u) + n_{\mathbb{O}}(\bar{v}u, \mathbf{p}) + n_{\mathbb{O}}(v) \in \mathbb{Z},$$

as claimed. Moreover, consulting (4.4.3)–(4.4.7), we see that $\mathrm{Ga}(\mathbb{O}) \subseteq M$, so M contains the Gaussian integers of $\mathbb{O}$.

Our next aim is to prove that M is a $\mathbb{Z}$-structure of $\mathbb{O}$, which will follow once we have shown that it is closed under multiplication, equivalently, that

$$\mathrm{Ga}(\mathbb{H})\,(\mathrm{Ga}(\mathbb{H})\mathbf{p}) \subseteq M, \tag{3}$$

$$(\mathrm{Ga}(\mathbb{H})\mathbf{p})\,\mathrm{Ga}(\mathbb{H}) \subseteq M, \tag{4}$$

$$(\mathrm{Ga}(\mathbb{H})\mathbf{p})\,(\mathrm{Ga}(\mathbb{H})\mathbf{p}) \subseteq M. \tag{5}$$

Noting that M is a unital integral quadratic lattice, we first let $u \in \mathrm{Ga}(\mathbb{H})$ and apply (1.6.12) to obtain

$$u\mathbf{p} + \mathbf{p}u = t_{\mathbb{O}}(u)\mathbf{p} + t_{\mathbb{O}}(\mathbf{p})u - n_{\mathbb{O}}(u, \mathbf{p})1_{\mathbb{O}} = (u - n_{\mathbb{O}}(u, \mathbf{p})1_{\mathbb{O}}) + t_{\mathbb{O}}(u)\mathbf{p},$$

which in view of (1.6.6) implies

$$u\mathbf{p} + \mathbf{p}u \equiv t_{\mathbb{O}}(u)\mathbf{p} \bmod \mathrm{Ga}(\mathbb{H}), \tag{6}$$

$$\mathbf{p}u \equiv \bar{u}\mathbf{p} \bmod \mathrm{Ga}(\mathbb{H}). \tag{7}$$

Now let $u, v \in \mathbb{H}$. Linearizing the first alternative law in 1.7 and using (6), (7) as well as Exc. 1.18 (a), we obtain

$$\begin{aligned} u(\mathbf{p}v) &\equiv (u\mathbf{p} + \mathbf{p}u)v - \mathbf{p}(uv) \equiv t_{\mathbb{O}}(u)\mathbf{p}v - \mathbf{p}(uv) \\ &\equiv \mathbf{p}(\bar{u}v) \equiv (\bar{v}u)\mathbf{p} \bmod \mathrm{Ga}(\mathbb{H}), \end{aligned}$$

hence $u(\mathbf{p}v) \in M$. But then (3) follows since $u(v\mathbf{p}) \equiv u(\mathbf{p}\bar{v}) \bmod \mathrm{Ga}(\mathbb{H})$ by (7). On the other hand,

$$\begin{aligned} (v\mathbf{p})u &= u(v\mathbf{p}) + (v\mathbf{p})u - u(v\mathbf{p}) \\ &= t_{\mathbb{O}}(u)v\mathbf{p} + t_{\mathbb{O}}(v\mathbf{p})u - n_{\mathbb{O}}(u, v\mathbf{p})1_{\mathbb{O}} - u(v\mathbf{p}), \end{aligned}$$

which by (3) proves (4). And finally, by (7), (3), Exc. 1.19 and Exc. 1.18 (c),

$$(u\mathbf{p})(v\mathbf{p}) \equiv (\mathbf{p}\bar{u})(v\mathbf{p}) \equiv \mathbf{p}(\bar{u}v)\mathbf{p} \equiv n_{\mathbb{O}}(\mathbf{p}, \bar{v}u)\mathbf{p} - n_{\mathbb{O}}(\mathbf{p})\bar{v}u \equiv 0 \bmod M,$$

which proves (5).

It remains to show that M is unimodular as an integral quadratic lattice. To this end, we compute the matrix $Dn_{\mathbb{O}}(E')$. Applying 1.9 gives $n_{\mathbb{O}}(u_r\mathbf{p}, u_s\mathbf{p}) = n_{\mathbb{O}}(u_r, u_s) = 2 \cdot \delta_{rs}$, so $Dn_{\mathbb{O}}(E')$ is the block matrix

$$\begin{pmatrix} 2 \cdot \mathbf{1}_4 & T \\ T^{\mathsf{T}} & 2 \cdot \mathbf{1}_4 \end{pmatrix},$$

where $T := (n_{\mathbb{O}}(u_r, u_s\mathbf{p}))_{r,s\in\{0,1,2,4\}}$ by (4.4.3)–(4.4.7) has the form

$$T = \begin{pmatrix} 1 & -1 & -1 & 0 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & 1 \end{pmatrix} \in \mathrm{Mat}_4(\mathbb{Z}).$$

One checks immediately that the columns of T all have euclidean length $\sqrt{3}$ and are mutually orthogonal. Hence Exc. 4.10 below implies $\det(Dn_{\mathbb{O}}(E')) = (2^2 - 3)^4 = 1$, and the proof of the theorem is complete. □

4.6 Vista: even positive definite inner product spaces. One of the key notions dominating the arithmetic theory of quadratic forms is that of a unimodular integral quadratic lattice as defined in 3.6 (b), which is studied, e.g., in Milnor-Husemoller [197] (see also Serre [259] or Kneser [156]), under the name "even positive definite inner product space over $\mathbb{Z}$". A prominent and particularly important example is furnished by the integral quadratic lattice underlying the Dickson-Coxeter octonions. In order to appreciate the significance of this example, we record the following facts.

(a) Every even positive definite inner product space over $\mathbb{Z}$ splits uniquely into the orthogonal sum of indecomposable subspaces [197, (6.4)].

(b) The rank of an even positive definite inner product space over $\mathbb{Z}$ is divisible by 8 [197, (5.1)].

(c) There exists an even positive definite inner product space of rank 8 over $\mathbb{Z}$ [197, (6.1)] which is unique up to isomorphism [255, Appendix 4, p. 399].

The integral quadratic lattice in (c), discovered independently by Smith [263] and Korkine-Zolotarev [162], is the root lattice of the root system E_8 and is therefore called the E_8-*lattice*. By (a), (b) above, the E_8-lattice is indecomposable, while uniqueness in (c) shows that it is isomorphic to the integral quadratic lattice underlying the Dickson-Coxeter octonions. We refer to Exc. 4.13 below for more details.

4.7 Remarks. (a) Since the automorphism group of $\mathbb{O}$ acts simply transitively on the set of Cartan-Schouten bases of $\mathbb{O}$, the Dickson-Coxeter octonions up to isomorphism do not depend on the Cartan-Schouten basis chosen.

(b) The similarity of our approach to the Hurwitz quaternions on the one hand and to the Dickson-Coxeter octonions on the other is not accidental: in [219], a purely algebraic formalism has been developed that contains both of these constructions as special cases.

(c) The reader is referred to Van der Blij-Springer [286] and Conway-Smith [55, Chap. 9–11] for a detailed study of arithmetic properties of the Dickson-Coxeter octonions. Concerning a purely arithmetic approach to a Jacobi-type formula for the number of ways a positive integer may be expressed as a sum of eight squares using the Dickson-Coxeter octonions, the reader may consult Rehm [248].

Exercises

4.8. *Characterization of the Hurwitz quaternions by congruence conditions.* Prove

$$\mathrm{Hur}(\mathbb{H}) = \{m1_{\mathbb{H}} + n\mathbf{i} + p\mathbf{j} + q\mathbf{k} \mid m,n,p,q \in \mathbb{Z} \text{ or } m,n,p,q \in \frac{1}{2} + \mathbb{Z}\}.$$

4.9. Complete the proof of Theorem 4.2 by showing that the Hurwitz quaternions form a maximal integral quadratic lattice in $\mathbb{H}$: if $L \subseteq \mathbb{H}$ is an integral quadratic lattice containing $\mathrm{Hur}(\mathbb{H})$, then $L = \mathrm{Hur}(\mathbb{H})$.

4.10. *A determinant formula.* Let p, q be positive integers and r, s be positive real num-

bers. Prove for matrices $T_1 \in \mathrm{Mat}_{p,q}(\mathbb{R})$, $T_2 \in \mathrm{Mat}_{q,p}(\mathbb{R})$ that the matrix

$$S := \begin{pmatrix} r \cdot \mathbf{1}_p & T_1 \\ T_2 & s \cdot \mathbf{1}_q \end{pmatrix} \in \mathrm{Mat}_{p+q}(\mathbb{R})$$

has determinant $\det(S) = r^{p-q}\,\mathrm{char}_{T_2T_1}(rs)$, where "char" stands for the characteristic polynomial of a square matrix. Conclude in the special case $T_1 = T$, $T_2 = T^{\mathsf{T}}$, where all the columns of $T \in \mathrm{Mat}_{p,q}(\mathbb{R})$ are assumed to have euclidean length $\sqrt{a}$ for some $a > 0$ and to be mutually orthogonal, that $\det(S) = r^{p-q}(rs-a)^q$ and that S is positive definite if $a < rs$. What happens if we drop the assumption of the columns of T all having the same euclidean length but retain the one that they be mutually orthogonal?

4.11. *Units of $\mathbb{Z}$-structures.* (a) Let M be a $\mathbb{Z}$-structure of $\mathbb{D}$, where $\mathbb{D}$ is one of the unital subalgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ of $\mathbb{O}$. Show for $u \in M$ that the following conditions are equivalent.

(i) u is a *left unit* or *left invertible* in M: $vu = 1_{\mathbb{D}}$ for some $v \in M$.
(ii) u is a *right unit* or *right invertible* in M: $uv = 1_{\mathbb{D}}$ for some $v \in M$.
(iii) $n_{\mathbb{D}}(u) = 1$.

In this case, u is said to be a *unit* of (or *invertible*) in M; moreover, the quantity v in (ii) (resp. (iii)) is unique and $v = \bar{u}$. Conclude that $M^\times$, the set of units of M, contains $1_{\mathbb{D}}$ and is closed under multiplication as well as under taking inverses.

(b) Determine the units of the Gaussian integers in $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ and of the Hurwitz quaternions.

Remark. The notions of this exercise should be seen within the more general context of alternative algebras: for invertibility (resp. one-sided invertibility), see 13.4 (resp. Exc. 14.10) below.

4.12 (Loos)**.** *Alternate description of the Hurwitz quaternions.* Show with

$$\varepsilon_1 := \frac{1}{2}(\mathbf{j}-\mathbf{k}), \quad \varepsilon_2 := -\frac{1}{2}(\mathbf{j}+\mathbf{k}), \quad \varepsilon_3 := \frac{1}{2}(1_{\mathbb{H}}+\mathbf{i}), \quad \varepsilon_4 := -\frac{1}{2}(1_{\mathbb{H}}-\mathbf{i})$$

that $(\varepsilon_i)_{1\le i\le 4}$ is an orthonormal basis of $\mathbb{H}$ relative to the modified euclidean scalar product $2\langle x, y\rangle = n_{\mathbb{H}}(x, y)$ and that

$$\mathrm{Hur}(\mathbb{H}) = \mathbb{Z}(\varepsilon_1-\varepsilon_2) \oplus \mathbb{Z}(\varepsilon_2-\varepsilon_3) \oplus \mathbb{Z}(\varepsilon_3-\varepsilon_4) \oplus \mathbb{Z}(\varepsilon_3+\varepsilon_4).$$

Conclude

$$\mathrm{Hur}(\mathbb{H}) = \{\sum_{i=1}^{4} \xi_i\varepsilon_i \mid \xi_i \in \mathbb{Z}\ (1 \le i \le 4), \quad \sum_{i=1}^{4} \xi_i \in 2\mathbb{Z}\}$$

and

$$\mathrm{Hur}(\mathbb{H})^\times = \{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \le i < j \le 4\}.$$

Remark. This exercise shows that $\mathrm{Hur}(\mathbb{H})$ is the root lattice of the root system D_4, while $\mathrm{Hur}(\mathbb{H})^\times$ consists precisely of the roots of that system. See 47.12 or [31, Plate IV] for more details.

4.13 (Loos)**.** *Alternate description of the Dickson-Coxeter octonions and their units.* Let $E = (u_r)_{0\le r\le 7}$ be a Cartan-Schouten basis of $\mathbb{O}$.

(a) Show with

$$\varepsilon_1 := \frac{1}{2}(-u_0+u_2),\quad \varepsilon_2 := \frac{1}{2}(u_0+u_2),\quad \varepsilon_3 := -\frac{1}{2}(u_1+u_3),\quad \varepsilon_4 := \frac{1}{2}(u_1-u_3),$$
$$\varepsilon_5 := \frac{1}{2}(-u_4+u_5),\quad \varepsilon_6 := \frac{1}{2}(u_4+u_5),\quad \varepsilon_7 := \frac{1}{2}(u_6-u_7),\quad \varepsilon_8 := \frac{1}{2}(u_6+u_7)$$

that $(\varepsilon_i)_{1\le i\le 8}$ is an orthonormal basis of $\mathbb{O}$ relative to the euclidean scalar product $2\langle x,y\rangle = n_{\mathbb{O}}(x,y)$.

(b) Conclude that $\mathrm{DiCo}(\mathbb{O})$ is the additive subgroup of $\mathbb{O}$ generated by the expressions

$$\pm\varepsilon_i \pm \varepsilon_j,\quad \frac{1}{2}\sum_{i=1}^{8} s_i\varepsilon_i, \tag{1}$$

where $1 \le i < j \le 8$ for the first type of (1), while $(s_i)_{1\le i\le 8}$ in the second type of (1) varies over the elements of $\{\pm 1\}^8$ such that the number of indices $i = 1,\dots,8$ having $s_i = -1$ is even.

(c) Show further that

$$\mathrm{DiCo}(\mathbb{O}) = \{\sum_{i=1}^{8}\xi_i\varepsilon_i \mid \xi_i\in\mathbb{R},\ 2\xi_i, \xi_i-\xi_j\in\mathbb{Z}\ (1\le i,j\le 8),\quad \sum_{i=1}^{8}\xi_i\in 2\mathbb{Z}\}. \tag{2}$$

(d) Deduce from (c) that the units of $\mathbb{O}$ are precisely the elements listed in (1) and that there are exactly 240 of them.

(*Hint*: In order to derive (b) (resp. (c)), show that the additive subgroup of $\mathbb{O}$ generated by the elements in (1) (resp. by the right-hand side of (2)) is an integral quadratic lattice of $\mathbb{O}$ containing $\mathrm{DiCo}(\mathbb{O})$.)

Remark. The elements of (1) are precisely the roots of the root system E_8 and, therefore, $\mathrm{DiCo}(\mathbb{O})$ is the corresponding root lattice. See 47.12 or [31, Plate VIII] for more details.

4.14 (Kirmse [152])**.** *The Kirmse lattice*. Let $E := (u_r)_{0\le r\le 7}$ be a Cartan-Schouten basis of $\mathbb{O}$. Show that

$$\mathrm{Kir}(\mathbb{O}) := \mathrm{Kir}_E(\mathbb{O}) := \mathrm{Ga}(\mathbb{O}) + \sum_{i=1}^{4}\mathbb{Z}v_i$$

with

$$v_1 := \frac{1}{2}(1_{\mathbb{O}}+u_1+u_2+u_4),\quad v_2 := \frac{1}{2}(u_3+u_5-u_6-u_7),$$
$$v_3 := \frac{1}{2}(1_{\mathbb{O}}+u_1+u_3-u_7),\quad v_4 := \frac{1}{2}(1_{\mathbb{O}}+u_2+u_3+u_5)$$

is a unital unimodular integral quadratic lattice in $\mathbb{O}$ which, however, contrary to what has been claimed in [152, p. 70], is *not* a $\mathbb{Z}$-structure of $\mathbb{O}$. (*Hint*: Consider the product v_1v_3.)

Remark. It follows from 4.7 that $\mathrm{Kir}(\mathbb{O})$ is isomorphic to the Dickson-Coxeter octonions as an integral quadratic lattice, hence, by what has been shown in Exercise 4.13 (d), must have exactly 240 units, in agreement with [152, p. 76].

The following exercise may be viewed as a corrected version of Kirmse's approach to the construction of "integer octonions".

4.15. *An alternate model of the Dickson-Coxeter octonions.* Let $(u_i)_{0\le i\le 7}$ be a Cartan-Shouten basis of $\mathbb{O}$ and put

$$v_1 := \frac{1}{2}(1_{\mathbb{O}} + u_1 + u_2 + u_4), \quad v_2 := \frac{1}{2}(1_{\mathbb{O}} + u_1 + u_5 + u_6),$$
$$v_3 := \frac{1}{2}(1_{\mathbb{O}} + u_1 + u_3 + u_7), \quad v_4 := \frac{1}{2}(u_1 + u_2 + u_3 + u_5).$$

Then show that

$$R := \mathrm{Ga}(\mathbb{O}) + \sum_{i=1}^{4} \mathbb{Z}v_i \subseteq \mathbb{O}$$

is a $\mathbb{Z}$-structure isomorphic to the Dickson-Coxeter octonions.

4.16. Show that there is an embedding of the Hurwitz quaternions into the Dickson-Coxeter octonions as $\mathbb{Z}$-algebras.

5 The euclidean Albert algebra

In the present section, we define the euclidean Albert algebra and derive some of its most basic properties. In doing so, we rely heavily on the Graves-Cayley octonions but also on rudiments from the theory of real Jordan algebras, which will be developed here from scratch.

5.1 The standard subalgebras of $\mathbb{O}$. Throughout this section, we fix a positive integer n and, as in 3.1, we write $\mathbb{D}$ for one of the four unital subalgebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ of $\mathbb{O}$. We also put $d := \dim_{\mathbb{R}}(\mathbb{D})$. As explained more fully in 3.1, the algebra $\mathbb{D}$ inherits its unit element, norm, trace, and conjugation from $\mathbb{O}$ via restriction. We identify the base field $\mathbb{R}$ canonically inside $\mathbb{D}$ via $\mathbb{R} = \mathbb{R}1_{\mathbb{D}} = \mathbb{R}1_{\mathbb{O}}$. Note by (1.6.7) that only the elements of $\mathbb{R}$ remain fixed under the conjugation of $\mathbb{D}$.

5.2 Hermitian matrices over $\mathbb{D}$. We denote by $\mathrm{Mat}_n(\mathbb{D})$ the real vector space of n-by-n matrices with entries in $\mathbb{D}$. It becomes a real algebra under ordinary matrix multiplication, with identity element given by $\mathbf{1}_n$, the n-by-n identity matrix. This algebra is associative for $\mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}$, but highly non-associative for $\mathbb{D} = \mathbb{O}$. One checks easily that the map

$$\mathrm{Mat}_n(\mathbb{D}) \longrightarrow \mathrm{Mat}_n(\mathbb{D}), \quad x \longmapsto \bar{x}^{\mathsf{T}}, \tag{1}$$

is an involution, i.e., it is $\mathbb{R}$-linear, gives the identity when applied twice, and satisfies the relations

$$\overline{xy}^{\mathsf{T}} = \bar{y}^{\mathsf{T}}\bar{x}^{\mathsf{T}} \qquad (x, y \in \mathrm{Mat}_n(\mathbb{D})). \tag{2}$$

We speak of the *conjugate transpose involution* in this context and denote by

$$\mathrm{Her}_n(\mathbb{D}) := \{x \in \mathrm{Mat}_n(\mathbb{D}) \mid x = \bar{x}^{\mathsf{T}}\} \tag{3}$$

the set of elements in $\mathrm{Mat}_n(\mathbb{D})$ that are hermitian in the sense that they remain fixed under the conjugate transpose involution. Note by the conventions of 5.1 that the diagonal entries of $x \in \mathrm{Her}_n(\mathbb{D})$ are all scalars, and so $\mathrm{Her}_n(\mathbb{D}) \subseteq \mathrm{Mat}_n(\mathbb{D})$ is a real subspace of dimension

$$\dim_{\mathbb{R}}(\mathrm{Her}_n(\mathbb{D})) = n + \frac{n(n-1)}{2}d. \tag{4}$$

The ordinary matrix units e_{ij}, $1 \le i, j \le n$, of $\mathrm{Mat}_n(\mathbb{D})$ canonically induce *primitive hermitian matrices* in $\mathrm{Her}_n(\mathbb{D})$ according to the rules

$$u[jl] := ue_{jl} + \bar{u}e_{lj} \qquad (u \in \mathbb{D},\ 1 \le j, l \le n,\ j \ne l). \tag{5}$$

5.3 The symmetric matrix product. The conjugate transpose involution by (5.2.2) does *not* preserve multiplication and hence the subspace $\mathrm{Her}_n(\mathbb{D}) \subseteq \mathrm{Mat}_n(\mathbb{D})$ is *not* a subalgebra. In order to remedy this deficiency, we pass from ordinary matrix multiplication to the *symmetric matrix product*

$$x \bullet y := \frac{1}{2}(xy + yx) \qquad (x, y \in \mathrm{Mat}_n(\mathbb{D})). \tag{1}$$

The ensuing real algebra, denoted by $\mathrm{Mat}_n(\mathbb{D})^+$, continues to be unital, with identity element $\mathbf{1}_n$, is obviously commutative, but fails to be associative even if $\mathbb{D}$ is.

On the positive side, the conjugate transpose involution, again by (5.2.2), does preserve multiplication of $\mathrm{Mat}_n(\mathbb{D})^+$, allowing us to conclude that $\mathrm{Her}_n(\mathbb{D})$ *becomes a unital commutative real algebra under the symmetric matrix product* and is, in fact, a unital subalgebra of $\mathrm{Mat}_n(\mathbb{D})^+$. Note that, thanks to the factor $\frac{1}{2}$ on the right-hand side of (1), the squarings of $\mathrm{Mat}_n(\mathbb{D})$ and of $\mathrm{Mat}_n(\mathbb{D})^+$ in the sense of 1.2 coincide and via restriction induce the squaring of $\mathrm{Her}_n(\mathbb{D})$.

The algebra $\mathrm{Her}_1(\mathbb{D})$ is none other than $\mathbb{R}$ itself. The algebra $\mathrm{Her}_2(\mathbb{D})$ is a Jordan algebra (Exc. 5.16). It belongs to a class of Jordan algebras that will later be referred to as "Jordan algebras of pointed quadratic modules" or "Jordan algebras of Clifford type" as defined in 29.12, see Cor. 37.3 below. The next case leads us to the heart of the present volume.

5.4 The case $n = 3$. The formalism described in 5.2, 5.3 will become particularly important for $n = 3$. The unital subalgebra $\mathrm{Her}_3(\mathbb{D}) \subseteq \mathrm{Mat}_3(\mathbb{D})^+$ by (5.2.4) has dimension

$$\dim_{\mathbb{R}} (\mathrm{Her}_3(\mathbb{D})) = 3(d+1) \tag{1}$$

and consists of the elements

$$x = \begin{pmatrix} \alpha_1 & u_3 & \bar{u}_2 \\ \bar{u}_3 & \alpha_2 & u_1 \\ u_2 & \bar{u}_1 & \alpha_3, \end{pmatrix} = \sum (\alpha_i e_{ii} + u_i[jl]) \quad (\alpha_i \in \mathbb{R},\ u_i \in \mathbb{D},\ 1 \le i \le 3), \tag{2}$$

where the sum on the very right is extended over all cyclic permutations $(i\,jl)$ of (123). As will be seen in due course, the structure of this algebra becomes extremely delicate for $\mathbb{D} = \mathbb{O}$.

5.5 Enter the euclidean Albert algebra. The real algebra

$$\mathrm{Her}_3(\mathbb{O})$$

of 3-by-3 hermitian matrices with entries in the Graves-Cayley octonions under the symmetric matrix product is called the *euclidean Albert algebra*[1]. It is commutative, contains an identity element and by (5.4.1) has dimension 27.

In order to obtain a proper understanding of the algebras $\mathrm{Her}_3(\mathbb{D})$, in particular of the euclidean Albert algebra, it will be crucial to connect them with the theory of Jordan algebras. We will do so in the remainder of this section.

5.6 Real and euclidean Jordan algebras. By a *real Jordan algebra* we mean a real algebra J (the term "real" being understood if there is no danger of confusion) satisfying the following identities, for all $x, y \in J$.

$$xy = yx \qquad \text{(commutative law)}, \tag{1}$$

$$x(x^2y) = x^2(xy) \qquad \text{(Jordan identity)}. \tag{2}$$

A real Jordan algebra J is said to be *euclidean* if, for all positive integers m, the equation $\sum_{r=1}^{m} x_r^2 = 0$ has only the trivial solution in J:

$$\forall x_1, \dots, x_m \in J: \quad \Big(\sum_{r=1}^{m} x_r^2 = 0 \quad \Longrightarrow \quad x_1 = \cdots = x_m = 0 \Big). \tag{3}$$

5.7 Special and exceptional real Jordan algebras. (a) Standard examples of real Jordan algebras are easy to construct: let A be an associative real algebra

[1] The prefix "euclidean" will be explained in 5.6 below.

with multiplication $(x, y) \mapsto xy$. Then it is readily checked that, in analogy to (5.3.1), the symmetric product

$$x \bullet y := \frac{1}{2}(xy + yx) \tag{1}$$

converts A into a Jordan algebra, which we denote by A^+. It follows that every subalgebra of A^+, which may or may not be one of A, is a Jordan algebra. Jordan algebras that are isomorphic to a subalgebra of A^+, for some associative algebra A, are said to be *special*, while non-special Jordan algebras are called *exceptional*.

(b) The real algebras $\mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ are all associative. Hence so is $\mathrm{Mat}_n(\mathbb{D})$, and we deduce from 5.3 that $\mathrm{Her}_n(\mathbb{D})$ is a special Jordan algebra. By contrast, the preceding argument breaks down for $\mathbb{D} = \mathbb{O}$ since $\mathbb{O}$ is not associative. In fact, while $\mathrm{Her}_3(\mathbb{O})$ continues to be a Jordan algebra, as a delicate argument in Theorem 5.10 below will show, it will be an exceptional one (Albert [3]). Moreover, $\mathrm{Her}_n(\mathbb{O})$ for $n > 3$ is not even a Jordan algebra anymore (Exc. 5.16).

(c) Our principal aim in the present section will be to show in a unified fashion that $\mathrm{Her}_3(\mathbb{D})$, for any $\mathbb{D}$, including $\mathbb{D} = \mathbb{O}$, is a euclidean Jordan algebra, thereby justifying the terminology of 5.5. We do so not by following Albert's original approach [3] but by adopting an idea of Springer [267], according to which some fundamental properties of ordinary 3-by-3 matrices over a field survive in the algebra $\mathrm{Her}_3(\mathbb{D})$.

5.8 Norm, trace and adjoint of $\mathrm{Her}_3(\mathbb{D})$. As in (5.4.2), the elements of $J := \mathrm{Her}_3(\mathbb{D})$ will be written systematically as

$$x = \sum (\alpha_i e_{ii} + u_i[jl]), \quad y = \sum (\beta_i e_{ii} + v_i[jl]), \tag{1}$$

where $\alpha_i, \beta_i \in \mathbb{R}$, $u_i, v_i \in \mathbb{D}$ for $1 \le i \le 3$, and unadorned summations will always be taken over the cyclic permutations (ijl) of (123). Then we define the *norm* $N := N_J : J \to \mathbb{R}$, the *trace* $T := T_J : J \to \mathbb{R}$ and the *adjoint* $\sharp : J \to J$, $x \mapsto x^\sharp$, by the formulas

$$N(x) := \alpha_1\alpha_2\alpha_3 - \sum \alpha_i n_{\mathbb{D}}(u_i) + t_{\mathbb{D}}(u_1u_2u_3), \tag{2}$$

$$T(x) := \sum \alpha_i, \tag{3}$$

$$x^\sharp := \sum \Big((\alpha_j\alpha_l - n_{\mathbb{D}}(u_i))e_{ii} + (-\alpha_i u_i + \overline{u_j u_l})[jl] \Big). \tag{4}$$

By Exc. 1.18 (b), the final term on the right of (2) is unambiguous. Moreover, the norm N is a cubic form, i.e., after choosing a basis of $\mathrm{Her}_3(\mathbb{D})$ as a real vector space, N is represented by a homogeneous polynomial of degree 3 in d variables. Similarly, the trace T is a linear form, while the adjoint is a real

quadratic map in the sense of 1.3. In particular, the expression $x \times y := (x + y)^\sharp - x^\sharp - y^\sharp$ is (symmetric) bilinear in x, y. More precisely,

$$x \times y = \sum \Big((\alpha_j\beta_l + \beta_j\alpha_l - n_{\mathbb{D}}(u_i, v_i))e_{ii} + (-\alpha_i v_i - \beta_i u_i + \overline{u_j v_l + v_j u_l})[jl] \Big). \tag{5}$$

Finally, we put

$$S(x) := T(x^\sharp) = \sum (\alpha_j\alpha_l - n_{\mathbb{D}}(u_i)) \tag{6}$$

and note that $S := S_J \colon J \to \mathbb{R}$ is a quadratic form with bilinearization given by

$$S(x, y) := DS(x, y) = T(x \times y) = \sum (\alpha_j\beta_l + \beta_j\alpha_l - n_{\mathbb{D}}(u_i, v_i)). \tag{7}$$

5.9 Fundamental identities. (a) For finite-dimensional real vector spaces V, W, equipped with the natural topology, a non-empty open subset $U \subseteq V$ and a smooth map $F \colon U \to W$ (e.g., a polynomial map), we write $DF(u)(x)$ for the directional derivative of F at $u \in U$ in the direction $x \in V$. Thus $DF(u)(x) \in W$ agrees with the factor of $t \in \mathbb{R}$, $|t|$ sufficiently small, in the Taylor expansion of $F(u + tx)$. For example, given a quadratic map $Q \colon V \to W$, we have $DQ(u)(x) = DQ(u, x)$ for $u, x \in J$, where the right-hand side is to be understood in the sense of 1.3.

(b) For arbitrary elements

$$x = \sum (\alpha_i e_{ii} + u_i[jl]), \quad y = \sum (\beta_i e_{ii} + v_i[jl]) \tag{1}$$

and z of $J := \mathrm{Her}_3(\mathbb{D})$, with $\alpha_i, \beta_i \in \mathbb{R}$, $u_i, v_i \in \mathbb{D}$, $1 \le i \le 3$, we denote by

$$x^3 := x \bullet x^2 = \frac{1}{2}(xx^2 + x^2x) \tag{2}$$

the *cube*, i.e., the third power, of x in J (which in general is not the same as its cube in $\mathrm{Mat}_3(\mathbb{D})$, see Exc. 36.11, (2)) and claim that the identities in 5a hold. Verifying them is either straightforward or part of Exc. 5.15 below.

5.10 Theorem. $\mathrm{Her}_3(\mathbb{D})$ *is a unital euclidean Jordan algebra.*

Proof We know from 5.3 that the algebra $J := \mathrm{Her}_3(\mathbb{D})$ is unital and commutative, so our first aim must be to establish the Jordan identity (5.6.2). To this end, we combine (5a.9) with (5a.5), (5a.7) and obtain

$$x^2 \bullet y = 2T(x)x \bullet y + T(y)x^2 - 2x \bullet (x \bullet y) - S(x)y - (T(x)T(y) - T(x \bullet y))x + (T(x^2 \bullet y) - T(x)T(x \bullet y) + S(x)T(y))\mathbf{1}_3. \tag{1}$$

$$x^2 = \sum \Big((\alpha_i^2 + n_{\mathbb{D}}(u_j) + n_{\mathbb{D}}(u_l))e_{ii} + ((\alpha_j + \alpha_l)u_i + \overline{u_j u_l})[jl] \Big) \quad (1)$$

$$x \bullet y = \sum \Big((\alpha_i\beta_i + \frac{1}{2} n_{\mathbb{D}}(u_j, v_j) + \frac{1}{2} n_{\mathbb{D}}(u_l, v_l))e_{ii} + \frac{1}{2}((\alpha_j + \alpha_l)v_i + (\beta_j + \beta_l)u_i + \overline{u_j v_l + v_j u_l})[jl] \Big) \quad (2)$$

$$T(x \bullet y) = \sum (\alpha_i\beta_i + n_{\mathbb{D}}(u_i, v_i)) \quad (3)$$

$$T((x \bullet y) \bullet z) = T(x \bullet (y \bullet z)) \quad (4)$$

$$S(x, y) = T(x)T(y) - T(x \bullet y) \quad (5)$$

$$x^\sharp = x^2 - T(x)x + S(x)\mathbf{1}_3 \quad (6)$$

$$DN(x)(y) = T(x^\sharp \bullet y) = T(x^2 \bullet y) - T(x)T(x \bullet y) + S(x)T(y) \quad (7)$$

$$x^3 = T(x)x^2 - S(x)x + N(x)\mathbf{1}_3 \quad (8)$$

$$x^2 \bullet y = 2T(x)x \bullet y + T(y)x^2 - S(x)y - S(x, y)x + DN(x)(y)\mathbf{1}_3 - 2x \bullet (x \bullet y) \quad (9)$$

Table of Identities 5a Identities for elements $x, y, z \in \mathrm{Her}_3(\mathbb{D})$.

Multiplying this equation by x, we conclude

$$\begin{aligned} x \bullet (x^2 \bullet y) = {} & 2T(x)x \bullet (x \bullet y) + T(y)x^3 - 2x \bullet (x \bullet (x \bullet y)) \\ & - S(x)x \bullet y - (T(x)T(y) - T(x \bullet y))x^2 \\ & + (T(x^2 \bullet y) - T(x)T(x \bullet y) + S(x)T(y))x. \end{aligned} \quad (2)$$

On the other hand, replacing y by $x \bullet y$ in (1) and applying (5a.4), we deduce

$$\begin{aligned} x^2 \bullet (x \bullet y) = {} & 2T(x)x \bullet (x \bullet y) + T(x \bullet y)x^2 - 2x \bullet (x \bullet (x \bullet y)) \\ & - S(x)x \bullet y - \Big(T(x)T(x \bullet y) - T(x \bullet (x \bullet y))\Big)x \\ & + \Big(T(x^2 \bullet (x \bullet y)) - T(x)T(x \bullet (x \bullet y)) + S(x)T(x \bullet y)\Big)\mathbf{1}_3 \\ = {} & 2T(x)x \bullet (x \bullet y) + T(x \bullet y)x^2 - 2x \bullet (x \bullet (x \bullet y)) \\ & - S(x)x \bullet y - (T(x)T(x \bullet y) - T(x^2 \bullet y))x \\ & + (T(x^3 \bullet y) - T(x)T(x^2 \bullet y) + S(x)T(x \bullet y))\mathbf{1}_3 \end{aligned}$$

Subtracting this from (2) and applying (5a.8) twice now yields

$$\begin{aligned} x \bullet (x^2 \bullet y) - x^2 \bullet (x \bullet y) = {} & T(y)x^3 - T(x)T(y)x^2 + S(x)T(y)x \\ & - T\Big((x^3 - T(x)x^2 + S(x)x) \bullet y\Big)\mathbf{1}_3 \\ = {} & T(y)(x^3 - T(x)x^2 + S(x)x - N(x)\mathbf{1}_3) = 0, \end{aligned}$$

and the Jordan identity holds. Thus J is a real Jordan algebra. To establish that it is euclidean is now anti-climactic: let m be a positive integer, $x_r = \sum(\alpha_{ir}e_{ii} + u_{ir}[jl]) \in J$ with $\alpha_{ir} \in \mathbb{R}$, $u_{ir} \in \mathbb{D}$ for $1 \le r \le m$, $1 \le i \le 3$, and suppose $\sum_r x_r^2 = 0$. Since some of the diagonal entries on the right-hand side of (5a.1) are strictly positive unless $x = 0$, we conclude $x_1 = \cdots = x_m = 0$, as claimed. □

5.11 Cubic euclidean Jordan matrix algebras. The algebras $\mathrm{Her}_3(\mathbb{D})$ are called *cubic euclidean Jordan matrix algebras*. This terminology is justified by Theorem 5.10 combined with (5a.8).

5.12 Corollary. *Let $x \in \mathrm{Her}_3(\mathbb{D})$. Then*

$$\mathbb{R}[x] := \mathbb{R}\mathbf{1}_3 + \mathbb{R}x + \mathbb{R}x^2 \subseteq \mathrm{Her}_3(\mathbb{D})$$

is a unital commutative associative subalgebra. In particular, $\mathrm{Her}_3(\mathbb{D})$ is power-associative.

Proof Since $x \bullet x^2 = x^3$ by (5a.2), we have $x \bullet \mathbb{R}[x] \subseteq \mathbb{R}[x]$ by (5a.8). Now the Jordan identity yields

$$(x^2)^2 = x^2 \bullet (x \bullet x) = x \bullet (x \bullet x^2) \in x \bullet (x \bullet \mathbb{R}[x]) \subseteq \mathbb{R}[x]. \tag{1}$$

Thus $\mathbb{R}[x] \subseteq J := \mathrm{Her}_3(\mathbb{D})$ is a unital subalgebra. While commutativity is inherited from J, associativity may be checked on the spanning set $\mathbf{1}_3, x, x^2$ of $\mathbb{R}[x]$ as a real vector space, where it is either obvious or a consequence of (1), resp. the Jordan identity. The final assertion follows immediately from the definition 3.3. □

5.13 The minimum polynomial. (a) As in 3.3, we denote by $\mu_x \in \mathbb{R}[\mathbf{t}]$ the minimum polynomial of x in the finite-dimensional unital power-associative real algebra $J := \mathrm{Her}_3(\mathbb{D})$. From (5a.8) we deduce

$$\mu_x = \mathbf{t}^3 - T(x)\mathbf{t}^2 + S(x)\mathbf{t} - N(x) \quad \Longleftrightarrow \quad \mathbf{1}_3 \wedge x \wedge x^2 \neq 0 \ \text{ in } \ \bigwedge\nolimits^3(J). \tag{1}$$

Note that since J is power-associative (Cor. 5.12) and euclidean (Thm. 5.10), it contains no nilpotent elements other than zero.

5.14 Corollary. *The minimum polynomial of $x \in \mathrm{Her}_3(\mathbb{D})$ splits into distinct linear factors over $\mathbb{R}$. We have*

$$1 \le m := \deg(\mu_x) = \dim_{\mathbb{R}}(\mathbb{R}[x]) \le 3,$$

and there exists a basis $(c_r)_{1\le r\le m}$ of $\mathbb{R}[x]$ as a real vector space that up to order

is uniquely determined by the conditions

$$c_r \bullet c_s = \delta_{rs} c_r \quad (1 \le r, s \le m) \quad \text{and} \quad \sum_{r=1}^{m} c_r = \mathbf{1}_3. \tag{1}$$

Proof Write μ for the product of the distinct irreducible factors of μ_x. Then μ_x divides μ^n for some positive integer n, which implies $\mu(x)^n = 0$. But $J := \mathrm{Her}_3(\mathbb{D})$ does not contain non-zero nilpotent elements (5.13). Hence $\mu(x) = 0$, and we conclude that $\mu_x = \mu$ has only simple irreducible factors over $\mathbb{R}$. Suppose one of these has degree 2. Then $\mathbb{C}$, by the Chinese Remainder Theorem [271, Tag 00DT], becomes a (possibly non-unital) subalgebra of $\mathbb{R}[x]$. It is euclidean because J is, contradicting the equation $1^2 + i^2 = 0$ in $\mathbb{C}$. Thus μ_x splits into distinct linear factors, and applying the Chinese Remainder Theorem again yields quantities c_r, $1 \le r \le m$, with the desired properties. It remains to prove uniqueness up to order. Let (d_r) be another basis of $\mathbb{R}[x]$ satisfying (1) after the obvious notational adjustments. Then, with indices always varying over $\{1, 2, 3\}$, we have $d_r = \sum_s \alpha_{rs} c_s$ for some $u := (\alpha_{rs}) \in \mathrm{GL}_3(\mathbb{R})$, and $d_r^2 = d_r$ yields $\alpha_{rs} \in \{0, 1\}$. On the other hand, $\sum_r d_r = \mathbf{1}_3$ amounts to $\sum_r \alpha_{rs} = 1$. Hence, given s, there is a unique index $\pi(s)$ such that $\alpha_{rs} = \delta_{r\pi(s)}$. Assuming $\pi(s) = \pi(s')$ for some $s \ne s'$ would therefore imply the contradiction that two distinct columns of $u \in \mathrm{GL}_3(\mathbb{R})$ are presented by the same vector in $\mathbb{R}^3$. Thus π is a permutation of $\{1, \dots, m\}$ and $c_r = d_{\pi(r)}$ for all r. □

Exercises

5.15. Verify the identities in 5a on page 33.

5.16. Show for a positive integer n that $\mathrm{Her}_n(\mathbb{O})$ under the symmetric matrix product is a Jordan algebra if and only if $n \le 3$. (*Hint*: Prove by repeated linearization, equivalently, by repeatedly taking directional derivatives, that a real Jordan algebra J satisfies the *fully linearized Jordan identity* $u((vw)x) + v((wu)x) + w((uv)x) = (uv)(wx) + (vw)(ux) + (wu)(vx)$ for all $u, v, w, x \in J$.)

5.17. *Invertibility in* $\mathrm{Her}_3(\mathbb{D})$. Let $x \in J := \mathrm{Her}_3(\mathbb{D})$ and denote by $L_x^0 \colon \mathbb{R}[x] \to \mathbb{R}[x]$ the linear map given by $L_x^0 y = x \bullet y$ for all $y \in \mathbb{R}[x]$. We say x is *invertible in* J if it is invertible in the unital commutative associative subalgebra $\mathbb{R}[x] \subseteq J$. Prove:

(a) If $\mathbf{1}_3 \wedge x \wedge x^2 \ne 0$ in $\bigwedge^3(J)$, then

$$\mu_x = \det(\mathbf{t}\mathbf{1}_{\mathbb{R}[x]} - L_x^0), \quad N(x) = \det(L_x^0), \quad T(x) = \mathrm{tr}(L_x^0).$$

(b) $N(u \bullet v) = N(u)N(v)$ for all $u, v \in \mathbb{R}[x]$ but *not* for all $u, v \in J$.

(c) x is invertible in J if and only if $N(x) \ne 0$. In this case,

$$N(x^{-1}) = N(x)^{-1} \quad \text{and} \quad x^{-1} = N(x)^{-1} x^\sharp.$$

(d) $x^{\sharp\sharp} = N(x)x$ (adjoint identity) and $N(x^\sharp) = N(x)^2$.

(*Hint*: For (b) and (d), use Zariski density arguments such as [29, §IV.2.3, Thm. 2].)

5.18. *Automorphisms of* $\mathrm{Her}_3(\mathbb{D})$. Prove with $J := \mathrm{Her}_3(\mathbb{D})$ that a linear bijection $\varphi\colon J \to J$ is an automorphism of J if and only if it preserves units and norms: $\varphi(\mathbf{1}_3) = \mathbf{1}_3$, $N \circ \varphi = N$. Conclude for $0 \neq u \in \mathbb{D}$ that $\varphi\colon J \to J$ defined by

$$\varphi\Big(\sum (\alpha_i e_{ii} + u_i[jl])\Big) := \sum \alpha_i e_{ii} + (u^{-1}u_1)[23] + (u_2u^{-1})[31] + (uu_3u)[12]$$

for $\alpha_i \in \mathbb{R}$, $u_i \in \mathbb{D}$, $1 \leq i \leq 3$, is an automorphism of J if and only if $n_{\mathbb{D}}(u) = 1$.

6 $\mathbb{Z}$-structures of unital real Jordan algebras

Extending the notion of a $\mathbb{Z}$-structure from the subalgebras $\mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ of the Graves-Cayley octonions to real Jordan algebras, most notably the cubic euclidean Jordan matrix algebras $\mathrm{Her}_3(\mathbb{D})$, turns out to be a remarkably delicate task. In particular, the idea of copying verbatim the formal definition 3.6 (d) in the Jordan setting, leading to the notion of a *linear* $\mathbb{Z}$*-structure* in the process, is practically useless since, as will be seen in due course, linear $\mathbb{Z}$-structures are marred by a number of serious deficiencies, the lack of natural examples being one of the most notorious.

In order to overcome this difficulty, we take up an idea of Knebusch [155] by defining what we call *quadratic* $\mathbb{Z}$*-structures* of finite-dimensional unital real Jordan algebras. In contradistinction to their linear counterpart, quadratic $\mathbb{Z}$-structures are based not on the bilinear product xy but on the cubic operation $U_x y$ provided by the U-operator (see 6.4 below) of the ambient Jordan algebra. This not only yields an abundant variety of natural examples but also a first glimpse at how Jordan algebras should be treated over commutative rings in which $\frac{1}{2}$ is not available: through McCrimmon's theory [181] of quadratic Jordan algebras.

Throughout this section, we let J be a finite-dimensional unital real Jordan algebra. As before, $\mathbb{D}$ stands for any of the unital subalgebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ of $\mathbb{O}$. We begin by naively rephrasing the definition of a $\mathbb{Z}$-structure, with a slight terminological twist, in the Jordan setting.

6.1 Linear $\mathbb{Z}$-structures. By a *linear* $\mathbb{Z}$*-structure* of J we mean a lattice $\Lambda \subseteq J$ which is *unital* in the sense that $1_J \in \Lambda$ and which is closed under multiplication: $xy \in \Lambda$ for all $x, y \in \Lambda$.

One is tempted to regard the preceding definition as a very natural one because, for instance, any linear $\mathbb{Z}$-structure in J may canonically be regarded as a Jordan algebra over the integers in its own right. And yet it is marred by serious deficiencies which already come to the fore when trying to construct examples.

6.2 Examples: the Jordan algebras $\mathbb{D}^+$. By definition (5.7) or by Exc. 6.13 below, $J := \mathbb{D}^+$ is a special unital real Jordan algebra, and it would be perfectly natural to expect any $\mathbb{Z}$-structure of $\mathbb{D}$ to be a linear one of J. But this, though valid in some isolated cases (see Exc. 6.14 below) *is not true in general*. In fact, it fails to be valid in the following important examples.

(a) (Knebusch [155, p. 175]) Let $\mathbb{D} := \mathbb{H}$ and $M := \mathrm{Hur}(\mathbb{H}) \subseteq \mathbb{H}$ be the $\mathbb{Z}$-structure of Hurwitz quaternions. Then $\mathbf{i}, \mathbf{h} \in M$ by Thm. 4.2, while (1.6.12) and (4.1.2) yield

$$\mathbf{i} \bullet \mathbf{h} = \frac{1}{2}(\mathbf{ih} + \mathbf{hi}) = \frac{1}{2}(t_{\mathbb{H}}(\mathbf{i})\mathbf{h} + t_{\mathbb{H}}(\mathbf{h})\mathbf{i} - n_{\mathbb{H}}(\mathbf{i}, \mathbf{h})1_{\mathbb{H}}) = \frac{1}{2}(-1_{\mathbb{H}} + \mathbf{i}),$$

which by Exc. 4.8 does not belong to M. Thus $\mathrm{Hur}(\mathbb{H}) \subseteq \mathbb{H}^+$ is *not* a linear $\mathbb{Z}$-structure.

(b) Similarly, let $\mathbb{D} := \mathbb{O}$ and $M := \mathrm{DiCo}_E(\mathbb{O}) \subseteq \mathbb{O}$ be the $\mathbb{Z}$-structure of Dickson-Coxeter octonions relative to a Cartan-Shouten basis $E = (u_i)_{0 \le i \le 7}$ of $\mathbb{O}$. Then $u_1, \mathbf{p} \in M$ by Thm. 4.5, while (1.6.12) and (4.4.8) yield

$$\begin{aligned} u_1 \bullet \mathbf{p} &= \frac{1}{2}(u_1\mathbf{p} + \mathbf{p}u_1) = \frac{1}{2}(t_{\mathbb{O}}(u_1)\mathbf{p} + t_{\mathbb{O}}(\mathbf{p})u_1 - n_{\mathbb{O}}(u_1, \mathbf{p})1_{\mathbb{O}}) \\ &= \frac{1}{2}(-1_{\mathbb{O}} + u_1) \in \mathbb{H}. \end{aligned}$$

If this were an element of M, then (4.5.1) would imply $u_1 \bullet \mathbf{p} \in \mathrm{DiCo}_E(\mathbb{O}) \cap \mathbb{H} = \mathrm{Ga}(\mathbb{H})$, a contradiction. Thus $u_1 \bullet \mathbf{p} \notin M$, and we conclude that $\mathrm{DiCo}_E(\mathbb{O})$ is *not* a linear $\mathbb{Z}$-structure of $\mathbb{O}^+$.

6.3 Examples: cubic euclidean Jordan matrix algebras. Again it would be perfectly natural to expect any $\mathbb{Z}$-structure of $\mathbb{D}$ giving rise, via 3-by-3 hermitian matrices, to a linear $\mathbb{Z}$-structure of $J := \mathrm{Her}_3(\mathbb{D})$. *But this never holds.* Indeed, let M be a $\mathbb{Z}$-structure of $\mathbb{D}$. Then M is stable under conjugation, so

$$\Lambda := \mathrm{Her}_3(M) := \{x \in \mathrm{Mat}_3(M) \mid x = \bar{x}^{\mathsf{T}}\}$$

makes sense and is a unital lattice in J. However, Λ fails to be closed under multiplication since, e.g., $1[23]$ and $1[31]$ both belong to Λ while $1[23] \bullet 1[31] = \frac{1}{2}[12]$ obviously does not. One could consider the linear $\mathbb{Z}$-subalgebra of J generated by Λ but computations similar to the previous one show that this is not a $\mathbb{Z}$-lattice.

In view of the deficiencies highlighted in the preceding examples, we will abandon linear $\mathbb{Z}$-structures of real Jordan algebras and replace them by quadratic ones, which are based on the following concept.

6.4 The U-operator. For $x \in J$, the linear map

$$U_x\colon J \longrightarrow J, \quad y \longmapsto U_x y := 2x(xy) - x^2 y, \tag{1}$$

is called the *U-operator of x*. The map

$$U\colon J \longrightarrow \mathrm{End}(J), \quad x \longmapsto U_x \tag{2}$$

is called the *U-operator of J*. Note that the U-operator of J is a quadratic map whose bilinearization yields the *Jordan triple product*

$$\{xyz\} := U_{x,z}y = (U_{x+z} - U_x - U_z)y = 2(x(zy) + z(xy) - (xz)y) \tag{3}$$

for $x, y, z \in J$. The U-operator is of the utmost importance for a deeper understanding of Jordan algebras. Its fundamental algebraic properties will be addressed in 27.10–27.12 and §29 below. For the time being, it will be enough to observe a few elementary facts assembled in Exercises 6.12, 6.13.

6.5 Quadratic $\mathbb{Z}$-structures (cf. Knebusch [155, p. 175])**.** By a *quadratic $\mathbb{Z}$-structure* of J we mean a unital lattice $\Lambda \subseteq J$ such that $U_x y \in \Lambda$ for all $x, y \in \Lambda$. This implies that Λ is closed under the Jordan triple product (6.4.3) and, in particular, $2xy = \{xy1_J\} \in \Lambda$ for all $x, y \in \Lambda$. However, while an inspection of (6.4.1) shows that linear $\mathbb{Z}$-structures are always quadratic ones, the converse does not hold, as may be seen from the following examples.

6.6 Examples. Let M be a $\mathbb{Z}$-structure of $\mathbb{D}$. Then $1_{\mathbb{D}^+} = 1_{\mathbb{D}} \in M$, and Exc. 6.13 yields $U_x y = xyx \in M$ for all $x, y \in M$. Thus M is a quadratic $\mathbb{Z}$-structure of $\mathbb{D}^+$; as such it will be denoted by M^+. Now it follows from 6.2 that both $\mathrm{Hur}(\mathbb{H})^+$ and $\mathrm{DiCo}_E(\mathbb{O})^+$ are quadratic $\mathbb{Z}$-structures of $\mathbb{H}^+$ and $\mathbb{O}^+$, respectively, but not linear ones.

We have observed in 6.3 that

$$\Lambda := \mathrm{Her}_3(M) = \{x \in \mathrm{Mat}_3(M) \mid x = \bar{x}^{\mathsf{T}}\}$$

is never a linear $\mathbb{Z}$-structure of $J := \mathrm{Her}_3(\mathbb{D})$. But we claim that *it is always a quadratic one*. Indeed, by Cor. 3.9, trace and norm of $\mathbb{D}$ take on integral values on M. Hence, given

$$x = \sum(\alpha_i e_{ii} + u_i[jl]), \quad y = \sum(\beta_i e_{ii} + v_i[jl]) \in \Lambda,$$

we have $\alpha_i, \beta_i \in M \cap \mathbb{R} = \mathbb{Z}$ by Exc. 3.19, $u_i, v_i \in M$ for $1 \le i \le 3$, and (5a.3), (5.8.4) yield $T(x \bullet y) \in \mathbb{Z}$, $x^\sharp \in \Lambda$. Linearizing and applying Exc. 6.12 (b), we therefore obtain $U_x y = T(x \bullet y)x - x^\sharp \times y \in \Lambda$, and the proof is complete.

Our next aim will be to show that, in analogy to Corollary 3.9, the linear form T, the quadratic form S, and the cubic form N of $J := \mathrm{Her}_3(\mathbb{D})$ all take

on integral values on any quadratic $\mathbb{Z}$-structure of J. Actually, we will be able to establish this result under slightly less restrictive conditions. The following lemma paves the way.

6.7 Lemma. *Let $\Lambda \subseteq J := \mathrm{Her}_3(\mathbb{D})$ be a unital lattice such that $\mathbb{Q}\Lambda \subseteq J$ is a subalgebra over $\mathbb{Q}$. Then $T(x), S(x), N(x) \in \mathbb{Q}$ for all $x \in \mathbb{Q}\Lambda$.*

Proof From Prop. 3.8 we deduce $\mu_x := \mu_x^{\mathbb{R}} = \mu_x^{\mathbb{Q}} \in \mathbb{Q}[\mathbf{t}]$, so $m := \deg(\mu_x)$ is at most 3. If $m = 3$, then (5.13.1) implies the assertion. At the other extreme, if $m = 1$, then $x = \alpha 1_J$ for some $\alpha \in \mathbb{Q}$, which again implies the assertion. We are left with the case $m = 2$, so $\mu_x = \mathbf{t}^2 - \alpha_1\mathbf{t} + \alpha_2$ for some $\alpha_1, \alpha_2 \in \mathbb{Q}$, and a short computation gives

$$x^3 = (\alpha_1^2 - \alpha_2)x - \alpha_1\alpha_2\mathbf{1}_3.$$

Similarly, invoking (5a.8), we obtain

$$x^3 = (\alpha_1 T(x) - S(x))x - (\alpha_2 T(x) - N(x))\mathbf{1}_3,$$

and comparing coefficients, we conclude

$$\alpha_1 T(x) - S(x), \quad \alpha_2 T(x) - N(x) \in \mathbb{Q}. \tag{1}$$

On the other hand, by Zariski density, we can find elements $y \in \mathbb{Q}\Lambda$ and $\alpha \in \mathbb{Q}^\times$ such that

$$\deg(\mu_y^{\mathbb{R}}) = \deg(\mu_y^{\mathbb{Q}}) = \deg(\mu_{\alpha x+y}^{\mathbb{R}}) = \deg(\mu_{\alpha x+y}^{\mathbb{Q}}) = 3.$$

This implies $T(y) \in \mathbb{Q}$ and $\alpha T(x) + T(y) = T(\alpha x + y) \in \mathbb{Q}$, hence $T(x) \in \mathbb{Q}$. But now (1) yields $S(x), N(x) \in \mathbb{Q}$ as well. □

6.8 Remark. Let B be a $\mathbb{Q}$-subspace of J that is closed under squaring. Then B *is a $\mathbb{Q}$-subalgebra* since $xy = \frac{1}{2}((x + y)^2 - x^2 - y^2) \in B$ for all $x, y \in B$.

6.9 Proposition. *Let $\Lambda \subseteq J := \mathrm{Her}_3(\mathbb{D})$ be a lattice that is stable under taking powers $x \mapsto x^n$ for $n \in \mathbb{N}$. Then every $x \in \Lambda$ is integral and $T(x), S(x), N(x) \in \mathbb{Z}$.*

Proof For $x \in \Lambda$ we have $1_J = x^0 \in \Lambda$ (so Λ is unital) and $x^2 \in \Lambda$. This property carries over to $\mathbb{Q}\Lambda$ which, by Remark 6.8, is a unital $\mathbb{Q}$-subalgebra of J. Given $x \in \Lambda$, Lemma 6.7 therefore implies $T(x), S(x), N(x) \in \mathbb{Q}$. Moreover, Λ being stable under powers, $\mathbb{Z}[x] \subseteq \Lambda$ is an additive subgroup which, along with Λ, is finitely generated. Thus Prop. 3.5 and 3.8 show that x is integral and $\mu_x := \mu_x^{\mathbb{R}} = \mu_x^{\mathbb{Q}} \in \mathbb{Z}[\mathbf{t}]$. Since the remaining assertions of the proposition will follow, either for obvious reasons or from 5.13 and Exc. 3.19, if $m := \deg(\mu_x) \in$

$\{1,3\}$, we may assume $m = 2$. Then Corollary 5.14 yields non-zero elements $c_1, c_2 \in \mathbb{R}[x]$ and scalars $\alpha_1, \alpha_2 \in \mathbb{R}$ such that

$$c_1 + c_2 = \mathbf{1}_3, \quad c_1^2 = c_1, \quad c_2^2 = c_2, \quad c_1 \bullet c_2 = 0, \tag{1}$$

$$x = \alpha_1 c_1 + \alpha_2 c_2. \tag{2}$$

Note that $\mathbb{R}[x] \subseteq J$ is a unital commutative associative subalgebra and write R for the integral closure of $\mathbb{Z}$ in $\mathbb{R}[x]$ (Bourbaki [27, V, §1, Def. 3]). From what we have just seen we deduce $x \in R$, while (1) implies $c_r \in R$ for $r = 1, 2$. Hence $\alpha_r c_r = x c_r \in R$ by (1), (2), and we conclude that $\alpha_r \in \mathbb{R}$ is integral. On the other hand, Exc. 6.15 below implies, or allows us to assume,

$$N(c_1) = N(c_2) = 0, \quad T(c_1) = 2, \quad S(c_1) = 1, \quad T(c_2) = 1, \quad S(c_2) = 0, \tag{3}$$

which by (5a.6) implies

$$c_1^\sharp = c_1 - 2c_1 + \mathbf{1}_3 = c_2, \quad c_2^\sharp = c_2 - c_2 = 0. \tag{4}$$

Combining (3), (4) with (5a.5) and Exc. 6.16, it follows that the rational numbers

$$\begin{aligned} T(x) &= 2\alpha_1 + \alpha_2, \\ S(x) &= \alpha_1^2 + \alpha_1\alpha_2 S(c_1, c_2) = \alpha_1^2 + \alpha_1\alpha_2(T(c_1)T(c_2) - T(c_1 \bullet c_2)) \\ &= \alpha_1^2 + 2\alpha_1\alpha_2, \\ N(x) &= \alpha_1^3 N(c_1) + \alpha_1^2\alpha_2 T(c_1^\sharp \bullet c_2) + \alpha_1\alpha_2^2 T(c_1 \bullet c_2^\sharp) + \alpha_2^3 N(c_2) = \alpha_1^2\alpha_2 \end{aligned}$$

are all integral, hence belong to $\mathbb{Z}$. □

Our next objective will be to derive a useful criterion for a unital lattice in J to be a quadratic $\mathbb{Z}$-structure. Before doing so, we need a lemma.

6.10 Lemma. *Let $X \subseteq \mathbb{Q}$ be closed under squaring (i.e., $\xi \in X \Rightarrow \xi^2 \in X$) and suppose the additive subgroup of $\mathbb{Q}$ generated by X is finitely generated. Then $X \subseteq \mathbb{Z}$.*

Proof Let $d_\xi > 0$ be the exact denominator of $\xi \in X$. By hypothesis, $\{d_\xi \mid \xi \in X\}$ is a finite set of positive integers. Pick $\eta \in X$ such that d_η is maximal. Then d_η^2 is the exact denominator of $\eta^2 \in X$, which implies $d_\eta^2 \leq d_\eta$ by maximality, hence $d_\eta = 1$ and therefore $d_\xi = 1$ for all $\xi \in X$. Thus $X \subseteq \mathbb{Z}$. □

6.11 Theorem (cf. Racine [243, Prop. IV.1, p. 102])**.** *For a unital lattice $\Lambda \subseteq J := \mathrm{Her}_3(\mathbb{D})$ the following conditions are equivalent.*

(i) Λ *is a quadratic $\mathbb{Z}$-structure in J.*
(ii) $x^2 \in \Lambda$ *for all* $x \in \Lambda$.

(iii) $x^\sharp \in \Lambda$ *for all* $x \in \Lambda$.

Proof (i) $\Rightarrow$ (ii). Let $x \in \Lambda$. Then (6.4.1) shows $x^2 = U_x \mathbf{1}_3 \in \Lambda$.

Before we can deal with the remaining implications, it will be important to note that

$$N(\Lambda) \text{ generates a finitely generated additive subgroup of } \mathbb{R}. \tag{1}$$

In order to see this, let $(e_1, \dots, e_n)$ be an $\mathbb{R}$-basis of J associated with Λ. Since $N(\Lambda)$ by Exc. 6.16 is contained in the additive subgroup of $\mathbb{R}$ generated by the quantities $N(e_i)$ $(1 \le i \le n)$, $T(e_i^\sharp, e_j)$ $(1 \le i, j \le n, i \ne j)$, $T(e_i \times e_j, e_l)$ $(1 \le i < j < l \le n)$, it generates a finitely generated additive subgroup of $\mathbb{R}$ on its own, as claimed. We also note

$$N(\mathbf{1}_3 \pm x) = 1 \pm T(x) + S(x) \pm N(x) \tag{2}$$

for all $x \in J$.

(ii) $\Rightarrow$ (iii). Since Λ is closed under squaring, so is $\mathbb{Q}\Lambda$, which therefore is a rational subalgebra of J (Remark 6.8). Now Lemma 6.7 implies $T(x)$, $S(x)$, $N(x) \in \mathbb{Q}$ for all $x \in \Lambda$. On the other hand, Exc. 5.17 (b) and (1) imply that $X := N(\Lambda)$ satisfies the hypotheses of Lemma 6.10. Hence $N(\Lambda) \subseteq \mathbb{Z}$. Combining (5a.5) with (2) for $x \in \Lambda$, we therefore conclude

$$T(x)^2 - T(x^2) = S(x, x) = 2S(x) = N(\mathbf{1}_3 + x) + N(\mathbf{1}_3 - x) - 2 \in \mathbb{Z}. \tag{3}$$

But from (2) we also deduce $2T(x) = N(\mathbf{1}_3 + x) - N(\mathbf{1}_3 - x) - 2N(x) \in \mathbb{Z}$, which combined with (3) shows that $X := \mathbb{Z} + T(\Lambda)$ satisfies the conditions of Lemma 6.10. Thus $T(x) \in \mathbb{Z}$ for all $x \in \Lambda$, and (2) gives $S(x) \in \mathbb{Z}$. Now (5a.6) shows $x^\sharp \in \Lambda$ and we have (iii).

(iii) $\Rightarrow$ (i). Since Λ is stable under the adjoint map, so is $\mathbb{Q}\Lambda$. For $0 \ne x \in \mathbb{Q}\Lambda$, we apply Exc. 5.17 (d) and obtain $N(x)x = x^{\sharp\sharp} \in \mathbb{Q}\Lambda$. Extending x to a $\mathbb{Q}$-basis of $\mathbb{Q}\Lambda$ yields an $\mathbb{R}$-basis of J (Lemma 3.7), and we conclude $N(x) \in \mathbb{Q}$. Now Exc. 5.17 (b) and (1) show that $X := N(\Lambda)$ satisfies the hypotheses of Lemma 6.10. Thus $N(\Lambda) \subseteq \mathbb{Z}$. On the other hand, by (5a.6) linearized, (iii) implies $T(x)\mathbf{1}_3 - x = \mathbf{1}_3 \times x \in \Lambda$, hence $T(x)\mathbf{1}_3 \in \Lambda$ and then $T(x)^3 = N(T(x)\mathbf{1}_3) \in \mathbb{Z}$. Hence $T(x) \in \mathbb{Q}$ is integral, which implies $T(x) \in \mathbb{Z}$, $S(x) = T(x^\sharp) \in \mathbb{Z}$. Now (5a.5) shows $T(x \bullet y) \in \mathbb{Z}$ for all $x, y \in \Lambda$, and from (6.4.1) combined with Exc. 6.12 (b) we conclude $U_x y = T(x \bullet y)x - x^\sharp \times y \in \Lambda$. Thus $\Lambda \subseteq J$ is a quadratic $\mathbb{Z}$-structure. □

Exercises

6.12. *Properties of the U-operator.* Let J be a real Jordan algebra. Prove:

(a) If J is a subalgebra of A^+ for some associative real algebra A, then $U_x y = xyx$ for all $x, y \in J$ in terms of the associative product $(x, y) \mapsto xy$ of A.

(b) If $J = \mathrm{Her}_3(\mathbb{D})$, then

$$U_x y = T(x \bullet y)x - x^\sharp \times y$$

for all $x, y \in J$.

6.13. Show that a linear map between commutative real algebras is a homomorphism if and only if it preserves squares. Conclude that the algebra $\mathbb{O}^+$ of Exc. 2.9 is a unital special real Jordan algebra such that $U_x y = xyx$ for all $x, y \in \mathbb{O}$. Is $\mathbb{O}^+$ euclidean?

6.14. Let $(e_i)_{0 \le i \le n}$ be an orthonormal basis of $\mathbb{D}$ as a euclidean real vector space such that $e_0 = 1_{\mathbb{D}}$. Prove that

$$\Lambda := \sum_{i=1}^{n} \mathbb{Z} e_i$$

is a linear $\mathbb{Z}$-structure of the special real Jordan algebra $\mathbb{D}^+$ (cf. Exc. 6.13). Conclude that the Gaussian integers $\mathrm{Ga}(\mathbb{D})$ form a linear $\mathbb{Z}$-structure of $\mathbb{D}^+$, denoted by $\mathrm{Ga}(\mathbb{D})^+$.

6.15. *Idempotents.* Let $c \in J := \mathrm{Her}_3(\mathbb{D})$ be an *idempotent* in the sense that $c^2 = c$, and assume $0 \ne c \ne \mathbf{1}_3$. Prove $N(c) = 0$ and either $T(c) = 1, S(c) = 0$ or $T(c) = 2, S(c) = 1$.

6.16. Prove

$$N(x + y) = N(x) + T(x^\sharp, y) + T(x, y^\sharp) + N(y)$$

for all $x, y \in J := \mathrm{Her}_3(\mathbb{D})$.

II

Foundations

Our main purpose in this chapter will be to introduce a number of important concepts and terminological prerequisites in a degree of generality that will be required in the subsequent development of the book. Throughout we let k be an arbitrary commutative ring. All k-modules are supposed to be unital left k-modules. Unadorned tensor products are always to be taken over k.

The possibility of $k = \{0\}$ being the zero ring is expressly allowed. The only module over $k = \{0\}$ is the zero module $M = \{0\}$.

7 The language of non-associative algebras

In this section, we give a quick introduction to the language of non-associative algebras. Without striving for completeness or maximum generality, we confine ourselves to what is indispensable for the subsequent development.

7.1 The concept of a non-associative algebra. A *non-associative algebra* or just an *algebra* over k (or a *k-algebra* for short) is a k-module A together with a bilinear map $A \times A \to A$, called the *multiplication* (or *product*) of A and usually indicated by juxtaposition: $(x, y) \mapsto xy$. Thus k-algebras satisfy both distributive laws and are compatible with scalar multiplication but may fail to be associative or commutative or to contain a unit element. Nevertheless, the standard vocabulary of ring theory (ideals, homomorphisms, quotients, direct products, ...) easily extends to this more general setting and will be used here mostly without further comment. To mention just three examples, a *subalgebra* of A is a submodule closed under multiplication, a *homomorphism* $h\colon A \to B$ of k-algebras is a linear map preserving products: $h(xy) = h(x)h(y)$ for all $x, y \in A$, and ideals in A are always two-sided ideals: $I \subseteq A$ is an *ideal* if and only if $xy, yx \in I$ for all $x \in I$, $y \in A$. Examples of k-algebras for $k = \mathbb{R}$ or $k = \mathbb{Z}$ have been discussed in the preceding chapter.

For the rest of this section we fix an algebra A over k.

7.2 Left and right multiplication. For $x \in A$, the linear map

$$L_x\colon A \longrightarrow A, \quad y \longmapsto L_x y := xy,$$

is called the *left multiplication operator* by x in A. Similarly, the *right multiplication operator* by x in A will be denoted by

$$R_x \colon A \longrightarrow A, \quad y \longmapsto R_x y := yx\,.$$

The linear map

$$L \colon A \longrightarrow \mathrm{End}_k(A), x \longmapsto L_x, \quad (\text{resp. } R \colon A \longrightarrow \mathrm{End}_k(A), x \longmapsto R_x)$$

is called the *left* (resp. *right*) *multiplication* of A.

7.3 Generators. For arbitrary subsets $X, Y \subseteq A$, we write XY as in 1.2 for the additive subgroup of A spanned by all products xy, $x \in X$, $y \in Y$. Similar conventions apply to other multi-linear mappings in place of the product of A. We abbreviate $X^2 := XX$. A submodule $B \subseteq A$ is a subalgebra if and only if $B^2 \subseteq B$.

Let $X \subseteq A$ be an arbitrary subset. Then the smallest subalgebra of A containing X is called the *subalgebra generated by* X. Roughly speaking, it consists of all linear combinations of finite products, bracketed arbitrarily, of elements in X. To make this a bit more precise, we introduce the following definition.

7.4 Monomials over a subset of an algebra. For a subset $X \subseteq A$, we define subsets $\mathrm{Mon}_m(X) \subseteq A$, $m \in \mathbb{Z}$, $m > 0$, recursively by setting $\mathrm{Mon}_1(X) = X$ and by requiring that $\mathrm{Mon}_m(X)$, $m \in \mathbb{Z}$, $m > 1$, consist of all products yz, $y \in \mathrm{Mon}_n(X)$, $z \in \mathrm{Mon}_p(X)$, $n, p \in \mathbb{Z}$, $n, p > 0$, $n + p = m$. The elements of

$$\mathrm{Mon}(X) := \bigcup_{m \in \mathbb{Z}, m > 0} \mathrm{Mon}_m(X)$$

are called *monomials* over X. With these definitions it is clear that the subalgebra of A generated by X agrees with $k\,\mathrm{Mon}(X)$, i.e., with the submodule of A spanned by the monomials over X.

7.5 Associators and commutators. The trilinear map

$$A \times A \times A \longrightarrow A, \quad (x, y, z) \longmapsto [x, y, z] := (xy)z - x(yz),$$

is called the *associator* of A, which we have described in Exc. 1.16 for the real algebra of Graves-Cayley octonions. Similarly, the bilinear map

$$A \times A \longrightarrow A, \quad (x, y) \longmapsto [x, y] := xy - yx$$

is called the *commutator* of A. It is straightforward to check that they satisfy the relations

$$[xy, z] - x[y, z] - [x, z]y = [x, y, z] - [x, z, y] + [z, x, y]\,, \tag{1}$$

$$[xy, z, w] - [x, yz, w] + [x, y, zw] = x[y, z, w] + [x, y, z]w \tag{2}$$

for all $x, y, z, w \in A$. Note that the commutator is alternating, so $[x, x] = 0$ for all $x \in A$, while the associator in general is not. This gives rise to the important concept of an alternative algebra that we encountered already in the study of Graves-Cayley octonions (1.7) and that will be discussed more systematically in Chap. III.

7.6 Commutative and associative algebras. The k-algebra A is *commutative* if it satisfies the commutative law $xy = yx$, equivalently, if its commutator is the zero map. Similarly, A is *associative* if it satisfies the associative law $(xy)z = x(yz)$, equivalently, if its associator is the zero map. Note that A is commutative if and only if its left and right multiplications are the same. Also, the following conditions are equivalent.

(i) A is associative.
(ii) The left multiplication $L\colon A \to \mathrm{End}_k(A)$ is an algebra homomorphism: $L_{xy} = L_x L_y$ for all $x, y \in A$.
(iii) The right multiplication $R\colon A \to \mathrm{End}_k(A)$ is an algebra *anti*-homomorphism: $R_{xy} = R_y R_x$ for all $x, y \in A$.

7.7 Powers. We define the powers with base $x \in A$ and exponent $n \in \mathbb{Z}$, $n > 0$, recursively by the rule

$$x^1 = x, \quad x^{n+1} = xx^n$$

and write $k_1[x] = \sum_{n\geq 1} kx^n$ for the submodule of A spanned by all powers of x with positive integral exponents. It consists of all "polynomials" in x with coefficients in k and zero constant term. A is said to be *power-associative* if $x^m x^n = x^{m+n}$ for all $x \in A$ and all $m, n \in \mathbb{Z}$, $m, n > 0$. This is equivalent to $k_1[x] \subseteq A$, $x \in A$, being a commutative associative subalgebra; in fact, it is then the subalgebra of A generated by x.

7.8 Idempotents. An element $c \in A$ is called an *idempotent* if $c^2 = c$. In particular, we count 0 as an idempotent. Two idempotents $c, d \in A$ are said to be *orthogonal* if $cd = dc = 0$; in this case, $c + d$ is also an idempotent. By an *orthogonal system* of idempotents in A we mean a family $(c_i)_{i\in I}$ consisting of mutually orthogonal idempotents: $c_i c_j = \delta_{ij} c_i$ for all $i, j \in I$.

7.9 Associative bilinear and linear forms. A bilinear form $\sigma\colon A \times A \to k$ is said to be *associative* if it is symmetric and satisfies the relation $\sigma(xy, z) = \sigma(x, yz)$ for all $x, y, z \in A$. If in this case $I \subseteq A$ is an ideal, then so is $I^\perp = \{x \in A \mid \sigma(x, I) = \{0\}\}$, the orthogonal complement of I relative to σ. Every linear form $t\colon A \to k$ gives a bilinear form $\sigma_t\colon A \times A \to k$ via $\sigma_t(x, y) := t(xy)$ for all $x, y \in A$. We say that t is *associative* if σ_t is, equivalently, if t vanishes on all

commutators and associators of A. For example, it follows immediately from Exc. 1.18 (b) that the trace form of the Graves-Cayley octonions is associative, even though the Graves-Cayley octonions themselves are not.

7.10 Structure constants. Generalizing the set-up described in 1.2, suppose A is free as a k-module, with basis $(e_i)_{i\in I}$. Then there exists a unique family $(\gamma_{ijl})_{i,j,l\in I}$ of scalars in k such that, for all $j, l \in I$,

$$\gamma_{ijl} = 0 \qquad \text{(for almost all } i \in I\text{)}, \tag{1}$$

$$e_j e_l = \sum_{i\in I} \gamma_{ijl} e_i. \tag{2}$$

The γ_{ijl}, $i, j, l \in I$, are called the *structure constants* of A relative to the basis (e_i). Conversely, let M be a free k-module with basis $(e_i)_{i\in I}$ and γ_{ijl} a family of scalars in k satisfying (1) for all $j, l \in I$, then there is a unique algebra structure A on M making the γ_{ijl} the structure constants of A relative to (e_i): just define the multiplication of A on the basis vectors by (2) and extend it bilinearly to all of M.

We conclude this section by quoting without proof an observation of Vasconcelos from the theory of modules that turns out to be useful in our study of non-associative algebras. Proofs may be found in Vasconcelos [287, Prop. 1.2], Knus-Ojanguren [158, I, Cor. 2.4], or the Stacks project [271, Tag 05G8].

7.11 Proposition. *Any surjective k-linear map from a finitely generated k-module onto itself is bijective.* □

Exercises

7.12. Let A, B be k-algebras and $f\colon A \to B$ a k-linear map such that, for all $x, y \in A$, we have $f(xy) = \pm f(x)f(y)$. Show that f or $-f$ is a homomorphism from A to B.

7.13. *The nil radical* (Behrens [22]). Let A be a k-algebra. An element $x \in A$ is said to be *nilpotent* if $0 \in \mathrm{Mon}(\{x\})$ is a monomial over x (7.4). This concept of nilpotency is the usual one for associative or, more generally, for power-associative algebras. A is said to be a *nil algebra* if it consists entirely of nilpotent elements, ditto for a *nil ideal*. Prove that, for any ideal $I \subseteq A$, A is a nil algebra if and only if I is a nil ideal and A/I is a nil algebra. Conclude that the sum of all nil ideals in A is a nil ideal, called the *nil radical* of A and denoted by $\mathrm{Nil}(A)$. Finally show $\mathrm{Nil}(k)A \subseteq \mathrm{Nil}(A)$.

7.14. *Lifting idempotents.* Let A be a power-associative k-algebra.

(a) Suppose $x \in A$ satisfies a *monic polynomial with invertible least coefficient*, i.e., there exist integers $n > d > 0$, and scalars $\alpha_d, \dots, \alpha_{n-1} \in k$ with $\alpha_d \in k^\times$ and $\alpha_d x^d + \cdots + \alpha_{n-1}x^{n-1} + x^n = 0$. Given $r \in \mathbb{Z}$, $r > 0$, write $k_r[x]$ for the k-submodule of A spanned by the powers x^n, $n \in \mathbb{Z}$, $n \geq r$. Then show that there is a unique element $c \in k_d[x]$ satisfying $cx^d = x^d$. Conclude that $c \in A$ is an idempotent. (*Hint*: Apply Prop. 7.11.)

(b) Let $\varphi\colon A \to A'$ be a surjective homomorphism of power-associative algebras over k and suppose $\mathrm{Ker}(\varphi) \subseteq A$ is a nil ideal (Exc. 7.13). Conclude from (a) that every idempotent $c' \in A'$ can be lifted to A, i.e., there exists an idempotent $c \in A$ satisfying $\varphi(c) = c'$.

Remark. If $k = F$ is a field, then (a) says for any element $x \in A$ which is not nilpotent and has $F_1[x]$ finite-dimensional over F that there exists a non-zero idempotent in $F_1[x]$ (Albert [9, §II.6, Thm. 8], Braun-Koecher [36, I, Lemma 3.2], Jacobson [136, III, Lemma 7.1]).

8 Unital algebras

Let A be a k-algebra.

8.1 The unit element. As usual, $e \in A$ is said to be a *unit* (or *identity*) *element* of A if $ex = xe = x$ for all $x \in A$. A unit element may not exist, but if it does it is unique and called *the* unit element of A, written as 1_A. In this case, A is said to be *unital*. A *unital subalgebra* of a unital algebra is a subalgebra containing the unit element. If A is unital, the *unital subalgebra of A generated by $X \subseteq A$* is defined as the smallest unital subalgebra of A containing X. A *unital homomorphism* of unital algebras is a homomorphism of algebras preserving unit elements.

8.2 Powers and idempotents revisited. Suppose A is unital.

(a) For $x \in A$, we define $x^0 := 1_A$ and, combining with 7.7, obtain powers x^n for all $n \in \mathbb{N}$. The submodule of A spanned by these powers will be denoted by $k[x]$, so we have $k[x] = k1_A + k_1[x]$. If A is power-associative, then $k[x] \subseteq A$ is a unital commutative associative subalgebra and, in fact, agrees with the unital subalgebra of A generated by x.

(b) An orthogonal system $\Omega = (c_i)_{i\in I}$ of idempotents in A as defined in 7.8 is said to be *complete* if $c_i = 0$ for almost all $i \in I$ and $\sum_{i\in I} c_i = 1_A$. Any orthogonal system $\Omega = (c_i)_{i\in I}$ of idempotents in A having $c_i = 0$ for almost all $i \in I$ can be enlarged to a complete one: with an additional index $\hat{\imath} \notin I$ and $\hat{I} := \{\hat{\imath}\} \cup I$ put $\hat{\Omega} := (c_i)_{i\in\hat{I}}$ where $c_{\hat{\imath}} := 1_A - \sum_{i\in I} c_i$.

8.3 The multiplication algebra. The unital subalgebra of $\mathrm{End}_k(A)$ generated by all left and right multiplication operators in A is called the *multiplication algebra* of A and will be denoted by $\mathrm{Mult}(A)$. We may view A as a (left) $\mathrm{Mult}(A)$-module in a natural way. The $\mathrm{Mult}(A)$-submodules of A are precisely its ideals.

8.4 The centre. Let A be unital. An element $a \in A$ is said to be *central* if $[a, x] = [a, x, y] = [x, a, y] = [x, y, a] = 0$ for all $x, y \in A$. The totality of central

elements in A, written as $\mathrm{Cent}(A)$, is called the *centre* of A. By (7.5.1), (7.5.2), $\mathrm{Cent}(A)$ is a unital commutative associative subalgebra of A. To illustrate why this is a useful idea, note that for $a \in \mathrm{Cent}(A)$ and $x, y \in A$, we have $(ay)x = a(yx)$ and $x(ay) = x(ya) = (xy)a = a(xy)$. It follows that, for every ideal $\mathfrak{a}$ of $\mathrm{Cent}(A)$, $\mathfrak{a}A$ is an ideal of A.

The assignment $\alpha \mapsto \alpha 1_A$ gives a unital homomorphism from k to $\mathrm{Cent}(A)$. If this homomorphism is an isomorphism, A is said to be *central*. By restricting the product of A to $\mathrm{Cent}(A) \times A$, we obtain a scalar multiplication on A by elements of the centre, that converts A into a central algebra over $\mathrm{Cent}(A)$, denoted by A_{cent} and called the *centralization* of A.

8.5 The nucleus. Slightly less important than the centre but still useful is the *nucleus* of a unital k-algebra A, defined by

$$\mathrm{Nuc}(A) := \{a \in A \mid [a, A, A] = [A, a, A] = [A, A, a] = \{0\}\}.$$

Evidently, $\mathrm{Cent}(A) \subseteq \mathrm{Nuc}(A)$. Following (7.5.2), the nucleus is a unital associative subalgebra of A, but will fail in general to be commutative. A subalgebra $B \subseteq A$ is said to be *nuclear* if it is unital (as a subalgebra) and is contained in the nucleus of A.

8.6 Simplicity and division algebras. A is said to be *simple* if it has non-trivial multiplication — so $A^2 \neq \{0\}$ — and $\{0\}$ and A are the only ideals of A. Examples are fields or, more generally, division algebras, where A is called a *division algebra* if it is non-zero and, for all $u, v \in A$, $u \neq 0$, the equations $ux = v$, $yu = v$ can be solved uniquely in A, equivalently, the left and right multiplication operators $L_u, R_u \colon A \to A$ for $0 \neq u \in A$ are both bijective. *Division algebras have no zero divisors*: if A is a division algebra and $x, y \in A$ satisfy $xy = 0$, then $x = 0$ or $y = 0$. Examples of division algebras are provided by arbitrary field extensions but also, for $k = \mathbb{R}$, by the Graves-Cayley octonions (1.8) and the Hamiltonian quaternions (1.12). Note that an algebra A over k with non-trivial multiplication is simple if and only if it is an irreducible $\mathrm{Mult}(A)$-module.

8.7 Matrices. For $n \in \mathbb{Z}$, $n > 0$, we write $\mathrm{Mat}_n(A)$ for the k-module of n-by-n matrices over A; it becomes a k-algebra under ordinary matrix multiplication. Moreover, if A is unital, then so is $\mathrm{Mat}_n(A)$, with identity element given by the n-by-n unit matrix $\mathbf{1}_n = (\delta_{ij} 1_A)_{1 \leq i,j \leq n}$ in terms of the Kronecker-delta, and the usual matrix units e_{ij}, $1 \leq i, j \leq n$, make sense in $\mathrm{Mat}_n(A)$: the (i, j)-th entry of e_{ij} is 1, while all other entries are 0. More generally, in obvious notation,

$$\mathrm{Mat}_n(A) = \bigoplus_{i,j=1}^{n} A e_{ij}$$

as a direct sum of k-modules (where each summand on the right identifies canonically with A as a k-module), and the expressions ae_{ij}, $a \in A$, $1 \le i, j \le n$, satisfy the multiplication rules

$$(ae_{ij})(be_{lm}) = \delta_{jl}(ab)e_{im} \qquad (a, b \in A,\ 1 \le i, j, l, m \le n). \tag{1}$$

8.8 Proposition. *Let $n \in \mathbb{Z}$, $n > 0$, and suppose A is unital. Then the assignment $\mathfrak{a} \mapsto \mathrm{Mat}_n(\mathfrak{a})$ gives an inclusion preserving bijection from the set of ideals in A to the set of ideals in $\mathrm{Mat}_n(A)$.*

Proof It suffices to show that any ideal in $\mathrm{Mat}_n(A)$ has the form $\mathrm{Mat}_n(\mathfrak{a})$ for some ideal $\mathfrak{a}$ in A, so let $I \subseteq \mathrm{Mat}_n(A)$ be an ideal and put $\mathfrak{a} := \{a \in A \mid ae_{11} \in I\}$. From (8.7.1) we deduce

$$(ab)e_{11} = (ae_{11})(be_{11}), \quad ae_{1j} = (ae_{11})e_{1j},$$
$$ae_{j1} = e_{j1}(ae_{11}), \quad \text{and} \quad ae_{ij} = e_{i1}(ae_{1j})$$

for $a, b \in A$, $1 \le i, j \le n$, which implies that $\mathfrak{a} \subseteq A$ is an ideal satisfying $\mathrm{Mat}_n(\mathfrak{a}) \subseteq I$. Conversely, let $x = \sum_{ij} a_{ij}e_{ij} \in I$, $a_{ij} \in A$. For $1 \le l, m \le n$, the matrix $a_{lm}e_{11} = \sum_{i,j}(e_{1l}(a_{ij}e_{ij}))e_{m1} = (e_{1l}x)e_{m1}$ is contained in I, forcing $a_{lm} \in \mathfrak{a}$, hence $x \in \mathrm{Mat}_n(\mathfrak{a})$, and the proposition is proved. □

8.9 Corollary. *Let A be unital and n a positive integer. Then $\mathrm{Mat}_n(A)$ is simple if and only if A is.* □

Exercises

8.10. *Ideals of finite direct products.* Let $(A_j)_{1 \le j \le n}$ be a finite family of unital k-algebras. Show that the ideals of the direct product $A = A_1 \times \cdots \times A_n$ (under the componentwise multiplication) are precisely of the form $I_1 \times \cdots \times I_n$ where I_j are ideals of A_j for $1 \le j \le n$. Does this conclusion also hold if the A_j, $1 \le j \le n$, are not assumed to be unital? Conclude that the decomposition of a unital algebra into the direct product of finitely many simple ideals, if at all possible, is unique up to order.

8.11. *Algebraic elements in power-associative algebras.* Let A be a unital power-associative algebra over a field F. An element $x \in A$ is said to be *algebraic* (over F) if the subalgebra $F[x] \subseteq A$ is finite-dimensional. In this case, generalizing the terminology introduced in 3.3, the unique monic polynomial of least degree in $F[\mathbf{t}]$ killing x is called the *minimum polynomial* of x (over F) and is denoted by μ_x; note that μ_x generates the ideal of all polynomials in $F[\mathbf{t}]$ killing x. We say that x is *split algebraic* (over F) if it is algebraic and its minimum polynomial decomposes into linear factors over F. The algebra A is called *algebraic* (resp. *split algebraic*) if every element of A has this property.

Now let x be a split algebraic element of A and write

$$\mu_x = \prod_{i=1}^{r} (\mathbf{t} - \alpha_i)^{n_i} \tag{1}$$

with positive integers $r, n_1, \dots, n_r$ and $\alpha_1, \dots, \alpha_r \in F$ distinct. Then prove:

(a) Setting $\mu_i := \frac{\mu_x}{(\mathbf{t}-\alpha_i)^{n_i}} \in F[\mathbf{t}]$ for $1 \le i \le r$, there are polynomials $f_1, \dots, f_r \in F[\mathbf{t}]$ such that $\sum_{i=1}^r \mu_i f_i = 1$. Conclude that $(c_1, \dots, c_r)$ with $c_i := \mu_i(x) f_i(x)$ for $1 \le i \le r$ is a complete orthogonal system of idempotents in $F[x]$, and that there exists an element $v \in F[x]$ satisfying

$$x = \sum_{i=1}^{r} \alpha_i c_i + v, \quad v^n = 0 \qquad (n := \max_{1 \le i \le r} n_i). \tag{2}$$

(b) $c \in F[x]$ is an idempotent if and only if there exists a subset $I \subseteq \{1, \dots, r\}$ such that $c = c_I := \sum_{i \in I} c_i$.

(c) The following conditions are equivalent.

(i) $\mathrm{Nil}(F[x]) = \{0\}$.
(ii) $n_1 = \cdots = n_r = 1$.
(iii) $x = \sum_{i=1}^r \alpha_i c_i$.

In this case, x is called *split semi-simple*.

(d) x is invertible in $F[x]$ if and only if $\alpha_i \neq 0$ for all $i = 1, \dots, r$.

(e) Assume $\mathrm{char}(F) \neq 2$ and that all α_i, $1 \le i \le r$, are non-zero squares in F. Then there exists a $y \in F[x]$ such that $y^2 = x$. (*Hint*: Reduce to the case $\alpha_1 = \cdots = \alpha_r = 1$.)

Remark. In the special case where $A = \mathrm{Mat}_d(F)$, the elements characterized in (c) are also called *diagonizable*.

8.12. *Central idempotents and direct sums of ideals.* Let A be a unital k-algebra. Idempotents of A belonging to the centre are said to be *central*. Show for a positive integer n that the assignment

$$(e_j)_{1 \le j \le n} \longmapsto (Ae_j)_{1 \le j \le n}$$

yields a bijection from the set of complete orthogonal systems of n central idempotents in A onto the set of decompositions of A into the direct sum of n complementary ideals.

8.13. *Primitive idempotents.* Let R be a commutative associative algebra of finite dimension over a field F. Note for an idempotent $c \in R$ that $Rc = \{x \in R \mid cx = x\} \subseteq R$ is a subalgebra containing c as its identity element.

(a) Prove that the following conditions are equivalent.

(i) c is *primitive*, i.e., $c \neq 0$ and c cannot be decomposed into the sum of two non-zero orthogonal idempotents.
(ii) c is the only non-zero idempotent in Rc.
(iii) $c \neq 0$ and the elements of Rc are either nilpotent or invertible (in Rc).

(b) Show that every idempotent in R splits into an orthogonal sum of primitive idempotents.

(c) Deduce from (a), (b) that R is isomorphic to the direct product of finite algebraic field extensions of F provided it contains no nilpotent elements other than zero.

8.14. Assume k is noetherian and let R be a unital commutative associative k-algebra containing an infinite orthogonal system of non-zero idempotents. Prove that R is not finitely generated as a k-algebra.

8.15. *Nucleus and centre of matrix algebras.* Let A be a unital k-algebra and n a positive integer. Show

$$\mathrm{Nuc}(\mathrm{Mat}_n(A)) = \mathrm{Mat}_n(\mathrm{Nuc}(A)), \quad \mathrm{Cent}(\mathrm{Mat}_n(A)) = \mathrm{Cent}(A)\mathbf{1}_n.$$

8.16. Let F be an algebraically closed field. Show that every finite-dimensional non-associative division algebra over F is isomorphic to F.

9 Scalar extensions

Scalar extensions belong to the most useful techniques in the study of modules and non-associative algebras over commutative rings. In this section, we briefly recall the main ingredients of this technique, remind the reader of some standard facts about projective modules and give a few applications to scalar extensions of simple algebras.

Throughout we let k be an arbitrary commutative ring.

9.1 The category k-alg. We denote by k-**alg** the category of unital commutative associative k-algebras. The objects of this category are commutative associative k-algebras containing an identity element, while its morphisms are k-algebra homomorphisms taking 1 into 1. In this language, the category of commutative rings is the same as $\mathbb{Z}$-**alg**. Note that an object of k-**alg** is basically nothing else than a commutative ring R, i.e., an object of $\mathbb{Z}$-**alg**, together with a ring homomorphism $k \to R$, called the *unit homomorphism* of $R \in k$-**alg**. The ring k together with its identity morphism is an initial object in k-**alg**, and the zero ring is the terminal object.

9.2 Scalar extensions of modules. We write k-**mod** for the category of k-modules, its objects being (left) k-modules and its morphisms being k-linear maps. For $M \in k$-**mod** and $R \in k$-**alg**, the k-module $M \otimes R$ may be converted into an R-module by the scalar multiplication

$$s(x \otimes r) = x \otimes (rs) \qquad (x \in M,\ r, s \in R). \tag{1}$$

This R-module, denoted by M_R, will be called the *scalar extension* or *base change* of M from k to R. If $f\colon M \to N$ is a k-linear map between k-modules, then

$$f_R := f \otimes \mathbf{1}_R\colon M_R \longrightarrow N_R, \quad x \otimes r \longmapsto f(x) \otimes r \tag{2}$$

is an R-linear map between R-modules, called the *base change* or *scalar extension* of f from k to R. Summing up, we thus obtain a functor from k-**mod** to

R-**mod**. We also have a natural map

$$\mathrm{can} := \mathrm{can}_M := \mathrm{can}_{M,R} \colon M \longrightarrow M_R, \quad x \longmapsto x_R := x \otimes 1_R, \tag{3}$$

which is k-linear but in general neither injective nor surjective. For any k-linear map $f \colon M \to N$, its R-linear extension $f_R \colon M_R \to N_R$ is the unique R-linear map making the diagram

$$\begin{array}{ccc} M & \xrightarrow[f]{} & N \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}} \\ M_R & \xrightarrow[f_R]{} & N_R \end{array} \tag{4}$$

commutative. Moreover, given an R-module M' and a k-linear map $g \colon M \to M'$, there is a unique R-linear map $g' \colon M_R \to M'$ such that $g' \circ \mathrm{can}_M = g$, namely the one given by

$$g'(x \otimes r) = rg(x) \qquad\qquad (x \in M,\ r \in R). \tag{5}$$

9.3 Reduction modulo an ideal. Let M be a k-module and $\mathfrak{a} \subseteq k$ an ideal. If we write $\alpha \mapsto \bar{\alpha}$ (resp. $x \mapsto \bar{x}$) for the canonical map from k to $\bar{k} := k/\mathfrak{a}$ (resp., from M to $\bar{M} := M/\mathfrak{a}M$), then $\bar{M}$ becomes a $\bar{k}$-module under the well-defined natural action

$$(\bar{\alpha}, \bar{x}) \longmapsto \overline{\alpha x} \qquad\qquad (\alpha \in k,\ \ x \in M)$$

from $\bar{k} \times \bar{M}$ to $\bar{M}$. We have $\bar{k} \in k$-**alg** and a natural identification $M_{\bar{k}} = \bar{M}$ as $\bar{k}$-modules such that

$$x \otimes \bar{\alpha} = \overline{\alpha x} \tag{1}$$

for $x \in M$ and $\alpha \in k$.

9.4 Iterated scalar extensions. Iterated scalar extensions collapse to simple ones: for $R \in k$-**alg**, we have R-**alg** $\subseteq k$-**alg** canonically as a faithful subcategory (though not a full one) and, given a k-module M, any $S \in R$-**alg** yields a natural identification $(M_R)_S = M_S$ as S-modules via

$$(x \otimes r) \otimes_R s = x \otimes (rs), \quad x \otimes s = (x \otimes 1_R) \otimes_R s = x_R \otimes_R s \tag{1}$$

for all $x \in M$, $r \in R$, $s \in S$. This identification is functorial in M, so we have $(x_R)_S = x_S$ for all $x \in M$ and $(\varphi_R)_S = \varphi_S$ for all k-linear maps $\varphi \colon M \to N$ of k-modules M, N. Moreover, the unit homomorphism $\vartheta \colon R \to S$, $r \mapsto r \cdot 1_S$, is a morphism in k-**alg** (even in R-**alg**) such that

$$(\mathbf{1}_M \otimes \vartheta)(x) = x_S \tag{2}$$

for all $x \in M_R$. Hence $\mathbf{1}_M \otimes \vartheta = \mathrm{can}_{M_R,S}$.

9.5 Localizations. Particularly important instances of scalar extensions are provided by localizations at prime ideals. Here are some of the relevant facts. Unless explicitly saying otherwise, we refer the reader to Bourbaki [27, II] for details and further reading.

We denote by $\mathrm{Spec}(k)$ the prime spectrum of k, i.e., the totality of prime ideals in k, endowed with the Zariski topology. Recall that a basis for this topology is provided by the *principal open sets*

$$D(f) := \{\mathfrak{p} \in \mathrm{Spec}(k) \mid f \notin \mathfrak{p}\} \subseteq \mathrm{Spec}(k) \qquad (f \in k). \tag{1}$$

We also put

$$V(Z) := \{\mathfrak{p} \in \mathrm{Spec}(k) \mid Z \subseteq \mathfrak{p}\} \qquad (Z \subseteq k), \tag{2}$$

$V(f) := V(\{f\}) = \mathrm{Spec}(k) \setminus D(f)$ for $f \in k$ and have $V(Z) = V(kZ)$ for $Z \subseteq k$. The open (resp. closed) subsets of $\mathrm{Spec}(k)$ relative to the Zariski topology are called *Zariski-open* (resp. *Zariski-closed*).

Let $\vartheta\colon k \to k'$ be a homomorphism of commutative rings, i.e., a morphism in $\mathbb{Z}$-**alg**. Then

$$\mathrm{Spec}(\vartheta)\colon\ \mathrm{Spec}(k') \to \mathrm{Spec}(k), \quad \mathfrak{p}' \mapsto \vartheta^{-1}(\mathfrak{p}'), \tag{3}$$

is a well-defined continuous map. In this way, Spec becomes a contra-variant functor from the category of commutative rings to the category of topological spaces.

The localization of k at a prime ideal $\mathfrak{p} \subseteq k$ will be denoted by $k_\mathfrak{p}$; it is a local ring, with maximal ideal denoted by $\mathfrak{p}_\mathfrak{p}$. The corresponding residue field, written as $k(\mathfrak{p}) = k_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$, agrees with the quotient field of $k/\mathfrak{p}$. Now let M be a k-module. We write $M_\mathfrak{p} := M \otimes k_\mathfrak{p}$ (resp. $M(\mathfrak{p}) := M \otimes k(\mathfrak{p}) = M_\mathfrak{p} \otimes_{k_\mathfrak{p}} k(\mathfrak{p})$) for the base change of M from k to $k_\mathfrak{p}$ (resp. to $k(\mathfrak{p})$), and obtain natural maps

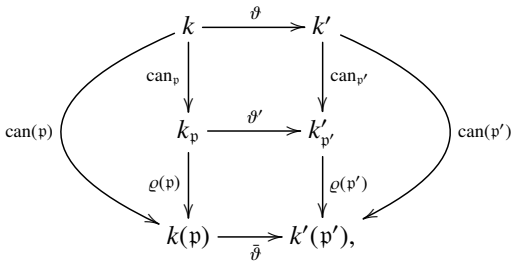
$$\mathrm{can}_\mathfrak{p} := \mathrm{can}_{M,k_\mathfrak{p}}\colon M \longrightarrow M_\mathfrak{p}, \quad x \longmapsto x_\mathfrak{p} := x_{k_\mathfrak{p}}, \tag{4}$$

$$\mathrm{can}(\mathfrak{p}) := \mathrm{can}_{M,k(\mathfrak{p})}\colon M \to M(\mathfrak{p}), \quad x \longmapsto x(\mathfrak{p}) := x_{k(\mathfrak{p})}. \tag{5}$$

Moreover, for any k-linear map $\varphi\colon M \to N$ of k-modules M, N, we put $\varphi_\mathfrak{p} := \varphi_{k_\mathfrak{p}}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ and $\varphi(\mathfrak{p}) := \varphi_{k(\mathfrak{p})}\colon M(\mathfrak{p}) \to N(\mathfrak{p})$.

Given a ring homomorphism $\vartheta\colon k \to k'$ as above, let $\mathfrak{p}' \in \mathrm{Spec}(k')$ and put

$\mathfrak{p} := \operatorname{Spec}(\vartheta)(\mathfrak{p}') = \vartheta^{-1}(\mathfrak{p}')$. Then we obtain a commutative diagram



(6)

where $\vartheta' \colon k_{\mathfrak{p}} \to k'_{\mathfrak{p}'}$ is the local homomorphism canonically induced by ϑ and $\varrho(\mathfrak{p}) \colon k_{\mathfrak{p}} \to k(\mathfrak{p})$ is the canonical projection, ditto for $\varrho(\mathfrak{p}')$. Hence ϑ' determines canonically a field homomorphism $\bar{\vartheta} \colon k(\mathfrak{p}) \to k(\mathfrak{p}')$, making the preceding diagram commutative and $k'(\mathfrak{p}')$ a field extension of $k(\mathfrak{p})$. Now let M be a k-module, regard k' (resp. $k'_{\mathfrak{p}'}$) as an element of k-**alg** (resp. $k_{\mathfrak{p}}$-**alg**) by means of ϑ (resp. ϑ') and put $M' := M_{k'}$ as a k'-module. Then (9.4.1) yields natural identifications

$$M'_{\mathfrak{p}'} = M_{\mathfrak{p}} \otimes_{k_{\mathfrak{p}}} k'_{\mathfrak{p}'} \tag{7}$$

as $k'_{\mathfrak{p}'}$-modules that are functorial in M. Similarly,

$$M'(\mathfrak{p}') = M(\mathfrak{p}) \otimes_{k(\mathfrak{p})} k'(\mathfrak{p}') \tag{8}$$

as vector spaces over $k'(\mathfrak{p}')$.

9.6 Principal open sets as spectra. For $f \in k$, we denote by

$$k_f := \{\alpha/f^n \mid \alpha \in k,\ n \in \mathbb{N}\} \tag{1}$$

the ring of fractions associated with the multiplicative subset $\{f^n \mid n \in \mathbb{N}\} \subseteq k$ and by

$$\operatorname{can}_f \colon k \longrightarrow k_f, \quad \alpha \longmapsto \alpha/1, \tag{2}$$

the canonical homomorphism, making k_f a k-algebra. The continuous map

$$\operatorname{Spec}(\operatorname{can}_f) \colon \operatorname{Spec}(k_f) \longrightarrow \operatorname{Spec}(k)$$

induces canonically a homeomorphism

$$\Phi_f \colon \operatorname{Spec}(k_f) \xrightarrow{\sim} D(f) \subseteq \operatorname{Spec}(k)$$

such that

$$\Phi_f(\mathfrak{q}) = \{\alpha \in k \mid \alpha/1 \in \mathfrak{q}\} \qquad (\mathfrak{q} \in \operatorname{Spec}(k_f)), \tag{3}$$

$$\Phi_f^{-1}(\mathfrak{p}) = \mathfrak{p}_f := \{\alpha/f^n \mid \alpha \in k,\ n \in \mathbb{N}\} \qquad (\mathfrak{p} \in D(f)). \tag{4}$$

Moreover, for $g \in k$, $n \in \mathbb{N}$, the principal open set $D(g/f^n) \subseteq \operatorname{Spec}(k_f)$ satisfies

$$\Phi_f(D(g/f^n)) = D(f) \cap D(g) = D(fg). \tag{5}$$

Finally, for a k-linear map $\varphi\colon M \to N$ of k-modules M, N, we denote by $\varphi_f := \varphi_{k_f}\colon M_{k_f} =: M_f \to N_f := N_{k_f}$ its k_f-linear extension.

9.7 Principal open sets of idempotents. Let $\varepsilon \in k$ be an idempotent and M a k-module. We put $\varepsilon_+ := \varepsilon$, $\varepsilon_- := 1 - \varepsilon$, $k_\pm = \varepsilon_\pm k$, $M_\pm := \varepsilon_\pm M = k_\pm M$ and have $k = k_+ \times k_-$ as a direct product of ideals, $M = M_+ \times M_-$ as a direct product of submodules. The projections

$$\pi_\pm\colon k \longrightarrow k_\pm, \quad \alpha \longmapsto \alpha_\pm := \varepsilon_\pm \alpha, \tag{1}$$

make $k_\pm$ elements of k-**alg**. Similarly, we have the projections $M \to M_\pm$, $x \mapsto x_\pm := \varepsilon_\pm x$, and obtain natural identifications

$$M_{k_\pm} = M \otimes k_\pm = M_\pm \tag{2}$$

as $k_\pm$-modules such that

$$x \otimes \alpha_\pm = \alpha_\pm x = \alpha_\pm x_\pm \qquad (\alpha_\pm \in k_\pm,\ x \in M). \tag{3}$$

Moreover, any k-linear map $\varphi\colon M \to N$ of k-modules M, N induces $k_\pm$-linear maps $\varphi_\pm\colon M_\pm \to N_\pm$ via restriction and $\varphi_\pm = \varphi_{k_\pm}$ is the base change of φ from k to $k_\pm$.

There is a unique morphism $\pi_{+\varepsilon}\colon k_\varepsilon \to k_+$ in k-**alg** that makes the diagram

$$\begin{array}{ccc} k & \xrightarrow{\pi_+} & k_+ \\ {\scriptstyle \mathrm{can}_\varepsilon}\downarrow & \nearrow_{\cong}\ {\scriptstyle \pi_{+\varepsilon}} & \\ k_\varepsilon, & & \end{array} \tag{4}$$

commutative and is actually an isomorphism. By 9.6, therefore,

$$\operatorname{Spec}(\pi_+)\colon\ \operatorname{Spec}(k_+) \to \operatorname{Spec}(k)$$

induces canonically a homeomorphism $\operatorname{Spec}(k_+) \xrightarrow{\sim} D(\varepsilon) \subseteq \operatorname{Spec}(k)$. Note that

$$\operatorname{Spec}(\pi_+)(\mathfrak{p}_+) = \mathfrak{p}_+ \times k_- \in D(\varepsilon) \tag{5}$$

for all $\mathfrak{p}_+ \in \operatorname{Spec}(k_+)$.

9.8 Projective modules. Recall that a k-module M is projective if it is a direct summand of a free k-module. This property is stable under base change, i.e., if M is projective as a k-module, then $M_R = M \otimes R$ is a projective R-module, for all $R \in k$-**alg**. A key result is Kaplansky's Theorem [271, Tag 0593]: If k is a local ring, then every projective k-module is free.

Let us use this result to define a notion of rank. When k is not the zero ring, $k^m \cong k^n$ if and only if $m = n$ [271, Tag 0FJ7]. We define the *rank* of the free module k^m, denoted $\mathrm{rk}(k^m)$, to be m. Note that this agrees with the notion of dimension of a vector space in case k is a field. For a free module M that is not finitely generated, we write simply $\mathrm{rk}(M) := \infty$, and do not bother to distinguish among infinite cardinals. When k is the zero ring, $k^m \cong k^n$ for all m, n and we do not define the notion of rank in this case. For a projective k-module M, by Kaplansky $M_\mathfrak{p}$ is free for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(k)$, and in this way we obtain a function

$$\mathrm{Spec}(k) \longrightarrow \mathbb{N} \cup \{\infty\}, \quad \mathfrak{p} \longmapsto \mathrm{rk}_\mathfrak{p}(M) := \mathrm{rk}_{k_\mathfrak{p}}(M_\mathfrak{p}) = \dim_{k(\mathfrak{p})}(M(\mathfrak{p})).$$

We call $\mathrm{rk}_\mathfrak{p}(M)$ the *rank of M at* $\mathfrak{p} \in \mathrm{Spec}(k)$.

For a projective k-module M and $r \in \mathbb{N}$, we say M *has rank* r if k is not the zero ring and $\mathrm{rk}_\mathfrak{p}(M) = r$ for all $\mathfrak{p} \in \mathrm{Spec}(k)$. This condition forces M to be finitely generated [288, Prop. 1.3]. If M is projective but not necessarily finitely generated, the preceding terminology makes sense and will be used also for $r = \infty$. Finally, a projective k-module is said to have *finite constant rank* if it has rank r, for some $r \in \mathbb{N}$. When we speak of the rank of a module, implicitly such a statement includes an assumption that $k \neq 0$.

We have by [271, Tag 00NX] or [27, II.5, Thm. 1] and [28, II.2, Cor. 1 of Prop. 4] that the following conditions are equivalent:

(i) M is finitely generated projective.

(ii) M is a direct summand of a free k-module of finite rank.

(iii) M is finitely generated and for all $\mathfrak{p} \in \mathrm{Spec}(k)$, the $k_\mathfrak{p}$-module $M_\mathfrak{p}$ is free, and the rank function of M is locally constant relative to the Zariski topology.

(iv) There exists a finite family $(f_i)_{i \in I}$ of elements in k generating k as an ideal such that, for all $i \in I$, the k_{f_i}-module M_{f_i} is free of finite rank.

For the case where we know that M is projective, we have the following criterion.

9.9 Lemma. *A projective k-module M is finitely generated if and only if $M_\mathfrak{p}$ is finitely generated for every $\mathfrak{p} \in \mathrm{Spec}(k)$ and the rank function of M is locally constant in the Zariski topology.*

Proof We first prove "if". For each $\mathfrak{p} \in \mathrm{Spec}(k)$ there is some $f_\mathfrak{p} \in k \setminus \mathfrak{p}$ such that the rank function is a finite constant on $D(f_\mathfrak{p})$, which we denote by $r_\mathfrak{p}$. Since $\mathrm{Spec}(k) = \cup D(f_\mathfrak{p})$ and $\mathrm{Spec}(k)$ is quasi-compact [27, II.4, Prop. 12], there exists a finite list $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of prime ideals such that $\mathrm{Spec}(k) =$

$\cup_{i=1}^{n} D(f_{\mathfrak{p}_i})$. In particular, the rank function has upper bound $\max\{r_{\mathfrak{p}_1}, \dots, r_{\mathfrak{p}_n}\}$, a finite number, so M is finitely generated by [288, Prop. 1.4].

Conversely, if M is generated by r elements, then so is $M_{\mathfrak{p}}$ for every prime $\mathfrak{p}$, whence $\mathrm{rk}_{\mathfrak{p}}(M) \leq r$. Property (iii) above completes the proof. □

9.10 Remark. We offer, without details, the following two interesting examples as cases where the hypotheses of the above results do not apply.

(i) Let $M \subset \mathbb{Q}$ be the set of rational numbers of the form a/b such that a, b are integers and b is not divisible by the square of any prime, viewed as a $\mathbb{Z}$-module. For every prime number p, M_p is free of rank 1, but M is neither finitely generated nor projective.

(ii) Let F be a field and take k to be the ring $\prod_{i\in\mathbb{N}} F$. (The space $\mathrm{Spec}(k)$ is identified with the Stone-Čech compactification of $\mathbb{N}$.) The k-module $\oplus_{i\in\mathbb{N}} F$ is projective and its rank at every $\mathfrak{p} \in \mathrm{Spec}(k)$ is 0 or 1. However, it is not finitely generated.

9.11 The dual module. If M is a k-module, then so is $M^* := \mathrm{Hom}_k(M, k)$, called the *dual* (*module*) of M. For example, in case $M = k^n$, the map

$$\begin{aligned} M &\to M^* \\ y &\mapsto (x \mapsto y^{\mathsf{T}} x) \end{aligned}$$

is an isomorphism [28, §II.2.6, Prop. 11]. It follows that the dual of a finitely generated projective module is also a finitely generated projective module.

If $f\colon M \to N$ is a morphism in k-**mod**, then so is $f^*\colon N^* \to M^*$, $y^* \mapsto y^* \circ f$. In this way, we obtain a contravariant additive functor $^*\colon k\text{-}\mathbf{mod} \to k\text{-}\mathbf{mod}$, called the *duality functor* of k-**mod**.

9.12 Line bundles. A *line bundle* over k is defined as a projective k-module of rank 1. This means that the following equivalent conditions are fulfilled.

(i) L is a finitely generated k-module and, for all $\mathfrak{p} \in \mathrm{Spec}(k)$, the $k_{\mathfrak{p}}$-module $L_{\mathfrak{p}}$ is free of rank 1.

(ii) There are finitely many elements $f_1, \dots, f_m \in k$ such that $\sum k f_i = k$ and, for each $i = 1, \dots, m$, the k_{f_i}-module L_{f_i} is free of rank 1.

For line bundles L, L' over k, we recall the following elementary but fundamental facts.

(a) $L \otimes L'$ and the dual module $L^* = \mathrm{Hom}_k(L, k)$ are line bundles over k.

(b) $\mathrm{Pic}(k) := \{[L] \mid L \text{ is a line bundle over } k\}$, where $[L]$ stands for the isomorphism class of L, is an abelian group under the operation $[L][L'] :=$

$[L \otimes L']$, with unit element and inverse of $[L]$ given by $[k]$ and $[L^*]$, respectively. $\mathrm{Pic}(k)$ is called the *Picard group* of k.

(c) For $R \in k$-**alg**, $L_R = L \otimes R$ is a line bundle over R and $L \mapsto L_R$ gives a group homomorphism $\mathrm{Pic}(k) \to \mathrm{Pic}(R)$. Thus we obtain a (covariant) functor Pic from k-**alg** to abelian groups.

(d) If $\varphi\colon L \to L'$ is an epimorphism, then it is, in fact, an isomorphism.

9.13 Unimodular elements. Fixing a k-module M, we write $(y^*, x) \mapsto \langle y^*, x\rangle$ for the canonical pairing $M^* \times M \to k$. Given $x \in M$,

$$\langle M^*, x\rangle := \{\langle y^*, x\rangle \mid y^* \in M^*\} \tag{1}$$

is an ideal in k. We say x is *unimodular* if $kx \subseteq M$ is a free submodule (of rank 1) and a direct summand of M at the same time. This obviously happens if and only if $\langle y^*, x\rangle = 1$ for some $y^* \in M^*$, i.e., $\langle M^*, x\rangle = k$; in this case, the k-module kx has (x) as a basis.

For example, an element x in the free module k^n is unimodular if and only if there is a $y \in k^n$ such that $y^{\mathsf{T}}x = 1_k$, if and only if the coordinates of x generate the unit ideal k.

Note that for an element x of a projective (hence free) module M over a *local* ring k to be unimodular it is necessary and sufficient that it can be extended to a basis of M. Indeed, if x is unimodular, choose any submodule N of M complementary to kx. Then N is free, and x together with any basis of N gives a basis of M extending x. Conversely, given any basis of M extending x, then kx is free, and the remaining basis vectors generate a submodule of M complementary to kx.

9.14 A notational ambiguity. Let M be a k-module, $x^* \in M^*$ and $R \in k$-**alg**. Then the symbol $x^*_R := (x^*)_R$ can be interpreted in two ways: on the one hand, as $x^*_R = x^* \otimes 1_R$ via (9.2.3), which belongs to $(M^*)_R$, on the other as $x^*_R = x^* \otimes \mathbf{1}_R\colon M_R \to k_R = R$ via (9.2.2), which belongs to $(M_R)^*$. In general, these interpretations lead to completely different objects, but, as the following result shows, in an important special case they may be identified under a canonical isomorphism. In fact, this isomorphism survives as a homomorphism in full generality as follows:

For a k-module M and any $R \in k$-**alg** as above, the assignment $x^* \mapsto x^* \otimes \mathbf{1}_R$ determines a k-linear map $M^* \to (M_R)^*$, which by (9.2.5) gives rise to an R-linear map $\varphi\colon (M^*)_R \to (M_R)^*$ satisfying $\varphi(x^* \otimes r) = r(x^* \otimes \mathbf{1}_R)$ for all $x^* \in M^*$, $r \in R$.

9.15 Lemma. *Let M be a finitely generated projective k-module and $R \in k$-**alg**.*

Then the natural map

$$\varphi\colon (M^*)_R \xrightarrow{\sim} (M_R)^*, \quad x^* \otimes r \longmapsto r(x^* \otimes \mathbf{1}_R)$$

is an isomorphism of R-modules. Identifying $(M^*)_R = (M_R)^* =: M_R^*$ *by means of this isomorphism, we have* $\langle x^*, x\rangle_R = \langle x_R^*, x_R\rangle$ *for all* $x \in M$, $x^* \in M^*$, *in other words, the canonical pairing* $M_R^* \times M_R \to R$ *is the R-bilinear extension of the canonical pairing* $M^* \times M \to k$.

Proof We must show that φ is bijective. Since φ is additive in M, we may assume that M is free of finite rank, with basis $(e_i)_{1\le i\le n}$. Let $(e_i^*)_{1\le i\le n}$ be the corresponding dual basis of M^*. Then (e_{iR}), (e_{iR}^*) are R-bases of M_R, $(M^*)_R$, respectively, while the family $(e_i^* \otimes \mathbf{1}_R)$ of elements of $(M_R)^*$ is dual to (e_{iR}), hence forms the corresponding dual basis of $(M_R)^*$. But $\varphi(e_i^* \otimes 1_R) = e_i^* \otimes \mathbf{1}_R$ for $1 \le i \le n$, forcing φ to be an isomorphism. Finally, using φ to identify $(M^*)_R = (M_R)^*$ and letting $x \in M$, $x^* \in M^*$, we conclude $\langle x_R^*, x_R\rangle = \langle x^* \otimes 1_R, x_R\rangle = \langle x^* \otimes \mathbf{1}_R, x \otimes 1_R\rangle = \langle x^*, x\rangle \otimes 1_R = \langle x^*, x\rangle_R$. □

9.16 Lemma (Loos [174, 0.3])**.** *Assume M is a finitely generated projective k-module and let* $x \in M$. *For each prime ideal* $\mathfrak{p}$ *of k,* $x(\mathfrak{p}) = 0$ *if and only if* $\langle M^*, x\rangle \subseteq \mathfrak{p}$.

Proof $M(\mathfrak{p})$ being a vector space over $k(\mathfrak{p})$, we have $x(\mathfrak{p}) = 0$ if and only if $\langle y^*, x(\mathfrak{p})\rangle = 0$ for all $y^* \in M(\mathfrak{p})^*$. Identifying $M(\mathfrak{p})^* = M^*(\mathfrak{p})$ by means of Lemma 9.15, we therefore obtain

$$\begin{aligned} x(\mathfrak{p}) = 0 &\iff \langle y^*(\mathfrak{p}), x(\mathfrak{p})\rangle = 0 && \text{for all } y^* \in M^* \\ &\iff \langle y^*, x\rangle(\mathfrak{p}) = 0 && \text{for all } y^* \in M^* \\ &\iff \langle y^*, x\rangle \in \mathfrak{p} && \text{for all } y^* \in M^*. \end{aligned}$$

That is, $\langle M^*, x\rangle \subseteq \mathfrak{p}$. □

9.17 Lemma. *Consider the following conditions, for a k-module M and* $x \in M$.

(i) x *is unimodular.*
(ii) $x_R \neq 0$ *for all non-zero* $R \in k$-**alg**.
(iii) $x_K \neq 0$ *for all fields* $K \in k$-**alg**.
(iv) $x(\mathfrak{p}) \neq 0$ *for all* $\mathfrak{p} \in \operatorname{Spec}(k)$.

Then the implications

$$(i) \Longrightarrow (ii) \Longleftrightarrow (iii) \Longleftrightarrow (iv)$$

hold. If M is finitely generated projective, then all four conditions are equivalent.

Proof The implications (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) are obvious. If M is finitely generated projective and (iv) holds, then by Lemma 9.16 $\langle M^*, x\rangle$ is an ideal of k not contained in any prime ideal, so it is all of k and (i) holds. It remains to prove (iv) ⇒ (iii) ⇒ (ii)

(iv) ⇒ (iii). If $K \in k$-**alg** is a field, then the kernel of the unit morphism $k \to K$ is a prime ideal $\mathfrak{p} \subseteq k$, making K a field containing $k(\mathfrak{p})$, and $x_K = x(\mathfrak{p})_K \neq 0$ by (iv).

(iii) ⇒ (ii). Let $\{0\} \neq R \in k$-**alg** and $\mathfrak{m} \subseteq R$ be a maximal ideal. Then $K := R/\mathfrak{m} \in k$-**alg** is a field and $(x_R)_K = x_K \neq 0$ by (iv), forcing $x_R \neq 0$. □

9.18 Tensor products of algebras. Given k-algebras A, B, the k-module $A \otimes B$ is again a k-algebra under the multiplication

$$(x_1 \otimes y_1)(x_2 \otimes y_2) = (x_1x_2) \otimes (y_1y_2) \qquad (x_i \in A, y_i \in B, i = 1, 2). \tag{1}$$

Moreover, if A and B are both unital, so is $A \otimes B$, with unit element $1_{A\otimes B} = 1_A \otimes 1_B$. For example, given any unital k-algebra A and a positive integer n, we have a natural identification $\mathrm{Mat}_n(k)\otimes A = \mathrm{Mat}_n(A)$ such that $x\otimes a = xa = (\xi_{ij}a)$ for $x = (\xi_{ij}) \in \mathrm{Mat}_n(k)$, $a \in A$.

Now let A be a k-algebra and $R \in k$-**alg**. Then the R-module structure of A_R (9.2) is compatible with the k-algebra structure of $A \otimes R$ as defined in (1). In other words, A_R is canonically an R-algebra, and the observations made in 9.2–9.13 carry over mutatis mutandis from modules to algebras. In particular, the assignment $A \mapsto A_R$ gives a functor from k-algebras to R-algebras.

We now give applications of the preceding set-up to simple algebras.

9.19 Proposition. *Let A be a unital k-algebra. Then the right multiplication of A induces an isomorphism*

$$R\colon\ \mathrm{Cent}(A) \xrightarrow{\sim} \mathrm{End}_{\mathrm{Mult}(A)}(A)$$

of k-algebras.

Proof For $a \in \mathrm{Cent}(A)$, R_a clearly belongs to $\mathrm{End}_{\mathrm{Mult}(A)}(A)$, so we obtain a unital homomorphism $R\colon\ \mathrm{Cent}(A) \to \mathrm{End}_{\mathrm{Mult}(A)}(A)$, which is obviously injective. To show that it is also surjective, let $d \in \mathrm{End}_{\mathrm{Mult}(A)}(A)$ act on A from the right by juxtaposition. Then $(xy)d = x(yd) = (xd)y$ for all $x, y \in A$. Putting $y = 1_A$, we conclude $d = R_a$, where $a := 1_Ad$. Hence the preceding relation is equivalent to $(xy)a = x(ya) = (xa)y$, which in turn is easily seen to imply that a belongs to the centre of A. □

9.20 Corollary. *The centre of a unital simple algebra is a field.*

Proof Since $\mathrm{Mult}(A)$ acts irreducibly on A, it suffices to combine Proposition 9.19 with Schur's lemma [142, p. 118]. □

For the remainder of this section, we use Prop. 9.19 to identify $\mathrm{Cent}(A) = \mathrm{End}_{\mathrm{Mult}(A)}(A)$ for any unital k-algebra A.

9.21 Corollary. *Let A be a unital finite-dimensional algebra over a field F and suppose A is simple. Then* $\mathrm{End}_{\mathrm{Cent}(A)}(A) = \mathrm{Mult}(A)$.

Proof Since $\mathrm{Mult}(A)$ acts faithfully and irreducibly on A, it is a primitive Artinian F-algebra [142, Def. 4.1], hence simple [142, Thm. 4.2]. Moreover, by Proposition 9.19, its centralizer in $\mathrm{End}_F(A)$ is $\mathrm{Cent}(A)$. Thus the assertion follows from the double centralizer theorem [142, Thm. 4.10]. □

Algebras that are both central and simple are called *central simple*.

9.22 Corollary. *A unital finite-dimensional algebra A over a field F is central simple if and only if it is non-zero and* $\mathrm{Mult}(A) = \mathrm{End}_F(A)$.

Proof If A is central simple, the assertion follows from Cor. 9.21. Conversely, suppose $A \neq \{0\}$ and $\mathrm{Mult}(A) = \mathrm{End}_F(A)$. Then A is simple, and Cor. 9.21 implies that $\mathrm{Cent}(A)$ belongs to the centre of $\mathrm{End}_F(A)$. Hence A is central. □

9.23 Corollary. *For a unital finite-dimensional algebra A over a field F, the following conditions are equivalent.*

(i) *A is central simple.*
(ii) *$A \otimes F'$ is central simple for every field $F' \in F$-**alg**.*
(iii) *$A \otimes \bar{F}$ is simple, where $\bar{F}$ denotes the algebraic closure of F.*

Proof (i) $\Rightarrow$ (ii). Let F' be an extension field of F and put $A' = A \otimes F'$ as an F'-algebra. After identifying $\mathrm{End}_{F'}(A') = \mathrm{End}_F(A) \otimes F'$ canonically, a moment's reflection shows $\mathrm{Mult}(A') = \mathrm{Mult}(A) \otimes F'$. Hence the assertion follows from Cor. 9.22.

The implication (ii) $\Rightarrow$ (iii) is obvious.

(iii) $\Rightarrow$ (i). If $I \subseteq A$ is a non-trivial ideal, then so is $I \otimes \bar{F} \subseteq A \otimes \bar{F}$, a contradiction. Hence A is simple. By Exc. 9.33 (a), $\mathrm{Cent}(A) \otimes \bar{F}$ agrees with the centre of $A \otimes \bar{F}$ and therefore is a finite algebraic field extension of $\bar{F}$. As such, it has degree 1, forcing $\mathrm{Cent}(A) = F1_A$, and A is central. □

Exercises

9.24. *Centre and nucleus under base change.* Show that the centre (resp. the nucleus) of a unital k-algebra A in general does not commute with base change, even if one assumes that the centre (resp. the nucleus) is free of finite rank and a direct summand

of A as a k-module. (*Hint*: Let A be the unital $\mathbb{Z}$-algebra given on a free $\mathbb{Z}$-module of rank 3 with basis $1_A, x, y$ by the multiplication table $x^2 = 2 \cdot 1_A$, $xy = yx = y^2 = 0$ and consider its base change to $R := \mathbb{Z}/2\mathbb{Z} \in \mathbb{Z}$-**alg**.)

9.25. Let A be a nonassociative F-algebra for a field F and suppose the dimension of A, as a vector space, is finite. Prove:

(a) If A has no zero divisors, then A is a division algebra in the sense of 8.6.
(b) If A is a division algebra, then so is A_K for $K = F(\mathbf{t})$ or $F((\mathbf{t}))$.

9.26. Call a unital commutative associative k-algebra k' with unit morphism $\vartheta\colon k \to k'$ a *cover* of k if the induced map $\operatorname{Spec}(\vartheta)\colon \operatorname{Spec}(k') \to \operatorname{Spec}(k)$ is surjective. Prove: For every field $K \in k$-**alg** and cover k' of k, there are a field $K' \in k'$-**alg** and a homomorphism $K \to K'$ making the diagram

$$\begin{array}{ccc} K & \longrightarrow & K' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\vartheta} & k' \end{array}$$

commutative.

9.27. *Fibers of prime spectra.* Let $\varphi\colon k \to k'$ be a homomorphism of commutative rings, let $\mathfrak{p} \in \operatorname{Spec}(k)$ and view k' as a k-algebra by means of φ. Consider the ring homomorphism

$$\operatorname{can}(\mathfrak{p}) = \operatorname{can}_{k',k(\mathfrak{p})}\colon k' \longrightarrow k'(\mathfrak{p}) = k' \otimes k(\mathfrak{p}), \quad \alpha' \longmapsto \operatorname{can}(\mathfrak{p})(\alpha') = \alpha'(\mathfrak{p}) = \alpha' \otimes 1_{k(\mathfrak{p})}$$

and show that the continuous map

$$\operatorname{Spec}(\operatorname{can}(\mathfrak{p}))\colon \operatorname{Spec}(k'(\mathfrak{p})) \longrightarrow \operatorname{Spec}(k')$$

induces canonically a homeomorphism

$$\operatorname{Spec}(k'(\mathfrak{p})) \xrightarrow{\sim} \operatorname{Spec}(\varphi)^{-1}(\mathfrak{p}),$$

where the right-hand side carries the topology induced by the Zariski topology of $\operatorname{Spec}(k')$.

9.28. Put $X := \operatorname{Spec}(k)$.

(a) Let $\psi, \chi\colon M \to N$ be k-linear maps of k-modules and suppose M is finitely generated. Show that

$$U := \{\mathfrak{p} \in X \mid \psi_{\mathfrak{p}} = \chi_{\mathfrak{p}}\}$$

is a Zariski-open subset of X.

(b) Let $\varphi\colon A \to B$ be a k-linear map of k-algebras and suppose A is finitely generated as a k-module. Prove that

$$V := \{\mathfrak{p} \in X \mid \varphi_{\mathfrak{p}}\colon A_{\mathfrak{p}} \to B_{\mathfrak{p}} \text{ is an algebra homomorphism}\}$$

is a Zariski-open subset of X.

9.29. *Idempotents and partitions.* Consider $X = \operatorname{Spec}(k)$ under the Zariski topology as in 9.5.

(a) Let $\varepsilon \in k$ be an idempotent. Prove

$$D(\varepsilon) = \{\mathfrak{p} \in X \mid \varepsilon_{\mathfrak{p}} = 1_{\mathfrak{p}}\} = \{\mathfrak{p} \in X \mid \varepsilon_{\mathfrak{p}} \neq 0\} = V(1-\varepsilon).$$

Conclude for an orthogonal system $(\varepsilon_i)_{i\in I}$ of idempotents in k satisfying $\varepsilon_i = 0$ for almost all $i \in I$ that $\bigcup D(\varepsilon_i) = D(\sum \varepsilon_i)$ and the union on the left is disjoint.

(b) Prove that the assignment $(\varepsilon_i)_{i\in I} \mapsto (D(\varepsilon_i))_{i\in I}$ yields a bijection from the set of complete orthogonal systems of idempotents in k in the sense of 8.2 (b) onto the set of decompositions of X into the disjoint union of open subsets almost all of which are empty. (*Hint*: To prove surjectivity, you may either argue with the structure sheaf of the geometric (= locally ringed) space attached to k (Grothendieck [107, Chap. 1, §1], Demazure-Gabriel [61, I, §1, no. 1,2, particularly Prop. 2.6], Hartshorne [116, II, §2]) or imitate the proof of Bourbaki [27, II.4, Prop. 15], but watch out in the latter case for a sticky point in the argument.)

9.30. Suppose M and N are projective k-modules, M is finitely generated, and $f\colon M \to N$ is a k-linear map. Prove: f is an isomorphism if the induced map $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective and $\mathrm{rk}_{\mathfrak{m}}(M) = \mathrm{rk}_{\mathfrak{m}}(N)$ for every maximal ideal $\mathfrak{m}$ of k.

9.31. *Rank decomposition.* Let M be a finitely generated projective k-module. Prove:

(a) The set

$$\mathrm{Rk}(M) := \{\mathrm{rk}_{\mathfrak{p}}(M) \mid \mathfrak{p} \in \mathrm{Spec}(k)\}$$

is finite.

(b) There exists a unique complete orthogonal system $(\varepsilon_i)_{i\in\mathbb{N}}$ of idempotents in k such that, with the induced decompositions

$$k = \prod_{i\in\mathbb{N}} k_i, \quad k_i = k\varepsilon_i \qquad (i \in \mathbb{N}), \tag{1}$$

$$M = \prod_{i\in\mathbb{N}} M_i, \quad M_i = M \otimes k_i \qquad (i \in \mathbb{N}) \tag{2}$$

as direct product of ideals (resp. of additive subgroups), the k_i-modules M_i are finitely generated projective of rank i, for all $i \in \mathbb{N}$ having $k_i \neq \{0\}$. Show further that $\varepsilon_i = 0$ for all $i \in \mathbb{N} \setminus \mathrm{Rk}(M)$.

Remark. Equation (2) is called the *rank decomposition of M*. It remains virtually unchanged by ignoring the components belonging to some or all indices $i \in \mathbb{N} \setminus \mathrm{Rk}(M)$. Note also that, if M carries an algebra structure, (2) is a direct product of ideals.

9.32. *Residually simple algebras.* (Cf. Knus [157, III, (5.1.8)]) Let A, A' be unital k-algebras that are finitely generated projective of the same rank $r \in \mathbb{N}$ as k-modules. Suppose A is *residually simple*, so $A(\mathfrak{p})$ is a simple algebra over the field $k(\mathfrak{p})$, for all $\mathfrak{p} \in \mathrm{Spec}(k)$. Prove that every unital algebra homomorphism from A to A' is an isomorphism.

9.33. *Groups of antomorphisms*[1]. By an *algebra with a group of antomorphisms* over k we mean a pair (A, G) consisting of a k-algebra A and a group G of automorphisms or anti-automorphisms of A. An *ideal* of (A, G) is an ideal of A which is stabilized by

[1] This is *not* a misprint.

every element of G. We say that (A, G) is *simple* if $A^2 \neq \{0\}$ and there are no ideals of (A, G) other than $\{0\}$ and A. If A contains an identity element, in which case we also say that (A, G) is *unital*, we define the *centre* of (A, G) as the set of elements in the centre of A that remain fixed under G:

$$\mathrm{Cent}(A, G) = \{a \in \mathrm{Cent}(A) \mid g(a) = a \text{ for all } g \in G\}.$$

If the natural map from k to $\mathrm{Cent}(A, G)$ is an isomorphism of k-algebras, then (A, G) is said to be *central*. Unital algebras with a group of antomorphisms which are both central and simple are called *central simple*. By the *multiplication algebra* of (A, G), written as $\mathrm{Mult}(A, G)$, we mean the unital subalgebra of $\mathrm{End}_k(A)$ generated by G and all left and right multiplication operators affected by arbitrary elements of A. Base change of algebras with a group of antomorphisms is defined canonically. Note that ordinary k-algebras are algebras with a group of antomorphisms in a natural way, as are algebras with involution.

Now let F be a field and (A, G) an F-algebra with a group of antomorphisms. Then prove:

(a) $\mathrm{Cent}((A, G) \otimes R) = (\mathrm{Cent}(A, G)) \otimes R$ as R-algebras, for any $R \in F$-**alg**.

(b) The right multiplication of A induces an isomorphism

$$R\colon\ \mathrm{Cent}(A, G) \xrightarrow{\sim} \mathrm{End}_{\mathrm{Mult}(A,G)}(A)$$

of F-algebras.

(c) The centre of a unital simple algebra with a group of antomorphisms is a field.

(d) If (A, G) is finite-dimensional, then $\mathrm{End}_{\mathrm{Cent}(A,G)}(A) = \mathrm{Mult}(A, G)$, and for (A, G) to be central simple it is necessary and sufficient that $A \neq \{0\}$ and $\mathrm{Mult}(A, G) = \mathrm{End}_F(A)$.

9.34. *Central simplicity of algebras with groups of antomorphisms.* Let (A, G) be a finite-dimensional unital algebra with a group of antomorphisms over a field F. Show that the following conditions are equivalent.

(i) (A, G) is central simple.
(ii) Every base field extension of (A, G) is central simple.
(iii) $(A, G) \otimes \bar{F}$ is simple, where $\bar{F}$ denotes the algebraic closure of k.

9.35. *Tensor products of algebras with groups of antomorphisms.* Let $(A, G), (A', G')$ be unital algebras with a group of antomorphisms over a field F and suppose (i) A is commutative or $G' \subseteq \mathrm{Aut}(A')$, and (ii) A' is commutative or $G \subseteq \mathrm{Aut}(A)$. Define $(A, G) \otimes (A', G') = (A \otimes A', G \otimes G')$, where $G \otimes G'$ is supposed to consist of all $g \otimes g'$, $g \in G, g' \in G'$ having the same *parity* in the sense that they are both either automorphisms or anti-automorphisms of A, A', respectively. Show that if (A, G) is central simple and (A', G') is simple, then $(A, G) \otimes (A', G')$ is simple.

10 Involutions

Involutions of associative algebras are a profound concept with important connections to other branches of algebra and arithmetic. An in-depth account of this concept over fields may be found in Knus-Merkurjev-Rost-Tignol [160].

Over arbitrary commutative rings, the reader may consult Knus [157, III, §8] for useful results on the subject. In the present section, elementary properties of involutions will be studied for unital non-associative algebras over an arbitrary commutative ring k.

10.1 Algebras with involution. An *involution* of a unital k-algebra B is a k-linear map $\tau\colon B \to B$ satisfying the following conditions.

(i) τ is *involutorial*, i.e., $\tau^2 = \mathbf{1}_B$.
(ii) τ is an *anti-homomorphism*, i.e., $\tau(xy) = \tau(y)\tau(x)$ for all $x, y \in B$.

In particular, τ is bijective, hence by (ii) may be viewed as an isomorphism $\tau\colon B \to B^{\mathrm{op}}$ of k-algebras, where the *opposite algebra* B^{op} lives on the same k-module as B under the new multiplication $x \cdot y := yx$ for $x, y \in B$. Examples of involutions are provided by the conjugation of the Graves-Cayley octonions or the Hamiltonian quaternions (Exc. 1.18 (a)) and by the map $x \mapsto \bar{x}^{\mathsf{T}}$ on matrices over those algebras as in 5.2.

10.2 Homomorphisms, base change and ideals of algebras with involution. By a *k-algebra with involution* we mean a pair (B, τ) consisting of a unital k-algebra B and an involution τ of B. A *homomorphism* $h\colon (B, \tau) \to (B', \tau')$ of k-algebras with involution is a unital homomorphism $h\colon B \to B'$ of k-algebras that respects the involutions, i.e., $\tau' \circ h = h \circ \tau$. In this way, we obtain the category of k-algebras with involution. If (B, τ) is a k-algebra with involution, then $(B, \tau)_R := (B_R, \tau_R)$ for $R \in k$-**alg** is an R-algebra with involution, called the *scalar extension* or *base change* of (B, τ) from k to R. By an *ideal* of (B, τ) we mean an ideal $I \subseteq B$ that is stabilized by τ: $\tau(I) = I$. In this case, $(B, \tau)/I := (\bar{B}, \bar{\tau})$, with $\bar{B} := B/I$ and $\bar{\tau}\colon \bar{B} \to \bar{B}$ being the k-linear map canonically induced by τ, is a k-algebra with involution making the canonical projection $B \to \bar{B}$ a homomorphism $(B, \tau) \to (\bar{B}, \bar{\tau})$ of k-algebras with involution.

10.3 The centre of an algebra with involution. If (B, τ) is a k-algebra with involution, then τ stabilizes the centre of B and via restriction yields an involution of $\mathrm{Cent}(B)$, i.e., an automorphism of period 2. We call

$$\mathrm{Cent}(B, \tau) := \{a \in \mathrm{Cent}(B) \mid \tau(a) = a\}$$

the *centre* of (B, τ). It is a unital (and commutative and associative) subalgebra of $\mathrm{Cent}(B)$.

10.4 Simplicity and the exchange involution. Let (B, τ) be a k-algebra with involution. We say that (B, τ) is *simple* (as an algebra with involution) if $B \neq \{0\}$ and there are no ideals of (B, τ) other than $\{0\}$ and B. If B is simple, so obviously is (B, τ). The converse, however, does not hold. To see this, we consider the following class of examples.

Let A be a unital k-algebra. Then a straightforward verification shows that the map

$$\varepsilon_A : A \times A^{\mathrm{op}} \longrightarrow A \times A^{\mathrm{op}}, \quad (x, y) \longmapsto \varepsilon_A((x, y)) := (y, x),$$

is an involution, called the *exchange involution* (or *switch*) of $A \times A^{\mathrm{op}}$.

10.5 Proposition. *Let (B, τ) be a k-algebra with involution. For (B, τ) to be simple as an algebra with involution it is necessary and sufficient that B be simple or there exist a simple unital k-algebra A such that $(B, \tau) \cong (A \times A^{\mathrm{op}}, \varepsilon_A)$.*

Proof By Exc. 8.10, the condition is clearly sufficient. Conversely, suppose (B, τ) is simple but B is not. Let $\{0\} \neq I \subset B$ be any proper ideal of B. Then $I + \tau(I)$, $I \cap \tau(I)$ are both ideals of (B, τ), the former being different from $\{0\}$, the latter being different from B. Since (B, τ) is simple, we conclude $B = I \oplus \tau(I)$ as a direct sum of ideals. Regarding $A = I$ as a unital k-algebra in its own right, any non-zero ideal J of A is a proper ideal of B, so by what we have just shown, $B = J \oplus \tau(J)$, which implies $J = A$, and A is simple. One now checks easily that the map

$$(A \times A^{\mathrm{op}}, \varepsilon_A) \xrightarrow{\sim} (B, \tau), \quad (x, y) \longmapsto x + \tau(y),$$

is an isomorphism of algebras with involution. □

10.6 Symmetric and skew elements. Let (B, τ) be a k-algebra with involution. Following the notational conventions of [160, I, §2], we put

$$H(B, \tau) := \mathrm{Sym}(B, \tau) := \{x \in B \mid \tau(x) = x\}, \tag{1}$$

$$\mathrm{Symd}(B, \tau) := \{y + \tau(y) \mid y \in B\}, \tag{2}$$

$$\mathrm{Skew}(B, \tau) := \{x \in B \mid \tau(x) = -x\}, \tag{3}$$

$$\mathrm{Alt}(B, \tau) := \{y - \tau(y) \mid y \in B\}, \tag{4}$$

which are all submodules of B, the first one among these containing the identity of B. The elements of $\mathrm{Sym}(B, \tau)$ (resp. $\mathrm{Skew}(B, \tau)$) are called *τ-symmetric* (resp. *τ-skew*). We always have

$$\mathrm{Symd}(B, \tau) \subseteq \mathrm{Sym}(B, \tau) \quad \text{and} \quad \mathrm{Alt}(B, \tau) \subseteq \mathrm{Skew}(B, \tau).$$

Moreover, if 2 is invertible in k, then $\mathrm{Sym}(B, \tau) = \mathrm{Symd}(B, \tau)$, $\mathrm{Skew}(B, \tau) = \mathrm{Alt}(B, \tau)$, and $B = \mathrm{Sym}(B, \tau) \oplus \mathrm{Skew}(B, \tau)$ as a direct sum of submodules. At the other extreme, if $2 = 0$ in k, then $\mathrm{Sym}(B, \tau) = \mathrm{Skew}(B, \tau)$ and $\mathrm{Symd}(B, \tau) = \mathrm{Alt}(B, \tau)$.

10.7 The conjugate transpose involution. Let B be a unital k-algebra and

$\tau\colon B \to B$, $x \mapsto \bar{x}$, an involution of B. Given $n \in \mathbb{Z}$, $n > 0$, it is readily checked that the map

$$\mathrm{Mat}_n(\tau)\colon\ \mathrm{Mat}_n(B) \longrightarrow \mathrm{Mat}_n(B), \quad x \longmapsto \bar{x}^{\mathsf{T}},$$

that sends an n-by-n matrix over B into its conjugate transpose, is an involution of $\mathrm{Mat}_n(B)$, called the *conjugate transpose involution* induced by τ. We put

$$\mathrm{Mat}_n(B,\tau) := (\mathrm{Mat}_n(B), \mathrm{Mat}_n(\tau)), \quad \mathrm{Sym}_n(B,\tau) := \mathrm{Sym}(\mathrm{Mat}_n(B), \mathrm{Mat}_n(\tau)).$$

In the special case $B = k$, $\tau = \mathbf{1}_k$, we obtain

$$\tau_{\mathrm{ort}}\colon\ \mathrm{Mat}_n(k) \longrightarrow \mathrm{Mat}_n(k), \quad S \longmapsto \tau(S) := S^{\mathsf{T}},$$

called the *split orthogonal involution of degree n* over k. We put

$$\mathrm{Sym}_n(k) :=\ \mathrm{Sym}_n(k, \mathbf{1}_k) = \{S \in \mathrm{Mat}_n(k) \mid S = S^{\mathsf{T}}\}, \tag{1}$$

$$\mathrm{Skew}_n(k) :=\ \mathrm{Skew}\,(\mathrm{Mat}_n(k), \tau_{\mathrm{ort}}) = \{S \in \mathrm{Mat}_n(k) \mid S^{\mathsf{T}} = -S\}. \tag{2}$$

In particular, $\mathrm{Sym}_n(k)$ is a free k-module of rank $\frac{1}{2}n(n+1)$.

10.8 Twisting involutions. Let (B,τ) be a k-algebra with involution and $q \in \mathrm{Nuc}(B)^\times$ an invertible element of the unital associative subalgebra $\mathrm{Nuc}(B) \subseteq B$ (8.5). Then the map $B \to B$, $x \mapsto q^{-1}xq$ is an unambiguously defined automorphism, forcing

$$\tau^q\colon\ B \longrightarrow B, \quad x \longmapsto \tau^q(x) := q^{-1}\tau(x)q, \tag{1}$$

to be an anti-automorphism of B. Moreover τ^q is an involution provided $\tau(q) = \pm q$, in which case we sometimes call τ^q the *q-twist* of τ

10.9 Alternating matrices. For $n \in \mathbb{Z}$, $n > 0$, a matrix $S \in \mathrm{Mat}_n(k)$ is said to be *alternating* if it satisfies one (hence all) of the following equivalent conditions.

(i) S is skew-symmetric and its diagonal entries are zero.
(ii) $S = T - T^{\mathsf{T}}$ for some $T \in \mathrm{Mat}_n(k)$.
(iii) $x^{\mathsf{T}} S\, x = 0$ for all $x \in k^n$.

The submodule of $\mathrm{Mat}_n(k)$ consisting of all alternating n-by-n matrices over k will be denoted by $\mathrm{Alt}_n(k)$. By 10.7 and (10.6.4), we obviously have $\mathrm{Alt}_n(k) = \mathrm{Alt}(\mathrm{Mat}_n(k), \tau_{\mathrm{ort}})$, which is a free k-module of rank $\frac{n(n-1)}{2}$.

10.10 The split symplectic involution. Let n be a positive integer.

(a) We begin by viewing the elements of $\mathrm{Mat}_{2n}(k)$ as 2-by-2 blocks of n-by-n matrices over k, put

$$I := I_n := \begin{pmatrix} 0 & \mathbf{1}_n \\ -\mathbf{1}_n & 0 \end{pmatrix} \in \mathrm{GL}_{2n}(k) \tag{1}$$

and have

$$I^2 = -\mathbf{1}_{2n}, \quad I^{-1} = I^{\mathsf{T}} = -I. \tag{2}$$

Hence we may form the I-twist (10.8) of the split orthogonal involution of degree $2n$ over k (10.7), which we call the *split symplectic involution of degree* n over k, denoted by

$$\begin{aligned} \tau_{\mathrm{spl}} \colon \operatorname{Mat}_{2n}(k) &\longrightarrow \operatorname{Mat}_{2n}(k), \\ S &\longmapsto \tau_{\mathrm{spl}}(S) := I^{-1}S^{\mathsf{T}}I = IS^{\mathsf{T}}I^{-1} = IS^{\mathsf{T}}I^{\mathsf{T}}. \end{aligned} \tag{3}$$

A verification shows

$$\tau_{\mathrm{spl}}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} d^{\mathsf{T}} & -b^{\mathsf{T}} \\ -c^{\mathsf{T}} & a^{\mathsf{T}} \end{pmatrix} \tag{4}$$

for $a, b, c, d \in \operatorname{Mat}_n(k)$, and we conclude

$$\operatorname{Sym}(\operatorname{Mat}_{2n}(k), \tau_{\mathrm{spl}}) = \left\{ \begin{pmatrix} a & b \\ c & a^{\mathsf{T}} \end{pmatrix} \mid a \in \operatorname{Mat}_n(k),\ b, c \in \operatorname{Skew}_n(k) \right\}. \tag{5}$$

On the other hand, combining 10.9 (ii) with (10.6.4) and (4), we deduce that

$$\begin{aligned} \operatorname{Symp}_n(k) &:= \operatorname{Symd}(\operatorname{Mat}_{2n}(k), \tau_{\mathrm{spl}}) \\ &= \left\{ \begin{pmatrix} a & b \\ c & a^{\mathsf{T}} \end{pmatrix} \mid a \in \operatorname{Mat}_n(k),\ b, c \in \operatorname{Alt}_n(k) \right\} \end{aligned} \tag{6}$$

is a free k-module of rank $2n^2 - n$.

(b) In (a), the case $n = 1$ is particularly interesting. We therefore work out the details in full. The associative k-algebra $\operatorname{Mat}_2(k)$ comes equipped with the orthogonal involution $\tau_{\mathrm{ort}} \colon \operatorname{Mat}_2(k) \to \operatorname{Mat}_2(k)$, $x \mapsto x^{\mathsf{T}}$, of 10.7, which in turn can be twisted by the alternating invertible matrix

$$j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \operatorname{Alt}_2(k) \cap \operatorname{GL}_2(k) \tag{7}$$

satisfying $j^2 = -\mathbf{1}_2$. The involution that ensues,

$$\iota := \tau_{\mathrm{ort}}^{j} \colon \operatorname{Mat}_2(k) \longrightarrow \operatorname{Mat}_2(k), \quad x \longmapsto \bar{x} := j^{-1}x^{\mathsf{T}}j, \tag{8}$$

is the *symplectic involution of degree* 1 or *of* $\operatorname{Mat}_2(k)$. From (4) we deduce

$$\overline{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \tag{9}$$

for $\alpha, \beta, \gamma, \delta \in k$. In particular, we obtain

$$x + \bar{x} = \operatorname{tr}(x)\mathbf{1}_2 \qquad (x \in \operatorname{Mat}_2(k)), \tag{10}$$

and (6) yields

$$\mathrm{Symp}_1(k) := \mathrm{Symd}(\mathrm{Mat}_2(k), \iota) = k \cdot \mathbf{1}_2. \tag{11}$$

(c) Now let n again be arbitrary. Viewing (a) through the lens of (b), we regard the elements of $\mathrm{Mat}_{2n}(k)$ as n-by-n blocks of 2-by-2 matrices, so we have a natural identification $\mathrm{Mat}_{2n}(k) = \mathrm{Mat}_n(B)$, $B := \mathrm{Mat}_2(k)$, as k-algebras. With $j := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ as in (7), we consider the alternating invertible matrix

$$J := \mathrm{diag}(j, \ldots, j) \in \mathrm{Mat}_n(B) \tag{12}$$

and then form the J-twist (10.8) of the split orthogonal involution of degree $2n$ over k (10.7), which up to conjugation by a permutation matrix identifies with the split symplectic involution of degree n over k as in (a) (cf. Exc. 10.11 for an elaborate argument). Hence we may write

$$\begin{aligned} \tau_{\mathrm{spl}} \colon \mathrm{Mat}_{2n}(k) = \mathrm{Mat}_n(B) &\longrightarrow \mathrm{Mat}_n(B) = \mathrm{Mat}_{2n}(k), \\ X &\longmapsto \tau_{\mathrm{spl}}(X) = J^{-1} X^{\mathsf{T}} J. \end{aligned} \tag{13}$$

On the other hand, consider the symplectic involution ι of B as in (8). One checks that τ_{spl} is just the conjugate transpose involution $\mathrm{Mat}_n(\iota)$ in the sense of 10.7, so we have

$$\tau_{\mathrm{spl}}(X) = \bar{X}^{\mathsf{T}} \qquad (X \in \mathrm{Mat}_n(B)) \tag{14}$$

and conclude that

$$\mathrm{Sym}(\mathrm{Mat}_{2n}(k), \tau_{\mathrm{spl}}) = \{X \in \mathrm{Mat}_n(B) \mid X = \bar{X}^{\mathsf{T}}\} \tag{15}$$

is the set of ι-hermitian n-by-n matrices with entries in B. Moreover, from (10) (or (11)) we deduce that $\mathrm{Symp}_n(k)$ consists of all ι-hermitian matrices in $\mathrm{Mat}_n(B)$ whose diagonal entries belong to $k \cdot \mathbf{1}_2$:

$$\mathrm{Symp}_n(k) = \{X = (x_{ij}) \in \mathrm{Mat}_n(B) \mid X = \bar{X}^{\mathsf{T}},\ x_{ii} \in k \cdot \mathbf{1}_2 \ \ (1 \le i \le n)\}. \tag{16}$$

Exercises

10.11. Let m be a positive integer and write e_{ij}, $1 \le i, j \le m$, for the matrix units of $\mathrm{Mat}_m(k)$.

(a) For $\pi \in \mathcal{S}_m$ (the symmetric group on m letters), define the permutation matrix

$$P_\pi := \sum_{i=1}^{m} e_{\pi(i),i}$$

and show that the assignment $\pi \mapsto P_\pi$ gives a group monomorphism from $\mathcal{S}_m$ to the orthogonal group of degree m over k.

(b) Now suppose $m = 2n$ is even. Conclude from (a) that, in the notation of 10.10, the assignment $S \mapsto P_\pi S P_\pi^{\mathsf{T}}$, where $\pi \in \mathcal{S}_{2n}$ is given by $\pi(i) = 2i - 1$, $\pi(i+n) = 2i$ for $1 \le i \le n$, defines an isomorphism

$$(\mathrm{Mat}_{2n}(k), \tau_{\mathrm{spl}}) \xrightarrow{\sim} (\mathrm{Mat}_{2n}(k), \tau^J_{\mathrm{ort}})$$

of algebras with involution.

11 Quadratic maps

In this section, we collect a few elementary facts about quadratic maps that in this generality are somewhat hard to find in the literature. For a brief appearance of this concept over the reals, see 1.3.

11.1 The concept of a quadratic map. Let M, N be k-modules. A map $Q\colon M \to N$ is said to be *quadratic* if it satisfies the following two conditions.

(i) Q is *homogeneous of degree* 2: $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in k$ and all $x \in M$.

(ii) The map

$$DQ\colon M \times M \longrightarrow N, \quad (x,y) \longmapsto (DQ)(x,y) := Q(x+y) - Q(x) - Q(y)$$

is (symmetric) bilinear.

We sometimes call DQ the *bilinearization* or *polar map* belonging to Q. Conditions (i), (ii) imply $(DQ)(x,x) = 2Q(x)$ for all $x \in M$, so the quadratic map Q may be recovered from its polar map DQ if $2 \in k^\times$ *but not in general*. At the other extreme, if $2 = 0$ in k, then DQ is alternating. In the general set-up, we often relax the notation and simply write $Q(x,y)$ instead of $(DQ)(x,y)$ for $x, y \in M$ if there is no danger of confusion. *Quadratic forms* are quadratic maps taking values in the base ring, hence arise in the special case $N = k$. The polar map of a quadratic form is of course called its polar *form*. Examples are provided by the positive definite real quadratic forms of 3.1 and, more specifically, by the norm of the Graves-Cayley octonions (1.6).

Elementary manipulations of quadratic maps, like scalar multiples, composition with linear maps and direct sums, are defined in the obvious manner; we omit the details. Less obvious are scalar extensions, which we address here in a slightly more general set-up. We begin with two preparations.

11.2 Tensor products of bilinear maps. If $b\colon M \times M \to N$ and $b'\colon M' \times M' \to N'$ are bilinear maps between k-modules, then so is

$$b \otimes b'\colon (M \otimes M') \times (M \otimes M') \to N \otimes N', \quad (x \otimes x', y \otimes y') \longmapsto b(x,y) \otimes b'(x',y').$$

The same simple-minded approach does not work for quadratic maps, see Milnor-Husemoller [197, p. 111] for comments.

11.3 Radicals of bilinear and quadratic maps. Let M, N be k-modules and $b\colon M \times M \to N$ a symmetric or skew-symmetric bilinear map. Then the submodule

$$\operatorname{Rad}(b) := \{x \in M \mid b(x, y) = 0 \text{ for all } y \in M\} \subseteq M \tag{1}$$

is called the *radical* of b. Now suppose we are given a k-module M_1 and a surjective linear map $\pi\colon M \to M_1$ such that $\operatorname{Ker}(\pi) \subseteq \operatorname{Rad}(b)$. Then b factors uniquely through $\pi \times \pi$ to a symmetric or skew-symmetric bilinear map $b_1\colon M_1 \times M_1 \to N$ satisfying $\operatorname{Rad}(b_1) = \operatorname{Rad}(b)/\operatorname{Ker}(\pi)$.

Along similar lines, let $Q\colon M \to N$ be a quadratic map. Then

$$\begin{aligned} \operatorname{Rad}(Q) &:= \{x \in \operatorname{Rad}(DQ) \mid Q(x) = 0\} \\ &= \{x \in M \mid Q(x) = (DQ)(x, y) = 0 \text{ for all } y \in M\} \end{aligned} \tag{2}$$

is a submodule of M, called the *radical* of Q. If, for M_1, π as above, we assume $\operatorname{Ker}(\pi) \subseteq \operatorname{Rad}(Q)$, then Q factors uniquely through π to a quadratic map $Q_1\colon M_1 \to N$ (well) defined by $Q_1(\pi(x)) := Q(x)$ for $x \in M$. Moreover, $\operatorname{Rad}(Q_1) = \operatorname{Rad}(Q)/\operatorname{Ker}(\pi)$ and $D(Q_1) = (DQ)_1$.

11.4 Proposition. *Let M, N, V, W be k-modules, $Q\colon M \to N$ a quadratic map and $b\colon V \times V \to W$ a symmetric bilinear map. Then there exists a unique quadratic map*

$$Q \otimes b\colon M \otimes V \longrightarrow N \otimes W$$

such that

$$(Q \otimes b)(x \otimes v) = Q(x) \otimes b(v, v) \qquad (x \in M,\ v \in V), \tag{1}$$

$$D(Q \otimes b) = (DQ) \otimes b. \tag{2}$$

Proof Uniqueness is clear, so we only have to show existence. We first consider the case that the k-module M is free, with basis $(e_i)_{i \in I}$ where we may assume the index set I to be totally ordered. Then every element $z \in M \otimes V$ can be written uniquely as $z = \sum_i e_i \otimes v_i$, $v_i \in V$, and setting

$$(Q \otimes b)(z) := \sum_i Q(e_i) \otimes b(v_i, v_i) + \sum_{i<j} Q(e_i, e_j) \otimes b(v_i, v_j),$$

we obtain a quadratic map which, since b is symmetric, has the desired properties. Now let M be arbitrary. Then there exists a short exact sequence

$$0 \longrightarrow L \xrightarrow{\ i\ } F \xrightarrow{\ \pi\ } M \longrightarrow 0$$

of k-modules, where F is free. Since the functor $-' := - \otimes V$ is right exact [28, II.3, Prop. 5], we obtain an induced exact sequence

$$L' \xrightarrow{i'} F' \xrightarrow{\pi'} M' \longrightarrow 0,$$

and the special case just treated yields a quadratic map $\hat{Q} := (Q \circ \pi) \otimes b \colon F' \to N \otimes W$ satisfying (1), (2). Let $z = \sum u_j \otimes v_j \in L'$, $u_j \in L$, $v_j \in V$, and $x \in F$, $v \in V$. Then

$$\begin{aligned}\hat{Q}(i'(z)) &= ((Q \circ \pi) \otimes b)(i'(\sum u_j \otimes v_j)) = ((Q \circ \pi) \otimes b)(\sum i(u_j) \otimes v_j) \\ &= \sum (Q \circ \pi \circ i)(u_j) \otimes b(v_j, v_j) + \sum_{j<l} (Q \circ \pi \circ i)(u_j, u_l) \otimes b(v_j, v_l) = 0,\end{aligned}$$

and

$$\begin{aligned}\hat{Q}(i'(z), x \otimes v) &= ((Q \circ \pi) \otimes b)(\sum i(u_j) \otimes v_j, x \otimes v) \\ &= \sum (Q \circ \pi \circ i)(u_j, x) \otimes b(v_j, v) = 0,\end{aligned}$$

hence $i'(z) \in \mathrm{Rad}(\hat{Q})$. We have thus shown $\mathrm{Ker}(\pi') = \mathrm{Im}(i') \subseteq \mathrm{Rad}(\hat{Q})$, and 11.3 yields a quadratic map $Q \otimes b \colon M' \to N \otimes W$ such that $(Q \circ \pi) \otimes b = (Q \otimes b) \circ \pi'$ and $D((Q \circ \pi) \otimes b) = [D(Q \otimes b)] \circ (\pi' \times \pi')$. Hence (1), (2) hold for $Q \otimes b$. □

11.5 Corollary. *Let $Q \colon M \to N$ be a k-quadratic map of k-modules and $R \in k$-**alg**. Then there exists a unique R-quadratic map $Q_R := Q \otimes R \colon M_R \to N_R$ of R-modules making a commutative diagram*

$$\begin{array}{ccc} M & \xrightarrow{Q} & N \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}} \\ M_R & \xrightarrow[Q_R]{} & N_R. \end{array} \tag{1}$$

In particular, $D(Q_R) = (DQ)_R$ is the R-bilinear extension of DQ. We call Q_R the scalar extension or *base change* of Q from k to R.

Proof Applying Prop. 11.4 to Q and the symmetric k-bilinear map $b \colon R \times R \to R$ given by the multiplication of R, we obtain a k-quadratic map $Q_R \colon M_R \to N_R$, which is in fact a quadratic map over R satisfying the condition of the corollary. □

We now proceed to list a few elementary properties of bilinear and quadratic forms.

11.6 Notation. Let M be a k-module. Then we write $\mathrm{Bil}(M)$ for the k-module of bilinear forms on M. The submodules of $\mathrm{Bil}(M)$ consisting of all symmetric,

skew-symmetric, alternating bilinear forms on M will be denoted respectively by $\mathrm{Sbil}(M)$, $\mathrm{Skil}(M)$, $\mathrm{Abil}(M)$. Recall that a bilinear form $\sigma\colon M \times M \to k$ is *alternating* if $\sigma(x,x) = 0$ for all $x \in M$. We then have $\mathrm{Abil}(M) \subseteq \mathrm{Skil}(M)$ with equality if $2 \in k^\times$. Finally, we write $\mathrm{Quad}_k(M) := \mathrm{Quad}(M)$ for the k-module of quadratic forms on M. The assignment $q \mapsto Dq$ defines a linear map from $\mathrm{Quad}(M)$ to $\mathrm{Sbil}(M)$.

11.7 Connecting matrices with bilinear and quadratic forms. Let n be a positive integer. For $S \in \mathrm{Mat}_n(k)$, the map

$$\langle S\rangle\colon k^n \times k^n \longrightarrow k, \quad (x,y) \longmapsto \langle S\rangle(x,y) := x^{\mathsf{T}} S\, y \tag{1}$$

is a bilinear form on k^n, and the assignment $S \mapsto \langle S\rangle$ gives a linear bijection from $\mathrm{Mat}_n(k)$ onto $\mathrm{Bil}(k^n)$ matching $\mathrm{Sym}_n(k)$, $\mathrm{Skew}_n(k)$, $\mathrm{Alt}_n(k)$ respectively with $\mathrm{Sbil}(k^n)$, $\mathrm{Skil}(k^n)$, $\mathrm{Abil}(k^n)$. If $S = \mathrm{diag}(\alpha_1,\dots,\alpha_n) \in \mathrm{Mat}_n(k)$ is a diagonal matrix, we put $\langle \alpha_1,\dots,\alpha_n\rangle := \langle S\rangle$ as a symmetric bilinear form on k^n; it sends

$$\left(\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}, \begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix}\right) \in k^n \times k^n \quad \text{to} \quad \sum_{i=1}^{n} \alpha_i \xi_i \eta_i.$$

On the other hand, the map

$$\langle S\rangle_{\mathrm{quad}}\colon k^n \longrightarrow k, \quad x \longmapsto \langle S\rangle_{\mathrm{quad}}(x) := x^{\mathsf{T}} S\, x \tag{2}$$

is a quadratic form on k^n such that $D\langle S\rangle_{\mathrm{quad}} = \langle S + S^{\mathsf{T}}\rangle$, and the assignment $S \mapsto \langle S\rangle_{\mathrm{quad}}$ gives rise to a short exact sequence

$$0 \longrightarrow \mathrm{Alt}_n(k) \longrightarrow \mathrm{Mat}_n(k) \longrightarrow \mathrm{Quad}(k^n) \longrightarrow 0 \tag{3}$$

of k-modules (surjectivity follows from 11.8 below). Thus, roughly speaking, quadratic forms on k^n are basically the same as arbitrary n-by-n matrices modulo alternating n-by-n matrices over k. Again, If $S = \mathrm{diag}(\alpha_1,\dots,\alpha_n) \in \mathrm{Mat}_n(k)$ is a diagonal matrix, we put $\langle \alpha_1,\dots,\alpha_n\rangle_{\mathrm{quad}} := \langle S\rangle_{\mathrm{quad}}$ as a quadratic form on k^n; it sends

$$\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} \in k^n \quad \text{to} \quad \sum_{i=1}^{n} \alpha_i \xi_i^2.$$

11.8 Bilinear and quadratic forms on free modules. Let M be a free k-module of finite rank $n > 0$ and $(e_i)_{1\le i\le n}$ a basis of M over k. Given a bilinear form $\sigma\colon M \times M \to k$, we call $S := (\sigma(e_i,e_j))_{1\le i,j\le n} \in \mathrm{Mat}_n(k)$ the *matrix of* σ with respect to the basis (e_i), and identifying $M = k^n$ by means of this basis

matches σ with the bilinear form $\langle S \rangle$ on k^n (11.7). On the other hand, given a quadratic form $q\colon M \to k$, we define a matrix $S = (s_{ij}) \in \mathrm{Mat}_n(k)$ by

$$s_{ij} := \begin{cases} q(e_i, e_j) & (1 \le i < j \le n), \\ q(e_i) & (1 \le i = j \le n), \\ 0 & (1 \le j < i \le n). \end{cases} \tag{1}$$

We call S the *matrix of* q with respect to the basis (e_i) and, again, identifying $M = k^n$ by means of this basis matches q with the quadratic form $\langle S \rangle_{\mathrm{quad}}$ on k^n.

11.9 Regularity of bilinear forms and generalizations. Let $\sigma\colon M \times M \to k$ be a symmetric or skew-symmetric bilinear form on a k-module M. For a submodule $N \subseteq M$, the submodule

$$N^{\perp} := N^{\perp\sigma} := \{x \in M \mid \sigma(x, y) = 0 \text{ for all } y \in N\} \subseteq M \tag{1}$$

is called the *orthogonal complement* of N in M. In particular, $M^{\perp} = \mathrm{Rad}(\sigma)$ (11.3) is the kernel of the natural map

$$\tilde{\sigma}\colon M \longrightarrow M^*, \quad x \longmapsto \sigma(x, -). \tag{2}$$

The bilinear form σ is said to be *regular* if

(i) M is finitely generated projective as a k-module and
(ii) $\tilde{\sigma}\colon M \xrightarrow{\sim} M^*$ is an isomorphism.

This implies $\mathrm{Rad}(\sigma) = \{0\}$ but not conversely. Since passing to the dual of a finitely generated projective module is compatible with base change (Lemma 9.15), so is the property of a (skew-)symmetric bilinear form to be regular. If $M = k^n$ is free of finite rank n and $S \in \mathrm{Mat}_n(k)$ is (skew-)symmetric, then the (skew-)symmetric bilinear form $\langle S \rangle\colon k^n \times k^n \to k$ is regular if and only if $S \in \mathrm{GL}_n(k)$.

11.10 Lemma. *Let $\sigma\colon M \times M \to k$ be a symmetric or skew-symmetric bilinear form over k and suppose $N \subseteq M$ is a submodule on which σ is regular. Then $M = N \oplus N^{\perp}$.*

Proof We write σ' for the restriction of σ to $N \times N$. Since $N \cap N^{\perp} = \mathrm{Rad}(\sigma') = \{0\}$, it remains to show $M = N + N^{\perp}$, so let $x \in M$. Then $\sigma(x, -)$ restricts to a linear form on N, which by regularity of σ' has the form $\sigma'(u, -)$ for some $u \in N$. Thus $x - u \in N^{\perp}$, proving the claim. □

11.11 Regularity of quadratic forms and generalizations. A quadratic form $q\colon M \to k$ is said to be *non-degenerate* if $\mathrm{Rad}(q) = \{0\}$. Unfortunately, this

property is not invariant under base change, even if we allow M to be finitely generated projective. We therefore call q *non-singular* if M is projective, possibly of infinite rank, and the scalar extension q_K is non-degenerate for all *fields* $K \in k$-**alg**. Indeed, the property of a quadratic form to be non-singular is clearly stable under base change. As a simple example, we note that the one-dimensional quadratic form $\langle\alpha\rangle_{\text{quad}}$, $\alpha \in k^\times$, is always non-singular but becomes degenerate if $2 = 0$ in k and k is not reduced, i.e., contains non-zero nilpotent elements. See Exc. 11.37 and Exc. 25.34 for more on non-singular quadratic forms.

A condition on quadratic forms even stronger than being non-singular is provided by the concept of regularity: q is said to be *regular* if its induced symmetric bilinear form Dq is regular, i.e., by 11.9, if M is finitely generated projective and Dq determines an isomorphism from M onto its dual module M^* in the usual way. Note that regular quadratic forms are non-singular; for a partial converse, see Exc. 11.39. If q is regular and $2 = 0$ in k, then Dq is an alternating regular bilinear form, forcing $\text{rk}_{\mathfrak{p}}(M)$ to be even for all $\mathfrak{p} \in \text{Spec}(k)$, in which case M is said to be *of locally even rank*. For a finitely generated free module $M = k^n$ over any commutative ring k and $S \in \text{Mat}_n(k)$, the quadratic form $\langle S \rangle_{\text{quad}} \colon k^n \to k$ is regular if and only if $S + S^{\mathsf{T}} \in \text{GL}_n(k)$. Trivially, the unique quadratic form on the zero module is regular. In the special case where k is a field, q is regular if and only if M is finite-dimensional and $\text{Rad}(Dq) = \{0\}$.

Finally, q is said to be *weakly regular* if for all $u \in M$, the relation $q(u, v) = 0$ for all $v \in M$ implies $u = 0$. This is equivalent to $Dq \colon M \to M^*$ being injective. Note that weak regularity is not stable under base change, making this notion distinctly less interesting than regularity.

11.12 Quadratic modules and spaces. It is sometimes linguistically convenient to think of a quadratic form $q \colon M \to k$ as a *quadratic module* (M, q). Given quadratic modules (M, q) and (M', q') over k, a k-linear map $h \colon M \to M'$ satisfying $q' \circ h = q$ is called a *homomorphism* $h \colon (M, q) \to (M', q')$. In this way one obtains the category of quadratic modules over k. Isomorphisms between quadratic modules over k are called *isometries*. A quadratic module (M, q) over k is said to be a *quadratic space* if q is regular. The zero module is a quadratic space over every ring k. We write $(M, q) \perp (M', q')$ for the *orthogonal sum* of the quadratic modules (M, q), (M', q') defined on the direct sum $M \oplus M'$ by the quadratic form

$$q \perp q' \colon M \oplus M' \longrightarrow k, \quad (x, x') \longmapsto q(x) + q'(x').$$

We sometimes use the alternate notation $(M, q) \oplus (M', q') := (M, q) \perp (M', q')$ and $q \oplus q' := q \perp q'$.

11.13 Example. For a k-module M, a quadratic form $q\colon M \to k$ and elements $\alpha_1, \dots, \alpha_n \in k$ ($n \in \mathbb{Z}$, $n > 0$), the natural identification $M \otimes k^n = M^n$ of k-modules yields an identification

$$q \otimes \langle \alpha_1, \dots, \alpha_n \rangle = \alpha_1 q \perp \cdots \perp \alpha_n q$$

of quadratic forms.

11.14 Pointed quadratic modules. By a *pointed quadratic module* over k we mean a triple (M, q, e) consisting of a quadratic module (M, q) and a distinguished element $e \in M$, called the *base point*, such that $q(e) = 1$. *Homomorphisms* of pointed quadratic modules are defined as homomorphism of the underlying quadratic modules preserving base points in the obvious sense. We speak of (M, q, e) as a *pointed quadratic space* (*of rank r*) if (M, q) is a quadratic space (of rank r).

Let (M, q, e) be a pointed quadratic module over k. We call q its *norm*, the linear form

$$t := (Dq)(e, -)\colon M \longrightarrow k, \quad x \longmapsto t(x) := q(e, x) \tag{1}$$

its (*linear*) *trace* and the linear map

$$\iota\colon M \longrightarrow M, \quad x \longmapsto \bar{x} := t(x)e - x, \tag{2}$$

its *conjugation*. Obviously, the trace satisfies $t(e) = 2$, while the conjugation has period 2 and preserves base point, norm and trace. In addition, the *bilinear trace* of (M, q, e), for convenience denoted by the same symbol as the linear one, is defined as the symmetric bilinear form

$$t\colon M \times M \longrightarrow k, \quad (x, y) \longmapsto t(x, y) := q(x, \bar{y}) = t(x)t(y) - q(x, y). \tag{3}$$

It satisfies $t(x, e) = t(x)$ and is preserved by conjugation.

In the special case where $2 \in k^\times$, the natural inclusion $k \hookrightarrow M$ given by $x \mapsto xe$ has left inverse $\frac{1}{2}t$. Therefore $M = ke \oplus (\operatorname{Ker} t)$ as a k-module, and this direct sum is orthogonal with respect to q. In particular, q is determined by its restriction to $\operatorname{Ker} t$.

The following lemma is obvious but quite useful.

11.15 Lemma. *Let (M, q, e) be a pointed quadratic module over k and suppose there exists a bilinear form $\beta\colon M \times M \to k$, possibly not symmetric, such that $q(x) = \beta(x, x)$ for all $x \in M$ (which holds automatically if $2 \in k^\times$ or M is projective as a k-module by Exc. 11.36), then the base point $e \in M$ is unimodular.*

Proof The linear form $\lambda := \beta(e, -)$ on M has $\lambda(e) = \beta(e, e) = q(e) = 1$. □

11.16 The naive discriminant. The multiplicative group $k^{\times 2}$ of squares in $k^\times$ acts on the additive group k by multiplication from the right, allowing us to form the quotient $k/k^{\times 2}$. Now suppose we are given a quadratic module (M, q) over k such that the underlying k-module M is free of finite rank. In analogy to 3.10–3.12 we let $E = (e_1, \ldots, e_n)$ be any k-basis of M, put

$$Dq(E) := \big(q(e_i, e_j)\big)_{1 \le i,j \le n} \in \mathrm{Mat}_n(k) \tag{1}$$

and have

$$Dq(E^S) = S^{\mathsf{T}} Dq(E) S \qquad \big(S = (s_{ij})_{1 \le i,j \le n} \in \mathrm{GL}_n(k)\big), \tag{2}$$

where $E^S = (e'_1, \ldots, e'_n)$ is the k-basis of M defined by $e'_j := \sum_i s_{ij} e_i$ for $1 \le j \le n$. Hence the expression

$$\mathrm{disc}\,((M, q)) := (-1)^{\lfloor \frac{n}{2} \rfloor} \det\big(Dq(E)\big) \bmod k^{\times 2}$$

is independent of the basis chosen and called the *discriminant* of (M, q). Since $\mathbb{Z}^{\times 2} = \{1\}$, this definition generalizes the one of the discriminant of an integral quadratic lattice as given in 3.12. For a more sophisticated definition of the discriminant that makes sense for arbitrary quadratic spaces, we refer the reader to Knus [157, Chap. IV, §4].

11.17 Isotropic elements and hyperbolic pairs. Let (M, q) be a quadratic module over k. Following [99, 1.8, p. 1297], an element $u \in M$ is said to be *isotropic* (relative to (M, q), or relative to q) if u is unimodular and $q(u) = 0$. By a *hyperbolic pair* (of (M, q), or of q) we mean a pair $(u, v) \in M^2$ such that $q(u) = q(v) = 0$ and $q(u, v) = 1$. Consider the following conditions on $u \in M$.

(i) u is isotropic.

(ii) u can be extended to a hyperbolic pair: there exists $v \in M$ making (u, v) a hyperbolic pair.

Then (ii) *implies* (i), *and if* (M, q) *is a quadratic space, both conditions are equivalent.* Indeed, the implication (ii) ⇒ (i) being obvious, assume (M, q) is a quadratic space and $u \in M$ is isotropic. By definition, u is unimodular, so some $\lambda \in M^*$ has $\lambda(u) = 1$. Since q is regular, there exists a unique $w \in M$ such that $\lambda = q(-, w)$, and we conclude $q(u, w) = 1$. Now one checks that (u, v), where $v := -q(w)u + w$, is a hyperbolic pair of (M, q), which completes the proof.

A quadratic module (M, q) (or q) will be called *isotropic* if M contains an isotropic element relative to q. A submodule $N \subseteq M$ is said to be *totally isotropic* (relative to q) if it is a direct summand of M and satisfies $q(N) = \{0\}$.

11.18 Hyperbolic spaces. Let M be a finitely generated projective k-module. Then

$$\mathbf{h}_M \colon M^* \oplus M \longrightarrow k, \quad (v^*, v) \longmapsto \mathbf{h}_M((v^*, v)) := \langle v^*, v \rangle, \tag{1}$$

is a regular quadratic form since M^{**} identifies canonically with M and, in the notation of (11.9.2),

$$(D\mathbf{h}_M)^{\sim} \colon M^* \oplus M \to M \oplus M^*$$

is the switch $(v^*, v) \mapsto (v, v^*)$. We abuse notation slightly by writing $\mathbf{h}_M$ also for the quadratic space $(M^* \oplus M, \mathbf{h}_M)$, and call this the *hyperbolic space* associated with M or simply a hyperbolic space. Observe that both M^* and M may be viewed canonically as totally isotropic submodules of $M^* \oplus M$ relative to $\mathbf{h}_M$. The functor assigning to M its associated hyperbolic space is additive, so for another finitely generated projective k-module N we obtain a natural isomorphism

$$\mathbf{h}_{M \oplus N} \cong \mathbf{h}_M \perp \mathbf{h}_N.$$

For L a *line bundle* in the sense of 9.12, $\mathbf{h}_L$ will be referred to as a *hyperbolic plane*, which is said to be *split* if L is free of rank 1. If $M \cong k^n$ is free of rank $n \in \mathbb{N}$, we speak of the *split* hyperbolic space of rank n.

11.19 Examples. (a) For every $\alpha \in k^\times$, the map $M^* \oplus M \to M^* \oplus M$ defined by $(y^*, x) \mapsto (y^*, \alpha x)$ is an isomorphism of quadratic spaces $\mathbf{h}_M \otimes \langle \alpha \rangle \xrightarrow{\sim} \mathbf{h}_M$.

(b) Taking E to be the standard basis of k^n, the matrix $D\mathbf{h}_{k^n}(E)$ from (11.16.1) is

$$\left(\begin{smallmatrix} 0 & \mathbf{1}_n \\ \mathbf{1}_n & 0 \end{smallmatrix}\right),$$

so the naive discriminant of $\mathbf{h}_{k^n}$ is 1 mod $k^{\times 2}$.

11.20 LG rings. There is a well-developed theory of quadratic spaces over a field that can be found in books such as [204], [255], or [72]. Already in the foundations of that theory, there are many results that hold over fields but do not have clear analogs over an arbitrary base ring. To address this, we introduce a class of rings known as LG rings, sometimes called "local-global rings" (hence the LG) or "rings with many units", which include all fields and where some of the desirable results that hold for fields will continue to hold.

LG rings are defined as follows. For $R \in k$-**alg**, a polynomial $f \in R[\mathbf{t}_1, \dots, \mathbf{t}_n]$ *represents an invertible element over* R if there exist $r_1, \dots, r_n \in R$ such that $f(r_1, \dots, r_n) \in R^\times$. Given $f \in k[\mathbf{t}_1, \dots, \mathbf{t}_n]$ and $R \in k$-**alg**, the homomorphism $k \to R$ allows us to view f also as a polynomial in $R[\mathbf{t}_1, \dots, \mathbf{t}_n]$, so we can

speak about whether it represents an invertible element over R. If it does so over k, then it does so over R for every R. We say that k is an *LG ring* if it has the property that, *for every* $n > 0$ *and* $f \in k[\mathbf{t}_1, \dots, \mathbf{t}_n]$, *if* f *represents a an invertible element over* $k_\mathfrak{m}$ *for every maximal ideal* $\mathfrak{m}$ *of* k, *then* f *represents an invertible element over* k. It would be equivalent to replace the local ring $k_\mathfrak{m}$ in the definition by its residue field $k(\mathfrak{m})$. Every field is trivially an LG ring, because the unique maximal ideal is $\mathfrak{m} = \{0\}$ and $k_\mathfrak{m} = k$. The zero ring is trivially an LG ring.

In the following, $\operatorname{Jac}(k)$ denotes the Jacobson radical of k (Bourbaki [34, §6, Def. 3]), the intersection of the maximal ideals of k.

11.21 Lemma. *(i) A ring* k *is an LG ring if and only if* $k/\operatorname{Jac}(k)$ *is an LG ring.*

(ii) For rings k_1, k_2, *the ring* $k_1 \times k_2$ *is an LG ring if and only if* k_1 *and* k_2 *are LG rings.*

We leave the proof as an exercise.

11.22 Semi-local rings. A ring is said to be *semi-local* if its set of maximal ideals is finite. It is equivalent (by Bourbaki [27, II.3, Prop. 16]) to require that $k/\operatorname{Jac}(k)$ is a finite direct product of fields. The lemma then gives: *Every semi-local ring is an LG ring.*

11.23 Finite and integral k-algebras. An element $r \in R$ for $R \in k$-**alg** is said to be *integral (over* k*)* if there is a monic polynomial $f \in k[\mathbf{t}]$ such that, for f^ϑ the image of f in $R[\mathbf{t}]$, we have $f^\vartheta(r) = 0$. (This notion was previously defined in the special case $k = \mathbb{Z}$ in 3.4.) The ring R is said to be *integral (over* k*)* if every $r \in R$ is integral. If k is an LG ring and R is integral over k, then R is also an LG ring by [73, Cor. 2.3].

We say that R is a *finite* k-algebra if it is finitely generated as a k-module. This is related to the previous property because a k-algebra R *is finite if and only if* R *is integral over* k *and is finitely generated as a* k*-algebra*, see [27, V.1, Prop. 16] or [271, Tag 02JJ]. As a corollary, we find: If k is an LG ring, then every finite k-algebra is also LG.

Note that if R is an integral (e.g., finite) k-algebra that contains k, then it is a cover of k in the sense of Exc. 9.26 [271, Tag 00GQ].

The papers [73] and [192] give more examples of rings that are LG, which we mention for the purpose of illustrating that the class of LG rings is larger than the class of semi-local rings. Specifically, LG rings include rings of dimension zero (i.e., rings where every prime ideal is maximal), the ring of all algebraic integers, and the ring of all real algebraic integers. Exc. 11.42 provides examples of rings that are not LG.

We proceed by collecting a few useful properties of LG rings, addressed to projective modules and quadratic forms. The following is a key result, proved in Estes-Guralnick [73, Thm. 2.10] and McDonald-Waterhouse [192, p. 457].

11.24 Proposition. *Every finitely generated projective module of constant rank over an LG ring is free.* □

Since LG rings need not be connected (as in Lemma 11.21 (i)), the condition on the rank function cannot be avoided.

11.25 Definition. It is a standard fact that for a finitely generated projective k-module M, the following conditions are equivalent.

(i) $M_R \neq \{0\}$ for all non-zero $R \in k$-**alg**.
(ii) $M_\mathfrak{p} \neq \{0\}$ for all prime ideals $\mathfrak{p} \subseteq k$.
(iii) $M_\mathfrak{m} \neq \{0\}$ for all maximal ideals $\mathfrak{m} \subseteq k$.
(iv) $M_F \neq \{0\}$ for all fields $F \in k$-**alg**.

We leave the proof as an exercise. If these equivalent conditions hold, M is said to *have full support*.

11.26 Lemma. *Let k be an LG ring and (M, q) a quadratic space over k. Then q represents an invertible element over k (i.e., $q(m) \in k^\times$ for some $m \in M$) if and only if M has full support.*

Proof Recall from the definition of a quadratic space (11.11, 11.12) that M is a finitely generated projective k-module. If $m \in M$ satisfies $q(m) \in k^\times$ and $F \in k$-**alg** is a field, then $q_F(m_F) = q(m)_F \in F^\times$, and we conclude $M_F \neq \{0\}$. Conversely, assume $M_F \neq \{0\}$ for all fields in $F \in k$-**alg**. Since this condition is stable under base change, the rank decomposition (Exc. 9.31) allows us to assume that M has constant rank. By Prop. 11.24, therefore, M is a free k-module of finite rank $n > 0$, so by 11.8 the quadratic form $q\colon M \to k$ may be viewed as a homogeneous polynomial $q \in k[\mathbf{t}_1, \dots, \mathbf{t}_n]$ of degree 2. Since $(M_F, q_F) = (M, q)_F$ is a quadratic space over F, the map $q_F\colon M_F \to F$ cannot be identically zero, so the polynomial q represents an invertible element over F, Since k is an LG ring, it represents an invertible element over k, as claimed. □

The following result, known as Witt Cancellation, plays a key foundational role in the theory of quadratic forms over a field. It also holds over LG rings.

11.27 Theorem (Witt cancellation)**.** *Suppose (M_1, q_1), (M_2, q_2), and (M_2', q_2') are quadratic spaces over an LG ring k such that*

$$(M_1, q_1) \perp (M_2, q_2) \cong (M_1, q_1) \perp (M_2', q_2').$$

Then $(M_2, q_2) \cong (M_2', q_2')$.

A proof of this can be found in [63, p. 38, II.6.4]. It is similar to the proof for semi-local rings from [18, Cor. III.4.3]. See Exc. 22.28 for an example of a ring k where Witt cancellation fails.

Exercises

11.28. *Associative linear forms and unitality.* Let A be a k-algebra. Show that A is unital provided it admits an associative linear form whose corresponding (symmetric) bilinear form is regular.

11.29. Let σ be a bilinear form on a k-module M. For $m_1, \dots, m_n \in M$, define a matrix $S := (\sigma(m_i, m_j))_{1 \le i,j \le n} \in \mathrm{Mat}_n(k)$. Prove: If $\det(S)$ is not a zero divisor in k, then $m_1, \dots, m_n$ are linearly independent.

11.30. *A splitness criterion for hyperbolic planes.* Let L be a line bundle over k. Show that the following conditions are equivalent.

(i) The hyperbolic plane $\mathbf{h}_L$ is split.
(ii) $\mathbf{h}_L$ contains a hyperbolic pair.
(iii) $L \cong k$ is free.

(*Hint*: To prove (ii) $\Rightarrow$ (iii), find a unimodular vector in L.)

11.31. Prove for the quadratic form $q := \langle 1, -1 \rangle_{\mathrm{quad}}$ over k that the following conditions are equivalent.

(i) q is a split hyperbolic plane.
(ii) q is regular.
(iii) 2 is invertible in k.

11.32. Let F be a field of characteristic different from 2. Verify: If a rank 2 quadratic space (M, q) over F has discriminant 1 mod $F^{\times 2}$, then (M, q) is a split hyperbolic plane.
Remark. The converse was already observed in 11.19. Also, a version of this statement that holds with weaker hypotheses on F is provided in [157, §V.2].

11.33. Let $\mathbf{h}$ be the split hyperbolic plane over k and (e_1, e_2) a hyperbolic pair in $\mathbf{h}$. Show for $u_1, u_2 \in \mathbf{h}$ that the following conditions are equivalent.

(i) (u_1, u_2) is a hyperbolic pair in $\mathbf{h}$.
(ii) There exists a decomposition $k = k_+ \times k_-$ of k as a direct product of ideals such that in the induced decompositions

$$\mathbf{h} = \mathbf{h}_+ \times \mathbf{h}_-, \quad e_j = (e_{j+}, e_{j-}), \quad u_j = (u_{j+}, u_{j-}) \qquad (j = 1, 2), \tag{1}$$

where $\mathbf{h}_\pm = \mathbf{h}_{k_\pm}$ is the split hyperbolic plane over $k_\pm$ with the corresponding hyperbolic pair $(e_{1\pm}, e_{2\pm}) = (e_1, e_2)_{k_\pm}$, the quantities $u_{j\pm} = (u_j)_{k_\pm} \in \mathbf{h}_\pm$ $(j = 1, 2)$ satisfy the relations

$$u_{1+} = \gamma_+ e_{1+}, \quad u_{2+} = \gamma_+^{-1} e_{2+}, \tag{2}$$

$$u_{1-} = \gamma_- e_{2-}, \quad u_{2-} = \gamma_-^{-1} e_{1-} \tag{3}$$

for some $\gamma_\pm \in k_\pm^\times$.

11.34. *Quadratic-linear maps.* Let M, N, P be k-modules and suppose the map $g\colon M \times N \to P$ is *quadratic-linear* (over k) in the sense that $g(-, y)\colon M \to P$ is k-quadratic for all $y \in N$ and, analogously, $g(x, -)\colon N \to P$ is k-linear for all $x \in M$. Show for all $R \in k$-**alg** that there exists a unique quadratic-linear map $g_R\colon M_R \times N_R \to P_R$ over R rendering the diagram

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & P \\ {\scriptstyle \text{can}}\downarrow & & \downarrow{\scriptstyle \text{can}} \\ M_R \times N_R & \xrightarrow[g_R]{} & P_R. \end{array} \tag{1}$$

commutative. We call g_R the *scalar extension* or *base change* of g from k to R.

11.35. *Multi-quadratic maps.* For a positive integer n and k-modules $M_1, \dots, M_n, M$, a map

$$F\colon M_1 \times \cdots \times M_n \longrightarrow M$$

is called *k-multi-quadratic* or *k-n-quadratic* if for all $i = 1, \dots, n$ and for all $u_j \in M_j$, $1 \le j \le n$, $j \ne i$,

$$M_i \longrightarrow M, \quad u_i \longmapsto F(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_n)$$

is a quadratic map over k. Show for $R \in k$-**alg** and a k-n-quadratic map $F\colon M_1 \times \cdots \times M_n \to M$ that there exists a unique R-n-quadratic map $F_R\colon M_{1R} \times \cdots \times M_{nR} \to M_R$ rendering the diagram

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{F} & M \\ {\scriptstyle \text{can}}\downarrow & & \downarrow{\scriptstyle \text{can}} \\ M_{1R} \times \cdots \times M_{nR} & \xrightarrow[F_R]{} & M_R. \end{array} \tag{1}$$

commutative, where $\text{can}\colon M_1 \times \cdots \times M_n \to M_{1R} \times \cdots \times M_{nR}$ is defined by

$$\text{can}(u_1, \dots, u_n) := (u_{1R}, \dots, u_{nR})$$

for all $u_i \in M_i$, $1 \le i \le n$. Writing $\text{Quad}(M_1, \dots, M_n; M)$ for the k-module of k-n-quadratic maps from $M_1 \times \cdots \times M_n$ to M, show further that the assignment $F \mapsto F_R$ defines a k-linear map from $\text{Quad}(M_1, \dots, M_n; M)$ to $\text{Quad}(M_{1R}, \dots, M_{nR}; M_R)$. We call F_R the *R-n-quadratic extension* of F.

11.36. Let $Q\colon M \to N$ be a quadratic map between k-modules M, N and suppose M is projective. Show that there exists a bilinear map $B\colon M \times M \to N$, possibly not symmetric, such that $Q(x) = B(x, x)$ for all $x \in M$.

11.37. *Non-singular quadratic forms over fields.* Let $q\colon V \to F$ be a quadratic form over a field F. Show that the following conditions are equivalent.

(i) q is non-singular.
(ii) q is non-degenerate and the radical of Dq has dimension at most 1 over F.

(iii) For some algebraically closed field $K \supseteq F$, the quadratic form $q_K \colon V_K \to K$ over K is non-degenerate.
(iv) For every algebraically closed field $K \supseteq F$, the quadratic form $q_K : V_K \to K$ over K is non-degenerate.

Remarks. (1) In the exercise, when $\dim V$ is finite, condition (ii) can be rephrased as: *Exactly one of the following two conditions hold:*

(a) $\operatorname{char} F = 2$ *and* $\dim V$ *is odd, in which case* $q = q_0 \perp \langle\alpha\rangle_{\text{quad}}$ *for some regular quadratic from* q_0 *and* $\alpha \in F^\times$.
(b) q *is regular.*

(2) Suppose (M, q) is a quadratic module over a ring k such that M is finitely generated projective of finite constant rank. Then (1) shows that our definition of "non-singular" for q is the same as what is called "non-degenerate" in [53, §6.1 and Exercise 1.6.10] or "ordinary" in [60, §XII.1] or "semiregular" in [157, §IV.3] or [42, §2.6].

11.38. Let (V, q) be a quadratic space of dimension n over the field F. Following [72, 7.7], an element $v \in V$ is called *anisotropic* (with respect to q) if $q(v) \neq 0$.

(a) If $n \geq 3$, show that every element in V is the sum of at most two anisotropic elements in V.
(b) Assume that (V, q) contains a hyperbolic subspace of dimension at least 6. Show for anisotropic vectors $x_1, x_2 \in V$ that $q(x_1, x_2) \neq 0$ or there exists an anisotropic vector $y \in V$ satisfying $q(x_1, y) \neq 0 \neq q(y, x_2)$.

Can the extra conditions on (V, q) in (a), (b) be avoided?

11.39. Suppose $Q = (M, q)$ is a quadratic module over a ring k such that M is finitely generated projective and q is non-singular. Prove: If $2 \in k^\times$ or $\operatorname{rk} M$ is locally even, then M is regular.

11.40. Let $q \colon M \to k$ be a quadratic form. Recall that $\operatorname{Rad}(Dq) \supseteq \operatorname{Rad}(q)$.

(a) Show: If 2 is invertible in k, then $\operatorname{Rad}(Dq) = \operatorname{Rad}(q)$.
(b) Suppose $2 = 0$ in k and $M' := \operatorname{Rad}(Dq)/\operatorname{Rad}(q)$ is a free k-module of finite rank. Verify that there are nonzero $\alpha_1, \ldots, \alpha_r \in k$ such that $q|_{M'}$ is isomorphic to $\langle\alpha_1, \ldots, \alpha_r\rangle_{\text{quad}}$ and $\alpha_i k^{\times 2} \neq \alpha_j k^{\times 2}$ for $i \neq j$.

Remark. One might call the quadratic module $(M', q|_{M'})$ the *anti-regular* part of q.

11.41. Let $Q := (M, q)$ be a quadratic module over k. The subgroup

$$\mathrm{O}(Q) := \mathrm{O}(M, q) := \{\eta \in \mathrm{GL}(M) \mid q \circ \eta = q\}$$

of $\mathrm{GL}(M)$ is called the *orthogonal group* of Q.

(i) Verify that $\mathrm{O}(Q)$ contains a normal subgroup R that is naturally isomorphic (as a set) to $\operatorname{Hom}_{k\text{-}\mathbf{mod}}(M/\operatorname{Rad}(q), \operatorname{Rad}(q))$.
(ii) q induces a quadratic form $\overline{q}$ on $M/\operatorname{Rad}(q)$ by setting $\overline{q}(m + r) = q(m)$ for $m \in M$ and $r \in \operatorname{Rad}(q)$, and we put $\overline{Q} := (M/\operatorname{Rad}(q), \overline{q})$ for the corresponding quadratic module. Prove that restriction defines a well-defined injective homomorphism $\phi \colon \mathrm{O}(Q)/R \to \mathrm{GL}(\operatorname{Rad}(q)) \times \mathrm{O}(\overline{Q})$.

(iii) Prove: If M is an internal direct sum $\mathrm{Rad}(q) \oplus M'$ for some submodule M', then the map ϕ defined in (ii) is an isomorphism.

11.42. *Examples of rings that are not LG.* Show that the following rings k are not LG: (a) $k = \mathbb{Z}$. (b) $k = R[\mathbf{t}]$, polynomials in one variable over a ring R, when R is an integral domain.

12 Polynomial laws

The differential calculus for polynomial (or rational) maps between finite-dimensional vector spaces, as explained in Braun-Koecher [36] or Jacobson [136], for example, belongs to the most useful techniques from the toolbox of elementary non-associative algebra. It elevates the linearization procedures that we have encountered so far, and that will become much more involved in subsequent portions of the book (see, e.g., the identities in 29.2 below), to a new level of systematic conciseness. While it works most smoothly over infinite base fields, it can be slightly adjusted to work over finite ones as well. There is also a variant due to McCrimmon [182] that allows infinite-dimensional vector spaces.

Extending this formalism to arbitrary modules over arbitrary commutative rings, however, requires a radically new approach. The one adopted in the present volume, due to Roby [249], is based on the concept of a polynomial law. In the present section, we explore this concept in detail and show, in particular, how the differential calculus for polynomial maps over infinite fields can be naturally extended to this more general setting. For a different approach, see Faulkner [76].

Throughout, we let k be an arbitrary commutative ring and $M, N, M_1, \dots, M_n$ ($n \in \mathbb{Z}$, $n > 0$) be arbitrary k-modules.

12.1 Reminder: polynomial maps. For the time being, let V, W be finite-dimensional vector spaces over an infinite field F and $(v_i)_{1\le i\le m}$, $(w_j)_{1\le j\le n}$ be bases of V, W, respectively, over F. By a *polynomial map* from V to W we mean a set map $f\colon V \to W$ such that there exist polynomials $p_1, \dots, p_n \in F[\mathbf{t}_1, \dots, \mathbf{t}_m]$ satisfying the equations

$$f\Big(\sum_{i=1}^{m} \alpha_i v_i\Big) = \sum_{j=1}^{n} p_j(\alpha_1, \dots, \alpha_m) w_j \qquad (\alpha_1, \dots, \alpha_m \in F). \tag{1}$$

Since F is infinite, (1) determines the polynomials p_j, $1 \le j \le n$, uniquely. Moreover, the concept of a polynomial map is obviously independent of the bases chosen. In the special case $W = F$, we speak of a *polynomial function*

on V. The totality of all polynomial functions on V forms a unital commutative associative F-algebra, denoted by $F[V]$ and canonically isomorphic to the polynomial ring $F[\mathbf{t}_1, \ldots, \mathbf{t}_m]$ over F.

Returning to our polynomial map $f\colon V \to W$ as above, we generalize (1) by defining a family of set maps $f_R\colon V_R \to W_R$, one for each $R \in F$-**alg**, given by

$$f_R(\sum_{i=1}^{m} r_i v_{iR}) := \sum_{j=1}^{n} p_j(r_1, \ldots, r_m) w_{jR} \qquad (r_1, \ldots, r_m \in R). \tag{2}$$

The key property of this family may be expressed by a coherence condition, saying that its constituents f_R *vary functorially* with $R \in k$-**alg**: every morphism $\varphi\colon R \to S$ in k-**alg** yields a commutative diagram

$$\begin{array}{ccc} V_R & \xrightarrow{f_R} & W_R \\ {\scriptstyle \mathbf{1}_V \otimes \varphi}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_W \otimes \varphi} \\ V_S & \xrightarrow[f_S]{} & W_S\,. \end{array} \tag{3}$$

as shown. This coherence condition will now be isolated in the formal definition of a polynomial law.

12.2 The concept of a polynomial law. With the k-module M we associate a (covariant) functor $M_{\mathbf{a}}\colon k$-**alg** $\to$ **set** (where **set** stands for the category of sets) by setting $M_{\mathbf{a}}(R) = M_R$ as sets for $R \in k$-**alg** and $M_{\mathbf{a}}(\varphi) = \mathbf{1}_M \otimes \varphi\colon M_R \to M_S$ as set maps for morphisms $\varphi\colon R \to S$ in k-**alg**; here $\mathbf{1}_M$ stands for the identity map on M. Analogously, we obtain the functor $N_{\mathbf{a}}\colon k$-**alg** $\to$ **set** associated with the k-module N. We then define a *polynomial law f from M to N* (over k) as a natural transformation $f\colon M_{\mathbf{a}} \to N_{\mathbf{a}}$. In explicit terms, this means that, for all $R \in k$-**alg**, we are given set maps $f_R\colon M_R \to N_R$ varying functorially with R, so whenever $\varphi\colon R \to S$ is a unital homomorphism of unital commutative associative k-algebras, the diagram

$$\begin{array}{ccc} M_R & \xrightarrow{f_R} & N_R \\ {\scriptstyle \mathbf{1}_M \otimes \varphi}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_N \otimes \varphi} \\ M_S & \xrightarrow[f_S]{} & N_S\,. \end{array} \tag{1}$$

commutes. A polynomial law from M to N will be symbolized by $f\colon M \to N$, in spite of the fact that it is *not* a map from M to N in the usual sense. But it induces one, namely $f_k\colon M \to N$, which, however, does not determine f uniquely. If $\varphi\colon R \to S$ is a morphism in k-**alg**, then S belongs to R-**alg** via φ,

and identifying $(M_R)_S = M_S$, $(N_R)_S = N_S$ canonically by means of (9.4.1), we conclude from (9.4.2) that (1) is equivalent to

$$f_R(x)_S = f_S(x_S) \qquad (x \in M_R). \tag{2}$$

The totality of polynomial laws from M to N will be denoted by $\mathrm{Pol}(M,N)$, or by $\mathrm{Pol}_k(M,N)$ to indicate dependence on k. (Bourbaki aficionados please note that this notion of polynomial laws aligns with the one considered in the exercises of §IV.5 of [29] and need not agree with the objects denoted $\mathrm{Pol}_k(M,N)$ in the §IV.5.10 of the main text of that book.) It is a k-module in a natural way, the sum of $f, g \in \mathrm{Pol}(M,N)$ being given by $(f+g)_R = f_R + g_R$ for all $R \in k$-**alg**, ditto for scalar multiplication. The multiplication of polynomial laws $M \to N$ by *scalar* polynomial laws $M \to k$ is defined analogously. In particular, $\mathrm{Pol}(M,k)$ is a unital commutative associative k-algebra. If $f\colon M \to N$ and $g\colon N \to P$ are polynomial laws over k, so obviously is $g \circ f\colon M \to P$, given by $(g \circ f)_R = g_R \circ f_R$, $R \in k$-**alg**. Every polynomial law $f\colon M \to N$ over k gives rise to its *scalar extension* or *base change* $f \otimes R\colon M_R \to N_R$, a polynomial law over R determined by the condition $(f \otimes R)_S := f_S$ for all $S \in R$-**alg** $\subseteq k$-**alg**, where $(M_R)_S = M_S$, $(N_R)_S = N_S$ are canonically identified as before. We often write f_R, or simply f, for $f \otimes R$ if there is no danger of confusion.

12.3 Example: the characteristic polynomial of a matrix. The determinant of an n-by-n matrix is a polynomial law $\det\colon \mathrm{Mat}_n(k) \to k$. Similarly, for $\mathbf{t}$ an indeterminate, sending a matrix x to its characteristic polynomial $\det(\mathbf{t}\cdot 1 - x) \in k[\mathbf{t}]$ is a polynomial law $\mathrm{Mat}_n(k) \to k[\mathbf{t}]$. The same reasoning applies to show that each of the coefficients of the characteristic polynomial, such as the trace (the coefficient of $-\mathbf{t}^{n-1}$), also defines a polynomial law $\mathrm{Mat}_n(k) \to k$.

Before we can proceed, we require a rather obvious but still useful observation.

12.4 Unimodular free base change. Let $R \in k$-**alg** and assume that 1_R can be extended to basis $(t_i)_{i\in I}$ of R as a k-module. Since tensor products commute with direct sums, the natural map $M \to M_R$, for any k-module M, is an embedding, and identifying $M \subseteq M_R$ canonically, we conclude

$$M_R = \bigoplus_{i\in I} (t_i M) \tag{1}$$

as a direct sum of k-modules. Moreover, any linear map $f\colon M \to N$ between k-modules M, N may be recovered from its R-linear extension $f_R\colon M_R \to N_R$ via restriction, and it follows that the assignment $f \mapsto f_R$ defines an injection from $\mathrm{Hom}_k(M,N)$ to $\mathrm{Hom}_R(M_R, N_R)$. We identify $\mathrm{Hom}_k(M,N) \subseteq \mathrm{Hom}_R(M_R, N_R)$

accordingly and claim that *the R-linear map*

$$\bigoplus_{i\in I}(t_i \operatorname{Hom}_k(M,N)) = \operatorname{Hom}_k(M,N)_R \longrightarrow \operatorname{Hom}_R(M_R,N_R)$$

extending the inclusion $\operatorname{Hom}_k(M,N) \hookrightarrow \operatorname{Hom}_R(M_R,N_R)$ *is injective*. Indeed, given a family (f_i) of elements in $\operatorname{Hom}_k(M,N)$ with finite support, the map in question, thanks to the preceding identifications, sends $\sum t_i f_i = \sum(f_i \otimes t_i)$ to $\sum t_i f_{iR} = \sum t_i f_i$, and if this is zero, then so is $\sum t_i f_i(x)$ for all $x \in M$, which by (1) implies $f_i = 0$ for all i and proves the assertion. Summing up we have shown that after the appropriate identifications, the following inclusions hold:

$$\operatorname{Hom}_k(M,N) \subseteq \operatorname{Hom}_k(M,N)_R = \bigoplus_{i\in I}(t_i \operatorname{Hom}_k(M,N)) \subseteq \operatorname{Hom}_R(M_R,N_R). \quad (2)$$

Moreover, the elements of $\operatorname{Hom}_k(M,N)_R$ act on M_R according to the rule

$$(t_i f)(t_j x) = t_i t_j f(x) \qquad (f \in \operatorname{Hom}_k(M,N),\ i,j \in I,\ x \in M) \quad (3)$$

since $(t_i f)(t_j x) = (t_i f_R)(x \otimes t_j) = t_i f_R(x \otimes t_j) = t_i(f(x) \otimes t_j) = f(x) \otimes (t_i t_j) = t_i t_j f(x)$.

12.5 Convention: multi-indices. For $R \in k$-**alg** it is often convenient to use the multi-index notation $r^\nu := r_1^{\nu_1} \cdots r_n^{\nu_n}$, where $r = (r_1,\dots,r_n) \in R^n$ and $\nu = (\nu_1,\dots,\nu_n) \in \mathbb{N}^n$ are sequences of length $n \geq 1$ in $R, \mathbb{N}$, respectively. Also, we put $|\nu| := \sum_{i=1}^n \nu_i$.

For example, given a finite chain $\mathbf{T} = (\mathbf{t}_1,\dots,\mathbf{t}_n)$ of indeterminates, the elements of the polynomial algebra $k[\mathbf{T}] = k[\mathbf{t}_1,\dots,\mathbf{t}_n]$ may be written as $\sum_{\nu\in\mathbb{N}^n} \alpha_\nu \mathbf{T}^\nu$, where $(\alpha_\nu)_{\nu\in\mathbb{N}^n}$ is a family of finite support in k. Moreover, observing the identifications of 12.4, we obtain

$$M_{k[\mathbf{T}]} = \bigoplus_{\nu\in\mathbb{N}^n}(\mathbf{T}^\nu M) \quad (1)$$

as a direct sum of k-modules. For a polynomial law $f\colon M \to N$ over k, these identifications (replacing k by R and f by $f \otimes R$) yield

$$f_{R[\mathbf{T}]}(x) = f_R(x) \qquad (R \in k\text{-}\mathbf{alg},\ x \in M_R) \quad (2)$$

since $f_{R[\mathbf{T}]}(x) = (f\otimes R)_{R[\mathbf{T}]}(x_{R[\mathbf{T}]}) = (f\otimes R)_R(x)_{R[\mathbf{T}]} = f_R(x)$ by 12.2, particularly by (12.2.2). Similarly, given a positive integer q and writing $k[\varepsilon]$ for the free k-algebra on a single generator ε, subject to the relation $\varepsilon^q = 0$ (so $k[\varepsilon] = k[\mathbf{t}_1]/(\mathbf{t}_1^q)$, $\varepsilon = \mathbf{t}_1 + (\mathbf{t}_1^q)$), we have

$$M_{k[\varepsilon]} = \bigoplus_{j=0}^{q-1}(\varepsilon^j M). \quad (3)$$

12.6 A standard identification. For all $R \in k$-**alg**, we will systematically adopt the canonical identification

$$(M_1 \times \cdots \times M_n)_R = M_{1R} \times \cdots \times M_{nR}$$

as R-modules such that

$$(v_1, \ldots, v_n) \otimes r = (v_1 \otimes r, \ldots, v_n \otimes r), \tag{1}$$

$$(v_1 \otimes r_1, \ldots, v_n \otimes r_n) = \sum_{i=1}^{n} (0, \ldots, 0, v_i, 0, \cdots, 0) \otimes r_i$$

for all $v_i \in M$, $r_i \in R$, $1 \leq i \leq n$. Given a morphism $\varphi\colon R \to S$ in k-**alg**, this identification implies

$$(\mathbf{1}_{M_1} \otimes \varphi) \times \cdots \times (\mathbf{1}_{M_n} \otimes \varphi) = \mathbf{1}_{M_1 \times \cdots \times M_n} \otimes \varphi. \tag{2}$$

12.7 Homogeneous polynomial laws. A polynomial law $f\colon M \to N$ is said to be *homogeneous of degree* $d \in \mathbb{N}$ if $f_R(rx) = r^d f_R(x)$ for all $R \in k$-**alg**, $r \in R$, $x \in M_R$. More generally, a polynomial law $f\colon M_1 \times \cdots \times M_n \to N$ is said to be *multi-homogeneous of multi-degree* $d = (d_1, \ldots, d_n) \in \mathbb{N}^n$ if

$$f_R(r_1 x_1, \ldots, r_n x_n) = r_1^{d_1} \cdots r_n^{d_n} f_R(x_1, \ldots, x_n)$$

for all $R \in k$-**alg**, $r_i \in R$, $x_i \in M_{iR}$, $i = 1, \ldots, n$. Here and in the sequel, we always identify $(M_1 \times \cdots \times M_n)_R = M_{1R} \times \cdots \times M_{nR}$ canonically by means of (12.6.1). Thanks to Exc. 12.33, multi-homogeneous (resp. homogeneous) polynomial laws of multi-degree $\hat{1} = (1, \ldots, 1)$ (resp. of degree 2) identify canonically with multi-linear (resp. quadratic) maps in the usual sense (resp. in the sense of 11.1). Notice also that a multi-homogeneous polynomial law of multi-degree $d \in \mathbb{N}^n$ is homogeneous of degree $|d|$. Scalar homogeneous polynomial laws are called *forms*. We speak of linear, quadratic, cubic, quartic, ... forms instead of forms of degree $d = 1, 2, 3, 4, \ldots$.

12.8 Local finiteness. A family $(f_i)_{i \in I}$ of polynomial laws $f_i\colon M \to N$ $(i \in I)$ is said to be *locally finite* if, for all $R \in k$-**alg** and all $x \in M_R$, the family $(f_{iR}(x))_{i \in I}$ of elements in N_R has finite support. In this case, we obtain a well-defined polynomial law

$$\sum_{i \in I} f_i\colon M \longrightarrow N$$

over k by setting

$$(\sum_{i \in I} f_i)_R(x) := \sum_{i \in I} f_{iR}(x) \qquad (R \in k\text{-}\mathbf{alg},\ x \in M_R).$$

Note that this definition mutatis mutandis makes sense also if each f_i, $i \in I$, is

merely assumed to be a family of set maps $f_{iR}\colon M_R \to N_R$, $R \in k\text{-}\mathbf{alg}$, which may or may not vary functorially with R.

12.9 Theorem. *Let $f\colon M \to N$ be a polynomial law over k and n a positive integer. Then there exists a unique locally finite family of polynomial laws*

$$\Pi^\nu f\colon M^n \longrightarrow N \qquad\qquad (\nu \in \mathbb{N}^n)$$

such that

$$f_R(\sum_{i=1}^n r_i x_i) = \sum_{\nu\in\mathbb{N}^n} r^\nu (\Pi^\nu f)_R(x) \tag{1}$$

for all $R \in k\text{-}\mathbf{alg}$, $r = (r_1, \dots, r_n) \in R^n$, $x = (x_1, \dots, x_n) \in (M_R)^n$. In particular,

$$f_{R[\mathbf{T}]}(\sum_{i=1}^n \mathbf{t}_i x_i) = \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu (\Pi^\nu f)_R(x), \tag{2}$$

and this condition alone determines the family $(\Pi^\nu f)_{\nu\in\mathbb{N}^n}$ uniquely.

Proof We begin by showing uniqueness, so suppose $(\Pi^\nu f)_{\nu\in\mathbb{N}^n}$ is a family of the desired kind. Replacing R by $R[\mathbf{T}]$ and r_i by $\mathbf{t}_i$ but keeping $x_i \in M_R$ for $1 \le i \le n$ in (1), the identification (12.5.1) implies

$$f_{R[\mathbf{T}]}(\sum_{i=1}^n \mathbf{t}_i x_i) = \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu (\Pi^\nu f)_{R[\mathbf{T}]}(x),$$

where the right-hand side by (12.5.2) agrees with the one of (2). Hence (2) holds, and in view of (12.5.1) again, (2) determines the quantities $(\Pi^\nu f)_R(x) \in N_R$ uniquely. Thus the family $(\Pi^\nu f)_{\nu\in\mathbb{N}^n}$ is unique. In order to establish its existence, we let $R \in k\text{-}\mathbf{alg}$ and $x = (x_1, \dots, x_n) \in M_R^n$. Then $f_{R[\mathbf{T}]}(\sum_{i=1}^n \mathbf{t}_i x_i) \in N_{R[\mathbf{T}]}$, and (12.5.1) yields a unique family $((\Pi^\nu f)_R(x))_{\nu\in\mathbb{N}^n}$ of elements in N_R having finite support such that (2) holds. We have thus obtained a locally finite family

$$(\Pi^\nu f)_{\nu\in\mathbb{N}^n} = \Big(((\Pi^\nu f)_R)_{R\in k\text{-}\mathbf{alg}}\Big)_{\nu\in\mathbb{N}^n}$$

of set maps $(\Pi^\nu f)_R\colon M_R^n \to N_R$, $\nu \in \mathbb{N}^n$, $R \in k\text{-}\mathbf{alg}$, satisfying (2).

Next we show (1), so let $R \in k\text{-}\mathbf{alg}$, $r = (r_1, \dots, r_n) \in R^n$, $x = (x_1, \dots, x_n) \in M_R^n$ and $\varphi\colon R[\mathbf{T}] \to R$ the R-algebra homomorphism having $\mathbf{t}_i \mapsto r_i$ for $1 \le i \le n$. Using the identification (9.4.1), we conclude $(\mathbf{1}_M \otimes \varphi)(\mathbf{T}^\nu y) = r^\nu y$ for $\nu \in \mathbb{N}^n$, $y \in M_R^n$, ditto for N in place of M. Hence (12.2.1) and (2) imply

$$\begin{aligned} f_R(\sum_{i=1}^n r_i x_i) &= f_R \circ (\mathbf{1}_M \otimes \varphi)(\sum_{i=1}^n \mathbf{t}_i x_i) = (\mathbf{1}_N \otimes \varphi) \circ f_{R[\mathbf{T}]}(\sum_{i=1}^n \mathbf{t}_i x_i) \\ &= \sum_{\nu\in\mathbb{N}^n} (\mathbf{1}_N \otimes \varphi)(\mathbf{T}^\nu (\Pi^\nu f)_R(x)) = \sum_{\nu\in\mathbb{N}^n} r^\nu (\Pi^\nu f)_R(x), \end{aligned}$$

which completes the proof of (1). It remains to show that the $(\Pi^\nu f)_R$, $\nu \in \mathbb{N}^n$ vary functorially with $R \in k$-**alg**, so let $\varphi\colon R \to S$ be any morphism in k-**alg** and $\psi\colon R[\mathbf{T}] \to S[\mathbf{T}]$ its natural extension fixing $\mathbf{t}_i$ for $1 \le i \le n$. One checks $(\mathbf{1}_M \otimes \psi)(\mathbf{T}^\nu y) = \mathbf{T}^\nu(\mathbf{1}_M \otimes \varphi)(y)$ for $\nu \in \mathbb{N}^n$, $y \in M_R$, ditto for N in place of M, and (12.6.2) yields $(\mathbf{1}_M \otimes \varphi)^n = \mathbf{1}_{M^n} \otimes \varphi$. Hence

$$\begin{aligned}
\sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu(\mathbf{1}_N \otimes \varphi) \circ (\Pi^\nu f)_R(x) &= (\mathbf{1}_N \otimes \psi)\Big(\sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu(\Pi^\nu f)_R(x)\Big) \\
&= (\mathbf{1}_N \otimes \psi) \circ f_{R[\mathbf{T}]}\Big(\sum_{i=1}^n \mathbf{t}_i x_i\Big) \\
&= f_{S[\mathbf{T}]} \circ (\mathbf{1}_M \otimes \psi)\Big(\sum_{i=1}^n \mathbf{t}_i x_i\Big) \\
&= f_{S[\mathbf{T}]}\Big(\sum_{i=1}^n \mathbf{t}_i(\mathbf{1}_M \otimes \varphi)(x_i)\Big) \\
&= \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu(\Pi^\nu f)_S\big((\mathbf{1}_M \otimes \varphi)(x_1), \ldots, (\mathbf{1}_M \otimes \varphi)(x_n)\big) \\
&= \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu\big((\Pi^\nu f)_S \circ (\mathbf{1}_{M^n} \otimes \varphi)\big)(x),
\end{aligned}$$

and comparing coefficients, the assertion follows. □

12.10 Linearizations. The polynomial laws $\Pi^\nu f$ for $\nu \in \mathbb{N}^n$, $n \in \mathbb{Z}$, $n > 0$ as constructed in Thm. 12.9 are called the *linearizations* or *polarizations* of the polynomial law $f\colon M \to N$ over k. We list a few elementary properties.

(a) For $\nu \in \mathbb{N}^n$, *the polynomial law* $\Pi^\nu f\colon M^n \to N$ *is multi-homogeneous of multi-degree* ν. Indeed, replacing x_i by $r_i x_i$ ($r_i \in R$, $1 \le i \le n$) on the left-hand side of (12.9.2) amounts to the same as carrying out the substitution $\mathbf{t}_i \mapsto r_i \mathbf{t}_i$ ($1 \le i \le n$). Hence the assertion follows from (12.9.1), (12.5.2).

(b) *Writing* $\pi.\nu := (\nu_{\pi^{-1}(1)}, \ldots, \nu_{\pi^{-1}(n)})$ *for* $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$ *and* $\pi \in \mathcal{S}_n$, *we have*

$$(\Pi^\nu f)_R(x_{\pi(1)}, \ldots, x_{\pi(n)}) = (\Pi^{\pi.\nu} f)_R(x_1, \ldots, x_n) \tag{1}$$

for all $R \in k$-**alg**, $x_1, \ldots, x_n \in M_R$, which follows immediately from the fact that the left-hand side of (12.9.2) remains unaffected by any permutation of the summands.

(c) *If* f *is homogeneous of degree* $d \in \mathbb{N}$, *then* $\Pi^\nu f = 0$ *for all* $\nu \in \mathbb{N}^n$, $n \in \mathbb{Z}$, $n > 0$, *unless* $|\nu| = d$. In order to see this, let $\mathbf{s}$ be a new variable, replace $\mathbf{t}_i$ by $\mathbf{s}\mathbf{t}_i$ for $1 \le i \le n$ in (12.9.2) and compare coefficients of $\mathbf{s}^{|\nu|}$.

In particular, assume $d > 0$, let $n = d$ and $\nu := \hat{1} := (1, \dots, 1) \in \mathbb{N}^d$. Then (a) shows that $\Pi^{\hat{1}} f\colon M^d \to N$ is multi-homogeneous of multi-degree $\hat{1}$, i.e., it is a multi-linear map (Exc. 12.33 (a)), while we conclude from (b) that it is totally symmetric. Putting $x_1 = \cdots = x_d =: y \in M_R$ in (12.9.2) and comparing coefficients of $\mathbf{t}_1 \cdots \mathbf{t}_d$ in

$$(\sum_{i_1,\dots,i_n=1}^{d} \mathbf{t}_{i_1} \cdots \mathbf{t}_{i_n}) f_R(y) = (\sum_{i=1}^{d} \mathbf{t}_i)^d f_R(y) = \sum_{\nu\in\mathbb{N}^d} \mathbf{T}^\nu (\Pi^\nu f)_R(y, \dots, y),$$

we conclude

$$(\Pi^{\hat{1}} f)_R(y, \dots, y) = d! f_R(y) \tag{2}$$

for all $R \in k$-**alg**, $y \in M_R$. We call $\Pi^{\hat{1}} f$ the *total linearization* of f.

12.11 Corollary. *Let $\mathbf{T} = (\mathbf{t}_i)_{i\geq 0}$ be a countably infinite family of indeterminates and $f\colon M \to N$ a polynomial law over k. Then the following conditions are equivalent.*

(i) $f = 0$ *as a polynomial law over k.*

(ii) $(\Pi^\nu f)_k = 0$ *as a set map $M^n \to N$, for all $n \in \mathbb{Z}$, $n > 0$, and all $\nu \in \mathbb{N}^n$.*

(iii) $f_{k[\mathbf{T}]} = 0$ *as a set map $M_{k[\mathbf{T}]} \to N_{k[\mathbf{T}]}$.*

Proof (i) $\Leftrightarrow$ (ii). The implication from left to right is obvious. Conversely, suppose $(\Pi^\nu f)_k = 0$ for all $n \in \mathbb{Z}$, $n > 0$, $\nu \in \mathbb{N}^n$. We must show $f_R = 0$ for all $R \in k$-**alg**. Every $x \in M_R$ can be written as $x = \sum_{i=1}^n r_i v_{iR}$ for some $n \in \mathbb{Z}$, $n > 0$, $r = (r_1, \dots, r_n) \in R^n$, $v = (v_1, \dots, v_n) \in M^n$. From (12.9.1) and (12.2.2) we therefore deduce

$$f_R(x) = \sum_{\nu\in\mathbb{N}^n} r^\nu (\Pi^\nu f)_R(v_R) = \sum_{\nu\in\mathbb{N}^n} r^\nu (\Pi^\nu f)_k(v)_R = 0,$$

as desired.

(i) $\Leftrightarrow$ (iii). Again the implications from left to right is obvious. Conversely, assume $f_{k[\mathbf{T}]} = 0$ as a set map and let $R \in k$-**alg**. We must show $f_R(x) = 0$ for all $x \in M_R$. Write $x = \sum_{i=0}^n x_i \otimes r_i$, $x_i \in M$, $r_i \in R$ for $0 \leq i \leq n$. Let $\varphi\colon k[\mathbf{T}] \to R$ be the unique morphism in k-**alg** sending $\mathbf{t}_i$ to r_i for $0 \leq i \leq n$ and to 0 for $i > n$. Then (12.2.1) implies $f_R(x) = f_R \circ (\mathbf{1}_M \otimes \varphi)(\sum_{i=0}^n x_i \otimes \mathbf{t}_i) = (\mathbf{1}_N \otimes \varphi) \circ f_{k[\mathbf{T}]}(\sum_{i=0}^n x_i \otimes \mathbf{t}_i) = 0$, as claimed. □

12.12 Corollary. *Assume the k-modules M and N are free of finite rank, with bases $(v_1, \dots, v_m)$ and $(w_1, \dots, w_n)$, respectively. A family of set maps $f_R\colon M_R \to N_R$, $R \in k$-**alg**, is a polynomial law over k if and only if there exist*

polynomials $p_1, \dots, p_n \in k[\mathbf{t}_1, \dots, \mathbf{t}_m]$ *such that*

$$f_R(\sum_{i=1}^{m} r_i v_{iR}) = \sum_{j=1}^{n} p_j(r_1, \dots, r_m) w_{jR} \tag{1}$$

for all $R \in k$-**alg**, $r_1, \dots, r_m \in R$.

Proof If such polynomials exist, it is readily checked that the f_R vary functorially with $R \in k$-**alg**, hence give rise to a polynomial law $f\colon M \to N$. Conversely, let $f\colon M \to N$ be a polynomial law over k. For $R \in k$-**alg** and $r = (r_1, \dots, r_m) \in R^m$, we put $v := (v_1, \dots, v_m)$ and apply (12.9.1) to conclude

$$f_R(\sum_{i=1}^{m} r_i v_{iR}) = \sum_{\nu \in \mathbb{N}^m} r^\nu (\Pi^\nu f)_R(v_R) = \sum_{\nu \in \mathbb{N}^m} r^\nu (\Pi^\nu f)_k(v)_R.$$

Here $(\Pi^\nu f)_k(v) \in N$, $\nu \in \mathbb{N}^m$, may be written as

$$(\Pi^\nu f)_k(v) = \sum_{j=1}^{n} \beta_{j\nu} w_j$$

with unique coefficients $\beta_{j\nu} \in k$, $1 \le j \le n$. Since the family $(\Pi^\nu f)_{\nu \in \mathbb{N}^m}$ is locally finite, we can form the polynomials

$$p_j := \sum_{\nu \in \mathbb{N}^m} \beta_{j\nu} \mathbf{T}^\nu \in k[\mathbf{T}] \qquad (\mathbf{T} := (\mathbf{t}_1, \dots, \mathbf{t}_m),\ 1 \le j \le n)$$

which obviously satisfy (1). □

12.13 Corollary. *Let V, W be finite-dimensional vector spaces over an infinite field F. Then the assignment $f \mapsto f_F$ defines a linear bijection from* $\mathrm{Pol}_F(V, W)$ *onto the vector space of polynomial maps from V to W. For bases $(v_1, \dots, v_m)$, $(w_1, \dots, w_n)$ of V, W, respectively, over F, the inverse of this bijection assigns to every polynomial map $f\colon V \to W$ the polynomial law given by the family of set maps $f_R\colon V_R \to W_R$, $R \in k$-**alg**, as defined in (12.1.2).*

Proof This follows from Cor. 12.12 combined with 12.1. □

12.14 Binary linearizations. It is sometimes useful to rewrite the formalism of Thm. 12.9 for $n = 2$, so let $f\colon M \to N$ be any polynomial law over k. With independent variables $\mathbf{s}, \mathbf{t}$, we then apply (12.9.2) and obtain

$$f_{R[\mathbf{s},\mathbf{t}]}(\mathbf{s}x + \mathbf{t}y) = \sum_{m \ge 0, n \ge 0} \mathbf{s}^m \mathbf{t}^n (\Pi^{(m,n)} f)_R(x, y) \tag{1}$$

for all $R \in k$-**alg**, $x, y \in M_R$, and (12.10.1) yields

$$(\Pi^{(m,n)} f)_R(x, y) = (\Pi^{(n,m)} f)_R(y, x). \tag{2}$$

If f is homogeneous of degree $d \in \mathbb{N}$, we obtain $\Pi^{(m,n)} f = 0$ for $m, n \geq 0$ unless $m + n = d$ (12.10 (c)), so (1) collapses to

$$f_{R[\mathbf{s},\mathbf{t}]}(\mathbf{s}x + \mathbf{t}y) = \sum_{n=0}^{d} \mathbf{s}^{d-n}\mathbf{t}^n (\Pi^{(d-n,n)} f)_R(x, y)$$

for all $R \in k$-**alg**, $x, y \in M_R$.

12.15 Total derivatives. Let $f\colon M \to N$ be any polynomial law over k. By Thm. 12.9, the family $(\Pi^{(m,n)} f)_{m,n\geq 0}$ of polynomial laws $M \times M \to N$ is locally finite, allowing us to define, for all $n \in \mathbb{N}$, a polynomial law

$$D^n f := \sum_{m\geq 0} \Pi^{(m,n)} f\colon M \times M \longrightarrow N, \tag{1}$$

called the *n-th (total) derivative* of f. By 12.10 (a), it is homogeneous of degree n in the second variable, i.e.,

$$(D^n f)_R(x, ry) = r^n (D^n f)_R(x, y). \qquad (R \in k\text{-}\mathbf{alg},\ r \in R,\ x, y \in M_R)$$

In particular, Exc. 12.30 and (12.9.1) imply

$$(D^0 f)_R(x, y) = \sum_{m\geq 0} (\Pi^{(m,0)} f)_R(x, y) = \sum_{m\geq 0} (\Pi^m f)_R(x) = f_R(x), \tag{2}$$

hence $D^0 f = f \circ \pi_1$ as polynomial laws over k, where $\pi_1\colon M \times M \to M$ is the projection onto the first factor. Moreover, abbreviating $Df := D^1 f$,

$$(Df)_R(x)\colon M_R \longrightarrow N_R, \quad y \longmapsto (Df)_R(x)(y) := (Df)_R(x, y),$$

by Exc. 12.33 (a) is an R-linear map for all $x \in M_R, R \in k$-**alg**. Similarly,

$$(D^2 f)_R(x)\colon M_R \longrightarrow N_R, \quad y \longmapsto (D^2 f_R)(x, y),$$

is an R-quadratic map in the sense of 11.1. Specializing $\mathbf{s} \mapsto 1$ in (12.14.1), we obtain the relation

$$f_{R[\mathbf{t}]}(x + \mathbf{t}y) = \sum_{n\geq 0} \mathbf{t}^n (D^n f)_R(x, y), \tag{3}$$

called the *Taylor expansion* of f at x. For $q \in \mathbb{Z}$, $q > 0$, it is sometimes convenient to replace $R[\mathbf{t}]$ by the algebra $R[\varepsilon], \varepsilon^{q+1} = 0$, and to apply (12.9.1). The ensuing relation

$$f_{R[\varepsilon]}(x + \varepsilon y) = \sum_{n=0}^{q} \varepsilon^n (D^n f)_R(x, y) \tag{4}$$

determines the first q derivatives of f uniquely. In particular, for $q = 1$, $R[\varepsilon]$ is the algebra of dual numbers and

$$f_{R[\varepsilon]}(x + \varepsilon y) = f_R(x) + \varepsilon(Df)_R(x, y). \tag{5}$$

12.16 Total derivatives of homogeneous polynomial laws. Let $f\colon M \to N$ be a homogeneous polynomial law of degree $d \geq 0$ over k. By 12.10 (c), the terms $\Pi^{(m,n)}f$ in the sum on the right of (12.15.1) vanish unless $m + n = d$. Thus $D^n f = 0$ for $n > d$ and

$$D^n f = \Pi^{(d-n,n)} f \qquad (0 \leq n \leq d). \tag{1}$$

Comparing this with (12.14.2), we conclude

$$(D^n f)_R(x, y) = (D^{d-n} f)_R(y, x) \qquad (R \in k\text{-}\mathbf{alg},\ 0 \leq n \leq d,\ x, y \in M_R). \tag{2}$$

We also obtain *Euler's differential equation*

$$(Df)_R(x, x) = d f_R(x) \tag{3}$$

by setting $y = x$ in (12.15.5), which gives $f_R(x) + \varepsilon(Df)(x, x) = (1 + \varepsilon)^d f_R(x) = f_R(x) + \varepsilon d f_R(x)$, as claimed.

12.17 Differential calculus. The standard rules of differentiation are valid for arbitrary polynomial laws and will henceforth be used without further comment. For convenience, we mention just a few examples.

Let $f\colon M \to N$, $g\colon N \to P$, $f_i\colon M \to N_i$ $(i = 1, 2)$ be polynomial laws over k and suppose $N_1 \times N_2 \to N$ is a k-bilinear map written multiplicatively. Furthermore, let $\lambda\colon M \to N$ (resp. $Q\colon M \to N$) be a linear (resp. quadratic) map. Then, dropping the subscript "R" for simplicity (e.g., by writing $f(x)$ instead of $f_R(x)$), we have

$$(D\lambda)(x, y) = \lambda(y), \tag{1}$$

$$(DQ)(x, y) = Q(x, y), \tag{2}$$

$$(D^2 Q)(x, y) = Q(y), \tag{3}$$

$$(D(g \circ f))(x, y) = (Dg)(f(x), (Df)(x, y)), \tag{4}$$

$$(D(g \circ \lambda))(x, y) = (Dg)(\lambda(x), \lambda(y)) \tag{5}$$

$$\begin{aligned}(D^2(g \circ f))(x, y) = {} & (Dg)(f(x), (D^2 f)(x, y)) \\ & + (D^2 g)(f(x), (Df)(x, y)),\end{aligned} \tag{6}$$

$$(D(f_1 f_2))(x, y) = (Df_1)(x, y) f_2(x) + f_1(x)(Df_2)(x, y), \tag{7}$$

$$(D^n(f_1 f_2))(x, y) = \sum_{i=0}^{n} (D^i f_1)(x, y)(D^{n-i} f_2)(x, y) \tag{8}$$

for all $R \in k$-**alg**, all $x, y \in M_R$ and all $n \in \mathbb{N}$. Note that (4) (resp. (6)) is the first (resp. second) order chain rule, while (7) (resp. (8)) is the first (resp. n-th) order product rule of the differential calculus. Moreover, (5) by (1) is a special case of (4).

12.18 Directional derivatives. Let $y \in M$. For any polynomial law $f\colon M \to N$ over k, the rule

$$(\partial_y f)_R(x) := (Df)_R(x, y_R) \in N_R \qquad (R \in k\text{-}\mathbf{alg},\ x \in M_R)$$

defines a new polynomial law $\partial_y f\colon M \to N$, called the *derivative of f in the direction y*, and the map

$$\partial_y\colon \operatorname{Pol}_k(M,N) \longrightarrow \operatorname{Pol}_k(M,N)$$

is obviously k-linear.

Our next aim will be to show that the operators ∂_y, $y \in M$, commute and that their iterations relate to the total linearization of a homogeneous polynomial law. To accomplish this, we need some preparation.

12.19 Lemma. *Let $f\colon M \to N$ be a polynomial law over k. Then*

$$(D^p f)_{R[\mathbf{T}]}(\sum_{i=1}^{n} \mathbf{t}_i x_i, x_{n+1}) = \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu (\Pi^{(\nu,p)} f)_R(x_1, \dots, x_n, x_{n+1})$$

*for all $R \in k$-**alg**, $p, n \in \mathbb{N}$, $n > 0$, $x_1, \dots, x_n, x_{n+1} \in M_R$.*

Proof With an additional indeterminate $\mathbf{t}_{n+1}$, we apply (12.9.2) and obtain

$$f_{R[\mathbf{T},\mathbf{t}_{n+1}]}(\sum_{i=1}^{n+1} \mathbf{t}_i x_i) = \sum_{\nu\in\mathbb{N}^n, p\geq 0} \mathbf{T}^\nu \mathbf{t}_{n+1}^p (\Pi^{(\nu,p)} f)_R(x_1, \dots, x_n, x_{n+1}).$$

Invoking the Taylor expansion (12.15.3) and comparing coefficients of $\mathbf{t}_{n+1}^p$, the lemma follows. □

12.20 Lemma. *Let $f\colon M \to N$ be a polynomial law over k and $y \in M$. Then*

$$(\Pi^\nu \partial_y f)_R(x_1, \dots, x_n) = (\Pi^{(\nu,1)} f)_R(x_1, \dots, x_n, y_R)$$

*for all $R \in k$-**alg**, $n \in \mathbb{Z}$, $n > 0$, $\nu \in \mathbb{N}^n$, $x_1, \dots, x_n \in M_R$.*

Proof Applying (12.9.2) to $\partial_y f$, we obtain

$$(\partial_y f)_{R[\mathbf{T}]}(\sum_{i=1}^{n} \mathbf{t}_i x_i) = \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu (\Pi^\nu \partial_y f)_R(x_1, \dots, x_n).$$

On the other hand, treating the left-hand side according to the definition of ∂_y (12.18) and applying Lemma 12.19 for $p = 1$, we conclude

$$(\partial_y f)_{R[\mathbf{T}]}(\sum_{i=1}^{n} \mathbf{t}_i x_i) = \sum_{\nu \in \mathbb{N}^n} \mathbf{T}^\nu (\Pi^{(\nu,1)} f)_R(x_1, \ldots, x_n, y_R),$$

as desired. □

12.21 Proposition. *Let $f\colon M \to N$ be a polynomial law over k, $p \in \mathbb{N}$, and $y_1, \ldots, y_p \in M$. Then*

$$(\partial_{y_1} \cdots \partial_{y_p} f)_R(x) = \sum_{i \geq 0} (\Pi^{(i,1,\ldots,1)} f)_R(x, y_{1R}, \ldots, y_{pR}) \tag{1}$$

*for all $R \in k$-**alg**, $x \in M_R$. In particular, the operators $\partial_y, y \in M$, commute.*

Proof To establish the first part, we argue by induction on p. For $p = 0$, the assertion is just (12.9.1), while the induction step follows immediately from Lemma 12.20. The second part now follows from the first for $p = 2$ and (12.10.1). □

12.22 Corollary. *Let $f\colon M \to N$ be a homogeneous polynomial law of degree $d > 0$. Then the total linearization of f relates to its directional derivatives by the formula*

$$(\hat{\Pi^1} f)_k(y_1, \ldots, y_{d-1}, y_d) = (\partial_{y_1} \cdots \partial_{y_{d-1}} f)_k(y_d) \tag{1}$$

for all $y_1, \ldots, y_{d-1}, y_d \in M$. In particular, the right-hand side is totally symmetric in $y_1, \ldots, y_d$.

Proof Since f is homogeneous of degree d, the right side of (12.21.1) collapses to the single term $(\Pi^{(d-p,1,\ldots,1)} f)_R(x, y_{1R}, \ldots, y_{pR})$ by 12.10 (c), and (1) follows for $p = d - 1$. The rest is clear. □

Our next aim in this section will be to show that a particularly simple and useful Zariski density argument extends from the setting of finite-dimensional vector spaces over infinite fields to arbitrary modules over commutative rings. The key to this extension is the following concept, which is modeled after standard notions in algebraic geometry (cf. Jantzen [146, 1.5], see also 24.16 below).

12.23 Subfunctors. Let A be a unital associative k-algebra, possibly not commutative, and $g\colon M \to A$ a polynomial law over k. For $R \in k$-**alg**, we put

$$\mathbf{D}(g)(R) := \{x \in M_R \mid g_R(x) \in A_R^\times\},$$

where $A_R^\times$ on the right as usual stands for the group of invertible elements in

A_R. Clearly, $\mathbf{D}(g)$ is a subfunctor of $M_{\mathbf{a}}$, i.e., $\mathbf{D}(g)(R) \subseteq M_{\mathbf{a}}(R) = M_R$ is a subset for all $R \in k$-**alg** and $(\mathbf{1}_M \otimes \varphi)(\mathbf{D}(g)(R)) \subseteq \mathbf{D}(g)(S)$ for all morphisms $\varphi\colon R \to S$ in k-**alg**.

12.24 Proposition ([95, Lemma 3.2])**.** *Let A be a unital associative k-algebra and $g\colon M \to A$ a polynomial law over k such that $\mathbf{D}(g)(k) \neq \emptyset$. If $f\colon M \to N$ is a homogeneous polynomial law over k that vanishes on $\mathbf{D}(g)$, i.e., $f_R|_{\mathbf{D}(g)(R)} = 0$ for all $R \in k$-**alg**, then $f = 0$.*

For most applications, this proposition is totally adequate. But sometimes the following more detailed, but also more technical, version will be needed.

12.25 Lemma. *With A and g as in Proposition 12.24, let $f\colon M \to N$ be a homogeneous polynomial law over k and $R \in k$-**alg** such that $f_S|_{\mathbf{D}(g)(S)} = 0$ for all $S \in R$-**alg** $\subseteq k$-**alg** which are free of positive rank as R-modules. Then $f_R = 0$.*

Proof After replacing g by $g \otimes R$ and f by $f \otimes R$ if necessary, we may assume $R = k$. Pick $e \in \mathbf{D}(g)(k)$, so $e \in M$ satisfies $u := g_k(e) \in A^\times$. Substituting $L_{u^{-1}} \circ g$ for g, we may assume $g_k(e) = 1_A$. Now write d for the degree of f and consider the k-algebra $S := k[\varepsilon], \varepsilon^{d+1} = 0$, which is free as a k-module of rank $d+1$. Picking any $x \in M$ and using the identifications of (12.5.3), the Taylor expansion (12.15.4) implies that

$$g_S(e + \varepsilon x) = 1_A + \sum_{n=1}^{d} \varepsilon^n (D^n g)_k(e, x)$$

is invertible in A_S. Hence $e + \varepsilon x \in \mathbf{D}(g)(S)$ and, by hypothesis,

$$0 = f_S(e + \varepsilon x) = \sum_{n=0}^{d} \varepsilon^n (D^n f)_k(e, x).$$

Comparing coefficients of ε^d, we conclude from (12.15.2), (12.16.2) that

$$f_k(x) = (D^0 f)_k(x, e) = (D^d f)_k(e, x) = 0. \qquad \square$$

In our subsequent applications, it will sometimes be necessary to compose polynomial laws with semi-linear maps. In order to explain the meaning of this procedure, the set-up of the present section requires a few minor adjustments.

12.26 Tensor products of semi-linear maps. Let $\sigma\colon K \to K'$ be a morphism in k-**alg** and M', N' be K'-modules. Viewing K' as a K-algebra by means of σ, restriction of scalars converts M' into a K-module, which we denote by ${}_K M'$, or simply by M' if there is no danger of confusion; ditto for N'. Since the

expression $x' \otimes_{K'} y' \in M' \otimes_{K'} N'$, $x' \in M'$, $y' \in N'$, is, in particular, K-bilinear, we obtain a natural K-linear, hence σ-semi-linear, map

$$\mathrm{can}_\sigma \colon {}_KM' \otimes_K {}_KN' \longrightarrow M' \otimes_{K'} N', \quad x' \otimes_K y' \longmapsto x' \otimes_{K'} y'. \tag{1}$$

Now suppose in addition that M, N are K-modules and $\varphi \colon M \to M'$, $\psi \colon N \to N'$ are σ-semi-linear maps. These may be regarded as K-linear maps ${}_K\varphi \colon M \to {}_KM'$, ${}_K\psi \colon N \to {}_KN'$, and the composite

$$M \otimes_K N \xrightarrow[{}_K\varphi \otimes_K {}_K\psi]{} {}_KM' \otimes_K {}_KN' \xrightarrow[\mathrm{can}_\sigma]{} M' \otimes_{K'} N'$$

gives rise to a σ-semi-linear map

$$\varphi \otimes_\sigma \psi \colon M \otimes_K N \longrightarrow M' \otimes_{K'} N', \quad x \otimes_K y \longmapsto \varphi(x) \otimes_{K'} \psi(y), \tag{2}$$

called the *σ-semi-linear tensor product of φ and ψ*.

12.27 Restriction of scalars. Let $K \in k$-**alg**. We wish to convert polynomial laws over K into ones over k. To this end, let M, N be K-modules. As in 12.26, we write ${}_kM$ for M viewed as a k-module. Similarly, every K-linear map $\varphi \colon M \to N$ may be viewed as a k-linear map ${}_k\varphi \colon {}_kM \to {}_kN$. Now let $R \in k$-**alg**. Then $R_K \in K$-**alg** and, using associativity of the tensor product [28, II.3, Prop. 8], we obtain a natural identification

$$\begin{aligned} M_{R_K} &= M \otimes_K (R \otimes K) = M \otimes_K (K \otimes R) \\ &= (M \otimes_K K) \otimes R = M \otimes R = ({}_kM)_R \end{aligned} \tag{1}$$

of R_K-modules such that

$$x \otimes r = x \otimes_K r_K = x \otimes_K (r \otimes 1_K), \quad x \otimes_K (r \otimes a) = (ax) \otimes r \tag{2}$$

for all $x \in M$, $r \in R$, $a \in K$. Here the natural action of R_K on M_{R_K} translates into one on $({}_kM)_R$ via

$$(r \otimes a)(x \otimes r') = (ax) \otimes (rr') \tag{3}$$

for $r, r' \in R$, $a \in K$, $x \in M$. If $\varphi \colon M \to N$ is a K-linear map, then (2) implies $({}_k\varphi)_R = \varphi_{R_K}$. Similarly, if $\varrho \colon R \to S$ is a morphism in k-**alg**, then $\varrho_K \colon R_K \to S_K$ is one in K-**alg**, and we have $\mathbf{1}_{{}_kM} \otimes \varrho = \mathbf{1}_M \otimes_K \varrho_K$. Given a polynomial law $f \colon M \to N$ over K, we therefore conclude that ${}_kf \colon {}_kM \to {}_kN$ defined by

$$({}_kf)_R := f_{R_K} \tag{4}$$

as a set map from $({}_kM)_R = M_{R_K}$ to $({}_kN)_R = N_{R_K}$, for all $R \in k$-**alg**, is a polynomial law over k. We say that ${}_kf$ arises from f *by restriction of scalars* from K to k. As an example, any K-quadratic map $Q \colon M \to N$ may be viewed canonically as a k-quadratic map ${}_kQ \colon {}_kM \to {}_kN$. Following Exc. 12.33 (b)

below, we thus obtain polynomial laws $\tilde{Q}\colon M \to N$ over K and $\widetilde{{}_kQ}\colon {}_kM \to {}_kN$ over k that are both homogeneous of degree 2, and one checks that ${}_k\tilde{Q} = \widetilde{{}_kQ}$. In other words, after the identification (1) we have

$$Q_{R_K} = ({}_kQ)_R \tag{5}$$

for all $R \in k$-**alg**.

Note for $L \in K$-**alg** $\subseteq k$-**alg** and a polynomial law $g\colon P \to Q$ over L that

$${}_k({}_Kg) = {}_kg, \tag{6}$$

as polynomial laws over k, so iterated restrictions of scalars collapse to single ones.

12.28 Semi-linear polynomial squares. Let $\sigma\colon K \to K'$ be a morphism in k-**alg**. By a *σ-semi-linear polynomial square* we mean a diagram of the form

$$\begin{array}{ccc} M & \xrightarrow[\varphi]{} & M' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ N & \xrightarrow[\psi]{} & N', \end{array} \tag{1}$$

where $f\colon M \to N$ is a polynomial law over K, $f'\colon M' \to N'$ is one over K', and $\varphi\colon M \to M'$, $\psi\colon N \to N'$ are σ-semi-linear maps. Note that φ may canonically be viewed as a k-linear map ${}_k\varphi\colon {}_kM \to {}_kM'$, ditto for ψ. We say that (1) *is commutative* if the diagram

$$\begin{array}{ccc} {}_kM & \xrightarrow[{}_k\varphi]{} & {}_kM' \\ {\scriptstyle {}_kf}\downarrow & & \downarrow{\scriptstyle {}_kf'} \\ {}_kN & \xrightarrow[{}_k\psi]{} & {}_kN' \end{array} \tag{2}$$

of polynomial laws over k in the sense of 12.27 is commutative. We wish to describe the meaning of this condition explicitly.

Let $R \in k$-**alg** and identify $R_K = K_R$ (resp. $R_{K'} = K'_R$) as K- (resp. K'-)algebras and as R-algebras canonically. Then

$$\sigma_R := {}_k\sigma \otimes \mathbf{1}_R\colon K_R \longrightarrow K'_R \tag{3}$$

is a σ-semi-linear morphism in R-**alg**, and one checks that

$$({}_k\varphi)_R = \varphi \otimes_\sigma \sigma_R, \quad ({}_k\psi)_R = \psi \otimes_\sigma \sigma_R, \tag{4}$$

where the right-hand sides refer to the σ-semi-linear tensor product as defined

in (12.26.2). Taking into account the identifications of 12.26, we therefore conclude that the σ-semi-linear polynomial square (1) (i.e., (2)) commutes if and only if, for all $R \in k$-**alg**, the diagram

$$\begin{array}{ccc} M_{K_R} & \xrightarrow[\varphi\otimes_\sigma \sigma_R]{} & M'_{K'_R} \\ {\scriptstyle f_{K_R}}\downarrow & & \downarrow{\scriptstyle f'_{K'_R}} \\ N_{K_R} & \xrightarrow[\psi\otimes_\sigma \sigma_R]{} & N'_{K'_R} \end{array} \tag{5}$$

of set maps commutes. In particular, since

$$\varphi \otimes_\sigma \sigma = \varphi, \quad \psi \otimes_\sigma \sigma = \psi, \tag{6}$$

the special case $R = k$ in (5) amounts to

$$\begin{array}{ccc} M & \xrightarrow[\varphi]{} & M' \\ {\scriptstyle f_K}\downarrow & & \downarrow{\scriptstyle f'_{K'}} \\ N & \xrightarrow[\psi]{} & N' \end{array} \tag{7}$$

being commutative.

Let

$$\begin{array}{ccccc} & & k & & \\ & & \downarrow & & \\ & & k' & & \\ & \swarrow & & \searrow & \\ K & & \xrightarrow[\sigma]{} & & K' \end{array} \tag{8}$$

be a commutative diagram in k-**alg**. If (1) commutes as a σ-semi-linear polynomial square, then so does

$$\begin{array}{ccc} {\scriptstyle k'}M & \xrightarrow[k'\varphi]{} & {\scriptstyle k'}M' \\ {\scriptstyle k'f}\downarrow & & \downarrow{\scriptstyle k'f'} \\ {\scriptstyle k'}N & \xrightarrow[k'\psi]{} & {\scriptstyle k'}N' \end{array} \tag{9}$$

as a diagram of polynomial laws over k' since by definition and (12.27.6), this becomes true when restricting scalars still further to k, allowing us to apply Exc. 12.45 below and to obtain the assertion.

12.29 Example. Let $\sigma\colon K \to K'$ be a morphism in k-**alg** and $f\colon M \to N$ a polynomial law over k. We claim that the σ-semi-linear polynomial square

$$\begin{array}{ccc} M_K & \xrightarrow[\mathbf{1}_M\otimes\sigma]{} & M_{K'} \\ {\scriptstyle f\otimes K}\downarrow & & \downarrow{\scriptstyle f\otimes K'} \\ N_K & \xrightarrow[\mathbf{1}_N\otimes\sigma]{} & N_{K'} \end{array} \tag{1}$$

commutes. Indeed, by (12.28.5), this will follow once we have shown that the diagram

$$\begin{array}{ccc} (M_K)_{K_R} & \xrightarrow[(\mathbf{1}_M\otimes\sigma)\otimes_\sigma\sigma_R]{} & (M_{K'})_{K'_R} \\ {\scriptstyle (f\otimes K)_{K_R}}\downarrow & & \downarrow{\scriptstyle (f\otimes K')_{K'_R}} \\ (N_K)_{K_R} & \xrightarrow[(\mathbf{1}_N\otimes\sigma)\otimes_\sigma\sigma_R]{} & (N_{K'})_{K'_R} \end{array}$$

of set maps commutes, for all $R \in k$-**alg**. But after natural identifications, this is the same as

$$\begin{array}{ccc} M_{K_R} & \xrightarrow[\mathbf{1}_M\otimes\sigma_R]{} & M_{K'_R} \\ {\scriptstyle f_{K_R}}\downarrow & & \downarrow{\scriptstyle f'_{K'_R}} \\ N_{K_R} & \xrightarrow{\mathbf{1}_N\otimes\sigma_R} & N_{K'_R} \end{array},$$

which commutes since f is a polynomial law over k.

Let us consider the special case that $\sigma\colon k \to K$ is the unit homomorphism of some $K \in k$-**alg**. For any k-module M, it follows that $\mathrm{can}_{M,K} = \mathbf{1}_M \otimes \sigma\colon M \to M_K$ is a σ-semi-linear map and, given a polynomial law $f\colon M \to N$ over k, equation (1) takes on the form

$$\begin{array}{ccc} M & \xrightarrow[\mathrm{can}_{M,K}]{} & M_K \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f\otimes K} \\ N & \xrightarrow[\mathrm{can}_{N,K}]{} & N_K. \end{array} \tag{2}$$

Thus, by definition,

$$\begin{array}{ccc} M & \xrightarrow[{}_k(\mathrm{can}_{M,K})]{} & {}_k(M_K) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle {}_k(f\otimes K)} \\ N & \xrightarrow[{}_k(\mathrm{can}_{N,K})]{} & {}_k(N_K) \end{array} \tag{3}$$

is a commutative diagram of polynomial laws over k.

Exercises

12.30. Let $f\colon M \to N$ be a polynomial law over k, $R \in k$-**alg**, n, p be positive integers and $x \in M_R^n$, $y \in M_R^p$. Prove for $\nu \in \mathbb{N}^n$ that

$$(\Pi^{(\nu,0,\dots,0)} f)_R(x, y) = (\Pi^{\nu} f)_R(x).$$

12.31 (Roby [249])**.** Let $f\colon M \to N$ be a polynomial law over k. Show that there is a unique family $(f_d)_{d\geq 0}$ of polynomial laws $M \to N$ over k such that the following conditions hold: (i) the family $(f_d)_{d\geq 0}$ is locally finite, (ii) $f = \sum f_d$, (iii) f_d is homogeneous of degree d for all $d \geq 0$. Give an example where $f_d \neq 0$ for all $d \geq 0$.

12.32 (Roby [249])**.** *Constant polynomial laws.* Show that the homogeneous polynomial laws $M \to N$ of degree 0 are precisely of the form $\hat{w}, w \in N$, where $\hat{w}_R\colon M_R \to N_R$ for $R \in k$-**alg** is given by $\hat{w}_R(x) := w_R, x \in M_R$.

12.33 (Roby [249])**.** (a) Let $\mu\colon M_1 \times \cdots \times M_n \to N$ be a multi-linear map. Show that $\tilde{\mu}\colon M_1 \times \cdots \times M_n \to N$ given by $\tilde{\mu}_R := \mu \otimes R$ (the R-multi-linear extension of μ) for $R \in k$-**alg** is a multi-homogeneous polynomial law of multi-degree $\hat{1} = (1, \dots, 1)$. Show that, conversely, every multi-homogeneous polynomial law $M_1 \times \cdots \times M_n \to N$ of multi-degree $\hat{1}$ uniquely arises in this way.

(b) If $Q\colon M \to N$ is a quadratic map, show that $\tilde{Q}\colon M \to N$ given by $\tilde{Q}_R := Q \otimes R$ (the base change of Q from k to R in the sense of 11.5) for $R \in k$-**alg** is a homogeneous polynomial law of degree 2 over k. Show that, conversely, every homogeneous polynomial law $M \to N$ of degree 2 over k uniquely arises in this way. Identifying quadratic maps and homogeneous polynomial laws of degree 2 accordingly, prove that the total first derivative $DQ\colon M \times M \to N$ of Q as a polynomial law is the same as the bilinearization of Q as quadratic map.

12.34 (Roby [249])**.** Let $f\colon M \to N$ be a polynomial law over k and $p \in \mathbb{N}$.

(a) Show for $n \in \mathbb{Z}, n > p, \nu_1, \dots, \nu_n \in \mathbb{N}, x, x_1, \dots, x_p \in M_R, R \in k$-**alg** that

$$\begin{aligned}&(\Pi^{(\nu_1,\dots,\nu_p,\nu_{p+1},\dots,\nu_n)} f)_R(x_1, \dots, x_p, x, \dots, x)\\ &\quad = \frac{(\nu_{p+1} + \cdots + \nu_n)!}{\nu_{p+1}! \cdots \nu_n!} (\Pi^{(\nu_1,\dots,\nu_p,\nu_{p+1}+\cdots+\nu_n)} f)_R(x_1, \dots, x_p, x)\end{aligned}$$

(b) Show for $y \in M$ that $\partial_y^{[p]} f\colon M \to N$ given by $(\partial_y^{[p]} f)_R(x) = (D^p f)_R(x, y_R)$ ($R \in k$-**alg**, $x \in M_R$) is a polynomial law over k. Moreover, the map $\partial_y^{[p]}\colon \mathrm{Pol}_k(M, N) \to \mathrm{Pol}_k(M, N)$ satisfies $(\partial_y)^p = p!\partial_y^{[p]}$.

(c) Show that $\partial_{y+z}^{[2]} = \partial_y^{[2]} + \partial_y\partial_z + \partial_z^{[2]}$ for $y, z \in M$.

12.35. *Polynomial laws over infinite fields.* Let K be an infinite field, V, W (possibly infinite-dimensional) K-vector spaces and $f\colon V \to W$ a polynomial law over K.

(a) Show that if $f_K = 0$ as a set map from V to W, then $f = 0$ as a polynomial law over K.

(b) Conclude from (a) for a scalar polynomial law $\varphi\colon V \to K$ over K that if the product polynomial law $\varphi f\colon V \to W$ defined by $(\varphi f)_R(x) := \varphi_R(x) f_R(x)$ for $R \in K$-**alg** and $x \in V_R$ is zero (as a polynomial law over K), then $\varphi = 0$ or $f = 0$ (as polynomial laws over K).

12.36. Let M, N be k-modules and suppose $f\colon M \to N$ is a polynomial law over k.

(a) Show that $f = 0$ (as a polynomial law over k) if and only if $f \otimes k_{\mathfrak{p}} = 0$ (as a polynomial law over $k_{\mathfrak{p}}$) for all $\mathfrak{p} \in \operatorname{Spec}(k)$.

(b) If f is homogeneous of degree $d \in \mathbb{N}$, show that $f = 0$ (as a polynomial law over k) if and only if $f_k = 0$ (as a set map $M \to N$) and $D^p f = 0$ (as a polynomial law $M \times M \to N$) for $0 \le p \le \lfloor \frac{d}{2} \rfloor$.

12.37 ([95, Lemma 3.1])**.** Let M be a finitely generated projective k-module, and suppose $f\colon M \to N$ is a polynomial law such that $f_k(0) = 0$. Prove: If $m \in M$ has $f_k(m)$ unimodular in N, then m is unimodular in M.

12.38. Let f be a form of degree d on a k-module M in the sense of 12.7. We say that f *represents zero* if $f_k(m) = 0$ for some nonzero $m \in M$. If moreover m can be chosen to be unimodular, then we say that f is *isotropic*. (In case $d = 2$, f is a quadratic form, and this definition of isotropic agrees with the one in 11.17.)

(a) Let $R = k[\mathbf{t}]$ or the power series ring $k[[\mathbf{t}]]$. Prove: If f does not represent zero, then f_R does not represent zero on M_R and, for every $m \in M_R$, the lowest degree term of $f_R(m)$ has degree divisible by d.

(The converse, "f represents zero $\Rightarrow$ f_R represents zero", is trivial.)

(b) Suppose $R \supseteq k$ is a localization (i.e., $R = k[S^{-1}]$ where S is a multiplicatively closed subset of k containing no zero divisors) and M is a torsion-free module (meaning that if $xm = 0$ for $x \in k$ and $m \in M$, then x is a zero divisor or $m = 0$). Verify: f represents zero on M if and only if f_R represents zero on M_R.

(c) Prove: If k is a principal ideal domain, M is a free module of finite rank, and f represents zero, then f is isotropic.

12.39. Suppose R is a discrete valuation ring (DVR) with residue field k and uniformizing parameter π. (See for example [27, §VI.3.6] for background on discrete valuations on fields.) Let f_i be a form of degree d on a free finitely generated R-module M_i for $0 \le i < d$. Verify: If the form $\bar{f}_i$ on $M_i \otimes_R k$ induced from f_i does not represent zero for all i, then the form $\sum_{i=0}^{d-1} \pi^i f_i$ on $M_0 \oplus M_1 \oplus \cdots \oplus M_{d-1}$ does not represent zero.

Remark. The case $d = 2$ is standard in the theory of quadratic forms, see for example [72, Lemma 19.5].

12.40. *Exotic cubic forms.* Even when working over a field, homogeneous polynomial laws of degree ≥ 3 are no longer determined by the set maps they induce over the base ring. Examples for this phenomenon will be discussed in the present exercise.

(a) Let $f\colon M \to N$ be a homogeneous polynomial law of degree 3 over k. Simplify notation by writing $f(x) = f_R(x)$ for $R \in k$-**alg**, $x \in M_R$ (ditto for other polynomial laws), and put

$$f(x,y) := (Df)(x,y), \quad f(x,y,z) := (\Pi^{(1,1,1)} f)(x,y,z) \tag{1}$$

for $x, y, z \in M_R$. Then prove

$$f(x + \mathbf{t}y) = f(x) + \mathbf{t}f(x,y) + \mathbf{t}^2 f(y,x) + \mathbf{t}^3 f(y), \tag{2}$$

$$f(x + y, z) = f(x,z) + f(x,y,z) + f(y,z), \tag{3}$$

$$f(x,y,z) = f(x+y+z) - f(x+y) - f(y+z) - f(z+x) \tag{4}$$

$$\begin{aligned} &+ f(x) + f(y) + f(z), \\ f(\sum_{i=1}^{n} r_i x_i) = &\sum_{i=1}^{n} r_i^3 f(x_i) + \sum_{1\le i,j\le n, i\ne j} r_i^2 r_j f(x_i, x_j) \\ &+ \sum_{1\le i<j<l\le n} r_i r_j r_l f(x_i, x_j, x_l) \end{aligned} \tag{5}$$

for all $R \in k$-**alg**, $n \in \mathbb{Z}$, $n > 0$, a variable $\mathbf{t}$ and elements $x, y, z, x_1, \dots, x_n \in M_R$, $r_1, \dots, r_n \in R$.

(b) Let F be a field, $n \in \mathbb{Z}$, $n > 0$, F^n n-dimensional column space over F with the canonical basis $(e_i)_{1\le i\le n}$ and $g\colon F^n \to F$ a cubic form. View F^n as a unital commutative associative F-algebra under the component-wise multiplication and prove that the following conditions are equivalent.

(i) The set map $g_F\colon F^n \to F$ is zero but g itself is not.

(ii) $F \cong \mathbb{F}_2$ consists of two elements,

$$g_F(e_i) = g_F(x, x) = g_F(x, y, z) = 0 \qquad (1 \le i \le n,\ x, y, z \in F^n), \tag{6}$$

and there are $x_0, y_0 \in F^n$ such that $g_F(x_0, y_0) \ne 0$.

(iii) $F \cong \mathbb{F}_2$ consists of two elements and there exists a non-zero alternating matrix $S \in \mathrm{Mat}_n(F)$ such that

$$g_R(x) = x^{\mathsf{T}} S_R x^2$$

for all $R \in F$-**alg** and all $x \in (F^n)_R = R^n$.

12.41 (Springer [267, p. 63])**.** Let F be a field and suppose f is a cubic form on an F-vector space V. Prove: if f does not represent zero, neither does $f \otimes K$, for any quadratic field extension K of F.

12.42. *The third order chain rule.* Let $f\colon M \to N$, $g\colon N \to P$ be polynomial laws over k. Given $R \in k$-**alg** and $u, v, w \in N_R$, simplify notation as in 12.17 and write

$$(D^2 g)(u, v, w) := (D^2 g)(u, v + w) - (D^2 g)(u, v) - (D^2 g)(u, w) \tag{1}$$

for the bilinearization of the quadratic map $(D^2 g)(u, -)\colon N_R \to P_R$. Then prove

$$\begin{aligned} (D^3(g \circ f))(x, y) = &(Dg)(f(x), (D^3 f)(x, y)) + (D^2 g)(f(x), (Df)(x, y), (D^2 f)(x, y)) \\ &+ (D^3 g)(f(x), (Df)(x, y)) \end{aligned}$$

for all $x, y \in M_R$.

12.43. *Cubic maps.* In this exercise, we compare Faulkner's approach [76] to homogeneous polynomial maps, for simplicity restricted here to the special case of degree 3, with the formalism of polynomial laws.

(a) Show that the totality of polynomial laws over k can be canonically converted into a category, denoted by k-**polaw**, and regard the homogeneous polynomial laws of degree 3 as a full subcategory, denoted by $k3$-**holaw**, of k-**polaw**.

Let M and N be k-modules. Following Faulkner [76], define a *cubic map* from M to N over k as a pair (f, g) of set maps $f\colon M \to N$ and $g\colon M \times M \to N$ satisfying the following conditions.

(i) f is homogeneous of degree 3: $f(\alpha x) = \alpha^3 f(x)$ for all $\alpha \in k$ and all $x \in M$.
(ii) g is quadratic-linear over k in the sense of Exercise 11.34.
(iii) (f, g) satisfies the expansion

$$f(x + y) = f(x) + g(x, y) + g(y, x) + f(y)$$

for all $x, y \in M$.
(iv) Euler's differential equation holds:

$$g(x, x) = 3f(x)$$

for all $x \in M$.

Cubic maps from M to N as above, symbolized by $(f, g)\colon M \to N$, form a k-module in the obvious way. Now prove:

(b) If $(f, g)\colon M \to N$ is a cubic map, then the assignment

$$(x, y, z) \longmapsto g(x, y, z) := g(x + y, z) - g(x, z) - g(y, z) \tag{1}$$

defines a trilinear map $M \times M \times M \to N$ which is totally symmetric. Moreover,

$$\mathrm{Rad}(f, g) := \{x \in M \mid \forall y \in M :\ f(x) = g(x, y) = g(y, x) = 0\}, \tag{2}$$

called the *radical* of (f, g), is a submodule of M such that

$$g(\mathrm{Rad}(f, g), M, M) = \{0\}, \tag{3}$$

and for any linear surjection $\pi\colon M \to M_1$ of k-modules having $\mathrm{Ker}(\pi) \subseteq \mathrm{Rad}(f, g)$, there is a unique cubic map $(f_1, g_1)\colon M_1 \to N$ such that $f_1 \circ \pi = f$ and $g_1 \circ (\pi \times \pi) = g$.

(c) Generalize (iii) to the expansion

$$\begin{aligned} f\Big(\sum_{i=1}^{n} \alpha_i x_i\Big) = &\sum_{i=1}^{n} \alpha_i^3 f(x_i) + \sum_{1 \le i, j \le n, i \ne j} \alpha_i^2 \alpha_j g(x_i, x_j) \\ &+ \sum_{1 \le i < j < l \le n} \alpha_i \alpha_j \alpha_l g(x_i, x_j, x_l) \end{aligned} \tag{4}$$

for all $n \in \mathbb{Z}$, $n \ge 1$, $\alpha_i \in k$, $x_i \in M$, $1 \le i \le n$. Conclude for all $R \in k$-**alg** that there is a unique cubic map $(f, g)_R = (f_R, g_R)\colon M_R \to N_R$ over R making the diagrams

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}} \\ M_R & \xrightarrow[f_R]{} & N_R, \end{array} \qquad \begin{array}{ccc} M \times M & \xrightarrow{g} & N \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}} \\ M_R \times N_R & \xrightarrow[g_R]{} & N_R \end{array} \tag{5}$$

commutative. We call $(f, g)_R$ the *R-cubic extension* of (f, g).

(d) The totality of cubic maps between k-modules can be canonically converted into a category, denoted by k-**cumap**. Furthermore, the assignment $f \mapsto (f_k, (Df)_k)$ on objects and the identity on morphisms yields a well-defined isomorphism of categories from $k3$-**holaw** onto k-**cumap**, the inverse of that isomorphism on objects being denoted by $(f, g) \mapsto f * g$.

12.44. Let $F\colon M \to N$ be a homogeneous polynomial law of degree 3 over k and suppose the k-module M is projective. Show that there exists a trilinear map $T\colon M \times M \times M \to N$, in general not symmetric, such that $F(x) = T(x,x,x)$ for all $x \in M_R$, $R \in k$-**alg**.

12.45. Let $K \in k$-**alg** and M, N be K-modules. Show that the k-linear map

$$\mathrm{Pol}_K(M,N) \longrightarrow \mathrm{Pol}_k({}_kM, {}_kN), \quad f \longmapsto {}_kf,$$

induced by the restriction of scalars is injective.

12.46. Let M, N, P be K-modules and $f\colon M \to N$, $g\colon N \to P$ be polynomial laws over K. Then

(a) ${}_k(g \circ f) = ({}_kg) \circ ({}_kf)$.
(b) If f is homogeneous of degree $d \in \mathbb{N}$, so is ${}_kf$.
(c) ${}_k(\Pi^\nu f) = \Pi^\nu({}_kf)$ for all $n \in \mathbb{N}$ and all $\nu \in \mathbb{N}^n$.
(d) If $(f_i)_{i\in I}$ is a locally finite family of polynomial laws $f_i\colon M \to N$, $i \in I$, over K, then $({}_kf_i)_{i\in I}$ is a locally finite family of polynomial laws ${}_kf_i\colon {}_kM \to {}_kN$ over k and
$${}_k\Big(\sum_{i\in I} f_i\Big) = \sum_{i\in I} ({}_kf_i).$$
(e) $D^n({}_kf) = {}_k(D^n f)$ for all $n \in \mathbb{N}$.
(f) $\partial_y({}_kf) = {}_k(\partial_y f)$ as polynomial laws ${}_kM \to {}_kN$ over k, for all $y \in M$.

12.47. Let $K \in k$-**alg**, M be a k-module and N a K-module. Given a polynomial law $f\colon M \to {}_kN$ over k, show that there is a unique polynomial law $g\colon M_K \to N$ over K making a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\ f\ } & {}_kN \\ {\scriptstyle {}_k(\mathrm{can}_{M,K})}\downarrow & \nearrow {\scriptstyle {}_kg} & \\ {}_k(M_K) & & \end{array} \tag{1}$$

of polynomial laws over k.

Remark. We denote by k-**pol** the category of k-modules with polynomial laws over k as morphisms. Given $K \in k$-**alg**, we obtain the (covariant) *base change functor* from k-**pol** to K-**pol** which converts a polynomial law $f\colon M \to N$ of k-modules to its scalar extension $f \otimes K\colon M_K \to N_K$. On the other hand, we have the (covariant) *scalar restriction functor* from K-**pol** to k-**pol** which converts a polynomial law $g\colon P \to Q$ of K-modules to its scalar restriction ${}_kg\colon {}_kP \to {}_kQ$. The preceding exercise shows that the latter functor is left adjoint to the former.

12.48. *Cubic maps and semi-linear polynomial squares.* (a) Let $K \in k$-**alg**, M, N be K-modules and $(f,g)\colon M \to N$ a cubic map over K in the sense of Exercise 12.43. Viewing f as a set map ${}_kf\colon {}_kM \to {}_kN$, $x \mapsto f(x)$, and g as a set map ${}_kg\colon {}_kM \times {}_kM \to {}_kN$, $(x,y) \mapsto g(x,y)$, prove that the *restriction of scalars*, ${}_k(f,g) := ({}_kf, {}_kg)\colon {}_kM \to {}_kN$, is a cubic map over k satisfying

$${}_k(f * g) = ({}_kf) * ({}_kg). \tag{1}$$

(b) Let $\sigma\colon K \to K'$ be a morphism in k-**alg** and M, N (resp. M', N') be K- (resp. K'-) modules. Given cubic maps $(f, g)\colon M \to N$ over K (resp. $(f', g')\colon M' \to N'$ over K') and σ-semi-linear maps $\varphi\colon M \to M'$ (resp. $\psi\colon N \to N'$), show that the σ-semi-linear polynomial square

$$\begin{array}{ccc} M & \xrightarrow[\varphi]{} & M' \\ {\scriptstyle f*g}\downarrow & & \downarrow{\scriptstyle f'*g'} \\ N & \xrightarrow[\psi]{} & N' \end{array} \tag{2}$$

commutes in the sense of 12.28 if and only if so do the diagrams

$$\begin{array}{ccc} M & \xrightarrow[\varphi]{} & M' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ N & \xrightarrow[\psi]{} & N', \end{array} \qquad \begin{array}{ccc} M \times M & \xrightarrow[\varphi\times\varphi]{} & M' \times M' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ N & \xrightarrow[\psi]{} & N' \end{array} \tag{3}$$

of set maps.

12.49. *Matching non-scalar polynomial laws with scalar ones* (Loos [171, 18.5]). Prove for k-modules M, N that there exists a unique k-linear map

$$\Psi\colon N \otimes \mathrm{Pol}(M, k) \longrightarrow \mathrm{Pol}(M, N)$$

satisfying

$$(\Psi(v \otimes f))_R(x) = v \otimes f_R(x) \tag{1}$$

for all $v \in N$, $f \in \mathrm{Pol}(M, k)$, $R \in k$-**alg**, $x \in M_R$. Moreover, Ψ is an isomorphism if N is finitely generated projective.

III

Alternative algebras

Alternative algebras are one of the most important building blocks of Albert algebras. The main examples are associative algebras, which the reader is familiar with from the theory of non-commutative rings; the Graves-Cayley octonions over the reals (1.5); and the Dickson-Coxeter octonions over the integers (4.5).

In this chapter, we focus on those properties of alternative algebras that are important for applications to Albert algebras. We derive a number of important identities, then proceed to establish a fairly general version of Artin's associativity theorem and investigate homotopes of alternative algebras.

13 Basic identities and invertibility

Having gained some proficiency in the language of arbitrary non-associative algebras, we are now adequately prepared to deal with the more specific class of alternative algebras. After giving the formal definition, we derive the Moufang identities and introduce the notion of invertibility. Throughout, we let k be an arbitrary commutative ring.

13.1 The concept of an alternative algebra. A k-algebra A is said to be *alternative* if its associator (cf. 7.5), i.e., the trilinear map $(x, y, z) \mapsto [x, y, z] = (xy)z - x(yz)$ from $A \times A \times A$ to A, is alternating. This means that the following identities hold in A:

$$x(xy) = x^2y, \qquad \text{(left alternative law)} \tag{1}$$

$$(yx)x = yx^2, \qquad \text{(right alternative law)} \tag{2}$$

$$(xy)x = x(yx). \qquad \text{(flexible law)} \tag{3}$$

In fact, since the symmetric group on three letters is generated by any two of the transpositions $(1, 2)$, $(2, 3)$, $(3, 1)$, any two of the above equations imply the third, hence force A to be alternative. An alternative algebra and its opposite have the same associator, so A^{op} is alternative if and only if A is. It is sometimes convenient to express the alternative laws in *operator form*, i.e., in terms of left

and right multiplication operators as follows:

$$L_x^2 = L_{x^2}, \tag{4}$$
$$R_x^2 = R_{x^2}, \tag{5}$$
$$L_x R_x = R_x L_x. \tag{6}$$

13.2 Linearizations. For the rest of this section, we fix an alternative algebra A over k. Then, thanks to flexibility, the expression xyx is unambiguous in A. Also, since (13.1.1)–(13.1.3) are quadratic in x, they may be linearized to yield new identities valid in A. For example, replacing x by $x + z$ in (13.1.1), collecting mixed terms and interchanging y with z, we obtain

$$x(yz) + y(xz) = (xy + yx)z. \tag{1}$$

Similarly,

$$(xy)z + (xz)y = x(yz + zy), \tag{2}$$
$$(xy)z + (zy)x = x(yz) + z(yx). \tag{3}$$

Again these relations can be expressed in terms of left and right multiplication operators; details are left to the reader. Also, it is now straightforward to check that the property of an algebra to be alternative remains stable under base change: A_R is alternative, for any $R \in k$-**alg**.

13.3 The Moufang identities. Less obvious is the fact that the *Moufang identities*

$$(xyx)z = x(y(xz)), \qquad \text{(left Moufang identity)} \tag{1}$$
$$z(xyx) = ((zx)y)x, \qquad \text{(right Moufang identity)} \tag{2}$$
$$(xy)(zx) = x(yz)x \qquad \text{(middle Moufang identity)} \tag{3}$$

hold in any alternative algebra. Since the associator is alternating, (1) follows from (13.1.1), (13.2.2) and

$$\begin{aligned}(xyx)z - x(y(xz)) &= [xy, x, z] + [x, y, xz] = -[x, xy, z] - [x, xz, y] \\ &= -(x^2y)z - (x^2z)y + x((xy)z + (xz)y) \\ &= -x^2(yz + zy) + x(x(yz + zy)) = 0.\end{aligned}$$

Reading the left Moufang identity in the opposite algebra A^{op} gives the right Moufang identity. Finally, again using the fact that the associator is alternating, but also (1), we obtain

$$\begin{aligned}(xy)(zx) - x(yz)x &= [x, y, zx] - x[y, z, x] = -[x, zx, y] - x[z, x, y] \\ &= -(xzx)y + x((zx)y) - x((zx)y) + x(z(xy)) = 0,\end{aligned}$$

and the middle Moufang identity is proved. For an ad-hoc approach to the Moufang identities for the Graves-Cayley octonions, see Exc. 1.19.

Viewing (1), (2) as linear maps in z and (3) as a bilinear one in y, z, the Moufang identities may also be expressed as

$$L_{xyx} = L_x L_y L_x, \tag{4}$$
$$R_{xyx} = R_x R_y R_x, \tag{5}$$
$$(L_x y)(R_x z) = L_x R_x (yz). \tag{6}$$

The linearization process is useful also in the present context. For example, linearizing the right Moufang identity (2) we deduce

$$z((wy)x) + z((xy)w) = ((zw)y)x + ((zx)y)w = z(w(yx)) + z(x(yw)). \tag{7}$$

13.4 Inverses. There is no useful concept of invertibility in arbitrary non-associative algebras. Fortunately, however, the standard notion for associative algebras carries over to the alternative case without change. If A is unital (with identity element 1_A), an element $x \in A$ is said to be *invertible* if there exists an element $y \in A$, called an *inverse* of x in A, that satisfies the relations $xy = 1_A = yx$. With an eye on Exc. 14.10 below, we sometimes speak of y as a *two-sided* inverse of x.

The concept of invertibility enjoys the usual properties. Before proving this, we need some preparation.

13.5 The U-operator. The *U-operator* of A (no longer assumed to be unital) is defined as the quadratic map

$$U : A \longrightarrow \mathrm{End}_k(A), \quad x \longmapsto U_x := L_x R_x = R_x L_x, \tag{1}$$

which acts on individual elements as

$$U_x y = xyx. \tag{2}$$

Note that the U-operator does not change when passing to the opposite algebra. Moreover, it may be used to rewrite the middle Moufang identity in the form

$$U_x(yz) = (L_x y)(R_x z). \tag{3}$$

Finally, the U-operator satisfies the following important relations:

$$U_{xy} = L_x U_y R_x = R_y U_x L_y \tag{4}$$

for all $x, y \in A$. Indeed, using (13.3.7), (13.3.3), (13.3.2), (13.1.1), we obtain

$$\begin{aligned} U_{xy}z &= ((xy)z)(xy) = x((yz)(xy) + [(xy)z]y) - ([x(xy)]z)y \\ &= x(y(zx)y + x(yzy)) - x^2(yzy) = x(y(zx)y) \\ &= L_x U_y R_x z \end{aligned}$$

for all $z \in A$, giving the first part of (4). The second one follows by passing to A^{op}.

13.6 Proposition. *Let A be unital and $x \in A$. Then the following conditions are equivalent.*

(i) x *is invertible.*
(ii) L_x *is bijective.*
(iii) R_x *is bijective.*
(iv) U_x *is bijective.*
(v) L_x *and* R_x *are surjective.*
(vi) U_x *is surjective.*
(vii) $1_A \in \mathrm{Im}(L_x) \cap \mathrm{Im}(R_x)$.
(viii) $1_A \in \mathrm{Im}(U_x)$.

If these conditions hold, then x has a unique inverse in A, denoted by x^{-1}, and

$$x^{-1} = L_x^{-1}1_A = R_x^{-1}1_A = U_x^{-1}x, \tag{1}$$

$$L_{x^{-1}} = L_x^{-1}, \quad R_{x^{-1}} = R_x^{-1}, \quad U_{x^{-1}} = U_x^{-1}. \tag{2}$$

Proof (i) $\Leftrightarrow$ (ii). If x is invertible with inverse y, we obtain $xy^2x = 1_A$ by (13.3.3), hence $L_xL_{y^2}L_x = \mathbf{1}_A$ by (13.3.4), and (ii) follows. Conversely, suppose L_x is bijective. Then there is a unique $y \in A$ satisfying $xy = 1_A$, and the relation $x(yx) = (xy)x = 1_Ax = x1_A$ combined with (ii) shows $yx = 1_A$, hence (i).

(i) $\Leftrightarrow$ (iii). This is just (i) $\Leftrightarrow$ (ii) in C^{op}.

(iii) $\Rightarrow$ (iv). Obvious since (iii) implies (ii).

(iv) $\Rightarrow$ (v). Obvious since L_x and R_x commute by flexibility (13.1.2).

(v) $\Rightarrow$ (vi) $\Rightarrow$ (vii). Obvious, again by flexibility.

(vii) $\Rightarrow$ (viii). We find elements $y, z \in A$ satisfying $xy = zx = 1_A$, and (13.3.3) gives $x(yz)x = 1_A$.

(viii) $\Rightarrow$ (ii). We find an element $w \in A$ satisfying $xwx = 1_A$, and (13.3.1) implies $L_xL_wL_x = \mathbf{1}_A$, forcing L_x to be bijective.

Uniqueness of the inverse and (1) now follow from (ii), (iii), (iv). Furthermore, $xx^{-1}x = x$ and the (13.3.4) implies $L_xL_{x^{-1}}L_x = L_x$, so (ii) gives $L_{x^{-1}} = L_x^{-1}$. Reading this in A^{op} yields $R_{x^{-1}} = R_x^{-1}$, hence $U_{x^{-1}} = U_x^{-1}$, and the proof of (2) is complete. □

13.7 The set of invertible elements. If A is unital, then the set of its invertible elements will be denoted by $A^\times$. Clearly, $1_A \in A^\times$, and $x \in A^\times$ implies $x^{-1} \in A^\times$ with $(x^{-1})^{-1} = x$. Moreover, $A^\times$ is closed under multiplication. More precisely, if $x, y \in A$ are invertible, so is xy and

$$(xy)^{-1} = y^{-1}x^{-1}. \tag{1}$$

Indeed, setting $z = y^{-1}x^{-1}$, the Moufang identities and (13.6.2) imply $((xy)z)y = x(y(y^{-1}x^{-1})y) = x(x^{-1}y) = y$, hence $(xy)z = 1_A$ by Prop. 13.6 (iii). Replacing x by y^{-1} and y by x^{-1} yields $z(xy) = 1_A$, and (1) follows.

The preceding considerations imply: If the equation $xy = z$ holds for $x, y, z \in A$, and if any two of x, y, z are invertible, so is the third, which is then uniquely determined. Thus, since A satisfies the Moufang identities, $A^\times$ is a "Moufang loop" under the operation induced from A by restriction; for the definition and more details on Moufang loops, see Bruck [40, Chap. VII, VIII] or Manin [178].

13.8 Remark. Proposition 13.6 shows that a unital alternative algebra is a division algebra in the sense of 8.6 if and only if $1_A \neq 0$ and every non-zero element is invertible.

13.9 Vista: simple alternative algebras over a field. In the next chapter, we will define notions of quaternion and octonion algebras generalizing the real algebras $\mathbb{H}$ and $\mathbb{O}$ from Chap. I, see 19.20 and 19.22. While quaternion algebras are associative, octonion algebras are merely alternative (Prop. 19.3).

Over a field F, quaternion and octonion algebras are simple (Exc. 19.28). Conversely, *Kleinfeld's theorem* says: If A is a simple alternative F-algebra, then A is associative or it is an octonion algebra. See [298, §7.3] or [254, Thm. 3.17]. Here is a more precise statement.

13.10 Theorem (Kleinfeld)**.** *An alternative algebra over a field F is simple if and only if it is either associative simple or it is an octonion algebra over some extension field of F in the sense of 19.22.* □

14 Strongly associative subsets

Our aim in this section will be to prove Artin's associativity theorem, which says that every alternative algebra on two generators is associative. Actually, we will derive a somewhat more general result by adopting the approach of Bourbaki [28, III, Appendix, §1], alternatively see Braun-Koecher [36, VII, §1]. Throughout we let k be a commutative ring and A an alternative k-algebra.

14.1 The concept of a strongly associative subset. A subset $X \subseteq A$ is said to be *strongly associative* if $[x, y, z] = 0$ provided at least two of the elements $x, y, z \in A$ belong to X. Since the associator is alternating, this is equivalent to the condition $[X, X, A] = \{0\}$. Hence, if $X \subseteq A$ is strongly associative, so is the submodule spanned by X, and $X \cup \{1_A\}$ provided A is unital. Examples of strongly associative subsets are $X = \{x\}$, for any $x \in A$ (by (13.1.1)), and $X = \{x, x^{-1}\}$, for A unital and any $x \in A^\times$ (by (13.1.1), (13.6.2)).

14.2 Lemma. *Let $X \subseteq A$ be a set of generators for A as a k-algebra. Suppose $M \subseteq A$ is a k-submodule that contains X and satisfies $XM + MX \subseteq M$. Then $M = A$.*

Proof We begin by showing that A', the set of elements $x \in A$ satisfying $xM + Mx \subseteq M$, is closed under multiplication, so let $x, y \in A'$. Then, for all $z \in M$, $(xy)z = [x, y, z] + x(yz) = x(yz) - [x, z, y] = x(yz) - (xz)y + x(zy) \in M$ and, similarly, $z(xy) \in M$, forcing $xy \in A'$, as claimed. It follows that A', being a subalgebra of A containing X, agrees with A, which implies $AM \subseteq M$. But then M must be a subalgebra of A containing X, and we conclude $M = A$. □

14.3 Proposition. *If X is a strongly associative subset of A, then so is the subalgebra of A generated by X.*

Proof By 7.4, it suffices to show that $\mathrm{Mon}(X) = \bigcup_{m>0} \mathrm{Mon}_m(X)$, the set of monomials over X, is a strongly associative subset of A. To this end, we only need to prove

$$[\mathrm{Mon}_m(X), \mathrm{Mon}_n(X), A] = \{0\} \qquad (m, n \in \mathbb{Z}, m, n > 0), \tag{1}$$

and we do so by induction on $p = m + n \geq 2$. The case $p = 2$ being obvious by hypothesis, let us assume $p > 2$. Since (1) is symmetric in m, n by alternativity, we may even assume $m > 1$. Hence, given $u \in \mathrm{Mon}_m(X)$, $v \in \mathrm{Mon}_n(X)$, $a \in A$, we obtain $u = u_1 u_2$, $u_i \in \mathrm{Mon}_{m_i}(X)$, $m_i \in \mathbb{Z}$, $m_i > 0$, $i = 1, 2$, $m_1 + m_2 = m$, and (7.5.2) yields

$$-[u, v, a] = [u_1 u_2, a, v] = -u_1[u_2, v, a] + [u_1, u_2, a]v - [u_1, v, u_2 a] - [u_1, u_2, av],$$

where all terms on the right vanish by the induction hypothesis. Hence $[u, v, a] = 0$, which completes the induction. □

14.4 Proposition. *Let X, Y be strongly associative subsets of A. Then the subalgebra of A generated by X and Y is associative.*

Proof We may not only assume that A itself is generated by X and Y but also, by Proposition 14.3, that $X, Y \subseteq A$ are subalgebras. Then the set B of elements $z \in A$ such that $[X, Y, z] = \{0\}$ is a submodule of A containing X and Y since

they are both strongly associative. The proof will be complete once we have shown $B = A$ since this implies $[X \cup Y, X \cup Y, A] = \{0\}$, forcing $X \cup Y$ to be a strongly associative subset of A; this property is inherited by the subalgebra generated by X and Y, which shows that A is associative, as desired. In order to prove $B = A$, we apply Lemma 14.2 and hence must show

$$XB + BX + YB + BY \subseteq B. \tag{1}$$

Accordingly, let $x, x' \in X, y \in Y, z \in B$. Then (7.5.2) yields

$$[x'x, z, y] - [x', xz, y] + [x', x, zy] = x'[x, z, y] + [x', x, z]y = 0$$

since $z \in B$ and X is strongly associative, which implies $[x', x, zy] = 0$ as well. But X is also a subalgebra of B, whence $[x'x, z, y] = 0$. Altogether, we conclude $[X, Xz, Y] = \{0\}$, forcing $Xz \subseteq B$. Interchanging the roles of X and Y and passing to the opposite algebra, we obtain (1), and the proof is complete. □

14.5 Corollary (Artin's theorem)**.** *Let $x, y \in A$. Then the subalgebra of A generated by x and y is associative. If A is unital, the same conclusion holds for the unital subalgebra of A generated by x, y and (if they exist) their inverses.*

Proof In the non-unital case, put $X = \{x\}, Y = \{y\}$. In the unital case, put $X = \{x, 1_A\}$ if x is not invertible, $X = \{x, 1_A, x^{-1}\}$ otherwise, ditto for Y. □

14.6 Corollary. *Alternative algebras are power-associative. Moreover, if A is unital, then $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ for all $x \in A^\times$, $m, n \in \mathbb{Z}$.* □

Exercises

14.7. Show that an alternative algebra A over k satisfies the relation $3[A, A, A] \subseteq [A, A] + A[A, A] + [A, A]A$. Conclude that commutative alternative algebras without 3-torsion are associative.

14.8. *The Kleinfeld function* (Kleinfeld [153]). Let A be a non-associative k-algebra. The *Kleinfeld function* $f\colon A^4 \to A$ is defined by

$$f(w, x, y, z) := [wx, y, z] - x[w, y, z] - [x, y, z]w$$

for $w, x, y, z \in A$. It is evidently linear in each of x, y, z, w. Prove: If A is an alternative algebra, then f is alternating (as a multilinear map).

14.9. *A characterization of unital alternative algebras* (McCrimmon [185]). Let A be an alternative k-algebra. Show that the following conditions are equivalent.

(i) A is unital.
(ii) For some $x \in A$, both L_x and R_x are bijective.
(iii) For some $x \in A$, both L_x and R_x are surjective.
(iv) For some $x \in A$, U_x is surjective.
(v) For some $x, y \in A$, both L_x and R_y are bijective.

14.10. *One-sided inverses* (McCrimmon [185]). Let A be a unital alternative k-algebra.

(a) Show for $x, y \in A$ that the following conditions are equivalent.

(i) $xy = 1_A$.
(ii) $L_x L_y = \mathbf{1}_A$.
(iii) $R_y R_x = \mathbf{1}_A$.

(*Hint*: For the implication (i) $\Rightarrow$ (ii) prove that $E = L_x L_y$, $F = R_y R_x$ are projections of the k-module A satisfying $EF = \mathbf{1}_A$.)

If these conditions are fulfilled, x (resp. y) is said to be *right-invertible* (resp. *left-invertible*) with *right* (resp. *left*) *inverse* y (resp. x) (in general not unique).

(b) Conclude from (a) that if A is finitely generated as a k-module, then any right (resp. left) invertible element of A is invertible, and any right (resp. left) inverse of x is its two-sided inverse.

(c) Give an example of an associative k-algebra A and elements $x, y \in A$ such that $xy = 1_A$ but neither x nor y are invertible.

14.11 (McCrimmon [185])**.** Let A be a unital alternative algebra over k and $x, y \in A$ such that xy is invertible. Show in the language of Exc. 14.10 that x is right-invertible with $y(xy)^{-1}$ as a right inverse and y is left-invertible with $(xy)^{-1}x$ as a left inverse. (*Hint*: For the first assertion, use (13.5.4) to show that L_y is injective.)

14.12. *The singular Peirce decomposition of alternative algebras* (cf. Schafer [254]).[1] Let A be a unital alternative algebra over k and $c \in A$ an arbitrary idempotent. Put $c_1 = c, c_2 = 1_A - c$ to prove that the maps $L_{c_i} R_{c_j} : A \to A$ $(i, j = 1, 2)$ form a complete orthogonal system of projections satisfying $(c_i x)c_j = c_i(xc_j) =: c_i x c_j$ for all $x \in A$. (*Hint*: Expand $U_{c_1+c_2}$.) Conclude

$$A = A_{11} \oplus A_{12} \oplus A_{21} \oplus A_{22} \tag{1}$$

as a direct sum of submodules

$$\begin{aligned} A_{ij} := A_{ij}(c) &:= \{x \in A \mid c_i x c_j = x\} = \{x \in A \mid c_i x = x = x c_j\} \qquad (2) \\ &= \{x \in A \mid cx = (2-i)x,\ xc = (2-j)x\} \subseteq A \qquad (i, j = 1, 2) \end{aligned}$$

that satisfy the multiplication rules

$$A_{ij} A_{jl} \subseteq A_{il}, \tag{3}$$

$$A_{ii} A_{jl} = A_{lj} A_{ii} = \{0\}, \qquad (i \neq j) \tag{4}$$

$$A_{ij}^2 \subseteq A_{ji} \qquad (i \neq j) \tag{5}$$

for all $i, j, l = 1, 2$. Prove $x^2 = 0$ for all $x \in A_{ij}$, $i \neq j$, and that (5) can be sharpened to $A_{ij}^2 = \{0\}$ (for $i \neq j$) if A is associative.

15 Homotopes

Homotopes have been established a long time ago as an extremely versatile tool in the theory of Jordan algebras and can look back to a long respectable

[1] The Peirce decomposition is credited to Benjamin Peirce (1809–1880) due to Prop. 41 on page 13 of [208]. Peirce is pronounced like the English word "purse".

history. Though they entered the scene of alternative algebras only much later, receiving the amount of attention they were accustomed to from the Jordan setting only quite recently (see Alsaody-Gille [15] and, in particular, Thm. 23.10 below), it will be shown in the present book that, also in these new surroundings, they provide a useful and convenient formalism for many problems related to Albert algebras.

In the present section, the conceptual foundations for homotopes and isotopes of alternative algebras will be laid down following McCrimmon [185]. Throughout, we let k be an arbitrary commutative ring and A an alternative algebra over k. We begin with an easy special case of the general concept.

15.1 Digression: associative algebras. For the time being, let B be an associative k-algebra and $p \in B$. Define a new k-algebra $B^{(p)}$ on the k-module B by the multiplication

$$x \cdot_{(p)} y := xpy \qquad (x, y \in B).$$

We call $B^{(p)}$ the *p-homotope* of B, which is obviously associative; moreover, the multiplication operators $L_p, R_p \colon B^{(p)} \to B$ are algebra homomorphisms. In particular, if B is unital and p is invertible, $B^{(p)} \cong B$ under L_p or R_p. This explains why homotopes do not play a significant role in (associative) ring theory.

15.2 The concept of a homotope. Returning to our original alternative algebra A, let $p, q \in A$. On the k-module A we define a new k-algebra $A^{(p,q)}$ by the multiplication

$$x \cdot_{p,q} y := (xp)(qy) \qquad (x, y \in A). \tag{1}$$

We call $A^{(p,q)}$ the *p,q-homotope* (or just a *homotope*) of A. We obviously have

$$(A^{(p,q)})^{\mathrm{op}} = (A^{\mathrm{op}})^{(q,p)}, \quad A^{(\alpha p, \alpha^{-1} q)} = A^{(p,q)} \qquad (\alpha \in k^\times). \tag{2}$$

A k-algebra is said to be *homotopic* to A if it is isomorphic to some of its homotopes. If A is associative, (1) collapses to $x \cdot_{p,q} y = xpqy$, so $A^{(p,q)} = A^{(pq)}$ as in 15.1.

Our next aim will be to show that homotopes of alternative algebras are alternative, and that homotopes of homotopes are homotopes. More precisely, we obtain the following proposition.

15.3 Proposition. *Let $p, q, p', q' \in A$. Then $A^{(p,q)}$ is an alternative k-algebra and*

$$(A^{(p,q)})^{(p',q')} = A^{(p'',q'')}, \quad p'' := p(qp')p, \quad q'' := q(q'p)q. \tag{1}$$

Proof For the first part, it suffices to verify the left alternative law (13.1.1) since by passing to the opposite algebra and invoking (15.2.2), we will obtain the right alternative law as well. So let $x, y \in A$. Then (13.5.4) and the Moufang identities (13.3.1), (13.3.2) imply

$$\begin{aligned} x \cdot_{p,q} (x \cdot_{p,q} y) &= (xp)(q[(xp)(qy)]) = (U_{xp}q)(qy) = (L_x U_p R_x q)(qy) \\ &= (x[p(qx)p])(qy) = ([(xp)(qx)]p)(qy) = (x \cdot_{p,q} x) \cdot_{p,q} y, \end{aligned}$$

hence (13.1.1) for $A^{(p,q)}$. The verification of the second part is straightforward and left to the reader. □

15.4 Functoriality. We denote by k-**alt** the category of (possibly non-unital) alternative k-algebras, morphisms being ordinary k-algebra homomorphisms (7.1). By contrast, the category of *weakly two-pointed alternative k-algebras* will be denoted by k-**twalt**. Its objects are triples (A, p, q) consisting of an alternative k-algebra A and a pair of elements $p, q \in A$, while its morphisms have the form $h\colon (A, p, q) \to (A', p', q')$ with weakly two-pointed alternative k-algebras (A, p, q), (A', p', q') and an algebra homomorphism $h\colon A \to A'$ satisfying $h(p) = p'$, $h(q) = q'$. It is then clear that the assignment $(A, p, q) \mapsto A^{(p,q)}$ gives rise to a (covariant) functor from k-**twalt** to k-**alt** which is the identity on morphisms.

15.5 The connection with unital algebras. We are particularly interested in homotopes containing an identity element. In order to find necessary and sufficient conditions for this to happen, we consider the U-operator $U^{(p,q)}$ of $A^{(p,q)}$ ($p, q \in A$), so $U_x^{(p,q)} = L_x^{(p,q)} R_x^{(p,q)}$ by (13.5.1), where $L^{(p,q)}, R^{(p,q)}$ stand for the left, right multiplication of $A^{(p,q)}$. We claim

$$U_x^{(p,q)} = U_x U_{pq} \qquad (x \in A). \tag{1}$$

To prove this, we let $x, y \in A$ and compute, using flexibility in $A^{(p,q)}$, the Moufang identities and (13.5.2), (13.5.4)

$$U_x^{(p,q)} y = ([(xp)(qy)]p)(qx) = (x[p(qy)p])(qx) = x(R_q U_p L_q y)x = U_x U_{pq} y,$$

as desired.

15.6 Proposition. *For $p, q \in A$, the p,q-homotope $A^{(p,q)}$ has a unit element if and only if A has a unit element and pq is invertible in A. In this case, $1_A^{(p,q)} := (pq)^{-1}$ is the unit element of $A^{(p,q)}$.*

Proof If $e \in A$ is a unit element for $A^{(p,q)}$, then (15.5.1) implies $\mathbf{1}_A = U_e^{(p,q)} = U_e U_{pq}$, so U_e is surjective. But then A is unital (Exc. 14.9), and e must be invertible in A (Prop. 13.6). Hence so is pq with $U_{pq}^{-1} = U_e$ and $(pq)^{-1} =$

$U_{pq}^{-1}(pq) = U_e(pq) = (ep)(qe) = e \cdot_{p,q} e = e$ since e is a unit element for $A^{(p,q)}$. Conversely, let A be unital and suppose $pq \in A$ is invertible with inverse $e := (pq)^{-1}$. Then Exc. 14.11 implies $(ep)q = 1_A$, forcing $L_{ep}L_q = \mathbf{1}_A$ by Exc. 14.10, and we conclude $e \cdot_{p,q} x = (ep)(qx) = x$ for all $x \in A$, so e is a left unit element for $A^{(p,q)}$. Passing to the opposite algebra of A will show that e is also a right unit for $A^{(p,q)}$, forcing $A^{(p,q)}$ to be unital with identity element e. □

15.7 Isotopes. If A is unital and $p, q \in A$ are *both* invertible (which is stronger than just requiring pq to be invertible, cf. Exc. 14.10 (c)), then $A^{(p,q)}$ is called the *p,q-isotope* (or simply an *isotope*) of A. By Props. 15.3, 15.6, $A^{(p,q)}$ is a unital alternative algebra in this case, with unit element

$$1_A^{(p,q)} = (pq)^{-1} = q^{-1}p^{-1}, \tag{1}$$

and (15.3.1) gives

$$(A^{(p,q)})^{(p',q')} = A \qquad (p' := q^{-1}p^{-2}, q' := q^{-2}p^{-1}). \tag{2}$$

We say that a k-algebra is *isotopic* to A if it is isomorphic to an isotope of A. Isotopy is an equivalence relation on unital alternative algebras.

By (1), the algebra $A^{(p,q)}$, for A unital and $p, q \in A^\times$, determines the product pq uniquely. But it is important to note that the factors of this product are *not* uniquely determined by $A^{(p,q)}$. Indeed, bringing in the nucleus of A (cf. 8.5), we have the following.

15.8 Proposition. *Let A be unital and $p, q, p', q' \in A^\times$. Then $A^{(p,q)} = A^{(p',q')}$ if and only if $p' = pu, q' = u^{-1}q$ for some $u \in \mathrm{Nuc}(A)^\times$.*

Proof $p' = pu, q' = u^{-1}q$ for some $u \in \mathrm{Nuc}(C)^\times$ clearly implies $A^{(p,q)} = A^{(p',q')}$. Conversely, assume $A^{(p,q)} = A^{(p',q')}$. Then

$$(xp)(qy) = (xp')(q'y) \qquad (x, y \in A). \tag{1}$$

Setting $u := p^{-1}p'$, we obtain $p' = pu$, and (1) for $x = p'^{-1}, y = 1_A$ yields $q' = u^{-1}q$, hence $u = qq'^{-1}$. It remains to prove $u \in \mathrm{Nuc}(A)$ and, since A is alternative, it suffices to show $[A, u, A] = \{0\}$. To this end, we put $y = q'^{-1}$ (resp. $x = p'^{-1}$) in (1) to obtain $(xp)u = xp'$, (resp. $u^{-1}(qy) = q'y$). Hence (1) reads $(xp)(qy) = ((xp)u)(u^{-1}(qy))$, and since p, q are invertible, this amounts to $xy = (xu)(u^{-1}y)$ for all $x, y \in A$. Replacing y by uy and invoking (13.6.2), we conclude $[A, u, A] = \{0\}$, as desired. □

15.9 Unital isotopes. If A is unital, an isotope of A is said to be a *unital isotope*

if it has the same identity element as A. By (15.7.1), unital isotopes have the form

$$A^p := A^{(p^{-1},p)} \qquad (p \in A^\times). \tag{1}$$

Note that the algebra structure of A^p is given by the formula

$$x \cdot_p y = (xp^{-1})(py) \tag{2}$$

for $x, y \in A$. By Exc. 15.13 below, invertibility and inverses in A and A^p ($p \in A^\times$) are the same, while from (15.2.2), (15.3.1) we conclude

$$(A^p)^{\mathrm{op}} = (A^{\mathrm{op}})^{p^{-1}}, \quad (A^p)^q = A^{pq}, \quad A^{\alpha p} = A^p \quad (p, q \in A^\times,\ \alpha \in k^\times). \tag{3}$$

Moreover, Prop. 15.8 implies

$$A^p = A^q \iff p = uq \text{ for some } u \in \mathrm{Nuc}(A)^\times \qquad (p, q \in A^\times). \tag{4}$$

In particular, $A^p = A$ for all $p \in A^\times$ if A is associative.

Unital isotopes are important for various reasons: for example, they play a useful role in the two Tits constructions of cubic Jordan algebras in Chap. VII. Moreover, arbitrary isotopes are always isomorphic to appropriate unital ones (cf. Exc. 15.18 below). And finally, working in unital isotopes turns out to be computationally smooth, as may be seen from the following lemma.

15.10 Lemma. *Let A be unital and $p \in A^\times$. Then A and A^p have the same U-operators as well as the same powers x^m for $x \in A$, $m \in \mathbb{N}$ (resp. for $x \in A^\times$, $m \in \mathbb{Z}$).*

Proof The equality of U-operators follows from (15.5.1). Since $U_{x^m}x^n = (U_x)^m x^n = x^{2m+n}$ for $x \in A$, $m, n \in \mathbb{N}$ (resp. $x \in A^\times$, $m, n \in \mathbb{Z}$), the remaining assertions can now be derived by induction. □

15.11 Functoriality. Adjusting the terminology of 15.4 to the unital case, we denote by k-**alt**$_1$ the category of *unital* alternative k-algebras, morphisms being unital k-algebra homomorphisms (8.1). By contrast, the category of *pointed alternative k-algebras* will be denoted by k-**palt**. Its objects are pairs (A, p) consisting of a unital alternative k-algebra A and an invertible element $p \in A$, while its morphisms have the form $h\colon (A, p) \to (A', p')$ with pointed alternative k-algebras (A, p), (A', p') and a unital algebra homomorphism $h\colon A \to A'$ satisfying $h(p) = p'$. Again, it is then clear that the assignment $(A, p) \mapsto A^p$ gives rise to a (covariant) functor from k-**palt** to k-**alt**$_1$ which is the identity on morphisms.

15.12 Isotopy versus isomorphism. Recall that unital alternative k-algebras

A, B are isotopic if $A \cong B^{(p,q)}$ for some invertible elements $p, q \in B$, equivalently by Exc. 15.18 (a) below, if $A \cong B^p$ for some invertible element $p \in B$. It is then a natural question to ask whether isotopic unital alternative algebras are always isomorphic. This question has a trivial affirmative answer in the associative case (cf. 15.1), but a less trivial negative one in general, see McCrimmon [185, p. 259] for a counterexample. It becomes much more delicate, however, when restricting oneself to unital alternative k-algebras that are finitely generated projective as k-modules. In fact, there is a profound connection with the norm equivalence problem for composition algebras that will be discussed in 23.8 (c)–23.11 below.

Exercises

15.13. *Inverses in isotopes.* Let A be a unital alternative k-algebra and $p, q \in A^\times$. Show that the invertible elements of A and $A^{(p,q)}$ are the same and that, for $x \in A^\times = A^{(p,q)\times}$,

$$x^{(-1,p,q)} := U_{pq}^{-1} x^{-1}$$

is the inverse of x in $A^{(p,q)}$.

15.14. *Albert isotopies* (Albert [4]). Given non-associative k-algebras A, B, an *Albert isotopy* from A to B is a triple (f, g, h) of k-linear bijections $f, g, h\colon A \to B$ such that $f(xy) = g(x)h(y)$ for all $x, y \in A$. Albert isotopies from A to itself are called *Albert autotopies* of A. They form a subgroup of $\mathrm{GL}(A) \times \mathrm{GL}(A) \times \mathrm{GL}(A)$, denoted by $\mathrm{Atp}(A)$. Now prove *Schafer's isotopy theorem* (Schafer [252], McCrimmon [185]). If A, B are k-algebras, with A alternative and B unital, and if (f, g, h) is an Albert isotopy from A to B, then A, B are both unital alternative, $g^{-1}(1_B), h^{-1}(1_B)$ are invertible in A, and $f\colon A^{(p,q)} \to B$, $p := h^{-1}(1_B)^{-1}$, $q := g^{-1}(1_B)^{-1}$, is an isomorphism.

15.15. *The structure group of an alternative algebra* (Petersson [217]). Let A be a unital alternative k-algebra and $\mathrm{Str}(A)$ the set of all triples (p, q, g) composed of elements $p, q \in A^\times$ and an isomorphism $g\colon A \xrightarrow{\sim} A^{(p,q)}$. Show that $\mathrm{Str}(A)$ is a group under the multiplication

$$(p, q, g)(p', q', g') := (p[qg(p')]p, q[g(q')p]q, gg') \tag{1}$$

for $(p, q, g), (p', q', g') \in \mathrm{Str}(A)$ by performing the following steps.

(a) $\mathrm{Str}(A)$ is closed under the operation (1).

(b) For $p, q \in A^\times$, $g \in \mathrm{GL}(A)$, the following conditions are equivalent.

(i) $(p, q, g) \in \mathrm{Str}(A)$.
(ii) $g(xy)p = g(x)[(pq)(g(y)p)]$ for all $x, y \in A$.
(iii) $qg(xy) = [(qg(x))(pq)]g(y)$ for all $x, y \in A$.

(c) The assignment $(f, g, h) \mapsto (h(1_A)^{-1}, g(1_A)^{-1}, f)$ determines a well-defined bijection from $\mathrm{Atp}(A)$, the group of Albert autotopies of A (Exc. 15.14), onto $\mathrm{Str}(A)$ that is compatible with multiplications and whose inverse is given by $(p, q, g) \mapsto (g, R_p g, L_q g)$. What is the unit element of $\mathrm{Str}(A)$? What is the inverse of $(p, q, g) \in \mathrm{Str}(A)$?

15.16. *Extended left and right multiplications* (Petersson [217]). Let A be a unital alternative algebra and $u \in A^\times$. Prove that

$$\tilde{L}_u := (u, u^{-2}, L_u), \quad \tilde{R}_u := (u^{-2}, u, R_u)$$

belong to the structure group of A (Exc. 15.15). Show further for $u, v \in A^\times$ that the following identities hold in $\mathrm{Str}(A)$:

$$\begin{aligned}
\tilde{L}_{uvu} &= \tilde{L}_u \tilde{L}_v \tilde{L}_u, \quad (\tilde{L}_u)^{-1} = \tilde{L}_{u^{-1}}, \\
\tilde{R}_{uvu} &= \tilde{R}_u \tilde{R}_v \tilde{R}_u, \quad (\tilde{R}_u)^{-1} = \tilde{R}_{u^{-1}}, \\
\tilde{L}_u \tilde{R}_v &= (v^{-2}u, u^{-1}vu^{-1}, L_u R_v), \\
\tilde{R}_v \tilde{L}_u &= (v^{-1}u^{-1}v^{-1}, vu^{-2}, R_v L_u), \\
\tilde{L}_u \tilde{R}_u &= \tilde{R}_u \tilde{L}_u.
\end{aligned}$$

15.17. *The unital structure group* (Petersson [217]). Let A be a unital alternative k-algebra. Show that the set $\mathrm{Str}_1(A)$ of all elements $(p, q, g) \in \mathrm{Str}(A)$ such that $g(1_A) = 1_A$ (equivalently, $p = q^{-1}$) is a subgroup of $\mathrm{Str}(A)$, called the *unital structure group* of A. More precisely, show:

(a) Abbreviating the elements of $\mathrm{Str}_1(A)$ as $(p, g) := (p^{-1}, p, g)$ (so for (p, g), $p \in A^\times$, $g \in \mathrm{GL}(A)$, to belong to the unital structure group of A it is necessary and sufficient that $g\colon A \xrightarrow{\sim} A^p$ be an isomorphism), its group structure is determined by $1_{\mathrm{Str}_1(A)} = (1_A, \mathbf{1}_A)$ and

$$(p, g)(p', g') = (pg(p'), gg')$$

for $(p, g), (p', g') \in \mathrm{Str}_1(A)$.

(b) $\mathrm{Int}(p) := (p^{-3}, L_p R_{p^{-1}})$ belongs to the unital structure group of A. Why can $\mathrm{Int}(p)$ be viewed as the alternative version of the inner automorphism affected by an invertible element of a unital associative algebra?

15.18. Let A be a unital alternative algebra over k.

(a) Show that arbitrary isotopes of A are canonically isomorphic to unital ones. (*Hint*: For $p, q \in A^\times$, consider the extended right multiplication by pq (Exercise 15.16).)

(b) Computing the iterated unital isotope $((A^p)^q)^r$ for $p, q, r \in A^\times$ in two different ways seems to imply $(pq)r = up(qr)$ for some invertible element $u \in \mathrm{Nuc}(A)$. What's wrong with this argument and with this conclusion?

15.19. *Nucleus and centre of an isotope* (Petersson [213]). Let A be a unital alternative k-algebra and $p, q \in A^\times$. Prove $\mathrm{Nuc}(A^{(p,q)}) = \mathrm{Nuc}(A)(pq)^{-1}$ and $\mathrm{Cent}(A^{(p,q)}) = \mathrm{Cent}(A)(pq)^{-1}$. (*Hint*: Reduce to the case of unital isotopes.)

IV

Composition algebras

We have seen in Theorem 1.8 that the algebra of Graves-Cayley octonions as defined in 1.5 carries a positive definite real quadratic form that permits composition. In the present chapter we will study a class of non-associative algebras over an arbitrary commutative ring for which such a property is characteristic. Many results we derived for the Graves-Cayley octonions in the first chapter will resurface here under far more general circumstances, and with much more natural proofs attached.

16 Conic algebras

By (1.6.10), every element x in the algebra of Graves-Cayley octonions satisfies a quadratic equation that is universal in the sense that its coefficients depend "algebraically" on x. This innocuous but useful property gives rise to the notion of a conic algebra that will be studied in the present section.

The term "conic algebra" made its first appearance in papers by Garibaldi-Petersson [92] and Loos [175]. It derives its justification from the fact that conic algebras, just like the curves called conics, are intimately tied up with quadratic equations; for a more sophisticated motivation of this term, see 16.3 below. In deriving the main properties of conic algebras, we adhere rather closely to the treatment of McCrimmon [189], who calls them degree 2 algebras, while other authors speak of quadratic algebras in this context. By contrast, the term "quadratic algebra" will be used here in a much more restrictive sense, as in Knus [157, I, (1.3.6)].

Throughout we let k be an arbitrary commutative ring.

16.1 The concept of a conic algebra. By a *conic algebra* over k we mean a unital k-algebra C together with a quadratic form $n_C\colon C \to k$ such that

$$n_C(1_C) = 1, \quad x^2 - n_C(1_C, x)x + n_C(x)1_C = 0 \qquad (x \in C). \tag{1}$$

We call n_C the *norm* of C. Most of the time, we will just speak of a conic algebra C over k, its norm n_C being understood. Even though it follows from Exc. 17.8 below that the algebra C and condition (1) *do not* determine the quadratic form n_C uniquely, we feel justified in phrasing our definition, as well as

similar ones later on, in this slightly informal manner because it is convenient and there is no danger of confusion.

Let C be a conic algebra over k. Viewing C merely as a k-module, $(C, n_C, 1_C)$ is a pointed quadratic module over k in the sense of 11.14, with norm n_C, base point 1_C, trace

$$t_C\colon C \longrightarrow k, \quad x \longmapsto t_C(x) := n_C(1_C, x),$$

and conjugation

$$\iota_C\colon C \longrightarrow C, \quad x \longmapsto \bar{x} := t_C(x)1_C - x;$$

in the present context we speak of the *trace* (resp. the *conjugation*) of C.

We also denote by t_C the *bilinear trace* of C, i.e., the bilinear form $C\times C \to k$, $(x, y) \mapsto t_C(x, y) := t_C(xy)$, which in general is not symmetric, and in general does not agree with the bilinear trace of the pointed quadratic module $(C, n_C, 1_C)$. Given a submodule $M \subseteq C$, we always write $M^\perp = \{x \in C \mid n_C(x, M) = \{0\}\}$ for the orthogonal complement of M in C relative to the polarized norm.

Let C' be another conic algebra over k. By a *homomorphism* $h\colon C \to C'$ *of conic algebras* we mean a *unital* k-algebra homomorphism which preserves norms in the sense that $n_{C'} \circ h = n_C$. It is clear that homomorphisms of conic algebras also preserve (linear as well as bilinear) traces and conjugations. If $B \subseteq C$ is a unital subalgebra, it may and always will be regarded as a conic algebra in its own right by defining its norm $n_B := n_C|_B$ as the restriction of the norm of C to B; in this way, the inclusion $B \hookrightarrow C$ becomes a homomorphism of conic algebras.

Conic algebras are clearly invariant under base change. If C is a conic algebra over k, then so is C^{op}, with the same norm, linear trace and conjugation as C, while the bilinear trace changes in the obvious way to $t_{C^{\mathrm{op}}}(x, y) := t_C(y, x)$.

16.2 Examples of conic algebras. (a) The Graves-Cayley octonions $\mathbb{O}$, the Hamiltonian quaternions $\mathbb{H}$ and, more generally, all unital subalgebras $\mathbb{D} \subseteq \mathbb{O}$ are conic algebras over the reals.

(b) For $\mathbb{D}$ as in (a), all $\mathbb{Z}$-structures of $\mathbb{D}$ in the sense of 3.6 (d) are conic algebras over the integers.

(c) The base ring k itself, with norm $n_k\colon k \to k$ given by the squaring: $n_k(\alpha) = \alpha^2$ for $\alpha \in k$, is a conic k-algebra. We have $t_k(\alpha) = 2\alpha$, and the conjugation of k is the identity.

(d) $R = k \times k$ (as a direct product of ideals), with norm $n_R\colon R \to k$ given by $n_R((\alpha, \beta)) = \alpha\beta$ for $\alpha, \beta \in k$, is a conic k-algebra. We have $t_R((\alpha, \beta)) = \alpha + \beta$,

and the conjugation of R is the "switch": $\overline{(\alpha,\beta)} = (\beta,\alpha)$. In particular, the quadratic module (R, n_R) is the split hyperbolic plane (11.18).

(e) $R = k[\varepsilon]/(\varepsilon^2)$, the k-algebra of dual numbers, is a conic k-algebra, with norm, trace, conjugation respectively given by $n_R(\alpha 1_R + \beta\varepsilon) = \alpha^2$, $t_R(\alpha 1_R + \beta\varepsilon) = 2\alpha$, $\overline{\alpha 1_R + \beta\varepsilon} = \alpha 1_R - \beta\varepsilon$ for $\alpha, \beta \in k$.

(f) $R = K$, where k is a field and K/k is a quadratic field extension. Then R is a conic k-algebra, with $n_R = N_{K/k}$ (resp. $t_R = T_{K/k}$) the field norm (resp. the field trace) of K/k. Moreover, ι_R is the non-trivial Galois automorphism of K/k if K/k is separable, and the identity otherwise.

(g) $C = \mathrm{Mat}_2(k)$ with n_C the determinant det. For $x \in C$, one finds that $t_C(x) = \mathrm{tr}(x)$, the usual trace, so the second equation in (16.1.1) is the familiar Cayley-Hamilton Theorem. For $\alpha, \beta, \gamma, \delta \in k$ we have

$$\overline{\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)} = \left(\begin{smallmatrix} \delta & -\beta \\ -\gamma & \alpha \end{smallmatrix}\right)$$

so $\bar{x} = yx^{\mathsf{T}}y^{-1}$ for $y = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

16.3 Motivation. Let k be a field and $X \subseteq \mathbb{P}^2_k$ a smooth conic in the plane, given by a regular quadratic form in three variables. Then one checks easily that the *scheme-theoretic* intersection (cf. [107, I, 4.4]) of X with appropriate lines in $\mathbb{P}^2_k$ has the form $\mathrm{Spec}(R)$ (viewed as an affine scheme), where R is one of the algebras listed in 16.2 (d),(e),(f) above. This gives another motivation of the term "conic algebra".

16.4 Quadratic algebras. In analogy to Knus [157, I, (1.3.6)], an algebra R over k is said to be *quadratic* if it contains an identity element and is projective of rank 2 as a k-module. It follows from the Cayley-Hamilton theorem that *a quadratic k-algebra R is conic*, with norm and trace given by

$$n_R(x) = \det(L_x), \quad t_R(x) = \mathrm{tr}(L_x) \qquad (x \in R), \tag{1}$$

in terms of the left multiplication of R. Moreover, we claim *that $1_R \in R$ is unimodular, R is commutative, associative, and its conjugation is an involution*, i.e., a k-automorphism of period two. As to the first part, we note that $R(\mathfrak{p})$, for any $\mathfrak{p} \in \mathrm{Spec}(k)$, is a unital two-dimensional $k(\mathfrak{p})$-algebra, forcing $1_R(\mathfrak{p}) \neq 0$. Hence 1_R is unimodular by Lemma 9.17. Since the remaining assertions are local on k, we may assume that k is a local ring, making R a free k-module of rank 2. Extending 1_R to a basis of R, which we are allowed to do by unimodularity, the commutative and the associative law for the multiplication of R trivially hold, as does the property of the conjugation being a k-automorphism of period two. Thus our assertion is proved.

16.5 Basic identities. Let C be a conic algebra over k. The following identities either hold by definition or are straightforward to check.

$$x^2 = t_C(x)x - n_C(x)1_C, \tag{1}$$
$$t_C(x) = n_C(1_C, x), \tag{2}$$
$$n_C(1_C) = 1, \quad t_C(1_C) = 2, \tag{3}$$
$$\bar{x} = t_C(x)1_C - x, \quad \bar{1}_C = 1_C, \quad \bar{\bar{x}} = x, \tag{4}$$
$$x \circ y := xy + yx = t_C(x)y + t_C(y)x - n_C(x, y)1_C, \tag{5}$$
$$x\bar{x} = n_C(x)1_C = \bar{x}x, \quad x + \bar{x} = t_C(x)1_C, \tag{6}$$
$$n_C(\bar{x}) = n_C(x), \quad t_C(\bar{x}) = t_C(x), \tag{7}$$
$$t_C(x^2) = t_C(x)^2 - 2n_C(x), \tag{8}$$
$$t_C(x \circ y) = t_C(x, y) + t_C(y, x) = 2[t_C(x)t_C(y) - n_C(x, y)], \tag{9}$$
$$n_C(x, \bar{y}) = t_C(x)t_C(y) - n_C(x, y), \tag{10}$$
$$\overline{xy} - \bar{y}\bar{x} = (t_C(x, y) - n_C(x, \bar{y}))1_C. \tag{11}$$

By (1) and 7.7, $k[x]$ agrees with the submodule of C spanned by 1_C and x; it is a commutative associative subalgebra. In particular, *conic algebras are power-associative*.

Before we can proceed, we require two short digressions.

16.6 Unimodular elements revisited. For several of our subsequent results it will be important to know that $1_C \in C$ is unimodular. While this is not always true, it does hold automatically if the linear trace of C is surjective, since this is equivalent to $t_C(x) = 1$ for some $x \in C$ and so the linear form $\lambda\colon C \to k$, $y \mapsto t_C(xy)$, satisfies $\lambda(1_C) = 1$.

For example, if $2 \in k^\times$, then $t_C(x) = 1$ for $x = \frac{1}{2} \cdot 1_C$ and 1_C is unimodular. Moreover, we have

$$C = k1_C \oplus C^0 \tag{1}$$

as a direct sum of submodules, where

$$C^0 := \mathrm{Ker}(t_C) = \{x \in C \mid \bar{x} = -x\}, \tag{2}$$

and

$$H(C, \iota_C) := \{x \in C \mid \bar{x} = x\} = k1_C. \tag{3}$$

Another important condition that ensures unimodularity of 1_C will be stated separately.

16.7 Proposition. *Let C be a conic algebra over k which is projective as a k-module. Then $1_C \in C$ is unimodular and $C_\mathfrak{p} \neq \{0\}$ for all prime ideals $\mathfrak{p} \subseteq k$.*

Proof The first part follows immediately from Lemma 11.15 (applied to the pointed quadratic module $(C, n_C, 1_C)$), which in turn implies the second, by Lemma 9.17. □

16.8 Trivial conjugation. A conic algebra C over k is said to have *trivial conjugation* if $\iota_C = \mathbf{1}_C$. Having trivial conjugation is a rather exotic phenomenon. For example, if $2 \in k^\times$, then (16.6.1), (16.6.2) show that C does not have trivial conjugation unless $C \cong k$. More generally, the same conclusion holds if t_C is surjective (Exc. 16.27). On the other hand, if $2 = 0$ in k and $t_C = 0$ (e.g., if k is a field and C an inseparable quadratic field extension of k), then C does have trivial conjugation.

16.9 The annihilator. The *annihilator* of a k-module M is defined by

$$\operatorname{Ann}(M) := \{\alpha \in k \mid \alpha M = \{0\}\}. \tag{1}$$

M is said to be *faithful* if $\operatorname{Ann}(M) = \{0\}$. If A is a unital k-algebra, then

$$\operatorname{Ann}(A) = \{\alpha \in k \mid \alpha 1_A = 0\}. \tag{2}$$

In subsequent applications, conic algebras which are *flexible* (i.e., satisfy the flexible law $(xy)x = x(yx)$) or whose conjugation is an (algebra) involution play an important role. These two properties will now be related to one another in various ways.

16.10 Proposition. *Let C be a conic algebra over k.*

(a) The conjugation of C is an involution if and only if

$$t_C(x, y) - n_C(x, \bar{y}) \in \operatorname{Ann}(C)$$

for all $x, y \in C$.

(b) C is flexible if and only if

$$(t_C(x, y) - n_C(x, \bar{y}))x = (n_C(x, xy) - t_C(y)n_C(x))1_C \tag{1}$$

for all $x, y \in C$.

Proof (a) follows immediately from (16.5.11) and (16.9.2). In (b) one simply notes $(xy)x - x(yx) = (xy) \circ x - x(x \circ y)$ and expands the right-hand side using (16.5.5), (16.5.1), (16.5.10). □

16.11 Corollary. *Let C be a conic k-algebra whose conjugation is an involution. Then C is flexible if and only if $n_C(x, xy) - t_C(y)n_C(x) \in \operatorname{Ann}(C)$ for all $x, y \in C$.* □

16.12 Proposition. *The following (collections of) identities are equivalent in any conic algebra C over k.*

$$n_C(x, yx) = t_C(y)n_C(x), \tag{1}$$
$$n_C(x, xy) = t_C(y)n_C(x), \tag{2}$$
$$n_C(xy, z) = n_C(x, z\bar{y}), \tag{3}$$
$$n_C(xy, z) = n_C(y, \bar{x}z), \tag{4}$$
$$t_C(x, y) = n_C(x, \bar{y}), \quad t_C(xy, z) = t_C(x, yz). \tag{5}$$

If these equations hold, the conjugation of C is an involution.

Proof Since (2) (resp. (4)) is (1) (resp. (3)) in C^{op}, the equivalence of (1)–(5) will follow once we have established the following implications.

(1) $\Leftrightarrow$ (2). Combine (16.5.2) with (16.5.5) to conclude that $n_C(x, x \circ y) = 2t_C(y)n_C(x)$.

(2) $\Rightarrow$ (3). Linearize (2) and apply (16.5.4).

(4) $\Rightarrow$ (2). Put $z = x$ in (4) and apply (16.5.6).

(3) $\Rightarrow$ (5). Put $z = 1_C$ in (3) and apply (16.5.2) to deduce the first equation of (5). But then, by Prop. 16.10 (a), ι_C is an involution of C, yielding the final statement of the proposition, while the last equation of (5) follows by a straightforward computation.

(5) $\Rightarrow$ (1). By Prop. 16.10 (a) and the first equation of (5), ι_C is an involution of C, which implies $n_C(x, yx) = t_C(x, \bar{x}\bar{y}) = t_C(x\bar{x}, \bar{y})$ by (5), and (1) follows from (16.5.6), (16.5.7). □

16.13 Norm-associative conic algebras. A conic algebra satisfying one (hence all) of the identities (16.12.1)–(16.12.5) is said to be *norm-associative*. If C is a norm-associative conic algebra, then (16.12.5) combined with (16.5.10) shows that the linear trace of C is an associative linear form, so

$$t_C(xy) = t_C(yx), \quad t_C((xy)z) = t_C(x(yz)) =: t_C(xyz). \tag{1}$$

Moreover, the bilinear trace of C agrees with the bilinear trace of the pointed quadratic module $(C, n_C, 1_C)$. The property of being norm-associative is clearly invariant under scalar extensions. Also, if C is a norm-associative conic algebra, then so is C^{op}.

16.14 Proposition. *Let C be a conic algebra over k.*

(a) If C is norm-associative, then it is flexible and its conjugation is an involution.

(b) If C is flexible and it is projective as a k-module, then it is norm-associative.

For a norm-associative conic algebra, the conjugation is called the *canonical involution*.

Proof If C is a norm-associative conic k-algebra, then by (16.12.5) and (16.12.2) combined with Proposition 16.10 (a), C is flexible and its conjugation is an involution. Conversely, suppose C is flexible and projective as a k-module. Given $y \in C$, it suffices to show

$$t_C(x, y) = n_C(x, \bar{y}) \qquad (x \in C) \tag{1}$$

since (16.10.1) and unimodularity of 1_C (Proposition 16.7) then imply identity (16.12.2). To establish (1), we may assume that k is a local ring and extend $e_0 := 1_C$ to a basis (e_i) of the k-module C. Then (1) holds for $x = e_0$ by (16.5.7) and for $x = e_i$, $i \neq 0$, by (16.10.1), hence on all of C by linearity. □

16.15 Corollary. *A faithful conic algebra over k is norm-associative if and only if it is flexible and its conjugation is an involution.*

Proof The "only if" direction is Proposition 16.14(a). Conversely, suppose C is a flexible faithful conic k-algebra whose conjugation is an involution. Combining Proposition 16.10 with faithfulness, we see that (16.12.2) holds, so C is norm-associative. □

16.16 Proposition. *Let C be a conic algebra over k. If C is projective as a k-module, then the norm of C is uniquely determined by the algebra structure of C.*

Proof Let $n\colon C \to k$ be any quadratic form making C a conic algebra and write t for the corresponding linear trace. Then $\lambda := t_C - t$ (resp. $q := n_C - n$) is a linear (resp. a quadratic) form on C, and (16.5.1) yields

$$\lambda(x)x = q(x)1_C, \tag{1}$$

for all $x \in C$. We have to prove $\lambda = q = 0$. Since $1_C \in C$ is unimodular by Proposition 16.7, it suffices to show $\lambda = 0$. This can be checked locally, so we may assume that k is a local ring, allowing us to extend $e_0 := 1_C$ to a basis (e_i) of C as a k-module. But $\lambda(e_0) = 0$ by (16.5.3). Hence it remains to show $\lambda(e_i) = 0$ for all $i \neq 0$, which follows immediately from (1). □

16.17 Semi-linear homomorphisms of conic algebras. Let $\sigma\colon K \to K'$ be a homomorphism in k-**alg** and C (resp. C') a conic algebra over K (resp. K'). A map $\varphi\colon C \to C'$ is called a *σ-semi-linear homomorphism* of conic algebras if the following conditions are fulfilled.

(i) φ is σ-semi-linear.

(ii) $\varphi\colon C \to C'$ is a unital homomorphism of k-algebras.

(iii) The σ-semi-linear polynomial square

$$\begin{array}{ccc} C & \xrightarrow{\varphi} & C' \\ {\scriptstyle n_C}\downarrow & & \downarrow{\scriptstyle n_{C'}} \\ K & \xrightarrow[\sigma]{} & K' \end{array} \tag{1}$$

commutes in the sense of 12.28.

By Corollary 11.5, condition (iii) is equivalent to (1) being commutative as a diagram of set maps. Because of (iii), we have

$$n_{C'}(\varphi(x)) = \sigma(n_C(x)), \quad t_{C'}(\varphi(x)) = \sigma(t_C(x)), \quad \varphi(\bar{x}) = \overline{\varphi(x)} \tag{2}$$

for all $x \in C$.

Exercises

16.18. Let C be a conic algebra over k and $x \in C$. Prove

(a) $n_C(yz) = n_C(y)n_C(z)$ for all $y, z \in k[x]$.

(b) x is invertible in (the commutative associative k-algebra) $k[x]$ if and only if $n_C(x)$ is invertible in k, in which case

$$x^{-1} = n_C(x)^{-1}\bar{x}, \quad n_C(x^{-1}) = n_C(x)^{-1}.$$

(c) x is a nilpotent element of C (Exc. 7.13) if and only if $t_C(x)$ and $n_C(x)$ are nilpotent elements of k.

16.19. Let C, C' be conic k-algebras and suppose C is projective as a k-module. Prove that every injective homomorphism $\varphi\colon C \to C'$ of unital k-algebras is, in fact, one of conic algebras, i.e., it preserves norms (hence traces and conjugations as well). Does this conclusion continue to hold without the hypothesis of φ being injective?

16.20. *Co-ordinates for conic algebras* (Loos [175]). Let k be a commutative ring, X a k-module, $e \in X$ a unimodular element and $\lambda\colon X \to k$ a linear form such that $\lambda(e) = 1$. Putting $M_\lambda := \mathrm{Ker}(\lambda)$, we then have $X = ke \oplus M_\lambda$ as a direct sum of submodules.

(a) Let (T, B, K) be a *conic co-ordinates system* relative to (X, e, λ) in the sense that $T\colon M_\lambda \to k$ is a linear form, $B\colon M_\lambda \times M_\lambda \to k$ is a (possibly non-symmetric) bilinear form and

$$K\colon M_\lambda \times M_\lambda \longrightarrow M_\lambda, \quad (x, y) \longmapsto x \times y,$$

is an alternating bilinear map. Define a k-algebra structure $C := \mathrm{Con}(T, B, K) = C_{X,e,\lambda}(T, B, K)$ on X by the multiplication

$$(\alpha e + x)(\beta e + y) := (\alpha\beta - B(x, y))e + ((\alpha + T(x))y + \beta x - x \times y)$$

for $\alpha, \beta \in k$, $x, y \in M_\lambda$. Show that C is a conic k-algebra with identity element e and norm $n_C \colon C \to k$ given by

$$n_C(\alpha e + x) := \alpha^2 + \alpha T(x) + B(x, x)$$

for $\alpha \in k$ and $x \in M_\lambda$.

(b) Conversely, suppose C is a conic k-algebra with underlying k-module X and identity element $1_C = e$. Show that (T_C, B_C, K_C), where $T = T_C \colon M_\lambda \to k$, $B = B_C \colon M_\lambda \times M_\lambda \to k$ and $K = K_C \colon M_\lambda \times M_\lambda \to M_\lambda$, $(x, y) \mapsto x \times y$ are defined by

$$T(x) := t_C(x), \quad B(x, y) := -\lambda(xy), \quad x \times y := t_C(x)y - xy + \lambda(xy) \quad (x, y \in M_\lambda),$$

is a conic co-ordinate system for (X, e, λ). Show further that the assignments $(T, B, K) \mapsto \mathrm{Con}(T, B, K)$ and $C \mapsto (T_C, B_C, K_C)$ define inverse bijections between the set of conic co-ordinate system for (X, e, λ) and the set of conic k-algebras with underlying k-module X and identity element e.

Remarks. (a) It is sometimes convenient to define conic co-ordinate systems on a k-module that is independent of the choice of λ, namely, on X/ke. This point of view, systematically adopted by Loos [175], turns out to be particularly useful when analyzing the question of how conic co-ordinate systems change with λ.

(b) Let C be a conic k-algebra, $X = C$ as a k-module and $e := 1_C$. If $2 \in k$ is a unit, then conic co-ordinate systems may be taken relative to (X, e, λ) with $\lambda := \frac{1}{2} t_C$, in which case the conic co-ordinate system corresponding to C is already in Osborn [205, Thm. 1].

16.21 (Dickson [65])**.** Let k be a field of characteristic not 2 and C a unital algebra over k. Show that C is conic if and only if $1_C, x, x^2$ are linearly dependent over k for all $x \in C$. (*Hint*: If this condition is fulfilled, linearize the expression $1_C \wedge x \wedge x^2 \in \bigwedge^3(C)$ to show that 0 and the elements $u \in C \setminus k1_C$ satisfying $u^2 \in k1_C$ form a vector subspace of C.)

16.22. *The Dickson condition.* Generalize Exc. 16.21 in the following way: let C be a unital algebra over k which is either free (possibly of infinite rank) or finitely generated projective as a k-module and whose identity element is unimodular. Show that there exists a quadratic form $n_C \colon C \to k$ making C a conic k-algebra if and only if C satisfies the *Dickson condition*: For all $R \in k\text{-}\mathbf{alg}$ and all $x \in C_R$, the element $x^2 \in C_R$ is an R-linear combination of x and 1_{C_R}.

16.23. *Elementary idempotents*. (a) Let C be a conic k-algebra. Show that, if $k \neq \{0\}$ is *connected* (so $0, 1$ are the only idempotents of k, equivalently by Exc. 9.29, the topological space $\mathrm{Spec}(k)$ is connected), an element $c \in C$ is an idempotent $\neq 0, 1_C$ if and only if $n_C(c) = 0$ and $t_C(c) = 1$.

(b) Conclude that, for any commutative ring k and any element $c \in C$, the following conditions are equivalent.

(i) c is an idempotent satisfying $c_R \neq 0, 1_{C_R}$ for all $R \in k\text{-}\mathbf{alg}$, $R \neq \{0\}$.
(ii) c is an idempotent satisfying $c_\mathfrak{p} \neq 0, 1_{C_\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subseteq k$.
(iii) $n_C(c) = 0, \quad t_C(c) = 1$.
(iv) c is an idempotent and the elements $c, 1_C - c$ are unimodular.

If these conditions are fulfilled, we call c an *elementary* idempotent of C.

16.24. *Conic ideals.* By a *conic ideal* in a conic k-algebra C we mean a pair $(\mathfrak{a}, I)$ consisting of an ideal $\mathfrak{a} \subseteq k$ and a (two-sided) ideal $I \subseteq C$ such that $\mathfrak{a}C \subseteq I$ and

$$n_C(x), n_C(x, y) \in \mathfrak{a} \tag{1}$$

for all $x \in I$, $y \in C$.

(a) Show that every ideal $\mathfrak{a} \subseteq k$ (resp. $I \subseteq C$) can be extended to a conic ideal in C. More precisely, there is a unique smallest ideal $I \subseteq C$ (resp. $\mathfrak{a} \subseteq k$) making $(\mathfrak{a}, I)$ a conic ideal in C.

(b) Let $\sigma\colon K \to K'$ be a morphism in k-**alg**, C (resp. C') a conic algebra over K (resp. K') and $\varphi\colon C \to C'$ a σ-semi-linear homomorphism of conic algebras. Prove that

$$\mathrm{Ker}(\sigma, \varphi) := (\mathrm{Ker}(\sigma), \mathrm{Ker}(\varphi))$$

is a conic ideal in C.

(c) Conversely, let C be a conic k-algebra, $(\mathfrak{a}, I)$ a conic ideal in C and write σ for the canonical projection from k to $k_0 := k/\mathfrak{a}$. Prove that $C_0 := C/I$ carries the unique structure of a conic k_0-algebra making the canonical projection $\pi\colon C \to C_0$ a σ-semi-linear homomorphism of conic algebras. Moreover, $\mathrm{Ker}(\sigma, \pi) = (\mathfrak{a}, I)$.

16.25. *Conic nil ideals and the lifting of elementary idempotents.* Let C be a conic algebra over k. By a *conic nil ideal* in C we mean a conic ideal $(\mathfrak{a}, I)$ such that $\mathfrak{a} \subseteq k$ or $I \subseteq C$ is a nil ideal.

(a) Prove that if $(\mathfrak{a}, I)$ is a conic nil ideal in C, then $\mathfrak{a}$ *and* I are both nil ideals in k, C, respectively.

(b) Prove that $(\mathrm{Nil}(k), \mathrm{Nil}(C))$ is a conic nil ideal in C.

(c) Let $(\mathfrak{a}, I)$ be a conic nil ideal in C and put $C_0 := C/I$, viewed as a conic algebra over $k_0 := k/\mathfrak{a}$ via Exc. 16.24 (c). Letting c_0 be an elementary idempotent in C_0, show with the canonical projection $\pi\colon C \to C_0$ that every idempotent in $\pi^{-1}(c_0)$ (whose existence is guaranteed by Exc. 7.14 (b)) is elementary.

16.26. Let C be a conic algebra over k. Prove for $c \in C$ that the following conditions are equivalent.

(i) c is an idempotent in C.

(ii) There exists a complete orthogonal system $(\varepsilon^{(0)}, \varepsilon^{(1)}, \varepsilon^{(2)})$ of idempotents in k, giving rise to decompositions

$$k = k^{(0)} \times k^{(1)} \times k^{(2)}, \quad C = C^{(0)} \times C^{(1)} \times C^{(2)}$$

as direct products of ideals, where $k^{(i)} = k\varepsilon^{(i)}$ and $C^{(i)} = \varepsilon^{(i)}C = C_{k^{(i)}}$ as a conic algebra over $k^{(i)}$ for $i = 0, 1, 2$, such that

$$c = (0, c^{(1)}, 1_{C^{(2)}}),$$

where $c^{(1)}$ is an elementary idempotent of $C^{(1)}$.

In this case, the idempotents $\varepsilon^{(i)}$, $i = 0, 1, 2$, in (ii) are unique and given by

$$\varepsilon^{(0)} := (1 - n_C(c))(1 - t_C(c)), \quad \varepsilon^{(1)} := (1 - n_C(c))t_C(c), \quad \varepsilon^{(2)} := n_C(c). \tag{1}$$

16.27. Let C be a conic k-algebra that is faithful as a k-module and whose linear trace is surjective. Show that C has trivial conjugation if and only if $C \cong k$.

16.28. *Norms of commutators* (Garibaldi-Petersson [92, Prop. 2.4]). Let C be a norm-associative conic k-algebra. Show that the trilinear map

$$C^3 \longrightarrow k, \quad (x, y, z) \longmapsto n_C(x, [y, z])$$

is alternating and that the following identities

$$n_C(xy) = n_C(yx), \tag{1}$$

$$n_C([x, y]) = 4n_C(xy) - t_C(x)^2 n_C(y) - t_C(y)^2 n_C(x) + n_C(x, y)n_C(x, \bar{y}) \tag{2}$$

hold for all $x, y \in C$.

17 Conic alternative algebras

In 5.5, we have defined the euclidean Albert algebra as a commutative non-associative real algebra that lives on the 3-by-3 hermitian matrices with entries in the Graves-Cayley octonions. As we will show in due course, this important construction can be generalized to arbitrary conic alternative algebras over commutative rings once a peculiar additional hypothesis has been inserted. The elementary properties of conic alternative algebras needed to carry out this generalization will be assembled in the present section. Throughout we let k be an arbitrary commutative ring.

We begin by identifying the "peculiar additional hypothesis".

17.1 Multiplicative conic algebras. A conic algebra C over k is said to be *multiplicative* if its norm *permits composition*:

$$n_C(xy) = n_C(x)n_C(y) \qquad (x, y \in C) \tag{1}$$

Linearizing this identity repeatedly, we conclude that multiplicative conic algebras also satisfy the relations

$$n_C(x_1 y, x_2 y) = n_C(x_1, x_2)n_C(y), \tag{2}$$

$$n_C(xy_1, xy_2) = n_C(x)n_C(y_1, y_2), \tag{3}$$

$$n_C(x_1 y_1, x_2 y_2) + n_C(x_1 y_2, x_2 y_1) = n_C(x_1, x_2)n_C(y_1, y_2) \tag{4}$$

for all $x, x_1, x_2, y, y_1, y_2 \in C$. We conclude from this that multiplicative conic algebras are stable under base change. Note further that, if C is a multiplicative conic algebra, so is C^{op}.

Putting $y_1 := 1_C$, $y_2 := y$ in (3), we see that multiplicative conic algebras satisfy the identity (16.12.2). Therefore Prop. 16.14 immediately implies the first part of the following observation, while the second part is a consequence of (16.4.1) .

17.2 Proposition. *(a) Multiplicative conic algebras are norm-associative. In particular, they are flexible, and their conjugation is an involution.*

(b) Quadratic algebras are multiplicative. □

17.3 Vector product and the Lagrange identity. Let C be a multiplicative conic k-algebra. Then Prop. 17.2 and (2) of Exc. 16.28 imply

$$\begin{aligned} n_C([x,y]) = 4n_C(x)n_C(y) - t_C(x)^2 n_C(y) \\ - t_C(y)^2 n_C(x) + n_C(x,y)n_C(x,\bar{y}) \end{aligned} \tag{1}$$

for all $x, y \in C$. Now suppose in addition $2 \in k^\times$. By (16.6.1), (16.6.2) we have

$$C = k1_C \oplus C^0, \quad C^0 = \mathrm{Ker}(t_C). \tag{2}$$

For $x, y \in C^0$, we deduce

$$x \times y := \frac{1}{2}[x,y] = \frac{1}{2}(xy - yx) \in C^0 \tag{3}$$

from (16.13.5) and call $x \times y$ the *vector product* of x and y, which is skew-symmetric in x, y. Since $\bar{y} = -y$, it follows that (1) collapses to what we call the *Lagrange identity of the vector product*:

$$n_C(x \times y) = n_C(x)n_C(y) - \left(\tfrac{1}{2}n_C(x,y)\right)^2. \tag{4}$$

In order to justify the preceding terminology, let $C := \mathbb{H}$ be the Hamiltonian quaternions over $k := \mathbb{R}$ and identify $\mathbb{H}^0 = \mathbb{R}^3$ via the basis in 1.11. The vector product as defined in (3) by (1.11.1) agrees with the ordinary vector product in 3-space. In view of (1.6.3), the Lagrange identity (4) takes on the usual form

$$\|x \times y\|^2 = \|x\|^2\|y\|^2 - (x^{\mathsf{T}}y)^2 \tag{5}$$

for $x, y \in \mathbb{R}^3$.

17.4 Identities in conic alternative algebras. Let C be a conic alternative algebra over k. Combining the left and right alternative laws, $x(xy) = x^2y$ and $(yx)x = yx^2$, with (16.5.1), (16.5.4), we deduce *Kirmse's identities* [152, p. 67]:

$$x(\bar{x}y) = n_C(x)y = (y\bar{x})x. \tag{1}$$

We can also derive a formula for the U-operator,

$$U_x y = xyx = n_C(x,\bar{y})x - n_C(x)\bar{y}, \tag{2}$$

which follows by using (16.5.1), (16.5.5), (16.5.4), (16.5.10) to manipulate the expression $xyx = (x \circ y)x - yx^2$, see Exc. 1.18 (c) in the special case $k = \mathbb{R}$,

$C = \mathbb{O}$. Applying the norm to the right-hand side of (2) and expanding, we conclude

$$n_C(U_x y) = n_C(xyx) = n_C(x)^2 n_C(y). \tag{3}$$

In view of this, one might be tempted to conjecture that conic alternative algebras are multiplicative. But, according to Exc. 17.8 below, this is not so. Fortunately, however, (3) is strong enough to characterize invertibility in conic alternative algebras.

17.5 Proposition. *Let C be a conic alternative algebra over k. An element $x \in C$ is invertible in C if and only if $n_C(x)$ is invertible in k. In this case, $x^{-1} = n_C(x)^{-1}\bar{x}$ and $n_C(x^{-1}) = n_C(x)^{-1}$.*

Proof If $n_C(x) \in k^\times$, then (16.5.6) shows that $y := n_C(x)^{-1}\bar{x}$ satisfies $xy = 1_C = yx$, forcing $x \in C^\times$ and $y = x^{-1}$ by Prop. 13.6. Conversely, suppose x is invertible in C. Then $U_x x^{-2} = 1_C$, and (17.4.3) yields $1 = n_C(x)^2 n_C(x^{-2})$, hence $n_C(x) \in k^\times$. The final formula follows from the fact that the conjugation of C leaves its norm invariant. □

While it is not true in general that conic alternative algebras are multiplicative, this implication does hold under natural conditions on the module structure.

17.6 Proposition. *Let C be a conic alternative algebra over k that is projective as a k-module. Then C is multiplicative.*

Proof As an alternative algebra, C is flexible, whence Proposition 16.14 implies that C is norm-associative. In particular, the conjugation of C is an involution. Let $x, y \in C$. By Artin's Theorem (Corollary 14.5), the unital subalgebra of C generated by x, y is associative. Moreover, by (16.5.4), it contains $\bar{x}$ and $\bar{y}$. Hence (16.5.6) yields

$$n_C(xy)1_C = xy\overline{xy} = xy\bar{y}\bar{x} = n_C(y)x\bar{x} = n_C(x)n_C(y)1_C,$$

and since 1_C is unimodular (Prop. 16.7), C is indeed multiplicative. □

17.7 Some categories of conic algebras. For future references it will be convenient to consider the category k-**conalg** whose objects are conic k-algebras and whose morphisms are homomorphisms of conic algebras as defined in 16.1. Multiplicative conic alternative algebras will be regarded as a full subcategory of k-**conalg**, denoted by k-**mcalt**. Strictly speaking, the objects of k-**mcalt** have the form (C, n_C) where C is a conic alternative k-algebra with norm n_C which is multiplicative in the sense of 17.1. We obtain the forgetful functor from

k-**mcalt** to k-$\mathbf{alt}_1$ defined by $(C, n_C) \mapsto C$ on objects and by the identity on morphisms. This functor is obviously faithful but, by Exc. 17.8 below, not full.

Exercises

17.8 (McCrimmon [189])**.** The following exercise will produce an example of an algebra that supports many different conic algebra structures, some of which are multiplicative (resp. norm-associative), while others are not.

Let $k = k_0[\varepsilon]$, $\varepsilon^2 = 0$, be the algebra of dual numbers over a commutative ring k_0, and view k_0 as a k-algebra via the natural map $k \to k_0$, $\varepsilon \mapsto 0$, the corresponding module action $k \times k_0 \to k_0$ being indicated by $(\alpha, \alpha_0) \mapsto \alpha.\alpha_0$. In particular, (column) 3-space k_0^3 becomes a k-module in this way. In fact, it becomes a k-algebra under the multiplication

$$\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix} := \begin{pmatrix}0\\ 0\\ \alpha_1\beta_2\end{pmatrix} \qquad (\alpha_i, \beta_i \in k_0,\ 1 \le i \le 3). \tag{1}$$

Furthermore, let

$$z = \begin{pmatrix}\delta_1\\ \delta_2\\ \delta_3\end{pmatrix} \in k_0^3$$

be arbitrary. Now consider the k-algebra C defined on the k-module $k \times k_0^3$ by the multiplication

$$(\alpha_1, u_1)(\alpha_2, u_2) := (\alpha_1\alpha_2, \alpha_1.u_2 + \alpha_2.u_1 + [u_1, u_2])$$

for $\alpha_i \in k$, $u_i \in k_0^3$, $i = 1, 2$, where $[u_1, u_2]$ is the commutator belonging to the k-algebra structure of k_0^3 just defined, and let $n_z \colon C \to k$ be given by

$$n_z((\alpha, u)) := \alpha^2 + (\alpha.(z^{\mathsf{T}}u))\varepsilon$$

for $\alpha \in k$, $u \in k_0^3$. Then show that C is an associative conic k-algebra with norm $n_C := n_z$, and that the following conditions are equivalent.

(i) C is multiplicative.
(ii) C is norm-associative.
(iii) The conjugation of C is an involution.
(iv) $\delta_3 = 0$.

17.9. Let C be a multiplicative conic algebra over k. Show that its nil radical has the form

$$\mathrm{Nil}(C) = \{x \in C \mid n_C(x), n_C(x, y) \in \mathrm{Nil}(k) \text{ for all } y \in C\}.$$

17.10. *Artin's theorem for conic alternative algebras*. Let C be a conic alternative k-algebra that is unitally generated by two elements $x, y \in C$. Show that C is spanned by $1_C, x, y, xy$ as a k-module. Conclude without recourse to Artin's theorem (Cor. 14.5) that C is associative.

17.11. *Norms of associators* (Garibaldi-Petersson [92, Thm. 2.8]). Let C be a multiplicative conic alternative algebra over k. Prove

$$\begin{aligned} n_C([x_1,x_2,x_3]) = 4n_C(x_1)n_C(x_2)n_C(x_3) &- \sum t_C(x_i)^2 n_C(x_j)n_C(x_l) \\ &+ \sum t_C(x_ix_j)n_C(x_i,x_j)n_C(x_l) - t_C(x_1x_2)t_C(x_2x_3)t_C(x_3x_1) \\ &+ t_C(x_1x_2x_3)t_C(x_2x_1x_3) \end{aligned}$$

for all $x_1, x_2, x_3 \in C$, where both summations on the right are to be taken over the cyclic permutations $(i\,j\,l)$ of (123).

17.12. *Isotopes of conic alternative algebras*. Let C be a conic alternative k-algebra. Prove for $p, q \in C^\times$ that $C^{(p,q)}$ is again a conic alternative k-algebra with norm $n_{C^{(p,q)}} = n_C(pq)n_C$. Moreover, trace and conjugation of $C^{(p,q)}$ are given by

$$t_{C^{(p,q)}}(x) = n_C(\overline{pq}, x), \quad \iota_{C^{(p,q)}}(x) = \overline{x}^{(p,q)} = n_C(pq)^{-1}\overline{pq}\;\overline{x}\;\overline{pq} \qquad (x \in C).$$

Show further that, if in addition, C is multiplicative, then so is $C^{(p,q)}$.

18 The Cayley-Dickson construction

The only example we have encountered so far of an alternative algebra which is not associative is the real algebra of Graves-Cayley octonions. The Cayley-Dickson construction will provide us with a tool to accomplish the same over any commutative ring. Moreover, it will play a crucial role in the structure theory of composition algebras over fields later on.

Throughout this section, we fix an arbitrary commutative ring k. Our first aim will be to present what might be called an internal version of the Cayley-Dickson construction.

18.1 Proposition (Internal Cayley-Dickson construction)**.** *Let C be a multiplicative conic alternative algebra over k and $B \subseteq C$ a unital subalgebra. If $l \in C$ is perpendicular to B relative to Dn_C, then $B + Bl \subseteq C$ is the subalgebra of C generated by B and l. Moreover, setting $\mu := -n_C(l)$, the identities*

$$u(vl) = (vu)l, \tag{1}$$
$$(vl)u = (v\bar{u})l, \tag{2}$$
$$(ul)(vl) = \mu\bar{v}u, \tag{3}$$
$$n_C(u + vl) = n_C(u) - \mu n_C(v), \tag{4}$$
$$t_C(u + vl) = t_C(u), \tag{5}$$
$$\overline{u + vl} = \bar{u} - vl \tag{6}$$

hold for all $u, v \in B$, *and*

$$Bl = lB \subseteq B^{\perp}. \tag{7}$$

Proof The first assertion follows from (1)–(3), so it will be enough to establish (1)–(7). Since l is orthogonal to B and, in particular, has trace zero, (16.5.5) implies

$$u \circ l = t_C(u)l, \tag{8}$$

hence $lu = t_C(u)l - ul$, and we have (2) in the special case $v := 1_C$, i.e.,

$$lu = \bar{u}l. \tag{9}$$

Combining (9) with the linearized left alternative law (13.2.1) and (8), we conclude $u(vl) = u(l\bar{v}) = (u \circ l)\bar{v} - l(u\bar{v}) = t_C(u)l\bar{v} - l(u\bar{v}) = l(\bar{u}\,\bar{v}) = (vu)l$, since ι_C is an involution by Prop. 17.2 (a). Thus (1) holds. Reading (1) in C^{op} and invoking (8), (9) once more gives (2) in full generality. In order to establish (3), we combine the middle Moufang identity (13.3.3) with (17.4.2) and (9) to conclude $(ul)(vl) = (l\bar{u})(vl) = l(\bar{u}v)l = n_C(l, \bar{v}u)l - n_C(l)\bar{v}u = \mu\bar{v}u$, as claimed. Turning to (4), we use (16.12.4) to expand the left-hand side and obtain $n_C(u+vl) = n_C(u) + n_C(u, vl) + n_C(v)n_C(l) = n_C(u) + n_C(\bar{v}u, l) - \mu n_C(v) = n_C(u) - \mu n_C(v)$, and the proof of (4) is complete. It is now straightforward to verify (5), (6). Finally, turning to (7), we have $Bl = lB$ by (9) and note that C is norm-associative by Prop. 17.2 (a). Hence (16.12.4) yields $n_C(u, vl) = n_C(\bar{v}u, l) = 0$ for all $u, v \in B$, which implies $Bl \subseteq B^{\perp}$ and (7) holds. □

18.2 Remark. The above sum $B + Bl$ of k-submodules of C need *not* be direct. For example, it could happen that $0 \neq l \in \mathrm{Rad}(Dn_B) \subseteq B$.

18.3 The external Cayley-Dickson construction. We will now recast the preceding considerations on a more abstract, but also more general, level. Let B be any conic algebra over k and $\mu \in k$ an arbitrary scalar (playing the role of $-n_C(l)$ in Prop. 18.1). We define a k-algebra C on the direct sum $B \oplus Bj$ of two copies of B as a k-module by the multiplication

$$(u_1 + v_1 j)(u_2 + v_2 j) := (u_1u_2 + \mu\overline{v_2}v_1) + (v_2u_1 + v_1\overline{u_2})j,$$

for $u_i, v_i \in B$, $i = 1, 2$, and a quadratic form $n_C \colon C \to k$ by

$$n_C(u + vj) := n_B(u) - \mu n_B(v) \qquad (u, v \in B).$$

C together with n_C is said to arise from B, μ by means of the *Cayley-Dickson construction*, and is written as $\mathrm{Cay}(B, \mu)$ in order to indicate dependence on the parameters involved. Note that $1_C = 1_B + 0 \cdot j$ is an identity element for C and that the assignment $u \mapsto u + 0 \cdot j$ gives an *embedding*, i.e., an injective

homomorphism, $B \hookrightarrow C$ of unital k-algebras, allowing us to identify $B \subseteq C$ as a unital subalgebra.

18.4 Proposition. *Let B be a conic k-algebra and $\mu \in k$ an arbitrary scalar. Then $C = \mathrm{Cay}(B, \mu)$ as defined in 18.3 is a conic k-algebra whose algebra structure, unit element, norm, polarized norm, trace, conjugation relate to the corresponding objects belonging to B by the formulas*

$$(u_1 + v_1 j)(u_2 + v_2 j) = (u_1 u_2 + \mu \overline{v_2} v_1) + (v_2 u_1 + v_1 \overline{u_2}) j, \tag{1}$$

$$1_C = 1_B, \tag{2}$$

$$n_C(u + vj) = n_B(u) - \mu n_B(v), \tag{3}$$

$$n_C(u_1 + v_1 j, u_2 + v_2 j) = n_B(u_1, u_2) - \mu n_B(v_1, v_2), \tag{4}$$

$$t_C(u + vj) = t_B(u), \tag{5}$$

$$\iota_C(u + vj) = \overline{u + vj} = \bar{u} - vj \tag{6}$$

for all $u, u_i, v, v_i \in B$, $i = 1, 2$. In particular,

$$Bj = jB \subseteq B^{\perp}. \tag{7}$$

Proof (1)–(3) are simply repetitions of things stated in 18.3 and immediately imply (4). Hence $n_C(1_C, x) = t_B(u)$ for $x = u + vj$, $u, v \in B$, and from (1), (16.5.4), (16.5.1) we conclude

$$\begin{aligned} x^2 &= (u^2 + \mu n_B(v) 1_B) + t_B(u) vj = t_B(u)(u + vj) - (n_B(u) - \mu n_B(v)) 1_B \\ &= n_C(1_C, x)x - n_C(x) 1_C. \end{aligned}$$

Thus C is a conic k-algebra. (1)–(6) are now clear, while (7) follows directly from (1) and (4). □

18.5 Remark. In the situation of Prop. 18.4, the norm of the Cayley-Dickson construction $\mathrm{Cay}(B, \mu)$ may be written more concisely as

$$n_{\mathrm{Cay}(B,\mu)} = n_B \perp (-\mu) n_B = n_B \otimes \langle 1, -\mu \rangle.$$

18.6 The Cayley Dickson process. Since the Cayley-Dickson construction stabilizes the category of conic algebras, it can be iterated: given a conic algebra B over k and scalars $\mu_1, \ldots, \mu_n \in k$, we say that

$$\mathrm{Cay}(B; \mu_1, \mu_2, \ldots, \mu_n) := \mathrm{Cay}\Big(\ldots (\mathrm{Cay}\,(\mathrm{Cay}(B, \mu_1), \mu_2)) \ldots, \mu_n \Big).$$

arises from B and $\mu_1, \ldots, \mu_n$ by means of the *Cayley-Dickson process*.

Confronting the external Cayley-Dickson construction with the internal one as described in Prop. 18.1, one obtains the following useful result.

18.7 Proposition (Universal property of the Cayley-Dickson construction)**.** *Let $g\colon B \to C$ be a homomorphism of conic k-algebras and suppose in addition that C is multiplicative alternative. Given $l \in g(B)^\perp \subseteq C$ and setting $\mu := -n_C(l)$, there exists a unique extension of g to a homomorphism $h\colon \mathrm{Cay}(B,\mu) \to C$ of conic algebras over k sending j to $h(j) = l$. The image of h is the subalgebra of C generated by $g(B)$ and l, while its kernel has the form*

$$\mathrm{Ker}(h) = \{u + vj \mid u, v \in B, g(u) = -g(v)l\}.$$

Proof Any such h has the form $h(u + vj) = g(u) + g(v)l$ for $u, v \in B$. Conversely, defining h in this manner, we obtain $h(j) = l$ and deduce from (18.1.1)–(18.1.4) combined with (18.4.1) that h is a homomorphism of conic algebras. The remaining assertions are clear. □

Before we can proceed, we will have to insert an easy technicality.

18.8 Zero divisors of modules. Let M be a k-module. In accordance with Bourbaki [28, I, 8.1], an element $\mu \in k$ is called a *zero divisor* of M if the homothety $x \mapsto \mu x$ from M to M is not injective. We claim *that, if M is projective and contains unimodular elements, the zero divisors of M are precisely the zero divisors of k*. Indeed, since the injectivity of linear maps can be tested locally, we may assume that k is a local ring, in which case $M \neq \{0\}$ is free as a k-module, and the assertion follows.

18.9 Corollary. *Under the hypotheses of Proposition 18.7, assume that g is injective, B is projective as a k-module, n_B is weakly regular and μ is not a zero divisor of k. Then h is an isomorphism from* $\mathrm{Cay}(B,\mu)$ *onto the subalgebra of C generated by B and l.*

Proof We need only show that h is injective, so let $u, v \in B$ satisfy $u + vj \in \mathrm{Ker}(h)$. By Prop. 18.7 and (18.1.7), we have $g(u) = -g(v)l \in g(B) \cap g(B)^\perp$, forcing $g(u) = g(v)l = 0$ by weak regularity of n_B, and (18.1.3) yields $g(\mu v) = \mu g(v) = (g(v)l)l = 0$, hence $\mu v = 0$. But μ, not being a zero divisor of k, neither is one of B by 18.8 since $1_B \in B$ is unimodular by Prop. 16.7. Thus $v = 0$, as claimed. □

18.10 Examples. Considering the conic algebras of Chap. I over the field $k = \mathbb{R}$ of real numbers, we note that $i \in \mathbb{C}$ belongs to $(\mathbb{R}1_C)^\perp$ and has norm 1. Hence Cor. 18.9 yields a canonical identification $\mathbb{C} = \mathrm{Cay}(\mathbb{R}, -1)$. Similarly, identifying $\mathbb{C} = \mathbb{R}[\mathbf{i}]$ as a subalgebra of $\mathbb{H}$, the Hamiltonian quaternions, $\mathbf{j} \in \mathbb{H}$ belongs to $\mathbb{C}^\perp$ and again has norm 1, which implies $\mathbb{H} = \mathrm{Cay}(\mathbb{C}, -1) = \mathrm{Cay}(\mathbb{R}; -1, -1)$. And finally, viewing $\mathbb{H}$ via 1.11 as a subalgebra of $\mathbb{O}$, the Graves-Cayley octonions, and consulting (1.6.1), (1.6.2), we conclude that $j :=$

$0 \oplus (ie_1) \in \mathbb{H}^\perp \subseteq \mathbb{O}$ has norm 1. Therefore $\mathbb{O} = \mathrm{Cay}(\mathbb{H}, -1) = \mathrm{Cay}(\mathbb{C}; -1, -1) = \mathrm{Cay}(\mathbb{R}; -1, -1, -1)$.

Useful properties of conic algebras preserved by the Cayley-Dickson construction are in short supply. For instance, the property to be projective as a k-module trivially carries over from a conic algebra B to any Cayley-Dickson construction $\mathrm{Cay}(B, \mu)$, $\mu \in k$. Other examples are provided by the following result.

18.11 Proposition. *Let B be a conic algebra over k and $\mu \in k$. If the conjugation of B is an involution, then so is the conjugation of $C := \mathrm{Cay}(B, \mu)$. If B is norm-associative, then so is C.*

Proof The first part follows by a straightforward computation. As to the second, it suffices to verify (16.13.2), so we must show

$$n_C(u_1 + v_1 j, (u_1 + v_1 j)(u_2 + v_2 j)) = t_C(u_2 + v_2 j) n_C(u_1 + v_1 j)$$

for $u_i, v_i \in B$, $i = 1, 2$. To this end, one expands the left-hand side using (18.4.1), (18.4.4) and observes that (16.13.4) holds for B. Details are left to the reader. □

On the other hand, preserving flexibility under the Cayley-Dickson construction is only possible with a caveat.

18.12 Proposition. *For a conic k-algebra B and $\mu \in k$, the Cayley-Dickson construction $C = \mathrm{Cay}(B, \mu)$ is flexible if and only if B is flexible and the conjugation of B is an involution.*

Proof Suppose first that C is flexible. Then B is flexible and (16.10.1) holds for all $x, y \in C$. In particular, for $u_1, u_2, v_1 \in B$, we set $x := u_1 + v_1 j$, $y := u_2$ and conclude that

$$\begin{aligned}(t_C(x, y) - n_C(x, \bar{y}))x &= (t_C((u_1 + v_1 j)u_2) - n_C(u_1 + v_1 j, \bar{u}_2))(u_1 + v_1 j) \\ &= \Big(t_B(u_1 u_2 + (v_1 \bar{u}_2) j) - n_B(u_1, \bar{u}_2)\Big)(u_1 + v_1 j) \\ &= (t_B(u_1, u_2) - n_B(u_1, \bar{u}_2))(u_1 + v_1 j),\end{aligned}$$

belongs to $k1_B \subseteq B$. Comparing Bj-components, we find that $t_B(u_1, u_2) - n_B(u_1, \bar{u}_2) \in \mathrm{Ann}(B)$, whence the conjugation of B is an involution by Prop. 16.10 (a).

Conversely, suppose B is flexible and its conjugation is an involution. Then, by Prop. 18.11, the conjugation of C is an involution, and we deduce from Cor. 16.11 that it suffices to show

$$n_C(x, xy) - t_C(y) n_C(x) \in \mathrm{Ann}(C)$$

for all $x, y \in C$. By linearity (in y), assuming $x = u_1 + v_1 j$ with $u_1, v_1 \in B$, we are left with two cases $y \in B$ or $y \in Bj$.

Suppose first that $y = u_2 \in B$. Then

$$\begin{aligned} n_C(x, xy) - t_C(y)n_C(x) &= n_C(u_1 + v_1 j, u_1 u_2 + (v_1 \bar{u}_2) j) - t_B(u_2) n_C(u_1 + v_1 j) \\ &= n_B(u_1, u_1 u_2) - \mu n_B(v_1, v_1 \bar{u}_2) \\ &\quad - t_B(u_2) n_B(u_1) + \mu t_B(u_2) n_B(v_1) \\ &= \big(n_B(u_1, u_1 u_2) - t_B(u_2) n_B(u_1)\big) \\ &\quad - \mu\big(n_B(v_1, v_1 \bar{u}_2) - t_B(\bar{u}_2) n_B(v_1)\big), \end{aligned}$$

where both summands on the right by the hypotheses on B and Cor. 16.11 belong to $\mathrm{Ann}(B) = \mathrm{Ann}(C)$. Hence so does $n_C(x, xy) - t_C(y)n_C(x)$.

Suppose now that $y = v_2 j$, $v_2 \in B$. Then

$$\begin{aligned} n_C(x, xy) - t_C(y)n_C(x) &= n_C\big(u_1 + v_1 j, \mu \bar{v}_2 v_1 + (v_2 u_1) j\big) \\ &= \mu\big(n_B(\bar{v}_2 v_1, u_1) - n_B(v_1, v_2 u_1)\big). \end{aligned}$$

It therefore remains to show $n_B(u, vw) - n_B(\bar{v}u, w) \in \mathrm{Ann}(B)$ for all $u, v, w \in B$. Since B^{op} is a flexible conic algebra whose conjugation is an involution, Cor. 16.11 implies $n_B(u, vu) - t_B(v)n_B(u) \in \mathrm{Ann}(B)$, so after linearization, $\mathrm{Ann}(B)$ contains $n_B(u, vw) + n_B(w, vu) - t_B(v)n_B(u, w) = n_B(u, vw) - n_B(\bar{v}u, w)$, as desired. □

18.13 Commutators and associators. Let B be a conic algebra over k. For $\mu \in k$, we wish to find conditions that are necessary and sufficient for the Cayley-Dickson construction $C = \mathrm{Cay}(B, \mu)$ to be commutative, associative, alternative, respectively. To this end, we will describe the commutator and the associator of C in terms of B and μ *under the assumption that, in case of the associator, the conjugation of B is an involution*. Then, letting $u_i, v_i \in B$, $i = 1, 2, 3$ and keeping the notation of 18.3, a lengthy but straightforward computation yields

$$\begin{aligned} [u_1 + v_1 j, u_2 + v_2 j] &= u + v j, \text{ and} \\ [u_1 + v_1 j, u_2 + v_2 j, u_3 + v_3 j] &= \tilde{u} + \tilde{v} j, \end{aligned}$$

where

$$u = [u_1, u_2] + \mu(\overline{v_2}v_1 - \overline{v_1}v_2), \tag{1}$$

$$v = v_2(u_1 - \overline{u_1}) - v_1(u_2 - \overline{u_2}), \tag{2}$$

$$\begin{aligned}\tilde{u} = {} & [u_1, u_2, u_3] + \mu((\overline{v_2}v_1)u_3 - (u_3\overline{v_2})v_1 + \\ & \overline{v_3}(v_2u_1) + \overline{v_3}(v_1\overline{u_2}) - u_1(\overline{v_3}v_2) - (\overline{u_2}\,\overline{v_3})v_1),\end{aligned} \tag{3}$$

$$\begin{aligned}\tilde{v} = {} & v_3(u_1u_2) - (v_3u_2)u_1 + (v_2u_1)\overline{u_3} + (v_1\overline{u_2})\overline{u_3} \\ & - (v_2\overline{u_3})u_1 - v_1(\overline{u_3}\,\overline{u_2}) + \mu(v_3(\overline{v_2}v_1) - v_1(\overline{v_2}v_3)).\end{aligned} \tag{4}$$

With the aid of these identities, we can now prove the following important result.

18.14 Theorem. *For a conic k-algebra B, an arbitrary scalar $\mu \in k$ and the corresponding Cayley-Dickson construction $C := \mathrm{Cay}(B, \mu)$, the following statements hold.*

(a) *C is commutative if and only if B is commutative and has trivial conjugation.*

(b) *C is associative if and only if B is commutative associative and its conjugation is an involution.*

(c) *C is alternative if and only if B is associative and its conjugation is an involution.*

Proof (a) If C is commutative, then so is B and (18.13.2) for $v_2 = 1_B, v_1 = 0$ implies $\iota_B = \mathbf{1}_B$. Conversely, let B be commutative and suppose $\iota_B = \mathbf{1}_B$. Then an inspection of (18.13.1), (18.13.2) shows that C is commutative as well.

(b) If C is associative, then so is B, its conjugation is an involution by Prop. 18.12, and (18.13.4) for $u_3 = v_1 = v_2 = 0, v_3 = 1_C$ shows that B is commutative as well. Conversely, if B is commutative associative and its conjugation is an involution, an inspection of (18.13.3), (18.13.4) shows that C is associative.

(c) If C is alternative, then the conjugation of B by Prop. 18.12 is an involution. Moreover, $\tilde{v} = 0$ for $u_1 = u_2$, $v_1 = v_2$, $v_3 = 0$ and (18.13.4) combined with (16.5.4) yield

$$\begin{aligned}0 &= (v_1u_1)\overline{u_3} + (v_1\overline{u_1})\overline{u_3} - (v_1\overline{u_3})u_1 - v_1(\overline{u_3}\,\overline{u_1}) \\ &= t_B(u_1)v_1\overline{u_3} - (v_1\overline{u_3})u_1 - t_B(u_1)v_1\overline{u_3} + v_1(\overline{u_3}u_1) \\ &= -[v_1, \overline{u_3}, u_1].\end{aligned}$$

Hence B is associative. Conversely, let this be so and suppose ι_B is an involution. Setting $u_1 = u_2, v_1 = v_2$ in (18.13.3), (18.13.4), Kirmse's identities

(17.4.1) and (16.5.4), (16.5.6) imply

$$\tilde{u} = \mu(n_B(v_1)u_3 - n_B(v_1)u_3 + t_B(u_1)\overline{v_3}v_1 - t_B(u_1)\overline{v_3}v_1) = 0,$$
$$\tilde{v} = t_B(u_1)v_1\overline{u_3} - t_B(u_1)v_1\overline{u_3} + \mu(n_B(v_1)v_3 - n_B(v_1)v_3) = 0,$$

forcing C to be alternative. □

18.15 Corollary. *In addition to the above, assume that B is projective as a k-module. Then*

(a) *C is associative if and only if B is commutative associative.*
(b) *C is alternative if and only if B is associative.*

Proof All the algebras of Thm. 18.14 are flexible. Hence in each case Proposition 16.14 shows that the hypothesis of the conjugation of B being an involution is automatic. □

18.16 Remark. Different characterizations of alternativity (resp. associativity or commutativity) for algebras arising from the Cayley-Dickson construction may be found in [189, Thm. 6.8] and [190, II, Thm. 2.5.2].

18.17 Examples. (a) Let R be a quadratic k-algebra whose conjugation is non-trivial. For any $\mu_1 \in k$, Cor. 18.15 (a) combined with Theorem 18.14 (a) shows that the conic algebra $B := \mathrm{Cay}(R, \mu_1)$ is associative but not commutative. Applying Cor. 18.15 again, we therefore conclude for any $\mu_2 \in k$ that the conic algebra $C := \mathrm{Cay}(B, \mu_2) = \mathrm{Cay}(R; \mu_1, \mu_2)$ is alternative but not associative. In view of Example 18.10, these results generalize what we have found in Exc. 1.16 combined with Cor. 1.12.

(b) At the other extreme, assume $2 = 0$ in k. If B is a commutative associative conic k-algebra with trivial conjugation (e.g., $B = k$), then by Theorem 18.14 and (18.4.6) so is the Cayley-Dickson process $C := \mathrm{Cay}(B; \mu_1, \ldots, \mu_n)$, for any positive integer n and any $\mu_1, \ldots, \mu_n \in k$.

Exercises

18.18. Let B be a multiplicative conic algebra over k and $\mu \in k$. Show that the Cayley-Dickson construction $\mathrm{Cay}(B, \mu)$ is multiplicative if and only if $\mu[B, B, B] \subseteq \mathrm{Rad}(Dn_B)$.

18.19 (McCrimmon [189, p. 103])**.** Let B be a multiplicative conic k-algebra, and let $\mu \in k$, $a \in \mathrm{Nuc}(B)$. Show that the map

$$\varphi\colon\ \mathrm{Cay}\,(B, n_B(a)\mu) \longrightarrow \mathrm{Cay}(B, \mu)$$

defined by $\varphi(u + vj) := u + (av)j$ for $u, v \in B$ is a homomorphism of conic algebras. Moreover, it is an isomorphism if and only if a is invertible in $\mathrm{Nuc}(B)$.

18.20. *Zero divisors of algebras*. Let A be a k-algebra. An element $x \in A$ is called a *right* (resp. *left*) *zero divisor* of A if the left (resp. right) multiplication operator $L_x\colon A \to A$ (resp. $R_x : A \to A$) of x in A is *not* injective. We say A has *zero divisors* if there are non-zero elements $x, y \in A$ such that $xy = 0$.

Now let C be a conic alternative k-algebra that is projective as a k-module. Prove for $x \in C$ that the following conditions are equivalent.

(i) x is a right zero divisor of C.
(ii) x is a left zero divisor of C.
(iii) $n_C(x)$ is a zero divisor of k.

(*Hint*: For the implication (i) $\Rightarrow$ (iii), argue indirectly and pass to the base change $C_f = C \otimes k_f, f = n_C(x)$.)

18.21. Let A be a nonassociative k-algebra. For $R = k[\mathbf{t}]$ or $k[[\mathbf{t}]]$ prove: A has zero divisors if and only if A_R has zero divisors.

18.22. *A variant of the Cayley-Dickson construction.* Let B be a conic k-algebra and $\mu \in k$. On the direct sum $B \oplus j'B$ of two copies of B as a k-module we define a k-algebra structure $\mathrm{Cay}'(B, \mu)$ by the formula

$$(u_1 + j'v_1)(u_2 + j'v_2) := (u_1u_2 + \mu v_2\bar{v}_1) + j'(\bar{u}_1v_2 + u_2v_1)$$

for $u_1, u_2, v_1, v_2 \in B$. Show that there is a natural isomorphism

$$\mathrm{Cay}(B^{\mathrm{op}}, \mu) \cong \mathrm{Cay}'(B, \mu)^{\mathrm{op}}$$

and conclude that $\mathrm{Cay}'(B, \mu)$ is a conic k-algebra with norm, trace and conjugation canonically isomorphic to the corresponding objects attached to $\mathrm{Cay}(B, \mu)$. Show further that, if the conjugation of B is an involution, then

$$\mathrm{Cay}(B, \mu) \xrightarrow{\sim} \mathrm{Cay}'(B, \mu), \quad u + vj \longmapsto u + j'\bar{v},$$

is an isomorphism of conic algebras.

19 Basic properties of composition algebras

Before being able to deal with the main topic of this section, it will be necessary to introduce an auxiliary notion that can hardly stand on its own but turns out to be technically useful. Throughout, we let k be an arbitrary commutative ring.

19.1 Pre-composition algebras. By a *pre-composition algebra* over k we mean a k-algebra C satisfying the following conditions.

(i) C is unital.
(ii) C is projective as a k-module.

(iii) There exists a non-degenerate quadratic form $n\colon C \to k$ that *permits composition*:

$$n(1_C) = 1, \tag{1}$$
$$n(xy) = n(x)n(y) \qquad (x, y \in C). \tag{2}$$

In this case, (2) may be linearized (repeatedly) and yields the relations

$$n(xy, xz) = n(x)n(y, z), \tag{3}$$
$$n(xy, zy) = n(x, z)n(y), \tag{4}$$
$$n(xy, wz) + n(wy, xz) = n(x, w)n(y, z) \tag{5}$$

for all $x, y, z, w \in C$.

19.2 Examples. Let $k := \mathbb{R}$ be the field of real numbers and $\mathbb{D}$ as in 3.1 (b) one of the subalgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ of the Graves-Cayley octonions $\mathbb{O}$. Let $M \subseteq \mathbb{D}$ be an arbitrary $\mathbb{Z}$-structure as defined in 3.6 (d). The property of the norm $n_{\mathbb{D}}$ of $\mathbb{D}$ to be positive definite and to permit composition is inherited by its restriction to M. Thus M is a pre-composition algebra over $\mathbb{Z}$. It follows in particular that the Gaussian integers $\mathrm{Ga}(\mathbb{C})$, $\mathrm{Ga}(\mathbb{H})$, $\mathrm{Ga}(\mathbb{O})$ of 3.16 are pre-composition algebras over $\mathbb{Z}$, as are the Hurwitz quaternions (Thm. 4.2) and the Dickson-Coxeter octonions (Thm. 4.5).

An analogous conclusion could have been drawn for the algebras $\mathbb{D}$ over $\mathbb{R}$ but in this case, as will be seen in a moment, one can do better than that.

In view of Prop. 17.6, conic alternative algebras that are projective as k-modules are pre-composition algebras provided their norm is a non-degenerate quadratic form. Remarkably, the converse of this is also true.

19.3 Proposition. *Let C be a pre-composition algebra over k and $n\colon C \to k$ any non-degenerate quadratic form that permits composition. Then C is a conic alternative k-algebra with unique norm $n_C = n$. Moreover,*

$$C^\perp := \mathrm{Rad}(Dn_C) = \{x \in C \mid n_C(x, y) = 0 \text{ for all } y \in C\} \subseteq \mathrm{Cent}(C)$$

is a central ideal of C satisfying

$$2C^\perp = n_C(x, y)C^\perp = \{0\}$$

for all $x, y \in C$.

Proof For the first part, it suffices to show that C is a conic alternative algebra with norm $n_C := n$ since uniqueness follows from Proposition 16.16. By (19.1.1), we have $n(1_C) = 1$. Now we put $z = 1_C$ in (19.1.3). Then

$$n(xy, x) = n(x)t(y), \tag{1}$$

where $t(y) := n(1_C, y)$. Setting $y = x, w = z = 1_C$ in (19.1.5), we obtain $t(x^2) + n(x, x) = t(x)^2$, hence

$$t(x^2) = t(x)^2 - 2n(x). \tag{2}$$

Furthermore, setting $z = x, w = 1_C$ in (19.1.5), we also obtain $n(xy, x) + n(x^2, y) = t(x)n(x, y)$, so by (1),

$$n(x^2 - t(x)x + n(x)1_C, y) = 0.$$

Similarly, one can show $n(x^2 - t(x)x + n(x)1_C) = 0$ by expanding the left-hand side and using (1) (for $y = x$) as well as (2). Since n is non-degenerate, C is therefore a conic k-algebra with norm $n_C = n$. Moreover, (1) shows that C is norm-associative, hence flexible by Proposition 16.14. Thus alternativity will follow once we have established the left alternative law, equivalently, the first of Kirmse's identities (17.4.1). To this end, we combine (16.12.4) with (19.1.3) and the multiplicativity of n to obtain $n(x(\overline{x}y), z)) = n(\overline{x}y, \overline{x}z) = n(n(x)y, z)$. A similar computation yields $n(x(\overline{x}y) - n(x)y) = 0$. The fact that n is non-degenerate implies the first Kirmse identity $x(\overline{x}y) = n(x)y$, as claimed.

We now turn to $C^\perp$. By non-degeneracy of n, the function $n\colon C^\perp \to k$ is an embedding of additive groups. In particular, $n(2x) = 2n(x, x) = 0$ for $x \in C^\perp$ implies $2C^\perp = \{0\}$. Moreover, (16.12.3) and (16.12.4) show that $C^\perp \subseteq C$ is an ideal. We claim that this ideal belongs to the centre of C. Indeed, for $x, y \in C, z \in C^\perp$, evaluating n at $(xy)z, x(yz) \in C^\perp$ yields the same value $n(x)n(y)n(z)$, which implies $[x, y, z] = 0$. Similarly, $[y, z] = 0$, and the assertion follows. It remains to prove $n(x, y)z = 0$. Since the conjugation of C is the identity on $C^\perp$, this follows from (16.12.5) and $n(x, y)z = t(x\overline{y})z = (x\overline{y})z + (y\overline{x})z = (zx)\overline{y} + y\overline{zx} = n(zx, y)1_C = 0$. □

19.4 Example. Let $K \supseteq k$ be fields of characteristic 2, with K purely inseparable of exponent at most 1, meaning that $K^2 \subseteq k$. (We allow the dimension $[K : k]$ to be infinite.) Then K is a pre-composition algebra over k whose norm, given by the squaring $K \to k, x \mapsto x^2$, is an anisotropic quadratic form with zero bilinearization.

If $K \neq k$, then there is some $\alpha \in K \setminus k$,

$$K \otimes K \supseteq K \otimes k[\alpha] \cong K[\mathbf{t}]/(\mathbf{t}^2 - \alpha^2) \cong K[\mathbf{t}]/(\mathbf{t} - \alpha)^2 \cong K[\varepsilon]/(\varepsilon^2),$$

and $n_K \otimes K$ is isotropic, hence degenerate. That is, *the corresponding scalar extension of the k-algebra K is not a pre-composition algebra anymore.*

We are now ready for the main concept of this section.

19.5 The concept of a composition algebra. We define a *composition algebra* over k as a k-algebra C satisfying the following conditions.

(i) C is unital.

(ii) C is projective as a k-module.

(iii) The rank function $\mathfrak{p} \mapsto \mathrm{rk}(C_{\mathfrak{p}})$ from $\mathrm{Spec}(k)$ to $\mathbb{N} \cup \{\infty\}$ is locally constant with respect to the Zariski topology of $\mathrm{Spec}(k)$.

(iv) There exists a non-singular quadratic form $n\colon C \to k$ that permits composition:

$$n(1_C) = 1, \tag{1}$$

$$n(xy) = n(x)n(y) \qquad (x, y \in C). \tag{2}$$

If the quadratic form in (iv) can be chosen to be regular (rather than just non-singular), we speak of a *regular* composition algebra. We will see later (Cor. 19.11) that requiring a composition algebra to be regular is a mild extra condition. Note further that among the preceding conditions, (ii) implies (iii) if C is finitely generated as a k-module (9.8).

19.6 Example: the base ring. The only quadratic form permitting composition on the k-algebra k is the squaring $\alpha \mapsto \alpha^2$, i.e., the norm of k (as a conic algebra, see Example 16.2 (c)), which is obviously non-singular. Hence k is a composition algebra over itself. It is a regular composition algebra if and only if $2 \in k^\times$.

On the other hand, k is a pre-composition algebra if and only if, for all $\alpha \in k$, the relations $\alpha^2 = 2\alpha = 0$ imply $\alpha = 0$, which fails to be the case if, e.g., k contains non-zero nilpotent elements and $2 = 0$ in k.

19.7 Remark. (a) Composition algebras are stable under base change (since non-singular quadratic forms are), while pre-composition algebras are not (Example 19.4). This is the main reason why the latter are less interesting than the former. In case k is the zero ring, the unique module — the zero module — is a composition algebra, albeit a rather uninteresting one.

(b) If C is a (regular, resp. a pre-) composition algebra, then so is C^{op}.

(c) Regular composition algebras are pre-composition algebras; in particular, they are conic alternative (Prop. 19.3). But, as Example 19.6 shows, arbitrary composition algebras may fail to be pre-composition algebras.

(d) There is no universal agreement in the literature on how to define composition algebras. Some authors, e.g., [92, 95, 212, 216, 270], require a *regular* quadratic form permitting composition and thus exclude the base ring from

counting as a composition algebra unless 2 is invertible (Example 19.6). Others, e.g., [70, 160], do not insist on an identity element, in which case composition algebras that contain one are called *Hurwitz algebras*. In some cases, e.g., in [189, 242], what we call pre-composition algebras are called composition algebras.

We now proceed by characterizing a class of composition algebras sitting inside arbitrary conic algebras as "small" unital subalgebras.

19.8 Proposition. *Let C be a conic algebra over k and $u \in C$. Then $D := k[u] \subseteq C$ is a unital commutative associative subalgebra and the following conditions are equivalent.*

(i) *D is a regular composition algebra of rank 2.*

(ii) *D is free of rank 2 as a k-module with basis $(1_C, u)$, and the quadratic form n_C is regular on D.*

(iii) $t_C(u)^2 - 4n_C(u) \in k^\times$.

In this case,

$$\operatorname{disc}((D, n_D)) = (t_C(u)^2 - 4n_C(u)) \bmod k^{\times 2} \tag{1}$$

is the discriminant of the quadratic space (D, n_D).

Proof Since conic algebras are power-associative by 16.5, the first part is clear.

(i) $\Leftrightarrow$ (ii). Suppose (i) holds. Since D is a finitely generated projective k-module of rank 2, the natural surjection $k^2 \to D$ determined by the elements $1_C, u$ must be a bijection (Exc. 9.30), giving the first part of (ii). As to the second, D is a pre-composition algebra, hence a conic one, so n_C by Prop. 19.3 restricts to the unique non-degenerate (actually, regular) quadratic form on D permitting composition. Conversely, (i) is a consequence of (ii) by Exc. 16.18 (a).

(ii) $\Leftrightarrow$ (iii). Since D is flexible, (ii) combined with Prop. 16.14 implies that it is norm-associative, so by (16.12.5) the bilinear trace $t_D = t_C|_{D\times D}$ is regular along with $n_D = n_C|_{D\times D}$. Computing the determinant of Dn_D relative to the basis $(1_D, u)$ of D, we obtain

$$\begin{aligned} \det\begin{pmatrix} n_C(1_C, 1_c) & n_C(1_C, u) \\ n_C(u, 1_C) & n_C(u, u) \end{pmatrix} &= \det\begin{pmatrix} 2 & t_C(u) \\ t_C(u) & 2n_C(u) \end{pmatrix} \\ &= 4n_C(u) - t_C(u)^2, \end{aligned} \tag{2}$$

hence (iii), and the formula for the discriminant. Conversely, if (iii) holds, it suffices to show that $1_C, u$ are linearly independent over k, so suppose $\alpha, \beta \in k$

satisfy the relation $\alpha 1_C + \beta u = 0$. Then $\alpha u + \beta u^2 = 0$, and taking traces we conclude

$$\begin{pmatrix} 2 & t_C(u) \\ t_C(u) & t_C(u)^2 - 2n_C(u) \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} t_C(1_C) & t_C(u) \\ t_C(u) & t_C(u^2) \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0.$$

But by (iii) the matrix on the very left is invertible, forcing $\alpha = \beta = 0$, as desired. □

19.9 Proposition (Kaplansky [149])**.** *If F is a field, an F-algebra C is a pre-composition algebra if and only if it is either a (finite-dimensional) regular composition algebra or a purely inseparable field extension of characteristic* 2 *and exponent at most* 1.

Proof In view of Example 19.4, we only have to prove that a pre-composition algebra C over F has the form indicated in the proposition. Adopting the notation of Prop. 19.3, we first assume $C^\perp \neq \{0\}$. Since $2C^\perp = \{0\}$ and $C^\perp$ is a central ideal of C whose non-zero elements, by non-degeneracy, are anisotropic relative to n_C, hence invertible in C (Prop. 17.5), we conclude that F has characteristic 2 and $K := C = C^\perp = \mathrm{Cent}(C)$ is an extension field of F whose trace (in its capacity as a conic algebra) vanishes identically. Thus K is a purely inseparable extension of F of exponent ≤ 1.

We are left with the case $C^\perp = \{0\}$, so n_C is weakly regular. It suffices to show that C is finite-dimensional. Our first aim will be to exhibit a unital subalgebra $D \subseteq C$ of dimension at most 2 on which n_C is regular. For $\mathrm{char}(F) \neq 2$, $D := F1_C$ will do, so suppose $\mathrm{char}(F) = 2$. Then weak regularity of n_C produces an element $u \in C$ of trace 1, and Prop. 19.8 shows that $D := F[u] \subseteq C$ is a subalgebra of the desired kind. Now let $B \subset C$ be any proper unital subalgebra of finite dimension on which n_C is regular. Then $C = B \oplus B^\perp$ by Lemma 11.10, and since n_C is weakly regular on C, we find an anisotropic vector $l \in B^\perp$. But C is a conic alternative F-algebra, so Cor. 18.9 leads to an embedding $\mathrm{Cay}(B, \mu) \hookrightarrow C$, $\mu = -n_C(l) \in F^\times$, whose image continues to be a unital subalgebra of C on which n_C is non-degenerate. Assuming C were infinite-dimensional and starting from D, we could repeat this procedure at most four times (Cor. 18.15) and would then arrive at a subalgebra of C that is no longer alternative. This contradiction to Prop. 19.3 shows that C is indeed finite-dimensional. □

19.10 Remark. The preceding proof actually yields more than is claimed in the proposition. But since the situation described here will soon be re-examined in the more general set-up of LG rings, we see no point at this stage to state this additional piece of information explicitly.

19.11 Corollary. *Let C be a composition algebra over k. Then C is finitely generated as a k-module. If C has constant rank r, then C is either regular, or $r = 1$ (i.e., $C \cong k$) and 2 is not invertible in k.*

Proof We first assume that k is a local ring with maximal ideal $\mathfrak{m}$. Then $C(\mathfrak{m})$ is a composition algebra, hence also a pre-composition algebra, over the field $k(\mathfrak{m})$ and thus, by Prop. 19.9 combined with Example 19.4, is either regular of finite dimension or one-dimensional of characteristic 2. It follows that C is a regular composition algebra (of finite rank) over k or has rank 1 with 2 not invertible in k.

For general k, we deduce that C is finitely generated from the local case, condition (iii) in the definition of a composition algebra (19.5), and Lemma 9.9. The remaining assertions of the proposition follow easily from the local case. □

19.12 Corollary. *If k is a ring with no non-zero nilpotent elements, then every composition algebra over k is a pre-composition algebra.*

Proof Suppose C is a composition algebra over k. Trivially, we may assume that C is of finite constant rank and not regular. The preceding corollary then implies that $C = k$ and 2 is not invertible in k. Therefore, $\mathrm{Rad}(n_C)$ consists of elements of k of square zero, so $\mathrm{Rad}(n_C) = 0$ and C is a pre-composition algebra. □

19.13 Theorem. *A k-algebra C is a composition algebra (resp. a regular composition algebra) if and only if it is a conic alternative algebra which is finitely generated projective as a k-module and has a non-singular (resp. regular) norm. In this case, the norm n_C (cf. Prop. 16.16) is the only non-singular quadratic form on C permitting composition.*

Proof A conic alternative algebra that is finitely generated projective as a k-module and has a non-singular (resp. regular) norm is a composition algebra (resp. a regular composition algebra) by Prop. 17.6. Conversely, let C be a composition algebra and $n\colon C \to k$ a non-singular quadratic form permitting composition. By Cor. 19.11, it suffices to show that C is conic alternative with norm $n_C = n$. By Prop. 19.3, we are done if C is a pre-composition algebra. Otherwise, C is a non-regular composition algebra. Since C is a finitely generated projective k-module, by Cor. 19.11, we may invoke the rank decomposition of Exc. 9.31 to assume that C has constant rank $r \in \mathbb{N}$, whence Cor. 19.11 again combined with Example 19.6 shows $C \cong k$ and $n \cong n_k$. □

In order to keep track of the logical interdependence between the various

classes of conic algebras introduced in the present section and the preceding ones, the reader may consult Figure 19a.

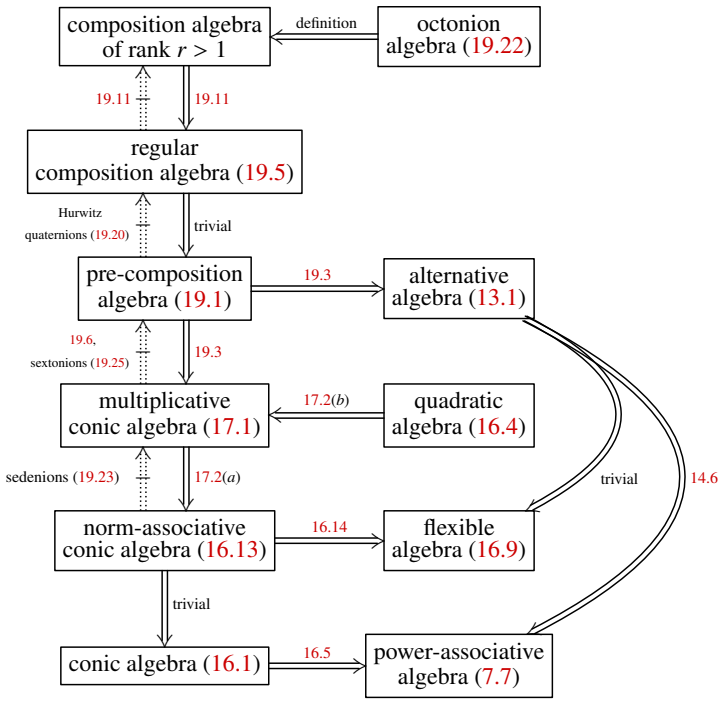


Figure 19a Diagram showing logical interdependence between different kinds of algebras related to composition algebras.

A more detailed understanding of composition algebras will now be obtained by exposing them to the Cayley-Dickson construction.

19.14 Theorem. *Let B be a conic k-algebra and $\mu \in k$ an arbitrary scalar. Then $C = \mathrm{Cay}(B, \mu)$ is a composition algebra if and only if B is a regular associative composition algebra and μ is invertible in k. In this case, C is a regular composition algebra as well.*

Proof Assume first that B is a regular associative composition algebra and $\mu \in k$ is a unit. Then B is conic associative by Thm. 19.13, forcing C to be conic alternative by Cor. 18.15 and $n_C \cong n_B \perp (-\mu)n_B$ (by (18.5)) to be a regular quadratic form. By Cor. 19.11 and Thm. 19.13, therefore, C is a regular composition algebra. Conversely, assume that C is a composition algebra. Since C is conic alternative by Thm. 19.13, B is conic associative

by Cor. 18.15. Furthermore, for every field $K \in k$-**alg**, the decomposition $(n_C)_K \cong (n_B)_K \perp (-\mu_K)(n_B)_K$ combines with the non-degeneracy of $(n_C)_K$ to show that $(n_B)_K$ is non-degenerate as well and $\mu_K \neq 0$. Hence B is a composition algebra, and specializing $K = k(\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$ implies $\mu \in k^\times$. It remains to prove that B is regular. Otherwise, $B_\mathfrak{p}$ would be a non-regular composition algebra over $k_\mathfrak{p}$, for some $\mathfrak{p} \in \operatorname{Spec}(k)$, forcing $C_\mathfrak{p}$ to be a non-regular composition algebra as well. But then Cor. 19.11 implies that $C_\mathfrak{p}$ has rank 1, a contradiction. □

Before exploiting the Cayley-Dickson construction still further, it is advisable to insert a technicality.

19.15 Lemma. *The linear trace of a regular composition algebra is surjective. Up to isomorphism, the only composition algebra over k having trivial conjugation is k itself.*

Proof For the first part, we combine regularity of the bilinear trace with unimodularity of the identity to find an element of trace 1 in C. For the second part, we let C be a composition algebra over k with trivial conjugation. Localizing if necessary, we may assume by Cor. 19.11 that C is regular. Then the assertion follows from the first part combined with Prop. 16.7 and Exc. 16.27. □

Our next aim will be to show that, under suitable conditions on k, all composition algebras arise from composition algebras of rank 2 by means of the Cayley-Dickson process. For this purpose, we return to the setting of LG rings from 11.20.

19.16 Theorem. *Let k be an LG ring and C a composition algebra of rank r over k.*

(a) *If $B \subseteq C$ is a regular composition subalgebra of rank $s < r$, there exists a unit $\mu \in k^\times$ such that the inclusion $B \hookrightarrow C$ extends to an embedding $\operatorname{Cay}(B, \mu) \to C$.*

(b) *If $r > 1$, then C contains a regular composition subalgebra of rank 2.*

Proof (a) Since n_C is regular on B, Lemma 11.10 yields an orthogonal splitting $C = B \perp B^\perp$, and the assumption $s < r$ implies that $(B^\perp, n_C|_{B^\perp})$ is a quadratic space over k having $B^\perp_\mathfrak{p} \neq \{0\}$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Thus, by Lemma 11.26, there exists an element $l \in B^\perp$ satisfying $\mu := -n_C(l) \in k^\times$. Now Cor. 18.9 implies (a).

(b) Prop. 19.8 shows that the existence of such a rank 2 subalgebra follows from the existence of $u \in C$ such that $t_C(u)^2 - 4n_C(u) \in k^\times$. Because C has constant rank r and k is LG, C is a free module (Prop. 11.24) and the function

$u \mapsto t_C(u)^2 - 4n_C(u)$ can be expressed as a polynomial in r variables with coefficients in k. The definition of LG ring reduces us to verifying that this polynomial represents a unit when k is a field, i.e., it suffices to prove (b) in the case where k is a field.

If k is a field of characteristic $\neq 2$, then k is a regular composition subalgebra of C and (a) produces a rank 2 subalgebra, which is regular by Thm. 19.14.

Finally, suppose k is a field of characteristic $= 2$. Since C is regular, there is a $u \in C$ with $t_C(u) = 1$, so $t_C(u)^2 - 4n_C(u) = 1 \in k^\times$. □

19.17 Corollary. *Every composition algebra of rank > 1 over an LG ring arises from a composition algebra of rank 2, and even from the base ring itself if 2 is a unit, by an application of the Cayley-Dickson process.* □

The preceding theorem has important consequences also in the case when the base ring is arbitrary.

19.18 Corollary (cf. Legrand [170])**.** *Let C be a composition algebra of rank r over k and assume $k \neq \{0\}$. Then $r = 1, 2, 4$ or 8 and the following statements hold.*

(a) *If $r = 1$, then $C \cong k$.*

(b) *If $r = 2$, then C is commutative associative and has non-trivial conjugation.*

(c) *If $r = 4$, then C is associative but not commutative.*

(d) *If $r = 8$, then C is alternative but not associative.*

Proof We conclude from Cor. 19.17 that $r = 2^s$ is a power of 2. Localizing whenever necessary, (a)–(d) now follow by a straightforward combined application of Cor. 19.11, Lemma 19.15 and Thms. 19.14, 19.16, 18.14. Finally, Thm. 19.13 and Cor. 18.15 show that $s > 3$ is impossible. □

Composition algebras of rank 1 are of course trivial. We conclude this section by taking a closer look at the remaining cases collected in Cor. 19.18.

19.19 Quadratic étale algebras. Let D be a unital commutative associative k-algebra that is finitely generated projective as a k-module. Then the following conditions are easily seen (and well known) to be equivalent.

(i) For all maximal ideals $\mathfrak{m} \subseteq k$, the algebra $D(\mathfrak{m})$ over the field $k(\mathfrak{m}) = k/\mathfrak{m}$ may be written as a (finite) direct product of (finite) separable field extensions.

(ii) For all prime ideals $\mathfrak{p} \subseteq k$, the $k(\mathfrak{p})$-algebra $D(\mathfrak{p})$ may be written as a (finite) direct product of (finite) separable field extensions.

(iii) The bilinear trace $D \times D \to k, (x, y) \mapsto \mathrm{tr}(L_{xy})$, L being the left multiplication of D, is a regular symmetric bilinear form.

If these conditions are fulfilled, D is said to be *finite étale* (or *separable*) over k. If, in addition, D has rank 2 as a finitely generated projective k-module, we speak of a *quadratic étale k-algebra*. Comparing (iii) with (16.12.5), 16.4 and Cor. 19.18, we see that being a quadratic étale k-algebra and a composition algebra over k of rank 2 are equivalent notions; therefore these terms will henceforth be used interchangeably.

Typical examples of quadratic étale k-algebras arise as follows.

(iv) Let $\lambda \in k$ and $D := k[\mathbf{t}]/(\mathbf{t}^2 - \mathbf{t} + \lambda) = k[u]$, where u, the canonical image of $\mathbf{t}$ in D, has trace 1 and norm λ. Then D is free of rank 2 as a k-module, with basis $1_D, u$, hence a quadratic k-algebra whose norm satisfies $n_D(\alpha 1_D + \beta u) = \alpha^2 + \alpha\beta + \lambda\beta^2$ for all $\alpha, \beta \in k$. By Prop. 19.8, the algebra D is quadratic étale if and only if $1 - 4\lambda \in k^\times$.

If k is a field of characteristic 2, then the map $\lambda \mapsto k[\mathbf{t}]/(\mathbf{t}^2 - \mathbf{t} + \lambda)$ defines a bijection

$$k/\{\alpha^2 - \alpha \mid \alpha \in k\} \xrightarrow{\sim} \left\{\begin{matrix}\text{isomorphism classes of} \\ \text{quadratic étale } k\text{-algebras}\end{matrix}\right\}.$$

This is part of the theory of Artin-Schreier extensions as in [271, Tag 09I7].

(v) If $2 \in k^\times$, the Cayley-Dickson construction $D := \mathrm{Cay}(k, \mu)$, $\mu \in k$, yields a quadratic algebra over k with norm $n_D \cong \langle 1, -\mu \rangle_{\mathrm{quad}}$ in the sense of 11.7. Moreover, D is quadratic étale if and only if $\mu \in k^\times$.

If k is a field of characteristic $\neq 2$, then the map $\mu \mapsto \mathrm{Cay}(k, \mu) = k[\mathbf{t}]/(\mathbf{t}^2 - \mu)$ defines a bijection

$$k^\times/k^{\times 2} \xrightarrow{\sim} \left\{\begin{matrix}\text{isomorphism classes of} \\ \text{quadratic étale } k\text{-algebras}\end{matrix}\right\}.$$

This is part of the theory of Kummer extensions as in [271, Tag 09I6].

The most prominent examples of quadratic étale algebras are

(vi) the conic k-algebra $D := k \times k$ of Example 16.2 (d), whose norm $n_D \colon D \to k$ defined by $n_D((\alpha, \beta)) = \alpha\beta$ for $\alpha, \beta \in k$ is binary split hyperbolic, hence regular; we call D the *split quadratic étale k-algebra* or the *split composition algebra of rank* 2 over k;

(vii) the complex numbers $\mathbb{C} = \mathrm{Cay}(\mathbb{R}, -1)$ (18.10) over the field $\mathbb{R}$ of real numbers.

19.20 Quaternion algebras. *Quaternion algebras* over k are defined as composition algebras of rank 4. By Cor. 19.18, they are associative but not commutative. Typical examples arise from the Cayley-Dickson construction as follows:

(i) $B = \mathrm{Cay}(D, \mu)$, D a quadratic étale k-algebra and $\mu \in k^\times$, by Thm. 19.14 is a quaternion algebra over k with norm

$$n_B = n_D \perp (-\mu) n_D = n_D \otimes \langle 1, -\mu \rangle.$$

If k is an LG ring, then every quaternion k-algebra is of this form by Cor. 19.17.

(ii) More specifically, if $2 \in k^\times$, then $B = \mathrm{Cay}(k; \mu_1, \mu_2)$, $\mu_1, \mu_2 \in k^\times$, is a quaternion algebra over k with norm

$$n_B = \langle 1, -\mu_1, -\mu_2, \mu_1\mu_2 \rangle_{\mathrm{quad}} \tag{1}$$

The most prominent examples of quaternion algebras are provided by

(iii) the algebra $\mathrm{Mat}_2(k)$ of 2-by-2 matrices over k whose norm is given by the determinant: indeed, $\det\colon \mathrm{Mat}_2(k) \to k$ is a quadratic form that permits composition and is isometric to $2\mathbf{h}$, the orthogonal sum of two copies of the split hyperbolic plane, hence regular. We call $\mathrm{Mat}_2(k)$ the *split quaternion algebra* over k;

(iv) the Hamiltonian quaternions $\mathbb{H} = \mathrm{Cay}(\mathbb{R}; -1, -1)$ (18.10) over the field $\mathbb{R}$ of real numbers as defined in 1.11.

But note that the Hurwitz quaternions of Thm. 4.2, though a pre-composition algebra over $\mathbb{Z}$ (19.2), are *not* a quaternion algebra since they have discriminant 4. They belong to the class of algebras known as *orders*, see for example [291].

19.21 Remark. A quaternion algebra in our sense is the same thing as an Azumaya algebra of rank 4 as in books such as Knus-Ojanguren [158] and Knus [157], see Exc. 19.32(b) and [157, p. 51]. We will return to Azumaya algebras as a subject in 42.6.

19.22 Octonion algebras. *Octonion algebras* over k are defined as composition algebras of rank 8. By Cor. 19.18, they are alternative but not associative. Typical examples arise again from the Cayley-Dickson construction:

(i) $C = \mathrm{Cay}(B, \mu)$, B a quaternion algebra over k, $\mu \in k^\times$, by Thm. 19.14 is an octonion algebra over k with norm

$$n_C \cong n_B \perp (-\mu) n_B \cong n_B \otimes \langle 1, -\mu \rangle.$$

(ii) $C = \mathrm{Cay}(D; \mu_1, \mu_2)$, D a quadratic étale k-algebra and $\mu_1, \mu_2 \in k^\times$, is an octonion algebra with norm

$$n_C = n_D \perp (-\mu_1)n_D \perp (-\mu_2)n_D \perp (\mu_1\mu_2)n_D = n_D \otimes \langle 1, -\mu_1, -\mu_2, \mu_1\mu_2\rangle.$$

If k is an LG ring, then every octonion k-algebra is of this form by Cor. 19.17.

(iii) If $2 \in k^\times$, then $C = \mathrm{Cay}(k; \mu_1, \mu_2, \mu_3)$, with $\mu_1, \mu_2, \mu_3 \in k^\times$, is an octonion algebra over k, whose norm is given by norm

$$n_C = \langle 1, -\mu_1, -\mu_2, \mu_1\mu_2, -\mu_3, \mu_1\mu_3, \mu_2\mu_3, -\mu_1\mu_2\mu_3\rangle_{\mathrm{quad}} \qquad (1)$$

The most prominent example of an octonion algebra is provided by

(iv) the Graves-Cayley octonions $\mathbb{O} = \mathrm{Cay}(\mathbb{R}; -1, -1, -1)$ (18.10) over the field $\mathbb{R}$ of real numbers as defined in 1.5.

In a more arithmetic vein,

(v) the Dickson-Coxeter octonions of Thm. 4.5 form an octonion algebra over the ring of rational integers. Since they are indecomposable as an integral quadratic lattice (cf. 4.6), they provide an example of an octonion algebra that cannot be obtained from the Cayley-Dickson construction. For other examples of this remarkable phenomenon, see Knus-Parimala-Sridharan [159] or Thakur [274].

We are not ready yet to define the notion of a split octonion algebra; this task has to be postponed to one of the next sections.

19.23 Sedenion algebras. One may continue the preceding examples by considering $C = \mathrm{Cay}(B, \mu)$ for an octonion algebra B over k and $\mu \in k^\times$. The resulting algebra is conic (18.4), norm-associative (18.11), and flexible (18.12). But it is not alternative (18.15), so its norm does not permit composition (19.3). These algebras are sometimes called *sedenion algebras*.

19.24 Remark. One could make an analogy between:

- The algebras of rank 2^r constructed by the Cayley-Dickson process, which are associative for $r < 3$, exceptional for $r = 3$ (octonions), and no longer composition algebras for $r > 3$ (Cor. 19.18).
- The hermitian matrices $\mathrm{Her}_r(\mathbb{O})$ from 5.2 and §36, which are special for $r < 3$ (Exc. 36.10), exceptional for $r = 3$ (Albert algebras), and no longer Jordan algebras for $r > 3$ (Exc. 5.16).

19.25 Sextonions. Let C be a conic algebra over k that contains a right ideal I and pick $\mu \in k$. The subspace S of $\mathrm{Cay}(C, \mu)$ consisting of elements of the form $u + vj$ with $u \in C$ and $v \in I$ is closed under multiplication and therefore is itself a conic algebra. It is, for example, alternative or norm-associative if $\mathrm{Cay}(C, \mu)$ is.

In the special case where $k = \mathbb{R}$, $C = \mathrm{Mat}_2(k)$, and I is the set of matrices with zeros on the bottom row, the algebra S is known as the *sextonions*. (You can check that choosing instead the other proper right ideal does not change the isomorphism class of S.) The algebra S is a multiplicative conic algebra. However, it is neither a pre-composition algebra nor a composition algebra because Dn_S has radical $Ij := \{vj \mid v \in I\}$.

For more on the sextonions and their relationship to "the Lie algebra $\mathfrak{e}_{7\frac{1}{2}}$", see for example [154], [168], [244], and [295].

Exercises

19.26. Let C be a unital k-algebra and $n\colon C \to k$ a quadratic form such that all the conditions of 19.1 hold, with the possible exception of (19.1.1). Show that the following conditions are equivalent.

(i) C is a pre-composition algebra.
(ii) $1_C \in C$ is unimodular in the sense of 9.13.
(iii) C is a faithful k-module.

19.27. Let F be a field. Show that a two-dimensional unital F-algebra is precisely one of the following.

(i) a separable quadratic extension field of F,
(ii) split quadratic étale,
(iii) an inseparable quadratic extension field of F,
(iv) isomorphic to the F-algebra of dual numbers.

Conclude that, if F is perfect of characteristic 2 and C is a conic F-algebra without nilpotent elements other than 0, then C has dimension at most 2.

19.28. Let F be a field and C a conic F-algebra whose conjugation is an involution and whose norm is a non-degenerate quadratic form. Prove that (C, ι_C) is simple as an algebra with involution and conclude that C is either simple or split quadratic étale.

19.29. For a conic algebra over a field to be a division algebra it is necessary that its norm be anisotropic. Show that the converse of this statement does not hold, even in the finite-dimensional case, by proving *Brown's theorem* (Brown [39, Thm. 3]): given an octonion algebra B over a field of characteristic not 2 and a non-zero scalar μ, the Cayley-Dickson construction $C = \mathrm{Cay}(B, \mu) = B \oplus Bj$ is a division algebra if and only if μ is not the norm of an element in B and $-\mu$ is not the norm of a trace zero element in B. In order to do so, let F be a field of *arbitrary* characteristic and with B, μ as above perform the following steps.

(a) Suppose $\mu \notin n_B(B^\times)$. Show for $0 \neq x_i = u_i + v_i j \in C$, $u_i, v_i \in B$, $i = 1, 2$ that $x_1 x_2 = 0$ if and only if $u_i \neq 0 \neq v_i$ for $i = 1, 2$ and the following relations hold.

(i) $n_B(u_1) = -\mu n_B(v_1)$,
(ii) $(u_1 u_2)\bar{v}_1 = -u_1(u_2 \bar{v}_1)$,
(iii) $v_2 = -(v_1 \bar{u}_2)u_1^{-1}$.

(b) Conclude from (a) that if F has characteristic 2, then C is a division algebra if and only if its norm is anisotropic.

(c) Suppose $\mathrm{char}(F) \neq 2$ and B is a division algebra. Then non-zero elements $x, y, z \in B$ satisfy the relation $(xy)z = -x(yz)$ if and only if there is a quaternion subalgebra $A \subseteq B$ with $x, y \in A$, $x \circ y = 0$, $z \in A^\perp$.

(d) Now prove Brown's theorem.

(e) Conclude from (d) that the norm of the *real sedenions*

$$\mathbb{S} := \mathrm{Cay}(\mathbb{O}; -1)$$

is anisotropic but the algebra itself fails to be a division algebra.

Remark. The final statement of (e) follows also from the Bott-Milnor-Kervaire theorem recalled in 1.14. For a more precise statement about the zero divisors of $\mathbb{S}$, see Exc. 23.34 below.

19.30. *Frobenius's theorem for alternative real division algebras*. Prove that a finite-dimensional alternative real division algebra is isomorphic to $\mathbb{R}, \mathbb{C}, \mathbb{H}$, or $\mathbb{O}$. (*Hint*: Exc. 14.9, Exc. 16.21.)

Remark. Frobenius's actual theorem in [86, §11] was the weaker result that the only *associative* real division algebras are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$.

19.31. *Isotopes and the Cayley-Dickson construction.* Let B be a multiplicative conic associative algebra over k, $\mu \in k$ and $p \in B^\times$. Prove that the assignment $u + vj \mapsto p^{-1}up + vj$ determines an isomorphism from $\mathrm{Cay}(B, \mu) = B \oplus Bj$ onto the unital isotope $\mathrm{Cay}(B, \mu)^p$. Conclude for an octonion algebra C over k and $p, q \in C^\times$ that the algebras C and $C^{(p,q)}$ are isomorphic provided the element pq^2 belongs to a quaternion subalgebra of C.

19.32. *Centre and nucleus of quaternion and octonion algebras.*

(a) Show for a quadratic k-algebra R and $u \in R$ that $u - \bar{u}$ is invertible if and only if R is étale and generated by u. Show further that a quadratic étale k-algebra D contains an element u with $u - \bar{u} \in D^\times$ provided k is LG. Conclude for k arbitrary that $H(D, \iota_D) = k1_D$.

(b) Conclude from (a) and Cor. 19.17 that a quaternion algebra over any commutative ring k is central, hence an Azumaya algebra (cf. Knus-Ojanguren [158, III, §5]). Prove similarly that an octonion algebra C over k satisfies

$$\mathrm{Nuc}(C) = \{x \in C \mid xy = yx \text{ for all } y \in C\} = k1_C.$$

19.33. *Automorphisms of quadratic étale algebras.* Let D be a quadratic étale k-algebra. Prove:

(a) If k is a local ring, then 1_D can be extended to a basis $(1_D, u)$ of D as a k-module, for some $u \in D$ of trace 1.

(b) A k-linear map $\varphi\colon D \to D$ is an automorphism of D if and only if there exists a decomposition $k = k_+ \times k_-$ of k as a direct product of ideals such that the induced decompositions

$$D = D_+ \times D_-, \quad D_\pm := D_{k_\pm}, \quad \varphi = \varphi_+ \times \varphi_-, \quad \varphi_\pm := \varphi_{k_\pm}$$

satisfy $\varphi_+ = \mathbf{1}_{D_+}, \varphi_- = \iota_{D_-}$.

19.34. *Ideals in composition algebras* (Petersson [221, Thm. 4.1]). Let C be a composition algebra over k and view $k \subseteq C$ as a subalgebra in the natural way. Show that the assignments

$$\mathfrak{a} \longmapsto \mathfrak{a}C, \quad I \longmapsto k \cap I$$

give inclusion-preserving inverse bijections between the ideals of k and

(i) the ideals of (C, ι_C) as an algebra with involution if C is quadratic étale,
(ii) the two-sided ideals of C if C is a quaternion algebra,
(iii) the one-sided ideals of C if C is an octonion algebra.

Show also that (iii) (resp. (ii)) does not hold for quaternion (resp. quadratic étale) algebras.

(*Hint*: Assume C has constant rank r as a k-module and perform the following steps: (a) One-sided ideals of octonion algebras are two-sided. (b) Let $I \subseteq C$ be a two-sided ideal. Then $I \cap k = \{0\}$ implies $I = \{0\}$ provided $r > 2$ or I is stable under conjugation. (c) $(\mathfrak{a}C) \cap k = \mathfrak{a}$ for all ideals $\mathfrak{a} \subseteq k$. (d) $I = (I \cap k)C$ for all two-sided ideals $I \subseteq C$ provided $r > 2$ or I is stable under conjugation.)

Remark. By [158, Cor. 5.2], (ii) also follows from the fact that quaternion algebras are Azumaya. Part (iii) has been known for a long time to hold for the Dickson-Coxeter octonions (Allcock [13], Van der Blij-Springer [286]).

19.35. *Elementary Peirce decomposition.* Let C be a multiplicative conic alternative algebra over k. If $c \in C$ is an elementary idempotent (cf. Exc. 16.23), put $c_1 := c$, $c_2 := 1_C - c$, $C_{ij} := C_{ij}(c)$ for $i, j = 1, 2$ and show

$$C_{ii} = kc_i \qquad (i = 1, 2). \tag{1}$$

Show further for elements

$$x = \alpha_1 c_1 + x_{12} + x_{21} + \alpha_2 c_2, \quad y = \beta_1 c_1 + y_{12} + y_{21} + \beta_2 c_2, \tag{2}$$

in C, where $\alpha_i, \beta_i \in k$, $x_{ij}, y_{ij} \in C_{ij}$ for $i, j = 1, 2$, $i \neq j$ (Excs. 14.12, 16.23), that

$$n_C(x) = \alpha_1\alpha_2 + n_C(x_{12}, x_{21}), \tag{3}$$
$$n_C(x, y) = \alpha_1\beta_2 + \alpha_2\beta_1 + n_C(x_{12}, y_{21}) + n_C(x_{21}, y_{12}), \tag{4}$$
$$t_C(x) = \alpha_1 + \alpha_2, \tag{5}$$
$$\overline{x} = \alpha_2 c_1 - x_{12} - x_{21} + \alpha_1 c_2. \tag{6}$$

Moreover, if C is a composition algebra, then the k-modules C_{12}, C_{21} are in duality to each other under Dn_C. Finally, for $i, j = 1, 2$ distinct, the trilinear form

$$C_{ij}^3 \longrightarrow k, \quad (x, y, z) \longmapsto t_C(xyz),$$

(cf. (16.13.1)) is alternating.

19.36. *Minimal splitting of quadratic étale algebras.* Let D be a quadratic étale k-algebra.

(a) Prove that the map $\varphi\colon D \otimes D \xrightarrow{\sim} D \times D$ defined by

$$\varphi(x \otimes d) := (xd, \bar{x}d)$$

for $x, d \in D$ is an isomorphism of D-algebras. (*Hint*: For $u \in D$ compute $\varphi(u \otimes 1_D - 1_D \otimes \bar{u})$ and $\varphi(1_D \otimes u - u \otimes 1_D)$.)

(b) Conclude from (a) that

$$\sigma := \mathbf{1}_D \otimes \iota_D\colon D \otimes D \longrightarrow D \otimes D,$$
$$\sigma' := \varphi \circ \sigma \circ \varphi^{-1}\colon D \times D \longrightarrow D \times D$$

are ι_D-semi-linear involutions of $D \otimes D$, $D \times D$, respectively, with

$$\sigma'((a, b)) = (\bar{b}, \bar{a})$$

for all $a, b \in D$.

19.37. *Quadratic forms permitting composition on quadratic algebras.* Let R be a quadratic algebra over k.

(a) Prove for an idempotent $e \in R$ with $n_R(e) = 0$ that

$$t_R \circ L_e\colon R \longrightarrow k, \quad x \longmapsto t_R(ex)$$

is a (possibly non-unital) algebra homomorphism.

(b) Conclude from (a) that for idempotents $\varepsilon \in k$, $e \in R$ with $\varepsilon e = 0$, $n_R(e) = 0$, the quadratic form

$$q\colon R \longrightarrow k, \quad x \longmapsto t_R(ex^2) + \varepsilon n_R(x)$$

permits composition.

(c) Let $D = k \times k$ be the split quadratic étale k-algebra. Show that a quadratic form $q\colon D \to k$ permits composition if and only if there exists an orthogonal system $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ of idempotents in k (possibly incomplete) such that

$$q((\alpha, \beta)) = \varepsilon_1\alpha^2 + \varepsilon_2\alpha\beta + \varepsilon_3\beta^2 \tag{1}$$

for all $\alpha, \beta, \gamma \in k$

(d) Finally, show that if D is étale, all quadratic forms on D permitting composition have the form described in (b). (*Hint*: Reduce to the split case $D = k \times k$ by using (c) and Exc. 19.36.)

19.38. *Embeddings into quaternion subalgebras.* Let C be an octonion algebra over an LG ring k and $R \subseteq C$ a quadratic subalgebra. Show that there exists a quaternion subalgebra of C containing R. (*Hint*: Show more precisely that there exists an element $b \in C$ making the subalgebra of C generated by R and b a quaternion algebra and reduce this assertion to the field case by using the LG property.)

Remark. Over fields, the preceding result amounts to [270, Prop. 1.6.4]: every element of an octonion algebra over a field can be embedded into a quaternion subalgebra.

19.39. *Reflections and involutions of composition algebra* (cf. Jacobson [132] and Racine-Zel'manov [245]). Let k be a commutative ring in which 2 is invertible and C a composition algebra of rank $r > 1$ over k.

(a) Let σ be a *reflection* of C, i.e., an automorphism of order 2. Show that its fixed algebra $\mathrm{Fix}(\sigma) := \{x \in C \mid \sigma(x) = x\} \subseteq C$ is a composition subalgebra of rank $\frac{r}{2}$ and that the assignment $\sigma \mapsto \mathrm{Fix}(\sigma)$ determines a bijection from the set of reflections of C onto the set of composition subalgebras of C having rank $\frac{r}{2}$. Show further that two reflections of C are conjugate under $\mathrm{Aut}(C)$ if and only if their fixed algebras are.

(b) Show that an involution of C commutes with its conjugation. Use this and (a) to set up a bijective correspondence between the set of involutions of C that are distinct from its conjugation (resp. the set of their isomorphism classes) and the set of composition subalgebras of C having rank $\frac{r}{2}$ (resp. the set of their conjugacy classes under $\mathrm{Aut}(C)$). Finally, show for an involution $\tau \neq \iota_C$ of C that $H(C, \tau) \subseteq C$ is a finitely generated projective submodule of rank $\frac{r}{2} + 1$.

20 Hermitian forms

Before proceeding with the study of composition algebras, it will be necessary to insert a few basic facts about hermitian forms over commutative rings that will be useful not only in the present context but also for cubic Jordan algebras later on. A systematic account of the subject may be found in Knus [157] or Hahn-O'Meara [111].

Throughout we let k be an arbitrary commutative ring and (B, τ) an associative algebra with involution over k in the sense of 10.1. In particular, B contains an identity element. We also write $\bar{x} := \tau(x)$ for $x \in B$.

20.1 Passing from left to right modules and conversely. Any left B-module M may be converted into a right B-module by defining $xa := \bar{a}x$ for $x \in M$ and $a \in B$. We denote this right B-module by M^τ. The identity of M, viewed as a map from M to M^τ, will be indicated by $x \mapsto x^\tau$, so we have $(ax)^\tau = x^\tau \bar{a}$ for all $a \in B$. A B-linear map $f\colon M \to N$, $x \mapsto (x)f$, of left B-modules may be viewed as a B-linear map $f^\tau\colon M^\tau \to N^\tau$ of right B-modules, so we have $f^\tau(x^\tau) = ((x)f)^\tau$ for all $x \in M$. The preceding conventions make equally good sense with left and right modules interchanged. We then have $M^{\tau\tau} = M$ and $x^{\tau\tau} = x$ for any left (right) module M over B and any $x \in M$. Moreover, $f^{\tau\tau} = f$ for any B-linear map $f\colon M \to N$ of left (right) B-modules.

Writing ${}_BB$ (resp. B_B) for B viewed as a left (resp. right) B-module, the map $\tau\colon ({}_BB)^\tau \to B_B$ is a linear bijection of right B-modules. Hence, if a left B-module is (finitely generated) projective (resp. free), then so is M^τ as a right B-module, and conversely.

20.2 The twisted dual of a module. Let M be a right B-module. Then the additive group $M^\bullet := \mathrm{Hom}_B(M, B)$ canonically becomes a left B-module if one defines $ax^\bullet\colon M \to B$ by $(ax^\bullet)(y) := ax^\bullet(y)$ for $a \in B$, $x^\bullet \in M^\bullet$ and $y \in M$.

Using the formalism of 20.1, we may then convert the left B-module $M^\bullet$ into the right B-module $M^* := M^{\bullet\tau}$, which we call the *τ-twisted dual*, or simply the *twisted dual*, of M. Note that for B commutative and $\tau = \mathbf{1}_B$, the terms "right B-module" and "left B-module" may be used interchangeably, and the twisted dual of M agrees with the ordinary dual as defined in 9.11. On the other hand, if (B still being commutative) τ is not the identity, the twisted dual and the ordinary dual are different notions. However, it will always be clear from the context which one of the two we have in mind.

For any right B-module M, we have its *canonical pairing*

$$\mathrm{cap}_M \colon M^* \times M \longrightarrow B, \quad (x^*, y) \longmapsto \langle x^*, y\rangle := x^*(y), \tag{1}$$

which is anti-linear in the first variable and linear in the second:

$$\langle x^* a, yb\rangle = \bar{a}\langle x^*, y\rangle b \qquad (a, b \in B,\ x^* \in M^*,\ y \in M). \tag{2}$$

If $f \colon M \to N$ is a linear map of right B-modules, then the assignment $y^* \mapsto y^* \circ f$ defines a linear map $f^* \colon N^* \to M^*$, called the *adjoint* of f because it is characterized by the relation

$$\langle f^*(y^*), x\rangle = \langle y^*, f(x)\rangle \qquad (y^* \in N^*,\ x \in M). \tag{3}$$

In this way, we obtain a contravariant additive functor from the category of right B-modules to itself.

20.3 Sesquilinear forms. By a *sesquilinear form* over B we mean a bi-additive map $h \colon M \times N \to B$, where M, N are right B-modules such that $h(xa, yb) = \bar{a}h(x, y)b$ for all $a, b \in B$ and all $x \in M$, $y \in N$. In this case, we define the *adjoint map* or simply the *adjoint* of h as the B-linear map

$$\varphi_h \colon M \to N^*, \quad x \longmapsto \varphi_h(x) := h(x, -).$$

Conversely, given a B-linear map $\varphi \colon M \to N^*$, we obtain a sesquilinear form $h_\varphi \colon M \times N \to B$ via $h_\varphi(x, y) := \langle \varphi(x), y\rangle$ for $x \in M$, $y \in N$, and the two constructions are inverse to each other.

As an example, let M be any right B-module. Then the canonical pairing of (20.2.1) by (20.2.2) is a sesquilinear form over B whose adjoint map $M^* \to M^*$ is the identity on M^*.

20.4 Base change. For $R \in k$-**alg**, we can form the base change $(B, \tau)_R = (B_R, \tau_R)$, which is an associative algebra with involution over R, and for a right B-module M, the R-module $M_R = M \otimes R$ becomes a right B_R-module in a natural way. If $f \colon M \to N$ is a homomorphism of right B-modules, then its R-linear extension $f_R \colon M_R \to N_R$ is in fact one of right B_R-modules.

For $x^* \in M^*$, we clearly have $x^* \otimes \mathbf{1}_R \in (M_R)^*$, and the assignment $x^* \mapsto$

$x^* \otimes \mathbf{1}_R$ gives a k-linear map $M^* \to (M_R)^*$, which in turn induces an R-linear map

$$\Phi_{M,R}\colon (M^*)_R \to (M_R)^*, \quad x^* \otimes r \longmapsto r(x^* \otimes \mathbf{1}_R).$$

This map is, in fact, a homomorphism of right B_R-modules and will henceforth be referred to as the *canonical homomorphism* from $(M^*)_R$ to $(M_R)^*$.

Any sesquilinear form $h\colon M \times N \to B$ over B yields canonically an extended sesquilinear form $h_R\colon M_R \times N_R \to B_R$ over B_R, called the *base change* or *scalar extension* of h from k to R, such that the diagram

$$\begin{array}{ccc} M_R & \xrightarrow{(\varphi_h)_R} & (N^*)_R \\ & \searrow^{\varphi_{(h_R)}} & \downarrow{\scriptstyle \Phi_{N,R}} \\ & & (N_R)^* \end{array} \tag{1}$$

commutes.

20.5 Sesquilinear modules. By a *sesquilinear module* over B, we mean a pair (M, h) consisting of a right B-module M and a sesquilinear form $h\colon M \times M \to B$. Given two sesquilinear modules (M, h) and (M', h') over B, a *homomorphism* from (M, h) to (M', h') (or from h to h') is a B-linear map $f\colon M \to M'$ preserving sesquilinear forms in the sense that $h' \circ (f \times f) = h$. In this way one obtains the category of sesquilinear modules over B. Isomorphisms in this category are called *isometries*.

20.6 Sesquilinear forms and matrices. Let p, q be positive integers. Viewing $M := B^p$, $N := B^q$ as free right B-modules in the natural way, every matrix $T \in \mathrm{Mat}_{p,q}(B)$ determines a sesquilinear form

$$\langle T \rangle_{\mathrm{sesq}}\colon B^p \times B^q \longrightarrow B, \quad (x, y) \longmapsto \bar{x}^{\mathsf{T}} T y,$$

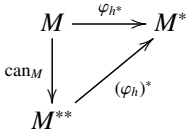
and every sesquilinear form on $B^p \times B^q$ can be written uniquely in this way. Identifying a vector $x \in B^q$ with the linear form $B^q \to B, y \mapsto \bar{x}^{\mathsf{T}} y$, we obtain an identification $B^q = B^{q*}$. The adjoint of $\langle T \rangle_{\mathrm{sesq}}$ then agrees with the linear map $\bar{T}^{\mathsf{T}}\colon B^p \to B^q$.

20.7 The double dual. Given a right B-module M, we obtain a natural B-linear map $\mathrm{can}_M\colon M \to M^{**}$ determined by the condition

$$\mathrm{can}_M(x)(y^*) := \overline{\langle y^*, x \rangle} \qquad (x \in M, y^* \in M^*).$$

In important cases, can_M is an isomorphism. For example, if $M = B^n$, then $B^{n**} = B^n$ and $\mathrm{can}_M = \mathbf{1}_{B^n}$ under the identifications of 20.6. Now let $h\colon M \times M \to B$ be a sesquilinear form. Then so is $h^*\colon M \times M \to B$ defined by

$h^*(x,y) := \overline{h(y,x)}$ for $x, y \in M$, and the adjoints of h, h^* are related to one another by the commutative diagram



Hence if can_M is bijective, allowing us to identify $M = M^{**}$ accordingly, the adjoint of h^* agrees with the adjoint of the adjoint of h.

20.8 Hermitian forms. By a *hermitian form* on a right B-module M we mean a sesquilinear form $h\colon M \times M \to B$ satisfying $h(y,x) = \overline{h(x,y)}$ for all $x, y \in M$; this is equivalent to $h = h^*$. For $T \in \mathrm{Mat}_n(B)$, we obtain $(\langle T\rangle_{\mathrm{sesq}})^* = \langle \bar{T}^{\mathsf{T}}\rangle_{\mathrm{sesq}}$, so $\langle T\rangle_{\mathrm{sesq}}$ is a hermitian form if and only if $T = \bar{T}^{\mathsf{T}}$ is a hermitian matrix. By a *hermitian module* we mean a pair (M,h) consisting of a right B-module M and a hermitian form $h\colon M \times M \to B$. We view hermitian modules as a full subcategory of sesquilinear modules.

21 Ternary hermitian spaces

The Cayley-Dickson construction discussed in some of the preceding sections is not an appropriate tool when dealing with octonion algebras that fail to contain any quaternion subalgebras. In the sequel, we therefore propose a different method of constructing composition algebras that is due to Thakur [274] over rings where 2 is invertible and has been sketched in [230, 3.8] over fields of arbitrary characteristic; if the characteristic is not two, the construction is already implicit in Jacobson [132, pp. 15,16]. The main constituents of this construction are quadratic étale algebras and ternary hermitian spaces. They always lead to octonion algebras and, conversely, every octonion algebra containing a quadratic étale subalgebra arises in this manner; in particular, this holds true for the Graves-Cayley octonions over the reals as defined in 1.5 and for arbitrary octonion algebras over any commutative ring that contains 2 in its Jacobson radical (Prop. 21.17 below). A slight generalization of our method leads to a similar construction of quaternion algebras due to Pumplün [241] provided 2 is invertible in the base ring. Both constructions, the octonionic as well as the quaternionic one, will be treated here in a unified fashion.

In this section, we fix a composition algebra D of rank $r \leq 2$ over a nonzero commutative ring k. By Cor. 19.18, D is commutative associative and is endowed with its canonical involution, which we abbreviate as $\iota := \iota_D$, $a \mapsto \bar{a}$.

The set-up of the preceding section may thus be specialized to $(B, \tau) := (D, \iota)$. By Exc. 19.32, we can identify $k = H(D, \iota)$ as a unital subalgebra of D, and this identification is compatible with base change.

21.1 Some useful identifications. Fix $R \in k$-**alg** and let M be a right D-module. In analogy to (12.27.1), (12.27.2), we obtain a natural identification

$$M_R = M \otimes R = M \otimes_D (D \otimes R) = M_{D_R} \tag{1}$$

as right D_R-modules such that

$$x \otimes r = x \otimes_D (1_D \otimes r) \quad \text{and} \quad x \otimes_D (a \otimes r) = (xa) \otimes r \tag{2}$$

for $x \in M$, $r \in R$, $a \in D$, ditto for left D-modules. It follows that, if M is finitely generated projective over D, then so is M_R over D_R. Moreover, M is a finitely generated projective k-module.

Now suppose that M is a left D-module. Since $M^\iota = M$ as k-modules, we obtain a canonical identification $(M^\iota)_R = (M_R)^{\iota_R}$ as right D_R-modules, and (1), (2) yield an identification $(M^\iota)_{D_R} = (M_{D_R})^{\iota_{D_R}}$ as right D_R-modules matching $x \otimes_D (a \otimes r)$ in $(M^\iota)_{D_R}$ with $x \otimes_D (\bar{a} \otimes r)$ in $(M_{D_R})^{\iota_{D_R}}$, for $x \in M$, $a \in D$, $r \in R$.

21.2 Lemma. *Let M be a finitely generated projective right D-module and $R \in k$-**alg**. Then the canonical homomorphism*

$$\Phi_{M,R} \colon (M^*)_R \longrightarrow (M_R)^*, \quad x^* \otimes r \longmapsto r(x^* \otimes \mathbf{1}_R),$$

is an isomorphism of right D_R-modules. Identifying $(M^*)_R = (M_R)^* =: M_R^*$ by means of this isomorphism, we have $\langle x^*, x\rangle_R = \langle x_R^*, x_R\rangle$ for all $x \in M$, $x^* \in M^*$, in other words, the canonical pairing $M_R^* \times M_R \to D_R$ is the R-hermitian extension of the canonical pairing $M^* \times M \to D$.

Proof The preceding identifications combined with 20.2, 20.4 yield $(M^*)_R = (M^{\bullet\iota})_R = ((M^\bullet)_R)^{\iota_R} = ((M^\bullet)_{D_R})^{\iota_R}$ and $(M_R)^* = ((M_{D_R})^\bullet)^{\iota_R}$. From Lemma 9.15 we derive an isomorphism $\varphi \colon (M^\bullet)_{D_R} \xrightarrow{\sim} (M_{D_R})^\bullet$ of left D_R-modules, which may be viewed as an isomorphism

$$\varphi^{\iota_R} \colon (M^*)_R = ((M^\bullet)_{D_R})^{\iota_R} \xrightarrow{\sim} ((M_{D_R})^\bullet)^{\iota_R} = (M_R)^*$$

of right D_R-modules, and one checks that φ^{ι_R} agrees with $\Phi_{M,R}$. □

21.3 Regular sesquilinear forms. A sesquilinear form $h \colon M \times M \to D$ over D with a right D-module M is said to be *regular* if M is finitely generated projective and the adjoint $\varphi_h \colon M \to M^*$ is an isomorphism. Combining (20.4.1) with Lemma 21.2 we see that the property of a sesquilinear form to be regular is stable under base change. By a *sesquilinear* (resp. *hermitian*) *space* over D we

mean a sesquilinear (resp. hermitian) module (M, h) such that the sesquilinear (resp. hermitian) form $h\colon M \times M \to D$ is regular. Given a positive integer n, we speak of a *hermitian space of rank n* if the underlying module has rank n as a finitely generated projective right D-module.

Our next aim will be to discuss exterior powers of sesquilinear forms over D. We begin with a reminder.

21.4 Reminder: exterior powers under base change. Following [28, III.7, Prop. 8], taking exterior powers is compatible with arbitrary base change. More precisely, let M be a k-module, $n \in \mathbb{N}$ and $R \in k$-**alg**. Then there is a natural identification

$$(\bigwedge^n(M))_R = \bigwedge^n(M_R) \tag{1}$$

as R-modules such that

$$(x_1 \wedge \cdots \wedge x_n) \otimes r = r(x_{1R} \wedge \cdots \wedge x_{nR}), \tag{2}$$

$$(x_1 \otimes r_1) \wedge \cdots \wedge (x_n \otimes r_n) = (x_1 \wedge \cdots \wedge x_n) \otimes (r_1 \cdots r_n) \tag{3}$$

for all $x_1, \ldots, x_n \in M$, $r, r_1, \ldots, r_n \in R$. Under this identification, $(\bigwedge^n f)_R = \bigwedge^n(f_R)$ for all k-linear maps $f\colon M \to N$.

21.5 Exterior powers of sesquilinear forms. Let M, N be right D-modules and $h\colon M \times N \to D$ a sesquilinear form. Given a positive integer n, we may pass to the n-th exterior power over D, i.e., to

$$\bigwedge^n h\colon \bigwedge^n M \times \bigwedge^n N \longrightarrow D$$

(well) defined by

$$(\bigwedge^n h)(x_1 \wedge \cdots \wedge x_n, y_1 \wedge \cdots \wedge y_n) = \det\big((h(x_i, y_j))_{1 \le i,j \le n}\big) \tag{1}$$

for $x_i \in M$, $y_j \in N$, $1 \le i, j \le n$. We call $\bigwedge^n h$, which is again a sesquilinear form over D, the *n-th exterior power* of h. Passing to the adjoint maps, we conclude that the diagram

$$\begin{array}{ccc} \bigwedge^n M & \xrightarrow{\bigwedge^n \varphi_h} & \bigwedge^n(N^*) \\ & \searrow^{\varphi_{\bigwedge^n h}} & \downarrow{\scriptstyle \varphi_{\bigwedge^n \mathrm{cap}_N}} \\ & & (\bigwedge^n N)^* \end{array} \tag{2}$$

commutes, where cap_N is defined as in 20.2. Note that not only $\bigwedge^n \varphi_h$ (for trivial reasons) and $\varphi_{\bigwedge^n h}$ by Exc. 21.20 below but also $\varphi_{\bigwedge^n \mathrm{cap}(N)}$ is compatible

with base change: for $R \in k$-**alg**, we obtain a commutative diagram

$$\begin{array}{ccc} (\bigwedge^n(N^*))_R = \bigwedge^n((N^*)_R) & \xrightarrow[\bigwedge^n(\Phi_{N,R})]{\cong} & \bigwedge^n((N_R)^*) \\ \Big\downarrow{\scriptstyle (\varphi_{\bigwedge^n \mathrm{cap}_N})_R} & & \Big\downarrow{\scriptstyle \varphi_{\bigwedge^n \mathrm{cap}(N_R)}} \\ ((\bigwedge^n N)^*)_R & \xrightarrow[\Phi_{\bigwedge^n(N),R}]{\cong} & ((\bigwedge^n N)_R)^* = (\bigwedge^n(N_R))^*. \end{array} \tag{3}$$

21.6 Lemma. *If $h\colon M \times M \to D$ is a regular sesquilinear form over D, then so is its n-th exterior power, for any positive integer n.*

Proof The claim is that the diagonal arrow in (21.5.2) is an isomorphism. Because the horizontal arrow is an isomorphism, it suffices to show that the vertical arrow in (21.5.2) is an isomorphism. By (21.5.3), the assertion is local on k, so Exc. 21.21 (a) below allows us to assume that M is free of finite rank $p \geq n$ over D. Let $(e_i)_{1\leq i\leq p}$ be a D-basis of M and $(e_i^*)_{1\leq i\leq p}$ the corresponding dual basis of M^*. Then

$$(e_{j_1} \wedge \cdots \wedge e_{j_n})_{1\leq j_1<\cdots<j_n\leq p} \tag{1}$$

is a D-basis of $\bigwedge^n M$, while

$$(e^*_{i_1} \wedge \cdots \wedge e^*_{i_n})_{1\leq i_1<\cdots<i_n\leq p} \tag{2}$$

is a D-basis of $\bigwedge^n(M^*)$ such that

$$(\varphi_{\bigwedge^n \mathrm{cap}_N}(e^*_{i_1} \wedge \cdots \wedge e^*_{i_n}))(e_{j_1} \wedge \cdots \wedge e_{j_n}) = \det((\langle e^*_{i_\lambda}, e_{j_\mu}\rangle)_{1\leq\lambda,\mu\leq n}),$$

which is 1 for $(i_1,\dots,i_n) = (j_1,\dots,j_n)$ and 0 otherwise. Thus $\varphi_{\bigwedge^n \mathrm{cap}_M}$ maps the D-basis (2) of $\bigwedge^n(M^*)$ onto the dual of the basis (1) of $\bigwedge^n M$, hence must be an isomorphism. □

21.7 Remark. Let M be a finitely generated projective right D-module and n a positive integer. Then the preceding result (or its proof) yields an identification $\bigwedge^n(M^*) = (\bigwedge^n M)^*$ such that the canonical pairing

$$\bigwedge^n(M^*) \times \bigwedge^n M = (\bigwedge^n M)^* \times \bigwedge^n M \longrightarrow D$$

is given by

$$\langle x_1^* \wedge \cdots \wedge x_n^*, y_1 \wedge \cdots \wedge y_n\rangle = \det((\langle x_i^*, y_j\rangle)_{1\leq i,j\leq n})$$

for $x_1^*,\dots,x_n^* \in M^*$, $y_1,\dots,y_n \in M$.

21.8 Determinants. Let (M,h) be a hermitian space of rank n over D. An isomorphism $\Delta\colon \bigwedge^n M \xrightarrow{\sim} D$ may not exist but if it does, we follow Asok et al [16] and call it an *orientation* of M; it is unique up to an invertible factor in D.

Given an orientation $\Delta\colon \bigwedge^n M \xrightarrow{\sim} D$, there exists a unique element $\det_\Delta(h) \in k^\times$, called the Δ-*determinant* of (M,h), or just h, such that $\Delta\colon \bigwedge^n(M,h) \xrightarrow{\sim} (D, \langle \det_\Delta(h)\rangle_{\mathrm{sesq}})$ is an isometry. In other words, $\det_\Delta(h)$ is the unique invertible element in k such that

$$\det_\Delta(h)\overline{\Delta(x_1 \wedge \cdots \wedge x_n)}\Delta(y_1 \wedge \cdots \wedge y_n) = \det\Big((h(x_i, y_j))_{1\le i,j\le n}\Big) \tag{1}$$

for all $x_i, y_j \in M$, $1 \le i, j \le n$. The Δ-determinant changes with Δ according to the rule

$$\det_{a\Delta}(h) = n_D(a)^{-1} \det_\Delta(h) \qquad (a \in D^\times). \tag{2}$$

If M is free of rank n as a right D-module with basis (e_i) and $T = (h(e_i, e_j)) \in \mathrm{GL}_n(D)$ stands for the corresponding hermitian matrix, then $\det_\Delta(h) = \det(T)$, where $\Delta\colon \bigwedge^n M \xrightarrow{\sim} D$ is the orientation normalized by $\Delta(e_1 \wedge \cdots \wedge e_n) = 1$.

21.9 Ternary hermitian spaces and the hermitian vector product. Let (M,h) be a hermitian space over D which is *ternary* in the sense that it has rank $n = 3$ and suppose $\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ is an orientation of M. By regularity of h, there exists a unique map $M \times M \to M, (x,y) \mapsto x \times_{h,\Delta} y$, such that

$$h(x \times_{h,\Delta} y, z) = \Delta(x \wedge y \wedge z). \qquad (x, y, z \in M)$$

We call $\times_{\Delta,h}$ the *hermitian vector product* induced by h and Δ. It is obviously bi-additive, alternating and anti-linear in both arguments. Moreover, the expression $h(x \times_{\Delta,h} y, z)$ remains unaffected by a cyclic change of variables and vanishes if two of them coincide. We have $x \times_{h,a\Delta} y = (x \times_{h,\Delta} y)\bar{a}$ for all $a \in D^\times$, and the hermitian vector product is stable under base change: Δ_R is an orientation of M_R over D_R for all $R \in k$-**alg** and $(x \times_{h,\Delta} y)_R = x_R \times_{h_R,\Delta_R} y_R$ for all $x, y \in D$.

21.10 Example. In keeping with the previous conventions, we regard D^3 as a free right D-module of rank 3 that is equipped with the canonical basis (e_1, e_2, e_3) of ordinary unit vectors, and denote by $x \times y$ the usual vector product of $x, y \in D^3$, as defined 1.1 for the special case $k = \mathbb{R}$, $D = \mathbb{C}$. It satisfies the Grassmann identity (1.1.3), i.e.,

$$(x \times y) \times z = y(z^{\mathsf{T}}x) - x(z^{\mathsf{T}}y), \tag{1}$$

but also

$$(Sx) \times (Sy) = (S^\sharp)^{\mathsf{T}}(x \times y) \tag{2}$$

for all $x, y, z \in D^3$ and all $S \in \mathrm{Mat}_3(D)$, where $S^\sharp \in \mathrm{Mat}_3(D)$ stands for the usual adjoint of S in the sense of linear algebra.

Now suppose $T \in \mathrm{GL}_3(D)$ is a hermitian matrix and consider the ternary

hermitian space $(D^3, \langle T\rangle_{\mathrm{sesq}})$. Writing $\Delta_0\colon \bigwedge^3 D^3 \xrightarrow{\sim} D$ for the ordinary determinant, i.e., for the orientation normalized by $\Delta_0(e_1 \wedge e_2 \wedge e_3) = 1$, any other volume element on D^3 has the form $\Delta = a\Delta_0$ for some $a \in D^\times$, and it is easily checked that the hermitian vector product induced by $\langle T\rangle_{\mathrm{sesq}}$ and Δ relates to the ordinary one according to the formula

$$x \times_{\langle T\rangle_{\mathrm{sesq}},\Delta} y = T^{-1}(\bar{x} \times \bar{y})\bar{a} = (\overline{Tx} \times \overline{Ty}) \det(T)^{-1}\bar{a}. \tag{3}$$

21.11 Proposition. *Let (M, h) be a ternary hermitian space over D and suppose $\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ is an orientation of M. Then the hermitian vector product induced by h and Δ satisfies the hermitian Grassmann identity*

$$(x \times_{h,\Delta} y) \times_{h,\Delta} z = \big(yh(z, x) - xh(z, y)\big) \det_\Delta(h)^{-1} \qquad (x, y, z \in M). \tag{1}$$

Proof The question is local on k, so by Exc. 21.21 (a) we may assume $M = D^3$, $h = \langle T\rangle_{\mathrm{sesq}}$, $\Delta = a\Delta_0$ as in Example 21.10. Then the assertion follows from (21.8.2), (21.10.1), (21.10.3) by a straightforward computation. □

We will now be able to derive the first main result of this section. It turns out to be a direct generalization of the construction leading to the Graves-Cayley octonions (1.5) and to Thm. 1.8.

21.12 Theorem (Thakur [274])**.** *Let D be a regular composition algebra of rank $r \leq 2$ over k, (M, h) a ternary hermitian space over D and suppose $\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ is an orientation of M satisfying $\det_\Delta(h) = 1$. Then the k-module $D \times M$ becomes a composition algebra over k under the multiplication*

$$(a, x)(b, y) := (ab - h(x, y), y\overline{a} + xb + x \times_{h,\Delta} y) \tag{1}$$

for $a, b \in D$, $x, y \in M$. Identifying $k \subseteq D$ canonically, this composition algebra, written as

$$C = \mathrm{Ter}(D; M, h, \Delta),$$

has unit element, norm, linearized norm, trace, conjugation given by

$$1_C = (1_D, 0), \tag{2}$$
$$n_C((a, x)) = n_D(a) + h(x, x), \tag{3}$$
$$n_C((a, x), (b, y)) = n_D(a, b) + t_D(h(x, y)), \tag{4}$$
$$t_C((a, x)) = t_D(a), \tag{5}$$
$$\overline{(a, x)} = (\bar{a}, -x) \tag{6}$$

for all $a, b \in D$, $x, y \in M$.

Proof C is clearly a k-algebra with unit element given by (2), and it follows from Exc. 21.21 below that the quadratic form $n_C\colon C \to k$ as defined in (3), which trivially satisfies (4), is regular. Therefore the theorem will follow once we have shown that n_C permits composition relative to the multiplication (1). Accordingly, using standard properties of the hermitian vector product (21.9), we expand

$$\begin{aligned} n_C((a,x)(b,y)) &= n_C\big(ab - h(x,y), y\bar{a} + xb + x \times_{h,\Delta} y\big) \\ &= n_D(ab) - n_D(ab, h(x,y)) + n_D(h(x,y)) \\ &\quad + h(y\bar{a} + xb + x \times_{h,\Delta} y, y\bar{a} + xb + x \times_{h,\Delta} y) \\ &= n_D(a)n_D(b) - n_D(ab, h(x,y)) + n_D(h(x,y)) \\ &\quad + n_D(a)h(y,y) + abh(y,x) + \bar{a}\,\bar{b}h(x,y) \\ &\quad + n_D(b)h(x,x) + h(x \times_{h,\Delta} y, x \times_{h,\Delta} y). \end{aligned}$$

Here $abh(y,x) + \bar{a}\,\bar{b}h(x,y) = n_D(ab, h(x,y))$ by (16.5.4), (16.12.5), and the hermitian Grassmann identity (21.11.1) yields

$$\begin{aligned} h(x \times_{h,\Delta} y, x \times_{h,\Delta} y) &= h(y, (x \times_{h,\Delta} y) \times_{h,\Delta} x) \\ &= h(y, yh(x,x) - xh(x,y)) \\ &= h(x,x)h(y,y) - n_D(h(x,y)). \end{aligned}$$

Hence n_C does indeed permit composition relative to (1) and the proof is complete. □

21.13 The ternary hermitian construction. The composition algebra

$$C = \mathrm{Ter}(D; M, h, \Delta)$$

obtained in Theorem 21.12 is said to arise from the parameters involved by means of the *ternary hermitian construction*. Note that C has rank $4r$. After the canonical identification $a = (a,0)$ for $a \in D$, the composition algebra C contains D as a composition subalgebra. The entire construction, which is clearly stable under base change, will now be reversed by showing that any composition algebra containing D as a composition subalgebra arises from D by means of the ternary hermitian construction.

21.14 Theorem (Thakur [274])**.** *Let C be a composition algebra of rank $4r$ over k containing D as a regular composition subalgebra of rank $r \leq 2$. Then there exist a ternary hermitian space (M,h) over D and an orientation $\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ satisfying $\det_\Delta(h) = 1$ such that the inclusion $D \hookrightarrow C$ extends to an isomorphism from $\mathrm{Ter}(D; M, h, \Delta)$ onto C.*

Proof Identifying $k = k1_C \subseteq C$ throughout, we proceed in several steps.

1°. Since n_C is regular on D, Lemma 11.10 yields a decomposition

$$C = D \oplus M, \quad M = D^{\perp} \tag{1}$$

as a direct sum of k-submodules. Associativity of the norm ((16.12.3) and (16.12.4)) implies $MD \subseteq M$ and we claim *that M becomes a right D-module in this way*. Localizing if necessary we may assume that D is generated by a single element (Exc. 19.33 (a)), in which case the assertion follows immediately from the alternative law. We also observe $M \subseteq \mathrm{Ker}(t_C)$ and

$$ax = x\bar{a} \qquad (x \in M, a \in D) \tag{2}$$

since $ax + xa = t_D(a)x$ by (16.5.5) and (1).

2°. Next we define k-bilinear maps $h\colon M \times M \to D$, $\times_D\colon M \times M \to M$ by

$$xy = -h(x,y) + x \times_D y, \quad h(x,y) \in D, \quad x \times_D y \in M, \tag{3}$$

for all $x, y \in M$. From $x^2 = -n_C(x)$ we conclude

$$n_C(x) = h(x,x) \tag{4}$$

and that the map $\times_D$ is alternating. Moreover, $\overline{xy} = \bar{y}\,\bar{x} = (-y)(-x) = yx$ yields

$$\overline{h(x,y)} = h(y,x), \tag{5}$$

hence

$$n_C(x,y) = t_D(h(x,y)). \tag{6}$$

In particular, $h(x,y) = 0$ for all $y \in M$ implies $x = 0$.

3°. We claim *that (M,h) is a hermitian module over D*. By (5), it suffices to show that h is linear in the second variable. Using (16.12.3), (16.12.4) repeatedly and observing that M is a right D-module by 1°, we obtain $n_C(x(yb),a) = n_C((xy)b,a)$ for all $x, y \in M$, $a, b \in D$, and (3) in conjunction with regularity of n_D leads to the required conclusion.

4°. Consider the k-trilinear map $\delta\colon M^3 \to D$ defined by $\delta(x,y,z) = h(x \times_D y, z)$, which by 3° is D-linear in z. We clearly have $\delta(x,x,z) = 0$, but also $\delta(x,y,y) = 0$ since (2), (3) imply $(x \times_D y)y = h(x,y)y + xy^2 = y\overline{h(x,y)} - n_C(y)x \in M$. Hence δ is alternating, forcing it to be in fact D-trilinear, and *we obtain a unique D-linear map $\Delta\colon \bigwedge^3 M \to D$ satisfying*

$$\Delta(x \wedge y \wedge z) = h(x \times_D y, z). \qquad (x,y,z \in M). \tag{7}$$

5°. We now show *that (M,h) is a ternary hermitian space over D, that*

$\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ *is an orientation of* M *satisfying* $\det_\Delta(h) = 1$ *and that* $\times_D$ *is the hermitian vector product induced by* h *and* Δ. The final statement follows immediately from (7) as soon as the preceding ones have been established. To do so, we may assume that k is a local ring, forcing C to arise from D by a twofold application of the Cayley-Dickson construction (Cor. 19.17): there are units $\mu_1, \mu_2 \in k$ satisfying

$$C = \mathrm{Cay}(D; \mu_1, \mu_2) = D \oplus Dj_1 \oplus Dj_2 \oplus Dj_3,$$

where $j_1 \in D^\perp = M$ satisfies $n_C(j_1) = -\mu_1$, $j_2 \in (D \oplus Dj_1)^\perp$ satisfies $n_C(j_2) = -\mu_2$, and $j_3 = j_1 j_2$. Hence, by (1),

$$M = j_1 D \oplus j_2 D \oplus j_3 D.$$

More precisely, (3), (4) and the relations $j_1 j_2 = j_3 \in M$, $j_1 j_3 = \mu_1 j_2 \in M$, $j_3 j_2 = \mu_2 j_1 \in M$ show that (j_1, j_2, j_3) is a basis of M over D with respect to which the matrix of h has the form $\mathrm{diag}(-\mu_1, -\mu_2, \mu_1\mu_2) \in \mathrm{GL}_3(D)$. Hence (M, h) is a ternary hermitian space over D; moreover, $j_1 \times_D j_2 = j_3$ by (3). Thus (7) gives $\Delta(j_1 \wedge j_2 \wedge j_3) = h(j_3, j_3) = \mu_1\mu_2 \in k^\times$, so Δ is indeed an orientation of M. The remaining assertion $\det_\Delta(h) = 1$ now follows from (21.8.1).

6°. In view of 5° we can form the composition algebra $C' := \mathrm{Ter}(D; V, h, \Delta)$ and our construction yields a natural identification $C = C'$ matching D with the first summand of C'. □

21.15 Corollary (Pumplün [241])**.** *If* $2 \in k^\times$*, then every quaternion algebra over* k *has the form* $\mathrm{Ter}(k; M, \beta, \Delta)$*, where* (M, β) *is a ternary symmetric bilinear space over* k *and* Δ *is an orientation of* M *satisfying* $\det_\Delta(\beta) = 1$*. Conversely, every such algebra is a quaternion algebra.* □

21.16 Example. Working over the field $k = \mathbb{R}$ of real numbers, we have

$$\mathbb{O} = \mathrm{Ter}(\mathbb{C}; \mathbb{C}^3, \langle \mathbf{1}_3 \rangle_{\mathrm{sesq}}, \Delta_0), \qquad \mathbb{H} = \mathrm{Ter}(\mathbb{R}; \mathbb{R}^3, \langle \mathbf{1}_3 \rangle, \Delta_0),$$

where Δ_0 is the normalized orientation of 21.10.

The Dickson-Coxeter octonions and the examples in the papers of Knus-Parimala-Sridharan [159] and Thakur [274] show that there are octonion algebras to which the ternary hermitian construction does not apply since they do not contain any quadratic étale subalgebras. On the other hand, if $2 \in k$ is sufficiently far removed from being a unit, then quadratic étale subalgebras always exist.

21.17 Proposition. *Let* C *be a composition algebra of rank* $r > 1$ *over* k *and assume* $2 \in k$ *is contained in the Jacobson radical of* k *(which holds, for example, if* $2 = 0$ *in* k*). Then* C *contains quadratic étale subalgebras.*

Proof By Lemma 19.15, C contains an element u of trace 1. Then $t_C(u)^2 - 4n_C(u) = 1 - 4n_C(u) \in k^\times$ by hypothesis, so $k[u] \subseteq C$ is a quadratic étale subalgebra by Proposition 19.8. □

21.18 Zorn vector matrices. Let $D := k \times k$ be the split quadratic étale k-algebra. Then $\iota = \iota_D$ is the exchange involution, and the free right D-module $D^3 = k^3 \times k^3$ is endowed with the normalized orientation $\Delta\colon \bigwedge^3 D^3 \xrightarrow{\sim} D$ as in 21.8 and with the unit hermitian form $h := \langle \mathbf{1}_3 \rangle_{\mathrm{sesq}}$, which satisfies $\det_\Delta(h) = 1$. Hence we may form the octonion algebra

$$C := \mathrm{Ter}(D; D^3, h, \Delta)$$

over k, which may now be described more explicitly as follows.

Writing elements $a, b \in D$, $x, y \in D^3 = k^3 \times k^3$ as

$$a = (\alpha_1, \alpha_2), \quad b = (\beta_1, \beta_2), \quad x = (u_1, u_2), \quad y = (v_1, v_2) \tag{1}$$

with $\alpha_i, \beta_i \in k$, $u_i, v_i \in k^3$, $i = 1, 2$, we have

$$h(x, y) = \overline{(u_1, u_2)}^{\mathsf{T}}(v_1, v_2) = (u_2, u_1)^{\mathsf{T}}(v_1, v_2),$$

hence

$$h(x, y) = (u_2^{\mathsf{T}} v_1, u_1^{\mathsf{T}} v_2), \tag{2}$$

and applying (21.10.3), we obtain

$$x \times_{h,\Delta} y = \bar{x} \times \bar{y} = (u_2 \times v_2, u_1 \times v_1). \tag{3}$$

Visualizing the elements of $C = D \times D^3$ in matrix form as

$$(a, x) = \begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix}, \quad (b, y) = \begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix},$$

we deduce from (21.12.1), (2), (3) that

$$\begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix}\begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 - u_2^{\mathsf{T}} v_1 & \alpha_1 v_2 + \beta_2 u_2 + u_1 \times v_1 \\ \beta_1 u_1 + \alpha_2 v_1 + u_2 \times v_2 & \alpha_2\beta_2 - u_1^{\mathsf{T}} v_2 \end{pmatrix}. \tag{4}$$

Consulting Thm. 21.12, we therefore conclude that the multiplication rule (4) converts the k-module

$$\mathrm{Zor}(k) := \begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix} \tag{5}$$

into an octonion algebra, called the octonion algebra of *Zorn vector matrices* over k. Norm, trace and conjugation of this octonion algebra are given by

$$n_{\mathrm{Zor}(k)}\left(\begin{pmatrix}\alpha_1 & u_2\\ u_1 & \alpha_2\end{pmatrix}\right) = \alpha_1\alpha_2 + u_1^{\mathsf{T}}u_2, \tag{6}$$

$$t_{\mathrm{Zor}(k)}\left(\begin{pmatrix}\alpha_1 & u_2\\ u_1 & \alpha_2\end{pmatrix}\right) = \alpha_1 + \alpha_2, \tag{7}$$

$$\overline{\begin{pmatrix}\alpha_1 & u_2\\ u_1 & \alpha_2\end{pmatrix}} = \begin{pmatrix}\alpha_2 & -u_2\\ -u_1 & \alpha_1\end{pmatrix}. \tag{8}$$

21.19 Split composition algebras. Let C be a composition algebra over k. We say that C is

(a) *split of rank* 1 if $C \cong k$,
(b) *split of rank* 2 or *split quadratic étale* if $C \cong k \times k$ (as a direct product of ideals).
(c) *split of rank* 4 or a *split quaternion algebra* if $C \cong \mathrm{Mat}_2(k)$,
(d) *split of rank* 8 or a *split octonion algebra* if $C \cong \mathrm{Zor}(k)$.

In case k is the zero ring, we define the zero module to be a split composition algebra.

If C is a composition algebra over a nonzero ring k, we consider the rank decomposition of C (Exc. 9.31), which in the special case at hand, thanks to Cor. 19.18, has the form

$$k = k_0 \times k_1 \times k_2 \times k_3, \quad k_i := k\varepsilon_i \qquad (0 \le i \le 3), \tag{1}$$

$$C = C_0 \times C_1 \times C_2 \times C_3, \quad C_i := C \otimes k_i \qquad (0 \le i \le 3) \tag{2}$$

as direct products of ideals induced by a complete orthogonal system $(\varepsilon_i)_{0\le i\le 3}$ of idempotents in k uniquely determined by the condition that C_i is a composition algebra of rank 2^i over k_i for $0 \le i \le 3$. Then C is said to be *split* if C_i is split of rank 2^i for all $i = 0, 1, 2, 3$. Note that the property of a composition algebra to be split is stable under base change.

For the split composition algebras of rank $r = 1, 2, 4, 8$ over k exhibited in (a)–(d) above, it is sometimes helpful to introduce a unified notation. We put

$$C_{0r}(k) := \begin{cases} k & \text{for } r = 1,\\ k \times k & \text{for } r = 2,\\ \mathrm{Mat}_2(k) & \text{for } r = 4,\\ \mathrm{Zor}(k) & \text{for } r = 8 \end{cases} \tag{3}$$

and have

$$C_{0r}(k)_R = C_{0r}(R)$$

for all $R \in k$-**alg**. We call $C_{0r}(k)$ the *standard* split composition algebra of rank r over k.

Exercises

21.20. Let D be a quadratic étale k-algebra, M, N be right D-modules and $h\colon M \times N \to D$ a sesquilinear form. Prove that exterior powers of h are compatible with base change, i.e., for all positive integers n and all $R \in k$-**alg**, the identifications 21.4 yield $(\bigwedge^n h)_R = \bigwedge^n(h_R)$.

21.21. Let D be a quadratic étale k-algebra, use Exc. 19.32 to identify $k = H(D, \iota_D) \subseteq D$ canonically, and let (M, h) be a hermitian space of rank n over D.

(a) If k is an LG ring, show that h can be diagonalized: there exist a basis $(e_i)_{1\le i\le n}$ of M as a right D-module and scalars $\alpha_1, \dots, \alpha_n \in k^\times$ such that $h(e_i, e_j) = \delta_{ij}\alpha_i$ for $1 \le i, j \le n$. In particular, M is a free right D-module of finite rank.

(b) Deduce from (a) that (M, q), where M is viewed canonically as a k-module and $q\colon M \to k$ is defined by $q(x) := h(x, x)$ for $x \in M$, is a quadratic space of rank $2n$ over k.

21.22. *Isotopes of the ternary hermitian construction.* Let D be a quadratic étale k-algebra, (M, h) a ternary hermitian space over D and $\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ an orientation of M satisfying $\det_\Delta(h) = 1$. Put $C = \mathrm{Ter}(D; M, h, \Delta)$. For $p \in D^\times \subseteq C^\times$, we refer to the concept of unital p-isotopes as defined in 15.9 and have $D = D^p \subseteq C^p$, so Theorem 21.14 yields a ternary hermitian space $(M, h)^p = (M^p, h^p)$ over D and an orientation Δ^p of M^p such that $C^p = \mathrm{Ter}(D; M^p, h^p, \Delta^p)$. Describe M^p, h^p, Δ^p explicitly. What does this description mean for the octonion algebras of Zorn vector matrices?

21.23 (Thakur [274])**.** For $i = 1, 2$, let (M_i, h_i) be a ternary hermitian space over a quadratic étale k-algebra D and let $\Delta_i\colon \bigwedge^3 M_i \xrightarrow{\sim} D$ be an orientation of M_i satisfying $\det_{\Delta_i}(h_i) = 1$. Put

$$C_i := \mathrm{Ter}(D; M_i, h_i, \Delta_i) = D \times M_i \qquad (i = 1, 2)$$

and prove for any map $\chi\colon M_1 \to M_2$ that the following conditions are equivalent.

(i) $\chi\colon (M_1, h_1, \Delta_1) \xrightarrow{\sim} (M_2, h_2, \Delta_2)$ is an *isomorphism*, i.e., $\chi\colon (M_1, h_1) \xrightarrow{\sim} (M_2, h_2)$ is an isometry satisfying $\Delta_2 \circ (\bigwedge^3 \chi) = \Delta_1$.

(ii) $\chi\colon (M_1, h_1) \xrightarrow{\sim} (M_2, h_2)$ is an isometry satisfying

$$\chi(x \times_{h_1,\Delta_1} y) = \chi(x) \times_{h_2,\Delta_2} \chi(y). \qquad (x, y \in M_1).$$

(iii) $\mathbf{1}_D \times \chi\colon C_1 \xrightarrow{\sim} C_2$ is an isomorphism.

21.24. *A presentation of the split octonions.* Show that $C := \mathrm{Zor}(k)$ is the free unital

alternative k-algebra on three generators E, X_1, X_2 satisfying the relations

$$E^2 = E, \quad X_1^2 = X_2^2 = 1_C, \quad X_1X_2X_1 = -X_2, \tag{1}$$
$$X_1EX_1 = X_2EX_2 = -(X_1X_2)E(X_1X_2) = \bar{E} := 1_C - E,$$

i.e., that C has three generators E, X_1, X_2 satisfying (1) and, conversely, given any unital alternative k-algebra A and three element $e, x_1, x_2 \in A$ such that (1) holds (after the obvious notational adjustments), there exists a unique homomorphism $C \to A$ of unital k-algebras sending E, X_1, X_2 respectively to e, x_1, x_2. Conclude that, for some ideal $\mathfrak{a} \subseteq k$, the subalgebra of A generated by e, x_1, x_2 is isomorphic to $\mathrm{Zor}(k/\mathfrak{a})$ as a k-algebra.

22 Reduced composition algebras

In the classical theory of finite-dimensional linear non-associative algebras over fields, the standard way to define the notion of a reduced algebra consists in requiring the existence of a complete orthogonal system of absolutely primitive idempotents. This approach will be adapted here to the setting of composition algebras over arbitrary commutative rings. We then proceed to explore more accurately the structure of reduced composition algebras and compare it with the more restrictive notion of splitness as defined in 21.19.

Throughout we let k be an arbitrary commutative ring.

22.1 Primitive and absolutely primitive idempotents. Recall from, e.g., Braun-Koecher [36, p. 52] or Schafer [254, pp. 39, 56], see also Exc. 8.13, that an idempotent of an algebra over a field is said to be *primitive* if it is non-zero and it cannot be decomposed into the sum of two non-zero orthogonal idempotents; we speak of an *absolutely primitive* idempotent if it remains primitive in every base field extension. These definitions have natural extensions to algebras over arbitrary commutative rings as follows.

Let A be a k-algebra. An idempotent $c \in A$ is called *primitive* if $c \neq 0$ and for all orthogonal idempotents $c_1, c_2 \in A$ satisfying $c = c_1 + c_2$, there exists a complete orthogonal system $(\varepsilon_1, \varepsilon_2)$ of idempotents in k such that $c_i = \varepsilon_i c$ for $i = 1, 2$; this notion obviously reduces to the previous one if k is a field (or, more generally, a *connected* commutative ring). The idempotent c is said to be *absolutely primitive* if it remains primitive in A_R for every non-zero $R \in k$-**alg**.

Note that for an alternative algebra A over a field, an idempotent $c \in A$ is primitive if and only if the subalgebra $A_{11}(c) \subseteq A$ contains no idempotents other than 0 and c.

22.2 Example. The identity element of the k-algebra k is an absolutely primitive idempotent if and only if $k \neq \{0\}$. On the other hand, it is an elementary idempotent in the sense of Exc. 16.23 if and only if $k = \{0\}$.

22.3 Proposition. *Let A be an algebra over k and suppose A is finitely generated projective as a k-module. Then every absolutely primitive idempotent of A is a unimodular element.*

Proof Let $c \in A$ be an absolutely primitive idempotent. Then, for all $\mathfrak{p} \in \operatorname{Spec}(k)$, the idempotent $c(\mathfrak{p}) \in A(\mathfrak{p})$ is primitive, hence non-zero. The assertion follows from Lemma 9.17. □

22.4 Separable alternative algebras over rings. A unital alternative algebra C over k is said to be *separable* if

(i) C is projective as a k-module.
(ii) $\operatorname{Nil}(C_F) = \{0\}$ for all fields $F \in k$-**alg**.

We claim that *composition algebras are separable alternative.* Indeed, condition (i) is part of the definition and alternativity follows from Thm. 19.13. In order to establish condition (ii), it suffices to show that a composition algebra C over a field F, being automatically finite-dimensional, satisfies $\operatorname{Nil}(C) = \{0\}$. Since the norm of C is a non-degenerate quadratic form by definition, this follows immediately from Exc. 17.9.

For a finite-dimensional separable alternative algebra, the property of an idempotent to be absolutely primitive can be characterized by means of its Peirce decomposition (Exc. 14.12).

22.5 Proposition. *Let A be a separable alternative algebra over k that is finitely generated as a k-module. For an idempotent $c \in A$ to be absolutely primitive it is necessary and sufficient that $A_{11}(c)$ be free of rank 1 as a k-module. In this case, c is a basis of $A_{11}(c)$.*

Proof Note first that by Exc. 14.12 the Peirce components of A relative to c are compatible with base change, i.e., $A_{ij}(c)_R \cong (A_R)_{ij}(c_R)$ canonically, for all $i, j = 1, 2$, $R \in k$-**alg**. In order to prove sufficiency, suppose $A_{11}(c)$ is free of rank 1 as a k-module. Then c is a basis of $A_{11}(c)$ and obviously a primitive idempotent, hence an absolutely primitive one since the property of $A_{11}(c)$ to be free of rank 1 remains stable under base change. Conversely, in order to prove necessity, suppose c is absolutely primitive. The Peirce decomposition shows that $A_{11}(c)$ is finitely generated projective as a k-module. For any prime ideal $\mathfrak{p} \subseteq k$, let $K \in k$-**alg** be the algebraic closure of the residue field $k(\mathfrak{p})$. Then $c_K \in A_K$ is a primitive idempotent and $\operatorname{Nil}(A_K) = \{0\}$ by separability. We conclude that $A_{11}(c)_K \cong (A_K)_{11}(c_K)$ has nil radical equal to $\{0\}$ [252, Cor. 3.8], whence $A_{11}(c)_K$ by [252, Lemma 3.5 and Thm. 3.7] is a finite-dimensional alternative division algebra over the algebraically closed field K. By Exc. 8.16,

this implies $\mathrm{rk}_{\mathfrak{p}}(A_{11}(c)) = \dim_K((A_K)_{11}(c_K)) = 1$, so $A_{11}(c)$ is a line bundle. But $c \in A_{11}(c)$ is a unimodular vector by Prop. 22.3, forcing $A_{11}(c)$ to be free of rank 1 with basis c. □

22.6 Reduced composition algebras. A composition algebra over k is said to be *reduced* if it contains an absolutely primitive idempotent. The base ring k itself is clearly a reduced composition algebra of rank 1. In order to describe the reduced composition algebras of rank > 1, we require a few preparations. The first one of these connects absolutely primitive idempotents with elementary ones as defined in Exc. 16.23.

22.7 Proposition. *If $k \neq \{0\}$, then elementary idempotents of conic algebras over k are absolutely primitive. Conversely, if C is a composition algebra of rank $r > 1$ over k, then every absolutely primitive idempotent in C is elementary.*

Proof Let C be a conic k-algebra and suppose $c \in C$ is an elementary idempotent. Since the property of an idempotent to be elementary is stable under base change, it suffices to show for the first part of the proposition that c is primitive. Accordingly, assume $c = c_1 + c_2$ with orthogonal idempotents $c_i \in C$, $i = 1, 2$. Then $2c_i = c \circ c_i = t_C(c)c_i + t_C(c_i)c - n_C(c, c_i)1_C$ and we conclude $c_i = t_C(c_i)c - n_C(c, c_i)1_C$. Multiplying this by c, we obtain $c_i = \varepsilon_i c$ for some $\varepsilon_i \in k$, and since c is unimodular, $(\varepsilon_1, \varepsilon_2)$ is a complete orthogonal system of idempotents in k. Thus c is primitive, as claimed.

For the second part of the proposition, assume C is a composition algebra of rank $r > 1$ and let $c \in C$ be an absolutely primitive idempotent. Then so is c_R, for any $R \in k$-**alg**, $R \neq \{0\}$. This gives $c_R \neq 0$ by definition, but also $c_R \neq 1_{C_R}$ since $r > 1$ and $C_{11}(c)$ is free of rank 1 as a k-module by Prop. 22.5. Hence c is elementary. □

22.8 Remark. The proof of the first part of the preceding proposition shows, more generally,

$$kc = \{x \in C \mid cx = x = xc\}$$

for any elementary idempotent in a conic algebra C over k.

22.9 Proposition. *Let C be a composition algebra of rank $r > 1$ over k. Then the following conditions are equivalent.*

(i) *C is reduced.*
(ii) *C contains a split quadratic étale subalgebra.*
(iii) *The norm of C is isotropic.*

(iv) The norm of C is hyperbolic.

If these conditions are fulfilled and $c \in C$ is an absolutely primitive idempotent, then

$$n_C \cong \mathbf{h}_{kc \oplus C_{12}(c)}. \tag{1}$$

Proof (i) $\Rightarrow$ (ii). By definition and Prop. 22.7, C contains an elementary idempotent c, whence Exc. 16.23 shows that $kc \oplus k\bar{c} \subseteq C$ is a split quadratic étale subalgebra.

(ii) $\Rightarrow$ (iii). Let $D \subseteq C$ be a split quadratic étale subalgebra. Since $n_D = n_C|_D$ is isotropic (Example 16.2 (d)), so is n_C.

(iii) $\Rightarrow$ (i). Choose an isotropic vector $u \in C$ relative to n_C. Since u is unimodular and n_C is regular, some $v \in C$ satisfies $t_C(uv) = n_C(u, \bar{v}) = 1$. But $n_C(uv) = n_C(u)n_C(v) = 0$, so (by Exc. 16.23) $c = uv \in C$ is an elementary, hence absolutely primitive, idempotent.

(i) $\Rightarrow$ (iv). Let $c \in C$ be an absolutely primitive idempotent with Peirce components $C_{ij} = C_{ij}(c)$, $i, j = 1, 2$. By Prop. 22.7, c is elementary, and (3), (4) of Exc. 19.35 imply that the norm n_C determines a duality between the k-modules $kc \oplus C_{12}$ and $k\bar{c} \oplus C_{21}$, on which it is identically zero. Hence (1) and (iv) follow.

(iv) $\Rightarrow$ (iii). If (iv) holds, $C = M_1 \oplus M_2$ may be written as the direct sum of two totally isotropic submodules $M_i \subseteq C$ relative to n_C, $i = 1, 2$. In particular, $1_C = e_1 + e_2$, $e_i \in M_i$, $i = 1, 2$, which implies $n_C(e_i) = 0$, $1 = n_C(1_C) = n_C(e_1, e_2)$. Thus (e_1, e_2) is a hyperbolic pair in (C, n_C). □

22.10 Corollary. *The reduced composition algebras of rank 2 over k are precisely the split quadratic étale k-algebras.* □

22.11 Example. Let B be a regular associative composition k-algebra of constant rank. For every $b \in B^\times$, we obtain a composition k-algebra $\mathrm{Cay}(B, n_B(b))$ that is regular by Theorem 19.14. We claim that $\mathrm{Cay}(B, n_B(b))$ *is reduced.* To see this, note that the algebra is isomorphic to $C := \mathrm{Cay}(B, 1)$ by Exc. 18.19, so we may assume that $n_B(b) = 1$. By Lemma 19.15, there exists an element $u \in B$ having $t_B(u) = 1$. Setting $c := u + uj \in C$, we apply (18.4.5) and (18.4.3) to conclude $t_C(c) = 1$, $n_C(c) = 0$, so c is an elementary idempotent in C and hence a primitive one. Thus C is reduced.

22.12 Twisted 2-by-2 matrices. Let L be a line bundle over k. Then there is a natural identification

$$\mathrm{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}$$

as k-algebras, where multiplication on the right is the usual matrix product, taking advantage of the canonical pairing $L^* \times L \to k$ at the appropriate place. We claim that $C := \mathrm{End}_k(k \oplus L)$ *is a quaternion algebra over* k, with norm, trace, conjugation respectively given by

$$n_C\left(\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}\right) = \alpha_1\alpha_2 - \langle u^*, v\rangle, \tag{1}$$

$$t_C\left(\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}\right) = \alpha_1 + \alpha_2, \tag{2}$$

$$\overline{\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}} = \begin{pmatrix} \alpha_2 & -u^* \\ -v & \alpha_1 \end{pmatrix}. \tag{3}$$

for $\alpha_1, \alpha_2 \in k$, $u^* \in L^*$ and $v \in L$. Since passing to the dual of a finitely generated projective module by Lemma 9.15 commutes with base change, so does the construction of C. Hence our claim may be checked locally, in which case L is a free k-module of rank 1 and C becomes isomorphic to the split quaternion algebra of 2-by-2 matrices, with (1)–(3) converted into the formulas for the ordinary determinant, trace, conjugation, respectively, of 2-by-2 matrices. We call $C = \mathrm{End}_k(k \oplus L)$ the quaternion algebra of *L-twisted 2-by-2 matrices* over k. Note that

$$e := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e' := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{4}$$

form a complete orthogonal system of elementary idempotents in C with off-diagonal Peirce components

$$C_{12}(e) = \begin{pmatrix} 0 & L^* \\ 0 & 0 \end{pmatrix}, \quad C_{21}(e) = \begin{pmatrix} 0 & 0 \\ L & 0 \end{pmatrix}. \tag{5}$$

We can now characterize reduced quaternion algebras in the following way.

22.13 Proposition (Petersson [216, Cor. 2.7])**.** *Up to isomorphism, the reduced quaternion algebras over k are precisely the quaternion algebras of L-twisted 2-by-2 matrices, for some line bundle L over k. More precisely, let C be a quaternion algebra over k and $c \in C$ an absolutely primitive idempotent. Then there exist a line bundle L over k and an isomorphism*

$$\phi\colon C \xrightarrow{\sim} \mathrm{End}_k(k \oplus L)$$

such that

$$\phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{1}$$

If L is a free module, then C is split.

Proof Let L be a line bundle over k. By (22.12.1), the norm of $C := \mathrm{End}_k(k \oplus L)$ is hyperbolic, and Prop. 22.9 shows that C is reduced. Conversely, suppose C is a reduced quaternion algebra over k and $c_1 := c \in C$ is an absolutely primitive idempotent. Then c is an elementary idempotent by Prop. 22.7, so the corresponding Peirce decomposition of C takes on the form $C = kc_1 \oplus C_{12} \oplus C_{21} \oplus kc_2$, with $c_2 := 1_C - c_1$ and finitely generated projective k-modules C_{12}, C_{21} which, by Exc. 19.35, are in duality under the bilinearized norm. Counting ranks, we conclude that $L := C_{21}$ is a line bundle over k and $C_{12} = L^*$ under the natural identification induced by the bilinearized norm. Since C is associative, Exc. 14.12 shows $C_{ij}^2 = \{0\}$. By the same token, given $x_{21} \in C_{21}$, $y_{21}^* \in C_{12}$, we obtain $y_{21}^* x_{21} = \alpha c_1$ for some $\alpha \in k$, and taking traces in conjunction with (6) of Exc. 19.35, yields

$$\alpha = t_C(y_{21}^*, x_{21}) = n_C(y_{21}^*, \bar{x}_{21}) = -n_C(y_{21}^*, x_{21}) = -\langle y_{21}^*, x_{21}\rangle.$$

Thus $y_{21}^* x_{21} = -\langle y_{21}^*, x_{21}\rangle c_1$. But then

$$x_{21}y_{21}^* = (-\bar{x}_{21})(-\bar{y}_{21}^*) = \bar{x}_{21}\bar{y}_{21}^* = \overline{y_{21}^* x_{21}} = -\langle y_{21}^*, x_{21}\rangle c_2.$$

Now one checks easily that

$$\phi\colon C \xrightarrow{\sim} \mathrm{End}(k \oplus L), \quad \alpha_1 c_1 \oplus x_{21}^* \oplus x_{21} + \alpha_2 c_2 \longmapsto \begin{pmatrix} \alpha_1 & -x_{21}^* \\ x_{21} & \alpha_2 \end{pmatrix}$$

is an isomorphism of quaternion algebras having the desired property.

The final claim, that C is split if L is free, was already observed in 22.12. □

22.14 Twisted Zorn vector matrices. Let M be a finitely generated projective k-module of rank 3 and θ an orientation of M, i.e., a k-linear bijection $\theta\colon \bigwedge^3 M \xrightarrow{\sim} k$. Dualizing by means of the identification 21.7, we obtain a k-linear bijection $\theta^*\colon k = k^* \xrightarrow{\sim} (\bigwedge^3 M)^* = \bigwedge^3(M^*)$, hence an induced orientation θ^{*-1} on M^* uniquely determined by the condition

$$\theta(v_1 \wedge v_2 \wedge v_3)\theta^{*-1}(v_1^* \wedge v_2^* \wedge v_3^*) = \det\left(\left(\langle v_i^*, v_j\rangle\right)_{1\le i,j\le 3}\right) \tag{1}$$

for $v_j \in M$, $v_i^* \in M^*$, $1 \le i, j \le 3$. These two orientations in turn give rise to alternating bilinear maps

$$M \times M \longrightarrow M^*, \quad (v, w) \longmapsto v \times_\theta w,$$
$$M^* \times M^* \longrightarrow M, \quad (v^*, w^*) \longmapsto v^* \times_\theta w^*,$$

called the *associated vector products*, according to the rules

$$\theta(u \wedge v \wedge w) = \langle u \times_\theta v, w\rangle, \quad \theta^{*-1}(u^* \wedge v^* \wedge w^*) = \langle w^*, u^* \times_\theta v^*\rangle \tag{2}$$

for $u, v, w \in M, u^*, v^*, w^* \in M^*$. Now the k-module

$$\mathrm{Zor}(M, \theta) = \begin{pmatrix} k & M^* \\ M & k \end{pmatrix}$$

becomes a unital k-algebra under the multiplication

$$\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} \begin{pmatrix} \beta_1 & w^* \\ w & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 - \langle v^*, w\rangle & \alpha_1 w^* + \beta_2 v^* + v \times_\theta w \\ \beta_1 v + \alpha_2 w + v^* \times_\theta w^* & -\langle w^*, v\rangle + \alpha_2\beta_2 \end{pmatrix} \tag{3}$$

for $\alpha_i, \beta_i \in k$, $v, w \in M$, $v^*, w^* \in M^*$, $i = 1, 2$, whose unit element is the identity matrix $\mathbf{1}_2$. We call $\mathrm{Zor}(M, \theta)$ the algebra of (M, θ)-*twisted Zorn vector matrices* over k. We claim that $C := \mathrm{Zor}(M, \theta)$ *is an octonion algebra over* k, with norm, trace, conjugation given by

$$n_C\left(\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}\right) = \alpha_1\alpha_2 - \langle u^*, v\rangle, \tag{4}$$

$$t_C\left(\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}\right) = \alpha_1 + \alpha_2, \tag{5}$$

$$\overline{\begin{pmatrix} \alpha_1 & u^* \\ v & \alpha_2 \end{pmatrix}} = \begin{pmatrix} \alpha_2 & -u^* \\ -v & \alpha_1 \end{pmatrix}. \tag{6}$$

for $\alpha_1, \alpha_2 \in k$, $u^* \in M^*$, $v \in M$. Since the construction of C, as in the quaternionic case, commutes with base change, this may be checked locally, so we may assume that M is a free k-module of rank 3. Hence there exist elements $u_1, u_2, u_3 \in M$ satisfying the following equivalent conditions.

(i) $\mathcal{B} := (u_1, u_2, u_3)$ is a basis of M.

(ii) $u_1 \wedge u_2 \wedge u_3 \in \bigwedge^3(M)$ is unimodular.

(iii) $\theta(u_1 \wedge u_2 \wedge u_3) \in k^\times$.

Replacing, e.g., u_3 by an appropriate scalar multiple, we may therefore assume $\mathcal{B}$ to be θ-*balanced* in the sense that $\theta(u_1 \wedge u_2 \wedge u_3) = 1$. Hence we find a natural identification $M = k^3$ such that $\mathcal{B} = (e_1, e_2, e_3)$ is the basis of ordinary unit vectors and $\theta = \det\colon \bigwedge^3(k^3) \to k$ is given by the ordinary determinant. This in turn yields a natural identification $M^* = k^3$ such that the canonical pairing $M^* \times M \to k$ agrees with the map $k^3 \times k^3 \to k$, $(u, v) \mapsto u^{\mathsf{T}}v$. Thus the basis $(e_i)_{1 \le i \le 3}$ is self-dual, and applying (1) we conclude $\theta^{*-1} = \det$ as well. Hence both vector products $\times_{\det}$ agree with the ordinary vector product $\times$ on k^3 and $\mathrm{Zor}(k^3, \det) = \mathrm{Zor}(k)$ is the same as the algebra of ordinary Zorn vector matrices over k. The assertion follows. As in the case of reduced quaternion

algebras,

$$e := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e' := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{7}$$

form a complete orthogonal system of elementary idempotents in C with off diagonal Peirce components

$$C_{12}(e) = \begin{pmatrix} 0 & M^* \\ 0 & 0 \end{pmatrix}, \quad C_{21}(e) = \begin{pmatrix} 0 & 0 \\ M & 0 \end{pmatrix}. \tag{8}$$

22.15 Theorem (Petersson [216, Thm. 3.5])**.** *Up to isomorphism, the reduced octonion algebras over k are precisely the algebras of (M, θ)-twisted Zorn vector matrices, for some finitely generated projective k-module M of rank 3 and some orientation θ of M. More precisely, given an octonion algebra C over k and an absolutely primitive idempotent $c \in C$, there exist M, θ as above and an isomorphism $\phi\colon C \xrightarrow{\sim} \mathrm{Zor}(M, \theta)$ such that*

$$\phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{1}$$

If M is a free module, then C is split.

Proof Let M be a finitely generated projective k-module of rank 3 and θ an orientation of M. Then (22.14.4) shows that the norm of the octonion algebra $\mathrm{Zor}(M, \theta)$ is hyperbolic, forcing the algebra itself to be reduced (Prop. 22.9). Conversely, suppose C is a reduced octonion algebra over k and $c_1 := c \in C$ is an absolutely primitive idempotent. Then c is an elementary one by Prop. 22.7, so the corresponding Peirce decomposition takes on the form $C = kc_1 \oplus C_{12} \oplus C_{21} \oplus kc_2$, with $c_2 := 1_C - c_1$ and finitely generated projective k-modules C_{12}, C_{21} in duality under the bilinearized norm (Exc. 19.35). Counting ranks, we conclude that $M := C_{21}$ is a finitely generated projective k-module of rank 3 and $C_{12} = M^*$ under the natural identification induced by the bilinearized norm. Given $v \in M = C_{21}$, $u^* \in M^* = C_{12}$, we claim

$$u^*v = -\langle u^*, v\rangle c_1, \quad vu^* = -\langle u^*, v\rangle c_2. \tag{2}$$

Indeed, the Peirce rule (3) of Exc. 14.12, yield $u^*v = \alpha c_1$ for some $\alpha \in k$, and taking traces in conjunction with (6) of Exc. 19.35, we conclude

$$\alpha = t_C(u^*v) = n_C(u^*, \bar{v}) = -n_C(u^*, v) = -\langle u^*, v\rangle.$$

Hence the first equation of (2) holds; the second one follows by applying the conjugation. Now combine (16.12.5) with Exc. 19.35, and observe that the expression $t_C(uvw) = n_C(uv, \bar{w}) = -n_C(uv, w)$ is alternating trilinear in $u, v, w \in$

M. Since $M^2 \subseteq M^*$ by the Peirce rules (Exc. 14.12), we therefore obtain a unique linear map $\theta\colon \bigwedge^3(M) \to k$ such that

$$\theta(u \wedge v \wedge w) = -t_C(uvw) = n_C(uv, w) = \langle uv, w\rangle \qquad (u, v, w \in M). \tag{3}$$

We claim that θ *is an isomorphism.* In order to see this, we may assume that k is a local ring and first treat the case that k is a field. Then we must show $\theta \neq 0$. Otherwise, $\langle uv, w\rangle = n_C(uv, w) = 0$ for all $u, v, w \in M$, hence $M^2 = \{0\}$. But then, given $u, v \in M$, $w^* \in M^*$, linearized right alternativity yields $(uv)w^* + (uw^*)v = u(vw^*) + u(w^*v)$, which combines with (2) to imply $\langle w^*, u\rangle c_2 v = \langle w^*, v\rangle(uc_2 + uc_1)$, hence the contradiction $\langle w^*, u\rangle v = \langle w^*, v\rangle u$. We are left with the case that k is a local ring. Given any basis (u_1, u_2, u_3) of M, the case just treated implies that $\theta(u_1 \wedge u_2 \wedge u_3)$ does not vanish after passing to the residue field of k. Hence $\theta(u_1 \wedge u_2 \wedge u_3)$ is invertible in k, and we conclude that θ is indeed an isomorphism. Moreover, combining (3) with (22.14.2) we obtain $u \times_\theta v = uv$ for the associated vector product of $u, v \in M$. Our next aim is to prove

$$\theta^{*-1}(u^* \wedge v^* \wedge w^*) = n_C(u^*v^*, w^*) = \langle w^*, u^*v^*\rangle \qquad (u^*, v^*, w^* \in M^*). \tag{4}$$

Localizing if necessary, we may assume that M is a free k-module, with basis $(e_i)_{1\leq i\leq 3}$ chosen in such a way that $\theta(e_1 \wedge e_2 \wedge e_3) = 1$. If we write $(e_i^*)_{1\leq i\leq 3}$ for the corresponding dual basis of M^*, then (22.14.1) shows $\theta^{*-1}(e_1^* \wedge e_2^* \wedge e_3^*) = 1$, and since both sides of (4) are alternating trilinear in u^*, v^*, w^*, the proof will be complete once we have shown $e_1^*e_2^* = e_3$. Consulting (3), and making use of its alternating character, we obtain $e_1e_2 = e_3^*$, whence a cyclic change of variables also yields $e_2e_3 = e_1^*$, $e_3e_1 = e_2^*$. Since $\bar{e}_i = -e_i$, $\bar{e}_i^* = -e_i^*$ for $i = 1, 2, 3$ by (6) of Exc. 19.35, the middle Moufang identity (13.3.3) combined with (17.4.2) yields

$$\begin{aligned} e_1^*e_2^* = \bar{e}_1^*\bar{e}_2^* &= (e_3e_2)(e_1e_3) = e_3(e_2e_1)e_3 = -e_3(e_1e_2)e_3 = -e_3e_3^*e_3 \\ &= -n_C(e_3, \bar{e}_3^*)e_3 + n_C(e_3)\bar{e}_3^* = \langle e_3^*, e_3\rangle e_3 = e_3, \end{aligned}$$

and (4) is proved. Consequently, $u^* \times_\theta v^* = u^*v^* \in M$ is the corresponding vector product of $u^*, v^* \in M^*$. Now one checks that $\phi\colon C \xrightarrow{\sim} \mathrm{Zor}(M, \theta)$ defined by

$$\phi(\alpha_1 c_1 + v^* + u + \alpha_2 c_2) := \begin{pmatrix} \alpha_1 & v^* \\ u & \alpha_2 \end{pmatrix}$$

for $\alpha_1, \alpha_2 \in k$, $v^* \in M^* = C_{12}$, $u \in M = C_{21}$ is an isomorphism of octonion algebras satisfying (1).

The final claim, that C is split if M is free, was already observed in 22.14. □

The next results concern rings k such that every projective k-module of constant finite rank is free. Examples of such rings are principal ideal domains and LG rings (Prop. 11.24). Exercises 22.27 and 22.30 provide related results for Dedekind domains.

22.16 Corollary. *Split composition algebras over any commutative ring are reduced. Conversely, if every projective k-module of constant finite rank is free, then every reduced composition algebra over k is split.*

Proof Let C be a composition algebra over k. Combining the rank decomposition (Exc. 9.31) with Example 22.2, we may assume that C has constant rank $r > 1$. If C is split, hence isomorphic to one of the algebras in 21.19 (b)–(d), it contains an elementary idempotent, which is absolutely primitive by Prop. 22.7. Thus C is reduced. Conversely, assume C is reduced. If projective k-modules of constant finite rank are free, splitness of C follows from Cor. 22.10 combined with Prop. 22.13 and Thm. 22.15. □

22.17 Corollary. *Suppose every projective k-module of constant finite rank is free. Then the automorphism group of a composition algebra C over k acts transitively on the elementary idempotents of C.*

Proof Using the rank decomposition (Exc. 9.31), we reduce to the case that C has rank $r = 1, 2, 4, 8$ as a k-module. The case $r = 1$ (resp. $r = 2$) is empty (resp. trivial). The case $r = 4$ is analogous to the case $r = 8$ (only easier), so let us assume $r = 8$. Let e be an elementary idempotent of C. Then e is absolutely primitive (Prop. 22.7), and Thm. 22.15 yields an isomorphism $C \to \mathrm{Zor}(M, \theta)$ sending e to

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{1}$$

for some finitely generated projective k-module M of rank 3 and some orientation θ of M. But M is free by hypothesis. By 22.14, therefore, (M, θ) is isomorphic to $(k^3, \det)$, so we find an isomorphism $\mathrm{Zor}(M, \theta) \to \mathrm{Zor}(k)$ extending the identity on the diagonals of both algebras. Summing up, therefore, we find an isomorphism $C \to \mathrm{Zor}(k)$ sending e to the idempotent (1). The assertion follows. □

22.18 Corollary. *Suppose every projective k-module of constant finite rank is free. For a composition algebra C of constant rank > 1 over k, the following conditions are equivalent.*

(i) *C is split.*
(ii) *The norm of C is isotropic.*

(iii) *The norm of C is hyperbolic.*

Moreover, if $k = F$ is a field, they are also equivalent to

(iv) *C is not a division algebra.*

Proof By Cor. 22.16, C is split if and only if it is reduced. Thus (i)–(iii) are equivalent (Prop. 22.9). Moreover, if $k = F$ is a field, the implication (i)⇒(iv) is obvious, while (iv)⇒(ii) follows from Prop. 17.5. □

22.19 Corollary. *Let k be a principal ideal domain with field of fractions F. For a composition algebra C of rank $r > 1$ over k, the following conditions are equivalent.*

(i) *C_F is split.*
(ii) *n_C is isotropic in the sense of 11.17.*
(iii) *n_C represents zero in the sense of Exc. 12.38.*
(iv) *C has left or right zero divisors in the sense of Exc. 18.20.*
(v) *C is split.*

We remark that the equivalence of (iv) and (v) is due to van der Blij-Springer [286, (3.4)], see also [216, Cor. 3.6].

Proof (i) ⇒ (ii). Because C_F is split, $(n_C)_F$ is isotropic. Because k is a principal ideal domain, Exc. 12.38 (b),(c) yield that n_C is isotropic.

(ii) ⇒ (iii). Obvious.

(iii) ⇒ (iv). Some non-zero $u \in C$ has $n_C(u) = 0$. This implies $u\bar{u} = 0$, so u is a left and $\bar{u}$ a right zero divisor in C.

(iv) ⇒ (v). Since k is an integral domain, Exc. 18.20 yields a non-zero element $u \in C$ such that $n_C(u) = 0$. On the other hand, k being a PID, C is free of finite rank as a k-module. Letting $(e_i)_{1\le i\le r}$ be a k-basis of C, we write $u = \sum_{i=1}^r \alpha_i e_i$ for some $\alpha_1, \dots, \alpha_r \in k$ not all zero. In fact, dividing by their greatest common divisor, we may assume that they are mutually prime, so we can find $\beta_1, \dots, \beta_r \in k$ such that $\sum_{i=1}^r \alpha_i\beta_i = 1$. Since C has rank > 1, it is regular, allowing us to consider the Dn_C-dual basis $(f_i)_{1\le i\le r}$ of C relative to (e_i). Setting $v := \sum_{i=1}^r \beta_i f_i \in C$, we therefore obtain $n_C(u, v) = 1$. Thus $c := u\bar{v}$ satisfies $t_C(c) = 1$, $n_C(c) = n_C(u)n_C(v) = 0$ and hence is an elementary idempotent. By Prop. 22.7, our composition algebra C is therefore reduced. By Cor. 22.10, it is split if the rank is 2. But by Prop. 22.13 and Thm. 22.15, the same conclusion holds also in ranks 4 and 8 since finitely generated projective k-modules are free.

(v) ⇒ (i). Obvious □

The equivalence (i)⇔(v) in 22.19 holds for other classes of integral domains k, see for example Lemma 57.1 (a) and Cor. 55.8 below. If k is a finitely generated algebra over a field, the answer can depend on the number of generators for k, see [16] for results on this and related questions.

22.20 Proposition. *Let C be a composition algebra over k and $D \subseteq C$ a quadratic étale subalgebra. Then C_D, the base change of C from k to D, is reduced.*

Proof By Lemma 11.10, we have $C = D \oplus D^\perp$ as a direct sum of k-modules, which implies $C_D = D_D \oplus (D^\perp)_D$ as a direct sum of D-modules. But D_D is split quadratic étale (Exc. 19.36 (a)), forcing C to be reduced by Prop. 22.9. □

22.21 Corollary. *Let C be a composition algebra of rank $r > 1$ over an LG ring k. Then for every quadratic étale subalgebra D of C, C_D is a split composition algebra over D.*

Proof Because D is a finitely generated module over an LG ring, it is itself an LG ring (11.23). Since C_D is reduced (Prop. 22.20), the claim follows by Cor. 22.16. □

Note that quadratic étale subalgebras of C as in Cor. 22.21 exist by Theorem 19.16 (b).

Exercises

22.22. Let k^+, k^- be commutative rings and $k = k^+ \times k^-$ their direct product. Assume that $A^\pm$ is a $k^\pm$-algebra and view $A := A^+ \times A^-$ canonically as a k-algebra. Show for $c = (c^+, c^-) \in A$ that the following conditions are equivalent.

(i) c is an absolutely primitive idempotent in A.
(ii) $k \neq \{0\}$ and for both signs $\pm$, either $k^\pm = \{0\}$ or $c^\pm$ is an absolutely primitive idempotent in $A^\pm$.

22.23. Let C be a composition algebra over k and $c \in C$. Use Exc. 16.26 to show that the following conditions are equivalent.

(i) c is an absolutely primitive idempotent of C.
(ii) $k \neq \{0\}$ and there exist a decomposition

$$k = k^{(1)} \times k^{(2)} \tag{1}$$

as a direct product of ideals, a composition algebra $C^{(1)}$ over $k^{(1)}$ as well as an elementary idempotent $c^{(1)} \in C^{(1)}$ such that

$$C \cong C^{(1)} \times k^{(2)} \tag{2}$$

as composition algebras over k and

$$c = (c^{(1)}, 1_{k^{(2)}})$$

under this isomorphism.

Conclude that C is reduced if and only if $k \neq \{0\}$ and C allows decompositions as in (1), (2) such that $C^{(1)}$ is a composition algebra over $k^{(1)}$ that contains an elementary idempotent.

22.24. *Elementary idempotents in reduced quaternion algebras.* Let L_0 be a line bundle over k and write

$$B = \operatorname{End}_k(k \oplus L_0) = \begin{pmatrix} k & L_0^* \\ L_0 & k \end{pmatrix}$$

for the corresponding reduced quaternion algebra over k. Prove:

(a) For $c \in B$, the following conditions are equivalent.

(i) c is an elementary idempotent.

(ii) c is an idempotent, and viewing c as a linear map $k \oplus L_0 \to k \oplus L_0$,

$$L_c := \operatorname{Im}(c) \subseteq k \oplus L_0$$

is a line bundle over k.

(iii) There exist a line bundle L over k and an isomorphism

$$\Phi\colon B \xrightarrow{\sim} \operatorname{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}$$

such that

$$\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

In this case $\bar{c} \in B$ is an elementary idempotent as well and

$$k \oplus L_0 = L_c \oplus L_{\bar{c}}, \quad L_0 \cong L_c \otimes L_{\bar{c}}. \tag{1}$$

Moreover, L in (iii) is unique up to isomorphism and

$$L \cong B_{21}(c) \cong L_0 \otimes L_c^{*\otimes 2}, \quad B_{12}(c) \cong L_0^* \otimes L_c^{\otimes 2}. \tag{2}$$

(b) Two elementary idempotents $c, d \in B$ are conjugate under *inner* automorphisms of B if and only if $L_c \cong L_d$. They are conjugate under *arbitrary* automorphisms of B if and only if $L_c^{\otimes 2} \cong L_d^{\otimes 2}$.

(c) If L is any line bundle over k, then $L \cong L_c$ for some elementary idempotent $c \in B$ if and only if L is (isomorphic to) a direct summand of $k \oplus L_0$.

22.25. *Line bundles on two generators.* Let L be a line bundle over k.

(a) Let n be a positive integer and suppose there are elements $f_1, \dots, f_n \in k$ such that $k = \sum kf_i$ and L_{f_i} is free (of rank one) over k_{f_i} for $1 \leq i \leq n$. Show that L is generated by n elements.

(b) Show that the following conditions are equivalent.

(i) L is generated by two elements.

(ii) $L \oplus L^*$ is a free k-module of rank two.

(iii) There exists an elementary idempotent $c \in B := \operatorname{Mat}_2(k)$ such that $L \cong L_c$.

(iv) There exist elements $f_1, f_2 \in k$ such that $kf_1 + kf_2 = k$ and L_{f_i} is free (of rank one) over k_{f_i} for $i = 1, 2$.

Conclude that if L satisfies one (hence all) conditions (i)–(iv) above, then so does $L^{\otimes n}$, for all $n \in \mathbb{Z}$. In particular, there exists an elementary idempotent $c^{(n)} \in \mathrm{Mat}_2(k)$, unique up to conjugation by inner automorphisms of B, satisfying $L^{\otimes n} \cong L_{c^{(n)}}$. Describe such an idempotent as explicitly as possible.

Remark. Let k be a Dedekind domain, i.e., a noetherian integral domain such that the localization of k at each maximal ideal is a principal ideal domain [27, §VII.2]. (For example, every principal ideal domain is also a Dedekind domain, as is every nonzero localization of a Dedekind domain.) There is a canonical identification of the class group of k with its Picard group, and every fractional ideal of k is generated by two elements (O'Meara [204, 22.5a, 22:5b]). Hence the preceding two exercises yield a bijective correspondence between the set of conjugacy classes of elementary idempotents in $\mathrm{Mat}_2(k)$ under inner automorphisms and the class group of k. In particular, for k the ring of integers of an algebraic number field K, the number of these conjugacy classes agrees with the class number of K.

22.26. *Isomorphisms of reduced quaternion algebras.* Let L_0, L_0' be line bundles over k and $B = \mathrm{End}_k(k \oplus L_0)$, $B' = \mathrm{End}_k(k \oplus L_0')$ the corresponding reduced quaternion algebras. Use Exc. 22.24 to show that the following conditions are equivalent.

(i) $B \cong B'$.

(ii) Every line bundle L over k that is a direct summand of $k \oplus L_0$ admits a line bundle L' over k that is a direct summand of $k \oplus L_0'$ and satisfies

$$L_0 \otimes L'^{\otimes 2} \cong L_0' \otimes L^{\otimes 2}. \tag{1}$$

(iii) There exist line bundles L, L' over k that are direct summands of $k \oplus L_0$, $k \oplus L_0'$, respectively, and satisfy (1).

22.27. Let L be a line bundle over k. Prove that the reduced quaternion algebra $\mathrm{End}_k(k \oplus L)$ is split if and only if $L \cong L'^{\otimes 2}$ for some line bundle L' on two generators over k. Use this to construct examples of reduced quaternion algebras over k that are free as k-modules but not split.

Remark. When k is a Dedekind domain, the result of this exercise is: *Every reduced quaternion algebra over k is split if and only if every element of* $\mathrm{Pic}(k)$ *is divisible by 2.*

22.28. *Failure of Witt cancellation.* Let L be a line bundle on two generators over k that is not of period 2 in $\mathrm{Pic}(k)$. Put $L' := L^{\otimes 2}$ and show $\mathbf{h} \perp \mathbf{h} \cong \mathbf{h} \perp \mathbf{h}_{L'}$ even though $\mathbf{h}_{L'}$ is not split. (*Hint*: Use Exc. 22.27 to prove that the reduced quaternion algebra $\mathrm{End}_k(k \oplus L')$ is split.)

22.29. Let M be a finitely generated projective k-module of rank 3 and θ an orientation of M. Show

$$(u \times_\theta v) \times_\theta w^* = \langle w^*, u\rangle v - \langle w^*, v\rangle u, \quad (u^* \times_\theta v^*) \times_\theta w = \langle u^*, w\rangle v^* - \langle v^*, w\rangle u^*$$

for all $u, v, w \in M$, $u^*, v^*, w^* \in M^*$.

22.30. Prove that every reduced octonion algebra over a Dedekind domain is split. (*Hint*: Use the well-known structure of finitely generated projective modules over a Dedekind domain, cf. Bourbaki [27, VII.4, Prop. 24].)

23 Norm equivalences and isomorphisms

One of the most important results in the classical theory of composition algebras is the norm equivalence theorem. It says that *composition algebras over fields are classified by their norms*, in other words, two composition algebras over a field are isomorphic if and only if their norms are equivalent, i.e., isometric. Our first aim in this section will be to establish this result in the more general setting of LG rings. As in the case of fields, the key ingredient of the proof is Witt cancellation of regular quadratic forms, which fails over arbitrary commutative rings (see Exc. 22.28 above) but is valid over LG rings. As an application, we classify composition algebras over special fields, like the reals and the complexes, finite fields, the p-adics and algebraic number fields, as well as over $\mathbb{Z}$. The section also contains a few general comments on norm equivalence over arbitrary commutative rings.

Let k be a commutative ring. We begin by introducing the concept of norm equivalence and some useful modifications.

23.1 Norm similarities. Let C, C' be conic algebras over k. A *norm similarity* from C to C' is a bijective k-linear map $f\colon C \to C'$ such that there exists a scalar $\mu_f \in k^\times$ satisfying $n_{C'} \circ f = \mu_f n_C$; in this case, $\mu_f = n_{C'}(f(1_C))$ is unique and called the *multiplier* of f. Norm similarities with multiplier 1 are called *norm isometries* or *norm equivalences*. We say that C and C' are *norm similar* (resp. *norm equivalent*) if there exists a norm similarity (resp. a norm equivalence) from C to C'. Norm similarities $f\colon C \to C'$ preserving units (so $f(1_C) = 1_{C'}$) automatically have multiplier 1; we speak of *unital norm equivalences* in this context.

It is clear that the preceding notions are stable under base change. The principal objective of the present section is to understand the connection between unital norm equivalences and isomorphisms (resp. anti-isomorphisms) of composition algebras.

23.2 Proposition. *Let C, C' be conic alternative k-algebras.*

(a) *If C is multiplicative, then for any $a \in C^\times$, the left and right multiplication operators $L_a, R_a\colon C \to C$ are norm similarities, with multipliers $\mu_{L_a} = \mu_{R_a} = n_C(a)$.*

(b) *Let $f\colon C \to C'$ be a norm similarity. Then $f(C^\times) = C'^\times$. Moreover, if f is even a unital norm equivalence, then f preserves norms, traces, conjugations and inverses.*

Proof (a) follows from the property of n_C permitting composition combined

with Prop. 17.5. In order to establish (b), it suffices to combine Prop. 17.5 with (16.5.2), (16.5.4). □

23.3 Corollary. *Multiplicative conic alternative algebras C, C' over k are norm similar if and only if there exists a unital norm equivalence from C to C'.*

Proof Let $f\colon C \to C'$ be a norm similarity. By Prop: 23.2 (b), the element $a' := f(1_C)$ is invertible in $C'^{\times}$, and $L_{a'^{-1}} \circ f\colon C \to C'$ is a unital norm equivalence. □

23.4 Proposition. *(a) Let C, C' be conic algebras over k that are projective as k-modules. Then every isomorphism or anti-isomorphism from C to C' is a unital norm equivalence.*

(b) A unital norm equivalence from one quadratic k-algebra onto another is an isomorphism.

Proof (a) follows immediately from Exc. 16.19.

(b) Let R, R' be quadratic k-algebras and $f\colon R \to R'$ a unital norm equivalence. In order to show that f is an isomorphism, we may assume that k is a local ring, which implies $R = k[u]$ for some $u \in R$ such that $1_R, u$ is a basis of R over k. Then $R' = k[u']$, $u' := f(u)$, and since f preserves units, norms and traces by Prop. 23.2 (b), we have $f(u^2) = u'^2 = f(u)^2$ and f is an isomorphism. □

The following result is well known in the case where k is a field, see for example Jacobson [132] or Van der Blij-Springer [286]. Over local rings, it is due to Bix [24, Lemma 1.1].

23.5 Norm Equivalence Theorem. *Let k be an LG ring and C, C' be composition algebras over k. Then the following conditions are equivalent.*

(i) *C and C' are isomorphic.*
(ii) *C and C' are norm equivalent.*
(iii) *C and C' are norm similar.*

Proof (i) ⇒ (ii). Prop. 23.4 (a).

(ii) ⇒ (iii). Cor. 23.3.

(iii) ⇒ (i). By the rank decomposition of Exc. 9.31, we may assume that C, C' both have constant rank $r \in \{1, 2, 4, 8\}$. There is nothing to prove for $r = 1$, so let us assume $r > 1$. Thm. 19.16 (b) yields a regular composition subalgebra $D \subseteq C$ of rank 2. By Cor. 23.3, there exists a unital norm equivalence $f\colon C \to C'$. Since f preserves units, norms and traces by Prop. 23.2 (b),

we conclude from the characterization of Prop. 19.8 that $D' := f(D)$ is also a regular composition subalgebra of C' and $f\colon D \to D'$ is an isomorphism (Prop. 23.4 (b)). Now suppose $B \subset C$, $B' \subset C'$ are regular composition subalgebras of rank s, $1 < s < r$, and $g\colon B \to B'$ is an isomorphism. Combining Lemma 11.26 with the Witt cancellation theorem (11.27), we find invertible elements $l \in B^\perp \subseteq C$, $l' \in B'^\perp \subseteq C'$ such that $n_C(l) = n_{C'}(l') \in k^\times$. Therefore B, l (resp. B', l') generate regular composition subalgebras $B_1 \subseteq C$ (resp. $B'_1 \subseteq C'$) of rank $2s$ that are isomorphic (Cor. 18.9). Continuing in this manner, we eventually obtain an isomorphism from C to C'. (Actually, we do so after at most two steps.) □

23.6 Corollary. *Let B be a regular associative composition algebra over an LG ring k and $\mu, \mu' \in k^\times$. Then*

$$\mathrm{Cay}(B,\mu) \cong \mathrm{Cay}(B,\mu') \iff \mu \equiv \mu' \bmod n_B(B^\times).$$

Proof Put $C := \mathrm{Cay}(B,\mu) = B \oplus Bj$, $C' := \mathrm{Cay}(B,\mu') = B \oplus Bj'$ as in 18.3. By Thm. 23.5, $C \cong C'$ implies $n_C \cong n_{C'}$, and Remark 18.5 combines with Witt cancellation (11.27) to yield an isometry $\varphi\colon \mu n_B \xrightarrow{\sim} \mu' n_B$. But then $\mu = \mu' n_B(u)$, $u = \varphi(1_B) \in B^\times$. Conversely, suppose $\mu = \mu' n_B(u)$ for some $u \in B^\times$. Since B is associative, the assignment $x + yj \mapsto x + (uy)j'$ gives an isomorphism from C onto C' (Exc. 18.19). □

23.7 Remark. Cor. 23.6 fails if B is singular. For example, let k be a field of characteristic 2 and $\mu, \mu' \in k$. Then one checks easily that $\mathrm{Cay}(k,\mu)$ and $\mathrm{Cay}(k,\mu')$ are isomorphic if and only if $\mu = \alpha^2 + \beta^2\mu'$ for some $\alpha \in k, \beta \in k^\times$.

23.8 Comments. Apart from its potential for a great many important applications, some of which will be dealt with in the remainder of this section, the norm equivalence theorem enjoys a few remarkable properties of a different kind. Here are some examples.

(a) The norm equivalence theorem does not claim that every unital norm equivalence between composition algebras over a field (or an LG ring) is an isomorphism or an anti-isomorphism. While this is certainly true for quadratic étale algebras over any ring (Prop. 23.4 (b)) and, as will be seen in 23.30 below (see also Knus [157, V, (4.3.2)] or Gille [97, Thm. 2.4]), is basically true for quaternion algebras, again over any ring, it fails in the octonionic case. The reader may either consult Exc. 23.32 below to see this or turn to the octonion algebra $\mathbb{O}$ over $k = \mathbb{R}$: in the latter case, the automorphisms or anti-automorphisms of $\mathbb{O}$ form a closed subset of $\mathrm{GL}(\mathbb{O})$ that may be written as the union of two 14-dimensional pieces (2.6.1), while the unital norm equivalences of $\mathbb{O}$ identify canonically with the Lie group O_7, which has dimension 21.

(b) The norm equivalence theorem was anticipated already by Zorn in [299, p. 399], where one finds the following remarkable statement, which we reproduce with the same emphasis as in the original:

> Das System wurde allein aus der quadratischen Form $\mathfrak{x} \circ \mathfrak{x}$ gewonnen, die *Äquivalenz der Formen ist also mit der Äquivalenz der Systeme gleichbedeutend.*

By "das System" (resp. the expression "$\mathfrak{x} \circ \mathfrak{x}$"), Zorn is referring to an octonion algebra (resp. to its norm). However, the reason given by him for the validity of the norm equivalence theorem is not convincing since, e.g., it would imply that any unital norm equivalence would be an isomorphism. A more profound reason why Zorn's argument cannot be valid will now be addressed.

(c) It is a natural question to ask whether the norm equivalence theorem holds over an arbitrary commutative ring. By (a), the answer is yes for composition algebras of rank 2 or 4. *In rank* 8*, however, i.e., for octonion algebras, the norm equivalence theorem does not hold.* In fact, there is a profound connection between this fundamental fact and the isotopy-versus-isomorphism problem for alternative algebras discussed in 15.12. This connection can be read off from the following two results.

23.9 Theorem (Gille [97, Thm. 3.3 and p. 308])**.** *There exists a ring k that is finitely generated as a $\mathbb{C}$-algebra such that there exist non-isomorphic octonion k-algebras whose norms are isometric. More specifically, there exists an octonion k-algebra that is not split but whose norm is split hyperbolic.* □

23.10 Theorem (Alsaody-Gille [15, Cor. 6.7])**.** *Let C, C' be octonion algebras over an arbitrary commutative ring. Then the following conditions are equivalent.*

(i) C *and* C' *are norm-equivalent.*
(ii) C *and* C' *are norm-similar.*
(iii) *There exist* $p, q \in C^\times$ *such that* $C' \cong C^{(p,q)}$.
(iv) *There exists* $p \in C^\times$ *such that* $C' \cong C^p$.
(v) *There exists* $p \in C$ *such that* $n_C(p) = 1$ *and* $C' \cong C^p$. □

23.11 Corollary. *There exist a ring k that is finitely generated as a $\mathbb{C}$-algebra and an invertible element p in the split octonion algebra $C := \mathrm{Zor}(k)$ over k such that C and C^p are not isomorphic. No such p can be embedded into a quaternion subalgebra of C.*

Proof The first part follows immediately from the preceding theorems. The final assertion is implied by Exc. 19.31. □

One reason for the importance of the norm equivalence theorem is that we know a lot about quadratic forms over special fields, and this knowledge may be used to classify composition algebras over these fields. Recall from Cor. 22.18 that composition algebras over any field are either split or division algebras. We can subdivide the classification problem into separate problems for each of the possible dimensions 2, 4, or 8, since the classification problem for rank 1 is trivial.

23.12 Algebraically closed fields and similar. Suppose first that F has no separable quadratic field extensions. This is equivalent to requiring that every rank 2 composition algebra is split. For example, this holds trivially if F is separably closed, meaning that it has no finite separable field extensions. For such an F, *there is a unique isomorphism class of composition F-algebras in each dimension 2, 4, 8*, namely the split one. For dimensions 4 and 8 it is by Cor. 19.17 and 22.9.

Alternatively, suppose that F is a field such that every element of F has a square root in F. (We may as well suppose further that F has characteristic 2, for otherwise this case is the same as the one considered in the previous paragraph.) For every quadratic étale F-algebra K, the norm $n_K\colon K \to F$ is surjective, so Cor. 19.17 and Example 22.11 imply that *every quaternion or octonion F-algebra is split*, i.e., there is a unique isomorphism class of composition F-algebras in each dimension 4 and 8.

23.13 The reals. Thanks to Sylvester's Law of Inertia, quadratic spaces over $\mathbb{R}$ (or, more generally, over any real closed field) are classified by their dimension and their signature, see, for example, [204, §61.A] or [255, Theorem 2.4.4]. In particular, in each dimension there are precisely two isometry classes of anisotropic quadratic forms, a positive definite and a negative definite one. Hence each dimension $r = 1, 2, 4, 8$ allows exactly one isomorphism class of composition division algebras over $\mathbb{R}$: uniqueness follows from the norm equivalence theorem 23.5, while existence is provided by the classical examples $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ of §1.

23.14 Finite fields. The key fact to be used here is the Chevalley-Warning theorem proved in, for example, [102, Thm. 6.2.6]: every form of degree d in $n > d$ indeterminates over a finite field $k = \mathbb{F}_q$, q a prime power, has a non-trivial zero in $\mathbb{F}_q^n$. It follows that every quadratic form in at least three variables over $\mathbb{F}_q$ is isotropic. In particular, quaternion and octonion algebras over $\mathbb{F}_q$ are all split (Cor. 22.18). The only non-split composition algebra of dimension 2 over $\mathbb{F}_q$ up to isomorphism is the unique quadratic field extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$.

23.15 Local fields. We say a field K is *local* if it is complete with respect to a

discrete valuation v and the residue field of K at v is finite. Such fields include the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ relative to its p-adic valuation for a prime p as well as the completion $\mathbb{F}_q((\mathbf{t}))$ of the rational function field $\mathbb{F}_q(\mathbf{t})$ for a finite field $\mathbb{F}_q$. Every local field is isomorphic to $\mathbb{F}_q((\mathbf{t}))$ for some q or a finite extension of $\mathbb{Q}_p$ for some p [196, p. 127, Remark 7.49].

We have the following classical results concerning a local field K:

(i) Every finite extension of K is local [204, 32:3].

(ii) Every quadratic form in at least five variables over K is isotropic. In case K has characteristic $\neq 2$, this can be found in [204, 63:19]. In case K has characteristic $\neq 0$, it is [104, Thm. 4.8]. It follows that all octonion algebras over K are split.

(iii) Up to isomorphism, there is a unique quaternion division algebra over K. This is [204, 63:11b] if K has characteristic $\neq 2$, [102, Prop. 6.3.9] if K has characteristic $\neq 0$, and [260, §XIII.3, Prop. 6] in general.

To complete the picture, it remains to classify composition algebras of dimension 2 over K. If K has characteristic $\neq 2$, these are parameterized by the group $K^\times/K^{\times 2}$. Describing this group is pretty straightforward if the residue field has odd characteristic, but requires some care for when it has characteristic 2; again we refer to Scharlau [255, Chap. 5, §6] and O'Meara [204, §63 A, particularly 63:9] for details.

We refer the reader to [212] and [92] for more results on composition algebras and discrete valuations.

23.16 Global fields. In this subsection, we assume some familiarity with the foundations of algebraic number theory. Let K be a *global field*, i.e., a finite extension of $\mathbb{Q}$ (an *algebraic number field*), or of $\mathbb{F}_p(\mathbf{t})$ for some prime p (an *algebraic function field*). We write Ω for the set of places of K, including the infinite ones (which exist only if K has characteristic zero), and by K_v the completion of K at the place $v \in \Omega$; the natural embedding $\lambda_v\colon K \to K_v$ makes the image $\lambda_v(K)$ a dense subfield of K_v relative to the v-adic topology. The set of real places of K will be denoted by S, so we have a natural identification $K_v = \mathbb{R}$ for $v \in S$; in fact, the assignment $v \mapsto \lambda_v$ determines a bijective correspondence between S and the set of embeddings $K \to \mathbb{R}$. Note that S is empty unless K has characteristic zero. Given an algebra A (resp. a quadratic form Q) over K, we abbreviate $A_v = A \otimes_K K_v$ (resp. $Q_v = Q \otimes_K K_v$) for $v \in \Omega$.

The key to understand composition algebras over K is provided by the Hasse-Minkowski theory of quadratic forms:

23.17 Theorem (Hasse-Minkowski)**.** *With the notation of 23.16,* the following statements hold.

(a) *A quadratic form Q over K is isotropic if and only if Q_v is isotropic over K_v for all $v \in \Omega$.*

(b) *Regular quadratic forms Q, Q' over K are isometric if and only if Q_v, Q'_v are isometric over K_v for all $v \in \Omega$.*

References See O'Meara [204, 66:1, 66:4] or Scharlau [255, Chap. 5, 7.2, 7.3] for K of characteristic $\neq 2$. For K of characteristic 2, see [236, Thm. 3.2] □

Since a regular quadratic form Q over a field represents a scalar α if and only if the form $\langle -\alpha \rangle_{\text{quad}} \perp Q$ is isotropic, the first part of the Hasse-Minkowski theorem immediately implies:

23.18 Corollary. *A regular quadratic form Q over K represents an element $\alpha \in K$ if and only if Q_v represents $\lambda_v(\alpha) \in K_v$ for all $v \in \Omega$.* □

Combining the second part of Thm. 23.17 with the norm equivalence theorem 23.5, it follows that composition algebras over number fields are completely determined by their local behavior:

23.19 Corollary. *Composition algebras C and C' over K are isomorphic if and only if C_v and C'_v are isomorphic over K_v for all $v \in \Omega$.* □

Corollary 23.19 may be regarded as the first step towards the classification of composition algebras over number fields. In order to complete this classification, it seems natural to invoke another fundamental fact from Hasse-Minkowski theory: every "local family" of regular quadratic forms $Q^{(v)}$ over K_v, $v \in \Omega$, has a "global realization" by a regular quadratic form Q over K satisfying $Q_v \cong Q^{(v)}$ for all $v \in \Omega$ if and only if a certain obstruction, based on Hilbert's reciprocity law and involving Hasse symbols, vanishes. But since there is no a priori guarantee that the property of being the norm of a composition algebra descends from the totality of forms Q_v, $v \in \Omega$, to the form Q, one has to argue in a different manner.

For simplicity, we confine ourselves to quaternion and octonion algebras. The classification of the former is accomplished by the following result from class field theory, which we record (again) without proof.

23.20 Theorem. *With the notation of 23.16, let $T \subseteq \Omega$ be a finite set consisting of an even number of real or finite places of K. Then there exists a quaternion algebra B over K, unique up to isomorphism, such that B_v is split for all $v \in \Omega \setminus T$ and a division algebra for all $v \in T$.*

References See O'Meara [204, 71:19] if K has characteristic 0 and [102, Cor. 6.5.4] if K has characteristic $\neq 0$.

Recall from 23.13 and 23.15 (iii) that K_v, for $v \in T$, admits precisely one quaternion division algebra, so uniqueness of B in the theorem follows from Cor. 23.19. □

The classification of octonion algebras over algebraic function fields is an easy consequence of Cor. 23.19 since there are no infinite places. Indeed, we have the following.

23.21 Corollary. *For a global field K, we have: If there are no homomorphisms $K \to \mathbb{R}$, then every octonion algebra over K is split.* □

Over algebraic number fields, the classification of octonion algebras is only slightly more complicated.

23.22 Theorem (Albert-Jacobson [11, Thm. 11])**.** *Let K be a number field, and write $B := \mathrm{Cay}(K; -1, -1)$ as a quaternion algebra over K. Then every octonion algebra over K is isomorphic to $\mathrm{Cay}(B, \mu)$ for some $\mu \in K^\times$. Moreover, given $\mu, \mu' \in K^\times$, the following conditions are equivalent.*

(i) $\mathrm{Cay}(B, \mu) \cong \mathrm{Cay}(B, \mu')$.
(ii) $\lambda_v(\mu\mu') > 0$ *for all $v \in S$ with the notation of 23.16.*

There is no conflict between the theorem and Cor. 23.21. In the case where the two results overlap, i.e., where K is a number field with no real places, condition (ii) of the theorem holds vacuously, and (i) says that every octonion algebras is isomorphic to the split one, $\mathrm{Cay}(B, 1)$.

Proof For the first part, it will be enough to prove that every octonion algebra C over K contains a unital subalgebra isomorphic to B. To this end, we claim *that every regular sub-form of n_C having dimension at least 5 represents the element $1 \in K$.*

Indeed, let Q be such a sub-form. By Cor. 23.18, it suffices to show for all $v \in \Omega$ that Q_v represents the element $1 \in K_v$. If C_v is split, n_{C_v} has maximal Witt index, and a dimension argument shows that every maximal totally isotropic subspace of C_v relative to n_{C_v} intersects Q_v non-trivially. Thus Q_v is isotropic, hence universal and so represents 1. On the other hand, if C_v is a division algebra, $v \in S$ must be real (23.12, 23.15), forcing n_{C_v} to be positive definite. But then so is Q_v, which therefore again represents 1. This proves our claim. We first apply the claim to n_C^0, the restriction of n_C to the pure octonions $C^0 = \mathrm{Ker}(t_C)$, and find an element $j_1 \in C$ satisfying $t_C(j_1) = 0$, $n_C(j_1) = 1$. By Cor. 18.9 and Prop. 19.8, $D := K[j_1] \cong \mathrm{Cay}(K, -1)$ is a quadratic étale subalgebra of C. Applying our claim once more, this time to the restriction of n_C to $D^\perp$, yields an element $j_2 \in D^\perp$ satisfying $n_C(j_2) = 1$, and invoking

Corollary 18.9 again, we see that the subalgebra of C generated by D and j_2 is isomorphic to B, giving the first part of the theorem. As to the second, we conclude $C_v \cong \mathrm{Cay}(\mathbb{H}, \lambda_v(\mu))$, $C'_v \cong \mathrm{Cay}(\mathbb{H}, \lambda_v(\mu'))$ for all $v \in S$, and since C_v, C'_v are both split for $v \in \Omega \setminus S$ (23.12, 23.15), we can apply Corollaries 23.19, 23.6 to obtain the following chain of equivalent conditions.

$$\begin{aligned} C \cong C' &\iff \forall v \in S : C_v \cong C'_v \\ &\iff \forall v \in S : \mathrm{Cay}(\mathbb{H}, \lambda_v(\mu)) \cong \mathrm{Cay}(\mathbb{H}, \lambda_v(\mu')) \\ &\iff \forall v \in S : \lambda_v(\mu\mu') \in n_{\mathbb{H}}(\mathbb{H}^\times) = \mathbb{R}_+^\times. \end{aligned}$$

□

23.23 Corollary (Zorn [299])**.** *With the notation of 23.16, there are precisely* $2^{|S|}$ *isomorphism classes of octonion algebras over* K*.*

Proof Adopting the notation of Thm. 23.22, let $T \subseteq S$. We apply the weak approximation theorem (O'Meara [204, 11:8]) and find an element $\mu_T \in K$ satisfying

$$|\lambda_v(\mu_T) + 1| < 1 \quad (v \in T), \qquad |\lambda_v(\mu_T) - 1| < 1 \quad (v \in S \setminus T).$$

Up to isomorphism, the octonion algebra $C_T := \mathrm{Cay}(B, \mu_T)$ does not depend on the choice of μ_T (Thm. 23.22), so the assignment $T \mapsto C_T$ gives a well-defined map from 2^S to the set of isomorphism classes of octonion algebras over K. Conversely, let C be an octonion algebra over K. Then $T_C := \{v \in S \mid C_v \cong \mathbb{O}\}$ is a subset of S, and $C \mapsto T_C$ gives a map in the opposite direction. Since the two maps thus defined are easily seen to be inverse to one another, the assertion follows. □

23.24 Remark. Given a family of octonion algebras $C^{(v)}$ over K_v, $v \in \Omega$, Cor. 23.23 shows that there always exists an octonion algebra C over K, unique up to isomorphism, which satisfies $C_v \cong C^{(v)}$ for all $v \in \Omega$, so the Hilbert reciprocity law yields no obstructions when dealing with octonion norms.

Finally, we turn to the classification of composition algebras over $\mathbb{Z}$. The proof of the following result will use some standard facts about the valuation theory of the p-adics.

23.25 Theorem. *Composition algebras over the integers are either split or isomorphic to the Dickson-Coxeter octonions.*

Proof If the rank is 1, the assertion is obvious. If the rank is 2 or 8, it will be verified in Exercises 23.38 and 23.39 below. Hence it remains to show that any quaternion algebra C over $\mathbb{Z}$ is split. For sake of contradiction, suppose C is not split, which by Cor. 22.19 and the Hasse-Minkowski Theorem 23.17

implies that $C \otimes_{\mathbb{Z}} \mathbb{Q}_v$ is division for some place v of $\mathbb{Q}$. Note that C is a free $\mathbb{Z}$-module, so C is naturally contained in $C \otimes_{\mathbb{Z}} R$ for every ring R containing $\mathbb{Z}$.

If $v = \infty$ is the infinite place, then $\mathbb{Q}_v = \mathbb{R}$, $C \otimes \mathbb{Q}_v \cong \mathbb{H}$ is the Hamiltonian quaternions, and (C, n_C) is a unimodular positive definite integral quadratic lattice. But, as we have noted in 4.6, such lattices exist only in ranks divisible by 8 while (C, n_C) has rank 4.

Therefore, $v = v_p$ is the p-adic place of $\mathbb{Q}$ for some prime $p \in \mathbb{Z}$, we have $\mathbb{Q}_v = \mathbb{Q}_p$ and put $D_p := C \otimes_{\mathbb{Z}} \mathbb{Q}_p$. Since D_p has no zero divisors, by [212, Prop. 1] the assignment $x \mapsto \frac{1}{2} v_p(n_{D_p}(x))$ yields the unique extension of the p-adic valuation v_p of $\mathbb{Q}_p$ to a discrete valuation of D_p, with corresponding valuation ring $\mathfrak{o}_p = \{x \in D_p \mid v_p(n_{D_p}(x)) \geq 0\}$ and valuation ideal $\mathfrak{m}_p = \{x \in D_p \mid v_p(n_{D_p}(x)) > 0\}$ making $\mathfrak{o}_p/\mathfrak{m}_p$ a division algebra over $\mathbb{F}_p$. Regarding $C_p := C \otimes_{\mathbb{Z}} \mathbb{Z}_p$ canonically as a $\mathbb{Z}_p$-subalgebra of D_p (which we may do because C is a flat $\mathbb{Z}$-module and $\mathbb{Z}_p \subset \mathbb{Q}_p$), we clearly have $C_p \subseteq \mathfrak{o}_p$. Conversely, let $u \in \mathfrak{o}_p$. Then $n_{D_p}(u, -)\colon C_p \to \mathbb{Z}_p$ is a linear form, and since C_p is a regular composition algebra over $\mathbb{Z}_p$ (C being one over $\mathbb{Z}$), we find an element $u' \in C_p$ such that $n_{D_p}(u, -) = n_{C_p}(u', -)$ on C_p. But C_p generates D_p as a $\mathbb{Q}_p$-algebra, and we obtain $u = u'$, hence $C_p = \mathfrak{o}_p$. On the other hand, $\mathfrak{o}_p/p\mathfrak{o}_p = C_p/pC_p = C_p \otimes_{\mathbb{Z}_p} \mathbb{F}_p = C \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a quaternion algebra over the finite field $\mathbb{F}_p$, hence split (23.14) and simple. This implies $\mathfrak{m}_p = p\mathfrak{o}_p$, and we conclude that $\mathfrak{o}_p/p\mathfrak{o}_p$ is a division algebra, a contradiction. □

23.26 Vista: splitting fields of composition algebras. Suppose C is a composition algebra over a field F. We say that a field $K \supseteq F$ is a *splitting field* of C if the base change C_K is split over K. In this subsection, we assemble a few observations about splitting fields of C. We may of course assume that C itself is not split, i.e., C is a division algebra; we may also assume that it has dimension at least 2.

(a) The smallest nontrivial case, where K is a quadratic field extension of F, is handled by Exc. 23.40 (a). It says: K is a splitting field of C if and only if C contains a subalgebra isomorphic to K.

(b) If $[K : F]$ is odd, then (by Springer's theorem for quadratic forms under odd-degree extensions [72, Cor. 18.5]) $(n_C)_K$ is anisotropic because n_C is, so C_K is a division algebra.

(c) For dimension 4, Detlev Hoffmann provides the following example of a quaternion algebra C and K of degree 4 over F such that C_K is split yet the largest F-subalgebra of K that embeds in C is F itself. Take $F = \mathbb{Q}$ and $C := \mathrm{Ga}(\mathbb{H})_{\mathbb{Q}} = \mathrm{Cay}(\mathbb{Q}; -1, -1)$. It is a division algebra because $C_{\mathbb{R}}$ is the division algebra $\mathbb{H}$. Now, the polynomial $f := \mathbf{t}^4 - \mathbf{t} + 1$ is irreducible in $\mathbb{Q}[\mathbf{t}]$ with Galois

group the symmetric group $\mathcal{S}_4$ (exercise), so $K := \mathbb{Q}[\mathbf{t}]/(f)$ is a field of degree 4 over $\mathbb{Q}$ and there are no fields — hence no finite-dimensional $\mathbb{Q}$-algebras — properly lying between $\mathbb{Q}$ and K. In particular, the largest subalgebra of K that embeds in C is $\mathbb{Q}$ itself. Yet in $\mathbb{Q}[\mathbf{t}]$ we have

$$(\mathbf{t}^3 + \mathbf{t}^2 - 1)^2 + (\mathbf{t}^3)^2 + (\mathbf{t}^2 + 1)^2 = 2(1 + \mathbf{t} + \mathbf{t}^2)f,$$

so the norm of C_K is isotropic, i.e., C_K is split. See Exc. 23.42 for another example over $\mathbb{Q}$, and see Hoffmann's paper [122] for examples where F has characteristic 2 and K is purely inseparable.

23.27 Vista: relations between pairs of composition algebras. Continuing to talk about composition algebras over a field F, the paper [238] asked whether two composition F-algebras of the same dimension are determined by the quadratic fields extensions that they contain. That is, if two quaternion or octonion division algebras contain the same quadratic extensions, are the algebras themselves isomorphic? It is true for quaternion algebras and many fields such as a rational function field (in a finite number of variables) over a local field, global field, real closed field, or algebraically closed field, but not for some fields that are not finitely generated over such a field, see [93], [246], [48]. (See [163] for the related problem about quaternion algebras with the same splitting fields.) There even exist fields F such that there are infinitely many non-isomorphic quaternion or octonion division F-algebras that all share the same quadratic extensions, see [194] and [23, Rem. 3.5].

From another perspective, Burt Totaro posed in [285] a question in the language of algebraic groups that asks: If C and C' are both quaternion or octonion algebras, and $C_{K_i} \cong C'_{K_i}$ for fields K_i, does there exist a field extension K of F such that $[K : F]$ divides $[K_i : F]$ for all i and $C_K \cong C'_K$? The answer is "yes" for quaternion algebras (classical) and for octonion algebras it is in [90]. Totaro's question is quite general and also applies to the Albert algebras studied later in the book. The answer is "yes" for reduced Albert algebras by [90], and the question remains open for Albert algebras that are not reduced.

Exercises

23.28. *The Skolem-Noether theorem for composition algebras.* Let k be an LG ring, C a composition algebra of rank r over k and $B, B' \subseteq C$ two composition subalgebras of the same rank $s \leq r$. Show that every isomorphism from B to B' can be extended to an automorphism of C. Conclude that, up to conjugation by automorphisms of $\mathbb{O}$ (the Graves-Cayley octonions), the only non-zero subalgebras of $\mathbb{O}$ are $\mathbb{R}, \mathbb{C}, \mathbb{H}$ and $\mathbb{O}$.

23.29. *Unital norm equivalences of conic alternative algebras* (à la Jacobson-Rickart

[145]). Let C, C' be conic alternative k-algebras and suppose $f\colon C \to C'$ is a unital norm equivalence.

(a) Show

$$f(U_x y) = U_{f(x)} f(y), \tag{1}$$
$$(f(xy) - f(x)f(y))(f(xy) - f(y)f(x)) = [f(x), f(xy), f(y)] \tag{2}$$

for all $x, y \in C$. In particular, the left-hand side of (2) is symmetric in x, y.

(b) Conclude from (1) and its linearizations that if $c \in C$ is an elementary idempotent, so is $c' := f(c) \in C'$ and

$$f(C_{12}(c) + C_{21}(c)) = C'_{12}(c') + C'_{21}(c').$$

23.30. *Unital norm equivalences of quaternion algebras* (Petersson [221]). (a) Show for quaternion algebras B, B' over k: if $f\colon B \to B'$ is a unital norm equivalence, then there exists a decomposition $k = k_+ \times k_-$ of k as a direct product of ideals such that, with the corresponding decompositions

$$B = B_+ \times B_-, \quad B_\pm = B_{k_\pm}, \quad B' = B'_+ \times B'_-, \quad B'_\pm = B'_{k_\pm}, \tag{1}$$
$$f = f_+ \times f_-, \quad f_\pm = f_{k_\pm},$$

$f_+\colon B_+ \to B'_+$ is an isomorphism of quaternion algebras over k_+, and $f_-\colon B_- \to B'_-$ is an anti-isomorphism of quaternion algebras over k_-. Reduce to the case that k is a local ring by applying Exc. 9.29. Then imitate the beginning of the proof of the implication (iii) $\Rightarrow$ (i) in the norm equivalence theorem.

(b) Use (a) to prove a slightly weakened version of Knus's theorem [157, V, (4.3.2)] (see also Gille [97, 2.4]): for quaternion algebra B, B' over k, the following conditions are equivalent.

(i) B and B' are isomorphic.
(ii) B and B' are norm equivalent.
(iii) B and B' are norm similar.

23.31. *Elementary idempotents and unital norm equivalences.* Write e_{ij} $(i, j = 1, 2)$ for the usual matrix units in the split quaternion algebra $B = \mathrm{Mat}_2(k)$ and prove for any element $c \in B$ that there exists an automorphism of B sending e_{11} to c if and only if there exists a unital norm equivalence of B sending e_{11} to c.

23.32. *Octonionic norm equivalences.* Let C be an octonion algebra over k and $p \in C^\times$. Show that $L_p R_{p^{-1}}$ is

(a) always a unital norm equivalence of C,
(b) an automorphism of C if and only if $p^3 \in k1_C$,
(c) never an anti-automorphism of C.

(*Hint*: Use Exercise 15.17 (c).)

23.33. *Isotopes of composition algebras.* Show that isotopes of a composition algebra C over k are composition algebras that are regular if C is, and that they are isomorphic to C if C is associative or k is an LG ring.

23.34. *Zero-divisor pairs of the real sedenions.* Recall that the real sedenions $\mathbb{S} = \mathrm{Cay}(\mathbb{O}, -1) = \mathbb{O} \oplus \mathbb{O}j$ as defined in Exc. 19.29 form a conic real algebra with norm

$n_{\mathbb{S}}$ canonically isometric to $n_{\mathbb{O}} \perp n_{\mathbb{O}}$. By a *zero-divisor pair* of $\mathbb{S}$ we mean a pair (x, y) of non-zero elements in $\mathbb{S}$ such that $xy = 0$. Note that if (x, y) is a zero-divisor pair of $\mathbb{S}$, then so is $(\alpha x, \beta y)$ for all $\alpha, \beta \in \mathbb{R}^\times$. Thus the study of arbitrary zero-divisor pairs in $\mathbb{S}$ is equivalent to the one of zero-divisor pairs with pre-assigned norm. With this in mind, we define

$$\mathrm{Zer}(\mathbb{S}) := \{(x, y) \in \mathbb{S} \times \mathbb{S} \mid xy = 0, \quad n_{\mathbb{S}}(x) = n_{\mathbb{S}}(y) = 2\} \tag{1}$$

and let $G := \mathrm{Aut}(\mathbb{O})$ act diagonally first on $\mathbb{S}$ and then on $\mathrm{Zer}(\mathbb{S})$ via

$$G \times \mathrm{Zer}(\mathbb{S}) \longrightarrow \mathrm{Zer}(\mathbb{S}), \quad (\sigma, (x, y)) \longmapsto (\sigma(x), \sigma(y)).$$

Use Exc. 19.29 and Exc. 2.8 to show that $\mathrm{Zer}(\mathbb{S})$ becomes a principal homogeneous G-space in this way , i.e., the action of G on $\mathrm{Zer}(\mathbb{S})$ is simply transitive.

Remark. This result is a refined version of Moreno's theorem [199, Cor. 2.14], which says that $\mathrm{Zer}(\mathbb{O}) \subseteq \mathbb{S} \times \mathbb{S}$ is a closed subset homeomorphic to $\mathrm{Aut}(\mathbb{O})$.

The following sequence of exercises is designed to put the units of the Coxeter octonions (Exc. 4.13) in a broader perspective.

23.35. Let q be a prime power and $C := \mathrm{Zor}(\mathbb{F}_q)$ the unique octonion algebra over the field with q elements. Show

$$|C^\times| = q^3(q-1)(q^4-1), \quad |\{x \in C \mid n_C(x) = 1\}| = q^3(q^4-1),$$

23.36. *Positive definite integral quadratic modules and minimal vectors.* By a *positive definite integral quadratic module* we mean a quadratic module (M, Q) over $\mathbb{Z}$ such that M is a finitely generated free abelian group and the quadratic form $Q\colon M \to \mathbb{Z}$ is positive definite. Then M is an integral quadratic lattice in the positive definite real quadratic space $(M_{\mathbb{R}}, Q_{\mathbb{R}})$ in the sense of 3.6 and, conversely, every integral quadratic lattice in a positive definite real quadratic space becomes a positive definite integral quadratic module in a natural way.The *discriminant* of a positive definite integral quadratic module may be defined as in 3.12. A positive definite integral quadratic module is called *indecomposable* if it cannot be written as the sum of two orthogonal non-zero submodules.

Now let (M, Q) be a positive definite integral quadratic module over $\mathbb{Z}$. A vector $x \in M$ is said to be *minimal* if cannot be written as the sum of two vectors of strictly shorter length: $x = y + z$ with $y, z \in M$ and $Q(y) < Q(x)$, $Q(z) < Q(x)$ is impossible. The set of minimal vectors in (M, Q) will be denoted by $\mathrm{Min}(M, Q)$. Two minimal vectors $x, y \in M$ are said to be *equivalent* if there exists a finite sequence $x = x_0, x_1, \ldots, x_{k-1}, x_k = y$ of minimal vectors in M such that $Q(x_{i-1}, x_i) \neq 0$ for $1 \leq i \leq k$.

(a) Show that $\mathrm{Min}(M, Q)$ generates the additive group M.

(b) Show that equivalence of minimal vectors defines an equivalence relation on $\mathrm{Min}(M, Q)$.

(c) Denoting by $[x]$ the equivalence class of $x \in \mathrm{Min}(M, Q)$ with respect to the equivalence relation defined in (b), and setting $M_{[x]} := \sum_{y \in [x]} \mathbb{Z}y$, prove *Eichler's theorem*: (M, Q) splits into the orthogonal sum of indecomposable integral quadratic submodules $M_{[x]}$, where $[x]$ varies over the equivalence classes of $\mathrm{Min}(M, Q)$.

23.37. Let C be a multiplicative conic alternative algebra over $\mathbb{Z}$ such that the following conditions are fulfilled.

(a) C is free of rank 8 as a $\mathbb{Z}$-module.
(b) The norm of C is positive definite.
(c) The discriminant of the integral quadratic module (C, n_C) is odd.

Prove that $|C^\times| \leq 240$, and that if $|C^\times| = 240$, then (C, n_C) is an indecomposable positive definite integral quadratic module. (*Hint*: Reduce C mod 2 to obtain an octonion algebra $C^\dagger$ over $\mathbb{F}_2$ and show that the fibers of the natural map $C^\times \to C^{\dagger\times}$ consist of two elements. Then apply Exercises 23.35–23.36.)

23.38. Show that a quadratic étale algebra over the integers is split. Conclude that the algebra of Hurwitz quaternions cannot be obtained from the Cayley-Dickson construction: there does not exist a quadratic $\mathbb{Z}$-algebra R and a scalar $\mu \in \mathbb{Z}$ such that $\mathrm{Hur}(\mathbb{H}) \cong \mathrm{Cay}(R, \mu)$.

23.39. *Classification of octonion algebras over the integers* (Van der Blij-Springer [286]). Show that an octonion algebra over $\mathbb{Z}$ is either split or isomorphic to the Dickson-Coxeter octonions. In order to do so, let C be a non-split octonion algebra over $\mathbb{Z}$ with product $x \cdot y$, write xy for the product in $\mathrm{DiCo}(\mathbb{O})$ and perform the following steps.

(a) Reduce to the case that $C = \mathrm{DiCo}(\mathbb{O})$ as additive groups, $1_C = 1_{\mathbb{O}}$ and $n_C = n_{\mathrm{DiCo}(\mathbb{O})}$. (*Hint*: Use 4.6 and Cor. 22.19.)
(b) Show that there is an isomorphism $\psi\colon C \otimes_{\mathbb{Z}} \mathbb{F}_2 \xrightarrow{\sim} \mathrm{DiCo}(\mathbb{O}) \otimes_{\mathbb{Z}} \mathbb{F}_2$ and use the fact that the orthogonal group of $n_C \otimes_{\mathbb{Z}} \mathbb{F}_2$ is generated by orthogonal transvections (Dieudonné [67, Prop. 14]) to lift ψ to an orthogonal transformation $\varphi\colon C \to \mathrm{DiCo}(\mathbb{O})$ such that $\varphi(x \cdot y) = \pm\varphi(x)\varphi(y)$ for all $x, y \in C^\times$. (*Hint*: Use the fact, known from the solution to Exc. 23.37, that the map $C^\times \to (C \otimes_{\mathbb{Z}} \mathbb{F}_2)^\times$ induced by the natural surjection $C \to C \otimes_{\mathbb{Z}} \mathbb{F}_2$ is itself surjective and that each fiber consists of two elements.)
(c) Now prove that φ or $-\varphi$ is an isomorphism.

23.40. *Splitting fields of composition algebras*. Let C be a composition algebra over a field F. Prove:

(a) (Ferrar [81, Lemma 5], Petersson-Racine [223, Prop. 4.3]). For a quadratic field extension K of F to be a splitting field of C it is necessary and sufficient that one of the following hold.
  (i) $C \cong F$.
  (ii) C is split quadratic étale.
  (iii) There exists an F-embedding $K \hookrightarrow C$.
(b) Suppose F has characteristic $\neq 2$, so $K \cong F[\sqrt{\alpha}]$ for some non-square $\alpha \in F^\times$, and suppose that $C \neq F$. Show: K is a splitting field for C if and only if the quadratic form $\langle\alpha\rangle_{\mathrm{quad}} \perp n_C|_{C^0}$ is isotropic over F.

23.41. Let C be a field extension of F of degree 2 or 3, and let K be any field containing F. Prove: $C \otimes_F K$ is not a field if and only if there is an F-embedding $C \hookrightarrow K$.

23.42 (Hoffmann)**.** Take $C := \mathrm{Cay}(\mathbb{Q}; -7, -15)$, a quaternion algebra, and define $K := \mathbb{Q}(\sqrt{-1}, \sqrt{5})$. Verify that C is a division algebra, C_K is split, and no subalgebra E lying properly between $\mathbb{Q}$ and K embeds in C.

Remark. If F has characteristic 2 and C is a quaternion F-algebra split by a biquadratic extension $K = F(\sqrt{a}, \sqrt{b})$, D. Hoffmann proved that there is a quadratic extension $E :=$

$F(\sqrt{c})$ contained in K such that C_E is split, see [122, Cor. 4.3]. This is a stark contrast to the example provided in this exercise. It is interesting also to compare Hoffmann's result with Albert's theorem [102, Thm. 9.1.1] on p-algebras split by purely inseparable extensions.

24 Affine schemes

A treatment of octonions and Albert algebras over commutative rings would be incomplete without taking advantage of, and giving applications to, the theory of affine group schemes. Our aim in the present section will be to carry out a first thrust into this important topic. We do so by explaining the most elementary and basic notions from scheme theory and by illustrating them through a number of simple examples. We always focus attention on what is absolutely essential for the intended applications. Though a considerable amount of what we will be doing here retains its validity under much more general circumstances (e.g., in the setting of category theory), generalizations of this sort will be completely ignored.

Throughout we let k be an arbitrary commutative ring. In our treatment of affine k-schemes, we follow Demazure-Gabriel [61] by adopting the functorial point of view. However, in order to keep matters simple, the delicate formalism developed by loc. cit. in order to stay within a consistent framework of set theory will be avoided; instead, we favor a more stream-lined "naive" approach as given, e.g., by Jantzen [146]. Our notation will combine that of Jantzen [146] and Loos [174].

24.1 k-functors, subfunctors and direct products. By a *k-functor* we mean a functor $\mathbf{X}$ from the category of unital commutative associative k-algebras to the category of sets:

$$\mathbf{X}\colon k\text{-}\mathbf{alg} \longrightarrow \mathbf{set}.$$

Morphisms of k-functors are defined as natural transformations, so if $\mathbf{X}, \mathbf{X}'$ are k-functors, a *morphism* $f\colon \mathbf{X} \to \mathbf{X}'$ is a family of set maps $f(R)\colon \mathbf{X}(R) \to \mathbf{X}'(R)$, one for each $R \in k\text{-}\mathbf{alg}$, such that, for each morphism $\varrho\colon R \to R'$ in k-**alg**, the diagram

$$\begin{array}{ccc} \mathbf{X}(R) & \xrightarrow{f(R)} & \mathbf{X}'(R) \\ {\scriptstyle \mathbf{X}(\varrho)}\downarrow & & \downarrow{\scriptstyle \mathbf{X}'(\varrho)} \\ \mathbf{X}(R') & \xrightarrow[f(R')]{} & \mathbf{X}'(R') \end{array} \tag{1}$$

commutes. We write k-**fct** for the category of k-functors. Given k-functors $\mathbf{X}$, $\mathbf{X}'$, we will write $\mathrm{Mor}(\mathbf{X}, \mathbf{X}')$ for the totality of morphisms from $\mathbf{X}$ to $\mathbf{X}'$. Note that a morphism $f\colon \mathbf{X} \to \mathbf{X}'$ is an isomorphism if and only if the set maps $f(R)\colon \mathbf{X}(R) \to \mathbf{X}'(R)$ are bijective for all $R \in k$-**alg**.

By a *subfunctor* of a k-functor $\mathbf{X}$ we mean a k-functor $\mathbf{Y}$ such that $\mathbf{Y}(R) \subseteq \mathbf{X}(R)$ for all $R \in k$-**alg** and the inclusion maps $i(R)\colon \mathbf{Y}(R) \hookrightarrow \mathbf{X}(R)$ give rise to a morphism $i\colon \mathbf{Y} \to \mathbf{X}$ of k-functors; in other words, for any morphism $\varrho\colon R \to R'$ in k-**alg**, we have $\mathbf{X}(\varrho)(\mathbf{Y}(R)) \subseteq \mathbf{Y}(R')$, and the set map $\mathbf{Y}(\varrho)\colon \mathbf{Y}(R) \to \mathbf{Y}(R')$ is induced by $\mathbf{X}(\varrho)$ via restriction. We sometimes write $\mathbf{Y} \subseteq \mathbf{X}$ for $\mathbf{Y}$ being a subfunctor of $\mathbf{X}$.

Let $\mathbf{X}_1, \mathbf{X}_2$ be k-functors. Then we define a k-functor $\mathbf{X}_1 \times \mathbf{X}_2$, called their *direct product*, by setting $(\mathbf{X}_1 \times \mathbf{X}_2)(R) := \mathbf{X}_1(R) \times \mathbf{X}_2(R)$ for all $R \in k$-**alg** and $(\mathbf{X}_1 \times \mathbf{X}_2)(\varrho) := \mathbf{X}_1(\varrho) \times \mathbf{X}_2(\rho)$ for all morphisms $\varrho\colon R \to R'$ in k-**alg**. The direct product comes equipped with two *projection morphisms* $p_i\colon \mathbf{X}_1 \times \mathbf{X}_2 \to \mathbf{X}_i$ for $i = 1, 2$ such that $p_i(R)$ is the projection from $\mathbf{X}_1(R) \times \mathbf{X}_2(R)$ onto the i-th factor, for each $R \in k$-**alg**. It then follows that $\mathbf{X}_1 \times \mathbf{X}_2$ together with p_1, p_2 is an honest-to-goodness direct product in the category k-**fct** because it satisfies the corresponding universal property.

24.2 The concept of an affine k-scheme. Let $R \in k$-**alg**. We define

$$\mathbf{Spec}(R) := \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, -)\colon k\text{-}\mathbf{alg} \longrightarrow \mathbf{set}, \tag{1}$$

so $\mathbf{Spec}(R)$ is the k-functor given by

$$\mathbf{Spec}(R)(S) = \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S) \tag{2}$$

for all $S \in k$-**alg** and

$$\begin{gathered}\mathbf{Spec}(R)(\sigma)\colon\ \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S) \longrightarrow \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S'), \\ \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S) \ni \varphi \longmapsto \mathbf{Spec}(R)(\sigma)(\varphi) := \sigma \circ \varphi \in \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S')\end{gathered} \tag{3}$$

for all morphisms $\sigma\colon S \to S'$ in k-**alg**. By an *affine k-scheme* or an *affine scheme over k* we mean a k-functor that is isomorphic to $\mathbf{Spec}(R)$, for some $R \in k$-**alg**. We view affine k-schemes as a full subcategory of k-**fct**, denoted by k-**aff**.

Let $\varphi\colon R' \to R$ be a morphism in k-**alg**. Then

$$\mathbf{Spec}(\varphi) := \mathrm{Hom}_{k\text{-}\mathbf{alg}}(-, \varphi)\colon \mathbf{Spec}(R) \longrightarrow \mathbf{Spec}(R') \tag{4}$$

is a morphism of k-functors, explicitly given by

$$\begin{gathered}\mathbf{Spec}(\varphi)(S)\colon \mathbf{Spec}(R)(S) \longrightarrow \mathbf{Spec}(R')(S), \\ \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, S) \ni \psi \longmapsto \mathbf{Spec}(\varphi)(S)(\psi) := \psi \circ \varphi \in \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R', S)\end{gathered} \tag{5}$$

for all $S \in k$-**alg**. If $\varphi' \colon R'' \to R'$ is another morphism in k-**alg**, we have

$$\mathbf{Spec}(\mathbf{1}_R) = \mathbf{1}_{\mathbf{Spec}(R)}, \quad \mathbf{Spec}(\varphi \circ \varphi') = \mathbf{Spec}(\varphi') \circ \mathbf{Spec}(\varphi). \tag{6}$$

Summing up we conclude that the data presented in (1), (4) define a contra-variant functor

$$\mathbf{Spec} \colon k\text{-}\mathbf{alg} \longrightarrow k\text{-}\mathbf{fct}, \tag{7}$$

which may also be regarded as a contra-variant functor

$$\mathbf{Spec} \colon k\text{-}\mathbf{alg} \longrightarrow k\text{-}\mathbf{aff}. \tag{8}$$

In the latter capacity, it will be seen in due course to induce an anti-equivalence of categories.

24.3 Affine n-space. Let n be a positive integer. We define a k-functor $\mathbb{A}^n_k$, called *affine n-space*, by setting $\mathbb{A}^n_k(R) := R^n$ as a set and

$$\begin{gathered} \mathbb{A}^n_k(\varrho) := \varrho^n \colon R^n \longrightarrow R'^n, \\ R^n \ni (r_1, \ldots, r_n) \longmapsto (\varrho(r_1), \ldots, \varrho(r_n)) \in R'^n \end{gathered} \tag{1}$$

for a morphism $\varrho \colon R \to R'$ in k-**alg** as a set map. With independent indeterminates $\mathbf{t}_1, \ldots, \mathbf{t}_n$, we claim that

$$\mathbb{A}^n_k \cong \mathbf{Spec}(k[\mathbf{t}_1, \ldots, \mathbf{t}_n]) \tag{2}$$

and, in particular, that $\mathbb{A}^n_k$ *is an affine scheme over k.* Indeed, letting $R \in k$-**alg** and $r_1, \ldots, r_n \in R$, write

$$\varepsilon^n(R)(r_1, \ldots, r_n) \colon k[\mathbf{t}_1, \ldots, \mathbf{t}_n] \longrightarrow R$$

for the morphism in k-**alg** given by

$$\varepsilon^n(R)(r_1, \ldots, r_n)(g) := g(r_1, \ldots, r_n) \qquad (g \in k[\mathbf{t}_1, \ldots, \mathbf{t}_n]). \tag{3}$$

Note that $\varepsilon^n(R)(r_1, \ldots, r_n)$ is uniquely determined by the condition of sending $\mathbf{t}_i$ to r_i for $1 \le i \le n$. In this way we obtain a bijective set map

$$\varepsilon^n(R) \colon R^n \xrightarrow{\sim} \mathrm{Hom}_{k\text{-}\mathbf{alg}}(k[\mathbf{t}_1, \ldots, \mathbf{t}_n], R) = \mathbf{Spec}(k[\mathbf{t}_1, \ldots, \mathbf{t}_n])(R)$$

varying functorially with R. Hence

$$\varepsilon^n \colon \mathbb{A}^n_k \xrightarrow{\sim} \mathbf{Spec}(k[\mathbf{t}_1, \ldots, \mathbf{t}_n])$$

is an isomorphism of k-functors.

24.4 Proposition (Yoneda Lemma)**.** *Let* $\mathbf{X}$ *be a* k*-functor and* $R \in k\text{-}\mathbf{alg}$*. Then the assignment*

$$\operatorname{Mor}(\mathbf{Spec}(R), \mathbf{X}) \ni f \longmapsto \Phi_{R,\mathbf{X}}(f) := f(R)(\mathbf{1}_R) \in \mathbf{X}(R) \tag{1}$$

defines a bijection

$$\Phi_{R,\mathbf{X}} \colon \operatorname{Mor}(\mathbf{Spec}(R), \mathbf{X}) \xrightarrow{\sim} \mathbf{X}(R), \tag{2}$$

and we have

$$\Phi^{-1}_{R,\mathbf{X}}(x)(S)(\varphi) = \mathbf{X}(\varphi)(x) \tag{3}$$

for all $x \in \mathbf{X}(R)$*,* $S \in k\text{-}\mathbf{alg}$*,* $\varphi \in \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, S)$*.*

Proof Given $x \in \mathbf{X}(R)$, $S \in k\text{-}\mathbf{alg}$, we define a set map

$$\Theta(x)(S) \colon \mathbf{Spec}(R)(S) \longrightarrow \mathbf{X}(S)$$

by

$$\Theta(x)(S)(\varphi) := \mathbf{X}(\varphi)(x) \qquad (\varphi \in \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, S)). \tag{4}$$

For a morphism $\sigma \colon S \to S'$ in $k\text{-}\mathbf{alg}$ it follows easily from (24.2.3) that the diagram

$$\begin{array}{ccc} \mathbf{Spec}(R)(S) & \xrightarrow{\Theta(x)(S)} & \mathbf{X}(S) \\ {\scriptstyle \mathbf{Spec}(R)(\sigma)}\downarrow & & \downarrow{\scriptstyle \mathbf{X}(\sigma)} \\ \mathbf{Spec}(R)(S') & \xrightarrow[\Theta(x)(S')]{} & \mathbf{X}(S') \end{array}$$

commutes. Thus $\Theta(x) \in \operatorname{Mor}(\mathbf{Spec}(R), \mathbf{X})$, and we have obtained a map

$$\Theta \colon \mathbf{X}(R) \longrightarrow \operatorname{Mor}(\mathbf{Spec}(R), \mathbf{X}).$$

It is now straightforward to verify that the composition $\Theta \circ \Phi_{R,\mathbf{X}}$ is the identity on $\operatorname{Mor}(\mathbf{Spec}(R), \mathbf{X})$ and $\Phi_{R,\mathbf{X}} \circ \Theta$ is the identity on $\mathbf{X}(R)$. Hence $\Phi_{R,\mathbf{X}}$ is bijective with inverse Θ. □

24.5 Corollary. *Let* $R, R' \in k\text{-}\mathbf{alg}$*.*

(a) The map

$$\begin{aligned} \operatorname{Mor}(\mathbf{Spec}(R), \mathbf{Spec}(R')) &\xrightarrow{\sim} \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R', R), \\ f &\longmapsto \Phi_{R,\mathbf{Spec}(R')}(f) = f(R)(\mathbf{1}_R) \end{aligned} \tag{1}$$

is a bijection with inverse

$$\operatorname{Hom}_{k\text{-}\mathbf{alg}}(R', R) \xrightarrow{\sim} \operatorname{Mor}(\mathbf{Spec}(R), \mathbf{Spec}(R')), \quad \varphi \longmapsto \mathbf{Spec}(\varphi). \tag{2}$$

(b) $\varphi \in \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R', R)$ *is an isomorphism if and only if*

$$\mathbf{Spec}(\varphi) \in \mathrm{Mor}(\mathbf{Spec}(R), \mathbf{Spec}(R'))$$

is an isomorphism, and in this case $\mathbf{Spec}(\varphi)^{-1} = \mathbf{Spec}(\varphi^{-1})$.

Proof Specializing Prop. 24.4 to $\mathbf{X} := \mathbf{Spec}(R')$ and applying (24.2.3) and (24.2.5), we obtain (a). It remains to establish (b). If φ is an isomorphism, then so is $\mathbf{Spec}(\varphi)$, by (24.2.6), with $\mathbf{Spec}(\varphi)^{-1} = \mathbf{Spec}(\varphi^{-1})$. Conversely, suppose $\mathbf{Spec}(\varphi)$ is an isomorphism. Then there exists a morphism $g\colon \mathbf{Spec}(R') \to \mathbf{Spec}(R)$ such that $g \circ \mathbf{Spec}(\varphi) = \mathbf{1}_{\mathbf{Spec}(R)}$, $\mathbf{Spec}(\varphi) \circ g = \mathbf{1}_{\mathbf{Spec}(R')}$. Here (a) implies $g = \mathbf{Spec}(\varphi')$ for some morphism $\varphi'\colon R \to R'$ in k-**alg**. From (24.2.6) we therefore deduce $\mathbf{Spec}(\varphi \circ \varphi') = \mathbf{1}_{\mathbf{Spec}(R)}$, $\mathbf{Spec}(\varphi' \circ \varphi) = \mathbf{1}_{\mathbf{Spec}(R')}$, and (a) again shows that φ is an isomorphism with inverse φ'. □

24.6 Regular functions. With affine 1-space $\mathbb{A}^1_k$, also called the *affine line*, we consider the contra-variant functor

$$k[-] := \mathrm{Mor}(-, \mathbb{A}^1_k)\colon k\text{-}\mathbf{fct} \longrightarrow \mathbf{set}, \tag{1}$$

so we have

$$k[\mathbf{X}] := \mathrm{Mor}(\mathbf{X}, \mathbb{A}^1_k) \tag{2}$$

for all k-functors $\mathbf{X}$ and

$$\begin{gathered} k[f]\colon k[\mathbf{X}'] \longrightarrow k[\mathbf{X}], \\ \mathrm{Mor}(\mathbf{X}', \mathbb{A}^1_k) \ni f' \longmapsto k[f](f') := f' \circ f \in \mathrm{Mor}(X, \mathbb{A}^1_k) \end{gathered} \tag{3}$$

for all morphisms $f\colon \mathbf{X} \to \mathbf{X}'$ of k-functors. Since $\mathbb{A}^1_k(R) = R$ for all $R \in k$-**alg**, the set $k[\mathbf{X}]$, for any k-functor $\mathbf{X}$, carries the structure of a unital commutative associative k-algebra by defining the scalar multiple $\alpha f \in k[\mathbf{X}]$, the sum $f_1 + f_2 \in k[\mathbf{X}]$ and the product $f_1 f_2 \in k[\mathbf{X}]$ according to the rules

$$\begin{aligned} (\alpha f)(R)(x) &:= \alpha f(R)(x), \\ (f_1 + f_2)(R)(x) &:= f_1(R)(x) + f_2(R)(x), \\ (f_1 f_2)(R)(x) &:= f_1(R)(x) f_2(R)(x) \end{aligned} \tag{4}$$

for $\alpha \in k$, $f, f_1, f_2 \in k[\mathbf{X}]$, $R \in k$-**alg** and $x \in \mathbf{X}(R)$. Thus $k[\mathbf{X}] \in k$-**alg**, with

$$1_{k[\mathbf{X}]}(R)(x) = 1_R \qquad (R \in k\text{-}\mathbf{alg},\quad x \in \mathbf{X}(R)). \tag{5}$$

We call $k[\mathbf{X}]$ the *k-algebra of regular functions* on $\mathbf{X}$. Note for $R \in k$-**alg** that the bijection

$$\Phi_{R,\mathbb{A}^1_k}\colon k[\mathbf{Spec}(R)] \xrightarrow{\sim} R \tag{6}$$

of Prop. 24.4 is an isomorphism of k-algebras.

If $f\colon \mathbf{X} \to \mathbf{X}'$ is a morphism of k-functors, then one checks easily that

$$k[f]\colon k[\mathbf{X}'] \longrightarrow k[\mathbf{X}]$$

is a morphism of unital commutative associative k-algebras. Thus the functor (1) may actually be viewed as a contra-variant functor

$$k[-] = \mathrm{Mor}(-, \mathbb{A}^1_k)\colon k\text{-}\mathbf{fct} \longrightarrow k\text{-}\mathbf{alg}, \tag{7}$$

from which we recover (1) by composing (7) with the forgetful functor k-**alg** $\to$ **set**. On the other hand, restricting the functor (7) to the category of affine k-schemes, we obtain a contra-variant functor

$$k[-] = \mathrm{Mor}(-, \mathbb{A}^1_k)\colon k\text{-}\mathbf{aff} \longrightarrow k\text{-}\mathbf{alg}. \tag{8}$$

The fact that all these functors are denoted by the same symbol should not cause any confusion.

24.7 Example. Let n be a positive integer. For $g \in k[\mathbf{t}_1, \ldots, \mathbf{t}_n]$, the set maps

$$\tilde{g}(R)\colon R^n \longrightarrow R, \quad (r_1, \ldots, r_n) \longmapsto \tilde{g}(R)(r_1, \ldots, r_n) := g(r_1, \ldots, r_n) \tag{1}$$

vary functorially with $R \in k$-**alg**, which therefore give rise to an element $\tilde{g} \in \mathrm{Mor}(\mathbb{A}^n_k, \mathbb{A}^1_k) = k[\mathbb{A}^n_k]$. On the other hand, g determines a unique morphism $g^*\colon k[\mathbf{t}] \to k[\mathbf{t}_1, \ldots, \mathbf{t}_n]$ in k-**alg** given by

$$g^*(h) := h(g) \qquad\qquad (h \in k[\mathbf{t}]), \tag{2}$$

and one checks that the diagram

$$\begin{array}{ccc} R^n & \xrightarrow{\quad\tilde{g}(R)\quad} & R \\ {\scriptstyle \varepsilon^n(R)}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \varepsilon^1(R)} \\ \mathbf{Spec}(k[\mathbf{t}_1, \ldots, \mathbf{t}_n])(R) & \xrightarrow[\mathbf{Spec}(g^*)(R)]{} & \mathbf{Spec}(k[\mathbf{t}])(R) \end{array} \tag{3}$$

commutes. Hence, by Cor. 24.5 (a), since every morphism $k[\mathbf{t}] \to k[\mathbf{t}_1, \ldots, \mathbf{t}_n]$ in k-**alg** has the form g^* for a unique $g \in k[\mathbf{t}_1, \ldots, \mathbf{t}_n]$,

$$k[\mathbf{t}_1, \ldots, \mathbf{t}_n] \xrightarrow{\sim} k[\mathbb{A}^n_k], \quad g \longmapsto \tilde{g} \tag{4}$$

is an isomorphism of k-algebras. We usually identify

$$k[\mathbf{t}_1, \ldots, \mathbf{t}_n] = k[\mathbb{A}^n_k], \quad k[\mathbf{t}_1, \ldots, \mathbf{t}_n] \ni g = \tilde{g} \in k[\mathbb{A}^n_k] \tag{5}$$

accordingly.

24.8 Proposition. *The contra-variant functors*

$$\mathbf{Spec}\colon k\text{-}\mathbf{alg} \longrightarrow k\text{-}\mathbf{fct}, \quad k[-]\colon k\text{-}\mathbf{fct} \longrightarrow k\text{-}\mathbf{alg}$$

are adjoint to one another in the sense that, for all k-functors $\mathbf{X}$ *and all* $R \in k\text{-}\mathbf{alg}$*, there exists a bijection*

$$\Psi_{\mathbf{X},R}\colon \operatorname{Mor}(\mathbf{X}, \mathbf{Spec}(R)) \xrightarrow{\sim} \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, k[\mathbf{X}]),$$

natural in $\mathbf{X}$ *and R, given by*

$$\Psi_{\mathbf{X},R}(f)(r)(S)(x) = f(S)(x)(r) \tag{1}$$

for all $f \in \operatorname{Mor}(\mathbf{X}, \mathbf{Spec}(R))$*,* $r \in R$*,* $S \in k\text{-}\mathbf{alg}$*,* $x \in \mathbf{X}(S)$*. Moreover,*

$$\Psi^{-1}_{\mathbf{X},R}(g)(S)(x)(r) = g(r)(S)(x) \tag{2}$$

for all $g \in \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, k[\mathbf{X}])$*,* $S \in k\text{-}\mathbf{alg}$*,* $x \in \mathbf{X}(S)$*,* $r \in R$*.*

Proof We define $\Psi := \Psi_{\mathbf{X},R}$ by (1). Since $f(S)(x)\colon R \to S$ is a morphism in k-**alg**, so will be $\Psi(f)\colon R \to k[\mathbf{X}]$ once we have shown that the left-hand side of (1) varies functorially with S. Thus, fixing $r \in R$ and a morphism $\sigma\colon S \to S'$ in k-**alg**, we must show with $g := \Psi(f)$ that the diagram

$$\begin{array}{ccc} \mathbf{X}(S) & \xrightarrow{g(r)(S)} & S \\ {\scriptstyle \mathbf{X}(\sigma)}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \mathbf{X}(S') & \xrightarrow[g(r)(S')]{} & S' \end{array} \tag{3}$$

commutes, which follows by a straightforward computation from (1) and the commutativity of

$$\begin{array}{ccc} \mathbf{X}(S) & \xrightarrow{f(S)} & \mathbf{Spec}(R)(S) \\ {\scriptstyle \mathbf{X}(\sigma)}\downarrow & & \downarrow{\scriptstyle \mathbf{Spec}(R)(\sigma)} \\ \mathbf{X}(S') & \xrightarrow[f(S')]{} & \mathbf{Spec}(R)(S'). \end{array}$$

Conversely, define $\Psi'\colon \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, k[\mathbf{X}]) \to \operatorname{Mor}(\mathbf{X}, \mathbf{Spec}(R))$ by

$$\Psi'(g)(S)(x)(r) := g(r)(S)(x) \tag{4}$$

for $g \in \operatorname{Hom}_{k\text{-}\mathbf{alg}}(R, k[\mathbf{X}])$, $S \in k\text{-}\mathbf{alg}$, $x \in \mathbf{X}(S)$, $r \in R$. Again we must show that the set map $\Psi'(g)(S)\colon \mathbf{X}(S) \to \mathbf{Spec}(R)(S)$ varies functorially with S, i.e.,

that for a morphism $\sigma\colon S \to S'$ in k-**alg** the diagram

$$\begin{array}{ccc} \mathbf{X}(S) & \xrightarrow{\Psi'(g)(S)} & \mathbf{Spec}(R)(S) \\ {\scriptstyle \mathbf{X}(\sigma)}\downarrow & & \downarrow{\scriptstyle \mathbf{Spec}(R)(\sigma)} \\ \mathbf{X}(S') & \xrightarrow[\Psi'(g)(S')]{} & \mathbf{Spec}(R)(S') \end{array}$$

commutes, which follows from the commutativity of (3) for all $r \in R$. Finally, the definitions (1), (4) show that the maps Ψ, Ψ' are inverse to one another. □

24.9 Example. The affine k-scheme $\mathbf{Spec}(k)$ satisfies

$$\mathbf{Spec}(k)(R) = \mathrm{Hom}_{k\text{-}\mathbf{alg}}(k, R) = \{\vartheta_R\} \tag{1}$$

for all $R \in k$-**alg**, where

$$\vartheta_R\colon k \longrightarrow R, \quad \alpha \longmapsto (\vartheta_R)(\alpha) := \alpha 1_R \tag{2}$$

is the unit morphism in k-**alg** corresponding to R. Hence

$$\mathbf{Spec}(k)(\varphi)(\vartheta_R) = \vartheta_S \tag{3}$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**.

Now let $\mathbf{X}$ be any k-functor. By Prop. 24.8, there is a unique morphism $\sigma_{\mathbf{X}}\colon \mathbf{X} \to \mathbf{Spec}(k)$, called the *structure morphism* of $\mathbf{X}$, and (1), (3) imply for all $R \in k$-**alg** that

$$\sigma_{\mathbf{X}}(R)\colon \mathbf{X}(R) \longrightarrow \mathbf{Spec}(k)(R) = \{\vartheta_R\}$$

is the constant map

$$\mathbf{X}(R) \ni x \longmapsto \vartheta_R \in \mathbf{Spec}(k)(R).$$

Moreover, every morphism $f\colon \mathbf{X} \to \mathbf{X}'$ of k-functors is one *over* $\mathbf{Spec}(k)$ in the sense that the triangle

$$\begin{array}{ccc} \mathbf{X} & \xrightarrow{\quad f \quad} & \mathbf{X}' \\ & {\scriptstyle \sigma_{\mathbf{X}}}\searrow \quad \swarrow{\scriptstyle \sigma_{\mathbf{X}'}} & \\ & \mathbf{Spec}(k) & \end{array}$$

commutes. Finally, if $\mathbf{X} = \mathbf{Spec}(R)$ is an affine k-scheme, then

$$\sigma_{\mathbf{X}} = \mathbf{Spec}(\vartheta_R). \tag{4}$$

24.10 Proposition. *(a) Let* $\mathbf{X}$ *be a* k*-functor. With the notation of Prop. 24.8,*

$$f_{\mathbf{X}} := \Psi^{-1}_{\mathbf{X},k[\mathbf{X}]}(\mathbf{1}_{k[\mathbf{X}]})\colon \mathbf{X} \longrightarrow \mathbf{Spec}(k[\mathbf{X}]) \tag{1}$$

is a morphism of k-functors such that

$$f_{\mathbf{X}}(R)(x)(g) = g(R)(x) \tag{2}$$

*for all $R \in k$-**alg**, $x \in \mathbf{X}(R)$, $g \in k[\mathbf{X}]$, and if $h\colon \mathbf{X} \to \mathbf{X}'$ is any morphism of k-functors, then the diagram*

$$\begin{array}{ccc} \mathbf{X} & \xrightarrow{f_{\mathbf{X}}} & \mathbf{Spec}(k[\mathbf{X}]) \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle \mathbf{Spec}(k[h])} \\ \mathbf{X}' & \xrightarrow[f_{\mathbf{X}'}]{} & \mathbf{Spec}(k[\mathbf{X}']) \end{array} \tag{3}$$

commutes.

(b) With the notation of Prop. 24.4,

$$f_{\mathbf{Spec}(R)} = \mathbf{Spec}(\Phi_{R,\mathbb{A}^1_k}). \tag{4}$$

(c) A k-functor $\mathbf{X}$ is an affine k-scheme if and only if $f_{\mathbf{X}}$ is an isomorphism.

Proof (a) That the k-functor $f_{\mathbf{X}}$ satisfies (2) follows immediately from (24.8.2). Using (2), it is now straightforward to verify the commutativity of (3).

(b) Put $\mathbf{X} := \mathbf{Spec}(R)$. We have noted in (24.6.6) that $\Phi_{R,\mathbb{A}^1_k}\colon k[\mathbf{X}] \to R$ is an isomorphism of k-algebras. By Cor. 24.5, therefore,

$$\mathbf{Spec}(\Phi_{R,\mathbb{A}^1_k})\colon \mathbf{X} \xrightarrow{\sim} \mathbf{Spec}(k[\mathbf{X}]) \tag{5}$$

is an isomorphism of k-functors. In order to establish (4), let $S \in k$-**alg**, $x \in \mathbf{X}(S)$, $g \in k[\mathbf{X}]$. With $\Phi := \Phi_{R,\mathbb{A}^1_k}$ we must show $\mathbf{Spec}(\Phi)(S)(x)(g) = f_{\mathbf{X}}(S)(x)(g)$, which follows easily by direct computation since the diagram

$$\begin{array}{ccc} \mathbf{Spec}(R)(R) & \xrightarrow{g(R)} & R \\ {\scriptstyle \mathbf{Spec}(R)(x)}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbf{Spec}(R)(S) & \xrightarrow[g(S)]{} & S \end{array}$$

commutes.

(c) follows immediately from (3), (4) and (5). □

24.11 Corollary. *The contra-variant functors*

$$k\text{-}\mathbf{alg} \underset{k[-]}{\overset{\mathbf{Spec}}{\rightleftarrows}} k\text{-}\mathbf{aff}$$

define an anti-equivalence of categories.

Proof Let $\mathbf{X}$ be an affine k-scheme. Then $f_{\mathbf{X}}\colon \mathbf{X} \xrightarrow{\sim} \mathbf{Spec}(k[\mathbf{X}])$ is an isomorphism by Prop. 24.10 (c), and (24.10.3) shows that the family $f_{\mathbf{X}}$, $\mathbf{X} \in k\text{-}\mathbf{aff}$, determines an isomorphism of functors from $\mathbf{1}_{k\text{-}\mathbf{aff}}$ to $\mathbf{Spec} \circ k[-]$. Conversely, let $R \in k\text{-}\mathbf{alg}$. Then the bijective map

$$\Phi = \Phi_{R,\mathbb{A}^1_k}\colon k[\mathbf{Spec}(R)] \xrightarrow{\sim} R$$

of Prop. 24.4 by (24.6.6) is an isomorphism of k-algebras. Now let $\varrho\colon R \to R'$ be a morphism of k-algebras. Since for all $f \in k[\mathbf{Spec}(R)]$ the diagram

$$\begin{array}{ccc} \mathbf{Spec}(R)(R) & \xrightarrow{f(R)} & R \\ {\scriptstyle \mathbf{Spec}(R)(\varrho)}\downarrow & & \downarrow{\scriptstyle \varrho} \\ \mathbf{Spec}(R)(R') & \xrightarrow[f(R')]{} & R' \end{array}$$

commutes, one checks that so does

$$\begin{array}{ccc} k[\mathbf{Spec}(R)] & \xrightarrow[\Phi_{R,\mathbb{A}^1_k}]{\cong} & R \\ {\scriptstyle k[\mathbf{Spec}(\varrho)]}\downarrow & & \downarrow{\scriptstyle \varrho} \\ k[\mathbf{Spec}(R')] & \xrightarrow[\Phi_{R',\mathbb{A}^1_k}]{\cong} & R'. \end{array}$$

Thus the family $\Phi_{R,\mathbb{A}^1_k}$, $R \in k\text{-}\mathbf{alg}$, determines an isomorphism of functors from the composition $k[-] \circ \mathbf{Spec}$ to $\mathbf{1}_{k\text{-}\mathbf{alg}}$. □

24.12 Notational conventions. (a) Let $f\colon \mathbf{X} \to \mathbf{X}'$ be a morphism of k-functors. If there is no danger of confusion, the set map $f(R)\colon \mathbf{X}(R) \to \mathbf{X}'(R)$ for $R \in k\text{-}\mathbf{alg}$ will simply be written as f:

$$f\colon \mathbf{X}(R) \longrightarrow \mathbf{X}'(R) \qquad (R \in k\text{-}\mathbf{alg}). \tag{1}$$

For a morphism $\varrho\colon R \to R'$ in $k\text{-}\mathbf{alg}$ and $x \in \mathbf{X}(R)$, we therefore have

$$f(\mathbf{X}(\varrho)(x)) = \mathbf{X}'(\varrho)(f(x)). \tag{2}$$

(b) Let $\mathbf{X}$ be an affine k-scheme. Then we identify

$$\mathbf{X} = \mathbf{Spec}(k[\mathbf{X}]) \tag{3}$$

by means of the isomorphism $f_{\mathbf{X}}$ of Prop. 24.10. Given $R \in k\text{-}\mathbf{alg}$, $x \in \mathbf{X}(R)$ and $f \in k[\mathbf{X}]$, an application of (24.10.2) yields $x(f) = f_{\mathbf{X}}(R)(x)(f) = f(R)(x)$, hence

$$x(f) = f(x). \tag{4}$$

(c) Let $f\colon \mathbf{X} \to \mathbf{X}'$ be a morphism of affine k-schemes. By Cor. 24.11, there is a unique morphism $f^*\colon k[\mathbf{X}'] \to k[\mathbf{X}]$ in k-**alg** having $f = \mathbf{Spec}(f^*)$. We call f^* the *co-morphism* of f.

24.13 Direct products of affine schemes. For $i = 1, 2$, let $\mathbf{X}_i$ be an affine k-scheme. Since the tensor product (over k) is the co-product in the category k-**alg**, it should not come as a surprise that *the k-functor $\mathbf{X}_1 \times \mathbf{X}_2$ of 24.1 is an affine k-scheme as well, corresponding to the k-algebra $k[\mathbf{X}_1] \otimes k[\mathbf{X}_2] \in k$-**alg***. More precisely,

$$\Pi\colon \mathbf{X}_1 \times \mathbf{X}_2 \xrightarrow{\sim} \mathbf{Spec}(k[\mathbf{X}_1] \otimes k[\mathbf{X}_2])$$

defined by

$$\Pi(x_1, x_2)(f_1 \otimes f_2) := x_1(f_1)x_2(f_2) = f_1(x_1)f_2(x_2)$$

for $R \in k$-**alg**, $x_i \in \mathbf{X}_i(R)$, $f_i \in k[\mathbf{X}_i]$, $i = 1, 2$ is easily checked to be an isomorphism of k-functors. Note that the projections $p_i\colon \mathbf{X}_1 \times \mathbf{X}_2 \to \mathbf{X}_i$ correspond to the co-morphisms $p_i^*\colon k[\mathbf{X}_i] \to k[\mathbf{X}_1] \otimes k[\mathbf{X}_2]$ given by $p_1^*(f_1) = f_1 \otimes 1_{k[\mathbf{X}_2]}$ and $p_2^*(f_2) = 1_{k[\mathbf{X}_1]} \otimes f_2$.

24.14 Remark. The material so far in this section, apart from 24.3 and 24.7, is not specific to the category k-**alg**. Speaking roughly, let $\mathbf{C}$ be a category that is *locally small* in the sense that $\mathrm{Mor}_{\mathbf{C}}(A, B)$ is a set for all objects $A, B \in \mathbf{C}$. For every object $A \in \mathbf{C}$, h_A defined by $h_A(B) := \mathrm{Mor}_{\mathbf{C}}(A, B)$ for $B \in \mathbf{C}$ defines a functor $\mathbf{C} \to$ **set**. Functors obtained in this way are called *representable*, and the Yoneda lemma says that the functor $\mathbf{C} \to \mathbf{Fun}(\mathbf{C}, \mathbf{set})$ given by $A \mapsto h_A$ is fully faithful, compare Cor. 24.11.

24.15 Closed subfunctors. Let $\mathbf{X}$ be an affine k-scheme. For any subset $I \subseteq k[\mathbf{X}]$, we use (24.12.4) to define a subfunctor $\mathbf{V}(I)$ of $\mathbf{X}$ by setting

$$\mathbf{V}(I)(R) := \{x \in \mathbf{X}(R) \mid x(I) = \{0\}\} = \{x \in \mathbf{X}(R) \mid \forall f \in I : f(x) = 0\} \qquad (1)$$

for all $R \in k$-**alg**. We call $\mathbf{V}(I)$ the *closed subfunctor of* $\mathbf{X}$ *determined by* I or simply a *closed subfunctor* of $\mathbf{X}$. It clearly depends only on the ideal generated by I. On the other hand, if $I \subseteq k[\mathbf{X}]$ is an ideal, with canonical projection $\pi\colon k[\mathbf{X}] \to k[\mathbf{X}]/I$, then $\mathbf{Spec}(\pi)\colon \mathbf{Spec}(k[\mathbf{X}]/I) \to \mathbf{Spec}(k[\mathbf{X}])$ may be regarded as an isomorphism

$$\mathbf{Spec}(\pi)\colon \mathbf{Spec}(k[\mathbf{X}]/I) \xrightarrow{\sim} \mathbf{V}(I). \qquad (2)$$

In particular, *closed subfunctors of* $\mathbf{X}$ *are affine k-schemes.* If I' is another ideal in $k[\mathbf{X}]$, with canonical projection $\pi'\colon k[\mathbf{X}] \to k[\mathbf{X}]/I'$, then we claim

$$I \subseteq I' \iff \mathbf{V}(I') \subseteq \mathbf{V}(I). \qquad (3)$$

The implication from left to right being obvious, let us assume $\mathbf{V}(I') \subseteq \mathbf{V}(I)$. Since these are both affine k-schemes, the inclusion $\mathbf{V}(I') \hookrightarrow \mathbf{V}(I)$ of closed subfunctors of $\mathbf{X}$ has the form $\mathbf{Spec}(\varrho)$ for some morphism $\varrho\colon k[\mathbf{X}]/I \to k[\mathbf{X}]/I'$ in k-**alg** satisfying $\varrho \circ \pi = \pi'$. Thus $I \subseteq \mathrm{Ker}(\varrho \circ \pi) = \mathrm{Ker}(\pi') = I'$.

24.16 Open subfunctors. Let $\mathbf{X}$ be an affine k-scheme. For any subset $I \subseteq k[\mathbf{X}]$, we define a subfunctor $\mathbf{D}(I)$ of $\mathbf{X}$ by setting

$$\mathbf{D}(I)(R) := \{x \in \mathbf{X}(R) \mid Rx(I) = R\} = \{x \in \mathbf{X}(R) \mid \sum_{f \in I} Rf(x) = R\} \tag{1}$$

for all $R \in k$-**alg**. This is indeed a subfunctor of $\mathbf{X}$ since, for all morphisms $\varrho\colon R \to R'$ in k-**alg** and all $x \in \mathbf{X}(R)$, we find finitely many $r_i \in R$, $f_i \in I$ such that $\sum r_i f_i(x) = 1_R$, which by (24.12.2) implies $\sum \varrho(r_i) f_i(\mathbf{X}(\varrho)(x)) = \sum \varrho(r_i)\varrho(f_i(x)) = \varrho(\sum r_i f_i(x)) = 1_{R'}$, and we conclude $\mathbf{X}(\varrho)(x) \in \mathbf{D}(I)(R')$.

Subfunctors of $\mathbf{X}$ having the form $\mathbf{D}(I)$ for some $I \subseteq k[\mathbf{X}]$ are said to be *open*. Of particular importance is the case of a *principal open subfunctor*, defined by the property that $I = \{f\}$, $f \in k[\mathbf{X}]$, is a singleton. We put $\mathbf{X}_f := \mathbf{D}(f) := \mathbf{D}(\{f\})$ and have

$$\mathbf{X}_f(R) = \{x \in \mathbf{X}(R) \mid f(x) \in R^\times\} = \{x \in \mathbf{X}(R) \mid x(f) \in R^\times\}. \tag{2}$$

The elements $x \in \mathbf{X}(R) = \mathrm{Hom}_{k\text{-}\mathbf{alg}}(k[\mathbf{X}], R)$ having $x(f) \in R^\times$ can be characterized by the property that they factor through the localization $k[\mathbf{X}]_f$, in which case they do so uniquely. Thus there is a natural identification

$$\mathbf{X}_f = \mathbf{Spec}(k[\mathbf{X}]_f) \tag{3}$$

such that the co-morphism of the inclusion $\mathbf{X}_f \hookrightarrow \mathbf{X}$ is the canonical map $k[\mathbf{X}] \to k[\mathbf{X}]_f$. In particular, *principal open subfunctors of affine k-schemes are affine.* Note, however, that an arbitrary open subfunctor of an affine k-scheme may not be affine.

24.17 k-group schemes. By a *k-group functor* we mean a functor from the category k-**alg** to the category of groups:

$$\mathbf{G}\colon k\text{-}\mathbf{alg} \longrightarrow \mathbf{grp}.$$

By composing $\mathbf{G}$ with the forgetful functor $\mathbf{grp} \to \mathbf{set}$, we obtain a k-functor, also denoted by $\mathbf{G}$, to which the formalism of the preceding subsections applies. By a *subgroup functor* of $\mathbf{G}$ we mean a subfunctor $\mathbf{H}$ of $\mathbf{G}$ (viewed as a k-functor) such that $\mathbf{H}(R)$ is a subgroup of $\mathbf{G}(R)$ for all $R \in k$-**alg**. Then $\mathbf{H}$ may be regarded as a k-group functor in its own right. More generally, *morphisms* of k-group functors are defined as natural transformations. Thus, given

k-group functors $\mathbf{G}, \mathbf{G}'$, a morphism $f\colon \mathbf{G} \to \mathbf{G}'$ is nothing else than a morphism of k-functors making $f(R)\colon \mathbf{G}(R) \to \mathbf{G}'(R)$ a group homomorphism for all $R \in k$-**alg**.

By an *affine k-group scheme*, we mean a k-group functor that, regarded as a k-functor, is isomorphic to an affine k-scheme, so we have $\mathbf{G} \cong \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, -)$ as k-functors, for some $R \in k$-**alg**. From now on, we will drop the prefix "affine" and just talk about *k-group schemes* to mean affine k-group schemes.

24.18 Remark. Given a k-group scheme $\mathbf{G}$, we obtain for each $R \in k$-**alg** maps $\mathbf{G}(R) \times \mathbf{G}(R) \to \mathbf{G}(R)$, $(x, y) \mapsto xy$, $\mathbf{G}(R) \to \mathbf{G}(R)$, $x \mapsto x^{-1}$ and a constant map $1 \to \mathbf{G}(R)$ whose image is the identity element of $\mathbf{G}(R)$. These maps are compatible with morphisms in k-**alg** and so define natural transformations of functors:

$$\mu\colon \mathbf{G} \times \mathbf{G} \longrightarrow \mathbf{G}, \quad i\colon \mathbf{G} \longrightarrow \mathbf{G}, \quad \varepsilon\colon \mathbf{Spec}(k) \longrightarrow \mathbf{G}.$$

(Real Lie groups are sometimes defined in a similar way, as in [292].) By the Yoneda lemma, these correspond to k-algebra homomorphisms of the coordinate algebra

$$k[\mathbf{G}] \otimes k[\mathbf{G}] \longleftarrow k[\mathbf{G}], \quad k[\mathbf{G}] \longleftarrow k[\mathbf{G}], \quad k \leftarrow k[\mathbf{G}].$$

Hence μ, i, and ε are morphisms of k-schemes satisfying properties that multiplication, inversion, and the identity usually do for groups, such as $\mu(x, i(x)) = \varepsilon$. Here is a simple example.

24.19 Examples. (a) The *additive group of k* is defined as the k-group functor $\mathbf{G_a}$ given by $\mathbf{G_a}(R) = R$ (viewed as an additive group) for all $R \in k$-**alg** and $\mathbf{G_a}(\varphi) = \varphi$ for all morphisms $\varphi\colon R \to S$ in k-**alg**. Thus $\mathbf{G_a} = \mathbb{A}^1_k$ as k-functors and $k[\mathbf{G_a}] \cong k[\mathbf{t}]$ canonically. The map $k[\mathbf{t}] \to k[\mathbf{t}] \otimes k[\mathbf{t}]$ corresponding to addition in R is given by $\mathbf{t} \mapsto \mathbf{t} \otimes 1 + 1 \otimes \mathbf{t}$ [293, p. 14].

(b) The *multiplicative group of k* is defined as the k-group functor $\mathbf{G_m}$ given by $\mathbf{G_m}(R) = R^\times$ (viewed as a multiplicative group) for all $R \in k$-**alg** and $\mathbf{G_m}(\varphi)\colon R^\times \to S^\times$ induced by a morphism $\varphi\colon R \to S$ in k-**alg** via restriction. Thus $\mathbf{G_m} = (\mathbb{A}^1_k)_{\mathbf{t}}$ as k-functors and $k[\mathbf{G_m}] \cong k[\mathbf{t}, \mathbf{t}^{-1}]$ canonically. The map $k[\mathbf{t}, \mathbf{t}^{-1}] \to k[\mathbf{t}, \mathbf{t}^{-1}] \otimes k[\mathbf{t}, \mathbf{t}^{-1}]$ corresponding to multiplication in $R^\times$ is given by $\mathbf{t} \mapsto \mathbf{t} \otimes \mathbf{t}$ [293, §2.2].

24.20 Example: constant group schemes. For a finite set Γ, put E_Γ for the product of $|\Gamma|$ copies of k, indexed by elements of Γ. Put $\mathbf{X}_\Gamma := \mathbf{Spec}(E_\Gamma)$. If R is a non-zero connected k-algebra, then the set of R-points $\mathbf{X}_\Gamma(R)$ is naturally identified with Γ. To see this, for each $\gamma \in \Gamma$, write 1_γ for the element of E_Γ that has a 1 in the copy of k labeled by γ and 0 elsewhere. The collection of

elements $\{1_\gamma \mid \gamma \in \Gamma\}$ forms a complete orthogonal system of idempotents in E_Γ. For a given homomorphism $\phi \in \mathbf{X}_\Gamma(R) = \operatorname{Hom}_{k\text{-}\mathbf{alg}}(E_\Gamma, R)$, at most one $\gamma \in \Gamma$ has the property that $\phi(1_\gamma) = 1 \in R$. Since $\phi(1) = 1$, we find that at least one $\gamma \in \Gamma$ has this property, so there is a unique $\gamma \in \Gamma$ such that $\phi(1_\gamma) = 1$. In summary, ϕ is a composition $E_\Gamma \to k \to R$ where the first arrow is projection on the γ factor and the second arrow is the unit homomorphism, allowing us to identify ϕ with the element $\gamma \in \Gamma$.

Suppose now that Γ is a group. We define a group operation on $\mathbf{X}_\Gamma(R)$ by specifying the corresponding k-algebra homomorphism $E_\Gamma \to E_\Gamma \otimes E_\Gamma$, for which it suffices to specify that

$$1_\gamma \mapsto \sum_{\sigma,\tau \in \Gamma \text{ s.t. } \sigma\tau = \gamma} 1_\sigma \otimes 1_\tau,$$

see [293, §2.3]. One can verify that, when R is connected, the identification of $\mathbf{X}_\Gamma(R)$ with Γ is compatible with the group operation on the two sets. A k-group scheme $\mathbf{X}_\Gamma$ obtained in this manner is called a *constant group scheme*. It is common to abuse notation and simply write Γ also for the k-group scheme $\mathbf{X}_\Gamma$.

24.21 Example. For a k-module M, we obtain a k-group functor $M_{\mathbf{a}}$ by setting $M_{\mathbf{a}}(R) := M_R = M \otimes R$ (viewed as an additive group) for all $R \in k\text{-}\mathbf{alg}$ and $M_{\mathbf{a}}(\varphi) := \mathbf{1}_M \otimes \varphi \colon M_{\mathbf{a}}(R) \to M_{\mathbf{a}}(S)$ (viewed as an additive group homomorphism) for all morphisms $\varphi \colon R \to S$ in $k\text{-}\mathbf{alg}$; regarded just as a k-functor. $M_{\mathbf{a}}$ has made its appearance before, in our treatment of polynomial laws (§12). Writing $S(M^*)$ for the symmetric algebra of the dual of M (Bourbaki [28, III, §6]), we claim that *if M is finitely generated projective, then $M_{\mathbf{a}}$ is a k-group scheme with $k[M_{\mathbf{a}}] \cong S(M^*)$ canonically.*

Indeed, for any $R \in k\text{-}\mathbf{alg}$, the universal property of the symmetric algebra combined with 9.2 and Lemma 9.15 yield the following chain of canonical isomorphisms.

$$\begin{aligned}\operatorname{Hom}_{k\text{-}\mathbf{alg}}(S(M^*), R) &\cong \operatorname{Hom}_k(M^*, R) \cong \operatorname{Hom}_R(M^* \otimes R, R)\\ &\cong (M^* \otimes R)^* \cong M^{**} \otimes R \cong M \otimes R = M_{\mathbf{a}}(R).\end{aligned}$$

Keeping track of how these isomorphisms act on individual elements, we obtain an identification

$$M_{\mathbf{a}}(R) = \operatorname{Hom}_{k\text{-}\mathbf{alg}}(S(M^*), R)$$

such that $u \otimes r$ for $u \in M$, $r \in R$ is the unique unital k-algebra homomorphism $S(M^*) \to R$ satisfying

$$(u \otimes r)(v^*) = \langle v^*, u\rangle r \tag{1}$$

for all $v^* \in M^*$. It is now easily checked that, for any morphism $\varphi\colon R \to S$ in k-**alg**, this identification matches $M_{\mathbf{a}}(\varphi)$ with $\mathrm{Hom}_{k\text{-}\mathbf{alg}}(S(M^*), \varphi)$, which completes the proof. In case M is k itself, $M_{\mathbf{a}}$ is just the additive group $\mathbf{G}_{\mathbf{a}}$ defined in 24.19(a).

24.22 Scalar polynomial laws revisited. Since $\mathbb{A}^1_k$, the affine line, is nothing else than the forgetful functor k-**alg** $\to$ **set**, it follows for any k-module M that $k[M_{\mathbf{a}}] = \mathrm{Mor}(M_{\mathbf{a}}, \mathbb{A}^1_k)$ agrees with the k-algebra of scalar polynomial laws on M as defined in 12.2. Thus Example 24.21 combined with Cor. 24.11 implies $\mathrm{Pol}_k(M, k) \cong S(M^*)$ as k-algebras provided M is finitely generated projective.

24.23 Example. Given a unital associative k-algebra A, we obtain a k-group functor $\mathbf{GL}_1(A)$ by setting $\mathbf{GL}_1(A)(R) := A_R^\times$ (viewed as a multiplicative group) for all $R \in k$-**alg** and by letting $\mathbf{GL}_1(A)(\varphi)\colon A_R^\times \to A_S^\times$ be the group homomorphism induced from a morphism $\varphi\colon R \to S$ in k-**alg** via restriction of $\mathbf{1}_A \otimes \varphi\colon A_R \to A_S$.

We claim that $\mathbf{GL}_1(A)$ *is a group scheme over k provided A is finitely generated projective as a k-module.* Indeed, we know from Example 24.21 that $A_{\mathbf{a}}$ is a group scheme over k. Let $f \in k[A_{\mathbf{a}}]$ be any regular function on $A_{\mathbf{a}}$ such that $x \in A_R$, $R \in k$-**alg**, is invertible if and only if $f(x)$ is invertible in R (for instance, one could choose $f = \det \circ L$, where $L\colon A \to \mathrm{End}_k(A)$ is the left multiplication of A and $\det\colon \mathrm{End}_k(A) \to k$ is the determinant, which are both compatible with base change). Then $\mathbf{GL}_1(A) = (A_{\mathbf{a}})_f$ as k-functors and (24.16.3) shows that $\mathbf{GL}_1(A)$ is a k-group scheme satisfying

$$k[\mathbf{GL}_1(A)] \cong k[A_{\mathbf{a}}]_f. \tag{1}$$

The preceding construction specializes to $\mathbf{G}_{\mathbf{m}} = \mathbf{GL}_1(k)$ but also to

$$\mathbf{GL}_n := \mathbf{GL}_1(\mathrm{Mat}_n(k)), \tag{2}$$

where we have

$$k[\mathbf{GL}_n] \cong k[\mathbf{t}_{ij} \mid 1 \le i, j \le n]_{\det}. \tag{3}$$

24.24 Example. Specializing 24.23, we let M be any k-module. Then

$$\mathbf{GL}(M) := \mathbf{GL}_1(\mathrm{End}_k(M)) \tag{1}$$

is a k-group functor having $\mathbf{GL}(M)(R) = \mathrm{GL}(M_R)$ for all $R \in k$-**alg** and

$$\mathbf{GL}(M)(\varphi)\colon \mathrm{GL}(M_R) \longrightarrow \mathrm{GL}(M_S), \quad \mathrm{GL}(M_R) \ni \eta \longmapsto \eta_S \in \mathrm{GL}(M_S) \tag{2}$$

for any morphism $\varphi\colon R \to S$ in k-**alg**. Moreover, if M is finitely generated

projective, then so is $\mathrm{End}_k(M)$ as a k-module, and 24.23 implies that $\mathbf{GL}(M)$ *is a k-group scheme.* Moreover, by (24.23.1),

$$k[\mathbf{GL}(M)] = k[\mathrm{End}_k(M)_{\mathbf{a}}]_{\det}. \tag{3}$$

24.25 Example. Let A be a non-associative k-algebra. We define a k-group subfunctor $\mathbf{Aut}(A)$ of $\mathbf{GL}(A)$ by setting $\mathbf{Aut}(A)(R) := \mathrm{Aut}(A_R)$ for all $R \in k\text{-}\mathbf{alg}$ and

$$\mathbf{Aut}(A)(\varphi)\colon\ \mathrm{Aut}(A_R) \longrightarrow \mathrm{Aut}(A_S),\quad \mathrm{Aut}(A_R) \ni \eta \longmapsto \eta_S \in \mathrm{Aut}(A_S)$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**, where we regard S as an R-algebra via φ and use (9.4.1) to identify $A_S = (A_R)_S$ as S-algebras. We claim:

(∗) If A is finitely generated projective as a k-module, then $\mathbf{Aut}(A)$ is a closed subfunctor of $\mathbf{GL}(A)$ and hence, in particular, a k-group scheme, called the *automorphism group scheme* of A.

In order to see this, let $u, v \in A$ and $w^* \in A^*$. For $R \in k\text{-}\mathbf{alg}$ we define a set map

$$f_{u,v,w^*}(R)\colon\ \mathrm{GL}(A_R) \longrightarrow R$$

by

$$f_{u,v,w^*}(\eta) := f_{u,v,w^*}(R)(\eta) := \langle w^*_R, \eta(u_R v_R) - \eta(u_R)\eta(v_R)\rangle$$

for $\eta \in \mathrm{GL}(A_R)$. It follows immediately from Lemma 9.15 that these set maps vary functorially with R. Thus $f_{u,v,w^*} \in k[\mathbf{GL}(A)]$. Moreover, since the canonical pairing $A^* \times A \to k$ is regular, $\eta \in \mathrm{GL}(A_R)$ belongs to $\mathrm{Aut}(A_R)$ if and only if $f_{u,v,w^*}(\eta) = 0$ for all $u, v \in A$ and all $w^* \in A^*$. Hence we deduce from 24.15 that $\mathbf{Aut}(A)$ *is the closed subfunctor of* $\mathbf{GL}(A)$ *determined by the ideal* $I \subseteq k[\mathbf{GL}(A)]$ *generated by the quantities* f_{u,v,w^*}, $u, v \in A$, $w^* \in A^*$. In particular, assertion (∗) follows. Note that, since A and A^* are both finitely generated as k-modules, so is I as an ideal in $k[\mathbf{GL}(A)]$.

24.26 Example. In a similar vein, let $Q := (M, q)$ be a quadratic module over k. Then

$$\mathrm{O}(Q) := \mathrm{O}(M, q) := \{\eta \in \mathrm{GL}(M) \mid q \circ \eta = q\} \tag{1}$$

is a subgroup of $\mathrm{GL}(M)$, called the *orthogonal group* of Q. (This group was defined previously in Exc. 11.41.) It may be converted into a k-group functor by using Cor. 11.5 to define $\mathbf{O}(Q)(R) := \mathrm{O}(Q_R)$, $Q_R := (M_R, q_R)$, for all $R \in k\text{-}\mathbf{alg}$, and

$$\mathbf{O}(Q)(\varphi)\colon \mathbf{O}(Q)(R) \longrightarrow \mathbf{O}(Q)(S),\quad \mathrm{O}(Q_R) \ni \eta \longmapsto \eta_S \in \mathrm{O}(Q_S) \tag{2}$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**,where we employ the same identifications as in 24.25. If M is finitely generated projective, we let $(w_i)_{1\le i\le n}$ be a finite family of generators for M and define set maps

$$f_i(R), f_{ij}(R)\colon \mathrm{GL}(M_R) \longrightarrow R$$

for $1 \le i, j \le n$ and all $R \in k$-**alg** by setting

$$\begin{aligned} f_i(R)(\eta) &:= q_R(\eta(w_{iR})) - q_R(w_{iR}),\\ f_{ij}(R)(\eta) &:= q_R(\eta(w_{iR}), \eta(w_{jR})) - q_R(w_{iR}, w_{jR}) \end{aligned}$$

for $\eta \in \mathrm{GL}(M_R)$. These set maps vary functorially with R, hence define elements $f_i, f_{ij} \in k[\mathbf{GL}(M)]$, and writing $I \subseteq k[\mathbf{GL}(M)]$ for the ideal they generate, $\mathbf{O}(Q)$ is clearly the closed subfunctor of $\mathbf{GL}(M)$ determined by I. In particular, $\mathbf{O}(Q)$ *is a k-group scheme*, called the *orthogonal group scheme* of Q.

24.27 Base change. Let k' be a fixed commutative associative k-algebra with 1. Under restriction of scalars, every k'-algebra becomes a k-algebra, and every homomorphism of k'-algebras becomes one of k-algebras. In particular, k'-**alg** may be viewed canonically as a subcategory, though not a full one, of k-**alg**:

$$k'\text{-}\mathbf{alg} \subseteq k\text{-}\mathbf{alg}. \tag{1}$$

Restricting a k-functor $\mathbf{X}$ as defined in 24.1 to k'-**alg**, we obtain a k'-functor, denoted by $\mathbf{X}_{k'}$ and called the *base change* or *scalar extension* of $\mathbf{X}$ from k to k'. Similarly, restricting a morphism $f\colon \mathbf{X} \to \mathbf{Y}$ of k-functors to k'-**alg**, we obtain a k'-functor $f_{k'}\colon \mathbf{X}_{k'} \to \mathbf{Y}_{k'}$, called the *base change* or *scalar extension* of f from k to k'.

Most of our preceding constructions commute with base change. For instance, we have

$$(\mathbb{A}^n_k)_{k'} = \mathbb{A}^n_{k'} \tag{2}$$

for any positive integer n. If M is a k-module, then

$$(M_{\mathbf{a}})_{k'} = (M_{k'})_{\mathbf{a}} \tag{3}$$

under the identification (9.4.1) since $(M_{\mathbf{a}})_{k'}(R') = M \otimes R' = (M \otimes k') \otimes_{k'} R' = (M_{k'})_{R'} = (M_{k'})_{\mathbf{a}}(R')$ for all $R' \in k'$-**alg**, similarly for morphisms in k'-**alg**.

Let $R \in k$-**alg**. For $R' \in k'$-**alg**, (9.2.5) yields a bijection

$$\mathrm{can}_R(R')\colon \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, R') \xrightarrow{\sim} \mathrm{Hom}_{k'\text{-}\mathbf{alg}}(R_{k'}, R') \tag{4}$$

given by

$$\mathrm{can}_R(R')(\varrho)(r \otimes \alpha') = \alpha' \varrho(r) \tag{5}$$

for all $\varrho \in \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, R')$, $r \in R$, $\alpha' \in k'$, and this bijection depends functorially on R'. Thus we obtain an isomorphism

$$\mathrm{can}_R \colon (\mathbf{Spec}(R))_{k'} \xrightarrow{\sim} \mathbf{Spec}(R_{k'}). \tag{6}$$

Moreover, for a morphism $\varphi \colon R \to S$ in k-**alg**, one checks that the diagram

$$\begin{array}{ccc} (\mathbf{Spec}(S))_{k'} & \xrightarrow[\mathrm{can}_S]{\cong} & \mathbf{Spec}(S_{k'}) \\ {\scriptstyle (\mathbf{Spec}(\varphi))_{k'}}\downarrow & & \downarrow{\scriptstyle \mathbf{Spec}(\varphi_{k'})} \\ (\mathbf{Spec}(R))_{k'} & \xrightarrow[\mathrm{can}_R]{\cong} & \mathbf{Spec}(R_{k'}) \end{array} \tag{7}$$

commutes.

24.28 Regular functions under base change. We continue the discussion begun in 24.27. Let $\mathbf{X}$ be a k-functor. An element $f \in k[\mathbf{X}]$ by (24.6.2) is a morphism $f \colon \mathbf{X} \to \mathbb{A}^1_k$ of k-functors, hence gives rise to a morphism $f_{k'} \colon \mathbf{X}_{k'} \to (\mathbb{A}^1_k)_{k'} = \mathbb{A}^1_{k'}$ of k'-functors, and we conclude $f_{k'} \in k'[\mathbf{X}_{k'}]$. By (24.6.4), the map

$$k[\mathbf{X}] \longrightarrow k'[\mathbf{X}_{k'}], \quad f \longmapsto f_{k'}, \tag{1}$$

is a morphism in k-**alg** and thus gives rise to a morphism

$$\mathrm{can}_{\mathbf{X}} \colon k[\mathbf{X}]_{k'} \longrightarrow k'[\mathbf{X}_{k'}] \tag{2}$$

in k'-**alg** given by

$$\mathrm{can}_{\mathbf{X}}(f \otimes \alpha') = \alpha' f_{k'} \tag{3}$$

for $f \in k[\mathbf{X}]$ and $\alpha' \in k'$-**alg**. Consulting the morphisms $f_{\mathbf{X}}$ (resp. $f_{\mathbf{X}_{k'}}$) described in (24.10.2) it is now easily checked, using (24.27.5), (24.27.6) and (3), that the diagram

$$\begin{array}{ccc} \mathbf{X}_{k'} & \xrightarrow[f_{\mathbf{X}_{k'}}]{} & \mathbf{Spec}(k'[\mathbf{X}_{k'}]) \\ {\scriptstyle (f_{\mathbf{X}})_{k'}}\downarrow & & \downarrow{\scriptstyle \mathbf{Spec}(\mathrm{can}_{\mathbf{X}})} \\ (\mathbf{Spec}(k[\mathbf{X}]))_{k'} & \xrightarrow[\mathrm{can}_{k[\mathbf{X}]}]{\cong} & \mathbf{Spec}(k[\mathbf{X}]_{k'}) \end{array} \tag{4}$$

commutes. Now suppose $\mathbf{X}$ is an affine k-scheme. Since $(f_{\mathbf{X}})_{k'}$ and $f_{\mathbf{X}_{k'}}$ are both isomorphisms of k'-functors, by Prop. 24.10 (c), so is $\mathbf{Spec}(\mathrm{can}_{\mathbf{X}})$ by (4), and we conclude from Cor. 24.5 (b) that

$$\mathrm{can}_{\mathbf{X}} \colon k[\mathbf{X}]_{k'} \xrightarrow{\sim} k'[\mathbf{X}_{k'}]$$

is an isomorphism of k'-algebras.

Exercises

24.29. *Automorphisms of quadratic étale algebras, revisited.* Let D be a quadratic étale k-algebra. Verify that $\mathbf{Aut}(D)$ is the constant group scheme $\mathbb{Z}/2$. (*Hint*: Use Exercise 19.33.)

24.30. Let $\mathbf{G}$ be a k-group scheme endowed with homomorphisms $\rho_i\colon \mathbf{G} \to \mathbf{GL}(M_i)$ for i in some index set I, where each M_i is a finitely generated projective k-module. Pick $m_i \in M_i$ for each i and define a k-group functor $\mathbf{H}$ via

$$\mathbf{H}(R) := \{g \in \mathbf{G}(R) \mid \rho_i(g)m_i = m_i \text{ for all } i\}$$

for $R \in k$-**alg**. Verify that $\mathbf{H}$ is a closed subfunctor of $\mathbf{G}$, hence that $\mathbf{H}$ is a k-group scheme.

25 Étale, smooth and fppf algebras

Given a commutative ring k, remaining fixed throughout this section, and a prime ideal $\mathfrak{p} \subseteq k$, it follows immediately from Exc. 23.40 (a) that a composition algebra over k becomes split after extending scalars to the separable closure of $k(\mathfrak{p})$. Unfortunately, this observation is as obvious as it is useless. For example, the base change from k to *any* field in k-**alg** trivializes the linear algebra of k and thus destroys all the relevant information one could possibly have about this important ingredient.

In order to overcome this deficiency, it will be necessary to focus attention on special classes of scalar extension, the ones mentioned in the title of this section being the most appropriate in the present context. They will be discussed here in fairly great detail. In order to provide the reader with an intuitive understanding of the topics at hand, proofs are sometimes included. The presentation culminates in quoting and explaining a number of fundamental scheme-theoretic results due to Grothendieck [108].

25.1 Flat and faithfully flat modules. For every k-module N, the functor $- \otimes N\colon k$-**mod** $\to k$-**mod** is *right exact* [28, II.3, Prop. 5], meaning that whenever we are given an exact sequence

$$M' \xrightarrow[\varphi]{} M \xrightarrow[\psi]{} M'' \longrightarrow 0\ ,$$

of k-modules, the induced sequence

$$M' \otimes N \xrightarrow[\varphi\otimes\mathbf{1}_N]{} M \otimes N \xrightarrow[\psi\otimes\mathbf{1}_N]{} M'' \otimes N \longrightarrow 0$$

is also exact. We say that N is *flat* if the functor $- \otimes N$ is exact in the sense that it preserves exact sequences, equivalently, if for every injective k-linear map $\varphi\colon M' \to M$ of k-modules, the induced linear map $\varphi \otimes \mathbf{1}_N\colon M' \otimes N \to M \otimes N$ is also injective [27, I.2, Prop. 1]. For example, any localization of k is a flat k-module [27, II.2, Thm. 1].

Here is a typical application of the notion of flatness. Suppose M has no α-torsion for some $\alpha \in k$, i.e., multiplication by α is an injection $M \to M$. Then $M \otimes N$ also has no α-torsion for every flat k-module N.

We say N is *faithfully flat* provided a sequence of k-modules is exact if and only if it becomes so after tensoring with N. A projective k-module M is always flat, while it is faithfully flat if and only if has full support, i.e., $M_{\mathfrak{p}} \neq \{0\}$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$. In particular, if k is a field, then every non-zero k-module is faithfully flat.

25.2 (Faithful) flatness under base change. Let $k' \in k$-**alg** and suppose that N is a k-module.

(a) Generalizing iterated scalar extensions as in 9.4, and in slight modification of the identifications agreed upon in 12.27, we consider a k'-module M' and let k' act on $M' \otimes N = M' \otimes_k N$ through the first factor, making $M' \otimes N$ a module over k'. We then have a natural identification

$$M' \otimes_k N = M' \otimes_{k'} N_{k'} \tag{1}$$

of k'-modules such that

$$x' \otimes_k y = x' \otimes_{k'} y_{k'}, \quad x' \otimes_{k'} (y \otimes \alpha') = (\alpha' x') \otimes_k y \tag{2}$$

for $x' \in M'$, $y \in N$, $\alpha' \in k'$. Moreover, for a k'-linear map $\varphi'\colon M' \to M'_1$ of k'-modules and a k-linear map $\psi\colon N \to N_1$ of k-modules, we obtain

$$\varphi' \otimes_k \psi = \varphi' \otimes_{k'} \psi_{k'} \tag{3}$$

under this identification.

(b) Let

$$M'_1 \xrightarrow[\varphi'_1]{} M'_2 \xrightarrow[\varphi'_2]{} M'_3 \tag{4}$$

be a sequence of k'-modules. Since $\mathbf{1}_{N_{k'}} = (\mathbf{1}_N)_{k'}$, we may apply (a) to obtain a

commutative diagram

$$\begin{array}{ccccc} M'_1 \otimes_{k'} N_{k'} & \xrightarrow[\varphi'_1 \otimes_{k'} \mathbf{1}_{N_{k'}}]{} & M'_2 \otimes_{k'} N_{k'} & \xrightarrow[\varphi'_2 \otimes_{k'} \mathbf{1}_{N_{k'}}]{} & M'_3 \otimes_{k'} N_{k'} \\ \mathbf{1} \downarrow \cong & & \mathbf{1} \downarrow \cong & & \mathbf{1} \downarrow \cong \\ M'_1 \otimes_k N & \xrightarrow[\varphi'_1 \otimes_k \mathbf{1}_N]{} & M'_2 \otimes_k N & \xrightarrow[\varphi'_2 \otimes_k \mathbf{1}_N]{} & M'_3 \otimes N. \end{array} \tag{5}$$

Now suppose N is flat over k and assume (4) is exact. Then so is the bottom row of (5), hence also its top row, and we conclude that $N_{k'}$ is flat over k'. Moreover, if N is faithfully flat over k and the top row of (5) is exact, so is its bottom row, hence also (4). Thus $N_{k'}$ is faithfully flat over k'.

In summary: (*faithful*) *flatness is stable under base change.*

25.3 Flat and faithfully flat algebras. By a (*faithfully*) *flat k-algebra* we mean a unital commutative associative algebra over k, i.e., an object of k-**alg**, that is (faithfully) flat as a k-module.

We list two elementary but useful properties.

(i) If $R \in k$-**alg** and $S \in R$-**alg** are both (faithfully) flat, then so is $S \in k$-**alg**. This follows immediately from the definitions and our convention on iterated scalar extensions (9.4).

(ii) Let R be a flat k-algebra. If M is a k-module and $N \subseteq M$ is a k-submodule, then the inclusion $i\colon N \hookrightarrow M$ gives rise to an R-linear injection $i_R\colon N_R \to M_R$, which may and always will be used to identify $N_R \subseteq M_R$ as an R-submodule. Extending the short exact sequence $0 \to N \to M \to M/N \to 0$ from k to R, we obtain

$$(M/N)_R = M_R/N_R. \tag{1}$$

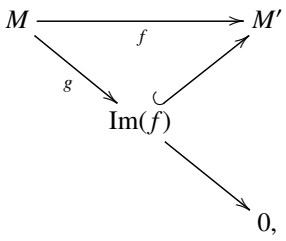
Similarly, given any k-linear map $f\colon M \to M'$ of k-modules and doing the same with

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow M \xrightarrow[f]{} M' \longrightarrow \mathrm{Coker}(f) \longrightarrow 0$$

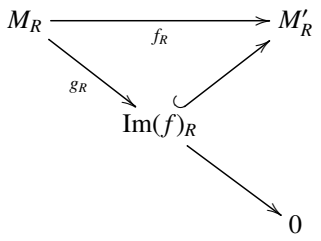
yields

$$\mathrm{Ker}(f_R) = \mathrm{Ker}(f)_R, \quad \mathrm{Coker}(f_R) = \mathrm{Coker}(f)_R. \tag{2}$$

Finally, the factorization



where $g\colon M \to \mathrm{Im}(f)$ is the unique k-linear map induced by f, gives rise to the commutative diagram



of R-modules, which shows

$$\mathrm{Im}(f_R) = \mathrm{Im}(f)_R. \tag{3}$$

25.4 Proposition. *For all $R \in k$-**alg**, the following conditions are equivalent.*

(i) *R is faithfully flat.*

(ii) *R is flat, and for all k-modules M, the linear map $\mathrm{can}_M := \mathrm{can}_{M,R}\colon M \to M_R$, $x \mapsto x_R$, is injective.*

(iii) *R is flat, and $M_R = \{0\}$ implies $M = \{0\}$, for all k-modules M.*

In particular, if R is faithfully flat, then the unit homomorphism $\vartheta\colon k \to R$ is injective.

Proof The final statement is (ii) for $M := k$.

(i) $\Rightarrow$ (ii). By definition, R is flat. Put $\varphi := \mathrm{can}_M$. By faithful flatness, it suffices to show that

$$\varphi_R\colon M \otimes R \longrightarrow (M \otimes R) \otimes R$$

is injective. But since it is easily checked that the k-linear map

$$\psi\colon (M \otimes R) \otimes R \longrightarrow M \otimes R, \quad (x \otimes r_1) \otimes r_2 \longmapsto x \otimes (r_1 r_2),$$

satisfies $\psi \circ \varphi_R = \mathbf{1}_{M\otimes R}$, the assertion follows.

(ii) $\Rightarrow$ (iii). Obvious.

(iii) ⇒ (i). Let

$$\begin{array}{ccccc} M' & \xrightarrow[\varphi]{} & M & \xrightarrow[\psi]{} & M'' \\ \downarrow & & \downarrow & & \downarrow \\ M'_R & \xrightarrow[\varphi_R]{} & M_R & \xrightarrow[\psi_R]{} & M''_R \end{array} \tag{1}$$

be a commutative diagram, with the top row being given as any sequence in k-**mod**, and the bottom row assumed to be exact. We must show that the top row is exact as well. The k-linear map $f := \psi \circ \varphi \colon M' \to M''$ satisfies $f_R = 0$, hence by (25.3.3) $\operatorname{Im}(f)_R = \operatorname{Im}(f_R) = \{0\}$ and then $f = 0$ by (iii). Thus $\operatorname{Im}(\varphi) \subseteq \operatorname{Ker}(\psi)$. On the other hand, (25.3.2), (25.3.3) and exactness of the bottom row imply $\operatorname{Im}(\varphi)_R = \operatorname{Im}(\varphi_R) = \operatorname{Ker}(\psi_R) = \operatorname{Ker}(\psi)_R$. From (25.3.1) we therefore deduce $(\operatorname{Ker}(\psi)/\operatorname{Im}(\varphi))_R = \{0\}$, and (iii) again shows $\operatorname{Im}(\varphi) = \operatorname{Ker}(\psi)$, as claimed. □

25.5 Remark. Here are some other examples of results concerning faithfully flat k-algebras. Suppose M is a k-module.

(i) Suppose $R \in k$-**alg** is faithfully flat. *If M_R is (a) finitely generated, (b) finitely presented or (c) projective, then M is also.* See [27, I.3, Prop. 11], [158, p. 13, Lemme I.3.6], or [271, Tags 03C4, 05A9].

(ii) *If M is finitely generated projective of constant rank, then there is a faithfully flat $R \in k$-**alg** such that M_R is a free R-module.* This is Exc. 8 in [27, II.5]. To see this, note that there are $f_1, \dots, f_n \in k$ for some n that generate k as a k-module and such that $M_{k_{f_i}}$ is a free k_{f_i}-module for all i (9.8 (iv)), all of the same finite rank. Take $R := k_{f_1} \times \cdots \times k_{f_n}$ and note that M_R is a free R-module because of the constant rank hypothesis. Moreover, R is faithfully flat by [27, II.5, Prop. 3] .

We can strengthen property (ii) slightly: *If $M_1, \dots, M_n$ are finitely generated projective k-modules, each of constant rank, then there is a faithfully flat $R \in k$-**alg** such that $(M_i)_R$ is a free R-module for all i.* One can see this by induction from (ii) leveraging that faithfully flat over faithfully flat is faithfully flat, or by repeating the proof of (ii).

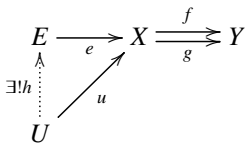
Leveraging these results, the following is proved in [95, Lemma 3.3]:

(iii) Let M and N be finitely generated projective k-modules and suppose $R \in k$-**alg** is flat. Writing $\operatorname{Pol}^d_k(M, N)$ for the k-module of polynomial laws $M \to N$ that are homogeneous of degree $d \in \mathbb{N}$, *the natural map*

$$\operatorname{Pol}^d_k(M, N) \otimes R \to \operatorname{Pol}^d_R(M_R, N_R)$$

is an isomorphism.

25.6 Equalizers. Let **C** be a category. By an *equalizer* of morphisms $f, g\colon X \to Y$ in **C** we mean a morphism $e\colon E \to X$ in **C** such that $f \circ e = g \circ e$ and, for any morphism $u\colon U \to X$ in **C** such that $f \circ u = g \circ u$, there is a unique morphism $h\colon U \to E$ in **C** such that the diagram



commutes. Clearly, if an equalizer exists, it is unique up to a unique isomorphism. For more details on this concept, see D. Pumplün [240, 4.2].

It is sometimes important to realize the linear map can_M in condition (ii) of Prop. 25.4 as an equalizer. To this end, we consider an arbitrary $R \in k$-**alg** and two morphisms

$$d^i = d^i_R\colon R \longrightarrow S := R \otimes R \qquad (i = 0, 1) \tag{1}$$

in k-**alg** defined by

$$d^0(r) := 1_R \otimes r, \quad d^1(r) := r \otimes 1_R \qquad (r \in R). \tag{2}$$

Given a k-module M, we also put

$$d^i_M := d^i_{R,M} := \mathbf{1}_M \otimes d^i\colon M_R \longrightarrow M_S\,. \tag{3}$$

25.7 Proposition. *Let M be a k-module and suppose $R \in k$-**alg** is faithfully flat. With the notation of 25.6, the sequence*

$$0 \longrightarrow M \xrightarrow[\mathrm{can}_M]{} M_R \underset{d^1_M}{\overset{d^0_M}{\rightrightarrows}} M_S \tag{1}$$

*is exact. Moreover, the natural map $\mathrm{can}_M\colon M \to M_R$ is an equalizer of d^0_M, d^1_M in the category k-**mod**.*

Proof The final statement follows immediately from the exactness of (1). By faithful flatness of R, it therefore suffices to show that

$$0 \longrightarrow M \otimes R \xrightarrow[\mathrm{can}_M \otimes \mathbf{1}_R]{} M_R \otimes R \xrightarrow[d \otimes \mathbf{1}_R]{} M_S \otimes R \tag{2}$$

is exact, where $d := d^1_M - d^0_M$. Since can_M is injective by Proposition 25.4, so is $\mathrm{can}_M \otimes \mathbf{1}_R$ by flatness of R, and we have exactness of (2) at $M \otimes R$. Since, obviously, $d \circ \mathrm{can}_M = 0$, we conclude $(d \otimes \mathbf{1}_R) \circ (\mathrm{can}_M \otimes \mathbf{1}_R) = (d \circ \mathrm{can}_M) \otimes \mathbf{1}_R = 0$, hence $\mathrm{Im}(\mathrm{can}_M \otimes \mathbf{1}_R) \subseteq \mathrm{Ker}(d \otimes \mathbf{1}_R)$, and exactness of (2) at $M_R \otimes R$ will follow

once we have shown the reverse inclusion. For this purpose, we define a k-linear map $\varphi\colon M_S \otimes R \to M_R \otimes R$ by

$$\varphi\Big((x \otimes (r_1 \otimes r_2)) \otimes r_3\Big) := (x \otimes r_1) \otimes (r_2 r_3)$$

for all $x \in M$ and all $r_1, r_2, r_3 \in R$. A straightforward verification shows

$$\varphi \circ (d_M^1 \otimes \mathbf{1}_R) = \mathbf{1}_{M_R \otimes R}, \quad \operatorname{Im}\big(\varphi \circ (d_M^0 \otimes \mathbf{1}_R)\big) \subseteq \operatorname{Im}(\operatorname{can}_M \otimes \mathbf{1}_R).$$

For $z \in \operatorname{Ker}(d \otimes \mathbf{1}_R)$, we therefore conclude $z = \varphi((d_M^1 \otimes \mathbf{1}_R)(z)) = \varphi((d_M^0 \otimes \mathbf{1}_R)(z)) \in \operatorname{Im}(\operatorname{can}_M \otimes \mathbf{1}_R)$, which completes the proof. □

25.8 Proposition. *Let $R \in k$-**alg** and $\mathfrak{p} \in \operatorname{Spec}(k)$. Writing $\vartheta_R\colon k \to R$ for the unit homomorphism corresponding to R as in 24.9, $\overline{k(\mathfrak{p})}$ for the algebraic closure of the field $k(\mathfrak{p})$ and setting $\mathbf{X} := \mathbf{Spec}(R)$ as an affine k-scheme, we consider the following conditions on R and $\mathfrak{p}$.*

(i) $\operatorname{Spec}(\vartheta_R)^{-1}(\mathfrak{p}) \neq \emptyset$.
(ii) $R \otimes k(\mathfrak{p}) \neq \{0\}$.
(iii) $\mathbf{X}(\overline{k(\mathfrak{p})}) \neq \emptyset$.

Then the implications

$$\textit{(i)} \iff \textit{(ii)} \impliedby \textit{(iii)} \tag{1}$$

hold. Moreover, if R is finitely generated as a k-algebra, then all three conditions are equivalent.

Proof Put $K := \overline{k(\mathfrak{p})}$.

(i) ⇔ (ii). Exc. 9.27.

(iii) ⇒ (ii). If $\mathbf{X}(K) \neq \emptyset$, then there exists a morphism $R \to K$ in k-**alg**, which in turn induces a unital homomorphism $R \otimes k(\mathfrak{p}) \to K$ of $k(\mathfrak{p})$-algebras. Hence (ii) holds.

We have thus shown (1). Assuming that R is finitely generated as a k-algebra, it remains to verify the implication (ii) ⇒ (iii). If (ii) holds, then $R \otimes k(\mathfrak{p})$ is a non-zero finitely generated $k(\mathfrak{p})$-algebra. By [27, V.3, Prop. 1], therefore, we find a morphism $R \otimes k(\mathfrak{p}) \to K$ in $k(\mathfrak{p})$-**alg**. Composing with the natural map $R \to R \otimes k(\mathfrak{p})$ yields an element of $\mathbf{X}(K)$. Hence (iii) holds. □

25.9 Proposition. *For a flat k-algebra R, the following conditions are equivalent.*

(i) *R is faithfully flat.*
(ii) *$R \otimes k(\mathfrak{p}) \neq \{0\}$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$.*
(iii) *The natural map $\operatorname{Spec}(R) \to \operatorname{Spec}(k)$ induced by the unit homomorphism $k \to R$ is surjective.*

(iv) $\mathfrak{m}R \neq R$ *for all maximal ideals* $\mathfrak{m} \subseteq k$.

Proof (i) ⇒ (ii). Apply Prop. 25.4.

(ii) ⇒ (iii). Apply Prop. 25.8.

(iii) ⇒ (iv). By (ii), some prime ideal $\mathfrak{q} \subseteq R$ lies above $\mathfrak{m}$. Hence $\mathfrak{m}R \subseteq \mathfrak{q} \subset R$.

(iv) ⇒ (i). By Prop. 25.4 we have to show $M_R \neq \{0\}$ for all k-modules $M \neq \{0\}$. Let $0 \neq x \in M$ and $I := \{\alpha \in k \mid \alpha x = 0\} \subset k$. Then $kx \cong k/I$ as k-modules, so we have an exact sequence $0 \to k/I \to M$. Since R is flat, this implies that the sequence $0 \to (k/I) \otimes R = R/IR \to M_R$ is also exact. Let $\mathfrak{m} \subseteq k$ be a maximal ideal in k containing I. Then $IR \subseteq \mathfrak{m}R \subset R$ by (iv), which implies $R/IR \neq \{0\}$ and then $M_R \neq \{0\}$. □

25.10 Remark. Condition (iii) in the proposition says that R is a cover of k in the sense of Exc. 9.26. By the equivalence of (i) and (iii), therefore, $R \in k$-**alg** is faithfully flat if and only if it is a flat cover of k. As an illustration, for any maximal ideal $\mathfrak{m}$ of k, the localization $k_{\mathfrak{m}}$ is a flat k-algebra which is a flat cover of k if and only if k is a local ring.

25.11 Convention. It is sometimes convenient to use notions originally defined for unital commutative associative k-algebras also for affine k-schemes and vice versa. This convention is justified by the anti-equivalence of these categories established in Cor. 24.11. For example, an affine k-scheme $\mathbf{X}$ is (faithfully) flat if and only if $k[\mathbf{X}] \in k$-**alg** has this property. In particular, the affine k-schemes $\mathbf{G_a}$, $\mathbf{G_m}$, $\mathbb{A}^n_k$ are faithfully flat. Moreover, if M is a projective k-module of finite type, then so is M^*, forcing $S(M^*)$ to be projective as well [28, III.6, Cor. of Thm. 1], and we conclude that the affine k-scheme $M_{\mathbf{a}}$ is flat.

25.12 Geometric fibers. For an affine k-scheme $\mathbf{X}$, the sets $\mathbf{X}(K)$, where K varies over the algebraically closed fields in k-**alg**, are called the *geometric fibers* of $\mathbf{X}$. In particular, if k is a field and $\mathbf{X}$ is of finite type in the sense that $k[\mathbf{X}]$ is a finitely generated k-algebra, then $\mathbf{X}$ has non-empty geometric fibers if and only if $k[\mathbf{X}]$ is not the zero ring. (This is one formulation of the Nullstellensatz as in [27, V.3, Prop. 1] or [271, Tag 00FV].)

25.13 Corollary. *Consider the following conditions, for any affine k-scheme* $\mathbf{X}$.

(i) $\mathbf{X}$ *is flat and has non-empty geometric fibers.*

(ii) $\mathbf{X}$ *is faithfully flat.*

Then (i) implies (ii), and both conditions are equivalent if $k[\mathbf{X}]$ *is finitely generated as a* k*-algebra.*

Proof If condition (i) holds, so does condition (iii) of Prop. 25.8, for $R := k[\mathbf{X}]$ and any $\mathfrak{p} \in \operatorname{Spec}(k)$, and then also condition (ii). Hence that proposition combined with Prop. 25.9 shows that $\mathbf{X}$ is faithfully flat. Conversely, suppose $\mathbf{X}$ is faithfully flat and R is finitely generated as a k-algebra. If $K \in k$-**alg** is an algebraically closed field, the kernel of the unit homomorphism $\vartheta_K : k \to K$ is some prime ideal $\mathfrak{p} \in \operatorname{Spec}(k)$, making K a $k(\mathfrak{p})$-algebra in a natural way. Hence the unit homomorphism ϑ_K factors uniquely through the unit homomorphism

$$\vartheta_L : k \longrightarrow L, \quad L := \overline{k(\mathfrak{p})}.$$

On the other hand, since $\operatorname{Spec}(\vartheta_R) : \operatorname{Spec}(R) \to \operatorname{Spec}(k)$ is surjective by Proposition 25.9, we have $\mathbf{X}(L) \neq \emptyset$ by Prop. 25.8. Therefore $\mathbf{X}(K) \neq \emptyset$, and $\mathbf{X}$ has non-empty geometric fibers. □

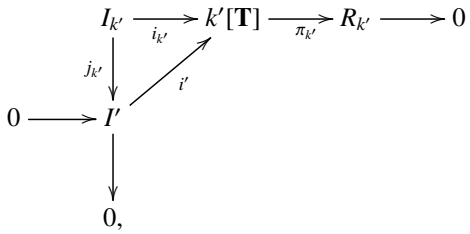
The property of an algebra to be finitely generated, which shows up as an important ingredient of Prop. 25.8, is sometimes not enough for the intended applications and has to be replaced by the following refinement.

25.14 Finitely presented k-algebras. By a *presentation* of a k-algebra $R \in k$-**alg**, we mean a short exact sequence

$$0 \longrightarrow I \xrightarrow[i]{} k[\mathbf{T}] \xrightarrow[\pi]{} R \longrightarrow 0, \tag{1}$$

where $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ is a finite chain of independent indeterminates, π is a morphism in k-**alg** and $I \subseteq k[\mathbf{T}]$ is an ideal. For a presentation of R to exist it is necessary and sufficient that R be finitely generated as a k-algebra. The presentation (1) of R is said to be *finite* if the ideal $I \subseteq k[\mathbf{T}]$ is finitely generated. We say a k-algebra R (the condition $R \in k$-**alg** being understood) is *finitely presented* if a finite presentation of R exists. If k is noetherian (e.g., if k is a field), then the property of being finitely presented is equivalent to being finitely generated by Hilbert's Basis Theorem.

25.15 Properties of finitely presented algebras. (a) The property of a k-algebra to be finitely presented is stable under base change. Indeed, tensoring (25.14.1) with any $k' \in k$-**alg**, we obtain a commutative diagram



where $I' := i_{k'}(I_{k'}) \subseteq k'[\mathbf{T}]$ and $j_{k'}$ is induced by $i_{k'}$. Since this diagram is

everywhere exact and $I' \subseteq k'[\mathbf{T}]$ is obviously a finitely generated ideal if $I \subseteq k[\mathbf{T}]$ is, the assertion follows.

(b) If $R \in k$-**alg** and $S \in R$-**alg** are both finitely presented, then so is $S \in k$-**alg**, see [108, 1.4, p. 230] or [271, Tag 00F4].

25.16 Proposition. *Every presentation of a finitely presented k-algebra is finite.*

Proof Let $R \in k$-**alg** be finitely presented and let

$$0 \longrightarrow I \longrightarrow k[\mathbf{T}] \xrightarrow[\pi]{} R \longrightarrow 0 \tag{1}$$

be any presentation of R as in (25.14.1). By hypothesis, there exists a finite presentation

$$0 \longrightarrow J \longrightarrow k[\mathbf{S}] \xrightarrow[\mu]{} R \longrightarrow 0 \tag{2}$$

of R, so $J \subseteq k[\mathbf{S}]$ is a finitely generated ideal. We must show that $I \subseteq k[\mathbf{T}]$ is a finitely generated ideal as well. Writing $\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_m)$, $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$, the quantities $\pi(\mathbf{t}_j) \in R$ by (2) have a lift under μ to polynomials $g_j \in k[\mathbf{S}]$. Thus

$$\mu(g_j) = \pi(\mathbf{t}_j) \qquad\qquad (1 \le j \le n). \tag{3}$$

The morphism

$$\varphi\colon k[\mathbf{S},\mathbf{T}] = k(\mathbf{S}) \otimes k[\mathbf{T}] \xrightarrow[\mu\otimes\pi]{} R \otimes R \xrightarrow[\mathrm{mult_R}]{} R \tag{4}$$

is surjective satisfying, in obvious notation,

$$\varphi(\mathbf{S}) = \mu(\mathbf{S}), \quad \varphi(\mathbf{T}) = \pi(\mathbf{T}). \tag{5}$$

We now claim

$$\mathrm{Ker}(\varphi) = J + \sum_{j=1}^{n} k[\mathbf{S},\mathbf{T}](\mathbf{t}_j - g_j). \tag{6}$$

Consulting (2), (3), (5), we see that the right-hand side is contained in the left. Conversely, let $f \in \mathrm{Ker}(\varphi)$, write $g := (g_1, \ldots, g_n) \in k[\mathbf{S}]^n$ and regard f as a polynomial $h(\mathbf{T}) \in k[\mathbf{S}][\mathbf{T}]$. Then (5), (3), (2) imply

$$h(g(\mathbf{S})) = f(\mathbf{S}, g(\mathbf{S})) \in J, \tag{7}$$

while the Taylor expansion (cf. (12.15.3)) yields

$$h(\mathbf{T}) = h(g(\mathbf{S}) + \mathbf{T} - g(\mathbf{S})) = h(g(\mathbf{S})) + \sum_{r\ge 1} (D^r h)(g(\mathbf{S}), \mathbf{T} - g(\mathbf{S})),$$

where the first summand on the right by (7) belongs to J. On the other hand,

$(D^r h)(g(\mathbf{S}), \mathbf{T})$ for $r \geq 1$ is homogeneous of degree r in $\mathbf{T}$ and thus belongs to the ideal in $k[\mathbf{S}, \mathbf{T}]$ generated by $\mathbf{t}_1, \ldots, \mathbf{t}_n$. We therefore conclude

$$(D^r h)(g(\mathbf{S}), \mathbf{T} - g(\mathbf{S})) \in \sum_{j=1}^{n} k[\mathbf{S}, \mathbf{T}](\mathbf{t}_j - g_j),$$

which completes the proof of (6). Now let $h_i \in k[\mathbf{T}]$ for $1 \leq i \leq m$ be lifts of $\mu(\mathbf{s}_i)$ under π, so

$$\pi(h_i) = \mu(\mathbf{s}_i) \qquad (1 \leq i \leq m). \tag{8}$$

Setting $h := (h_1, \ldots, h_m) \in k[\mathbf{T}]^m$, we consider the surjective homomorphism

$$\psi \colon k[\mathbf{S}, \mathbf{T}] \to k[\mathbf{T}]$$

of unital k-algebras given by

$$\psi(\mathbf{S}) = h, \quad \psi(\mathbf{T}) = \mathbf{T}. \tag{9}$$

Since $\mathrm{Ker}(\varphi) \subseteq k[\mathbf{S}, \mathbf{T}]$ is a finitely generated ideal by (6), the proof will be complete once we have shown

$$\psi(\mathrm{Ker}(\varphi)) = I. \tag{10}$$

By (2), (3), (6), (8), (9), the left-hand side is clearly contained in the right. Conversely, let $f(\mathbf{T}) \in I$. Then (1), (3) show $f(g(\mathbf{S})) \in J$, hence

$$\begin{aligned} f(\mathbf{T}) &= f(g(\mathbf{S}) + \mathbf{T} - g(\mathbf{S})) = f(g(\mathbf{S})) + \sum_{r \geq 1} (D^r f)(g(\mathbf{S}), \mathbf{T} - g(\mathbf{S})) \\ &\in J + \sum_{r \geq 1} k[\mathbf{S}, \mathbf{T}](\mathbf{t}_j - g_j). \end{aligned}$$

Now (6) implies $f(\mathbf{T}) \in \mathrm{Ker}(\varphi) \cap k[\mathbf{T}]$, and from (9) we deduce $f(\mathbf{T}) = \psi(f(\mathbf{T})) \in \psi(\mathrm{Ker}(\varphi))$, which completes the proof of (10). □

25.17 Corollary. *Let $R, k' \in k$-**alg** and suppose k' is faithfully flat. If $R_{k'}$ is finitely generated* (*resp. finitely presented*) *over k', then so is R over k.*

Proof Assume first that $R_{k'}$ is finitely generated over k'. Then there exists an exact sequence

$$k'[\mathbf{T}'] \xrightarrow[\pi']{} R_{k'} \longrightarrow 0 \tag{1}$$

in k'-**alg** with $\mathbf{T}' = (\mathbf{t}'_1, \ldots, \mathbf{t}'_n)$, and the quantities $\pi'(\mathbf{t}'_j) \in R_{k'}$ for $1 \leq j \leq n$ may be written as

$$\pi'(\mathbf{t}'_j) = \sum_{i=1}^{m} r_{ij} \otimes \alpha'_{ij}, \quad r_{ij} \in R, \alpha'_{ij} \in k' \qquad (1 \leq i \leq m, \ \ 1 \leq j \leq n). \tag{2}$$

Let $\mathbf{T} = (\mathbf{t}_{ij})_{1\le i\le m, 1\le j\le n}$ be a collection of independent indeterminates and $\pi\colon k[\mathbf{T}] \to R$ be the morphism in k-**alg** given by $\pi(\mathbf{t}_{ij}) = r_{ij}$ for $1 \le i \le m$, $1 \le j \le n$. Since the $\pi'(\mathbf{t}'_j)$, $1 \le j \le n$, generate $R_{k'}$ as a k'-algebra, so do the $(r_{ij})_{k'}$, $1 \le i \le m$, $1 \le j \le n$, by (2). Thus the sequence

$$k[\mathbf{T}] \xrightarrow[\pi]{} R \longrightarrow 0 \tag{3}$$

in k-**alg** becomes exact after tensoring with k', hence must have been so all along since k' is faithfully flat over k. Thus it follows from the exactness of (3) that R is a finitely generated k-algebra.

Now suppose $R_{k'}$ is finitely presented over k'. By what we have just seen, R is finitely generated over k, so we have a presentation

$$0 \longrightarrow I \longrightarrow k[\mathbf{T}] \xrightarrow[\pi]{} R \longrightarrow 0 \tag{4}$$

of R as in (25.14.1). By faithful flatness of k', the extended sequence

$$0 \longrightarrow I \otimes k' \longrightarrow k'[\mathbf{T}] \xrightarrow[\pi_{k'}]{} R_{k'} \longrightarrow 0$$

continues to be exact. By Prop. 25.16, therefore, $I \otimes k' \subseteq k'[\mathbf{T}]$ is a finitely generated ideal, i.e., a finitely generated $k'[\mathbf{T}]$-module. On the other hand, from (25.2.1) we deduce $I \otimes k' = I \otimes_{k[\mathbf{T}]} k'[\mathbf{T}]$ as $k'[\mathbf{T}]$-modules, and by 25.2 (b) $k'[\mathbf{T}] = k' \otimes k[\mathbf{T}]$ is a faithfully flat $k[\mathbf{T}]$-algebra. Applying 25.5 (i), we conclude that $I \subseteq k[\mathbf{T}]$ is a finitely generated ideal. Hence R is finitely presented as a k-algebra. □

25.18 Étale k-algebras. The notion of a finite étale algebra as defined in 19.19 will now be generalized as follows. A k-algebra R is said to be *étale* if it is finitely presented and satisfies one of the following equivalent conditions (see [108, (17.1.1), (17.3.1), (17.6.2)], applied to the structure morphism $\mathbf{Spec}(R) \to \mathbf{Spec}(k)$ of 24.9, and apply Exc. 8.14)

(i) For all $k' \in k$-**alg** and all ideals $I' \subseteq k'$ satisfying $I'^2 = \{0\}$, the set map

$$\mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, k') \xrightarrow[\mathrm{Hom}_{k\text{-}\mathbf{alg}}(R,\pi)]{} \mathrm{Hom}_{k\text{-}\mathbf{alg}}(R, k'/I')$$

induced by the projection $\pi\colon k' \to k'/I'$ is bijective.

(ii) R is flat over k, and for all $\mathfrak{p} \in \mathrm{Spec}(k)$, the extended algebra $R(\mathfrak{p}) = R \otimes k(\mathfrak{p})$ over the field $k(\mathfrak{p})$ is a finite direct product of finite separable extension fields of $k(\mathfrak{p})$.

In accordance with convention 25.11, an affine k-scheme $\mathbf{X}$ is said to be *étale* if $k[\mathbf{X}]$ is an étale k-algebra.

If R is an étale k-algebra that is finite in the sense of 11.23, then [271, Tag

0564] and [27, II.5, Cor. 2] imply that R is a projective k-module. In particular, R is a finite étale algebra in the sense of 19.19.

25.19 Examples of étale algebras. (i) For all $r \in \mathbb{N}$, a product of r copies of k is an étale k-algebra, known as the *split étale k-algebra of rank r*. (This is the same as the algebra E_Γ defined in Example 24.20, where Γ is a set with r elements.)

(ii) The zero ring is an étale k-algebra.

(iii) For each $f \in k$, the localization k_f is an étale k-algebra.

(iv) If R and S are étale k algebras, then so is $R \times S$.

(v) If R is an étale k-algebra and S is an étale R-algebra, then S is an étale k-algebra [108, Prop. 17.3.3(ii)].

(vi) By Prop. 25.9, an étale k-algebra R is faithfully flat if and only if the function $\operatorname{Spec}(R) \to \operatorname{Spec}(k)$ is surjective. When these equivalent conditions hold, we say that R is an *étale cover* of k.

(vii) If R is an étale k-algebra that is finite in the sense of 11.23 (i.e., R is a finite étale algebra) and $R \supseteq k$, then R is an étale cover of k.

(viii) If R is a smooth k-algebra (in the sense of 25.20) that is finite in the sense of 11.23, then R is an étale k-algebra by [108, 17.6.2].

(ix) Let K be a number field and put O_K for its ring of integers. Consider $k := O_K[1/n]$ for some nonzero $n \in O_K$, and let R be the integral closure of k in a finite extension L of K. (Note that $R = O_L[1/n]$ by [27, V.1, Prop. 16].) We leverage some facts from commutative algebra to give conditions for R to be an étale cover of k.

First, O_K is a Dedekind domain, hence so also are k and R and in particular they are integrally closed. It follows by [271, Tag 032L] that R is a finitely generated k-module and, since k is noetherian, it is clear from the definition that R is finitely presented. It is also torsion free as a module over the Dedekind domain k, so it is projective hence flat [27, VII.4, Prop. 22]. And the map $\operatorname{Spec} R \to \operatorname{Spec} k$ is surjective because R is the integral closure of k, so we have shown that R is a faithfully flat k-algebra.

To check whether R is étale, we use condition 25.18(ii). For $\mathfrak{p} = 0$, $k(\mathfrak{p}) = K$ and $R \otimes k(\mathfrak{p}) = L$, a finite separable field extension. For a nonzero prime $\mathfrak{p} \in \operatorname{Spec} k$, we write $R\mathfrak{p} = \prod \mathfrak{q}_i^{e(i)}$ where the $\mathfrak{q}_i$ are distinct prime ideals in R and each $e(i) \geq 1$. By the Chinese Remainder Theorem, $R \otimes k(\mathfrak{p}) \cong \prod R/\mathfrak{q}_i^{e(i)}$. If $e(i) > 1$, then $R/\mathfrak{q}_i^{e(i)}$ is not a field; if $e(i) = 1$, then it is a finite extension of the finite field $k/\mathfrak{p}$ and so is separable. We conclude that R is étale over k (in

which case it is an étale cover) if and only if every prime of K that ramifies in L divides n.

25.20 Smooth affine schemes. Since the original definition of smoothness as given in [61, I, 4.1] is rather technical, although more akin to what one expects from the study of classical algebraic varieties or differentiable manifolds, we prefer to recall the one of [108, (17.1.1), (17.3.1)] (see also the characterization in [61, I, 4.6]) because it is more easily accessible in the present context. Accordingly, an affine k-scheme $\mathbf{X}$ is said to be *smooth* if $\mathbf{X}$ is finitely presented and, for all $R \in k$-**alg** and all ideals $I \subseteq R$ having $I^2 = \{0\}$, the set map $\mathbf{X}(R) \to \mathbf{X}(R/I)$ induced by the projection from R to R/I is surjective.

25.21 Properties of smooth affine schemes. (a) *Smoothness is stable under base change* [108, (17.3.3) (iii)]: if $\mathbf{X}$ is a smooth affine k-scheme, then $\mathbf{X}_R$ is a smooth affine R-scheme, for all $R \in k$-**alg**.

(b) *Smoothness is transitive* [108, (17.3.3) (ii)]: Keeping in mind Convention 25.11, assume $R \in k$-**alg** and $S \in R$-**alg** are both smooth, then so is $S \in k$-**alg**.

(c) *Smooth affine schemes are flat* [108, (17.5.2)].

(d) *Étale affine schemes are smooth* because if $\mathbf{X}$ is an étale affine k-scheme, then the set maps of 25.18 (i) with $R = k[\mathbf{X}]$ are bijective while the same maps for smooth affine k-schemes are only required to be surjective.

(e) *Smooth affine schemes satisfy the separable Nullstellensatz*, see [271, Tag 056U]: Suppose $\mathbf{X}$ is a smooth affine k-scheme and k is a field. Then the set

$$\{\text{closed } x \in \mathbf{X} \mid k(x) \text{ is a finite separable extension of } k\}$$

is dense in $\mathbf{X}$. In particular, if $\mathbf{X}$ is smooth and K is a separably closed field, then $\mathbf{X}(K) \neq \emptyset$ if and only if $k[\mathbf{X}]$ is not the zero ring.

25.22 Remark. For (M, q) a non-degenerate quadratic module over k, the group scheme $\mathbf{O}(q)$ defined in 24.26 is smooth if n is even, or if n is odd and $2 \in k^\times$, see Exc. 26.12, [53, Thm. C.1.5], or [61, III.5.2.3 and II.5.2.7].

Within the framework of the present investigation, smooth affine schemes mostly arise in conjunction with two other important properties that we have encountered before and that are usually combined in the following concept.

25.23 Fppf schemes. An affine k-scheme is said to be *fppf* ("fidèlement plat et de présentation finie") if it is faithfully flat and finitely presented. For example, when k is a field, $\mathbf{X}$ is fppf if and only if $k[\mathbf{X}]$ is a finitely generated k-algebra that is not zero.

A first glimpse at the connection between this notion and smoothness may be read off from the following result.

25.24 Proposition. *Smooth affine k-schemes that have non-empty geometric fibers are fppf.*

Proof If $\mathbf{X}$ is such a scheme, then $\mathbf{X}$ is flat (25.21 (c)), and having non-empty geometric fibers implies that $\mathbf{X}$ is faithfully flat (Cor. 25.13). Being finitely presented by definition, it is in fact fppf. □

25.25 Properties of affine fppf schemes. Given an affine k-scheme $\mathbf{X}$, the following statements hold.

(i) *If $\mathbf{X}$ is fppf, then there exists an fppf $R \in k$-**alg** such that $\mathbf{X}(R) \neq \emptyset$.* Indeed, $R := k[\mathbf{X}] \in \mathbf{k}$-**alg** is fppf and $\mathbf{X}(R) = \mathrm{Hom}_{k\text{-}\mathbf{alg}}(k[\mathbf{X}], R)$ contains $\mathbf{1}_{k[\mathbf{X}]}$. (One can arrange for R to be quasi-finite, see [110, (17.16.2)].)

(ii) *If $\mathbf{X}$ is fppf and smooth, then there exists an étale cover $R \in k$-**alg** such that $\mathbf{X}(R) \neq \emptyset$* by [110, (17.16.3)(ii)].

(iii) *If $R \in k$-**alg** is faithfully flat, then for $\mathbf{X}$ to be smooth over k it is necessary and sufficient that the base change*

$$\mathbf{X}_R \cong \mathbf{Spec}(k[\mathbf{X}]_R) \in R\text{-}\mathbf{aff}$$

be smooth over R by [110, (17.7.3)(ii)] and 24.28.

25.26 Torsors. Let $\mathbf{X}$ be an affine k-scheme and $\mathbf{G}$ a k-group scheme acting on $\mathbf{X}$ from the right, so we have a morphism $\mathbf{X} \times \mathbf{G} \to \mathbf{X}$ of k-functors such that, for all $R \in k$-**alg**,

$$\mathbf{X}(R) \times \mathbf{G}(R) \longrightarrow \mathbf{X}(R), \quad (x, g) \longmapsto xg,$$

is a group action in the usual sense depending functorially on R. Note that $\mathbf{X}(R)$ may well be empty! We say $\mathbf{X}$ is a *torsor in the flat topology with structure group* $\mathbf{G}$ if

(i) the action of $\mathbf{G}$ on $\mathbf{X}$ is simply transitive, i.e., for all $R \in k$-**alg** and all $x, y \in \mathbf{X}(R)$, there is a unique $g \in \mathbf{G}(R)$ satisfying $y = xg$.

(ii) There exists an fppf $S \in k$-**alg** such that $\mathbf{X}(S) \neq \emptyset$

In this case, fixing S as in (ii), we may apply (i) to obtain an isomorphism $\mathbf{X}_S \xrightarrow{\sim} \mathbf{G}_S$ of affine S-schemes, allowing us to conclude from 25.25 (iii) that, e.g., $\mathbf{X}$ is smooth if and only if $\mathbf{G}$ is.

Finally, if instead of (ii), we even have

(iii) there exists an étale cover $S \in k$-**alg** having $\mathbf{X}(S) \neq \emptyset$,

then $\mathbf{X}$ is called a *torsor* (*with structure group* $\mathbf{G}$) *in the étale topology.*

Evidently, if $\mathbf{X}$ is a torsor in the étale topology, then it is a torsor in the flat topology. Conversely, if $\mathbf{X}$ is a torsor in the flat topology and $\mathbf{G}$ is smooth, then $\mathbf{X}$ is smooth, and as in 25.25 (ii) we conclude that $\mathbf{X}$ is a torsor in the étale topology.

25.27 Example. Let $\mathbf{G}$ be a k-group scheme. Taking $\mathbf{X} = \mathbf{G}$, the multiplication $\mathbf{X}\times\mathbf{G} \to \mathbf{X}$ defines a group action and $\mathbf{X}(k) = \mathbf{G}(k)$ is nonempty for it contains the identity element of $\mathbf{G}(k)$. Thus $\mathbf{G}$ is itself a $\mathbf{G}$-torsor in the étale topology. It is called the *trivial* $\mathbf{G}$-torsor.

In case k is a field and $\mathbf{X}$ is an affine k-scheme of finite type, some of the conditions in the definition of torsor can be rephrased.

25.28 Proposition. *Let k be a field and $\mathbf{X}$ be an affine k-scheme of finite type. If $\mathbf{X}(R) \neq \emptyset$ for some finitely generated (resp., smooth) and nonzero $R \in k$-**alg**, then $\mathbf{X}(K) \neq \emptyset$ for some field K that is finite-dimensional (resp., finite-dimensional and separable) over k.*

Proof Since R is not the zero ring, by the Nullstellensatz (resp., the separable Nullstellensatz), there is a field K that is finite-dimensional (resp., finite-dimensional and separable) over k and a homomorphism of k-algebras $R \to K$. Thus $\mathbf{X}(K) \neq \emptyset$. □

It follows from the proposition that, for $\mathbf{X}$ and k as in the proposition, $\mathbf{X}(R) \neq \emptyset$ for some nonzero finitely generated R if and only if $\mathbf{X}(K) \neq \emptyset$ for K the algebraic closure of k. Similarly, $\mathbf{X}(R) \neq \emptyset$ for some nonzero smooth R if and only if $\mathbf{X}(K) \neq \emptyset$ for K the separable closure of k.

25.29 Concluding remarks. The three fundamental facts from algebraic geometry assembled in 25.25 form an extremely versatile tool to derive nontrivial results about non-associative algebras over commutative rings, having first been applied in the setting of Jordan pairs more than forty years ago by Loos [173]. Further application in many different directions will be given in subsequent portions of this work.

Exercises

25.30. Let R be a finitely presented k-algebra.

(a) Prove that a finitely presented R-algebra is finitely presented over k.
(b) Conclude from (a) that R_f is a finitely presented k-algebra, for any $f \in R$.

25.31. Let $\varphi\colon R \to R'$ be a surjective morphism in k-**alg**. Prove:

(a) (cf. [61, I, §3, 1.3 (b)]) If R is finitely generated and R' is finitely presented, then $\mathrm{Ker}(\varphi) \subseteq R$ is a finitely generated ideal.

(b) If R is finitely presented and $\mathrm{Ker}(\varphi) \subseteq R$ is a finitely generated ideal, then R' is finitely presented.

25.32. Let M be a finitely generated projective k-module. Show that the affine k-scheme $M_{\mathbf{a}}$ of 24.21 is finitely presented.

25.33. Let M be a k-module and $w \in M$. Show that $\tilde{w}\colon k\text{-}\mathbf{alg} \to \mathbf{set}$ define by $\tilde{w}(R) = \{w_R\} \subseteq M_R$ for all $R \in k\text{-}\mathbf{alg}$ is a subfunctor of $M_{\mathbf{a}}$, and even a finitely presented closed affine subscheme if M is finitely generated projective.

25.34. Let M be a projective k-module, $q\colon M \to k$ a quadratic form and R a faithfully flat k-algebra. Show that if $q_R\colon M_R \to R$ is non-singular over R in the sense of 11.11, then so is q over k.

25.35. *Faithfully flat descent of polynomial laws.* Let R be a faithfully flat k-algebra. As in 25.6, consider the two morphisms

$$d^i\colon R \longrightarrow S := R \otimes R \qquad (i = 0, 1) \tag{1}$$

in k-**alg** defined by

$$d^0(r) := 1_R \otimes r, \quad d^1(r) := r \otimes 1_R \qquad (r \in R). \tag{2}$$

Pulling back scalar multiplication from S to R by means of d^i converts any $T \in S\text{-}\mathbf{alg}$ into some $T_i \in R\text{-}\mathbf{alg}$ such that $T_0 = T_1 = T$ as k-algebras. Now let M, N be k-modules and suppose $g\colon M_R \to N_R$ is a polynomial law over R. Then prove:

(a) For $i = 0, 1$, there are unique polynomial laws $g_i\colon M_S \to N_S$ over S such that $g_{iT} := (g_i)_T = g_{T_i}$ as set maps from $(M_S)_T = M_T = M_{T_i} = (M_R)_{T_i}$ to $(N_S)_T = N_T = N_{T_i} = (N_R)_{T_i}$ for all $T \in S\text{-}\mathbf{alg}$.

(b) There exists a polynomial law $f\colon M \to N$ over k satisfying $f \otimes R = g$ if and only if $g_0 = g_1$. In this case, f is unique, and for all $k' \in k\text{-}\mathbf{alg}$, the morphism

$$\psi\colon k' \longrightarrow R_{k'}, \quad \alpha' \longmapsto 1_R \otimes \alpha',$$

in k-**alg** makes the diagram

$$\begin{array}{ccccccc}
M_{k'} & \xrightarrow[1_{M_{k'}}]{} & M_{k'} & \xrightarrow[f_{k'}]{} & N_{k'} & \xrightarrow[1_{N_{k'}}]{} & N_{k'} \\
\downarrow{\scriptstyle 1_M \otimes \psi} & & \downarrow{\scriptstyle \mathrm{can}_{M_{k'}, R_{k'}}} & & \downarrow{\scriptstyle \mathrm{can}_{N_{k'}, R_{k'}}} & & \downarrow{\scriptstyle 1_N \otimes \psi} \\
M_{R_{k'}} & \xrightarrow[1_{M_{R_{k'}}}]{} & (M_{k'})_{R_{k'}} = (M_R)_{R_{k'}} & \xrightarrow[g_{R_{k'}}]{} & (N_R)_{R_{k'}} = (N_{k'})_{R_{k'}} & \xrightarrow[1_{N_{R_{k'}}}]{} & N_{R_{k'}}
\end{array} \tag{3}$$

commutative.

25.36. Prove: If M, N are finitely generated projective k-modules, then for each $d \geq 0$ the natural map

$$\Phi\colon S^d(M^*) \otimes N \to \mathrm{Pol}^d(M, N)$$

is an isomorphism.

Remark. Compare Exc. 12.49.

25.37. *Faithfully flat descent of conic algebras.* Let C be a non-associative k-algebra und suppose $R \in k$-**alg** is faithfully flat. Prove:

(a) If C_R is unital, then so is C.
(b) If C is projective as a k-module and C_R carries a quadratic form over R making it a conic R-algebra, then C carries a quadratic form over k making it a conic k-algebra such that the base change from k to R of C as a conic k-algebra is C_R as a conic R-algebra.

Remark. This exercise is a routine application of 25.35. Applications of this kind will occur quite frequently in the present volume. Rather than always carrying out the details, we from now on refer to these applications by saying that the corresponding results are obtained *by faithfully flat descent*.

25.38. (a) Let M be a finitely generated projective k-module. Prove that there is a characteristic polynomial $\mathrm{End}_k(M) \to k[\mathbf{t}]$, where $\mathbf{t}$ is an indeterminate, and that it is a polynomial law.

(b) For $x \in \mathrm{End}_k(M)$, define $\det x$ to be the constant term of the characteristic polynomial of $-x$. Verify for $x, y \in \mathrm{End}_k(M)$:

(i) $\det(xy) = (\det x)(\det y)$.
(ii) The Cayley-Hamilton Theorem holds, in the sense that plugging x into its characteristic polynomial yields zero in $\mathrm{End}_k(M)$.
(iii) x is invertible if and only if $\det x$ is invertible in k.

25.39. *Smoothness and direct products.* Let $\mathbf{X}_1, \mathbf{X}_2$ be affine k-schemes. Show that if $\mathbf{X}_1$ and $\mathbf{X}_2$ are both smooth, then so is their direct product $\mathbf{X}_1 \times \mathbf{X}_2$. Conversely, assume $\mathbf{X}_1 \times \mathbf{X}_2$ is smooth, $\mathbf{X}_1$ is finitely presented over k, and $\mathbf{X}_2(k) \neq \emptyset$. Show that $\mathbf{X}_1$ is smooth.

25.40. Let k be a ring and suppose $d \geq 2$ is an integer and $x \in k$. Prove: The k-algebra $R := k[\mathbf{t}]/(\mathbf{t}^d - x)$ is an étale k-algebra if and only if both d and x are invertible in k.

25.41. *n-th roots of unity.* Let n be a positive integer. Prove:

(a) Setting

$$\boldsymbol{\mu}_n(R) := \{r \in R \mid r^n = 1_R\}$$

for all $R \in k$-**alg** gives a closed k-group subscheme $\boldsymbol{\mu}_n$ of $\mathbf{G_m}$ whose co-ordinate algebra is

$$k[\boldsymbol{\mu}_n] = k[\mathbf{t}]/k[\mathbf{t}](\mathbf{t}^n - 1) \cong k[\mathbf{t}, \mathbf{t}^{-1}]/k[\mathbf{t}, \mathbf{t}^{-1}](\mathbf{t}^n - 1).$$

(b) If $n = lm$ with relatively prime positive integers l, m, then $\boldsymbol{\mu}_n \cong \boldsymbol{\mu}_l \times \boldsymbol{\mu}_m$.

(c) The following conditions are equivalent.

(i) $\boldsymbol{\mu}_n$ is étale.
(ii) $\boldsymbol{\mu}_n$ is smooth.
(iii) $n \cdot 1_k \in k^\times$.

25.42. In this problem, k is a field and E is an étale k-algebra of finite dimension d.

(a) Prove that there is a Zariski-open subset of E consisting of elements e such that $k[e] = E$, and that this set is non-empty if k is infinite.

(b) In the case when $E = \prod_{i=1}^{d} k$, prove that this Zariski-open subset (of $e \in E$ with $k[e] = E$) is non-empty if and only if $|k| \geq d$.

Remark. One says that $R \in k$-**alg** is *monogenic* or *one-generated* if there is an $r \in R$ such that $R = k[r]$. In this problem, we have investigated whether étale k-algebras are monogenic in the case where k is a field. For an example of a result that holds when k is semi-local, see [21, Prop. 7.3].

25.43. Let A be a unital non-associative k-algebra, in the sense of 8.6. Prove: If $A \otimes R$ is simple for some faithfully flat $R \in k$-**alg**, then A is simple.

25.44. Let M, M' be k-modules and $R \in k$-**alg** be faithfully flat. Prove that the exact sequence

$$0 \longrightarrow k \longrightarrow R \xrightarrow{d^0 - d^1} R \otimes R$$

from Prop. 25.7 induces an exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(M, M') \longrightarrow \mathrm{Hom}_R(M_R, M'_R) \longrightarrow \mathrm{Hom}_{R\otimes R}(M_{R\otimes R}, M'_{R\otimes R}).$$

25.45. Let $\mathbf{G}$ be a k-group scheme. Prove that the k-group functor of automorphisms of $\mathbf{G}$, viewed as the trivial $\mathbf{G}$-torsor from Example 25.27, is naturally identified with $\mathbf{G}$ itself.

25.46. Recall the split étale algebra E_Γ defined by a finite set Γ from Example 24.20.

(i) Verify that, when k is non-zero connected, the group of k-algebra automorphisms of E_Γ is the group of permutations of Γ.
(ii) Deduce that the k-group scheme $\mathbf{Aut}(E_\Gamma)$ is naturally identified with the constant group scheme corresponding to the group of permutations of Γ.

(The case $|\Gamma| = 2$ was Exc. 24.29.)

25.47. Let E be a k-algebra. Prove:

(i) If E is finite étale, then E_R is a finite étale R-algebra for every $R \in k$-**alg**.
(ii) E is finite étale if and only if there is a faithfully flat $R \in k$-**alg** such that E_R is a finite étale algebra over R.

(*Hint*: It may be helpful to use the notions of separable and étale algebras from Bourbaki [29, Chap. V]. Namely, in case k is a field, a k-algebra A is *separable* if A_L is reduced for every field L containing k. The definition of étale algebra over a field in Bourbaki agrees with our definition.)

26 Splitting composition algebras with étale covers

We will now be able to show as the main result of the present section that every composition algebra C over any commutative ring becomes split after a faithfully flat étale base change. The proof, following [176], is not at all

obvious, relying as it does on the results of Grothendieck we have assembled before. As an important by-product of our approach we also show that the group scheme **Aut**(C) as defined in Example 24.25 is smooth in the sense of 25.20.

Throughout we let k be an arbitrary commutative ring.

26.1 The set-up. Unless other arrangements have been made, we fix a composition algebra C of rank r over k. By Cor. 19.18, we have $r \in \{1, 2, 4, 8\}$. Moreover, if $r > 1$, then C is regular (19.11) and, given an elementary idempotent $e \in C$, the Peirce components $C_{12}(e)$, $C_{21}(e)$ by Ex. 19.35 are in duality to each other under the bilinearized norm of C; hence they are finitely generated projective k-modules of rank $m = \frac{r}{2} - 1$.

26.2 The concept of a splitting datum. In order to define splitting data for C, we discuss the cases $r = 1, 2, 4, 8$ separately.

(a) For $r = 1$, a *splitting datum* for $C \cong k$ by definition has the form $\Delta = (1_C) \in C^1$.

(b) For $r = 2$, a *splitting datum* for C by definition has the form $\Delta = (e) \in C^1$, where $e \in C$ is an elementary idempotent.

(c) For $r = 4$, a *splitting datum* for C by definition has the form $\Delta = (e, x, y) \in C^3$, where $e \in C$ is an elementary idempotent and $x \in C_{21}(e)$, $y \in C_{12}(e)$ satisfy the following conditions, with $e' := 1_C - e$.

$$xy = e', \quad t_C(xy) = 1, \quad yx = e. \tag{1}$$

Actually, one checks easily that these equations are mutually equivalent.

(d) For $r = 8$, a *splitting datum* for C by definition has the form $\Delta = (e, x_1, x_2, x_3) \in C^4$, where $e \in C$ is an elementary idempotent and $x_1, x_2, x_3 \in C_{21}(e)$ satisfy the following conditions.

$$(x_1x_2)x_3 = -e, \quad t_C(x_1x_2x_3) = -1, \quad (x_ix_j)x_l = -e \tag{2}$$

for all cyclic permutations $(i\,jl)$ of (123). Again one checks that these equations are mutually equivalent.

In summary, splitting data for C belong to C^{n_r}, where n_r for $r = 1, 2, 4, 8$ is defined by the following table.

r	1	2	4	8
n_r	1	1	3	4

Moreover, they are preserved by isomorphisms: if $\eta\colon C \to C'$ is an isomorphism of composition algebras of rank r over k, and Δ is a splitting datum for

C, then the linear bijection $\eta^{n_r}\colon C^{n_r} \to C'^{n_r}$ maps $\Delta \subseteq C^{n_r}$ to the splitting datum $\eta(\Delta) := \eta^{n_r}(\Delta) \subseteq C'^{n_r}$ of C'. Finally, splitting data are stable under base change, so if $\Delta \subseteq C^{n_r}$ is a splitting datum for C, then $\Delta_R \subseteq C_R^{n_r}$ is one for C_R, for all $R \in k$-**alg**. The set of all splitting data for C will be denoted by

$$\mathrm{Splid}(C) := \{\Delta \mid \Delta \text{ is a splitting datum for } C\}. \tag{3}$$

26.3 The affine scheme of splitting data. Again we treat the cases $r = 1, 2, 4, 8$ separately and let $R \in k$-**alg** be arbitrary.

(a) Let $r = 1$. Then $(s1_{C_R}) \in C_R^1$ for $s \in R$ is a splitting datum for C_R if and only if

$$s - 1_R = 0. \tag{1}$$

(b) Let $r = 2$. Then $(e) \in C_R^1$ by Exc. 16.23 is a splitting datum for C_R if and only if

$$n_C(e) = 0, \quad t_C(e) = 1. \tag{2}$$

(c) Let $r = 4$. Then $(e, x, y) \in C_R^3$ is a splitting datum for C_R if and only if

$$\begin{aligned} n_C(e) = 0, \quad t_C(e) = 1, \\ \langle u_R^*, ex\rangle = \langle u_R^*, xe - x\rangle = \langle u_R^*, ye\rangle = \langle u_R^*, ey - y\rangle = 0, \\ t_C(xy) = 1 \end{aligned} \tag{3}$$

for all $u^* \in C^*$.

(d) Let $r = 8$. Then $(e, x_1, x_2, x_3) \in C_R^4$ is a splitting datum for C_R if and only if

$$\begin{aligned} n_C(e) = 0, \quad t_C(e) = 1, \\ \langle u_R^*, ex_i\rangle = \langle u_R^*, x_ie - x_i\rangle = 0, \\ t_C(x_1x_2x_3) = -1 \end{aligned} \tag{4}$$

for all $u^* \in C^*$ and all $i = 1, 2, 3$.

Summing up, we therefore conclude that equations (1)–(4) define a closed subscheme of $C_{\mathbf{a}}^{n_r} := (C^{n_r})_{\mathbf{a}} = (C_{\mathbf{a}})^{n_r}$ in the sense of 24.15, denoted by $\mathbf{Splid}(C)$ and called the *affine scheme of splitting data* for C. By definition we have

$$\mathbf{Splid}(C)(R) := \mathrm{Splid}(C_R) := \{\Delta \mid \Delta \text{ is a splitting datum for } C_R\} \tag{5}$$

for all $R \in k$-**alg** and, in view of (9.4.2),

$$\begin{aligned} \mathbf{Splid}(C)(\varphi)\colon \mathbf{Splid}(C)(R) &\longrightarrow \mathbf{Splid}(C)(S), \\ \mathrm{Splid}(C_R) \ni \Delta &\longmapsto \Delta_S = (\mathbf{1}_{C^{n_r}} \otimes \varphi)(\Delta) \in \mathrm{Splid}(C_S), \end{aligned} \tag{6}$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**. Passing from C to its affine scheme of splitting data is obviously compatible with base change.

As will be seen in due course, for a splitting datum to exist it is necessary and sufficient that the ambient composition algebra be split. In fact, a much more precise statement will be derived in Prop. 26.7 below. Before proceeding to this result, we discuss a few examples.

26.4 Standard examples of splitting data. Here we present examples of splitting data for the standard split composition algebras $C_0 := C_{0r}(k)$ of rank r over k as described in 21.19 (a)–(d). Again we treat the cases $r = 1, 2, 4, 8$ separately.

(a) $r = 1$. Then $C_0 = k$, and

$$\Delta_0 := \Delta_{01}(k) := (1) \tag{1}$$

is the only splitting datum for C_0.

(b) $r = 2$. Then $C_0 = k \times k$ is the direct product of two copies of k as ideals and

$$\Delta_0 := \Delta_{02}(k) := (E), \quad E := (1, 0) \in C \tag{2}$$

is a splitting datum for C.

(c) $r = 4$. Then $C_0 = \mathrm{Mat}_2(k)$ is the algebra of 2-by-2 matrices with entries in k and

$$\Delta_0 := \Delta_{04}(k) := (E, X, Y), \tag{3}$$
$$E := E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X := E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad Y := E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is a splitting datum for C_0.

(d) $r = 8$. Then $C_0 = \mathrm{Zor}(k)$ is the algebra of Zorn vector matrices over k and, writing $(e_i)_{1 \le i \le 3}$ for the canonical basis of k^3 over k,

$$\Delta_0 := \Delta_{08}(k) := (E, X_1, X_2, X_3), \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_i = \begin{pmatrix} 0 & 0 \\ e_i & 0 \end{pmatrix} \quad (1 \le i \le 3) \tag{4}$$

is a splitting datum for C since (21.18.4) implies

$$\begin{aligned} (X_1X_2)X_3 &= \begin{pmatrix} 0 & e_1 \times e_2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ e_3 & 0 \end{pmatrix} \\ &= -(e_1 \times e_2)^{\mathsf{T}} e_3 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = -\det(e_1, e_2, e_3)E = -E. \end{aligned} \tag{5}$$

The splitting datum $\Delta_{0r}(k)$ exhibited in (1)–(4) above will henceforth be referred to as the *standard splitting datum* for $C_{0r}(k)$ ($r = 1, 2, 4, 8$). We clearly have $\Delta_{0r}(k)_R = \Delta_{0r}(R)$ for all $R \in k$-**alg**.

26.5 Proposition. *The affine k-scheme of splitting data for C is smooth.*

Proof Consulting (26.3.1)–(26.3.4) we see that $\mathbf{X} := \mathbf{Splid}(C)$ is defined by finitely many equations as a closed subscheme of $C_{\mathbf{a}}^{n_r}$. By Exc. 25.31 (b) and Exc. 25.32, therefore, $\mathbf{X}$ is finitely presented. Hence, by 25.20, it suffices to show that the set map $\mathbf{X}(R) \to \mathbf{X}(R/I)$ induced by the projections $R \to R/I$ is surjective, for all $R \in k$-**alg** and all ideals $I \subseteq R$ satisfying $I^2 = \{0\}$. In order to do so, we may assume $R = k$ and write $\alpha \mapsto \bar{\alpha}$, $x \mapsto \bar{x}$ for the projection $k \to \bar{k} := k/I$, $C \longrightarrow \bar{C} := C \otimes \bar{k} = C/IC$, respectively. We must show that every splitting datum Δ' of $\bar{C}$ can be lifted to a splitting datum Δ of C satisfying $\bar{\Delta} = \Delta'$. The case $r = 1$ being obvious, we are left with the cases $r = 2, 4, 8$, which we treat separately.

Suppose first that $r = 2$. A splitting datum for $\bar{C}$ has the form $\Delta' = (e')$ for some elementary idempotent $e' \in \bar{C}$. By Exc. 16.25, e' can be lifted to an elementary idempotent $e \in C$. Thus $\Delta := (e)$ is a splitting datum for C such that $\bar{\Delta} = \Delta'$.

Suppose next that $r = 4$. A splitting datum for $\bar{C}$ has the form $\Delta' = (e', x', y')$ for some elementary idempotent $e' \in \bar{C}$, where $x' \in \bar{C}_{21}(e')$, $y' \in \bar{C}_{12}(e')$ satisfy $t_{\bar{C}}(x'y') = 1_{\bar{k}}$. As in (a), we find an elementary idempotent $e \in C$ satisfying $\bar{e} = e'$. The canonical projection $C \to \bar{C}$ induces surjections $C_{ij}(e) \to \bar{C}_{ij}(e')$ for $\{i, j\} = \{1, 2\}$. Hence x', y' can be lifted to elements $u \in C_{21}(e)$, $v \in C_{12}(e)$, respectively, satisfying $\bar{u} = x'$, $\bar{v} = y'$. Hence

$$\overline{t_C(uv)} = t_{\bar{C}}(x'y') = 1_{\bar{k}},$$

and we conclude $t_C(uv) = 1 + \alpha$ for some $\alpha \in I$. This implies $1 + \alpha \in k^\times$ with inverse $1 - \alpha$ since $I^2 = \{0\}$. Setting $x := u \in C_{21}(e)$, $y := (1 - \alpha)v \in C_{12}(e)$, we therefore deduce not only $\bar{x} = x'$, $\bar{y} = y'$ but also $t_C(xy) = 1$, so $\Delta := (e, x, y)$ is a splitting datum for C such that $\bar{\Delta} = \Delta'$.

Suppose finally that $r = 8$. A splitting datum for C has the form $\Delta' = (e', x'_1, x'_2, x'_3)$ for some elementary idempotent $e' \in \bar{C}$ and some $x'_1, x'_2, x'_3 \in \bar{C}_{21}(e')$ satisfying $t_{\bar{C}}(x'_1 x'_2 x'_3) = -1_{\bar{k}}$. Again e' can be lifted to an elementary idempotent $e \in C$ satisfying $\bar{e} = e'$, and again x'_i can be lifted to an element $u_i \in C_{21}(e)$ satisfying $\bar{u}_i = x'_i$ for $1 \le i \le 3$. Hence

$$\overline{t_C(u_1 u_2 u_3)} = t_{\bar{C}}(x'_1 x'_2 x'_3) = -1_{\bar{k}},$$

and we conclude $t_C(u_1 u_2 u_3) = -1 + \alpha$ for some $\alpha \in I$. This implies $-1 + \alpha \in k^\times$ with inverse $-(1 + \alpha)$. Setting $x_i := u_i$ for $i = 1, 2$ and $x_3 := -(1 + \alpha)u_3$,

we therefore deduce not only $x_i \in C_{21}(e)$ and $\bar{x}_i = x_i'$ for $1 \le i \le 3$ but also $t_C(x_1x_2x_3) = -1$. Thus $\Delta := (e, x_1, x_2, x_3)$ is a splitting datum for C such that $\bar{\Delta} = \Delta'$. □

26.6 The k-functor of isomorphisms. Let A, B be non-associative algebras over k.

(a) In partial generalization of 24.25, we consider the set of (k-algebra) isomorphisms from A to B:

$$\mathrm{Isom}_k(A,B) := \mathrm{Isom}(A,B) := \{\eta \mid \eta\colon A \xrightarrow{\sim} B \text{ is a } k\text{-isomorphism}\}. \tag{1}$$

This set will in general be empty but it gives rise to a k-functor

$$\mathbf{Isom}_k(A,B) := \mathbf{Isom}(A,B)\colon k\text{-}\mathbf{alg} \longrightarrow \mathbf{set}$$

by defining

$$\mathbf{Isom}(A,B)(R) := \mathrm{Isom}_R(A_R, B_R) \tag{2}$$

for all $R \in k$-**alg** and

$$\begin{aligned} \mathbf{Isom}(A,B)(\varphi)\colon \mathbf{Isom}(A,B)(R) &\longrightarrow \mathbf{Isom}(A,B)(S), \\ \mathrm{Isom}(A_R, B_R) \ni \eta &\longmapsto \eta_S \in \mathrm{Isom}_S(A_S, B_S) \end{aligned} \tag{3}$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**, where we view S as an R-algebra via φ and identify $A_S = (A_R)_S$, $B_S = (B_R)_S$ as S-algebras via (9.4.1).

(b) The k-group functor $\mathbf{Aut}(A)$ of 24.25 acts canonically on $\mathbf{Isom}(A,B)$ from the right via

$$\mathrm{Isom}_R(A_R, B_R) \times \mathrm{Aut}(A_R) \longrightarrow \mathrm{Isom}(A_R, B_R), \quad (\eta, \zeta) \longmapsto \eta \circ \zeta,$$

and this action is simply transitive.

(c) Returning to our composition algebra C of rank r over k, we define a *splitting* of C as an isomorphism from $C_{0r}(k)$ onto C, where $C_{0r}(k)$ is the split composition algebra of rank r over k described in 21.19. Thus $\mathrm{Isom}(C_{0r}(k), C)$ is the set of splittings of C.

26.7 Proposition. *Let C be a composition algebra of rank r over k and denote by $\Delta_{0r}(k)$ the standard splitting datum for $C_{0r}(k)$ as defined in 26.4. Then $\Delta_{0r}(k)$ generates $C_{0r}(k)$ as a unital k-algebra, and the assignment*

$$\eta \longmapsto \eta(\Delta_{0r}(k))$$

defines a bijection $\Phi = \Phi(k)$ *from the set of splittings of* C *onto the set of splitting data of* C*:*

$$\Phi := \Phi(k)\colon \operatorname{Isom}(C_{0r}(k), C) \xrightarrow{\sim} \operatorname{Splid}(C).$$

Proof Since $\Delta_0 := \Delta_{0r}(k)$ is a splitting datum for $C_0 := C_{0r}(k)$, its image under an isomorphism $\eta\colon C_0 \xrightarrow{\sim} C$ is a splitting datum for C. Thus the map Φ is well-defined, and it remains to show that it is bijective.

We begin by showing that Δ_0 generates C_0 as a unital k-algebra. By 26.4, this is trivial for $r = 1, 2$ and obvious for $r = 4$, while for $r = 8$ it suffices to note $X_iX_j = \left(\begin{smallmatrix} 0 & e_l \\ 0 & 0 \end{smallmatrix}\right)$ for all cyclic permutations (ijl) of (123), which follows immediately from (21.18.4) and (26.4.4). It is now clear that the map Φ is injective

In order to show that it is also surjective, we pick any splitting datum Δ of C and have to find an isomorphism $\eta\colon C_0 \xrightarrow{\sim} C$ sending Δ_0 to Δ. We do so again by noting that the case $r = 1$ is obvious and by treating the cases $r = 2, 4, 8$ separately.

$r = 2$. Then $\Delta = (e)$ for some elementary idempotent $e \in C$. From Exc. 16.23, we deduce that $e, \bar{e}$ are unimodular and $ke + k\bar{e}$ is a quadratic étale subalgebra of C. Hence $C = ke \oplus k\bar{e}$ since C has rank 2 as a k-module, and

$$\eta\colon C_0 \longrightarrow C, \quad (\alpha, \beta) \longmapsto \alpha e + \beta\bar{e}$$

is an isomorphism sending Δ_0 to Δ.

$r = 4$. Then $\Delta = (e, x, y)$, with $e \in C$ an elementary idempotent and $x, y \in C_{21}(e)$ satisfying (26.2.1). By Prop. 22.13, we may assume

$$C = \operatorname{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

for some line bundle L over k, and (22.12.5) yields elements $u \in L$, $v^* \in L^*$ such that $x = \left(\begin{smallmatrix} 0 & 0 \\ u & 0 \end{smallmatrix}\right)$, $y = \left(\begin{smallmatrix} 0 & v^* \\ 0 & 0 \end{smallmatrix}\right)$. Now (26.2.1) implies $\langle v^*, u\rangle = 1$, forcing L, L^* to be free k-modules of rank 1 with dual basis vectors u, v^*, respectively. Hence the assignment

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \alpha & \beta v^* \\ \gamma u & \delta \end{pmatrix} \qquad (\alpha, \beta, \gamma, \delta \in k)$$

defines an isomorphism $\eta\colon C_0 \xrightarrow{\sim} C$ sending Δ_0 to Δ.

$r = 8$. Then $\Delta = (e, x_1, x_2, x_3)$, where $e \in C$ is an elementary idempotent and $x_1, x_2, x_3 \in C_{21}(e)$ satisfy (26.2.2). By Thm. 22.15, we may assume

$$C = \operatorname{Zor}(M, \theta) = \begin{pmatrix} k & M^* \\ M & k \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

for some finitely generated projective k-module M of rank 3 and some orientation θ of M, where (22.14.8) yields elements $u_1, u_2, u_3 \in M$ satisfying $x_i = \left(\begin{smallmatrix} 0 & 0 \\ u_i & 0 \end{smallmatrix}\right)$ for $i = 1, 2, 3$. Combining (26.2.2) with (22.14.3), (22.14.2), we conclude

$$\begin{aligned} -e = (x_1 x_2)x_3 &= \begin{pmatrix} 0 & u_1 \times_\theta u_2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ u_3 & 0 \end{pmatrix} = \begin{pmatrix} -\langle u_1 \times_\theta u_2, u_3\rangle & 0 \\ 0 & 0 \end{pmatrix} \\ &= -\theta(u_1 \wedge u_2 \wedge u_3)e, \end{aligned}$$

hence $\theta(u_1 \wedge u_2 \wedge u_3) = 1$. Thus (u_1, u_2, u_3) is a θ-balanced basis of M in the sense of 22.14, which also implies that there is an identification $C = \mathrm{Zor}(k) = C_{08}(k) = C_0$ matching u_i with e_i for $i = 1, 2, 3$. But this means we have found an isomorphism from C_0 to C sending Δ_0 to Δ. □

26.8 Theorem (Loos-Petersson-Racine [176, Thm. 4.10])**.** *Let C be a composition algebra of rank $r \in \{1, 2, 4, 8\}$ over k. Then the k-functor*

$$\mathbf{Isom}(C_{0r}(k), C)$$

is a smooth affine torsor in the étale topology with structure group $\mathbf{G} = \mathbf{Aut}(C_{0r}(k))$.

Proof Putting $\mathbf{X} := \mathbf{Isom}(C_{0r}(k), C)$, the set maps

$$\Phi(R)\colon \mathbf{X}(R) \xrightarrow{\sim} \mathbf{Splid}(C)(R)$$

given by Prop. 26.7 for any $R \in k$-**alg** are bijective and one checks that they are compatible with base change, hence give rise to an isomorphism

$$\Phi\colon \mathbf{X} \xrightarrow{\sim} \mathbf{Splid}(C)$$

of k-functors. By Prop. 26.5, therefore, $\mathbf{X}$ is a smooth affine k-scheme acted upon by $\mathbf{G}$ from the right in a simply transitive manner (26.6 (b)). Moreover, it follows from 23.12 that $\mathbf{X}$ has non-empty geometric fibers. Hence, by Prop. 25.24, $\mathbf{X}$ is fppf and thus, in view of 25.25 (ii) and the definition 25.26 (iii), a smooth affine torsor with structure group $\mathbf{G}$ in the étale topology. □

The preceding theorem has two corollaries which, up to a point, will be proved simultaneously.

26.9 Corollary (Loos-Petersson-Racine [176, Cor. 4.11])**.** *For any k-algebra C, the following conditions are equivalent.*

(i) *C is a composition algebra over k.*

(ii) *There exists a faithfully flat $R \in k$-**alg** such that C_R is a composition algebra over R.*

(iii) *There exists a faithfully flat $R \in k$-**alg** such that C_R is a split composition algebra over R.*

(iv) *There exists an étale cover $R \in k$-**alg** such that C_R is a split composition algebra over R.*

26.10 Corollary (Loos-Petersson-Racine [176, Cor. 4.12])**.** *Let C be a composition algebra over k. Then* **Aut**(C) *is a smooth k-group scheme.*

Proof of 26.9 and 26.10 We first note that in 26.9, the implications (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) are obvious, while the implication (ii) $\Rightarrow$ (i) follows from the fact that C is a conic algebra (by Exc. 25.37) whose norm, n_C, is non-singular (by Exc. 25.34, since $(n_C)_R = n_{C_R}$ is and R is faithfully flat) and permits composition (since $(n_C)_R$ does and the natural map $C \to C_R$ by Prop. 25.4 is injective). In 26.9, therefore, it remains to prove the implication (i) $\Rightarrow$ (iv).

Next we reduce both corollaries to the case that

$$C \text{ has rank } r \in \{1, 2, 4, 8\} \text{ as a } k\text{-module.} \tag{1}$$

This is accomplished by considering the rank decomposition of C, which, by 21.19, attains the form

$$k = k_0 \times k_1 \times k_2 \times k_3, \quad C = C_0 \times C_1 \times C_2 \times C_3 \tag{2}$$

as direct products of ideals, where $C_j := C_{k_j}$ is a composition algebra of rank 2^j over k_j for $0 \le j \le 3$. Hence, assuming the implication (i) $\Rightarrow$ (iv) of 26.9 if (1) holds. we find an étale covers R_j of k_j for $0 \le j \le 3$ such that the composition algebra C_{jR_j} over R_j is split of rank 2^j. It is now straightforward to check that $R := R_0 \times R_1 \times R_2 \times R_3$ is an étale cover of k making $C_R = C_{0R_0} \times C_{1R_1} \times C_{2R_2} \times C_{3R_3}$ a split composition algebra over k. This completes the reduction for 26.9.

Assuming 26.10 if (1) holds, let $R \in k$-**alg** and $I \subseteq R$ be an ideal having $I^2 = \{0\}$. Using Exc. 8.10, and arguing as before, we have

$$\begin{aligned} R &= R_0 \times R_1 \times R_2 \times R_3, \\ I &= I_0 \times I_1 \times I_2 \times I_3, \\ C_R &= C_{0R_0} \times C_{1R_1} \times C_{2R_2} \times C_{3R_3}, \\ C_{R/I} &= C_{0,R_0/I_0} \times C_{1,R_1/I_1} \times C_{2,R_2/I_2} \times C_{3,R_3/I_3}. \end{aligned} \tag{3}$$

Since $C_{j,R_j} = 1_{k_j} C_R$, we conclude that $\mathrm{Aut}(C_R)$ stabilizes C_{j,R_j} for $0 \le j \le 3$. Thus

$$\mathrm{Aut}(C_R) = \mathrm{Aut}(C_{0R_0}) \times \mathrm{Aut}(C_{1R_1}) \times \mathrm{Aut}(C_{2R_2}) \times \mathrm{Aut}(C_{3R_3}),$$

and, similarly,

$$\mathrm{Aut}(C_{R/I}) = \mathrm{Aut}(C_{0,R_0/I_0}) \times \mathrm{Aut}(C_{1,R_1/I_1}) \times \mathrm{Aut}(C_{2,R_2/I_2}) \times \mathrm{Aut}(C_{3,R_3/I_3}).$$

Since C_{jR_j} has rank 2^j over R_j, the k_j-group scheme $\mathbf{Aut}(C_j)$ is smooth, forcing it to be finitely presented and the natural map $\mathrm{Aut}(C_{jR_j}) \to \mathrm{Aut}(C_{j,R_j/I_j})$ to be surjective for $0 \le j \le 3$. Hence so is the natural map $\mathrm{Aut}(C_R) \to \mathrm{Aut}(C_{R/I})$, which completes the reduction also for 26.10.

For the remainder of the proof, we may therefore assume that (1) holds. Hence Thm. 26.8 implies that $\mathbf{X} := \mathbf{Isom}(C_{0r}(k), C)$ is a smooth torsor in the étale topology, with structure group $\mathbf{G} = \mathbf{Aut}(C_{0r}(k))$. Thus condition (iii) of 25.26 implies $\mathbf{X}(R) \neq \emptyset$ for some étale cover $R \in k\text{-}\mathbf{alg}$. Hence $C_R \cong C_{0k}(R)$ is split of rank r over R. This completes the proof of 26.9. Moreover, the chain of isomorphisms

$$\mathbf{Aut}(C)_R \cong \mathbf{Aut}(C_R) \cong \mathbf{Aut}(C_{0r}(R)) \cong \mathbf{G}_R \cong \mathbf{X}_R$$

shows that $\mathbf{Aut}(C)_R$ is smooth over R. But then, by 25.25 (iii), $\mathbf{Aut}(C)$ must be smooth over k. □

26.11 Example. Let us exhibit covers as in 26.9(iii) and (iv) in the case of $C = \mathrm{DiCo}(\mathbb{O})$, the Dickson-Coxeter octonions over the integers.

Let R be the ring of integers in $\mathbb{Q}(\sqrt{-d})$ for some positive integer d. The norm $(n_C)_{\mathbb{Q}(\sqrt{-d})}$ is isotropic, so $C_{\mathbb{Q}(\sqrt{-d})}$ is split. Looking ahead to Lemma 57.1 (a), we deduce that C_R is split. Since R is an fppf $\mathbb{Z}$-algebra (Example 25.19), this verifies Cor. 26.9(iii).

But note that R is not an étale $\mathbb{Z}$-algebra because it is ramified at the primes dividing the discriminant of $\mathbb{Q}(\sqrt{-d})$. Consider instead the quadratic extensions $K_1 := \mathbb{Q}(\sqrt{-1})$ and $K_2 := \mathbb{Q}(\sqrt{-3})$. They are ramified only at the primes $p_1 := 2$ and $p_2 := 3$ respectively. Consequently, the integral closure R_i of $\mathbb{Z}[1/p_i]$ in K_i is an étale $\mathbb{Z}[1/p_i]$-algebra. Since $\mathbb{Z}[1/p_i]$ is an étale $\mathbb{Z}$-algebra, R_i is étale over $\mathbb{Z}$. Moreover, $\operatorname{Spec} R_i \to \operatorname{Spec} \mathbb{Z}$ only misses p_i, so $R_1 \times R_2$ is an étale cover of $\mathbb{Z}$. As in the previous paragraph, C_{R_i} is split for each i, so $C_{R_1 \times R_2}$ is split as an octonion algebra over $R_1 \times R_2$.

Exercises

26.12. Let $Q := (M, q)$ be a quadratic space of rank $2n$, $n \in \mathbb{N}$, over k. By a *hyperbolic basis* of Q we mean a family $(w_i)_{1 \le i \le 2n}$ of elements in M such that

$$q(w_i) = q(w_{n+i}) = q(w_i, w_j) = q(w_{n+i}, w_{n+j}) = 0, \quad q(w_i, w_{n+j}) = \delta_{ij} \tag{1}$$

for $1 \le i, j \le n$. The set of hyperbolic bases of Q will be denoted by $\mathrm{Hyp}(Q) \subseteq M^{2n}$.

(a) Show that the k-functor

$$\mathbf{Hyp}(Q)\colon k\text{-}\mathbf{alg} \longrightarrow \mathbf{set}$$

given by

$$\mathbf{Hyp}(Q)(R) := \mathrm{Hyp}(Q_R), \quad Q_R := (M_R, q_R),$$

for all $R \in k$-**alg** and

$$\mathbf{Hyp}(Q)(\varphi)\colon \mathbf{Hyp}(Q)(R) \longrightarrow \mathbf{Hyp}(Q)(S),$$
$$\mathrm{Hyp}(Q_R) \ni (w_i)_{1\le i\le 2n} \longmapsto (w_{iS})_{1\le i\le 2n} \in \mathrm{Hyp}(Q_S)$$

for all morphisms $\varphi\colon R \to S$ in k-**alg** is a smooth closed k-subscheme of $M_{\mathbf{a}}^{2n}$.

(b) Conclude from (a) that

(i) there exists an étale cover $R \in k$-**alg** making Q_R a split hyperbolic quadratic space over R in the sense of 11.18.

(ii) $\mathbf{O}(Q)$ is a smooth group scheme.

(*Hint*: Imitate the arguments of 26.6–26.10.)

V

Jordan algebras

In the preceding chapter, we investigated some fundamental properties of composition algebras, particularly of octonions, over arbitrary commutative rings. Our next main objective will be to accomplish the same for what we call cubic Jordan algebras, among which Albert algebras are arguably the most important. In order to achieve this objective, a few prerequisites from the general theory of Jordan algebras are indispensable. Rather than striving for maximum generality, we confine ourselves to what is absolutely necessary for the intended applications.

27 Linear Jordan algebras

Linear Jordan algebras were introduced by Albert, who in three fundamental papers [5, 6, 7] developed a virtually complete structure theory of the finite-dimensional ones over arbitrary fields of characteristic not two. While the main focus of the present volume is primarily on (quadratic) Jordan algebras, linear Jordan algebras are still of some interest since, e.g., they motivate the study of quadratic ones and provide useful illustrations of why certain weird phenomena can only occur in characteristic 2. In this section, the most elementary properties of linear Jordan algebras will be discussed. Since linear Jordan algebras have been extensively treated in book form (Braun-Koecher [36], Jacobson [136], Zhevlakov et al [298], and particularly McCrimmon [190]), proofs will often be omitted.

Throughout we let k be a commutative ring such that $2 \in k^\times$. We begin by repeating definitions 5.6, 5.7 in the present more general context.

27.1 The concept of a linear Jordan algebra. By a *linear Jordan algebra* over k we mean a (non-associative) k-algebra J satisfying the following identities, for all $x, y \in J$.

$$xy = yx \qquad \text{(commutative law)}, \tag{1}$$

$$x(x^2y) = x^2(xy) \qquad \text{(Jordan identity)}. \tag{2}$$

27.2 Remark. The Jordan identity is *the* minimal nontrivial polynomial identity

one can ask for on a commutative k-algebra, in a certain sense. Specifically, suppose k is a field of characteristic $\neq 2, 3, 5$ and J is a finite-dimensional commutative (non-associative) k-algebra with an associative bilinear form as in 7.9 that is nondegenerate. *If J satisfies a polynomial identity of degree ≤ 4 not implied by the commutative law, then J is a linear Jordan algebra*, see [49, Prop. A.8].

27.3 Special and exceptional linear Jordan algebras. (a) Let A be a k-algebra with multiplication $(x, y) \mapsto xy$. Then the *symmetric product*

$$x \bullet y := \frac{1}{2}(xy + yx)$$

converts A into a commutative algebra over k, denoted by A^+. Moreover, one checks easily that, if A is associative, then A^+ is a linear Jordan algebra. Linear Jordan algebras that are isomorphic to a subalgebra of A^+, for some associative algebra A, are said to be *special*. Non-special linear Jordan algebras are called *exceptional*.

(b) For example, let B be a unital k-algebra and $\tau\colon B \to B$ an involution. Then $H(B, \tau) = \{x \in B \mid \tau(x) = x\}$ is a unital subalgebra of B^+. In particular, if B is associative, then $H(B, \tau)$ is a unital special Jordan algebra.

27.4 Elementary identities. The Jordan identity (27.1.2) can be expressed in terms of left multiplication operators as

$$[L_x, L_{x^2}] = 0, \tag{1}$$

so a commutative algebra is linear Jordan if and only if (1) holds, i.e., if and only if the left multiplication operators L_x and L_{x^2} commute.

Now let J be a linear Jordan algebra over k. Replacing x by $\alpha x + y$ in (1) for $x, y \in J$, $\alpha \in k$, expanding and comparing mixed terms by using the fact that J is commutative and 2 is invertible, we conclude

$$2[L_x, L_{xy}] + [L_y, L_{x^2}] = 0. \tag{2}$$

Repeating this procedure and dividing by 2 yields

$$[L_x, L_{yz}] + [L_y, L_{zx}] + [L_z, L_{xy}] = 0, \tag{3}$$

which, when applied to any $w \in J$, amounts to

$$x((yz)w) + y((zx)w) + z((xy)w) = (yz)(xw) + (zx)(yw) + (xy)(zw). \tag{4}$$

We call (3) or (4) the *fully linearized Jordan identity*. Viewing (4) as a linear

operator in x, we deduce, after an obvious change of notation,

$$L_{(xy)z} = L_{xy}L_z + L_{yz}L_x + L_{zx}L_y - L_xL_zL_y - L_yL_zL_x. \tag{5}$$

Here the sum of the first three terms on the right is symmetric in x, y, z, hence remains unaffected by interchanging x and z. Since $[x, y, z] = (xy)z - (zy)x = z(xy) - x(zy)$, this implies

$$L_{[x,y,z]} = L_{[L_z,L_x]y} = [[L_z, L_x], L_y]. \tag{6}$$

For any integer $m > 1$, we may put $y := x^{m-1}$, $z := x$ in (5) and obtain the identity

$$L_{x^{m+1}} = 2L_{x^m}L_x + L_{x^2}L_{x^{m-1}} - L_x^2L_{x^{m-1}} - L_{x^{m-1}}L_x^2, \tag{7}$$

which for $m = 2$ reduces to

$$L_{x^3} = 3L_xL_{x^2} - 2L_x^3. \tag{8}$$

27.5 Proposition. *Linear Jordan algebras are stable under base change: if J is a linear Jordan algebra over k, then J_R is a linear Jordan algebra over R, for any $R \in k$-**alg**.*

Proof It suffices to check the Jordan identity (27.1.2) for J_R, which is straightforward, using the identities derived in 27.4. See [190, p. 149] for details. □

27.6 Proposition. *Let J be a linear Jordan algebra over k and $x \in J$.*

(a) For $u \in k_1[x]$ (resp. $u \in k[x]$ if J is unital), L_u is a polynomial in L_x and L_{x^2}.

(b) For $u, v \in k_1[x]$ (resp. $u, v \in k[x]$ if J is unital), L_u and L_v commute: $[L_u, L_v] = 0$.

Proof (a) We may assume $u = x^m$ for some $m \in \mathbb{Z}$, $m > 0$ (resp. $m \in \mathbb{N}$). Then the assertion follows from (27.4.7) by induction on m.

(b) Since L_x, L_{x^2} commute by (27.4.1), so do L_u, L_v by (a). □

27.7 Corollary. *Linear Jordan algebras over k are power-associative.*

Proof This follows from a straightforward application of Prop. 27.6 (b). Details are left to the reader. □

27.8 Remark. In view of Prop. 27.6, equation (27.4.7) simplifies to

$$L_{x^{m+1}} = 2(L_{x^m} - L_{x^{m-1}}L_x)L_x + L_{x^2}L_{x^{m-1}}. \tag{1}$$

We have encountered examples of linear Jordan algebras in 27.3 (special Jordan algebras) and in Thm. 5.10 (cubic euclidean Jordan matrix algebras, in

particular the euclidean Albert algebra). Other examples, seemingly of a completely different nature, will now be introduced.

27.9 The linear Jordan algebra of a pointed quadratic module. Let (M, q, e) be a pointed quadratic module over k, with trace t and conjugation ι, cf. 11.14 for details. Then the k-module M becomes a k-algebra $J = J(M, q, e)$ under the multiplication

$$xy := \frac{1}{2}(t(x)y + t(y)x - q(x, y)e) \qquad (x, y \in M). \tag{1}$$

J is obviously commutative and unital, with identity element $1_J = e$. (Recall from 11.14 that $M = ke \oplus \operatorname{Ker} t$. With this interpretation, formula (1) amounts to the statement that e is the identity in J and that $xy = -\frac{1}{2}q(x, y)e$ for $x, y \in \operatorname{Ker} t$.)

We have

$$x^2 - t(x)x + q(x)1_J = 0 \tag{2}$$

for all $x \in J$. Thus L_{x^2}, being a linear combination of L_x and $\mathbf{1}_J$, commutes with L_x, and we conclude that J *is a unital linear Jordan algebra*, called the *linear Jordan algebra of the pointed quadratic module* (M, q, e).

It is a *special* Jordan algebra by [136, Thm. VII.1]. That result is proved by showing that $J(M, q, e)$ is isomorphic to a subalgebra of something called the Clifford algebra of $q|_{\operatorname{Ker} t}$. While that proof is written for fields of characteristic not 2, it extends to commutative rings where 2 is invertible in an obvious way.

Since $q(e) = 1$, we conclude from (2) that $J = J(M, q, e)$ is a commutative conic k-algebra in the sense of 16.1 whose norm, trace, conjugation agree with the corresponding data attached to (M, q, e). Conversely, consider any conic algebra C over k. As we have noted before, $(C, n_C, 1_C)$ is a pointed quadratic module, and comparing (1) with (16.5.5) divided by 2, we obtain

$$J(C, n_C, 1_C) = C^+. \tag{3}$$

We now extend the definition of the U-operator as given in 6.4 to the present more general context.

27.10 The U-operator of a linear Jordan algebra. Let J be a linear Jordan algebra over k. For $x \in J$, the linear map

$$U_x \colon J \longrightarrow J, \quad y \longmapsto U_x y := 2x(xy) - x^2 y, \tag{1}$$

is called the *U-operator of x*. The quadratic map

$$U \colon J \longrightarrow \operatorname{End}_k(J), \quad x \longmapsto U_x = 2L_x^2 - L_{x^2}, \tag{2}$$

is called the *U-operator of J*. Its bilinearization gives rise to the tri-linear *Jordan triple product*

$$\{xyz\} := U_{x,z}y = (U_{x+z} - U_x - U_z)y = 2(x(zy) + z(xy) - (xz)y). \tag{3}$$

Viewing this as a map acting on z, we obtain the linear operators

$$V_{x,y} := 2(L_{xy} + [L_x, L_y]), \tag{4}$$

uniquely determined by the condition

$$V_{x,y}z = \{xyz\}. \tag{5}$$

In particular, we have

$$V_x := V_{x,1_J} = V_{1_J,x} = 2L_x, \tag{6}$$

so up to the factor 2, the operator V_x agrees with the left multiplication by x in J.

27.11 Examples. In addition to the U-operator of real cubic Jordan matrix algebras (Exc. 6.12 (b)), we now discuss the following cases.

(a) Let A be an associative algebra over k. As in Exc. 6.12 (a), the U-operator of the linear Jordan algebra A^+ is given by the formula

$$U_x y = xyx \qquad\qquad (x, y \in A) \tag{1}$$

in terms of the associative product in A. In particular, any subalgebra of A^+ is closed under the binary operation $(x, y) \mapsto xyx$.

(b) Let (M, q, e) be a pointed quadratic module over k, with trace t and conjugation $x \mapsto \bar{x}$. Then the U-operator of the linear Jordan algebra $J(M, q, e)$ is given by the formula

$$U_x y = q(x, \bar{y})x - q(x)\bar{y} \qquad\qquad (x, y \in J) \tag{2}$$

since (27.9.1), (27.9.2), (27.10.1) and (11.14.2) yield

$$\begin{aligned} U_x y &= 2x(xy) - x^2 y = t(x)xy + t(y)x^2 - q(x, y)x - t(x)xy + q(x)y \\ &= q(x, e)t(y)x - q(x)t(y)e - q(x, y)x + q(x)y \\ &= q(x, t(y)e - y)x - q(x)(t(y)e - y) = q(x, \bar{y})x - q(x)\bar{y}, \end{aligned}$$

as claimed.

The U-operator and its variants described in 27.10 are of the utmost importance for a proper understanding of (linear) Jordan algebras. This is primarily due to a number of fundamental identities satisfied by these operators.

27.12 Advanced identities. Let J be a linear Jordan algebra over k. Then the following identities hold for all $x, y, z, u, v \in J$, where for the validity of the first, J is required to be unital.

$$U_{1_J} = \mathbf{1}_J, \tag{1}$$
$$L_y U_x + U_x L_y = U_{xy,x}, \tag{2}$$
$$L_y U_{x,z} + U_{x,z} L_y = U_{xy,z} + U_{zy,x}, \tag{3}$$
$$\{xyz\} = \{zyx\}, \tag{4}$$
$$[V_{x,y}, V_{u,v}] = V_{\{xyu\},v} - V_{u,\{yxv\}}, \tag{5}$$
$$V_{x,y} U_x = U_x V_{y,x} = U_{U_x y,x}, \tag{6}$$
$$V_{U_x y,y} = V_{x,U_y x}, \tag{7}$$
$$U_{U_x y} = U_x U_y U_x. \tag{8}$$

A verification of these identities, which (with the exception of (1) and (4)) are highly non-trivial, will be omitted because they are logically not strictly necessary for the subsequent applications to cubic Jordan algebras. The interested reader is referred to McCrimmon [190, p. 202] or Meyberg [193].

Exercises

27.13. Let k be a commutative ring with $2 \in k^\times$. Prove:

(a) For every associative k-algebra A: The linear Jordan algebra A^+ is associative if and only if $[x, y] \in \mathrm{Cent}(A)$ for all $x, y \in A$.
(b) $\mathrm{Mat}_n(k)^+$ is a Jordan algebra that is not associative, for all $n \geq 2$, if $k \neq \{0\}$.

28 Para-quadratic algebras

Just as linear Jordan algebras fit naturally into the more general framework of arbitrary non-associative algebras, i.e., of modules (over a commutative ring) equipped with a binary operation that is linear in each variable, (quadratic) Jordan algebras to be investigated below fit naturally into the more general framework of what we call para-quadratic algebras—modules equipped with a binary operation that is quadratic in the first variable and linear in the second. It is the purpose of the present section to extend the language of (linear) non-associative algebras as explained in §7 to this modified setting.

Throughout we let k be an arbitrary commutative ring. With an eye on subsequent applications, we discuss the notion of a para-quadratic algebra only in the presence of a base point which serves as a "weak identity element".

28.1 The concept of a para-quadratic algebra. By a *para-quadratic algebra* over k we mean a k-module J together with a quadratic map

$$U\colon J \longrightarrow \mathrm{End}_k(J), \quad x \longmapsto U_x, \tag{1}$$

the *U-operator*, and a distinguished element $1_J \in J$, the *base point*, such that

$$U_{1_J} = \mathbf{1}_J. \tag{2}$$

We then write

$$\{xyz\} := U_{x,z}y = (U_{x+z} - U_x - U_z)y \qquad (x, y, z \in J) \tag{3}$$

for the associated trilinear *triple product*, and

$$x \circ y := \{x1_Jy\} \qquad (x, y \in J) \tag{4}$$

for the associated bilinear *circle product*. Note that the triple product (3) is symmetric in the outer variables, whence the circle product (4) is commutative. Moreover, $\{xyx\} = 2U_xy$ for all $x, y \in J$. Viewing (3) (resp. (4)) as a linear operator in z (resp. y), we obtain linear maps

$$V_{x,y}\colon J \longrightarrow J, \quad z \longmapsto \{xyz\}, \tag{5}$$

$$V_x := V_{x,1_J}\colon J \to J, \quad y \longmapsto x \circ y = \{x1_Jy\}. \tag{6}$$

that depend bilinearly on x, y (resp. linearly on x). We refer to the map $V\colon J \times J \to \mathrm{End}_k(J)$ defined by (5) as the *V-operator* of J. Most of the time,we simply write J for a para-quadratic algebra, its U-operator, base point, triple and circle product being understood. In keeping with our introductory promise, 1_J because of (2) may be regarded as a *weak identity element* for J.

If J and J' are para-quadratic algebras over k, a *homomorphism* from J to J' is defined as a k-linear map $\varphi\colon J \to J'$ preserving U-operators and base points in the sense that

$$\varphi(U_xy) = U_{\varphi(x)}\varphi(y), \quad \varphi(1_J) = 1_{J'} \tag{7}$$

for all $x, y \in J$. In this case, φ also preserves triple and circle products, so we have

$$\varphi(\{xyz\}) = \{\varphi(x)\varphi(y)\varphi(z)\}, \quad \varphi(x \circ y) = \varphi(x) \circ \varphi(y) \qquad (x, y, z \in J). \tag{8}$$

Summing up we obtain the category k-**paquad** of para-quadratic k-algebras.

28.2 Unital para-quadratic algebras. A para-quadratic algebra J over k is said to be *unital* if $x \circ y = \{1_Jxy\}$ for all $x, y \in J$. Since the triple product is symmetric in the outer variables, and because of (28.1.4), we then have

$$x \circ y = \{1_Jxy\} = \{x1_Jy\} = \{xy1_J\} \tag{1}$$

for all $x, y \in J$ and, in particular, $1_J \circ x = 2U_{1_J}x = 2x$. If J is unital, the weak identity element 1_J is called the *unit* or *identity element* of J.

For the rest of this section, we fix a para-quadratic algebra J over k.

28.3 Subalgebras. For $X, Y, Z \subseteq J$ we denote by U_XY (resp. $\{XYZ\}$) the additive subgroup of J generated by the expressions U_xy (resp. $\{xyz\}$) for $x \in X$, $y \in Y$, $z \in Z$. We say that J' is a *subalgebra* of J if $J' \subseteq J$ is a k-submodule satisfying $1_J \in J'$ and $U_{J'}J' \subseteq J'$. Then $\{J'J'J'\} + J' \circ J' \subseteq J'$ and there is a unique way of viewing J' as a para-quadratic k-algebra in its own right such that the inclusion $J' \to J$ is a homomorphism. This implies not only $1_{J'} = 1_J$ but also that the triple (resp. circle) product of J' is obtained from the triple (resp. circle) product of J via restriction.

28.4 Example. Let A be a flexible unital k-algebra, so we have $(xy)x = x(yx) =: xyx$ for all $x, y \in A$. Then the U-operator defined by

$$U_xy := xyx \qquad (x, y \in A) \tag{1}$$

and the unit element of A convert A into a para-quadratic k-algebra denoted by $A^{(+)}$. Triple and circle product of $A^{(+)}$ are given by

$$\{xyz\} = (xy)z + (zy)x = x(yz) + z(yx), \quad x \circ y = xy + yx \quad (x, y, z \in A). \tag{2}$$

In particular, the para-quadratic algebra $A^{(+)}$ is unital. Obviously, $(A^{\mathrm{op}})^{(+)} = A^{(+)}$.

28.5 Ideals. We say I is an *ideal* in J if it is a k-submodule satisfying the inclusion relations

$$U_IJ + U_JI + \{JJI\} \subseteq I. \tag{1}$$

In this case, there is a unique way of making the k-module $J' := J/I$ into a para-quadratic k-algebra such that the canonical map from J to J' is a homomorphism. Conversely, the kernel of any homomorphism of para-quadratic algebras is an ideal. Moreover, if I_1 and I_2 are ideals in J, then so is $I_1 + I_2$, and the standard isomorphism theorems of abstract algebra continue to hold in this modified setting.

28.6 Inner and outer ideals. There is a vague analogy between one-sided ideals in ring theory and the following notions for para-quadratic algebras. A k-submodule $I \subseteq J$ is said to be an *inner* (resp. an *outer*) *ideal* if

$$U_IJ \subseteq I \quad (\text{resp. } U_JI + \{JJI\} \subseteq I). \tag{1}$$

Thus a submodule of J is an ideal if and only if it is an inner and an outer

ideal. But the analogy to one-sided ideals goes only so far: for example, let $I \subseteq J$ be an outer ideal and $x \in I$, $y \in J$. The $2U_x y = \{xyx\} \in \{JJI\} \subseteq I$, and we conclude that, *if* $2 \in k^\times$*, then outer ideals of* J *are ideals.*

28.7 Direct products of ideals. Let $J_1, \dots, J_r$ be para-quadratic algebras over k. Then

$$J := J_1 \times \cdots \times J_r,$$

their direct product as a k-module, becomes a para-quadratic k-algebra, with U-operator and base point respectively given by

$$U_{(x_1,\dots,x_r)}(y_1, \dots, y_r) = (U_{x_1} y_1, \dots, U_{x_r} y_r), \quad 1_J = (1_{J_1}, \dots, 1_{J_r})$$

for $x_i, y_i \in J_i$, $1 \le i \le r$. It follows immediately from the definition that also the triple and circle product of J are carried out component-wise. In particular, J is unital if and only if J_i is unital, for each $i = 1, \dots, r$. Identifying $J_i \subseteq J$ canonically for $1 \le i \le r$, we clearly have $U_{J_i} J_j = \{0\}$ for $1 \le i, j \le r$, $i \ne j$ and $\{J_i J_j J_l\} = \{0\}$ for $1 \le i, j, l \le r$ unless $i = j = l$.

Conversely, let J be a any para-quadratic algebra over k and suppose that $I_1, \dots, I_r \subseteq J$ are ideals such that $J = I_1 \oplus \cdots \oplus I_r$ as a direct sum of submodules (i.e., of ideals). For all $i, j, l = 1, \dots, r$, this implies $U_{I_i} I_j = \{0\}$ unless $i = j$ and $\{I_i I_j I_l\} = \{0\}$ unless $i = j = l$. It follows that $I_1, \dots, I_r$ are para-quadratic k-algebras in their own right, and J identifies canonically with their direct product as para-quadratic algebras.

28.8 Powers. Let $x \in J$. We define the powers $x^n \in J$ for $n \in \mathbb{N}$ inductively by

$$x^0 := 1_J, \quad x^1 := x, \quad x^n := U_x x^{n-2} \qquad (n \in \mathbb{N}, n \ge 2). \tag{1}$$

It can be useful to note that, with this definition,

$$(x + y)^2 = x^2 + x \circ y + y^2$$

for all $x, y \in J$. We write

$$k[x] := \sum_{n \in \mathbb{N}} k x^n \tag{2}$$

for the submodule of J spanned by the powers of x. More generally, we define

$$k_r[x] := \sum_{n \ge r} k x^n \tag{3}$$

for $r \in \mathbb{N}$ as a submodule of $k[x]$. We say J is *power-associative at* x if

$$U_{x^m} x^n = x^{2m+n}, \quad \{x^m x^n x^p\} = 2x^{m+n+p} \tag{4}$$

for all $m, n, p \in \mathbb{N}$. This is easily seen to imply

$$(x^m)^n = x^{mn} \tag{5}$$

for all $m, n \in \mathbb{N}$, and that $k[x] \subseteq J$ is a para-quadratic subalgebra. We say J is *power-associative* if it is so at every element of J.

For example, let A be a unital flexible k-algebra as in 28.4. Then the powers of $x \in A$ are the same in A and $A^{(+)}$. In particular, if A is power-associative, then so is $A^{(+)}$ and conversely.

28.9 Idempotents. An element $c \in J$ is called an *idempotent* if $c^3 = c^2 = c$. This implies $c^n = c$ for all positive integers n, hence $k[c] = k1_J + kc$; in particular, J is power-associative at c. There are always the trivial idempotents 0 and 1_J but possibly no others. Two idempotents $c, d \in J$ are said to be *orthogonal*, written as $c \perp d$, if

$$U_c d = U_d c = \{ccd\} = \{ddc\} = c \circ d = 0. \tag{1}$$

Orthogonality of idempotents is obviously a symmetric relation. Moreover, $c \perp d$ is easily seen to imply that $c + d \in J$ is an idempotent. If $c \in J$ is an idempotent, then so is $1_J - c$, and the idempotents $c, 1_J - c$ are orthogonal.

Let A be a unital flexible k-algebra. Then the idempotents of A and $A^{(+)}$ are the same. Moreover, for two idempotents c, d in A to be orthogonal in $A^{(+)}$ it is necessary and sufficient that they be orthogonal in A, i.e., $cd = dc = 0$.

28.10 The multiplication algebra. The subalgebra of $\mathrm{End}_k(J)$ generated by the linear operators $U_x, V_{x,y}$ for $x, y \in J$ is called the *multiplication algebra* of J, denoted my $\mathrm{Mult}(J)$. Note by (28.1.2) that $\mathrm{Mult}(J)$ is a unital subalgebra of $\mathrm{End}_k(J)$, so $\mathbf{1}_J \in \mathrm{Mult}(J)$. We may view J canonically as a $\mathrm{Mult}(J)$-left module. Then the $\mathrm{Mult}(J)$-submodules of J are precisely the outer ideals of J.

28.11 Simplicity and division algebras. J is said to be *simple* if it is non-zero and has only the trivial ideals $\{0\}$ and J. We say J is *outer simple* if it is non-zero and the only outer ideals are $\{0\}$ and J. Note by 28.6 that simplicity and outer simplicity are equivalent notions if $2 \in k^\times$ but not in general, see Example 28.12 below. Note further by 28.10 that outer simplicity (and *not* simplicity) is equivalent to J being an irreducible $\mathrm{Mult}(J)$-module.

And finally, J is said to be a *division algebra* if it is non-zero and $U_x \colon J \to J$ is bijective for all nonzero elements $x \in J$. For example, let A be a unital flexible k-algebra. Then A is a division algebra in the sense of 8.6 if and only if $A^{(+)}$ is a para-quadratic division algebra. This follows immediately from (28.4.1), which thanks to flexibility may be written in operator form as $L_x R_x = U_x = R_x L_x$, so if, e.g., U_x is bijective, then L_x is surjective by the first equation and injective by the second.

We note that *para-quadratic division algebras have only the trivial inner ideals and, in particular, are simple.* Indeed, let I be a non-zero inner ideal in a para-quadratic division algebra J and pick $0 \neq x \in I$. Then U_x is bijective, which implies $J = U_x J \subseteq I$, and the assertion follows.

28.12 Example. Let $K \supset F$ be a purely inseparable field extension of characteristic 2 and exponent 1. Since K is a flexible division algebra over $k := F$, $K^{(+)}$ is a para-quadratic one, with U-operators $U_x y = x^2 y$ and triple product $\{xyz\} = 2xyz = 0$. Hence $K^{(+)}$ is a simple para-quadratic F-algebra. However, since $x^2 \in F$ for all $x \in K$, every F-subspace of K is an outer ideal of $K^{(+)}$. In particular, F is an outer ideal in $K^{(+)}$ that is neither $\{0\}$ nor K, so $K^{(+)}$ is not outer simple.

28.13 Scalar extensions. Giving a para-quadratic k-algebra amounts to the same as giving a k-module M, a quadratic-linear composition $g\colon M \times M \to M$ in the sense of Exc. 11.34, and a distinguished element $1 \in M$ such that $g(1, y) = y$ for all $y \in M$. Since scalar extensions of quadratic-linear maps exist, by Exc. 11.34, so do scalar extensions of para-quadratic algebras. More specifically, given $R \in k$-**alg**, the scalar extension of J from k to R, denoted by J_R, is the unique para-quadratic algebra over R living on the R-module J_R (base change of the k-module J from k to R) and characterized by the condition that

$$(U_x y)_R = U_{x_R} y_R, \quad 1_{J_R} = (1_J)_R$$

for all $x, y \in J$. It follows that the triple (resp. circle) product of J_R is the R-trilinear (resp. R-bilinear) extension of the triple (resp. circle) product of J. The standard properties enjoyed by the scalar extensions of k-modules or linear non-associative algebras over k (cf. 9.2) carry over to this modified setting without change.

28.14 The centroid. Due to the non-linear character of para-quadratic algebras, it seems impossible to define a meaningful analogue of the centre inside the algebras themselves. Instead, just as in the case of linear non-associative algebras without a unit (e.g., of Lie algebras, cf. Jacobson [135, Chap. X, §1]), one has to work inside their endomorphism algebras.

Accordingly, we define the *centroid* of J, denoted by $\mathrm{Cent}(J)$, as the set of all elements $a \in \mathrm{End}_k(J)$ such that, writing $ax := a(x)$ ($a \in \mathrm{End}_k(J)$, $x \in J$) for simplicity,

$$U_{ax} = a^2 U_x, \quad U_{ax,y} = a U_{x,y}, \quad a U_x = U_x a, \qquad (x, y \in J). \tag{1}$$

The difficulty with this definition is that one of the conditions imposed on the elements of the centroid is no longer linear in a, and hence it is not at

all clear whether $\mathrm{Cent}(J) \subseteq \mathrm{End}_k(J)$ is a submodule, let alone a commutative subalgebra. Before discussing this question any further, let us observe for $a \in \mathrm{Cent}(J)$ and $x, y \in J$ that

$$aU_{x,y} = U_{ax,y} = U_{x,ay} = U_{x,y}a \quad \text{and} \quad aV_{x,y} = V_{ax,y} = V_{x,ay} = V_{x,y}a. \tag{2}$$

These relations either follow by linearizing (1) or by straightforward verification, e.g., $aV_{x,y}z = aU_{x,z}y = U_{ax,z}y = V_{ax,y}z$ for $z \in J$. Note that, in view of (1), (2), the elements of the centroid behave "just like scalars" not only with respect to the U-operator but also with respect to the triple and circle product:

$$a\{xyz\} = \{(ax)yz\} = \{x(ay)z\} = \{xy(az)\}, \tag{3}$$

$$a(x \circ y) = (ax) \circ y = x \circ (ay) \tag{4}$$

for all $a \in \mathrm{Cent}(J)$, $x, y, z \in J$.

Our next aim will be to exhibit conditions under which the centroid becomes a commutative subalgebra (resp. a subfield) of the endomorphism algebra of J.

28.15 Proposition (cf. McCrimmon [184, Thm. 2])**.** *The following conditions are equivalent.*

(i) $\mathrm{Cent}(J)$ *is a commutative (unital) subalgebra of* $\mathrm{End}_k(J)$.
(ii) $\mathrm{Cent}(J)$ *is a (unital) subalgebra of* $\mathrm{End}_k(J)$.
(iii) $\mathrm{Cent}(J)$ *is an additive subgroup of* $\mathrm{End}_k(J)$.
(iv) The elements of $\mathrm{Cent}(J)$ *commute by pairs:* $[a, b] = 0$ *for all* $a, b \in \mathrm{Cent}(J)$.

Proof In (i), (ii), unitality is automatic since $\mathbf{1}_J \in \mathrm{Cent}(J)$.

(i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Obvious.

Before tackling the remaining implications (iii)$\Rightarrow$(iv)$\Rightarrow$(i), we claim, for all $a, b \in \mathrm{Cent}(J)$,

$$\begin{aligned} a + b \in \mathrm{Cent}(J) \quad &\Longleftrightarrow \quad \forall x \in J : \ U_{(a+b)x} = (a+b)^2 U_x \\ &\Longleftrightarrow \quad [a, b] = 0. \end{aligned} \tag{1}$$

Indeed, since the last two conditions of (28.14.1) are linear in a, the first equivalence in (1) is obvious. As to the second, we use (28.14.1), (28.14.2) and compute

$$\begin{aligned} U_{(a+b)x} - (a+b)^2 U_x &= U_{ax} + U_{ax,bx} + U_{bx} - a^2 U_x - (ab + ba)U_x - b^2 U_x \\ &= (2ab - ab - ba)U_x = [a, b]U_x, \end{aligned}$$

which by (28.1.2) is zero for all $x \in J$ if and only if $[a, b] = 0$. This completes the proof of (1).

(iii) $\Rightarrow$ (iv). This follows immediately from (1).

(iv) ⇒ (i). By (1) and (iv), we need only show that Cent(J) is closed under multiplication, so let $a, b \in \mathrm{Cent}(J)$. Then

$$U_{(ab)x} = a^2 U_{bx} = a^2 b^2 U_x = (ab)^2 U_x$$

since a and b by (iv) commute. Thus $ab \in \mathrm{Cent}(J)$. □

28.16 Central para-quadratic algebras. J is said to be *central* if the linear map $k \to \mathrm{End}_k(J)$, $\alpha \mapsto \alpha \cdot \mathbf{1}_J$, is injective with image Cent(J). In this case, $\mathrm{Cent}(J) \subseteq \mathrm{End}_k(J)$ is a unital subalgebra isomorphic to k. Conversely, suppose $\mathrm{Cent}(J) \subseteq \mathrm{End}_k(J)$ is a subalgebra, automatically unital and commutative by Prop. 28.15. Then the natural action of Cent(J) on J converts J into a central para-quadratic algebra over Cent(J), denoted by J_{cent} and called the *centralization* of J. See 8.4 for the analogous, but more elementary, concept in the context of linear non-associative algebras.

28.17 The extreme radical. We wish to show that, under some mild extra condition, the centroid of a simple para-quadratic algebra is a field. This extra condition is best understood in terms of the *extreme radical* of J, which is defined by

$$\mathrm{Rex}(J) := \{z \in J \mid U_z = U_{z,x} = 0 \ \text{ for all } x \in J\} \tag{1}$$

and obviously a submodule of J. In fact, the extreme radical of J agrees with the radical of the quadratic map $x \mapsto U_x$ as defined in 11.3.

28.18 Theorem (Schur's lemma, cf. McCrimmon [184, Thm. 3])**.** *The centroid of a simple para-quadratic algebra with zero extreme radical is a field.*

Proof Let $a, b \in \mathrm{Cent}(J)$ and $x, y \in J$. Then (28.14.1), (28.14.2) yield

$$\begin{aligned} U_{[a,b]x} &= U_{abx-bax} = U_{abx} - U_{abx,bax} + U_{bax} = a^2 U_{bx} - a U_{bx,ax} b + U_{ax} b^2 \\ &= a^2 U_x b^2 - 2a^2 U_x b^2 + a^2 U_x b^2 = 0 \end{aligned}$$

and

$$U_{[a,b]x,y} = U_{abx-bax,y} = a U_{x,y} b - a U_{x,y} b = 0.$$

Hence $[a, b]x \in \mathrm{Rex}(J) = \{0\}$, and we deduce from Prop. 28.15 that $\mathrm{Cent}(J) \subseteq \mathrm{End}_k(J)$ is a commutative unital subalgebra. It remains to show that its non-zero elements are invertible, so let $a \in \mathrm{Cent}(J)$ be non-zero. For $x, y, z \in J$ we have

$$U_{ax} y = a^2 U_x y \in \mathrm{Im}(a), \quad U_y ax = a U_y x \in \mathrm{Im}(a), \quad \text{and}$$
$$\{yz(ax)\} = a\{yzx\} \in \mathrm{Im}(a),$$

whence $\mathrm{Im}(a) \subseteq J$ is a non-zero ideal. Thus $\mathrm{Im}(a) = J$ by simplicity, and a is surjective. On the other hand, let $z \in I := \mathrm{Ker}(a)$. Then $a\{xyz\} = \{xy(az)\} = 0$ for all $x, y \in J$, forcing $\{JJI\} \subseteq I$. Similarly, $U_J I \subseteq I$. And finally, since a is surjective, $x = aw$ for some $w \in J$, which implies $aU_z x = aU_z aw = a^2 U_z w = U_{az} w = 0$, hence $U_z x \in I$. Thus $I \subset J$ is an ideal, and we conclude $I = \{0\}$. Summing up, we have shown that $a\colon J \to J$ is bijective. □

As a consequence of this result, *para-quadratic division k-algebras may always be viewed as para-quadratic algebras over some field $F \in k$-**alg** which induce their para-quadratic k-algebra structure by restriction of scalars.* Indeed, since they obviously have zero extreme radical, we arrive at the following more precise corollary.

28.19 Corollary. *Let J be a para-quadratic division k-algebra. Then $F := \mathrm{Cent}(J)$ is a field in k-**alg** and the centralization J_{cent} of J is a central para-quadratic division algebra over F.* □

Exercises

28.20. *Monomials and the nil radical in para-quadratic algebras.* Let J be a para-quadratic algebra over k. For $X \subseteq J$ and $m \in \mathbb{N}$ we define subsets $\mathrm{Mon}_m(X) \subseteq J$ by setting $\mathrm{Mon}_0(X) := \{1_J\}$, $\mathrm{Mon}_1(X) := X$ and by requiring that $\mathrm{Mon}_m(X)$ for $m > 1$ consist of all elements $U_y z$ with $y \in \mathrm{Mon}_n(X)$, $z \in \mathrm{Mon}_p(X)$, $n, p \in \mathbb{N}$, $n > 0$, $m = 2n+p$. The elements of

$$\mathrm{Mon}(X) := \bigcup_{m \in \mathbb{N}} \mathrm{Mon}_m(X)$$

are called *monomials* (in J) over X.

(a) Prove $\mathrm{Mon}_m(\{x\}) = \{x^m\}$ for all $x \in J$ and all $m \in \mathbb{N}$ if J is power-associative.

(b) An element $x \in J$ is said to be *nilpotent* if $0 \in \mathrm{Mon}(\{x\})$ is a monomial over $\{x\}$. We say $I \subseteq J$ is a *nil ideal* if it is an ideal consisting entirely of nilpotent elements. Prove that the image of a nilpotent element under a homomorphism of para-quadratic algebras is nilpotent, and that for ideals $I' \subseteq I$ in J, the ideal I is nil if and only if I' is nil and I/I' is a nil ideal in J/I'. Conclude that the sum of all nil ideals in J is a nil ideal, called the *nil radical* of J, denoted by $\mathrm{Nil}(J)$.

(c) Prove $\mathrm{Nil}(k)J \subseteq \mathrm{Nil}(J)$.

28.21. *Para-quadratic evaluation.* Let J be a para-quadratic algebra over k and $x \in J$ such that J is power-associative at x. We define the *evaluation* at $x \in J$ as the linear map $\varepsilon_x\colon k[\mathbf{t}] \to J$ determined by $\varepsilon_x(\mathbf{t}^n) = x^n$ for all $n \in \mathbb{N}$ and put $f(x) := \varepsilon_x(f)$ for all $f \in k[\mathbf{t}]$.

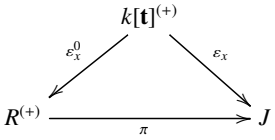
(a) Show that $\varepsilon_x\colon k[\mathbf{t}]^{(+)} \to J$ is a homomorphism of para-quadratic k-algebras and conclude that

$$I := I_x := \mathrm{Ker}(\varepsilon_x) := \{f \in k[\mathbf{t}] \mid f(x) = 0\}$$

is an ideal in $k[\mathbf{t}]^{(+)}$. Show further that

$$I^0 := I_x^0 := \mathrm{Ker}^0(\varepsilon_x) := \{f \in k[\mathbf{t}] \mid f(x) = (\mathbf{t}f)(x) = 0\}$$

is the unique largest ideal in $k[\mathbf{t}]$ contained in I. Moreover, both f^2 and $2f$ belong to I^0 for all $f \in I$. It follows that $R := k[\mathbf{t}]/I^0$ is a unital commutative associative k-algebra, and with the canonical projection $\varepsilon_x^0 \colon k[\mathbf{t}] \to R$, there is a unique homomorphism $\pi \colon R^{(+)} \to J$ of para-quadratic algebras making the diagram



commutative. In particular, $k[x] = \mathrm{Im}(\pi) \subseteq J$ is a para-quadratic subalgebra of J, and $a^2 = 2a = 0$ for all $a \in \mathrm{Ker}(\pi)$.

(b) Suppose $2 = 0$ in k and let $n \geq 2$ be an integer. Show that

$$I_n := k\mathbf{t}^n + \mathbf{t}^{n+2}k[\mathbf{t}]$$

is an ideal in $k[\mathbf{t}]^{(+)}$ but not in $k[\mathbf{t}]$. Conclude from the relations

$$x^{n+1} \neq 0 = x^n = x^{n+2} = x^{n+3} = \cdots$$

for the image x of $\mathbf{t}$ under the canonical projection $k[\mathbf{t}]^{(+)} \to J_n := k[\mathbf{t}]^{(+)}/I_n$ that J_n *has no linear structure*, i.e., there is no unital flexible algebra A over k satisfying $J_n \cong A^{(+)}$.

28.22. *Para-quadratic lifting of idempotents.* Let J be a para-quadratic algebra over k and $x \in J$ such that J is power-associative at x.

(a) For $v \in k[x]$, let $U'_v \colon k[x] \to k[x]$ be the restriction of U_x to $k[x]$. Prove

$$U'_{(fg)(x)} = U'_{f(x)}U'_{g(x)} \tag{1}$$

for all $f, g \in k[\mathbf{t}]$ and conclude

$$[U'_v, U'_w] = 0, \quad U'_{U_v w} = U'^2_v U'_w, \quad U'_{v^n} = U'^n_v \tag{2}$$

for all $v, w \in k[x]$ and all $n \in \mathbb{N}$.

(b) Assume there are integers $n > d > 0$ and scalars $\alpha_d, \ldots, \alpha_{n-1} \in k$ such that $\alpha_d \in k^\times$ and

$$\alpha_d x^d + \alpha_{d+1}x^{d+1} + \cdots + \alpha_{n-1}x^{n-1} + x^n = 0.$$

Show that there is a unique element $v \in k_{2d}[x]$ satisfying $U_{x^d}v = x^{2d}$. Conclude $U_v = \mathbf{1}$ on $k_{2d}[x]$ and that $c := v^2$ is an idempotent in $k_{2d}[x]$ satisfying $U_c = \mathbf{1}$ on $k_{2d}[x]$. (*Hint*: Apply Exc. 7.14 (a) and Exc. 28.21 (a).)

(c) Let $\varphi \colon J \to J'$ be a surjective homomorphism of power-associative para-quadratic algebras over k and suppose $\mathrm{Ker}(\varphi) \subseteq J$ is a nil ideal (Exc. 28.20). Conclude from (b) that every idempotent $c' \in J'$ can be lifted to J, i.e., there exists an idempotent $c \in J$ satisfying $\varphi(c) = c'$.

28.23 (Petersson-Racine [224, Lemma 3])**.** Let J be a para-quadratic algebra over k and $x \in J$. Show that, if J is power-associative at x, the following conditions are equivalent.

(i) x is nilpotent in the sense of Exc. 28.20 (b).
(ii) $x^m = 0$ for some positive integer m.
(iii) There exists a positive integer m such that $x^n = 0$ for all integers $n \geq m$.

Show further for the para-quadratic subalgebra $k[x] \subseteq J$ (cf. Exc. 28.21 (a)) that

$$\mathrm{Nil}(k[x]) = \{v \in k[x] \mid v \text{ is nilpotent}\}.$$

28.24. *The outer centroid.* Let J be a para-quadratic algebra over k and define the *outer centroid* of J, denoted by $\mathrm{Cent}_{\mathrm{out}}(J)$, as the centralizer of the multiplication algebra of J. We say J is *outer central* if the natural map $\alpha \mapsto \alpha \mathbf{1}_J$ from k to the outer centroid of J is an isomorphism. Prove:

(a) If J is outer simple, then its outer centroid is a(n associative) division ring.
(b) If k is a field and J is finite-dimensional and outer simple over k, then

$$\mathrm{End}_{\mathrm{Cent}_{\mathrm{out}}(J)}(J) = \mathrm{Mult}(J).$$

(c) Assume k is a field and J is finite-dimensional over k. Then J is outer central and outer simple if and only if it is non-zero and $\mathrm{Mult}(J) = \mathrm{End}_k(J)$.
(d) For a finite-dimensional para-quadratic algebra over a field, the following conditions are equivalent.
  (i) J is outer central and outer simple.
  (ii) Every base field extension of J is outer simple.
  (iii) The scalar extension of J to the algebraic closure of the base field is outer simple.

28.25. *Orthogonal systems of idempotents.* Let J be a para-quadratic algebra over k. A finite family $(c_1, \ldots, c_r)$ of elements in J is called an *orthogonal system of idempotents* if each c_i, $1 \leq i \leq r$, is an idempotent, and the following relations hold, for all $i, j, l = 1, \ldots, r$.

$$U_{c_i} c_j = \{c_i c_i c_j\} = c_i \circ c_j = 0 \quad (i \neq j), \quad \{c_i c_j c_l\} = 0 \quad (i, j, l \text{ mutually distinct}). \quad (1)$$

An orthogonal system $(c_1, \ldots, c_r)$ of idempotents in J is said to be *complete* if $\sum_{i=1}^r c_i = 1_J$. Prove:

(a) If $(c_1, \ldots, c_r)$ is an orthogonal system of idempotents in J, then $\sum_{i=1}^r c_i$ is an idempotent, and

$$(c_1, \ldots, c_r, 1_J - \sum_{i=1}^r c_i)$$

is a complete orthogonal system of idempotents in J.
(b) If $J = A^{(+)}$ for some unital flexible k-algebra A, then the (complete) orthogonal systems of idempotents in J and in A are the same.

29 Jordan algebras and basic identities

Experimental studies carried out by Jacobson in the 1950s suggest that the most promising way of extending the theory of linear Jordan algebras to arbi-

trary commutative rings from those where 2 is invertible consists in axiomatizing properties of the U-operator. The fruitfulness of this approach is underscored by the fact that the explicit formulas for the U-operator in our examples of linear Jordan algebras (Exc. 6.12 (b), (27.11.1), (27.11.2)), as opposed to the ones for the bilinear product ((5.3.1), 27.3, (27.9.1)), are defined over the integers and hence make sense over any commutative ring. Unfortunately, however, the question of which specific properties of the U-operator should be singled out as axioms remained a mystery for a long time. But then, in 1966, McCrimmon [181] introduced the concept of what he called a *quadratic Jordan algebra*. He showed that this concept is equivalent to the concept of a unital linear Jordan algebra over rings where 2 is invertible and that it gives rise to a far reaching structure theory, culminating eventually in the Zel'manov-McCrimmon enumeration [191] of non-degenerate prime quadratic Jordan algebras.

Our aim in the present section will be to define quadratic Jordan algebras (henceforth referred to simply as *Jordan algebras*) and to show that in the presence of $\frac{1}{2}$ they are categorically isomorphic to unital linear Jordan algebras. Using some basic identities, we derive a few elementary properties of Jordan algebras and extend the standard examples previously obtained in the linear case to the more general quadratic setting.

Throughout we let k be an arbitrary commutative ring. In deriving the elementary properties of Jordan algebras required in the present volume, we mostly follow Jacobson [140].

29.1 The concept of a Jordan algebra. By a *Jordan algebra* over k we mean a para-quadratic k-algebra J with U-operator U and base point 1_J satisfying the following identities in all scalar extensions:

$$U_{U_x y} = U_x U_y U_x, \tag{1}$$

$$U_x V_{y,x} = V_{x,y} U_x. \tag{2}$$

Equation (1) is called the *fundamental formula*. We write k-**jord** for the category of Jordan algebras over k, viewed as a full subcategory of k-**paquad**, the category of para-quadratic algebras over k. By definition, Jordan algebras remain stable under base change.

Let J be a Jordan algebra over k. The triple (resp. circle) product associated with J in its capacity as a para-quadratic algebra will be referred to as the *Jordan triple product* (resp. the *Jordan circle product*) of J. Setting $x = 1_J$ in (2) and observing (28.1.2), (28.1.6), we conclude $V_{1_J,x} = V_x$, hence $\{1_J xy\} = \{x1_J y\} = x \circ y$ for all $x, y \in J$. Thus *Jordan algebras are unital para-quadratic algebras.*

29.2 Basic identities. *Let J be a Jordan algebra over k. The identities listed in 29a on the facing page hold* strictly *in J, i.e., for all x, y, z, w in every scalar extension.*

Proof Since Jordan algebras are stable under base change, it suffices to verify these identities for all $x, y, z, u, v, w \in J$. Here (1), (5) hold since J is unital para-quadratic, while (2) and the first equation in (4) are valid by the definition of a Jordan algebra. Applying this part of (4) to z, viewing the result as a linear map acting on y, using the fact that the Jordan triple product is symmetric in the outer variables and writing again y for z, the second equation of (4) drops out. On the other hand, (3) follows immediately by linearizing (2) with respect to y. Fixing $y \in J$ and computing the first and second derivatives of both sides of the fundamental formula $U_{U_{xy}} = U_x U_y U_x$ with respect to x by means of the differential calculus 12.17, we obtain (6) and (7). Linearizing (6) (resp. (4)) with respect to x yields (8) (resp. (9)). Specializing y and z to 1_J in (7), we obtain $V_{x^2} + 4U_x = 2U_x + V_x^2$, hence (10). On the other hand, since Jordan algebras are unital para-quadratic, setting $y = 1_J$ in (4) yields (11). Next we put $x = 1_J$ in (9) and observe (5). Writing x for z, we end up with (12), which, when applied to z, amounts to

$$x \circ (y \circ z) + \{yxz\} = y \circ (x \circ z) + \{xyz\}.$$

Putting $z = x$ and applying (10) we conclude

$$x \circ (x \circ y) + U_{x,y}x = 2x^2 \circ y + 2U_x y = 2x^2 \circ y + x \circ (x \circ y) - x^2 \circ y.$$

Thus (13) holds, which linearizes to $\{xzy\} + \{zxy\} = (x \circ z) \circ y$ and yields (14) after interchanging x and y. Next we put $z = 1_J$ in (7) to obtain (15), while linearizing (11) yields (16). Applying this to y and using (13), we conclude

$$\begin{aligned} 2U_x y^2 + \{x(x \circ y)y\} &= x \circ \{xyy\} + y \circ (U_x y) = x \circ (x \circ y^2) + y \circ (U_x y) \\ &= V_x^2 y^2 + y \circ (U_x y). \end{aligned}$$

Now (10) yields with

$$\begin{aligned} y \circ (U_x y) &= \{x(x \circ y)y\} + (2U_x - V_x^2)y^2 = \{x(x \circ y)y\} - V_{x^2} y \\ &= \{x(x \circ y)y\} - x^2 \circ y^2 \end{aligned}$$

an equation whose right-hand side is symmetric in x and y. Hence so is the left, and we have proved (17). Linearizing gives

$$y \circ (U_x z) + z \circ (U_x y) = x \circ (U_{y,z} x) = x \circ (V_{y,x} z),$$

and viewing this as a linear map in z, we arrive at

$$V_{U_{xy}} = V_x V_{y,x} - V_y U_x. \tag{33}$$

$$U_{1_J} = \mathbf{1}_J, \tag{1}$$
$$U_{U_x y} = U_x U_y U_x, \tag{2}$$
$$U_{U_x y, U_x z} = U_x U_{y,z} U_x, \tag{3}$$
$$U_x V_{y,x} = V_{x,y} U_x = U_{x,U_x y}, \tag{4}$$
$$V_x = V_{1_J,x} = U_{1_J,x}, \tag{5}$$
$$U_{U_x y,\{xyz\}} = U_x U_y U_{x,z} + U_{x,z} U_y U_x, \tag{6}$$
$$U_{U_x y,U_z y} + U_{\{xyz\}} = U_x U_y U_z + U_z U_y U_x + U_{x,z} U_y U_{x,z} \tag{7}$$
$$U_{U_{x,w}y,U_{x,z}y} + U_{U_x y,U_{z,w}y} = U_{x,w} U_y U_{x,z} + U_x U_y U_{z,w} + U_{z,w} U_y U_x + U_{x,z} U_y U_{x,w}, \tag{8}$$
$$U_{x,z} V_{y,x} + U_x V_{y,z} = V_{z,y} U_x + V_{x,y} U_{x,z} = U_{z,U_x y} + U_{x,U_{x,z}y}, \tag{9}$$
$$2U_x = V_x^2 - V_{x^2}, \tag{10}$$
$$U_x V_x = V_x U_x = U_{x,x^2}, \tag{11}$$
$$V_x V_y + V_{y,x} = V_y V_x + V_{x,y}, \tag{12}$$
$$U_{x,y} x = \{xxy\} = x^2 \circ y, \tag{13}$$
$$U_{x,y} = V_x V_y - V_{x,y}, \tag{14}$$
$$U_{x\circ y} + U_{U_x y,y} = U_x U_y + U_y U_x + V_x U_y V_x, \tag{15}$$
$$U_x V_y + U_{x,y} V_x = V_x U_{x,y} + V_y U_x, \tag{16}$$
$$(U_x y) \circ y = x \circ (U_y x), \tag{17}$$
$$V_x V_{y,x} + U_x V_y = V_y U_x + V_{x,y} V_x, \tag{18}$$
$$V_{U_x y} = V_x V_{y,x} - V_y U_x = V_{x,y} V_x - U_x V_y, \tag{19}$$
$$V_{U_x y,y} = V_{x,U_y x}, \tag{20}$$
$$V_{U_x y,z} + V_{U_x z,y} = V_{x,\{yxz\}}, \tag{21}$$
$$U_{U_x y,z} = U_{x,z} V_{y,x} - V_{z,y} U_x = V_{x,y} U_{x,z} - U_x V_{y,z}, \tag{22}$$
$$V_{x,\{yxz\}} + U_x U_{y,z} = V_{x,y} V_{x,z} + V_{U_x z,y} = V_{x,z} V_{x,y} + V_{U_x y,z}, \tag{23}$$
$$V_{\{xyz\},y} = V_{x,U_y z} + V_{z,U_y x}, \tag{24}$$
$$V_{x,y} V_{z,y} = V_{x,U_y z} + U_{x,z} U_y, \tag{25}$$
$$V_{x,y} U_z + U_z V_{y,x} = U_{z,\{xyz\}}, \tag{26}$$
$$V_{x,y} V_{x,z} = V_{U_x y,z} + U_x U_{y,z}, \tag{27}$$
$$[V_{x,y}, V_{u,v}] = V_{\{xyu\},v} - V_{u,\{yxv\}}, \tag{28}$$
$$V_{U_x y,z} U_x = U_x V_{y,U_x z}, \tag{29}$$
$$V_{U_x y,z} V_{x,y} = U_x U_y V_{x,z} + V_{x,U_y U_x z}, \tag{30}$$
$$U_{\{xyz\}} + U_{U_x U_y z,z} = U_x U_y U_z + U_z U_y U_x + V_{x,y} U_z V_{y,x}, \tag{31}$$
$$U_{U_x U_y z,\{xyz\}} = U_x U_y U_z V_{y,x} + V_{x,y} U_z U_y U_x. \tag{32}$$

Table of Identities 29a Identities that hold strictly for every Jordan k-algebra J, i.e., that hold for every $x, y, z, w \in J_R$ for every $R \in k$-**alg**.

Setting $z = 1_J$ in (9), we obtain (18), which combines with (33) to imply (19). Using (14), (19) and (15), we can now compute

$$\begin{aligned} V_{U_x y,y} - V_{x,U_y x} &= V_{U_x y} V_y - U_{U_x y,y} - V_x V_{U_y x} + U_{x,U_y x} \\ &= (V_x V_{y,x} - V_y U_x) V_y - (U_x U_y + U_y U_x + V_x U_y V_x - U_{x \circ y}) \\ &\quad - V_x (V_{y,x} V_y - U_y V_x) + (U_y U_x + U_x U_y + V_y U_x V_y - U_{y \circ x}) \\ &= 0. \end{aligned}$$

This proves (20), which linearizes to (21). Applying this to $w \in J$, we obtain

$$\{(U_x y) z w\} + \{(U_x z) y w\} = \{x \{y x z\} w\},$$

which in turn may be viewed as a linear map in z and, writing z for w, yields the first equation of (22), while the second now follows from (9). We now apply (9) to u and obtain

$$\{x\{yxu\}z\} + U_x\{yzu\} = \{zy(U_x u)\} + \{xy\{xuz\}\} = \{zu(U_x y)\} + \{xu\{xyz\}\}.$$

Viewing this as a linear map in z and replacing u by z, we arrive at (23). Next we apply (20) to z and linearize the resulting equation, $\{(U_x y) y z\} = \{x (U_y x) z\}$, with respect to x:

$$\{\{xyw\}yz\} = \{w(U_y x)z\} + \{x(U_y w)z\}. \tag{34}$$

Viewing (34) as a linear map in z and replacing w by z gives (24), while viewing it as a linear map in w and interchanging x with z gives (25). Combining (22) with (9) and interchanging x with z, we obtain

$$V_{x,y} U_z + U_z V_{y,x} = U_{z,\{xyz\}},$$

hence (26). Combining (23) with (21) yields

$$V_{x,y} V_{x,z} + V_{U_x z,y} = V_{x,\{yxz\}} + U_x U_{y,z} = V_{U_x y,z} + V_{U_x z,y} + U_x U_{y,z},$$

hence (27). Linearizing (26) at z in the direction u and applying the result to v, we obtain

$$\{xy\{uvz\}\} + \{u\{yxv\}z\} = \{uv\{xyz\}\} + \{\{xyu\}vz\},$$

which, when viewed as a linear map in z, amounts to (28). Letting the left-hand side of (29) act on w and observing (3), we conclude

$$V_{U_x y,z} U_x w = U_{U_x y,U_x w} z = U_x U_{y,w} U_x z = U_x V_{y,U_x z} w,$$

and (29) is proved. Applying the left-hand side of (30) to w and observing (6) implies

$$V_{U_x y,z} V_{x,y} w = U_{U_x y,\{xyw\}} z = U_x U_y U_{x,w} z + U_{x,w} U_y U_x z = (U_x U_y V_{x,z} + V_{x,U_y U_x z}) w,$$

hence (30). Consulting (22), (27) and (22) again, we now compute

$$\begin{aligned} V_{x,y}U_zV_{y,x} &= U_{x,z}V_{y,z}V_{y,x} - U_{U_zy,x}V_{y,x} = U_{x,z}V_{U_yz,x} + U_{x,z}U_yU_{x,z} - U_{x,U_zy}V_{y,x} \\ &= U_{x,z}U_yU_{x,z} + U_{U_xU_yz,z} + V_{z,U_yz}U_x - U_{U_xy,U_zy} - V_{U_zy,y}U_x, \end{aligned}$$

which by (20) implies

$$V_{x,y}U_zV_{y,x} = U_{x,z}U_yU_{x,z} + U_{U_xU_yz,z} - U_{U_xy,U_zy},$$

hence combines with (7) to yield

$$\begin{aligned} U_{\{xyz\}} + U_{U_xU_yz,z} &= U_{\{xyz\}} + V_{x,y}U_zV_{y,x} + U_{U_xy,U_zy} - U_{x,z}U_yU_{x,z} \\ &= U_xU_yU_z + U_zU_yU_x + V_{x,y}U_zV_{y,x}, \end{aligned}$$

and this is (31). Finally, in order to derive (32), we linearize (6) with respect to y and obtain

$$U_{U_xu,\{xyz\}} + U_{U_xy,\{xuz\}} = U_xU_{y,u}U_{x,z} + U_{x,z}U_{y,u}U_x.$$

Here we replace u by U_yz. Then a computation involving (4), (20), (22) and (6) (with U_zy in place of z) yields

$$\begin{aligned} U_{U_xU_yz,\{xyz\}} &= U_xU_{y,U_yz}U_{x,z} + U_{x,z}U_{y,U_yz}U_x - U_{U_xy,\{x(U_yz)z\}} \\ &= U_xU_yV_{z,y}U_{x,z} + U_{x,z}V_{y,z}U_yU_x - U_{U_xy,\{xy(U_zy)\}} \\ &= U_xU_y(U_{U_zy,x} + U_zV_{y,x}) + (U_{U_zy,x} + V_{x,y}U_z)U_yU_x - U_{U_xy,\{xy(U_zy)\}} \\ &= U_xU_yU_zV_{y,x} + V_{x,y}U_zU_yU_x + U_xU_yU_{U_zy,x} + U_{x,U_zy}U_yU_z \\ &\quad -U_{U_xy,\{xy(U_zy)\}} \\ &= U_xU_yU_zV_{y,x} + V_{x,y}U_zU_yU_x, \end{aligned}$$

which completes the proof of (32). □

29.3 The connection with unital linear Jordan algebras. Assume that 2 is invertible in k. Let J be a unital linear Jordan algebra over k. Then its identity element and the U-operator (27.10.1) convert J into a para-quadratic algebra J^{quad}, which by the advanced identities (27.12.1), (27.12.6), (27.12.8) combined with the usual scalar extension argument (cf. Prop. 27.5) is a Jordan algebra.

Conversely, let J be a Jordan algebra over k Then the bilinear multiplication

$$xy := \frac{1}{2}U_{x,y}1_J = \frac{1}{2}\{x1_Jy\} = \frac{1}{2}V_xy$$

gives J the structure of a non-associative k-algebra J^{lin} with left multiplication operator $L_x = \frac{1}{2}V_x$ for $x \in J$. By definition and (29a.1), (29a.5), J^{lin} is commutative with identity element 1_J, and its squaring agrees with the one of J.

By (29a.11), the linear operators V_x, U_x commute, hence by (29a.10) so do V_x and V_{x^2}. This shows $[L_x, L_{x^2}] = 0$, and from (27.4.1) we conclude that J^{lin} is a unital linear Jordan algebra. One checks easily that the two constructions $J \mapsto J^{\mathrm{quad}}$ and $J \mapsto J^{\mathrm{lin}}$ are inverse to each other, and that a linear map between unital linear Jordan algebras is a homomorphism of unital linear Jordan algebras if and only if it is one of Jordan algebras. Summing up, we have thus proved the following result.

29.4 Theorem. *If $2 \in k^\times$, then the constructions presented in 29.3 yield inverse isomorphisms between the categories of unital linear Jordan algebras over k and Jordan algebras over k.* □

29.5 Convention. Assume that 2 is invertible in k. If there is no danger of confusion, we will always use Thm. 29.4 to identify Jordan algebras over k in the sense of 29.1 with unital linear Jordan algebras over k in the sense of 27.1; accordingly, the terms "unital linear Jordan algebra over k" and "Jordan algebra over k" will be used interchangeably. Note that under the preceding identification, the advanced identities 27.12 valid in linear Jordan algebras translate equivalently to appropriate identities in the long list of formulas in Figure 29a.

The reader may wonder why, in defining Jordan algebras over arbitrary base rings, we have insisted on an identity element. The reason is that removing this restriction would lead to an algebraic structure that would be computationally much more challenging. We refer to McCrimmon [186] for details.

29.6 Counter-examples: para-quadratic algebras. It should not come as a surprise that para-quadratic algebras which are not Jordan exist in abundance. Exhibiting explicit examples is of course another matter. Here is a whole class of them.

Let k be a commutative ring in which 2 is invertible and let J be a unital linear Jordan k-algebra with product xy. Since J is commutative, it is also flexible, so we can form the para-quadratic algebra $P := P(J) := J^{(+)}$ in the sense of 28.4, with U-operator $(xy)x = x(xy)$ and base point $1_P := 1_J$. We claim:

(∗) *P is a Jordan algebra if and only if J is alternative.*

Recall from Exc. 14.7 that commutative alternative algebras are associative if there is no 3-torsion. By Exc. 27.13 (b), therefore, $P(J)$ is para-quadratic but not Jordan for $J := \mathrm{Mat}_n(k)^+$, $n \geq 2$, $k \neq \{0\}$, $6 \in k^\times$.

Proof of (∗) If J is alternative, then the U-operator of J by (27.10.1) has the form $U_x y = 2x(xy) - x^2 y = x(xy)$, so $P = J^{\mathrm{quad}}$ in the sense of 29.3 is Jordan.

Conversely, assume P is a Jordan algebra. The Jordan triple product of P is given by $\{xyz\} = (xy)z + (zy)x$, which implies $x \circ y = \{x1_J y\} = 2xy$. By 29.3 again, $P^{\mathrm{lin}} = J$, hence $P = (P^{\mathrm{lin}})^{\mathrm{quad}} = J^{\mathrm{quad}}$, in other words, P and J have the same U-operator. But this means $x(xy) = 2x(xy) - x^2y$, i.e., $x(xy) = x^2y$. Thus, J is left alternative and hence alternative since it is commutative to begin with. □

29.7 Examples: associative algebras. Let A be a unital associative k-algebra. We claim that *the para-quadratic algebra $A^{(+)}$ of 28.4 with base point $1_{A^{(+)}} = 1_A$ and U-operator*

$$U_x y = xyx \qquad (x, y \in A) \tag{1}$$

is in fact a Jordan algebra. Indeed, since associativity is preserved by scalar extensions, it suffices to verify (29a.2) and (29a.4) over the base ring, so let $x, y, z \in A$. Then

$$\begin{aligned} U_{U_x y}z &= (xyx)z(xyx) = x(y(xzx)y)x = U_x U_y U_x z, \\ U_x V_{y,x}z &= x(yxz + zxy)x = xy(xzx) + (xzx)yx = V_{x,y}U_x z, \end{aligned}$$

as desired. Recall from (28.4.2) that the Jordan triple and circle products of $A^{(+)}$ are respectively given by

$$\{xyz\} = xyz + zyx, \quad x \circ y = xy + yx \tag{2}$$

for all $x, y \in A$. Recall further that, if $2 \in k$ is invertible, the identifications of 29.5 show $A^{(+)} = A^+$ as unital linear Jordan algebras over k.

29.8 Examples: associative algebras with involution. Let (B, τ) be an associative algebra with involution over k. By definition, B is unital and

$$H(B, \tau) = \{x \in B \mid \tau(x) = x\}$$

is obviously a subalgebra of $B^{(+)}$ and hence by Exc. 29.17 is a Jordan algebra.

Along slightly different lines, consider $\mathrm{Symd}(B, \tau)$. For $x, z \in B$, we have

$$x(z + \tau(z))\tau(x) = xz\tau(x) + \tau(xz\tau(x)) \in \mathrm{Symd}(B, \tau),$$

so $U_{\mathrm{Symd}(B,\tau)}\,\mathrm{Symd}(B, \tau) \subseteq \mathrm{Symd}(B, \tau)$. Therefore, if $1_J \in \mathrm{Symd}(B, \tau)$ (which holds, for example, if $2 \in k^\times$), then $\mathrm{Symd}(B, \tau)$ is a Jordan algebra. For any positive integer n, it follows that the k-module $\mathrm{Symp}_n(k)$ of (10.10.6) is a subalgebra of $\mathrm{Mat}_{2n}(k)^{(+)}$ and hence a Jordan algebra.

As another special case, if $(B, \tau) = (A \times A^{\mathrm{op}}, \varepsilon_A)$ as in 10.4, with ε_A the

exchange involution, then the diagonal embedding $A \to A \times A$ determines an isomorphism

$$A^{(+)} \xrightarrow{\sim} H(A \times A^{\mathrm{op}}, \varepsilon_A), \quad x \longmapsto (x, x), \tag{1}$$

of Jordan algebras.

29.9 Special and exceptional Jordan algebras. A Jordan algebra over k is said to be *special* if it is isomorphic to a subalgebra of $A^{(+)}$, for some unital associative k-algebra A. Otherwise, it is said to be *exceptional*. If $2 \in k^\times$, one checks easily that these notions are equivalent to the ones defined in 27.3 (a), which in turn agree with the definitions in 5.7 (a) when $k = \mathbb{R}$.

29.10 Examples: alternative algebras. Let A be a unital alternative k-algebra. Then the left Moufang identity (13.3.1) implies that the left multiplication of A,

$$L\colon A^{(+)} \longrightarrow \mathrm{End}_k(A)^{(+)}, \quad x \longmapsto L_x,$$

is a homomorphism of para-quadratic algebras and obviously injective. Hence $A^{(+)}$ *is a special Jordan algebra.* Recall that we have encountered the U-operator of $A^{(+)}$ already in 13.5, where it was referred to as the U-operator of A.

29.11 Examples: pointed quadratic modules. Assume (M, q, e) is a pointed quadratic module over k and write $x \mapsto \bar{x}$ for its conjugation. Then we claim that *the base point e and the quadratic map $x \mapsto U_x$ from M to* $\mathrm{End}_k(M)$ *given by*

$$U_x y := q(x, \bar{y})x - q(x)\bar{y} \qquad (x, y \in M) \tag{1}$$

give M the structure of a Jordan algebra over k. We denote this Jordan algebra $J := J(M, q, e)$ and call it the Jordan algebra of (M, q, e). To verify the claim, write t for the linear trace of (M, q, e), so that $U_e y = t(\bar{y})e - \bar{y} = t(y)e - (t(y)e - y) = y$ for all $y \in M$, hence $U_e = \mathbf{1}_M$. Thus J is a para-quadratic k-algebra. In order to show that this para-quadratic algebra is, in fact, a Jordan algebra, we first note that the construction of J out of (M, q, e) is compatible with base change, so it suffices to verify (29.1.1) and (29.1.2) over k. First of all, (1) implies

$$V_{x,y}z = \{xyz\} = q(x, \bar{y})z + q(z, \bar{y})x - q(x, z)\bar{y} \tag{2}$$

and a straightforward verification shows

$$q(U_x y) = q(x)^2 q(y), \tag{3}$$
$$q(U_x y, z) = q(x, \bar{y})q(x, z) - q(x)q(y, \bar{z}), \tag{4}$$
$$U_x \bar{x} = q(x)x, \tag{5}$$
$$V_{x,y} x = 2(q(x, \bar{y})x - q(x)\bar{y}). \tag{6}$$

Combining these identities with the fact that the conjugation leaves q invariant, we can now compute

$$\begin{aligned}
U_x U_y U_x z &= U_x U_y (q(x, \bar{z})x - q(x)\bar{z}) \\
&= U_x (q(x, \bar{z})q(y, \bar{x})y - q(x, \bar{z})q(y)\bar{x} - q(x)q(y, z)y + q(x)q(y)z) \\
&= q(x, \bar{y})q(x, \bar{z})q(x, \bar{y})x - q(x)q(x, \bar{y})q(x, \bar{z})\bar{y} - q(x)q(y)q(x, \bar{z})x \\
&\quad - q(x)q(y, z)q(x, \bar{y})x + q(x)q(y, z)q(x)\bar{y} \\
&\quad + q(x)q(y)q(x, \bar{z})x - q(x)q(y)q(x)\bar{z} \\
&= q(x, \bar{y})(q(x, \bar{y})q(x, \bar{z}) - q(x)q(y, z))x \\
&\quad - q(x)(q(x, \bar{y})q(x, \bar{z}) - q(x)q(y, z))\bar{y} - q(x)^2 q(y)\bar{z} \\
&= q(U_x y, \bar{z})(q(x, \bar{y})x - q(x)\bar{y}) - q(U_x y)\bar{z} \\
&= q(U_x y, \bar{z})U_x y - q(U_x y)\bar{z} = U_{U_x y} z.
\end{aligned}$$

Similarly,

$$\begin{aligned}
U_x V_{y,x} z &= U_x (q(y, \bar{x})z + q(z, \bar{x})y - q(y, z)\bar{x}) \\
&= q(x, \bar{y})q(x, \bar{z})x - q(x, \bar{y})q(x)\bar{z} \\
&\quad + q(x, \bar{z})q(x, \bar{y})x - q(x, \bar{z})q(x)\bar{y} - q(x)q(y, z)x \\
&= (2q(x, \bar{y})q(x, \bar{z}) - q(x)q(y, z))x - q(x)(q(x, \bar{y})\bar{z} + q(x, \bar{z})\bar{y}) \\
&= 2q(x, \bar{y})q(x, \bar{z})x - 2q(x)q(x, \bar{z})\bar{y} \\
&\quad - q(x)q(x, \bar{y})\bar{z} - q(x)q(\bar{z}, \bar{y})x + q(x)q(x, \bar{z})\bar{y} \\
&= V_{x,y}(q(x, \bar{z})x - q(x)\bar{z}) = V_{x,y} U_x z.
\end{aligned}$$

Thus (29.1.1) and (29.1.2) hold in J and the proof is complete.

Assuming $2 \in k^\times$ and exploiting the isomorphism between the categories of Jordan algebras and linear Jordan algebras as described in 29.3, we conclude from Example 27.11 that the linear Jordan algebra of a pointed quadratic k-module as defined in 27.9 identifies canonically with the Jordan algebra of the same pointed quadratic k-module as defined above.

29.12 The Jordan algebra of a pointed quadratic module: identities. Letting (M, q, e) be a pointed quadratic module over k, we maintain the notation

of 29.11. The identities in 29b are either easily verified or have been checked before, and are collected here for convenience. Note the analogy of these formulas with the ones of 16.5.

$$t(x) = q(e, x), \tag{1}$$
$$q(e) = 1, \quad t(e) = 2, \tag{2}$$
$$\bar{x} = t(x)e - x, \quad \bar{e} = e, \quad \bar{\bar{x}} = x, \tag{3}$$
$$t(x, y) = q(x, \bar{y}) = t(x)t(y) - q(x, y), \tag{4}$$
$$U_x y = q(x, \bar{y})x - q(x)\bar{y}, \tag{5}$$
$$x^2 = t(x)x - q(x)e, \tag{6}$$
$$x^3 = t(x)x^2 - q(x)x, \tag{7}$$
$$V_{x,y}z = \{xyz\} = q(x, \bar{y})z + q(\bar{y}, z)x - q(z, x)\bar{y}, \tag{8}$$
$$x \circ y = t(x)y + t(y)x - q(x, y)e, \tag{9}$$
$$U_x\bar{x} = q(x)x, \quad U_x\bar{x}^2 = q(x)^2 e, \quad x + \bar{x} = t(x)e, \tag{10}$$
$$q(\bar{x}) = q(x), \quad t(\bar{x}) = t(x), \quad t(\bar{x}, \bar{y}) = t(x, y), \tag{11}$$
$$q(U_x y) = q(x)^2 q(y), \quad q(x^n) = q(x)^n, \tag{12}$$
$$t(x^2) = t(x)^2 - 2q(x), \tag{13}$$
$$t(x \circ y) = 2(t(x)t(y) - q(x, y)), \tag{14}$$
$$t(U_x y, z) = t(y, U_x z), \tag{15}$$
$$t(\{xyz\}, w) = t(z, \{yxw\}), \tag{16}$$
$$\overline{U_x y} = U_{\bar{x}}\bar{y}. \tag{17}$$

Table of Identities 29b Some identities that hold in the Jordan algebra of a pointed quadratic module, valid for all $x, y, z \in J$ and all $n \in \mathbb{N}$.

The Jordan algebras of pointed quadratic modules are often referred to collectively as Jordan algebras *of Clifford type*.

29.13 Jordan algebras of Clifford type: elementary idempotents. Continue the notation of 11.14 and 29.12. Arguing as in Exc. 16.23, it follows that, for any element $c \in J := J(M, q, e)$, the following conditions are equivalent.

(i) c is an idempotent satisfying $c_R \neq 0, 1_{J_R}$ for all $R \in k$-**alg**, $R \neq \{0\}$.
(ii) c is an idempotent satisfying $c_\mathfrak{p} \neq 0, 1_{J_\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subseteq k$.
(iii) $q(c) = 0$ and $t(c) = 1$.
(iv) c is an idempotent and the elements $c, 1_J - c$ are unimodular.

If these conditions are fulfilled, we call c an *elementary* idempotent of J.

The description of arbitrary idempotents in J is exactly the same as the one in conic algebras provided by Exc. 16.26.

29.14 Quadratic $\mathbb{Z}$-structures as Jordan algebras. Let $\mathbb{D}$ be one of the subalgebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ of the Graves-Cayley octonions. We have seen in Thm. 5.10 that $J := \mathrm{Her}_3(\mathbb{D})$ is a unital linear Jordan algebra over $\mathbb{R}$ and hence may be viewed canonically as a real Jordan algebra by means of the identification 29.5. Now suppose $\Lambda \subseteq J$ is a quadratic $\mathbb{Z}$-structure of J. By its very definition (cf. 6.5), Λ is a $\mathbb{Z}$-subalgebra of J as a (quadratic) Jordan algebra. Hence Λ *is a quadratic Jordan algebra over $\mathbb{Z}$ in its own right but, in general, not a linear one.* For example, if M is a $\mathbb{Z}$-structure of $\mathbb{D}$ in the sense of 3.6 (d), then $\Lambda := \mathrm{Her}_3(M)$ by 6.3 is not closed under the bilinear Jordan product of J.

29.15 Towards power-associativity. We wish to show in analogy to Cor. 27.7 that Jordan algebras are power-associative. Combining the fundamental formula (29a.2) and its linearization (29a.3) with the recursive definition of powers in (28.8.1), we see by induction that any Jordan algebra J over k satisfies the identities

$$U_{x^n} = U_x^n, \quad U_x U_{x^m, x^n} U_x = U_{x^{m+2}, x^{n+2}} \tag{1}$$

for all $x \in J$ and all $m, n \in \mathbb{N}$.

29.16 Proposition. *Jordan algebras are power-associative: for all Jordan algebras J over k, all $x \in J$ and all $m, n, p \in \mathbb{N}$ we have*

$$U_{x^m} x^n = x^{2m+n}, \tag{1}$$

$$\{x^m x^n x^p\} = 2x^{m+n+p}. \tag{2}$$

In particular, $k[x] \subseteq J$ is a Jordan subalgebra.

Proof Equation (1) follows immediately from (29.15.1) by induction on m. Equation (2) will now be proved by induction on $l := m + n + p$. We first note that (2) follows from (1) for $m = p$ and is symmetric in m, p. Hence we may always assume if necessary that $m < p$. Moreover, (2) is obvious if two of the exponents m, n, p are zero. Summing up, not only the induction beginning $l = 0$ is trivial, but also the cases $l = 1, 2$ are. Let us now assume $l \geq 3$ and that (2) holds for all exponents $m', n', n' \in \mathbb{N}$ having $m' + n' + p' < l$. We consider the following cases.

Suppose first that $m = 0$. Then (2) amounts to $x^n \circ x^p = 2x^{n+p}$, hence is symmetric in n, p and obvious for $n = 0$ or $n = p$. Thus we may assume $1 \leq n < p$. But the assertion can also be written in the form $\{x^n 1_J x^p\} = 2x^{n+p}$, so we have reduced the proof to the case $m \geq 1$.

Suppose next that $m = 1$. Then $p \geq 2$, and (28.8.1), (29a.4) combine with the induction hypothesis to imply

$$\{xx^n x^p\} = V_{x,x^n} U_x x^{p-2} = U_x V_{x^n,x} x^{p-2} = U_x\{x^n x x^{p-2}\} = 2U_x x^{n+p-1} = 2x^{1+n+p},$$

as claimed.

Finally, suppose $m \geq 2$. Then $p > m \geq 2$ and the induction hypothesis combined with (29.15.1) yields

$$\begin{aligned}\{x^m x^n x^p\} &= U_{U_x x^{m-2}, U_x x^{p-2}} x^n = U_x U_{x^{m-2},x^{p-2}} U_x x^n = U_x\{x^{m-2} x^{n+2} x^{p-2}\} \\ &= 2U_x x^{m+n+p-2} = 2x^{m+n+p},\end{aligned}$$

which completes the induction. □

Exercises

29.17. Show for a para-quadratic algebra J over k that the following conditions are equivalent.

(i) J is a Jordan algebra.
(ii) The identities

$$U_{U_x y} = U_x U_y U_x, \tag{1}$$
$$U_x V_{y,x} = V_{x,y} U_x, \tag{2}$$
$$U_{U_x y, U_x z} y = U_x U_y U_{x,z} + U_{x,z} U_y U_x, \tag{3}$$
$$U_{U_x y, U_z y} + U_{U_{x,z} y} = U_x U_y U_z + U_z U_y U_x + U_{x,z} U_y U_{x,z}, \tag{4}$$
$$\begin{aligned} U_{U_{x,w} y, U_{x,z} y} + U_{U_x y, U_{z,w} y} &= U_{x,w} U_y U_{x,z} + U_x U_y U_{z,w} \\ &\quad + U_{z,w} U_y U_x + U_{x,z} U_y U_{x,w}, \end{aligned} \tag{5}$$
$$U_{x,z} V_{y,x} + U_x V_{y,z} = V_{z,y} U_x + V_{x,y} U_{x,z} \tag{6}$$

hold in J.
(iii) The identities (1), (2) hold in $J_{k[\mathbf{T}]}$, where $\mathbf{T} = (\mathbf{t}_i)_{i \geq 0}$ is a countably infinite family of indeterminates.

Conclude that subalgebras and homomorphic images of Jordan algebras (in the category k-**paquad**) are Jordan algebras.

29.18. Let J be a Jordan algebra over k. Show that

(a) a k-submodule $I \subseteq J$ is an outer ideal (resp. an ideal) if and only if $U_J I \subseteq I$ (resp. $U_I J + U_J I \subseteq I$),
(b) an element $c \in J$ is an idempotent if and only if $c^2 = c$,
(c) the extreme radical of J is an ideal. Conclude that the centroid of a simple Jordan algebra is a field.

29.19. Assume $2 \in k^\times$ and let J be a unital linear Jordan algebra over k. Show that the centroid of J^{quad} is a unital commutative associative subalgebra of $\text{End}_k(J)$ and that the left multiplication of J induces an isomorphism $\text{Cent}(J) \cong \text{Cent}(J^{\text{quad}})$.

29.20. Let J be a Jordan algebra over k and $q\colon J \to k$ a quadratic form with $q(1_J) = 1$, so that (M, q, e) is a pointed quadratic module over k, where M stands for the k-module underlying J and $e = 1_J$. Write t for the trace of (M, q, e) and prove that $J = J(M, q, e)$ if and only if the equations

$$x^2 - t(x)x + q(x)e = 0 = x^3 - t(x)x^2 + q(x)x \tag{1}$$

hold strictly in J.

29.21. Let (M, q, e) be a pointed quadratic module over k and $J = J(M, q, e)$ the corresponding Jordan algebra. Write t for the trace of (M, q, e) and show that an element $x \in J$ is nilpotent if and only if $t(x)$ and $q(x)$ are nilpotent elements of k. Conclude that

$$\mathrm{Nil}(J) = \{x \in M \mid q(x), q(x, y) \in \mathrm{Nil}(k) \text{ for all } y \in M\}.$$

29.22. (a) Suppose $2 = 0$ in k and consider the situation of Exc. 28.21 (b) for $n = 2$. Decide whether there exists a Jordan algebra J of Clifford type over k such that $J \cong J_2 = k[\mathbf{t}]^{(+)}/I_2$.

(b) Show that, over an appropriate commutative ring, there exists a Jordan algebra of Clifford type that contains an element x satisfying $x^2 = 0 \neq x^3$.

29.23. The functor ${}^{(+)}\colon k\text{-}\mathbf{alg} \to k\text{-}\mathbf{jord}$ is clearly a full embedding if $2 \in k^\times$. But show that this is not true in general.

29.24. Let $E := E_\Gamma$ from Example 24.20 and Exc. 25.46. Verify that the natural inclusion of ordinary groups $\mathrm{Aut}_{k\text{-}\mathbf{alg}}(E) \subseteq \mathrm{Aut}_{k\text{-}\mathbf{jord}}(E^{(+)})$ is an isomorphism.

Remark. It follows that the natural map of k-group schemes $\mathbf{Aut}(E) \to \mathbf{Aut}(E^{(+)})$ is an isomorphism.

29.25. Let C be a flexible conic algebra over k. Show that the para-quadratic algebra $C^{(+)}$ agrees with the Jordan algebra of the pointed quadratic module $(C, n_C, 1_C)$ if and only if C is alternative.

29.26. Let $k\text{-}\mathbf{poqua}_{\mathrm{inj}}$ be the category of pointed quadratic modules over k whose underlying k-modules are projective, with injective homomorphisms of pointed quadratic modules as morphisms, and similarly, let $k\text{-}\mathbf{jord}_{\mathrm{inj}}$ the category of Jordan algebras over k, with injective homomorphisms of para-quadratic algebras as morphisms. Prove that the assignment

$$(\varphi\colon (M, q, e) \longrightarrow (M', q', e')) \longmapsto (\varphi\colon J(M, q, e) \longrightarrow J(M', q', e'))$$

defines a faithful and full embedding from $k\text{-}\mathbf{poqua}_{\mathrm{inj}}$ to $k\text{-}\mathbf{jord}_{\mathrm{inj}}$.

29.27. Let (V, q, e) be a regular pointed quadratic module of dimension 3 over a field F of characteristic not 2. Show that there exist a quaternion algebra B over F and an involution τ of B such that $J(V, q, e) \cong H(B, \tau)$. Show further that (B, τ) is uniquely determined by this condition. (*Hint*: Use Exc. 19.39.)

30 Power identities

By showing in Cor. 27.7 that linear Jordan algebras over a commutative ring where 2 is invertible are power-associative, we derived what may be called a local property: every subalgebra on a single generator is associative. The proof of this result has been reduced to yet another property of linear Jordan algebras that, though no longer local, could at least be called "quasi-local": given any element x in a linear Jordan algebra J, the left multiplication operators of arbitrary elements in $k_1[x] \subseteq J$ acting on all of J commute by pairs.

The local property of a linear Jordan algebra to be power-associative has been extended to the setting of Jordan algebras in Prop. 29.16. It is the purpose of the present section to accomplish the same objective for the quasi-local analogue of this property alluded to above. More specifically, fixing a Jordan algebra J over an arbitrary commutative ring k throughout this section, the main result we wish to establish reads as follows.

30.1 Theorem. *Let $x \in J$. Then*

$$U_{(fg)(x)} = U_{f(x)} U_{g(x)}$$

for all $f, g \in k[\mathbf{t}]$.

30.2 Remark. The proof of this result given in Jacobson [140, Cor. 3.3.3] rests on a general principle [140, 3.3.1] that may be regarded as a weak version of Macdonald's theorem [140, Thm. 3.4.15]. The proof we are going to provide below will work instead with explicit and elementary manipulations of some of the basic identities in Figure 29a valid in arbitrary Jordan algebras.

30.3 A first reduction. In order to derive Thm. 30.1, we write the polynomials $f, g \in k[\mathbf{t}]$ in the form

$$f = \sum_{i \in \mathbb{N}} \alpha_i \mathbf{t}^i, \quad g = \sum_{m \in \mathbb{N}} \beta_m \mathbf{t}^m,$$

where the families $(\alpha_i)_{i \in \mathbb{N}}, (\beta_m)_{m \in \mathbb{N}} \in k^{\mathbb{N}}$ both have finite support. With $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$, this implies

$$fg = \sum_{(i,m) \in \mathbb{N}^2} \alpha_i \beta_m \mathbf{t}^{i+m},$$

hence

$$(fg)(x) = \sum_{(i,m) \in \mathbb{N}^2} \alpha_i \beta_m x^{i+m},$$

and endowing $\mathbb{N}^2$ with the lexicographic ordering, we apply (29.15.1) to obtain the expansion

$$\begin{aligned} U_{(fg)(x)} &= \sum_{(i,m)\in\mathbb{N}^2} \alpha_i^2\beta_m^2 U_x^{i+m} + \sum_{(i,m),(j,n)\in\mathbb{N}^2,(i,m)<(j,n)} \alpha_i\alpha_j\beta_m\beta_n U_{x^{i+m},x^{j+n}} \\ &= \sum_{i,m\in\mathbb{N}} \alpha_i^2\beta_m^2 U_x^{i+m} + \sum_{i,j,m,n\in\mathbb{N},i<j} \alpha_i\alpha_j\beta_m\beta_n U_{x^{i+m},x^{j+n}} \\ &\quad + \sum_{i,m,n\in\mathbb{N},m<n} \alpha_i^2\beta_m\beta_n U_{x^{i+m},x^{i+n}}. \end{aligned}$$

Thus we have

$$\begin{aligned} U_{(fg)(x)} = &\sum_{i,m\in\mathbb{N}} \alpha_i^2\beta_m^2 U_x^{i+m} + \sum_{i,m,n\in\mathbb{N},m<n} \alpha_i^2\beta_m\beta_n U_{x^{i+m},x^{i+n}} \\ &+ \sum_{i,j,m\in\mathbb{N},i<j} \alpha_i\alpha_j\beta_m^2 U_{x^{i+m},x^{j+m}} \\ &+ \sum_{i,j,m,n\in\mathbb{N},i<j,m<n} \alpha_i\alpha_j\beta_m\beta_n (U_{x^{i+m},x^{j+n}} + U_{x^{i+n},x^{j+m}}). \end{aligned} \tag{1}$$

On the other hand, from

$$f(x) = \sum_{i\in\mathbb{N}} \alpha_i x^i \quad \text{and} \quad g(x) = \sum_{m\in\mathbb{N}} \beta_m x^m$$

we deduce

$$\begin{aligned} U_{f(x)}U_{g(x)} &= \Big(\sum_{i\in\mathbb{N}} \alpha_i^2 U_x^i + \sum_{i,j\in\mathbb{N},i<j} \alpha_i\alpha_j U_{x^i,x^j}\Big)\Big(\sum_{m\in\mathbb{N}} \beta_m^2 U_x^m + \sum_{m,n\in\mathbb{N},m<n} \beta_m\beta_n U_{x^m,x^n}\Big) \\ &= \sum_{i,m\in\mathbb{N}} \alpha_i^2\beta_m^2 U_x^{i+m} + \sum_{i,m,n\in\mathbb{N},m<n} \alpha_i^2\beta_m\beta_n U_x^i U_{x^m,x^n} \\ &\quad + \sum_{i,j,m\in\mathbb{N},i<j} \alpha_i\alpha_j\beta_m^2 U_{x^i,x^j} U_x^m + \sum_{i,j,m,n,i<j,m<n} \alpha_i\alpha_j\beta_m\beta_n U_{x^i,x^j} U_{x^m,x^n}. \end{aligned}$$

Comparing this with (1), we see that Thm. 30.1 will be a consequence of the identities (30.4.5), (30.4.6) below.

30.4 Proposition. *For all $x \in J$ and all $i, j, m, n \in \mathbb{N}$, the following identities*

hold.

$$V_{x^{n+2}} = V_x^2 V_{x^n} - U_x V_{x^n} - V_x U_{x,x^n}, \tag{1}$$
$$U_{x,x^{n+2}} = U_x(V_x V_{x^n} - U_{x,x^n}), \tag{2}$$
$$V_{x^{n+1}} = V_x V_{x^n} - U_{x,x^n}, \tag{3}$$
$$V_{x^m,x^n} = V_{x^{m+n}}, \tag{4}$$
$$U_{x^i} U_{x^m,x^n} = U_{x^{i+m},x^{i+n}} = U_{x^m,x^n} U_{x^i}, \tag{5}$$
$$U_{x^i,x^j} U_{x^m,x^n} = U_{x^{i+m},x^{j+n}} + U_{x^{i+n},x^{j+m}}. \tag{6}$$

The proof of this result will be preceded by the following lemma.

30.5 Lemma. *For $x \in J$, the linear operators U_{x^i}, V_{x^j}, U_{x^m,x^n} $(i, j, m, n \in \mathbb{N})$ commute by pairs, and we have*

$$V_{x^{n+2}} = V_x V_{x^n} V_x - V_x U_{x,x^n} - V_{x^n} U_x, \tag{1}$$
$$U_{x,x^{n+2}} = U_x(V_{x^n} V_x - U_{x,x^n}) \tag{2}$$

for all $n \in \mathbb{N}$.

Proof We first apply (29a.19) to obtain $V_{x^{n+2}} = V_{U_x x^n} = V_x V_{x^n,x} - V_{x^n} U_x$ and (29a.14) yields (1). Similarly, since $U_{x,x^{n+2}} = U_{x,U_x x^n} = U_x V_{x^n,x}$ by (29a.4), another application of (29a.14) gives (2). It remains to prove

$$[U_{x^i}, U_{x^m,x^n}] = 0, \tag{3}$$
$$[U_{x^i,x^j}, U_{x^m,x^n}] = 0 \tag{4}$$

for all $i, j, m, n \in \mathbb{N}$ since $V_{x^j} = U_{x^j,1_J}$.

We begin with (3), note by symmetry and (29.15.1) that we may assume $i = 1$, $m < n$, and argue by induction on $l := m + n$. For $l = 0$, there is nothing to prove. For $l = 1$, we have $m = 0$, $n = 1$, and the assertion comes down to $[U_x, V_x] = 0$, which holds by (29a.11). Now suppose $l \geq 2$ and assume (3) holds for all natural numbers m', n' in place of m, n having $m' + n' < l$. Then we consider the following cases.

Suppose first that $m = 0$ and $n = l$. Then the assertion comes down to $[U_x, V_{x^l}] = 0$, which follows from (1) for $n = l-2$ and the induction hypothesis since, in particular, $[U_x, U_{x,x^{l-2}}] = 0$.

Suppose next that $0 < m < n$. Then $l \geq 3$. Here $m = 1$ implies $n = l - 1$, and the assertion comes down to $[U_x, U_{x,x^{l-1}}] = 0$, which follows from (2) for $n = l - 3$ since $[U_x, V_{x^{l-3}}] = 0 = [U_x, U_{x,x^{l-3}}]$ by the induction hypothesis. On the other hand, if $n > m \geq 2$, then (29a.3) gives $U_{x^m,x^n} = U_{U_x x^{m-2},U_x x^{n-2}} = U_x U_{x^{m-2},x^{n-2}} U_x$, and the assertion follows from the induction hypothesis. This completes the proof (3).

Turning to (4), we note that the assertion is symmetric in (i, j) and (m, n) and that, by (3), we may assume $i < j$, $m < n$. Now we argue by induction on $l := i + j + m + n$. The cases $l = 0, 1$ are obvious by what we have just noted, while for $l = 2$ we may assume $i = m = 0$, $j = n = 1$, in which case the assertion reduces to the triviality $[V_x, V_x] = 0$. Now let $l \geq 3$ and assume the assertion holds for all natural numbers i', j', m', n' in place of i, j, m, n having $i' + j' + m' + n' < l$. Then we consider the following cases.

Suppose first that $i = m = 0$. Then we have to show $[V_{x^j}, V_{x^n}] = 0$. For $j = 1$, hence $n = l - j \geq 2$, the assertion follows from (1) for $n - 2$ in place of n since the induction hypothesis implies $[V_x, U_{x,x^{n-2}}] = 0$. On the other hand, if $j \geq 2$, the assertion follows again from (1) (this time for $j - 2$ in place of n) since the induction hypothesis and (3) imply $[U_{x,x^{j-2}}, V_{x^n}] = [U_x, V_{x^n}] = 0$.

Suppose next that $i = m = 1$. This implies $j \geq 2$, and we have to show $[U_{x,x^j}, U_{x,x^n}] = 0$, which follows from (2) for $n = j - 2$ since the induction hypothesis implies $[V_{x^{j-2}}, U_{x,x^n}] = 0 = [U_{x,x^{j-2}}, U_{x,x^n}]$.

Suppose finally that $j > i \geq 2$, which is by symmetry the only remaining case. Then equation (29a.3) yields $U_{x^i,x^j} = U_{U_x x^{i-2}, U_x x^{j-2}} = U_x U_{x^{i-2},x^{j-2}} U_x$, which commutes with U_{x^m,x^n} by (3) and the induction hypothesis. □

Proof of Proposition 30.4 Combining the first part of Lemma 30.5 with equation (30.5.1), we obtain (30.4.1), while (30.4.2) agrees with (30.5.2).

Next we prove (30.4.5) for $i = 1$, $m = 0$, i.e.,

$$U_x V_{x^n} = U_{x,x^{n+1}}, \tag{5}$$

and (30.4.3) *simultaneously* by induction on n. Both equations are obvious for $n = 0$. Now suppose $n > 0$ and assume (30.4.3) and (5) both hold for all natural numbers $< n$. Then (30.4.2) for $n - 1$ in place of n and the induction hypothesis for (30.4.3) imply

$$U_{x,x^{n+1}} = U_x(V_x V_{x^{n-1}} - U_{x,x^{n-1}}) = U_x V_{x^n},$$

hence (5). Combining both parts of the induction hypothesis with (30.4.1) for $n - 1$ in place of n, we now obtain

$$V_x V_{x^n} - U_{x,x^n} = V_x^2 V_{x^{n-1}} - V_x U_{x,x^{n-1}} - U_x V_{x^{n-1}} = V_{x^{n+1}},$$

hence (30.4.3). This completes the proof of (30.4.3) and (5).

We are now in a position to prove (30.4.5), where (29.15.1) allows us to assume $i = 1$, and first deduce from Lemma 30.5 that it suffices to establish the first one of the two equations. By symmetry and (29.15.1) we may assume $m < n$ and then argue by induction on m. The case $m = 0$ has been settled in

(5). For $m > 0$, we apply (29a.3) and the induction hypothesis to conclude

$$U_{x^{m+1},x^{n+1}} = U_{U_x x^{m-1},U_x x^{n-1}} = U_x U_{x^{m-1},x^{n-1}} U_x = U_{x^m,x^n} U_x = U_x U_{x^m,x^n},$$

as claimed.

Turning to (30.4.4), we have by Lemma 30.5 that the linear operators V_{x^m}, V_{x^n} commute. Hence (29a.12) implies $V_{x^m,x^n} = V_{x^n,x^m}$, so our assertion is symmetric in m and n. We now argue by induction on m. For $m = 0$ there is nothing to prove. For $m = 1$, we apply (29a.14) and (30.4.3) to obtain $V_{x,x^n} = V_x V_{x^n} - U_{x,x^n} = V_{x^{n+1}}$, hence the assertion. Now suppose $m \geq 2$ and assume the assertion holds for all $m' \in \mathbb{N}$ in place of m satisfying $m' < m$. Combining (29a.21) with Prop. 29.16, the case $m = 1$ and the induction hypothesis, we deduce

$$\begin{aligned} V_{x^m,x^n} &= V_{U_x x^{m-2},x^n} = V_{x,\{x^{m-2}xx^n\}} - V_{U_x x^n,x^{m-2}} = 2V_{x,x^{m+n-1}} - V_{x^{n+2},x^{m-2}} \\ &= 2V_{x^{m+n}} - V_{x^{m-2},x^{n+2}} = 2V_{x^{m+n}} - V_{x^{m+n}} = V_{x^{m+n}}, \end{aligned}$$

and the proof of (30.4.4) is complete.

Finally, turning to (30.4.6), we may assume $i < j$ and $m < n$ by symmetry, Lemma 30.5 and (30.4.5). Then we argue by induction on $l := i + m$. For $l = 0$, i.e., $i = m = 0$, we have to prove $V_{x^j} V_{x^n} = V_{x^{j+n}} + U_{x^j,x^n}$. But $V_{x^j} V_{x^n} = U_{x^j,x^n} + V_{x^j,x^n}$ by (29a.14), and the assertion follows from (30.4.4). Next suppose $l = i+m > 0$ and assume (30.4.6) for all natural numbers i', j', m', n' in place of i, j, m, n satisfying $i'+m' < l$. Since U_{x^i,x^j} and U_{x^m,x^n} commute by Lemma 30.5, we may assume $i > 0$. Then (30.4.5) and the induction hypothesis yield

$$\begin{aligned} U_{x^i,x^j} U_{x^m,x^n} &= U_x U_{x^{i-1},x^{j-1}} U_{x^m,x^n} = U_x U_{x^{i+m-1},x^{j+n-1}} + U_x U_{x^{i+n-1},x^{j+m-1}} \\ &= U_{x^{i+m},x^{j+n}} + U_{x^{i+n},x^{j+m}}, \end{aligned}$$

which completes the induction and the proof of Prop. 30.4. □

With the proof of Prop. 30.4, we have also established Th. 30.1. The remainder of this section will be devoted to a useful application. We begin with an auxiliary result, where we use the notation already employed in Exc. 28.21.

30.6 Proposition. *For $x \in J$ and $R \in k$-**alg** such that $R = k[x]$ as k-modules, the following conditions are equivalent.*

(i) $R^{(+)} = k[x]$ *as Jordan algebras.*
(ii) *The powers of x in R and in J coincide.*
(iii) $f(x) = 0$ *implies* $(\mathbf{t}f)(x) = 0$, *for all* $f \in k[\mathbf{t}]$.
(iv) $I_x := \{f \in k[\mathbf{t}] \mid f(x) = 0\} \subseteq k[\mathbf{t}]$ *is an ideal.*
(v) $I_x^0 := \{f \in k[\mathbf{t}] \mid f(x) = (\mathbf{t}f)(x) = 0\}$ *equals* I_x.

If these conditions are fulfilled, then R is unique. In fact, the evaluation map $\varepsilon_x\colon k[\mathbf{t}] \to J$ of Exc. 28.21 (a) induces canonically an isomorphism

$$\bar{\varepsilon}_x\colon k[\mathbf{t}]/I_x \xrightarrow{\sim} R, \quad f + I_x \longmapsto f(x), \tag{1}$$

of unital commutative associative k-algebras.

Proof (i) $\Rightarrow$ (ii). By 28.4 and 28.8, the powers of x in R and $R^{(+)}$ coincide.

(ii) $\Rightarrow$ (iii). Denote the multiplication of R by juxtaposition. Assume $f = \sum \alpha_i \mathbf{t}^i \in k[\mathbf{t}]$ with $\alpha_i \in k$ satisfies $f(x) = 0$. From (ii) we deduce $(\mathbf{t}f)(x) = \sum \alpha_i x^{i+1} = x \sum \alpha_i x^i = xf(x) = 0$. Thus (iii) holds.

(iii) $\Rightarrow$ (v). We trivially have $I_x^0 \subseteq I_x$, while the reverse inclusion follows from (iii).

(v) $\Rightarrow$ (iv). By Exc. 28.21 (a), $I_x = I_x^0$ is an ideal in $k[\mathbf{t}]$. Thus (iv) holds.

(iv) $\Rightarrow$ (i). The evaluation $\varepsilon_x\colon k[\mathbf{t}] \to k[x]$ (Exc. 28.21) induces a k-linear bijection $\bar{\varepsilon}_x\colon k[\mathbf{t}]/I_x \to k[x]$. Let $R \in k\text{-}\mathbf{alg}$ be the unique k-algebra having $R = k[x]$ as k-modules and making $\bar{\varepsilon}_x\colon k[\mathbf{t}]/I_x \xrightarrow{\sim} R$ an isomorphism in $k\text{-}\mathbf{alg}$. But then $\bar{\varepsilon}_x$ is an isomorphism of Jordan algebras from $(k[\mathbf{t}]/I_x)^{(+)} = k[\mathbf{t}]^{(+)}/I_x$ not only to $R^{(+)}$ but also to $k[x] \subseteq J$. Hence (i) holds.

Uniqueness of R follows from the fact that it is spanned by the powers of x in J as a k-module. The rest is clear. □

30.7 Remark. The preceding arguments show that the proposition holds, more generally, for para-quadratic algebras that are power-associative at x.

30.8 Local linearity. Our Jordan algebra J is said to be *linear at* $x \in J$ if there exists a unital commutative associative k-algebra R, necessarily unique, such that $R = k[x]$ as k-modules and the equivalent conditions (i)–(v) of Prop. 30.6 hold. By abuse of language, we simply write $R = k[x]$ for this k-algebra and have

$$(fg)(x) = f(x)g(x) \qquad (f, g \in k[\mathbf{t}]). \tag{1}$$

Finally, we say J is *locally linear* if it is linear at x, for every $x \in J$.

30.9 Examples. (a) If $2 \in k^\times$, then every Jordan algebra over k is locally linear. This follows from Exc. 28.21 (a) combined with Prop. 30.6.

(b) Every special Jordan algebra is locally linear. Indeed, if A is a unital associative k-algebra and $J \subseteq A^{(+)}$ is a subalgebra, then for any $x \in J$ the meanings of $k[x]$ in J and in A are the same.

(c) There are Jordan algebras of Clifford type over appropriate base rings that are *not* locally linear (Exc. 29.22 (b)).

30.10 Absolute zero divisors. An element $x \in J$ is called an *absolute zero divisor* (in J) if $U_x = 0$. By abuse of language we say that J *has no absolute zero divisors* if $U_x = 0$ implies $x = 0$, for all $x \in J$, in other words, if 0 is the only absolute zero divisor of J.

30.11 Theorem (McCrimmon [184, Prop. 1])**.** *J is locally linear provided it has no absolute zero divisors.*

Proof Let $x \in J$ and $f \in I_x$ (cf. Prop. 30.6 (iii)). Then Thm. 30.1 implies $U_{(fg)(x)} = U_{f(x)}U_{g(x)} = 0$ for all $g \in k[\mathbf{t}]$, forcing $(fg)(x) = 0$ by hypothesis, hence $fg \in I_x$. Thus $I_x \subseteq k[\mathbf{t}]$ is an ideal, whence J is linear at x, by Prop. 30.6 (iii). Thus J is locally linear. □

Exercises

30.12. *Absolute zero divisors in Jordan algebras of Clifford type.* Let (M, q, e) be a pointed quadratic module over k and $J := J(M, q, e)$ the corresponding Jordan algebra of Clifford type.

(a) Show that if k is reduced, then $x \in J$ is an absolute zero divisor if and only if $x \in \mathrm{Rad}(q)$, i.e., $q(x) = q(x, y) = 0$ for all $y \in J$.
(b) Deduce from (a) that the absolute zero divisors of J are contained in the nil radical of J. Conclude that J is locally linear if $\mathrm{Nil}(J) = \{0\}$ but not in general.

30.13. *The Dickson condition for Jordan algebras over fields.* Let J be a Jordan algebra over a field F and assume J is *strictly locally linear*, i.e., J_K is locally linear over K, for every field extension K/F. Show that there exists a pointed quadratic module (M, q, e) over F such that $J = J(M, q, e)$ if and only if J satisfies the *Dickson condition*: for all field extensions K/F and all elements $x \in J_K$, the quantities $1_{J_K}, x, x^2$ are linearly dependent over K.

31 Inverses, isotopes and the structure group

The present section is devoted to three fundamental concepts that have dominated the theory of Jordan algebras since ancient times. To begin with, the notions of invertibility and inverses arise naturally out of the analogy connecting the U-operator of Jordan algebras with the left (or right) multiplication operator of associative algebras. Isotopes, on the other hand, have been discussed earlier for alternative algebras but unfold their full potential only in the setting of Jordan algebras. And, finally, the structure group derives its importance not only from the connection with isotopes but, more significantly, from the one with exceptional algebraic groups that will be discussed more fully in later portions of the book.

Throughout this section, we let k be a commutative ring and J, J', J'' be Jordan algebras over k.

31.1 The concept of invertibility. The idea of defining invertibility of an element in a linear Jordan algebra by properties (e.g., as in the alternative or associative case, by the bijectiveness) of its left multiplication operator is not a particularly useful one, see Exc. 31.36 below for details. Instead, it turns out to be much more profitable to do so by properties of the U-operator, an approach that has the additional advantage of making sense also for arbitrary Jordan algebras.

Accordingly, an element $x \in J$ is said to be *invertible* (in J) if there exists an element $y \in J$, called an *inverse* of x (in J), such that

$$U_x y = x, \quad U_x y^2 = 1_J. \tag{1}$$

We will see in a moment that an inverse of x in J, if it exists, is unique. More precisely, we can derive the following characterization of invertibility.

31.2 Proposition. *For $x \in J$, the following conditions are equivalent.*

(i) x *is invertible.*
(ii) U_x *is bijective.*
(iii) U_x *is surjective.*
(iv) $1_J \in \mathrm{Im}(U_x)$.

If these conditions hold, then x has a unique inverse, written as x^{-1} and given by

$$x^{-1} = U_x^{-1} x. \tag{1}$$

Proof (i) $\Rightarrow$ (ii). Let $y \in J$ be an inverse of x. Then (31.1.1) and the fundamental formula (29a.2) imply $U_x U_{y^2} U_x = \mathbf{1}_J$. Hence U_x, having a left and a right inverse in $\mathrm{End}_k(J)$, is bijective.

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv). Clear.

(iv) $\Rightarrow$ (ii). Let $z \in J$ satisfy $U_x z = 1_J$. Then $U_x U_z U_x = \mathbf{1}_J$, and as before it follows that U_x is bijective.

(ii) $\Rightarrow$ (i). Put $y := U_x^{-1} x \in J$. Then $U_x y = x$, $U_x U_y U_x = U_{U_x y} = U_x$, and since U_x is bijective, we conclude $U_y = U_x^{-1}$. Hence $U_x y^2 = U_x U_y 1_J = U_x U_x^{-1} 1_J = 1_J$. Thus (31.1.1) holds, and x is invertible with inverse y. Combining (31.1.1) with condition (ii), we see that the remaining assertions of the proposition also hold, □

31.3 Proposition. *Let $x, y \in J$.*

(a) If x is invertible, then so is x^{-1} and

$$(x^{-1})^{-1} = x, \quad U_{x^{-1}} = U_x^{-1}, \quad V_{x^{-1}} = U_x^{-1}V_x = V_xU_x^{-1}. \tag{1}$$

(b) x and y are both invertible if and only if U_xy is invertible. In this case,

$$(U_xy)^{-1} = U_{x^{-1}}y^{-1}. \tag{2}$$

Proof (a) From the fundamental formula and (31.1.1) we deduce $U_xU_{x^{-1}}U_x = U_{U_xx^{-1}} = U_x$, which implies $U_{x^{-1}} = U_x^{-1}$ since U_x is bijective by Prop. 31.2. Thus x^{-1} is invertible, and (31.2.1) yields $(x^{-1})^{-1} = U_{x^{-1}}^{-1}x^{-1} = U_xx^{-1} = x$. Finally, (29a.4) implies $U_xV_{x^{-1},x} = U_{x,U_xx^{-1}} = 2U_x$, hence $V_{x^{-1},x} = 2 \cdot \mathbf{1}_J$. Now (29a.19) yields $V_x = V_{U_xx^{-1}} = V_xV_{x^{-1},x} - V_{x^{-1}}U_x = 2V_x - V_{x^{-1}}U_x$, hence $V_x = V_{x^{-1}}U_x$ and, similarly, $V_x = U_xV_{x^{-1}}$. This completes the proof of (a).

(b) By Prop. 31.2, the element $U_xy \in J$ is invertible iff the linear map $U_{U_xy} = U_xU_yU_x$ is bijective iff so are U_x and U_y iff x and y are both invertible. In this case, (31.2.1) gives $(U_xy)^{-1} = U_{U_xy}^{-1}U_xy = U_x^{-1}U_y^{-1}U_x^{-1}U_xy = U_x^{-1}y^{-1}$, as claimed. □

31.4 The set of invertible elements. We write $J^\times$ for the set of invertible elements in J. By Prop. 31.3 (b), it contains the identity element and is closed under the para-quadratic operation $(x, y) \mapsto U_xy$. Note for a subalgebra $J' \subseteq J$ that, if an element $x \in J'$ is invertible in J', then it is so in J and the two inverses are the same.

We say that J is a *Jordan division algebra* if $J \neq \{0\}$ and all its non-zero elements are invertible, i.e., if $J^\times = J \setminus \{0\}$. Thanks to Prop. 31.2, this agrees with the notion of division algebra for para-quadratic algebras given in 28.11. When 2 is invertible, then we may also view J as a linear Jordan algebra and compare this notion of division algebra with the sense of 8.6. We find:

(a) For cubic Jordan algebras, a family that will be defined in 34.1 and includes Albert algebras, the two notions agree, see Exc. 46.24.

(b) For Jordan algebras that are not cubic, the two notions need not agree, as can be seen by combining Exc. 31.36 and Exc. 31.33.

The following result is an immediate consequence of the definitions.

31.5 Proposition. *If $\varphi\colon J \to J'$ is a homomorphism, then $\varphi(J^\times) \subseteq J'^\times$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in J^\times$.* □

31.6 Examples: alternative algebras. Let A be a unital alternative algebra over k. We claim that *an element $x \in A$ is invertible in the Jordan algebra $A^{(+)}$ if and only if it is so in A, in which case the two inverses coincide.* This follows

immediately from Propositions 13.6 and 31.2 since the U-operator of A in the sense of 13.5 is the same as the U-operator of $A^{(+)}$ in the sense of 28.4. In particular, *$A^{(+)}$ is a Jordan division algebra if and only if A is an alternative division algebra.*

31.7 Examples: associative algebras with involution. Let (B,τ) be an associative k-algebra with involution and $J := H(B,\tau)$ the Jordan algebra of τ-symmetric elements in B. For all $x \in B^\times$, we have $\tau(x) \in B^\times$ and $\tau(x)^{-1} = \tau(x^{-1})$. Hence *$x \in J$ is invertible in J if and only if it is so in B, in which case its inverses in J and B coincide.* In particular, *if B is an associative division algebra, then J is a Jordan division algebra.*

But the converse of this implication does not hold: let A be an associative division algebra and ε the exchange involution on $B := A \times A^{\mathrm{op}}$. Then $H(B,\varepsilon)$ is a Jordan division algebra by (29.8.1) and 31.6 but B is not an associative division algebra.

31.8 Isotopes. Let $p \in J$ be invertible. On the k-module J we define a new para-quadratic algebra over k, depending on p and written as $J^{(p)}$, by the U-operator $U^{(p)}\colon J \to \mathrm{End}_k(J)$, $x \mapsto U_x^{(p)} := U_x U_p$ and the base point $1_{J^{(p)}} := 1^{(p)} := p^{-1}$, which by (31.3.1) does indeed satisfy the relation $U^{(p)}_{1^{(p)}} = \mathbf{1}_{J^{(p)}}$. For $x,y,z \in J$, the triple and circle product associated with $J^{(p)}$ are given by $\{xyz\}^{(p)} = U^{(p)}_{x,z}y = U_{x,z}U_p y = \{x(U_p y)z\}$ and $x \circ^{(p)} y = \{x1^{(p)}y\}^{(p)} = \{x(U_p p^{-1})y\} = \{xpy\}$, respectively. Summing up, writing $V^{(p)}$ for the V-operator of $J^{(p)}$, we obtain the formulas

$$1_{J^{(p)}} = 1^{(p)} = p^{-1}, \tag{1}$$
$$U_x^{(p)} = U_x U_p, \tag{2}$$
$$U_{x,y}^{(p)} = U_{x,y} U_p, \tag{3}$$
$$\{xyz\}^{(p)} = \{x(U_p y)z\}, \tag{4}$$
$$x \circ^{(p)} y = \{xpy\}, \tag{5}$$
$$V_{x,y}^{(p)} = V_{x,U_p y}, \tag{6}$$
$$V_x^{(p)} = V_{x,p} \tag{7}$$

for all $x,y,z \in J$. The para-quadratic algebra $J^{(p)}$ is called the *p-isotope* (or simply *an* isotope) of J. Note that passing to isotopes is

(i) unital: $J^{(1_J)} = J$.

(ii) functorial: if $\varphi\colon J \to J'$ is a homomorphism, then $\varphi\colon J^{(p)} \to J'^{(\varphi(p))}$ is a homomorphism of para-quadratic algebras.

(iii) compatible with base change: $(J^{(p)})_R = (J_R)^{(p_R)}$ for all $R \in k$-**alg**.

For $n \in \mathbb{N}$, the n-th power of $x \in J$ performed in the p-isotope $J^{(p)}$ will be denoted by $x^{(n,p)}$. For example $x^{(2,p)} = U_x^{(p)} 1^{(p)} = U_x U_p p^{-1}$, hence

$$x^{(2,p)} = U_x p. \tag{8}$$

The first fundamental fact to be derived in the present context is that isotopes of Jordan algebras are Jordan algebras.

31.9 Theorem. *$J^{(p)}$ is a Jordan algebra over k, for all $p \in J^\times$.*

Proof Since passing to isotopes is compatible with base change (31.8 (iii)), it suffices to prove (29.1.1), (29.1.2) for $J^{(p)}$. Let $x, y \in J$. Then (29.1.1) for J and (31.8.2) imply

$$U^{(p)}_{U_x^{(p)} y} = U_{U_x U_p y} U_p = U_x U_p U_y U_p U_x U_p = U_x^{(p)} U_y^{(p)} U_x^{(p)},$$

hence (29.1.1) for $J^{(p)}$. In order to accomplish the same for the identity (29.1.2), we apply (29.1.2) and (29a.29), (31.8.2), (31.8.6) for J to conclude

$$\begin{aligned} U_p U_x^{(p)} V^{(p)}_{y,x} &= U_p U_x U_p V_{y,U_p x} = U_{U_p x} V_{y,U_p x} = V_{U_p x, y} U_{U_p x} = V_{U_p x, y} U_p U_x U_p \\ &= U_p V_{x,U_p y} U_x U_p = U_p V^{(p)}_{x,y} U_x^{(p)}, \end{aligned}$$

and canceling U_p yields (29.1.2) for $J^{(p)}$. □

31.10 Theorem. *Let $p \in J$ be invertible.*

(a) *An element $x \in J$ is invertible in $J^{(p)}$ if and only if it is so in J. In this case, its inverse in $J^{(p)}$ is given by $x^{(-1,p)} = U_p^{-1} x^{-1}$.*

(b) *Let $q \in J^{(p)\times} = J^\times$. Then $(J^{(p)})^{(q)} = J^{(U_p q)}$.*

Proof (a) The first part follows immediately from (31.8.2) combined with Prop. 31.2. Moreover, applying (31.2.1) to $J^{(p)}$ and J, we conclude

$$x^{(-1,p)} = U_x^{(p)-1} x = U_p^{-1} U_x^{-1} x = U_p^{-1} x^{-1},$$

as claimed.

(b) From (31.8.1) and (a) we deduce $(1^{(p)})^{(q)} = q^{(-1,p)} = U_{p^{-1}} q^{-1} = (U_p q)^{-1} = 1^{(U_p q)}$. Moreover, for $x \in J$ we apply (31.8.2) repeatedly and obtain

$$(U^{(p)})^{(q)}_x = U_x^{(p)} U_q^{(p)} = U_x U_p U_q U_p = U_x U_{U_p q} = U_x^{(U_p q)}.$$

Summing up, we have proved (b). □

31.11 Corollary. *Setting $p^{-2} := (p^{-1})^2$, we have $(J^{(p)})^{(p^{-2})} = J$ for all $p \in J^\times$.*

Proof $(J^{(p)})^{(p^{-2})} = J^{(U_p (p^{-1})^2)} = J$ by (31.1.1). □

31.12 Example. For $p \in J^\times$ and I an ideal in J, the subset I of $J^{(p)}$ is also an ideal in $J^{(p)}$. To see this, one can examine each term on the left side of (28.5.1), for example:

$$\{JJI\}^{(p)} = \{J(U_pJ)I\} = \{JJI\} \subseteq I.$$

In view of Cor. 31.11, the ideals of J and $J^{(p)}$ are the same. In particular, *J is simple if and only if $J^{(p)}$ is.*

31.13 Examples: alternative algebras. Let A be a unital alternative algebra over k and $p \in A^{(+)\times} = A^\times$ (31.6). Writing R_p for the right multiplication operator of p in A, we claim that

$$R_p \colon A^{(+)(p)} \xrightarrow{\sim} A^{(+)} \tag{1}$$

is an isomorphism of Jordan algebras. Indeed, $R_p 1_{A^{(+)(p)}} = R_p p^{-1} = 1_{A^{(+)}}$, so R_p preserves identity elements. Moreover, letting $x, y \in A$ and applying (13.5.4), we obtain

$$R_p U_x^{(p)} y = R_p U_x U_p y = R_p U_x L_p R_p y = U_{xp} R_p y = U_{R_p x} R_p y,$$

hence the assertion.

In particular, we can now conclude that *isotopes of special Jordan algebras are special.* Indeed, if J is special, then there exists a unital associative algebra A over k and an injective homomorphism $\varphi \colon J \to A^{(+)}$. Therefore we deduce for $p \in J^\times$ that φ is also an injective homomorphism from $J^{(p)}$ to $A^{(+)(\varphi(p))} \cong A^{(+)}$. Thus $J^{(p)}$ is special.

31.14 The connection with isotopes of alternative algebras. Let A be a unital alternative algebra over k and $p, q \in A^\times$. Consulting (15.5.1) and Prop. 15.6, we conclude

$$A^{(p,q)(+)} = A^{(+)(pq)}. \tag{1}$$

In particular, as is already implicit in Lemma 15.10, passing to unital isotopes of alternative algebras does not change the Jordan structure:

$$A^{p(+)} = A^{(+)} \qquad (p \in A^\times). \tag{2}$$

31.15 Examples: associative algebras with involution. Let (B, τ) be an associative k-algebra with involution and $p \in H(B,\tau)^\times = H(B,\tau) \cap B^\times$ (31.7).Then it follows from Prop. 43.7 that

$$\tau^p \colon B \longrightarrow B, \quad x \longmapsto \tau^p(x) := p^{-1}\tau(x)p \tag{1}$$

is an involution of B satisfying

$$H(B, \tau^p) = H(B, \tau)p. \tag{2}$$

In view of 31.13, we therefore conclude that

$$R_p \colon H(B, \tau)^{(p)} \xrightarrow{\sim} H(B, \tau^p) \tag{3}$$

is an isomorphism of Jordan algebras that fits into the commutative diagram

$$\begin{array}{ccc} B^{(+)(p)} & \xrightarrow[R_p]{\cong} & B^{(+)} \\ \uparrow & & \uparrow \\ H(B, \tau)^{(p)} & \xrightarrow[R_p]{\cong} & H(B, \tau^p). \end{array}$$

31.16 Remark. The second fundamental fact to be observed in the present context is that isotopes of J, though they are always Jordan algebras, will in general not be isomorphic to J. For examples along these lines, see Exc. 31.34 (d), (e) below.

31.17 Homotopies. Homotopies of Jordan algebras are homomorphisms into appropriate isotopes. More precisely, a *homotopy* from J to J' is a map $\eta \colon J \to J'$ such that $\eta \colon J \to J'^{(p')}$ is a homomorphism, for some $p' \in J'^{\times}$. In this case, Prop. 31.5 and Thm. 31.10 (a) imply $\eta(J^{\times}) \subseteq J'^{(p')\times} = J'^{\times}$, and p' is uniquely determined since $\eta(1_J) = 1_{J'^{(p')}} = p'^{-1}$, hence

$$p' = \eta(1_J)^{-1}. \tag{1}$$

In Prop. 31.18 (c) we will see that compositions of homotopies are homotopies. Hence Jordan k-algebras under homotopies form a category, denoted by k-$\mathbf{jord}_{\mathrm{hmt}}$. By (d) of the same proposition, the isomorphisms in this category are precisely the bijective homotopies and are called *isotopies*. The isotopies from J to itself are called *autotopies*.

31.18 Proposition. *(a) $\eta \colon J \to J'$ is a homomorphism if and only if η is a homotopy preserving identity elements: $\eta(1_J) = 1_{J'}$.*

(b) Let $p \in J^{\times}$, $p' \in J'^{\times}$. Then $\eta \colon J \to J'$ is a homotopy if and only if $\eta \colon J^{(p)} \to J'^{(p')}$ is a homotopy.

(c) If $\eta \colon J \to J'$ and $\eta' \colon J' \to J''$ are homotopies, then so is $\eta' \circ \eta \colon J \to J''$.

(d) If $\eta \colon J \to J'$ is a bijective homotopy, then so is $\eta^{-1} \colon J' \to J$.

Proof (a) A homomorphism is a homotopy preserving units. Conversely, let $\eta \colon J \to J'$ be a homotopy preserving units. By (31.17.1), therefore, $\eta \colon J \to J'^{(p')}$ is a homomorphism, with $p' = \eta(1_J)^{-1} = 1_{J'}$.

(b) Assume first that $\eta\colon J \to J'$ is a homotopy. Then some $q' \in J'^{\times}$ makes $\eta\colon J \to J'^{(q')}$ a homomorphism. Hence a repeated application of Thm. 31.10 (b) implies that so is $\eta\colon J^{(p)} \to J'^{(p')(q'_1)}$, with $q'_1 = U_{p'^{-1}} U_{q'} \eta(p)$. Thus $\eta\colon J^{(p)} \to J'^{(p')}$ is a homotopy. Conversely, if $\eta\colon J^{(p)} \to J'^{(p')}$ is a homotopy, then what we have just shown implies that so is $\eta\colon J = J^{(p)(p^{-2})} \to J'^{(p')(p'^{-2})} = J'$.

(c) Some $p' \in J'^{\times}$ makes $\eta\colon J \to J'^{(p')}$ a homomorphism. But $\eta'\colon J'^{(p')} \to J''$ is a homotopy by (a), so some $p'' \in J''^{\times}$ makes $\eta'\colon J'^{(p')} \to J''^{(p'')}$ a homomorphism. Hence so is $\eta' \circ \eta\colon J \to J''^{(p'')}$, implying (c).

(d) For some $p' \in J'^{\times}$, $\eta\colon J \to J'^{(p')}$ is an isomorphism. Hence so is $\eta^{-1}\colon J'^{(p')} \to J$, and (b) shows that $\eta^{-1}\colon J' \to J$ is a bijective isotopy. □

31.19 Proposition. *For all linear maps $\eta\colon J \to J'$, the following conditions are equivalent.*

(i) *η is an isotopy from J to J'.*

(ii) *η is bijective and there exists a bijective linear map $\eta^\sharp\colon J' \to J$ such that*

$$U_{\eta(x)} = \eta U_x \eta^\sharp \tag{1}$$

for all $x \in J$.

In this case, $\eta^\sharp$ is uniquely determined and satisfies

$$\eta^\sharp = \eta^{-1} U_{\eta(1_J)}. \tag{2}$$

Proof The final assertion follows immediately from (1) for $x = 1_J$.

(i) ⇒ (ii). Some $p' \in J'^{\times}$ makes $\eta\colon J \to J'^{(p')}$ an isomorphism. For $x, y \in J$ we therefore conclude $\eta(U_x y) = U^{(p')}_{\eta(x)} \eta(y) = U_{\eta(x)} U_{p'} \eta(y)$, hence $\eta U_x = U_{\eta(x)} U_{p'} \eta$, and we obtain (1) by setting $\eta^\sharp := \eta^{-1} U_{p'^{-1}}$.

(ii) ⇒ (i). If $x \in J$ is invertible, then so is $\eta(x) \in J'$, by (1). In particular, $p' := \eta(1_J)^{-1} \in J'^{\times}$. Then $\eta(1_J) = p'^{-1}$ and (1) yields $U_{p'} = U^{-1}_{\eta(1_J)} = (\eta\eta^\sharp)^{-1} = \eta^{\sharp -1} \eta^{-1}$. Applying (1) once more, we therefore deduce

$$U^{(p')}_{\eta(x)} \eta(y) = U_{\eta(x)} U_{p'} \eta(y) = \eta U_x \eta^\sharp \eta^{\sharp -1} \eta^{-1} \eta(y) = \eta(U_x y)$$

for all $x, y \in J$. Thus $\eta\colon J \to J'^{(p')}$ is an isomorphism, making $\eta\colon J \to J'$ an isotopy. □

31.20 The structure group. The group of autotopies of J is denoted by $\mathrm{Str}(J)$ and called the *structure group* of J. By Prop. 31.19 for $J' = J$, it consists of all $\eta \in \mathrm{GL}(J)$ such that there exists an $\eta^\sharp \in \mathrm{GL}(J)$ satisfying

$$U_{\eta(x)} = \eta U_x \eta^\sharp \tag{1}$$

for all $x \in J$. Combining this with the fundamental formula (29.1.1) and Prop. 31.2, we see that $U_x \in \mathrm{Str}(J)$ for all $x \in J^\times$; in fact, we then have $U_x^\sharp = U_x$. The subgroup of $\mathrm{Str}(J)$ generated by the linear operators U_x, $x \in J^\times$, is called the *inner structure group* of J, denoted by $\mathrm{Instr}(J)$. Combining (1) with (31.19.2), we obtain $\eta U_x \eta^{-1} = U_{\eta(x)} U_{\eta(1_J)^{-1}}$ for all $\eta \in \mathrm{Str}(J)$ and all $x \in J^\times$. Thus $\mathrm{Instr}(J) \subseteq \mathrm{Str}(J)$ is actually a *normal* subgroup. Note that $\alpha 1_J$ for $\alpha \in k^\times$ belongs to the structure group of J, but not necessarily to the inner one, unless $\alpha \in k^{\times 2}$. Finally, it will follow from Cor. 31.21 below that $\eta \in \mathrm{Str}(J)$ implies $\eta^\sharp \in \mathrm{Str}(J)$, and the assignment $\eta \mapsto \eta^\sharp$ determines an involution of $\mathrm{Str}(J)$, i.e., an anti-automorphism of period 2; for more on this, see Exc. 40.18 below.

31.21 Corollary. *If $\eta\colon J \to J'$ and $\eta'\colon J' \to J''$ are isotopies, then $(\eta' \circ \eta)^\sharp = \eta^\sharp \circ (\eta')^\sharp$. Moreover, $\eta^\sharp\colon J' \to J$ is an isotopy and $\eta^{\sharp\sharp} = \eta$.*

Proof For the first part we compute $U_{(\eta'\eta)(x)} = \eta' U_{\eta(x)} (\eta')^\sharp = \eta' \eta U_x \eta^\sharp (\eta')^\sharp$ for $x \in J$ and apply Prop. 31.19. Combining 31.20 with (31.19.1), we now see that $\eta^\sharp$ is an isotopy and $\eta^{\sharp\sharp} = U_{\eta(1_J)} \eta^{\sharp -1} = U_{\eta(1_J)} U_{\eta(1_J)}^{-1} \eta = \eta$. □

31.22 Theorem. *(a) Both the structure group and the inner structure group remain unchanged when passing to isotopes:*

$$\mathrm{Str}(J^{(p)}) = \mathrm{Str}(J), \quad \mathrm{Instr}(J^{(p)}) = \mathrm{Instr}(J) \qquad (p \in J^\times). \tag{1}$$

(b) The natural action of the structure group of J on J stabilizes $J^\times$, and we have

$$\eta(x)^{-1} = \eta^{\sharp -1}(x^{-1}) \qquad (\eta \in \mathrm{Str}(J),\ x \in J^\times). \tag{2}$$

(c) The stabilizer of 1_J in $\mathrm{Str}(J)$ is $\mathrm{Aut}(J)$, the automorphism group of J.

(d) For $p, q \in J^\times$ and $\eta \in \mathrm{End}_k(J)$, the following conditions are equivalent.

- *(i)* $\eta\colon J^{(p)} \to J^{(q)}$ *is an isomorphism.*
- *(ii)* $\eta \in \mathrm{Str}(J)$ *and* $\eta(p^{-1}) = q^{-1}$.
- *(iii)* $\eta \in \mathrm{Str}(J)$ *and* $\eta^\sharp(q) = p$.

Proof (a) follows immediately from Prop. 31.18 (b) and (31.8.2).

(b) The first part follows immediately from (31.20.1) combined with Proposition 31.2. Moreover, given $x \in J^\times$, an application of (31.20.1) and (31.2.1) yields $\eta(x)^{-1} = U_{\eta(x)}^{-1} \eta(x) = \eta^{\sharp -1} U_x^{-1} \eta^{-1} \eta(x)$, hence (2).

(c) follows immediately from Prop. 31.18 (a).

(d) (i) ⇔ (ii): By Prop. 31.18, condition (i) holds if and only if $\eta \in \mathrm{Str}(J)$ and $\eta(p^{-1}) = \eta(1^{(p)}) = 1^{(q)} = q^{-1}$.

(d) (ii) $\Leftrightarrow$ (iii): For $\eta \in \mathrm{Str}(J)$, the condition $\eta(p^{-1}) = q^{-1}$ by (2) is equivalent to $q = \eta(p^{-1})^{-1} = \eta^{\sharp -1}(p)$, hence to $\eta^{\sharp}(q) = p$. □

31.23 Corollary. *For $p, q \in J^\times$, the isotopes $J^{(p)}$ and $J^{(q)}$ are isomorphic if and only if p and q belong to the same orbit of $J^\times$ under the action of the structure group of J.* □

31.24 Example. Let $p \in J$ and assume $p^3 = \alpha 1_J$ for some $\alpha \in k^\times$. Then $\alpha^{-1} U_p$ belongs to the structure group of J and $\alpha^{-1} U_p p = 1_J$, $p \in J^\times$. Hence Cor. 31.23 shows that J and $J^{(p)}$ are isomorphic.

31.25 Corollary. *Let J be a (linear) Jordan algebra over an algebraically closed field of characteristic not 2. If J is algebraic in the sense of Exc. 8.11, then the inner structure group of J acts transitively on $J^\times$ and any two isotopes of J are isomorphic.*

Proof Let $p \in J^\times$. By Exc. 8.11, there exists a $q \in J^\times$ such that $p = q^2 = U_q 1_J$. Hence p belongs to the orbit of 1_J under the inner structure group of J. This proves the first assertion, while the second one now follows immediately from Cor. 31.23. □

Note that Cor. 31.25 does not hold in characteristic 2, see Exc. 31.34 (e) below.

31.26 On the methodological importance of isotopes. By deriving the results of the present section, we have brought to the fore the close analogy connecting the U-operator of Jordan algebras with the left (or right) multiplication operator of associative algebras. There are important differences, however. For example, the trivial observation that the group of left multiplications induced by invertible elements of a unital associative algebra A is transitive on $A^\times$ has no analogue in the Jordan setting. In fact, combining Cor. 31.23 with Exc. 31.34 (d) below, it follows that there are Jordan algebras over fields where not even the full structure group, let alone the inner one, acts transitively on their invertible elements.

Isotopes may be regarded as a substitute for this deficiency. For example, one is often confronted with the task of proving an identity for Jordan algebras involving invertible elements $x, y, z, \ldots$. This task can sometimes be simplified by passing to an appropriate isotope, which would then allow one to assume that, e.g., x is the identity element. Here is a typical result where the procedure just described turns out to be successful.

31.27 Theorem (Jacobson [140, Prop. 1.7.10])**.** *Let x, y be elements of J and*

assume that y is invertible. If two of the elements $x, x + U_x y, x + y^{-1}$ are invertible, then so is the third and

$$(x + U_x y)^{-1} + (x + y^{-1})^{-1} = x^{-1}. \tag{1}$$

Proof We first treat the case $y = 1_J$ by showing that if two of the elements $x, x + x^2, 1_J + x$ are invertible, then so is the third and

$$(x + x^2)^{-1} + (1_J + x)^{-1} = x^{-1}. \tag{2}$$

We begin by applying Thm. 30.1 to deduce

$$U_{x+x^2} = U_x U_{1_J + x}. \tag{3}$$

Hence our first intermediate assertion holds. Moreover, combining (29a.11) with (29.16.2), we obtain $U_{x,x^2} x^{-1} = V_x U_x x^{-1} = V_x x = 2x^2$, which together with (3) implies

$$\begin{aligned} U_{x+x^2}((x + x^2)^{-1} + (1_J + x)^{-1}) &= x + x^2 + U_x(1_J + x) = x + 2x^2 + x^3 \\ &= U_x x^{-1} + U_{x,x^2} x^{-1} + U_{x^2} x^{-1} = U_{x+x^2} x^{-1}, \end{aligned}$$

hence (2).

Next let $y \in J^\times$ be arbitrary. Passing to the y-isotope $J^{(y)}$, which satisfies $J^{(y)\times} = J^\times$ by Thm. 31.10 (a), the relations

$$x + U_x y = x + x^{(2,y)}, \quad x + y^{-1} = 1^{(y)} + x$$

and the special case treated before prove the first part of the theorem. Moreover, by Thm. 31.10 (a) again and (2) for $J^{(y)}$,

$$\begin{aligned} (x + U_x y)^{-1} + (x + y^{-1})^{-1} &= U_y((x + x^{(2,y)})^{(-1,y)} + (1^{(y)} + x)^{(-1,y)}) \\ &= U_y x^{(-1,y)} = x^{-1}. \end{aligned}$$

□

31.28 Corollary (Hua identity)**.** *Let $x, y \in J$ be invertible such that $x - y^{-1}$ is invertible as well. Then so is $x^{-1} - (x - y^{-1})^{-1}$ and*

$$U_x y = x - (x^{-1} - (x - y^{-1})^{-1})^{-1}.$$

Proof Thm. 31.27 for $-x$ in place of x shows that $-x + U_x y$ is invertible and

$$(-x + U_x y)^{-1} = -(x^{-1} - (x - y^{-1})^{-1}).$$

The assertion follows. □

Exercises

31.29. Let J be a Jordan algebra over k that is finitely generated projective as a k-module. Prove that the following conditions are equivalent.

(i) All invertible elements of J are unimodular.
(ii) J contains unimodular elements.
(iii) $\mathrm{rk}_{\mathfrak{p}}(J) > 0$ for all $\mathfrak{p} \in \mathrm{Spec}(k)$, i.e., J has full support as a k-module.

31.30. *Evaluation at invertible elements.* Let x be an invertible element of J.

(a) Define

$$x^{-n} := (x^{-1})^n \tag{1}$$

for all positive integers n (see Cor. 31.11 for $n = 2$) and prove

$$U_{x^n} = U_x^n, \tag{2}$$
$$U_{x^m} x^n = x^{2m+n}, \tag{3}$$
$$(x^m)^n = x^{mn}, \tag{4}$$
$$\{x^m x^n x^p\} = 2x^{m+n+p}, \tag{5}$$
$$V_{x^m,x^n} = V_{x^{m+n}}, \tag{6}$$
$$U_{x^i} U_{x^m,x^n} = U_{x^{i+m},x^{i+n}} = U_{x^m,x^n} U_{x^i}, \tag{7}$$
$$U_{x^i,x^j} U_{x^m,x^n} = U_{x^{i+m},x^{j+n}} + U_{x^{i+n},x^{j+m}} \tag{8}$$

for all $i, j, m, n \in \mathbb{Z}$.

(b) Write $k[\mathbf{t}, \mathbf{t}^{-1}]$ for the ring of Laurent polynomials in the variable $\mathbf{t}$ over k and

$$\varepsilon_x^{\times} \colon k[\mathbf{t}, \mathbf{t}^{-1}]^{(+)} \to J$$

for the unique linear map sending $\mathbf{t}^n$ to x^n for all $n \in \mathbb{Z}$. Show that $\varepsilon_x^{\times}$ is a homomorphism of Jordan algebras and that $k[x, x^{-1}] := \mathrm{Im}(\varepsilon_x^{\times})$ is the subalgebra of J generated by x and x^{-1}.

(c) Write $f(x) := \varepsilon_x^{\times}(f)$ for $f \in k[\mathbf{t}, \mathbf{t}^{-1}]$ and show that

$$U_{(fg)(x)} = U_{f(x)} U_{g(x)} \tag{9}$$

for all $f, g \in k[\mathbf{t}, \mathbf{t}^{-1}]$. Conclude that if J has no absolute zero divisors, then $k[x, x^{-1}]$ carries the structure of a unique algebra $R \in k\text{-}\mathbf{alg}$ such that $k[x, x^{-1}] = R^{(+)}$ as Jordan algebras.

31.31. Let $u \in J$ be nilpotent in the sense of Exc. 28.20 (b) and prove that $1_J - u$ is invertible in J with inverse

$$(1_J - u)^{-1} = \sum_{n \geq 0} u^n.$$

Conclude for a nil ideal $I \subseteq J$ and the canonical projection $x \mapsto \bar{x}$ from J to $\bar{J} := J/I$ that $x \in J$ is invertible in J if and only if $\bar{x}$ is invertible in $\bar{J}$.

31.32. *Invertibility in linear Jordan algebras.* Let J be a linear Jordan algebra over a commutative ring where 2 is invertible. Elements $x, y \in J$ are said to *operator commute* if $[L_x, L_y] = 0$.

(a) Prove for $x, y \in J$ that x^2 and y operator commute if and only if so do x and xy.

(b) Prove for $x \in J$ that the following conditions are equivalent.

(i) x is invertible.

(ii) There exists an element $y \in J$ such that $xy = 1_J$ and x, y operator commute.

(iii) There exists an element $y \in J$ such that $xy = 1_J$ and $x^2 y = x$.

Show further that if these conditions are fulfilled, then y as in (ii) (resp. (iii)) is unique and equal to x^{-1}.

Remark. The characterization of invertibility in (b) (ii) is due to Koecher (unpublished).

31.33. *Invertibility in pointed quadratic modules.* Let (M, q, e) be a pointed quadratic module with conjugation $x \mapsto \bar{x}$ over k. Prove that an element $x \in M$ is invertible in the Jordan algebra $J := J(M, q, e)$ if and only if $q(x) \in k$ is invertible in k. In this case,

$$x^{-1} = q(x)^{-1}\bar{x}, \quad q(x^{-1}) = q(x)^{-1}. \tag{1}$$

If x is invertible in J, we also say *x is invertible in (M, q, e) with inverse x^{-1}*. Thus the Jordan algebra of a pointed quadratic module (M, q, e) over a field is a Jordan division algebra if and only if the quadratic form q is anisotropic.

31.34. *Isotopes of pointed quadratic modules.* Let (M, q, e) be a pointed quadratic module over k, with trace t and conjugation $x \mapsto \bar{x}$.

(a) Let $f \in M$ be invertible in (M, q, e) (Exc. 31.33). Show that

$$(M, q, e)^{(f)} := (M, q^{(f)}, e^{(f)}), \quad q^{(f)} := q(f)q, \quad e^{(f)} := f^{-1} \tag{1}$$

is a pointed quadratic module over k with trace

$$t^{(f)} \colon M \longrightarrow k, \quad x \longmapsto t^{(f)}(x) := q(\bar{f}, x), \tag{2}$$

and conjugation

$$x \longmapsto \bar{x}^{(f)} := q(f)^{-1} q(\bar{f}, x)\bar{f} - x. \tag{3}$$

Show further

$$J((M, q, e)^{(f)}) = (J(M, q, e))^{(f)}. \tag{4}$$

We call $(M, q, e)^{(f)}$ the *f-isotope* (or simply *an* isotope) of (M, q, e).

(b) Let $f \in M$ be invertible in (M, q, e). Prove that the invertible elements of (M, q, e) and $(M, q, e)^{(f)}$ are the same, and that

$$((M, q, e)^{(f)})^{(g)} = (M, q, e)^{(U_f g)}$$

for all invertible elements g of (M, q, e), where U stands for the U-operator of the Jordan algebra $J(M, q, e)$.

(c) Prove that if M is projective as a k-module, then the structure group of $J(M, q, e)$ agrees with the group of similarity transformations of the quadratic module (M, q), consisting by definition of all bijective linear maps $\eta \colon M \to M$ such that $q \circ \eta = \alpha q$ for some $\alpha \in k^\times$.

(d) Let $k := \mathbb{R}$ and $M := \mathbb{R}^3$ with the canonical basis (e_1, e_2, e_3). Put $e := e_1$ and $q := \langle S \rangle_{\text{quad}}$ with

$$S := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Find an isotope of $J := J(M, q, e)$ which is not isomorphic to J.

(e) Let $k := F$ be a field of characteristic 2 and assume (M, q, e) is *traceless* in the sense that $t = 0$. Furthermore, let $f \in M$ be anisotropic relative to q and assume $f \notin \text{Rad}(Dq)$. Then put $J := J(M, q, e)$ and prove that the isotope $J^{(f)}$ is not isomorphic to J. Finally, give an example where the preceding hypotheses are fulfilled even when F is algebraically closed.

31.35. *A useful formula for the U-operator* (cf. Braun-Koecher [36, IV, Satz 3.8]). Let x, y be invertible elements of J. Prove

$$U_x U_{x^{-1}+y^{-1}} U_y = U_{x+y}.$$

(*Hint*: Pass to the isotope $J^{(y)}$ and apply Exc. 31.30 (9).)

31.36. *Linear invertibility.* Let J be a linear Jordan algebra over a commutative ring k where 2 is invertible. An element $x \in J$ is said to be *linearly invertible* if the left multiplication operator $L_x \colon J \to J$ is bijective. In this case we call $x^{-1} := L_x^{-1} 1_J$ the *linear inverse* of x in J. Prove that if x is linearly invertible, then it is invertible, and its linear inverse and its ordinary inverse are the same; moreover, x^{-1} is linearly invertible with (linear) inverse x. Finally, prove that invertible elements of J need not be linearly invertible by showing for any pointed quadratic module (M, q, e) over a field of characteristic not 2 that $J := J(M, q, e)$ is a linear division algebra in the sense of 8.6 if and only if q is anisotropic and $\dim_F(J) \leq 2$.

Remark. For more on the connection between linear and ordinary Jordan division algebras, see Petersson [215].

31.37. *Strong homotopies.* A linear map $\eta \colon J \to J'$ is called a *strong homotopy* if some $p \in J^\times$ makes $\eta \colon J^{(p)} \to J'$ a homomorphism.

(a) Prove that strong homotopies are homotopies. Conversely, if $\eta \colon J \to J'$ is a homotopy and $\eta(J^\times) = J'^\times$, show that η is a strong homotopy.

(b) Give an example of a homotopy which is not a strong homotopy.

31.38. *Discrete valuations of Jordan division rings* (Petersson [211, 214]).[1] Let J be a Jordan division ring, i.e., a Jordan division algebra over $\mathbb{Z}$, and write F for the centroid of J. Recall from Exc. 29.18 (c) that F is a field and that J may canonically be regarded as a Jordan algebra over F.

By a *discrete valuation* of J we mean a map $\lambda \colon J \to \mathbb{Z}_\infty := \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions, for all $x, y \in J$.

$$\lambda(x) = \infty \iff x = 0, \tag{1}$$

$$\lambda(U_x y) = 2\lambda(x) + \lambda(y), \tag{2}$$

$$\lambda(x + y) \geq \min\{\lambda(x), \lambda(y)\}. \tag{3}$$

[1] In this exercise, the reader is assumed to be familiar with the rudiments of valuation theory.

For the rest of this exercise, fix a discrete valuation λ of J and observe by Thm. 30.11 that J is locally linear. Then prove:

(a) For all $x \in J^\times$ and all $n \in \mathbb{Z}$, we have $\lambda(x^n) = n\lambda(x)$.
(b) For all $x \in J$ and all $v, w \in F[x]$, we have $\lambda(vw) = \lambda(v) + \lambda(w)$. Conclude that

$$\lambda_0 \colon F \longrightarrow \mathbb{Z}_\infty, \quad a \longmapsto \lambda_0(a) := \lambda(a1_J),$$

is a discrete valuation of of F, with valuation ring, valuation ideal, and residue field respectively given by

$$\begin{aligned} \mathfrak{v}_0 &:= \{a \in F \mid \lambda_0(a) \geq 0\}, \\ \mathfrak{p}_0 &:= \{a \in F \mid \lambda_0(a) > 0\}, \\ \bar{F} &:= \mathfrak{v}_0/\mathfrak{p}_0. \end{aligned}$$

(c) The sets

$$\begin{aligned} \mathfrak{O} &:= \{x \in J \mid \lambda(x) \geq 0\} \subseteq J, \\ \mathfrak{P} &:= \{x \in J \mid \lambda(x) > 0\} \subseteq \mathfrak{O}, \\ \bar{J} &:= \mathfrak{O}/\mathfrak{P} \end{aligned}$$

are respectively an $\mathfrak{v}_0$-subalgebra of J, an ideal in $\mathfrak{O}$, a Jordan division algebra over $\bar{F}$. But note that, even if J is a linear Jordan algebra over F (i.e., F has characteristic not 2), $\mathfrak{O}$ need not be one over $\mathfrak{v}_0$, and $\bar{J}$ need not be one over $\bar{F}$.
(d) $\lambda(J^\times)$ is a subgroup of $\mathbb{Z}$, called the *value group* of λ.
(e) For $p \in J^\times$, the map

$$\lambda^{(p)} \colon J^{(p)} \longrightarrow \mathbb{Z}_\infty, \quad x \longmapsto \lambda^{(p)}(x) := \lambda(p) + \lambda(x),$$

is a discrete valuation of $J^{(p)}$ having the same value group as λ. We call $\lambda^{(p)}$ the *p-isotope* of λ. Given another element $q \in J^\times$, show further $(\lambda^{(p)})^{(q)} = \lambda^{(U_p q)}$.
(f) λ satisfies the Jordan triple product inequality

$$\lambda(\{xyz\}) \geq \lambda(x) + \lambda(y) + \lambda(z) \tag{4}$$

for all $x, y, z \in J$. (*Hint*: Reduce to the case $y = 1_J$. Then derive and use the formula

$$(x \circ y)^2 = U_x y^2 + U_y x^2 + x \circ (U_y x), \tag{5}$$

valid for all x, y in arbitrary Jordan algebras.)

31.39. Let J be an algebraic Jordan division algebra over a field F. Prove:

(a) For $x \in J$, the subalgebra $F[x] \subseteq J$ is a finite algebraic field extension of F.
(b) If F is algebraically closed, then $J \cong F^{(+)}$.
(c) For $F = \mathbb{R}$, there exists a pointed quadratic module (M, q, e) over $\mathbb{R}$ such that $J \cong J(M, q, e)$ and q is positive definite.

32 The Peirce decomposition

The Peirce decomposition in its various guises belongs to the most powerful techniques in the structure theory of Jordan algebras. Initiated by Jordan-von

Neumann-Wigner [148] in their study of euclidean Jordan algebras, it dominated the scene well into the 1960s, losing a certain amount of its appeal only when research began to focus on Jordan algebras without finiteness conditions where idempotents (the principal ingredient of the Peirce decomposition) are in short supply.

This section is devoted to those properties of the Peirce decomposition that are relevant for our subsequent applications to cubic Jordan algebras. Our treatment of the subject relies quite heavily on the approach of Loos [171, §5] (after being specialized from Jordan pairs to algebras), which in turn owes much to that of Springer [268, §10].

Throughout we let k be a commutative ring and J a Jordan algebra over k. Recall from Exc. 29.18 (b) that an idempotent in J is an element c satisfying $c^2 = c$. The additional hypothesis $c^3 = c$ that has to be imposed in the setting of arbitrary para-quadratic algebras (cf. 28.9), implying $c^n = c$ for all positive integers n, holds automatically in the Jordan case.

32.1 Lemma. *Let c be an idempotent in J and put $d := 1_J - c$. Writing $D := k \times k$ for the split quadratic étale k-algebra,*

$$\Theta_c \colon D \longrightarrow \mathrm{End}_k(J), \quad (\gamma, \delta) \longmapsto \Theta_c((\gamma, \delta)) := U_{\gamma c + \delta d} \qquad (\gamma, \delta \in k)$$

is a quadratic map that permits composition:

$$\Theta_c(1_D) = \mathbf{1}_J, \quad \Theta_c((\gamma_1, \delta_1)(\gamma_2, \delta_2)) = \Theta_c((\gamma_1, \delta_1))\Theta_c((\gamma_2, \delta_2)) \tag{1}$$

for all $\gamma_i, \delta_i \in k$, $i = 1, 2$. In particular,

$$\Theta_c((\gamma, \delta)) \in \mathrm{GL}(J) \qquad (\gamma, \delta \in k^\times). \tag{2}$$

*Moreover, Θ_c is compatible with base change: $\Theta_{c_R} = (\Theta_c)_R$ for all $R \in k$-**alg**.*

Proof The first equation of (1) is obvious. In order to prove the second, we let $i = 1, 2$ and note $\Theta_c((\gamma_i, \delta_i)) = U_{\delta_i 1_J + (\gamma_i - \delta_i)c} = U_{f_i(c)}$, where $f_i := \delta_i + (\gamma_i - \delta_i)\mathbf{t} \in k[\mathbf{t}]$. Hence Thm. 30.1 implies $\Theta_c((\gamma_1, \delta_1))\Theta_c((\gamma_2, \delta_2)) = U_{(f_1 f_2)(c)}$, where

$$f_1 f_2 = \delta_1\delta_2 + ((\gamma_1 - \delta_1)\delta_2 + \delta_1(\gamma_2 - \delta_2))\mathbf{t} + (\gamma_1 - \delta_1)(\gamma_2 - \delta_2)\mathbf{t}^2.$$

Evaluating at c, we conclude

$$\begin{aligned}(f_1 f_2)(c) &= \delta_1\delta_2 1_J + ((\gamma_1 - \delta_1)\delta_2 + \delta_1(\gamma_2 - \delta_2) + (\gamma_1 - \delta_1)(\gamma_2 - \delta_2))c \\ &= \delta_1\delta_2 1_J + ((\gamma_1 - \delta_1)\gamma_2 + \delta_1(\gamma_2 - \delta_2))c \\ &= \delta_1\delta_2 1_J + (\gamma_1\gamma_2 - \delta_1\delta_2)c \\ &= (\gamma_1\gamma_2)c + (\delta_1\delta_2)d,\end{aligned}$$

and the second equation of (1) is proved. The remaining assertions are now obvious. □

32.2 Theorem (Singular Peirce decomposition)**.** *Let c be an idempotent in J and put $d := 1_J - c$. Then the following statements hold.*

(a) *The linear endomorphisms of J defined by*

$$E_2 := E_2(c) := U_c, \quad E_1 := E_1(c) := U_{c,d} = V_c - 2U_c, \quad \text{and} \quad E_0 := E_0(c) := U_d \tag{1}$$

satisfy the relation

$$U_{tc_R+d_R} = E_{0R} + tE_{1R} + t^2E_{2R} \tag{2}$$

*for all $R \in k$-**alg** and all $t \in R$.*

(b) *The E_i, $i = 0, 1, 2$, are orthogonal projections of J, called its* Peirce projections *relative to c, and their sum is the identity. Hence they give rise to a decomposition*

$$J = J_2 \oplus J_1 \oplus J_0 \tag{3}$$

as a direct sum of submodules $J_i := J_i(c) := \operatorname{Im}(E_i)$ for $i = 0, 1, 2$, called the Peirce components *of J relative to c.*

(c) *We have*

$$J_2 = \operatorname{Im}(U_c), \quad J_1 \oplus J_0 = \operatorname{Ker}(U_c), \tag{4}$$

$$J_0 = \operatorname{Ker}(U_c) \cap \operatorname{Ker}(V_c), \tag{5}$$

$$J_i \subseteq \{x \in J \mid c \circ x = ix\} \qquad (i = 0, 1, 2), \tag{6}$$

$$J_1 = \{x \in J \mid c \circ x = x\} = \{x \in J \mid \{ccx\} = x\}. \tag{7}$$

(d) *Setting $J_i := \{0\}$ for $i \in \mathbb{Z} \setminus \{0, 1, 2\}$, the following composition rules hold, for all $i, j, l \in \{0, 1, 2\}$.*

$$U_{J_i} J_j \subseteq J_{2i-j}, \tag{8}$$

$$\{J_i J_j J_l\} \subseteq J_{i-j+l}, \tag{9}$$

$$\{J_2 J_0 J\} = \{0\} = \{J_0 J_2 J\}. \tag{10}$$

Proof (a) Expanding $U_{c,d}$ with respect to d gives the second equation for E_1 in (1), while (2) is equally obvious.

(b) $R := k[\mathbf{s}, \mathbf{t}]$, the polynomial ring in two independent variables $\mathbf{s}, \mathbf{t}$ over k, is free as a k-module with basis $(\mathbf{s}^i\mathbf{t}^j)_{i,j\in\mathbb{N}}$. Hence the identifications of 12.4 imply

$$J \subseteq J_R = \bigoplus_{i,j\geq 0} (\mathbf{s}^i\mathbf{t}^j J)$$

and

$$\mathrm{End}_k(J) \subseteq \mathrm{End}_k(J)_R = \bigoplus_{i,j\geq 0} (\mathbf{s}^i\mathbf{t}^j \mathrm{End}_k(J)) \subseteq \mathrm{End}_R(J_R)$$

as direct sums of k-modules. With this in mind, Lemma 32.1 combined with (2) yields

$$\sum_{i,j=0}^{2} \mathbf{s}^i\mathbf{t}^j E_i E_j = (\sum_{i=0}^{2} \mathbf{s}^i E_i)(\sum_{j=0}^{2} \mathbf{t}^j E_j) = \Theta_{c_R}((\mathbf{s}, 1_R))\Theta_{c_R}((\mathbf{t}, 1_R))$$

$$= \Theta_{c_R}((\mathbf{s}, 1_R)(\mathbf{t}, 1_R)) = \Theta_{c_R}((\mathbf{st}, 1_R)) = \sum_{i=0}^{2} \mathbf{s}^i\mathbf{t}^i E_i.$$

Comparing coefficients of $\mathbf{s}^i\mathbf{t}^j$, we obtain $E_iE_j = \delta_{ij}E_i$ for $i, j = 0, 1, 2$, and the first assertion of (b) follows. The remaining ones are obvious.

(c) Since $U_c = E_2$ by (1), equation (4) is obvious. Applying (1) once more, we conclude $J_0 = \mathrm{Ker}(E_2) \cap \mathrm{Ker}(E_1) = \mathrm{Ker}(U_c) \cap \mathrm{Ker}(V_c - 2U_c)$, and (5) follows. From (1) we also deduce $V_c = E_1 + 2U_c = 2E_2 + E_1 = \sum_{j=0}^{2} jE_j$, and applying this to $x_i \in J_i$, we obtain $c \circ x_i = V_c x_i = \sum jE_j x_i = ix_i$, giving (6) and the inclusion from left to right in (7). Conversely, suppose $x \in J$ satisfies $c \circ x = x$ and write $x = x_2 + x_1 + x_0$, $x_i \in J_i$. Then (6) implies $x = 2x_2 + x_1$ and comparing J_i-components for $i = 0, 1, 2$, we conclude $x_2 = x_0 = 0$, hence $x = x_1 \in J_1$. This completes the proof of the first equation of (7). Since $\{ccx\} = c \circ x - \{cdx\}$, the second equation will follow once we have established (10), which will be done in due course.

(d) Let $R = k[\mathbf{t}, \mathbf{t}^{-1}]$ be the k-algebra of Laurent polynomials in the variable $\mathbf{t}$ over k, which is free as a k-module with basis $(\mathbf{t}^i)_{i\in\mathbb{Z}}$. Hence 12.4 yields the identifications

$$J \subseteq J_R = \bigoplus_{i\in\mathbb{Z}} (\mathbf{t}^i J)$$

and

$$\mathrm{End}_k(J) \subseteq \mathrm{End}_k(J)_R = \bigoplus_{i\in\mathbb{Z}} (\mathbf{t}^i \mathrm{End}_k(J)) \subseteq \mathrm{End}_R(J_R)$$

as direct sums of k-modules. Since $\mathbf{t} \in R^\times$, we deduce from (2) and Lemma 32.1 that the map

$$U_{\mathbf{t}c+d} = \sum_{j=0}^{2} \mathbf{t}^j E_j \colon J_R \to J_R$$

is bijective with inverse $U_{\mathbf{t}^{-1}c+d}$. Moreover, for $x = \sum_{l\in\mathbb{Z}} x_l$, $x_l \in J_l$, $l \in \mathbb{Z}$, we

compute

$$U_{\mathbf{t}c+d}x = \sum_{j,l=0}^{2} \mathbf{t}^j E_j x_l = \sum_{l=0}^{2} \mathbf{t}^l x_l = \sum_{i\in\mathbb{Z}} \mathbf{t}^i x_i,$$

which shows

$$J_i = \{x \in J \mid U_{\mathbf{t}c+d}x = \mathbf{t}^i x\} = \{x \in J \mid U_{\mathbf{t}^{-1}c+d}x = \mathbf{t}^{-i}x\} \qquad (i \in \mathbb{Z}). \tag{11}$$

Now let $i, j, l \in \mathbb{Z}$ and $x_i \in J_i$, $y_j \in J_j$, $z_l \in J_l$. Then the fundamental formula and (11) imply

$$\begin{aligned} U_{\mathbf{t}c+d}U_{x_i}y_j &= U_{\mathbf{t}c+d}U_{x_i}U_{\mathbf{t}c+d}U_{\mathbf{t}^{-1}c+d}y_j = U_{U_{\mathbf{t}c+d}x_i}U_{\mathbf{t}^{-1}c+d}y_j \\ &= U_{\mathbf{t}^i x_i}\mathbf{t}^{-j}y_j = \mathbf{t}^{2i-j}U_{x_i}y_j, \end{aligned}$$

hence $U_{x_i}y_j \in J_{2i-j}$. This proves (8). Similarly,

$$\begin{aligned} U_{\mathbf{t}c+d}\{x_i y_j z_l\} &= U_{\mathbf{t}c+d}U_{x_i,z_l}U_{\mathbf{t}c+d}U_{\mathbf{t}^{-1}c+d}y_j \\ &= U_{U_{\mathbf{t}c+d}x_i,U_{\mathbf{t}c+d}z_l}U_{\mathbf{t}^{-1}c+d}y_j = U_{\mathbf{t}^i x_i,\mathbf{t}^l z_l}\mathbf{t}^{-j}y_j \\ &= \mathbf{t}^{i-j+l}\{x_i y_j z_l\}, \end{aligned}$$

which proves $\{x_i y_j z_l\} \in J_{i-j+l}$, hence (9). It remains to prove the first equation of (10) since the second one then follows after the substitution $c \mapsto d$. For $x_i \in J_i$, $i = 0, 2$, we must show $V_{x_2,x_0} = 0$. Applying (29a.21), (29a.13) and (1), (4), (6), we first obtain $V_{c,x_0} = V_{U_c c,x_0} = V_{c,\{cc x_0\}} - V_{U_c x_0,c} = V_{c,c\circ x_0} = 0$ from (1), (6) and then $V_{x_2,x_0} = V_{U_c x_2,x_0} = V_{c,\{x_2 c x_0\}} - V_{U_c x_0,x_2} = 0$ since $\{x_2 c x_0\} \in J_0$ by (9). This completes the proof. □

32.3 Corollary. *Let c be an idempotent in J and put $d := 1_J - c$.*

(a) *For all $R \in k$-**alg**, there are natural identifications*

$$(J_R)_i(c_R) = J_i(c)_R \qquad (i = 0, 1, 2).$$

(b) *d is an idempotent in J satisfying $J_i(d) = J_{2-i}(c)$ for $i = 0, 1, 2$.*

(c) *The k-module $J_2(c)$ (resp. $J_0(c)$) is a Jordan algebra over k with unit element c (resp. d) whose U-operator is derived from the U-operator of J by restriction. Moreover, $J_2(c) \oplus J_0(c)$ is a direct sum of ideals and a subalgebra of J.*

(d) *The Peirce components $J_i := J_i(c)$ of J ($i = 0, 1, 2$) satisfy the bilinear composition rules*

$$J_i \circ J_i \subseteq J_i, \quad J_i \circ J_1 \subseteq J_1, \quad J_2 \circ J_0 = \{0\}, \quad J_1 \circ J_1 \subseteq J_2 \oplus J_0 \tag{1}$$

for $i = 0, 2$.

Proof (a) This follows immediately from (32.2.3) and the fact that scalar extensions of k-modules commute with direct sums.

(b) This follows immediately from Thm. 32.2 (a), (b).

(c) We put $c_2 := c$, $c_0 := d$ and let $i = 0, 2$. From (32.2.8) we deduce $U_{J_i} J_i \subseteq J_i$, so restricting the U-operator of J to J_i gives a quadratic map $U\colon J_i \to \mathrm{End}_k(J_i)$ which by Thm. 32.2 sends c_i to the identity on J_i. In this way, therefore, J_i becomes a para-quadratic algebra over k, which is in fact a Jordan algebra since the defining identities (29.1.1), (29.1.2) hold not only on J_i but by (a) on all scalar extensions as well. By (32.2.8) we have $U_{J_2} J_0 + U_{J_0} J_2 = \{0\}$, which together with (32.2.10) implies that $J_2 \oplus J_0$ is a direct sum of ideals. As such it is a Jordan algebra in its own right with identity element $c_1 + c_0 = 1_J$, hence a subalgebra of J.

(d) For $i = 0, 2$, $j = 0, 1, 2$, we apply (32.2.9), (32.2.10) and obtain $J_i \circ J_j \subseteq \{J_i J_i J_j\} + \{J_i J_{2-i} J_j\} \subseteq J_j$ hence first two relations of (1), while the third one now follows by symmetry: $J_2 \circ J_0 \subseteq J_0 \cap J_2 = \{0\}$. On the other hand, $J_1 \circ J_1 \subseteq \{J_1 J_2 J_1\} + \{J_1 J_0 J_1\} \subseteq J_0 + J_2$ by (32.2.9), giving also the fourth relation, and the proof of (1) is complete. □

32.4 Remark. $J_2(c)$, though a Jordan algebra, in general is not a subalgebra of J; in fact, it is one if and only if $c = 1_J$.

32.5 The Peirce decomposition in linear Jordan algebras. Suppose $2 \in k^\times$ and let c be an idempotent in J. We claim

$$J_i(c) = \{x \in J \mid c \circ x = ix\} \qquad (i = 0, 1, 2). \tag{1}$$

By (32.2.6), (32.2.7), the left-hand side is contained in the right and we have equality for $i = 1$. Now assume $i = 0, 2$ and that $x \in J$ satisfies $c \circ x = ix$.Writing $x = x_2 + x_1 + x_0$, $x_j \in J_j(c)$ for $j = 0, 1, 2$, we conclude $ix_2 + ix_1 + ix_0 = c \circ x = 2x_2 + x_1$. For $i = 0$, this implies $2x_2 = x_1 = 0$, hence $x = x_0 \in J_0(c)$ since $2 \in k^\times$. By the same token, $i = 2$ implies $x_1 = 2x_0 = 0$, hence $x = x_2 \in J_2(c)$. This completes the proof.

Viewing J as a unital linear Jordan algebra over k via Thm. 29.4, with bilinear multiplication $xy = \frac{1}{2} x \circ y = \frac{1}{2} V_x y$, the left multiplication operator of c in J is $L_c = \frac{1}{2} V_c$, and (1) may be rewritten as

$$J_i := J_i(c) = \{x \in J \mid cx = \frac{i}{2} x\} \qquad (i = 0, 1, 2), \tag{2}$$

so the Peirce components of c are basically the "eigenspaces" of L_c with respect to the "eigenvalues" $0, \frac{1}{2}, 1$. For this reason, the i-th Peirce component of c, $i = 0, 1, 2$, in the classical literature is usually denoted by $J_{\frac{i}{2}}(c)$. *But we will never adhere to this convention.* Instead we confine ourselves to rewriting

the composition rules (32.3.1) in the language of linear Jordan algebras: for $i = 0, 2$ we have

$$J_i^2 \subseteq J_i, \quad J_iJ_1 \subseteq J_1, \quad J_2J_0 = \{0\}, \quad J_1^2 \subseteq J_2 \oplus J_0$$

32.6 Example. Let's work through the details of the Singular Peirce Decomposition for J the real euclidean Jordan algebra $\mathrm{Her}_3(\mathbb{D})$ for $\mathbb{D} = \mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$ from §5 and the idempotent $c = e_{11}$. We write a general element $x \in J$ as in (5.4.2):

$$x = \sum \alpha_i e_{ii} + u_i[jl].$$

We have

$$c \bullet x = \begin{pmatrix} \alpha_1 & \frac{1}{2}u_3 & \frac{1}{2}\bar{u}_2 \\ \frac{1}{2}\bar{u}_3 & 0 & 0 \\ \frac{1}{2}u_2 & 0 & 0 \end{pmatrix} = \alpha_1 e_{11} + \frac{1}{2}u_3[12] + \frac{1}{2}u_2[31],$$

so (32.5.2) implies

$$J_0(c) = \mathbb{R}e_{22} + \mathbb{R}e_{33} + \mathbb{D}[23], \quad J_1(c) = \mathbb{D}[31] + \mathbb{D}[12], \quad \text{and} \quad J_2(c) = \mathbb{R}e_{11}.$$

32.7 Example. Let A be a unital alternative k-algebra and recall that $c \in A$ is an idempotent in A if and only if it is one in the Jordan algebra $A^{(+)}$. In this case, the Peirce decompositions of A and of $A^{(+)}$ with respect to c relate to one another by the formulas

$$A_2^{(+)}(c) = A_{11}(c), \quad A_1^{(+)}(c) = A_{12}(c) + A_{21}(c), \quad A_0^{(+)}(c) = A_{22}(c).$$

This follows immediately from comparing (2) of Exc. 14.12 with Thm. 32.2.

32.8 Proposition. *Let (M, q, e) be a pointed quadratic module over k. An element $c \in M$ is an elementary idempotent in $J := J(M, q, e)$ (cf. 29.13) if and only if (c, d) with $d := e - c$ is a hyperbolic pair in the quadratic module (M, q). In this case, d is an elementary idempotent of J as well and*

$$J_2(c) = kc, \quad J_1(c) = (kc \oplus kd)^{\perp}, \quad J_0(c) = kd, \tag{1}$$

where "$\perp$" stands for orthogonal complementation relative to the bilinearization of q, are the Peirce components of J relative to c.

Proof Write t for the trace and $x \mapsto \bar{x}$ for the conjugation of (M, q, e). If (c, d) is a hyperbolic pair of (M, q), then $q(c) = 0$ and $t(c) = q(c, c + d) = 2q(c) + q(c, d) = 1$. Thus $c \in J$ is an elementary idempotent. Conversely, let this be so. Then $q(d) = q(e - c) = 1 - t(c) + q(c) = 0$ and $q(c, d) = q(c, e - c) = t(c) - 2q(c) = 1$. Thus (c, d) is a hyperbolic pair of (M, q). It remains to determine the Peirce components of J relative to c. To begin with, let $x \in J_2(c)$. Then (29b.5) implies $x = U_c x = q(c, \bar{x})c - q(c)\bar{x} = q(c, \bar{x})c \in kc$, and the first

equation of (1) holds. But then $J_0(c) = J_2(d) = kd$ since d is an elementary idempotent. It remains to prove $J_1(c) = (kc \oplus kd)^\perp$. Letting $x \in J$ and applying (29b.9), we obtain $c \circ x = t(c)x + t(x)c - q(c,x)e = x + t(x)c - q(c,x)e$, and (32.2.7) yields

$$J_1(c) = \{x \in M \mid t(x)c = q(c,x)e\}. \tag{2}$$

Suppose first $x \in J_1(c)$. Then (2) implies $q(c,x) = t(c)q(c,x) = q(q(c,x)e, c) = q(t(x)c, c) = 2t(x)q(c) = 0$, hence $t(x)c = q(c,x)e = 0$, forcing $t(x) = 0$ since c is unimodular, and then $q(d,x) = t(x) - q(c,x) = 0$. Thus $x \in (kc \oplus kd)^\perp$. Conversely, let $x \in (kc \oplus kd)^\perp$. Then $q(c,x) = q(d,x) = 0$ implies $t(x) = q(c,x) + q(d,x) = 0$, and (2) implies $x \in J_1(c)$. □

The Peirce decomposition of a Jordan algebra relative to a single idempotent is often not fine enough for the intended applications. We therefore wish to replace it by a Peirce decomposition relative to a complete orthogonal system of as many idempotents as possible. In order to accomplish this, we require a number of preparations that we are now going to address.

Orthogonality of a family of idempotents has been defined in 28.9 and Exc. 28.25 for arbitrary para-quadratic algebras. In the case of Jordan algebras, there is a simple characterization in terms of the Peirce decomposition.

32.9 Proposition. *For idempotents $c_1, c_2 \in J$, the following conditions are equivalent.*

(i) $c_1 \perp c_2$.
(ii) $c_2 \in J_0(c_1)$.
(iii) $c_1 \in J_0(c_2)$.

Proof Orthogonality being a symmetric relation on idempotents, it suffices to establish the equivalence of (i) and (ii). Combining (28.9.1) with (29a.13), we see that (i) holds if and only if $U_{c_1}c_2 = U_{c_2}c_1 = V_{c_1}c_2 = 0$. In this case, (32.2.5) implies $c_2 \in J_0(c_1)$. Conversely, suppose $c_2 \in J_0(c_1)$. Then $U_{c_1}c_2 = V_{c_1}c_2 = 0$, but also $U_{c_2}c_1 \in U_{J_0(c_1)}J_2(c_1) = \{0\}$ by (32.2.8). Thus (i) holds. □

32.10 Corollary. *A finite family $(c_1, \ldots, c_r)$ ($r \in \mathbb{Z}$, $r > 0$) of idempotents in J is an orthogonal system of idempotents in the sense of Exc. 28.25 if and only if $c_i \perp c_j$ for $1 \le i, j \le r$, $i \ne j$.*

Proof Assume $c_i \perp c_j$ for $1 \le i, j \le r$, $i \ne j$ and let $i, j, l \in \{1, \ldots, r\}$. The first set of relations in Exc. 28.25 (1) holds by the definition of orthogonality (cf. (28.9.1)). For the second set, let i, j, l be mutually distinct. From Prop. 32.9 and (32.2.10) we deduce $\{c_ic_jc_l\} \in \{J_2(c_i)J_0(c_i)J\} = \{0\}$. Thus all of Exc. 28.25

(1) holds, so $(c_1, \dots, c_r)$ is an orthogonal system of idempotents. The converse is obvious, again by Exc. 28.25 (1). □

32.11 Lemma. *Let $d, e \in J$ be orthogonal idempotents. Then $c := d + e \in J$ is an idempotent and $d \in J_2(d) \subseteq J_2(c)$.*

Proof c is an idempotent in J by Exc. 28.25 (a). Moreover, $U_c d = U_d d + \{dde\} + U_e d$, where $U_d d = d^3 = d$ and $\{dde\} = U_e d = 0$ by (1) of Exc. 28.25. Hence $U_c d = d$, which by (32.2.4) implies $d \in J_2(d) = U_d J = U_{U_c d} J = U_c U_d U_c J \subseteq U_c J = J_2(c)$. □

32.12 Proposition. *Let $\Omega = (c_1, \dots, c_r)$ be a complete orthogonal system of idempotents in J and define linear maps*

$$E_{ii} := E_{ii}(\Omega) := U_{c_i}, \quad E_{ij} := E_{ij}(\Omega) := U_{c_i, c_j} \qquad (1 \le i, j \le r,\ i \ne j). \tag{1}$$

Then $E_{ij} = E_{ji}$ for $1 \le i, j \le r$, and the E_{ij}, $1 \le i \le j \le r$, are orthogonal projections of J, called its Peirce projections relative to Ω, such that $\sum_{1 \le i \le j \le r} E_{ij}$ is the identity.

Proof The first assertion is obvious, and we clearly have $\sum_{i \le j} E_{ij} = U_{\sum c_i} = U_{1_J} = \mathbf{1}_J$, so we need only show that the E_{ij}, $1 \le i \le j \le r$, are orthogonal projections. We do so in two steps.

1°. Let $1 \le i, j \le r$, $i \ne j$. Lemma 32.11 shows that $c := c_i + c_j \in J$ is an idempotent, forcing $J' := J_2(c)$ by Cor. 32.3 (b) to be a Jordan algebra with identity element c. Moreover, Lemma 32.11 implies that c_i is an idempotent in J' and $c_j = 1_{J'} - c_i$. Applying Thm. 32.2 to J', c_i in place of J, c, respectively, we see that E_{ii}, E_{ij}, E_{jj} act as orthogonal projections on J' and vanish identically on $J_1(c) \oplus J_0(c)$ because

$$\begin{aligned} E_{ll} J_m(c) + E_{ij} J_m(c) &= U_{U_c c_l} J_m(c) + U_{U_c c_i, U_c c_j} J_m(c) \\ &= U_c U_{c_l} U_c J_m(c) + U_c U_{c_i, c_j} U_c J_m(c) = \{0\} \end{aligned}$$

for $l = i, j$ and $m = 0, 1$. Hence they are orthogonal projections on all of J that map J to J'.

2°. The proof will be complete once we have shown

$$E_{ij} E_{lm} = 0 \qquad (1 \le i, j, l, m \le r,\ \{i, j\} \ne \{l, m\}). \tag{2}$$

First suppose $i = j$ in (2). By 1°, we may assume $l \ne m$ and $i \notin \{l, m\}$. Then $c_l \perp c_i \perp c_m$, which implies $c_l + c_m \perp c_i$ by Prop. 32.9 and then

$$E_{ii} E_{lm} J + E_{lm} E_{ii} J \subseteq U_{J_0(c_l + c_m)} J_2(c_l + c_m) + \{J_2(c_l + c_m) J_0(c_l + c_m) J\} = \{0\}.$$

This shows (2) not only for for $i = j$ but also for $l = m$. We are left with the case $i \neq j$, $l \neq m$. By symmetry, we may assume $i \notin \{l, m\}$, which implies

$$E_{ij}E_{lm}J \subseteq \{c_iJ_2(c_l + c_m)c_j\} \subseteq \{J_0(c_l + c_m)J_2(c_l + c_m)J\} = \{0\}$$

and completes the proof of (2). □

32.13 Corollary. *Let $\Omega = (c_1, \ldots, c_r)$ be a complete orthogonal system of idempotents in J and put $D := k \times \cdots \times k \in k$-**alg** ($r$ factors) as a direct product of ideals. Then*

$$\Theta_\Omega \colon D \longrightarrow \mathrm{End}_k(J), \quad x \longmapsto U_{\sum_{i=1}^r \gamma_i c_i},$$

for $x = (\gamma_1, \cdots, \gamma_r) \in D$, $\gamma_i \in k$, $1 \leq i \leq r$, is a quadratic map that permits composition:

$$\Theta_\Omega(1_D) = \mathbf{1}_J, \quad \Theta_\Omega(xy) = \Theta_\Omega(x)\Theta_\Omega(y) \tag{1}$$

for all $x, y \in D$. In particular, $\Theta_\Omega(x) \in \mathrm{GL}(J)$ for all $x \in D^\times$. Moreover, Θ_Ω is compatible with base change: $(\Theta_\Omega)_R = \Theta_{\Omega_R}$, $\Omega_R := (c_{1R}, \ldots, c_{rR})$, for all $R \in k$-**alg**.

Proof All assertions are obvious except, possibly, the property of Θ_Ω permitting composition. But this follows immediately from Prop. 32.12 since $\Theta_\Omega(x) = \sum_{i \leq j} \gamma_i\gamma_j E_{ij}(\Omega)$. □

32.14 Peirce triples. By a *Peirce triple*, we mean an *ordered* triple of *unordered* pairs of positive integers. Thus a Peirce triple has the form

$$(ij, lm, np) := (\{i, j\}, \{l, m\}, \{n, p\})$$

for integers $i, j, l, m, n, p > 0$. A Peirce triple (ij, lm, np) will always be identified with the Peirce triple (np, lm, ij). It is said to be *connected* if (up to the identification just defined) it can be written in the form (ij, jm, mp). For example, the Peirce triple $(43, 23, 12)$ is connected but $(54, 23, 12)$ is not.

32.15 Theorem (Multiple Peirce decomposition)**.** *Let $\Omega = (c_1, \ldots, c_r)$ be a complete orthogonal system of idempotents in J.*

(a) *Setting $J_{ij} := J_{ij}(\Omega) := \mathrm{Im}(E_{ij}(\Omega))$ in the notation of Prop. 32.12, we have $J_{ij} = J_{ji}$ for $1 \leq i, j \leq r$ and*

$$J = \bigoplus_{1 \leq i \leq j \leq r} J_{ij} \tag{1}$$

as a direct sum of submodules, called the Peirce components of J relative to Ω. *Furthermore, the following relations hold, for all* $i, j = 1, \dots, r$*:*

$$J_2(c_i) = J_{ii}, \quad J_1(c_i) = \sum_{l \neq i} J_{il}, \quad J_0(c_i) = \sum_{l,m \neq i} J_{lm}, \tag{2}$$

$$J_{ij} = J_1(c_i) \cap J_1(c_j) \qquad (i \neq j). \tag{3}$$

(b) *More generally, if* $I \subseteq \{1, \dots, r\}$*, then* $c_I := \sum_{i \in I} c_i$ *is an idempotent in* J *with the Peirce components*

$$J_2(c_I) = \sum_{i,j \in I} J_{ij}, \quad J_1(c_I) = \sum_{i \in I, j \notin I} J_{ij}, \quad J_0(c_I) = \sum_{i,j \notin I} J_{ij}. \tag{4}$$

(c) *The composition rule*

$$\{J_{ij} J_{jl} J_{lm}\} \subseteq J_{im} \tag{5}$$

holds for all $i, j, l, m = 1, \dots, r$*. Moreover, if the Peirce triple* (ij, jl, ij) *is connected, there exists a unique* $m = 1, \dots, r$ *such that* $ij = lm$*, and we have*

$$U_{J_{ij}} J_{jl} \subseteq J_{im}. \tag{6}$$

In particular,

$$U_{J_{ij}} J_{ij} \subseteq J_{ij}. \tag{7}$$

Finally, if (ij, lm, np) *(*resp. (ij, lm, ij)*) is not connected, then*

$$\{J_{ij} J_{lm} J_{np}\} = \{0\} \quad (\textit{resp. } U_{J_{ij}} J_{lm} = \{0\}). \tag{8}$$

Proof (a), (b). The first assertion of (a) and eqn. (1) follow immediately from Prop. 32.12, eqn. (3) is a consequence of (2), and (2) is a special case of (4). In order to complete the proof of (a) and (b) , it therefore suffices to establish (4). To this end, we put $d_I := 1_J - c_I = \sum_{i \notin I} c_i$ and apply Thm. 32.2 to obtain

$$\begin{aligned} J_2(c_I) &= \operatorname{Im}(U_{c_I}) = \operatorname{Im}\Big(\sum_{i,j \in I, i \leq j} E_{ij}\Big) = \sum_{i,j \in I} J_{ij}, \\ J_1(c_I) &= \operatorname{Im}(U_{c_I, d_I}) = \operatorname{Im}\Big(\sum_{i \in I, j \notin I} E_{ij}\Big) = \sum_{i \in I, j \notin I} J_{ij}, \\ J_0(c_I) &= \operatorname{Im}(U_{d_I}) = \sum_{i,j \notin I} J_{ij}. \end{aligned}$$

(c) Let $R := k[\mathbf{t}_1^{\pm 1}, \dots, \mathbf{t}_r^{\pm 1}]$ be the ring of Laurent polynomials over k in the

variables $\mathbf{t}_1, \dots, \mathbf{t}_r$, which is free as a k-module with basis $(\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r})_{i_1,\dots,i_r \in \mathbb{Z}}$. Thus the identifications of 12.4 imply

$$J \subseteq J_R = \bigoplus_{i_1,\dots,i_r \in \mathbb{Z}} (\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} J),$$

$$\mathrm{End}_k(J) \subseteq \mathrm{End}_k(J)_R = \bigoplus_{i_1,\dots,i_r \in \mathbb{Z}} (\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} \mathrm{End}_k(J)) \subseteq \mathrm{End}_R(J_R)$$

as direct sums of k-modules. We now claim

$$w := \sum_{\lambda=1}^{r} \mathbf{t}_\lambda c_\lambda \in J_R^\times \quad \text{and} \quad w^{-1} = \sum_{\lambda=1}^{r} \mathbf{t}_\lambda^{-1} c_\lambda. \tag{9}$$

Indeed, since $\mathbf{t}_\lambda \in R^\times$ for $1 \le \lambda \le r$, Cor. 32.13 shows not only $U_w \in \mathrm{GL}(J_R)$ but also $U_{w'} = U_w^{-1}$, where $w' = \sum \mathbf{t}_\lambda^{-1} c_\lambda$. Hence $w \in J_R^\times$ by Prop. 31.2, and since $c_\lambda \in J_{\lambda\lambda}$ by (2), we conclude

$$U_w w' = \sum_{i \le j} \mathbf{t}_i \mathbf{t}_j E_{ij} \sum_{\lambda} \mathbf{t}_\lambda^{-1} c_\lambda = \sum_{i=1}^{r} \mathbf{t}_i^2 \mathbf{t}_i^{-1} c_i = \sum_{i=1}^{r} \mathbf{t}_i c_i = w,$$

which in turn implies $w' = U_w^{-1} w = w^{-1}$ by (31.2.1). Next we claim

$$J_{ij} = \{x \in J \mid U_w x = \mathbf{t}_i \mathbf{t}_j x\} = \{x \in J \mid U_{w^{-1}} x = \mathbf{t}_i^{-1} \mathbf{t}_j^{-1} x\}. \tag{10}$$

Indeed, given $x \in J$, the expansion $U_w x = \sum_{\lambda \le \mu} \mathbf{t}_\lambda \mathbf{t}_\mu E_{\lambda\mu} x$, where $E_{\lambda\mu} x \in J_{\lambda\mu}$, combined with (1) yields the first equation of (10), while the second follows from the first. We now put

$$T := \{\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} \mid i_1, \dots, i_r \in \mathbb{Z}\}, \quad T_0 := \{\mathbf{t}_i \mathbf{t}_j \mid 1 \le i, j \le r\}$$

and claim

(∗) *Every $t \in T$ such that $U_w x = tx$ for some non-zero $x \in J$ belongs to T_0.*

In order to see this, we write $x = \sum_{i \le j} x_{ij}$, $x_{ij} \in J_{ij}$, and deduce

$$\sum_{i \le j} t x_{ij} = tx = U_w x = \sum_{i \le j} \mathbf{t}_i \mathbf{t}_j x_{ij}$$

from (10), and comparing Peirce components, the assertion follows. Now fix integers $i, j, l, m, n, p = 1, \dots, r$ and $x \in J_{ij}$, $y \in J_{lm}$, $z \in J_{np}$. Then we claim

$$U_w\{xyz\} = \mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} \mathbf{t}_n \mathbf{t}_p \{xyz\}, \tag{11}$$

$$U_w U_x y = \mathbf{t}_i^2 \mathbf{t}_j^2 \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} U_x y. \tag{12}$$

In order to prove (11), we apply (9), (10), (29a.3) and obtain

$$U_w\{xyz\} = U_w U_{x,z} U_w U_{w^{-1}} y = U_{U_w x, U_w z} U_{w^{-1}} y = U_{\mathbf{t}_i \mathbf{t}_j x, \mathbf{t}_n \mathbf{t}_p z} \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} y,$$

hence (11). Similarly,

$$U_w U_x y = U_w U_x U_w U_{w^{-1}} y = U_{U_w x} U_{w^{-1}} y = U_{\mathbf{t}_i \mathbf{t}_j x} \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} y,$$

and this yields (12). Now (5) follows by specializing $l = j, n = m = l, p = m$ in (11) and applying (10). Next suppose the Peirce triple (ij, jl, ij) is connected. By Exc. 32.21 below, there is a unique $m = 1, \dots, r$ such that $ij = lm$, and specializing $l = j$, $m = l$ in (12) gives $\mathbf{t}_i^2 \mathbf{t}_j^2 \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} = \mathbf{t}_i \mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} = \mathbf{t}_i \mathbf{t}_m$, hence (6), which for $l = i$ specializes to (7). It remains to establish (8). To this end, assume first that (ij, lm, np) is not connected. If $\{i, j\} \cap \{l, m\} = \emptyset = \{l, m\} \cap \{n, p\}$, then $\mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} \mathbf{t}_n \mathbf{t}_p \notin T_0$, and (∗) implies $\{xyz\} = 0$. Otherwise, since the k-module $\{J_{ij} J_{lm} J_{np}\}$ remains unaffected by the identification of Peirce triples described in 32.14, Exc. 32.21 below allows us to assume $l = n = j$, $m = l$, $p = n$, with $l \neq i, j, n$, which implies $\mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} \mathbf{t}_n \mathbf{t}_p = \mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} \mathbf{t}_n \notin T_0$, hence again $\{xyz\} = 0$. This proves the first part of (8). As to the second, assume that (ij, lm, ij) is not connected. If $\{i, j\} \cap \{l, m\} = \emptyset$, the $\mathbf{t}_i^2 \mathbf{t}_j^2 \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} \notin T_0$, and we conclude $U_x y = 0$ from (∗). Otherwise, we may assume $l = j$, put $m := l$ and have $i \neq l \neq j$, hence $\mathbf{t}_i^2 \mathbf{t}_j^2 \mathbf{t}_l^{-1} \mathbf{t}_m^{-1} = \mathbf{t}_i^2 \mathbf{t}_j \mathbf{t}_l^{-1} \notin T_0$, This again implies $U_x y = 0$ and completes the proof of (8). □

32.16 Corollary. *Let $\Omega = (c_1, \dots, c_r)$ be a complete orthogonal system of idempotents in J.*

(a) *For $R \in k$-**alg**, $\Omega_R := (c_{1R}, \dots, c_{rR})$ is a complete orthogonal system of idempotents in J_R and there are canonical identifications*

$$(J_R)_{ij}(\Omega_R) = J_{ij}(\Omega)_R \qquad (1 \leq i, j \leq r). \tag{1}$$

(b) *For $1 \leq i \leq r$, the k-module $J_{ii}(\Omega)$ is a Jordan algebra over k with unit element c_i whose U-operator is derived from the U-operator of J by means of restriction. Moreover $\bigoplus_{i=1}^r J_{ii}(\Omega)$ is a direct sum of ideals and a subalgebra of J.*

(c) *The Peirce components of J relative to Ω satisfy the bilinear composition rules*

$$J_{ij}(\Omega) \circ J_{jl}(\Omega) \subseteq J_{il}(\Omega), \quad J_{ij}(\Omega) \circ J_{ij}(\Omega) \subseteq J_{ii}(\Omega) + J_{jj}(\Omega)$$

for $1 \leq i \leq j \leq l \leq r$.

Proof This is established in exactly the same manner as Cor. 32.3 has been derived from Thm. 32.2. □

32.17 Example. Let's consider the Multiple Peirce Decomposition for $J =$

$\mathrm{Her}_3(\mathbb{D})$ with respect to the complete system (c_1, c_2, c_3) of orthogonal idempotents where $c_i := e_{ii}$. Consulting the calculation for the Singular Peirce Decomposition in 32.6 and applying symmetry, we find that $J_{ii} = \mathbb{R}e_{ii}$ and, for $ij = 12$, 23, or 31, we have $J_{ij} = \mathbb{D}[ij]$. To say the same thing in a different way: J_{ij} consists of elements that have zeros except possibly in the (i, j) and (j, i)-entries.

Exercises

32.18. Show that J is linear at c, for every idempotent $c \in J$.

32.19. Let $c \in J$ be an idempotent and suppose $v \in J_1(c)$ is invertible in J. Prove that U_v via restriction induces an isotopy from $J_2(c)$ onto $J_0(c)$. Moreover, this isotopy is an isomorphism if and only if $v^2 = 1_J$.

32.20. Let c be an idempotent in J and put $J_i := J_i(c)$ for $i = 0, 1, 2$. Then prove that

$$\varphi\colon J_2 \longrightarrow \mathrm{End}_k(J_1), \quad x \longmapsto V_x|_{J_1},$$

is a homomorphism of Jordan algebras. Conclude that, if the Jordan algebra J_2 is simple and $J_1 \neq \{0\}$, then J_2 is special.

Remark. By a theorem of McCrimmon [188], if J is simple, then so is J_2. Moreover, if $c \neq 0, 1_J$, then $J_1 \neq \{0\}$ by Cor. 32.3 (b). Thus for a simple Jordan algebra J and an idempotent $c \neq 0, 1_J$ in J, the Jordan algebra $J_2(c)$ is special.

32.21. Show for a Peirce triple $T := (ij, lm, np)$ that the following conditions are equivalent.

(i) T is not connected.
(ii) Always up to the identification of 32.14, either $\{i, j\} \cap \{l, m\} = \emptyset$ or

$$T = (ij, jm, jp), \quad m \neq i, j, p.$$

Conclude that a Peirce triple (ij, jl, ij) is connected if and only if $l = i$ or $l = j$, in which case there is a unique positive integer m such that $ij = lm$.

32.22. *The multiple Peirce decomposition for alternative algebras* (cf. Schafer [254]). Let A be a unital alternative algebra over k and $\Omega := (c_1, \ldots, c_r)$ a complete orthogonal system of idempotents in A.

(a) Put

$$E_{ij} := E_{ij}(\Omega) := L_{c_i} R_{c_j} \qquad (1 \leq i, j \leq r) \tag{1}$$

and show that $(E_{ij})_{1 \leq i,j \leq r}$ is a family of orthogonal projections of A whose sum is the identity. Conclude

$$A = \bigoplus_{1 \leq i,j \leq r} A_{ij} \tag{2}$$

as a direct sum of k-modules, where $A_{ij} := A_{ij}(\Omega) = \mathrm{Im}(E_{ij})$ for $1 \leq i, j \leq r$. The A_{ij} are called the *Peirce components* of A relative to Ω.

(b) Show

$$A_{ij} = \{x \in A \mid c_l x = \delta_{il} x, \quad x c_l = \delta_{jl} x \ \ (1 \le l \le r)\} \tag{3}$$

for $1 \le i, j \le r$.

(c) Prove that the Peirce components of A relative to Ω satisfy the following composition rules, for all $i, j, l, m = 1, \dots, r$.

$$A_{ij} A_{jl} \subseteq A_{il}, \tag{4}$$

$$A_{ij}^2 \subseteq A_{ji}, \tag{5}$$

$$A_{ij} A_{lm} = \{0\} \qquad (j \ne l, \ \ (i, j) \ne (l, m)) \tag{6}$$

Finally, prove $x^2 = 0$ for all $x \in A_{ij}$, $1 \le i, j \le r$, $i \ne j$.

(d) Note by Exc. 28.25 (b) that Ω is a complete orthogonal system of idempotents in $A^{(+)}$, with Peirce components $A_{ij}^{(+)} := A_{ij}^{(+)}(\Omega)$ $(1 \le i \le j \le r)$, and prove

$$A_{ii}^{(+)} = A_{ii} \quad (1 \le i \le r), \qquad A_{ij}^{(+)} = A_{ij} \oplus A_{ji} \quad (1 \le i < j \le r).$$

32.23. *Connectedness in complete orthogonal systems of idempotents* (Jacobson [140, Prop. 5.3.3]). Let $\Omega = (c_1, \dots, c_r)$ be a complete orthogonal system of idempotents in J, with Peirce components $J_{ij} = J_{ij}(\Omega)$, $1 \le i, j \le r$. Fix indices $i, j = 1, \dots, r$ with $i \ne j$ and prove:

(a) For $v_{ij} \in J_{ij}$, the following conditions are equivalent.

(i) $v_{ij} \in J_2(c_i + c_j)^\times$.

(ii) $U_{v_{ij}} J_{ii}^\times \subseteq J_{jj}^\times$, $U_{v_{ij}} J_{jj}^\times \subseteq J_{ii}^\times$.

(iii) $U_{v_{ij}} c_i \in J_{jj}^\times$, $U_{v_{ij}} c_j \in J_{ii}^\times$.

(iv) $v_{ij}^2 \in (J_{ii} \oplus J_{jj})^\times$.

In this case, c_i and c_j are said to be *connected by* v_{ij}. We say c_i and c_j are *connected* if $v_{ij} \in J_{ij}$ exists connecting c_i and c_j. And finally, we say Ω is *connected* if c_i and c_j are connected, for all $i, j = 1, \dots, r$ distinct.

(b) For $v_{ij} \in J_{ij}$, the following conditions are equivalent.

(i) $v_{ij}^2 = c_i + c_j$.

(ii) $U_{v_{ij}} c_i = c_j$, $U_{v_{ij}} c_j = c_i$

In this case, c_i and c_j are said to be *strongly connected by* v_{ij}. We say c_i and c_j are *strongly connected* if $v_{ij} \in J_{ij}$ exists strongly connecting c_i and c_j. And finally, we say Ω is *strongly connected* if c_i and c_j are strongly connected, for all $i, j = 1, \dots, r$ distinct.

(c) Let $1 \le l \le r$ and assume $i \ne l \ne j$. If c_i and c_j are (strongly) connected by $v_{ij} \in J_{ij}$, and c_j and c_l are (strongly) connected by $v_{jl} \in J_{jl}$, then c_i and c_l are (strongly) connected by $v_{ij} \circ v_{jl} \in J_{il}$.

32.24. *Isotopes and complete orthogonal systems of idempotents* (Jacobson [140, Prop. 5.3.4]). Let $\Omega = (c_1, \dots, c_r)$ be a complete orthogonal system of idempotents in J, with Peirce components $J_{ij} := J_{ij}(\Omega)$, $1 \le i, j \le r$. Following Cor. 32.16 (b), consider the subalgebra of J defined by

$$\mathrm{Diag}_\Omega(J) := \bigoplus_{i=1}^{r} J_{ii} \tag{1}$$

as a direct sum of ideals. For $1 \le i \le r$, let $p_i \in J_{ii}^\times$ and put

$$p := \sum_{i=1}^{r} p_i \in \mathrm{Diag}_\Omega(J)^\times \subseteq J^\times. \tag{2}$$

(a) Put $c_i^{(p)} := p_i^{-1} \in J_{ii}$ (the inverse of p_i in J_{ii}) for $1 \le i \le r$ and show that

$$\Omega^{(p)} := (c_1^{(p)}, \dots, c_r^{(p)})$$

is a complete orthogonal system of idempotents in the isotope $J^{(p)}$ such that

$$J_{ij}^{(p)} := (J^{(p)})_{ij}(\Omega^{(p)}) = J_{ij} \tag{3}$$

for $1 \le i, j \le r$. In particular, $\mathrm{Diag}_{\Omega^{(p)}}(J^{(p)}) = \mathrm{Diag}_\Omega(J)^{(p)}$.

(b) Let also $q_i \in J_{ii}^\times$ for $1 \le i \le r$ and $q := \sum_{i=1}^r q_i \in \mathrm{Diag}_\Omega(J)^\times$. Then show $(\Omega^{(p)})^{(q)} = \Omega^{(U_p q)}$.

(c) Assume c_1 and c_i are connected for $2 \le i \le r$ (cf. Exc. 32.23). Show that there exist $p_i \in J_{ii}^\times$, $1 \le i \le r$, such that $c_1^{(p)}$ and $c_i^{(p)}$ with $p := \sum_{j=1}^r p_j$ are strongly connected in their capacity as members of the complete orthogonal system $\Omega^{(p)}$ of idempotents in $J^{(p)}$.

32.25. *Lifting of complete orthogonal systems of idempotents.* Let $\varphi\colon J \to J'$ be a surjective homomorphism of Jordan algebras and suppose $\mathrm{Ker}(\varphi) \subseteq J$ is a nil ideal. Show that every complete orthogonal system $(c'_1, \dots, c'_r)$ of idempotents in J' can be lifted to J: there exists a complete orthogonal system $(c_1, \dots, c_r)$ of idempotents in J such that $\varphi(c_i) = c'_i$ for $1 \le i \le r$.

32.26. *Simple Jordan algebras of Clifford type* (compare Jacobson-McCrimmon [144, Thm. 11]). Let (M, q, e) be a non-zero pointed quadratic module over a field F and suppose q is non-degenerate. Show that the Jordan algebra $J(M, q, e)$ is either simple or isomorphic to $(F \times F)^{(+)}$.

VI

Cubic Jordan algebras

With the aim of describing an adequate framework for the study of octonion algebras over commutative rings, we investigated in Chap. IV a class of algebraic structures where all elements satisfy a universal algebraic equation of degree 2. In particular, we considered multiplicative conic alternative algebras in section 17 which, as a category, allow a natural faithful (though not full) embedding into arbitrary (unital) alternative algebras (17.7). Within this category, we then singled out composition algebras by certain regularity conditions (Thm. 19.13). And, finally, we defined octonion algebras as composition algebras of the greatest possible rank.

In the present chapter, an analogous approach will be adopted for the study of Albert algebras over commutative rings. After having prepared the ground by introducing the concept of a cubic norm structure in section 33, we proceed to define cubic Jordan algebras in section 34, where all elements satisfy a universal algebraic equation of degree 3, and which, as a category, allow a natural faithful non-full embedding into arbitrary Jordan algebras. We then consider Freudenthal algebras as cubic Jordan algebras with certain regularity properties, which in turn will allow us to define Albert algebras as Freudenthal algebras of the greatest possible rank.

In order to carry out this program, quite a few technical difficulties that did not show up in the octonionic setting will have to be overcome. These difficulties, some of which are already implicit in the need to consider para-quadratic algebras (section 28) rather than linear non-associative ones, will be addressed further as we go along and show up, most conspicuously, in section 35. Cubic Jordan matrix algebras, the most "hands-on" examples of cubic Jordan algebras, will be investigated in section 36, emphasizing a presentation that, under very general circumstances, commutes with arbitrary base change. Section 37 is devoted to elementary idempotents in cubic Jordan algebras and culminates in a proof of the Jacobson co-ordinatization theorem. The chapter concludes with exhibiting classifying invariants of reduced Freudenthal algebras over fields in section 41.

33 Cubic norm structures

Cubic norm structures form an important auxiliary notion that will pave the way to our understanding of cubic Jordan algebras. They will be investigated here by closely following the treatment of McCrimmon [183].

Throughout k stands for an arbitrary commutative ring. Relaxing our previous conventions, we do not distinguish anymore between the notation for a polynomial law $f\colon M \to N$ and that for its induced set maps $f = f_R\colon M_R \to N_R, R \in k\text{-}\mathbf{alg}$. We begin with a preliminary concept of a more technical nature that will be included here only for convenience.

33.1 Cubic arrays. By a *cubic array* over k we mean a k-module X together with

- a distinguished element $1_X \in X$ (the *base point*),
- a quadratic map $\sharp = \sharp_X\colon X \to X$, $x \mapsto x^\sharp$ (the *adjoint*, dependence on X most of the time being understood),
- a cubic form $N_X\colon X \to k$ (the *norm*)

such that the following conditions are fulfilled.

(i) $1_X \in X$ is unimodular.
(ii) The *base point identities* hold:

$$1_X^\sharp = 1_X, \qquad N_X(1_X) = 1. \tag{1}$$

We claim: *If X is projective as a k-module, then (ii) implies (i).* Indeed, Exercise 12.44 yields a trilinear form $T\colon X \times X \times X \to k$ such that $N_X(x) = T(x, x, x)$ in all scalar extensions, so the linear form $\lambda\colon X \to k$, $x \mapsto T(x, 1_X, 1_X)$ by (ii) has $\lambda(1_X) = 1$, making $1_X \in X$ unimodular, as claimed.

Given another cubic array X' over k, a *homomorphism* from X to X' is defined as a linear map $\varphi\colon X \to X'$ preserving base points, adjoints and norms: $\varphi(1_X) = 1_{X'}$, $\varphi(x^{\sharp_X}) = \varphi(x)^{\sharp_{X'}}$ for all $x \in X$, and $N_{X'} \circ \varphi = N_X$ as polynomial laws over k. In this way, we obtain the category of cubic arrays over k, denoted by k-**cuar**. For $R \in k$-**alg**, the R-module X_R together with the base point $1_{X_R} := (1_X)_R \in X_R$, the adjoint $\sharp = \sharp_{X_R} = (\sharp_X)_R\colon X_R \to X_R$ defined as the R-quadratic extension of the adjoint of X, and the norm $N_{X_R} := N_X \otimes R\colon X_R \to R$ as a cubic form over R is a cubic array over R, called the *scalar extension* or *base change* of X from k to R.

33.2 Traces of cubic arrays. Let X be a cubic array over k. We write

$$x \times y := (D\sharp)(x, y) = (x + y)^\sharp - x^\sharp - y^\sharp \tag{1}$$

for the bilinearization of the adjoint and, with regard to the norm, combine the

notational simplifications of Exc. 12.40 with (12.16.2) and Cor. 12.22 to obtain not only

$$N_X(x,y) = (DN_X)(x,y) = (D^2N_X)(y,x) = (\partial_y N_X)(x) \tag{2}$$

but also

$$N_X(x,y,z) = (\partial_y\partial_z N_X)(x) = (\Pi^{(1,1,1)}N_X)(x,y,z) \tag{3}$$

for the total linearization of the cubic form N_X, which is therefore trilinear and totally symmetric in x, y, z (cf. 12.10 (c)). Recall further from Exc. 12.40 that

$$N_X(x+y) = N_X(x) + N_X(x,y) + N_X(y,x) + N_X(y), \tag{4}$$
$$N_X(x,y,z) = N_X(x+y,z) - N_X(x,z) - N_X(y,z). \tag{5}$$

The linear map

$$T_X\colon X \longrightarrow k, \quad y \longmapsto T_X(y) := N_X(1_X, y), \tag{6}$$

is called the *linear trace* of X, while the quadratic form

$$S_X\colon X \longrightarrow k, \quad y \longmapsto S_X(y) := N_X(y, 1_X) \tag{7}$$

is called the *quadratic trace* of X. And finally, we define the *bilinear trace* of X as the symmetric bilinear form $T_X\colon X \times X \to k$ given by

$$\begin{aligned} T_X(y,z) &= (\partial_y N_X)(1_X)(\partial_z N_X)(1_X) - (\partial_y\partial_z N_X)(1_X) \\ &= N_X(1_X,y)N_X(1_X,z) - N_X(y,z,1_X), \end{aligned} \tag{8}$$

which up to a sign agrees with the logarithmic Hessian of N_X at 1_X:

$$T_X(y,z) = -(\partial_y\partial_z \log N_X)(1_X) = -\partial_y\Big(\frac{\partial_z N_X}{N_X}\Big)(1_X). \tag{9}$$

In view of (5)–(7), we may rewrite (8) as

$$T_X(y,z) = T_X(y)T_X(z) - S_X(y,z). \tag{10}$$

Combining all this with Euler's differential equation (12.16.3) and (33.1.1), we obtain

$$T_X(1_X) = S_X(1_X) = 3, \quad T_X(y,1_X) = T_X(y) \tag{11}$$

since (5) and (7) yield $S_X(y,1_X) = N_X(y,1_X,1_X) = N(1_X,1_X,y) = 2N(1_X,y)$, hence

$$S_X(y,1_X) = 2T_X(y). \tag{12}$$

If $\varphi\colon X \to X'$ is a homomorphism of cubic arrays, then the chain rule (12.17.4) and (5) yield

$$N_{X'}(\varphi(x),\varphi(y)) = N_X(x,y), \quad N_{X'}(\varphi(x),\varphi(y),\varphi(z)) = N_X(x,y,z). \tag{13}$$

Combining this with (6)–(8) and the property of φ to preserve base points, we conclude that φ preserves (bi-)linear and quadratic traces:

$$T_{X'}(\varphi(y)) = T_X(y), \quad T_{X'}(\varphi(y),\varphi(z)) = T_X(y,z), \quad S_{X'}(\varphi(y)) = S_X(y). \tag{14}$$

33.3 Regularity. A cubic array X over k is said to be *regular* if it is finitely generated projective as a k-module and its bilinear trace, T_X, is regular as a symmetric bilinear form, i.e., if T_X induces a linear isomorphism from the k-module X onto its dual module X^* in the usual way. This notion is clearly stable under base change: if X is regular, then so is X_R, for all $R \in k$-**alg**.

33.4 The concept of a cubic norm structure. By a *cubic norm structure* over k we mean a cubic k-array X satisfying the following identities *strictly*, i.e., in all scalar extensions:

$$1_X \times x = T_X(x)1_X - x \qquad \text{(unit identity)}, \tag{1}$$

$$N_X(x,y) = T_X(x^\sharp, y) \qquad \text{(gradient identity)}, \tag{2}$$

$$x^{\sharp\sharp} = N_X(x)x \qquad \text{(adjoint identity)}. \tag{3}$$

A *homomorphism* of cubic norm structures is defined as a homomorphism of them as cubic arrays. Thus cubic norm structures over k form a full subcategory of k-**cuar** denoted by k-**cuno**. By definition, cubic norm structures are stable under base change, so if X is a cubic norm structure over k, then the cubic array X_R over R is, in fact, a cubic norm structure, for all $R \in k$-**alg**.

33.5 Cubic norm substructures. Let X be a cubic array over k. By a *cubic subarray* of X we mean a cubic array Y such that $Y \subseteq X$ is a k-submodule and the inclusion $i\colon Y \to X$ is a homomorphism of cubic arrays. This is equivalent to requiring (i) $1_X \in Y$, (ii) $Y^\sharp \subseteq Y$, i.e., Y is stabilized by the adjoint of X, and (iii) $N_X \circ i = N_Y$ as polynomial laws over k, i.e., $(N_X)_R \circ i_R = (N_Y)_R$ as set maps $Y_R \to R$, for all $R \in k$-**alg**. Thus any submodule Y of X, with corresponding inclusion $i\colon Y \to X$, that contains 1_X and is stabilized by the adjoint of X may canonically be regarded as a cubic subarray of X, with base point $1_Y = 1_X$, adjoint $\sharp\colon Y \to Y$ given by restricting the adjoint $\sharp\colon X \to X$ of X to Y, and norm $N_Y := N_X|_Y := N_X \circ i$. In this case, the (bi-)linear and quadratic traces of Y by (33.2.14) are just the corresponding objects of X restricted to Y (resp. to $Y \times Y$).

Now suppose X is a cubic norm structure over k and let $Y \subseteq X$ be a cubic

subarray. Then it follows either from Cor. 12.11 or from Exc. 33.14 that Y is, in fact, a cubic norm structure, called a *cubic norm substructure* of X. If $E \subseteq X$ is an arbitrary subset, the smallest cubic norm substructure of X containing E is called the cubic norm substructure *generated by* E.

Our next aim will be to derive a number of basic identities for cubic norm structures. In order to do so, we require two preparations, the first one connecting cubic norm structures with para-quadratic algebras, the second one spelling out a sufficient condition for elements of a cubic array to be unimodular.

33.6 Connecting with para-quadratic algebras. Let X be a cubic array over k. We define a U-operator, i.e., a quadratic map $U\colon X \to \mathrm{End}_k(X)$, $x \mapsto U_x$, by

$$U_x y := T_X(x,y)x - x^\sharp \times y \qquad (x, y \in X), \tag{1}$$

which in analogy to (28.1.3), (28.1.5) linearizes to the associated triple product

$$\{xyz\} := V_{x,y}z := U_{x,z}y = T_X(x,y)z + T_X(y,z)x - (z \times x) \times y \tag{2}$$

for $x, y, z \in X$. Moreover, if X is a cubic norm structure, then the unit identity (33.4.1) shows $U_{1_X} = \mathbf{1}_X$. Hence the k-module X together with the U-operator (1) and the base point $1_X \in X$ forms a para-quadratic algebra over k, which we denote by $J(X)$ and call the para-quadratic algebra *associated with* or *corresponding to* X. It will be shown in due course to be a Jordan algebra. Passing from X to $J(X)$ is clearly compatible with base change: $J(X_R) = J(X)_R$ for all $R \in k$-**alg**.

33.7 Lemma. *Let X be a cubic array over k such that*

$$\{xx^\sharp y\} = 2N_X(x)y$$

for all $x, y \in X$. Then every element $x \in X$ such that $N_X(x) \in k^\times$ is unimodular.

Proof Since $1_X \in X$ is unimodular by definition, there exists a linear form $\lambda\colon X \to k$ such that $\lambda(1_X) = 1$. Now suppose $x \in X$ satisfies $N_X(x) \in k^\times$. Thanks to Euler's differential equation combined with the hypothesis of the lemma, the linear form

$$\lambda_x\colon X \longrightarrow k, \quad y \longmapsto N_X(x)^{-1}(N_X(x,y) - \lambda(\{yx^\sharp 1_X\}))$$

satisfies $\lambda_x(x) = 1$. Hence x is unimodular. □

33.8 Basic identities for cubic norm structures. Let X be a cubic norm structure over k. Using the abbreviations $1 := 1_X$, $N := N_X$, $T := T_X$, $S := S_X$, we claim that *the identities in Figure 33a hold strictly in X.* (In compiling the list

$$1^\sharp = 1, \quad N(1) = 1, \tag{1}$$

$$T(1) = S(1) = 3, \quad T(y,1) = T(y), \quad S(y,1) = 2T(y), \tag{2}$$

$$1 \times x = T(x)1 - x, \tag{3}$$

$$N(x,y) = T(x^\sharp, y), \tag{4}$$

$$x^{\sharp\sharp} = N(x)x, \tag{5}$$

$$N(x+y) = N(x) + T(x^\sharp, y) + T(x, y^\sharp) + N(y), \tag{6}$$

$$T(x \times y, z) = T(x, y \times z), \tag{7}$$

$$x^\sharp \times (x \times y) = N(x)y + T(x^\sharp, y)x, \tag{8}$$

$$(x \times y) \times (x \times z) + x^\sharp \times (y \times z) = T(x^\sharp, y)z + T(x^\sharp, z)y + T(x \times y, z)x, \tag{9}$$

$$x^\sharp \times y^\sharp + (x \times y)^\sharp = T(x^\sharp, y)y + T(x, y^\sharp)x, \tag{10}$$

$$T(x^\sharp, x) = 3N(x), \tag{11}$$

$$S(x) = T(x^\sharp), \tag{12}$$

$$S(x,y) = T(x \times y) = T(x)T(y) - T(x,y), \tag{13}$$

$$x^\sharp \times x = (T(x)S(x) - N(x))1 - S(x)x - T(x)x^\sharp, \tag{14}$$

$$U_x y = T(x,y)x - x^\sharp \times y, \tag{15}$$

$$U_x(x \times y) = T(x^\sharp, y)x - N(x)y, \tag{16}$$

$$\{xx^\sharp y\} = 2N(x)y, \tag{17}$$

$$N(x^\sharp) = N(x)^2, \tag{18}$$

$$x \times (x^\sharp \times y) = N(x)y + T(x,y)x^\sharp, \tag{19}$$

$$(U_x y)^\sharp = U_{x^\sharp} y^\sharp = T(x^\sharp, y^\sharp)x^\sharp - N(x)x \times y^\sharp, \tag{20}$$

$$N(U_x y) = N(x)^2 N(y), \tag{21}$$

$$x^\sharp = x^2 - T(x)x + S(x)1, \tag{22}$$

$$x \times y = x \circ y - T(x)y - T(y)x + (T(x)T(y) - T(x,y))1, \tag{23}$$

$$T(x \circ y) = 2T(x,y), \tag{24}$$

$$(x \times y) \times (z \times w) + (y \times z) \times (x \times w) + (z \times x) \times (y \times w) \tag{25}$$
$$= T(x \times y, z)w + T(y \times z, w)x + T(z \times w, x)y + T(w \times x, y)z,$$

$$x \times (y \times (x \times z)) = T(x,y)x \times z + T(x^\sharp, z)y + T(y,z)x^\sharp - (x^\sharp \times y) \times z \tag{26}$$
$$= (U_x y) \times z + T(x^\sharp, z)y + T(y,z)x^\sharp,$$

$$x \times (y \times (z \times w)) + z \times (y \times (w \times x)) + w \times (y \times (x \times z)) \tag{27}$$
$$= T(x,y)z \times w + T(z,y)w \times x + T(w,y)x \times z + T(x \times z, w)y,$$

$$x \times (x \times y) = (T(x)S(x,y) + S(x)T(y) - T(x^\sharp, y))1 - \tag{28}$$
$$S(x,y)x - S(x)y - T(x)x \times y - T(y)x^\sharp - x^\sharp \times y,$$

$$N(x \times y) = T(x^\sharp, y)T(x, y^\sharp) - N(x)N(y), \tag{29}$$

$$\{xyz\} = V_{xy}z - V_{xz}y = T(x,y)z + T(y,z)x - (z \times x) \times y, \tag{30}$$

$$T(U_x y, z) = T(y, U_x z), \tag{31}$$

$$T(\{xyz\}, w) = T(z, \{yxw\}), \tag{32}$$

$$T(x \circ y, z) = T(x, y \circ z). \tag{33}$$

Table of Identities 33a Identities holding in a cubic norm structure.

of identities, we do not hesitate to include identities that have been introduced or derived earlier.)

Proof It clearly suffices to verify these identities for all $x, y, z, w \in X$. Moreover, thanks to Prop. 12.24, we may always assume if necessary that some of the elements involved have an invertible norm. Now, while the base point identities (1) are valid even in arbitrary cubic arrays and (3)–(5) belong to the very definition of a cubic norm structure, (2) has been observed already in (33.2.11), (33.2.12). Next, combining (33.2.4) with the gradient identity (4), we obtain (6). Differentiating the gradient identity gives $T(x \times y, z) = N(x, y, z)$, which is totally symmetric in x, y, z. Hence (7) follows. To establish (8), we differentiate the adjoint identity (5) by making use of the chain and the product rule. Linearizing still further and using (7) yields (9), while (10) follows from (5) combined with the second order chain and product rules (12.17.6), (12.17.7). To derive (11), we combine the gradient identity (4) with Euler's differential equation (12.3). The gradient identity (4) for $y = 1$ and (2) imply (12). To establish (13), we linearize (12) and apply (33.2.10). Similarly, specializing $y = 1$ in (8) and observing (3), we obtain (14), while (15) is just a repetition of (33.6.1). To derive (16), we combine (7) with (1), (8) and conclude $U_x(x \times y) = T(x, x \times y)x - x^\sharp \times (x \times y) = T(x \times x, y)x - N(x)y - T(x^\sharp, y)x$, hence (16) since $x \times x = 2x^\sharp$. Next, (15) linearized, (11) and (8) immediately imply (17). Combining this with Lemma 33.7, we can therefore conclude that *all elements of X with invertible norm are unimodular.* To establish (18), we assume $N(x) \in k^\times$, apply the adjoint identity (5) and obtain

$$N(x^\sharp)x^\sharp = x^{\sharp\sharp\sharp} = N(x)^2 x^\sharp. \tag{34}$$

Taking adjoints again, we deduce $N(x^\sharp)^2 x = N(x)^4 x$, hence $N(x^\sharp)^2 = N(x)^4 \in k^\times$ since x is unimodular. This shows that $N(x^\sharp) \in k^\times$, and (18) follows from (34). Turning to (19), we again assume that $N(x) \in k^\times$, replace x by $x^\sharp$ in (8), observe (18) and obtain $N(x)x \times (x^\sharp \times y) = N(x^\sharp)y + N(x)T(x, y)x^\sharp = N(x)(N(x)y + T(x, y)x^\sharp)$, hence (19). Now (20) follows by expanding the left-hand side and observing (19), (10) as well as the adjoint identity (5). In (21), we may assume that the norm of $U_x y$ is invertible since $U_1 1 = 1$. Then (20) and the adjoint identity yield $N(U_x y)U_x y = (U_x y)^{\sharp\sharp} = U_{x^{\sharp\sharp}} y^{\sharp\sharp} = N(x)^2 N(y)U_x y$, so the assertion follows from the unimodularity of $U_x y$. To derive (22), we note that $x^2 = U_x 1 = T(x, 1)x - x^\sharp \times 1$, whence the unit identity (3) and (12) lead to the desired conclusion. (23) follows immediately from linearizing (22) and observing (13). Combining (23) with (13), we deduce

$$T(x)T(y) - T(x, y) = T(x \times y) = T(x \circ y) - 2T(x)T(y) + 3(T(x)T(y) - T(x, y)),$$

hence (24). Next, linearizing (9), we obtain $(w\times y)\times(x\times z)+(x\times y)\times(w\times z)+(x\times w)\times(y\times z) = T(x\times w,y)z+T(x\times w,z)y+T(x\times y,z)w+T(w\times y,z)x$, and (7) yields (25). Similarly, (19) and (4) imply $z\times(x^\sharp\times y)+x\times((x\times z)\times y) = T(x^\sharp,z)y+T(z,y)x^\sharp+T(x,y)x\times z$, hence the first part of (26), while the remaining one now follows from (15). Linearizing (26) gives $x\times(y\times(w\times z))+w\times(y\times(x\times z)) = T(w,y)x\times z+T(x,y)w\times z+T(x\times w,z)y+T(y,z)x\times w-((x\times w)\times y)\times z$, and after interchanging w with z, we obtain (27). Similarly, (14) implies $(x\times y)\times x+x^\sharp\times y = (T(y)S(x)+T(x)S(x,y)-T(x^\sharp,y))1-S(x,y)x-S(x)y-T(x)x\times y-T(y)x^\sharp$, hence (28). In order to derive (29), we combine the third-order chain rule (Exc. 12.42) with the observations of 12.15 and the equations (12.16.3), (4) linearized, (8), (11) to obtain

$$(D^3(N\circ\sharp))(x,y) = 3N(x)N(y)+T(x^\sharp,y)T(x,y^\sharp)+N(x\times y).$$

On the other hand, the third order product rule (12.17.8) (for $n=3$) yields

$$(D^3N^2)(x,y) = 2N(x)N(y)+2T(x^\sharp,y)T(x,y^\sharp).$$

Comparing and invoking (18), we indeed end up with (29). Equation (30) has already been noted in (33.6.2). To derive (31), we expand the left-hand side by (15) and, using (7), obtain the expression $T(U_xy,z) = T(T(x,y)x-x^\sharp\times y,z) = T(x,y)T(x,z)-T(x^\sharp,y\times z)$, which is symmetric in y,z; hence (31) holds. Similarly, (30) yields $T(\{xyz\},w) = T(x,y)T(z,w)+T(y,z)T(x,w)-T((z\times x)\times y,w)$, which by (7) remains unchanged under the substitution $x\leftrightarrow y$, $z\leftrightarrow w$. This yields (32), while (33) follows from (23) and the fact that the right-hand side of $T(x\circ y,z) = T(x\times y,z)+T(x)T(y,z)+T(y)T(x,z)-T((T(x)T(y)-T(x,y))1,z) = T(x\times y,z)+T(x)T(y,z)+T(y)T(z,x)+T(z)T(x,y)-T(x)T(y)T(z)$ is totally symmetric in x,y,z. □

After these preparations, we are ready for the first main result of this section.

33.9 Theorem (McCrimmon [183, Thm. 1])**.** *Let X be a cubic norm structure over k. Then $J(X)$, the para-quadratic algebra associated with X, having base point 1_X and U-operator given by*

$$U_xy := T_X(x,y)x-x^\sharp\times y, \tag{1}$$

is a Jordan algebra over k such that the identities

$$x^3-T_X(x)x^2+S_X(x)x-N_X(x)1_X = 0, \tag{2}$$

$$x^4-T_X(x)x^3+S_X(x)x^2-N_X(x)x = 0, \tag{3}$$

$$U_xx^\sharp = N_X(x)x, \quad U_xx^{\sharp 2} = N_X(x)^2 1_X, \tag{4}$$

hold strictly in $J(X)$.

Proof For $J = J(X)$ to be a Jordan algebra we must show that the identities

$$U_{1_x} x = x, \tag{5}$$
$$U_{U_x y} z = U_x U_y U_x z, \tag{6}$$
$$U_x\{yxz\} = \{xyU_x z\} \tag{7}$$

hold for all $x, y, z \in X$. Here (5) follows immediately from J being para-quadratic (33.6). To establish (6), we abbreviate $1 := 1_X$, $N := N_X$, $T := T_X$, $S := S_X$ and first combine (33a.19) with (33a.7) to conclude

$$T(x \times y, x^\sharp \times z) = N(x)T(y,z) + T(x^\sharp, y)T(x,z) = T(x, (x^\sharp \times z) \times y). \tag{8}$$

Next we expand the left-hand side of (6), using the definition of the U-operator (1) and (33a.20). A short computation gives

$$U_{U_x y} z = (T(x,y)T(x,z) - T(x^\sharp \times y, z))U_x y \\ - T(x^\sharp, y^\sharp)x^\sharp \times z + N(x)(x \times y^\sharp) \times z.$$

Similarly, expanding the right-hand side of (6) and applying (33a.7), (33a.16), (33a.8), we obtain

$$U_x U_y U_x z = (T(x,y)T(x,z) - T(x^\sharp \times y, z))U_x y + N(x)T(y^\sharp, z)x \\ + N(x)T(x,z)y^\sharp - x^\sharp \times (y^\sharp \times (x^\sharp \times z)).$$

To establish (6), we therefore have to prove

$$x^\sharp \times (y^\sharp \times (x^\sharp \times z)) = N(x)T(y^\sharp, z)x + N(x)T(x,z)y^\sharp \\ + T(x^\sharp, y^\sharp)x^\sharp \times z - N(x)(x \times y^\sharp) \times z.$$

But this follows immediately from (33a.26) combined with the adjoint identity (33a.5). Finally, we must prove (7), which is less troublesome. One simply expands the left-hand side, using (1), (33.6.2), and applies (33a.16) to obtain

$$U_x\{yxz\} = T(x,y)U_x z + (T(x,y)T(x,z) - T(x^\sharp \times y, z))x \\ - T(x,z)x^\sharp \times y + N(x)y \times z.$$

Similarly, one expands the right-hand side, using (33a.19), and arrives at the same expression. Thus J is a Jordan algebra, and it remains to verify (2), (3), (4). Observing $T(x,x) = T(x)^2 - 2S(x)$ by (33a.13), we further obtain, using (33a.14),

$$\begin{aligned} x^3 &= U_x x = T(x,x)x - x^\sharp \times x \\ &= (T(x)^2 - 2S(x))x - (T(x)S(x) - N(x))1 + S(x)x + T(x)x^\sharp, \end{aligned}$$

which by (33a.22) yields (2). Before dealing with (3), we turn to (4). From (1), (33a.11) and (33a.5) we deduce $U_x x^\sharp = T(x, x^\sharp)x - x^\sharp \times x^\sharp = 3N(x)x - 2x^{\sharp\sharp} = 3N(x)x - 2N(x)x$, giving the first equation of (4). As to the second, we apply the first, (33a.22), (33a.12), (33a.5) and obtain $U_x x^{\sharp 2} = U_x(x^{\sharp\sharp} + T(x^\sharp)x^\sharp - S(x^\sharp)1) = N(x)x^3 + S(x)N(x)x - T(x)N(x)x^2$, and (2) completes the proof of (4).

Applying (4) and again (33a.22), we now conclude

$$\begin{aligned} x^4 = U_x x^2 &= U_x x^\sharp + T(x)U_x x - S(x)U_x 1 \\ &= N(x)x + T(x)x^3 - S(x)x^2, \end{aligned}$$

hence (3). Strictness is clear. □

For a cubic norm structure X over k, we henceforth refer to $J(X)$ as the *Jordan algebra associated with* or *corresponding to* X.

33.10 Corollary (McCrimmon [183, Thm. 2])**.** *Let X be a cubic norm structure over k and $J = J(X)$ the Jordan algebra associated with X. An element $x \in X$ is invertible in J if and only if $N_X(x)$ is invertible in k. In this case,*

$$x^{-1} = N_X(x)^{-1}x^\sharp, \quad (x^{-1})^\sharp = N_X(x)^{-1}x, \quad N_X(x^{-1}) = N_X(x)^{-1}. \tag{1}$$

Proof Put $1 := 1_X$, $N := N_X$. If $x \in J^\times$, then (33a.21) implies $1 = N(1) = N(U_x x^{-2}) = N(x)^2 N(x^{-2})$, hence $N(x) \in k^\times$. Conversely, assume $N(x) \in k^\times$ and put $y := N(x)^{-1}x^\sharp$. From (33.9.4) we then deduce $U_x y = x$, $U_x y^2 = 1$, hence $x \in J^\times$ and the first equation of (1) holds. Taking adjoints, we immediately obtain the second. In order to prove the third, we again apply (33a.21) to obtain $N(x) = N(U_x x^{-1}) = N(x)^2 N(x^{-1})$ and therefore $N(x^{-1}) = N(x)^{-1}$. □

33.11 Isotopes of cubic norm structures. Isotopes of Jordan algebras have a counterpart on the level of cubic norm structures which we now proceed to discuss. Let X be a cubic norm structure over k. Given an element $p \in X$ that is invertible in $J := J(X)$ and writing p^{-1} for the corresponding inverse (cf. Cor. 33.10), we claim that *the k-module $X^{(p)} := X$ together with the base point $1_{X^{(p)}} := 1_X^{(p)} \in X^{(p)}$, the adjoint $x \mapsto x^{(\sharp,p)}$ (a quadratic map $X \to X$), and the norm $N_{X^{(p)}} := N_X^{(p)}$ (a cubic form $X^{(p)} \to k$) defined respectively by*

$$1_{X^{(p)}} := 1_X^{(p)} := p^{-1}, \tag{1}$$

$$x^{(\sharp,p)} := N_X(p)U_{p^{-1}}x^\sharp = N_X(p)U_p^{-1}x^\sharp, \tag{2}$$

$$N_{X^{(p)}}(x) := N_X^{(p)}(x) = N_X(p)N_X(x) \tag{3}$$

in all scalar extensions is a cubic norm structure over k, denoted by $X^{(p)}$ and

called the p-isotope *of* X. *Moreover, the (bi-)linear trace* $T_{X^{(p)}} =: T_X^{(p)}$ *and the quadratic trace* $S_{X^{(p)}} =: S_X^{(p)}$ *of* $X^{(p)}$ *are given by*

$$T_{X^{(p)}}(y,z) = T_X^{(p)}(y,z) = T_X(U_p y, z), \tag{4}$$

$$T_{X^{(p)}}(y) = T_X^{(p)}(y) = T_X(p,y), \tag{5}$$

$$S_{X^{(p)}}(y) = S_X^{(p)}(y) = T_X(p^\sharp, y^\sharp) \tag{6}$$

for all $y, z \in X$. Indeed, dropping the subscripts for convenience, (33.10.1) combined with (33a.17) and Lemma 33.7 shows that $X^{(p)}$ is a cubic array over k whose bilinear trace by (33.2.8), (33a.7), (1) and the gradient identity (33a.4) has the form

$$\begin{aligned} T^{(p)}(y,z) &= N^{(p)}(p^{-1},y)N^{(p)}(p^{-1},z) - N^{(p)}(p^{-1},y,z) \\ &= N(p)^2 T(p^{-1\sharp},y)T(p^{-1\sharp},z) - N(p)T(p^{-1}\times y, z) \\ &= T(p,y)T(p,z) - T(p^\sharp \times y, z). \end{aligned}$$

Hence (4) holds, as do (5), (6). The defining conditions, (33a.3), (33a.4), (33a.5), of a cubic norm structure are now straightforward to check, using the relation $y \times^{(p)} z = N(p)U_p^{-1}(y \times z)$ for the bilinearization of $(\sharp, p)$. As an example, verifying the adjoint identity, we apply (33.10.1), (33a.20) and obtain

$$\begin{aligned} x^{(\sharp,p)(\sharp,p)} &= N(p)U_p^{-1}(N(p)U_{p^{-1}}x^\sharp)^\sharp = N(p)^3 U_p^{-1} U_{p^{-1\sharp}} x^{\sharp\sharp} \\ &= N(p)^3 U_p^{-1} U_{N(p)^{-1}p} x^{\sharp\sharp} = N(p)U_p^{-1}U_p x^{\sharp\sharp} \\ &= N(p)N(x)x = N^{(p)}(x)x. \end{aligned}$$

33.12 Proposition (McCrimmon [183])**.** *Let* X *be a cubic norm structure over* k.

(a) *If* $p \in X$ *is invertible in* $J(X)$, *then* $J(X^{(p)}) = J(X)^{(p)}$ *is the* p*-isotope of the Jordan algebra associated with* X.

(b) *If* $p, q \in X$ *are invertible in* $J(X)$, *then so is* $U_p q$ *and* $(X^{(p)})^{(q)} = X^{(U_p q)}$.

Proof (a) Both algebras live on the same k-module and have the same unit element, so it remains to show that they have the same U-operator as well. To do so, we write U' for the U-operator of $J(X^{(p)})$, abbreviate $T := T_X$ and obtain, combining (33a.20) with (33.11.2) and its linearization,

$$\begin{aligned} U'_x y &= T^{(p)}(x,y)x - x^{(\sharp,p)} \times^{(p)} y = T(U_p x, y)x - N(p)^2 U_p^{-1}((U_{p^{-1}}x^\sharp)\times y) \\ &= T(U_p x, y)x - U_p^{-1}((U_{p^\sharp}x^\sharp)\times y) = T(U_p x, y)x - U_p^{-1}((U_p x)^\sharp \times y) \\ &= U_p^{-1}(T(U_p x, y)U_p x - (U_p x)^\sharp \times y) \\ &= U_p^{-1} U_{U_p x} y = U_p^{-1} U_p U_x U_p y = U_x U_p y = U_x^{(p)} y, \end{aligned}$$

which is exactly what we had to prove.

(b) The first part follows from (33a.21) and Cor. 33.10, the rest from (a) and a straightforward computation. □

Exercises

33.13. *Regular pointed cubic forms* (Springer [266], McCrimmon [183]). By a *pointed cubic form* over k we mean a k-module X together with a distinguished element $1 = 1_X \in X$ (the *base point*) and a cubic form $N = N_X\colon X \to k$ (the *norm*) such that $N(1) = 1$. We then define the associated *(bilinear) trace* of X as the symmetric bilinear form $T = T_X\colon X \times X \to k$ given by

$$T(y,z) := N(1,y)N(1,z) - N(1,y,z) \qquad (y,z \in X).$$

A *homomorphism* of pointed cubic forms is a linear map preserving norms and base points. A pointed cubic form X with base point 1, norm N and trace T is said to be *regular* if X is finitely generated projective as a k-module and T is regular as a symmetric bilinear form, i.e., it induces an isomorphism from X onto its dual X^* in the usual way.

Now let X be a regular pointed cubic form over k as above.

(a) Show that there is a unique map $x \mapsto x^\sharp$ from X to X satisfying the gradient identity

$$T(x^\sharp, y) = N(x,y) \qquad (x,y \in X).$$

Conclude that X together with 1, $\sharp$ and N is a cubic array satisfying the unit identity. In particular, X is a cubic norm structure if and only if the adjoint identity holds.

(b) Let $\varphi\colon X \to X'$ be a surjective homomorphism of pointed cubic forms and assume X' is finitely generated projective as a k-module. Show that X' is regular and φ is an isomorphism of cubic arrays.

33.14. Show that a cubic array X over k is a cubic norm structure if and only if the identities

$$1 \times x = T(x)1 - x, \tag{1}$$
$$N(x,y) = T(x^\sharp, y), \tag{2}$$
$$x^{\sharp\sharp} = N(x)x, \tag{3}$$
$$x^\sharp \times y^\sharp + (x \times y)^\sharp = T(x^\sharp, y)y + T(x, y^\sharp)x, \tag{4}$$
$$x^\sharp \times (x \times y) = T(x^\sharp, y)x + N(x)y. \tag{5}$$

hold for all $x, y, z \in X$.

33.15 (Brühne [41])**.** Let X be a cubic norm structure over k. Show that the cubic norm substructure of X generated by arbitrary elements $x, y \in X$ is spanned as a k-module by

$$1, x, x^\sharp, y, y^\sharp, x \times y, x^\sharp \times y, x \times y^\sharp, x^\sharp \times y^\sharp. \tag{1}$$

34 Basic properties of cubic Jordan algebras

In this section, cubic Jordan algebras will be defined and it will be shown that they are categorically isomorphic to cubic norm structures. We also define cubic alternative algebras and clarify their connection with cubic Jordan algebras.

34.1 The concept of a cubic Jordan algebra. In analogy to the concept of a multiplicative conic alternative algebra as in 17.4–17.7, we define a *cubic Jordan algebra* over k as a Jordan k-algebra J together with a cubic form $N_J\colon J \to k$ (the *norm*) such that the following conditions hold.

(i) $1_J \in J$ is unimodular.

(ii) The norm of J *permits Jordan composition* in the sense that the equations

$$N_J(1_J) = 1, \quad N_J(U_x y) = N_J(x)^2 N_J(y) \tag{1}$$

hold strictly in J.

(iii) For all $R \in k$-**alg** and all $x \in J_R$, the monic cubic polynomial

$$m_{J,x}(\mathbf{t}) := N_J(\mathbf{t}1_{J_R} - x) \in R[\mathbf{t}]$$

satisfies the equations

$$m_{J,x}(x) = (\mathbf{t}m_{J,x})(x) = 0.$$

As in the case of cubic arrays, the unimodularity condition (i) by Exc. 12.44 holds automatically if J is projective as a k-module. By definition, cubic Jordan algebras are invariant under base change. If J' is another cubic Jordan algebra over k, a *homomorphism* $\varphi\colon J \to J'$ *of cubic Jordan algebras* is defined as a homomorphism of Jordan algebras preserving norms in the sense that $N_{J'} \circ \varphi = N_J$ as polynomial laws over k. In this way we obtain the category of cubic Jordan algebras over k, denoted by k-**cujo**. Note that, strictly speaking, the objects of k-**cujo** are pairs (J, N) consisting of a Jordan k-algebra J and a cubic form $N\colon J \to k$ such that conditions (i)–(iii) above are fulfilled. The forgetful functor defined by $(J, N) \mapsto J$ on objects and by the identity on morphisms is a faithful embedding from k-**cujo** into k-**jord**, the category of Jordan algebras over k, but not a full one, as we shall see in 34.15 below. Compare with the analogous situation for multiplicative conic alternative algebras (17.7).

In order to make condition (iii) above more explicit, we imitate the procedure of 33.2 to define the *linear trace* of J as the linear map

$$T_J\colon J \longrightarrow k, \quad x \longmapsto T_J(x) := N_J(1_J, x), \tag{2}$$

as well as the *quadratic trace* of J as the quadratic form

$$S_J\colon J \longrightarrow k, \quad x \longmapsto S_J(x) := N_J(x, 1_J). \tag{3}$$

Then condition (iii) above is equivalent to the strict validity of the equations

$$x^3 - T_J(x)x^2 + S_J(x)x - N_J(x)1_J = 0, \tag{4}$$
$$x^4 - T_J(x)x^3 + S_J(x)x^2 - N_J(x)x = 0 \tag{5}$$

in J. Note that (4) implies (5) if $2 \in k^\times$ since J is then a linear Jordan algebra. Furthermore, (2), (3) combined with Euler's differential equation imply

$$T_J(1_J) = S_J(1_J) = 3. \tag{6}$$

Inspired by (33a.22), we define the *adjoint* of J as the quadratic map $\sharp = \sharp_J\colon J \to J$, $x \mapsto x^\sharp$ from J to J given by

$$x^\sharp := x^2 - T_J(x)x + S_J(x)1_J, \tag{7}$$

dependence on J being understood. The adjoint linearizes to

$$x \times y := (x + y)^\sharp - x^\sharp - y^\sharp = x \circ y - T_J(x)y - T_J(y)x + S_J(x, y)1_J. \tag{8}$$

Combining (7) with (6), we conclude $1_J^\sharp = 1_J$, so the k-module J together with the base point 1_J, the adjoint $\sharp$ and the norm N_J is a cubic array over k, denoted by $X(J)$. In particular, we have the bilinear trace of $X(J)$, which we call the *bilinear trace* of J, denoted by $T_J\colon J \times J \to k$. Summing up, we conclude that not only the norm and adjoint but also the (bi-)linear and quadratic trace of J and $X(J)$ are the same.

Clearly, every homomorphism of cubic Jordan algebras preserves not only norms but also (bi-)linear and quadratic traces. If there is no danger of confusion, we will always extend the notational conventions spelled out for cubic arrays in 33.1 to cubic Jordan algebras by writing their identity elements as 1, their norms as N, and their (bi-)linear and quadratic traces as T, S, respectively.

Before we can proceed, we need a lemma.

34.2 Lemma. *Let X be a cubic array over k such that the unit identity and the adjoint identity hold strictly in X:*

$$1_X \times x = T_X(x)1_X - x, \quad x^{\sharp\sharp} = N_X(x)x. \tag{1}$$

Then

$$S_X(x) = T_X(x^\sharp) \tag{2}$$

for all $x \in X$.

Proof Applying the second order chain and product rules to the second equation of (1), we obtain

$$x^\sharp \times y^\sharp + (x \times y)^\sharp = N_X(x,y)y + N_X(y,x)x.$$

Putting $y = 1_X$ and combining with the first equation of (1), we obtain

$$\begin{aligned} S_X(x)1_X + T_X(x)x &= T_X(x^\sharp)1_X - x^\sharp + (T_X(x)1_X - x)^\sharp \\ &= T_X(x^\sharp)1_X - x^\sharp + T_X(x)^2 1_X - T_X(x)(T_X(x)1_X - x) + x^\sharp \\ &= T_X(x^\sharp)1_X + T_X(x)x, \end{aligned}$$

and since 1_X is unimodular, the assertion follows. □

34.3 Theorem. *Let J be a cubic Jordan algebra over k.*

(a) The cubic array $X := X(J)$ of 34.1 is a cubic norm structure over k such that $J = J(X)$.

(b) An element x of a cubic Jordan k-algebra J is invertible in J if and only if $N_J(x)$ is invertible in k. In this case, $x^{-1} = N_J(x)^{-1}x^\sharp$ and x is unimodular.

Proof We always drop the subscript "X" for convenience and then proceed in several steps, where we try to read some of the preceding arguments backwards.

1°. *An element $x \in J$ is invertible in J if and only if $N(x)$ is invertible in k. In this case, $x^{-1} = N(x)^{-1}x^\sharp$ and $N(x^{-1}) = N(x)^{-1}$.* Indeed, assume first $x \in J^\times$. Since N permits Jordan composition, we obtain $1 = N(1) = N(U_x x^{-2}) = N(x)^2 N(x^{-2})$, hence $N(x) \in k^\times$, and $N(x) = N(U_x x^{-1}) = N(x)^2 N(x^{-1})$ implies $N(x^{-1}) = N(x)^{-1}$. Before proving the converse of our assertion, assume for the time being that x is arbitrary. Combining (34.1.5) with (34.1.7) we obtain

$$U_x x^\sharp = N(x)x, \tag{1}$$

while Thm. 30.1 and (34.1.4) yield $U_x U_{x^\sharp} = N(x)^2 \mathbf{1}_J$, hence

$$U_x x^{\sharp 2} = N(x)^2 1. \tag{2}$$

Now suppose $N(x) \in k^\times$. Then (1) and (2) show that $y := N(x)^{-1}x^\sharp$ satisfies $U_x y = x$, $U_x y^2 = 1$, hence $x \in J^\times$ and $y = x^{-1}$. In particular, we have thus proved part (b) of the theorem.

2°. *The following identities hold strictly in J.*

$$1 \times x = T(x)1 - x, \tag{3}$$
$$x^{\sharp\sharp} = N(x)x, \tag{4}$$
$$N(x^\sharp) = N(x)^2, \tag{5}$$
$$S(x) = T(x^\sharp), \tag{6}$$
$$\{xx^\sharp y\} = 2N(x)y = \{x^\sharp xy\}, \tag{7}$$
$$U_x(x \times y) = N(x,y)x - N(x)y, \tag{8}$$
$$(U_x y)^\sharp = U_{x^\sharp} y^\sharp, \tag{9}$$
$$N(U_x y, U_x z) = N(x)^2 N(y,z), \tag{10}$$
$$N(x)U_x y = N(x^\sharp, y)x - N(x)x^\sharp \times y. \tag{11}$$

We put $y = 1$ in (34.1.8) and obtain $1 \times x = 2x - T(x)1 - 3x + S(x,1)1$, which implies (3) since $S(x,1) = T(x)T(1) - T(x,1) = 2T(x)$ by (33.2.10) (34.1.6). Turning to (4), (5), Prop. 12.24 and 1° allow us to assume that x is invertible. Then 1° implies $x^{\sharp\sharp} = (N(x)x^{-1})^\sharp = N(x)^2(x^{-1})^\sharp = N(x)^2 N(x^{-1})(x^{-1})^{-1} = N(x)x$, hence (4). But then (1) implies $N(x)^4 = N(N(x)x) = N(U_x x^\sharp) = N(x)^2 N(x^\sharp)$, and (5) drops out as well. Identity (6) follows from (3), (4) and Lemma 34.2. For the first part of (7) we combine (34.1.7) with (30.4.4) and (34.1.4) and obtain

$$\begin{aligned}\{xx^\sharp y\} &= V_{x,x^\sharp} y = (V_{x,x^2} - T(x)V_{x,x} + S(x)V_x)y \\ &= (V_{x^3} - T(x)V_{x^2} + S(x)V_x)y = (x^3 - T(x)x^2 + S(x)x) \circ y \\ &= N(x)1 \circ y = 2N(x)y,\end{aligned}$$

as desired. The second equation follows analogously. In order to derive (8), we differentiate (1) in the direction y, which yields $N(x,y)x + N(x)y = U_{x,y}x^\sharp + U_x(x \times y) = \{xx^\sharp y\} + U_x(x \times y)$, and (8) follows from (7). In (9), we apply Prop. 12.24 to the polynomial law $g\colon J \times J \to \mathrm{End}_k(J)$ given by $g(x,y) := U_x y$. Hence we may assume that x and y are both invertible. Then so is $U_x y$ by Prop. 31.3, and 1° combined with (31.3.2) implies

$$(U_x y)^\sharp = N(U_x y)(U_x y)^{-1} = N(x)^2 N(y) U_{x^{-1}} y^{-1} = U_{N(x)x^{-1}} N(y) y^{-1} = U_{x^\sharp} y^\sharp.$$

Equation (10) follows by fixing x and differentiating (34.1.1) at y in the direction z. Finally, in order to derive (11), we replace x by $x^\sharp$ in (1) and obtain $N(x)U_{x^\sharp}x = N(x)^2 x^\sharp$, hence $U_{x^\sharp}x = N(x)x^\sharp$ first for x invertible and then in full generality. Differentiating in the direction y, we conclude $N(x,y)x^\sharp + N(x)x \times y = U_{x^\sharp, x\times y}x + U_{x^\sharp}y = \{x^\sharp x(x \times y)\} + U_{x^\sharp}y = 2N(x)x \times y + U_{x^\sharp}y$ by (7). Thus

$$U_{x^\sharp}y = N(x,y)x^\sharp - N(x)x \times y.$$

Here we replace x by $x^\sharp$ to deduce $N(x)^2 U_x y = N(x)N(x^\sharp, y)x - N(x)^2 x^\sharp \times y$, which yields (11) first for $x \in J^\times$ and then in full generality.

3°. *For $p \in J^\times$, the k-module J together with the base point $1^{(p)} := p^{-1}$, the adjoint $x \mapsto x^{(\sharp,p)} := N(p)U_{p^{-1}}x^\sharp$ and the norm $N^{(p)} := N(p)N\colon J \to k$ is a cubic array $X^{(p)}$ whose linear and quadratic traces are given by*

$$T^{(p)}(x) = N(p)N(p^{-1}, x), \quad S^{(p)}(x) = N(x, p^\sharp). \tag{12}$$

Moreover, $X^{(p)}$ strictly satisfies the unit and adjoint identities:

$$1^{(p)} \times^{(p)} x = T^{(p)}(x)1^{(p)} - x, \quad x^{(\sharp,p)(\sharp,p)} = N^{(p)}(x)x, \tag{13}$$

where $\times^{(p)}$ stands for the bilinearized adjoint of $X^{(p)}$. The straightforward verification that $X^{(p)}$ is a cubic array satisfying (12) is left to the reader. It therefore remains to check (13). First of all, 1° and (8), (12) imply

$$\begin{aligned} 1^{(p)} \times^{(p)} x &= N(p)U_{p^{-1}}(p^{-1} \times x) = N(p)N(p^{-1}, x)p^{-1} - N(p)N(p^{-1})x \\ &= T^{(p)}(x)1^{(p)} - x, \end{aligned}$$

while 1°, (9), (4), (34.1.1) yield

$$\begin{aligned} x^{(\sharp,p)(\sharp,p)} &= (N(p)U_{p^{-1}}x^\sharp)^{(\sharp,p)} = N(p)U_{p^{-1}}\Big((N(p)U_{p^{-1}}x^\sharp)^\sharp\Big) \\ &= N(p)U_{p^{-1}}\Big((N(p)^{-1}U_{p^\sharp}x^\sharp)^\sharp\Big) = N(p)^{-1}U_{p^{-1}}((U_p x)^{\sharp\sharp}) \\ &= N(p)^{-1}U_p^{-1}(N(U_p x)U_p x) = N(p)N(x)x = N^{(p)}(x)x, \end{aligned}$$

as claimed.

4°. We can now show that X is a cubic norm structure. In view of (3), (4), we only have to verify the gradient identity. To this end, let $p \in J^\times$. Then 3° and (34.2.2) imply $S^{(p)}(x) = T^{(p)}(x^{(\sharp,p)})$. But $S^{(p)}(x) = N(x, p^\sharp)$ by (12), while (12) and (10) imply

$$T^{(p)}(x^{(\sharp,p)}) = N(p)N(p^{-1}, N(p)U_{p^{-1}}x^\sharp)) = N(p)^2 N(U_{p^{-1}}p, U_{p^{-1}}x^\sharp) = N(p, x^\sharp).$$

Thus $N(x, p^\sharp) = N(p, x^\sharp)$, and in view of Prop. 12.24, we have shown that the identity

$$N(x, y^\sharp) = N(y, x^\sharp)$$

holds strictly in J. Differentiating in the direction y, we conclude

$$N(x, y \times z) = N(y, z, x^\sharp).$$

Putting $z = 1$ and applying (34.1.3), (3), (33.1.10), (6), we therefore obtain

$$\begin{aligned} T(y)S(x) - N(x,y) &= T(y)N(x,1) - N(x,y) = N(x, T(y)1 - y) = N(x, y \times 1) \\ &= N(y, 1, x^\sharp) = N(x^\sharp, y, 1) = S(x^\sharp, y) = T(x^\sharp)T(y) - T(x^\sharp, y) \\ &= S(x)T(y) - T(x^\sharp, y), \end{aligned}$$

and the gradient identity is proved. It remains to show that $J = J(X)$ is the Jordan algebra associated with X. In (11), the gradient identity implies $N(x^\sharp, y) = T(x^{\sharp\sharp}, y) = N(x)T(x, y)$, and the formula $U_x y = T(x, y)x - x^\sharp \times y$ drops out for x invertible, hence in full generality. But this means $J = J(X)$.

The second part of (b) now follows from Lemma 33.7 and (33a.17). □

34.4 Remark. In case J is finitely generated projective as a k-module, part (b) of Thm. 34.3 may also be derived as follows: $N_J(x)$ is invertible in k, hence unimodular, which implies that so is x, by Exc. 12.37.

34.5 Towards an isomorphism of categories. Let J be a cubic Jordan algebra over k. Then Thm. 34.3 (a) shows $J = J(X(J))$. Conversely, let X be a cubic norm structure over k. By Thm. 33.9 combined with (33a.21), $J(X)$, always considered together with the norm of X: $N_{J(X)} = N_X$, is a cubic Jordan algebra, and (33a.22) implies $X = X(J(X))$. Now let $\varphi\colon X \to X'$ be a homomorphism of cubic norm structures. Since φ preserves not only base points, adjoints and norms but also linear and quadratic traces, it is a homomorphism $\varphi\colon J(X) \to J(X')$ of cubic Jordan algebras. Conversely let $\varphi\colon J \to J'$ be a homomorphism of cubic Jordan algebras. Since φ preserves units, norms, linear and quadratic traces, it follows from (34.1.7) that it preserves adjoints as well. Thus $\varphi\colon X(J) \to X(J')$ is a homomorphism of cubic norm structures. Summing up, we have shown the following result.

34.6 Corollary. *The formalism set up in 34.5 yields an isomorphism of categories between cubic norm structures and cubic Jordan algebras over k.* □

34.7 Convention. Cor. 34.6 may be used to identify cubic norm structures and cubic Jordan algebras over k canonically. Thus the two terms will sometimes be employed interchangeably.

34.8 Example. *Isotopes of cubic Jordan algebras are cubic Jordan algebras.* More precisely, let J be a cubic Jordan k-algebra with norm N_J and suppose J' is an isotope of J, so $J' = J^{(p)}$ for some invertible element $p \in J$. Then $J = J(X)$ for $X = X(J)$ (Thm. 34.3 (a)), and we conclude $N_J(p) \in k^\times$ from Thm. 34.3 (b). Now Prop. 33.12 (a) implies that $J' = J(X^{(p)})$ is a cubic Jordan algebra with norm $N_{J'} = N_J(p)N_J$.

34.9 Examples (Inner ideals)**.** Let J be a cubic Jordan algebra over a ring k.

(a) *If I is a k-submodule of J such that $x^\sharp = 0$ for every $x \in I$, then I is an inner ideal.* Indeed, the hypothesis on x implies that $U_x y = T(x,y)x \in kx \subseteq I$ for all $y \in J$.

(b) *If $x \in J$ satisfies $x^\sharp = 0$, then $(x \times J)^\sharp$ is an inner ideal contained in kx.* Indeed, for $y \in J$, we have

$$(x \times y)^\sharp = T(x, y^\sharp)x \tag{1}$$

by (33a.10), verifying the second claim. The first claim follows immediately from the formula (33.9.1).

(c) Consider the special case $J = \mathrm{Mat}_3(F)^{(+)}$ for a field F. An element $x \in J$ has $x^\sharp = 0$ if and only if it has rank ≤ 1 as a matrix, therefore a nonzero element $x \in J$ has $x^\sharp = 0$ if and only if x has rank 1 as a matrix. See Exc. 40.15 and 41.28 below for generalizations.

34.10 Semi-linear homomorphisms of cubic gadgets. Just as semi-linear homomorphisms play a useful role in, e.g., associative algebras, they are also relevant in the context of cubic Jordan algebras. Although they will be used only in a few exercises below or much later in the main text of the book, we find it convenient to present the relevant definitions already at this stage. Let $\sigma\colon K \to K'$ be a morphism in k-**alg**.

(a) If X (resp. X') are cubic arrays over K (resp. K'), a map $\varphi\colon X \to X'$ is said to be a *semi-linear homomorphism* of cubic arrays if the following conditions are fulfilled.

(i) φ is σ-semi-linear.

(ii) $\varphi(1_X) = 1_{X'}$.

(iii) The σ-semi-linear polynomial squares

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ {\scriptstyle \sharp_X}\downarrow & & \downarrow{\scriptstyle \sharp_{X'}} \\ X & \xrightarrow[\varphi]{} & X' \end{array} \tag{1}$$

and

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ {\scriptstyle N_X}\downarrow & & \downarrow{\scriptstyle N_{X'}} \\ K & \xrightarrow[\sigma]{} & K' \end{array} \tag{2}$$

commute in the sense of 12.28.

Note that this definition in particular applies to cubic norm structures.

(b) If J (resp. J') are cubic Jordan algebras over K (resp. K'), a map $\varphi\colon J \to J'$ is a *σ-semi-linear homomorphism* of cubic Jordan algebras if the following conditions are fulfilled.

(i) φ is σ-semi-linear.

(ii) $\varphi\colon J \to J'$ is a homomorphism of Jordan algebras over k.

(iii) The σ-semi-linear polynomial square

$$\begin{array}{ccc} J & \xrightarrow[\varphi]{} & J' \\ {\scriptstyle N_J}\downarrow & & \downarrow{\scriptstyle N_{J'}} \\ K & \xrightarrow[\sigma]{} & K' \end{array} \tag{3}$$

is commutative.

Note that (iii) amounts to

$$\begin{array}{ccc} {}_kJ & \xrightarrow[{}_k\varphi]{} & {}_kJ' \\ {\scriptstyle {}_k(N_J)}\downarrow & & \downarrow{\scriptstyle {}_k(N_{J'})} \\ {}_kK & \xrightarrow[{}_k\sigma]{} & {}_kK' \end{array} \tag{4}$$

being a commutative diagram of polynomial laws over k. Combining (4) with the differential calculus 12.17, Exc. 12.46, (33.2.6), (33.2.7) and (33.2.10), we conclude

$$\begin{aligned} N_{J'}(\varphi(x),\varphi(y)) &= \sigma(N_J(x,y)), \quad T_{J'}(\varphi(x)) = \sigma(T_J(x)), \\ S_{J'}(\varphi(x)) &= \sigma(S_J(x)), \quad T_{J'}(\varphi(x),\varphi(y) = \sigma(T_J(x,y)) \end{aligned} \tag{5}$$

for all $x, y \in J$, while (34.1.7) and (5) imply

$$\varphi(x^{\sharp_J}) = \varphi(x)^{\sharp_{J'}} \tag{6}$$

for all $x \in J$.

(c) Let X (resp. X') be a cubic norm structure over K (resp. K'). By (5), (6), a map $\varphi\colon X \to X'$ is a σ-semi-linear homomorphism of cubic norm structures if and only if $\varphi\colon J(X) \to J(X')$ is a σ-semi-linear homomorphism of cubic Jordan algebras.

(d) Let X be a cubic array over k and $\sigma\colon k \to K$ the unit morphism of $K \in k$-**alg**. Then the σ-semi-linear map $\mathrm{can}_{X,K}\colon X \to X_K$ is, in fact, a σ-semi-linear homomorphism of cubic arrays since (1), (2) follow immediately from (12.29.2) for $M := X$.

34.11 Cubic alternative algebras. By a *cubic alternative algebra* over k we mean a unital alternative algebra A over k together with a cubic form $N_A\colon A \to k$ (the *norm*) such that the following conditions are fulfilled.

(i) $1_A \in A$ is unimodular.

(ii) The norm of A *permits composition*: the equations

$$N_A(1_A) = 1, \quad N_A(xy) = N_A(x)N_A(y) \tag{1}$$

hold strictly in A.

(iii) For all $R \in k$-**alg** and all $x \in A_R$, the monic polynomial

$$m_{A,x}(\mathbf{t}) = N_A(\mathbf{t}1_{A_R} - x) \in R[\mathbf{t}]$$

annihilates x:

$$m_{A,x}(x) = 0.$$

As in the case of cubic Jordan algebras, we then define the *linear* and the *quadratic trace* of A by

$$T_A\colon A \longrightarrow k, \quad x \longmapsto T_A(x) := N_A(1_A, x), \tag{2}$$

$$S_A\colon A \longrightarrow k, \quad x \longmapsto S_A(x) := N_A(x, 1_A), \tag{3}$$

respectively. Condition (iii) may then be rephrased by saying that the equation

$$x^3 - T_A(x)x^2 + S_A(x)x - N_A(x)1_A = 0 \tag{4}$$

holds strictly in A. If A' is another cubic alternative k-algebra, a *homomorphism* $\varphi\colon A \to A'$ of cubic alternative k-algebras is defined as a homomorphism of unital k-algebras that preserves norms: $N_{A'} \circ \varphi = N_A$ as polynomial laws over k. In this way we obtain the category of cubic alternative algebras over k, denoted by k-**cual**. Strictly speaking, the objects of k-**cual** are pairs (A, N) consisting of a unital alternative k-algebra A and a cubic form $N\colon A \to k$ (the norm) such that the conditions (i)–(iii) above are fulfilled. Ignoring the norm, i.e., passing from (A, N) to A and acting as the identity on morphisms, we obtain the forgetful functor from k-**cual** to k-$\mathbf{alt}_1$, which is obviously faithful but, as will be seen in 34.15 below, is not full.

If A in the preceding discussion is associative, then we speak of a *cubic associative algebra* over k. Cubic associative k-algebras may and always will be viewed canonically as a full subcategory, denoted by k-**cuas**, of cubic alternative k-algebras. Similar conventions apply to commutative associative algebras.

By definition cubic alternative algebras are stable under base change. Moreover, combining Exc. 17.8 with Exc. 34.24 below, it follows that condition (ii) above does not follow from (i) and (iii); also, the norm of a cubic alternative

algebra need not be uniquely determined by the algebra structure alone. For examples of cubic alternative algebras that are not associative, see Exc. 34.24 (b).

34.12 Proposition. *Let A be a cubic alternative algebra over k. Then $A^{(+)}$ together with the norm $N_{A^{(+)}} := N_A$ is a cubic Jordan algebra over k whose linear and quadratic traces agree with those of A: $T_{A^{(+)}} = T_A$, $S_{A^{(+)}} = S_A$. Moreover, the bilinear trace of $A^{(+)}$ is given by $T_{A^{(+)}}(x,y) = T_A(xy)$ for all $x, y \in A$.*

Proof Equation (34.1.4) agrees with (34.11.4), while (34.1.5) follows after multiplying (34.11.4) by x in A. Moreover, from (34.11.1) we deduce that $N := N_A = N_{A^{(+)}}$ permits Jordan composition: $N(U_x y) = N(xyx) = N(x)^2 N(y)$ holds strictly in $J := A^{(+)}$. Thus J together with N is a cubic Jordan algebra whose linear and quadratic traces by definition are the same as those of A. With $T := T_A$ (the linear trace of A, hence of J) and $T' := T_J$ (the bilinear trace of J), it remains to show $T'(x,y) = T(xy)$ for all $x, y \in A$. By Prop. 12.24, we may assume $p := y \in A^\times$. From (33.11.5) combined with Prop. 33.12 and Thm. 34.3 (a) we therefore conclude that $J^{(p)}$ is a cubic Jordan algebra with linear trace $T^{(p)}$ given by $T^{(p)}(x) = T'(x,p)$ for all $x \in A$. On the other hand, since N_A permits composition, $R_p \colon J^{(p)} \to J$ by 31.13 is an isomorphism of cubic Jordan algebras. As such it preserves linear traces, which implies $T(xp) = T^{(p)}(x) = T'(x,p)$, as claimed. □

34.13 The bilinear trace revisited. Let A be a cubic alternative algebra over k. Inspired by the preceding proposition, we define the *bilinear trace* of A, under the same notation as the linear one, as the bilinear form

$$T_A \colon A \times A \longrightarrow k, \quad (x,y) \longmapsto T_A(x,y) := T_A(xy).$$

It is the same as the bilinear trace of the cubic Jordan algebra $A^{(+)}$ and, in particular, a symmetric bilinear form.

34.14 Example. The base ring carries the structure of a cubic commutative associative k-algebra through the cubic form $N_k \colon k \to k$ given by

$$N_k(r) := r^3 \qquad (r \in R,\ R \in k\text{-}\mathbf{alg}). \tag{1}$$

The linear and quadratic traces of k as well as its adjoint have the form

$$T_k(\alpha) = 3\alpha, \quad S_k(\alpha) = 3\alpha^2, \quad \alpha^\sharp = \alpha^2 \qquad (\alpha \in k). \tag{2}$$

In view of all this, we can now speak of $k^{(+)}$ as a cubic Jordan algebra over k. In fact, since the norm of a cubic Jordan algebra J sends 1_J to $1 \in k$, by (34.1.1), $N_{k^{(+)}} := N_k$ as defined in (1) is the *unique* cubic form making $k^{(+)}$ a cubic

Jordan algebra. It follows that $k^{(+)}$ *is the initial object in the category* k-**cujo**, so every cubic Jordan k-algebra J allows a unique homomorphism $k^{(+)} \to J$ of cubic Jordan algebras, namely the map $\alpha \mapsto \alpha 1_J$.

We remark that $k^{(+)}$ is regular (as a cubic Jordan algebra) if and only if 3 is invertible in k.

34.15 Cubic structures on the split quadratic étale algebra. Let $C := k \times k$ be the split quadratic étale k-algebra as in 21.19. Define a cubic form $N\colon C \to k$ by

$$N((r_1, r_2)) := r_1 r_2^2 \tag{1}$$

for $R \in k$-**alg** and $r_1, r_2 \in R$. If also $s_1, s_2 \in R$, then

$$N((r_1, r_2), (s_1, s_2)) = s_1 r_2^2 + 2 r_1 r_2 s_2,$$

hence

$$T((r_1, r_2)) = r_1 + 2r_2, \quad S((r_1, r_2)) = 2r_1 r_2 + r_2^2. \tag{2}$$

It follows immediately from (1) that N permits composition. Also, a straightforward verification shows

$$x^3 - T(x)x^2 + S(x)x - N(x)1_C = 0$$

for $x = (r_1, r_2) \in C_R = R \times R$. Thus C together with the norm N is a cubic commutative associative algebra over k, which we denote by

$$(k \times k)_{\mathrm{cub}}.$$

Note that

$$x^\sharp = (r_2^2, r_1 r_2) \tag{3}$$

for $x = (r_1, r_2) \in C_R = R \times R$, which follows immediately from (2) and (33a.22), applied to the cubic Jordan algebra $C^{(+)}$.

On the other hand, we may define a cubic form $N'\colon C \to k$ by

$$N'((r_1, r_2)) := r_1^2 r_2$$

for $R \in k$-**alg** and $r_1, r_2 \in R$. Arguing as before, it follows that C together with the norm N' is a cubic commutative associative algebra over k as well, which we denote by

$$(k \times k)^{\mathrm{op}}_{\mathrm{cub}}.$$

Thus the algebra structure alone of a cubic alternative algebra will in general *not* determine its norm uniquely, even if the underlying module is free of finite

rank. Returning to our example, the conjugation of C is an automorphism of C *but is not an automorphism of* $(k \times k)_{\mathrm{cub}}$ *nor one of* $(k \times k)^{\mathrm{op}}_{\mathrm{cub}}$; in fact, it is an isomorphism from the former to the latter:

$$\iota_{k\times k} \colon (k \times k)_{\mathrm{cub}} \xrightarrow{\sim} (k \times k)^{\mathrm{op}}_{\mathrm{cub}}.$$

In particular, the forgetful functor k-**cual** $\to$ k-**alt**$_1$ is not a full embedding, and neither is the forgetful functor k-**cujo** $\to$ k-**jord**, as may be seen from the present example by passing from C to $C^{(+)}$.

34.16 Example: 3-by-3 matrices. $\mathrm{Mat}_3(k)$ is a cubic associative k-algebra with norm (resp. linear trace) given by the ordinary determinant (resp. trace) of matrices since $\det(\mathbf{1}_3, x) = \mathrm{tr}(x)$ for all $x \in \mathrm{Mat}_3(k)$. On the other hand, the bilinear trace of $\mathrm{Mat}_3(k)^{(+)}$, viewed as a cubic Jordan algebra, may be read off from Prop. 34.12: $T(x, y) = \mathrm{tr}(xy)$. In particular, the cubic Jordan matrix algebra $\mathrm{Mat}_3(k)^{(+)}$ is regular. The adjoint of $\mathrm{Mat}_3(k)^{(+)}$ is the usual adjoint of matrices, by its definition (34.1.7).

34.17 Examples: cubic étale algebras. Let E be a unital commutative associative k-algebra that is finitely generated projective of rank 3 as a k-module and finite étale (in the sense of 19.19) as an algebra over k. Then $N(x) := \det(L_x)$ for x in any scalar extension of E, where L stands for the left multiplication of E, defines a cubic form $N = N_E \colon E \to k$ which converts E into a cubic commutative associative k-algebra; we speak of a *cubic étale algebra* in this context. The linear trace of E is then given by $T(x) = \mathrm{tr}(L_x)$, while the bilinear one by Prop. 34.12 has the form $T(x, y) = \mathrm{tr}(L_{xy})$. It follows from 19.19, therefore, that $E^{(+)}$, viewed as a cubic Jordan algebra over k, is regular. By abuse of language, we often say a Jordan algebra is *cubic étale* if it is cubic and, as such, isomorphic to $E^{(+)}$, for some cubic étale algebra E.

A particularly simple case is that of the *split cubic étale k-algebra* defined by $E = k\times k\times k$ as a direct product of ideals, with identity element $1_E = (1, 1, 1)$ and norm $N = N_E \colon E \to k$ given by

$$N(x) = \xi_1\xi_2\xi_3 \tag{1}$$

for $x = (\xi_1, \xi_2, \xi_3) \in E_R$, $R \in k$-**alg**. The linear and quadratic traces of E have the form

$$T(x) = \xi_1 + \xi_2 + \xi_3, \tag{2}$$

$$S(x) = \xi_2\xi_3 + \xi_3\xi_1 + \xi_1\xi_2, \tag{3}$$

while the adjoint and the bilinear trace of $E^{(+)}$ are given by

$$x^\sharp = (\xi_2\xi_3, \xi_3\xi_1, \xi_1\xi_2), \tag{4}$$

$$T(x, y) = \xi_1\eta_1 + \xi_2\eta_2 + \xi_3\eta_3 \tag{5}$$

for $y = (\eta_1, \eta_2, \eta_3) \in E_R$. It is sometimes convenient to identify E canonically with the algebra of 3-by-3 diagonal matrices over k:

$$E = \mathrm{Diag}_3(k) = \{\mathrm{diag}(\gamma_1, \gamma_2, \gamma_3) \mid \gamma_1, \gamma_2, \gamma_3 \in k\}, \tag{6}$$

viewed as a cubic commutative associative subalgebra of $\mathrm{Mat}_3(k)$. For

$$\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathrm{Diag}_3(k)$$

we have

$$N(\Gamma) = \det(\Gamma) = \gamma_1\gamma_2\gamma_3, \tag{7}$$

$$T(\Gamma) = \mathrm{tr}(\Gamma) = \gamma_1 + \gamma_2 + \gamma_3, \tag{8}$$

$$S(\Gamma) = \gamma_2\gamma_3 + \gamma_3\gamma_1 + \gamma_1\gamma_2, \tag{9}$$

$$\Gamma^\sharp = \mathrm{diag}(\gamma_2\gamma_3, \gamma_3\gamma_1, \gamma_1\gamma_2). \tag{10}$$

Exercises

34.18. Let $\varphi\colon J \to J'$ be a k-linear map of cubic Jordan algebras over k. Prove that φ is

(a) a homomorphism of cubic Jordan algebras if it preserves unit elements and adjoints,

(b) an isomorphism of cubic Jordan algebras if J is regular, J' is finitely generated projective as a k-module and φ is surjective preserving unit elements and norms.

34.19. *Traceless cubic Jordan algebras*. Let J be a cubic Jordan algebra over k which is *traceless* in the sense that its linear trace vanishes identically. Show $3 = 0$ in k and that J, viewed as a linear Jordan algebra, is a cubic commutative alternative k-algebra.

34.20. *Rational cubic norm structures* (Tits-Weiss [283], Mühlherr-Weiss [200]). The following exercise characterizes cubic norm structures in terms of conditions that avoid scalar extensions. By a *rational cubic norm structure* over k we mean a k-module X together with

- a distinguished element $1 \in X$ (the *base point*),
- a map $X \to X$, $x \mapsto x^\sharp$ (the *adjoint*),
- a bilinear map $X \times X \to X$, $(x, y) \mapsto x \times y$ (the *bilinearized adjoint*),
- a symmetric bilinear form $T\colon X \times X \to k$ (the *bilinear trace*),
- a map $N\colon X \to k$ (the *norm*)

such that the following conditions are fulfilled.

(i) $1 \in X$ is unimodular.

(ii) The following equations hold for all $\alpha \in k$ and all $x, y, z \in X$.

$$(\alpha x)^\sharp = \alpha^2 x^\sharp, \tag{1}$$
$$N(\alpha x) = \alpha^3 N(x), \tag{2}$$
$$(x+y)^\sharp = x^\sharp + x \times y + y^\sharp, \tag{3}$$
$$N(x+y) = N(x) + T(x^\sharp, y) + T(x, y^\sharp) + N(y), \tag{4}$$
$$T(x^\sharp, x) = 3N(x), \tag{5}$$
$$x^{\sharp\sharp} = N(x)x, \tag{6}$$
$$x^\sharp \times y^\sharp + (x \times y)^\sharp = T(x^\sharp, y)y + T(x, y^\sharp)x, \tag{7}$$
$$x^\sharp \times (x \times y) = N(x)y + T(x^\sharp, y)x, \tag{8}$$
$$1^\sharp = 1, \tag{9}$$
$$1 \times y = T(1, y)1 - y. \tag{10}$$

A *homomorphism* of rational cubic norm structures over k is defined as a linear map preserving base points, (bilinearized) adjoints, traces and norms in the obvious sense. In this way we obtain the category of rational cubic norm structures over k, denoted by k-**racuno**. Show for a rational cubic norm structure X over k, with $1, \sharp, \times, T, N$ as above, that $x \mapsto x^\sharp$ is a quadratic map and that there exists a unique cubic form $\tilde{N}\colon X \to k$ which makes the k-module X together with $1, \sharp, \tilde{N}$ a cubic norm structure over k, written as $\tilde{X}$, having bilinear trace T and satisfying $\tilde{N}_k = N$. Conclude that the assignment $X \mapsto \tilde{X}$ on objects and the identity on morphisms yields an isomorphism of categories from k-**racuno** to k-**cuno**.

Remark. What we call a rational cubic norm structure is called a cubic norm structure in [283, (15.15)] and [201, 4.1.1]. Moreover, in addition to the identities listed in the present exercise, both sources require the validity of the formula $T(x \times y, z) = T(x, y \times z)$. As our solution will show, however, this formula follows from the other identities we have displayed.

34.21. *Cubic ideals.* In this exercise, we extend the notion of a conic ideal as defined in Exc. 16.24 to the setting of cubic Jordan algebras. Let J be a cubic Jordan algebra over k. By a *cubic ideal* in J we mean a pair $(\mathfrak{a}, I)$ consisting of an ideal $\mathfrak{a} \subseteq k$ and an ideal $I \subseteq J$ such that the following conditions are fulfilled.

(i) $\mathfrak{a}J \subseteq I$.
(ii) $T_J(x, y), T_J(x^\sharp, y), N_J(x) \in \mathfrak{a}$ for all $x \in I$, $y \in J$.

A cubic ideal $(\mathfrak{a}, I)$ in J is said to be *separated* if

(iii) there exists a k-linear map $\lambda\colon J \to k/\mathfrak{a}$ satisfying

$$\lambda(1_J) = 1_{k/\mathfrak{a}}, \quad \lambda(I) = \{0\}. \tag{1}$$

(a) Let $\mathfrak{a} \subseteq k$ be an ideal and $I \subseteq J$ a k-submodule such that conditions (i), (ii) above are fulfilled. Show that $(\mathfrak{a}, I)$ is a cubic ideal in J if and only if the relation

(iv) $I^\sharp + I \times J \subseteq I$

holds.

(b) Let $\sigma\colon K \to K'$ be a morphism in k-**alg**, J_1 (resp. J_1') a cubic Jordan algebra over

K (resp. K') and $\varphi\colon J_1 \to J_1'$ a σ-semi-linear homomorphism of cubic Jordan algebras in the sense of 34.10. Prove that

$$\mathrm{Ker}(\sigma,\varphi) := (\mathrm{Ker}(\sigma), \mathrm{Ker}(\varphi))$$

is a cubic ideal in J_1, and even a separated one if σ is surjective.

(c) Conversely, let $(\mathfrak{a}, I)$ be a separated cubic ideal in J. Write $\sigma\colon k \to k_0 := k/\mathfrak{a}$ for the canonical projection and prove that the "abstract" Jordan algebra $J_0 := J/I$ over k carries a unique cubic Jordan algebra structure over k_0 such that the canonical projection $\pi\colon J \to J_0$ is a σ-semi-linear homomorphism of cubic Jordan algebras.

(d) Prove that a cubic ideal in J is separated if the linear trace of J is surjective.

(e) Show for every ideal $\mathfrak{a} \subseteq k$ that $(\mathfrak{a}, \mathfrak{a}J)$ is a separated cubic ideal in J, the corresponding cubic Jordan algebra J_0 over k_0 defined in (c) being the base change of J from k to k_0. Conversely, can every ideal of J be extended to a cubic one?

(f) Let $\mathfrak{a} \subseteq k$ (resp. $I \subseteq J$) be an ideal in k (resp. a k-submodule of J) such that conditions (i), (iii), (iv) and

(v) $N_J(x) \in \mathfrak{a}$ for all $x \in J$

are fulfilled. Show that $(\mathfrak{a}, I)$ is a separated cubic ideal in J.

34.22. Let $\sigma\colon K \to K'$ be a morphism in k-**alg** and view K' as a K-algebra by means of σ.

(a) Prove for cubic arrays X over K and X' over K' that the assignment $\varphi' \mapsto \varphi' \circ \mathrm{can}_{X,K'}$, where $\mathrm{can}_{X,K'}\colon X \to X_{K'}$ is the natural map of 9.2, defines a bijection from the set of homomorphisms $X_{K'} \to X'$ of cubic arrays over K' onto the set of σ-semi-linear homomorphisms $X \to X'$ of cubic arrays.

(b) Let X (resp. X') be a cubic norm structure over K (resp. K'). Deduce from (a) that a map $\varphi\colon X \to X'$ is a σ-semi-linear homomorphism of cubic norm structures if and only if φ is σ-semi-linear, sends 1_X to $1_{X'}$, and makes

$$\begin{array}{ccc} X & \xrightarrow[\varphi]{} & X' \\ {\scriptstyle \sharp_X}\downarrow & & \downarrow{\scriptstyle \sharp_{X'}} \\ X & \xrightarrow[\varphi]{} & X' \end{array} \tag{1}$$

a commutative diagram of set maps.

34.23 (Petersson-Racine [224], Loos [174])**.** Let J be a cubic Jordan algebra over k. Prove that an element $x \in J$ is nilpotent if and only if $T(x), S(x), N(x) \in k$ are nilpotent. Conclude that the nil radical of J (Exc. 28.20) can be described as

$$\mathrm{Nil}(J) = \{x \in J \mid \forall y \in J:\ T(x,y), T(x^\sharp, y), N(x) \in \mathrm{Nil}(k)\}, \tag{1}$$

$$\mathrm{Nil}(J) = \{x \in J \mid \forall y \in J:\ T(x,y), N(x) \in \mathrm{Nil}(k)\} \quad (\text{if } 2 \in k^\times), \tag{2}$$

$$\mathrm{Nil}(J) = \{x \in J \mid \forall y \in J:\ T(x,y), T(x^\sharp, y) \in \mathrm{Nil}(k)\} \quad (\text{if } 3 \in k^\times), \tag{3}$$

$$\mathrm{Nil}(J) = \{x \in J \mid \forall y \in J:\ T(x,y) \in \mathrm{Nil}(k)\} \quad (\text{if } 6 \in k^\times). \tag{4}$$

34.24. In this exercise, cubic Jordan (resp. alternative) algebras will be constructed out of Jordan algebras of Clifford type (resp. out of conic alternative algebras).

(a) Let (M, q, e) be a pointed quadratic module with trace t and conjugation $u \mapsto \bar{u}$ over k, and let $J := J(M, q, e)$ be the corresponding Jordan algebra of Clifford type. Show that

$$\hat{J} := k^{(+)} \times J$$

as a direct product of ideals in the category of para-quadratic k-algebras is a cubic Jordan algebra over k, with norm $N\colon \hat{J} \to k$ given by

$$N((r,u)) := rq(u) \qquad (R \in k\text{-}\mathbf{alg},\quad r \in R,\quad u \in J_R) \tag{1}$$

Show further that the (bi-)linear and quadratic traces of $\hat{J}$ as well as its adjoint have the form

$$T((\alpha,u),(\beta,v)) = \alpha\beta + q(u,\bar{v}), \tag{2}$$
$$T((\alpha,u)) = \alpha + t(u), \tag{3}$$
$$S((\alpha,u)) = \alpha t(u) + q(u), \tag{4}$$
$$(\alpha,u)^\sharp = (q(u), \alpha\bar{u}), \tag{5}$$
$$(\alpha,u) \times (\beta,v) = (q(u,v), \alpha\bar{v} + \beta\bar{u}) \tag{6}$$

for all $\alpha, \beta \in k$, $u, v \in J$.

(b) Let C be a conic alternative algebra over k. Show that

$$\mathrm{Cub}(C) := \hat{C} := k \times C$$

as a direct product of ideals is a cubic alternative k-algebra if and only if C is multiplicative. In this case, norm, trace and quadratic trace of $\hat{C}$ are given by (1), (3), (4), respectively, with q systematically replaced by n_C. Show further that $\hat{C}$ arises from C by adjoining a unit element. Finally, explain the connection of this exercise with Example 34.15.

34.25. Let F be a field of characteristic 2. Every quadratic étale F-algebra is of the form $K := F[\mathbf{t}]/(\mathbf{t}^2 + \mathbf{t} + \beta)$ for some $\beta \in F$, as recalled in 19.19(iv). Using the notation $[a,b]$ to denote the regular 2-dimensional quadratic form $(x,y) \mapsto ax^2 + xy + by^2$ on F^2, we have $n_K \cong [1,\beta]$. Prove:

(a) For $E := F \times K$ and $J := E^{(+)}$, $S_J \cong \langle 1\rangle_{\mathrm{quad}} \perp n_K$.
(b) The restriction of S_J to $\mathrm{Ker}(T_J)$ is isomorphic to $[1, \beta + 1]$.

Remark. The results of [72, p. 49] show that $S_J \cong \langle 1\rangle_{\mathrm{quad}} \perp \mathbf{h}$. In particular, the isomorphism class of the quadratic form does not depend on the choice of β (equivalently, K). On the other hand, the isomorphism class of the restriction of S_J to $\mathrm{Ker}\, T_J$ appearing in (c) does depend on the choice of β, as can be seen by computing the Arf invariant of $[1, \beta + 1]$.

34.26. Let F be a field of characteristic $\neq 2$. Every quadratic étale F-algebra is of the form $K := F[\mathbf{t}]/(\mathbf{t}^2 - \beta)$ for some $\beta \in F^\times$, as recalled in 19.19(v), and $n_K \cong \langle 1, -\beta\rangle_{\mathrm{quad}}$. Prove:

(a) For $E := F \times K$ and $J := E^{(+)}$, $S_J \cong \langle -\beta\rangle_{\mathrm{quad}} \perp \mathbf{h}$.
(b) The restriction of S_J to $\mathrm{Ker}(T_J)$ is isomorphic to $\langle -3, -\beta\rangle_{\mathrm{quad}}$.

(c) If K is the split algebra $F \times F$, then $S_J^0 \cong \langle -1 \rangle \otimes [1,1]$.

Remark. Note in (c) that when $\mathrm{char}(F) = 2$, then $\beta = 0$ in the notation of Exc. 34.25, so part (b) of that exercise says $S_J^0 \cong [1,1]$. That is, the expression for S_J^0 provided in (c) of this exercise is valid regardless of $\mathrm{char}(F)$.

Remark. The preceding two exercises are closely related to the results of [228, §3].

34.27. *Cubic norm structures supported by pointed quadratic modules.* Let (M,q,e) be a pointed quadratic module over k with trace t and conjugation $x \mapsto \bar{x}$. Assume the k-module M is projective and show that the following conditions are equivalent.

(i) There exists a cubic norm structure X over k such that $J(X) = J(M,q,e)$ as abstract Jordan algebras.

(ii) There exists a linear form $\lambda\colon M \to k$ such that $\lambda(e) = 1$ and

$$q(x) = \lambda(x)\lambda(\bar{x}) \tag{1}$$

for all $x \in M$.

If in this case $X = (M, e, \sharp, N)$ satisfies (i), then λ as in (ii) may be so chosen that, writing T (resp. S) for the (bi-)linear (resp. quadratic) trace of X, the following identities hold strictly.

$$t(x) = \lambda(x) + \lambda(\bar{x}), \tag{2}$$

$$x^\sharp = \lambda(x)\bar{x}, \tag{3}$$

$$N(x) = \lambda(x)^2\lambda(\bar{x}), \tag{4}$$

$$T(x) = 2\lambda(x) + \lambda(\bar{x}), \tag{5}$$

$$S(x) = \lambda(x)^2 + 2\lambda(x)\lambda(\bar{x}), \tag{6}$$

$$T(x,y) = 2\lambda(x)\lambda(y) + \lambda(\bar{x})\lambda(\bar{y}). \tag{7}$$

Moreover, the nil radical of J can be described as

$$\mathrm{Nil}(J) = \{x \in J \mid x \text{ is nilpotent}\} = \{x \in J \mid \lambda(x), \lambda(\bar{x}) \in k \text{ are nilpotent}\}. \tag{8}$$

Finally, if (M,q,e) is a pointed quadratic space of rank $r > 1$ over k, then (i), (ii) are also equivalent to

(iii) $J(M,q,e) \cong (k \times k)^{(+)}_{\mathrm{cub}}$ as abstract Jordan algebras.

In particular, for a quadratic étale k-algebra R to admit a cubic norm structure X over k having $J(X) = R^{(+)}$ as abstract Jordan algebras it is necessary and sufficient that R be split.

34.28. *Cubic norm pseudo-structures* (Petersson-Racine [224]). In this exercise, we consider a family of objects somewhat more general than cubic norm structures. By a *cubic norm pseudo-structure* over k we mean a k-module X together with an element $1 \in X$, a quadratic map $x \mapsto x^\sharp$ from X to X and a cubic form $N\colon X \to k$ such that all conditions of 33.1 and 33.4 hold, with the possible exception of the base point 1 being unimodular. As in 33.2, we can then speak of the (bi-)linear and the quadratic trace of X. Similarly, by a *rational cubic norm pseudo-structure* over k, we mean a k-module X together with data $1, \sharp, \times, T, N$ as in Exc. 34.20 such that equations (1)–(10) of that exercise hold for all $\alpha \in k$, $x, y, z \in X$ but the base point $1 \in X$ may fail to be unimodular.

(a) Show for a rational cubic norm pseudo-structure X over k that there exists a unique cubic form $\tilde{N}\colon X \to k$ making X together with base point and adjoint a cubic norm pseudo-structure.

(b) Let V, W be vector spaces over a field F and suppose V is finite-dimensional, with basis $(e_1, \dots, e_n)$. Given a quadratic map $v \mapsto v^\sharp$ from V to V, with bilinearization $(v, v') \mapsto v \times v'$, a symmetric bilinear map $\sigma\colon V \times V \to W$ and arbitrary elements $w_1, \dots, w_n \in W$, show that the following conditions are equivalent.

  (i) There exists a homogeneous polynomial law $\mu\colon V \to W$ of degree 3 such that $\mu(e_i) = w_i$ for $1 \le i \le n$ and $\mu(v, v') = \sigma(v^\sharp, v')$ holds strictly in V.

  (ii) $\sigma(e_i^\sharp, e_i) = 3w_i$ for $1 \le i \le n$ and the trilinear map

$$V \times V \times V \longrightarrow (v_1, v_2, v_3) \longmapsto \sigma(v_1 \times v_2, v_3),$$

  is totally symmetric.

  In this case, μ is unique.

(c) Use (a), (b) to give an example of a cubic norm pseudo-structure X such that the relation $N(x^\sharp) = N(x)^2$ does not always hold and the bilinear trace of X is different from zero. (*Hint*: The proof of [224, Thm. 2.10] contains a gap that should be filled by means of (a).)

35 Building up cubic norm structures

In this rather technical section, we develop some basic tools for constructing a cubic norm structure out of a cubic norm substructure that will be used especially in 37.13, 38.7, and many places in Chapter VII. At that extremely coarse level of detail, this section might be viewed as an analog for cubic Jordan algebras of the construction of composition algebras from ternary hermitian spaces in section 21. The construction here is connected with Springer's approach to twisted compositions as in Springer [267, p. 95], Springer-Veldkamp [270, 6.5], Knus-Merkurjev-Rost-Tignol [160, §38A, p. 527]) (where k is a field of characteristic not 2) or Petersson-Racine [225, (3.1)] (with a sign change and X_0 coming from a cubic étale k-algebra).

Throughout this section, we fix an arbitrary commutative ring k and a cubic norm structure X over k, with base point $1 = 1_X$, adjoint $x \mapsto x^\sharp$, bilinearized adjoint $(x, y) \mapsto x \times y$, norm $N = N_X$, (bi-)linear trace $T = T_X$ and quadratic trace $S = S_X$. Generally speaking, we will be concerned with the question of which additional ingredients are needed in order to understand X in terms of a given cubic norm substructure of X. These ingredients are based on a number of useful identities that are our main focus in the present section. In order to describe their range of validity in a precise manner, a peculiar conceptual framework will be needed that we now proceed to consider.

35.1 The orthogonal complement of a cubic norm substructure. Let X_0 be a cubic norm substructure of X and write

$$X_0^\perp := \{u \in X \mid \forall x_0 \in X_0 : \ T(x_0, u) = 0\} \tag{1}$$

for the orthogonal complement of X_0 relative to the bilinear trace of X. From (33a.7) we obtain a well-defined bilinear action

$$X_0 \times X_0^\perp \longrightarrow X_0^\perp, \quad (x_0, u) \longmapsto x_0 \,.\, u := -x_0 \times u \tag{2}$$

that will be of fundamental importance later on. Unfortunately, however, the ingredients of this action are in general *not* compatible with base change: for $R \in k$-**alg**, the scalar extension X_{0R} need not be a cubic norm substructure of X_R, and even if it is, $(X_{0R})^\perp$, its orthogonal complement in X_R relative to the bilinear trace, need not be the same as $(X_0^\perp)_R$. To remedy this deficiency, the following refinement of the present set-up will be introduced.

35.2 Complemented cubic norm substructures. By a *complemented cubic norm substructure* of X we mean a pair (X_0, V) such that $X_0 \subseteq X$ is a cubic norm substructure, $V \subseteq X$ is a k-submodule and the relations

$$X = X_0 \oplus V, \quad V \subseteq X_0^\perp, \quad X_0 \,.\, V \subseteq V \tag{1}$$

hold. This concept is clearly compatible with base change, so if (X_0, V) is a complemented cubic norm substructure of X, then $(X_0, V)_R := (X_{0R}, V_R)$ is one of X_R, for all $R \in k$-**alg**. Note that (1) implies

$$X_0^\perp = (X_0 \cap X_0^\perp) \oplus V. \tag{2}$$

35.3 Remark. If $X_0 \subseteq X$ is a regular cubic norm substructure, then we deduce from Lemma 11.10 and (35.2.2) that $(X_0, X_0^\perp)$ is the unique complemented cubic norm substructure of X extended from X_0. Conversely, suppose X itself is regular and (X_0, V) is a complemented cubic norm substructure of X. Then X_0 is regular and $V = X_0^\perp$.

35.4 The action of X_0 on V. Let (X_0, V) be a complemented cubic norm substructure of X and write N_0 for the norm of X_0. We claim that the following relations hold, for all $R \in k$-**alg** and all $x_0, y_0 \in X_{0R}$, all $u \in V_R$.

$$1 \,.\, u = u, \tag{1}$$

$$U_{x_0} u = x_0^\sharp \,.\, u, \tag{2}$$

$$x_0 \,.\, (y_0 \,.\, (x_0 \,.\, u)) = (U_{x_0} y_0) \,.\, u, \tag{3}$$

$$x_0 \,.\, (x_0^\sharp \,.\, u) = N_0(x_0) u = x_0^\sharp \,.\, (x_0 \,.\, u), \tag{4}$$

$$N(x_0 \,.\, u) = N_0(x_0) N(u). \tag{5}$$

We may assume $R = k$. Then (1) follows immediately from (35.1.2) and the unit identity (33a.3), while the definition of the U-operator (33a.15) combined with (35.1.2) and the relation $T(x_0, u) = 0$ gives (2). To derive (3), we apply (33a.26) with $z = u$, observe $T(x_0^\sharp, u) = T(y_0, u) = 0$ and obtain $x_0 \,.\, (y_0 \,.\, (x_0 \,.\, u)) = -x_0 \times (y_0 \times (x_0 \times u)) = -(U_{x_0} y_0) \times u = (U_{x_0} y_0) \,.\, u$, hence (3). Since $T(x_0, u) = T(x_0^\sharp, u) = 0$, we obtain (4) immediately from (35.1.2) and (33a.8), (33a.19). To prove (5), we observe that (33a.29) reduces to $N(x_0 \,.\, u) = -N(x_0 \times u) = N(x_0)N(u)$, and this is (5).

Relations (1), (3) above are equivalent to saying that the linear map $\sigma\colon J_0 := J(X_0) \to \mathrm{End}_k(X_0^\perp)^{(+)}$ given by $\sigma(x_0)u := x_0 \,.\, u$ for $x_0 \in J_0$, $u \in X_0^\perp$ is a homomorphism of Jordan algebras. Thus if $k = F$ is a field, J_0 is simple as a Jordan algebra over F and $X_0^\perp \neq \{0\}$, then J_0 is special.

35.5 Strong orthogonality. With (X_0, V) as in 35.4, an element $u \in X$ is said to be *strongly orthogonal* (or *strongly perpendicular*) to X_0 if u and $u^\sharp$ both belong to V. Note that strong orthogonality depends not only on X_0 but, in fact, on all of (X_0, V) and that elements strongly orthogonal to X_0 may not exist. On the other hand, if $u \in X$ is strongly orthogonal to X_0, so is $u^\sharp$ by the adjoint identity. We now claim that the relations in 35a hold, for all $R \in k$-**alg**, all $x_0, y_0, z_0 \in X_{0R}$ and all $u \in X_R$ strongly orthogonal to X_{0R}.

$$(x_0 \,.\, u)^\sharp = x_0^\sharp \,.\, u^\sharp, \tag{1}$$

$$(x_0 \,.\, u) \times (y_0 \,.\, u) = (x_0 \times y_0) \,.\, u^\sharp, \tag{2}$$

$$(x_0 \,.\, u) \times u^\sharp = -N(u)x_0 = (x_0 \,.\, u^\sharp) \times u, \tag{3}$$

$$T(x_0 \,.\, u, y_0 \,.\, u) = 0, \tag{4}$$

$$T(x_0 \,.\, u, y_0 \,.\, u^\sharp) = N(u)T_0(x_0, y_0), \tag{5}$$

$$(x_0 \,.\, (y_0 \,.\, u)) \times u = T_0(x_0, y_0)u^\sharp - y_0 \,.\, (x_0 \,.\, u^\sharp), \tag{6}$$

$$(x_0 \,.\, (y_0 \,.\, u)) \times u^\sharp + u \times (x_0 \,.\, (y_0 \,.\, u^\sharp)) = -N(u)x_0 \circ y_0, \tag{7}$$

$$(x_0 \,.\, (y_0 \,.\, u)) \times (x_0 \,.\, u^\sharp) = -N(u)U_{x_0} y_0, \tag{8}$$

$$(x_0 \,.\, (y_0 \,.\, u)) \times (z_0 \,.\, u^\sharp) + (z_0 \,.\, (y_0 \,.\, u)) \times (x_0 \,.\, u^\sharp) = -N(u)\{x_0 y_0 z_0\}, \tag{9}$$

$$(x_0 \,.\, (y_0 \,.\, u)) \times u^\sharp = u \times (y_0 \,.\, (x_0 \,.\, u^\sharp)) = (x_0 \,.\, u) \times (y_0 \,.\, u^\sharp), \tag{10}$$

$$(x_0 \,.\, u) \times ((x_0 \,.\, u) \times (y_0 \,.\, u^\sharp)) = N(u)(U_{x_0} y_0) \,.\, u. \tag{11}$$

Table of Identities 35a Identities considered in 35.5.

Proof As before, we may assume $R = k$. The relations $T(x_0^\sharp, u) = T(x_0, u^\sharp) = 0$ combined with (33a.10) imply (1), which immediately yields (2) after linearizing with respect to x_0, while the first relation of (3) follows from $(x_0 \,.\, u)\times u^\sharp = -(x_0 \times u) \times u^\sharp$ and (33a.8); the same argument replacing (33a.8) by (33a.19) also gives the second. To establish (4), (5), we apply (35.1.1), (33a.7) and (2) to obtain $T(x_0 \,.\, u, y_0 \,.\, u) = -T(x_0 \,.\, u, y_0 \times u) = -T((x_0 \,.\, u) \times u, y_0) = -T((x_0 \times 1) \,.\, u^\sharp, y_0) = 0$ and $T(x_0 \,.\, u, y_0 \,.\, u^\sharp) = T(x_0 \times u, y_0 \times u^\sharp) = T((x_0 \times u) \times u^\sharp, y) = N(u)T_0(x_0, y_0)$. Turning to (6), we put $x := u$, $y := x_0$, $z := y_0$ in (33a.26) and obtain $u \times (x_0 \,.\, (y_0 \,.\, u)) = u \times (x_0 \times (u \times y_0)) = T(u, x_0)u \times y_0 + T(u^\sharp, y_0)x_0 + T(x_0, y_0)u^\sharp - (u^\sharp \times x_0) \times y_0 = -T(x_0, u)y_0 \,.\, u + T(y_0, u^\sharp)x_0 + T(x_0, y_0)u^\sharp - y_0 \,.\, (x_0 \,.\, u^\sharp)$; since u is strongly perpendicular to X_0, (6) follows. Similarly, setting $x := u^\sharp$, $y := x_0$, $z := y_0$, $w := u$ in (33a.27) yields

$$\begin{aligned} u^\sharp \times (x_0 \times (y_0 \times u)) + y_0 \times (x_0 \times (u \times u^\sharp)) + u \times (x_0 \times (u^\sharp \times y_0)) \\ = T(u^\sharp, x_0)y_0 \times u + T(y_0, x_0)u \times u^\sharp + T(u, x_0)u^\sharp \times y_0 \\ + T(u^\sharp \times y_0, u)x_0. \end{aligned}$$

But $u \times u^\sharp = -N(u)1$ by (3), which implies $T(u^\sharp \times y_0, u) = T(y_0, u \times u^\sharp) = -N(u)T(y_0)$, and we conclude

$$\begin{aligned} (x_0 \,.\, (y_0 \,.\, u)) \times u^\sharp - N(u)(1 \times x_0) \times y_0 + u \times (x_0 \,.\, (y_0 \,.\, u^\sharp)) \\ = -N(u)T(x_0, y_0)1 - N(u)T(y_0)x_0, \end{aligned}$$

where

$$(1 \times x_0) \times y_0 = T(x_0)1 \times y_0 - x_0 \times y_0 = T(x_0)T(y_0)1 - T(x_0)y_0 - x_0 \times y_0.$$

Thus

$$\begin{aligned} &(x_0 \,.\, (y_0 \,.\, u)) \times u^\sharp + u \times (x_0 \,.\, (y_0 \,.\, u^\sharp)) \\ &\quad = -N(u)\Big(x_0 \times y_0 + T(x_0)y_0 + T(y_0)x_0 - \big(T(x_0)T(y_0) - T(x_0, y_0)\big)1\Big) \\ &\quad = -N(u)x_0 \circ y_0 \end{aligned}$$

by (33a.23). This proves (7). In (8) we may assume by Lemma 12.25 that x_0 is invertible. Then (35.1.4) implies $u = x_0 \,.\, v$, where $v = x_0^{-1} \,.\, u$ is strongly orthogonal to X_0 by (1), and using (35.4.3), (1), (35.4.4), (3), (35.4.5), we obtain

$$\begin{aligned} (x_0 \,.\, (y_0 \,.\, u)) \times (x_0 \,.\, u^\sharp) &= \Big(x_0 \,.\, \big(y_0 \,.\, (x_0 \,.\, v)\big)\Big) \times \big(x_0 \,.\, (x_0 \,.\, v)^\sharp\big) \\ &= ((U_{x_0}y_0) \,.\, v) \times (x_0 \,.\, (x_0^\sharp \,.\, v^\sharp)) \\ &= N_0(x_0)((U_{x_0}y_0) \,.\, v) \times v^\sharp \\ &= -N_0(x_0)N(v)U_{x_0}y_0 = -N_0(x_0 \,.\, v)U_{x_0}y_0 = -N(u)U_{x_0}y_0, \end{aligned}$$

hence (8), which implies (9) after linearization. Comparing (9) for $z_0 = 1$ with (7) we obtain $(x_0 \,.\, (y_0 \,.\, u))\times u^\sharp + (y_0 \,.\, u)\times(x_0 \,.\, u^\sharp) = -N(u)x_0 \circ y_0 = (x_0 \,.\, (y_0 \,.\, u))\times u^\sharp + u \times (x_0 \,.\, (y_0 \,.\, u^\sharp))$, giving the second relation of (10) with x_0 and y_0 interchanged. On the other hand, linearizing (35.4.3) we obtain $(x_0 \,.\, (y_0 \,.\, u)) \times u^\sharp + (y_0 \,.\, (x_0 \,.\, u)) \times u^\sharp = ((x_0 \circ y_0) \,.\, u) \times u^\sharp = -N(u)x_0 \circ y_0$ by (3), and comparing with (7), we also obtain the first relation of (10) with x_0 and y_0 interchanged. Finally, to establish (11), we apply (33a.28) to $x_0 \,.\, u, y_0 \,.\, u^\sharp$ instead of x, y, respectively. Since $x_0 \,.\, u, y_0 \,.\, u^\sharp$ are strongly orthogonal to X_0 by (1), we have $T(x_0 \,.\, u) = T(y_0 \,.\, u^\sharp) = S(x_0 \,.\, u) = 0$, $T((x_0 \,.\, u)^\sharp, y_0 \,.\, u^\sharp) = T(x_0^\sharp \,.\, u^\sharp, y_0 \,.\, u^\sharp) = 0$ by (4), $S(x_0 \,.\, u, y_0 \,.\, u^\sharp) = -T(x_0 \,.\, u, y_0 \,.\, u^\sharp) = -N(u)T_0(x_0, y_0)$ by (5), and $(x_0 \,.\, u)^\sharp \times (y_0 \,.\, u^\sharp) = (x_0^\sharp \,.\, u^\sharp) \times (y_0 \,.\, u^\sharp) = (x_0^\sharp \times y_0) \,.\, u^{\sharp\sharp} = N(u)(x_0^\sharp \times y_0) \,.\, u$ by (1), (2). Hence (33a.28) yields $(x_0 \,.\, u) \times ((x_0 \,.\, u) \times (y_0 \,.\, u^\sharp)) = N(u)(T_0(x_0, y_0)x_0 - x_0^\sharp \times y_0) \,.\, u = N(u)(U_{x_0} y_0) \,.\, u$, as desired. □

For the remainder of this section, we fix a complemented cubic norm substructure (X_0, V) of X and write N_0 for the norm, T_0 (resp. S_0) for the (bi-)linear (resp. quadratic) trace of X_0.

35.6 Splitting the adjoint. We define quadratic maps $Q\colon V \to X_0$, $H\colon V \to V$ by

$$u^\sharp = -Q(u) + H(u) \qquad (u \in V, \quad Q(u) \in X_0, \quad H(u) \in V). \tag{1}$$

Thus $u \in X$ is strongly orthogonal to X_0 if and only if $u \in V$ and $Q(u) = 0$. We claim that the identities

$$(x_0 + u)^\sharp = (x_0^\sharp - Q(u)) + (-x_0 \,.\, u + H(u)), \tag{2}$$

$$N(x_0 + u) = N_0(x_0) - T_0(x_0, Q(u)) + N(u), \tag{3}$$

$$T(y_0 + v, z_0 + w) = T_0(y_0, z_0) + T_0(Q(v, w)), \tag{4}$$

$$T(y_0 + v) = T_0(y_0), \tag{5}$$

$$S(x_0 + u) = S_0(x_0) - T_0(Q(u)) \tag{6}$$

hold strictly for $x_0, y_0, z_0 \in X_0$, $u, v, w \in V$. Indeed, $N(x_0 + u) = N_0(x_0) + T(x_0^\sharp, u) + T(x_0, u^\sharp) + N(u) = N_0(x_0) - T_0(x_0, Q(u)) + N(u)$ by (35.2.1), (1) and $(x_0 + u)^\sharp = x_0^\sharp + x_0 \times u + u^\sharp = x_0^\sharp - x_0 \,.\, u - Q(u) + H(u)$ by (35.1.2) and (1). Finally, $T(y_0 + v, z_0 + w) = T_0(y_0, z_0) + T(v, w)$, and (33a.13) yields $T(v, w) = T(v)T(w) - T(v \times w) = -T(v \times w) = T(Q(v, w) - H(v, w)) = T_0(Q(v, w))$, giving (4), which immediately implies first (5) and then (6).

35.7 Identities for Q and H. We claim that the identities in 35b hold strictly for all $x_0, y_0, z_0 \in X_0$, $u, v, w \in V$.

Proof (33a.10) yields $(x_0 \,.\, u)^\sharp = (x_0 \times u)^\sharp = T(x_0^\sharp, u)u + T(x_0, u^\sharp)x_0 - x_0^\sharp \times$

$$
\begin{aligned}
Q(x_0 \,.\, u) &= U_{x_0} Q(u), && (1)\\
Q(x_0 \,.\, u, y_0 \,.\, u) &= U_{x_0,y_0} Q(u), && (2)\\
Q(x_0 \,.\, u, x_0 \,.\, v) &= U_{x_0} Q(u,v), && (3)\\
Q(x_0 \,.\, u, y_0 \,.\, v) + Q(x_0 \,.\, v, y_0 \,.\, u) &= U_{x_0,y_0} Q(u,v), && (4)\\
H(x_0 \,.\, u) &= x_0^\sharp \,.\, H(u), && (5)\\
H(x_0 \,.\, u, y_0 \,.\, u) &= (x_0 \times y_0) \,.\, H(u), && (6)\\
H(x_0 \,.\, u, x_0 \,.\, v) &= x_0^\sharp \,.\, H(u,v), && (7)\\
H(x_0 \,.\, u, y_0 \,.\, v) + H(x_0 \,.\, v, y_0 \,.\, u) &= (x_0 \times y_0) \,.\, H(u,v), && (8)\\
Q(H(u)) &= Q(u)^\sharp, && (9)\\
H(H(u)) &= N(u)u - Q(u) \,.\, H(u), && (10)\\
Q(x_0 \,.\, u, H(u)) &= N(u)x_0 = Q(u, x_0 \,.\, H(u)), && (11)\\
Q(H(u), v) + Q(u, H(u,v)) &= T_0\Big(Q(H(u), v)\Big)1, && (12)\\
H(x_0 \,.\, u, H(u)) &= T_0(x_0, Q(u))u - Q(u) \,.\, (x_0 \,.\, u), && (13)\\
H(u, x_0 \,.\, H(u)) &= (x_0 \times Q(u)) \,.\, u, && (14)\\
T_0(x_0, Q(u,v)) &= T_0(Q(x_0 \,.\, u, v)), && (15)\\
Q(H(u,v)) + Q(H(u), H(v)) &= Q(u,v)^\sharp + Q(u) \times Q(v), && (16)\\
H(H(u,v)) + H(H(u), H(v)) &= T_0\Big(Q(u, H(v))\Big)u + T_0\Big(Q(H(u), v)\Big)v && (17)\\
&\quad - Q(u) \,.\, H(v) - Q(u,v) \,.\, H(u,v)\\
&\quad - Q(v) \,.\, H(u),\\
N(H(u)) &= N(u)^2 - 2N_0(Q(u)). && (18)
\end{aligned}
$$

Table of Identities 35b Identities considered in 35.7.

$u^\sharp = -T_0(x_0, Q(u))x_0 + x_0^\sharp \times Q(u) - x_0^\sharp \times H(u) = -U_{x_0} Q(u) + x_0^\sharp \,.\, H(u)$, and comparing X_0- and V-components by means of (35.6.1), we obtain (1), (5). (Repeatedly) linearizing (1) (resp. (5)) implies (2)–(4) (resp. (6)–(8)). Similarly, by the adjoint identity and (35.6.2), $N(u)u = u^{\sharp\sharp} = (-Q(u) + H(u))^\sharp = Q(u)^\sharp - Q(H(u)) + (Q(u) \,.\, H(u) + H(H(u)))$, which leads to (9),(10). Applying (33a.8) we obtain $N(u)x_0 - T_0(x_0, Q(u))u = N(u)x_0 + T(u^\sharp, x_0)u = u^\sharp \times (u \times x_0) = -(x_0 \,.\, u) \times (-Q(u) + H(u)) = -Q(u) \,.\, (x_0 \,.\, u) + Q(x_0 \,.\, u, H(u)) - H(x_0 \,.\, u, H(u))$, hence (13) and the first relation of (11). Similarly, (33a.19) implies $N(u)x_0 = N(u)x_0 + T(u, x_0)u^\sharp = u \times (u^\sharp \times x_0) = u \times (-Q(u) \times x_0 + H(u) \times x_0) = (x_0 \times Q(u)) \,.\, u - u \times (x_0 \,.\, H(u)) = (x_0 \times Q(u)) \,.\, u + Q(u, x_0 \,.\, H(u)) - H(u, x_0 \,.\, H(u))$ implies (14) and

the second relation of (11). Linearizing (11) for $x_0 = 1$ with respect to u and applying (35.6.4) gives $Q(v, H(u)) + Q(u, H(u, v)) = T(u^\sharp, v)1 = T(H(u), v)1 = T_0(Q(H(u), v))1$, hence (12). To derive (15), we apply (1) and (33a.7) to obtain $T_0(x_0, Q(u, v)) = -T(x_0, u \times v) = -T(x_0 \times u, v) = T(x_0 \,.\, u, v) = T_0(Q(x_0 \,.\, u, v))$ by (35.6.4). Next (16), (17) will follow from (9), (10), respectively, by using the second order chain and product rules of the differential calculus for polynomial laws; we omit the details. And finally, turning to (18), we combine (33a.18) with (35.6.1),(35.6.3),(9) and obtain

$$\begin{aligned} N(u)^2 &= N(u^\sharp) = N(-Q(u) + H(u)) \\ &= -N_0(Q(u)) + T_0\Big(Q(u), Q(H(u))\Big) + N(H(u)) \\ &= -N_0(Q(u)) + T_0(Q(u), Q(u)^\sharp) + N(H(u)) \\ &= -N_0(Q(u)) + 3N_0(Q(u)) + N(H(u)) \end{aligned}$$

by Euler's differential equation (33a.11), and (18) follows. □

35.8 The build-up. The identities derived in the preceding subsection provide the opportunity of building up new cubic norm structures out of old ones. Let X_0 be a cubic norm structure over k, with base point 1, adjoint $x_0 \mapsto x_0^\sharp$, norm N_0, (bi-)linear trace T_0 and quadratic trace S_0. Suppose we are given

(i) a k-module V,
(ii) a bilinear action $X_0 \times V \to V$, $(x_0, u) \mapsto x_0 \,.\, u$,
(iii) quadratic maps $Q\colon V \to X_0$, $H\colon V \to V$ such that $Q(u, H(u)) \in R1_{X_{0R}}$ for all $u \in V_R$, $R \in k$-**alg**.

Since $1 \in X_0$ is a unimodular vector, condition (iii) yields a unique cubic form $\hat{N}\colon V \to k$ such that

$$\hat{N}(u)1_{X_{0R}} = Q(u, H(u)) \qquad (u \in V_R, R \in k\text{-}\mathbf{alg}). \tag{1}$$

Put $X := X_0 \times V$ as a k-module, identify X_0, V canonically as submodules of X and define a cubic form $N\colon X \to k$ as well as a quadratic map $\sharp\colon X \to X$ by requiring that

$$(x_0, u)^\sharp := (x_0^\sharp - Q(u), -x_0 \,.\, u + H(u)), \tag{2}$$

$$N((x_0, u)) := N_0(x_0) - T_0(x_0, Q(u)) + \hat{N}(u) \tag{3}$$

hold strictly for all $x_0 \in X_0$, $u \in V$. Inspecting (2), (3), we see that the k-module X together with the base point 1, adjoint $\sharp$ and norm N is a cubic array over k whose adjoint bilinearizes to

$$(x_0, u) \times (y_0, v) = (x_0 \times y_0 - Q(u, v), -x_0 \,.\, v - y_0 \,.\, u + H(u, v)) \tag{4}$$

for all $x_0, y_0 \in X_0$, $u, v \in V$. We also claim that the (bi-)linear and the quadratic trace of X are given by

$$T((y_0, v), (z_0, w)) = T_0(y_0, z_0) + T_0(Q(v, w)), \tag{5}$$
$$T((y_0, v)) = T_0(y_0) \tag{6}$$
$$S((x_0, u)) = S_0(x_0) - T_0(Q(u)) \tag{7}$$

for $x_0, y_0.z_0 \in X_0$, $u, v, w \in V$. Indeed, differentiating (3) implies

$$N((x_0, u), (y_0, v)) = N_0(x_0, y_0) - T_0(x_0, Q(u, v)) - T_0(Q(u), y_0) + \hat{N}(u, v), \tag{8}$$

where putting $x_0 = 1$, $u = 0$ (resp. $y_0 = 1$, $v = 0$) yields (6) (resp. (7)). Now (5) follows by linearizing (7) and applying (33.2.10).

35.9 Proposition (Petersson-Racine [225, Lemma 3.3])**.** *For X as defined in 35.8 to be a cubic norm structure over k it is necessary and sufficient that the identities in 35c hold in all scalar extensions.*

$$1 \,.\, u = u, \tag{1}$$
$$x_0^\sharp \,.\, (x_0 \,.\, u) = N_0(x_0)u, \tag{2}$$
$$Q(x_0 \,.\, u) = U_{x_0} Q(u), \tag{3}$$
$$H(x_0 \,.\, u) = x_0^\sharp \,.\, H(u), \tag{4}$$
$$Q(H(u)) = Q(u)^\sharp, \tag{5}$$
$$H(H(u)) = \hat{N}(u)u - Q(u) \,.\, H(u), \tag{6}$$
$$Q(x_0 \,.\, u, H(u)) = \hat{N}(u)x_0, \tag{7}$$
$$Q(H(u), v) + Q(u, H(u, v)) = T_0\Big(Q(H(u), v)\Big)1, \tag{8}$$
$$T_0(x_0, Q(u, v)) = T_0(Q(x_0 \,.\, u, v)), \tag{9}$$
$$H(x_0 \,.\, u, H(u)) = T_0(x_0, Q(u))u - Q(u) \,.\, (x_0 \,.\, u). \tag{10}$$

Table of Identities 35c Identities considered in 35.9.

Proof Assume first that X is a cubic norm structure. Then the set-up described in 35.8 shows that (X_0, V) is a complemented cubic norm substructure of X. Moreover, the identities (1)–(10), being a subset of the ones assembled in 35.4 and 35.7, hold strictly for $x_0 \in X_0$, $u, v \in V$. Conversely, let this be so. We must show the unit, gradient and adjoint identity. The unit identity is the least troublesome since the unit identity for X_0 combined with (35.8.2), (35.8.6)

and (1) implies $1 \times (x_0, u) = 1 \times x_0 - 1 \,.\, u = T_0(x_0)1 - x_0 - u = T((x_0, u))1 - (x_0, u)$. In order to derive the gradient identity, we differentiate (35.8.1) and combine the result with (8) to obtain $\hat{N}(u, v)1 = Q(v, H(u)) + Q(u, H(u, v)) = T_0(Q(H(u), v))1$, hence

$$\hat{N}(u, v) = T_0\Big(Q(H(u), v)\Big). \tag{11}$$

Now (35.8.8), the gradient identity for X_0 and (11), (9), (35.8.5), (35.8.2) imply

$$\begin{aligned}
N((x_0, u), (y_0, v)) &= T_0(x_0^\sharp, y_0) - T_0(x_0, Q(u, v)) - T_0(Q(u), y_0) + T_0\Big(Q(H(u), v)\Big) \\
&= T_0(x_0^\sharp - Q(u), y_0) - T_0(Q(x_0 \,.\, u, v)) + T_0\Big(Q(H(u), v)\Big) \\
&= T_0(x_0^\sharp - Q(u), y_0) + T_0\Big(Q(-x_0 \,.\, u + H(u), v)\Big) \\
&= T\Big((x_0^\sharp - Q(u), -x_0 \,.\, u + H(u)), (y_0, v)\Big) \\
&= T((x_0, u)^\sharp, (y_0, v),
\end{aligned}$$

as claimed. Finally, we apply the adjoint identity for X_0 and (35.8.2), (5), (3), (7), (2), (4), (10), (6), (33a.15), (35.8.3) to derive

$$\begin{aligned}
(x_0, u)^{\sharp\sharp} &= (x_0^\sharp - Q(u), -x_0 \,.\, u + H(u))^\sharp \\
&= \Big((x_0^\sharp - Q(u))^\sharp - Q(-x_0 \,.\, u + H(u)), \\
&\qquad - (x_0^\sharp - Q(u)) \,.\, (-x_0 \,.\, u + H(u)) + H(-x_0 \,.\, u + H(u))\Big) \\
&= \Big(x_0^{\sharp\sharp\sharp} - x_0^\sharp \times Q(u) + Q(u)^\sharp - Q(x_0 \,.\, u) \\
&\qquad + Q(x_0 \,.\, u, H(u)) - Q(H(u)), \\
&\quad x_0^\sharp \,.\, (x_0 \,.\, u) - x_0^\sharp \,.\, H(u) - Q(u) \,.\, (x_0 \,.\, u) + Q(u) \,.\, H(u) \\
&\qquad + H(x_0 \,.\, u) - H(x_0 \,.\, u, H(u)) + H(H(u))\Big) \\
&= (N_0(x_0)x_0 - x_0^\sharp \times Q(u) - U_{x_0}Q(u) + \hat{N}(u)x_0, \\
&\qquad N_0(x_0)u - T_0(x_0, Q(u))u + \hat{N}(u)u\Big) \\
&= (N_0(x_0)x_0 - T_0(x_0, Q(u))x_0 + \hat{N}(u)x_0, \\
&\qquad N_0(x_0)u - T_0(x_0, Q(u))u + \hat{N}(u)u\Big) \\
&= N((x_0, u))(x_0, u),
\end{aligned}$$

hence the adjoint identity for X. □

35.10 Passing to isotopes. Let X_0 be a cubic norm substructure of X and $p \in X_0$ an invertible element of $J(X_0)$. Then $X_0^{(p)}$, the p-isotope of X_0, is a cubic norm

substructure of $X^{(p)}$, and (33.11.4) shows

$$X_0^{(p)\perp} = X_0^{\perp} \tag{1}$$

as k-submodules of X. Moreover, the natural action of $X_0^{(p)}$ on $X_0^{(p)\perp}$ as defined in (35.1.2) is given by the formula

$$x_0 \mathbin{.^{(p)}} u = p \,.\, (x_0 \,.\, u) \tag{2}$$

for $x_0 \in X_0^{(p)}$ and $u \in X_0^{(p)\perp}$. Indeed, (33.11.2) and (35.4.2) imply

$$\begin{aligned} x_0 \mathbin{.^{(p)}} u &= -x_0 \times^{(p)} u = -N(p)U_{p^{-1}}(x_0 \times u) = N(p)U_{p^{-1}}(x_0 \,.\, u) \\ &= N(p^{-1})^{-1}p^{-1\sharp} \,.\, (x_0 \,.\, u) = (p^{-1})^{-1} \,.\, (x_0 \,.\, u) = p \,.\, (x_0 \,.\, u), \end{aligned}$$

as claimed. Similarly, one checks that $u \in X^{(p)}$ is strongly orthogonal to $X_0^{(p)}$ if and only if it is strongly orthogonal to X_0, in which case

$$u^{(\sharp,p)} = p \,.\, u^{\sharp}. \tag{3}$$

35.11 Complemented cubic norm substructures under isotopy. Let (X_0, V) be a complemented cubic norm substructure of X and $p \in X_0$ an invertible element of $J(X_0)$. From (35.2.1), (35.10.1) and (35.10.2) we conclude that $(X_0, V)^{(p)} := (X_0^{(p)}, V)$ is a complemented cubic norm substructure of $X^{(p)}$. Writing $Q^{(p)}, H^{(p)}$ for the analogues of Q, H as defined in 35.6, with (X_0, V) replaced by $(X_0, V)^{(p)}$, we claim

$$Q^{(p)}(u) = N(p)U_{p^{-1}}Q(u), \quad H^{(p)}(u) = p \,.\, H(u) \qquad (u \in V). \tag{1}$$

Indeed, applying (35.6.1), (33.11.2), (35.1.2) we get

$$\begin{aligned} -Q^{(p)}(u) + H^{(p)}(u) = u^{(\sharp,p)} &= N(p)U_{p^{-1}}u^{\sharp} = -N(p)U_{p^{-1}}Q(u) + N(p)U_{p^{-1}}H(u) \\ &= -N(p)U_{p^{-1}}Q(u) + N(p^{-1})^{-1}(p^{-1})^{\sharp} \,.\, H(u) \\ &= -N(p)U_{p^{-1}}Q(u) + (p^{-1})^{-1} \,.\, H(u) \\ &= -N(p)U_{p^{-1}}Q(u) + p \,.\, H(u), \end{aligned}$$

and comparing the components in X_0, V, respectively, the assertion follows.

Exercises

35.12. *Cubic solutions of the eikonal equation* (Tkachev [284]). Let k be a commutative ring containing $\frac{1}{6}$. By an *eikonal triple* over k we mean a triple (V, Q, N) consisting of a quadratic space (V, Q) over k and a cubic form $N\colon V \to k$ such that the quadratic map $H\colon V \to V$ uniquely determined by the strict validity of

$$Q(H(u), v) = \frac{1}{3}N(u, v) \tag{1}$$

in $V \times V$ strictly satisfies the *eikonal equation*

$$Q(H(u)) = Q(u)^2 \tag{2}$$

in V. Prove:

(i) If (V, Q, N) is an eikonal triple over k, then the k-module $X := k \times V$ together with the base point $1 \in X$, the adjoint $X \to X$, $x \mapsto x^\sharp$ and the norm $N\colon X \to k$ respectively defined by

$$1 := (1, 0), \tag{3}$$

$$(r, u)^\sharp = (r^2 - Q(u), -ru + H(u)), \tag{4}$$

$$N((r, u)) := r^3 - 3rQ(u) + N(u) \tag{5}$$

for $R \in k$-**alg**, $r \in R$, $u \in V_R$, is a regular cubic norm structure over k.

(ii) Conversely, let X be a regular cubic norm structure over k. Then $X_0 := k = k1 \subseteq X$ is a regular cubic norm substructure, and if we put $V := X_0^\perp$ to define $Q\colon V \to k$ by the condition $Q(u) + u^\sharp \in V$ for all $u \in V$, then $(V, Q, N|_V)$ is an eikonal triple over k.

(iii) The constructions presented in (i), (ii) are inverse to each other.

(iv) If $(\mathbb{R}^n, Q, N)$ is an eikonal triple over the field of real numbers, then the eikonal equation (2) takes on the co-ordinate form

$$\sum_{i,j=1}^{n} q^{ij} \frac{\partial N}{\partial x_i}(u) \frac{\partial N}{\partial x_j}(u) = 9\Big(\sum_{i,j=1}^{n} q_{ij} u_i u_j\Big)^2 \tag{6}$$

for

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{R}^n,$$

where $Q = (q_{ij}) \in \mathrm{Sym}_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$ corresponds to the quadratic form Q and $Q^{-1} = (q^{ij})$.

36 Cubic Jordan matrix algebras

An encounter with cubic Jordan matrix algebras has already taken place in section 5 over the field of real numbers. Using the formalism of cubic norm structures, we are now in a position to extend a twisted version of this concept to arbitrary base rings. For convenience, the following notational convention will be introduced.

36.1 The ternary cyclicity convention. Unless explicitly stated otherwise, indices i, j, l (or m, n, p) are always tacitly assumed to vary over all cyclic permutations (ijl) (or (mnp)) of (123). For example, given arbitrary elements x_{ijl} of an arbitrary k-module, this convention allows us to write $\sum x_{ijl}$ for $x_{123} + x_{231} + x_{312}$.

36.2 Twisted matrix involutions. Let C be a conic algebra over k whose conjugation is an involution, and which is faithful as a k-module, allowing us to identify $k \subseteq C$ canonically as a unital subalgebra. If m is a positive integer, then $\mathrm{Mat}_m(k) \subseteq \mathrm{Mat}_m(C)$ by Exc. 8.15 is a nuclear subalgebra. Twisting the conjugate transpose involution of $\mathrm{Mat}_m(C)$ in the sense of 10.7 by means of a diagonal matrix

$$\Gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_m) \in \mathrm{GL}_m(k) \tag{1}$$

in the sense of 10.8, we therefore conclude that the map

$$\mathrm{Mat}_m(C) \longrightarrow \mathrm{Mat}_m(C), \quad x \longmapsto \Gamma^{-1}\bar{x}^{\mathsf{T}}\Gamma \tag{2}$$

is an involution, called the Γ-*twisted conjugate transpose involution* of $\mathrm{Mat}_m(C)$. The elements of $\mathrm{Mat}_m(C)$ remaining fixed under this involution are called Γ-*twisted hermitian matrices*, and simply *hermitian matrices* if $\Gamma = \mathbf{1}_m$ is the m-by-m unit matrix. The Γ-twisted hermitian matrices of $\mathrm{Mat}_m(C)$ *having diagonal entries in* k form a k-submodule of $\mathrm{Mat}_m(C)$ which we denote by

$$\mathrm{Her}_m(C, \Gamma); \tag{3}$$

in particular, we put

$$\mathrm{Her}_m(C) := \mathrm{Her}_m(C, \mathbf{1}_m). \tag{4}$$

If 2 is invertible in k, then $\mathrm{Her}_m(C, \Gamma)$ is the totality of all Γ-twisted hermitian matrices in $\mathrm{Mat}_m(C)$, the condition on the diagonal entries being automatic since $H(C, \iota_C) = k1_C = k$ by (16.6.3).

Now assume $m = 3$. Writing e_{ij}, $1 \leq i, j \leq 3$, for the ordinary matrix units of $\mathrm{Mat}_3(k) \subseteq \mathrm{Mat}_3(C)$, we obtain a natural set of generators for the k-module $\mathrm{Her}_3(C, \Gamma)$ by considering the quantities

$$u[jl] := \gamma_l u e_{jl} + \gamma_j \bar{u} e_{lj} \qquad (u \in C, \quad j, l = 1, 2, 3 \ \text{ distinct}), \tag{5}$$

called *primitive* Γ-*twisted hermitian matrices*. Indeed, a straightforward verification shows that $x \in \mathrm{Mat}_3(C)$ belongs to $\mathrm{Her}_3(C, \Gamma)$ if and only if it can be written in the form (necessarily unique)

$$x = \sum (\xi_i e_{ii} + u_i[jl]) \qquad (\xi_i \in k, \quad u_i \in C, \quad i = 1, 2, 3). \tag{6}$$

Thus we have a natural identification

$$\mathrm{Her}_3(C, \Gamma) = \sum (k e_{ii} \oplus C[jl]) = (k \oplus C) \oplus (k \oplus C) \oplus (k \oplus C) \tag{7}$$

as k-modules.

With a few extra hypotheses on C, we wish to define a cubic norm structure on the k-module $\mathrm{Her}_3(C, \Gamma)$ in a natural way that commutes with base change.

Actually, we will be able to do so without any conditions on C as a k-module, and without assuming that the diagonal matrix $\Gamma \in \mathrm{Mat}_3(k)$ be invertible. This will be accomplished by formalizing the preceding set-up in a slightly different manner. We begin by introducing a convenient terminology.

36.3 Co-ordinate pairs. By a *pre-co-ordinate pair* over k we mean a pair (C, Γ) consisting of a multiplicative conic alternative k-algebra C and a diagonal matrix $\Gamma \in \mathrm{Mat}_3(k)$. In this case, it will always be tacitly assumed that Γ has the form $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3)$, with $\gamma_i \in k$, $1 \leq i \leq 3$. If Γ is invertible, we speak of a *co-ordinate pair* over k. For $\Gamma = \mathbf{1}_3$, we identify $C = (C, \mathbf{1}_3)$ and refer to this as a *co-ordinate algebra* over k. If C is an octonion algebra, the terms *octonionic (pre-)co-ordinate pair*, *octonionic co-ordinate algebra*, respectively, will be used, ditto for C being a quaternion or quadratic étale k-algebra.

36.4 Towards a hermitian cubic norm structure. Let (C, Γ) be a pre-co-ordinate pair over k. By Prop. 17.2, C is norm-associative (i.e., the identities (16.12.1)–(16.12.5) hold in C) and its conjugation is an involution. Guided by the formulas of 36.2, but abandoning their interpretation by means of hermitian matrices, we consider the k-module of all formal expressions

$$\sum (\xi_i e_{ii} + u_i[jl])$$

for $\xi_i \in k$, $u_i \in C$ and $i = 1, 2, 3$. Thanks to the formal character of these expressions, and in analogy of (36.2.7), this k-module, denoted by $X(C)$, may be written as

$$X(C) = \sum (k e_{ii} + C[jl]) = (k \oplus C) \oplus (k \oplus C) \oplus (k \oplus C), \tag{1}$$

and hence its dependence on C is compatible with base change: $X(C)_R = X(C_R)$ for all $R \in k$-**alg**. Note, however, that the diagonal matrix $\Gamma \in \mathrm{Mat}_3(k)$ has not yet entered the scene, which will happen only after we have given $X(C)$ the structure of a cubic array over k. In order to do so, we consider elements

$$x = \sum (\xi_i e_{ii} + u_i[jl]), \quad y = \sum (\eta_i e_{ii} + v_i[jl]) \tag{2}$$

of $X(C)_R$, with $\xi_i, \eta_i \in R$, $u_i, v_i \in C_R$ for $i = 1, 2, 3$, to define base point, adjoint and norm on $X(C)$ by the formulas

$$1 = 1_X := \sum e_{ii}, \tag{3}$$

$$x^\sharp = \sum \Big((\xi_j \xi_l - \gamma_j \gamma_l n_C(u_i)) e_{ii} + (- \xi_i u_i + \gamma_i \overline{u_j u_l})[jl] \Big), \tag{4}$$

$$N(x) := N_X(x) = \xi_1 \xi_2 \xi_3 - \sum \gamma_j \gamma_l \xi_i n_C(u_i) + \gamma_1 \gamma_2 \gamma_3 t_C(u_1 u_2 u_3), \tag{5}$$

the very last expression on the right of (5) being unambiguous by (16.13.1). One checks easily that these formulas make $X(C)$ a cubic array over k, which

we denote by $\mathrm{Her}_3(C,\Gamma)$and which is clearly compatible with base change: $\mathrm{Her}_3(C,\Gamma)_R = \mathrm{Her}_3(C_R,\Gamma_R)$ for all $R \in k$-**alg**. Moreover, the adjoint bilinearizes to

$$x \times y = \sum \Big((\xi_j\eta_l + \eta_j\xi_l - \gamma_j\gamma_l n_C(u_i,v_i))e_{ii} + (-\xi_i v_i - \eta_i u_i + \gamma_i\overline{u_j v_l + v_j u_l})[jl] \Big), \tag{6}$$

and we claim that *the (bi-)linear and quadratic traces of X are given by*

$$T(x,y) = \sum (\xi_i\eta_i + \gamma_j\gamma_l n_C(u_i,v_i)), \tag{7}$$

$$T(x) = \sum \xi_i, \tag{8}$$

$$S(x) = \sum (\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i)). \tag{9}$$

Indeed, differentiating (5) at x in the direction y, we obtain, using (16.13.1),

$$N(x,y) = \sum \Big(\xi_j\xi_l\eta_i - \gamma_j\gamma_l(\eta_i n_C(u_i) + \xi_i n_C(u_i,v_i)) + \gamma_1\gamma_2\gamma_3 t_C(u_i u_j v_l) \Big), \tag{10}$$

and setting $x = 1$ gives (8), while setting $y = 1$ yields (9). On the other hand, linearizing (9) we deduce

$$S(x,y) = \sum (\xi_j\eta_l + \eta_j\xi_l - \gamma_j\gamma_l n_C(u_i,v_i)). \tag{11}$$

Finally, combining (11) with (8) and (33.2.10), we end up with (7).

36.5 Theorem (Freudenthal [83, 84], McCrimmon [183, Thm. 3])**.** *Let (C,Γ) be a pre-co-ordinate pair over k. Then the cubic array $\mathrm{Her}_3(C,\Gamma)$ of 36.4 is a cubic norm structure and hence may be viewed canonically (cf. 34.6) as a cubic Jordan k-algebra. As a module, $\mathrm{Her}_3(C,\Gamma)$ is finitely generated projective if and only if C is. As a cubic Jordan algebra, it is regular in the sense of 33.3 if and only if C is a regular composition algebra.*

Proof The unit (resp. gradient) identity follows from (36.4.3), (36.4.6), (36.4.8) (resp. (36.4.4), (36.4.7), (36.4.11)) by a straightforward verification. It remains to prove the adjoint identity over k. To this end we put

$$x^\sharp = \sum (\xi_i^\sharp e_{ii} + u_i^\sharp[jl]), \tag{1}$$

where $\xi_i^\sharp \in k$ and $u_i^\sharp \in C$ can be read off from (36.4.4). We must show $\xi_i^{\sharp\sharp} = N(x)\xi_i$ and $u_i^{\sharp\sharp} = N(x)u_i$. We begin with the former by repeatedly applying (36.4.4):

$$\begin{aligned}\xi_i^{\sharp\sharp} &= \xi_j^\sharp\xi_l^\sharp - \gamma_j\gamma_l n_C(u_i^\sharp)\\ &= (\xi_l\xi_i - \gamma_l\gamma_i n_C(u_j))(\xi_i\xi_j - \gamma_i\gamma_j n_C(u_l)) - \gamma_j\gamma_l n_C(-\xi_i u_i + \gamma_i\overline{u_j u_l}).\end{aligned}$$

Expanding the terms on the right-hand side of the last equation and combining (16.5.7), (17.1.1), (16.5.5) with the fact that the expression $t_C(u_1u_2u_3)$ is invariant under cyclic permutations of its arguments, we conclude

$$\begin{aligned}\xi_i^{\sharp\sharp} &= \xi_1\xi_2\xi_3\xi_i - \gamma_i\gamma_j\xi_l\xi_i n_C(u_l) - \gamma_l\gamma_i\xi_i\xi_j n_C(u_j) + \gamma_1\gamma_2\gamma_3\gamma_i n_C(u_j)n_C(u_l)\\ &\quad - \gamma_j\gamma_l\xi_i^2 n_C(u_i) + \gamma_1\gamma_2\gamma_3\xi_i n_C(u_i,\overline{u_ju_l}) - \gamma_1\gamma_2\gamma_3\gamma_i n_C(\overline{u_ju_l})\\ &= (\xi_1\xi_2\xi_3 - \gamma_j\gamma_l\xi_i n_C(u_i) - \gamma_l\gamma_i\xi_j n_C(u_j) - \gamma_i\gamma_j\xi_l n_C(u_l) + \gamma_1\gamma_2\gamma_3 t_C(u_1u_2u_3))\xi_i\\ &= N(x)\xi_i,\end{aligned}$$

as desired. Similarly, we expand

$$\begin{aligned}u_i^{\sharp\sharp} &= -\xi_i^\sharp u_i^\sharp + \gamma_i\overline{u_j^\sharp u_l^\sharp} = -(\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i))(-\xi_i u_i + \gamma_i\overline{u_ju_l})\\ &\quad + \gamma_i(-\xi_l\bar{u}_l + \gamma_l u_iu_j)(-\xi_j\bar{u}_j + \gamma_j u_lu_i)\\ &= \xi_1\xi_2\xi_3u_i - \gamma_i\xi_j\xi_l\overline{u_ju_l} - \gamma_j\gamma_l\xi_i n_C(u_i)u_i + \gamma_1\gamma_2\gamma_3 n_C(u_i)\overline{u_ju_l}\\ &\quad + \gamma_i\xi_j\xi_l\bar{u}_l\bar{u}_j - \gamma_i\gamma_j\xi_l\bar{u}_l(u_lu_i) - \gamma_l\gamma_i\xi_j(u_iu_j)\bar{u}_j + \gamma_1\gamma_2\gamma_3(u_iu_j)(u_lu_i).\end{aligned}$$

Here we combine the fact that the conjugation of C is an involution with Kirmse's identities (17.4.1) to conclude

$$u_i^{\sharp\sharp} = (\xi_1\xi_2\xi_3 - \sum\gamma_n\gamma_p\xi_m n_C(u_m))u_i + \gamma_1\gamma_2\gamma_3(n_C(u_i)\overline{u_ju_l} + (u_iu_j)(u_lu_i)),$$

where the middle Moufang identity (13.3.3) and (17.4.2) yield

$$\begin{aligned}n_C(u_i)\overline{u_ju_l} + (u_iu_j)(u_lu_i) &= n_C(u_i)\overline{u_ju_l} + u_i(u_ju_l)u_i = n_C(u_i,\overline{u_ju_l})u_i\\ &= t_C(u_1u_2u_3)u_i.\end{aligned}$$

Thus $u_i^{\sharp\sharp} = N(x)u_i$, and the proof of the adjoint identity is complete.

As a k-module, $\mathrm{Her}_3(C,\Gamma)$ is the sum of three copies of C and three copies of k. Therefore, it is finitely generated projective if and only if C is. The formula (36.4.7) for the bilinear form T in terms of the bilinear form Dn_C gives the claim on regularity. □

36.6 The concept of a cubic Jordan matrix algebras. The cubic Jordan algebra $\mathrm{Her}_3(C,\Gamma)$ of Thm. 36.5 is called a *cubic Jordan matrix algebra.* The justification of this terminology derives from the fact that, if $1_C \in C$ is unimodular and $\Gamma \in \mathrm{GL}_3(k)$, then the elements of J by 36.2 may be identified canonically with the Γ-twisted 3-by-3 hermitian matrices having entries in C and scalars down the diagonal, i.e., with the matrices

$$x = \sum(\xi_i e_{ii} + u_i[jl]) = \begin{pmatrix}\xi_1 & \gamma_2u_3 & \gamma_3\bar{u}_2\\ \gamma_1\bar{u}_3 & \xi_2 & \gamma_3u_1\\ \gamma_1u_2 & \gamma_2\bar{u}_1 & \xi_3\end{pmatrix} \tag{1}$$

for $\xi_i \in k$, $u_i \in C$, $1 \le i \le 3$, and this identification is compatible with base change. Note, however, that the Jordan structure of J is not as closely linked to ordinary matrix multiplication as one would naively expect. On the positive side, it follows from Exc. 36.11 below that the squaring of J and that of $\mathrm{Mat}_3(C)$ coincide on J. Hence so do the circle product of J and the symmetric matrix product $(x, y) \mapsto xy + yx$ of $\mathrm{Mat}_3(C)$. Thus, if $2 \in k^\times$, then its linear Jordan structure makes J a unital subalgebra of $\mathrm{Mat}_3(C)^{(+)}$; in particular, the euclidean Albert algebra $\mathrm{Her}_3(\mathbb{O})$ of 5.5 is a (very important) example of a cubic Jordan matrix algebra over the reals. On the other hand, returning to the case of an arbitrary base ring, if C is alternative but not associative, then the k-algebra $\mathrm{Mat}_3(C)$ is not flexible, and the U-operator $U_x y$ of J will in general not be the same as $(xy)x$ or $x(yx)$ (Exc. 36.11, eqn. (3), below). On the other hand, the same formula immediately implies the following useful observation.

36.7 Proposition. *Let (C, Γ) be a co-ordinate pair over k such that $1_C \in C$ is unimodular. If C is associative, then the Jordan algebra $\mathrm{Her}_3(C, \Gamma)$ is a subalgebra of $\mathrm{Mat}_3(C)^{(+)}$.* □

36.8 Examples. We illustrate the preceding formulas by exhibiting some inner ideals in a cubic Jordan matrix algebra $J := \mathrm{Her}_3(C, \Gamma)$.

(i) When $x = e_{11}$, the calculations in Example 32.6 show that $x \times J$ (an inner ideal by Example 34.9) is the Peirce space $ke_{22} + ke_{33} + C[23]$. In case C is an octonion algebra, $x \times J$ is finitely generated projective of rank 10 as a k-module.

(ii) If V is a totally isotropic subspace of C, then $I := ke_{11} + V[12]$ is an inner ideal. To see this, note that any $x \in I$ satisfies $x^\sharp = 0$ because each of the terms in (36.4.4) vanishes.

(iii) If V is a submodule of C such that $uv = 0$ for all $u, v \in V$, then $I := V[12] + V[23] + V[31]$ is an inner ideal. For this the verification is the same: one checks that $x^\sharp = 0$ for every $x \in I$. In case C is the split octonions over a field, V can have dimension 2 (at most) [209, pp. 544-545], so this example yields inner ideals of dimension 6.

36.9 Proposition. *The map $\varphi\colon \mathrm{Mat}_3(k)^{(+)} \to \mathrm{Her}_3(k \times k)$ defined by*

$$\varphi(x) := \sum (\xi_{ii} e_{ii} + (\xi_{jl}, \xi_{lj})[jl])$$

for $x = (\xi_{ij})_{1 \le i,j \le 3} \in \mathrm{Mat}_3(k)$ is an isomorphism of cubic Jordan algebras.

Proof φ is a linear bijection sending $\mathbf{1}_3$ to 1_J with $J := \mathrm{Her}_3(k \times k)$. By Example 34.16 and Exc. 34.18, therefore, it suffices to show that φ preserves norms. Actually, since φ commutes with base change, we need only show

$N_J(\varphi(x)) = \det(x)$ for all $x = (\xi_{ij}) \in \mathrm{Mat}_3(k)$. To this end we put $C := k \times k$ and note $n_C((\alpha,\beta)) = \alpha\beta$, $t_C((\alpha,\beta)) = \alpha + \beta$ for $\alpha, \beta \in k$. Hence (36.4.5) implies

$$\begin{aligned} N_J(\varphi(x)) &= N_J\Big(\sum (\xi_{ii}e_{ii} + (\xi_{jl}, \xi_{lj})[jl])\Big) \\ &= \xi_{11}\xi_{22}\xi_{33} - \sum \xi_{ii}\xi_{jl}\xi_{lj} + \xi_{23}\xi_{31}\xi_{12} + \xi_{32}\xi_{13}\xi_{21} \\ &= \xi_{11}\xi_{22}\xi_{33} + \xi_{12}\xi_{23}\xi_{31} + \xi_{13}\xi_{21}\xi_{32} \\ &\quad - \xi_{31}\xi_{22}\xi_{13} - \xi_{32}\xi_{23}\xi_{11} - \xi_{33}\xi_{21}\xi_{12} \\ &= \det(x), \end{aligned}$$

as claimed. □

Exercises

36.10. Let C be a conic k-algebra whose identity element is unimodular, and let $\Gamma \in \mathrm{GL}_2(k)$ be a diagonal matrix. In slight modification of (36.2.3), write $\mathrm{Her}_2(C,\Gamma)$ for the k-module of all 2-by-2 matrices x with entries in C that are Γ-hermitian (i.e., $x = \Gamma^{-1}\bar{x}^{\mathsf{T}}\Gamma$) and have diagonal entries in $k = k1_C$. Show that $\mathrm{Her}_2(C,\Gamma)$ carries canonically the structure of a Jordan algebra J of Clifford type whose identity element is the 2-by-2 unit matrix and whose U-operator may be described as

$$U_x y = (xy)x + [y,x,x] = x(yx) - [x,x,y] \qquad (x, y \in J) \tag{1}$$

in terms of matrix multiplication. Show further that the pointed quadratic module underlying J is uniquely determined by these conditions provided C is projective as a k-module.

Remark. Putting $y = \mathbf{1}_2$ in (1) shows that the squaring in J agrees with the restriction to J of the squaring of 2-by-2 matrices. Hence the para-quadratic circle product in J is the same as the symmetric matrix product: $x \circ y = xy + yx$.

36.11. *The U-operator and matrix multiplication.* Let (C,Γ) be a co-ordinate pair over k and assume that $1_C \in C$ is unimodular. Let

$$x = \sum(\xi_i e_{ii} + u_i[jl]), \quad y = \sum(\eta_i e_{ii} + v_i[jl]) \in J := \mathrm{Her}_3(C,\Gamma)$$

with $\xi_i, \eta_i \in k$, $u_i, v_i \in C$ for $i = 1,2,3$ and write $1, x, x^2, x^3, \ldots$ for the powers of x in J, while denoting matrix multiplication in $\mathrm{Mat}_3(C)$ by juxtaposition. Then prove

$$x^2 = xx, \tag{1}$$

$$x^3 = x(xx) + \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3]\mathbf{1}_3 = (xx)x - \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3]\mathbf{1}_3, \tag{2}$$

$$\begin{aligned} U_x y &= x(yx) - [x,x,y] + \gamma_1\gamma_2\gamma_3([u_1,u_2,v_3] + [u_2,u_3,v_1] + [u_3,u_1,v_2])\mathbf{1}_3 \\ &= (xy)x + [y,x,x] - \gamma_1\gamma_2\gamma_3([u_1,u_2,v_3] + [u_2,u_3,v_1] + [u_3,u_1,v_2])\mathbf{1}_3, \end{aligned} \tag{3}$$

$$[x,x,x] = 2\gamma_1\gamma_2\gamma_3[u_1,u_2,u_3]\mathbf{1}_3, \tag{4}$$

$$x^\sharp x = (N(x)1_C + \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3])\mathbf{1}_3, \tag{5}$$

$$xx^\sharp = (N(x)1_C - \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3])\mathbf{1}_3. \tag{6}$$

Finally, writing $x^\sharp$ as

$$x^\sharp = \sum (\xi_i^\sharp + u_i^\sharp [jl])$$

with $\xi_i^\sharp \in k$, $u_i^\sharp \in C$ for $i = 1, 2, 3$, conclude that

$$[u_1^\sharp, u_2^\sharp, u_3^\sharp] = -N(x)[u_1, u_2, u_3]. \tag{7}$$

Remark. If $2 \in k^\times$, then

$$\mathrm{Mat}_3(C) = \mathrm{Her}_3(C, \Gamma) \oplus \mathrm{Her}_3^-(C, \Gamma), \tag{8}$$

where $\mathrm{Her}_3^-(C, \Gamma) = \{x \in \mathrm{Mat}_3(C) \mid x = -\Gamma^{-1} \bar{x}^\mathsf{T} \Gamma\}$. Since the trace of C is an associative linear form, the expressions $[u, v, w]\mathbf{1}_3$ for $u, v, w \in C$ all belong to $\mathrm{Her}_3^-(C, \Gamma)$. Hence (3) implies that, with respect to the decomposition (8), $U_x y$ is the $\mathrm{Her}_3(C, \Gamma)$-component of $x(yx) - [x, x, y]$ and also of $(xy)x + [y, x, x]$. Compare this with eqn. (1) of Exc. 36.10.

37 Elementary idempotents and co-ordinatization

Elementary idempotents as defined in Exc. 16.23 have been a useful tool in our study of composition algebras. We will see in this section that the natural extension of this concept to cubic Jordan algebras turns out to be even more momentous. After introducing the concept itself, we describe the Peirce decomposition relative to elementary idempotents, and to complete orthogonal systems thereof, called elementary frames, purely in terms of cubic norm structures. We then identify elementary idempotents in cubic Jordan matrix algebras and prove the Jacobson co-ordinatization theorem 37.17, which basically says that every cubic Jordan algebra containing an elementary frame that is connected (cf. Exc. 32.23) is isomorphic to a cubic Jordan matrix algebra.

Throughout this section, we let k be a commutative ring and, unless other arrangements have been made, let J be a cubic Jordan algebra over k, with unit element $1 = 1_J$, adjoint $x \mapsto x^\sharp$, norm $N = N_J$, (bi-)linear trace $T = T_J$ and quadratic trace $S = S_J$.

37.1 The concept of an elementary idempotent. An element $e \in J$ is called an *elementary idempotent* if $e^\sharp = 0$ and $T(e) = 1$. In this case, $S(e) = T(e^\sharp) = 0$, and (33a.22) implies $e^2 = e$, so e is indeed an idempotent and a unimodular one at that. In particular, the adjoint identity yields $N(e)e = e^{\sharp\sharp} = 0$, hence $N(e) = 0$. We also have $T(e, e) = T(e)^2 - 2S(e)$ by (33a.13), hence $T(e, e) = 1$. Note by the base point identities (33a.1) that $1 = 1_J$ is an elementary idempotent if and only if $k = \{0\}$ (hence $J = \{0\}$). The property of being an elementary idempotent is clearly preserved by homomorphisms and scalar extensions of cubic Jordan algebras.

37.2 Proposition (cf. Racine [242], Petersson-Racine [228]). *Let e be an elementary idempotent of J.*

(a) *The complementary idempotent $e_0 = 1 - e$ satisfies $e_0^\sharp = e$ and $T(e_0) = 2$.*

(b) *The Peirce components of J relative to e are orthogonal with respect to T and can be described as*

$$J_2(e) = ke, \tag{1}$$

$$J_1(e) = \{x \in J \mid T(x) = 0,\ e \times x = 0\}, \tag{2}$$

$$J_0(e) = \{x \in J \mid e \times x = T(x)e_0 - x\}. \tag{3}$$

(c) $x^\sharp = S(x)e$ *for all* $x \in J_0(e)$.

Proof (a) $e_0^\sharp = (1-e)^\sharp = 1^\sharp - 1 \times e + e^\sharp = 1 - T(e)1 + e = e$ and $T(e_0) = T(1) - T(e) = 3 - 1 = 2$.

(b) Let $x_i \in J_i := J_i(e)$ for $i = 0, 1, 2$. We must show $T(x_i, x_j) = 0$ for $i, j = 0, 1, 2$ distinct. First of all, for $j = 1$ or 2, Thm. 32.2 and (33a.31) yield $T(x_2, x_j) = T(U_e x_2, x_j) = T(x_2, U_e x_j) = 0$. Similarly, $T(x_0, x_1) = T(U_{e_0} x_0, x_1) = T(x_0, U_{e_0} x_1)) = 0$ since $J_i(e_0) = J_{2-i}$ by Cor. 32.3 (b). This proves the first part of (b).

As to the explicit description of the Peirce components, we have $J_2(e) = \mathrm{Im}(U_e)$ by (32.2.4) and $U_e x = T(e, x)e - e^\sharp \times x = T(e, x)e \in ke$ for $x \in J$, hence $J_2(e) \subseteq ke$. Here the relation $U_e e = e^3 = e$ gives equality. To prove (2), (3), we apply (33a.23) to obtain $e \times x = e \circ x - T(e)x - T(x)e + (T(e)T(x) - T(e, x))1 = e \circ x - x + T(x)e_0 - T(e, x)1$, hence

$$e \circ x = x + e \times x - T(x)e_0 + T(e, x)1 \qquad (x \in J). \tag{4}$$

But $x \in J_1$ if and only if $e \circ x = x$ by (32.2.7), and from (4) we conclude

$$x \in J_1 \quad \Longleftrightarrow \quad e \times x = T(x)e_0 - T(e, x)1. \tag{5}$$

Now suppose $x \in J_1$. Then $T(e, x) = T(e_0, x) = 0$ by the first part, hence $T(x) = T(e, x) + T(e_0, x) = 0$, and (5) yields $e \times x = 0$ as well. Conversely, suppose $e \times x = 0$ and $T(x) = 0$. Taking traces of the first equation, we conclude $0 = T(e \times x) = T(e)T(x) - T(e, x) = -T(e, x)$, and (5) shows $x \in J_1$. This proves (2). Turning to (3), let $x \in J_0$. Then $e \circ x = 0$ by (32.2.6) and $T(e, x) = 0$ by the first part, forcing $e \times x = T(x)e_0 - x$ by (4). Conversely, if this relation holds, then $T(x) = 2T(x) - T(x) = T(x)T(e_0) - T(x) = T(e \times x) = T(e)T(x) - T(e, x) = T(x) - T(e, x)$, which implies $T(e, x) = 0$ and then $T(x) = T(1, x) = T(e, x) + T(e_0, x) = T(e_0, x)$. Thus (a) gives $U_{e_0} x = T(e_0, x)e_0 - e_0^\sharp \times x = T(x)e_0 - e \times x = x$, forcing $x \in J_0$, and the proof of (b) is complete.

(c) For $x \in J_0 = J_2(e_0)$ we have $x = U_{e_0}x$, and (33a.20) combined with (a) implies $x^\sharp = (U_{e_0}x)^\sharp = U_{e_0{}^\sharp}x^\sharp = U_e x^\sharp$. Hence $x^\sharp \in J_2 = ke$, and we find a scalar $\alpha \in k$ with $x^\sharp = \alpha e$. Taking traces, (c) follows. □

37.3 Corollary (Faulkner's lemma [74, Lemma 1.5])**.** *Let $e \in J$ be an elementary idempotent and put*

$$M_0 := J_0(e) \ \ (\textit{as a } k\textit{-module}), \quad q_0 := S|_{M_0}, \quad e_0 := 1 - e. \tag{1}$$

Then (M_0, q_0, e_0) is a pointed quadratic module over k and $J_0(e) = J(M_0, q_0, e_0)$ as Jordan algebras. Moreover, $T|_{M_0}$ (resp. $T|_{M_0\times M_0}$) is the linear (resp. bilinear) trace of (M_0, q_0, e_0), while its conjugation is given by $x_0 \mapsto \bar{x}_0 = T(x_0)e_0 - x_0 = e \times x_0$. Finally, the elementary idempotents of $J(M_0, q_0, e_0)$ in the sense of 29.13 are precisely the elementary idempotents of J belonging to $J_0(e)$.

Proof Prop. 37.2 (a) implies $q_0(e_0) = T(e) = 1$. Hence (M_0, q_0, e_0) is a pointed quadratic module over k. Write t_0 for its (bi-)linear trace and let $x_0, y_0 \in M_0$. From (29b.1), (29b.4), (33a.13) and Prop. 37.2 (b) we deduce $t_0(x_0) = S(e_0, x_0) = T(e_0)T(x_0) - T(e_0, x_0) = 2T(x_0) - T(1, x_0) = T(x_0)$, hence $t_0 = T|_{M_0}$ as linear traces, and $t_0(x_0, y_0) = t_0(x_0)t_0(y_0) - q_0(x_0, y_0) = T(x_0)T(y_0) - S(x_0, y_0) = T(x_0, y_0)$, hence $t_0 = T|_{M_0\times M_0}$ as bilinear traces. By (29b.3) and (37.2.3) this implies $\bar{x}_0 = T(x_0)e_0 - x_0 = e \times x_0$. Applying Prop. 37.2 (c), the U-operator of $J(M_0, q_0, e_0)$ may now be written as $U_{x_0}y_0 = q_0(x_0, \bar{y}_0)x_0 - q(x_0)\bar{y}_0 = t_0(x_0, y_0)x_0 - q(x_0)e \times x_0 = T(x_0, y_0)x_0 - x_0^\sharp \times y_0$, and we conclude $J_0(e) = J(M_0, q_0, e_0)$ as Jordan algebras. Finally, an element $c_0 \in J_0(e)$ is an elementary idempotent of $J(M_0, q_0, e_0)$ if and only if $T(c_0) = t_0(c_0) = 1$ and $q_0(c_0) = 0$, the latter condition by Prop. 37.2 (c) being equivalent to $c_0^\sharp = S(c_0)e = 0$. This proves the final assertion of the corollary. □

37.4 Proposition. *Elementary idempotents $e_1, e_2 \in J$ are orthogonal if and only if $e_1 \times e_2 = 1 - e_1 - e_2 =: e_3$. In this case, (e_1, e_2, e_3) is a complete orthogonal system of elementary idempotents in J, and with the corresponding Peirce decomposition $J = \sum(J_{ii} + J_{jl})$, the following statements hold.*

(a) $e_i \times e_j = e_l$.

(b) $J_{ii} = ke_i$.

(c) *The Peirce components of J relative to (e_1, e_2, e_3) are orthogonal with respect to the bilinear trace.*

(d) *The linear trace of J vanishes on $J_{23} + J_{31} + J_{12}$.*

(e) $x \circ y = x \times y$ *for all* $x \in J_{ij}$, $y \in J_{jl}$.

(f) $x^2 = -S(x)(e_j + e_l)$ *for all* $x \in J_{jl}$.

Proof The very first assertion follows from (37.2.3) and the following chain of equivalent conditions.

$$\begin{aligned} e_1, e_2 \text{ are orthogonal} &\iff e_2 \in J_0(e_1) \\ &\iff e_1 \times e_2 = T(e_2)(1 - e_1) - e_2 \\ &\iff e_1 \times e_2 = e_3. \end{aligned}$$

In this case, $T(e_3) = T(1) - T(e_1) - T(e_2) = 3 - 1 - 1 = 1$, and applying (33a.10) we obtain $e_3^\sharp = (e_1 \times e_2)^\sharp = T(e_1^\sharp, e_2)e_2 + T(e_1, e_2^\sharp)e_1 - e_1^\sharp \times e_2^\sharp = 0$. Hence e_3 is an elementary idempotent, making (e_1, e_2, e_3) a complete orthogonal system of the desired kind.

(a) is now clear by symmetry.

(b) This is just (32.15.2) and (37.2.1).

(c), (d) By (32.15.4) we have $J_{ij} \subseteq J_1(e_i) \cap J_0(e_l)$. Therefore $T(e_i, J_{ij}) = T(e_l, J_{ij}) = T(J_{ij}, J_{jl}) = \{0\}$, giving (c) and $T(J_{ij}) = T(\sum e_l, J_{ij}) = \{0\}$, hence (d).

(e) By (c), (d), $T(x) = T(y) = T(x, y) = 0$, and (33a.23) yields the assertion.

(f) We have $x \in J_0(e_i)$ by (32.15.2), and Cor. 37.3 combined with (d) implies $x^2 = T(x)x - S(x)(1 - e_i) = -S(x)(e_j + e_l)$. □

37.5 The concept of an elementary frame. Adapting the terminology of Loos [171, 10.12] to the present set-up, we define an *elementary frame* of J to be a complete orthogonal system of elementary idempotents in J. By Prop. 37.4, an elementary frame of J has length 3 unless $k = \{0\}$, in which case $J = \{0\}$ and the length can be arbitrary.

If (e_1, e_2, e_3) is an elementary frame of J, then we write

$$J = \sum (J_{ii} + J_{jl}) \tag{1}$$

for the corresponding Peirce decomposition. Combining Prop. 37.2 (b) with (32.15.2), (32.15.3), we conclude

$$J_{ii} = ke_i, \quad J_{jl} = \{x \in J \mid T(x) = 0, \ \ e_j \times x = e_l \times x = 0\}. \tag{2}$$

In Exc. 32.23, we have introduced the concept of (strong) connectedness for orthogonal systems of idempotents. In the present set-up, this concept allows a natural characterization by means of data belonging exclusively to the underlying cubic norm structure.

37.6 Proposition. *Let (e_1, e_2, e_3) be an elementary frame of J with the Peirce decomposition $J = \sum(ke_i + J_{jl})$. For elements $u_{jl} \in J_{jl}$, the following conditions are equivalent.*

(i) e_j *and* e_l *are connected (resp. strongly connected) by* u_{jl}.

(ii) $S(u_{jl}) \in k^\times$ *(resp.* $S(u_{jl}) = -1$*).*

Proof By Cor. 37.3, we have $J_2(e_j + e_l) = J_0(e_i) = J(M_0, S_0, f)$, where $M_0 = J_0(e_i)$ as k-modules, $S_0 = S|_{M_0}$ and $f = 1 - e_i = e_j + e_l$. Now e_j and e_l are connected by u_{jl} if and only if $u_{jl} \in J_2(e_j + e_l)^\times$, which by Exc. 31.33 happens if and only if $S(u_{jl}) = S_0(u_{jl}) \in k^\times$. On the other hand, $u_{jl}^2 = -S(u_{jl})(e_j + e_l)$ by Prop. 37.4 (f), so e_j and e_l are strongly connected by u_{jl} if and only if $S(u_{jl}) = -1$. □

37.7 Elementary identities in cubic Jordan matrix algebras. Let (C, Γ) be a pre-co-ordinate pair over k as defined in 36.3. One checks that the cubic Jordan matrix algebra $\mathrm{Her}_3(C, \Gamma)$ satisfies the identities

$$e_{ii}^\sharp = 0, \quad T(e_{ii}) = 1, \quad e_{ii} \times e_{jj} = e_{ll}, \tag{1}$$

$$e_{jj} \times u_i[jl] = e_{ll} \times u_i[jl] = 0, \quad e_{ii} \times u_i[jl] = -u_i[jl], \tag{2}$$

$$u_i[jl]^\sharp = -\gamma_j\gamma_l n_C(u_i) e_{ii}, \tag{3}$$

$$u_i[jl] \circ v_j[li] = u_i[jl] \times v_j[li] = \gamma_l \overline{u_i v_j}[ij], \tag{4}$$

$$U_{u_i[jl]} v_i[jl] = \gamma_j\gamma_l (u_i \bar{v}_i u_i)[jl], \tag{5}$$

$$U_{u_i[jl]} e_{jj} = \gamma_j\gamma_l n_C(u_i) e_{ll}, \tag{6}$$

$$U_{u_i[jl]} e_{ll} = \gamma_j\gamma_l n_C(u_i) e_{jj}, \tag{7}$$

$$\{u_i[jl] u_j[li] u_l[ij]\} = \gamma_1\gamma_2\gamma_3 t_C(u_1u_2u_3) e_{jj} \tag{8}$$

for all $u_i, v_i \in C$, $i = 1, 2, 3$.

We are now in a position to investigate more closely the role played by elementary frames in cubic Jordan matrix algebras.

37.8 Proposition. *Let* (C, Γ) *be a pre-co-ordinate pair over* k*. Then* (e_{11}, e_{22}, e_{33}) *is an elementary frame in* $J := \mathrm{Her}_3(C, \Gamma)$*, called its* diagonal frame*, whose Peirce components are given by*

$$J_{ii} = ke_{ii}, \quad J_{jl} = C[jl]. \tag{1}$$

Moreover, for $u_i \in C$*, the orthogonal idempotents* e_{jj} *and* e_{ll} *are connected by* $u_i[jl] \in J_{jl}$ *if and only if* $u_i \in C^\times$ *and* $\gamma_j, \gamma_l \in k^\times$.

Proof That the diagonal matrix units form an elementary frame of J follows immediately from (37.7.1) combined with Prop. 37.4. It remains to establish (1), the first relation being obvious by (37.5.2). As to the second, let

$$x = \sum (\xi_m e_{mm} + u_m[np]) \in J \qquad (\xi_m \in k,\ u_m \in C,\ m = 1, 2, 3).$$

Then (37.5.2), (36.4.8), (37.7.1), (37.7.2) imply

$$\begin{aligned} x \in J_{jl} &\iff T(x) = 0,\ e_{jj} \times x = e_{ll} \times x = 0 \\ &\iff \sum \xi_m = 0, \\ &\quad \xi_i e_{ll} + \xi_l e_{ii} - u_j[li] = 0 = \xi_j e_{ii} + \xi_i e_{jj} - u_l[ij] \\ &\iff \xi_1 = \xi_2 = \xi_3 = 0,\ u_j = u_l = 0 \\ &\iff x = u_i[jl] \\ &\iff x \in C[jl]. \end{aligned}$$

The final statement follows immediately from Prop. 37.4 (f) combined with Exc. 32.23 and (36.4.9), which implies $S(u_i[jl]) = -\gamma_j\gamma_l n_C(u_i)$. □

37.9 Corollary. *The diagonal frame of* $\mathrm{Her}_3(C,\Gamma)$ *is connected if and only if* $\Gamma \in \mathrm{GL}_3(k)$*, i.e.,* (C,Γ) *is a co-ordinate pair over* k*.* □

37.10 Co-ordinate systems. By a *co-ordinate system* of a cubic Jordan algebra J over k we mean a quintuple $\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31}) \in J^5$ such that (e_1, e_2, e_3) is an elementary frame of J, inducing the corresponding Peirce decomposition $J = \sum(ke_i + J_{jl})$, and for $i = 1, 2$, the orthogonal idempotents e_j, e_l are connected by $u_{jl} \in J_{jl}$. We refer to (e_1, e_2, e_3) as the elementary frame *associated with* $\mathfrak{S}$. A pair $(J, \mathfrak{S})$ consisting of a cubic Jordan algebra J over k and a co-ordinate system $\mathfrak{S}$ of J will be called a *co-ordinated cubic Jordan algebra*.

37.11 Example. Let (C,Γ) be a co-ordinate pair over k. Then Prop. 37.8 shows that

$$\mathfrak{D}(C,\Gamma) := (e_{11}, e_{22}, e_{33}, 1_C[23], 1_C[31]) \tag{1}$$

is a co-ordinate system of the cubic Jordan algebra $\mathrm{Her}_3(C,\Gamma)$, called its *diagonal co-ordinate system*. We write

$$\mathbf{Her}_3(C,\Gamma) := (\mathrm{Her}_3(C,\Gamma), \mathfrak{D}(C,\Gamma)) \tag{2}$$

for the corresponding co-ordinated cubic Jordan algebra.

In the remainder of this section, we will show that, conversely, every co-ordinated cubic Jordan algebra is isomorphic to a cubic Jordan matrix algebra, under an isomorphism matching the given co-ordinate system of the former with the diagonal one of the latter. This will be the content of the Jacobson co-ordinatization theorem 37.17 below.

In order to accomplish this result, we fix a cubic Jordan k-algebra J, with identity element 1, trace T, quadratic trace S, norm N, and begin with a series of preparations.

37.12 Lemma. *We have*

$$S(x \times y, z) = T(x)T(y)T(z) - T(x,y)T(z) - T(x \times y, z)$$

for all $x, y, z \in J$.

Proof Applying (33a.13) twice, we obtain

$$\begin{aligned} S(x \times y, z) &= T(x \times y)T(z) - T(x \times y, z) \\ &= T(x)T(y)T(z) - T(x,y)T(z) - T(x \times y, z), \end{aligned}$$

as claimed. □

37.13 Proposition. *Let* (e_1, e_2, e_3) *be an elementary frame of* J *and* $J = \sum(ke_i + J_{jl})$ *the corresponding Peirce decomposition of* J. *Then* $J_0 := \sum ke_i$ *is a regular cubic subalgebra of* J *canonically isomorphic to* $E^{(+)}$, *where* E *stands for the split cubic étale* k*-algebra. Moreover,*

$$J_{ij} \times J_{jl} \subseteq J_{li}, \tag{1}$$

and given

$$x = \sum(\xi_i e_i + u_{jl}), \quad y = \sum(\eta_i e_i + v_{jl}) \in J$$

with $\xi_i, \eta_i \in k$, $u_{jl}, v_{jl} \in J_{jl}$, $i = 1, 2, 3$, *the following relations hold.*

$$N(x) = \xi_1\xi_2\xi_3 + \sum \xi_i S(u_{jl}) + T(u_{23} \times u_{31}, u_{12}), \tag{2}$$

$$x^\sharp = \sum \Big((\xi_j\xi_l + S(u_{jl}))e_i + (-\xi_i u_{jl} + u_{li} \times u_{ij})\Big), \tag{3}$$

$$\begin{aligned} x \times y = \sum \Big((\xi_j\eta_l + \eta_j\xi_l - T(u_{jl}, v_{jl}))e_i \\ + (-\xi_i v_{jl} - \eta_i u_{jl} + u_{li} \times v_{ij} + v_{li} \times u_{ij})\Big), \end{aligned} \tag{4}$$

$$T(x,y) = \sum \xi_i\eta_i + \sum T(u_{jl}, v_{jl}), \tag{5}$$

$$T(x) = \sum \xi_i, \tag{6}$$

$$S(x) = \sum (\xi_j\xi_l + S(u_{jl})), \tag{7}$$

$$S(x,y) = \sum (\xi_j\eta_l + \eta_j\xi_l - T(u_{jl}, v_{jl})). \tag{8}$$

Proof Relation (1) follows from $J_{ij} \times J_{jl} = J_{ij} \circ J_{jl}$ (by Prop. 37.4 (e)) and the Peirce rules. For the remaining assertions, we proceed in three steps.

1°. Noting that $J_0 = \sum ke_i$ is a direct sum of ideals by Cor. 32.16 (b), our first aim will be to show that J_0 and $E^{(+)}$ are canonically isomorphic. Since $e_i^\sharp = 0$ by definition and $N(e_i) = 0$ by 37.1, combining equation (5) of Exc. 12.40

with Prop. 37.4 (a) yields $N(\sum \xi_i e_i) = \xi_1\xi_2\xi_3 T(e_1 \times e_2, e_3) = \xi_1\xi_2\xi_3 T(e_3, e_3)$, so 37.1 again yields

$$N(\sum \xi_i e_i) = \xi_1\xi_2\xi_3 \tag{9}$$

in all scalar extensions. Thus the map $\varphi\colon E^{(+)} \to J_0$ defined by

$$\varphi((\xi_1, \xi_2, \xi_3)) := \sum \xi_i e_i$$

for $\xi_1, \xi_2, \xi_3 \in k$ is an isomorphism of cubic Jordan algebras (Exc. 34.18 (b)). Hence (34.17.4), (34.17.5) yield

$$(\sum \xi_i e_i)^\sharp = \sum \xi_j\xi_l e_i, \tag{10}$$

$$T(\sum \xi_i e_i, \sum \eta_i e_i) = \sum \xi_i\eta_i. \tag{11}$$

2°. We now apply the formalism of 35.6, derive the relation

$$V := X_0^\perp = J_{23} + J_{31} + J_{12} \tag{12}$$

from Prop. 37.4 (c) and recall from Remark 35.3 that (X_0, V) is a complemented cubic norm substructure of J, so it makes sense to compute the quadratic maps Q, H of 35.6 in the special case at hand. Following (12), let

$$u = u_{23} + u_{31} + u_{12} \in V, \quad u_{jl} \in J_{jl}. \tag{13}$$

Since $J_{jl} \subseteq J_0(e_i)$ by (32.15.2), Prop. 37.2 (c) implies

$$\begin{aligned} u^\sharp &= (u_{23} + u_{31} + u_{12})^\sharp \\ &= u_{23}^\sharp + u_{31}^\sharp + u_{12}^\sharp + u_{23} \times u_{31} + u_{31} \times u_{12} + u_{12} \times u_{23} \\ &= S(u_{23})e_1 + S(u_{31})e_2 + S(u_{12})e_3 + u_{23} \times u_{31} + u_{31} \times u_{12} + u_{12} \times u_{23}. \end{aligned}$$

Combining this with (1) and (35.6.1), we deduce

$$Q(u) = -\sum S(u_{jl})e_i, \tag{14}$$

$$H(u) = \sum u_{li} \times u_{ij}. \tag{15}$$

We also wish to know how N acts on $V = X_0^\perp$. Using (35b.11) (for $x_0 = 1$), (15) and linearizing (14), we obtain

$$N(u)1 = Q(u, H(u)) = -\sum S(u_{jl}, u_{li} \times u_{ij})e_i,$$

where Lemma 37.12 and Prop. 37.4 (d) imply

$$S(u_{li} \times u_{ij}, u_{jl}) = -T(u_{li} \times u_{ij}, u_{jl}) = -T(u_{23} \times u_{31}, u_{12})$$

since the expression $T(x \times y, z)$ is totally symmetric in its arguments. Thus

$$N(u) = T(u_{23} \times u_{31}, u_{12}). \tag{16}$$

3°. It is now easy to complete the proof of the proposition. Combining (35.6.3), (35.6.2) with (9), (11), (16), we obtain

$$\begin{aligned} N(x) = N(\sum \xi_i e_i + u) &= N(\sum \xi_i e_i) - T(\sum \xi_i e_i, Q(u)) + N(u) \\ &= \xi_1\xi_2\xi_3 + \sum \xi_i S(u_{jl}) + T(u_{23} \times u_{31}, u_{12}), \end{aligned}$$

giving (4), and

$$x^\sharp = (\sum \xi_i e_i + u)^\sharp = \big((\sum \xi_i e_i)^\sharp - Q(u)\big) + \big(\sum \xi_i e_i \times u + H(u)\big).$$

But $u_{jl} \in J_0(e_i)$, while $u_{li}, u_{ij} \in J_1(e_i)$. Hence $e_i \times u = -u_{jl}$ by (37.2.2), (37.2.3), Prop. 37.4 (d), and (10), (14), (15) imply

$$x^\sharp = \sum (\xi_j\xi_l + S(u_{jl}))e_i + \sum (-\xi_i u_{jl} + u_{li} \times u_{ij}),$$

giving (3), which by Prop. 37.4 (d) and (33a.13) linearizes to (4). Applying Prop. 37.4 (c), we obtain (5), which immediately implies (6) and combines with (3) to yield (7). Linearizing (7), we obtain

$$S(x, y) = \sum (\xi_j\eta_l + \eta_j\xi_l + S(u_{jl}, v_{jl})).$$

Since $T(u_{jl}) = 0$ by (6), we deduce $S(u_{jl}, v_{jl}) = -T(u_{jl}, v_{jl})$ from (33a.13), and (8) follows. □

37.14 Lemma. *Under the assumptions of Prop. 37.13, the relations*

$$S(u_{jl}, v_{jl}) = -T(u_{jl}, v_{jl}), \tag{1}$$

$$u_{jl} \times (u_{jl} \times u_{li}) = -S(u_{jl})u_{li}, \tag{2}$$

$$(u_{li} \times u_{ij}) \times u_{ij} = -S(u_{ij})u_{li}, \tag{3}$$

$$u_{jl} \times (v_{jl} \times u_{li}) + v_{jl} \times (u_{jl} \times u_{li}) = T(u_{jl}, v_{jl})u_{li}, \tag{4}$$

$$(u_{li} \times u_{ij}) \times v_{ij} + (u_{li} \times v_{ij}) \times u_{ij} = T(u_{ij}, v_{ij})u_{li}, \tag{5}$$

$$S(u_{jl} \times u_{li}) = -S(u_{jl})S(u_{li}) \tag{6}$$

hold for all $u_{jl}, v_{jl} \in J_{jl}$, $u_{li} \in J_{li}$.

Proof (1) is an immediate consequence of (37.13.8). In order to establish (2), we first note $J_{li} \subseteq J_1(e_j + e_l)$, $J_{jl} \subseteq J_2(e_j + e_l)$. Hence Prop. 37.4 combined with (37.13.1) and Exc. 32.20 yields

$$u_{jl} \times (u_{jl} \times u_{li}) = u_{jl} \circ (u_{jl} \circ u_{li}) = u_{jl}^2 \circ u_{li} = -S(u_{jl})(e_j + e_l) \circ u_{li} = -S(u_{jl})u_{li},$$

hence (2). An analogous computation yields (3). Linearizing (2) (resp. (3)) and

combining with (1) gives (4) (resp. (5)). Finally, in order to establish (6), we apply (33a.10) to conclude

$$S(u_{jl} \times u_{li}) = T((u_{jl} \times u_{li})^\sharp) = T(T(u_{jl}^\sharp, u_{li})u_{li} + T(u_{jl}, u_{li}^\sharp)u_{jl} - u_{jl}^\sharp \times u_{li}^\sharp),$$

which by Prop. 37.13 reduces to

$$S(u_{jl} \times u_{li}) = -S(u_{jl})S(u_{li})T(e_i \times e_j) = -S(u_{jl})S(u_{li})T(e_l) = -S(u_{jl})S(u_{li}),$$

as claimed. □

37.15 Proposition. *Let $(J, \mathfrak{S})$ be a co-ordinated cubic Jordan algebra over k, with $\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31})$ the corresponding co-ordinate system, and let $J = \sum(ke_i + J_{jl})$ be the Peirce decomposition of J relative to the elementary frame belonging to $\mathfrak{S}$. Then $S(u_{jl}) \in k^\times$ for $i = 1, 2$, and with*

$$\omega := \omega_{J,\mathfrak{S}} := S(u_{23})^{-1}S(u_{31})^{-1} \in k^\times, \tag{1}$$

the k-module

$$C := C_{J,\mathfrak{S}} := J_{12} \tag{2}$$

becomes a multiplicative conic alternative k-algebra with multiplication, norm, unit element, trace, conjugation respectively given by

$$uv := \omega(u \times u_{23}) \times (u_{31} \times v), \tag{3}$$
$$n_C(u) = -\omega S(u), \tag{4}$$
$$n_C(u, v) = \omega T(u, v), \tag{5}$$
$$1_C = u_{12} := u_{23} \times u_{31}, \tag{6}$$
$$t_C(u) = \omega T(u_{12}, u), \tag{7}$$
$$\bar{u} = \omega T(u_{12}, u)u_{12} - u \tag{8}$$

for all $u, v \in C$. Moreover,

$$(C, \Gamma) = (C_{J,\mathfrak{S}}, \Gamma_{J,\mathfrak{S}}) =: \mathrm{Cop}(J, \mathfrak{S}) \tag{9}$$

with

$$\Gamma := \Gamma_{J,\mathfrak{S}} := \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3),\ \gamma_1 = -S(u_{31}),\ \gamma_2 = -S(u_{23}),\ \gamma_3 = 1. \tag{10}$$

is a co-ordinate pair over k, called the co-ordinate pair associated with $(J, \mathfrak{S})$.

Proof We have $S(u_{jl}) \in k^\times$ by Prop. 37.6; in particular, $\omega \in k^\times$ exists, and (3) by (37.13.1) defines a non-associative algebra structure on $C = J_{12}$. It remains to show that C is a multiplicative conic alternative algebra with norm,

bilinearized norm, unit element, trace, conjugation as indicated. Let $u, v \in C$. The element $u_{12} \in C$ by (37.14.1), (37.14.3) satisfies

$$\begin{aligned} u_{12}v &= \omega\big((u_{23} \times u_{31}) \times u_{23}\big) \times (u_{31} \times v) \\ &= -S(u_{23})\omega u_{31} \times (u_{31} \times v) = S(u_{23})S(u_{31})\omega v = v \end{aligned}$$

and

$$\begin{aligned} uu_{12} &= \omega(u \times u_{23}) \times \big(u_{31} \times (u_{23} \times u_{31})\big) \\ &= -S(u_{31})\omega(u \times u_{23}) \times u_{23} = S(u_{23})S(u_{31})\omega u = u. \end{aligned}$$

Thus C is unital with unit element $1_C = u_{12}$, and (6) holds. Defining the quadratic form $n_C : C \to k$ by (4), we apply (37.14.6) to derive the relation $n_C(1_C) = -\omega S(u_{23} \times u_{31}) = \omega S(u_{23})S(u_{31})$, and (1) yields

$$n_C(1_C) = 1. \tag{11}$$

Moreover, linearizing (4) and observing (33.2.10) gives (5) since the linear trace of J by (37.13.6) vanishes on the off-diagonal Peirce components. In order to distinguish the squaring in J from the one in C, we write $u^{\cdot 2}$ for the latter. Applying Lemma 37.14, (33a.7), (1), we then obtain

$$\begin{aligned} u^{\cdot 2} &= \omega(u \times u_{23}) \times (u_{31} \times u) \\ &= \omega T(u_{23}, u_{31} \times u)u - \omega\big(u \times (u_{31} \times u)\big) \times u_{23} \\ &= \omega T(u_{12}, u)u + \omega S(u)u_{31} \times u_{23} = \omega T(u_{12}, u)u - n_C(u)1_C, \end{aligned}$$

where (5) yields $n_C(1_C, u) = \omega T(u_{12}, u)$. Thus C is a conic k-algebra with norm, bilinearized norm, unit, trace given by (4)–(7), respectively. Relation (8) is now clear. Next we show alternativity, again by appealing to the relations of Lemma 37.14 and (7):

$$\begin{aligned} u(uv) &= \omega^2(u \times u_{23}) \times \Big(u_{31} \times \big((u \times u_{23}) \times (u_{31} \times v)\big)\Big) \\ &= \omega^2 T(u_{31}, u \times u_{23})(u \times u_{23}) \times (u_{31} \times v) - \\ &\quad \omega^2(u \times u_{23}) \times \Big((u \times u_{23}) \times \big(u_{31} \times (u_{31} \times v)\big)\Big) \\ &= t_C(u)uv - \omega^2 S(u \times u_{23})S(u_{31})v = t_C(u)uv + \omega^2 S(u_{23})S(u_{31})S(u)v \\ &= t_C(u)uv - n_C(u)v = \big(t_C(u)u - n_C(u)1_C\big)v = u^{\cdot 2}v \end{aligned}$$

and

$$\begin{aligned}(vu)u &= \omega^2\Big(\big((v\times u_{23})\times(u_{31}\times u)\big)\times u_{23}\Big)\times(u_{31}\times u)\\ &= \omega^2 T(u_{23}, u_{31}\times u)(v\times u_{23})\times(u_{31}\times u)-\\ &\quad\ \omega^2\Big(\big((v\times u_{23})\times(u_{31}\times u)\big)\times(u_{31}\times u)\Big)\times u_{23}\\ &= t_C(u)vu - \omega^2 S(u_{31}\times u)S(u_{23})v = t_C(u)vu + \omega^2 S(u_{31})S(u_{23})S(u)v\\ &= t_C(u)vu - n_C(u)v = v(t_C(u)u - n_C(u)1_C) = vu^{\cdot 2}.\end{aligned}$$

Finally, by (37.14.6), (3), (4), the norm of C permits composition:

$$\begin{aligned}n_C(uv) &= -\omega^3 S\big((u\times u_{23})\times(u_{31}\times v)\big)\\ &= \omega^3 S(u\times u_{23})S(u_{31}\times v) = \omega^2 S(u)S(v) = n_C(u)n_C(v).\end{aligned}$$

Summing up we have thus shown that C is a multiplicative conic alternative algebra over k. □

37.16 Example. Letting (C,Γ) with $\Gamma = \operatorname{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{GL}_3(k)$ be a co-ordinate pair over k, we consider the co-ordinated cubic Jordan algebra

$$(J,\mathfrak{S}) = \mathbf{Her}_3(C,\Gamma) = (\mathrm{Her}_3(C,\Gamma), \mathfrak{D}(C,\Gamma))$$

of (37.11.2). Combining Prop. 37.15 with (37.7.4) and (36.4.9), one checks that

$$\omega_{J,\mathfrak{S}} = (\gamma_1\gamma_2\gamma_3^2)^{-1} \tag{1}$$

and

$$\varphi\colon C \xrightarrow{\sim} C_{J,\mathfrak{S}}, \quad u \longmapsto \gamma_3 u[12] \tag{2}$$

is an isomorphism of conic algebras.

37.17 Jacobson Co-ordinatization Theorem. *Let $(J,\mathfrak{S})$ be a co-ordinated cubic Jordan algebra over k. With the notation of Prop. 37.15, the map*

$$\phi_{J,\mathfrak{S}}\colon \mathrm{Her}_3(C,\Gamma) \to J$$

defined by

$$\phi_{J,\mathfrak{S}}(x) := \sum(\xi_i e_i + v_{jl}), \tag{1}$$

for

$$x = \sum(\xi_i e_{ii} + v_i[jl]) \in \mathrm{Her}_3(C,\Gamma) \qquad (\xi_i \in k,\ v_i \in C,\ i = 1,2,3), \tag{2}$$

where

$$v_{23} := -S(u_{31})^{-1}u_{31}\times\bar{v}_1, \quad v_{31} := -S(u_{23})^{-1}u_{23}\times\bar{v}_2, \quad v_{12} := v_3, \tag{3}$$

is an isomorphism of cubic Jordan algebras matching the diagonal co-ordinate system of $\mathrm{Her}_3(C,\Gamma)$ *with the co-ordinate system* $\mathfrak{S}$ *of* J.

Proof Note by (37.15.2) that $C = J_{12}$ as k-modules. Since the conjugation of *any* conic algebra leaves its norm invariant, (37.15.4) shows

$$S(\bar{v}) = S(v) \qquad (v \in C = J_{12}). \tag{4}$$

Putting $\phi := \phi_{J,\mathfrak{S}}$ and defining $\psi\colon J \to \mathrm{Her}_3(C,\Gamma)$ by

$$\psi\Big(\sum(\xi_i e_i + v_{jl})\Big) := \sum(\xi_i e_{ii} + v_i[jl])$$

for $\xi_i \in k$, $v_{jl} \in J_{jl}$, $i = 1,2,3$, where

$$v_1 := \overline{u_{31} \times v_{23}}, \quad v_2 := \overline{u_{23} \times v_{31}}, \quad v_3 := v_{12},$$

(37.14.2), (37.14.3) imply $\phi \circ \psi = \mathbf{1}_J$ and $\psi \circ \phi := \mathbf{1}_{\mathrm{Her}_3(C,\Gamma)}$. Thus ϕ is a bijective linear map. It remains to show that ϕ is a homomorphism of cubic Jordan algebras. Since ϕ obviously preserves unit elements, the assertion will follow from Exc. 34.18 (a) once we have shown that ϕ preserves adjoints. In order to do so, we denote by $x^{\sharp'}$ the adjoint of $x \in \mathrm{Her}_3(C,\Gamma)$ as given by (2) and deduce from (36.4.4) that

$$x^{\sharp'} = \sum(\eta_i e_{ii} + w_i[jl]), \tag{5}$$

where

$$\eta_i = \xi_j\xi_l - \gamma_j\gamma_l n_C(v_i), \tag{6}$$

$$w_i = -\xi_i v_i + \gamma_i \overline{v_j v_l}. \tag{7}$$

Hence (2), (3) imply

$$\phi(x^{\sharp'}) = \sum(\eta_i e_i + w_{jl}), \tag{8}$$

where

$$w_{23} := -S(u_{31})^{-1}u_{31} \times \bar{w}_1, \quad w_{31} := -S(u_{23})^{-1}u_{23} \times \bar{w}_2, \quad w_{12} := w_3. \tag{9}$$

Before we can proceed, we require the identity

$$S(v_{jl}) = -\gamma_j\gamma_l n_C(v_i), \tag{10}$$

which follows by combining (3), (4) with (37.14.6), (37.15.1), (37.15.4) and (37.15.10), and with the computations

$$\begin{aligned} S(v_{23}) &= S(u_{31})^{-2}S(u_{31} \times \bar{v}_1) = -S(u_{31})^{-1}S(v_1) \\ &= -S(u_{23})\omega S(v_1) = -\gamma_2\gamma_3 n_C(v_1), \end{aligned}$$

$$S(v_{31}) = S(u_{23})^{-2}S(u_{23} \times \bar{v}_2) = -S(u_{23})^{-1}S(v_2)$$
$$= -S(u_{31})\omega S(v_2) = -\gamma_3\gamma_1 n_C(v_2),$$

and

$$S(v_{12}) = S(v_3) = -\omega^{-1}n_C(v_3) = -\gamma_1\gamma_2 n_C(v_3).$$

Applying (10) and (6), we now conclude

$$\eta_i = \xi_j\xi_l + S(v_{jl}). \tag{11}$$

On the other hand, combining (9), (7), (3), (37.15.10) gives

$$w_{23} = -S(u_{31})^{-1}u_{31} \times \bar{w}_1 = S(u_{31})^{-1}\xi_1 u_{31} \times \bar{v}_1 - S(u_{31})^{-1}\gamma_1 u_{31} \times (v_2v_3)$$
$$= -\xi_1 v_{23} + u_{31} \times (v_2v_3),$$

where Lemma 37.14 and Prop. 37.15 imply

$$\begin{aligned} u_{31} \times (v_2v_3) &= \omega u_{31} \times ((v_2 \times u_{23}) \times (u_{31} \times v_3)) \\ &= \omega T(u_{31}, v_2 \times u_{23})u_{31} \times v_3 - \omega(v_2 \times u_{23}) \times (u_{31} \times (u_{31} \times v_3)) \\ &= t_C(v_2)u_{31} \times v_3 + S(u_{23})^{-1}(v_2 \times u_{23}) \times v_3 \\ &= -S(u_{23})^{-1}(t_C(v_2)(u_{23} \times u_{31}) \times u_{23} - v_2 \times u_{23}) \times v_3 \\ &= -S(u_{23})^{-1}\Big((t_C(v_2)1_C - v_2) \times u_{23}\Big) \times v_3 \\ &= -S(u_{23})^{-1}(u_{23} \times \bar{v}_2) \times v_3 = v_{31} \times v_{12}. \end{aligned}$$

Summing up,

$$w_{23} = -\xi_1 v_{23} + v_{31} \times v_{12}.$$

Similarly,

$$w_{31} = -S(u_{23})^{-1}u_{23} \times \bar{w}_2 = \xi_2 S(u_{23})^{-1}u_{23} \times \bar{v}_2 - S(u_{23})^{-1}\gamma_2 u_{23} \times (v_3v_1)$$
$$= -\xi_2 v_{31} + u_{23} \times (v_3v_1),$$

where

$$\begin{aligned} u_{23} \times (v_3v_1) &= \omega u_{23} \times ((v_3 \times u_{23}) \times (u_{31} \times v_1)) \\ &= \omega T(u_{23}, u_{31} \times v_1)v_3 \times u_{23} - \omega(u_{31} \times v_1) \times ((v_3 \times u_{23}) \times u_{23}) \\ &= t_C(v_1)v_3 \times u_{23} + S(u_{31})^{-1}(u_{31} \times v_1) \times v_3 \\ &= -S(u_{31})^{-1}(t_C(v_1)(u_{23} \times u_{31}) \times u_{31} - u_{31} \times v_1) \times v_3 \\ &= -S(u_{31})^{-1}\Big((t_C(v_1)1_C - v_1) \times u_{31}\Big) \times v_3 \\ &= -S(u_{31})^{-1}(\bar{v}_1 \times u_{31}) \times v_3 = v_{23} \times v_{12}. \end{aligned}$$

Thus

$$w_{31} = -\xi_2 v_{31} + v_{12} \times v_{23}.$$

Since

$$\begin{aligned} w_{12} = w_3 &= -\xi_3 v_3 + \gamma_3 \overline{v_1 v_2} = -\xi_3 v_{12} + \bar{v}_2 \bar{v}_1 \\ &= -\xi_3 v_{12} + \omega(\bar{v}_2 \times u_{23}) \times (u_{31} \times \bar{v}_1) = -\xi_3 v_{12} + v_{23} \times v_{31}, \end{aligned}$$

our computations can be unified to

$$w_{jl} = -\xi_i v_{jl} + v_{li} \times v_{ij}. \tag{12}$$

Inserting (11) and (12) into (8), we may apply (37.13.3) and (1) to obtain

$$\begin{aligned} \phi(x^{\sharp'}) &= \sum (\xi_j \xi_l + S(v_{jl}))e_i + \sum (-\xi_i v_{jl} + v_{li} \times v_{ij}) \\ &= (\sum \xi_i e_i + \sum v_{jl})^{\sharp} = \phi(x)^{\sharp}. \end{aligned}$$

Hence ϕ preserves adjoints and thus is an isomorphism of cubic Jordan algebras.

It remains to show that ϕ matches the respective co-ordinate systems. To this end, we have to prove $\phi(1_C[jl]) = u_{jl}$ for $i = 1, 2$, which follows from (1), (3), (37.14.2), (37.15.6) and

$$\begin{aligned} \phi(1_C[23]) &= -S(u_{31})^{-1} u_{31} \times 1_C = -S(u_{31})^{-1} u_{31} \times (u_{23} \times u_{31}) = u_{23}, \\ \phi(1_C([31]) &= -S(u_{23})^{-1} u_{23} \times 1_C = -S(u_{23})^{-1} u_{23} \times (u_{23} \times u_{31}) = u_{31}, \end{aligned}$$

completing the proof of the entire theorem. □

37.18 Remark. Versions of the Jacobson co-ordinatization theorem which in many ways are much more general than the one presented here may be found in the literature, see, e.g., Jacobson [136, 137, 140] and McCrimmon [181] for details. Given any integer $m \geq 3$, the most important difference is that instead of co-ordinate pairs one has to consider quadruples (D, τ, D_0, Δ) consisting of

- a unital alternative k-algebra D,
- an involution $\tau\colon D \to D$,
- a unital subalgebra D_0 of $H(D, \tau)$ contained in the nucleus of D and being *D-ample* in the sense that $uD_0\tau(u) \subseteq D_0$ for all $u \in D$,
- and an invertible diagonal matrix $\Delta \in \mathrm{Mat}_m(D_0)$.

With considerable effort, it can then be shown that the k-module

$$\mathrm{Her}_m(D, \tau, D_0, \Delta)$$

of all Δ-twisted m-by-m hermitian matrices with entries in D and diagonal ones

in D_0, carries the structure of a Jordan algebra over k provided $m = 3$ or D is associative. Conversely, given a Jordan algebra J over k *whose extreme radical is zero* and a connected orthogonal system $\Omega = (e_1, \dots, e_m)$ of idempotents in J, the Jacobson co-ordinatization theorem says that there exist a quadruple (D, τ, D_0, Δ) as above and an isomorphism from J onto $\mathrm{Her}_m(D, \tau, D_0, \Delta)$ matching the orthogonal system Ω of the former with the diagonal one of the latter.

Here the condition on the extreme radical, being automatic for the algebras $\mathrm{Her}_m(D, \tau, D_0, \Delta)$, cannot be avoided. One may therefore wonder why it is absent from our version of the Jacobson co-ordinatization theorem. The answer rests on our formal definition of cubic Jordan matrix algebras in 36.4, 36.6 which, for a co-ordinate pair (C, Γ), allows a concrete base change invariant interpretation of $\mathrm{Her}_3(C, \Gamma)$ in terms of Γ-twisted hermitian matrices only if $1_C \in C$ is unimodular. Indeed, dropping this hypothesis, the extreme radical of $\mathrm{Her}_3(C, \Gamma)$ may very well be different from zero, while otherwise it is not (Exc. 37.31).

Exercises

37.19. *Idempotents in cubic Jordan algebras.* Let J be a cubic Jordan algebra over k. An idempotent $e \in J$ is said to be *co-elementary* if the complementary idempotent $1 - e$ is elementary. Now let e be any idempotent in J. Prove that there exists a complete orthogonal system $(\varepsilon^{(i)})_{0 \le i \le 3}$ of idempotents in k, giving rise to decompositions

$$k = k^{(0)} \times k^{(1)} \times k^{(2)} \times k^{(3)}, \quad J = J^{(0)} \times J^{(1)} \times J^{(2)} \times J^{(3)}$$

as direct products of ideals, where $k^{(i)} = \varepsilon^{(i)} k$, $J^{(i)} = \varepsilon^{(i)} J = J_{k^{(i)}}$ as cubic Jordan algebras over $k^{(i)}$ for $0 \le i \le 3$, such that

$$e = (0, e^{(1)}, e^{(2)}, 1_{J^{(3)}}),$$

where $e^{(1)}$ is an elementary idempotent of $J^{(1)}$ and $e^{(2)}$ is a co-elementary idempotent of $J^{(2)}$. Show further that the $\varepsilon^{(i)}$ are unique and given by

$$\varepsilon^{(0)} = N(1 - e) = 1 - T(e) + S(e) - N(e), \tag{1}$$

$$\varepsilon^{(1)} = T(e) - 2S(e) + 3N(e), \tag{2}$$

$$\varepsilon^{(2)} = S(e) - 3N(e), \tag{3}$$

$$\varepsilon^{(3)} = N(e). \tag{4}$$

37.20. *Ferrar's lemma* ([74, Lemma 1.10]). Let u_1, u_2, u_3 be elements of a cubic Jordan algebra J over k such $u_i^\sharp = 0$ for $i = 1, 2, 3$. Prove that $q := \sum u_i$ is invertible in J if and only if $T(u_1 \times u_2, u_3)$ is invertible in k, and that, in this case, (u_1, u_2, u_3) is an elementary frame in the isotope $J^{(p)}$, $p := q^{-1}$. Conclude that three elementary idempotents in J adding up to 1 form an elementary frame of J.

37.21. *Cubic nil ideals and the lifting of elementary idempotents.* Let J be a cubic

Jordan algebra over k. A cubic ideal $(\mathfrak{a}, I)$ in J in the sense of Exc. 34.21 is said to be *nil* if the ideals $\mathfrak{a} \subseteq k$ and $I \subseteq J$ are both nil.

(a) Show that $(\mathrm{Nil}(k), \mathrm{Nil}(J))$ is a cubic nil ideal in J.
(b) Assume that $(\mathfrak{a}, I)$ is a separated cubic nil ideal in J, write $\sigma\colon K \to k_0 := k/\mathfrak{a}$, $\pi\colon J \to J_0 := J/I$ for the canonical projections , view J_0 as a cubic Jordan algebra over k_0 via Exc. 34.21 and let $e_0 \in J_0$ be an elementary idempotent. Prove that every idempotent in $\pi^{-1}(e_0)$ (whose existence is guaranteed by Exc. 28.22 (c) and Prop. 29.16) is elementary.

37.22. Let (C, Γ) and (C, Γ') with

$$\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3), \quad \Gamma' = \mathrm{diag}(\gamma'_1, \gamma'_2, \gamma'_3) \in \mathrm{Diag}_3(k)^\times$$

be two co-ordinate pairs over k.

(a) View $\mathrm{Diag}_3(k)$ via 34.17 as the split cubic étale k-algebra and consider the following conditions, for any $\Delta = \mathrm{diag}(\delta_1, \delta_2, \delta_3) \in \mathrm{Diag}_3(k)^\times$.

(i) $\gamma'_j\gamma'_l = \delta_i^2\gamma_j\gamma_l$ for $i = 1, 2, 3$ and $\gamma'_1\gamma'_2\gamma'_3 = \delta_1\delta_2\delta_3\gamma_1\gamma_2\gamma_3$, i.e., $\Gamma'^\sharp = \Delta^2\Gamma^\sharp$ and $N(\Gamma') = N(\Delta)N(\Gamma)$.
(ii) $\gamma'_i = \delta_j\delta_l\delta_i^{-1}\gamma_i$ for $i = 1, 2, 3$, i.e., $\Gamma' = \Delta^\sharp\Delta^{-1}\Gamma$.
(iii) The map

$$\varphi_{C,\Delta}\colon \mathrm{Her}_3(C, \Gamma) \xrightarrow{\sim} \mathrm{Her}_3(C, \Gamma')$$

defined by

$$\varphi_{C,\Delta}\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) = \sum(\xi_i e_{ii} + (\delta_i^{-1}u_i)[jl]) \tag{1}$$

for $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$ is an isomorphism of cubic Jordan algebras.

Show that the implications

$$\text{(i)} \iff \text{(ii)} \implies \text{(iii)}$$

hold, and that all three conditions are equivalent if $1_C \in C$ is unimodular.

(b) Call two cubic matrix Jordan algebras *diagonally isomorphic* if there exists an isomorphism from one to the other that is *diagonal* in the sense that it matches the respective diagonal frames. Then conclude from (a) that the diagonal isomorphism class of $\mathrm{Her}_3(C, \Gamma)$ does not change if

(i) Γ is multiplied by an invertible scalar,
(ii) each diagonal entry of Γ is multiplied by an invertible square,
(iii) Γ is replaced by an appropriate diagonal matrix in $\mathrm{Mat}_3(k)$ of determinant 1.

37.23. *Diagonal isotopes of cubic Jordan matrix algebras.* Let (C, Γ) be a co-ordinate pair over k. Prove that

$$p := \sum \gamma_i e_{ii} \in \mathrm{Her}_3(C, \Gamma)$$

is invertible and that the map

$$\varphi\colon \mathrm{Her}_3(C, \Gamma)^{(p)} \xrightarrow{\sim} \mathrm{Her}_3(C)$$

defined by

$$\varphi\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum((\gamma_i\xi_i)e_{ii} + (\gamma_j\gamma_l u_i)[jl]) \tag{1}$$

for $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$ is an isomorphism of cubic Jordan algebras.

37.24. *Isotopes of pre-co-ordinate pairs* (McCrimmon [185, Thm. 3]). Let (C, Γ) be a pre-co-ordinate pair over k and $p, q \in C^\times$. Put

$$\Gamma^{(p,q)} := \operatorname{diag}(\gamma_1^{(p,q)}, \gamma_2^{(p,q)}, \gamma_3^{(p,q)}) := \operatorname{diag}\left(n_C(q)\gamma_1, n_C(p)\gamma_2, n_C(pq)^{-1}\gamma_3\right),$$

so that

$$(C, \Gamma)^{(p,q)} := (C^{(p,q)}, \Gamma^{(p,q)})$$

is a pre-co-ordinate pair over k, and show that the map

$$\varphi\colon\ \operatorname{Her}_3(C^{(p,q)}, \Gamma^{(p,q)}) \xrightarrow{\sim} \operatorname{Her}_3(C, \Gamma)$$

defined by

$$\varphi\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum(\xi_i e_{ii} + u_i'[jl]) \tag{1}$$

for $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$, where

$$u_1' := u_1 p, \quad u_2' := q u_2, \quad u_3' := (pq) u_3 (pq), \tag{2}$$

is a diagonal isomorphism of cubic Jordan algebras. Conclude that the cubic Jordan matrix algebras

$$\operatorname{Her}_3(C, \Gamma) \text{ and } \operatorname{Her}_3(C^{(p,q)}, \Gamma'), \quad \Gamma' = \operatorname{diag}\left(n_C(p)\gamma_1, n_C(q)\gamma_2, \gamma_3\right) \tag{3}$$

are isomorphic.

37.25. Let (C, Γ) be a co-ordinate pair over k, Show that the cubic Jordan matrix algebra $J = \operatorname{Her}_3(C, \Gamma)$ over k is outer central in the sense of Exc. 28.24.

37.26. *Ideals of cubic Jordan matrix algebras.* Let (C, Γ) be a co-ordinate pair over k and suppose $1_C \in C$ is unimodular, so that we obtain a natural identification $k \subseteq C$ as a unital subalgebra which is stable under base change. Prove:

(a) The outer ideals of the Jordan algebra $J := \operatorname{Her}_3(C, \Gamma)$ are precisely of the form

$$H_3(I_0, I, \Gamma) := \sum(I_0 e_{ii} + I[jl]) = \{\sum(\xi_i e_{ii} + u_i[jl]) \mid \xi_i \in I_0,\ \ u_i \in I,\ \ 1 \le i \le 3\}, \tag{1}$$

where I is an ideal in (C, ι_C) (viewed as an algebra with involution) and I_0 is an ideal in k, contained in $I \cap k$ and *weakly I-ample* in the sense that it contains the trace of arbitrary elements in I:

$$t_C(I) \subseteq I_0 \subseteq I \cap k. \tag{2}$$

(b) The ideals of J are precisely of the form (1), where I as in (a) is an ideal in (C, ι_C) and I_0 is an ideal in k, contained in $I \cap k$ and *I-ample* in the sense that it contains norm and trace of arbitrary elements in I:

$$k n_C(I) + t_C(I) \subseteq I_0 \subseteq I \cap k. \tag{3}$$

(c) For I_0, I as in (a), we have $2(I \cap k) \subseteq I_0$, hence $I_0 = I \cap k$ if $2 \in k^\times$.

(d) If C is a regular composition algebra, then the outer ideals of J are ideals and have the form $\mathfrak{a}J$ with $\mathfrak{a}$ varying over the ideals of k. Conclude that a homomorphism $\phi\colon J \to A$ of para-quadratic algebras is injective provided the base point of A is unimodular.

(e) If $k = F$ is a field and C is a pre-composition algebra over F, then the outer ideals of $J = \mathrm{Her}_3(C, \Gamma)$ are precisely of the form $\{0\}$, $\mathrm{Rad}(T)$ (the radical of the bilinear trace), and J. In particular, J is a simple Jordan algebra. Moreover, J is outer simple if and only if C is a regular composition algebra over F.

37.27. *Absolute zero divisors in cubic Jordan algebras.* Let J be a cubic Jordan algebra over k.

(a) Show that if $x \in J$ is an absolute zero divisor, then so is $x^\sharp$.
(b) Assume that k is reduced and consider the following conditions on $x \in J$.
  (i) x is an absolute zero divisor.
  (ii) $x^\sharp = 0$ and $T(x, y) = 0$ for all $y \in J$.
  (iii) $N(x) = 0$ and $T(x, y) = 0$ for all $y \in J$.

  Then prove that the implications

$$\text{(i)} \iff \text{(ii)} \implies \text{(iii)}$$

  hold.
(c) Prove that every absolute zero divisor of J is contained in the nil radical of J.
(d) (Weiss) Show that, contrary to what has been claimed in Petersson-Racine [226, p. 214], conditions (i), (ii), (iii) of part (b) are *not* equivalent, even if $k = F$ is a field and J is a simple Jordan algebra.
(e) Show that the nil radical of J is zero if and only if k is reduced and J has no absolute zero divisors.

37.28 Remark. Part (c) of this exercise holds, more generally, for arbitrary Jordan algebras [140, Prop. 4.6.2].

37.29. *The nil radical of Peirce components.* Let J be a cubic Jordan algebra over k. Prove

$$\mathrm{Nil}(J_i(e)) = J_i(e) \cap \mathrm{Nil}(J) \qquad (i = 0, 2)$$

for all idempotents $e \in J$. (*Hint*: Exc. 37.19.)

37.30. *Reducing cubic Jordan matrix algebras modulo their nil radical.* Let (C, Γ) be a co-ordinate pair over k and suppose $1_C \in C$ is unimodular. Prove

$$kn_C(\mathrm{Nil}(C)) + t_C(\mathrm{Nil}(C)) \subseteq \mathrm{Nil}(k) = \mathrm{Nil}(C) \cap k, \tag{1}$$

$$\mathrm{Nil}(\mathrm{Her}(C, \Gamma)) = H_3(\mathrm{Nil}(k), \mathrm{Nil}(C), \Gamma), \tag{2}$$

using the notation and conventions of Exc. 37.26. Writing $\sigma\colon k \to k_0 := k/\mathrm{Nil}(k)$, $\pi\colon C \to C_0 := C/\mathrm{Nil}(C)$ for the canonical projections and $\Gamma_0 \in \mathrm{GL}_3(k_0)$ for the image of Γ under σ, show further that (C_0, Γ_0) is a co-ordinate pair over k_0, and there is a canonical identification

$$\mathrm{Her}_3(C, \Gamma)/\mathrm{Nil}(\mathrm{Her}_3(C, \Gamma)) = \mathrm{Her}_3(C_0, \Gamma_0)$$

as cubic Jordan algebras over k_0 in the sense of Exercises 16.24 and 34.21 such that

$$\sum(\alpha_i e_{ii} + u_i[jl]) \bmod \mathrm{Nil}(\mathrm{Her}_3(C, \Gamma)) = \sum(\sigma(\alpha_i)e_{ii} + \pi(u_i)[jl])$$

for all $\alpha_i \in k$, $u_i \in C$, $i = 1, 2, 3$.

37.31. *The extreme radical of co-ordinated cubic Jordan algebras.* Assume we are given a co-ordinate system $\mathfrak{E} = (e_1, e_2, e_3, u_{23}, u_{31})$ of a cubic Jordan algebra J over k and write $J = \sum(ke_i + J_{jl})$ for the Peirce decomposition of J relative to the elementary frame (e_1, e_2, e_3). Prove without recourse to the Jacobson co-ordinatization theorem that the extreme radical of J may be described as

$$\begin{aligned} \mathrm{Rex}(J) &= \{ \sum \xi_i e_i \mid \xi_i \in k, \ \ \xi_i J_{ij} = \{0\} \ \text{ for } \ i = 1,2,3\} \\ &\subseteq \{ \sum \xi_i e_i \mid \xi_i^2 = 2\xi_i = 0 \ \text{ for } \ i = 1,2,3\}. \end{aligned} \tag{1}$$

Conclude for a co-ordinate pair (C, Γ) over k that the extreme radical of $\mathrm{Her}_3(C, \Gamma)$ is zero if $1_C \in C$ is unimodular but not in general.

37.32. *A categorical set-up for the Jacobson co-ordinatization theorem.* (a) Let (C, Γ) and (C', Γ') be co-ordinate pairs over k. We define a *homomorphism* from (C, Γ) to (C', Γ') as a pair (η, Δ) consisting of

(i) a homomorphism $\eta\colon C \to C'$ of conic k-algebras,
(ii) a matrix $\Delta \in \mathrm{Diag}_3(k)^\times$ such that $\Gamma' = \Delta^\sharp \Delta^{-1} \Gamma$.

In this way we obtain the category of co-ordinate pairs over k, denoted by k-**copa**.

(b) Let $(J, \mathfrak{E})$ and $(J', \mathfrak{E}')$ be co-ordinated cubic Jordan algebras over k and write

$$\mathfrak{E} = (e_1, e_2, e_3, u_{23}, u_{31}) \in J^5, \quad \mathfrak{E}' = (e_1', e_2', e_3', u_{23}', u_{31}') \in J'^5.$$

We define a *homomorphism* from $(J, \mathfrak{E})$ to $(J', \mathfrak{E}')$ as a triple $(\varphi; \delta_1, \delta_2)$ consisting of

(iii) a homomorphism $\varphi\colon J \to J'$ of cubic Jordan algebras satisfying $\varphi(e_i) = e_i'$ for $i = 1, 2, 3$,
(iv) scalars $\delta_1, \delta_2 \in k^\times$ such that $\varphi(u_{jl}) = \delta_i^{-1} u_{jl}'$ for $i = 1, 2$.

In this way we obtain the category of co-ordinated cubic Jordan algebras over k, denoted by k-**cocujo**.

(c) Let $(\eta, \Delta)\colon (C, \Gamma) \to (C', \Gamma')$ with $\Delta = \mathrm{diag}(\delta_1, \delta_2, \delta_3) \in \mathrm{Diag}_3(k)^\times$ be a homomorphism of co-ordinate pairs over k. Define

$$\mathrm{Her}_3(\eta, \Delta)\colon \ \mathrm{Her}_3(C, \Gamma) \longrightarrow \mathrm{Her}_3(C', \Gamma')$$

by

$$\mathrm{Her}_3(\eta, \Delta)\Big(\sum (\xi_i e_{ii} + u_i[jl]) \Big) := \sum \Big(\xi_i e_{ii} + (\delta_i^{-1} \eta(u_i))[jl] \Big) \tag{1}$$

for $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$ and show in the notation of 37.11 that

$$\mathbf{Her}_3(\eta, \Delta) := (\mathrm{Her}_3(\eta, \Delta); \delta_1, \delta_2)\colon \mathbf{Her}_3(C, \Gamma) \longrightarrow \mathbf{Her}_3(C', \Gamma')$$

is a homomorphism of co-ordinated cubic Jordan algebras over k, giving rise to a functor

$$\mathbf{Her}_3\colon k\text{-}\mathbf{copa} \longrightarrow k\text{-}\mathbf{cocujo}.$$

(d) Let $(\varphi; \delta_1, \delta_2)\colon (J, \mathfrak{E}) \to (J', \mathfrak{E}')$ be a homomorphism of co-ordinated cubic Jordan algebras over k. Write $J = \sum(ke_i + J_{jl})$ for the Peirce decomposition of J relative to the elementary frame belonging to $\mathfrak{E}$, ditto for J', and φ_{12} for the linear map $J_{12} \to J'_{12}$ induced by φ via restriction. Then prove that

$$\mathrm{Cop}(\varphi; \delta_1, \delta_2)\colon \ \mathrm{Cop}(J, \mathfrak{E}) \longrightarrow \mathrm{Cop}(J', \mathfrak{E}'),$$

where

$$\mathrm{Cop}(\varphi;\delta_1,\delta_2) := (\delta_1\delta_2\varphi_{12},\Delta), \quad \Delta = \mathrm{diag}(\delta_1,\delta_2,\delta_3), \quad \delta_3 := \delta_1\delta_2, \tag{2}$$

is a homomorphism of co-ordinate pairs over k, giving rise to a functor

$$\mathrm{Cop}\colon k\text{-}\mathbf{cocujo} \longrightarrow k\text{-}\mathbf{copa}.$$

(e) Let (C,Γ) be a co-ordinate pair over k and put

$$(C',\Gamma') := \mathrm{Cop}(\mathbf{Her}_3(C,\Gamma)). \tag{3}$$

Show $C' = C[12]$ as k-modules and that

$$\Psi_{C,\Gamma} := (\psi_{C,\Gamma},\Lambda_{C,\Gamma})\colon (C,\Gamma) \xrightarrow{\sim} (C',\Gamma'),$$

where

$$\psi_{C,\Gamma}\colon C \longrightarrow C', \quad u \longmapsto \gamma_3 u[12], \tag{4}$$

$$\Lambda_{C,\Gamma} := \mathrm{diag}(\lambda_1,\lambda_2,\lambda_3), \quad \lambda_1 = \lambda_2 = 1, \quad \lambda_3 = \gamma_3, \tag{5}$$

is an isomorphism of co-ordinate pairs over k.

(f) Let $(J,\mathfrak{S})$ be a co-ordinated cubic Jordan algebra over k and put

$$(J',\mathfrak{S}') := \mathbf{Her}_3(\mathrm{Cop}(J,\mathfrak{S})). \tag{6}$$

Show with the terminology of Thm. 37.17 that

$$\Phi_{J,\mathfrak{S}} := (\phi_{J,\mathfrak{S}};1,1)\colon (J',\mathfrak{S}') \xrightarrow{\sim} (J,\mathfrak{S}) \tag{7}$$

is an isomorphism of co-ordinated cubic Jordan algebras.

(g) Conclude that the functors

$$k\text{-}\mathbf{copa} \underset{\mathrm{Cop}}{\overset{\mathbf{Her}_3}{\rightleftarrows}} k\text{-}\mathbf{cocujo}$$

give an equivalence of categories.

38 Jordan algebras of degree three

We have seen in 34.15 that the forgetful functor from cubic Jordan algebras to arbitrary ones (34.1), though faithful, is not a full embedding. In the present section, this difficulty will be overcome by passing to a full subcategory of cubic Jordan algebras whose objects are called Jordan algebras of degree 3. Indeed, one of our main results (Thm. 38.13) says that, under suitable restrictions, the cubic norm structure underlying a Jordan algebra of degree three is unique. In order to prove this, we rely on the method of faithfully flat descent combined with an explicit description (Thm. 38.11) of cubic Jordan algebras with elementary idempotents in terms of pointed quadratic modules and what we call their admissible Peirce-one extensions.

The results of this section could have been obtained in more elegant a manner, and in greater generality to boot, by appealing to the theory of generically algebraic Jordan algebras over commutative rings [174], see 38.15 below for more on this connection. Instead, we have preferred the ad hoc approach adopted here because, within the framework of the present volume, it is essentially self-contained.

Before introducing the main concept of the present section, we remind the reader that a cubic Jordan algebra is a Jordan algebra J together with a (quite often notationally suppressed) cubic form $N_J\colon J \to k$ satisfying the conditions of 34.1. If we ignore this cubic form, equivalently, if we pass from $J \in k$-**cujo** to its image in k-**jord** under the forgetful functor k-**cujo** $\to$ k-**jord**, we say that J is viewed as an *abstract* Jordan algebra.

38.1 The concept of a Jordan algebra of degree three.

(a) Let J be a unital para-quadratic algebra over k in the sense of 28.2. We define a family of set maps

$$\Xi_R^J\colon J_R \longrightarrow \bigwedge\nolimits^3(J_R) = \big(\bigwedge\nolimits^3(J)\big)_R,$$

one for each $R \in k$-**alg**, by setting

$$\Xi_R^J(x) := 1_{J_R} \wedge x \wedge x^2 \tag{1}$$

for all $x \in J_R$. Using (21.4.2), (21.4.3), one checks that this family is a homogeneous cubic polynomial law $\Xi^J\colon J \to \bigwedge^3(J)$ over k that is compatible with base change in the sense that

$$\Xi^{J_R} = \Xi^J \otimes R \tag{2}$$

for all $R \in k$-**alg**.

(b) By a *Jordan algebra of degree* 3 over k we mean a Jordan algebra J over k with the following properties.

(i) There exists a cubic form $N\colon J \to k$ making J a cubic Jordan algebra.

(ii) The set maps $\Xi_K^J\colon J_K \to \bigwedge^3(J_K)$ as defined in (1) are different from zero for all algebraically closed fields $K \in k$-**alg**.

In this case, we also say that the Jordan algebra J *has degree* 3. Intuitively speaking, condition (i) says that the degree of J is at most 3, while condition (ii) says it cannot be smaller. One might refer to (ii) as the "anti-Dickson condition", because it is in some sense opposite to the Dickson condition defined in Exc. 16.22. Also, condition (ii) is equivalent to

(ii′) The set maps $\Xi_K^J\colon J_K \to \bigwedge^3(J_K)$ as defined in (1) are different from zero for all infinite fields $K \in k$-**alg**.

Our principal aim in this section will be to show that, under suitable restrictions for a Jordan algebra J of degree 3, the cubic form N in (i) is uniquely determined by the algebra structure of J alone.

38.2 Proposition. *(a) Let J be a Jordan algebra of degree 3 over k. Then J_R is a Jordan algebra of degree 3 over R, for any $R \in k$-**alg**.*

(b) Let J be a cubic Jordan algebra over k and suppose R is a faithfully flat k-algebra. If the abstract Jordan algebra J_R has degree 3 over R, then the abstract Jordan algebra J has degree 3 over k.

Proof (a) This follows immediately from (38.1.2).

(b) Let $N\colon J \to k$ be a cubic form over k making J a cubic Jordan k-algebra. Then $N \otimes R\colon J_R \to R$ is a cubic form over R making J_R a cubic Jordan R-algebra. Let $K \in k$-**alg** be an algebraically closed field and apply Exc. 9.26 to find an algebraically closed field $L \in R$-**alg** that is also an extension field of K. Since $L \in R$-**alg** and J_R has degree 3 over R, the set map $\Xi_L^{J_R}$ is different from zero. But we also have $L \in K$-**alg**, its induced k-algebra structure by the diagram in Exc. 9.26 being the same as the one induced from $L \in R$-**alg**. Hence $\Xi_L^{J_K} = \Xi_L^J = \Xi_L^{J_R} \neq 0$. Assuming now $\Xi_K^{J_K} = 0$, Exc. 12.35 (a) implies $\Xi^{J_K} = 0$ as a polynomial law over K, a contradiction. Thus $\Xi_K^J = \Xi_K^{J_K} \neq 0$, whence J has degree 3 over k. □

38.3 Remark. Prop. 38.2 (b) *does not* claim that Jordan algebras of degree 3 are stable under faithfully flat descent because it rests on the overall assumption that J is a *cubic* Jordan algebra to begin with, and cubic Jordan algebras are *not* stable under faithfully flat descent (Exc. 34.27). Under comparatively mild restrictions, however, this difficulty will be resolved in Cor. 38.14 below.

38.4 Lemma (Racine [242])**.** *Let F be a field and J a cubic Jordan F-algebra whose nil radical is zero. For $0 \neq u \in J$, the following conditions are equivalent.*

(a) $u^2 = 0$.

(b) *u is nilpotent and there exists an elementary idempotent $e \in J$ such that $u \in J_0(e)$.*

Proof (a) ⇒ (b). With the usual abbreviations, we have $T(u) = S(u) = N(u) = 0$ by Exc. 34.23, and (33a.22) implies $u^\sharp = 0$. Since $\mathrm{Nil}(J) = \{0\}$, the same exercise shows $T(u, v) = 1$ for some $v \in J$. Put $w := u \times v$. Then (33a.13) implies $T(w) = T(u)T(v) - T(u, v) = -1$, hence in particular $w \neq 0$. On the other hand, from (33a.10) we deduce $w^\sharp = T(u^\sharp, v)v + T(u, v^\sharp)u - u^\sharp \times v^\sharp =$

$T(u, v^\sharp)u$, hence $S(w) = N(w) = 0$. Now put $e := w^\sharp - w$. Then $T(e) = 1$, and (33a.14) combined with the adjoint identity yields

$$\begin{aligned} e^\sharp &= (w^\sharp - w)^\sharp = w^{\sharp\sharp} - w^\sharp \times w + w^\sharp \\ &= N(w)w - \big(T(w)S(w) - N(w)\big)1 + S(w)w + T(w)w^\sharp + w^\sharp = 0. \end{aligned}$$

Thus e is an elementary idempotent in J. Applying (33a.28), we obtain $e \times u = w^\sharp \times u - w \times u = 2T(u, v^\sharp)u^\sharp - u \times (u \times v) = T(u \times v)u = T(u)u - u$, hence $u \in J_0(e)$ by (37.2.3).

(b) $\Rightarrow$ (a). Cor. 37.3 shows that u is a nilpotent element in a Jordan F-algebra of Clifford type. Hence $u^2 = 0$ by Exc. 29.21. □

38.5 Proposition (cf. Racine [242, Lemma 1])**.** *For a cubic Jordan algebra J over a field F and $I := \mathrm{Nil}(J)$, the following conditions are equivalent.*

(i) J/I *is* not *a Jordan division algebra.*
(ii) *There exists an element $u \in J \setminus I$ such that $u^\sharp \in I$.*
(iii) *J contains an elementary idempotent.*

Proof By Exercises 34.21 (c) and 37.21 (a), $\bar{J} := J/I$ carries the unique structure of a cubic Jordan algebra over F such that the canonical projection $x \mapsto \bar{x}$ from J to $\bar{J}$ is a homomorphism of cubic Jordan algebras.

(i) $\Rightarrow$ (ii). Since $\bar{J}$ is non-zero, there exists an element $x \in J \setminus I$ such that $\bar{x} \in \bar{J}$ is not invertible. But then neither is $x \in J$, by Prop. 31.5. Hence $N(x) = 0$, and the adjoint identity implies $x^{\sharp\sharp} = 0$. Thus $u = x$ or $u = x^\sharp$ satisfies (ii).

(ii) $\Rightarrow$ (iii). Since elementary idempotents in $\bar{J}$ can be lifted to elementary idempotents in J, by Exc. 37.21 (b), we may assume $I = \{0\}$, i.e., $J = \bar{J}$. By (ii), therefore, some non-zero $u \in J$ has $u^\sharp = 0$. If $T(u) \neq 0$, then $T(u)^{-1}u$ is an elementary idempotent in J, so we may assume $T(u) = 0$, which implies $u^2 = 0$ by (33a.22). Hence the implication (ii)$\Rightarrow$(iii) follows from Lemma 38.4.

(iii) $\Rightarrow$ (i). Assume $\bar{J}$ is a Jordan division algebra. Then the elementary idempotent $\bar{e} \in \bar{J}$ is invertible, forcing $N_{\bar{J}}(\bar{e}) \in F^\times$, a contradiction to 37.1. □

38.6 Theorem. *Let J be a cubic Jordan algebra over k that is finitely generated projective as a k-module and satisfies the condition*

$$\dim_K \left(J_K / \mathrm{Nil}(J_K)\right) \geq 2 \tag{1}$$

*for all algebraically closed fields $K \in k$-**alg**. Then the subfunctor $\mathbf{Elid}(J) \subseteq J_{\mathbf{a}}$ defined by*

$$\mathbf{Elid}(J)(R) := \mathrm{Elid}(J_R) := \{e \in J_R \mid e \text{ is an elementary idempotent}\} \tag{2}$$

*for all $R \in k$-**alg** is an fppf smooth closed subscheme, and there exists an étale cover R of k such that J_R contains an elementary idempotent.*

The functor $J_{\mathbf{a}}$ was defined in Example 24.21.

Proof The second statement follows immediately from the first combined with 25.25 (ii). Since elementary idempotents are invariant under base change, (2) does indeed define a subfunctor of $J_{\mathbf{a}}$. Let $u_1^*, \dots, u_m^*$ be a finite set of generators of J^*, the dual of the k-module J. Then

$$\mathbf{Elid}(J)(R) = \{e \in J_R \mid T_J(e) = 1,\ \langle u_{iR}^*, e^\sharp \rangle = 0 \ \ (1 \le i \le m)\}$$

for all $R \in k$-**alg**, and we conclude from 24.15, 25.11, Exercises 25.32 and 25.31 (b) that $\mathbf{X} := \mathbf{Elid}(J)$ is a finitely presented closed subscheme of $J_{\mathbf{a}}$; in particular, it is affine. It remains to show that $\mathbf{X}$ is fppf and smooth. Beginning with smoothness, let $R \in k$-**alg** and $\mathfrak{a} \subseteq R$ be an ideal such that $\mathfrak{a}^2 = \{0\}$. By 25.20, we must prove that every elementary idempotent of $J_{R/\mathfrak{a}} = J_R/\mathfrak{a}J_R$ can be lifted to an elementary idempotent of J_R. But this follows from Exercises 37.21 (b) and 34.21 (e). In order to prove that $\mathbf{X}$ is fppf, it suffices to show by Prop. 25.24 that $\mathbf{X}$ has non-empty geometric fibers, so let $K \in k$-**alg** be an algebraically closed field and put $I := \mathrm{Nil}(J_K)$. By (1) and Exc. 31.39 (b), J_K/I is not a Jordan division algebra, and Prop. 38.5 shows $\mathbf{X}(K) \neq \emptyset$. Thus $\mathbf{X}$ is fppf. □

38.7 Cubic norm structures and Peirce decompositions (cf. Racine [242, p. 97])**.** We fix a cubic Jordan algebra J over k, with identity element 1, adjoint $x \mapsto x^\sharp$, norm N, (bi-)linear trace T, quadratic trace S, and let $e \in J$ be an elementary idempotent. Writing X for the cubic norm structure underlying J, we wish to understand more fully the interplay between X and the Peirce components of J relative to e. Appealing to the notion of a complemented cubic norm substructure as defined in 35.2, this will be accomplished in several steps.

(a) Following Cor. 37.3, $\mathbf{M}_0 := (M_0, q_0, e_0)$ as defined in (37.3.1) is a pointed quadratic module over k having $J_0(e) = J(\mathbf{M}_0)$ as Jordan algebras. Writing t_0 for the (bi-)linear trace of $\mathbf{M}_0$ and $x_0 \mapsto \bar{x}_0$ for its conjugation, we claim

$$N|_{J_i(e)} = 0 \quad \text{(as a polynomial law)} \qquad (i = 0, 1, 2), \tag{1}$$

$$J_1(e)^\sharp \subseteq J_0(e), \tag{2}$$

$$J_0(e) \times J_1(e) \subseteq J_1(e). \tag{3}$$

Indeed, (1) for $i = 2$ follows from 37.1 and (37.2.1). Next, we let $x_0 \in J_0(e)$ and first expand $N(e_0) = N(1 - e) = 1 - T(e) + S(e) - N(e) = 1 - 1 = 0$, which by (33a.21) implies $N(x_0) = N(U_{e_0} x_0) = N(e_0)^2 N(x_0) = 0$. Thus (1) holds for $i = 0$. Now let $x_1 \in J_1(e)$. Then $e \times x_1 = 0$, $T(x_1) = 0$ by (37.2.2), and the unit

identity yields $e_0 \times x_1 = (1-e) \times x_1 = T(x_1)1 - x_1$, hence

$$e_0 \times x_1 = -x_1. \tag{4}$$

Combining (4) with (33a.29), Prop. 37.2 (a), (b) and (1) for $i = 0$, we conclude

$$\begin{aligned} N(x_1) &= -N(e_0 \times x_1) = -T(e_0^\sharp, x_1)T(e_0, x_1^\sharp) + N(e_0)N(x_1) \\ &= -T(e, x_1)T(e_0, x_1^\sharp) = 0. \end{aligned}$$

Since our set-up is stable under base change, this completes the proof of (1). Applying (4) again, this time in conjunction with (33a.10) and (33a.15) yields $x_1^\sharp = (e_0 \times x_1)^\sharp = T(e_0^\sharp, x_1)x_1 + T(e_0, x_1^\sharp)e_0 - e_0^\sharp \times x_1^\sharp = U_{e_0}x_1^\sharp$, hence $x_1^\sharp \in J_0(e)$. Thus (2) holds. Finally, let $x_i \in J_i(e)$ for $i = 0, 1$. From (33a.23), Prop. 37.2 and Cor. 37.3 we deduce $x_0 \times x_1 = x_0 \circ x_1 - T(x_0)x_1 - T(x_1)x_0 + (T(x_0)T(x_1) - T(x_0, x_1))1 = x_0 \circ x_1 - t_0(x_0)x_1 \in J_1(e)$ by the Peirce rules, which now imply $x_0 \times x_1 = -(t_0(x_0)e_0 - x_0) \circ x_1$, hence

$$x_0 \times x_1 = -\bar{x}_0 \circ x_1 \in J_1(e) \qquad (x_i \in J_i(e),\ i = 0, 1). \tag{5}$$

In particular, (3) holds.

(b) By the Peirce rules,

$$\hat{J}_0 := ke \oplus J_0(e) = ke \oplus M_0 \tag{6}$$

is a direct sum of ideals; it is also a cubic Jordan subalgebra of J. We denote by X_0 the cubic norm structure underlying $\hat{J}_0$. Actually, after the obvious identifications, one checks that X_0 is just the cubic norm structure belonging to the cubic Jordan algebra built up from $J(\mathbf{M}_0)$ by means of Exc. 34.24, i.e., by (1), (4), Prop. 37.2 (c) and Cor. 37.3, the identities

$$(\xi e + x_0)^\sharp = q_0(x_0)e + \xi\bar{x}_0, \tag{7}$$

$$N(\xi e + x_0) = \xi q_0(x_0) \tag{8}$$

hold strictly for $\xi \in k$, $x_0 \in M_0$.

(c) Now we put $M_1 := J_1(e)$ as a k-module and have $M_1 \subseteq X_0^\perp$ as well as $X = X_0 \oplus M_1$. Applying (37.2.2) and (5), we obtain

$$(\xi e + x_0)\,.\,x_1 = \bar{x}_0 \circ x_1 \in M_1 \tag{9}$$

in the sense of (35.1.2) for $\xi \in k$, $x_i \in M_i$, $i = 0, 1$. Thus (X_0, M_1) is a complemented cubic norm substructure of X in the sense of 35.2. By (35.6.1), therefore, (X_0, M_1) comes equipped with two quadratic maps $Q\colon M_1 \to X_0$, $H\colon M_1 \to M_1$, determined by the condition $x_1^\sharp = -Q(x_1) + H(x_1)$, $Q(x_1) \in X_0$,

$H(x_1) \in M_1$ for $x_1 \in M_1$. From (2) we therefore deduce $H = 0$ and that $Q\colon M_1 \to M_0$ is a quadratic map satisfying

$$x_1^\sharp = -Q(x_1) \qquad (x_1 \in M_1). \tag{10}$$

Specializing (35.6.2)–(35.6.6) accordingly and combining (1), (7), (8), (9) with the formulas of Exc. 34.24, we conclude that the identities

$$(\xi e + x_1 + x_0)^\sharp = q_0(x_0)e - \bar{x}_0 \circ x_1 + (\xi\bar{x}_0 - Q(x_1)), \tag{11}$$

$$N(\xi e + x_1 + x_0) = \xi q_0(x_0) - t_0(x_0, Q(x_1)), \tag{12}$$

$$T(\xi e + x_1 + x_0, \eta e + y_1 + y_0) = \xi\eta + t_0(Q(x_1, y_1)) + t_0(x_0, y_0), \tag{13}$$

$$T(\xi e + x_1 + x_0) = \xi + t_0(x_0), \tag{14}$$

$$S(\xi e + x_1 + x_0) = \xi t_0(x_0) - t_0(Q(x_1)) + q_0(x_0) \tag{15}$$

hold strictly for $\xi, \eta \in k$, $x_i, y_i \in M_i$, $i = 0, 1$.

38.8 Peirce-one extensions. Let $\mathbf{M}_0 = (M_0, q_0, e_0)$ be a pointed quadratic module over k. By a *Peirce-one extension* of $\mathbf{M}_0$ we mean a triple $\mathbf{M}_1 = (M_1, .\,, Q)$ with the following properties.

(i) M_1 is a k-module,
(ii) $. : M_0 \times M_1 \to M_1, (x_0, x_1) \mapsto x_0 \,.\, x_1$, is a bilinear map,
(iii) $Q\colon M_1 \to M_0$ is a quadratic map.

Peirce-one extensions of pointed quadratic modules are clearly stable under base change: if $\mathbf{M}_0$ is a pointed quadratic module over k and $\mathbf{M}_1 = (M_1, .\,, Q)$ is a Peirce-one extension of $\mathbf{M}_0$, then $\mathbf{M}_{1R} := (M_{1R}, .\,_R, Q_R)$ is a Peirce-one extension of the pointed quadratic module $\mathbf{M}_{0R}$ over R.

38.9 Building up cubic Jordan algebras with elementary idempotents. Let $\mathbf{M}_0 = (M_0, q_0, e_0)$ be a pointed quadratic k-module with (bi-)linear trace t_0 and conjugation $x_0 \mapsto \bar{x}_0$, and let $\mathbf{M}_1 = (M_1, .\,, Q)$ be a Peirce-one extension of $\mathbf{M}_0$. With a free k-module ke of rank 1, we construct a cubic array $X = X(\mathbf{M}_0, \mathbf{M}_1)$ over k by setting

$$X := ke \oplus M_1 \oplus M_0 \tag{1}$$

as a k-module and defining base point, adjoint and norm by the strict validity of the formulas

$$1 := e + e_0 := (e, 0, e_0), \tag{2}$$

$$x^\sharp := (q_0(x_0)e, -x_0 \,.\, x_1, \xi\bar{x}_0 - Q(x_1)), \tag{3}$$

$$N(x) := \xi q_0(x_0) - t_0(x_0, Q(x_1)) \tag{4}$$

for $x = (\xi e, x_1, x_0), \xi \in k, x_i \in M_i, i = 0, 1$. Note in particular that the projection onto the first summand in (1) determines a linear form $\lambda\colon X \to k$ satisfying $\lambda(1) = 1$. Hence $1 \in X$ is unimodular. With another element $y = (\eta e, y_1, y_0) \in X, \eta \in k, y_i \in M_i, i = 0, 1$, we conclude

$$x \times y = (q_0(x_0, y_0)e, -x_0 \,.\, y_1 - y_0 \,.\, x_1, \xi\bar{y}_0 + \eta\bar{x}_0 - Q(x_1, y_1)), \tag{5}$$
$$N(x, y) = \xi q_0(x_0, y_0) + \eta q_0(x_0) - t_0(x_0, Q(x_1, y_1)) - t_0(y_0, Q(x_1)), \tag{6}$$
$$T(x) = \xi + t_0(x_0), \tag{7}$$
$$S(x) = \xi t_0(x_0) + q_0(x_0) - t_0(Q(x_1)), \tag{8}$$
$$S(x, y) = \xi t_0(y_0) + \eta t_0(x_0) + q_0(x_0, y_0) - t_0(Q(x_1, y_1)), \tag{9}$$
$$T(x, y) = \xi\eta + t_0(Q(x_1, y_1)) + t_0(x_0, y_0). \tag{10}$$

From now on, we identify $ke, M_1, M_0 \subseteq X$ canonically. Also, we will use occasionally the U-operator of the Jordan algebra $J(\mathbf{M}_0)$.

38.10 Proposition. *Let $\mathbf{M}_0 = (M_0, q_0, e_0)$ be a pointed quadratic k-module with (bi-)linear trace t_0 and conjugation $x_0 \mapsto \bar{x}_0$, and let $\mathbf{M}_1 = (M_1, \,.\,, Q)$ be a Peirce-one extension of $\mathbf{M}_0$. Then the cubic array $X = X(\mathbf{M}_0, \mathbf{M}_1)$ of 38.9 is a cubic norm structure over k if and only if the Peirce-one extension $\mathbf{M}_1$ of $\mathbf{M}_0$ is* admissible *in the sense that the identities*

$$e_0 \,.\, x_1 = x_1, \tag{1}$$
$$\bar{x}_0 \,.\, (x_0 \,.\, x_1) = q_0(x_0)x_1, \tag{2}$$
$$Q(x_0 \,.\, x_1) = U_{x_0} Q(x_1), \tag{3}$$
$$q_0(Q(x_1)) = 0, \tag{4}$$
$$t_0(x_0, Q(x_1, y_1)) = t_0(Q(x_0 \,.\, x_1, y_1)), \tag{5}$$
$$Q(x_1) \,.\, (x_0 \,.\, x_1) = t_0(x_0, Q(x_1))x_1 \tag{6}$$

hold strictly for all $x_0 \in M_0$, $x_1, y_1 \in M_1$. In this case, e is an elementary idempotent in

$$J := J(\mathbf{M}_0, \mathbf{M}_1) := J(X(\mathbf{M}_0, \mathbf{M}_1)), \tag{7}$$

called its distinguished *elementary idempotent, whose Peirce components have the form*

$$J_2(e) = ke, \quad J_1(e) = M_1, \quad J_0(e) = M_0. \tag{8}$$

More precisely, $J_0(e) = J(\mathbf{M}_0)$ as Jordan algebras.

Proof Putting $x_1 = 0$ in (38.9.3), (38.9.4) we see that $X_0 := ke \oplus M_0$ is not only a cubic subarray of X but, as such, the cubic norm structure derived from

$J(\mathbf{M}_0)$ via Exc. 34.24. By letting e act trivially on M_1, the bilinear action of M_0 on M_1 belonging to the Peirce-one extension $\mathbf{M}_1$ of $\mathbf{M}_0$ extends to a bilinear action

$$X_0 \times M_1 \longrightarrow M_1, \quad ((\xi e, x_0), x_1) \longmapsto (\xi e, x_0) \,.\, x_1 := x_0 \,.\, x_1. \tag{9}$$

We have thus arrived at the set-up of 35.8, with V replaced by M_1, $H = 0$ and Q viewed as a quadratic map $M_1 \to X_0$. By (35.8.1), this implies $\hat{N} = 0$ as a cubic form on M_1, and (35.8.2), (35.8.3) are converted to (38.9.3), (38.9.4) after the appropriate substitutions. From Prop. 35.9 we therefore deduce that X is a cubic norm structure over k if and only if the identities (35c.1)–(35c.10) hold strictly, where we have to replace u by x_1 and x_0 by $(\xi e, x_0)$, $\xi \in k$, $x_0 \in M_0$. Since e acts trivially on M_1, one checks that (35c.1)–(35c.3) are equivalent to (1)–(3), while $H = 0$ implies that (35c.5), (35c.9), (35c.10) in this order correspond to (4), (5), (6). For the same reason, (35c.4), (35c.6)–(35c.8) are trivially fulfilled. This proves the first part of the proposition. The second part follows immediately from (38.9.7), (38.9.3), (38.9.5) and Prop. 37.2. □

Collecting what we have achieved so far, we arrive at the following result.

38.11 Theorem. *If $\mathbf{M}_0$ is a pointed quadratic module over k and $\mathbf{M}_1$ is an admissible Peirce-one extension of $\mathbf{M}_0$, then $J(\mathbf{M}_0, \mathbf{M}_1)$ is a cubic Jordan algebra over k containing the element e of (38.9.1) as its distinguished elementary idempotent and satisfying (38.9.2)–(38.9.10). Conversely, let J be a cubic Jordan algebra over k and $e \in J$ an elementary idempotent. Then there exist a pointed quadratic module $\mathbf{M}_0$, an admissible Peirce-one extension $\mathbf{M}_1$ of $\mathbf{M}_0$ and an identification $J = J(\mathbf{M}_0, \mathbf{M}_1)$ matching $e \in J$ with the distinguished elementary idempotent of $J(\mathbf{M}_0, \mathbf{M}_1)$.* □

38.12 Proposition. *Let J be a Jordan algebra of degree 3 over k. An idempotent $c \in J$ is elementary if and only if $J_2(c) = kc$ is a free k-module of rank 1.*

Proof If c is an elementary idempotent, then (37.2.1) implies that the k-module $J_2(c) = kc$ is free of rank 1. Conversely, let this be so. Localizing if necessary, we may assume that the ring $k \neq \{0\}$ is connected. Then Exc. 37.19 leaves the following options for c. (i) $c = 0$, (ii) $c = 1$, (iii) c is elementary, (iv) c is co-elementary. Options (i), (ii) can be ruled out, either for trivial reasons or since J has degree 3. It remains to show that also (iv) leads to a contradiction, so let us assume that c is co-elementary. By Exc. 38.19 (d) below, there exists a weird quadratic module (M, q) over k and an identification $J = J_{\mathrm{cub}}(M, q) = ke \oplus M \oplus ke_0$ matching c with the co-elementary idempotent e_0 of Exc. 38.19 (c). After an appropriate base change, we may assume that

$K = k$ is an algebraically closed field. Then Exc. 38.19 (b) implies $q = 0$. Given $\xi, \xi_0 \in K$, $u \in M$ and setting $x := (\xi e, u, \xi_0 e_0) \in J$, we combine (33a.22) with Exc. 38.19, (8), (12), (13) to obtain

$$\begin{aligned} x^2 &= x^\sharp + T(x)x - S(x)1 \\ &= (\xi_0^2 e, -\xi_0 u, \xi\xi_0 e_0) + (\xi + 2\xi_0)(\xi e, u, \xi_0 e_0) - (\xi_0^2 + 2\xi\xi_0)(e, 0, e_0) \\ &= (\xi^2 e, (\xi + \xi_0)u, \xi_0^2 e_0) \\ &= (\xi + \xi_0)x - (\xi\xi_0)1. \end{aligned}$$

Hence the set map Ξ_K^J is identically zero, in contradiction to J having degree 3. □

The preceding result derives its importance from the fact that the property of an idempotent to be elementary is characterized purely in terms of the underlying *abstract* Jordan algebra. This point is crucial in the following important application.

38.13 Theorem. *Let J be a cubic Jordan algebra with norm N over k such that J is a Jordan algebra of degree 3. If J is finitely generated projective as a k-module and satisfies*

$$\dim_K (J_K / \operatorname{Nil}(J_K)) \geq 2 \tag{1}$$

*for all algebraically closed fields $K \in k$-**alg**, then N is the unique cubic form making J a cubic Jordan algebra.*

When there is a unique cubic form making J a cubic Jordan algebra (as in the conclusion of the theorem), that form is called the *norm* of J and it is denoted by N_J.

Proof Let $N, N' : J \to k$ be two cubic forms that both make J a cubic Jordan algebra. By 34.1, 34.3 (a), they extend to cubic norm structures X, X' over k satisfying $J(X) = J = J(X')$ as abstract Jordan algebras. We will show $X = X'$. Note first that $J(X)$ and $J(X')$ both have degree 3. Next, passing to an appropriate faithfully flat base change by combining Exc. 25.35 with Thm. 38.6, we may assume that there is an elementary idempotent in the cubic Jordan algebra $J(X)$. Following Prop. 38.12, therefore, e is also an elementary idempotent in $J(X')$. Hence Thm. 38.11 yields pointed quadratic modules $\mathbf{M}_0 = (M_0, q_0, e_0)$, $\mathbf{M}_0' = (M_0', q_0', e_0')$ over k, an admissible Peirce-one extension $\mathbf{M}_1 = (M_1, \ ., Q)$ of $\mathbf{M}_0$, an admissible Peirce-one extension $\mathbf{M}_1' = (M_1', \ .', Q')$ of $\mathbf{M}_0'$ and identifications $J(X) = J(\mathbf{M}_0, \mathbf{M}_1)$, $J(X') = J(\mathbf{M}_0', \mathbf{M}_1')$ as cubic Jordan algebras matching e with the distinguished elementary idempotent of $J(\mathbf{M}_0, \mathbf{M}_1)$,

$J(\mathbf{M}_0', \mathbf{M}_1')$, respectively. From (38.10.8) we deduce $M_0 = J_0(e) = M_0'$ as projective k-modules, which by Exc. 29.26 implies not only $e_0 = e_0'$ but also $q_0 = q_0'$. Hence the linear traces of $\mathbf{M}_0$ and $\mathbf{M}_0'$ are the same as well: $t_0 = t_0'$. Now (38.9.7) implies $T_X = T_{X'}$ for the linear traces of X and X'. Moreover, $M_1 = J_1(e) = M_1'$ by (38.10.8), and for $x_1 \in M_1$ we apply (33a.22), (38.9.3), (38.9.7) and (38.9.8) to compute $-Q(x_1) = x_1^{\sharp_X} = x_1^2 - T_X(x_1)x_1 + S_X(x_1)1 = x_1^2 - t_0(Q(x_1))1$. Since this expression belongs to $J_0(e)$, we conclude $U_e x_1^2 = t_0(Q(x_1))e$, hence $t_0(Q(x_1)) = T_X(U_e x_1^2) = T_{X'}(U_e x_1^2) = t_0(Q'(x_1))$. Thus (38.9.8) yields $S_X = S_{X'}$, which implies $\sharp_X = \sharp_{X'}$ by (33a.22) and $N_X = N_{X'}$ by (33.9.2). □

38.14 Corollary. *Let J be a Jordan algebra over k that is finitely generated projective as a k-module and satisfies*

$$\dim_K (J_K / \operatorname{Nil}(J_K)) \geq 2$$

*for all algebraically closed fields $K \in k$-**alg**. If R is a faithfully flat k-algebra and J_R has degree 3 over R, then J has degree 3 over k.*

Proof Combining Theorem 38.13 with Exc. 25.35 and Prop. 38.2 (b), this follows by faithfully flat descent. □

38.15 The connection with generically algebraic Jordan algebras. The ad hoc method we used to establish Thm. 38.13 is probably not strong enough to dispense with the hypothesis of the nil radical of J_K, $K \in k$-**alg** an algebraically closed field, to have co-dimension at least 2. This can be accomplished either by throwing in some additional hypothesis on the base ring, see Exc. 38.20 below, or by appealing to Loos's theory [174] of generically algebraic Jordan algebras as follows. We claim:

> *Let J be a Jordan algebra of degree 3 over k in the sense of 38.1 (b) and assume J is finitely generated projective as a k-module. Then J is generically algebraic of (constant) degree 3 in the sense of [174, 2.1, 2.2], and any cubic form making J a cubic Jordan algebra in the sense of 34.1 agrees with its generic norm in the sense of [174, 2.7 (a)].*

Indeed, once this claim has been established, Thm. 38.13 without the hypothesis (38.13.1) drops out immediately.

Proof Let $N\colon J \to k$ be a cubic form making J a cubic Jordan algebra (38.1 (b) (i)) and write T (resp. S) for the corresponding linear (resp. quadratic) trace. By 34.1 (iii), the polynomial

$$m_J(\mathbf{t}) = \mathbf{t}^3 - T \cdot \mathbf{t}^2 + S \cdot \mathbf{t} - N \cdot 1 \in k[J_{\mathbf{a}}][\mathbf{t}] \tag{1}$$

satisfies condition (i) of [174, 2.2]. Now let $K \in k$-**alg** be any field and write L for an algebraic closure of K. Then J_L is finite-dimensional over L, hence generically algebraic (Jacobson-Katz [143, Thm. 2]). Since $m_{J,x}(x) = (\mathbf{t}m_{J,x})(x)$ is zero for all $x \in J_L$, the degree of J_L is at most 3. It cannot be 1 or 2 since this would contradict 38.1 (b) (ii). Thus $\deg_L(J_L) = 3$, forcing $\deg_K(J_K) = 3$ by [174, 2.7 (b)] and its proof. Hence $m_J(\mathbf{t})_K$ is the generic minimum polynomial of J_K, and we have verified condition (ii') of [174, 2.2]. Summing up, therefore, J is generically algebraic of degree 3 over k, with its generic minimum polynomial given by (1). In particular, N is the generic norm of J. □

Our next aim will be to derive a criterion that, under suitable regularity conditions, is necessary and sufficient for a cubic Jordan algebra to have degree 3. These regularity conditions are based on the following concept.

38.16 Separable Jordan algebras. A Jordan algebra J over k is said to be *separable* if it is projective (but possibly *not* finitely generated) as a k-module and $\mathrm{Nil}(J_K) = \{0\}$ for all *fields* $K \in k$-**alg**. The notion of separability is clearly stable under base change. Moreover, regular cubic Jordan algebras by Exc. 34.23 are separable while the converse is not true: let $J := \mathrm{Her}_3(F)$ be the cubic Jordan algebra of 3-by-3 symmetric matrices with entries in a field F of characteristic 2. Then every base field extension of J is simple, by Exc. 37.26 (e), so J is, in fact, separable. On the other hand, (36.4.7) shows that the radical of the bilinear trace consists of those elements in J that have zeros down the diagonal; in particular, J is singular.

38.17 Theorem. *A separable cubic Jordan algebra over k having rank $r \in \mathbb{N} \cup \{\infty\}$ as a projective module is a Jordan algebra of degree 3 if and only if $r > 2$.*

Proof If $r \leq 2$ then $\dim_K(J_K) \leq 2$ for every field $K \in k$-**alg**, forcing $\Xi^J_K = 0$ as a set map $J_K \to \bigwedge^3(J_K)$. In particular, J cannot have degree 3. Conversely, assume the degree of J is not 3. By 38.1 (b), there exists an algebraically closed field $K \in k$-**alg** such that $(\Xi^J \otimes K)_K = \Xi^J_K = 0$ as a set map $J_K \to \bigwedge^3(J_K)$. By Exc. 12.35 (a), therefore, $\Xi^J \otimes K = 0$ as a polynomial law over K. Hence the Jordan algebra J_K over K satisfies the Dickson condition of Exc. 30.13. Moreover, no base field extension of J_K has absolute zero divisors (Exc. 37.27 (c)) and we conclude from Thm. 30.11 that J_K is strictly locally linear, again in the sense of Exc. 37.27, which therefore yields a pointed quadratic module (M, q, e) over K satisfying $J_K = J(M, q, e)$ as abstract Jordan algebras. Now it follows from Exc. 34.27 that there exists a linear form $\lambda\colon J_K \to K$ satisfying $\lambda(1_{J_K}) = 1_K$ and $q(x) = \lambda(x)\lambda(\bar{x})$ for all $x \in J_K$, where $\iota\colon M \to M$, $x \mapsto \bar{x}$, stands for the conjugation of (M, q, e), and $t(x) = \lambda(x) + \lambda(\bar{x})$ for all

$x \in J_K$, where t stands for the linear trace of (M, q, e). Invoking separability and Exc. 29.21, one checks $\{0\} = \mathrm{Nil}(J_K) = \mathrm{Ker}(\lambda) \cap \mathrm{Ker}(\lambda \circ \iota)$, which implies $r = \dim_K(J_K) \leq 2$. □

38.18 Corollary. *Let J be a separable cubic Jordan algebra over k whose rank function takes values in $\mathbb{N} \setminus \{2\}$, and let J' be any cubic Jordan algebra over k. Then every isomorphism $\varphi\colon J \to J'$ of para-quadratic algebras is in fact one of cubic Jordan algebras.*

The hypothesis that the rank does not take the value 2 is necessary by 34.15.

Proof By standard arguments based on the rank decomposition (Exc. 9.31), we may assume that J has finite constant rank $r > 0$. The case $r = 1$ being obvious, we are left with the case $r > 2$. By Thm. 38.17, J has degree 3 and hence, as an abstract Jordan algebra, determines its underlying cubic norm structure uniquely (Thm. 38.13). Since $N := N_{J'} \circ \varphi\colon J \to k$ is a cubic form permitting Jordan composition and satisfying $m_x(x) = (\mathbf{t}m_x)(x) = 0$ strictly for all $x \in J$, where $m_x(\mathbf{t}) := N(\mathbf{t}\mathbf{1} - x)$, we conclude $N = N_J$, as claimed. □

Exercises

38.19. *Weird quadratic modules.* A quadratic module (M, q) over k is said to be *weird* if the identities

$$q(u)^2 = 0, \quad q(u)u = 0 \tag{1}$$

hold strictly for all $u \in M$. Let (M, q) be any quadratic module over k.

(a) Show that (M, q) is weird if and only if (1) and

$$2q(u)q(u, v) = 0, \tag{2}$$
$$2(q(u, v)q(u, w) + q(u)q(v, w)) = 0, \tag{3}$$
$$q(u, v)^2 + 2q(u)q(v) = 0, \tag{4}$$
$$q(u, v)u + q(u)v = 0 \tag{5}$$

hold for all $u, v \in M$. Conclude that weird quadratic modules (M, q) with $q \neq 0$ exist.

(b) But prove that, if (M, q) is weird and M is projective, then $q = 0$.

(c) Let ke, ke_0 be free k-modules of rank 1 and prove that the k-module

$$X := ke \oplus M \oplus ke_0 \tag{6}$$

together with the base point, adjoint, norm given by the strict validity of the formulas

$$1 := e + e_0 := (e, 0, e_0), \tag{7}$$
$$x^\sharp := \big(\xi_0^2 e, -\xi_0 u, (\xi\xi_0 - q(u))e_0\big), \tag{8}$$
$$N(x) := \xi\xi_0^2 - 2\xi_0 q(u) \tag{9}$$

for $x = \xi e \oplus u \oplus \xi_0 e_0$, $\xi, \xi_0 \in k$, $u \in M$ is a cubic array over k such that

$$x \times y = \big(2\xi_0\eta_0 e, -\xi_0 v - \eta_0 u, (\xi\eta_0 + \eta\xi_0 - q(u,v))e_0\big), \tag{10}$$

$$N(x,y) = 2\xi\xi_0\eta_0 + \xi_0^2\eta - 2\xi_0 q(u,v) - 2q(u)\eta_0, \tag{11}$$

$$T(x) = \xi + 2\xi_0, \tag{12}$$

$$S(x) = \xi_0^2 + 2(\xi\xi_0 - q(u)), \tag{13}$$

$$T(x,y) = \xi\eta + 2\xi_0\eta_0 + 2q(u,v), \tag{14}$$

where $y = (\eta e, v, \eta_0 e_0)$, $\eta, \eta_0 \in k$, $v \in M$. Moreover, X is a cubic norm structure if and only if (M,q) is weird. Writing in this case

$$J := J_{\text{cub}}(M,q) := J(X) \tag{15}$$

for the associated cubic Jordan algebra, both $J_2(e) = ke$, $J_2(e_0) = ke_0$ are free k-modules of rank 1 and e is an elementary idempotent in J while e_0 is a co-elementary one in the sense of Exc. 37.19.

(d) Let J be a cubic Jordan algebra over k and suppose $c \in J$ is a co-elementary idempotent such that $J_2(c) = kc$ is a free k-module of rank 1. Show that there exist a weird quadratic module (M,q) over k and an isomorphism $J \cong J' := J_{\text{cub}}(M,q)$ matching c with the co-elementary idempotent e_0 of J' exhibited in (c).

38.20. Let J be a Jordan algebra of degree 3 over k and assume k is reduced, i.e., $\text{Nil}(k) = \{0\}$. Show that the cubic norm structure underlying J is uniquely determined by J as an abstract Jordan algebra.

38.21. Let $\mathbf{M}_0 = (M_0, q_0, e_0)$ be a pointed quadratic module over k, with linear trace t_0 and conjugation $x_0 \mapsto \bar{x}_0$, and let $\mathbf{M}_1 = (M_1, \,.\,, Q)$ be an admissible Peirce-one extension of $\mathbf{M}_0$, so that $J := J(\mathbf{M}_0, \mathbf{M}_1)$ is a cubic Jordan algebra over k with distinguished elementary idempotent e.

(a) Show that

$$x = (\xi e, x_1, x_0) \in J \qquad (\xi \in k,\ x_i \in M_i,\ i = 0,1) \tag{1}$$

belongs to the nil radical of J if and only if the quantities

$$\xi,\ q_0(x_0),\ q_0(x_0, y_0),\ t_0(Q(x_1, y_1)),\ q_0(Q(x_1), y_0) \tag{2}$$

belong to the nil radical of k for all $y_i \in M_i$, $i = 0,1$.

(b) Conclude from (a) that the following conditions are equivalent.

(i) $\text{Nil}(J) \subseteq J_1(e)$.

(ii) k is reduced, and q_0 is non-degenerate in the sense of 11.11.

(iii) $\text{Nil}(J) = \{x_1 \in M_1 \mid \forall\, y_1 \in M_1 : Q(x_1) = 0,\ t_0(Q(x_1, y_1)) = 0\}$.

38.22 (cf. Racine [242, pp. 97–98])**.** Let $\mathbf{M}_0 = (M_0, q_0, e_0)$ be a pointed quadratic module over k whose linear trace is identically zero: $t_0 = 0$ as a linear form on M_0. Let $\mathbf{M}_1 = (M_1, \,.\,, Q)$ be an admissible Peirce-one extension of $\mathbf{M}_0$ and $J = J(\mathbf{M}_0, \mathbf{M}_1)$ the corresponding cubic Jordan algebra with distinguished elementary idempotent e. Assume $\text{Nil}(J) = \{0\}$ and let $x_1 \in M_1$ be non-zero. Show $Q(x_1) \neq 0$ and conclude that

$$e' := (e, x_1, -Q(x_1)) \in J$$

is an elementary idempotent. Moreover, the pointed quadratic module $\mathbf{M}'_0 := (M'_0, q'_0, e'_0)$ corresponding to e' and J via Cor. 37.3 has a non-zero linear trace: $t'_0 \neq 0$.

38.23. Let J be a separable cubic Jordan algebra of rank $r \in \mathbb{N} \cup \{\infty\}$ as a projective module over k. Prove that precisely one of the following holds.

(i) J has degree 3.
(ii) J and $(k \times k)^{(+)}_{\mathrm{cub}}$ are isomorphic as cubic Jordan algebras.
(iii) J is isomorphic to $k^{(+)}$ as a cubic Jordan algebra.

39 Freudenthal and Albert algebras

After a long journey, we have almost reached the point where the concept of an Albert algebra can finally be defined in its most general form. The only step still missing is to prove a theorem of Racine [242] that provides a detailed description of semi-simple cubic Jordan algebras over an arbitrary field. Once this result has been established, we are led quite naturally to the category of Freudenthal algebras (for their definition in the case of a field of characteristic $\neq 2$, see [160, §37.C]), of which Albert algebras form the most important subcategory. As the main result of this section, we then prove, in fairly close analogy to the case of composition algebras (Cor. 26.9), that all Freudenthal algebras are split by an appropriate fppf extension of the base ring; aside from minor exceptions, this extension can even be chosen to be étale.

39.1 Semi-simplicity. A Jordan algebra J over a field F is said to be *semi-simple* if its nil radical is zero: $\mathrm{Nil}(J) = \{0\}$. If J is cubic, this is equivalent to J having no absolute zero divisors (Exc. 37.27 (e)). Since the identity element of a non-zero Jordan algebra J over F is not nilpotent, the nil radical of J cannot be all of J, ergo *every simple Jordan F-algebra is semi-simple*.

Note also that separable (hence, in particular, regular) cubic Jordan algebras over F are semi-simple but not conversely. For example, if $\mathrm{char}(F) = 2$ and $K \supset F$ is a purely inseparable field extension of exponent 1, then $J := \mathrm{Her}_3(K)$ is semi-simple, even simple (Exc. 37.26 (e)), but not separable since K, after changing scalars to the algebraic closure $\bar{F}$ of F, picks up non-zero nilpotent elements, forcing $J_{\bar{F}}$ by Exc. 37.30 to pick up a non-zero nil radical in the process.

39.2 Proposition. *Let J be a semi-simple cubic Jordan algebra over a field F and $\Omega = (e_1, e_2, e_3)$ an elementary frame of J. Then the following conditions are equivalent.*

(i) *Ω can be extended to a co-ordinate system of J.*

(ii) *There exist a pre-composition algebra C over F, a diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ and an isomorphism from J onto $\mathrm{Her}_3(C,\Gamma)$ matching Ω with the diagonal frame of $\mathrm{Her}_3(C,\Gamma)$.*

(iii) *$J \cong \mathrm{Her}_3(C,\Gamma)$, for some pre-composition algebra C over F and some diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$.*

(iv) *J is simple.*

(v) *$J_1(e_i) \neq \{0\}$ for $i = 1,2,3$.*

Proof (i) $\Rightarrow$ (ii). By the Jacobson co-ordinatization theorem (37.17), there exist a multiplicative conic alternative F-algebra C, a diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ and an isomorphism $J \xrightarrow{\sim} J' := \mathrm{Her}_3(C,\Gamma)$ sending Ω to the diagonal frame of J'. In particular, J' is semi-simple and so is C (Exc. 37.30), i.e., C is a pre-composition algebra (Exc. 17.9).

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (iv). Exc. 37.26 (e).

(iv) $\Rightarrow$ (v). If $J_1(e_i) = \{0\}$ for some $i = 0,1,2$, then the Peirce decomposition of J relative to e_i collapses to $J \cong F^{(+)} \times J_0(e_i)$ as a direct product of ideals, contradicting the simplicity of J.

(v) $\Rightarrow$ (i). From (v) and (32.15.4) we conclude that at least two of the off-diagonal Peirce components, J_{jl}, relative to Ω are different from zero. Renumbering if necessary, we may assume $J_{23} \neq \{0\} \neq J_{31}$. For $i = 1,2$, we apply Cor. 37.3 to find a pointed quadratic module $\mathbf{M}_{i0} = (M_{i0}, q_{i0}, e_{i0})$, $e_{i0} = e_j + e_l$, over F such that

$$Fe_j \oplus J_{jl} \oplus Fe_l = J_2(e_j + e_l) = J_0(e_i) = J(\mathbf{M}_{i0}).$$

Here $J_0(e_i)$ along with J is semi-simple (Exc. 37.29), forcing $\mathbf{M}_{i0}$ to be non-degenerate (Exc. 29.21). Now e_j, e_l are complementary elementary idempotents in $J(\mathbf{M}_{i0})$ generating (by Prop. 32.8) a hyperbolic plane H_{i0} in the quadratic module (M_{i0}, q_{i0}) such that $H_{i0}^{\perp} = J_{jl}$. Hence the restriction of q_{i0} to $J_{jl} \neq \{0\}$ is non-degenerate. In particular, there exists an element $u_{jl} \in J_{jl}$ such that $q_{i0}(u_{jl}) \neq 0$. By Exc. 31.33, therefore, u_{jl} is invertible in $J_2(e_j + e_l)$ and thus connects e_j and e_l in the sense of Exc. 32.23. Summing up, we have extended Ω to a co-ordinate system $(e_1, e_2, e_3, u_{23}, u_{31})$ of J. □

39.3 Corollary. *Let J be a simple cubic Jordan algebra over an algebraically closed field F. Then the automorphism group of J acts transitively on the elementary frames of J.*

Proof Let Ω_1, Ω_2 be elementary frames of J. Since F is algebraically closed, Propositions 19.9 and 39.2 lead to composition algebras C_i $(i = 1,2)$ over F, diagonal matrices $\Gamma_i \in \mathrm{GL}_3(F)$ and isomorphisms $\Phi_i \colon J \xrightarrow{\sim} J_i := \mathrm{Her}_3(C_i, \Gamma_i)$

sending Ω_i to the diagonal frame of J_i. By Exc. 37.22 (b), we may assume $\Gamma_i = \mathbf{1}_3$. Moreover, C_1 and C_2, having the same dimension over F, are isomorphic, again since F is algebraically closed. Let $\varphi\colon C_1 \xrightarrow{\sim} C_2$ be any isomorphism. Then $\Phi_2^{-1} \circ \mathrm{Her}_3(\varphi) \circ \Phi_1 \in \mathrm{Aut}(J)$ sends Ω_1 to Ω_2. □

39.4 Remark. For a version of this result over arbitrary fields, see Exc. 41.31.

39.5 Proposition (Jacobson-McCrimmon [144, Thm. 11])**.** *Let (M, q, e) be a non-degenerate pointed quadratic module over the field F and write t for its linear trace. The Jordan algebra $J := J(M, q, e)$ over F contains an elementary idempotent if and only if the quadratic form q is isotropic and the linear form t is different from zero.*

Proof If J contains an elementary idempotent, then the definition in 29.13 implies $t \neq 0$ and that q is isotropic. Conversely, let this be so. If $q(z) = 0$ and $t(z) \neq 0$, for some $z \in M$, then $t(z)^{-1}z$ is an elementary idempotent in J. Hence we may assume that $q(z) = 0$ implies $t(z) = 0$, for all $z \in M$, and must show that this leads to a contradiction. We begin with a hyperbolic vector $v \in M$ relative to q. Since q is non-degenerate, v may be completed to a hyperbolic pair (v, w) of M relative to q, so we have $q(v) = q(w) = 0$, $q(v, w) = 1$. By assumption, t kills the hyperbolic plane $H := Fv + Fw$, and we have the decomposition $M = H \oplus H^\perp$. By hypothesis, some $x \in M$ has $t(x) \neq 0$. This implies $t(y) \neq 0$, where y denotes the $H^\perp$-component of x. It follows that $z := v - q(y)w + y \in M$ satisfies $t(z) \neq 0 = q(z)$, a contradiction. □

39.6 Theorem (Racine [242, Thm. 1])**.** *A cubic Jordan algebra J over a field F is semi-simple if and only if it satisfies one of the following mutually exclusive conditions.*

(i) *J is a cubic Jordan division algebra.*

(ii) *There exists a non-degenerate pointed quadratic module (M, q, e) over F such that*

$$J \cong F^{(+)} \times J(M, q, e),$$

where the right-hand side is a direct product of ideals, to be viewed as a cubic Jordan algebra over F via Exc. 34.24.

(iii) *There exist a pre-composition algebra C over F and a diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ such that*

$$J \cong \mathrm{Her}_3(C, \Gamma)$$

as cubic Jordan algebras.

Proof One checks easily that cubic Jordan algebras of type (i), (ii), (iii) are semi-simple, by consulting Exc. 29.21 in case (ii) and 37.26 in case (iii). Conversely, let J be a semi-simple cubic Jordan algebra over F and suppose J is not a Jordan division algebra. Then Prop. 38.5 implies that J contains an elementary idempotent. Let e be *any* elementary idempotent in J. Then Thm. 38.11 yields an identification $J = J(\mathbf{M}_0, \mathbf{M}_1)$, for some pointed quadratic module $\mathbf{M}_0 = (M_0, q_0, e_0)$ over F and some admissible Peirce-one extension $\mathbf{M}_1 = (M_1, \cdot, Q_1)$ for $\mathbf{M}_0$, such that e becomes the distinguished elementary idempotent of $J(\mathbf{M}_0, \mathbf{M}_1)$. Hence Prop. 38.10 implies $J(\mathbf{M}_0) = J_0(e)$, and we conclude from Exc. 38.21 that $\mathbf{M}_0$ is non-degenerate. Assume first that $J_1(e) = \{0\}$. Then $M_1 = \{0\}$ by (38.10.8), and from (38.9.3), (38.9.4) combined with Exc. 34.24 we deduce $J = Fe \oplus J(\mathbf{M}_0) \cong F^{(+)} \times J(\mathbf{M}_0)$ as in (ii). For the remainder of the proof, we may therefore assume $J_1(e) \neq \{0\}$ *for all* elementary idempotents $e \in J$. By semi-simplicity combined with Exc. 38.21 (b) (iii), the quadratic map $Q_1 \colon M_1 \to M_0$ cannot be zero. Hence (38.10.4) implies that the non-degenerate pointed quadratic module $\mathbf{M}_0$ is isotropic. Thanks to Exc. 38.22, we may also assume that the linear trace of $\mathbf{M}_0$ is different from zero. By Prop. 39.5, therefore, $J(\mathbf{M}_0)$ contains an elementary idempotent, which is also elementary in J (Cor. 37.3) and orthogonal to e. Consulting Prop. 37.4, we have thus found an elementary frame $\Omega = (e_1, e_2, e_3)$ in J. Since our assumptions imply $J_1(e_i) \neq \{0\}$ for all $i = 1, 2, 3$, we deduce from Prop. 39.2 that J is as in (iii) of the theorem. □

39.7 Corollary. *A cubic Jordan algebra over an algebraically closed field F is simple if and only if it is isomorphic to precisely one of the following.*

(a) $F^{(+)}$,
(b) $\mathrm{Her}_3(F) = \mathrm{Sym}_3(F)$,
(c) $\mathrm{Her}_3(F \times F) \cong \mathrm{Mat}_3(F)^{(+)}$,
(d) $\mathrm{Her}_3(\mathrm{Mat}_2(F)) = \mathrm{Symp}_3(F)$,
(e) $\mathrm{Her}_3(\mathrm{Zor}(F))$.

Proof Note that the isomorphism in (c) (resp. the identification in (d)) has been established in Prop. 36.9 (resp. in (10.10.16)). The cubic Jordan algebras (a)–(e) are simple by Exc. 37.26. Conversely, let J be a simple cubic Jordan algebra over F. Then J satisfies one of the conditions (i), (ii), (iii) of Thm. 39.6. If condition (i) holds, i.e., if J is a cubic Jordan division algebra, then Exc. 31.39 implies that J satisfies (a). Condition (ii) cannot hold since J is simple. Hence we are left with condition (iii), so $J \cong \mathrm{Her}_3(C, \Gamma)$ for some pre-composition algebra C over F and some diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$. But since F is algebraically closed, there are no purely inseparable extension fields of F other

than F itself. Hence C, by Prop. 19.9, is in fact a composition algebra over F, which must be split by 23.12. Moreover, since the entries of Γ by Exc. 37.22 are unique only up to invertible square factors in F, we may assume $\Gamma = \mathbf{1}_3$. Hence J satisfies one of the conditions (b)–(e). □

39.8 The concept of a Freudenthal algebra. By a *Freudenthal algebra* over k, we mean a cubic Jordan k-algebra J satisfying the following conditions.

(i) J is projective as a k-module.

(ii) The rank function $\mathfrak{p} \mapsto \mathrm{rk}_{\mathfrak{p}}(J)$ from $\mathrm{Spec}(k)$ to $\mathbb{N} \cup \{\infty\}$ is locally constant with respect to the Zariski topology.

(iii) For all fields $K \in k$-**alg**, the cubic Jordan algebra J_K over K is simple or is cubic étale in the sense of Example 34.17.

39.9 Examples of Freudenthal algebras.

(a) If k is the zero ring, then $J = \{0\}$ is a Freudenthal algebra, but a rather uninteresting one.

(b) $k^{(+)}$, viewed as a cubic Jordan algebra via 34.14, is a Freudenthal algebra of rank 1.

(c) If E is a cubic étale k-algebra, then $E^{(+)}$ is a Freudenthal algebra of rank 3.

(d) If (C, Γ) is a co-ordinate pair over k, with C a composition algebra, then $\mathrm{Her}_3(C, \Gamma)$ is a Freudenthal algebra. Indeed, while conditions (i), (ii) of 39.8 trivially hold, (iii) follows from Exc. 37.26 (e) combined with the fact that, over fields, composition algebras are the same as pre-composition algebras stable under base change (Prop. 19.9).

39.10 Elementary properties of Freudenthal algebras.

(a) Freudenthal algebras are stable under base change.

(b) Freudenthal algebras are separable.

(c) If J is a Freudenthal k-algebra, then so is the isotope $J^{(p)}$, for any $p \in J^\times$. Indeed, $J^{(p)}$ is a cubic Jordan algebra (Example 34.8) and $J^{(p)} = J$ as k-modules, so conditions (i), (ii) of 39.8 hold. As to (iii), we may assume that k is a field. Then J is simple, and hence so is $J^{(p)}$ (31.12).

39.11 Corollary. *If J is a Freudenthal algebra over k, then J is finitely generated as a k-module and the rank of J at each prime ideal is one of the numbers*

$$1, 3, 6, 9, 15, 27.$$

Proof For any $\mathfrak{p} \in \operatorname{Spec}(k)$, let $K \in k$-**alg** be an algebraically closed field containing $k(\mathfrak{p})$. Then J_K is either simple or split cubic étale, and Cor. 39.7 shows that the dimension of J_K, i.e., the rank of J at $\mathfrak{p}$, is one of the listed numbers. Finally, since each $J_{\mathfrak{p}}$ is finitely generated as a $k_{\mathfrak{p}}$-module and the rank function is locally constant in the Zariski topology, by 39.8 (ii), J is finitely generated as a k-module by Lemma 9.9. □

39.12 Rank decomposition. In the typical case where $k \neq \{0\}$, we will consider the rank decomposition of a Freudenthal algebra J in the sense of Exc. 9.31. Thanks to the corollary, if we set

$$\mathbb{N}_{\mathrm{Fr}} := \{1, 3, 6, 9, 15, 27\}, \tag{1}$$

then the rank decomposition takes the form

$$k = \prod_{n \in \mathbb{N}_{\mathrm{Fr}}} k_n, \quad k_n = k\varepsilon_n \qquad (n \in \mathbb{N}_{\mathrm{Fr}}), \tag{2}$$

$$J = \prod_{n \in \mathbb{N}_{\mathrm{Fr}}} J_n, \quad J_n = J \otimes k_n \qquad (n \in \mathbb{N}_{\mathrm{Fr}}), \tag{3}$$

induced by a complete orthogonal system $(\varepsilon_n)_{n \in \mathbb{N}_{\mathrm{Fr}}}$ of idempotents in k, uniquely determined by the condition that J_n is a Freudenthal algebra of rank n over k_n for all $n \in \mathbb{N}_{\mathrm{Fr}}$.

A Freudenthal k-algebra is defined as a cubic Jordan k-algebra (i.e., an object in k-**cujo**) with special properties. The following says that for detecting isomorphism we may ignore the cubic structure.

39.13 Corollary. *Freudenthal k-algebras are isomorphic as cubic Jordan algebras if and only if they are isomorphic as para-quadratic algebras over k.*

Proof Using the rank decomposition, we may assume that the given Freudenthal algebras have constant rank. Since that rank is not 2, the conclusion follows by Cor. 38.18. □

39.14 Corollary. *A Freudenthal algebra over k having finite constant rank as a projective module either has degree 3 or is isomorphic to $k^{(+)}$.*

Proof Combine Thm. 38.17 with Cor. 39.11. □

39.15 Corollary. *A Freudenthal algebra of constant rank n over k is either regular or satisfies one of the following conditions.*

(i) $n = 1$ *and* 3 *is not invertible in k.*

(ii) $n = 6$ *and* 2 *is not invertible in k.*

Proof By Exc. 39.37 below, if J is singular, then so is J_K, for some algebraically closed field $K \in k$-**alg**. Moreover, since J_K cannot be cubic étale, it belongs to the list of Cor. 39.7. Using (36.4.7), one checks that the singular members of that list are precisely the ones singled out in (i), (ii) above. □

39.16 Corollary. *A Freudenthal k-algebra J is cubic étale if and only if it has rank 3 as a k-module. If k is connected, then J is either cubic étale or J_K is simple for all fields $K \in k$-**alg**.*

Proof If J has rank 3, then it is regular (Cor. 39.15) and Exc. 39.42 below gives that J is cubic étale. The converse is trivial, so we have proved the first claim. The second claim follows from the first. □

Here is a criterion for a Freudenthal algebra to be a Jordan division algebra. Note that a Jordan division algebra over k automatically is one over F, for some field $F \in k$-**alg** (Cor. 28.19).

39.17 Proposition. *Let J be a Freudenthal algebra of constant rank ≥ 6 over a ring k. Among the statements*

(i) $J \cong \mathrm{Her}_3(C, \Gamma)$ *for some co-ordinate pair (C, Γ) such that C is a composition algebra.*
(ii) *J contains an elementary frame.*
(iii) *Some isotope of J contains an elementary idempotent.*
(iv) *There exists a nonzero $x \in J$ such that $N_J(x) = 0$.*
(v) *J is not a division algebra, i.e., there exists a $0 \neq x \in J$ such that $N_J(x) \notin k^\times$.*

we have the implications

$$(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v).$$

If k is a field, then all five statements are equivalent and additionally are equivalent to

(vi) *There exists a nonzero $x \in J$ such that $x^\sharp = 0$.*

The two statements in (v) are equivalent by Cor. 33.10. The Albert algebra Λ_0 over $\mathbb{Z}$ constructed in §56 below satisfies (iii) but not (ii) by Lemma 56.5.

Proof The first two implications are trivial. If (iii) holds, then $J^{(p)}$ contains an elementary idempotent e, for some $p \in J^\times$, hence $0 = N_{J^{(p)}}(e) = N_J(p)N_J(e)$, so $N_J(e) = 0$, and (iv) holds. Since $k \neq \{0\}$, (iv) trivially implies (v).

Suppose k is a field and (v) holds. Then J satisfies condition (iii) of Theorem 39.6: there is a pre-composition algebra C over F and a diagonal matrix

$\Gamma \in \mathrm{GL}_3(F)$ having $J \cong \mathrm{Her}_3(C, \Gamma)$. But J is also separable (39.10 (b)), and Exercise 37.30, eqn. (2), combined with Exc. 17.9 shows that C is in fact a composition algebra, proving (i).

Assuming (vi), we have $0 = N(x)^2$ by (33a.18), whence (iv). Assuming (iv), since $0 = N(x)x = x^{\sharp\sharp}$, either $x^\sharp = 0$ or $y := x^\sharp \neq 0$ and $y^\sharp = 0$. □

39.18 Feierlich, Misterioso: enter Albert algebras. By an *Albert algebra* over k we mean a Freudenthal k-algebra having rank 27 as a projective k-module.

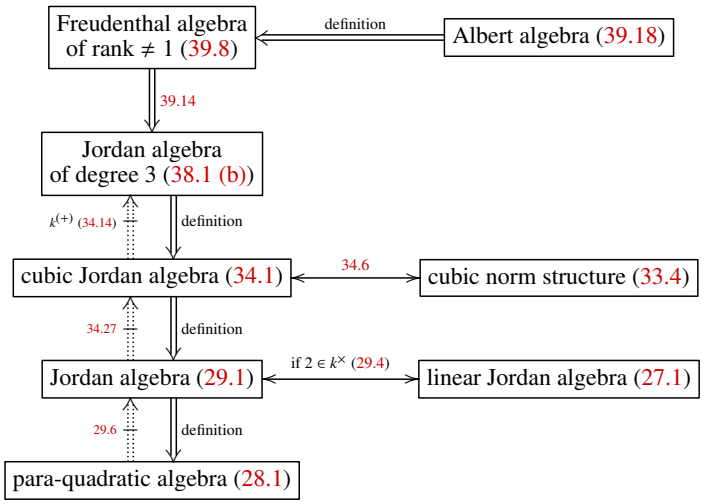


Figure 39a Diagram showing relationships between different kinds of algebras related to Albert algebras. The symbol ↔ denotes an equivalence of categories.

39.19 Examples and elementary properties of Albert algebras.

(a) Let (C, Γ) be a co-ordinate pair over k. Then $\mathrm{Her}_3(C, \Gamma)$ is an Albert algebra if and only if C is an octonion algebra. A particularly important example is the euclidean Albert algebra $\mathrm{Her}_3(\mathbb{O})$ over the reals from 5.5.

(b) By Corollaries 39.14 and 39.15, Albert algebras are regular Jordan algebras of degree 3.

(c) Albert algebras are stable under base change.

(d) If J is an Albert k-algebra, then so is the isotope $J^{(p)}$, for any $p \in J^\times$.

We are now ready for a definition that mimics the one for split composition algebras in 21.19.

39.20 Split Freudenthal algebras. In the uninteresting case where k is the zero ring, $J = \{0\}$ is a Freudenthal algebra which we say is split. Let us now define the notion of being split for a Freudenthal algebra J over a ring $k \neq \{0\}$. Define

$$J_{0n}(k) := \begin{cases} k^{(+)} & \text{for } n = 1, \\ (k \times k \times k)^{(+)} & \text{for } n = 3, \\ \mathrm{Her}_3(k) = \mathrm{Sym}_3(k) & \text{for } n = 6, \\ \mathrm{Her}_3(k \times k) & \text{for } n = 9, \\ \mathrm{Her}_3(\mathrm{Mat}_2(k)) = \mathrm{Symp}_3(k) & \text{for } n = 15, \\ \mathrm{Her}_3(\mathrm{Zor}(k)) & \text{for } n = 27; \end{cases} \tag{1}$$

which we call the *standard split Freudenthal algebra of rank n* over k. Note that

$$J_{0n}(k)_R = J_{0n}(R) \qquad (n \in \mathbb{N}_{\mathrm{Fr}},\ R \in k\text{-}\mathbf{alg}). \tag{2}$$

We say that a Freudenthal algebra J is *split of rank n* if it is isomorphic to $J_{0n}(k)$. More generally, we say that J is merely *split* if, in the rank decomposition (39.12.3), each J_n is split of rank n. Note that the property of a Freudenthal algebra to be split (resp. split of rank $n \in \mathbb{N}_{\mathrm{Fr}}$) is stable under base change.

Our principal aim in the present section will be to show that Freudenthal algebras are split by some fppf extension, which in addition we may choose to be étale most of the time, e.g., for Albert algebras. Our method of proof mimics the one we have employed to derive the analogous result for composition algebras in Cor. 26.9.

39.21 Strong co-ordinate systems. By a *strong co-ordinate system* of a cubic Jordan algebra J over k we mean a quintuple $\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31})$ such that (e_1, e_2, e_3) is an elementary frame in J, inducing the corresponding Peirce decomposition $J = \sum(ke_i + J_{jl})$, and $u_{23} \in J_{23}$, $u_{31} \in J_{31}$ satisfy

$$S(u_{23}) = S(u_{31}) = -1. \tag{1}$$

Thanks to Prop. 37.6, this is equivalent to saying that e_j and e_l, for $i = 1, 2$, are strongly connected by u_{jl}. In particular, strong co-ordinate systems are ordinary ones.

Now let $(J, \mathfrak{S})$ be a *strongly co-ordinated cubic Jordan algebra* over k, i.e., a cubic Jordan k-algebra J together with a strong co-ordinate system

$$\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31})$$

of J, the corresponding Peirce decomposition being indicated by $J = \sum(ke_i + J_{jl})$. Then Prop. 37.15 and (1) imply that $C_{J,\mathfrak{S}} = J_{12}$ becomes a multiplicative conic alternative k-algebra whose multiplication, norm, bilinearized norm, unit element, linear trace and conjugation are respectively given by

$$uv = (u \circ u_{23}) \circ (u_{31} \circ v) = (u \times u_{23}) \times (u_{31} \times v), \tag{2}$$

$$n_C(u) = -S(u), \tag{3}$$

$$n_C(u,v) = T(u,v), \tag{4}$$

$$1_C = u_{12} := u_{23} \circ u_{31} = u_{23} \times u_{31}, \tag{5}$$

$$t_C(u) = T(u_{12}, u), \tag{6}$$

$$\bar{u} = T(u_{12}, u)u_{12} - u \tag{7}$$

for all $u, v \in C$. Moreover, the Jacobson co-ordinatization theorem 37.17 yields an isomorphism

$$\phi_{J,\mathfrak{S}} \colon \operatorname{Her}_3(C) \xrightarrow{\sim} J$$

matching the diagonal co-ordinate system of $\operatorname{Her}_3(C)$ with $\mathfrak{S}$ and satisfying

$$\phi_{J,\mathfrak{S}}\Big(\sum(\xi_i e_{ii} + v_i[jl])\Big) = \sum(\xi_i e_i + v_{jl}) \tag{8}$$

for all $\xi_i \in k$, $v_i \in C$, $1 \le i \le 3$, where

$$v_{23} = u_{31} \times \bar{v}_1, \quad v_{31} = u_{23} \times \bar{v}_2, \quad v_{12} = v_3. \tag{9}$$

39.22 Splitting data for Freudenthal algebras. Let J be a Freudenthal algebra over k having rank $n \in \mathbb{N}_{\mathrm{Fr}}$ as a projective module. We define the notion of a *splitting datum* for J by considering the following cases.

(a) $n = 1$. Then $J \cong k^{(+)}$, and a *splitting datum* for J by definition has the form $\Sigma = (1_J)$.

(b) $n = 3$. Then $J \cong E^{(+)}$ is cubic étale, and a *splitting datum* for J by definition has the form $\Sigma = (e_1, e_2, e_3)$ and is an elementary frame of J.

(c) $n > 3$. Then a *splitting datum* for J by definition has the form $\Sigma = (\mathfrak{S}, \Delta)$ such that the following conditions hold.

(i) $\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31})$ is a strong co-ordinate system of J, with the Peirce decomposition $J = \sum(ke_i + J_{jl})$ relative to the elementary frame (e_1, e_2, e_3) of J.

Since J is a Freudenthal algebra, hence separable, it follows from Exc. 39.38 below that the multiplicative conic alternative algebra $C = C_{J,\mathfrak{S}}$ of 39.21 is, in fact, a composition algebra, of rank $r = \frac{n-3}{3}$.

(ii) Δ is a splitting datum for C in the sense of 26.2.

In summary, splitting data for J belong to J^{m_n}, where $m_n \in \mathbb{N}$ is defined by the following table.

n	1	3	6	9	15	27
m_n	1	3	6	6	8	9

Moreover, as in 26.2, splitting data are preserved by isomorphisms and are stable under base change. Finally, the set of all splitting data for J will be denoted by

$$\mathrm{Splid}(J) := \{\Sigma \mid \Sigma \text{ is a splitting datum for } J\} \subseteq J^{m_n}. \tag{1}$$

39.23 Setting the stage. Until further notice, we fix a Freudenthal algebra J over k having rank $n \in \mathbb{N}_{\mathrm{Fr}}$ as a projective module. As usual, we abbreviate $1 = 1_J$, $\sharp = \sharp_J$, $\times = \times_J$, $N = N_J$, $T = T_J$, $S = S_J$. The notational conventions of 39.22 remain in force.

39.24 The affine scheme of splitting data for J. Prop. 37.4 implies that $(e_1, e_2, e_3) \in J^3$ is an elementary frame of J if and only if

$$e_i^\sharp = 0, \quad T(e_i) = 1, \quad e_1 \times e_2 = e_3 = 1 - e_1 - e_2 \qquad (i = 1, 2). \tag{1}$$

Similarly, (37.5.2) and 39.21 imply that $\mathfrak{S} = (e_1, e_2, e_3, u_{23}, u_{31}) \in J^5$ is a strong co-ordinate system of J if and only if (1) and

$$T(u_{jl}) = 0, \quad e_j \times u_{jl} = e_l \times u_{jl} = 0, \quad S(u_{jl}) = -1 \qquad (i = 1, 2) \tag{2}$$

hold. These observations will simplify the task of characterizing the splitting data for J (and all its scalar extensions) by finitely many equations. Letting $R \in k$-**alg** be arbitrary, we treat the different ranks separately.

(a) $n = 1$. Then $\Sigma = (s \cdot 1_{J_R})$ for $s \in R$ is a splitting datum for J_R if and only if

$$s = 1_R \tag{3}$$

holds.

(b) $n = 3$. Then $\Sigma = (e_1, e_2, e_3) \in J_R^3$ is a splitting datum for J_R if and only if (1) holds.

(c) $n = 6$. Then $r = 1$, and

$$\Sigma = (e_1, e_2, e_3, u_{23}, u_{31}, u_{12}) \in J_R^6 \tag{4}$$

is a splitting datum for J_R if and only if (1), (2) and

$$u_{12} = u_{23} \times u_{31} \tag{5}$$

hold.

(d) $n = 9$. Then $r = 2$, and

$$\Sigma = (e_1, e_2, e_3, u_{23}, u_{31}, e_{12}) \in J_R^6 \tag{6}$$

is a splitting datum for J_R if and only if (1), (2) and

$$T(e_{12}) = S(e_{12}) = 0, \quad T(u_{23} \times u_{31}, e_{12}) = 1, \quad e_1 \times e_{12} = e_2 \times e_{12} = 0 \tag{7}$$

hold.

(e) $n = 15$. Then $r = 4$, and

$$\Sigma = (e_1, e_2, e_3, u_{23}, u_{31}, e_{12}, v_{12}, w_{12}) \in J_R^8 \tag{8}$$

is a splitting datum for J_R if and only if (1), (2), (7) and

$$T(v_{12}) = T(w_{12}) = 0, \quad e_1 \times v_{12} = e_2 \times v_{12} = e_1 \times w_{12} = e_2 \times w_{12} = 0, \tag{9}$$

$$(e_{12} \times u_{23}) \times (u_{31} \times v_{12}) = 0, \quad (v_{12} \times u_{23}) \times (u_{31} \times e_{12}) = v_{12}, \tag{10}$$

$$(e_{12} \times u_{23}) \times (u_{31} \times w_{12}) = w_{12}, \quad (w_{12} \times u_{23}) \times (u_{31} \times e_{12}) = 0, \tag{11}$$

$$T(u_{23} \times u_{31}, (v_{12} \times u_{23}) \times (u_{31} \times w_{12})) = 1_R \tag{12}$$

hold.

(f) $n = 27$. Then $r = 8$, and

$$\Sigma = (e_1, e_2, e_3, u_{23}, u_{31}, e_{12}, v_{12}, w_{12}, z_{12}) \in J_R^9 \tag{13}$$

is a splitting datum for J_R if and only if (1), (2), (7), (9), (10) and

$$(e_{12} \times u_{23}) \times (u_{31} \times w_{12}) = (e_{12} \times u_{23}) \times (u_{31} \times z_{12}) = 0, \tag{14}$$

$$(w_{12} \times u_{23}) \times (u_{31} \times e_{12}) = w_{12}, \quad (z_{12} \times u_{23}) \times (u_{31} \times e_{12}) = z_{12}, \tag{15}$$

$$T\Big(u_{23} \times u_{31}, \big([(v_{12} \times u_{23}) \times (u_{31} \times w_{12})] \times u_{23}\big) \times (u_{31} \times z_{12})\Big) = -1_R \tag{16}$$

hold.

Summing up, we therefore conclude that the natural selections (depending on $n \in \mathbb{N}_{\mathrm{Fr}}$) from the equations (1)–(3), (5), (7), (9)–(12), (14)–(16) define a closed, hence affine, subscheme of $J_{\mathbf{a}}^{m_n} = (J^{m_n})_{\mathbf{a}} = (J_{\mathbf{a}})^{m_n}$ in the sense of 24.15, denoted by $\mathbf{Splid}(J)$ and called the *affine scheme of splitting data* for J. By definition we have

$$\mathbf{Splid}(J)(R) = \mathrm{Splid}(J_R) := \{\Sigma \mid \Sigma \text{ is a splitting datum for } J_R\} \tag{17}$$

for all $R \in k$-**alg** and

$$\begin{aligned} \mathbf{Splid}(J)(\varphi)\colon \mathbf{Splid}(J)(R) &\longrightarrow \mathbf{Splid}(J)(S), \\ \mathrm{Splid}(J_R) \ni \Sigma &\longmapsto \Sigma_S = (\mathbf{1}_{J^{m_n}} \otimes \varphi)(\Sigma) \in \mathrm{Splid}(J_S) \end{aligned} \tag{18}$$

for all morphisms $\varphi\colon R \to S$ in k-**alg**.

39.25 Standard splitting data. Here we present explicit examples of splitting data for the standard split Freudenthal algebras $J_0 := J_{0n}(k)$ of 39.20. Up to a point, we will have to treat the different values of n separately.

(a) $n = 1$. Then $J_0 = k^{(+)}$, and

$$\Sigma_0 := \Sigma_{01}(k) = (1) \tag{1}$$

is the only splitting datum for J_0.

(b) $n = 3$. Then $J_0 = (k \times k \times k)^{(+)}$, and

$$\Sigma_0 := \Sigma_{03}(k) = ((1,0,0),(0,1,0),(0,0,1)) \tag{2}$$

is a splitting datum for J_0.

(c) $n > 3$. Then $J_0 := J_{0n}(k) = \mathrm{Her}_3(C_0)$, $C_0 := C_{0r}(k)$, $r = \frac{n-3}{3}$. With the diagonal co-ordinate system

$$\mathfrak{S}_0 := \mathfrak{S}_{0n}(k) = \mathfrak{D}(C_0, \mathbf{1}_3) = (e_{11}, e_{22}, e_{33}, 1_{C_0}[23], 1_{C_0}[31]) \tag{3}$$

of $J_0 = \mathrm{Her}_3(C_0)$ in the sense of 37.11, we use Example 37.16 to identify $C_0 = C_{J_0,\mathfrak{S}_0}$ via $u = u[12]$ for all $u \in C_0$. Then

$$\Sigma_0 := \Sigma_{0n}(k) = (\mathfrak{S}_0, \Delta_0) \tag{4}$$

is a splitting datum for J_0, where $\Delta_0 = \Delta_{0r}(k)$ is the standard splitting datum for C_0 in the sense of 26.4. The splitting datum $\Sigma_{0n}(k)$, $n \in \mathbb{N}_{\mathrm{Fr}}$, exhibited above will henceforth be referred to as the *standard splitting datum* for $J_{0n}(k)$. We clearly have $\Sigma_{0n}(k)_R = \Sigma_{0n}(R)$ for all $R \in k$-**alg**.

39.26 Proposition. *The affine k-scheme of splitting data for J is finitely presented and has non-empty geometric fibers. Moreover, it is smooth unless $n = 6$ and 2 is not invertible in k.*

Proof Equations (39.24.1)–(39.24.16) show that $\mathbf{X} := \mathbf{Splid}(J)$ is defined by finitely many equations as a closed subscheme of $J_{\mathbf{a}}^{m_n}$. By Exercises 25.31 and 25.33, therefore, $\mathbf{X}$ is finitely presented. If $K \in k$-**alg** is an algebraically closed field, then splitting data for J_K exist (39.25) since J_K is split by Cor. 39.7. Thus $\mathbf{X}$ has non-empty geometric fibers. Under the assumption $n \neq 6$ or $2 \in k^\times$, it remains to show that $\mathbf{X}$ is smooth. For $R \in k$-**alg** and an ideal $I \subseteq R$ satisfying $I^2 = \{0\}$, we have to prove that the set map $\mathbf{X}(R) \to \mathbf{X}(R/I)$ is surjective. We may clearly assume $R = k$, write $\alpha \mapsto \bar{\alpha}$, $x \mapsto \bar{x}$ for the natural projections $k \to \bar{k} := k/I$, $J \to \bar{J} := J/IJ = J_{\bar{k}}$, respectively, and let Σ' be a splitting datum for $\bar{J}$. We wish to find a splitting datum Σ for J having $\bar{\Sigma} = \Sigma'$. The case $n = 1$ being

obvious, by 39.22, we may assume $n > 1$. Then the cases we have excluded and Cor. 39.15 guarantee that J is regular. If $n = 3$, then $J = E^{(+)}$ is cubic étale and Σ' is an elementary frame of $\bar{J}$, which by Exercises 32.25 and 37.21 (b) can be lifted to an elementary frame, i.e., a splitting datum for J. We are left with the case $n > 3$. Then $\Sigma' = (\mathfrak{S}', \Delta')$, where $\mathfrak{S}' = (e'_1, e'_2, e'_3, u'_{23}, u'_{31})$ is a strong co-ordinate system for $\bar{J}$ and Δ' is a splitting datum for the composition algebra $C' = C_{\bar{J},\mathfrak{S}'}$ over $\bar{k}$. Note by Prop. 37.15 that $C' = J'_{12}$ as $\bar{k}$-modules, where $\bar{J} = \sum(\bar{k}e'_i + J'_{jl})$ is the Peirce decomposition of $\bar{J}$ relative to the elementary frame (e'_1, e'_2, e'_3). As before, we can lift (e'_1, e'_2, e'_3) to an elementary frame (e_1, e_2, e_3) of J, with Peirce decomposition $J = \sum(ke_i + J_{jl})$, and then have $\bar{J}_{jl} := (J_{jl})_{\bar{k}} = J'_{jl}$ for $1 \le i \le 3$. In addition, for $i = 1, 2$, the quantities $u'_{jl} \in J'_{jl}$ can be lifted to elements $v_{jl} \in J_{jl}$ such that there exist $\alpha_{jl} \in I$ satisfying

$$S(v_{jl}) = -1 + \alpha_{jl}. \tag{1}$$

Thus $\mathfrak{T} := (e_1, e_2, e_3, v_{23}, v_{31})$ is a co-ordinate system of J satisfying $\bar{\mathfrak{T}} = \mathfrak{S}'$, but possibly not a strong one. This deficiency will be removed by a slight modification of $\mathfrak{T}$ that may be described as follows. If $2 \in k^\times$, we put $u_{jl} := (1 + \frac{\alpha_{jl}}{2})v_{jl}$ and obtain $S(u_{jl}) = -1$ by (1). Hence $\mathfrak{S} := (e_1, e_2, e_3, u_{23}, u_{31})$ is a lift of $\mathfrak{S}'$ to a strong co-ordinate system of J. To accomplish the same for an arbitrary base ring, our assumptions allow us to assume $n \ge 9$, whence C' is a composition algebra of rank $r \ge 2$ over $\bar{k}$. By the same token, $D := C_{J,\mathfrak{T}}$ is a composition algebra of rank r over k, and in the notation of Prop. 37.15, we have $\omega_{J,\mathfrak{T}} = S(v_{23})^{-1}S(v_{31})^{-1} = (1 + \alpha_{23})(1 + \alpha_{31})$, hence

$$\omega_{J,\mathfrak{T}} = 1 + \alpha, \quad \alpha = \alpha_{23} + \alpha_{31} \in I. \tag{2}$$

This and (37.15.3) imply $\bar{D} := D/ID = D_{\bar{k}} = C'$. But C', admitting Δ' as a splitting datum, is split and thus contains an elementary idempotent c', which in turn can be lifted to an elementary idempotent $c \in D$. Setting $c_1 := 1_D - c = u_{12} - c$ and

$$v_{12} := c + (1 + \alpha_{31} + \alpha)c_1 \in J_{12}, \quad u_{23} := v_{31} \times v_{12} \in J_{23}, \tag{3}$$

we apply (37.14.6), (37.15.4), (1), (2) to obtain

$$\begin{aligned} S(u_{23}) &= -S(v_{31})S(v_{12}) = (-1 + \alpha_{31})(1 - \alpha)n_D(c + (1 + \alpha_{31} + \alpha)c_1) \\ &= (-1 + \alpha_{31})(1 - \alpha)(1 + \alpha_{31} + \alpha) = (-1 + \alpha_{31} + \alpha)(1 + \alpha_{31} + \alpha) \\ &= -1, \end{aligned}$$

while $\bar{v}_{12} = 1_{C'} = u'_{12} = u'_{23} \times u'_{31}$, and (3), (37.14.2) yield

$$\bar{u}_{23} = u'_{31} \times (u'_{31} \times u'_{23}) = -S(u'_{31})u'_{23} = u'_{23}.$$

Similar computations, using

$$w_{12} := c + (1 + \alpha_{23} + \alpha)c_1 \in J_{12}, \quad u_{31} := w_{12} \times v_{23} \in J_{31} \tag{4}$$

instead of the quantities in (3) imply $S(u_{31}) = -1$ and $\bar{u}_{31} = u'_{31}$. Summing up, therefore, $\mathfrak{E} := (e_1, e_2, e_3, u_{23}, u_{31})$ is a strong co-ordinate system of J lifting $\mathfrak{E}'$. As before $C := C_{J,\mathfrak{E}}$ is a composition algebra of rank r over k having $\bar{C} = C/IC = C_{\bar{k}} = C'$. Since the affine k-scheme of splitting data for C by Prop. 26.5 is smooth, the splitting datum Δ' for C' can be lifted to a splitting datum Δ of C. Hence $\Sigma := (\mathfrak{E}, \Delta)$ is a splitting datum for J lifting Σ'. □

39.27 Splittings of Freudenthal algebras. By a *splitting* of a Freudenthal algebra J we understand an isomorphism

$$J_{0n}(k) \xrightarrow{\sim} J$$

of cubic Jordan algebras, which by Cor. 39.13 is the same as an isomorphism of abstract Jordan algebras. Extending canonically terminology and notation of 26.6 from linear non-associative algebras to para-quadratic ones, the set of splittings of J is $\mathrm{Isom}(J_{0n}(k), J)$.

Some Freudenthal algebras of rank 6 have been excluded from Prop. 39.26. The following result is the crucial step towards a substitute for this deficiency.

39.28 Proposition. *Let J be a Freudenthal k-algebra of rank 6 and $E \subseteq J$ a cubic étale subalgebra. Then there exist an fppf algebra $R \in k$-**alg** and a splitting $J_{0n}(R) \xrightarrow{\sim} J_R$ matching E_R with the diagonal of $J_{0n}(R)$.*

Proof Note by 25.19 (v) (resp. 25.3 (i) and 25.15 (b)) that the top of a tower of étale covers (resp. fppf algebras) is an étale cover of (resp. fppf over) the base ring. Up to an fppf base change we may therefore assume that E (hence J) contains an elementary frame $\Omega = (e_1, e_2, e_3)$ (Thm. 38.6), so $E = \sum ke_i$ and $J = \sum(ke_i + J_{jl})$ in terms of the corresponding Peirce decompositions. We let $\mathfrak{p} \subseteq k$ be any prime ideal. By 39.8 (iii), the cubic Jordan algebra $J(\mathfrak{p})$ over the field $k(\mathfrak{p})$ is simple, and Prop. 39.2 implies that $\Omega(\mathfrak{p})$ can be extended to a co-ordinate system of $J(\mathfrak{p})$, so there are elements $u_{jl} \in J_{jl\mathfrak{p}}$ for $i = 1, 2$ having $S(u_{jl}(\mathfrak{p})) \in k(\mathfrak{p})^\times$, hence $S(u_{jl}) \in k_\mathfrak{p}^\times$. By (37.13.1) and (37.14.2), the assignment $x \mapsto u_{23} \times x$ gives a linear bijection $J_{31\mathfrak{p}} \to J_{12\mathfrak{p}}$. Thus the off-diagonal Peirce components relative to $\Omega_\mathfrak{p}$ are all different from zero, and counting ranks we conclude that the J_{jl} are all line bundles over k. Combining 25.5 (ii) with 25.19 (iii)–(v), we find an étale cover of k making J_{jl} free of rank 1 for $i = 1, 2, 3$. In particular, up to an fppf base change, we may assume that the J_{jl} themselves are free of rank 1. Let $e_{jl} \in J_{jl}$ for $i = 1, 2$ be a basis vector. Then $u_{jl} = \alpha_i e_{jl\mathfrak{p}}$ for some $\alpha_i \in k_\mathfrak{p}$, and $S(u_{jl}) \in k_\mathfrak{p}^\times$ implies $S(e_{jl})_\mathfrak{p} = S(e_{jl\mathfrak{p}}) \in k_\mathfrak{p}^\times$.

Since $\mathfrak{p} \in \operatorname{Spec}(k)$ is arbitrary, we conclude $S(e_{jl}) \in k^\times$, so (Ω, e_{23}, e_{31}) is a co-ordinate system of J. Now the Jacobson co-ordinatization theorem 37.17 shows $J \cong \operatorname{Her}_3(C, \Gamma)$ for some diagonal matrix $\Gamma \in \mathrm{GL}_3(k)$ with diagonal entries γ_i, $1 \le i \le 3$. Then

$$R = k[\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3]/(\mathbf{t}_1^2 - \gamma_1, \mathbf{t}_2^2 - \gamma_2, \mathbf{t}_3^2 - \gamma_3) \cong \bigotimes_{i=1}^{3} k[\mathbf{t}_i]/(\mathbf{t}_i^2 - \gamma_i) \in k\text{-}\mathbf{alg}$$

is free of rank 6 as a k-module and hence fppf. We have $J_R \cong \operatorname{Her}_3(R, \Gamma_R)$, and the diagonal entries γ_{iR} of Γ_R by construction are all squares in $R^\times$. Now Exc. 37.22 (b) (ii) implies that $J_R \cong \operatorname{Her}_3(R)$ is split over R. □

39.29 Corollary. *Every Freudenthal k-algebra J of rank 6 is split by some fppf algebra $R \in k$-**alg**.*

Proof After an appropriate étale cover of k, Exc. 39.42 (a) allows us to assume that J contains an elementary frame, say (e_1, e_2, e_3). Now Prop. 39.28 applies to J and $E := \sum k e_i$. □

39.30 Proposition. *Let J be a Freudenthal algebra of constant rank n over k and denote by $\Sigma_{0n}(k)$ the standard splitting datum for $J_{0n}(k)$ as defined in 39.25. Then the assignment*

$$\psi \longmapsto \psi(\Sigma_{0n}(k))$$

defines a bijection $\Theta = \Theta(k)$ from the set of splittings of J onto the set of splitting data for J:

$$\Theta := \Theta(k)\colon\ \operatorname{Isom}(J_{0n}(k), J) \xrightarrow{\sim} \operatorname{Splid}(J).$$

Proof The assertion is trivial for $n = 1$ and straightforward to verify for $n = 3$. We may therefore assume $n \ge 6$. Then $J_0 := J_{0n}(k) = \operatorname{Her}_3(C_0)$, $C_0 := C_{0r}(k)$, $r = \frac{n-3}{3}$, and $\Sigma_0 := \Sigma_{0n}(k) = (\mathfrak{S}_0, \Delta_0)$, where $\mathfrak{S}_0$ is the diagonal co-ordinate system $(e_{11}, e_{22}, e_{33}, 1_{C_0}[23], 1_{C_0}[31])$ of J_0 and Δ_0 is the standard splitting datum for C_0, the latter being identified with $C_{J_0,\mathfrak{S}_0} \subseteq J_0$ via Example 37.16. Injectivity of Θ will now follow once we have shown that J_0', the cubic subalgebra of J generated by $\mathfrak{S}_0 \cup \Delta_0$, is all of J_0. The diagonal $\sum k e_{ii}$ of J_0 clearly belongs to J_0'. Moreover, since the algebra structure of C_0 by (39.21.2) is built up from the bilinearized adjoint and $\Delta_0 \subseteq C_0$ by Prop. 26.7 generates C_0 as a unital k-algebra, $C_0 = C_0[12]$ is contained in J_0'. Hence so are $C_0[23] = 1_{C_0}[31] \times C_0[12]$, $C_0[31] = 1_{C_0}[23] \times C_0[12]$, and we conclude $J_0' = J_0$. It remains to show that Θ is surjective, so let $\Sigma = (\mathfrak{S}, \Delta)$ be any splitting datum for J. Setting $C := C_{J,\mathfrak{S}}$, the Jacobson co-ordinatization theorem,

specialized to the case at hand in 39.21, yields an isomorphism

$$\phi = \phi_{J,\mathfrak{S}} \colon \operatorname{Her}_3(C) \xrightarrow{\sim} J$$

as described in (39.21.8), (39.21.9), matching the diagonal co-ordinate system of $\operatorname{Her}_3(C)$ with $\mathfrak{S}$. On the other hand, the splitting datum Δ of C by Prop. 26.7 yields an isomorphism $\eta \colon C_0 \to C$ sending Δ_0 to Δ. Hence

$$\phi \circ \operatorname{Her}_3(\eta) \colon J_0 \xrightarrow{\sim} J$$

is an isomorphism of the desired kind. □

39.31 Theorem. *Let J be a Freudenthal algebra of constant rank n over k. Then the k-functor*

$$\mathbf{Isom}(J_{0n}(k), J)$$

is a torsor in the flat topology with structure group $\mathbf{G} := \mathbf{Aut}(J)$. Moreover,

$$\mathbf{Isom}(J_{0n}(k), J)$$

is a smooth torsor in the étale topology with structure group $\mathbf{G}$ if $n \neq 6$ or $2 \in k^\times$.

Proof Putting $\mathbf{X} := \mathbf{Isom}(J_{0n}(k), J)$, the set maps

$$\Theta(R) \colon \mathbf{X}(R) \xrightarrow{\sim} \mathbf{Splid}(J)(R),$$

given by Prop. 39.30 for any $R \in k$-**alg** are bijective and easily checked to vary functorially with R, hence they give rise to an isomorphism

$$\Theta \colon \mathbf{X} \xrightarrow{\sim} \mathbf{Splid}(J)$$

of k-functors whose target, by Prop. 39.26, is a finitely presented affine k-scheme acted upon by $\mathbf{G}$ from the right in a simply transitive manner (26.6 (b)). Therefore the same is true for the k-functor $\mathbf{X}$, and the first part of the theorem for $n = 6$ follows from Cor. 39.29. For the rest of the proof, we may therefore assume $n \neq 6$ or $2 \in k^\times$. By Prop. 39.26, $\mathbf{X}$ along with $\mathbf{Splid}(J)$ is smooth with non-empty geometric fibers, hence fppf by Prop. 25.24, so this part of the theorem follows from 25.25 (ii). □

39.32 Corollary. *Let J be a para-quadratic k-algebra in the sense of 28.1. Then the following conditions are equivalent.*

(i) *J is a Freudenthal algebra over k.*

(ii) *There exists a faithfully flat $R \in k$-**alg** such that J_R is a Freudenthal algebra over R.*

(iii) *There exists a faithfully flat $R \in k$-**alg** such that J_R is a split Freudenthal algebra over R.*

(iv) *There exists an fppf $R \in k$-**alg** such that J_R is a split Freudenthal algebra over k.*

If J is finitely generated projective as a k-module such that either its rank function avoids the number 6 or $2 \in k^\times$, then these conditions are also equivalent to

(v) *There exists an étale cover $R \in k$-**alg** such that J_R is a split Freudenthal algebra over R.*

39.33 Corollary. *Let J be a Freudenthal algebra over k and assume that, either, (i) $2 \in k^\times$ or (ii) its rank function (as a projective module) avoids the number 6. Then $\mathbf{Aut}(J)$ is a smooth k-group scheme.*

Proof of 39.32 and 39.33 Since finitely generated projective modules are stable under faithfully flat descent (see 25.5), we may assume that J is finitely generated projective as a k-module. Then the implications (v) $\Rightarrow$ (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) of 39.32 are obvious. It therefore remains to show (ii) $\Rightarrow$ (i) $\Rightarrow$ (iv) (resp. (ii) $\Rightarrow$ (i) $\Rightarrow$ (v) if the additional hypotheses immediately preceding (v) are fulfilled).

(ii) $\Rightarrow$ (i). Since the property of $R \in k$-**alg** to be faithfully flat is stable under base change (25.2) we may assume that J has (finite) rank n as a projective k-module. The case $n = 1$ is obvious, so let us assume $n \geq 3$. For any $S \in R$-**alg**, Cor. 39.14 implies that the base change $J_S = (J_R)_S$ has degree 3 over S and so allows a *unique* cubic form making J_S a cubic Jordan algebra (Thm. 38.13). By faithfully flat descent (Exc. 25.35), therefore, J is a cubic Jordan algebra over k. Let $K \in k$-**alg** be any field. By Exc. 9.26, there exists a field $L \in R$-**alg** that is also an extension field of K. By definition, $(J_R)_L = J_L = (J_K)_L$ is simple or cubic étale, whence so is J_K, and we have shown that J is a Freudenthal algebra over k.

(i) $\Rightarrow$ (iv) (resp. (i) $\Rightarrow$ (v) if the additional hypotheses immediately preceding (v) are fulfilled). The proofs of these implications, as well as those of Cor. 39.33, follow almost verbatim the corresponding ones of the analogous implications of Cor. 26.9, as well as Cor. 26.10. Details are left to the reader as an easy exercise. □

Here is a particularly important special case of Cor. 39.32. If J is a paraquadratic algebra over k and there is a faithfully flat $R \in k$-**alg** such that J_R is an Albert algebra over R, then J is an Albert algebra over k. We restate this as:

39.34 Corollary. *Albert algebras are stable under faithfully flat descent.* □

39.35 Example. We give an example of a rank 6 Freudenthal algebra that is not split by any étale cover of the base ring.

Let k be a field of characteristic 2 and suppose $\gamma \in k^\times$ is not a square. For $\alpha \in \{1, \gamma\}$ put $J_\alpha := \mathrm{Her}_3(k, \mathrm{diag}(1, 1, \alpha))$ and note that $J_1 = J_{06}(k)$ is split. Writing T_α (resp. S_α) for the bilinear (resp. quadratic) trace of J_α, we denote by $\mathrm{Rad}(S_\alpha, T_\alpha)$ the radical of the quadratic form $S_\alpha|_{\mathrm{Rad}(T_\alpha)}$, which is an invariant of J_α since isomorphisms of Freudenthal algebras preserve bilinear and quadratic traces. We also put $\delta_\alpha = \dim_k(\mathrm{Rad}(S_\alpha, T_\alpha))$. From (36.4.7) we deduce $\mathrm{Rad}(T_\alpha) = \sum k[jl]$, while (36.4.11) implies that $S_\alpha|_{\mathrm{Rad}(T_\alpha)}$ bilinearizes to zero. Hence

$$\mathrm{Rad}(S_\alpha, T_\alpha) = \{x \in \mathrm{Rad}(T_\alpha) \mid S_\alpha(x) = 0\}.$$

On the other hand, by (36.4.9),

$$S(\sum \alpha_i[jl]) = \alpha(\alpha_1^2 + \alpha_2^2) + \alpha_3^2 = \alpha(\alpha_1 + \alpha_2)^2 + \alpha_3^2 \quad (\alpha_i \in k,\ 1 \le i \le 3),$$

and since γ is not a square in k, we conclude

$$\delta(J_\alpha) = \begin{cases} 1 & \text{for } \alpha = \gamma, \\ 2 & \text{for } \alpha = 1. \end{cases} \tag{1}$$

Now let K be any finite-dimensional separable extension of k. We still have $\gamma \in K^\times \setminus K^{\times 2}$ since adjoining a square root of γ to k yields a purely inseparable quadratic extension. From (1) we therefore deduce $\delta(J_{\gamma K}) \neq \delta(J_{1K})$, so $J_{\gamma K}$ and J_{1K} cannot be K-isomorphic. In other words, we have $\mathbf{Isom}(J_{06}(k), J_\gamma)(K) = \emptyset$ and Prop. 25.28 implies that $\mathbf{Isom}(J_{06}(k), J_\gamma)(R)$ is empty for all étale covers R of k. In particular, $\mathbf{Isom}(J_{06}(k), J_\gamma)$ is a torsor in the flat topology but not in the étale topology.

39.36 An alternative definition of Freudenthal algebra. It is possible to give an equivalent definition of Freudenthal algebra in the elementary language of para-quadratic algebras from 28.1 as follows. The split Freudenthal algebras listed in 39.20 have explicit U-operators in the case $k = \mathbb{Z}[\frac{1}{2}]$ defined as in 27.10. The formulas for these U-operators do not involve any denominators, not even a 2 (by direct inspection as in 37.7 or Exc. 36.11, or a fortiori from the construction via cubic norm structures) and so make sense also for $k = \mathbb{Z}$, and in this way we define a split Freudenthal $\mathbb{Z}$-algebra. For a ring k, we define a split Freudenthal k-algebra as follows. Write $k = \prod k_i$ where each k_i is a ring. A para-quadratic k-algebra $J = \prod J_i$, where each J_i is a para-quadratic k_i-algebra, is a split Freudenthal algebra if J_i is obtained from a split Freudenthal $\mathbb{Z}$-algebra by base change. As in [95, 7.1] we could say that a para-quadratic

k-algebra J is a Freudenthal algebra if J_R is a split Freudenthal R-algebra for some faithfully flat $R \in k$-**alg**.

Note by Cor. 39.32 that a para-quadratic algebra is a Freudenthal algebra in the sense of 39.8 if and only if it is a Freudenthal algebra in this sense.

The definition presented in this remark has the advantage of requiring very little machinery. However, it has the disadvantage that it is tiresome to compute with, because one does not have the convenience of the cubic norm structure machinery. For our purposes, this disadvantage is decisive.

Exercises

39.37. Let M, N be finitely generated projective modules over k. Show that a linear map $\varphi\colon M \to N$ is bijective if and only if the base change $\varphi_K\colon M_K \to N_K$ is bijective for all fields $K \in k$-**alg**. Conclude that a cubic Jordan algebra J over k that is finitely generated projective as a k-module is regular if and only if the bilinear trace T_K of J_K, for any field $K \in k$-**alg**, is a non-degenerate symmetric bilinear form.

39.38. Let (C,Γ) be a co-ordinate pair over k in the sense of 36.3. Prove that the cubic Jordan algebra $J := \mathrm{Her}_3(C,\Gamma)$ is separable if and only if C is a composition algebra.

39.39. Let C be a conic alternative algebra without zero divisors over k that is finitely generated projective as a k-module. Fixing a diagonal matrix $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{Mat}_3(k)$ and

$$x = \sum (\alpha_i e_{ii} + v_i[jl]) \in J \qquad (\alpha_i \in F, \quad v_i \in C, \quad 1 \le i \le 3),$$

consider the following conditions on x.

(i) $x^\sharp = 0$.
(ii) $\alpha_j\alpha_l = \gamma_j\gamma_l n_C(v_i)$ for $i = 1,2,3$ and $\gamma_1\gamma_2\gamma_3 v_1(v_2v_3) = \alpha_1\alpha_2\alpha_3 1_C$.
(iii) $\alpha_j\alpha_l = \gamma_j\gamma_l n_C(v_i)$ *and*

$$\gamma_1\gamma_2\gamma_3(v_iv_j)v_l = \alpha_1\alpha_2\alpha_3 1_C = \gamma_1\gamma_2\gamma_3 v_i(v_jv_l)$$

for $i = 1,2,3$.

Prove that the implications

$$\text{(i)} \Longrightarrow \text{(ii)} \Longrightarrow \text{(iii)}$$

hold. Moreover, if k is an integral domain and $\gamma_i \neq 0$ for $1 \le i \le 3$, show that all three conditions are equivalent.

39.40. Let $f : M \to M'$ be a k-linear map of k-modules and $N, P \subseteq M$, $N' \subseteq M'$ be arbitrary k-submodules. Let $R \in k$-**alg** be a flat k-algebra, recall the conventions of 25.3 and prove:

(a) $f(N)_R = f_R(N_R)$, $\quad f^{-1}(N')_R = f_R^{-1}(N'_R)$.

(b) $(N \cap P)_R = N_R \cap P_R$.

(c) For every family $(N_\alpha)_{\alpha\in I}$ of k-submodules in M we have

$$(\sum_{\alpha\in I} N_\alpha)_R = \sum_{\alpha\in I}(N_\alpha)_R.$$

(d) If N is generated as a k-module by a family $(x_\alpha)_{\alpha\in I}$ of elements in M, then N_R is generated as an R-module by the family $(x_{\alpha R})_{\alpha\in I}$ of elements in M_R.

39.41. *Ideals in Freudenthal algebras* ([95, Thm. 8.2]). Let J be a Freudenthal algebra of rank $n \in \mathbb{N}_{\mathrm{Fr}}$ over k.

(a) Show that the submodule of J spanned over k by the squares in J is all of J. (*Hint*: Denote this submodule by $\mathrm{Sq}(J)$, prove $\mathrm{Sq}(J_R) = \mathrm{Sq}(J)_R$ for all flat k-algebras $R \in k$-**alg** and apply Cor. 39.32.)

(b) If J is regular of rank $n \geq 6$, identify $k = k1_J \subseteq J$ canonically and deduce from (a) that the assignments

$$\mathfrak{a} \longmapsto \mathfrak{a}J, \quad I \longmapsto I \cap k$$

define inclusion preserving inverse bijections between the ideals of k and the outer ideals of J. (*Hint*: Apply (a), Exc. 37.26 and again Cor. 39.32.) In particular, outer ideals in J are ideals.

39.42. (a) Let J be a cubic Jordan k-algebra that is finitely generated projective as a k-module and satisfies the condition

$$\dim_K (J/\operatorname{Nil}(J_K)) \geq 3$$

for all algebraically closed fields $K \in k$-**alg**. Show that the subfunctor $\mathbf{Elfr}(J) \subseteq J^3_{\mathbf{a}}$ defined by

$$\mathbf{Elfr}(J)(R) := \{\Omega \mid \Omega \text{ is an elementary frame in } J_R\}$$

for all $R \in k$-**alg** is a closed subscheme that is smooth and fppf. Conclude that there exists an étale cover R of k such that J_R contains an elementary frame. (*Hint*: Argue as in the proof of Thm. 38.6 and, at a critical stage, apply Hilbert's Nullstellensatz.)

(b) Let J be a regular cubic Jordan k-algebra having rank 3 as a projective k-module. Prove that J is cubic étale in the sense of Example 34.17. More precisely: there exists a unique cubic commutative associative k-algebra E such that $E^{(+)} = J$ as cubic Jordan algebras, and this algebra is cubic étale.

39.43. Let J be a Freudenthal algebra of rank $r \geq 6$ over k.

(a) Let $e \in J$ be an elementary idempotent and

$$x = \xi e + x_1 + x_0, \quad \xi \in k,\ x_i \in J_i(e),\ i = 0, 1.$$

be the Peirce decomposition of $x \in J$ relative to e. Show that

$$U_x e = \xi^2 e + \xi x_1 + U_{x_1} x_0, \quad U_{x_1} x_0 \in J_0(e). \tag{1}$$

(b) ([95, Example 7.4]) Show for $x \in J$ that $U_x = \mathbf{1}_J$ implies $x = \xi 1_J$ for some $\xi \in k^\times$ with $\xi^2 = 1$.

40 Isotopy, norm similarity, and isomorphism

We introduce in this section a notion for cubic Jordan algebras called norm similarity, which we discover is mostly the same as isotopy (Cor. 40.5). We furthermore study isotopy and isomorphism classes of Freudenthal algebras in the special case of an LG ring (Thm. 40.10).

40.1 Round forms. Round quadratic forms were introduced by Witt (unpublished, [296, pp. 35–39]) and turned out to be a useful tool in the study of Pfister quadratic forms [72, §9]. The concept allows a straightforward extension to scalar polynomial laws, as we now illustrate.

Let $f\colon M \to k$ and $g\colon N \to k$ (with k-modules M, N) be scalar polynomial laws over our base ring k. A *morphism* from f to g is a linear map $\varphi\colon M \to N$ such that $f = g \circ \varphi$ as polynomial laws over k. In this way, we obtain the category of scalar polynomial laws over k. Thus f and g are isomorphic, written as $f \cong g$, if and only if a *bijective* linear map $\varphi\colon M \to N$ exists having $f = g \circ \varphi$.

Given a scalar polynomial law f as above, we may define two subsets of $k^\times$:

$$G_f := \{\mu \in k^\times \mid \mu f \cong f\}.$$

and

$$D_f := \{\mu \in k^\times \mid \exists m \in M \text{ such that } f(m) = \mu\}.$$

There are some easy relationships between the two. For example, *if* $1 \in D_f$, *then* $G_f \subseteq D_f$.

We say that f is *round* if $G_f = D_f$. For example, this holds when M is a multiplicative conic alternative algebra (e.g., a composition algebra) and f is its norm. In that case, for every invertible element $y \in M$, we have $f(y) \in k^\times$ (Prop. 17.5), $f(xy) = f(x)f(y)$ for every $x \in M_R$, $R \in k$-**alg**, and right multiplication by y is bijective (Prop. 13.6), so $f(y)$ belongs to G_f, showing that f is round.

40.2 Lemma. *The norm of a cubic Jordan algebra is round.*

Proof Put J for the cubic Jordan algebra and N for its norm. Let $\mu \in k^\times$ be such that there is an $x \in J$ with $N(x) = \mu$. Then x is invertible (Cor. 33.10) and we define $\phi := \mu U_{x^{-1}}$. By (33.8.21), $N \circ \phi = \mu^3 N(x^{-1})^2 N = \mu N$, so $\mu \in G_N$. □

40.3 Example. Let $J = \mathrm{Her}_3(C, \Gamma)$ be a cubic Jordan matrix algebra in the sense of 36.6. For each $\mu \in k^\times$, the element $x := \mu e_{11} + e_{22} + e_{33} \in J$ satisfies $N_J(x) = \mu$. Therefore, $N_J \cong \mu N_J$ by the lemma.

40.4 Lemma. *Let J, J' be cubic Jordan algebras over k such that J is regular,*

its rank function does not take the value 2 *and* J' *is finitely generated projective as a* k*-module. A function* $\eta\colon J \to J'$ *is an isotopy if and only if* η *is an isomorphism of* k*-modules and there exists* $\mu(\eta) \in k^\times$ *such that* $N'_J \circ \eta = \mu(\eta) N_J$ *as polynomial laws over* k*.*

When these properties hold, $\mu(\eta)$ *is unique,* $\eta^\sharp$ *and* η^{-1} *are isotopies* $J' \to J$*, and we have for all* $x, y \in J$*:*

(i) $\mu(\eta^{-1}) = \mu(\eta)^{-1}$.
(ii) $\mu(\eta^\sharp) = \mu(\eta)$.
(iii) $(\eta(x))^{\sharp'} = \mu(\eta)\, \eta^{\sharp -1}(x^\sharp)$.
(iv) $T_{J'}(\eta(x), \eta^{\sharp -1}(y)) = T_J(x, y)$.

Proof The "only if" direction follows from Corollary 38.18 and (33.11.3), so we prove the "if" direction. Suppose $N_{J'} \circ \eta = \mu(\eta) N_J$ as polynomial laws over k, for some $\mu(\eta) \in k^\times$. Setting $u := \eta(1_J)$, we have $N_{J'}(u) = \mu(\eta)$, so u is invertible and $\mu(\eta)$ is unique. Write J'' for the isotope $J'^{(u^{-1})}$ of J', which has the same underlying k-module as J', so we may view η also as a linear map $J \to J''$. For $x \in J$ we have

$$N_{J''}(\eta(x)) = N_{J'}(\eta(x)) N_{J'}(u^{-1}) = N_J(x)$$

by (33.10.1). Also, u is the identity element in J'' by (33.11.1), so η is an isomorphism $J \to J''$ of cubic Jordan algebras by Exc. 34.18 (b). Since J'' was constructed to be isotopic to J', the claim follows.

So suppose η is an isotopy. The fact that η^{-1} is an isotopy follows from Prop. 31.18 (d). Moreover, for $x' \in J'$,

$$\mu(\eta)^{-1} N_{J'}(x') = N_J(\eta^{-1}(x')),$$

verifying (i).

We observed in Cor. 31.21 that $\eta^\sharp$ is an isotopy. We have

$$\mu(\eta^\sharp) = N_J(\eta^\sharp(1_{J'})),$$

so (31.19.2) implies

$$\mu(\eta^\sharp) = N_J(\eta^{-1} U_{\eta(1_J)} 1_{J'}) = \mu(\eta)^{-1} N_{J'}(\eta(1_J))^2 = \mu(\eta).$$

For (iii), we note that $\eta\colon J \to J'' = J'^{(u^{-1})}$, being an isomorphism of cubic Jordan algebras, preserves adjoints, and (33.11.2) implies

$$\eta(x^\sharp) = \eta(x)^{(\sharp', u^{-1})} = N_{J'(u)}^{-1} U_u \eta(x)^{\sharp'},$$

hence $\eta(x)^{\sharp'} = \mu(\eta) U^{-1}_{\eta(1_J)} \eta(x^\sharp) = \mu(\eta) \eta^{\sharp -1}(x^\sharp)$ by Prop. 31.19; we have verified (iii).

For (iv), the isomorphism $\eta\colon J \to J''$ preserves bilinear traces, and (33.11.4) combined with (31.19.2) yields

$$T_J(x,y) = T_{J''}(\eta(x),\eta(y)) = T_{J'}(\eta(x), U_{\eta(1_J)^{-1}}\eta(y)) = T_{J'}(\eta(x), \eta^{\sharp -1}(y)),$$

proving (iv). □

For a regular cubic Jordan algebra J, a *norm similarity* is an element $\phi \in \mathrm{GL}(J)$ such that $N_J \circ \phi = \mu N_J$ for some $\mu \in k^\times$. In this language, the lemma says that the structure group $\mathrm{Str}(J)$ defined in 31.20 is the group of norm similarities of J.

One says that $\phi \in \mathrm{GL}(J)$ is a *norm isometry* if $N_J \circ \phi = N_J$. The collection of norm isometries is a normal subgroup of $\mathrm{Str}(J)$, which we denote by $\mathrm{Inv}(J)$. The automorphism group $\mathrm{Aut}(J)$ of J is itself a normal subgroup of $\mathrm{Inv}(J)$, namely the subgroup of elements that stabilize 1_J by Thm. 31.22 and Exc. 34.18 (b).

40.5 Corollary. *Let J, J' be cubic Jordan algebras over k such that J is regular, its rank function does not take the value 2, and J' is finitely generated projective as a k-module. The following are equivalent:*

(i) *J and J' are isotopic.*
(ii) *There is a $\mu \in k^\times$ such that $N_J \cong \mu N_{J'}$.*
(iii) *$N_J \cong N_{J'}$.*

Proof Lemma 40.4 proves that (i) is equivalent to (ii), which is trivially implied by (iii). Suppose (ii) and let $\phi\colon J' \to J$ be a k-module isomorphism so that $N_J \circ \phi = \mu N_{J'}$. Then $N_J(\phi(1_{J'})) = \mu N_{J'}(1_{J'}) = \mu$, so by Lemma 40.2 we have $\mu N_J \cong N_J \cong \mu N_{J'}$ and we conclude (iii). □

For every co-ordinate pair (C,Γ) over k, $\mathrm{Her}_3(C,\Gamma)$ is isotopic to $\mathrm{Her}_3(C)$ by Exc. 37.23, so the corollary says that the isomorphism class of the cubic form $N_{\mathrm{Her}_3(C,\Gamma)}$ depends only on C and not on Γ, provided C is a regular composition algebra.

The following gives a case where the conclusion is about isomorphism.

40.6 Proposition. *Let C be a split composition k-algebra of constant rank $r > 1$. Then $\mathrm{Her}_3(C,\Gamma)$ and $\mathrm{Her}_3(C)$ are diagonally isomorphic in the sense of Exc. 37.22 (b), for every diagonal matrix $\Gamma \in \mathrm{GL}_3(k)$.*

Proof Write $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3)$. We may assume $\gamma_3 = 1$. For any $p,q \in C^\times$, we may apply (37.24.3) to conclude $\mathrm{Her}_3(C,\Gamma) \cong \mathrm{Her}_3(C^{(p,q)},\Gamma')$, where $\Gamma' = \mathrm{diag}(n_C(p)\gamma_1, n_C(q)\gamma_2, 1)$. If $r \le 4$, then C is associative, so $C^{(p,q)} \cong C$ by 15.1, 15.2, and since the norm of C, being hyperbolic, is surjective, there are $p,q \in$

$C^\times$ such that $\Gamma' = \mathbf{1}_3$, hence $\mathrm{Her}_3(C,\Gamma) \cong \mathrm{Her}_3(C)$ diagonally. On the other hand, if $r = 8$, then C, being split, contains a split quaternion subalgebra B, whose norm, therefore, is hyperbolic. Thus we find $p, q \in B^\times$ having $\Gamma' = \mathbf{1}_3$. Moreover, by Exc. 19.31, $C^{(p,q)} \cong C$, and the assertion follows. □

40.7 Remark. For a (split) composition algebra C of rank 1, in which case $\mathrm{Her}_3(C,\Gamma)$ has rank 6, the conclusion of the proposition may fail because $\mathrm{Her}_3(\mathbb{R}, \mathrm{diag}(1,-1,-1))$ is isotopic to the split Freudenthal algebra $\mathrm{Her}_3(\mathbb{R})$ but is not isomorphic to it, thanks to the following result.

40.8 Corollary. *If J is a Freudenthal algebra over $\mathbb{R}$ then, up to isomorphism, it is one of the following algebras.*

(a) $\mathbb{R}^{(+)}$,

(b) $E^{(+)}$ *for* $E = \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ *or* $\mathbb{R}\times\mathbb{C}$,

(c) $\mathrm{Her}_3(\mathbb{R})$, $\mathrm{Her}_3(\mathbb{R}, \mathrm{diag}(1,-1,1))$,

(d) *For each of the dimensions* $d = 2, 4, 8$ *of a composition algebra* C*:*

$$\begin{cases} \mathrm{Her}_3(C) & \text{for } C \text{ split or division of dimension } d; \\ \mathrm{Her}_3(C, \mathrm{diag}(1,-1,-1)) & \text{for } C \text{ a division algebra of dimension } d. \end{cases}$$

That is, there are 14 isomorphism classes of Freudenthal algebras over $\mathbb{R}$, of which 3 are Albert algebras, namely

$$\mathrm{Her}_3(\mathrm{Zor}(\mathbb{R})), \quad \mathrm{Her}_3(\mathbb{O}), \quad \textit{and} \quad \mathrm{Her}_3(\mathbb{O}, \mathrm{diag}(1,-1,-1)).$$

Proof Let J be a Freudenthal algebra over $\mathbb{R}$. If J is of dimension 1 then $J \cong \mathbb{R}^{(+)}$ and we have (a). Otherwise, J is of dimension ≥ 3 (Cor. 39.11) and of degree 3 (Cor. 39.14). If J is a division algebra then for any $x \in J$, $\mathbb{R}[x]$ is a finite field extension of $\mathbb{R}$ (Example 31.39 (a)). Since there are x's of degree 3 this leads to a contradiction. If J is of dimension 3 it is of the form $\mathbb{R}e \times J_0(e)$ for e an elementary idempotent. If $J_0(e)$ contains an elementary idempotent then $J \cong \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ is split. Otherwise $J_0(e)$ is a division algebra and $J_0(e) \cong \mathbb{C}^{(+)}$. So we have (b).

For higher dimensions $J \cong \mathrm{Her}_3(C,\Gamma)$ for some composition algebra C by Prop. 39.17. By Exercise 37.22 (b), the isomorphism class of $\mathrm{Her}_3(C,\Gamma)$ does not change if (i) Γ is multiplied by an invertible scalar or (ii) each diagonal entry of Γ is multiplied by an invertible square. By (ii) we may assume $\gamma_i = \pm 1$. By (i), multiplying by -1 and permuting the elements of the frame if necessary, we may assume that $\Gamma = \mathrm{diag}(1, s, s)$ for $s = \pm 1$.

If J has rank 6, it is isomorphic to (at least) one of the algebras in (c) because $\mathbb{R}$ is the only possibility for C. If J has rank 9, 15, or 27 and C is split, then J

is $\mathrm{Her}_3(C)$ by Prop. 40.6, and it follows that J is one of the algebras listed in (d).

It remains to show that the algebras listed in (c) and (d) are pairwise non-isomorphic. Consider the bilinear trace T_J, whose formula appeared in (36.4.7). Since we are only considering here the case $k = \mathbb{R}$, it suffices to compute the signature. The $\xi_i\eta_i$ terms contribute a total of 3 to the signature of the form and the $\gamma_j\gamma_l n_C$ terms contribute $(1 + 2s)$ times the signature of n_C.

Write 2^r for the dimension of C. If C is split, then n_C has signature 0 and T has signature 3. If C is division and $s = 1$, then T has signature $3(1+2^r)$. If C is division and $s = -1$, then T has signature $3 - 2^r$. For $r = 1$, we find signatures 9 and 1, so the two algebras in (c) are not isomorphic. For $r = 2, 4, 8$, the three values given for the signature of T are distinct, and we conclude that the three exhibited algebras for that r are pairwise non-isomorphic. □

To review what has come before: The isotopy class of $\mathrm{Her}_3(C, \Gamma)$ depends only on C and not on Γ. Our next aim is to study those algebras that are isotopic to one of the form $\mathrm{Her}_3(C, \Gamma)$, see Theorem 40.10 below. The crux of the proof is a detailed study of the isometries of the norm of $\mathrm{Her}_3(C)$, for which we need the following examples.

40.9 Examples. (1) Let $J = \mathrm{Her}_3(C)$, $\{i, j, l\} = \{1, 2, 3\}$ and $(i\,j)$ be the transposition of $\{1, 2, 3\}$ interchanging i and j. The transposition matrix $M_{(i\,j)} := e_{ll} + e_{ij} + e_{ji} = e_{ll} + 1_C[ij]$ belongs to J. For any transposition π of $\{1, 2, 3\}$, $N_J(M_\pi) = -1$ and U_{M_π} is a norm preserving map. Using the identities 36.4 and 37.7, one checks that $U_{M_\pi}(\alpha_i e_{ii}) = \alpha_i e_{\pi(i)\pi(i)}$ and $U_{M_\pi}(a_i[jl]) = a_i[\pi(j)\pi(l)]$. Since U_{M_π} fixes 1_J, it is an automorphism of J. In the proof of Lemma 40.11 below, we will abuse notation and denote the transformation $U_{M_{(i\,j)}}$ simply by $(i\,j)$.

(2) Let $J = \mathrm{Her}_3(C, \Gamma)$, C any composition algebra, and let $x = \sum_i \xi_i e_{ii} + \sum_{i\neq j} \gamma_j u_{ij} e_{ij} \in J$, $\xi_i \in k$, $u_{ji} = \overline{u_{ij}} \in C$.

We will need some norm preserving maps of J described over fields of characteristic not 2 in [134, §5] (which credits them to Freudenthal) and over $\mathbb{Z}$ in [165, §2]. For $c \in C$, $d \in k[c] \subseteq C$ and $\{q, r, s\} = \{1, 2, 3\}$, we claim that *the value of the matrix product*

$$(\mathbf{1}_3 + \gamma_s d e_{rs})(\mathbf{1}_3 + \gamma_s c e_{rs})x(\mathbf{1}_3 + \gamma_r \bar{c} e_{sr})(\mathbf{1}_3 + \gamma_r \bar{d} e_{sr}) \tag{1}$$

is independent of the order in which we perform the multiplications. Indeed, by linearity in x, we may assume $x \in ke_{ii}$ or $x \in C[jl]$ for some $i = 1, 2, 3$. In either case, all factors in the above product belong to $\mathrm{Mat}_3(B)$, where $B \subseteq C$ is a unital subalgebra generated by two elements and hence, thanks to Artin's theorem (Cor. 14.5 or Exc. 17.10), is associative.

Now consider

$$\begin{aligned}
&(\mathbf{1}_3 + \gamma_s c e_{rs}) x (\mathbf{1}_3 + \gamma_r \bar{c} e_{sr}) \\
&\quad = (x + \gamma_s \xi_s c e_{rs} + \gamma_s \gamma_r c u_{sr} e_{rr} + \gamma_s \gamma_q c u_{sq} e_{rq})(\mathbf{1}_3 + \gamma_r \bar{c} e_{sr}) \\
&\quad = x + \gamma_s \xi_s c e_{rs} + \gamma_s \gamma_r c u_{sr} e_{rr} + \gamma_s \gamma_q c u_{sq} e_{rq} \\
&\qquad + \gamma_r \xi_s \bar{c} e_{sr} + \gamma_r \gamma_s u_{rs} \bar{c} e_{rr} + \gamma_r \gamma_s u_{qs} \bar{c} e_{qr} + \gamma_r \gamma_s \xi_s n_C(c) e_{rr} \\
&\quad = x + \gamma_r \gamma_s (n_C(u_{rs}, c) + \xi_s n_C(c)) e_{rr} + \xi_s (\gamma_s c e_{rs} + \gamma_r \bar{c} e_{sr}) \\
&\qquad + \gamma_s (\gamma_q c u_{sq} e_{rq} + \gamma_r u_{qs} \bar{c} e_{qr}).
\end{aligned}$$

So $(\mathbf{1}_3 + \gamma_s c e_{rs}) x (\mathbf{1}_3 + \gamma_r \bar{c} e_{sr}) \in \mathrm{Her}_3(C, \Gamma)$. We denote this element by $\nu_{(r,s,c)}(x)$ and so obtain a k-linear map $\nu_{(r,s,c)} \colon J \to J$. Note that the ss, qq, sq and qs entries of x are left fixed. Using $(\mathbf{1}_3 + \gamma_s c e_{rs})(\mathbf{1}_3 - \gamma_s c e_{rs}) = \mathbf{1}_3$, we deduce from (1) that $\nu_{(r,s,c)} \nu_{(r,s,-c)} = \mathbf{1}_J = \nu_{(r,s,-c)} \nu_{(r,s,c)}$. Letting

$$\begin{aligned}
y = \gamma_r \gamma_s (n_C(u_{rs}, c) + \xi_s n_C(c)) e_{rr} + \xi_s (\gamma_s c e_{rs} + \gamma_r \bar{c} e_{sr}) \\
+ \gamma_s (\gamma_q c u_{sq} e_{rq} + \gamma_r u_{qs} \bar{c} e_{qr}),
\end{aligned}$$

we have by (36.4.5), $N(y) = 0$ and by (36.4.4),

$$y^\sharp = -\xi_s^2 \gamma_r \gamma_s n(c) e_{qq} - \gamma_s^2 \gamma_r \gamma_q n(c) n(u_{sq}) e_{ss} + \xi_s \gamma_r \gamma_s n(c) (\gamma_q u_{sq} e_{sq} + \gamma_s u_{qs} e_{qs}).$$

By (33.2.4), (33.4.2), $N(\nu_{(r,s,c)}(x)) = N(x) + T(x^\sharp, y) + T(x, y^\sharp)$ where

$$\begin{aligned}
T(x^\sharp, y) &= (\xi_s \xi_q - \gamma_s \gamma_q n_C(u_{sq})) \gamma_r \gamma_s (n_C(u_{rs}, c) + \xi_s n_C(c)) \\
&\quad + \gamma_r \gamma_s n_C(-\xi_q u_{rs} + \gamma_q \overline{u_{sq} u_{qr}},\ \xi_s c) \\
&\quad + \gamma_q \gamma_r n_C(-\xi_s u_{qr} + \gamma_s \overline{u_{rs} u_{sq}},\ \gamma_s \overline{c u}_{sq}) \\
&= \xi_s^2 \xi_q \gamma_r \gamma_s n_C(c) - \xi_s \gamma_r \gamma_s^2 \gamma_q n_C(c) n_C(u_{sq}),
\end{aligned}$$

using (17.1.2), (17.1.3), Prop. 16.12 (4), (5). By (36.4.7),

$$T(x, y^\sharp) = -\xi_s^2 \xi_q \gamma_r \gamma_s n_C(c) - \xi_s \gamma_r \gamma_s^2 \gamma_q n_C(c) n_C(u_{sq}) + \xi_s \gamma_r \gamma_s^2 \gamma_q n_C(c) n_C(u_{sq}, u_{sq}).$$

Since $n_C(u_{sq}, u_{sq}) = 2 n_C(u_{sq})$, $N(\nu(r,s,c)(x)) = N(x)$ and $N_J \nu_{(r,s,c)} = N_J$. So $\nu_{(r,s,c)}$ is a norm-preserving map. Note that we are *not* assuming that (r, s, q) is a cyclic permutation of $(1, 2, 3)$.

40.10 Theorem. *Suppose J is a Jordan k-algebra that is isotopic to $\mathrm{Her}_3(C, \Gamma)$ for some regular composition algebra C and some $\Gamma \in \mathrm{GL}_3(k)$. If k is an LG ring, then J is isomorphic to $\mathrm{Her}_3(C, \Gamma')$ for some $\Gamma' \in \mathrm{GL}_3(k)$.*

Proof As in previous proofs, we reduce to the case where C has finite constant rank. In view of Exc. 37.23, J is isotopic to $\mathrm{Her}_3(C)$, i.e., $J \cong \mathrm{Her}_3(C)^{(u^{-1})}$ for some invertible $u \in \mathrm{Her}_3(C)$. The same exercise shows we are done if u is diagonal.

We will apply successive elements $\eta \in \mathrm{Inv}(\mathrm{Her}_3(C))$. Note that each such η defines an isomorphism of k-modules

$$\eta\colon\ \mathrm{Her}_3(C)^{(u^{-1})} \to \mathrm{Her}_3(C)^{(\eta(u)^{-1})}, \tag{1}$$

which is an isotopy by Lemma 40.4 and Prop. 31.18 (b) sending the unit element of its domain to the unit element of its range, hence is an isomorphism (Prop. 31.18 (a)). Thus, the following lemma suffices to complete the proof of the theorem. We state it separately because it may be of independent interest. □

40.11 Lemma. *If C is a regular composition algebra over an LG ring k, then for $J := \mathrm{Her}_3(C)$, every $\mathrm{Inv}(J)$-orbit of $J^\times$ contains a diagonal element.*

Proof As in other proofs, we reduce to the case where C has constant rank. Let $x = \sum_i \alpha_i e_{ii} + c_i[jl] \in J^\times$ for $\alpha_i \in k$ and $c_i \in C$. Our aim is to find elements of $\mathrm{Inv}(J)$ that transform x to eliminate the c_i terms.

1°. Suppose first that $\alpha_1 \in k^\times$. We claim that after modifying x by an element of $\mathrm{Inv}(J)$, we may assume that $c_2 = c_3 = 0$.

For $b \in C$, the element $\nu_{(2,1,b)}(x)$ has top row entries α_1, $c_3 + \alpha_1\bar{b}$, $\bar{c}_2$. Taking $b = -\bar{c}_3\alpha_1^{-1}$, we may assume that x has $\alpha_1 \in k^\times$ and $c_3 = 0$.

The same calculation, now with $\nu_{(3,1,b)}(x)$, allows us to zero out the c_2 entry.

2°. If $\alpha_1, \alpha_2 \in k^\times$ and $c_2 = c_3 = 0$, then the same argument as in the previous step, now with $\nu_{(3,2,b)}(x)$, allows us to zero out also the c_1 entry, The resulting element is then diagonal, which would complete the proof.

3°. Now suppose that k is a field.

If some $\alpha_i \neq 0$, then we may employ a permutation transformation as in Example 40.9(1) to arrange $\alpha_1 \neq 0$. Otherwise, $\alpha_i = 0$ for all i, then $0 \neq N(x) = t_C(c_1c_2c_3)$, so $c_3 \neq 0$. Since n_C is regular, some $b \in C$ has $n_C(b, c_3) \neq 0$. Replacing x with $\nu_{(1,2,b)}(x)$, we may assume that $\alpha_1 \neq 0$.

Applying step 1, we may assume that $c_2 = c_3 = 0$. If $\alpha_2 \neq 0$, then we are done by step 2. If $\alpha_3 \neq 0$, then we may apply a permutation transformation to arrange that $\alpha_2 \neq 0$, and we are again done.

Finally, if $\alpha_2 = \alpha_3 = 0$, we have $0 \neq N(x) = -\alpha_1 n_C(c_3)$, so $c_3 \neq 0$. The element $\nu_{(2,3,b)}(x)$, for b chosen by the same method as at the start of step 1, is diagonal, completing the proof in the case where k is a field.

4°. Finally, suppose that k is an LG ring. For $b_1, b_2, b_3 \in C$, define elements of $\mathrm{Inv}(J)$:

$$\nu_3(b_1, b_2, b_3) := \nu_{(3,1,b_1)}\nu_{(2,1,b_2)}\nu_{(1,2,b_3)} \quad \text{and} \quad \nu_2(b_1, b_2) := \nu_{(3,2,b_1)}\nu_{(2,3,b_2)}.$$

Note that $\nu_3(0,0,0) = \nu_2(0,0) = \mathbf{1}_J$. We combine the transformations ν_3, ν_2, and permutations together into a function $C^{21} \to \mathrm{Inv}(J)$, namely

$$(\nu_2\,(2\,3)\,\nu_2\nu_3\,(1\,3))\,(\nu_2\,(2\,3)\,\nu_2\nu_3\,(1\,3))\,(\nu_2\,(2\,3)\,\nu_2\nu_3) \tag{1}$$

where the arguments to the various ν_2, ν_3 are assigned independently. Combining this with the polynomial function that sends $g \in \mathrm{Inv}(J)$ to the $(1,1)$-entry of gx, we obtain a polynomial law $C^{21} \to k$. But more is true. Because k is LG and C is projective of constant rank, C is a free module, see Prop. 11.24. Choosing a basis for C expresses this polynomial law as a polynomial with coefficients in k.

We claim that this polynomial represents a unit over every $F \in k$-**alg**. For a given F, here is how to pick the element of C^{21} that produces a unit by picking the arguments of the transformation (1). If all α_i are zero, we apply the rightmost $\nu_{(1,2,*)}$ transformation in the rightmost instance of ν_3 to arrange $\alpha_1 \neq 0$. Otherwise, we plug 0 into this $\nu_{(1,2,*)}$ to obtain the identity in that term. (Here is a first branch point.) If, after this step, $\alpha_1 \neq 0$, we apply the other two terms in the rightmost ν_3 to arrange that $c_2 = c_3 = 0$ as in step 1. If $\alpha_2 = \alpha_3 = 0$, we apply the rightmost $\nu_{(2,3,*)}$ transformation in the rightmost instance of ν_2 to arrange $\alpha_2 \neq 0$. (Here is a second branch point.) If, after this step, $\alpha_2 \neq 0$, then we apply the $\nu_{(3,2,*)}$ term of the rightmost ν_2 to arrange that x is diagonal as in step 2. In this case we plug zeros in for the remaining ν_2 and ν_3 terms in (1). The remaining terms of (1), the permutation transformations, only rearrange the diagonal entries of x and therefore do not change the property that the $(1,1)$-entry is a unit.

However, at the second branch point, it may occur that $\alpha_2 = 0$ but $\alpha_3 \neq 0$. In that case, we plug zeros into the rightmost ν_2 in (1). After the permutation $(2\,3)$, we have $\alpha_2 \neq 0$ and may follow the original plan at the second branch point.

However, at the first branch point, it may occur that $\alpha_1 = 0$ but $\alpha_2 \neq 0$ or $\alpha_3 \neq 0$. If $\alpha_2 \neq 0$, then after applying the rightmost terms $(1\,3)\nu_2(2\,3)\nu_2\nu_3$ to x, we have arrived at the situation where $\alpha_1 \neq 0$ and we may follow the first branch point. If $\alpha_3 \neq 0$, we may apply all but the leftmost $\nu_2(2\,3)\nu_2\nu_3$ to arrange that $\alpha_1 \neq 0$, and again we may follow the first branch point.

We have verified the claim, and therefore using the LG property of k we conclude that there is an element of $z \in C^{21}$ such that after plugging z into (1) and applying it to x, we may assume that $\alpha_1 \in k^\times$. Following step 1, we may further assume that $c_2 = c_3 = 0$.

Applying now an argument as in the preceding five paragraphs, with the

function

$$\nu_2\,(2\,3)\,\nu_2 \colon C^4 \to \mathrm{Inv}(J),$$

we conclude that we may transform x to further assume that α_2 is invertible, and therefore apply a transformation $\nu_{(3,2,b)}$ to transform it into a diagonal element, as required. □

Now that the proof of Theorem 40.10 is complete, we provide a consequence.

40.12 Corollary. *Suppose J is a Jordan algebra over an LG ring k. If J is isotopic to a split Freudenthal algebra whose rank does not take the value 6, then J is itself a split Freudenthal algebra.*

Proof Because J is isotopic to a Freudenthal algebra, it is itself a Freudenthal algebra. As in previous proofs, one is reduced to the case where J has constant rank, which is not 6. If J has rank 1 or 3, then isotopy is the same as isomorphism, so there is nothing to prove. In the remaining cases, the theorem and Prop. 40.6 give the claim. □

40.13 Remarks. (1) Corollary 40.12 does not hold for Albert algebras over every ring. Indeed, Alsaody proves in [14, Thm. 2.7] that there is a smooth $k \in \mathbb{C}$-**alg** and an Albert k-algebra J that is isotopic to the split Albert algebra but is not itself split. He also proves in ibid., Cor. 4.4, that there is a smooth $k \in \mathbb{R}$-**alg** and octonion k-algebras C, C' such that $\mathrm{Her}_3(C) \cong \mathrm{Her}_3(C')$ yet $n_C \not\simeq n_{C'}$.

(2) The material in this section is largely adapted from [95], where some of it appeared for the first time in the generality presented here. Lemma 40.11 for LG rings is of the same type as a theorem of Krutelevich for the split Albert algebra over $\mathbb{Z}$, see [165].

Exercises

40.14. *Spanning reduced cubic Jordan algebras by invertible elements.* Let F be a field and write J^0 for the space of trace-zero elements in a cubic Jordan algebra J over F.

(a) Let (C,Γ) be a co-ordinate pair over F and suppose C as a vector space over F is spanned by its invertible elements. Put $J := \mathrm{Her}_3(C,\Gamma)$ and prove that J^0 is spanned by $J^0 \cap J^\times$ as a vector space over F.

(b) Deduce from (a) that J^0, for any simple cubic Jordan algebra J over F, is spanned as a vector space over F by the invertible trace-zero elements of J. Conclude that J itself is spanned as a vector space over F by its invertible elements.

40.15. *Elements of rank one and two.* Let J be a cubic Jordan algebra over a field F.

An element $u \in J$ is said to have *rank* 1 (resp. *rank* 2) if $u^\sharp = 0 \neq u$ (resp. $u^\sharp$ has rank 1). Prove:

(a) The property of an element in J to have rank 1 (resp. 2) is stable under isotopy.

(b) If J is simple, an element in J has rank 1 (resp. 2) if and only if it is an elementary (resp. a co-elementary) idempotent in some isotope of J.

(c) If J is simple, then an elementary idempotent $e \in J$ can be extended to an elementary frame in J if and only if the linear trace of J does not vanish on $J_0(e)$.

(d) Let $K \supseteq F$ be a purely inseparable field extension of characteristic 2 and exponent at most 1. Put $J := \mathrm{Her}_3(K)$ over F and prove that

$$e := \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in J$$

is an elementary idempotent that cannot be extended to an elementary frame in J. Show further that

$$u := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in J$$

is an element of rank 2 that cannot be written as the sum of two elements of rank 1 in J.

(e) Let $F := \mathbb{F}_2$ be the field with two elements. What are the elements of rank 1 and the elementary idempotents in $J := \mathrm{Her}_3(F)$?

(f) If J is simple and not a division algebra, then the following conditions are equivalent.

(i) Every elementary idempotent of any isotope J' of J can be extended to an elementary frame of J'.

(ii) Every co-elementary idempotent of any isotope J' of J can be decomposed into the sum of two orthogonal elementary idempotents in J'.

(iii) Every element of rank 2 in J can be decomposed into the sum of two elements of rank 1.

(iv) J is regular.

Remarks. (1) The (easy) proof of (a) does not use that F is a field and so holds for cubic Jordan algebras over rings. However, in Lemma 56.5 we will exhibit an Albert algebra over $\mathbb{Z}$ that has no elementary idempotents yet is isotopic to an Albert algebra with an elementary frame.

(2) Combining part (f) with 39.3 allows us to conclude: *If J is a simple and regular cubic Jordan algebra over an algebraically closed field F, then* $\mathrm{Aut}(J)$ *acts transitively on the set of elementary idempotents in J.*

40.16. Let C be a regular composition algebra over an LG ring k. Prove: If every element of k is a square in k, then for $J := \mathrm{Her}_3(C)$, the group $\mathrm{Inv}(J)$ acts transitively on the set $\{x \in J \mid N_J(x) = 1\}$.

40.17. *Composition algebras and Freudenthal algebras over finite rings.* Prove:

(a) Freudenthal algebras of rank $n > 6$ over a *finite field* F are split or isomorphic to $\mathrm{Her}_3(K)$, where K is the unique quadratic field extension of F. (*Hint*: Compare 23.14.)
(b) Composition algebras of rank $r > 2$ and Freudenthal algebras of rank $n > 9$ over a *finite commutative ring* are split. (*Hint*: Reduce to the case of a finite field by Prop. 39.26.)

Remark. The hypothesis $n > 6$ in part (a) can be strengthened to $n \geq 6$, see Exc. 41.30 below.

40.18. Let J be a cubic Jordan algebra over k that is regular and the rank of J does not take the value 2. The map $\eta \mapsto \eta^{\sharp -1}$ is an automorphism of $\mathrm{Str}(J)$ of order 2, compare 31.20. Prove:

(a) If there is a $c \in k^\times$ such that $c^6 \neq 1$, then the automorphism is not inner, i.e., there is no $\phi \in \mathrm{Str}(J)$ such that $\phi\eta\phi^{-1} = \eta^{\sharp -1}$ for all $\eta \in \mathrm{Str}(J)$.
(b) If J is a Freudenthal algebra of rank ≥ 6, then (1) the subgroup of $\mathrm{Str}(J)$ of elements fixed by the automorphism is $\boldsymbol{\mu}_2(k)\,\mathrm{Aut}(J)$, for $\boldsymbol{\mu}_2$ the group scheme of 2nd roots of unity as defined in Exc. 25.41 and (2) the subgroup of $\mathrm{Inv}(J)$ of elements fixed by the automorphism is $\mathrm{Aut}(J)$.

41 Reduced Freudenthal algebras over fields

The present section is devoted to the classification of regular simple reduced Freudenthal algebras over arbitrary fields. This will be accomplished in Thm. 41.21 below by identifying certain quadratic forms associated with the quadratic trace in one way or another as classifying invariants. The idea of working with the quadratic trace instead of the bilinear one, which was used by Springer [264] but fails in characteristic 2, is due to Racine [242]. In applications, we study nilpotent elements of regular simple reduced Freudenthal algebras and the action of the group of norm similarities on the elements of rank 1.

Throughout this section, we let F be an arbitrary field.

41.1 The concept of a reduced Freudenthal algebra. A Freudenthal algebra over F is said to be *reduced* if it contains an elementary frame. By Cor. 39.11, a reduced Freudenthal algebra J over F either has dimension 3, in which case $J \cong (F \times F \times F)^{(+)}$ is split cubic étale (Cor. 39.16), or is simple (equivalently, has dimension at least 6), in which case it is isomorphic to $\mathrm{Her}_3(C, \Gamma)$, for some composition F-algebra C and some diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ (Prop. 39.17). Our first aim is to show that C is an isotopy invariant of J. To this end, we follow [72, Chap. II, §9] for a short digression into Pfister forms.

41.2 The concept of a Pfister form. Recall from 11.7 that $\langle \alpha_1, \ldots, \alpha_n \rangle$ for $n \in \mathbb{Z}$, $n > 0$, and $\alpha_1, \ldots, \alpha_n \in F$ is the symmetric bilinear form on F^n given

by the symmetric matrix $\operatorname{diag}(\alpha_1, \dots, \alpha_n)$. Furthermore, we recall from 11.13 that for an F-vector space V and a quadratic form $q\colon V \to F$, the natural identification $V \otimes F^n = V^n$ of vector spaces yields an identification

$$q \otimes \langle \alpha_1, \dots, \alpha_n \rangle = \alpha_1 q \perp \cdots \perp \alpha_n q \tag{1}$$

of quadratic forms, where the left-hand side of (1) is to be understood in the sense of Prop. 11.4.

Assuming $\alpha_i \in F^\times$ for $1 \le i \le n$, we put

$$\langle\!\langle \alpha_1, \dots, \alpha_n \rangle\!\rangle := \langle 1, -\alpha_1 \rangle \otimes \cdots \otimes \langle 1, -\alpha_n \rangle$$

as a regular symmetric bilinear form over F of dimension 2^n, which makes sense also for $n = 0$ by setting $\langle\!\langle\rangle\!\rangle := \langle 1 \rangle$. Bilinear forms of this type are called *Pfister bilinear forms*. By a *Pfister quadratic form*, or a *Pfister form* for short, we mean a quadratic form over F that is isometric to

$$n_K \otimes \langle\!\langle \alpha_1, \dots, \alpha_{n-1} \rangle\!\rangle, \tag{2}$$

for some quadratic étale F-algebra K, $n \in \mathbb{Z}$, $n > 0$, and $\alpha_1, \dots, \alpha_{n-1} \in F^\times$. More specifically, we call a quadratic form of the type displayed in (2) an *n-fold Pfister form* or just an *n-Pfister form*. Such forms have dimension 2^n. This is also true for $n = 0$ if we agree to call a quadratic form isometric to $\langle 1 \rangle_{\text{quad}}$ a 0-fold Pfister form. If $\operatorname{char}(F) \neq 2$, quadratic and symmetric bilinear forms over F are basically the same, and $\langle\!\langle \alpha_1, \dots, \alpha_n \rangle\!\rangle \cong n_K \otimes \langle\!\langle \alpha_1, \dots, \alpha_{n-1} \rangle\!\rangle$ with $K := F[\mathbf{t}]/(\mathbf{t}^2 - \alpha_n)$ is an n-Pfister form over F. It follows that in all characteristics, n-Pfister forms are regular if and only if (i) $n > 0$ or (ii) $n = 0$ and $\operatorname{char}(F) \neq 2$.

41.3 Examples of Pfister forms.

(a) The norm of F viewed as a composition F-algebra is $\langle 1 \rangle_{\text{quad}}$, hence a 0-fold Pfister form.

(b) Setting $n = 1$ in (41.2.2) we see that the norm of a quadratic étale F-algebra is a 2-fold Pfister form and conversely.

(c) If q is a regular m-Pfister form and $\alpha_1, \dots, \alpha_n \in F^\times$ for $m, n \in \mathbb{N}$, then $q \otimes \langle\!\langle \alpha_1, \dots, \alpha_n \rangle\!\rangle$ is an $(m+n)$-Pfister form.

(d) Let B be a conic F-algebra, $\mu \in F^\times$ and $C := \operatorname{Cay}(B, \mu)$ the corresponding Cayley-Dickson construction. We claim: *if n_B is an n-Pfister form for some integer $n > 0$, then n_C is an $(n+1)$-Pfister form*. Indeed, Remark 18.5 implies $n_C \cong n_B \otimes \langle\!\langle \mu \rangle\!\rangle$, and the assertion follows from (c).

(e) Since any composition F-algebra of dimension > 1 by Cor. 19.17 arises

from a quadratic étale subalgebra by means of the Cayley-Dickson process in the sense of 18.6, we deduce from (a)–(c) that *the norm of any composition F-algebra is a Pfister form.*

41.4 Properties of Pfister forms. n-fold Pfister forms for $n \in \mathbb{N}$ are

(a) stable under base field extensions;

(b) regular unless $n = 0$ and $\operatorname{char}(F) = 2$;

(c) round [72, Cor. 9.9]; and

(d) either anisotropic or hyperbolic [72, Cor. 9.10].

(e) Moreover, two regular n-fold Pfister forms are isometric if and only if they have the same splitting fields [72, Cor. 23.6], where a *splitting field* of a regular quadratic form over F is a field extension of F making the extended quadratic form hyperbolic.

The classification of reduced Freudenthal algebras over a field is in terms of the quadratic trace S_J. However, for technical reasons occurring in characteristic 2, we will need to also consider its restriction to the subspace J^0 of trace zero elements; we denote this restriction by S_J^0.

For a cubic Jordan algebra J, since $T_J(y, 1) = T_J(y)$, $F1_J$ and J^0 are orthogonal relative to the bilinear trace. It follows then by (33a.13) that $F1_J$ and J^0 are also orthogonal relative to the bilinearization DS_J of S_J.

41.5 Examples. (a) If $\operatorname{char}(F) \neq 3$, then every cubic Jordan algebra J has $S_J(1_J) = 3 \neq 0$, and therefore $1_J \notin J^0$, $J = F1_J \perp J^0$, and the relationship between S_J and S_J^0 takes the especially simple form $S_J \cong \langle 3 \rangle_{\text{quad}} \perp S_J^0$.

(b) For $E := (F \times F \times F)^{(+)}$, the form S_E^0 was calculated in Exercises 34.25 and 34.26. It is regular if and only if $\operatorname{char}(F) \neq 3$.

(c) For a co–ordinate pair (C, Γ), the algebra $J := \operatorname{Her}_3(C, \Gamma)$ contains a copy of E from part (b). Formula (36.4.9) shows that S_J^0 decomposes as an orthogonal sum of S_E^0 and the restriction of S_J^0 to the off-diagonal entries, $C[12] + C[23] + C[31]$, which is isomorphic to $\langle -\gamma_2\gamma_3, -\gamma_3\gamma_1, -\gamma_1\gamma_2 \rangle \otimes n_C$. Assume C is regular, in which case so is this latter form.

Below, we will write Q_J for the quadratic form

$$Q_J := \langle \gamma_2\gamma_3, \gamma_3\gamma_1, \gamma_1\gamma_2 \rangle \otimes n_C. \tag{1}$$

A useful property of Q_J is that, since

$$\langle 1, \gamma_2\gamma_3, \gamma_3\gamma_1, \gamma_1\gamma_2 \rangle \cong \langle 1, \gamma_2\gamma_3, \gamma_3\gamma_1, (\gamma_2\gamma_3)(\gamma_3\gamma_1) \rangle \cong \langle\!\langle -\gamma_2\gamma_3, -\gamma_3\gamma_1 \rangle\!\rangle,$$

we have

$$n_C \perp Q_J \cong \langle\!\langle -\gamma_2\gamma_3, -\gamma_3\gamma_1 \rangle\!\rangle \otimes n_C.$$

Since n_C is a Pfister form, so is $n_C \perp Q_J$. We summarize the relationship between Q_J, S_J, and S_J^0 with

$$S_J \cong S_E \perp \langle -1 \rangle \otimes Q_J \quad \text{and} \quad S_J^0 \cong S_E^0 \perp \langle -1 \rangle \otimes Q_J. \tag{2}$$

41.6 Proposition. *Let J be a regular cubic Jordan algebra over F.*

(a) If $\operatorname{char}(F) \neq 2$*, the quadratic trace S_J of J is a regular quadratic form.*

(b) If $\operatorname{char}(F) = 2$*, then* $\operatorname{Rad}(DS_J) = F1_J$ *and S_J is a non-singular quadratic form in the sense of 11.11.*

(c) If $\operatorname{char}(F) \neq 3$*, then the restriction S_J^0 of S_J to the space J^0 of trace zero elements of J is a regular quadratic form.*

Proof Note that by regularity J is finite-dimensional.

Assume first $\operatorname{char}(F) \neq 2$ and suppose $x \in J$ satisfies $S_J(x, J) = \{0\}$. By (33a.2), therefore, $2T_J(x) = S_J(x, 1_J) = 0$, hence $T_J(x) = 0$, and (33a.13) implies $T_J(x, J) = \{0\}$. We conclude $x = 0$ since J is regular. Hence (a) holds.

Next assume $\operatorname{char}(F) \neq 3$. The bilinear form DS_J^0 is the restriction of $-T_J$ to $J^0 \times J^0$ by (33a.13), hence a regular symmetric bilinear form, i.e., we have (c). Since $S_J(1_J) = 3$, we conclude that S_J is non-degenerate. And since J stays regular under all base field extensions, S_J is in fact non-singular. □

41.7 Lemma. *Let (C, Γ) be a co-ordinate pair over F, with C a regular composition F-algebra, and put $J := \operatorname{Her}_3(C, \Gamma)$.*

(a) The isomorphism class of the quadratic form Q_J defined in (41.5.1) depends only on the isomorphism class of J (or merely the isomorphism class of S_J^0) and not on C nor Γ.

(b) If C has dimension at least 2, then C is split if and only if Q_J is hyperbolic.

Proof (a) Suppose that J is isomorphic to $J' \cong \operatorname{Her}_3(C', \Gamma')$ for a coordinate pair (C', Γ') with C' regular. If $\operatorname{char}(F) \neq 3$, then S_J^0 is regular (Prop. 41.6) and by (41.5.2) we have

$$S_E^0 \perp \langle -1 \rangle \otimes Q_J \cong S_J^0 \cong S_{J'}^0 \cong S_E^0 \perp \langle -1 \rangle \otimes Q_{J'}. \tag{1}$$

The three forms S_E^0, Q_J, $Q_{J'}$ are all regular, so by Witt cancellation we conclude $Q_J \cong Q_{J'}$.

In case $\operatorname{char}(F) = 3$, $S_E^0 \cong \langle 0, -1 \rangle_{\text{quad}}$ by Exc. 34.26(b) and we can quotient

out both sides of (1) by the radical to find

$$\langle -1\rangle_{\text{quad}} \perp \langle -1\rangle \otimes Q_J \cong \langle -1\rangle_{\text{quad}} \perp \langle -1\rangle \otimes Q_{J'}$$

and again conclude that $Q_J \cong Q_{J'}$.

(b) If C is split, then n_C is hyperbolic and hence so is Q_J, by (41.5.1). Conversely, if Q_J is hyperbolic, then the Pfister form $n_C \perp Q_J$ (cf. 41.5 (c)) is isotropic, hence hyperbolic (41.4 (d)). Witt cancellation and hyperbolicity of Q_J now imply that n_C is hyperbolic, so C is split. □

41.8 Theorem (Jacobson [136, Thm. IX.2.2], Faulkner [74, Thm. 1.8])**.** *Let* (C,Γ) *and* (C',Γ') *be co-ordinate pairs over* F *and suppose* C, C' *are composition algebras. Then the following conditions are equivalent.*

(i) C *and* C' *are isomorphic.*
(ii) $J := \mathrm{Her}_3(C,\Gamma)$ *and* $J' := \mathrm{Her}_3(C',\Gamma')$ *are isotopic.*

In case C, C' are regular, Cor. 40.5 shows that the equivalent conditions in the theorem are also equivalent to the statements "N_J and $N_{J'}$ are similar" and "N_J and $N_{J'}$ are isometric".

Proof (i) ⇒ (ii). By Exc. 37.23, J is isotopic to $\mathrm{Her}_3(C)$ and J' is isotopic to $\mathrm{Her}_3(C')$. But (i) implies that $\mathrm{Her}_3(C)$ and $\mathrm{Her}_3(C')$ are isomorphic. Hence (ii) holds.

(ii) ⇒ (i). Suppose C, C' have rank at least 2, for otherwise there is nothing to prove. In particular, they are both regular. Since J is isotopic to $\mathrm{Her}_3(C',\Gamma')$, we deduce from Thm. 40.10 that J is isomorphic to $J'_1 := \mathrm{Her}_3(C',\Gamma'_1)$, for some diagonal matrix $\Gamma'_1 \in \mathrm{GL}_3(F)$. By Lemma 41.7 (a), the quadratic forms Q_J and $Q_{J'_1}$ are isometric, hence have the same splitting fields. But now Lemma 41.7 (b) shows that n_C and $n_{C'}$ have the same splitting fields. Both being Pfister forms, they must be isometric (41.4 (e)). Thus, by the norm equivalence theorem 23.5, $C \cong C'$. □

41.9 Corollary. *There are exactly* 10 *isotopy classes of Freudenthal algebras over* $\mathbb{R}$*, namely* $\mathbb{R}^{(+)}$, $(\mathbb{R}\times\mathbb{R}\times\mathbb{R})^{(+)}$, $(\mathbb{R}\times\mathbb{C})^{(+)}$, $\mathrm{Her}_3(\mathbb{R})$*, and* $\mathrm{Her}_3(C)$ *for* C *a split or division composition algebra of dimension 2, 4, or 8.*

Proof For ranks 1 and 3, isotopy is the same as isomorphism, so this amounts to Cor. 40.8. For the other ranks, each isomorphism class listed in Cor. 40.8 is isotopic to one of the form $\mathrm{Her}_3(C)$ for some composition algebra, so the claimed list touches every isotopy class. Finally, Thm. 41.8 shows that the algebras in the claimed list are pairwise non-isotopic. □

41.10 Corollary. *Let* (C,Γ) *be a co-ordinate pair over* F *with* C *a regular*

composition algebra, and put $J := \mathrm{Her}_3(C,\Gamma)$. *The isometry classes of the Pfister forms* n_C *and* $n_C \perp Q_J$ *depend only on the isomorphism class of* J *and not on the choice of* (C,Γ).

Proof The theorem says that the isomorphism class of C depends only on the isomorphism class of J, so the same is true of n_C. Since Q_J is determined by J (Lemma 41.7 (a)), the same is true of $n_C \perp Q_J$. □

41.11 The Pfister forms of a Freudenthal algebra. Given a regular simple reduced Freudenthal algebra J over a field F, we define Pfister forms Pf_J and Pf_J^{+2} by writing $J := \mathrm{Her}_3(C,\Gamma)$ as in Cor. 41.10 and setting

$$\mathrm{Pf}_J := n_C \quad \text{and} \quad \mathrm{Pf}_J^{+2} := n_C \perp Q_J = \mathrm{Pf}_J \perp Q_J.$$

41.12 Co-ordinatizations. Let J be a regular simple reduced Freudenthal algebra over F. By Prop. 39.17 and Thm. 41.8, there exists a regular composition F-algebra C, uniquely determined up to isomorphism, such that $J \cong \mathrm{Her}_3(C,\Gamma)$, for some diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$. By abuse of language, we call C the *co-ordinate* (or *coefficient*) *algebra* of J. Any isomorphism $\eta\colon J \xrightarrow{\sim} \mathrm{Her}_3(C,\Gamma)$ is called a *co-ordinatization* of J. Passing from one co-ordinatization of J to another will be expressed by saying that J is being *re-co-ordinatized*. If Ω is the elementary frame that is mapped by a co-ordinatization onto the diagonal frame of the target Jordan matrix algebra, we speak, more specifically, of an Ω-*co-ordinatization*. Note that by the uniqueness of the co-ordinate algebra and Prop. 39.2, every elementary frame Ω of J allows an Ω-co-ordinatization of J.

41.13 The norm class of an elementary idempotent. Let J be a regular simple reduced Freudenthal algebra over F and write C for its co-ordinate algebra. Since n_C permits composition and the invertible elements of C are precisely the anisotropic vectors relative to n_C (Prop. 17.5), $n_C(C^\times)$ is a subgroup of $F^\times$. We call the quotient $\mathrm{Cl}(J) := F^\times/n_C(C^\times)$ the *class group* of J and denote by $\mathrm{cl}\colon F^\times \to \mathrm{Cl}(J)$ the natural epimorphism.

Now let e be an elementary idempotent of J. By Exc. 40.15 (f), e can be extended to an elementary frame $\Omega = (e_1,e_2,e_3)$ of J with $e_1 = e$. Pick any Ω-co-ordinatization $\eta\colon J \to H := \mathrm{Her}_3(C,\Gamma)$, $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{GL}_3(F)$. Then

$$\kappa(e) := \mathrm{cl}(-\gamma_2\gamma_3) \in \mathrm{Cl}(J) \tag{1}$$

is called the *norm class* of e (with respect to J). We show that $\kappa(e)$ *is independent of all choices made*: let $\Omega' = (e_1',e_2',e_3')$ be another elementary frame of J

with $e'_1 = e$ and $\eta' : J \to H' := \mathrm{Her}_3(C, \Gamma')$, $\Gamma' = \mathrm{diag}(\gamma'_1, \gamma'_2, \gamma'_3) \in \mathrm{GL}_3(F)$, be any Ω'-co-ordinatization of J. Then the isomorphism $\phi := \eta' \circ \eta^{-1} : H \to H'$ maps $e_{11} \in H$ to $e_{11} \in H'$, hence ϕ maps

$$H_0(e_{11}) = Fe_{22} + Fe_{33} + C[23] \subseteq H \text{ to } H'_0(e_{11}) = Fe_{22} + Fe_{33} + C[23] \subseteq H'.$$

Since ϕ preserves quadratic traces, it induces an isometry from $S_H|_{H_0(e_{11})} \cong \mathbf{h} \perp (-\gamma_2\gamma_3)n_C$ (by (36.4.9)) to $S_{H'}|_{H'_0(e_{11})} \cong \mathbf{h} \perp (-\gamma'_2\gamma'_3)n_C$. Thanks to Witt cancellation, therefore, $(-\gamma_2\gamma_3)n_C \cong (-\gamma'_2\gamma'_3)n_C$, and since n_C is round, this implies $\mathrm{cl}(-\gamma_2\gamma_3) = \mathrm{cl}(-\gamma'_2\gamma'_3)$. Thus $\kappa(e)$ is well defined.

41.14 Remark. Our preceding considerations, and many more still to come, rely on the possibility of extending an elementary idempotent to an elementary frame. In spite of the fact that this possibility can be guaranteed only by working (as we do) with simple reduced Freudenthal algebras that are also regular, there is much room for generalizations. For example, passing from Jordan algebras to Jordan pairs, which provide us with a much more generous supply of elementary idempotents, the Jacobson-Faulkner theorem 41.8 has been generalized in [213, p. 196] to what is called there the *isotopy theorem*, a special case of which says the following: given arbitrary co-ordinate pairs (C, Γ) and (C', Γ') over a *local* ring, the cubic Jordan matrix algebras $\mathrm{Her}_3(C, \Gamma)$ and $\mathrm{Her}_3(C', \Gamma')$ are isotopic if and only if C and C' are isotopic, i.e., there exist $p, q \in C^\times$ such that $C' \cong C^{(p,q)}$ as conic algebras. In particular, *conditions (i), (ii) of Theorem 41.8 are equivalent if C and C' are only assumed to be pre-composition algebras.*

We now proceed to derive a couple of technical lemmas that pave the way for the proof of the classification theorem 41.21.

41.15 Lemma. *Let C be a regular composition algebra over F, and with $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathrm{GL}_3(F)$, put $J := \mathrm{Her}_3(C, \Gamma)$ and $S := S_J$.*

(i) *If the norm of C is surjective (in particular, if C is split of dimension > 1), then the class group of J is trivial and $\kappa(e) = 1_{\mathrm{Cl}(J)}$ for all elementary idempotents $e \in J$.*

(ii) *If C is a division algebra and $0 \neq x \in C[jl]$ for some $1 \leq i \leq 3$, then $\kappa(e_{ii}) = \mathrm{cl}(S(x))$.*

(iii) *If C is a division algebra and $x \in J_1(e_{ii})$ for some $1 \leq i \leq 3$, with $S(x) \in F^\times$, then $g = S(x)^{-1}x^\sharp$ is an elementary idempotent in $J_0(e_{ii})$ with $\kappa(g) = \mathrm{cl}(S(x))$.*

Proof (i) follows immediately from the definitions.

(ii) Since $x \neq 0$, $x = d[jl]$, $d \in C^\times$. So $S(x) = -\gamma_j\gamma_l n_C(d)$ and $\mathrm{cl}(S(x)) = \mathrm{cl}(-\gamma_j\gamma_l) = \kappa(e_{ii})$.

(iii) We may assume $i = 1$ and have $0 \neq S(x) = T(x^\sharp)$ (33a.12), so $x^\sharp \neq 0$, $x^\sharp \in J_0(e_{11})$ by (38.7.2), $x^{\sharp\sharp} = 0$ by (38.7.1). Therefore $g_3 := S(x)^{-1}x^\sharp$ is an elementary idempotent in $J_0(e_{11})$, and $\Omega := (g_1, g_2, g_3) = (e_{11}, 1_J - e_{11} - g_3, g_3)$ is an elementary frame in J. Now (37.2.2) and (33a.3) imply $(g_2+g_3)\times x = -x$. But $g_3 \times x = S(x)^{-1}x^\sharp \times x = -x$ by (33a.14). Therefore $g_2 \times x = 0$ and, since $T(x) = 0$, $x \in J_1(g_2)$ (37.2.2). So $x \in J_1(g_1) \cap J_1(g_2) = J_{12}(\Omega)$ and $\kappa(g_3) = \mathrm{cl}(S(x))$ by (ii). □

Continue the hypothesis that J and J' are regular cubic Jordan algebras over F. We would like to compare the conditions $S_J \cong S_{J'}$ and $S^0_J \cong S^0_{J'}$. One direction is obvious when $\mathrm{char}(F) \neq 3$: Because of the hypothesis on the characteristic, $S_J \cong \langle 3\rangle_{\mathrm{quad}} \perp S^0_J$ and similarly for J', and we deduce immediately: *If $S^0_J \cong S^0_{J'}$, then $S_J \cong S_{J'}$*. Conversely, we have the following.

41.16 Proposition. *Suppose J and J' are regular simple reduced Freudenthal algebras.*

(a) *If $S^0_J \cong S^0_{J'}$, then $S_J \cong S_{J'}$.*

(b) *Suppose* $\mathrm{char}(F) \neq 2$ *or J has rank 15 or 27. If $S_J \cong S_{J'}$, then $S^0_J \cong S^0_{J'}$.*

Proof Suppose first that $\mathrm{char}(F) \neq 2, 3$, in which case we exploit Example 41.5(a) to see that $S_J \cong \langle 3\rangle_{\mathrm{quad}} \perp S^0_J$ and similarly for J', where all the quadratic forms are regular. Witt Cancellation 11.27 gives that $S^0_J \cong S^0_{J'}$ if and only if $S_J \cong S_{J'}$.

For (a), since $S^0_J \cong S^0_{J'}$, we have $Q_J \cong Q_{J'}$ by Lemma 41.7(a), so

$$S_J \cong S_E \perp \langle -1\rangle \otimes Q_J \cong S_E \perp \langle -1\rangle \otimes Q_{J'} \cong S_{J'}.$$

Let us next consider (b) in case $\mathrm{char}(F) = 3$. As in the proof of Lemma 41.7, we use the first equation of (41.5.2) to conclude that $Q_J \cong Q_{J'}$, from which we use the second equation of (41.5.2) to conclude that $S^0_J \cong S^0_{J'}$.

It remains to prove (b) in case $\mathrm{char}(F) = 2$ and J has rank 15 or 27. We use some concepts from the theory of quadratic forms as described in Part 1 of [72]. In particular, we consider the Witt group of regular quadratic forms over F, which is a module under the Witt ring of non-degenerate symmetric bilinear forms, as well as its submodule $I^2_q(F)$ that is generated by 2-Pfister forms.

We first claim that $S^0_J \perp [1,1]$ belongs to $I^2_q(F)$. Write J as $\mathrm{Her}_3(C,\Gamma)$. The calculation in Example 41.5 (b) shows that

$$S^0_J \cong [1,1] \perp \mathfrak{b} \otimes n_C$$

for a rank 3 bilinear form $\mathfrak{b}$. Since $\dim C = 4$ or 8 by hypothesis, n_C is regular and lies in the subgroup $I^2_q(F)$ in the Witt group, as does $\langle 1,1\rangle \otimes [1,1]$, hence so does their sum $S^0_J \perp [1,1]$.

Using the hypothesis that $S_J \cong S_{J'}$ and rearranging terms, we find

$$\langle 1\rangle_{\text{quad}} \perp S_J^0 \perp S_{J'}^0 \cong \langle 1\rangle_{\text{quad}} \perp S_J^0 \perp S_J^0.$$

The regular quadratic form $S_J^0 \perp S_J^0$ is hyperbolic [72, Lemma 8.13]. Thus, $S_J^0 \perp S_{J'}^0$ is isomorphic to a regular 2-dimensional form q plus a hyperbolic form [72, Prop. 8.8]. On the other hand,

$$S_J^0 \perp S_{J'}^0 \perp 2\mathbf{h} \cong S_J^0 \perp [1,1] \perp S_{J'}^0 \perp [1,1],$$

so $S_J^0 \perp S_{J'}^0$ and hence also q lie in $I_q^2(F)$. It follows that q must be isotropic by the Arason-Pfister Hauptsatz [72, Thm. 23.7(1)], hence hyperbolic. In summary, $S_J^0 \cong S_{J'}^0$, as required. □

One could extend the preceding result to include the case where J and J' are not reduced, by extending scalars to a cubic extension that reduces J or J' as in Prop. 46.6 below.

In the case of characteristic 2, (b), one might wonder about the omitted ranks. We already have an example such that $S_J \cong S_{J'}$ does not imply $S_J^0 \cong S_{J'}^0$ when J, J' have dimension 3, see Exc. 34.25. For rank 6, J is not regular. For rank 9, we have the following.

41.17 Example. Suppose $\text{char}(F) = 2$ and $J := \text{Her}_3(K)$ for K a quadratic étale F-algebra. Then $K = F[\mathbf{t}]/(\mathbf{t}^2 + \mathbf{t} + \beta)$ for some $\beta \in F$ and by the calculations of Example 41.5,

$$\begin{aligned} S_J^0 &\cong [1,1] \perp n_K \perp n_K \perp n_K \cong [1,1] \perp [1,\beta] \perp 2\mathbf{h} \\ &\cong [1,\beta+1] \perp 3\mathbf{h}, \end{aligned}$$

where the last isomorphism is by [72, Example 7.23]. In any case, just as in Exc. 34.25, we find that

$$S_J \cong \langle 1\rangle_{\text{quad}} \perp S_J^0 \cong \langle 1\rangle_{\text{quad}} \perp 4\mathbf{h},$$

regardless of the choice of K.

For example, let F be a finite field of characteristic 2 such that adjoining the cube roots of unity is a proper extension K. (E.g., take $F = \mathbb{F}_2$.) Take $J := \text{Her}_3(K)$ and take J' to be the split Freudenthal algebra over F of rank 9, $\text{Her}_3(F \times F) \cong \text{Mat}_3(F)^{(+)}$. Then $S_J \cong S_{J'}$ but $S_J^0 \cong 4\mathbf{h} \not\cong n_K \perp 3\mathbf{h} \cong S_{J'}^0$.

In the following result, we use the hypothesis $S_J^0 \cong S_{J'}^0$. One can translate this to an alternative version that uses the hypothesis $S_J \cong S_{J'}$ instead by using Prop. 41.16.

41.18 Lemma. *Let J and J' be two regular simple reduced Freudenthal F-algebras and suppose that $S_J^0 \cong S_{J'}^0$.*

(a) The coefficient algebras of J and J' are isomorphic; in particular, J and J' have the same class group.

(b) Any two elementary idempotents $e \in J$, $e' \in J'$ with $\kappa(e) = \kappa(e')$ can be mapped into each other by an isomorphism of J' onto J.

Proof Write $J = \mathrm{Her}_3(C,\Gamma)$, $J' = \mathrm{Her}_3(C',\Gamma')$ for composition algebras C, C' and diagonal matrices $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3)$, $\Gamma' = \mathrm{diag}(\gamma'_1,\gamma'_2,\gamma'_3) \in \mathrm{GL}_3(F)$.

(a) There is nothing to prove for $r := \dim_F(C) = \dim_F(C') = 1$, so let us assume $r > 1$. Since S^0_J and $S^0_{J'}$ are isometric, so are Q_J and $Q_{J'}$ (Lemma 41.7). In particular, Q_J and $Q_{J'}$ have the same splitting fields and by Lemma 41.7 (b), this property carries over to n_C and $n_{C'}$, forcing $n_C \cong n_{C'}$ by 41.4 (e): Thus C and C' are isomorphic and $\mathrm{Cl}(J) = \mathrm{Cl}(J')$.

(b) If $C \cong C'$ are both split of dimension $r > 1$, then Prop. 40.6 shows $J \cong J' \cong \mathrm{Her}_3(C)$. Any elementary idempotent of $\mathrm{Her}_3(C)$ has trivial norm class (Lemma 41.15 (i)), and that any two of them can be mapped into each other by an automorphism is an easy exercise.

We may therefore assume that C and C' are division algebras. We may further assume that $e = e_{11}$ and $e' = e'_{11}$ where (e_{11}, e_{22}, e_{33}) and $(e'_{11}, e'_{22}, e'_{33})$ are the diagonal elementary frames of J and J' respectively. We wish to show that J can be re-co-ordinatized in such a way that $J \cong \mathrm{Her}_3(C,\Gamma')$. To this end, we consider the quadratic space S^* and S'^*, which we define to be S_J, $S_{J'}$ if $\mathrm{char}(F) \neq 2$ and S^0_J, $S^0_{J'}$ if $\mathrm{char}(F) = 2$. By hypothesis, $S^* \cong S'^*$ (Prop. 41.16) and the quadratic form is regular (Prop. 41.6). We write J^*, J'^* for the module underlying S^*, S'^* respectively.

Put $J_{jl} = C[jl] \subseteq J^*$, $J'_{jl} = C'[jl] \subseteq J'^*$. Since $\kappa(e) = \kappa(e')$, there is an isometry of $\psi_0 \colon J'_{23} \to J_{23}$. We define subspaces $E^* \subseteq J^*$, $E'^* \subseteq J'^*$ by $E^* := \sum Fe_{ii} \subseteq J$, $E'^* := \sum Fe'_{ii} \subseteq J'$ for $\mathrm{char}(F) \neq 2$ and $E^* := E^0 = \sum_{i=1}^2 F(e_{ii} - e_{33})$, $E'^* := E'^0 = \sum_{i=1}^2 F(e'_{ii} - e'_{33}) \subseteq J'^0$ for $\mathrm{char}(F) = 2$. Then we extend ψ_0 to an isometry $\psi \colon W' := E'^* \oplus J'_{23} \to W := E^* \oplus J_{23}$ having $\psi(e'_{ii}) = e_{ii}$ for $1 \leq i \leq 3$ and $\mathrm{char}(F) \neq 2$, $\psi(e'_{ii} - e'_{33}) = e_{ii} - e_{33}$ for $i = 1,2$ and $\mathrm{char}(F) = 2$. Applying the Witt extension theorem [72, Thm. 8.3], we can extend ψ still further to an isometry $\phi \colon J'^* \to J^*$, which in turn maps $W'^\perp$ onto $W^\perp$, orthogonal complementation referring to S'^*, S^*, respectively. Thus $W'^\perp = J'_{31} \oplus J'_{12}$ and $W^\perp = J_{31} \oplus J_{12}$ in all characteristics. We now observe $1_{C'}[31] \in J'_{31} \subseteq W'^\perp$ and put $y := \phi(1_{C'}[31]) \in W^\perp = J_1(e_{11})$ to obtain $S(y) = S'(1_{C'}[31]) = -\gamma'_3\gamma'_1$. By Lemma 41.15 (iii), $g_2 := S(y)^{-1}y^\sharp$ is an elementary idempotent in $J_0(e_{11})$, giving rise to the elementary frame

$$\Omega := (g_1, g_2, g_3) := (e_{11}, g_2, 1_J - e_{11} - g_2)$$

of J. Since $y \in J_1(g_1)$, (37.2.2) and (33a.3) imply $(g_2 + g_3) \times y = -y$. But

$g_2 \times y = S(y)^{-1}y^\sharp \times y = -y$ by (33a.14) since $N_J(y) = 0$ by (38.7.1). Thus $g_3 \times y = 0$ and, since $T_J(y) = 0$, $y \in J_1(g_3)$. So $y \in J_1(g_1) \cap J_1(g_3) = J_{31}(\Omega)$. On the other hand, $\kappa(g_1) = \kappa(e_{11}) = \kappa(e'_{11})$, so there is an $x \in J_{23}(\Omega)$ having $S(x) = -\gamma'_2\gamma'_3$. Summing up, therefore, we deduce from Prop. 37.6 that $\mathfrak{S} := (\Omega, x, y)$ is a co-ordinate system for J, and the Jacobson co-ordinatization theorem 37.17 combined with the uniqueness of the coefficient algebra yields a co-ordinatization $\eta\colon J \xrightarrow{\sim} \mathrm{Her}_3(C, \Gamma'')$,

$$\Gamma'' = \mathrm{diag}\,(-S(y), -S(x), 1) = \mathrm{diag}(\gamma'_3\gamma'_1, \gamma'_2\gamma'_3, 1).$$

Multiplying Γ'' by γ'_3 and clearing squares, Γ'' is converted to Γ', which by Exc. 37.22 (b) completes the proof. □

41.19 Corollary. *If J is a regular simple reduced Freudenthal algebra over F, then two elementary idempotents $e, e' \in J$ are in the same orbit of the automorphism group of J if and only if $\kappa(e) = \kappa(e')$.* □

41.20 Lemma. *Let J and J' be two regular simple reduced Freudenthal F-algebras and suppose that $S^0_J \cong S^0_{J'}$. Then there exist elementary idempotents $e \in J$ and $e' \in J'$ with $\kappa(e) = \kappa(e')$.*

Proof We adopt the notation used in the proof of Lemma 41.18 and, in particular, write $J = \mathrm{Her}_3(C, \Gamma)$, $J' = \mathrm{Her}_3(C, \Gamma')$. If C is split of dimension > 1 then the class groups of J and J' are trivial and all elementary idempotents of J and J' have the same norm class. In view of Exercise 41.35, we may therefore assume that C is a division algebra of dimension > 1.

By Lemma 41.7, the quadratic forms Q_J and $Q_{J'}$, which act on $J_{23} \oplus J_{31} \oplus J_{12}$ and $J'_{23} \oplus J'_{31} \oplus J'_{12}$, respectively, are isometric. So there exists an $x \in J_{23} \oplus J_{31} \oplus J_{12}$ such that $S(x) = -\gamma'_2\gamma'_3$. If $x \in J_1(e_{ii})$ for some $1 \le i \le 3$ then by Lemma 41.15 (iii), we obtain an elementary idempotent $e \in J$ with $\kappa(e) = \mathrm{cl}(S(x)) = \kappa(e'_{11}) = \kappa(e')$ and we are done. If not, then

$$x = \sum c_i[jl] \qquad (c_1, c_2, c_3 \in C^\times). \tag{1}$$

By (36.4.5) and (36.4.9) we have

$$S(x) = -\sum \gamma_j\gamma_l n_C(c_i), \quad N_J(x) = \gamma_1\gamma_2\gamma_3 t_C(c_1c_2c_3). \tag{2}$$

Our next aim will be to show that *we may assume* $N_J(x) = 0$. Indeed, if this is not so, we may use the co-ordinate system $(e_{11}, e_{22}, e_{33}, c_1[23], c_2[31])$ to re-co-ordinatize J, allowing us to assume $c_1 = c_2 = 1_C$. Since $\dim_F(C) > 1$, we find an element $b \in C^\times$ having $t_C(\bar{b}c_3) = n_C(b, c_3) = 0$. Putting $y := \bar{b}[23] + b[31] + \bar{b}c_3[12]$, we conclude $S(y) = n_C(b)S(x)$ and $N_J(y) = \gamma_1\gamma_2\gamma_3 t_C(\bar{b}b(\bar{b}c_3)) = \gamma_1\gamma_2\gamma_3 n_C(b)t_C(\bar{b}c_3) = 0$. Thus we may assume that x as in (1) satisfies $\kappa(e') =$

$\mathrm{cl}(S(x))$ and $N_J(x) = 0$. This implies $x^{\#\#} = 0$ and forces $g := S(x)^{-1}x^\#$ to be an elementary idempotent. Since $T_J(x) = 0$ and $g \times x = -x$ by (33a.14), Prop. 37.2 (b) implies $x \in J_0(g)$.

Put $T := T_J$ and assume first $T(e_{11}, g) = 1$. Since Peirce components are orthogonal relative to the bilinear trace (Prop. 37.2 (b)), the Peirce-2-component of $x^\#$ relative to e_{11} is $S(x)e_{11}$, while, by (1), (36.4.4) combined with Prop. 37.8 and (32.15.2), it agrees with $-\gamma_2\gamma_3 n_C(c_1)e_{11}$. Thus $y = c_1[23] \in C[23]$ has $\kappa(e') = \mathrm{cl}(S(x)) = \mathrm{cl}(S(y)) = \mathrm{cl}(-\gamma_2\gamma_3) = \kappa(e_{11})$.

Turning to the case $T(e_{11}, g) \neq 1$, put $f := 1_J - g$ and consider the quantity $U_f e_{11} \in J_0(g)$. We have $(U_f e_{11})^\# = U_{f^\#} e_{11}^\# = 0$ and $T(U_f e_{11}) = T(U_f e_{11}, 1_J) = T(e_{11}, f) = T(e_{11}, 1_J - g) = 1 - T(e_{11}, g) \neq 0$. Therefore $g_2 := T(U_f e_{11})^{-1} U_f e_{11}$ is an elementary idempotent in $J_0(g)$ satisfying $T(g_2, x) = 0$ since $T(U_f e_{11}, x) = T(e_{11}, U_f x) = T(e_{11}, x) = 0$. Since also $T(x) = T(g, x) = 0$, we conclude with $g_3 := f - g_2$ that

$$x \in (Fg \oplus Fg_2 \oplus Fg_3)^\perp \cap J_0(g),$$

orthogonal complements being taken relative to the bilinear trace. Thus x belongs to the Peirce-2, 3-component relative to the elementary frame (g, g_2, g_3) of J. But this means $\kappa(g) = \kappa(e')$, and the proof is complete. □

Collecting results, we quickly obtain:

41.21 Theorem. *If J and J' are regular simple reduced Freudenthal algebras over F, then the following are equivalent.*

(i) *The algebras J and J' are isomorphic.*
(ii) *The quadratic forms S_J^0 and $S_{J'}^0$ are isometric.*
(iii) *The regular quadratic forms Q_J and $Q_{J'}$ are isometric.*
(iv) *The two Pfister forms of J and J' are isometric:* $\mathrm{Pf}_J \cong \mathrm{Pf}_{J'}$ *and* $\mathrm{Pf}_J^{+2} \cong \mathrm{Pf}_{J'}^{+2}$.

Proof The key implication is (ii) ⇒ (i). By Lemma 41.18 (a), J and J' have isomorphic coefficient algebras. Lemma 41.20 provides elementary idempotents $e \in J$ and $e' \in J'$ such that $\kappa(e) = \kappa(e')$. Then Lemma 41.18 (b) yields an isomorphism between J and J'.

The implication (i) ⇒ (iii) is Lemma 41.7 and (iii) ⇒ (ii) is by (41.5.2). And finally, the implication (i) ⇒ (iv) follows from 41.11, while Witt cancellation and 41.11 yield (iv) ⇒ (iii). □

41.22 Remark. If J, J' are Albert algebras (say) or F has characteristic $\neq 2$, then the equivalent conditions of Thm. 41.21 are equivalent to

(v) The quadratic forms S_J and $S_{J'}$ are isometric.

thanks to Prop. 41.16. However, Example 41.17 shows that (v) is not in general equivalent to the statements in Thm. 41.21. (The corresponding statement of Theorem 3 in [242] should be adjusted.)

41.23 Remark. For Freudenthal algebras of rank 9, the equivalent conditions collected in Thm. 41.21 may be viewed in the context of a 3-Pfister form attached to a unitary involution on a central simple associative algebra of degree 3 as in [160, (19.4) and Thm. (19.6)] (for $\mathrm{char}(F) \neq 2$) or [218, Thm. 2.4] (for $\mathrm{char}(F)$ arbitrary), which can in turn be related to a statement about the Rost invariant for affine group schemes of type A_2 as in [218, Remark 2.5]

The following result can be found in a variety of places, such as Springer [264], Knus-Merkurjev-Rost-Tignol [160, Thm. 37.13], or Serre [261, §9.2, §9.4].

41.24 Corollary. *If F has characteristic $\neq 2$, then two simple reduced Freudenthal algebras J, J' over F are isomorphic if and only if their bilinear traces are isometric.*

Proof Since the characteristic is not 2, J and J' are regular (Cor. 39.15). Hence $J \cong J'$ iff $Q_J \cong Q_{J'}$ (Thm. 41.21) iff $T_J \cong T_{J'}$ as symmetric bilinear forms since (36.4.7) implies $T_J = \langle 1, 1, 1\rangle \perp (DQ_J)$, ditto for $T_{J'}$. □

41.25 Vista: S^0_J versus Q_J. We have proved that the quadratic forms S^0_J or Q_J serve to classify regular simple reduced Freudenthal algebras (Thm. 41.21), but there is more to observe.

(i) While S^0_J is a classifying invariant for regular simple reduced Freudenthal algebras over fields, it is still a strange one. For instance, by Example 41.17, even if S^0_J is regular then neither does J split imply S^0_J hyperbolic nor, conversely, does S^0_J hyperbolic imply J split.

(ii) From this point of view, the classifying invariant Q_J is more natural: indeed, if the co-ordinate algebra of J has dimension at least 2, then Q_J is hyperbolic iff J is split, by Lemma 41.7 (b).

(iii) For an Albert algebra J, other references write $f_3(J)$ instead of Pf_J, calling it the 3-*Pfister form of* J or its 3-*invariant* mod 2, and $f_5(J)$ instead of Pf^{+2}_J, calling it the 5-*Pfister form of* J or its 5-*invariant* mod 2. The fact that these invariants classify reduced Albert algebras (i.e., the equivalence of (i) and (iv) in Theorem 41.21) for the case $\mathrm{char}(F) \neq 2$ appears in [94, p. 50, Thm. 22.4], while an explicit reference to this fact in arbitrary characteristic doesn't seem to exist.

It is worth noting that these invariants are defined for every Albert algebra

over a field F, not just reduced ones. See Exc. 46.23 and [230] (in general), and [160, 40.2] or [94, p. 50] (for the case $\mathrm{char}(F) \neq 2$).

We give two applications of the preceding results and begin with a useful criterion for the existence of non-zero nilpotent elements.

41.26 Theorem. *For a regular Freudenthal algebra J of dimension ≥ 6 over F, the following are equivalent.*

(i) J *contains non-zero nilpotent elements.*

(ii) $J \cong \mathrm{Her}_3(C, \mathrm{diag}(-1,-1,1))$*, for some regular composition algebra C over F.*

(iii) J *is reduced and the quadratic form Q_J is isotropic.*

(iv) J *is reduced and the Pfister form Pf_J^{+2} is hyperbolic.*

Proof (ii) $\Rightarrow$ (i). Note first that by Exc. 34.23 elements in a cubic Jordan algebra over a field are nilpotent if and only if their linear trace, their quadratic trace and their norm are equal to zero We begin by assuming $J \cong J' := \mathrm{Her}_3(C,\Gamma)$ with C and Γ as indicated in (ii). Then $u := e_{22} - e_{33} + 1_C[23] \in J'$ is a non-zero nilpotent, by the formulas in 36.4, so J contains non-zero nilpotent elements.

(i) $\Rightarrow$ (ii). If $0 \neq u \in J$ is nilpotent, then (33.9.3) implies $(u^2)^2 = u^4 = 0$, so replacing u by u^2 if necessary we may assume $u^2 = 0$. By Lemma 38.4, there exists an elementary idempotent $e \in J$ such that $u \in J_0(e)$. Extending e to an elementary frame $\Omega = (e = e_1, e_2, e_3)$ in J by Exc. 40.15 (f), we write C for the co-ordinate algebra of J. If C contains zero divisors, then $J \cong \mathrm{Her}_3(C,\Gamma)$ for any diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ (Prop. 40.6), so we may assume that C is a division algebra. Letting $J \xrightarrow{\sim} \mathrm{Her}_3(C,\Gamma)$ be an Ω-co-ordinatization of J, with some diagonal matrix $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{GL}_3(F)$, we may identify $J = \mathrm{Her}_3(C,\Gamma)$ in such a way that $e = e_{11}$, hence $u = \alpha_2 e_{22} + \alpha_3 e_{33} + a_1[23]$, $\alpha_2, \alpha_3 \in F$, $a_1 \in C$ not all zero. We may assume $\gamma_3 = 1$. Thus $\alpha_2 + \alpha_3 = T_J(u) = 0$ and $\alpha_2\alpha_3 - \gamma_2 n_C(a_1) = S_J(u) = 0$. With $\alpha := \alpha_2 = -\alpha_3$, we therefore conclude $\alpha^2 + \gamma_2 n_C(a_1) = 0$. Hence $\alpha \neq 0$ and $a_1 \in C^\times$, so with $p := \alpha^{-1} a_1$ we obtain $\gamma_2 n_C(p) = -1$. In view of Exc. 37.24, we may therefore assume $\gamma_2 = -1$. Consulting (41.5.1), we see that Q_J is Witt equivalent to $-n_C$, so the Witt class of Q_J is independent of γ_1. Since Q_J by Thm. 41.21 is a classifying invariant for J, we may therefore assume $\gamma_1 = -1$, and (ii) holds.

(ii) $\Rightarrow$ (iii). From (ii) and (41.5.1) we deduce $Q_J = (-n_C) \perp (-n_C) \perp n_C$, and this is isotropic.

(iii) $\Rightarrow$ (iv). If (iii) holds, then Pf_J^{+2} is isotropic, hence hyperbolic by 41.4 (d).

(iv) $\Rightarrow$ (ii). If Pf_J^{+2} is hyperbolic, then $\mathrm{Pf}_J^{+2} \cong n_C \perp (-n_C) \perp (-n_C) \perp n_C$, which by Witt cancellation implies $Q_J \cong (-n_C) \perp (-n_C) \perp n_C$. Since J is reduced, Q_J is a classifying invariant for J, whence condition (ii) holds. □

41.27 Remark. For J a reduced Albert algebra over F, the equivalence of (i) and (ii) goes back to Albert-Jacobson [11, Thm. 6] if $\mathrm{char}(F) \neq 2$, while the equivalence of (i), (iii), (iv) is due to Petersson [218, Thm. 4.4].

In our second application, we will be concerned with elements of rank 1 as defined in Exc. 40.15 and their connection with the structure group.

41.28 Rank-one elements and isotopies. Let J be a cubic Jordan algebra over F and write

$$Y := Y(J) := \{y \in J \mid y \text{ has rank } 1\}$$

for the collection of its rank-one elements. The lines Fy, $y \in Y$, form the set of F-points of the projective variety $\mathbf{Y} = \mathbf{Y}(J)$ defined by the homogeneous quadratic equation $x^\sharp = 0$. Note that, for J an Albert algebra, $\mathbf{Y}(J)$ is the E_6-variety of the introduction.

(a) Typical examples of rank-one elements are elementary idempotents but also *nilpotents of index* 2, i.e., elements $u \in J$ satisfying $u^2 = 0 \neq u$. Indeed, we have $T_J(u) = S_J(u) = 0$ by Exc. 34.23, and (33a.22) yields $u^\sharp = 0$. Moreover, Y is stable under homotheties $x \mapsto \alpha x$, $\alpha \in F^\times$, and this procedure combined with the preceding examples exhausts the totality of rank-one elements.

(b) By Exc. 40.15 (a), rank-one elements are stable under isotopy, so $Y(J) = Y(J^{(p)})$, for all $p \in J^\times$. Since isotopies are homomorphisms into appropriate isotopes, and homomorphisms of cubic Jordan algebras preserve adjoints, it follows that isotopies of cubic Jordan algebras preserve rank-one elements. In particular, the structure group of J acts canonically on $Y(J)$. Note that the structure group of J agrees with the group of norm similarities, hence contains the group of norm isometries, provided J is regular (Lemma 40.4).

41.29 Theorem. *Let J be a regular simple reduced Freudenthal F-algebra.*

(a) The group of norm similarities of J acts transitively on the rank-one elements of J.

(b) The group of norm isometries of J acts transitively on the F-points of the projective variety $\mathbf{Y}(J)$: given $y, y' \in Y(J)$, there exists a norm isometry of J sending y to $\alpha y'$, for some $\alpha \in F^\times$.

Proof (a) After passing to an appropriate isotope, we may assume that $J = \mathrm{Her}_3(C)$ for some regular composition F-algebra C. Given $y \in Y(J)$, we must find a norm similarity of J sending y to e_{11}. In order to do so, we apply Exc. 40.15 (a) and find an element $p \in J^\times$ making $e := y \in J^{(p)}$ an elementary idempotent. Using Exc. 40.15 (f), we extend e to an elementary frame

$\Omega = (e = e_1, e_2, e_3)$ of $J^{(p)}$, which in turn, by Prop. 39.2, yields an Ω-coordinatization $\chi\colon J^{(p)} \xrightarrow{\sim} J' := \mathrm{Her}_3(C', \Gamma)$, for some composition algebra C' over F and some diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$; in particular $\chi(y) = \chi(e) = e'_{11} \in J'$. From Thm. 41.8 we deduce $C \cong C'$, so we may actually assume $C = C'$ and $J' = \mathrm{Her}_3(C, \Gamma)$. Applying Exc. 37.23, we find an element $q \in J'^{\times}$ and an isomorphism $\psi\colon J'^{(q)} \xrightarrow{\sim} \mathrm{Her}_3(C) = J$ satisfying $\psi(\chi(y)) = \gamma e_{11}$, for some $\gamma \in F^{\times}$. Note that ψ, χ are bijective strong homotopies in the sense of Exc. 31.37, hence isotopies by (a) of the same exercise. We have thus found in $\phi := \gamma^{-1}\psi \circ \chi \in \mathrm{Str}(J)$ a norm similarity satisfying $\phi(y) = e_{11}$.

(b) Write $\mu \in F^{\times}$ for the multiplier of ϕ, so $N_J \circ \phi = \mu N_J$ (as polynomial laws over F). Setting $p := e_{11} + \mu e_{22} + e_{33} \in J^{\times}$, we obtain $N_J(p) = \mu$,

$$N_J \circ (N_J(p)^{-1} U_p \circ \phi) = N_J, \quad \text{and} \quad N_J(p)^{-1} U_p \circ \phi(y) = \mu^{-1} e_{11},$$

which completes the proof of (b). □

Exercises

41.30. Extend the result of Exc. 40.17(a) by proving that every Freudenthal algebra of rank 6 over a finite field is split.

41.31. *Norm classes of elementary frames* (Albert-Jacobson [11, Thm. 9]). Let J be a regular reduced simple Freudenthal algebra over F. For an elementary frame $\Omega = (e_1, e_2, e_3)$ of J,

$$\kappa(\Omega) := (\kappa(e_1), \kappa(e_2)) \in \mathrm{Cl}(J) \times \mathrm{Cl}(J) \tag{1}$$

is called the *norm class* of Ω in J. Prove that two elementary frames of J are in the same orbit under the automorphism group of J if and only if they have the same norm class. Conclude that this is always the case provided J is split of dimension at least 9.

41.32. Let J be a regular Freudenthal algebra over a field F. Show that for every rank 1 element $x \in J$, we have $F\left((x \times J)^{\sharp}\right) = Fx$.

Remark. Note that Fx and $x \times J$ are inner ideals, see Example 34.9. Such inner ideals are sometimes called "points" and "hyperlines" respectively, compare [277, p. 25] or [43, §7]. This exercise gives an explicit bijection between the collection of points and the collection of hyperlines in J.

41.33. *The projective octave plane.* Let C be a regular composition division algebra over a field F and consider the Freudenthal algebra $J := \mathrm{Her}_3(C, \Gamma)$ for some Γ. In this exercise, we define a projective plane in the sense of 2.4 with "points" the set $\mathcal{P}$ of rank 1 elements of J, taken projectively, and "lines" the set $\mathcal{L}$ of hyperlines as in Exercise 41.32, which are in bijection with the points.

(i) Suppose x, y are linearly independent rank 1 elements. Prove: $x \times y$ is also of rank 1 (and in particular is not zero).

(ii) Suppose x, y are rank 1 elements. Prove: $T(x, y) = 0$ if and only if $x \in y \times J$.

We say that a point Fx lies on a line $y \times J$ if $T(x, y) = 0$.

(iii) Suppose Fx and Fy are distinct points. Prove that $(x \times y) \times J$ is the unique line containing both of them.
(iv) Prove that the axioms of a projective plane from 2.4 hold.

Remark. This exercise was inspired by the treatment in [265], see alternatively [85, §7] or [147]. However, our treatment here does not put any hypotheses on the field F (other than the existence of C), whereas the results in the references require at a minimum that F has characteristic $\neq 2, 3$.

41.34. *The Skolem-Noether theorem for reduced Freudenthal algebras* (Jacobson [136, Thm. IX.3]). Let J be a Freudenthal algebra over a field F and suppose J_1', J_2' are reduced simple Freudenthal subalgebras of J. Prove that every isomorphism from J_1' to J_2' can be extended to an automorphism of J[1].

41.35. Let J, J' be regular reduced Freudenthal F-algebras of dimension 6. Complete the proof of Lemma 41.20 by showing that if S_J^0 and $S_{J'}^0$ are isometric, then J and J' are isomorphic.

Remark. We will see in Theorem 46.8 that Freudenthal algebras of dimension 6 are always reduced.

[1] Since the algebras involved here have dimension at least 6, it doesn't matter by Cor. 38.18 whether we are considering isomorphisms (resp. automorphisms) of para-quadratic algebras or of cubic Jordan algebras.

VII

The two Tits constructions

This chapter is devoted to the two Tits constructions of cubic Jordan algebras over arbitrary commutative rings. These constructions, derived from ideas of Jacques Tits, play a role for cubic Jordan algebras similar to that of the Cayley-Dickson construction for composition algebras; compare for example Cor. 45.12 for Albert algebras with Cor. 19.17 for composition algebras. For more description of the main ingredients and additional background information, the reader is referred to the introduction.

Throughout this chapter, we let k be an arbitrary commutative ring. We systematically identify cubic norm structures and cubic Jordan algebras over k via 34.7.

42 Kummer elements

Kummer elements form the connecting thread between cubic Jordan algebras, cubic alternative algebras and the first Tits construction. Before they can be introduced, however, we require a few preparations on cubic alternative algebras as defined in 34.11.

42.1 Proposition. *Let A be a cubic alternative algebra over k.*

(a) *The linear trace of A is an associative linear form:*

$$T_A(x_1x_2) = T_A(x_2x_1), \quad T_A((x_1x_2)x_3) = T_A(x_1(x_2x_3)) \tag{1}$$

for all $x_1, x_2, x_3 \in A$.

(b) *The identities*

$$(xy)^\sharp = y^\sharp x^\sharp, \tag{2}$$

$$x(x^\sharp y) = x^\sharp(xy) = N_A(x)y = (yx)x^\sharp = (yx^\sharp)x \tag{3}$$

hold strictly for all $x, y \in A$.

Proof (a) The first equation of (1) follows from Prop. 34.12. As to the second, let $R = k[\varepsilon_1, \varepsilon_2, \varepsilon_3]$ be the unital commutative associative k-algebra on

generators ε_i, subject to the relations $\varepsilon_i^2 = 0$ $(1 \le i \le 3)$. Since N_A permits composition, we have

$$N_A\Big(((1_A + \varepsilon_1 x_1)(1_A + \varepsilon_2 x_2))(1_A + \varepsilon_3 x_3)\Big) \\ = N_A\Big((1_A + \varepsilon_1 x_1)((1_A + \varepsilon_2 x_2)(1_A + \varepsilon_3 x_3))\Big).$$

Expanding both arguments of N_A and setting $a := \sum \varepsilon_i x_i + \sum_{i<j} \varepsilon_i \varepsilon_j x_i x_j$, $b_1 := \varepsilon_1\varepsilon_2\varepsilon_3(x_1x_2)x_3$, $b_2 := \varepsilon_1\varepsilon_2\varepsilon_3 x_1(x_2x_3)$, we conclude that

$$N_A(1_A + a + b_i) = N_A(1_A + a) + T_A((1_A + a)^\sharp b_i) + T_A((1_A + a)b_i^\sharp) + N_A(b_i)$$

does not depend on $i = 1, 2$. But $b_i^\sharp = a^\sharp b_i = a \times b_i = 0$ and $N_A(b_i) = 0$, while

$$T_A((1_A + a)^\sharp b_i) = T_A(b_i) + T_A((1_A \times a)b_i) + T_A(a^\sharp b_i) \\ = T_A(b_i) + T_A(a \times b_i) = T_A(b_i).$$

Thus $T_A(b_i)$ is independent of $i = 1, 2$, which is precisely what we had to prove.

(b) By Prop. 12.24, we may assume that x and y are both invertible in A. Hence so they are in $A^{(+)}$, and the corresponding inverses coincide (31.6). From Prop. 34.12, (13.7.1) and (33.10.1) we therefore conclude

$$(xy)^\sharp = N_A(xy)(xy)^{-1} = N_A(x)N_A(y)y^{-1}x^{-1} = y^\sharp x^\sharp,$$

hence (2). Using (13.6.1), (13.6.2), a similar argument yields (3). □

42.2 Corollary. *Let A be a cubic alternative algebra over k. Then*

$$\mathrm{Nil}(A) = \mathrm{Nil}(A^{(+)}).$$

Proof The left-hand side is contained in the right since the nil radical of A is a nil ideal in $A^{(+)}$. To prove equality, it suffices to show that the nil radical of $A^{(+)}$ is a two-sided ideal in A. Let $x \in N := \mathrm{Nil}(A^{(+)})$ and $y, z \in A$. From Propositions 34.12 and 42.1 we conclude that

$$T_{A^{(+)}}(xz, y) = T_A((xz)y) = T_A(x(zy)) = T_{A^{(+)}}(x, zy), \\ T_{A^{(+)}}((xz)^\sharp, y) = T_A((z^\sharp x^\sharp)y) = T_{A^{(+)}}(x^\sharp, yz^\sharp), \text{ and} \\ N_{A^{(+)}}(xz) = N_{A^{(+)}}(x)N_A(z)$$

are all nilpotent. Hence Exercise 34.23 implies $xz \in N$. This implies $zx = -xz + x \circ z \in N$, and the assertion follows. □

42.3 Alternative algebras of degree 3. An alternative algebra A over k is said to *be of* (or to *have*) *degree* 3 if the following conditions are fulfilled.

(i) There exists a cubic form $N\colon A \to k$ making A a cubic alternative k-algebra.

(ii) For all algebraically closed fields $K \in k$-**alg**, the set map

$$A_K \longrightarrow \bigwedge^3(A_K) = (\bigwedge^3(A))_K, \quad x \longmapsto 1_{A_K} \wedge x \wedge x^2$$

is different from zero.

In this case, any cubic form satisfying (i) makes $A^{(+)}$ a cubic Jordan algebra over k, and we conclude that $A^{(+)}$ is a Jordan algebra of degree 3. Moreover, Cor. 42.2 implies $\mathrm{Nil}(A) = \mathrm{Nil}(A^{(+)})$. Combining all this with Theorem 38.13, we arrive at the following conclusion.

42.4 Corollary. *Let A be an alternative algebra of degree 3 over k that is finitely generated projective as a k-module and satisfies*

$$\dim_K (A_K / \mathrm{Nil}(A_K)) \geq 2$$

*for all algebraically closed fields $K \in k$-**alg**. Then there is a* unique *cubic form over k, called the* norm *of A and denoted by N_A, making A a cubic alternative k-algebra.* □

42.5 Regularity and semi-linearity for cubic alternative algebras. (a) A cubic alternative algebra A over k is said to be *regular* if it is finitely generated projective as a k-module and the symmetric bilinear form $(x, y) \mapsto T_A(xy)$ on A, called its *bilinear trace*, is regular in the sense of 11.9. This notion is stable under base change. Moreover, by Prop. 34.12, A is regular if and only if $A^{(+)}$ is regular as a cubic Jordan algebra.

(b) Let $\sigma\colon K \to K'$ be a morphism in k-**alg** and A (resp. A') be cubic alternative algebras over K (resp. K'). A map $\varphi\colon A \to A'$ is called a *σ-semi-linear homomorphism* of cubic alternative algebras if

(i) φ is σ-semi-linear.

(ii) $\varphi\colon A \to A'$ is a unital homomorphism of unital k-algebras.

(iii) The σ-semi-linear polynomial square

$$\begin{array}{ccc} A & \xrightarrow[\varphi]{} & A' \\ {\scriptstyle N_A}\downarrow & & \downarrow{\scriptstyle N_{A'}} \\ K & \xrightarrow[\sigma]{} & K' \end{array}$$

commutes in the sense of 12.28.

By 34.10 (b), this is equivalent to $\varphi\colon A^{(+)} \to A'^{(+)}$ being a σ-semi-linear homomorphism of cubic Jordan algebras such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in A$.

42.6 Azumaya algebras of degree n. Azumaya algebras are the analogue over commutative rings of finite-dimensional central simple associative algebras over fields. For details on this important topic, the reader may consult Knus-Ojanguren [158] or Knus [157]. In particular, we remind the reader of the fact that a unital associative k-algebra that is finitely generated projective as a k-module is separable in the sense of 22.4 if and only if it is separable in the sense of [158, III, 1.4]; the proof follows easily from the definitions and standard results assembled in [158, III].

Let n be a positive integer. By an *Azumaya algebra of degree n* over k we mean a *twisted form* of the algebra of n-by-n matrices over k, i.e., a k-algebra A such that there exist a faithfully flat k-algebra $R \in k\text{-}\mathbf{alg}$ and an isomorphism $A_R \cong \mathrm{Mat}_n(R)$ of R-algebras. In this case, A is unital, associative, central and separable of rank n^2 as a finitely generated projective k-module (Remark 25.5, Exc. 25.37 (a) and [158, III, 2.1, 2.2, 5.1]). Moreover, by [158, p. 110], there is a unique homogeneous polynomial law $\mathrm{Nrd}_A : A \to k$ of degree n over k (the *reduced norm* of A) that becomes the determinant after a faithfully flat base change of the kind mentioned above and, in particular, permits composition in the obvious sense. Up to isomorphism, the only Azumaya algebra of degree 1 is the base ring itself, while Cor. 26.9 shows that the Azumaya algebras of degree 2 are precisely the quaternion algebras over k. In this section, we will be primarily concerned with Azumaya algebras of degree 3. Their connection with cubic Jordan algebras is the subject of the following proposition.

42.7 Proposition. *A k-algebra A is an Azumaya algebra of degree 3 if and only if A is associative and $A^{(+)}$ is a Freudenthal algebra that has rank 9 as a finitely generated projective module.*

Proof If A is an Azumaya algebra of degree 3, its reduced norm combined with the Cayley-Hamilton theorem [158, IV, Corollaire 2.3] makes A a separable cubic associative algebra having rank 9 as a projective k-module. By Exc. 42.21 (a), therefore, $A_L \cong \mathrm{Mat}_3(L)$ for any algebraically closed field $L \in k\text{-}\mathbf{alg}$, forcing $A_L^{(+)} \cong \mathrm{Her}_3(L \times L)$ by Thm. 39.6 and Cor. 39.7 to be a simple cubic Jordan algebra over L. Hence $A_K^{(+)}$ is a simple cubic Jordan algebra over K, for any field $K \in k\text{-}\mathbf{alg}$, and we conclude from 39.8 that $A^{(+)}$ is a Freudenthal algebra over k.

Conversely, assume A is associative and $A^{(+)}$ is a Freudenthal algebra over k having rank 9 as a finitely generated projective module. Then $A_K^{(+)}$ is simple, for any field $K \in k\text{-}\mathbf{alg}$, and hence so is A_K, forcing A itself to be separable. By [158, III, 5.1], therefore, it remains to show that A is central. By Cor. 39.32 and 39.20, there exists a faithfully flat k-algebra R making $A_R^{(+)} \cong \mathrm{Mat}_3(R)^{(+)}$ split over R. By faithful flatness, it suffices to show that A_R is central. Letting x be a

central element of A_R, the left multiplication operator of x in A_R commutes with the operators $U_y, V_{y,z}$ $(y, z \in A_R)$ of $A_R^{(+)}$, hence belongs to the outer centroid of $A_R^{(+)}$. But by Exc. 37.25, the outer centroid of $A_R^{(+)} \cong \mathrm{Her}_3(R \times R)$ is trivial, and we conclude $x \in R1_{A_R}$, as desired. □

After these preparations, we are now ready for the definition of Kummer elements[1].

42.8 The concept of a Kummer element. Let (J_0, V) be a complemented cubic Jordan subalgebra of J in the sense of 35.2. This amounts to the following: $J_0 \subseteq J$ is a cubic Jordan subalgebra (in particular, $J_0^\sharp \subseteq J_0$) and $V \subseteq J$ is a k-submodule such that

$$J = J_0 \oplus V, \quad V \subseteq J_0^\perp, \quad J_0 \,.\, V \subseteq V, \tag{1}$$

where $J_0^\perp$ stands for the orthogonal complement of J_0 relative to the bilinear trace of J and $x \,.\, v = -x \times v$ as in (35.1.2) for $x \in J_0$ and $v \in V$. By a *Kummer element* of J relative to (J_0, V), we mean an element $l \in J$ satisfying

(i) the *invertibility condition*: l is invertible in J,
(ii) the *strong orthogonality condition*: l and $l^\sharp$ both belong to V,
(iii) the *stability condition*: $J_0 \,.\, (J_0 \,.\, l) \subseteq J_0 \,.\, l$.

In particular, l is strongly orthogonal to (J_0, V) in the sense of 35.5. Clearly, if $l \in J$ is a Kummer element relative to (J_0, V), then $l_R \in J_R$ is a Kummer element relative to $(J_0, V)_R = (J_{0R}, V_R)$, for all $R \in k$-**alg**. Also, since the linear map $x \mapsto x \,.\, l$ from J_0 to V is injective, by the invertibility condition (i) and (35.5.3), the stability condition (iii) produces a unique non-associative k-algebra structure

$$A_l = A_l(J, J_0, V) \tag{2}$$

living on the k-module J_0 through the multiplication $(x, y) \mapsto xy$ defined by

$$x \,.\, (y \,.\, l) = (xy) \,.\, l \qquad\qquad (x, y \in J_0). \tag{3}$$

Note that if $l \in J$ is a Kummer element relative to (J_0, V), then so is αl, for any $\alpha \in k^\times$, and $A_{\alpha l} = A_l$. Also, the construction of A_l is compatible with base change:

$$A_l(J, J_0, V)_R = A_{l_R}(J_R, J_{0R}, V_R) \tag{4}$$

for all $R \in k$-**alg**.

[1] In [220, 8.5], Kummer elements are called *pure elements*.

If J_0 is regular, then $V = J_0^\perp$, allowing us to simplify terminology and notation, so we speak of a Kummer element of J relative to J_0 (rather than $(J_0, J_0^\perp)$), and we abbreviate

$$A_l(J, J_0) := A_l(J, J_0, J_0^\perp). \tag{5}$$

42.9 Example. Let J be a cubic Jordan algebra over k and assume $3 \in k^\times$. Then $k1_J \subseteq J$ is a regular cubic Jordan subalgebra isomorphic to $k^{(+)}$ and $(k1_J)^\perp = \mathrm{Ker}(T_J)$ is the kernel of the linear trace of J. Hence $l \in J$ is a Kummer element relative to $k1_J$ if and only if $l \in (k1_J)^\perp$ satisfies $l^3 = \mu 1_J$, for some $\mu \in k^\times$, i.e., l is a Kummer element of J in the sense of Thakur [275, p. 431].

42.10 Theorem (The internal first Tits construction)**.** *Let J be a cubic Jordan algebra over k and (J_0, V) a complemented cubic Jordan subalgebra of J. If l is a Kummer element of J relative to (J_0, V), then so is $l^\sharp$, and the following statements hold.*

(a) $N_{A_l} := N_{J_0}$ *makes* $A_l = A_l(J, J_0, V)$ *a cubic alternative k-algebra, and* $A_l^{(+)} = J_0$ *as cubic Jordan algebras.*

(b) $A_{l^\sharp} = A_l^{\mathrm{op}}$.

(c) *With* $\mu := N_J(l)$, *the equations*

$$1_J = 1_{A_l} + 0 \,.\, l + 0 \,.\, l^\sharp, \tag{1}$$

$$(x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp)^\sharp = (x_0^\sharp - \mu x_1 x_2) + (\mu x_2^\sharp - x_0 x_1) \,.\, l + (x_1^\sharp - x_2 x_0) \,.\, l^\sharp, \tag{2}$$

$$N_J(x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp) = N_{A_l}(x_0) + \mu N_{A_l}(x_1) + \mu^2 N_{A_l}(x_2) - \mu T_{A_l}(x_0 x_1 x_2) \tag{3}$$

hold strictly for all $x_0, x_1, x_2 \in A_l$.

In (3), the expression $T_{A_l}(x_0 x_1 x_2)$ is unambiguous because of (a) and (42.1.1).

Proof Abbreviating $N := N_J$, $T := T_J$, $S := S_J$, $N_0 := N_{J_0}$, $T_0 := T_{J_0}$, $S_0 := S_{J_0}$, we first prove (a), (b) by proceeding in several steps.

1°. *A_l is unital with $1_{A_l} = 1_J =: 1$ and*

$$U_x y = x(yx) \tag{4}$$

for all $x, y \in A_l$. The first part follows immediately from (42.8.3) and (35.4.1). Similarly, from (35.4.3) we deduce $(U_x y) \,.\, l = x \,.\, (y \,.\, (x \,.\, l)) = (x(yx)) \,.\, l$, and (4) holds.

2°. *Squares and cubes in J_0 and A_l are the same.* Put $y = 1, x$ in (4).

3°. *N_0 permits composition on A_l* : $N_0(xy) = N_0(x)N_0(y)$ *holds strictly for all* $x, y \in A_l$. Indeed, applying (35.4.5), we obtain $N_0(xy)N(l) = N((xy) \,.\, l) = N(x \,.\, (y \,.\, l)) = N_0(x)N(y \,.\, l) = N_0(x)N_0(y)N(l)$, and since $\mu = N(l) \in k$ is invertible, the assertion follows.

4°. *A_l is left alternative.* From 2°, (35.4.1) and (35.4.3) we deduce $x \,.\, (x \,.\, v) = x \,.\, (1 \,.\, (x \,.\, v)) = (U_x 1) \,.\, v = x^2 \,.\, v$ for all $x \in A_l$, $v \in V$. Given $y \in A_l$, this implies $(x^2 y) \,.\, l = x^2 \,.\, (y \,.\, l) = x \,.\, (x \,.\, (y \,.\, l)) = x \,.\, ((xy) \,.\, l) = (x(xy)) \,.\, l$, hence the left alternative law.

5°. *$T_0(xy) = T_0(x, y)$ for all $x, y \in A_l$.* By Prop. 12.24, we may assume that x is invertible in J_0. Then (35.4.4) yields $x \,.\, (x^{-1} \,.\, v) = v$ for all $v \in V$, and for $y \in J_0$ we conclude $(x(x^{-1}y)) \,.\, l = x \,.\, ((x^{-1}y) \,.\, l) = x \,.\, (x^{-1} \,.\, (y \,.\, l)) = y \,.\, l$, hence $x(x^{-1}y) = y$. We now change scalars to $R := k[\varepsilon]$, $\varepsilon^2 = 0$, and then use 3°, which holds in all scalar extensions, to expand both sides of

$$N_0(x)N_0(1 + \varepsilon x^{-1}y) = N_0\big(x(1 + \varepsilon x^{-1}y)\big) = N_0(x + \varepsilon y).$$

Comparing coefficients of ε yields $T_0(x^\sharp, y) = N_0(x)T_0(x^{-1}y) = T_0(x^\sharp y)$. Replacing x by $x^\sharp$, the assertion follows from the adjoint identity.

6°. *$l^\sharp$ is a Kummer element of J relative to (J_0, V) and $A_{l^\sharp} = A_l^{\mathrm{op}}$.* From (33.8.18) we conclude that $l^\sharp$ is invertible in J, while the adjoint identity implies that $l^\sharp$ satisfies the strong orthogonality condition. Therefore the assertion will follow once we have shown the stability condition in the form $x \,.\, (y \,.\, l^\sharp) = (yx) \,.\, l^\sharp$ for all $x, y \in J_0$. In order to do so, we combine (35a.6), (35a.2) and (42.8.3) with 5° to obtain

$$\begin{aligned} x \,.\, (y \,.\, l^\sharp) &= T_0(x, y)l^\sharp - ((yx) \,.\, l) \times l = T_0(x, y)l^\sharp - ((yx) \times 1) \,.\, l^\sharp \\ &= \Big((T_0(y, x) - T_0(yx))1 + yx\Big) \,.\, l^\sharp = (yx) \,.\, l^\sharp, \end{aligned}$$

as claimed.

Combining 6° with 4° for $l^\sharp$ and with 1°, it follows that A_l is alternative such that $A_l^{(+)} = J_0$. In fact, N_0 by 3° makes A_l a cubic alternative k-algebra. This completes the proof of (a) and (b).

(c) To begin with, (1) is obvious. In order to establish (2), we invoke (b) and (35a.1), (35a.10), (35a.3) to obtain

$$\begin{aligned} (x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp)^\sharp &= x_0^\sharp + x_0 \times (x_1 \,.\, l) + x_0 \times (x_2 \,.\, l^\sharp) \\ &\quad + (x_1 \,.\, l)^\sharp + (x_1 \,.\, l) \times (x_2 \,.\, l^\sharp) + (x_2 \,.\, l^\sharp)^\sharp \\ &= x_0^\sharp - (x_0 x_1) \,.\, l - (x_2 x_0) \,.\, l^\sharp + x_1^\sharp \,.\, l^\sharp \\ &\quad + ((x_1 x_2) \,.\, l) \times l^\sharp + \mu x_2^\sharp \,.\, l \end{aligned}$$

$$= (x_0^\sharp - \mu x_1 x_2) + (\mu x_2^\sharp - x_0 x_1) \,.\, l + (x_1^\sharp - x_2 x_0) \,.\, l^\sharp,$$

as desired. Finally, in order to establish (3), we use Exc. 12.40 (a) to expand the left-hand side:

$$\begin{aligned} N(x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp) = {} & N_0(x_0) + N(x_1 \,.\, l) + N(x_2 \,.\, l^\sharp) + T(x_0^\sharp, x_1 \,.\, l) \\ & + T(x_0^\sharp, x_2 \,.\, l^\sharp) + T(x_0, (x_1 \,.\, l)^\sharp) + T((x_1 \,.\, l)^\sharp, x_2 \,.\, l^\sharp) \\ & + T(x_0, (x_2 \,.\, l^\sharp)^\sharp) + T(x_1 \,.\, l, (x_2 \,.\, l^\sharp)^\sharp) \\ & + T(x_0 \times (x_1 \,.\, l), x_2 \,.\, l^\sharp). \end{aligned} \tag{5}$$

Here $N(x_1 \,.\, l) = \mu N_0(x_1)$ by (35.4.5), while this and (33a.18) yield $N(x_2 \,.\, l^\sharp) = \mu^2 N_0(x_2)$. Since $J_0 \,.\, V \subseteq V \subseteq J_0^\perp$, we have $T(x_0^\sharp, x_1 \,.\, l) = T(x_0^\sharp, x_2 \,.\, l^\sharp) = 0$. From (35a.1) we deduce $(x_1 \,.\, l)^\sharp = x_1^\sharp \,.\, l^\sharp$, $(x_2 \,.\, l^\sharp)^\sharp = \mu x_2^\sharp \,.\, l$, hence

$$T(x_0, (x_1 \,.\, l)^\sharp) = T(x_0, (x_2 \,.\, l^\sharp)^\sharp) = 0.$$

Combining with (35a.4) yields

$$T((x_1 \,.\, l)^\sharp, x_2 \,.\, l^\sharp) = T(x_1^\sharp \,.\, l^\sharp, x_2 \,.\, l^\sharp) = 0 = \mu T(x_1 \,.\, l, x_2^\sharp \,.\, l) = T(x_1 \,.\, l, (x_2 \,.\, l^\sharp)^\sharp).$$

Finally, by (35a.5),

$$T(x_0 \times (x_1 \,.\, l), x_2 \,.\, l^\sharp) = -T((x_0 x_1) \,.\, l, x_2 \,.\, l^\sharp) = -\mu T_0(x_0 x_1, x_2) = -\mu T_0(x_0 x_1 x_2).$$

Plugging all this into (5), we end up with (3). □

42.11 Theorem (The external first Tits construction)**.** *Let A be a cubic alternative algebra over k. If $\mu \in k$ is an arbitrary scalar, then the direct sum*

$$J := A \oplus A j_1 \oplus A j_2 \tag{1}$$

of three copies of A as a k-module, into which A naturally embeds through the initial summand, carries the unique structure of a cubic Jordan algebra over k whose identity element, adjoint and norm are respectively given by the strict validity of the formulas

$$1_J = 1_A, \tag{2}$$

$$x^\sharp = (x_0^\sharp - \mu x_1 x_2) + (\mu x_2^\sharp - x_0 x_1) j_1 + (x_1^\sharp - x_2 x_0) j_2, \tag{3}$$

$$N_J(x) = N_A(x_0) + \mu N_A(x_1) + \mu^2 N_A(x_2) - \mu T_A(x_0 x_1 x_2), \tag{4}$$

for all $x = x_0 + x_1 j_1 + x_2 j_2 \in J$, $x_0, x_1, x_2 \in A$. Moreover, with another element $y = y_0 + y_1 j_1 + y_2 j_2 \in J$, $y_0, y_1, y_2 \in A$, the bilinearized adjoint, trace and

(*bilinearized*) *quadratic trace of J have the form*

$$\begin{aligned} x \times y &= (x_0 \times y_0 - \mu x_1 y_2 - \mu y_1 x_2) + (\mu x_2 \times y_2 - x_0 y_1 - y_0 x_1) j_1 \\ &\quad + (x_1 \times y_1 - x_2 y_0 - y_2 x_0) j_2, \end{aligned} \tag{5}$$

$$T_J(x,y) = T_A(x_0,y_0) + \mu T_A(x_1,y_2) + \mu T_A(x_2,y_1), \tag{6}$$

$$T_J(x) = T_A(x_0), \tag{7}$$

$$S_J(x) = S_A(x_0) - \mu T_A(x_1,x_2), \tag{8}$$

$$S_J(x,y) = S_A(x_0,y_0) - \mu T_A(x_1,y_2) - \mu T_A(x_2,y_1). \tag{9}$$

Proof Thanks to Cor. 34.6, the first part will follow once we have shown that the k-module J together with base point, adjoint, and norm defined by (2)–(4) is a cubic norm structure X over k. It is certainly a cubic array, and setting $N := N_X$, $T := T_X$, $S := S_X$, $N_0 := N_A$, $T_0 := T_A$, $S_0 := S_A$, we obtain

$$\begin{aligned} N(x,y) &= N_0(x_0,y_0) + \mu N_0(x_1,y_1) + \mu^2 N_0(x_2,y_2) \\ &\quad - \mu T_0(y_0 x_1 x_2 + x_0 y_1 x_2 + x_0 x_1 y_2) \end{aligned} \tag{10}$$

which implies (5)–(9) in a straightforward manner; details are left to the reader. This done, we can now tackle the defining identities (33.4.1), (33.4.2), (33.4.3) of a cubic norm structure. They certainly hold for the elements of A. Hence the unit identity follows immediately from (5) and (6). Moreover, (3), (4), (6) imply

$$\begin{aligned} T(x^\sharp, y) &= T_0(x_0^\sharp - \mu x_1 x_2, y_0) + \mu T_0(\mu x_2^\sharp - x_0 x_1, y_2) + \mu T_0(x_1^\sharp - x_2 x_0, y_1) \\ &= N_0(x_0,y_0) + \mu^2 N_0(x_2,y_2) + \mu N_0(x_1,y_1) \\ &\quad - \mu T_0(x_1 x_2 y_0 + x_0 x_1 y_2 + x_2 x_0 y_1), \end{aligned}$$

and comparing with (10), the gradient identity follows. Finally, turning to the adjoint identity, we abbreviate $x^\sharp = z_0 + z_1 j_1 + z_2 j_2$, $x^{\sharp\sharp} = w_0 + w_1 j_1 + w_2 j_2$, for some $z_i, w_i \in A$, $i = 0,1,2$ and must show $w_i = N(x) x_i$. Indeed, (4), Prop. 42.1, the middle Moufang identity (13.3.3), and (33.8.15) imply

$$\begin{aligned} w_0 &= z_0^\sharp - \mu z_1 z_2 \\ &= x_0^{\sharp\sharp} - \mu x_0^\sharp \times (x_1 x_2) + \mu^2 (x_1 x_2)^\sharp - \mu^2 x_2^\sharp x_1^\sharp \\ &\quad + \mu^2 x_2^\sharp (x_2 x_0) + \mu (x_0 x_1) x_1^\sharp - \mu (x_0 x_1)(x_2 x_0) \\ &= N_0(x_0) x_0 - \mu U_{x_0}(x_1 x_2) - \mu x_0^\sharp \times (x_1 x_2) + \mu^2 N_0(x_2) x_0 + \mu N_0(x_1) x_0 \\ &= (N_0(x_0) + \mu N_0(x_1) + \mu^2 N_0(x_2) - \mu T_0(x_0 x_1 x_2)) x_0 \\ &= N(x) x_0. \end{aligned}$$

The remaining equations $w_i = N(x) x_i$ for $i = 1,2$ can be proved similarly. □

42.12 The formal first Tits construction. Let A be a cubic alternative k-algebra and $\mu \in k$.

(a) The cubic Jordan algebra constructed in Theorem 42.11 is said to arise from A, μ by means of the *first Tits construction* and will be denoted by $J(A, \mu)$. The natural map from A to the initial summand of $J(A, \mu)$ is an embedding $A^{(+)} \hookrightarrow J(A, \mu)$ of cubic Jordan algebras; we usually identify $A^{(+)} \subseteq J(A, \mu)$ as a cubic Jordan subalgebra accordingly. Note that $V := Aj_1 \oplus Aj_2$ makes $(A^{(+)}, V)$ a complemented cubic Jordan subalgebra of $J(A, \mu)$ such that

$$x_0 \,.\, (y_1 j_1 + y_2 j_2) = (x_0 y_1) j_1 + (y_2 x_0) j_2 \tag{1}$$

for all $x_0, y_1, y_2 \in A$. *Hence $J(A, \mu)$ is generated by $A^{(+)}$ and j_1 as a Jordan k-algebra.*

(b) We have $j_1^2 = j_1^\sharp = j_2$ and hence $1_J \wedge j_1 \wedge j_1^2 \neq 0$ in every scalar extension. Thus $J(A, \mu)$ is a Jordan algebra of degree 3 over k.

(c) If $\mu \in k$ is invertible, then j_1 is a Kummer element of $J(A, \mu)$ relative to $(A^{(+)}, V)$ satisfying $j_1^\sharp = j_2$, and (1) implies

$$A_{j_1}(J, A^{(+)}, V) = A. \tag{2}$$

(d) We continue to assume that $\mu \in k$ is invertible and define a change of variables $\varphi\colon J \to J$ given by

$$\varphi(x) := x_0 + x_1 j_1 + (\mu^{-1} x_2) j_2$$

for $x = x_0 + x_1 j_1 + x_2 j_2$, $x_0, x_1, x_2 \in A$. For another quantity $y = y_0 + y_1 j_1 + y_2 j_2$, $y_0, y_1, y_2 \in A$, one checks

$$\begin{aligned} x^{\sharp'} &:= \varphi^{-1}(\varphi(x)^\sharp) = (x_0^\sharp - x_1 x_2) + (\mu^{-1} x_2^\sharp - x_0 x_1) j_1 \\ &\quad + (\mu x_1^\sharp - x_2 x_0) j_2, \end{aligned} \tag{3}$$

$$N'_J(x) := N_J(\varphi(x)) := N_A(x_0) + \mu N_A(x_1) + \mu^{-1} N_A(x_2) - T_A(x_0 x_1 x_2), \tag{4}$$

$$T'_J(x, y) := T_J(\varphi(x), \varphi(y)) = T_A(x_0, y_0) + T_A(x_1, y_2) + T_A(x_2, y_1), \tag{5}$$

$$S'_J(x) := S_J(\varphi(x)) = S_A(x_0) - T_A(x_1, x_2) \tag{6}$$

and thus arrives at formulas that are familiar from the classical first Tits construction in the literature, where it is also assumed that A be associative (see, e.g., McCrimmon [183, pp. 507–508]). Note that in these co-ordinates neither the bilinear nor the quadratic trace of $J(A, \mu)$ depends on μ.

42.13 Corollary. *Let J be a cubic Jordan algebra over k and (J_0, V) a complemented cubic Jordan subalgebra of J. If $l \in J$ is a Kummer element relative*

to (J_0, V) *and* $A_l := A_l(J, J_0, V)$ *the corresponding cubic alternative* k*-algebra, then the inclusion*

$$A_l^{(+)} = J_0 \hookrightarrow J$$

has a unique extension to a homomorphism

$$\varphi\colon J(A_l, N_J(l)) \longrightarrow J$$

of cubic Jordan algebras satisfying $\varphi(j_1) = l$*. This homomorphism is an embedding and*

$$\varphi(x_0 + x_1 j_1 + x_2 j_2) = x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp \tag{1}$$

for all $x_0, x_1, x_2 \in A$*.*

Proof Since any such homomorphism preserves (bilinearized) adjoints, it automatically satisfies (1). Conversely, defining φ in this way and comparing (42.10.1)–(42.10.3) with (42.11.2)–(42.11.4), we see that φ preserves base points, norms and adjoints, hence is a homomorphism of cubic Jordan algebras. It remains to show that φ is injective. Assume $x_0, x_1, x_2 \in A$ satisfy $x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp = 0$. Since the first summand belongs to J_0 while the other two belong to V, we conclude $x_0 = 0$ and $x_1 \,.\, l + x_2 \,.\, l^\sharp = 0$. Using (35a.2), (35a.3), this implies

$$0 = (x_1 \,.\, l) \times l + (x_2 \,.\, l^\sharp) \times l = (1 \times x_1) \,.\, l^\sharp - N_J(l) x_2,$$

hence $x_2 = 0$ and then $0 = (x_1 \,.\, l) \times l^\sharp = -N_J(l) x_1$, hence $x_1 = 0$. □

42.14 Corollary. *Let* A *be a cubic alternative* k*-algebra and* $\mu \in k$*. Then the first Tits construction* $J(A, \mu)$ *is regular if and only if* A *is regular and* μ *is invertible in* k*.*

Proof $J := J(A, \mu)$ is finitely generated projective as a k-module if and only if so is A. Let this be the case and identify J (resp. its dual J^*) with column space A^3 (resp. A^{*3}) in such a way that the canonical pairing $J^* \times J \to k$ is given by $x^{*\mathsf{T}} y$ for $x^* \in A^{*3}$, $y \in A^3$. Let $\varphi\colon A \to A^*$ (resp. $\Phi\colon J \to J^*$) be the k-linear map derived from the bilinear trace of A (resp. J). By (42.11.6) the map Φ has the matrix form

$$\Phi = \begin{pmatrix} \varphi & 0 & 0 \\ 0 & 0 & \mu\varphi \\ 0 & \mu\varphi & 0 \end{pmatrix},$$

which is invertible if and only if so are φ and μ. □

42.15 Corollary. *Let A be an Azumaya algebra of degree 3 over k and $\mu \in k^\times$. Then the first Tits construction $J(A,\mu)$ is an Albert algebra over k.*

Proof From Prop. 42.7, Cor. 39.15 and Cor. 42.14 we conclude that $J := J(A,\mu)$ is regular, while Prop. 39.2 implies that $J_K = J(A_K,\mu_K)$ not only has dimension 27 but is also simple, for any algebraically closed field $K \in k$-**alg**, since already the diagonal idempotents $e_{ii} \in A_K^{(+)} \cong \mathrm{Her}_3(K \times K)$ satisfy $(A_K^{(+)})_1(e_{ii}) \neq \{0\}$ for $1 \leq i \leq 3$. Hence $J(A,\mu)$ is an Albert algebra over k. □

Among the defining properties of Kummer elements, the stability condition (iii) of 42.8 is arguably the most delicate. Remarkably it can be ignored under some rather mild additional hypotheses pertaining to the linear algebra of the situation.

42.16 Theorem. *Let n be a positive integer and J a cubic Jordan algebra over k that is finitely generated projective of rank $r \leq 3n$ as a k-module. Assume $J_0 \subseteq J$ is a regular cubic Jordan subalgebra having rank exactly n as a projective module. For $l \in J$ to be a Kummer element relative to J_0 it is necessary and sufficient that l be invertible and strongly orthogonal to J_0. In this case, $r = 3n$ and setting $\mu := N_J(l)$, $A := A_l(J, J_0)$, there is a unique homomorphism of cubic Jordan algebras from the first Tits construction $J(A,\mu)$ to J extending the identity of J_0 and sending j_1 to l. Moreover, this homomorphism is an isomorphism, and J is regular.*

42.17 Remark. Without the rank conditions, an invertible element of J that is strongly orthogonal to J_0 may fail to be a Kummer element relative to J_0: see Exc. 42.23 (b) below for an example.

Proof Necessity being obvious, let us assume that, conversely, l is invertible and strongly orthogonal to J_0. Then so is $l^\sharp$, and from (35.1.2) we deduce

$$J_0 \,.\, l + J_0 \,.\, l^\sharp \subseteq J_0^\perp. \tag{1}$$

Now suppose $x_0, x_1, x_2 \in J_0$ satisfy $x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp = 0$. Here the first summand belongs to J_0, while the other two by (1) belong to $J_0^\perp$. Hence $x_0 = 0$ and $x_1 \,.\, l + x_2 \,.\, l^\sharp = 0$. By (35a.2), (35a.3), this implies

$$0 = (x_1 \,.\, l) \times l + (x_2 \,.\, l^\sharp) \times l = (1 \times x_1) \,.\, l^\sharp - \mu x_2,$$

and we conclude first $x_2 = 0$ and then $x_1 = 0$ as well. Thus

$$J_0[l] := J_0 \oplus J_0 \,.\, l \oplus J_0 \,.\, l^\sharp \subseteq J$$

is a finitely generated projective submodule of rank $3n$. Invoking (35a.4) for

$u = l, l^\sharp$ and (35a.5) for $u = l$, we obtain

$$T_J(x,y) = T_J(x_0,y_0) + \mu T_J(x_1,y_2) + \mu T_J(x_2,y_1)$$

for $x = x_0 + x_1 . l + x_2 . l^\sharp$, $y = y_0 + y_1 . l + y_2 . l^\sharp$, $x_i, y_i \in J_0$, $i = 0,1,2$. Hence T_J restricts to a regular symmetric bilinear form on $J_0[l]$. This implies $J = J_0[l] \oplus J_0[l]^\perp$, and comparing ranks we deduce $J_0[l]^\perp = \{0\}$, i.e.,

$$J_0[l] = J_0 \oplus J_0 . l \oplus J_0 . l^\sharp = J. \tag{2}$$

In particular, J is regular of rank $3n$. We are now in a position to tackle the stability condition, so let $x, y \in J_0$. Then $x . (y . l) \in J_0^\perp = J_0 . l + J_0 . l^\sharp$ by (1), (2), and we find $z_1, z_2 \in J_0$ such that $x . (y . l) = z_1 . l + z_2 . l^\sharp$. Hence, arguing as before,

$$(x . (y . l)) \times l = (z_1 \times 1) . l^\sharp - \mu z_2, \tag{3}$$

where the first summand on the right belongs to $J_0^\perp$. But so does the left-hand side, by (35a.6) being equal to $T_J(x,y) l^\sharp - y . (x . l^\sharp)$. Comparing $J_0^\perp$-components, (3) yields $z_2 = 0$, i.e., $x . (y . l) \in J_0 . l$, and we have established the stability condition for l. Summing up, therefore, l is a Kummer element with respect to J_0. Finally, the unique homomorphism $J(A,\mu) \to J$ of Cor. 42.13 is surjective by (2) and injective since $J(A,\mu)$ by Cor. 42.14 is regular. □

42.18 Remark. Let $J = J(D,\mu)$ be an Albert algebra arising from a first Tits construction over a field F of characteristic $\neq 3$. Any smooth compactification of the varieties defined by the equations $\mathrm{Nrd}_D = \mu$ or $\mathrm{Nrd}_J = \nu$ (for any $\mu, \nu \in F^\times$) is a norm variety in the sense of Rost [251, §3], see [258, p. 175] for a table of such examples.

Exercises

42.19. Let A be a cubic alternative k-algebra with norm N_A, (bi-)linear trace T_A, quadratic trace S_A over k and let $p, q \in A^\times$. Deduce from 33.11 and Prop. 42.1 that $A^{(p,q)}$ is a cubic alternative k-algebra with norm $N_{A^{(p,q)}} = N_A(pq)N_A$ whose linear and quadratic traces are given by

$$T_{A^{(p,q)}}(x) = T_A(pqx), \quad S_{A^{(p,q)}}(x) = S_A(q^\sharp p^\sharp x) \tag{1}$$

for all $x \in A$. In particular, the unital isotope A^p of A is a cubic alternative k-algebra with the same norm, (bi-)linear trace and quadratic trace as A.

42.20. *Cubic ideals revisited.* Let A be a cubic alternative k-algebra. By a *(separated) cubic ideal in* A we mean a pair $(\mathfrak{a}, I)$ consisting of an ideal $\mathfrak{a} \subseteq k$ and a two-sided ideal $I \subseteq A$ such that $(\mathfrak{a}, I)$ is a (separated) cubic ideal of the cubic Jordan algebra $A^{(+)}$ in the sense of Exc. 34.21. We speak of a cubic *nil* ideal in A if, in addition $(\mathfrak{a}, I)$ is a cubic nil ideal in $A^{(+)}$ in the sense of Exc. 37.21. Now let $\mu \in k$ and write $J := J(A,\mu)$ for the corresponding first Tits construction. Prove:

(a) If $(\mathfrak{a}, I)$ is a cubic (nil) ideal in A, then

$$(\mathfrak{a}, J(I,\mu)), \quad J(I,\mu) := I \oplus I j_1 \oplus I j_2 \tag{1}$$

is a cubic (nil) ideal in J. Moreover, if $(\mathfrak{a}, I)$ is separated, then so is $(\mathfrak{a}, J(I,\mu))$, and with the canonical projection $\sigma\colon k \to k_0 := k/\mathfrak{a}$, the algebra A/I carries a unique cubic alternative algebra structure over k_0 such that the canonical projection $\pi\colon A \to A/I$ becomes a σ-semi-linear homomorphism of cubic alternative algebras. Finally, $(\mathfrak{a}, I)$ still being separated, the assignment

$$x_0 + x_1 j_1 + x_2 j_2 \longmapsto \pi(x_0) + \pi(x_1) j_1 + \pi(x_2) j_2 \qquad (x_0, x_1, x_2 \in A) \tag{2}$$

canonically induces an isomorphism

$$J(A,\mu)/J(I,\mu) \xrightarrow{\sim} J(A/I, \sigma(\mu)) \tag{3}$$

of cubic Jordan algebras over k_0.

(b) $(\mathrm{Nil}(k), \mathrm{Nil}(A))$ is a cubic nil ideal in A and

$$J(\mathrm{Nil}(A), \mu) \subseteq \mathrm{Nil}\,(J(A,\mu)). \tag{4}$$

Here we never (resp. not always) have equality for $k \neq \{0\}$ and μ nilpotent (resp. $\mu = 1$).

(c) If the cubic nil ideal $(\mathrm{Nil}(k), \mathrm{Nil}(A))$ is separated, $A/\mathrm{Nil}(A)$ is regular over k_0 (cf. (a)) and $\mu \in k^\times$, then

$$\mathrm{Nil}\,(J(A,\mu)) = J(\mathrm{Nil}(A), \mu). \tag{5}$$

42.21. (a) Show that the semi-simple cubic alternative algebras over a field F up to isomorphism are precisely one of the following.

(i) F.
(ii) A purely inseparable field extension K/F of characteristic 3 and exponent 1.
(iii) A separable cubic field extension of F.
(iv) The split cubic étale F-algebra.
(v) $\hat{C} = F \times C$ in the sense of Exc. 34.24 (b), where C is a pre-composition algebra over F that is not split quadratic étale.
(vi) $\mathrm{Mat}_3(F)$.
(vii) A central associative division algebra of degree 3 over F.

(b) Let A be a cubic alternative k-algebra that is finitely generated projective of rank n as a k-module. Prove that the following conditions are equivalent.

(i) A is regular.
(ii) A is separable, and
  (a) if $A \cong k$, then $3 \in k^\times$,
  (b) if $A \cong (k \times k)_{\mathrm{cub}}$, then $2 \in k^\times$.

42.22. (a) Let A be a cubic associative k-algebra and $\mu \in k$, $p \in A$. Show that the map

$$\varphi_{A,\mu,p}\colon J(A, N_A(p)\mu) \longrightarrow J(A,\mu)$$

defined by

$$\varphi_{A,\mu,p}(x) := x_0 + (x_1 p) j_1 + (p^\sharp x_2) j_2 \tag{1}$$

for all $x = x_0 + x_1 j_1 + x_2 j_2$ with $x_0, x_1, x_2 \in A$ is a homomorphism of cubic Jordan algebras. Moreover, $\varphi_{A,\mu,p}$ is an isomorphism if and only if p is invertible in A.

(b) Let A be an Azumaya algebra of degree 3 over k and $\mu, \nu \in k^\times$. Show for any map $\varphi\colon J(A,\nu) \to J(A,\mu)$ that the following conditions are equivalent.

(i) φ is a homomorphism of cubic Jordan algebras extending the identity of $A^{(+)}$.

(ii) $\nu = N_A(p)\mu$ and $\varphi = \varphi_{A,\mu,p}$ for some $p \in A$.

In this case, φ is an isomorphism. (*Hint*: Prove first for $x \in A$ that $x[A,A] = \{0\}$ implies $x = 0$.)

(c) Let A be a cubic alternative k-algebra and $\mu \in k$, $p \in A^\times$. Show with the unital p-isotope A^p of A (which is a cubic alternative algebra in its own right having the same norm and, more generally, the same cubic Jordan algebra structure as A) that the map

$$\psi_{A,\mu,p}\colon J(A^p,\mu) \longrightarrow J(A, N_A(p)\mu)$$

defined by

$$\psi_{A,\mu,p}(x) := x_0 + (x_1 p^{-1})j_1 + N_A(p)^{-1}(px_2)j_2 \tag{2}$$

for all $x = x_0 + x_1 j_1 + x_2 j_2$ with $x_0, x_1, x_2 \in A$ is an isomorphism of cubic Jordan algebras such that, for another element $q \in A^\times$, the diagram

$$\begin{array}{ccc} J(A^{pq},\mu) = J((A^p)^q,\mu) & \xrightarrow{\quad\psi_{A^p,\mu,q}\quad} & J(A^p, N_A(q)\mu) \\ & {\scriptstyle \psi_{A^{pq},\mu,pq}} \searrow \quad \swarrow {\scriptstyle \psi_{A,N_A(q)\mu,p}} & \\ & J(A, N_A(pq)\mu) & \end{array} \tag{3}$$

commutes.

(d) Prove for a cubic alternative k-algebra A and $\mu \in k^\times$ that the k-linear map

$$\varphi\colon J(A,\mu) \xrightarrow{\sim} J(A^{\mathrm{op}}, \mu^{-1})$$

defined by

$$\varphi(x) := x_0 + \mu x_2 j_1 + \mu x_1 j_2 \tag{4}$$

for $x = x_0 + x_1 j_1 + x_2 j_2$ with $x_0, x_1, x_2 \in A$ is an isomorphism of cubic Jordan algebras.

42.23. Let $J := \mathrm{Her}_3(C)$ be the split Albert algebra over k, where $C := \mathrm{Zor}(k)$ is the octonion algebra of Zorn vector matrices over k. Prove:

(a) The first Tits construction $J(\mathrm{Mat}_3(k),\mu)$ is split for all $\mu \in k^\times$. (*Hint*: Reduce to the case $\mu = 1$, identify $J_0 := \mathrm{Mat}_3(k)^{(+)} = \mathrm{Her}_3(k \times k) \subseteq J$ by matching $k \times k$ with the diagonal in C and construct a Kummer element of J relative to J_0.)

(b) If $2 \in k^\times$, then $J_0 := \mathrm{Sym}_3(k)$ is a regular cubic Jordan subalgebra of J, and there exists an invertible element in J that is strongly orthogonal to J_0 but *not* a Kummer element of J relative to J_0.

42.24. Let J be an Albert algebra over an algebraically closed field F. Show that the automorphism group of J acts transitively on the nilpotent elements of index 2. (*Hint*: Recall that $u \in J$ is said to be *nilpotent of index* 2 if $u^2 = 0 \neq u$ and, in this case, use Lemma 38.4 to exhibit a cubic Jordan subalgebra J' of J that contains u and is isomorphic to $\mathrm{Mat}_3(F)^{(+)}$.)

42.25. Let A be a cubic alternative k-algebra, $\mu \in k$ and $p \in A^\times$. Prove for $x_0, x_1, x_2 \in A$ and $x = x_0 + x_1 j_1 + x_2 j_2 \in J(A,\mu)$ that

$$U_p(x) = px_0p + (p^\sharp x_1)j_1 + (x_2p^\sharp)j_2, \tag{1}$$

and

$$x^{(\sharp,p)} = p^\sharp(x_0^\sharp - \mu x_1x_2)p^{-1} + \big(p(\mu x_2^\sharp - x_0x_1)\big)j_1 + \big((x_1^\sharp - x_2x_0)p\big)j_2 \tag{2}$$

is the adjoint of x in the isotope $J(A,\mu)^{(p)}$. Show further that

$$\tilde{L}_p, \tilde{R}_p \colon J(A,\mu)^{(p)} \xrightarrow{\sim} J(A,\mu)$$

defined by

$$\tilde{L}_p(x) := px_0 + (x_1p)j_1 + (p^\sharp x_2 p^{-1})j_2, \tag{3}$$

$$\tilde{R}_p(x) := x_0p + (p^{-1}x_2p^\sharp)j_1 + (px_2)j_2 \tag{4}$$

are isomorphisms of cubic Jordan algebras such that

$$\tilde{L}_{pqp} = \tilde{L}_p\tilde{L}_q\tilde{L}_p, \quad \tilde{R}_{pqp} = \tilde{R}_p\tilde{R}_q\tilde{R}_p, \quad U_{pq} = \tilde{L}_pU_q\tilde{R}_p = \tilde{R}_qU_p\tilde{L}_q \tag{5}$$

for all $p, q \in A^\times$. But note that the relations $\tilde{L}_{pq} = \tilde{L}_p\tilde{L}_q$ and $\tilde{R}_{pq} = \tilde{R}_q\tilde{R}_p$ do not always hold, even when A is associative.

42.26. *The Springer form of a cubic étale subalgebra* (Springer [267, pp. 94–95], Springer-Veldkamp [270, pp. 163–165], Petersson-Racine [223, Prop. 2.1, 2.2]). Let J be a cubic Jordan algebra over k and $E \subseteq J$ a cubic étale subalgebra. As in 35.1, we denote by $E^\perp$ the orthogonal complement of E relative to the bilinear trace of J. Prove:

(a) The action

$$E \times E^\perp \longrightarrow E^\perp, \quad (x,u) \longmapsto x\,.\,u = -x \times u \tag{1}$$

of (35.1.2) converts $E^\perp$ into a left E-module.

(b) There is a unique map $q_E \colon E^\perp \to E$ such that

$$T_E(z, q_E(u)) = -T_J(z, u^\sharp) \tag{2}$$

for all $z \in E$, $u \in E^\perp$, and q_E is a quadratic form over E. We call q_E the *Springer form* of E (relative to J).

(c) The Springer form of E is compatible with base change in the following sense: for any $R \in k$-**alg**, $E_R \subseteq J_R$ is a cubic étale subalgebra over R satisfying $E_R^\perp = (E_R)^\perp = (E^\perp)_R$ as R-modules, and the diagram

$$\begin{array}{ccc} E_R^\perp = (E^\perp)_R & \xrightarrow[q_{E_R}]{} & E_R \\ \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle 1} \\ (E^\perp)_{R_E} & \xrightarrow[(q_E)_{R_E}]{} & R_E \end{array} \tag{3}$$

commutes, where the vertical arrow on the left is the identification (12.27.1), while the vertical arrow on the right is the identification under the switch $x \otimes r \mapsto r \otimes x$.

(d) If J is a Freudenthal algebra over k having rank $n > 3$ as a projective module, then there exists an fppf algebra $R \in k$-**alg** and a splitting of J_R matching E_R with the diagonal of $J_{0n}(R)$. Conclude that the Springer form of E is non-singular, and even regular unless $n = 6$ and 2 is not invertible in k.

(e) An element $l \in E^\perp$ is a Kummer element of J relative to E if and only if l is invertible in J and $q_E(l) = 0$. In this case, $A_l(J, E) = E$ and, setting $\lambda := N_E(l) \in k^\times$, the assignment

$$x_0 + x_1 j_1 + x_2 j_2 \longmapsto x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp$$

defines an embedding of cubic Jordan algebras from the first Tits construction $J(E, \lambda)$ to J. Finally, l is isotropic relative to q_E.

42.27. Let C be a multiplicative conic alternative k-algebra whose trace form is surjective (e.g., a regular composition algebra) and put

$$A := \mathrm{Cub}(C) = \hat{C} = k \times C \tag{1}$$

as a direct product of ideals.

(a) Regard A as a cubic alternative k-algebra by means of Exc. 34.24 (b) and prove

$$J(A, \mu) \cong \mathrm{Her}_3(C^p, \Gamma_0), \quad \Gamma_0 := \mathrm{diag}(-1, -1, 1), \tag{2}$$

for all $\mu \in k^\times$, $p \in C^\times$ by reducing to the case $\mu = 1$, $p = 1_C$ and then performing the following steps.

(i) $e_1 := (1, 0) \in A^{(+)} \subseteq J := J(A, 1)$ is an elementary idempotent with the Peirce components

$$J_2(e_1) = ke_1, \tag{3}$$
$$J_1(e_1) = C j_1 \oplus C j_2, \tag{4}$$
$$J_0(e_1) = C \oplus (ke_1) j_1 \oplus (ke_1) j_2. \tag{5}$$

(ii) Picking an element $u_0 \in C$ of trace 1, the quantities e_1,

$$e_2 := u_0 + e_1 j_1 + \big(n_C(u_0) e_1\big) j_2, \quad e_3 := \bar{u}_0 - e_1 j_1 - \big(n_C(u_0) e_1\big) j_2$$

form an elementary frame $\Omega = (e_1, e_2, e_3)$ of J.

(iii) The off-diagonal Peirce components of J relative to Ω are given by

$$J_{23} = \{v + \alpha e_1 j_1 + \big(n_C(u_0, v) - n_C(u_0)\alpha\big) e_1 j_2 \mid v \in C^0,\ \alpha \in k\}, \tag{6}$$
$$J_{31} = \{-(u_0 \bar{v}) j_1 + v j_2 \mid v \in C\}, \tag{7}$$
$$J_{12} = \{(\bar{u}_0 \bar{v}) j_1 + v j_2 \mid v \in C\}. \tag{8}$$

(iv) $\mathfrak{S} := (e_1, e_2, e_3, u_{23}, u_{31})$ with

$$u_{23} := (2u_0 - 1_C) + 2e_1 j_1 + (2n_C(u_0) - 1) e_1 j_2, \tag{9}$$
$$u_{31} := -u_0 j_1 + 1_C j_2 \tag{10}$$

is a co-ordinate system of J satisfying

$$S_J(u_{23}) = S_J(u_{31}) = 1.$$

(v) Complete the proof by showing that the map $\varphi\colon C \to C_{J,\Xi}$ defined by

$$\varphi(v) := -\big((\bar{u}_0\bar{v})j_1 + vj_2\big)$$

for all $v \in C$ is an isomorphism of conic algebras. (*Hint*: First establish the formula

$$(uv - \bar{u}\bar{v})(uw) = \big(t_C(u)n_C(u,\bar{v}) - n_C(u)t_C(v)\big)w - t_C(u)\bar{u}(\bar{v}w) \qquad (11)$$

for all $u, v, w \in C$.)

(b) Let C be an octonion algebra over k whose norm is split hyperbolic. Deduce from (a) and Exc. 37.24 that the Albert algebra $\mathrm{Her}_3(C,\Gamma)$ is split, for any diagonal matrix $\Gamma \in \mathrm{GL}_3(k)$.

Remark. We have recorded in Cor. 23.11 that octonion algebras exist whose norm is split hyperbolic but which are not split themselves. According to part (b) above, however, their difference from the split octonions is so small that it cannot be detected inside the reduced Albert algebras they determine.

43 Isotopy involutions

Before we can describe the second Tits construction of cubic Jordan algebras, it will be necessary to generalize the concept of an involution in the setting of alternative algebras. We have learned in 10.8 how to twist involutions of unital non-associative algebras by symmetric or skew-symmetric invertible elements in the nucleus. This procedure is useful when the nucleus is big, e.g., for associative algebras, but distinctly less so when it is small, e.g., when it agrees with the scalar multiples of the identity element, as happens, for example, in the case of octonions (Exc. 19.32). In the present section, we describe a way out of this impasse by introducing the notion of isotopy involution for alternative algebras that allows twisting by arbitrary symmetric or skew-symmetric invertible elements.

We begin with a simple but useful preparation.

43.1 Lemma. *Let B be a unital alternative k-algebra, $p \in B^\times$ and $\tau\colon B \to B^p$ a unital homomorphism or anti-homomorphism. Then τ preserves U-operators and arbitrary powers: $\tau \circ U_x = U_{\tau(x)} \circ \tau$ for all $x \in B$ and $\tau(x^n) = \tau(x)^n$ for all $x \in B$, $n \in \mathbb{N}$ (resp. $x \in B^\times$, $n \in \mathbb{Z}$).*

Proof By Lemma 15.10, U-operators and powers do not change when passing to the opposite or a unital isotope of B. □

43.2 The concept of an isotopy involution. Let B be a unital alternative algebra over k. By an *isotopy involution* of B we mean a pair (τ, p) satisfying the following conditions.

(i) $p \in B^\times$.
(ii) $\tau\colon B \to B^p$ is an anti-isomorphism and $\tau(p) = p$.
(iii) $\tau^2 = \mathbf{1}_B$.

In explicit terms, the first part of condition (ii) by (15.9.2) is equivalent to τ being a linear bijection satisfying

$$\tau(xy) = (\tau(y)p^{-1})(p\tau(x)) \qquad (x, y \in B). \tag{1}$$

Note that the preceding conditions are compatible in the following sense: suppose the pair (τ, p) satisfies (i), (ii). Then Lemma 43.1 implies $\tau(p^{-1}) = p^{-1}$, we obtain isomorphisms $\tau\colon B \to (B^p)^{\mathrm{op}}$, $\tau\colon B^{\mathrm{op}} \to B^p$, and functoriality 15.11 applied to the latter yields the second arrow in

$$B \xrightarrow[\tau]{} (B^p)^{\mathrm{op}} = (B^{\mathrm{op}})^{p^{-1}} \xrightarrow[\tau]{} (B^p)^{\tau(p^{-1})} = (B^p)^{p^{-1}} = B.$$

Thus, regardless of (iii), it follows from (i), (ii) alone that $\tau^2\colon B \to B$ is an isomorphism, so in the presence of (i), (ii), condition (iii) makes sense.

Trivial examples of isotopy involutions are provided by the observation that the isotopy involutions of an *associative* algebra B have the form (τ, p), where $\tau\colon B \to B$ is an ordinary involution and $p \in B^\times$ is symmetric relative to τ. Less trivial examples may be found by consulting the following lemma, which gives a first indication of twisting in the setting of alternative algebras.

43.3 Lemma. *Let (B, τ) be an alternative k-algebra with involution and suppose $q \in B^\times$ satisfies $\tau(q) = q$. Then (τ^q, q^3) with*

$$\tau^q\colon B \longrightarrow B^{q^3}, \quad x \longmapsto \tau^q(x) := q^{-1}\tau(x)q$$

is an isotopy involution of B.

Proof By Cor. 14.5, the definition of τ^q is unambiguous, and we have $(\tau^q)^2 = \mathbf{1}_B$, $\tau^q(q^3) = q^3$. From Exc. 15.17 we deduce that $L_{q^{-1}}R_q\colon B \to B^{q^3}$ is an isomorphism, forcing $\tau^q = L_{q^{-1}}R_q \circ \tau\colon B \to B^{q^3}$ to be an anti-isomorphism. □

43.4 Homomorphisms and base change. By an *alternative k-algebra with isotopy involution* we mean a triple (B, τ, p) consisting of a unital alternative k-algebra B and an isotopy involution (τ, p) of B. A *homomorphism* $h\colon (B, \tau, p) \to (B', \tau', p')$ of alternative k-algebras with isotopy involution is a unital homomorphism $h\colon B \to B'$ of k-algebras that respects the isotopy involutions: $\tau' \circ h = h \circ \tau$ and satisfies $h(p) = p'$. In this way, we obtain the category of alternative k-algebras with isotopy involution. If (B, τ, p) is an alternative k-algebra with isotopy involution over k, then $(B, \tau, p)_R := (B_R, \tau_R, p_R)$ is one over R, for any $R \in k$-**alg**, called the *scalar extension* or *base change* of (B, τ, p)

from k to R. Note that $(B, \tau, 1_B)$ is an alternative algebra with isotopy involution if and only if (B, τ) is an alternative algebra with involution.

We now proceed to assemble a few elementary properties of isotopy involutions. For the time being, we fix an alternative algebra (B, τ, p) with isotopy involution over k.

43.5 Lemma. *The following identities hold for all $x, y \in B$ and all $n \in \mathbb{Z}$.*

$$\tau(xp^n) = p^n\tau(x), \quad \tau(p^n x) = \tau(x)p^n, \tag{1}$$

$$\tau(\tau(x)(py)) = \tau(y)(px), \quad \tau\Big((\tau(x)p^{-1})y\Big) = (\tau(y)p^{-1})x, \tag{2}$$

$$\tau((xy)p) = p\tau(xy) = (p\tau(y))\tau(x), \tag{3}$$

$$\tau(p^{-1}(xy)) = \tau(xy)p^{-1} = \tau(y)(\tau(x)p^{-1}). \tag{4}$$

Proof Since τ preserves powers by Lemma 43.1, applying (43.2.1) to $y = p^n$ (resp. $x = p^n$ and $y = x$) yields (1). Using this for $n = 1$ and (43.2.1) again, we deduce $\tau(\tau(x)(py)) = (\tau(py)p^{-1})(px) = ((\tau(y)p)p^{-1})(px) = \tau(y)(px)$, hence the first relation of (2); the second one follows analogously. To derive the first relation in (3), one applies (1) for $n = 1$, while the second one is a consequence of the Moufang identities (13.3.1), (13.3.3): $p\tau(xy) = p((\tau(y)p^{-1})(p\tau(x))) = [p(\tau(y)p^{-1})p]\tau(x) = (p\tau(y))\tau(x)$. Relation (4) follows in a similar way. □

43.6 Symmetric elements. We put

$$H(B, \tau) := \mathrm{Sym}(B, \tau) := \{x \in B \mid \tau(x) = x\}, \tag{1}$$

which by Lemma 43.1 is a subalgebra of the Jordan algebra $B^{(+)}$, and by 43.2 (ii) we have $p \in H(B, \tau)$. Applying (43.5.2) for $y = x$ yields

$$\tau(x)(px), (\tau(x)p^{-1})x \in H(B, \tau) \qquad (x \in B). \tag{2}$$

By contrast,$(\tau(x)p)x$ or $\tau(x)(p^{-1}x)$ will in general *not* belong to $H(B, \tau)$ (see Exc. 43.12 below).

The twisting of isotopy involutions, which we now proceed to discuss, takes on a slightly different form from what we have seen in the case of ordinary involutions (Lemma 43.3).

43.7 Proposition. *Let $q \in H(B, \tau)^\times$. Then*

$$(B, \tau, p)^q := (B^q, \tau^q, p^q) \tag{1}$$

with

$$\tau^q(x) := q^{-1}\tau(qx), \quad p^q = pq \qquad (x \in B) \tag{2}$$

is an alternative k-algebra with isotopy involution, called the q-isotope *of* (B, τ, p)*, such that*

$$\tau^q(xq) = \tau(x)q, \tag{3}$$

$$H(B^q, \tau^q) = q^{-1}H(B, \tau) = H(B, \tau)q, \tag{4}$$

$$((B, \tau, p)^q)^{q'} = (B, \tau, p)^{qq'} \tag{5}$$

for all $x \in B$, and all $q' \in H(B^q, \tau^q)^\times$.

Proof Starting with (3), we apply Lemma 43.1 to obtain $\tau^q(xq) = q^{-1}\tau(qxq) = q^{-1}\tau(U_q x) = q^{-1}U_{\tau(q)}\tau(x) = q^{-1}[q\tau(x)q]$, and (3) follows. Setting $x = p$, this implies $\tau^q(p^q) = \tau(p)q = p^q$, while applying τ^q to (3) yields $(\tau^q)^2(xq) = \tau^q(\tau(x)q) = \tau^2(x)q = xq$, hence $(\tau^q)^2 = \mathbf{1}_{B^q}$. In order to establish (1) as an alternative k-algebra with isotopy involution, it therefore suffices to show that $\tau\colon B^q \to (B^q)^{p^q} = B^{qpq}$ is an anti-isomorphism, equivalently, that

$$(\tau^q(y)(qpq)^{-1})((qpq)\tau^q(x)) = \tau^q((xq^{-1})(qy)) \qquad (x, y \in B). \tag{6}$$

In order to do so, we replace y by yq and apply (2), (3), (43.5.3), the Moufang identities and (43.2.1) to compute

$$\begin{aligned}
(\tau^q(yq)(qpq)^{-1})((qpq)\tau^q(x)) &= \Big[\Big((\tau(y)q)q^{-1}\Big)p^{-1}\Big]q^{-1} \cdot q\Big[p\Big(q(q^{-1}\tau(qx))\Big)\Big] \\
&= (\tau(y)p^{-1})q^{-1} \cdot q(p\tau(qx)) \\
&= (\tau(y)p^{-1})q^{-1} \cdot q(p\tau(x))q \\
&= \Big((\tau(y)p^{-1})(p\tau(x))\Big)q \\
&= \tau(xy)q = \tau^q((xy)q) \\
&= \tau^q\Big((xq^{-1})(q(yq))\Big),
\end{aligned}$$

and (6) holds. It remains to establish (4), (5).While (4) follows immediately from (2), (3), we note in (5) that $(B^q)^{q'} = B^{qq'}$ by (15.9.3). Also, with $p' := p^q$ it must be borne in mind that the expression $(p')^{q'}$ has to be computed *not* in B but in B^q, so $(p')^{q'} = ((pq)q^{-1})(qq') = p(qq') = p^{qq'}$. Moreover, by (4), $\tau(qq') = qq'$, so the right-hand side of (5) makes sense. And finally, (3) gives

$$\begin{aligned}
(\tau^q)^{q'}(x(qq')) = (\tau^q)^{q'}\Big(((xq)q^{-1})(qq')\Big) &= (\tau^q(xq)q^{-1})(qq') \\
&= \tau(x)(qq') = \tau^{qq'}(x(qq'))
\end{aligned}$$

for all $x \in B$, and the proof of (5) is complete. □

43.8 Corollary. *Up to isomorphism, the alternative k-algebras with isotopy involution are precisely of the form*

$$(B, \tau, 1_B)^q = (B^q, \tau^q, q),$$

where (B,τ) is an alternative k-algebra with involution and $q \in H(B,\tau)$ is invertible. Moreover,

$$\tau^q(x) = q^{-1}\tau(x)q \qquad (x \in B). \tag{1}$$

Proof Let (B',τ',p') be an alternative k-algebra with isotopy involution and put $q := p'$. Then Prop. 43.7 implies $(B',\tau',p') = (B,\tau,1_B)^q$, with $B := (B')^{q^{-1}}$, $\tau := (\tau')^{q^{-1}}$. In particular, (B,τ) is an alternative k-algebra with involution, which combines with (43.7.2) to yield $\tau'(x) = \tau^q(x) = q^{-1}\tau(qx) = q^{-1}\tau(x)\tau(q) = q^{-1}\tau(x)q$, hence (1). □

43.9 Remark. According to Cor. 43.8, (τ^q,q) is an isotopy involution of B^q, so $\tau^q\colon B^q \to B^{q^2}$ is an anti-isomorphism. This is in agreement with Lemma 43.3 since τ^q, being an isomorphism $B \to B^{q^3\,\mathrm{op}}$ fixing q, is also one $B^q \to (B^{q^3\,\mathrm{op}})^q = (B^{q^3})^{q^{-1}\,\mathrm{op}} = B^{q^2\,\mathrm{op}}$.

43.10 Concluding remark. In order to twist involutions of alternative algebras not only by symmetric but also by skew-symmetric invertible elements (for which there is no need in the present volume), isotopy involutions would have to be generalized to *isotopy involutions of type* $\varepsilon = \pm$, the only difference being that the second condition in 43.2 (ii) would have to be replaced by $\tau(p) = \varepsilon p$. Mutatis mutandis, the results of the present section carry over to this slightly more general set-up virtually without change.

Exercises

43.11. Show that the category of alternative k-algebras with isotopy involution as defined in 43.4 is isomorphic to the category of *pointed* alternative k-algebras with involution, which we define as follows: its objects are the pairs $((B,\tau),q)$ where (B,τ) is an alternative k-algebra with involution and $q \in H(B,\tau)^\times$ is called the *base point* of $((B,\tau),q)$, while its morphisms are homomorphisms of alternative algebras with involution preserving base points.

43.12. Let A be a unital alternative k-algebra and $q \in A^\times$. Show that $(A^q \times A^{\mathrm{op}}, \varepsilon_A, p)$, where ε_A is the switch (10.4) and $p := (q^{-1},q^{-1})$, is an alternative k-algebra with isotopy involution. Show further that $(\varepsilon_A(z)p)z \in H(A^q \times A^{\mathrm{op}}, \varepsilon_A)$ for all $z \in A^q \times A^{\mathrm{op}}$ if and only if $q^2 \in \mathrm{Nuc}(A)$.

44 Involutorial systems and étale elements

The second Tits construction relies on two conceptual foundations: isotopy involutions and étale elements. Isotopy involutions for cubic (rather than arbitrary) alternative algebras are best treated within the framework of what we

call involutorial systems. The role played by étale elements in the second Tits construction, on the other hand, is akin to the one played by Kummer elements in the first.

Before entering into the proper subject matter of the present section, we recall the following observation.

44.1 The opposite and unital isotopes of cubic alternative algebras. Let B be a cubic alternative algebra over k and $p \in B^\times$. Then both B^{op} and the unital isotope B^p in the sense of 15.9 are cubic alternative k-algebras with the same norm as B: $N_{B^{\mathrm{op}}} = N_{B^p} = N_B$. This is obvious for B^{op} and follows immediately from Exc. 42.19 for B^p. By the same token, B^{op} and B^p have the same adjoint as well as the same (bi-)linear and quadratic trace as B.

44.2 The concept of an involutorial system. (a) By an *involutorial system* over k we mean a quadruple

$$\mathcal{B} = (K, B, \tau, p)$$

with the following properties.

(i) K is a composition algebra of rank $r \in \{1, 2\}$ over k, called the *core* of $\mathcal{B}$ and denoted by $\mathrm{Core}(\mathcal{B})$, so $K \cong k$ for $r = 1$ and $K \in k$-**alg** is quadratic étale for $r = 2$. We write $\iota := \iota_K \colon K \to K$, $a \mapsto \bar{a}$, for the conjugation of K, always identify $k \subseteq K$ canonically and have $H(K, \iota) = k$ by Exc. 19.32 (a).

(ii) B is a cubic alternative algebra over K.

(iii) (τ, p) is an ι-semi-linear isotopy involution of B , i.e., (τ, p) is an isotopy involution of B as an alternative k-algebra that is ι-semi-linear and makes a commutative ι-semi-linear polynomial square

$$\begin{array}{ccc} B & \xrightarrow[\tau]{} & B \\ {\scriptstyle N_B}\downarrow & & \downarrow{\scriptstyle N_B} \\ K & \xrightarrow[\iota]{} & K \end{array} \tag{1}$$

in the sense of 12.28.

We then speak, more specifically, of an involutorial system *of the r-th kind*. Involutorial systems of the second kind are also called *unitary*. By 44.1, the diagram (1) can also be written in the form

$$\begin{array}{ccc} B & \xrightarrow[\tau]{} & B^{p\,\mathrm{op}} \\ {\scriptstyle N_B}\downarrow & & \downarrow{\scriptstyle N_{B^{p\,\mathrm{op}}}} \\ K & \xrightarrow[\iota]{} & K, \end{array} \tag{2}$$

so in analogy to 34.10 (b), we may refer to τ as an ι-semi-linear isomorphism from B to $B^{p\,\mathrm{op}}$ as cubic alternative algebras over K. Note that (B, τ, p) is an alternative k-algebra with isotopy involution in the sense of 43.4.

(b) Let $\mathcal{B}' = (K', B', \tau', p')$ be another involutorial system over k. By a *homomorphism* from $\mathcal{B}$ to $\mathcal{B}'$ we mean a pair (σ, φ) such that $\sigma\colon K \to K'$ is an *iso*morphism in k-**alg**, hence an isomorphism of composition algebras, and $\varphi\colon B \to B'$ is a σ-semi-linear homomorphism of cubic alternative algebras such that $\tau' \circ \varphi = \varphi \circ \tau$ and $\varphi(p) = p'$; in particular, the σ-semi-linear polynomial square

$$\begin{array}{ccc} B & \xrightarrow[\varphi]{} & B' \\ {\scriptstyle N_B}\downarrow & & \downarrow{\scriptstyle N_{B'}} \\ K & \xrightarrow[\sigma]{} & K' \end{array} \tag{3}$$

commutes, equivalently, by Exc. 34.22 (b), φ is a σ-semi-linear homomorphism of algebras making

$$\begin{array}{ccc} B & \xrightarrow[\varphi]{} & B' \\ {\scriptstyle \sharp}\downarrow & & \downarrow{\scriptstyle \sharp'} \\ B & \xrightarrow[\varphi]{} & B' \end{array} \tag{4}$$

a commutative diagram of set maps. In this way, we obtain the category of involutorial systems over k, denoted by k-**invsys**.

(c) With $\mathcal{B}$ as in (a) and $R \in k$-**alg**, we call

$$\mathcal{B}_R := (K_R, B_R, \tau_R, p_R) \tag{5}$$

the *scalar extension* of *base change* of $\mathcal{B}$ from k to R. Identifying $R_K = K_R$ as $K-$ and as $R-$algebras, 12.27 yields the identifications $B_R = ({}_kB)_R = B_{R_K} = B_{K_R}$, under which $\tau_R = \tau \otimes_\iota \iota_R$ as a tensor product of ι-semi-linear maps in the sense of 12.26. Thus $\mathcal{B}_R$ is an involutorial system of the r-th kind over R.

44.3 Core splitness. Some of our subsequent considerations are addressed to involutorial systems (of the second kind) whose core is split quadratic étale, i.e., isomorphic to $k \times k$. More specifically, these considerations often depend on an isomorphism from the core to $k \times k$ being explicitly singled out. We therefore define a *core-split* involutorial system over k as a pair $(\mathcal{B}, \varrho)$ consisting of an involutorial system $\mathcal{B}$ over k and an isomorphism $\varrho\colon \mathrm{Core}(\mathcal{B}) \xrightarrow{\sim} k \times k$ of k-algebras. If $(\mathcal{B}', \varrho')$ is another core-split involutorial system over k, a *homomorphism* from $(\mathcal{B}, \varrho)$ to $(\mathcal{B}', \varrho')$ is a homomorphism $(\sigma, \varphi)\colon \mathcal{B} \to \mathcal{B}'$ of

involutorial k-systems such that $\varrho' \circ \sigma = \varrho$. In this way we obtain the category of core-split involutorial systems over k, denoted by k-**cosp**. Note that our definitions give rise to the forgetful functor from k-**cosp** to k-**invsys** defined by the assignment $(\mathcal{B}, \varrho) \mapsto \mathcal{B}$ on objects and the identity map on morphisms. Note further that if $(\mathcal{B}, \varrho)$ is a core-split involutorial system over k, then the *base change* $(\mathcal{B}, \varrho)_R := (\mathcal{B}_R, \varrho_R)$ is one over R, for all $R \in k$-**alg**.

44.4 Admissible scalars. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k. Since τ fixes p, hence ι fixes $N_B(p)$, we conclude $N_B(p) \in k^\times$. By an *admissible scalar* for $\mathcal{B}$ we mean a quantity $\mu \in K^\times$ such that

$$\mu\bar{\mu} = N_B(p). \tag{1}$$

If in this case $(\sigma, \varphi)\colon \mathcal{B} \to \mathcal{B}' = (K', B', \tau', p')$ is a homomorphism of involutorial systems, then $\sigma(\mu) \in K'$ is an admissible scalar for $\mathcal{B}'$. Equation (1) looks like a rather restrictive condition but, actually, it isn't: for any $\mu \in K^\times$, put $\alpha := \mu\bar{\mu}N_B(p)^{-1} \in k^\times$, $p_1 := \alpha p$ and $\mu_1 := \alpha\mu \in K^\times$. Then $\mathcal{B}_1 := (K, B, \tau, p_1)$ is an involutorial system over k and μ_1 is an admissible scalar for $\mathcal{B}_1$.

44.5 Associativity conventions. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and μ an admissible scalar for $\mathcal{B}$. By (44.4.1), the link between $\mathcal{B}$ and μ is provided solely by the quantity p, regardless of whether B is associative or not. On the other hand, if B is associative, then p becomes completely isolated from the rest of $\mathcal{B}$ since $B^p = B$ and $\tau\colon B \to B$ is a K/k-involution of B. This observation gives rise to the following terminological shift: by an *associative involutorial system* over k, we mean a triple $\mathcal{B} = (K, B, \tau)$ consisting of a composition algebra K of rank $r \in \{1, 2\}$ over k, a cubic associative algebra B over K, and a K/k-involution τ of B. By abuse of language, an *admissible scalar* for $\mathcal{B}$ is then defined as a pair (p, μ) consisting of invertible elements $p \in H(B, \tau)$, $\mu \in K$ satisfying (44.4.1), i.e., $n_K(\mu) = N_B(p)$.

Our approach to the second Tits construction relies heavily on Thm. 42.16. It is therefore convenient to introduce the following terminology.

44.6 Balanced pairs of cubic Jordan algebras. A pair (J, J_0) of cubic Jordan algebras over k is said to be *balanced* if the following conditions hold.

(i) $J_0 \subseteq J$ is a regular cubic Jordan subalgebra of rank $n \in \mathbb{N}$.
(ii) As a k-module, J is finitely generated projective of rank $3n$.

In this case we say, more specifically, that the pair (J, J_0) is *n-balanced*. By a *homomorphism* $\varphi\colon (J, J_0) \to (J', J_0')$ between balanced pairs of cubic Jordan k-algebras we mean a homomorphism $\varphi\colon J \to J'$ of cubic Jordan algebras

satisfying $\varphi(J_0) \subseteq J_0'$. In this way, we obtain the category of balanced pairs of cubic Jordan algebras, denoted by k-**bapa**.

44.7 Examples: the first Tits construction and balanced pairs. Denote by k-$\mathbf{cual}_{\mathrm{reg}}$ the full subcategory of k-**cual** consisting of all regular cubic alternative k-algebras of finite constant rank as projective k-modules and fix a scalar $\lambda \in k^\times$. Consider the category k-$\mathbf{bapaku}_\lambda$, whose objects are triples (J, J_0, l) consisting of balanced pairs (J, J_0) of cubic Jordan k-algebras and Kummer elements $l \in J$ relative to J_0 such that $N_J(l) = \lambda$. Its morphisms, on the other hand, are defined as balanced pair homomorphisms respecting the corresponding Kummer elements. By Theorem 42.11 (see also 42.12), the first Tits construction determines a functor

$$\mathbf{J}(-, \lambda)\colon k\text{-}\mathbf{cual}_{\mathrm{reg}} \xrightarrow{\sim} k\text{-}\mathbf{bapaku}_\lambda$$

defined by

$$\mathbf{J}(A, \lambda) := (J(A, \lambda), A^{(+)}, j_1)$$

on objects $A \in k$-$\mathbf{cual}_{\mathrm{reg}}$ and

$$\mathbf{J}(\varphi, \lambda) := J(\varphi, \lambda)\colon \mathbf{J}(A, \lambda) \longrightarrow \mathbf{J}(A', \lambda)$$

on morphisms $\varphi\colon A \to A'$ in k-$\mathbf{cual}_{\mathrm{reg}}$. In fact, $\mathbf{J}(-, \lambda)$ *is an equivalence of categories*, the opposite functor being given by the assignments

$$(J, J_0, l) \longmapsto A_l(J, J_0)$$

on objects and

$$(\varphi\colon (J, J_0, l) \longrightarrow (J', J_0', l')) \longmapsto (\varphi|_{J_0}\colon J_0 \longrightarrow J_0')$$

on morphisms.

44.8 Étale elements. Let (J, J_0) be a balanced pair of cubic Jordan algebras over k. We write N (resp. N_0) for the norm of J (resp. J_0), ditto for the various traces. In view of 44.6 (i), we obtain a direct sum decomposition $J = J_0 \oplus J_0^\perp$ of k-modules and, thanks to 35.6, have the quadratic maps $Q\colon J_0^\perp \to J_0$, $H\colon J_0^\perp \to J_0^\perp$ given by $u^\sharp = -Q(u) + H(u)$ for all $u \in J_0^\perp$. Now let $w \in J_0^\perp$. Then

$$K := K_w := k[\mathbf{t}]\Big/\big(\mathbf{t}^2 - N(w)\mathbf{t} + N_0(Q(w))\big) \tag{1}$$

is a quadratic k-algebra that is free of rank 2 as a k-module, with basis $1_K, \xi$, where ξ stands for the canonical image of $\mathbf{t}$ in K. Thus (1) implies

$$\begin{aligned} K =& k[\xi], \quad \xi^2 - N(w)\xi + N_0(Q(w))1_K = 0, \\ & t_K(\xi) = N(w), \quad n_K(\xi) = N_0(Q(w)). \end{aligned} \tag{2}$$

Hence the discriminant of K/k is given by

$$\Delta := \Delta_w = N(w)^2 - 4N_0(Q(w)), \tag{3}$$

and one checks

$$n_K(\xi - \bar{\xi}) = -\Delta. \tag{4}$$

In the sequel, we identify $k \subseteq K$, $J \subseteq J_K$, $J_0 \subseteq J_{0K}$, $J_0^\perp \subseteq (J_0^\perp)_K$ canonically. Changing scalars from k to K, we then obtain

$$J_K = J \oplus \xi J,\ J_{0K} = J_0 \oplus \xi J_0,\ (J_0^\perp)_K = J_0^\perp \oplus \xi J_0^\perp. \tag{5}$$

By an *étale element* of J relative to J_0 we mean an element $w \in J_0^\perp$ such that

$$Q(w) \in J_0^\times, \quad \Delta = N(w)^2 - 4N_0(Q(w)) \in k^\times, \tag{6}$$

equivalently, by Prop. 19.8, the algebra $K = k[\xi]$ is quadratic étale over k and $\xi \in K^\times$. The property of an element of J to be étale relative to J_0 is stable under base change in the obvious sense.

44.9 Lemma. *Let (J, J_0) be a balanced pair of cubic Jordan algebras over k and suppose w is an étale element of J relative to J_0. With the notation of 44.8,*

$$l := l_w := -Q(w)\,.\,H(w) + \xi w \in J_{0K}^\perp \subseteq J_K \tag{1}$$

is a Kummer element of J_K relative to J_{0K} satisfying

$$\mu := \mu_w := N(l) = \Delta\Big(-2N_0(Q(w)) + N(w)\xi\Big), \quad n_K(\mu) = -\Delta^3 N_0(Q(w)). \tag{2}$$

Proof Using (35b.11), (35b.1), (35b.9), (44.8.2) and expanding yields

$$\begin{aligned} Q(l) &= \xi^2 Q(w) - \xi Q(w, Q(w)\,.\,H(w)) + Q(Q(w)\,.\,H(w)) \\ &= \Big(\xi^2 - N(w)\xi + N_0(Q(w))\Big)Q(w) = 0. \end{aligned}$$

Hence l is strongly orthogonal to J_0 and by Theorem 42.16, it suffices to show that l is invertible in J_K. This in turn will follow once we have established (2). In order to do so, we first prove

$$T(w, Q(w)^\sharp\,.\,w) = 6N_0(Q(w)) = T(w^\sharp, Q(w)\,.\,H(w)), \tag{3}$$

$$T\Big(w, Q(w)^\sharp\,.\,(Q(w)\,.\,H(w))\Big) = 3N_0(Q(w))N(w) = T\Big(w, (Q(w)\,.\,H(w))^\sharp\Big). \tag{4}$$

Indeed,

$$T(w, Q(w)^\sharp\,.\,w) = -T(w, Q(w)^\sharp \times w) = -T(Q(w)^\sharp, w \times w) = 2T(Q(w)^\sharp, Q(w)),$$

and the first relation of (3) follows from Euler's differential equation. Similarly, (35b.9) implies

$$\begin{aligned} T(w^\sharp, Q(w)\,.\,H(w)) &= -T(H(w), Q(w)\times H(w)) = -2T(Q(w), H(w)^\sharp) \\ &= 2T\Big(Q(w), Q(H(w))\Big) = 2T(Q(w), Q(w)^\sharp), \end{aligned}$$

and the second equation of (3) follows as well. Next, applying (35.4.4), we conclude

$$T(w, Q(w)^\sharp\,.\,(Q(w)\,.\,H(w))) = N_0(Q(w))T(w, H(w)) = N_0(Q(w))T(w, w^\sharp),$$

giving the first equation of (4). As to the second, we apply the first, (35b.5), (35b.10) and (3) to obtain

$$\begin{aligned} T\Big(w, (Q(w)\,.\,H(w))^\sharp\Big) &= T\Big(w, H(Q(w)\,.\,H(w))\Big) = T\Big(w, Q(w)^\sharp\,.\,H(H(w))\Big) \\ &= N(w)T(w, Q(w)^\sharp\,.\,w) - T\Big(w, Q(w)^\sharp\,.\,(Q(w)\,.\,H(w))\Big) \\ &= 3N_0(Q(w))N(w), \end{aligned}$$

as claimed. Expanding $N(l)$ by using (3), (4), (35.4.5), (35b.18), we obtain $N(l) = g(\xi)$, where

$$\begin{aligned} g(\mathbf{t}) = N(w)\mathbf{t}^3 - 6N_0(Q(w))\mathbf{t}^2 + 3N(w)N_0(Q(w))\mathbf{t} \\ - \Big(N(w)^2 - 2N_0(Q(w))\Big)N_0(Q(w)) \end{aligned}$$

and $f(\mathbf{t}) = \mathbf{t}^2 - N(w)\mathbf{t} + N_0(Q(w)) \in k[\mathbf{t}]$ satisfy

$$g(\mathbf{t}) = \Big(N(w)\mathbf{t} - 6N_0(Q(w)) + N(w)^2\Big)f(\mathbf{t}) + \Delta\Big(N(w)\mathbf{t} - 2N_0(Q(w))\Big).$$

Since $f(\xi) = 0$ by (44.8.2), we deduce $N(l) = g(\xi) = \Delta(N(w)\xi - 2N_0(Q(w)))$, hence the first equation of (2). The second one follows from (44.8.3) and

$$\begin{aligned} n_K\Big(N(w)\xi - 2N_0(Q(w))\Big) &= \Big(N(w)\xi - 2N_0(Q(w))\Big)\Big(N(w)\bar{\xi} - 2N_0(Q(w))\Big) \\ &= N(w)^2N_0(Q(w)) - 2N(w)^2N_0(Q(w)) \\ &\quad + 4N_0(Q(w))^2 \\ &= -\Delta N_0(Q(w)). \end{aligned}$$

□

44.10 Enter the first Tits construction. In the situation of Lemma 44.9, we put

$$B := B_w := A_l(J_K, J_{0K}) = A_{l_w}(J_{K_w}, J_{0K_w}) \tag{1}$$

as a cubic alternative algebra over K, with norm $N_B = N_0 \otimes K$. By Thm. 42.16, there is a canonical identification of the first Tits construction

$$J(B, \mu) = B \oplus Bj_1 \oplus Bj_2 \tag{2}$$

over K with J_K that matches $B^{(+)}$ with J_{0K} as cubic Jordan algebras and j_1 with l, hence $j_2 = j_1^\sharp$ with $l^\sharp$. In particular, B is a regular cubic alternative K-algebra. Letting $\iota = \iota_K$ act on J_K and J_{0K} through the second factor, we obtain ι-semi-linear maps

$$\chi := \chi_w := \mathbf{1}_J \otimes \iota \colon J_K \longrightarrow J_K, \quad \tau := \tau_w := \mathbf{1}_{J_0} \otimes \iota \colon J_{0K} \longrightarrow J_{0K} \tag{3}$$

that by (12.29.1) give rise to commuting ι-semi-linear polynomial squares:

$$\begin{array}{ccc} J_K & \xrightarrow[\chi]{} & J_K \\ \sharp\downarrow & & \downarrow\sharp \\ J_K & \xrightarrow[\chi]{} & J_K \\ {\scriptstyle N\otimes K}\downarrow & & \downarrow{\scriptstyle N\otimes K} \\ K & \xrightarrow[\iota]{} & K, \end{array} \qquad \begin{array}{ccc} J_{0K} & \xrightarrow[\tau]{} & J_{0K} \\ \sharp\downarrow & & \downarrow\sharp \\ J_{0K} & \xrightarrow[\tau]{} & J_{0K} \\ {\scriptstyle N_0\otimes K}\downarrow & & \downarrow{\scriptstyle N_0\otimes K} \\ K & \xrightarrow[\iota]{} & K. \end{array} \tag{4}$$

In the sense of 34.10, therefore, $\chi \colon J_K \to J_K$ and $\tau \colon B^{(+)} \to B^{(+)}$ are ι-semi-linear homomorphisms of cubic Jordan algebras over K. We clearly have

$$\chi(x_0 \,.\, u) = \tau(x_0) \,.\, \chi(u) \qquad\qquad (x_0 \in J_{0K},\ u \in J_{0K}^\perp), \tag{5}$$

and since K is étale over k, we deduce $\xi - \bar{\xi} \in K^\times$ from (44.8.4), (44.8.6), which combines with (4) to imply

$$H(J_K, \chi) = J, \quad H(J_{0K}, \tau) = J_0. \tag{6}$$

44.11 Base change. Under the natural identifications, particularly those described in 12.27 and 44.2 (c), the preceding constructions are compatible with base change: if (J, J_0) is a balanced pair of cubic Jordan algebras over k, then (J_R, J_{0R}) is one over R, for any $R \in k$-**alg**. Given $w \in J_0^\perp \subseteq J$, then $w_R \in J_{0R}^\perp \subseteq J_R$ and $K_{w_R} = (K_w)_R$. Moreover, if $w \in J$ is étale relative to J_0, then so is $w_R \in J_R$ relative to J_{0R}, and $l_{w_R} = (l_w)_{R_K}$, $B_{w_R} = B_{R_K} = ({}_kB)_R$ and $\tau_{w_R} = (\tau_w)_R$.

44.12 Theorem (The internal second Tits construction)**.** *Let (J, J_0) be a balanced pair of cubic Jordan algebras over k and suppose w is an étale element of J relative to J_0. With the notation of 44.8 through 44.10, the following statements hold.*

(a) *There is a unique element $p_w \in B$ such that $\chi_w(j_1) = (\mu^{-1} p_w) j_2$.*

(b) *$\mathcal{B} := \mathcal{B}_w := (K_w, B_w, \tau_w, p_w) =: (K, B, \tau, p)$ is an involutorial system of the second kind over k that is compatible with base change: $\mathcal{B}_{w_R} = (\mathcal{B}_w)_R$ for all $R \in k$-**alg**. Moreover, μ is admissible for $\mathcal{B}$: $N(p) = \mu\bar{\mu}$.*

(c) *We have the relations*

$$J = \{x_0 + uj_1 + (\mu^{-1}p\tau(u))j_2 \mid x_0 \in J_0,\ u \in B\}, \tag{1}$$

$$x^\sharp = \Big(x_0^\sharp - u(p\tau(u))\Big) + (\bar{\mu}\tau(u)^\sharp p^{-1} - x_0 u)j_1 + \Big(\mu^{-1}p\tau(\bar{\mu}\tau(u)^\sharp p^{-1} - x_0 u)\Big)j_2, \tag{2}$$

$$N(x) = N_0(x_0) + \mu N(u) + \bar{\mu}\overline{N(u)} - T_0\Big(x_0, u(p\tau(u))\Big) \tag{3}$$

for all $x = x_0 + uj_1 + (\mu^{-1}p\tau(u))j_2 \in J_R$, $x_0 \in J_{0R}$, $u \in ({}_kB)_R = B_{R_K}$, $R \in k$-**alg**.

(d) *The element* $\xi - \bar{\xi}$ *is invertible in* K *and*

$$w = ((\xi - \bar{\xi})^{-1}1_B)j_1 + \Big(\mu^{-1}p\tau((\xi - \bar{\xi})^{-1}1_B)\Big)j_2. \tag{4}$$

Recall from (43.5.2) that $u(p\tau(u))$ belongs to $H(B,\tau) = J_0$.

Proof (a) Both $\chi(j_1)$ and $\chi(j_1)^\sharp = \chi(j_1^\sharp) = \chi(j_2)$ belong to $J_{0K}^\perp$. Hence we can write

$$\chi(j_1) = x_1 j_1 + x_2 j_2 \tag{5}$$

for some $x_1, x_2 \in B$, and since $\mu = N(l)$ by Lemma 44.9 is invertible in K, we may apply (42.11.3) to conclude $x_1 x_2 = 0$, hence $N_B(x_1)N_B(x_2) = 0$. By (44.10.4), and (42.11.4), on the other hand, $\bar{\mu} = \overline{N(j_1)} = N(\chi(j_1)) = \mu N_B(x_1) + \mu^2 N_B(x_2)$ is invertible in K, and we find $b_1, b_2 \in K^\times$ satisfying $b_1 N_B(x_1) + b_2 N_B(x_2) = 1$. Thus c_1, c_2, with $c_i = b_i N_B(x_i)$ for $i = 1,2$, is a complete orthogonal system of idempotents in K, forcing $K = K_1 \times K_2$ as a direct product of ideals $K_i = Kc_i \in K$-**alg** $\subseteq k$-**alg** for $i = 1,2$. Hence $B = B_1 \times B_2$, $B_i = c_i B = B_{K_i}$, where $B_{K_i}^{(+)} = J_{K_i}$ as cubic Jordan algebras over K_i. From (42.1.3) we deduce $x_{2K_1} = c_1 x_2 = b_1 N_B(x_1)x_2 = b_1 x_1^\sharp(x_1 x_2) = 0$. On the other hand, (44.9.1) yields $j_1 = l = \xi w - Q(w)\,.\,H(w)$, hence $\chi(j_1) = \bar{\xi}w - Q(w)\,.\,H(w)$, and since $\xi - \bar{\xi}$ is invertible in K, we apply (5) to conclude

$$w = (\xi - \bar{\xi})^{-1}((1_B - x_1)j_1 - x_2 j_2), \tag{6}$$

hence $w_{K_1} = (\xi - \bar{\xi})_{K_1}^{-1}((1_{B_{K_1}} - x_{1K_1})j_{1K_1} - x_{2K_1}j_{2K_1}) \in B_{K_1}j_{1K_1}$ since $x_{2K_1} = 0$. Thus $w_{K_1} \in J_{K_1}$ is strongly orthogonal to J_{0K_1}, forcing $Q(w)_{K_1} = Q(w_{K_1}) = 0$. But $Q(w)_{K_1}$ is invertible in J_{0K_1} by (44.8.6), forcing $N_0(Q(w))_{K_1} = 0 \in K_1$ to be invertible in K_1, which is impossible unless $K_1 = \{0\}$. This implies $c_1 = 0$, hence $b_2 N_B(x_2) = c_2 = 1$. Thus x_2 is invertible in B, and from $x_1 x_2 = 0$ we deduce $x_1 = 0$. Hence (5) reduces to $\chi(j_1) = x_2 j_2$, and (a) is proved.

(b) Combining (a) with (42.11.4), we obtain $N(\chi(j_1)) = \mu^{-3}\mu^2 N_0(p) = \mu^{-1}N_0(p)$, while (44.10.4) gives $N(\chi(j_1)) = \overline{N(j_1)} = \bar{\mu}$. Comparing, we end

up with the final statement of (b). Moreover, χ being ι-semi-linear of period 2 combines with (a), (42.11.5), (42.11.3) and (44.10.4), (44.10.5) to yield

$$\begin{aligned} j_1 &= \chi(\chi(j_1)) = \chi(\mu^{-1}pj_2) = \bar{\mu}^{-1}\chi(p\,.\,j_1^\sharp) = \bar{\mu}^{-1}\tau(p)\,.\,\chi(j_1)^\sharp \\ &= \bar{\mu}^{-1}\tau(p)\,.\,(\mu^{-1}pj_2)^\sharp = \bar{\mu}^{-1}\tau(p)\,.\,((\mu^{-1}p^\sharp)j_1) \\ &= N_0(p)^{-1}(\tau(p)p^\sharp)j_1 = (\tau(p)p^{-1})j_1. \end{aligned}$$

Thus $\tau(p) = p$. Finally, for all $x, y \in J_{0K}$, we obtain

$$\chi((xy)j_1) = \chi((xy)\,.\,j_1) = \tau(xy)\,.\chi(j_1) = \tau(xy)\,.\,(\mu^{-1}pj_2) = (\mu^{-1}p\tau(xy))j_2$$

on the one hand, and

$$\begin{aligned} \chi((xy)j_1) &= \chi(x\,.\,(y\,.\,j_1)) = \tau(x)\,.\chi(y\,.\,j_1) = \tau(x)\,.\,(\tau(y)\,.\chi(j_1)) \\ &= \mu^{-1}\tau(x)\,.\,(\tau(y)\,.\,(pj_2)) = \mu^{-1}((p\tau(y))\tau(x))j_2 \end{aligned}$$

on the other, so we conclude

$$p\tau(xy) = (p\tau(y))\tau(x) = (p(\tau(y)p^{-1})p)\tau(x) = p\Big((\tau(y)p^{-1})(p\tau(x))\Big),$$

hence $\tau(xy) = (\tau(y)p^{-1})(p\tau(x))$. Summing up, we have thus shown that $\mathcal{B} = (K, B, \tau, p)$ is a unitary involutorial system over k.

(c) For $x_0, x_1, x_2 \in J_{0K} = B$ we put $x := x_0 + x_1j_1 + x_2j_2 \in J(B,\mu) = J_K$ and compute

$$\begin{aligned} \chi(x) &= \tau(x_0) + \tau(x_1)\,.\chi(j_1) + \tau(x_2)\,.\chi(j_1)^\sharp \\ &= \tau(x_0) + \mu^{-1}\tau(x_1)\,.\,(pj_2) + \tau(x_2)\,.\,(\mu^{-1}pj_2)^\sharp \\ &= \tau(x_0) + \mu^{-1}(p\tau(x_1))j_2 + \mu^{-2}\tau(x_2)\,.\,(\mu p^\sharp)j_1 \\ &= \tau(x_0) + \mu^{-1}(\tau(x_2)p^\sharp)j_1 + \mu^{-1}(p\tau(x_1))j_2 \\ &= \tau(x_0) + \bar{\mu}(\tau(x_2)p^{-1})j_1 + \mu^{-1}(p\tau(x_1))j_2. \end{aligned}$$

Combining this with (44.10.6), we obtain the following chain of equivalent conditions.

$$\begin{aligned} x \in J &\iff \chi(x) = x \\ &\iff \tau(x_0) = x_0, \quad x_1 = \bar{\mu}\tau(x_2)p^{-1}, \quad x_2 = \mu^{-1}p\tau(x_1) \\ &\iff x_0 \in J_0, \quad x_2 = \mu^{-1}p\tau(x_1) \end{aligned}$$

since this implies $\tau(x_2) = \bar{\mu}^{-1}\tau(p\tau(x_1)) = \bar{\mu}^{-1}x_1p$ by (43.5.3), hence $x_1 = \bar{\mu}\tau(x_2)p^{-1}$. We have thus proved (1). In (2), (3) we may assume $R = k$ since our constructions commute with base change. First of all, consulting (43.6.2) and (44.10.6), we see that the right-hand sides of (2), (3) make sense. Now (3)

follows from (42.11.4) since $\mu^2 N_0(\mu^{-1}p\tau(u)) = \mu^{-1}N_0(p)N_0(\tau(u)) = \bar{\mu}\overline{N_0(u)}$ by (1) and (b), while (44.10.2) and (43.2.1), (43.5.3) yield (2) because

$$\mu(\mu^{-1}p\tau(u))^\sharp = \mu^{-1}\tau(u)^\sharp p^\sharp = \mu^{-1}N_0(p)\tau(u)^\sharp p^{-1} = \bar{\mu}\tau(u)^\sharp p^{-1}$$

and $\mu^{-1}(p\tau(\bar{\mu}\tau(u)^\sharp p^{-1} - x_0 u)) = x^\sharp - \mu^{-1}(p\tau(u))x_0$.

(d) In (6) we have $x_1 = 0$, $x_2 = \mu^{-1}p$, which immediately implies the assertion. □

Before we are able to discuss the external second Tits construction (in analogy to Thm. 42.11), it will be necessary to insert the following technical observation.

44.13 Proposition. *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system of the r-th kind ($r = 1, 2$) over k, write $\vartheta\colon k \to K$ for the unit homomorphism of K and put $J := B^{(+)}$ as a cubic Jordan algebra over K. Then there is a unique way of making*

$$J_0 := H(\mathcal{B}) := H(B, \tau) = \{x \in J \mid \tau(x) = x\} \tag{1}$$

a cubic Jordan algebra over k such that the inclusion $i\colon J_0 \hookrightarrow J$ is a ϑ-semi-linear homomorphism of cubic Jordan algebras, i.e., there is a unique cubic form $N_{J_0}\colon J_0 \to k$ making

$$\begin{array}{ccc} J_0 & \xrightarrow[i]{} & J = B^{(+)} \\ {\scriptstyle N_{J_0}}\downarrow & & \downarrow{\scriptstyle N_J = N_B} \\ k & \xrightarrow[\vartheta]{} & K \end{array} \tag{2}$$

a commutative ϑ-semi-linear polynomial square and J_0 a cubic Jordan algebra over k.

Proof By 44.1 and 44.2 (a), the map $\tau\colon B^{(+)} \to B^{\mathrm{op}\,p(+)} = B^{(+)}$ is an ι_K-semi-linear isomorphism of cubic Jordan algebras over K, and we conclude that J_0 is a Jordan k-subalgebra of J. Hence we only have to worry about its cubic structure.

First assume $r = 1$, i.e., $K = k$ and $\vartheta = \mathbf{1}_k$. Since J_0 by (34.10.6) is stable under the adjoint of J, we deduce from 33.5 and 34.6 that it becomes a cubic Jordan algebra of the desired kind by defining its norm by $N_{J_0} = N_J|_{J_0} = N_J \circ i$ as a polynomial law over k. Uniqueness is clear.

We are left with the case $r = 2$, i.e., K is quadratic étale. Uniqueness follows from the fact that ϑ and, by Exc. 44.29 (b), the inclusion $i\colon J_0 \hookrightarrow J$ are strictly injective. In order to prove existence, we first show that $1_{J_0} = 1_J \in J_0$ is unimodular over k. It is certainly so over K, hence some K-linear form $\sigma\colon J \to$

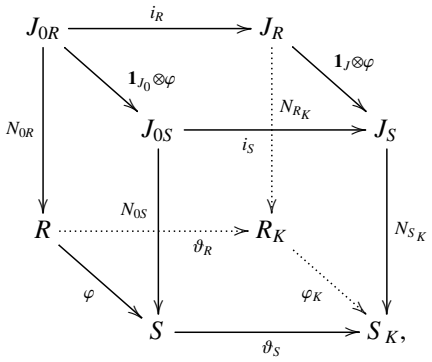
K has $\sigma(1_{J_0}) = 1_K$. But 1_K is unimodular over k, so some k-linear form $\varrho\colon K \to k$ has $\varrho(1_K) = 1$. Thus $\lambda := \varrho \circ \sigma_{J_0}\colon J_0 \to k$ is k-linear and satisfies $\lambda(1_{J_0}) = 1$. Turning next to the existence of N_{J_0}, we put $N := N_J$ and let $R \in k$-**alg** be arbitrary. In view of the identifications in 12.27, the set maps

$$N_{R_K} = N_{K_R}\colon J_R = ({}_kJ)_R = J_{R_K} = J_{K_R} \longrightarrow K_R = R_K$$

by (44.2.1) satisfy $N_{R_K}(\tau_R(x)) = \overline{N_{R_K}(x)}$ for all $x \in J_R$. Hence there exists a unique set map $N_{0R}\colon J_{0R} \to R$ such that the diagram

$$\begin{array}{ccc} J_{0R} = H(B_R, \tau_R) & \xrightarrow[i_R]{} & J_R \\ {\scriptstyle \exists! N_{0R}}\big\downarrow & & \big\downarrow{\scriptstyle N_{R_K}} \\ R & \xrightarrow[\vartheta_R]{} & R_K \end{array} \tag{3}$$

commutes. We claim that the family of set maps N_{0R}, $R \in k$-**alg**, is a polynomial law (hence a cubic form N_0 on J_0) over k. To prove this, let $\varphi\colon R \to S$ be a morphism in k-**alg** and consider the cube



where the natural identifications show that

$$\mathbf{1}_J \otimes \varphi\colon J_R \longrightarrow J_S \quad \text{and} \quad \mathbf{1}_J \otimes_K \varphi_K\colon J_{R_K} \to J_{S_K}$$

are the same. Hence all squares in the preceding cube commute, with the possible exception of the vertical one on the left, which by diagram chasing must therefore commute as well since K is flat over k, so ϑ_S is injective. Thus $N_{J_0} := N_0\colon J_0 \to k$ is indeed a cubic form over k making the diagram (2) commutative, and J_0 a cubic Jordan algebra over k. □

44.14 Remark. In Prop. 44.13, we sometimes write $J_0 = J_0(\mathcal{B})$ to indicate dependence on $\mathcal{B}$. By Exercises 39.40 and 44.29, passing from $\mathcal{B}$ to $J_0(\mathcal{B})$

is compatible with flat (resp. arbitrary) base change provided $\mathcal{B}$ is of the first (resp. the second) kind. In our next result, we recall from Prop. 42.1 (a) that

$$T_B((uv)w) = T_B(u(vw)) =: T_B(uvw) \tag{1}$$

for all $u, v, w \in B$.

44.15 Theorem (The external second Tits construction)**.** *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system of the r-th kind ($r = 1, 2$) over k and $\mu \in K$ an admissible scalar for $\mathcal{B}$. Writing $J_0 = H(\mathcal{B})$ as a cubic Jordan algebra over k in the sense of 44.13, the direct sum*

$$J := J_0 \oplus Bj \tag{1}$$

of J_0 and B as k-modules, into which J_0 naturally embeds through the initial summand, carries the unique structure of a cubic Jordan algebra over k whose identity element, adjoint and norm are uniquely determined by the formulas

$$1_J = 1_{J_0} = 1_B = 1_B + 0 \cdot j, \tag{2}$$

$$x^\sharp = \Big(x_0^\sharp - u(p\tau(u))\Big) + (\bar{\mu}\tau(u^\sharp)p^{-1} - x_0 u)j, \tag{3}$$

$$N_J(x) = N_{J_0}(x_0) + \mu N_B(u) + \bar{\mu}\overline{N_B(u)} - T_{J_0}\Big(x_0, u(p\tau(u))\Big) \tag{4}$$

for all $x = x_0 + uj \in J_R$, $x_0 \in J_{0R}$, $u \in B_R$ and for all flat *algebras $R \in k$-**alg**. Moreover, with another element $y = y_0 + vj \in J_R$, $y_0 \in J_{0R}$, $v \in B_R$, the bilinearized adjoint, trace and quadratic trace of J have the form*

$$\begin{aligned} x \times y &= \Big(x_0 \times y_0 - u(p\tau(v)) - v(p\tau(u))\Big) \\ &\quad + (\bar{\mu}\tau(u \times v)p^{-1} - x_0 v - y_0 u)j, \end{aligned} \tag{5}$$

$$\begin{aligned} T_J(x, y) &= T_{J_0}(x_0, y_0) + T_B(up\tau(v)) + \overline{T_B(up\tau(v))} \\ &= T_{J_0}(x_0, y_0) + T_B(up\tau(v)) + T_B(vp\tau(u)), \end{aligned} \tag{6}$$

$$T_J(x) = T_{J_0}(x_0), \tag{7}$$

$$S_J(x) = S_{J_0}(x_0) - T_{J_0}(up\tau(u)), \tag{8}$$

$$\begin{aligned} S_J(x, y) &= S_{J_0}(x_0, y_0) - T_B(up\tau(v)) - \overline{T_B(up\tau(v))} \\ &= S_{J_0}(x_0, y_0) - T_B(up\tau(v)) - T_B(vp\tau(u)). \end{aligned} \tag{9}$$

Proof $1_J = 1_{J_0}$ is a unimodular element of J_0 by Prop. 44.13, hence of J. Since the polynomial ring $k[\mathbf{T}]$, $\mathbf{T} = (\mathbf{t}_0, \mathbf{t}_1, \mathbf{t}_2, \dots)$ is a flat k-algebra, uniqueness follows from Cor. 12.11. In order to prove existence, we note that (3) defines a quadratic map $x \mapsto x^\sharp$ from J to J in the sense of 11.1. By Cor. 11.5, therefore, it allows a natural R-quadratic extension, for any $R \in k$-**alg** irrespective of whether the right-hand side of (3) is compatible with this particular

scalar extension, which can be guaranteed only if R is flat (44.14). Along similar lines, the assignment $u \mapsto u(p\tau(u))$ gives a quadratic map $Q\colon B \to J_0$, by means of which (4) may be rewritten as

$$N_J(x) = N_{J_0}(x_0) + (t_K \circ (\mu N_B))(u) - T_{J_0}(x_0, Q(u)). \tag{10}$$

Hence (10) defines a cubic form N_J on J. Summing up, therefore, J together with $1_J, \sharp, N_J$ is a cubic array over k, and it remains to show that it is, in fact, a cubic norm structure. In order to do so, we abbreviate $N := N_B$, $T := T_B$, $S := S_B$, $N_0 := N_{J_0}$, $T_0 := T_{J_0}$, $S_0 := S_{J_0}$. While (5) is obvious, (10) combines with the gradient identity for J_0 and $B^{(+)}$ to imply

$$\begin{aligned} N_J(x,y) = {} & T_0(x_0^\sharp, y_0) + t_K(\mu T(u^\sharp, v)) \\ & - T_0\Big(x_0, u(p\tau(v)) + v(p\tau(u))\Big) - T_0\Big(y_0, u(p\tau(u))\Big) \end{aligned} \tag{11}$$

which yields (6)–(9) in the usual manner, see 33.2, 34.10, 43.5 for details. It remains to verify the defining identities (33.4.1)–(33.4.3) of a cubic norm structure in every scalar extension J_R, $R \in k$-**alg**. By Cor. 12.11, it suffices to do so for $R = k[\mathbf{T}]$, and since this is a flat k-algebra, it actually suffices to do so over the base ring. The verification of the unit identity using (5) is left to the reader. Turning to the gradient identity, let $x = x_0 + uj$, $y = y_0 + vj$, $x_0, y_0 \in J_0$, $u, v \in B$. Combining (3), (6) with (43.2.1), (43.5.2), we compute

$$\begin{aligned} T(x^\sharp, y) &= T_0\Big(x_0^\sharp - u(p\tau(u)), y_0\Big) + t_K\Big(T([\bar\mu\tau(u^\sharp)p^{-1} - x_0 u]p\tau(v))\Big) \\ &= T_0(x_0^\sharp, y_0) - T_0\Big(y_0, u(p\tau(u))\Big) + t_K\Big(T(\bar\mu\tau(vu^\sharp))\Big) - t_K\Big(T(x_0, u[p\tau(v)])\Big) \\ &= T_0(x_0^\sharp, y_0) + t_K(\mu T(u^\sharp, v)) - T_0\Big(y_0, u(p\tau(u))\Big) \\ &\quad - T_0\Big(x_0, u(p\tau(v)) + v(p\tau(u))\Big), \end{aligned}$$

and comparing with (11), the gradient identity follows. Finally, in order to derive the adjoint identity, we let $x = x_0 + uj$, $x_0 \in J_0$, $u \in B$ and write $x^{\sharp\sharp} = y_0 + vj$, for some $y_0 \in J_0$, $v \in B$. Then we must show

$$y_0 = N(x)x_0, \quad v = N(x)u. \tag{12}$$

From (3) we deduce, using (43.5.3),

$$\begin{aligned} y_0 &= \Big(x_0^\sharp - u(p\tau(u))\Big)^\sharp - (\bar\mu\tau(u)^\sharp p^{-1} - x_0 u)\Big(p\tau(\bar\mu\tau(u^\sharp)p^{-1} - x_0 u)\Big) \\ &= x_0^{\sharp\sharp} - x_0^\sharp \times \Big(u(p\tau(u))\Big) + \Big(u(p\tau(u))\Big)^\sharp \\ &\quad - \Big(\bar\mu\tau(u)^\sharp p^{-1} - x_0 u\Big)\Big(p(\mu p^{-1} u^\sharp - \tau(x_0 u))\Big) \\ &= N_0(x_0)x_0 - x_0^\sharp \times \Big(u(p\tau(u))\Big) + (\tau(u)^\sharp p^\sharp)u^\sharp - \mu\bar\mu(\tau(u)^\sharp p^{-1})u^\sharp \end{aligned}$$

$$+\bar{\mu}(\tau(u^\sharp)p^{-1})(p\tau(x_0u)) + \mu(x_0u)u^\sharp - (x_0u)(p\tau(x_0u)).$$

Since μ is admissible for $\mathcal{B}$, we conclude $\mu\bar{\mu}(\tau(u)^\sharp p^{-1})u^\sharp = (\tau(u)^\sharp p^\sharp)u^\sharp$, while (43.2.1) implies $\bar{\mu}(\tau(u^\sharp)p^{-1})(p\tau(x_0u)) = \bar{\mu}\tau((x_0u)u^\sharp) = \bar{\mu}\overline{N_0(u)}x_0$. Moreover, (43.5.3) yields

$$\begin{aligned}(x_0u)(p\tau(x_0u)) &= (x_0u)\Big((p\tau(u))x_0\Big) = x_0\Big(u(p\tau(u))\Big)x_0\\ &= U_{x_0}\Big(u(p\tau(u))\Big) = T_0\Big(x_0, u(p\tau(u))\Big)x_0 - x_0^\sharp \times \Big(u(p\tau(u))\Big).\end{aligned}$$

Thus $y_0 = N_0(x_0) + \mu N_0(u)x_0 + \bar{\mu}\overline{N_0(u)}\,x_0 - T_0(x_0, u(p\tau(u)))x_0 = N(x)x_0$, and we have established the first part of (12). As to the second, again by (3),

$$\begin{aligned}v &= \bar{\mu}\tau(\bar{\mu}\tau(u^\sharp)p^{-1} - x_0u)^\sharp p^{-1} - \Big(x_0^\sharp - u(p\tau(u))\Big)\Big(\bar{\mu}\tau(u)^\sharp p^{-1} - x_0u\Big)\\
&= \bar{\mu}(\mu p^{-1}u^\sharp - \tau(x_0u))^\sharp p^{-1} - \bar{\mu}x_0^\sharp(\tau(u)^\sharp p^{-1})\\
&\qquad + x_0^\sharp(x_0u) + \bar{\mu}\Big(u(p\tau(u))\Big)(\tau(u)^\sharp p^{-1}) - \Big(u(p\tau(u))\Big)(x_0u)\\
&= N_0(x_0)u + \mu^2\bar{\mu}u^{\sharp\sharp}p^{-1\sharp}p^{-1} - \mu\bar{\mu}((p^{-1}u^\sharp)\times\tau(x_0u))p^{-1}\\
&\qquad + \bar{\mu}\tau(u^\sharp x_0^\sharp)p^{-1} - \bar{\mu}x_0^\sharp(\tau(u)^\sharp p^{-1})\\
&\qquad + \bar{\mu}\Big(u(p\tau(u))\Big)(\tau(u^\sharp)p^{-1}) - u\Big((p\tau(u))x_0\Big)u.\end{aligned}$$

Here $\mu^2\bar{\mu}u^{\sharp\sharp}p^{-1\sharp}p^{-1} = \mu N(u)u$ since μ is admissible for $\mathcal{B}$, while linearizing $(ab)^\sharp = b^\sharp a^\sharp$ gives $(ab_1)\times(ab_2) = (b_1\times b_2)a^\sharp$, hence $\mu\bar{\mu}((p^{-1}u^\sharp)\times\tau(x_0u))p^{-1} = ((p^{-1}u^\sharp)\times\tau(x_0u))p^\sharp = (p(p^{-1}u^\sharp))\times(p\tau(x_0u)) = u^\sharp\times((p\tau(u))x_0)$ by (43.5.3). From (43.5.4) we conclude $\bar{\mu}\tau(u^\sharp x_0^\sharp)p^{-1} = \bar{\mu}x_0^\sharp(\tau(u)^\sharp p^{-1})$, while (43.5.1) and Prop. 34.12 yield

$$\begin{aligned}\bar{\mu}\Big(u(p\tau(u))\Big)(\tau(u)^\sharp p^{-1})) &= \mu^{-1}\Big(u(p\tau(u))\Big)(\tau(u)^\sharp p^\sharp))\\
&= \mu^{-1}((u\tau(up)))\tau(p^\sharp u^\sharp)\\
&= \mu^{-1}(u\tau(up))\tau(up)^\sharp = \mu^{-1}\overline{N(u)}N_0(p)u = \bar{\mu}\overline{N(u)}\,u.\end{aligned}$$

Finally,

$$\begin{aligned}u((p\tau(u))x_0)u &= T_0(u(p\tau(u)), x_0)u - u^\sharp\times((p\tau(u))x_0)\\
&= T_0(x_0, u(p\tau(u)))u - u^\sharp\times((p\tau(u))x_0).\end{aligned}$$

Summing up,

$$v = N_0(x_0)u + \mu N(u)u + \bar{\mu}\overline{N(u)}\,u - T_0\Big(x_0u(p\tau(u))\Big)u = N(x)u,$$

and also the second part of (12) has been established. □

44.16 The formal second Tits construction. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and $\mu \in K$ an admissible scalar for $\mathcal{B}$.

(a) The cubic Jordan algebra constructed in Thm. 44.15 is said to arise from $\mathcal{B}, \mu$ by means of the *second Tits construction*. With $J_0 := H(\mathcal{B})$ we therefore have $J(\mathcal{B}, \mu) = J_0 \oplus Bj$ as a direct sum of k-modules, and the natural map from J_0 to the initial summand of $J(\mathcal{B}, \mu)$ is an embedding of cubic Jordan algebras; we usually identify $J_0 \subseteq J(\mathcal{B}, \mu)$ accordingly. By 44.14, the second Tits construction is compatible with flat base change, and even with arbitrary base change if $\mathcal{B}$ is of the second kind or $2 \in k^\times$ since, in the latter case, J_0 is a direct summand of B as a k-module.

(b) By (44.15.5), (44.15.6), the pair (J_0, Bj) is a complementary cubic Jordan subalgebra of $J(\mathcal{B}, \mu)$ and

$$x_0 \,.\, (uj) = (x_0 u)j$$

for all $x_0 \in J_0$ and all $u \in B$.

44.17 Corollary. *Let (J, J_0) be a balanced pair of cubic Jordan algebras over k and $w \in J$ an étale element relative to J_0. With the notation of Thm. 44.12, the map*

$$\varphi\colon J(\mathcal{B}_w, \mu_w) \xrightarrow{\sim} J$$

defined by

$$\varphi(x_0 + uj) := x_0 + uj_1 + \big(\mu_w^{-1} p_w \tau_w(u)\big) j_2 \tag{1}$$

for $x_0 \in H(B_w, \tau_w) = J_0$ and $u \in B_w = J_{K_w}$ is an isomorphism of cubic Jordan algebras satisfying

$$\varphi\Big(\big((\xi_w - \bar{\xi}_w)^{-1} 1_B\big) j\Big) = w. \tag{2}$$

Proof This follows immediately from Theorems 44.12, 44.15. □

Slightly modifying the parameters entering into the second Tits construction, we can do better than that by finding an isomorphism that matches the quantity j itself, rather than an appropriate scalar multiple, with the pre-assigned étale element:

44.18 Corollary. *In Cor. 44.17, put $v := (\xi_w - \bar{\xi}_w)^{-1} 1_B$ and $\mathcal{B}_w^\circ := \mathcal{B}_w \,.\, v^{-1}$ in the sense of Exc. 44.33. Then*

$$\mathcal{B}_w^\circ = (K_w, B_w, \tau_w, p_w^\circ), \quad p_w^\circ = -\Delta_w^{-1} p_w \tag{1}$$

and

$$N_{B_w}(v)\mu_w = \xi_w \tag{2}$$

is an admissible scalar for $\mathcal{B}^\circ_w$. *Moreover, the isomorphism*

$$\Phi_{\mathcal{B}^\circ_w,v}\colon J(\mathcal{B}^\circ_w,\xi_w)\xrightarrow{\sim} J(\mathcal{B}_w,\mu_w) \tag{3}$$

of Exc. 44.33 combines with the isomorphism φ *of Cor. 44.17 to yield an isomorphism*

$$\varphi^\circ := \varphi\circ\Phi_{\mathcal{B}^\circ_w,v}\colon J(\mathcal{B}^\circ_w,\xi_w)\xrightarrow{\sim} J \tag{4}$$

such $\varphi^\circ(j) = w$.

Proof We simplify notation by dropping the subscript w whenever there is no danger of confusion. Since $v^{-1} = (\xi-\bar\xi)1_B$ is a central element of B, we have $B^{v^{-1}} = B$ as cubic alternative K-algebras, while $p^\circ = p\,.\,v^{-1} = n_K(\xi-\bar\xi)^{-1}p = -\Delta^{-1}p$ by (44.8.4). This proves (1). Next one checks

$$N_B(v) = \Delta^{-2}(\xi-\bar\xi)$$

and combines this with (44.8.2), (44.8.3), (44.9.2) to derive (2) by a straightforward computation. Now Exc. 44.33 produces the isomorphism (3). Summing up, $\varphi^\circ\colon J(\mathcal{B}^\circ,\xi)\to J$ is an isomorphism sending j to $\varphi((\xi-\bar\xi)^{-1}1_B) = w$. □

Our next aim will be to describe the most elementary connections between the two Tits constructions. Our approach will be based on the equivalence of categories k-**cosp** (of core-split involutorial systems) and k-**pocu** (of pointed cubic alternative k-algebras) described in Exc. 44.31.

44.19 Theorem. *Let* (A,q) *be a pointed cubic alternative algebra over* k *and*

$$\mathrm{Cosp}(A,q) = (\mathcal{B}(A,q),\mathbf{1}_{k\times k})$$

the corresponding core-split involutorial k*-system in the sense of Exc. 44.31. A quantity* $\mu = (\lambda,\lambda')\in k\times k$ *is an admissible scalar for* $\mathcal{B}(A,q)$ *if and only if* $\lambda\in k^\times$ *and* $\lambda' = \lambda^{-1}N_A(q)$. *In this case, the map*

$$\Phi_{A,q}\colon J(\mathcal{B}(A.q),\mu)\xrightarrow{\sim} J(A,\lambda) \tag{1}$$

defined by

$$\Phi_{A,q}((x_0,x_0)+(x_1,x_2)j) := x_0 + x_1j_1 + (\lambda^{-1}qx_2)j_2 \tag{2}$$

for $x_0,x_1,x_2\in A$ *is an isomorphism of cubic Jordan algebras. Moreover,*

for any homomorphism $\varphi\colon (A,q) \to (A',q')$ *of pointed cubic alternative* k*-algebras, the diagram*

$$\begin{array}{ccc} J(\mathcal{B}(A,q),\mu) & \xrightarrow[\Phi_{A,q}]{\cong} & J(A,\lambda) \\ {\scriptstyle J(\mathbf{V}(\mathrm{Cosp}(\varphi)),\mu)}\downarrow & & \downarrow{\scriptstyle J(\varphi,\lambda)} \\ J(\mathcal{B}(A',q'),\mu) & \xrightarrow[\Phi_{A',q'}]{\cong} & J(A',\lambda) \end{array} \tag{3}$$

commutes, where $\mathbf{V}\colon k$-**cosp** $\to k$-**invsys** *is the forgetful functor.*

Roughly speaking, therefore, *every first Tits construction is a second Tits construction.*

Proof The very first assertion being obvious, we show that $\Phi := \Phi_{A,q}$ is an isomorphism. By Exc. 34.18 (a), it suffices to verify that Φ preserves adjoints. Putting $x := (x_0,x_0) + (x_1,x_2)j$, one checks that

$$\Phi(x)^\sharp = (x_0^\sharp - x_1(qx_2)) + (\lambda^{-1}(qx_2)^\sharp - x_0x_1)j_1 + (x_1^\sharp - \lambda^{-1}(qx_2)x_0)j_2. \tag{4}$$

On the other hand, setting $x^\sharp = (y_0,y_0) + (y_1,y_2)j$, a short computation yields

$$y_0 = x_0^\sharp - x_1(qx_2),\ y_1 = \lambda^{-1}(qx_2)^\sharp - x_0x_1,\ y_2 = \lambda q^{-1}x_1^\sharp - (x_2q^{-1})(qx_0).$$

Hence (2) implies

$$\begin{aligned} \Phi(x^\sharp) &= (x_0^\sharp - x_1(qx_2)) + (\lambda^{-1}(qx_2)^\sharp - x_0x_1)j_1 + \Big(x_1^\sharp - \lambda^{-1}q((x_2q^{-1})(qx_0)\Big)j_2 \\ &= (x_0^\sharp - x_1(qx_2)) + (\lambda^{-1}(qx_2)^\sharp - x_0x_1)j_1 + (x_1^\sharp - \lambda^{-1}(qx_2)x_0)j_2, \end{aligned}$$

which agrees with $\Phi(x)^\sharp$ by (4). It remains to prove that the diagram (3) commutes, which is obvious since

$$J(\mathbf{V}(\mathrm{Cosp}(\varphi)),\mu) = \varphi_0 \times (\varphi\times\varphi), \text{ where } \varphi_0\colon H(\mathcal{B}(A,q)) \to H(\mathcal{B}(A',q'))$$

is induced by $\varphi\times\varphi$ via restriction. □

44.20 Corollary. *Let* $\mathcal{B} = (K,B,\tau,p)$ *be an involutorial system of the second kind over* k*.*

(a) If we define $\varrho\colon K_K \to K\times K$ *by* $\varrho(a\otimes b) := (ab,\bar{a}b)$ *for all* $a,b\in K$*, then* $(\mathcal{B}_K,\varrho)$ *is a core-split involutorial system over* K*.*

(b) Put $(A,q) := \mathrm{Pocu}(\mathcal{B}_K,\varrho)$ *as a pointed cubic alternative* K*-algebra in the sense of Exc. 44.31. Then* $B\cong A$ *canonically as cubic alternative* K*-algebras, and letting* μ *be any admissible scalar for* $\mathcal{B}$*, there exists a canonical isomorphism*

$$J(\mathcal{B},\mu)_K = J(\mathcal{B}_K,\mu_K) \xrightarrow{\sim} J(A,\mu) \cong J(B,\mu)$$

of cubic Jordan algebras over K.

Proof (a) By Exc. 19.36 (a), ϱ is an isomorphism of K-algebras, forcing $(\mathcal{B}_K, \varrho)$ to be a core-split involutorial K-system.

(b) By Exc. 44.31 (c), we find a natural isomorphism

$$(\sigma, \varphi)\colon (\mathcal{B}_K, \varrho) \xrightarrow{\sim} \mathrm{Cosp}(A, q) = (\mathcal{B}(A, q), \mathbf{1}_{K\times K})$$

of core-split involutorial systems over K. In particular, we have $\sigma = \varrho$, whence $\varrho(\mu_K) = (\mu, \bar{\mu})$ is an admissible scalar for $\mathcal{B}(A, q)$. We have

$$\mathcal{B}_K = (K_K, B_K, \tau_K, p_K),$$

and with the projection $\pi_+\colon K \times K \to K$ onto the first factor, Exc. 44.31 (b) implies $A = {}^{\varrho}(B_{K_K})_+ \cong B$ since the composite map

$$K \xrightarrow[\mathrm{can}]{} K_K \xrightarrow[\varrho]{} K \times K \xrightarrow[\pi_+]{} K$$

is the identity. Now stability under arbitrary base change and functoriality of the second Tits construction combine with Thm. 44.19 to yield isomorphisms

$$J(\mathcal{B}, \mu)_K = J(\mathcal{B}_K, \mu_K) \xrightarrow{\cong} J(\mathcal{B}(A, q), (\mu, \bar{\mu})) \xrightarrow[\Phi_{A,q}]{\cong} J(A, \mu) \xrightarrow{\cong} J(B, \mu),$$

as claimed. □

A simpler version of the preceding argument yields the following result.

44.21 Corollary. *Let $(\mathcal{B}, \varrho)$ be a core-split involutorial system over k and $(A, q) = \mathrm{Pocu}(\mathcal{B}, \varrho)$ the corresponding pointed cubic alternative k-algebra. For any admissible scalar μ for $\mathcal{B}$, there is a natural isomorphism*

$$J(\mathcal{B}, \mu) \xrightarrow{\sim} J(A, \mu_+)$$

of cubic Jordan algebras over k, where $\varrho(\mu) = (\mu_+, \mu_-) \in k^\times \times k^\times$. □

44.22 Corollary. *Let $\mathcal{B}$ be an involutorial system of the second kind over k and μ an admissible scalar for $\mathcal{B}$. Then the following conditions are equivalent.*

(i) $J(\mathcal{B}, \mu)$ *is regular over k.*

(ii) B *is regular over* $K := \mathrm{Core}(\mathcal{B})$.

(iii) $H(\mathcal{B})$ *is regular over k.*

When the equivalent conditions of the corollary hold, we say $\mathcal{B}$ is *regular* over k.

Proof As an étale algebra, K is faithfully flat over k. Hence (i) holds if and only if $J(\mathcal{B},\mu)_K \cong J(B,\mu)$ (by Cor. 44.20) is regular over K. By Cor. 42.14, therefore, and since μ is invertible to begin with, (i) and (ii) are equivalent. Since $B^{(+)} \cong H(\mathcal{B})_K$ as cubic Jordan algebras over K by Exc. 44.29 (a), the same argument shows that (ii) and (iii) are equivalent. □

44.23 Azumaya algebras with unitary involution. By an *Azumaya algebra of degree $n \geq 1$ with unitary involution* over k we mean a pair (A,τ) consisting of an Azumaya algebra A of degree n over some quadratic étale k-algebra K and a K/k-involution τ of A, i.e., an involution of A as a k-algebra that (stabilizes the centre $K \cong K1_A$ of A and) induces the conjugation of K via restriction. In this case, we also speak of an Azumaya algebra of degree n with involution *of the second kind*. For example, let A be any Azumaya algebra of degree n over k. Then $A \times A^{\mathrm{op}}$ is an Azumaya algebra of degree n over $K = k \times k$, the split quadratic étale k-algebra, and the switch $\varepsilon_A : A \times A^{\mathrm{op}} \to A \times A^{\mathrm{op}}$ of 10.4 makes $(A \times A^{\mathrm{op}}, \varepsilon_A)$ an Azumaya algebra of degree n with unitary involution over k.

Most important in the present context is of course the case $n = 3$. Let (A,τ) be an Azumaya algebra of degree 3 with unitary involution over k. Then $\mathcal{A} := (K, A, \tau)$, with $K := \mathrm{Cent}(A)$ the centre of A, is an associative involutorial system in the sense of the associativity convention 44.5. By an *admissible scalar for* (A,τ) we mean an admissible scalar for $\mathcal{A}$, i.e., a pair (p,μ) consisting of invertible elements $p \in H(A,\tau)$, $\mu \in K$ such that $N_A(p) = n_K(\mu)$.

44.24 Corollary. *Let (A,τ) be an Azumaya algebra of degree 3 with unitary involution over k and (p,μ) an admissible scalar for (A,τ). Then the second Tits construction*

$$J := J(A,\tau,p,\mu) := J(\mathcal{A},\mu), \quad \mathcal{A} = (K, A, \tau, p), \quad K := \mathrm{Cent}(A)$$

is an Albert algebra over k such that $J_K \cong J(A,\mu)$.

Proof By Corollaries 44.20 and 42.15, $J_K \cong J(A,\mu)$ is an Albert algebra over K. Since K is a faithfully flat k-algebra, Cor. 39.32 therefore implies that J is an Albert algebra over k. □

We conclude this section by describing certain isotopes of second Tits constructions in terms of appropriate isotopes of their co-ordinatizing involutorial systems. The kind of isotopy we have in mind may be introduced as follows.

44.25 Isotopes of involutorial systems. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and $q \in H(\mathcal{B})^\times$. Prop. 43.7 implies that

$$\mathcal{B}^q := (K, B^q, \tau^q, p^q) \tag{1}$$

is again an involutorial k-system, called the *right q-isotope* of $\mathcal{B}$. Recall

$$\tau^q(x) = q^{-1}\tau(qx), \quad p^q = pq \qquad (x \in B) \tag{2}$$

from (43.7.2) and $H(\mathcal{B}^q) = H(\mathcal{B})q = q^{-1}H(\mathcal{B})$ as well as

$$(\mathcal{B}^q)^{q'} = \mathcal{B}^{qq'} \tag{3}$$

for all $q' \in H(\mathcal{B}^q)^\times$ from (43.7.4), (43.7.5).

We also define the *left q-isotope* of $\mathcal{B}$

$$^q\mathcal{B} := (K, {}^qB, {}^q\tau, {}^qp) := \mathcal{B}^{q^\sharp}, \tag{4}$$

where

$${}^qB = B^{q^{-1}}, \quad {}^q\tau(u) = q\tau(q^{-1}u), \quad {}^qp = pq^\sharp \qquad (x \in B), \tag{5}$$

and have $H({}^q\mathcal{B}) = H(\mathcal{B})q^{-1} = qH(\mathcal{B})$ as well as

$${}^{q'}({}^q\mathcal{B}) = {}^{q'q}\mathcal{B} \tag{6}$$

for all $q' \in H({}^q\mathcal{B})^\times$.

The following result was stated as Prop. 32 in the survey [220]. However, that proposition is not correct as stated and has to be replaced by the version presented here.

44.26 Theorem. *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and $q \in H(\mathcal{B})^\times$. If μ is an admissible scalar for $\mathcal{B}$, then $N_B(q)\mu$ is an admissible scalar for ${}^q\mathcal{B}$ and the map*

$$\Phi\colon J(\mathcal{B}, \mu)^{(q)} \xrightarrow{\sim} J({}^q\mathcal{B}, N_B(q)\mu)$$

defined by

$$\Phi(x_0 + uj) := qx_0 + uj \qquad (x_0 \in H(\mathcal{B}),\ u \in B) \tag{1}$$

is an isomorphism of cubic Jordan algebras.

Proof The first part follows from (44.25.5). Since Φ preserves identity elements, the second part will follow once we have shown that Φ preserves adjoints (Exc. 34.18). Setting $J := J(\mathcal{B}, \mu)$, we first compute the adjoint of $J^{(q)}$. For $x_0 \in H(\mathcal{B})$, $u \in B$ we obtain $U_q x_0 = qx_0q$, while (33.8.15), (44.15.6), (44.15.5) yield $U_q(uj) = T(q, uj)q - q^\sharp \times (uj) = (q^\sharp u)j$. Summing up, we therefore obtain

$$U_q(x_0 + uj) = qx_0q + (q^\sharp u)j. \tag{2}$$

Replacing q by q^{-1}, writing N_0 for the norm of $H(\mathcal{B})$ and invoking (33.11.2), (44.26.3), we conclude

$$\begin{aligned}(x_0+uj)^{(\sharp,q)} &= N_0(q)U_{q^{-1}}(x_0+uj)^\sharp\\ &= N_0(q)U_{q^{-1}}\Big([x_0^\sharp - u(p\tau(u))] + [\bar\mu\tau(u^\sharp)p^{-1} - x_0u]j\Big)\\ &= \Big[N_0(q)q^{-1}\Big(x_0^\sharp - u(p\tau(u))\Big)q^{-1}\Big]\\ &\quad + \Big[N_0(q)\bar\mu q^{-1\sharp}(\tau(u^\sharp)p^{-1} - x_0u)\Big]j.\end{aligned}$$

Since $N_0(q)1_B = qq^\sharp$ and

$$\tau(v)p^{-1} = \tau(p^{-1}v) \qquad (v\in B) \tag{3}$$

by (43.5.1), we thus obtain

$$(x_0+uj)^{(\sharp,q)} = \Big[q^{-1}\Big(x_0^\sharp - u(p\tau(u))\Big)q^\sharp\Big] + \Big[\bar\mu q(\tau(p^{-1}u^\sharp) - x_0u)\Big]j,$$

hence

$$\Phi((x_0+uj)^{(\sharp,q)}) = \Big[x_0^\sharp q^\sharp - \Big(u(p\tau(u))\Big)q^\sharp\Big] + [\bar\mu q\tau(p^{-1}u^\sharp) - q(x_0u)]j. \tag{4}$$

On the other hand, we have to compute the adjoint of $\Phi(x_0+uj)$ in $J' = J({}^q\mathcal{B}, N_0(q)\mu)$. Writing $x\cdot y$ for the product in ${}^qB$, we obtain

$$\Phi(x_0+uj)^\sharp = (qx_0+uj)^\sharp = a+bj, \tag{5}$$

where $a\in H({}^q\mathcal{B})$, $b\in B$ by (44.15.3) and (3) (for ${}^q\tau$ in place of τ) are determined by

$$a = (qx_0)^\sharp - u\cdot((pq^\sharp)\cdot {}^q\tau(u)), \tag{6}$$

$$b = N_0(q)\bar\mu\, {}^q\tau((pq^\sharp)^{-1}\cdot u^\sharp) - (qx_0)\cdot u. \tag{7}$$

We have $(qx_0)^\sharp = x_0^\sharp q^\sharp$, and (43.5.3) implies

$$\begin{aligned}(pq^\sharp)\cdot {}^q\tau(u) &= [(pq^\sharp)q][q^{-1}(q\tau(q^{-1}u))] = N_0(q)p\tau(q^{-1}u)\\ &= N_0(q)(p\tau(u))q^{-1},\end{aligned}$$

hence

$$\begin{aligned}u\cdot((pq^\sharp)\cdot {}^q\tau(u)) &= N_0(q)(uq)\Big(q^{-1}(p\tau(u))q^{-1}\Big) = N_0(q)\Big(u(p\tau(u))\Big)q^{-1}\\ &= \Big(u(p\tau(u))\Big)q^\sharp.\end{aligned}$$

By (6), therefore, a agrees with the first term on the right of (4). Similarly, $(qx_0)\cdot u = (qx_0q)(q^{-1}u) = q(x_0u)$ and

$$N_0(q)\,{}^q\tau((pq^\sharp)^{-1}\cdot u^\sharp) = {}^q\tau((qp^{-1}q)(q^{-1}u^\sharp) = {}^q\tau(q(p^{-1}u^\sharp)) = q\tau(p^{-1}u^\sharp),$$

forcing the factor of j on the right of (4) by (7) to agree with b. Thus $\Phi((x_0 + uj)^{(\sharp,q)}) = \Phi(x_0 + uj)^\sharp$, as desired. □

44.27 Corollary (Petersson-Racine [226, Prop. 3.9])**.** *Let (K, B, τ) be an associative involutorial system over k and $q \in H(B,\tau)^\times$. If (p, μ) is an admissible scalar for (K, B, τ), then $(pq^\sharp, N_B(q)\mu)$ is an admissible scalar for $(K, B, {}^q\tau)$, with ${}^q\tau(u) = q\tau(u)q^{-1}$ for $u \in B$, and the assignment*

$$x_0 + uj \longmapsto qx_0 + uj$$

defines an isomorphism

$$J((K, B, \tau), p, \mu)^{(q)} \xrightarrow{\sim} J((K, B, {}^q\tau), pq^\sharp, N_B(q)\mu)$$

of cubic Jordan algebras over k. □

44.28 Corollary. *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and μ an admissible scalar for $\mathcal{B}$. Then the isotope $J(\mathcal{B}, \mu)^{(p)}$ can be realized by the second Tits construction in such a way that the isotopy involution of the corresponding involutorial system is, in fact, an ordinary involution.*

Proof $pp^\sharp = N_B(p)1_B$. □

Exercises

44.29. Let K be a quadratic étale k-algebra and write $\iota = \iota_K$, $a \mapsto \bar{a}$, for the conjugation of K. Let M be a K-module and $\tau\colon M \to M$ an ι-semi-linear map of order 2: $\tau^2 = \mathbf{1}_M$.

(a) Prove with the k-submodule

$$M_0 := H(M,\tau) := \{x \in M \mid \tau(x) = x\}$$

of τ-symmetric elements in M that the K-linear map $\Phi\colon M_0 \otimes K \to M$ induced by the inclusion $M_0 \hookrightarrow M$ is bijective and makes the diagram

$$\begin{array}{ccc} M_0 \otimes K & \xrightarrow[\mathbf{1}_{M_0}\otimes\iota]{} & M_0 \otimes K \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\Phi} \\ M & \xrightarrow[\tau]{} & M \end{array} \tag{1}$$

commutative. (*Hint*: If k is a local ring, there is a basis $1_K, \theta$ of K as a k-module such that $t_K(\theta) = 1$ and $n_K(1 - 2\theta) = -(1 - 4n_K(\theta)) \in k^\times$.)

(b) Deduce from (a) that the passage from (M,τ) to $H(M,\tau)$ is compatible with base change in the following sense: for any $R \in k$-**alg**, the usual identifications yield $M_R := ({}_kM)_R = M_{R_K} = M_{K_R}$ as modules over the quadratic étale R-algebra K_R (cf. 12.27) and $\tau_R\colon M_R \to M_R$ is an $\iota_R(= \iota_{K_R})$-semi-linear map of order 2. Moreover, the k-linear map $x \mapsto x_R$ from M to M_R induces a k-linear map $H(M,\tau) \to H(M_R, \tau_R)$ via restriction, which in turn induces an R-linear isomorphism

$$H(M,\tau)_R \xrightarrow{\sim} H(M_R, \tau_R). \tag{2}$$

(*Hint*: Show first that $x_0 \mapsto x_{0K}$ defines a k-linear isomorphism from M_0 onto $M_0 \otimes 1_K = H(M_0 \otimes K, \mathbf{1}_{M_0} \otimes \iota)$.) Summing up, we thus obtain an identification $H(M,\tau)_R = H(M_R, \tau_R)$ such that the inclusion

$$H(M,\tau)_R = H(M_R,\tau_R) \hookrightarrow M_R$$

is the R-linear extension of the inclusion $H(M,\tau) \hookrightarrow M$. In particular, the k-submodule $H(M,\tau) \subseteq {}_kM$ is *pure* in the sense that the inclusion $H(M,\tau) \hookrightarrow {}_kM$ stays injective under all scalar extensions.

44.30. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k and $\varrho\colon K \xrightarrow{\sim} K'$ an isomorphism of k-algebras. View ${}^{\varrho}K := K'$ as a K-algebra by means of ϱ and ${}^{\varrho}B := B_{\varrho K}$ as a cubic alternative ${}^{\varrho}K$-algebra (with norm $N_{\varrho B} = N_B \otimes_K {}^{\varrho}K$) in the natural way to show that the canonical map

$$\mathrm{can}_{\mathcal{B}} := \mathrm{can}_{B,\varrho K}\colon B \longrightarrow {}^{\varrho}B, \quad u \longmapsto {}^{\varrho}u := u_{\varrho K},$$

is bijective. Conclude that the map ${}^{\varrho}\tau\colon {}^{\varrho}B \to {}^{\varrho}B$ (well) defined by ${}^{\varrho}\tau({}^{\varrho}u) = {}^{\varrho}(\tau(u))$ for all $u \in B$ makes

$${}^{\varrho}\mathcal{B} := ({}^{\varrho}K,\ {}^{\varrho}B,\ {}^{\varrho}\tau,\ {}^{\varrho}p)$$

an involutorial system over k such that

$$(\varrho, \mathrm{can}_{\mathcal{B}})\colon \mathcal{B} \xrightarrow{\sim} {}^{\varrho}\mathcal{B}$$

is an isomorphism of involutorial k-systems.

44.31. *Pointed cubic alternative algebras and core splitness.* We define a *pointed cubic alternative k-algebra* as a pair (A,q) consisting of a cubic alternative algebra A over k and an invertible element $q \in A$, called the *base point* of (A,q). A *homomorphism* $\varphi\colon (A,q) \to (A',q')$ of pointed cubic alternative k-algebras is a homomorphism $\varphi\colon A \to A'$ of cubic alternative algebras preserving base points: $\varphi(q) = q'$. In this way, we obtain the category of pointed cubic alternative algebras over k, denoted by k-**pocu**. If (A,q) is a pointed cubic alternative algebra over k, then $(A,q)_R := (A_R, q_R)$ is one over R, for all $R \in k$-**alg**, called the *base change* or *scalar extension* of (A,q) from k to R.

(a) Let (A,q) be a pointed cubic alternative algebra over k and put

$$\mathrm{Cosp}(A,q) := \big(\mathcal{B}(A,q), \mathbf{1}_K\big), \quad \mathcal{B}(A,q) = (K, B, \varepsilon_A, p), \tag{1}$$

where $K := k \times k$ is the split quadratic étale k-algebra, $B := A \times (A^q)^{\mathrm{op}}$, viewed canonically as a cubic alternative K-algebra with norm $N_B := N_A \times N_A$,

$$\varepsilon_A\colon B \longrightarrow B, \quad (u_1,u_2) \longmapsto (u_2,u_1), \tag{2}$$

is the *switch* and $p := (q,q)$. Then show that $\mathrm{Cosp}(A,q)$ is a core-split involutorial system over k. Moreover, every morphism $\varphi\colon (A,q) \to (A',q')$ in k-**pocu** gives rise to a morphism

$$\mathrm{Cosp}(\varphi) := (\mathbf{1}_K, \varphi \times \varphi)\colon\ \mathrm{Cosp}(A,q) \to \mathrm{Cosp}(A',q') \tag{3}$$

in k-**cosp**.

(b) Conversely, let $(\mathcal{B},\varrho)$ be a core-split involutorial system over k and write $\mathcal{B} =$

(K, B, τ, p). Write $\pi_\pm\colon k \times k \to k$ for the canonical projections, view k as a K-algebra ${}^{\varrho}k_\pm$ by means of the homomorphism $\pi_\pm \circ \varrho\colon K \to k$ and show that

$$\mathrm{Pocu}(\mathcal{B}, \varrho) := ({}^{\varrho}B_+, {}^{\varrho}p_+), \tag{4}$$

where ${}^{\varrho}B_+ := B \otimes_K {}^{\varrho}k_+$ and ${}^{\varrho}p_+$ is the canonical image of $p \in B$ in ${}^{\varrho}B_+$, is a pointed cubic alternative k-algebra. Show further, for any morphism $(\sigma, \varphi)\colon (\mathcal{B}, \varrho) \to (\mathcal{B}', \varrho')$ in k-**cosp**, $\mathcal{B}' = (K', B', \tau', p')$, that $\mathbf{1}_k\colon {}^{\varrho}k_+ \to {}^{\varrho'}k_+$ is σ-semi-linear and

$$\mathrm{Pocu}(\sigma, \varphi) := \varphi \otimes_\sigma \mathbf{1}_k\colon ({}^{\varrho}B_+, {}^{\varrho}p_+) \longrightarrow ({}^{\varrho'}B'_+, {}^{\varrho'}p'_+) \tag{5}$$

is a homomorphism of pointed cubic alternative k-algebras.

(c) Conclude that the correspondences set up in (a), (b) determine an equivalence of categories between k-**pocu** and k-**cosp**.

44.32. *Étale elements in second Tits constructions.* Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system of the second kind over k and μ an admissible scalar for $\mathcal{B}$. Write $J := J(\mathcal{B}, \mu)$ for the corresponding second Tits construction, put $J_0 := H(\mathcal{B}) \subseteq J$ and assume (J, J_0) is a balanced pair of cubic Jordan algebras.

(a) Show for $u \in B$ that the following conditions are equivalent.

(i) $w := uj \in J$ is étale relative to J_0.

(ii) We have $u \in B^\times$ and

$$t_K(\mu N_B(u))^2 - 4n_K(\mu N_B(u)) \in k^\times. \tag{1}$$

(iii) We have $u \in B^\times$ and $K = k[\mu N_B(u)]$.

In this case, using the notation of 44.8, $K_w \cong K$ under the k-isomorphism matching ξ with $\mu N_B(u)$.

(b) Conclude that if $j \in J$ is étale relative to J_0, then J is generated by J_0 and j as a Jordan k-algebra.

44.33. *Moving the base point.* In an involutorial system $\mathcal{B} = (K, B, \tau, p)$ over k, the quantity p is sometimes called the *base point*. Prove:

(a) (cf. Petersson-Racine [226, Prop. 3.7]) If $w \in B$ is invertible, then

$$\mathcal{B} \,.\, w := (K, B^w, \tau, p \,.\, w), \quad p \,.\, w := w^{-1}(p\tau(w^{-1})) \in B^w \tag{1}$$

is an involutorial system over k. Moreover, a quantity $\mu \in K$ is an admissible scalar for $\mathcal{B} \,.\, w$ if and only if $N_B(w)\mu$ is an admissible scalar for $\mathcal{B}$, and in this case,

$$\Phi_{\mathcal{B},w}\colon J(\mathcal{B}, N_B(w)\mu) \xrightarrow{\sim} J(\mathcal{B} \,.\, w, \mu)$$

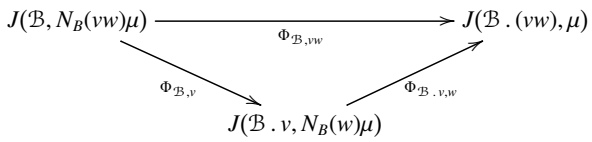
defined by

$$\Phi_{\mathcal{B},w}(x_0 + uj) := x_0 + (uw)j, \tag{2}$$

for $x_0 \in H(\mathcal{B}) = H(\mathcal{B} \,.\, w)$ and $u \in B$, is an isomorphism of cubic Jordan algebras over k.

(b) Let $v, w \in B^\times$. Then $(\mathcal{B} \,.\, v) \,.\, w = \mathcal{B} \,.\, (vw)$. Moreover, if $\mu \in K$ is an admissible

scalar for $\mathcal{B}\,.\,(vw)$, then $N_B(w)\mu$ (resp. $N_B(vw)\mu$) is an admissible scalar for $\mathcal{B}\,.\,v$ (resp. $\mathcal{B}$) and the diagram



(3)

commutes.

(c) (cf. Knus-Merkurjev-Rost-Tignol [160, (39.2)(2)]) To every admissible scalar μ for $\mathcal{B}$, there exist a $w \in B^\times$, an admissible scalar μ' for $\mathcal{B}\,.\,w$, and an isomorphism $J(\mathcal{B}\,.\,w, \mu') \cong J(\mathcal{B}, \mu)$ extending the identity of $H(\mathcal{B}) = H(\mathcal{B}\,.\,w)$ such that $n_K(\mu') = N_{B^w}(p\,.\,w) = 1$. More precisely, we have $\mu' = \bar{\mu}\mu^{-1}$.

Remark. Over fields, the condition $n_K(\mu') = 1$ is equivalent to $\mu' = \bar{\mu}\mu^{-1}$ for some $\mu \in K^\times$ provided $\mathcal{B}$ is of the second kind (Hilbert's Theorem 90). The next exercise will show that this theorem does not hold for quadratic algebras over commutative rings, although the example provided is fppf but not étale, compare 25.19(ix).

44.34. Let $C = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i = \mathrm{Cay}(\mathbb{Z}, -1)$ be the quadratic $\mathbb{Z}$-algebra of Gaussian integers as defined in 3.16. Note that the norm of C is induced via restriction by the norm of the two-dimensional composition algebra $\mathbb{C} = \mathrm{Cay}(\mathbb{R}, -1)$ over the reals, so $n_C(z) = |z|^2$ for all $z \in C$. In particular, $n_C(i) = 1$. But show that there is no invertible element $z \in C$ satisfying $i = \bar{z}z^{-1}$.

44.35. *Core-split Azumaya algebras with unitary involution.* Let (A, τ) be an Azumaya algebra of degree n with unitary involution over k and suppose $K := \mathrm{Cent}(A)$ is split quadratic étale. Show that there is an Azumaya algebra B of degree n over k such that $(A, \tau) \cong (B \times B^{\mathrm{op}}, \varepsilon_B)$. Conclude that, if K is arbitrary (quadratic étale), then $(A, \tau)_K = (A_K, \tau_K) \cong (A \times A^{\mathrm{op}}, \varepsilon_A)$.

44.36. Let $\mathcal{B} = (k, B, \tau, p)$ be an involutorial system of the first kind over k and μ an admissible scalar for $\mathcal{B}$. Show that the cubic Jordan algebra $J(\mathcal{B}, \mu)$ is regular if and only if B is regular and $2 \in k^\times$.

44.37. Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over k. Show for any admissible scalar μ for $\mathcal{B}$ that, up to isotopy of the second Tits construction $J := J(\mathcal{B}, \mu)$, we may assume $p = 1_B$. Moreover, if the norm of B is surjective as a set map from B to K, then, up to isomorphism (resp. isotopy) of J, we may assume $\mu = 1_K$ (resp, $p = 1_B$ and $\mu = 1_K$).

44.38. Assume $2 \in k^\times$, let C be a composition algebra of rank $2r$ ($r = 1, 2, 4$) over k and $B \subseteq C$ a composition subalgebra of rank r, so that we have the decomposition $C = B \oplus B^\perp$ as a direct sum of k-modules.

(a) Show that the map $\tau_B \colon C \to C$ defined by

$$\tau_B(v + w) := \bar{v} + w \qquad (v \in B\ w \in B^\perp) \tag{1}$$

is an involution of C such that

$$H(C, \tau_B) = k1_B \oplus B^\perp. \tag{2}$$

(b) Conclude that $\hat{\mathcal{C}} := \hat{\mathcal{C}}_B := (k, \hat{C}, \hat{\tau}_B, 1_{\hat{C}})$ is an involutorial system of the first kind over k, where $\hat{C} = k \times C$ is the cubic alternative k-algebra of Exc. 34.24 (c) and $\hat{\tau}_B \colon \hat{C} \to \hat{C}$ is the *unital extension* of τ:

$$\hat{\tau}_B((\alpha, x)) := (\alpha, \tau_B(x)) \qquad (\alpha \in k,\ x \in C).$$

(c) Show that the elementary idempotent

$$e_1 := (1, 0) \in J_0 := H(\hat{\mathcal{C}}) \subseteq J := J(\hat{\mathcal{C}}, 1) \tag{3}$$

can be extended to an elementary frame $\Omega = (e_1, e_2, e_3)$ of J_0 if and only if there is an identification

$$C = \mathrm{Cay}(B, 1) = B \oplus Bj_0 \tag{4}$$

by means of the Cayley-Dickson construction such that

$$e_2 := (0, \frac{1}{2}(1_B + j_0)), \quad e_3 = (0, \frac{1}{2}(1_B - j_0)). \tag{5}$$

In this case, Ω can be extended to a strong co-ordinate system of J and

$$J \cong \mathrm{Her}_3(B) \tag{6}$$

under an isomorphism matching Ω with the diagonal frame of $\mathrm{Her}_3(B)$. Finally, for any diagonal matrix $\Gamma \in \mathrm{GL}_3(k)$, there is a $q \in H(\hat{\mathcal{C}})$ of norm 1 such that

$$\mathrm{Her}_3(B, \Gamma) \cong J({}^q\mathcal{B}, 1), \quad \mathcal{B} := \hat{\mathcal{C}}_B. \tag{7}$$

44.39. Consider the involutorial system

$$\hat{\mathcal{C}} := (k, \hat{C}, \hat{\iota}_C, 1)$$

of the first kind over k, where C is a composition algebra of rank $r = 1, 2, 4, 8$ over k, $\hat{C} := k \times C$ is the cubic alternative k-algebra of Exc. 34.24 (b), and $\hat{\iota}_C \colon \hat{C} \to \hat{C}$ is the involution defined by

$$\hat{\iota}_C((\alpha, v)) := (\alpha, \bar{v}) \qquad (\alpha \in k,\ v \in C). \tag{1}$$

We wish to study the second Tits construction

$$J := J(\hat{\mathcal{C}}, 1) = J_0 \oplus \hat{C}j, \quad J_0 := H(\hat{\mathcal{C}}) = H(\hat{C}, \hat{\iota}_C). \tag{2}$$

(a) Assume $2 \in k^\times$ and show that $\Omega := (e_1, e_2, e_3)$ with

$$e_1 := (1, 0), \quad e_2 := \frac{1}{2}(e_0 + e_1 j), \quad e_3 := \frac{1}{2}(e_0 - e_1 j), \quad e_0 := (0, 1_C) \tag{3}$$

is an elementary frame of J such that $J_1(e_3) = \{0\}$. Conclude that

$$J \cong k \times J(M_0, q_0, e_0), \tag{4}$$

where (M_0, q_0, e_0) is a pointed quadratic module having $M_0 = J_0(e_3)$ as k-modules and $q_0 \cong \mathbf{h} \perp (-2n_C)$ as quadratic forms.

(b) Assume $2 = 0$ in k and $r > 1$. Then show that J has rank $2r + 1$ as a finitely generated projective k-module. Moreover,

(i) The assignment
$$v \longmapsto e_v := (1, n_C(v)1_C) + (n_C(v), v)j$$
defines an isomorphism of k-schemes from $C_{\mathbf{a}}$ to $\mathbf{Elid}(J)$.
(ii) J does not contain elementary frames.
(iii) If k is reduced, then
$$\mathrm{Nil}(J) = \{(0, \alpha 1_C) + (\alpha, v)j \mid \alpha \in k,\ v \in C\};$$
in particular, $\mathrm{Nil}(J)$ is finitely generated projective of rank $r+1$ as a k-module.

Remark. By Exc. 19.39, the examples presented in Exercises 44.38, 44.39 (a) exhaust the involutions (of the first kind) living on a composition algebra of rank $r = 1, 2, 4, 8$ and their cubic companions over any commutative ring in which 2 is a unit. Also, by Exc. 44.37, up to isotopy of the second Tits constructions arising from involutorial systems $(k, \hat{C}, \hat{\tau}, p)$ and appropriate admissible scalars μ, it may always be assumed that $p = 1_{\hat{C}}, \mu = 1$.

44.40. Let K be a quadratic étale k-algebra, C a composition algebra of rank r over K and τ a k-involution of C that is an ι_K-semi-linear homomorphism from C to C^{op} in the sense of 16.17.

(a) Show that there exists a composition algebra C_0 over k such that (C, τ) and $(C_0 \otimes K, \iota_{C_0} \otimes \iota_K)$ are isomorphic as k-algebras with involution.

(b) Show that $\mathcal{B} := (K, \hat{C}, \hat{\tau}, 1_{\hat{C}})$, with $\hat{C} = K \times C$ as a cubic alternative K-algebra in the sense of Exc. 34.24 (b) and $\hat{\tau}((a, v)) = (\iota_K(a), \tau(v))$ for $a \in K$ and $v \in C$, is an involutorial system of the second kind over k. Moreover, $J(\mathcal{B}, \mu)$, for any admissible scalar μ for $\mathcal{B}$, is a Freudenthal algebra of rank $3(r+1)$ over k.

(c) Does there exist a diagonal matrix $\Gamma \in \mathrm{GL}_3(k)$ such that $J(\mathcal{B}, \mu) \cong \mathrm{Her}_3(C, \Gamma)$?[2]

44.41. *The opposite of an involutorial system.* Show that, if $\mathcal{B} = (K, B, \tau, p)$ is an involutorial system over k, then so is
$$\mathcal{B}^{\mathrm{op}} := (K, B^{\mathrm{op}}, \tau, p^{-1}),$$
called the *opposite* of $\mathcal{B}$. Moreover, if μ is an admissible scalar for $\mathcal{B}$, then μ^{-1} is an admissible scalar for $\mathcal{B}^{\mathrm{op}}$ and
$$\Phi\colon J(\mathcal{B}, \mu) \xrightarrow{\sim} J(\mathcal{B}^{\mathrm{op}}, \mu^{-1})$$
defined by
$$\Phi(x_0 + uj) := x_0 + \tau(up)j, \tag{1}$$
for $x_0 \in H(\mathcal{B}) = H(\mathcal{B}^{\mathrm{op}})$ and $u \in B$, is an isomorphism of cubic Jordan algebras over k.

45 Freudenthal pairs and the search for étale elements

Our approach to the second Tits construction of cubic Jordan algebras, relying as it does on the notion of an étale element, would be entirely useless were we

[2] The answer to this question is not known, not even for $\mu = 1_K$.

not able to prove that, under suitable hypotheses, étale elements do indeed exist. This will be accomplished in the present section, with suitable hypotheses pertaining to certain properties of LG rings (11.20). We begin by introducing the relevant terminology.

45.1 Freudenthal pairs. By a *Freudenthal pair of rank* $3n$ ($n \in \mathbb{Z}$, $n > 0$) over k we mean an n-balanced pair (J, J_0) of cubic Jordan k-algebras such that J is a Freudenthal algebra. More explicitly, therefore, J is a Freudenthal algebra of rank $3n$ containing J_0 as a regular cubic Jordan subalgebra of rank n. We simply speak of a Freudenthal pair if the rank does not require specifications. Freudenthal pairs will be viewed as a full subcategory, denoted by k-**frapa**, of k-**bapa**, the category of balanced pairs of cubic Jordan k-algebras. Freudenthal pairs of rank 27 are also called *Albert pairs*. In the sequel, the *base change of Freudenthal pairs* plays an important role: if (J, J_0) is a Freudenthal pair over k, then $(J, J_0)_R := (J_R, J_{0R})$ is one over R, for any $R \in k$-**alg**. It is also useful to observe that two Freudenthal pairs (J, J_0) and (J, J_0') with the same Freudenthal algebra J "on top" are isomorphic if and only if J_0 and J_0' are conjugate under the automorphism group of J.

Finally, by abuse of language, the Freudenthal pair (J, J_0) is said to *admit étale* (*resp. Kummer*) *elements* if étale (resp. Kummer) elements of J relative to J_0 exist. Note by 42.12 (c) and Cor. 42.13 that a Freudenthal pair admits Kummer elements if and only if it *arises from the first Tits construction*, i.e., it is isomorphic to $(J(A, \mu), A^{(+)})$, for some regular cubic alternative algebra A of constant rank and some invertible element μ in the base ring. Similarly, if a Freudenthal pair admits étale elements, then by Cor. 44.17 it *arises from the second Tits construction*, i.e., there exist a regular involutorial system $\mathcal{B}$ of the second kind over k as well as an admissible scalar μ for $\mathcal{B}$ making it isomorphic to $(J(\mathcal{B}, \mu), H(\mathcal{B}))$. But note that, conversely, *a second Tits construction of the second kind need not admit étale elements*, see Remark 45.5 below for an example.

45.2 Proposition. *Let A be a regular cubic alternative k-algebra of constant rank and $\mu \in k$ an invertible scalar. Viewing $A^{(+)} \subseteq J := J(A, \mu)$ as a regular cubic Jordan subalgebra via 42.12 (a), and letting $x_1, x_2 \in A$, the following conditions are equivalent.*

(i) $x := x_1 j_1 + x_2 j_2$ *is an étale element of J relative $A^{(+)}$.*

(ii) $x_1, x_2 \in A^\times$ *and* $N_A(x_1) - \mu N_A(x_2) \in k^\times$.

Proof By (42.11.3) and (42.11.4), $x^\sharp = -\mu x_1 x_2 + \mu x_2^\sharp j_1 + x_1^\sharp j_2$ and $N_J(x) =$

$\mu N_A(x_1) + \mu^2 N_A(x_2)$. In the notation of 44.8, this implies $Q(x) = \mu x_1 x_2$, hence

$$\begin{aligned} N_J(x)^2 - 4N_{J_0}(Q(x)) &= \mu^2 N_A(x_1)^2 + 2\mu^3 N_A(x_1x_2) + \mu^4 N_A(x_2)^2 - 4\mu^3 N_A(x_1x_2) \\ &= \mu^2 (N_A(x_1) - \mu N_A(x_2))^2. \end{aligned}$$

The assertion follows from the definition of an étale element. □

Note by Exercise 45.22 that $(J(A,\mu), A^{(+)})$, for any regular cubic alternative k-algebra A of constant rank and any $\mu \in k^\times$, will always be a Freudenthal pair over k.

45.3 Corollary. *Let A be a regular cubic alternative k-algebra of constant rank and $\mu \in k^\times$. If the Freudenthal pair $(J(A,\mu), A^{(+)})$ admits étale elements, then for every maximal ideal $\mathfrak{m} \subseteq k$ the field $k/\mathfrak{m}$ is not $\mathbb{F}_2$.*

Proof Otherwise, $\mathbb{F}_2$ would belong to k-**alg**, so in order to arrive at a contradiction, we may change scalars and assume $k = \mathbb{F}_2$. But then $N_A(x_1) - \mu N_A(x_2) = 0$ for all $x_1, x_2 \in A^\times$, violating condition (ii) of Prop. 45.2. □

45.4 Corollary. *Let A be a regular cubic alternative algebra over a field F and $\mu \in F^\times$. Assume the norm of A is surjective as a set map from A to F. The Freudenthal pair $(J(A,\mu), A^{(+)})$ admits étale elements if and only if $F \ncong \mathbb{F}_2$.*

Proof Necessity follows from Cor. 45.3. Conversely, assume F contains more than two elements. By hypothesis, some $x_1 \in A^\times$ satisfies $N_A(x_1) \neq \mu$. Hence $x_1 j_1 + j_2$ by Prop. 45.2 is an étale element of $J(A,\mu)$ relative to $A^{(+)}$. □

45.5 Remark. (a) Let A be a regular cubic alternative algebra over $\mathbb{F}_2$. Then $(J(A,1), A^{(+)})$, the corresponding Freudenthal pair, by Cor. 45.3 does not admit étale elements despite being a second Tits construction arising from an appropriate core-split involutorial system (Thm. 44.19).

(b) In Cor. 45.4, the hypothesis on the norm of A is fulfilled if $\dim_F(A) > 1$ and F is finite (Exc. 42.21(a)).

Our next aim will be to show that Freudenthal pairs over an algebraically closed field always admit Kummer elements. For this we need a preparation.

45.6 Lemma. *Let C be a composition algebra over a field F and $K \subseteq C$ a quadratic étale subalgebra. Then (J, J_0), where*

$$J := \mathrm{Her}_3(C), \quad J_0 := \sum Fe_{ii} + K^\perp[23] \tag{1}$$

and $K^\perp$ refers to the orthogonal complement of K relative to the polarized norm of C, is a Freudenthal pair over F. Moreover, this Freudenthal pair admits étale elements provided K is a field or F contains more than two elements.

Proof Put $r := \dim_F(C)$. Then J is a Freudenthal algebra of dimension $3(r+1)$, while $J_0 \subseteq J$ is a subspace of dimension $r+1$. But J_0 is also a regular cubic Jordan subalgebra since (36.4.4) shows that it is stable under the adjoint map. Summing up, therefore, (J, J_0) is a Freudenthal pair, and we have $J_0^\perp = K[23]+C[31]+C[12]$ by (36.4.7). Thanks to our hypotheses on K and F, there exists an invertible element $a \in C$ of trace 1 that generates K as an F-algebra. Put $w := a[23] + 1_C[31] + 1_C[12] \in J_0^\perp$. Then (36.4.5) and (36.4.4) imply

$$N_J(w) = t_K(a) = 1,$$
$$w^\sharp = -n_K(a)e_{11} - e_{22} - e_{33} + 1_C[23] + \bar{a}[31] + \bar{a}[12].$$

In the notation of 44.8, therefore, $Q(w) = n_K(a)e_{11} + e_{22} + e_{33}$ is invertible in J_0 and $N_J(w)^2 - 4N_{J_0}(Q(w)) = t_K(a)^2 - 4n_K(a) \in F^\times$ by Prop. 19.8. Thus $w \in J$ is étale relative to J_0. □

45.7 Proposition. *Let C be a composition algebra of dimension $r \geq 4$ over a field F all of whose regular binary quadratic spaces are universal. Put $J := \mathrm{Her}_3(C)$ and let $J_0 \subseteq J$ be a regular cubic Jordan subalgebra of dimension $r+1$. Then the following statements hold.*

(a) *C is split.*

(b) *If J_0 is not simple, then up to isomorphism of (J, J_0) there exists a quadratic étale subalgebra $K \subseteq C$ such that*

$$J_0 = \sum Fe_{ii} + K^\perp[23]. \tag{1}$$

Proof (a) By Thm. 19.16, there exists a quadratic étale subalgebra $K \subseteq C$ and, for some $\mu \in F^\times$, the inclusion $K \hookrightarrow C$ extends to an embedding from the quaternion algebra $B := \mathrm{Cay}(K, \mu)$ to C. By hypothesis, μ is a norm of K. Now Cor. 23.6 shows that the norm of B is isotropic. Hence so is the norm of C, and C is split (Cor. 22.18).

(b) Since J_0 is not simple, we deduce from Thm. 39.6 that $J_0 \cong F^{(+)} \times J(M_0, q_0, e_0)$ for some regular pointed quadratic module (M_0, q_0, e_0) over F. By Exercises 40.15 (f) and 41.31, the automorphism group of J acts transitively on the elementary idempotents of J. Up to isomorphism of (J, J_0), we may therefore assume

$$J_0 = Fe_{11} \oplus J(M_0, q_0, e_0),$$

where $M_0 \subseteq J_0(e_{11}) = Fe_{22} + Fe_{33} + C[23]$ is a subspace of dimension r, $e_0 = e_{22} + e_{33}$, and q_0 is the restriction of S_J to M_0 (Cor. 37.3). By (a) and (36.4.9), the quadratic space $(J_0(e_{11}), S_J|_{J_0(e_{11})})$ is hyperbolic of dimension $r+2$ containing (M_0, q_0) as an r-dimensional quadratic subspace. Since $r > \frac{1}{2}(r+2)$, this subspace is therefore isotropic. By hypothesis, it is also regular, and we

conclude from Prop. 39.5 that $J(M_0, q_0, e_0)$ contains an elementary idempotent. Consulting Exc. 41.31 again, we may therefore assume up to isomorphism of (J, J_0) that $J_0 = \sum Fe_{ii} \oplus U_1[23]$, for some regular subspace $U_1 \subseteq C$ of dimension $r-2$. Thus $C = U_1 \oplus U_1^\perp$, and $U_1^\perp$, being a regular binary quadratic subspace of C, by hypothesis contains an element u_1 of norm 1. One checks that the assignment

$$\sum(\xi_i e_{ii} + v_i[jl]) \longmapsto \sum \xi_i e_{ii} + (u_1^{-1}v_1)[23] + (v_2u_1^{-1})[31] + (u_1v_3u_1)[12]$$

defines an automorphism of J (cf. Exc. 5.18), so up to isomorphism of (J, J_0) we may assume $1_C \in U_1^\perp$. Hence $K := U_1^\perp \subseteq C$ is a quadratic étale subalgebra, and we have established (1). □

45.8 Corollary. *Every Freudenthal pair over an algebraically closed field admits Kummer elements.*

Proof Let F be an algebraically closed field and (J, J_0) a Freudenthal pair over F. By Thm. 42.16, it suffices to show that J contains an invertible element $l \in J_0^\perp$ having $l^\sharp \in J_0^\perp$ as well. In order to do so, we first note by Cor. 39.11 that the dimension of J_0 is one of the numbers $n = 1, 2, 3, 5, 9$. The corresponding cases will now be discussed separately, bearing in mind the structure of simple cubic Jordan algebras over algebraically closed fields as described in Cor. 39.7.

Suppose first that $n = 1$. Then $\mathrm{char}(F) \neq 3$ and $J = E^{(+)}$, where $E := F \times F \times F$ is the split cubic étale F-algebra. Hence $J_0 = F \cdot 1_E$ and $J_0^\perp = \mathrm{Ker}(T_E)$. Let $\zeta \in F$ be a cube root of 1. Then one checks that $l := (1, \zeta, \zeta^2)$ is a Kummer element of J relative to J_0.

Suppose next that $n = 2$. Then $\mathrm{char}(F) \neq 2$, $J = \mathrm{Her}_3(F)$ and $J_0 \cong (k \times k)_{\mathrm{cub}}^{(+)}$, where $(k \times k)_{\mathrm{cub}}$ is defined as in 34.15. By Cor. 39.3 and Exc. 40.15 (f), up to isomorphism of $(J.J_0)$ we may assume $J_0 = Fe_{11} + F(e_{22} + e_{33})$. This implies $J_0^\perp = F(e_{22} - e_{33}) + \sum F[jl]$. Letting $\beta_1 \in F$ satisfy $\beta_1^2 = -1$, one checks using the formulas from 36.4 that $l = e_{22} - e_{33} + \beta_1[23] - \beta_1[31] + 1[12] \in J_0^\perp$ is a Kummer element of J relative to J_0.

Finally suppose that $n = 3$, 5 or 9. Let us first assume that J_0 is not simple, which holds automatically for $n \neq 9$. Up to isomorphism of (J, J_0), either for trivial reasons or by Prop. 45.7, there exists a quadratic étale subalgebra $K \subseteq C$ such that $J_0 = \sum Fe_{ii} + K^\perp[23]$, and F being algebraically closed, K is split. Let $c \in K$ be an elementary idempotent. The quantity $l := \sum c[jl]$ belongs to $J_0^\perp = K[23] + C[31] + C[12]$, has norm $N_J(l) = t_C(c) = 1$ and adjoint $l^\sharp = \sum \bar{c}[jl] \in J_0^\perp$, hence is a Kummer element of J relative to J_0.

We are left with the case that J_0 is simple, i.e., isomorphic to $\mathrm{Mat}_3(F)^{(+)}$. Then J is the split Albert algebra over F and by (45.18.1) combined with

Prop. 40.6, we have an isomorphism

$$(J, J_0) \cong \big(\mathrm{Her}_3(\mathrm{Zor}(F)), \mathrm{Her}_3(F \times F)\big),$$

so the assertion follows from Exc. 42.23. □

45.9 Residually big rings. We now introduce a terminology that is not standard but turns out to be convenient for our subsequent applications. We will say that a commutative ring k is *residually big* if the residue fields $k/\mathfrak{m} \ncong \mathbb{F}_2, \mathbb{F}_4$ for all maximal ideals $\mathfrak{m} \subseteq k$. We say k is *residually small* otherwise. For example, any commutative ring containing $1/2$ or containing a field with more than four elements is residually big.

45.10 Theorem. *For any LG ring k, the following conditions are equivalent.*

(i) *k is residually big.*
(ii) *All Freudenthal pairs over k admit étale elements.*

Proof (ii) ⇒ (i). If k were residually small, we would find a maximal ideal $\mathfrak{m} \subseteq k$ having $k/\mathfrak{m} = \mathbb{F}_2$ or $k/\mathfrak{m} = \mathbb{F}_4$. In the former (resp. the latter) case, Cor. 45.3 (resp. Exc. 45.15 (d)(ii)) would lead to a contradiction.

(i) ⇒ (ii). Let (J, J_0) be an arbitrary Freudenthal pair over k and write n for the rank of J_0 as a k-module. Since k is an LG ring, $J_0^\perp$ is a free k-module of rank $2n$ (11.24). In the notation of 44.8, therefore, the scalar polynomial law

$$f := f_{J,J_0} \colon J_0^\perp \longrightarrow k, \quad u \longmapsto N_{J_0}(Q(u))\Big(N_J(u)^2 - 4N_{J_0}(Q(u))\Big)$$

may be viewed as a polynomial $f \in k[\mathbf{t}_1, \ldots, \mathbf{t}_{2n}]$ that by (44.8.6) represents an invertible element in $k_\mathfrak{m}$, $\mathfrak{m} \subseteq k$ any maximal ideal, if and only if the Freudenthal pair $(J, J_0)(\mathfrak{m})$ over $k/\mathfrak{m}$ admits étale elements. By the definition of an LG ring, we may thus assume from now on that $F := k$ *is a field having characteristic* 3 *or containing more than four elements*.

Let $(\bar{J}, \bar{J}_0)$ be the base change of (J, J_0) to the algebraic closure of F, which by Cor. 45.8 admits Kummer elements, hence arises form the first Tits construction. By Prop. 45.2, therefore, $(\bar{J}, \bar{J}_0)$ admits étale elements whence f_{J,J_0} is not the zero polynomial. Hence a Zariski density argument shows that (J, J_0) itself admits étale elements provided F is infinite. We are thus reduced to the case that F *is a finite field of characteristic* 3 *or containing more than four elements.* By 23.14 all composition algebras of dimension at least 4 over F are split, as are all Freudenthal algebra of dimension at least 15 (Exc. 40.17).

As in the proof of Cor. 45.8 we have $n = 1, 2, 3, 5, 9$, and each of these cases will now be treated individually. However, the discussion that ensues will be more complicated than in loc. cit. since F is not algebraically closed.

This holds true, in particular, for the structure of regular cubic alternative F-algebras as described in Exc. 42.21.

(a) $n = 1$. Then $\mathrm{char}(F) \neq 3$, $J = E^{(+)}$ for some cubic étale F-algebra E and $J_0 = F \cdot 1_E$. The assertion follows from Exc. 45.15 (c), (d).

(b) $n = 2$. Then $\mathrm{char}(F) \neq 2$ and J_0 is a regular cubic Jordan algebra of dimension 2 which, thanks to Exc. 16.21, is supported by some pointed quadratic module in the sense of Exc. 34.27. Thus, by (iii) of that exercise, $J_0 \cong (k \times k)^{(+)}_{\mathrm{cub}}$ as cubic Jordan algebras. On the other hand, J is a regular simple cubic Jordan algebra of dimension 6 that inherits from J_0 an elementary idempotent, denoted by e_1 and corresponding to $(1,0) \in (k \times k)^{(+)}_{\mathrm{cub}}$. By Exc. 40.15 (f), e_1 can be extended to an elementary frame (e_1, e_2, e_3) of J such that $e_0 := 1_J - e_1 = e_2 + e_3$. Applying Prop. 39.2, we therefore find an identification

$$(J, J_0) = (\mathrm{Her}_3(F, \Gamma), Fe_{11} + F(e_{22} + e_{33})),$$

for some diagonal matrix $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathrm{GL}_3(F)$. This implies $J_0^\perp = F(e_{22} - e_{33}) + F[23] + F[31] + F[12]$. Hence $w := 1[23] + 1[31] \in J_0^\perp$ satisfies $N_J(w) = 0$ and

$$w^\sharp = -\gamma_2\gamma_3 e_{11} - \frac{1}{2}\gamma_3\gamma_1(e_{22} + e_{33}) - \frac{1}{2}\gamma_3\gamma_1(e_{22} - e_{33}) + \gamma_3[23].$$

We conclude $Q(w) = \gamma_2\gamma_3 e_{11} + \frac{1}{2}\gamma_3\gamma_1(e_{22} + e_{33})$ and $N(w)^2 - 4N_{J_0}(Q(w)) = -\frac{1}{4}\gamma_1^2\gamma_2\gamma_3^3 \neq 0$, so w is an étale element of J relative to J_0.

(c) $n = 3$. Then $J_0 = E^{(+)}$ for some cubic étale F-algebra E, and J is a Freudenthal algebra of dimension 9, hence identifies with $\mathrm{Her}_3(L)$, where L is either split quadratic étale over F or the unique (separable) quadratic field extension of F. In any event, the norm of L is universal, so in $\mathrm{Her}_3(L)$ no twist by an invertible 3-by-3 diagonal matrix is required ((37.24.3)). Moreover, every elementary idempotent of J can be extended to an elementary frame (Exc. 40.15 (f)), and any two elementary frames of J are conjugate under $\mathrm{Aut}(J)$ (Exc. 41.31). We now discuss the following subcases.

(c1) *E is split.* Up to isomorphism of (J, J_0) we may assume $J_0 = \sum Fe_{ii}$, and setting $K := L$ in Lemma 45.6, we have $K^\perp = \{0\}$, so J_0 is as in (45.6.1) and there are étale elements of J relative to J_0.

(c2) *$E \cong F \times K$, where K is the unique quadratic field extension of F.* By what we have just seen, we may assume

$$J_0 = Fe_{11} \oplus K, \quad K \subseteq J_0(e_{11}) \subseteq J. \tag{1}$$

More precisely, by Prop. 37.2 and its corollary 37.3, K is a separable quadratic

subfield of the Jordan algebra of Clifford type $J(M_0, q_0, e_0)$ with

$$M_0 = Fe_{22} + Fe_{33} + L[23], \quad q_0 := S_J|_{M_0}, \quad e_0 := e_{22} + e_{33}. \tag{2}$$

Combining (2) with (36.4.9), we obtain

$$q_0(\xi_2 e_{22} + \xi_3 e_{33} + u[23]) = \xi_2\xi_3 - n_L(u) \tag{3}$$

for all $\xi_2, \xi_3 \in F$ and $u \in L$. In particular, since n_L is a universal Pfister form, we conclude

$$q_0 \cong \mathbf{h} \perp n_L. \tag{4}$$

The orthogonal complements of K in M_0 relative to Dq_0 will be denoted by $K^\perp$, so we have $M_0 = K \oplus K^\perp$. There are the following two subcases.

(c2.1) *$L = F \times F$ is split.* Then $J = A^{(+)}$ with $A := \mathrm{Mat}_3(F)$ after the natural identification of Prop. 36.9. Writing e_{ij}, $1 \le i, j \le 3$, for the usual matrix units of A, we deduce from (1) that

$$J_0 = Fe_{11} \oplus K, \tag{5}$$

where K is a subfield of the Peirce component $A_{00}(e_{11}) = Fe_{22} + Fe_{23} + Fe_{32} + Fe_{33}$, which canonically identifies with the split quaternion algebra $B := \mathrm{Mat}_2(F)$. Note that q_0 by (4) and (c2.1) is hyperbolic, so its restriction to $K^\perp$ must be anisotropic. From (5) we conclude

$$J_0^\perp = J_1(e_{11}) \oplus K^\perp = Fe_{12} + Fe_{13} + Fe_{21} + Fe_{31} + K^\perp. \tag{6}$$

In particular,

$$w = w_1 + w_0, \quad w_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = (1, -1)[12] \in J_1(e_{11}) \tag{7}$$

with an as yet unspecified quantity $w_0 \in K^\perp \subseteq M_0$ belongs to $J_0^\perp$. Hence (36.4.4) implies $w_1^\sharp = e_{33} \in B \setminus B^\times$, which is therefore neither contained in K nor in $K^\perp$. Thus

$$e_{33} = w_1^\sharp = a + b, \quad a \in K^\times, \quad b \in K^\perp \setminus \{0\}. \tag{8}$$

Combining (38.7.11) with the fact that $w_0 \in K^\perp$ has trace zero in B, hence satisfies $\bar{w}_0 = -w_0$, we conclude

$$w^\sharp = q_0(w_0)e_{11} + w_0 \circ w_1 + e_{33}, \tag{9}$$

while (38.7.12), (11.14.3) and (8) imply

$$N_J(w) = -q_0(w_0, e_{33}) = -q_0(w_0, b) \tag{10}$$

On the other hand, combining (9) with (8) and the Peirce rules yields $Q(w) = -q_0(w_0)e_{11} - a$, hence

$$N_{J_0}(Q(w)) = -q_0(w_0)n_K(a) = -q_0(w_0)q_0(a). \tag{11}$$

Now, if $\mathrm{char}(F) \neq 2$,, then some $w_0 \in K^\perp \setminus \{0\}$ satisfies $q_0(w_0, b) = 0$, and (10), (11) imply $N_{J_0}(Q(w)) \neq 0 \neq N_J(w)^2 - 4N_J(Q(w))$. Thus $w \in J$ is étale relative to J_0. On the other hand, if $\mathrm{char}(F) = 2$, regularity of q_0 on $K^\perp$ implies that some $w_0 \in K^\perp$ has $q_0(w_0, e_{33}) \neq 0$, so (10) shows again that w is an étale element of J relative to J_0.

(c2.2) $L \cong K$. Since F contains more than two elements, it suffices to show that (J, J_0) admits Kummer elements (Cor. 45.4). This in turn will follow from Exc. 45.16 below once we have shown that the binary quadratic space $(E^\perp, q_E)$ derived from the Springer form of E in the sense of Exc. 42.26 is a split hyperbolic plane. If E were a field, it would be enough to find an isotropic vector in $E^\perp$ relative to q_E. But under the present circumstances where $E \cong F \times K$, we have to argue differently by invoking the formalism of 9.7 that will eventually allow us to reduce everything to the field case.

Accordingly, we put $\varepsilon_+ := e_{11}$, $\varepsilon_- := e_{22} + e_{33}$ and obtain a complete orthogonal system $(\varepsilon_+, \varepsilon_-)$ of idempotents in E such that $E = E_+ \oplus E_-$, $E_+ = Fe_{11} = F$ and $E_- = \varepsilon_- E = K$ after the canonical identifications. From (1) we deduce

$$E^\perp = J_0^\perp = J_1(e_{11}) \oplus K^\perp = L[31] \oplus L[12] \oplus K^\perp, \tag{12}$$

which by Prop. 37.2 (b) gives rise to the decomposition

$$E^\perp = E_+^\perp \oplus E_-^\perp, \quad E_+^\perp := \varepsilon_+ \cdot E^\perp = K^\perp, \quad E_-^\perp := \varepsilon_- \cdot E^\perp = L[31] \oplus L[12]. \tag{13}$$

as a direct sum of E-modules. Note that (9.7.2), (9.7.3) yield canonical identifications $E_\pm^\perp = E^\perp \otimes_E E_\pm$ as $E_\pm$-modules, allowing us to consider the regular quadratic forms

$$(q_E)_\pm := q_E \otimes_E E_\pm \colon E_\pm^\perp \longrightarrow E_\pm \tag{14}$$

over the fields $E_\pm$. From these q_E can be recovered via (13) and

$$q_E = (q_E)_+ \oplus (q_E)_-. \tag{15}$$

We will therefore be through as soon as we have shown that $(q_E)_\pm$ are both isotropic. Note first that $(q_E)_\pm(x_\pm) = q_E(x_\pm)$ for all $x_\pm \in E_\pm^\perp \subseteq E^\perp$. Next we claim

(i) $(q_E)_+$ is the restriction of $-q_0$ to $K^\perp$.

(ii) $(q_E)_-(u_2[31] + u_3[12])$ for $u_2, u_3 \in L$ is the K-component along $K^\perp$ of

$$n_L(u_2)e_{22} + n_L(u_3)e_{33} - \overline{u_2u_3}[23] \in M_0 = K \oplus K^\perp.$$

In order to prove (i), let $x_+ \in E_+^\perp = K^\perp$. Since the elements of $K^\perp$ have trace zero in $J_0(e_{11})$, we may write $x_+ = \xi(e_{11}-e_{22})+u_1[23]$ for some $\xi \in F$ and some $u_1 \in L$. Hence (36.4.4) implies $x_1^\sharp = -(\xi^2+n_L(u_1))e_{11} = q_0(x_+)e_{11} \in Fe_{11} \subseteq E$, and by the definition of Springer forms, (i) follows. In (ii) we use (36.4.4) again to compute

$$(u_2[31] + u_3[12])^\sharp = -n_L(u_2)e_{22} - n_L(u_3)e_{33} + \overline{u_2u_3}[23],$$

and the assertion follows.

Combining (4) with the decomposition $q_0 = n_K \perp q_0|_{K^\perp} \cong n_L \perp q_0|_{K^\perp}$ and Witt cancellation, we conclude that $q_0|_{K^\perp}$ is isotropic By (i), therefore, so is $(q_E)_+$. Moreover, some $w_1 \in L$ makes $h := e_{22} - e_{33} + w_1[23] \in K^\perp$ isotropic relative to q_0, which means $n_L(w_1) = -1$. We now put $u_2 := 1_L$and $u_3 := -\bar{w}_1$, which implies $n_L(u_2)e_{22} + n_L(u_3)e_{33} - \overline{u_2u_3}[23] = h \in K^\perp$, so by (ii), $u_2[31] + u_3[12] \in E_-^\perp$ is isotropic relative to $(q_E)_-$.

(c3) *E is the unique cubic (cyclic) field extension of F.* Again we consider the Springer form $q_E\colon E^\perp \to E$ of E relative to J, which by Exc. 42.26 (d) is a regular binary quadratic form over the field E. Assume first that q_E is isotropic, hence a (split) hyperbolic plane since E is a field. By Exc. 45.16, J contains Kummer elements relative to E, so $J = J(E,\mu)$ arises from E by means of the first Tits construction, for some $\mu \in F^\times$. But now Cor. 45.4 implies that (J, E) admits étale elements. We are left with the case that q_E is anisotropic. For $\mathrm{char}(F) \neq 2$ we note that the restriction of N_J to $E^\perp$ is a cubic form in six variables over the finite field F, hence by the Chevalley-Warning theorem has a non-trivial zero. Accordingly, let $w \in E^\perp \setminus \{0\}$ have $N_J(w) = 0$. Then $N_J(w)^2 - 4N_E(q_E(w)) \neq 0$, and $w \in J$ is étale relative to E. On the other hand, for $\mathrm{char}(F) = 2$, Exc. 45.19 leads us to an element $w \in E^\perp$ having $N_J(w) \neq 0$, and we conclude $N_J(w)^2 - 4N_E(q_E(w)) \neq 0$, so again w is étale relative to E.

(d) $n = 5$. By Racine's theorem 39.6, J_0 is not simple, and by Exc. 40.17, J is the split Freudenthal algebra of dimension 15. Combining Lemma 45.6 with Prop. 45.7, it follows that (J, J_0) admits étale elements.

(e) $n = 9$. Then J is the split Albert algebra over F and there are three cases.

(e1) *J_0 is not simple.* Repeating the argument in (d) shows that (J, J_0) admits étale elements.

(e2) $J_0 \cong \mathrm{Mat}_3(F)^{(+)} \cong \mathrm{Her}_3(F \times F)$. By Exc. 42.23 (a) and 45.18 below, we may assume $(J, J_0) = (J(\mathrm{Mat}_3(F), 1), \mathrm{Mat}_3(F)^{(+)})$. The assertion follows from Cor. 45.4.

(e3) $J_0 \cong \mathrm{Her}_3(K)$. By Exc. 45.18 we may assume that we are in the situation of Exc. 45.17 with $D := K$. Since K is a field, it follows that (J, J_0) admits étale elements. □

For Freudenthal algebras over an LG ring, Thm. 45.10 is useful only if they can be completed to Freudenthal pairs. Here our results are not complete but substantial enough to cover the Albert case.

45.11 Theorem. *Every Albert algebra J over an LG ring k can be completed to an Albert pair: there exists a Freudenthal algebra J_0 of rank 9 such that (J, J_0) is an Albert pair over k.*

Proof We define polynomial laws $e_i \colon J \times J \to J$ for $1 \le i \le 9$ by

$$e_1(x,y) := 1_{J_R}, \quad e_2(x,y) := x, \quad e_3(x,y) := x^\sharp, \quad e_4(x,y) := y,$$
$$e_5(x,y) := y^\sharp, \quad e_6(x,y) := x \times y, \quad e_7(x,y) := x^\sharp \times y,$$
$$e_8(x,y) := x \times y^\sharp, \quad e_9(x,y) := x^\sharp \times y^\sharp$$

for all $x, y \in J_R$, $R \in k$-**alg**. We claim that *it suffices to show*

$$\det\Big((T_J(e_i(x,y), e_j(x,y))_{1\le i,j\le 9}\Big) \in k^\times \tag{1}$$

for some $x, y \in J$. Indeed, once such elements have been exhibited, the quantities $e_i(x,y)$, $1 \le i \le 9$, generate a free submodule J_0 of rank 9 in J on which the bilinear trace of J is regular. Moreover, by Exc. 33.15, J_0 is the subalgebra of J generated by x, y. Summing up, therefore, $J_0 \subseteq J$ is a regular cubic Jordan subalgebra, and it remains to show that J_0 is, in fact, a Freudenthal algebra. By definition (39.8), we may assume that $k = F$ is a field and must show that J_0 is simple. Otherwise, Racine's theorem would imply $J_0 \cong F \times J(M,q,e)$ for some regular pointed quadratic module (M,q,e) over F, in which case the minimal number of generators for J_0 would be 7, a contradiction. Thus J_0 is indeed a Freudenthal algebra.

We therefore need only show that elements $x, y \in J$ satisfying (1) exist. Since k is an LG ring, the k-module $J \times J$ is free of rank 54, so the scalar polynomial law $\det(T_J(e_i, e_j))$ by Cor. 12.12 may be regarded as a polynomial in $k[\mathbf{t}_1, \ldots, \mathbf{t}_{54}]$, which by the LG property represents an element of $k^\times$ if and only if it represents an invertible element in $k/\mathfrak{m}$, for each maximal ideal $\mathfrak{m} \subseteq k$.

We are thus reduced to the case that $k = F$ *is a field*, which we will assume from now on. If J is split, it contains $J_0 := \mathrm{Her}_3(F \times F)$ as a 9-dimensional Freudenthal subalgebra, which by Exc. 45.20 is generated by two elements. In view of Exc. 33.15, therefore, some elements $x, y \in J_0$ satisfy (1). This settles the split case, and we are done if F is algebraically closed or finite. On the

other hand, the former alternative combines with a Zariski density argument to settle the case of an infinite base field as well. □

45.12 Corollary. *If k is (1) a field or (2) a residually big LG ring, then every Albert algebra over k can be realized by the second Tits construction.*

Proof Let J be an Albert algebra over k. By Thm. 45.11, J can be completed to an Albert pair (J, J_0) over k. If k is a residually big LG ring, then Thm. 45.10 shows that (J, J_0) admits étale elements, and hence J can be realized by the second Tits construction. On the other hand, if k is a field, then what we have just proved allows us to assume $k = \mathbb{F}_2$ or $k = \mathbb{F}_4$. Then J is split, hence isomorphic to the first Tits construction $J(\mathrm{Mat}_3(F), 1)$ (Exc. 42.23), hence also a second Tits construction. □

45.13 Remark. For a field F of characteristic $\neq 2, 3$, Parimala, Sridharan, and Thakur have constructed in [207] examples of Albert algebras over $k := F[\mathbf{t}_1, \mathbf{t}_2]$ that do not arise from the second Tits construction, so some hypothesis on k is necessary in Cor. 45.12. Note that such a k is not LG by Exc. 11.42.

45.14 A comparison. There are important analogies connecting Thm. 45.10 with the enumeration theorem of Petersson-Racine for algebras arising from what they call the *Tits process* [225, Thm. 3.1]. In order to work out the details of these analogies, we make the following observations.

(a) The Tits process is more general than (our version of) the second Tits construction as it is addressed to involutorial systems whose core, though quadratic, need not be étale. Also, it works over arbitrary base fields whereas our approach is restricted to those obeying the constraints of residual bigness; that these constraints are a necessary methodological ingredient of our approach follows from Thm. 45.10. On the other hand, the Tits process is less general than the second Tits construction as it allows only involutorial systems whose underlying alternative algebras are associative and hence are equipped with ordinary involutions rather than isotopy ones.

(b) While [225, Thm. 3.1] is confined to arbitrary base fields, Thm. 45.10 works more generally for arbitrary LG rings. Ignoring this distinction for simplicity, we assume from now on that $k = F$ is an arbitrary field.

(c) Thm. 45.10 spells out conditions that are necessary and sufficient for any Freudenthal pair (J, J_0) over F to admit étale elements. The existence of such elements, in turn, is sufficient (but not necessary) for J to be realizable by means of the second Tits construction starting from J_0. Note that these results are confined to cubic Jordan algebras J, J_0 that, in particular, are required to be

regular. By contrast, [225, Thm. 3.1] says, among other things, that *any* simple Jordan F-algebra of degree 3, regular or not, can be obtained by a successive application of the Tits process either from the base field itself or from a cubic étale subalgebra (provided there is any), depending on whether the characteristic is not or is equal to 3.

(d) Both proofs are based on careful case-by case analyses, but the one of [225, Thm. 3.1] doesn't seem to stand a chance of being extended to LG rings.

Exercises

45.15. Let F be a field and E a cubic étale F-algebra. Show:

(a) If F contains more than two elements, then E as a unital F-algebra is generated by a single element.

(b) If F contains precisely two elements, then the conclusion of (a) fails if and only if E is split.

(c) If F contains more than two elements and $\operatorname{char}(F) \neq 3$, then $(J, J_0) := (E^{(+)}, F \cdot 1_E)$ is a Freudenthal pair over F such that $J_0^\perp = \operatorname{Ker}(T_J)$.

(d) If F contains more than two elements and $\operatorname{char}(F) \neq 3$, then, with (J, J_0) as above:
(i) $a \in J$ is an étale element relative to J_0 if and only if a has trace zero, generates E as a unital F-algebra and satisfies $S_J(a) \neq 0$.
(ii) Either (J, J_0) admits étale elements or E is split cubic étale over $F = \mathbb{F}_4$ and $J \cong J(F, 1)$ arises from F and 1 by means of the first Tits construction.

45.16 (Petersson-Thakur [232, 2.8])**.** Let (J, J_0) be a Freudenthal pair over a field F, assume $J_0 = E^{(+)}$ for some cubic étale F-algebra E and write $q_E\colon E^\perp \to E$ for the Springer form of E in the sense of Exc. 42.26. Show that if the binary quadratic space $(E^\perp, q_E)$ over E is split hyperbolic, then (J, J_0) admits Kummer elements. (*Hint*: Argue indirectly and use Exc. 42.26 (e).)

45.17. Let k be a commutative ring, D a quadratic étale k-algebra, (M, h) a ternary hermitian space over D and $\Delta\colon \bigwedge^3(M) \xrightarrow{\sim} D$ an orientation satisfying $\det_\Delta(h) = 1$. Write $C := \operatorname{Ter}(D; M, h, \Delta)$ for the octonion algebra over k arising from the preceding data by means of the ternary hermitian construction of 21.13 and let $\Gamma = \operatorname{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathrm{GL}_3(k)$. Identify $D \subseteq C$, $M \subseteq C$ canonically and prove:

(a) (J, J_0) with $J := \operatorname{Her}_3(C, \Gamma)$ and $J_0 := \operatorname{Her}_3(D, \Gamma)$ is an Albert pair over k satisfying $J_0^\perp = \sum M[jl]$.

(b) For $w = \sum w_i[jl] \in J_0^\perp$, $w_i \in M$, $1 \leq i \leq 3$ we have

$$N_J(w) = -\gamma_1\gamma_2\gamma_3 t_D(\Delta(w_1 \wedge w_2 \wedge w_3)), \tag{1}$$

$$N_{J_0}(Q(w)) = (\gamma_1\gamma_2\gamma_3)^2 n_D(\Delta(w_1 \wedge w_2 \wedge w_3)) \tag{2}$$

with Q as in 44.8.

(c) Defining

$$\delta\colon J_0^\perp \longrightarrow D, \quad \sum v_i[jl] \longmapsto \gamma_1\gamma_2\gamma_3\Delta(v_1 \wedge v_2 \wedge v_3),$$

and letting $w = \sum w_i[jl] \in J_0^\perp$, $w_i \in M$, the following conditions are equivalent.

(i) w is an étale element of J relative to J_0.

(ii) $\delta(w) \in D$ is invertible and $D = k[\delta(w)]$.

(d) Conclude that (J, J_0) admits étale elements if and only if M is a free D-module and $D = k[a]$, for some invertible element $a \in D$.

45.18. Let J, J_0 be reduced simple Freudenthal algebras over a field F and suppose J_0 is a subalgebra of J. Writing C (resp. C_0) for the co-ordinate algebra of J (resp. J_0), show that C_0 up to isomorphism is a unital subalgebra of C and, no matter how this isomorphism has been chosen, there exists an invertible diagonal matrix $\Gamma \in \mathrm{GL}_3(F)$ satisfying

$$(J, J_0) \cong (\mathrm{Her}_3(C, \Gamma), \mathrm{Her}_3(C_0, \Gamma)). \tag{1}$$

45.19. Let (J, J_0) be a Freudenthal pair of dimension 9 over a field F. Prove that there exists an element $u \in J_0^\perp$ such that $N_J(u) \neq 0$. (*Hint*: Apply Exc. 12.40.)

45.20. Let J be a Freudenthal algebra of rank 9 over an LG ring k. Show that J is generated by two elements.

45.21. Let J be a Freudenthal algebra of rank 9 over an LG ring k. Show that J can be completed to a Freudenthal pair over k.

45.22. Let A be a regular cubic alternative k-algebra of constant rank and $\mu \in k^\times$. Show that $(J(A, \mu), A^{(+)})$ is a Freudenthal pair over k.

46 Cubic Jordan division algebras

This section is devoted to studying cubic Jordan algebras that are division algebras, i.e., in which every non-zero element is invertible. For such an algebra, the centroid is a field (Cor. 28.19), so without loss of generality we only consider the case of a base field F.

Apart from the trivial example $F^{(+)}$ and, when $\mathrm{char}(F) = 3$, $E^{(+)}$ for E a purely inseparable field extension of F of exponent at most 1, we find that every cubic Jordan division algebra is a regular Freudenthal algebra and such division algebras must have dimension 1, 3, 9, or 27 (Thm. 46.8).

While division algebras of the first three dimensions are relatively easy to exhibit, the problem of proving the existence of a cubic Jordan division algebra of dimension 27 — an Albert division algebra — was historically very challenging. Indeed, it took 25 years from the first appearance of Albert algebras in [3] to the first example of a division algebra in [8], and during the intervening years there was an erroneous claim of non-existence [253, Thm. 1]. We obtain examples here (see Example 46.14) using one of the Tits constructions,

as an application of general criteria for when those constructions produce division algebras. Finally, we classify Albert algebras over some special fields, showing in particular that all Albert algebras over a global field are reduced

46.1 Proposition. *For a cubic Jordan algebra J over F, the following conditions are equivalent.*

(i) *J is a Jordan division algebra.*
(ii) *The norm of J is anisotropic: for all $x \in J$, $N_J(x) = 0$ implies $x = 0$.*
(iii) *For all $x \in J$, $x^\sharp = 0$ implies $x = 0$.*

Proof This is an easy exercise, the relevant arguments being contained in the proof of 39.17. □

46.2 Corollary. *If a cubic Jordan algebra over F is a division algebra, then so is any cubic Jordan subalgebra.* □

46.3 Corollary. *Let J be a cubic Jordan division F-algebra and K a quadratic field extension of F. Then the base change J_K is a cubic Jordan division algebra over K.*

Proof By Prop. 46.1, the norm of J is anisotropic, hence by Exc. 12.41 so is its base change from F to K. By Prop. 46.1 again, J_K is a cubic Jordan division algebra over K. □

46.4 Remark. There are more profound results along these lines pertaining to associative, octonion and Albert division algebras. For example, if D is a finite-dimensional central associative division F-algebra of degree n and $K \supseteq F$ is a finite algebraic extension of degree prime to n, then D_K continues to be an associative division algebra [102, Cor. 4.5.11(2)]. Also, it follows from Springer's theorem for quadratic forms [72, Cor. 18.5] that an octonion division algebra over F stays division under odd degree field extensions. And, finally, using methods from Galois cohomology, it follows that an Albert division algebra over F (see 46.14 below for an example) stays division under all field extensions of degree not divisible by 3 [220, Cor. 50].

46.5 Lemma. *If J is a finite-dimensional cubic Jordan division algebra over F, then either (1) J is regular or (2) F has characteristic 3 and $J \cong E^{(+)}$ for some purely inseparable field extension E of F with exponent at most 1.*

Proof If $\mathrm{char}(F) \neq 3$, Euler's differential equation (33a.11) implies $T_J(x, x^\sharp) = 3N_J(x) \neq 0$ for all $x \neq 0$ in J. Hence J is regular. For $\mathrm{char}(F) = 3$, we first assume that the bilinear trace of J is not zero. Since $T_J(U_x y, z) = T_J(y, U_x z)$ for all $x, y, z \in J$ by (33a.31), $\mathrm{Rad}(T_J) \subset J$ is an outer ideal (Exc. 29.18 (a)) and

hence an ideal since the characteristic is not 2 (28.6). But J is a simple algebra by 28.11, and we conclude $\mathrm{Rad}(T_J) = \{0\}$. Thus J is regular. We are left with the case $T_J = 0$. By (33a.6) and the property of J being a division algebra, the set map $N_J\colon J \to F^{(+)}$ is an injective homomorphism of Jordan $\mathbb{Z}$-algebras. In particular, $N_J(J) \subseteq F^{(+)}$ is a Jordan division subring which, thanks to the formula

$$N_J(x)N_J(y) = N_J(N_J(x)N_J(y)U_{x^{-1}}y^{-2})$$

for all $x, y \in J^\times$, is closed under the multiplication of F and thus is a subfield of F. It follows that the F-vector space J carries the unique structure of a field extension E of F making $N_J\colon E \to F$ a field homomorphism. Since $N_J\colon J \to F^{(+)}$ and $N_J\colon E^{(+)} \to F^{(+)}$ are both monomorphisms of Jordan $\mathbb{Z}$-algebras, we obtain $J = E^{(+)}$. Identifying $F \subseteq E$ canonically, we have $x^3 = N_J(x) \in F$ for all $x \in E$ by (33.9.2), so the field extension E of F is purely inseparable of exponent at most 1. □

46.6 Proposition. *Let J be a cubic Jordan division algebra over F.*

(a) J is strictly locally linear in the sense of 30.8 and Exc. 30.13.

(b) For all $x \in J \setminus F1_J$,

(1) $E := F[x] \subseteq J$ is a cubic subfield of J.

(2) $m_{J,x} = \mathbf{t}^3 - T_J(x)\mathbf{t}^2 + S_J(x)\mathbf{t} - N_J(x) \in F[\mathbf{t}]$ is the minimum polynomial of x with respect to E.

(3) The trace of E/F is the linear trace of J restricted to E: $T_{E/F} = T_J|_E$.

(4) E/F is separable if and only if T_J does not vanish identically on E.

(5) The base change J_E over E is no longer a division algebra.

Proof (a) For any field extension K/F we must show that J_K over K is locally linear. This is clear if $J \cong E^{(+)}$, for some purely inseparable field extension E/F of characteristic 3 and exponent at most 1. By Lemma 46.5, we may therefore assume that J is regular over F. Then so is J_K over K, hence satisfies $\mathrm{Nil}(J_K) = \{0\}$ (Exc. 34.23) and thus has no absolute zero divisors (Exc. 37.27 (e)). The assertion now follows from Thm. 30.11.

(b)(1) From (a) we deduce that E carries the unique structure of a unital commutative associative F-algebra making $E^{(+)} \subseteq J$ a cubic Jordan subalgebra., while Cor. 33.10 implies that E is in fact a field. Consulting (33.9.2), we conclude $2 \leq [E : F] \leq 3$. Assume $[E : F] = 2$. Then $E^{(+)}$ satisfies the Dickson condition of Exc. 30.13, so there exists a pointed quadratic module (M, q, e) over F having $E^{(+)} = J(M, q, e)$. But (34.27.4) implies that the norm of J is isotropic on E, in contradiction to J being a division algebra. Thus E is indeed a cubic field extension of F.

(b)(2) By (33.9.2), the polynomial $m_{J,x}$ kills x, hence is divisible by the minimum polynomial of x over E. But that polynomial by (b)(1) has degree 3, so both polynomials must be equal.

(b)(3) For $y \in E$ we must show $T_{E/F}(y) = T_J(y)$. This is clear for $y \in F1_J$, while otherwise $E = F[y]$ by (b)(1), and the assertion follows from (b)(2).

(b)(4) Being a field extension of prime degree, E/F is either separable or purely inseparable. Hence the former case is equivalent to $T_{E/F} \neq 0$, and the assertion follows from (b)(3).

(b)(5) J_E contains $E_E = E \otimes E$ as a unital commutative associative subalgebra. But this subalgebra has zero divisors, hence is not a field. By (b)(1), therefore, J cannot be a cubic Jordan division algebra. □

46.7 Corollary. *A regular cubic Jordan division algebra J of dimension > 1 over F contains a separable cubic subfield.*

Proof Note that $\mathrm{Ker}(T_J)$ is neither 0 (by dimension count) nor J (because J is regular). If $\mathrm{char}(F) \neq 3$, pick any non-zero $u \in \mathrm{Ker}(T_J)$ and put $x := 1_J + u$. If $\mathrm{char}(F) = 3$, pick any $x \in J \setminus \mathrm{Ker}(T_J)$. Then apply Prop. 46.6, (b)(1) and (b)(4). □

46.8 Theorem. *Let J be a finite-dimensional cubic Jordan division algebra over F that is not of the form described in Lemma 46.5(2). Then J is regular, is a Freudenthal algebra, and has dimension 1, 3, 9, or 27.*

Proof Lemma 46.5 gives that J is regular. If $\dim J = 1$, then $J = F^{(+)}$ and J is Freudenthal. So assume $\dim J > 1$. By Cor. 46.7, J has dimension at least 3, and if the dimension is equal to 3, then J is a separable cubic field extension, hence a Freudenthal algebra. On the other hand, suppose J has dimension > 3 and write F_s for the separable closure of F. Since J contains separable cubic subfields (Cor. 46.7), and the base change to separable cubic subfields destroys the property of being a division algebra (Prop. 46.6(b)(5)), $J_s := J_{F_s}$ is no longer a cubic Jordan division algebra. But J_s is still regular, hence semi-simple, and thus satisfies one of the conditions (ii), (iii) of Thm. 39.6. If (ii) holds, then up to isomorphism $J_s = F^{(+)} \times J(M, q, e)$ for some non-degenerate pointed quadratic module (M, q, e) over F_s. The elementary idempotents of J_s have the form $e_1 := (1, 0)$ and $c := (0, c')$ for some elementary idempotent $c' \in J' := J(M, q, e)$. From Prop. 32.8 we deduce $J_1(c') \neq \{0\}$ since $\dim_{F_s}(J') \geq 3$, so e_1 is the only elementary idempotent of J_s having $J_{s1}(e_1) = \{0\}$. Therefore the absolute Galois group of F, acting on J_s by semi-linear automorphisms through the second factor, fixes e_1, and we arrive at the contradiction $e_1 \in J$. Hence J_s satisfies condition (iii) of Thm. 39.6

and, being regular, is a Freudenthal algebra over F_s. But then so is J over F, by Cor. 39.32.

By Cor. 39.11, the proof will be complete once we have excluded dimensions 6 and 15 for J. Arguing indirectly, let us assume that J has dimension 6 or 15. Since J is regular, we may apply Cor. 46.7 and pick an element $x \in J$ making $E := F[x] \subseteq J$ a separable cubic subfield. We have the decomposition $J = E \oplus E^\perp$ as a direct sum of vector spaces over F, orthogonal complementation being taken with respect to the bilinear trace of J.

Assume first $\dim_F(J) = 6$. By Exc. 42.26 (a),(b), we may regard $E^\perp$ canonically as a one-dimensional vector space over E carrying the Springer form $q_E\colon E^\perp \to E$ as a quadratic form over E. Moreover, the formalism of 35.6 provides us with an F-quadratic map $H_E\colon E^\perp \to E^\perp$ such that $v^\sharp = -q_E(v)+H_E(v)$ for all $v \in E^\perp$. Let u be a basis of $E^\perp$ as a vector space over E, put $s := q_E(u) \in E$ and define $t \in E$ by $H_E(u) = t\,.\,u$. Then (35.8.1) implies $N_J(u)1_E = q_E(u, H_E(u)) = 2st$, whence $\mathrm{char}(F) \neq 2$, $\theta := N_J(u) \in F^\times$ and $st = \frac{\theta}{2}1_E$. In particular $t \in E^\times$. Now pass to the isotope $J^{(p)}$ of J, $p := t^{-1}$, which contains $E^{(p)} := E^{(+)(p)}$ as a separable cubic subfield and satisfies $E^{(p)\perp} = E^\perp$ as vector spaces over F. From (35.11.1) we deduce $H_E^{(p)}(u) = t^{-1}\,.\,(t\,.\,u) = u$. Thus we may assume $t = 1_E$ and obtain $s = \frac{\theta}{2}1_E$. Applying (35.9.6), we conclude $u = H(H(u)) = \theta u - \frac{\theta}{2}u = \frac{\theta}{2}u$, hence $\theta = 2$ and thus $s = 1_E$. Setting $x := 1_E - u \in J^\times$ and applying (35.8.2) now yields $x^\sharp = 0$, a contradiction.

Next assume $\dim_F(J) = 15$. For $y \in E^\perp$, $y \neq 0$, write J_0 for the cubic Jordan subalgebra of J generated by x and y. By Cor. 46.2, J_0 is a cubic Jordan division algebra. It contains E as a separable cubic subfield, so it cannot be a purely inseparable field extension of F and hence, by Prop. 46.5, is regular, hence Freudenthal, giving rise to a decomposition $J = J_0 \oplus J_0^\perp$ as a direct sum of subspaces. Also, by construction and Exc. 33.15, $4 \leq \dim_F(J_0) \leq 9$. Since we have just excluded dimension 6, Cor. 39.11 implies $\dim_F(J_0) = 9$. Now let $0 \neq u \in J_0^\perp$. Using the notation of (35.1.2), the linear map $x_0 \mapsto x_0\,.\,u = -x_0 \times u$ from J_0 to $J_0^\perp$ by (35.4.4) satisfies $x_0^{-1}\,.\,(x_0\,.\,u) = u$ for $x_0 \in J_0^\times$ and hence is injective, a contradiction to $J_0^\perp$ having dimension 6. □

46.9 Remark. The standard proof for the preceding theorem, whose critical part consists in excluding the numbers 6 and 15 as dimensions of cubic Jordan division algebras, relies on properties of associative algebras with involution. By structure theory of finite-dimensional simple Jordan algebras [191, 15.6] or Exc. 55.13, a Freudenthal algebra of dimension 6 (resp., 15) has the form $H(A, \tau)$, where A is a central simple associative algebra of degree 3 (resp., 6) and τ is an orthogonal (resp., symplectic) involution of the first kind on A. But

A cannot be a division algebra, hence neither can J, since for A to be a division algebra it is necessary that its degree be a power of 2 [160, Thm. 3.1(1)].

We now turn to the question of when the first or second Tits construction leads to cubic Jordan division algebras. The key result in this context reads as follows.

46.10 Theorem (cf. Petersson-Racine [226, Thm. 5.2])**.** *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system over F and $\mu \in K$ an admissible scalar for $\mathcal{B}$. Then $J(\mathcal{B}, \mu)$ is a cubic Jordan division algebra over F if and only if the following conditions are fulfilled.*

(i) $H(\mathcal{B})$ *is a cubic Jordan division algebra.*
(ii) μ *is not a norm of B: $\mu \notin N_B(B^\times)$.*

In this case,

$$\mu - \bar{\mu} \in K^\times. \tag{1}$$

Proof Suppose first $J := J(\mathcal{B}, \mu)$ is a division algebra. Then so is $J_0 := H(\mathcal{B})$ (Cor. 46.2)., and (i) holds. Assuming (ii) fails, we conclude $\mu = N_B(u)$ for some $u \in B^\times$. From (43.5.2) we deduce $(\tau(u)p^{-1})u \in J_0$, hence $x := (\tau(u)p^{-1})u + u^{-1}j \in J^\times$, and (44.15.4) yields

$$\begin{aligned} N_J(x) &= N_{J_0}\Big((\tau(u)p^{-1})u\Big) + \mu N_J(u)^{-1} \\ &\quad + \overline{\mu N_J(u)^{-1}} - T_{J_0}\Big((\tau(u)p^{-1})u, u^{-1}(p\tau(u^{-1}))\Big) \\ &= 1 + 1 + 1 - 3 = 0, \end{aligned}$$

a contradiction. Thus (ii) holds.

Conversely suppose conditions (i), (ii) hold. Assume $x = x_0 + uj \in J$, $x_0 \in J_0$, $u \in B$ satisfies $x^\sharp = 0$, i.e., by (44.15.3),

$$x_0^\sharp = u(p\tau(u)), \quad \bar{\mu}\tau(u^\sharp)p^{-1} = x_0 u. \tag{2}$$

By Prop. 46.1, we must show $x_0 = u = 0$. Taking adjoints in (2) and combining admissibility of μ with (42.1.2), we conclude

$$N_{J_0}(x_0)x_0 = x_0^{\sharp\sharp} = (\tau(u^\sharp)p^\sharp)u^\sharp = \mu\bar{\mu}(\tau(u^\sharp)p^{-1})u^\sharp = \mu(x_0 u)u^\sharp = \mu N_B(u)x_0.$$

If x_0 were different from zero, hence invertible by (i), we would have $N_B(x_0) = \mu N_B(u)$, forcing $u \in B^\times$ and $\mu = N_B(x_0 u^{-1})$, contradicting (ii). Hence $x_0 = 0$, and (2) combined with the adjoint identity implies

$$u(p\tau(u)) = u^\sharp = 0, \quad N_B(u) = 0. \tag{3}$$

Next we claim that (1) holds. If $\mu \in F1_K$, then $\mu = \bar{\mu}$, hence $N_B(p) = \mu^2$, and

we arrive at the contradiction $\mu = N_B(\mu p^{-1})$. Thus $\mu \notin F1_K$ generates K as a unital F-algebra, and (1) follows from Exc. 19.32 (a).

Now consider any $v \in B$. Then (3) implies $(uv)^\sharp = v^\sharp u^\sharp = 0$, $N_B(uv) = N_B(u)N_B(v) = 0$, so $w := uv \in B$ satisfies $w + \tau(w) \in J_0$ as well as

$$N_{J_0}(w + \tau(w)) = N_B(w) + T_B(w^\sharp, \tau(w)) + T_B(w, \tau(w^\sharp)) + \overline{N_B(w)} = 0.$$

By (i) we therefore have $\tau(w) = -w$. In the special case $v = 1_B$, this gives $\tau(u) = -u$ and then

$$uv = -\tau(uv) = -(\tau(v)p^{-1})(p\tau(u)) = (\tau(v)p^{-1})(pu).$$

For $v = \mu 1_B$, this amounts to $\mu u = \bar{\mu} u$, i.e., $(\mu - \bar{\mu})u = 0$, and (1) yields $u = 0$. □

46.11 Corollary. *Let $\mathcal{B}$ be an involutorial system of the first kind and μ an admissible scalar for $\mathcal{B}$. Then $J(\mathcal{B}, \mu)$ is not a cubic Jordan division algebra.*

Proof (46.10.1) does not hold since $\mathrm{Core}(\mathcal{B}) = F$. □

46.12 Corollary. *Let A be a cubic alternative F-algebra and $\lambda \in F^\times$. The first Tits construction $J(A, \lambda)$ is a cubic Jordan division algebra if and only if A is a cubic associative division algebra and λ is not a norm of A: $\lambda \notin N_A(A^\times)$.*

Proof Regarding $(A, 1_A)$ as a pointed alternative algebra over F, we apply Thm. 44.19 with $q := 1_A$ and obtain an isomorphism $J(A, \lambda) \cong J(\mathcal{B}, \mu)$, where

$$\mathcal{B} = (F \times F, A \times A^{\mathrm{op}}, \varepsilon_A, (1_A, 1_A)), \quad N_B = N_A \times N_A, \quad \mu = (\lambda, \lambda^{-1}).$$

We now explore what conditions (i), (ii) of Thm. 46.10 mean for A and λ.

(i) Since ε_A by Exc. 44.31 is the switch, $H(\mathcal{B}) \cong A^{(+)}$, so $H(\mathcal{B})$ is a cubic Jordan division algebra if and only if A is a cubic alternative division algebra. But cubic alternative division algebras do not exist unless they are associative, so (i) is equivalent to A being a cubic associative division algebra.

(ii) $B^\times = A^\times \times A^{\mathrm{op}\times}$ and, obviously, (ii) holds if and only if $\lambda \notin N_A(A^\times)$. □

46.13 Corollary. *Let A be a cubic associative F-algebra that is division. For $K = F(\mathbf{t})$ or $F((\mathbf{t}))$, the first Tits construction $J(A_K, \mathbf{t})$ is a division algebra.*

Proof Since A is a division algebra, so is A_K by Exc. 9.25. The field K is the fraction field of $R := F[\mathbf{t}]$ or $F[[\mathbf{t}]]$, so every element of A_K can be written as a/y for some $a \in A_R$ and nonzero $y \in R$. We find that $N_{A_K}(a/y) = N_{A_R}(a)/y^3$, so by Exc. 12.38(a) the norm $N_{A_K}(a/y)$ has degree (in $\mathbf{t}$) divisible by 3. In particular, it is not equal to $\mathbf{t}$, so $J(A_K, \mathbf{t})$ is a division algebra by Cor. 46.12. □

46.14 Examples of Freudenthal division algebras. Let us construct Freudenthal division algebras of all dimensions allowed by Thm. 46.8, as promised in the introduction. Dimension 1 is trivial, take $F^{(+)}$.

For dimension 3, let F be a field that has a separable cubic field extension E, and take $E^{(+)}$. For example, one can take F to be any finite field. Or $F = \mathbb{Q}$ and $E = \mathbb{Q}[\mathbf{t}]/(\mathbf{t}^3 - p)$ for p a prime.

If we take one of the examples $E^{(+)}$ of dimension 3 from the preceding paragraph, then the first Tits construction $J(E_{F(\mathbf{t})}, \mathbf{t})$ is a division algebra of dimension 9 over $F(\mathbf{t})$ by Cor. 46.13. Alternatively, take F to be a field that has a (cyclic) associative division algebra D of degree 3 as in [255, Thm. VIII.12.1 and Lemma VIII.12.6], in which case $D^{(+)}$ is a cubic Jordan division algebra of dimension 9. (Every global field F has such a D, thanks to the Albert-Brauer-Hasse-Noether Theorem.)

Finally, for dimension 27, take a D and F as in the alternative construction of dimension 9 algebras in the preceding paragraph. Then $J(D_{F(\mathbf{t})}, \mathbf{t})$ is a division algebra over $F(\mathbf{t})$ by Cor. 46.13. In particular, taking $F = \mathbb{Q}$, we obtain an Albert division algebra over $\mathbb{Q}(\mathbf{t})$.

46.15 Albert algebras over special fields. Let J be an Albert algebra over F. In what follows we specialize F to one of those fields that had already been under consideration in connection with composition algebras.

(a) *Separably closed fields.* If F is separably closed, it does not admit any separable cubic field extensions, so J cannot be a division algebra (Cor. 46.7) and hence is reduced (Prop. 39.17), with co-ordinate algebra an octonion F-algebra C. But C is split by 23.12 and, therefore, J is split.

(b) *The real field.* By Cor. 40.8, there are precisely three non-isomorphic Albert algebras over $F := \mathbb{R}$: (i) $\mathrm{Her}_3(\mathrm{Zor}(\mathbb{R}))$, the split one, (ii) $\mathrm{Her}_3(\mathbb{O})$, the euclidean one, (iii) $\mathrm{Her}_3(\mathbb{O}, \mathrm{diag}(-1, 1, 1))$, the non-split one containing non-zero nilpotents.

(c) *Finite fields.* By Exc. 40.17, Albert algebras over a finite field, more generally, over any finite commutative ring, are split.

(d) *Local fields.* Let F be a local field in the sense of 23.15. Since the norm of an Albert algebra J over F is a cubic form in at least 10 variables, it is isotropic [235, Thm. 2], and therefore J is reduced. (This can alternatively be seen using Prop. 1.2 and Kor. 2 of Satz 6.5 in [211].) The coefficient algebra C is an octonion algebra and so itself is split by 23.15, hence *all Albert algebras over F are split.*

The fact we have just used about cubic forms in 10 variables also shows that

the reduced norm of any central simple associative algebra of degree 3 over F is surjective. In fact, this result holds in any degree.

(e) *C_2 fields.* A field F is said to be C_i if every homogeneous polynomial of degree d with coefficients in F in at least d^i+1 variables is isotropic. Trivially, a C_i field is also C_j for all $j > i$. Certainly, every algebraically closed field is a C_0 field. Every finite field is a C_1 field, by the Chevalley-Warning theorem. If F is an algebraic extension of a C_i field K, then F is also C_i; if F has transcendence degree d over such a K, then F is C_{i+d} [255, Thm. 2.15.2]. For more on this subject, see [102, §6.2], [104], [255, §2.15], or [262, §II.4.5].

The class of C_2 fields, therefore, includes fields of transcendence degree ≤ 1 over a finite field (e.g., global fields of prime characteristic), or of transcendence degree ≤ 2 over an algebraically closed field. If F is a C_2 field, then:

(i) *The norm of a central simple associative F-algebra A is surjective*, see Exc. 46.22.

(ii) *Every octonion F-algebra is split*. Since the norm of such an algebra is a quadratic form in more than 4 variables, it is isotropic, so the algebra is split by Cor. 22.18.

(iii) *Every Albert F-algebra is split*. To see this, note that such an algebra is reduced, because its norm is a cubic form in more than 9 variables, i.e., the algebra is $\mathrm{Her}_3(C,\Gamma)$ for some octonion algebra C. Since C is split by (ii), so is the Albert algebra.

(f) *Global fields.* Let F be a global field in the sense of 23.16. We wish to show that Albert algebras over F are reduced. To this end, we require the following result from algebraic number theory.

46.16 Proposition. *If A is a finite-dimensional central simple associative F-algebra of degree 3, for F a global field, then the set map $\mathrm{Nrd}_A\colon A \to F$ is surjective.*

Proof If F has characteristic different from zero, then it is a C_2 field and the claim is a special case of 46.15(e)(i).

So assume F has characteristic zero. Since A has degree 3, A_v is split for every real place v of F and in particular $\mathrm{Nrd}_{A_v}\colon A_v \to F_v$ is surjective. The Hasse-Schilling Theorem [256] implies that $\mathrm{Nrd}_A\colon A \to F$ is surjective. □

46.17 Corollary. *Albert algebras over global fields are reduced.*

Proof Let F be a global field and assume J is an Albert division algebra over F. Following Cor. 45.12, we may write $J = J(\mathcal{B},\mu)$ for some involutorial system $\mathcal{B}$ over F and some admissible scalar μ for $\mathcal{B}$. Applying Cor. 46.11 we deduce that $\mathcal{B}$ is of the second kind, so $K := \mathrm{Core}(\mathcal{B})$ is a quadratic étale

F-algebra. Changing scalars from F to K if necessary, we may assume that $K = F \times F$ is split, making J by Cor. 44.21 a first Tits construction: $J \cong J(A, \lambda)$ for some central simple associative F-algebra A of degree 3 and some $\lambda \in F^\times$. But $J(A, \lambda)$ continues to be a division algebra (Cor. 46.3), so A is a division algebra and $\lambda \notin N_A(A^\times)$ by Cor. 46.12, contradicting Prop. 46.16. □

46.18 Example (isotopy over global fields)**.** For $K = \mathbb{R}$ or a global field, there is a bijection between the isomorphism classes of octonion algebras and isotopy classes of Albert algebras given by $C \leftrightarrow \mathrm{Her}_3(C)$. Indeed, every Albert K-algebra is reduced by 46.15 (b) and Cor. 46.17, so $C \mapsto \mathrm{Her}_3(C)$ touches every isotopy class. Injectivity of this map follows from the Jacobson-Faulkner theorem 41.8.

46.19 Corollary. *If F is a global field with no real places, then all Albert F-algebras are split.*

Proof Let J be an Albert algebra over F. Then J is reduced by Cor. 46.17, with an octonion F-algebra C as coefficient algebra. From Cor. 23.21 we deduce that C is split. Hence so is J. □

Note that in Cor. 46.19 the hypothesis on F holds automatically if $\mathrm{char}(F) > 0$. What is missing, therefore, is a precise description of (reduced) Albert algebras over algebraic number fields that are not purely imaginary. With the notation of 23.16, such a desription will be provided by the following result.

46.20 Theorem (Albert-Jacobson [11, Thm. 12])**.** *Let F be an algebraic number field, write S for the finite set of real places of F and consider the quaternion algebra $B := \mathrm{Cay}(F, -1, -1)$ over F.*

(a) Every Albert algebra over F is isomorphic to

$$\mathrm{Her}_3(\mathrm{Cay}(B, \mu), \mathrm{diag}(\gamma, 1, 1)),$$

for some $\mu, \gamma \in F^\times$.

(b) For $\mu, \mu', \gamma, \gamma' \in F^\times$, the Albert F-algebras

$$\mathrm{Her}_3(\mathrm{Cay}(B, \mu), \mathrm{diag}(\gamma, 1, 1)) \quad \textit{and} \quad \mathrm{Her}_3(\mathrm{Cay}(B, \mu'), \mathrm{diag}(\gamma', 1, 1))$$

are isomorphic if and only if, for all $v \in S$,

(i) $\lambda_v(\mu\mu') > 0$.

(ii) *If $\lambda_v(\mu) < 0$, then $\lambda_v(\gamma\gamma') > 0$.*

Proof We perform the following steps.

1°. Since Albert algebras J over F are reduced (Cor. 46.17) and hence (in

view of Thm. 41.21) are classified by the quadratic form invariants Q_J of (41.5.1), the Hasse-Minkowski theorem 23.17 implies that two Albert algebras J, J' over F are isomorphic if and only if J_v and J'_v are isomorphic over F_v, for all $v \in \Omega$. But since Albert algebras over F_v are split unless v is real (46.15 (a),(d)), we actually have

$$J \cong J' \iff \forall v \in S : \ J_v \cong J'_v. \tag{1}$$

2°. Let J be one of the three Albert algebras over $\mathbb{R}$ (46.15 (b)), written as $J = \mathrm{Her}_3(C, \Gamma)$, with C being one of the two real octonion algebras and $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, 1)$, $\gamma_1, \gamma_2 \in \mathbb{R}^\times$. We have

$$\begin{aligned} J \text{ is split} &\iff C = \mathrm{Zor}(\mathbb{R}) \text{ is split.} \\ J \text{ is euclidean} &\iff C = \mathbb{O},\ \gamma_1 > 0,\ \gamma_2 > 0. \\ J \text{ is neither split nor euclidean} &\iff C = \mathbb{O} \text{ and } (\gamma_1 < 0 \text{ or } \gamma_2 < 0). \end{aligned}$$

3°. We can now prove (a). Let J be an Albert algebra over F. Since J is reduced, it has the form $J = \mathrm{Her}_3(C, \Gamma)$, C an octonion algebra over F and $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, 1) \in \mathrm{GL}_3(F)$. By Thm. 23.22, we may assume $C = \mathrm{Cay}(B, \mu)$ for some $\mu \in F^\times$. Given $v \in S$, either C_v is split or $C_v \cong \mathbb{O}$ according as $\lambda_v(\mu) > 0$ or $\lambda_v(\mu) < 0$. We now define a real number γ_v by

$$\gamma_v := \begin{cases} 1 & \text{if } \lambda_v(\mu) > 0 \text{ or } (\lambda_v(\mu) < 0 \text{ and } \lambda_v(\gamma_1) > 0, \lambda_v(\gamma_2) > 0), \\ -1 & \text{if } \lambda_v(\mu) < 0 \text{ and } (\lambda_v(\gamma_1) < 0 \text{ or } \lambda_v(\gamma_2) < 0). \end{cases}$$

Applying the weak approximation theorem [204, 11:8] leads to an element $\gamma \in F$ having $|\lambda_v(\gamma) - \gamma_v| < 1$ for all $v \in S$. Then $\lambda_v(\gamma), \gamma_v \in \mathbb{R}$ have the same sign, and setting $J' := \mathrm{Her}_3(C, \Gamma')$, $\Gamma' := \mathrm{diag}(\gamma, 1, 1)$, we deduce from 2° that $J_v \cong J'_v$ for all $v \in S$, which implies $J \cong J'$ by 1°.

Turning to (b), we put $C := \mathrm{Cay}(B, \mu)$, $C' := \mathrm{Cay}(B, \mu')$, $\Gamma := \mathrm{diag}(\gamma, 1, 1)$, $\Gamma' := \mathrm{diag}(\gamma', 1, 1)$. If $J := \mathrm{Her}_3(C, \Gamma)$ and $J' := \mathrm{Her}_3(C', \Gamma')$ are isomorphic, then $C \cong C'$ by Thm. 41.8, and Thm. 23.22 implies (i). If $\lambda_v(\mu) < 0$, then neither J_v nor J'_v is split, and J_v by 2° is euclidean (resp., not euclidean) if and only if $\lambda_v(\gamma) > 0$ (resp., $\lambda_v(\gamma) < 0$), ditto for J'_v. Hence $\lambda_v(\gamma\gamma') > 0$ in any case, and (ii) holds. Conversely, suppose (i) and (ii) hold. Then 2° shows $J_v \cong J'_v$ for all $v \in S$, hence $J \cong J'$ by 1°. □

46.21 Corollary (Albert-Jacobson [11, Thm. 12]). *There are precisely* $3^{|S|}$ *isomorphism classes of Albert algebras over* F.

Proof Put $n := |S|$ and conclude from Thm. 46.20 combined with the weak

approximation theorem that for $\mu, \gamma \in F^\times$, the assignment

$$J \cong \mathrm{Her}_3(\mathrm{Cay}(B,\mu), \mathrm{diag}(\gamma,1,1)) \longmapsto (T_J, T_J^*),$$

where

$$T_J := \{v \in S \mid \lambda_v(\mu) < 0\}, \quad T_J^* := \{v \in T_J \mid \lambda_v(\gamma) > 0\}$$

yields a well-defined bijection from the isomorphism classes of Albert F-algebras onto the set

$$X := \{(T, T^*) \mid T \in 2^S,\ T^* \in 2^T\}.$$

Hence the number of these isomorphism classes is

$$|X| = \sum_{r=0}^{n} \binom{n}{r} 2^r = 3^n. \qquad \square$$

Exercises

46.22. Suppose F is a C_2 field. Prove: For every Azumaya F-algebra A, $\mathrm{Nrd}_A : A \to F$ is surjective.

46.23. *The* 3*-invariant* mod 2 *of Albert algebras* (Petersson-Racine [228, Thm. 1.8]).

(a) Let (B,τ) be a central simple associative algebra of degree 3 with unitary involution over a field F and put $K := \mathrm{Cent}(B)$ as a quadratic étale F-algebra. Show that the second Tits construction $J := J(B,\tau,1_B,1_K)$ is a reduced Albert algebra over F and call the norm of its coefficient algebra the 3-*Pfister form* of τ.

(b) Let J be an arbitrary Albert algebra over F. Prove that there exists a 3-Pfister form $f_3(J)$ over F, called the 3-*invariant* mod 2 of J, that up to isometry is uniquely determined by the following condition: for all field extensions E/F making the base change J_E a reduced Albert algebra over E, the extended quadratic form $f_3(J)_E$ is the norm of the coefficient algebra of J_E. Moreover, if $J \cong J(B,\tau,p,\mu)$ is realized by the second Tits construction, with (B,τ) as in (a) and (p,μ) is an admissible scalar for (B,τ) in the sense of 44.23, then $f_3(J)$ is the 3-Pfister form in the sense of (a) of the p-twist ${}^p\tau$ in the sense of (44.25.5). (*Hint*: For uniqueness, use Springer's theorem [72, Cor. 18.5, 18.6] on quadratic forms under odd degree field extensions.)

46.24. Let J be a cubic Jordan division algebra over a field F of characteristic not 2. Show that J, viewed as a linear Jordan algebra as in 29.3, is a division algebra in the sense of 8.6. (*Hint*: Reduce to the finite-dimensional case and then show that there are no linear zero divisors:

$$\forall x, y \in J\ (x \circ y = 0 \implies x = 0 \text{ or } y = 0). \tag{1}$$

In order to do so, argue indirectly and assume $x \circ y = 0$ for some non-zero elements $x, y \in J$ to distinguish between the cases that $E := F[x] \subseteq J$ is or is not a separable cubic subfield of J.)

Remark. In his two fundamental papers [8, 10] on exceptional division algebras, Albert does not explain how Jordan *division* algebras are defined. But since he always excludes

characteristic 2, and the U-operator doesn't show up in his investigations, it is safe to assume that he understood Jordan division algebras, in contradistinction to the present work, in the linear sense of 8.6. The preceding exercise closes the gap by showing that, over fields of characteristic not 2, Albert and we are talking about the same thing.

46.25. *Cyclic cubic subfields of Freudenthal division algebras* (Petersson-Racine [222, Thm. 4]). Let J be a Freudenthal division algebra of dimension at least 9 over a field F of characteristic not 2 or 3 containing the cube roots of unity. Show that J contains a cyclic cubic subfield. (*Hint*: Note that, by the hypothesis on F, any field extension $F(\sqrt[3]{\alpha})$ for $\alpha \in F^\times \setminus F^{\times 3}$ is automatically cyclic over F and apply Springer's theorem [72, Cor. 18.5, 18.6] on quadratic forms under odd-degree field extensions.)

Remark. By a classical theorem of Wedderburn [9, Thm. IX.5], every central associative division algebra D of degree 3 over F contains a cyclic cubic subfield, so the preceding exercise is valid for $J \cong D^{(+)}$, irrespective of any hypothesis on F. But it is not valid for all cubic Jordan division algebras of dimension 9 [222, Prop. 5].

On the other hand, Albert [10, p. 378] has asked whether every Albert division algebra over F contains a cyclic cubic subfield. While the present exercise provides a positive answer to this question if the characteristic is not 2 or 3 and in the presence of the cube roots of unity, the answer in general is not known. But there is an important affirmative variant due to Thakur [276], which says that *any Albert division algebra over any field has an isotope that contains a cyclic cubic subfield.* Again, this statement is not true for Freudenthal division algebras of dimension 9.

VIII

Lie algebras

The rest of the book will concern connections between Freudenthal and composition algebras on the one hand and Lie algebras and group schemes on the other. We begin with Lie algebras, the subject of this chapter. The classification of finite-dimensional simple Lie algebras over the complex numbers (47.9) leads to the notion of root system (47.10), a language that will be used for the rest of the book. In that classification, one finds infinite families that are related to the unitary, orthogonal and symplectic involutions of n-by-n matrices (see section 10). The five isolated cases are usually referred to as exceptional, and those cases are where we find the closest links with Albert and octonion algebras. Most of this chapter is devoted to the study of $\mathrm{Der}(A)$ for A a non-associative or para-quadratic k-algebra.

47 Lie algebras

47.1 Definition. As usual let k be a commutative associative ring. A non-associative k-algebra L is a *Lie algebra* if its product, denoted $[-,-]\colon L\times L\to L$, satisfies

$$[x,x]=0, \tag{1}$$

$$[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0, \tag{2}$$

for all $x,y,z\in L$. The first equation linearizes to

$$[x,y]=-[y,x]. \tag{3}$$

Equation (2) is called the *Jacobi identity*. The theory of Lie algebras can be found, for example, in books by Bourbaki [31, 33], Humphreys [126], and Jacobson [135].

47.2 Examples. (1) The cross product $\times$ endows $\mathbb{R}^3$ with a Lie algebra structure (1.1).

(2) Any associative k-algebra A can be endowed with a Lie algebra structure $A^{(-)}$ by defining the product

$$[x,y]:=xy-yx$$

where juxtaposition denotes the multiplication in A. This product is easily seen to satisfy (47.1.1) and (47.1.2). If B is a subalgebra of A then $B^{(-)}$ is a Lie subalgebra of $A^{(-)}$.

(3) For any k-module M, denote $\mathrm{End}_k(M)^{(-)}$ by $\mathfrak{gl}(M)$. In the special case $M = k^n$, we write $\mathfrak{gl}_n(k)$ instead of $\mathfrak{gl}(M)$.

(4) If τ is an involution of A, then $\mathrm{Skew}(A,\tau)$ (10.6.3) is a Lie subalgebra of $A^{(-)}$ and $\mathrm{Alt}(A,\tau)$ (10.6.4) is a Lie subalgebra of $\mathrm{Skew}(A,\tau)$ and of $A^{(-)}$.

(5) Let $\mathbb{O}$ be the Graves-Cayley octonions and u_i, $0 \le i \le 7$, a Cartan-Schouten basis of $\mathbb{O}$ (2.1). Since

$$[u_1,[u_2,u_3]] + [u_2,[u_3,u_1]] + [u_3,[u_1,u_2]] = 12u_6,$$

$\mathbb{O}^{(-)}$ is not a Lie algebra. Instead, it is merely a "Malcev algebra", see Exc. 47.16.

A Lie algebra L is *abelian* if $[L,L] = \{0\}$. For example if $L = \mathrm{Mat}_n(k)^{(-)}$ then the diagonal matrices H form an abelian subalgebra of L. The map $x \mapsto \mathrm{ad}_x \in \mathrm{End}_k(L)$ given by $\mathrm{ad}_x(y) := [x,y]$ for all $x, y \in L$, is the *adjoint representation* of L.

Before working out a useful example, we recall some standard facts from commutative algebra.

47.3 Base change of endomorphisms of finitely generated modules.

(a) Let $R \in k$-**alg** be flat, M a k-module, $N \subseteq M$ a submodule and $i\colon N \to M$ the inclusion. Since the R-linear extension $i_R\colon N_R \to M_R$ is injective by flatness of R, we may and always will identify $N_R \subseteq M_R$ as an R-submodule accordingly.

(b) Let $R \in k$-**alg** be arbitrary and suppose M, N are k-modules. Then the natural k-linear map

$$\mathrm{Hom}_k(M,N) \longrightarrow \mathrm{Hom}_R(M_R,N_R), \quad f \longmapsto f_R,$$

canonically extends to an R-linear map $\mathrm{Hom}_k(M,N)_R \to \mathrm{Hom}_R(M_R,N_R)$ (9.2), which is injective if R is a flat k-algebra and M is finitely generated [27, I.2.10, Prop. 11]; we will then identify $\mathrm{Hom}_k(M,N)_R \subseteq \mathrm{Hom}_R(M_R,N_R)$ as an R-submodule canonically.

(c) If M is a finitely generated projective k-module, (b) can be improved: for any $R \in k$-**alg**, [28, II.5.3, Prop. 7(ii)] yields an identification

$$\mathrm{Hom}_k(M,N)_R = \mathrm{Hom}_R(M_R,N_R)$$

of R-modules such that

$$(f \otimes r)(x \otimes r') = f(x) \otimes rr' \qquad (x \in M,\ r, r' \in R). \tag{1}$$

Note that this identification yields $f_R = f \otimes \mathbf{1}_R = f \otimes 1_R$ for the R-linear extension f_R of f.

47.4 Orthogonal Lie algebras. Let (M, q) be a quadratic module over k (11.12). Consider

$$\mathfrak{o}(q) := \mathfrak{o}(M, q) := \{\phi \in \mathrm{End}_k(M) \mid q(\phi x, x) = 0\ \forall x \in M\}.$$

If $\phi \in \mathfrak{o}(q)$ then $q(\phi x, y) + q(x, \phi y) = 0$. One checks that $\mathfrak{o}(q)$ is closed under the bracket on $\mathrm{End}_k(M)^{(-)}$ and therefore is a Lie subalgebra. It is called the *orthogonal Lie algebra of* (M, q). (Note that $\mathfrak{o}(q)$ depends on the bilinear form Dq rather than the quadratic form q, i.e., if q' is a quadratic form such that $Dq \cong Dq'$, then $\mathfrak{o}(q) \cong \mathfrak{o}(q')$.)

47.5 Lemma. *Let (M, q) be a quadratic module over k with M finitely generated projective. Then for every $R \in k$-**alg**, $\mathfrak{o}(M, q)_R \subseteq \mathfrak{o}(M_R, q_R)$. If R is flat, then the containment is an equality.*

Proof Put $\mathsf{TS}^2(M)$ for the submodule of $M \otimes M$ consisting of elements fixed by the automorphism $\tau\colon m \otimes m' \mapsto m' \otimes m$, called the *symmetric tensors* in [28, §III.6.3]. Then $\mathfrak{o}(M, q)$ is the kernel of the linear map

$$\delta\colon\ \mathrm{End}_k(M) \to \mathrm{Hom}_k(\mathsf{TS}^2(M), k)$$

defined by $\delta(\phi)(m \otimes m') := q(m, \phi m')$. The claimed containment is immediate.

So suppose R is flat. Because $\mathsf{TS}^2(M)$ can be defined as the kernel of $\tau - \mathbf{1}_{M\otimes M} \in \mathrm{End}_k(M \otimes M)$, we have a natural identification $(\mathsf{TS}^2(M))_R \cong \mathsf{TS}^2(M_R)$.

We note that if M is finitely generated free, so is $\mathsf{TS}^2(M)$ by [29, §IV.5.5, Prop. 4]. From this, in the general case where M is finitely generated projective, standard reductions such as in the solution to Exc. 25.36 show that $\mathsf{TS}^2(M)$ is also finitely generated projective. Consequently,

$$\mathrm{Hom}_k(\mathsf{TS}^2(M), k)_R = \mathrm{Hom}_R(\mathsf{TS}^2(M)_R, R) \cong \mathrm{Hom}_R(\mathsf{TS}^2(M_R), R).$$

where the first identification is as in 47.3. From the flatness of R, we find that

$$\mathfrak{o}(q)_R = (\mathrm{Ker}\,\delta)_R = \mathrm{Ker}(\delta_R) = \mathfrak{o}(q_R),$$

as desired. □

47.6 Remark. Readers who are familiar with Lie algebras of affine group schemes (as described in §52, for example) may prefer to view the conclusion of the lemma as a consequence of the fact that $\mathbf{O}(M, q)$ is smooth via

[61, Prop. II.4.8], which requires some additional hypotheses on (M, q) as in Remark 25.22.

47.7 Elementary orthogonal transformations. Let (M, q) be a quadratic module over k. For any $a, b \in M$ define the *elementary orthogonal transformation* $S_{a,b} \in \mathrm{End}_k(M)$ via

$$S_{a,b}(m) := q(a, m)b - q(b, m)a \ \in M$$

for $m \in M$. Not only does $S_{a,b}$ belong to $\mathfrak{o}(q)$ but since for all $\phi \in \mathfrak{o}(q)$ and a, $b \in M$,

$$[\phi, S_{a,b}] = S_{\phi a,b} + S_{a,\phi b},$$

the span $\mathfrak{s}(q)$ of the $S_{a,b}$ for $a, b \in M$ is an ideal of $\mathfrak{o}(q)$.

47.8 Proposition. *Let (M, q) be quadratic space over k. If M is of constant even rank then $\mathfrak{o}(q) = \mathfrak{s}(q)$.*

Proof Suppose first (M, q) is a split hyperbolic space of rank $2l$ (11.18). Write $M = \oplus_{1 \le i \le l}(kx_i \oplus ky_i)$, a finite direct sum of mutually orthogonal hyperbolic planes. Suppose $E \in \mathfrak{o}(q)$ and define

$$L := \sum_{1 \le i < j \le l} q(Ey_i, y_j) S_{x_i,x_j} + \sum_{1 \le i < j \le l} q(Ex_i,\ x_j) S_{y_i,y_j} + \sum_{i,j} q(Ex_i, y_j) S_{y_i,x_j}.$$

Using $q(Ex, x) = 0$ and $q(Ex, y) + q(Ey, x) = 0$ for all $x, y \in M$, one computes

$$\begin{aligned} Lx_r &= \sum_{1 \le i < j \le l} q(Ex_i,\ x_j)(\delta_{ir} y_j - \delta_{jr} y_i) + \sum_{i,j} q(Ex_i,\ y_j)\delta_{ir} x_j \\ &= \sum_{1 \le j \le l} q(Ex_r,\ x_j) y_j + \sum_{1 \le j \le l} q(Ex_r,\ y_j) x_j \\ &= Ex_r. \end{aligned}$$

Similarly $Ly_r = Ey_r$ and for an arbitrary $a \in M$, $La = Ea$.

In the general case, by Exc. 26.12, there exists an étale cover $R \in k$-**alg** making (M_R, q_R) a split hyperbolic quadratic space over R. Concerning $\mathfrak{s}(q)$, it is the image of a linear map $M \otimes M \to \mathrm{End}_k(M)$. Since $(\mathrm{End}_k(M))_R \cong \mathrm{End}_R(M_R)$ and R is flat, we obtain via 25.3 (3) a natural identification $\mathfrak{s}(q)_R = \mathfrak{s}(q_R)$. Concerning $\mathfrak{o}(q)$, Lemma 47.5 gives $\mathfrak{o}(q)_R = \mathfrak{o}(q_R)$. The inclusion $\mathfrak{s}(q) \hookrightarrow \mathfrak{o}(q)$ by the special case just treated becomes an isomorphism when changing scalars from k to R, so it must have been one all along. □

47.9 Lie algebras over a field of characteristic zero. Suppose now that L is a finite-dimensional Lie algebra over a field F of characteristic 0. We say that

L is *semisimple* if the only abelian ideal in L is 0. It is *simple* if $[L, L] \neq 0$ and the only ideals in L are 0 and L. (Note that this definition agrees with the one in 8.6.) For example, $\{0\}$ is a semisimple Lie algebra but not a simple one. A semisimple Lie algebra is a direct sum of simple Lie algebras [30, §I.6.2, Prop. 2].

Suppose now that L is semisimple and F is algebraically closed. An element $a \in L$ is *semisimple* if the minimal polynomial of $\mathrm{ad}_a \in \mathrm{End}_F(L)$ has no repeated roots, compare Exc. 8.11. Let S be the set of abelian subalgebras of L whose elements are all semisimple. Maximal elements of S are called *Cartan subalgebras*. Cartan subalgebras exist [33, §§VII.2.3, VII.2.4] and are conjugate under the action of the group $\mathrm{Aut}(L)$ [33, §VII.3.2, Thm. 1]. Let H be a Cartan subalgebra of L. For every $\alpha \in H^*$ the dual of H, let L_α be the set of elements $a \in L$ such that $[h, a] = \alpha(h)a$ for all $h \in H$. If $\alpha = 0$ then $L_\alpha = H$. The set R of nonzero $\alpha \in H^*$ such that $L_\alpha \neq \{0\}$ is called the set of *roots* of L with respect to H. The pair (V, R), where V is the real subspace of $H^* \otimes \mathbb{R}$ spanned by R, is something called a root system, whose definition we now recall. The historical origin of root systems came from the discovery that isomorphism classes of semisimple Lie algebras over $\mathbb{C}$ are in bijection with isomorphism classes of root systems; this powerful theorem reduces the classification problem for Lie algebras to one of finite combinatorial data.

47.10 Root systems. Our aim is to recall the classification of irreducible root systems. Let V be a finite-dimensional real euclidean vector space. A *reflection with respect to* $\alpha \in V \setminus \{0\}$ is an endomorphism $s \in \mathrm{End}(V)$ such that $s(\alpha) = -\alpha$ and $s|_W = \mathrm{Id}$ for some hyperplane $W \subset V$.

Consider the natural pairing $V^* \otimes V \to \mathbb{R}$, $\lambda \otimes v \mapsto \langle \lambda, v \rangle = \lambda(v)$. A reflection with respect to α is given by $s_\alpha(v) := v - \langle \alpha^\vee, v \rangle \alpha$, where $\alpha^\vee$ is the unique element of V^* such that $\alpha^\vee|_W = 0$, where $W = \alpha^\perp$ with respect to the euclidean structure, and $\langle \alpha^\vee, \alpha \rangle = 2$.

47.11 Definition. A *root system* is a pair (V, R) where V is a finite-dimensional real euclidean space and R is a subset of V which satisfies

I. R is finite, $0 \notin R$ and R generates V.
II. For every $\alpha \in R$, s_α stabilizes R.
III. For any $\alpha \in R$, $\alpha^\vee(R) \subset \mathbb{Z}$.

We will focus on root systems that are *reduced*, meaning that they also satisfy:

IV. If $\alpha, r\alpha \in R$ for some $r \in \mathbb{R}$, then $r = \pm 1$.

For example:

(a) $(0, \emptyset)$ is a reduced root system, called the zero root system.

(b) $(\mathbb{R}, \{\pm 1\})$ is also a reduced root system, called A_1.

(c) In the situation of 47.9, for each $\alpha \in R$, the subspace $[L_\alpha, L_{-\alpha}] \subseteq H$ is 1-dimensional and contains a unique element H_α such that $\alpha(H_\alpha) = 2$. For V the real subspace of $H^* \otimes \mathbb{R}$ spanned by R and $\alpha \in R$, we define $s_\alpha \colon v \mapsto v - v(H_\alpha)\alpha$. With the inner product on V as in [33, §VIII.2.2, Rmk. 2], (V, R) is a reduced root system.

If (V, R) and (V', R') are root systems, an *isomorphism* of (V, R) to (V', R') is an isomorphism of euclidean vector spaces $\phi : V \to V'$ such that $\phi(R) = R'$. Two root systems (V, R) and (V', R') are *isomorphic* if there exists an isomorphism between them. A subset $B \subset R$ is said to be a *basis* of a root system (V, R) if for any $\alpha \in R$, $\alpha = \sum_{\beta \in B} c_\beta \beta$ for some uniquely determined $c_\beta \in \mathbb{Z}$ such that $c_\beta \geq 0$ for all $\beta \in B$ or $c_\beta \leq 0$ for all $\beta \in B$. We say that the root α is *positive* or *negative* depending on which case applies. Every root system has a basis [31, §§VI.1.5, VI.1.6] and any two bases of (V, R) can be mapped to each other by an automorphism of (V, R).

We are furthermore interested in reduced root systems that are also irreducible, defined as follows: If (V_i, R_i), $1 \leq i \leq n$, are root systems then $R = R_1 + R_2 + \cdots + R_n := \cup_{i=1}^n R_i$ is a root system on $V = \oplus_{i=1}^n V_i$. A root system V, R is *irreducible* if $V \neq 0$ and $(V, R) \cong (V_1, R_1) + (V_2, R_2)$ implies (V_1, R_1) or (V_2, R_2) is zero. In the setting of 47.9, the root system R is irreducible if and only if the Lie algebra L is simple.

47.12 Dynkin Diagrams. The key properties of a particular root system (V, R) can be summarized by its *Dynkin diagram*. It is a graph whose vertex set is a basis B of the root system. Vertices $\alpha \neq \beta$ are connected by $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle$ edges. In particular, α, β are connected by a single edge if and only if they have the same length [31, §VI.4.2]. If α, β are connected by more than one edge, then the two roots have different lengths, and one draws a $<$ sign on those multiple edges, indicating that the shorter root is "less than" the longer root. (Formally, the Dynkin diagram is a directed graph, where vertices connected by a single edge are bidirectional, and vertices connected by multiple edges have those edges going from the longer root to the shorter.)

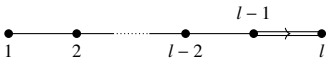
Up to isomorphism, this diagram is independent of the choice of basis. The Dynkin diagram determines the root system up to isomorphism. A root system is irreducible if and only if its Dynkin diagram is connected. Finite-dimensional simple Lie algebras over an algebraically closed field of characteristic 0 correspond to irreducible reduced root systems and hence to connected Dynkin diagrams. These have been classified [31, §VI.4.2, Thm. 3]. We repro-

duce part of the information found in the appendices of ibid. In each case, we specify a basis $B = \{\alpha_1, \ldots, \alpha_l\}$ and we label the vertex $\alpha_i \in B$ in the diagram by the symbol i. We omit the root systems E_7 and E_8, because we do not use the properties of those root systems in this book.

A_l 

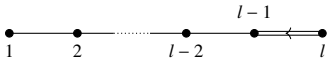
$(l \geq 1)$

Let V be the hyperplane of $E = \mathbb{R}^{l+1}$ composed of the points orthogonal to $\epsilon_1 + \epsilon_2 + \cdots + \epsilon_{l+1}$ where ϵ_i, $1 \leq i \leq l+1$ is the standard basis of E . The roots are $\epsilon_i - \epsilon_j$, $1 \leq i \neq j \leq l+1$. The roots $\alpha_1 = \epsilon_1 - \epsilon_2$, $\alpha_2 = \epsilon_2 - \epsilon_3$, …, $\alpha_l = \epsilon_l - \epsilon_{l+1}$ form a basis of this root system.

B_l 

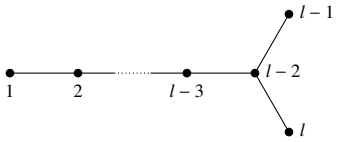
$(l \geq 2)$

Let $V = E = \mathbb{R}^l$. The roots are $\pm\epsilon_i$, $1 \leq i \leq l$; $\pm\epsilon_i \pm \epsilon_j$, $1 \leq i \neq j \leq l$. The roots $\alpha_1 = \epsilon_1 - \epsilon_2$, $\alpha_2 = \epsilon_2 - \epsilon_3$, …, $\alpha_{l-1} = \epsilon_{l-1} - \epsilon_l$, $\alpha_l = \epsilon_l$ form a basis of this root system.

C_l 

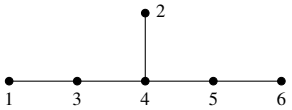
$(l \geq 2)$

Let $V = E = \mathbb{R}^l$. The roots are $\pm 2\epsilon_i$, $1 \leq i \leq l$; $\pm\epsilon_i \pm \epsilon_j$, $1 \leq i < j \leq l$. The roots $\alpha_1 = \epsilon_1 - \epsilon_2$, $\alpha_2 = \epsilon_2 - \epsilon_3$, …, $\alpha_{l-1} = \epsilon_{l-1} - \epsilon_l$, $\alpha_l = 2\epsilon_l$ form a basis of this root system.

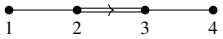
D_l 

$(l \geq 3)$

Let $V = E = \mathbb{R}^l$. The roots are $\pm\epsilon_i \pm \epsilon_j$, $1 \leq i < j \leq l$. The roots $\alpha_1 = \epsilon_1 - \epsilon_2$, $\alpha_2 = \epsilon_2 - \epsilon_3$, …, $\alpha_{l-1} = \epsilon_{l-1} - \epsilon_l$, $\alpha_l = \epsilon_{l-1} + \epsilon_l$ form a basis of this root system.

E_6 

Let V be the subspace of $E = \mathbb{R}^8$ whose points have coordinates (ξ_i) such that $\xi_6 = \xi_7 = -\xi_8$. The roots are $\pm\epsilon_i \pm \epsilon_j$, $1 \le i < j \le 5$, $\pm\frac{1}{2}(\epsilon_8 - \epsilon_7 - \epsilon_6 + \sum_{i=1}^5 (-1)^{\nu(i)}\epsilon_i)$ with $\sum_{i=1}^5 \nu(i)$ even. The roots $\alpha_1 = \frac{1}{2}(\epsilon_1 + \epsilon_8) - \frac{1}{2}(\epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 + \epsilon_7)$, $\alpha_2 = \epsilon_1 + \epsilon_2$, $\alpha_3 = \epsilon_2 - \epsilon_1$, $\alpha_4 = \epsilon_3 - \epsilon_2$, $\alpha_5 = \epsilon_4 - \epsilon_3$, $\alpha_6 = \epsilon_5 - \epsilon_4$ form a basis of this root system.

F_4 

Let $V = E = \mathbb{R}^4$. The roots are $\pm\epsilon_i$, $1 \le i \le 4$; $\pm\epsilon_i \pm \epsilon_j$, $1 \le i < j \le 4$, $\frac{1}{2}(\pm\epsilon_1 \pm \epsilon_2 \pm \epsilon_3 \pm \epsilon_4)$. The roots $\alpha_1 = \epsilon_2 - \epsilon_3$, $\alpha_2 = \epsilon_3 - \epsilon_4$, $\alpha_3 = \epsilon_4$, $\alpha_4 = \frac{1}{2}(\epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4)$ form a basis of this root system.

G_2 

Let V be the hyperplane of $E = \mathbb{R}^3$ orthogonal to $\epsilon_1 + \epsilon_2 + \epsilon_3$. The roots are $\epsilon_i - \epsilon_j$, $1 \le i \ne j \le 3$ and $\pm(2\epsilon_i - \epsilon_j - \epsilon_k)$, $\{i, j, k\}$ a cyclic permutation of $\{1, 2, 3\}$. The roots $\alpha_1 = \epsilon_1 - \epsilon_2$ and $\alpha_2 = -2\epsilon_1 + \epsilon_2 + \epsilon_3$ form a basis of this root system.

47.13 Example. Let us now produce a root system in the case of the Lie algebra $\mathfrak{o}(M, q)$, where q is a split hyperbolic quadratic space with basis $x_1, \dots, x_l$, $y_1, \dots, y_l$ of M as in the proof of Prop. 47.8. In this case, one typically writes simply $\mathfrak{o}_{2l}(k)$ instead of $\mathfrak{o}(M, q)$.

Writing $E_{i,j}$ for the matrix units of $\mathrm{Mat}_{2l}(k)$, S_{y_i,x_j} corresponds to $E_{j,i} - E_{l+i,l+j}$. For $i < j$, S_{x_i,x_j} corresponds to $E_{j,l+i} - E_{i,l+j}$ and S_{y_i,y_j} corresponds to $E_{l+j,i} - E_{l+i,j}$. So $\mathfrak{o}_{2l}$ corresponds to the matrices

$$\begin{pmatrix} A & B \\ C & -A^{\mathsf{T}} \end{pmatrix} \tag{1}$$

where $A \in \mathrm{Mat}_l(k)$ and $B, C \in \mathrm{Alt}_l(k)$. In particular, $\mathfrak{o}_{2l}$ *is free as a* k*-module of rank* $2l^2 - l$. It has a Cartan subalgebra $\mathfrak{h}$ with basis

$$H_i = E_{i,i} - E_{l+i,l+i}, \qquad 1 \le i \le l.$$

(In the special case where $\ell = 1$, we have $\mathfrak{o}(q) = \mathfrak{h}$.) Let ϵ_i be the basis of the dual $\mathfrak{h}^*$ which is dual to the H_i. For $1 \le i, j \le l$, let

$$\begin{aligned} X_{\epsilon_i - \epsilon_j} &= E_{i,j} - E_{l+j,l+i} \quad i \ne j, \\ X_{\epsilon_i + \epsilon_j} &= E_{j,l+i} - E_{i,l+j} \quad i < j, \\ X_{-\epsilon_i - \epsilon_j} &= E_{l+i,j} - E_{l+j,i} \quad i < j. \end{aligned}$$

For $l \geq 4$ this is a root decomposition of $\mathfrak{o}_{2l}(k)$ of type D_l. If we let $H_{\alpha_i} = H_i - H_{i+1}$, $1 \leq i \leq l-1$ and $H_{\alpha_l} = H_{l-1} + H_l$, we have a basis of $\mathfrak{o}_{2l}(k)$.

47.14 Example. For b an alternating bilinear form on a k-module M, define $\mathfrak{sp}(M, b)$ to be the subspace of $\mathfrak{gl}(M)$ consisting of elements ϕ such that $b(\phi x, y) + b(x, \phi y) = 0$ for all $x, y \in M$. One checks that it is closed under the bracket and so it is a subalgebra of $\mathfrak{gl}(M)$, called the symplectic Lie algebra.

In the case where $M = k^{2l}$ and b is the bilinear form

$$\left\langle \begin{pmatrix} 0 & \mathbf{1}_l \\ -\mathbf{1}_l & 0 \end{pmatrix} \right\rangle$$

in the notation of 11.7, we find that $\mathfrak{sp}(M, b)$ consists of matrices as in (47.13.1) with $A \in \mathrm{Mat}_l(k)$ and $B, C \in \mathrm{Sym}_l(k)$. We will denote this algebra $\mathfrak{sp}_{2l}(k)$. In a manner similar to the previous example, one can exhibit inside $\mathfrak{sp}_{2l}(k)$ a root system of type C_l, see for example [33, §VIII.13.3].

47.15 Remark. Lie algebras, even over a field, are sensitive to whether the field has characteristic zero or not (see for example [257], [273]) and even to whether the field has characteristic 2, 3, or 5, see for example [239]. The case of characteristic 2 poses particular challenges, leading McCrimmon to quip [190, §0.3]: "Lie algebras in characteristic 2 are weak, pitiable things."

Exercises

47.16. A non-associative k-algebra L is a *Malcev algebra* if the product $[-,-]\colon L \times L \to L$ is alternating (i.e., $[x, x] = 0$ for all $x \in L$) and the identity

$$[[x, y], [x, z]] = [[[x, y], z], x] + [[[y, z], x], x] + [[[z, x], x], y],$$

called the *Malcev identity*, holds for all $x, y, z \in L$.

(a) Put $J(x, y, z) := [[xy]z] + [[yz]x] + [[zx]y]$, so the Jacobi identity (47.1.2) reads $J(x, y, z) = 0$. Verify that, if the product in L is alternating, then the Malcev identity is equivalent to the identity

$$J(x, y, [xz]) = [J(x, y, z), x].$$

It immediately follows that every Lie algebra is a Malcev algebra.

(b) Let A be a non-associative k-algebra that is flexible, meaning that the flexible law (13.1.3) holds. Define

$$S(x, y, z) := [x, y, z] + [y, z, x] + [z, x, y]$$

for $x, y, z \in A$. Verify that, for every permutation π of $\{1, 2, 3\}$, we have

$$S(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) = (\operatorname{sgn} \pi) S(x_1, x_2, x_3),$$

where $\operatorname{sgn} \pi = 1$ if π is an even permutation and -1 if π is odd.

Remark. This is a weaker statement than to say that S is alternating, as we do not claim

that S vanishes whenever two of its arguments are equal. Let $A^{(-)}$ be the algebra defined from A as in 47.2 with product $[-,-]$. Expanding the definitions shows that

$$J(x,y,z) = S(x,y,z) - S(x,z,y) \quad \forall x,y,z \in A$$

where the expression on the left is computed in $A^{(-)}$.

(c) Continue the notation of (b), except we assume the stronger hypothesis that A is alternative. Prove that $A^{(-)}$ is Malcev. Prove: in case 6 is invertible in k, $A^{(-)}$ is a Lie algebra if and only if A is associative. (*Hint*: Use the Kleinfeld function of Exercise 14.8.)

47.17. Let C be a composition k-algebra of rank 4 or 8. Then $C^{(-)}$ is a Malcev algebra by the preceding exercise and k is an ideal in $C^{(-)}$, so $C^{(-)}/k$ is also a Malcev algebra. Assuming k is a field, prove: $C^{(-)}/k$ is simple (as a Malcev algebra) if and only if k has characteristic different from 2.

Remark. It turns out that, if k is a field of characteristic $\neq 2, 3$, then every simple Malcev algebra over k is either a Lie algebra or is of the form $C^{(-)}/k$ for C an octonion k-algebra, see [167, Thm. 3.11] and [82]. This statement is strongly reminiscent of (1) Kleinfeld's Theorem 13.10, which says that every simple alternative algebra is associative (and therefore described by the Wedderburn-Artin Theorem) or an octonion algebra, and (2) the fact that every simple Jordan algebra is either special (and therefore arises from an associative algebra) or is an Albert algebra.

47.18. For a ring k and $n \geq 1$, write $\mathfrak{sl}_n(k)$ for the collection of trace zero matrices in $\mathfrak{gl}_n(k)$. Since $\mathrm{tr}(xy) = \mathrm{tr}(yx)$ for $x, y \in \mathrm{Mat}_n(k)$, $\mathfrak{sl}_n(k)$ is closed under the bracket and so is a Lie subalgebra of $\mathfrak{gl}_n(k)$. Trivially, $\mathfrak{sl}_1(k) = \{0\}$. In the case of a field F, prove:

(a) If char F does not divide n, then $\mathfrak{sl}_n(F)$ is simple for $n \geq 2$.
(b) If char F divides n and $n > 2$, then $F\mathbf{1}_n$ is the unique proper nonzero ideal in $\mathfrak{sl}_n(F)$.
(c) In the cases considered in (a) and (b), verify that $[\mathfrak{sl}_n(F), \mathfrak{sl}_n(F)] = \mathfrak{sl}_n(F)$.

47.19. Let F be a field of characteristic 2 and consider the Lie algebra $\mathfrak{sp}_{2n}(F)$ defined in Example 47.14. Prove:

(a) $[\mathfrak{sp}_{2n}(F), \mathfrak{sp}_{2n}(F)] = \mathfrak{o}_{2n}(F)$ if $n \geq 2$.
(b) $[\mathfrak{o}_{2n}(F), \mathfrak{o}_{2n}(F)]$ is the subalgebra of $\mathfrak{o}_{2n}(F)$ consisting of matrices as in (47.13.1) with $A \in \mathfrak{sl}_n(F)$ (and $B, C \in \mathrm{Alt}_n(F)$).

47.20. Pick an orientation $\Delta\colon \wedge^{2n}(k^{2n}) \to k$ and define a bilinear form b on $\wedge^n k^{2n}$ via $b(x,y) := \Delta(x \wedge y)$. It is symmetric if n is even and alternating if n is odd. (We assume $n \geq 1$ to avoid triviality.) Prove:

(a) The action of $\mathfrak{sl}_{2n}(k)$ on $\wedge^n(k^{2n})$ gives a nonzero homomorphism of Lie algebras $\rho\colon \mathfrak{sl}_{2n}(k) \to \mathfrak{g}$, where $\mathfrak{g} := \mathfrak{o}(\wedge^n k^{2n}, b)$ if n is even and $\mathfrak{sp}(\wedge^n k^{2n}, b)$ if n is odd.
(b) If k is a field of characteristic not dividing $2n$ and $n \geq 1$, then ρ is injective. If additionally $n = 2$, then ρ is an isomorphism $\mathfrak{sl}_4(k) \cong \mathfrak{o}_6(k)$.
(c) If k is a field of characteristic 2 and $n > 1$, then $\mathrm{Ker}(\rho) = k\mathbf{1}_{2n}$. If additionally $n = 2$, then ρ induces an isomorphism

$$\mathfrak{sl}_4(k)/k\mathbf{1}_{2n} \cong [\mathfrak{o}_6(k), \mathfrak{o}_6(k)].$$

Remark. The root systems A_3 and D_3 have isomorphic Dynkin diagrams and so are isomorphic, and it follows that the simple Lie algebras $\mathfrak{sl}_4(\mathbb{C})$ and $\mathfrak{o}_6(\mathbb{C})$ are isomorphic. This exercise provides corresponding statements over an arbitrary field.

48 Derivations

Most results of the next two sections can be found in [176], some in more generality. Unless otherwise specified, we assume that k is a commutative ring.

48.1 Definition. A *derivation* of a non-associative algebra A is an element $D \in \mathrm{End}_k(A)$, the associative algebra of endomorphisms of A as a k-module, satisfying one (and hence all) of the following equivalent relations, for all $x, y \in A$:

$$D(xy) = (Dx)y + x(Dy), \tag{1}$$

$$[D, L_x] = L_{Dx}, \tag{2}$$

$$[D, R_y] = R_{Dy}. \tag{3}$$

The derivations of A form a Lie algebra — more precisely, a subalgebra of $\mathrm{End}_k(A)^{(-)}$ — denoted by $\mathrm{Der}(A)$. The elements of $\mathrm{Der}(A)$ also act on commutators and associators in a derivation-like manner, i.e., we have

$$D([x, y]) = [Dx, y] + [x, Dy], \tag{4}$$

$$D([x, y, z]) = [Dx, y, z] + [x, Dy, z] + [x, y, Dz] \tag{5}$$

for all $x, y, z \in A$. Moreover if A is unital,

$$D1_A = 0. \tag{6}$$

In general we will refer to the action of $\mathrm{Der}(A)$ on A as the *natural representation* of $\mathrm{Der}(A)$. If A is unital, in view of (6) we consider the action of $\mathrm{Der}(A)$ on $A/k1_A$ as the natural representation.

48.2 Example. The notion of a derivation for a non-associative algebra A over k is naturally related to the notion of an automorphism as follows. Suppose $D \in \mathrm{End}_k(A)$ and put $R := k[\varepsilon]$ for the k-algebra of dual numbers. We have: *D is a derivation of A if and only if $\phi_D \colon A_R \to A_R$ defined by*

$$\phi_D(x + \varepsilon y) := x + \varepsilon(Dx + y)$$

for $x, y \in A$ is an automorphism of A_R. While R-linearity is straightforward to

check, the equations

$$\begin{aligned}\phi_D((x+\varepsilon y)(x'+\varepsilon y')) &= \phi_D(xx'+\varepsilon(xy'+yx'))\\ &= xx'+\varepsilon(D(xx')+xy'+yx')\end{aligned}$$

and

$$\begin{aligned}\phi_D(x+\varepsilon y)\phi_D(x'+\varepsilon y') &= (x+\varepsilon(Dx+y))(x'+\varepsilon(Dx'+y'))\\ &= xx'+\varepsilon(x(Dx')+xy'+(Dx)x'+yx')\end{aligned}$$

for all $x, x', y, y' \in A$ show the desired equivalence.

48.3 Example. If A is an associative algebra then for $a \in A$, $E_a := L_a - R_a$ is a derivation of A and also of the Lie algebra $A^{(-)}$. (We will see that this is not true in general for alternative algebras.) Such derivations of an associative algebra are said to be *inner*. Note that $[E_a, E_b] = E_{[a,b]}$ so $\mathrm{InDer}_{\mathrm{ass}}(A) := \{E_a \mid a \in A\}$ is a subalgebra of $\mathrm{Der}(A)$ which is in fact an ideal of $\mathrm{Der}(A)$ since (48.1.2), (48.1.3) give $[D, E_a] = E_{Da}$. Jacobson showed that if A is a finite-dimensional central simple associative algebra over a field, then all derivations of A are inner [131, Thm. 7]. The same holds for separable algebras (42.6) over a ring k [158, III, Theorem 1.4 (7)] and semisimple Lie algebras over a field of characteristic zero [30, §I.6.2, Cor. 3].

48.4 Proposition. *Let A be a k-algebra that is a finitely generated projective k-module and suppose $R \in k$-**alg** is flat. Then*

$$(\mathrm{Der}_k(A))_R = \mathrm{Der}_R(A_R)$$

under the identifications of 47.3.

Proof Let

$$\delta_A\colon \mathrm{End}_k(A) \to \mathrm{Hom}_k(A \otimes A, A)$$

be the unique linear map satisfying

$$\delta_A(f)(a_1 \otimes a_2) = f(a_1a_2) - f(a_1)a_2 - a_1f(a_2)$$

$a_1, a_2 \in A$, so that $\mathrm{Der}_k(A) = \mathrm{Ker}\,\delta_A$. Combining the identifications of 47.3 with $(A \otimes A)_R = A_R \otimes_R A_R$, one checks that $(\delta_A)_R = \delta_{A_R}$, and the assertion follows. □

The conclusion of the proposition may be stated informally as "Der(A) is compatible with flat base change".

Regardless of whether A is associative, the subset $\{E_a\}$ of $\mathrm{End}_k(A)$ is the image of a linear map $A \to \mathrm{End}_k(A)$, and so the same proof shows that $\mathrm{InDer}_{\mathrm{ass}}(A)$

is also compatible with flat base change, i.e., $\mathrm{InDer}_{\mathrm{ass}}(A)_R \cong \mathrm{InDer}_{\mathrm{ass}}(A_R)$ for flat $R \in k$-**alg**.

48.5 Identities of alternative algebras. To study derivations of alternative algebras we will need some identities which we collect here. Let $V_y := L_y + R_y$ and $x \circ y := V_x y = V_y x = xy + yx$.

$$[L_a, R_b] = [R_a, L_b], \tag{1}$$
$$[L_a, L_b] = L_{[a,b]} - 2[L_a, R_b], \tag{2}$$
$$[R_a, R_b] = -R_{[a,b]} - 2[L_a, R_b], \tag{3}$$
$$[[L_a, R_b], L_c] = L_{[a,b,c]} - [L_{[a,b]}, R_c], \tag{4}$$
$$[[L_a, R_b], R_c] = R_{[a,b,c]} - [L_c, R_{[a,b]}], \tag{5}$$
$$[L_a, R_b]L_c = -L_c[L_a, V_b] - L_{[V_a,R_b]c}, \tag{6}$$
$$[L_a, R_b](xy) = ([L_a, R_b]x)y + x([L_a, R_b]y) + [x, [a, b], y]. \tag{7}$$

Identity (1) is the linearized version of flexibility (13.1.3). Since the associator is alternating, $[a, c, b] = -[a, b, c] = [b, a, c]$. So in operator form,

$$-[L_a, R_b] = -L_{ab} + L_a L_b = L_{ba} - L_b L_a \tag{8}$$

which yields (2). Reading (2) in the opposite algebra, using (1), yields (3). From the last equality of (8) we get

$$L_a L_b = -L_b L_a + L_{a\circ b} \tag{9}$$

and from the first

$$R_b L_a = L_a V_b - L_{ab}. \tag{10}$$

We will prove (6) next. Using (9) and (10),

$$\begin{aligned} L_a R_b L_c &= L_a(L_c V_b - L_{cb}) \\ &= -L_c L_a V_b + L_{a\circ c} V_b + L_{cb} L_a - L_{a\circ(cb)}, \\ R_b L_a L_c &= R_b(-L_c L_a + L_{a\circ c}) \\ &= -L_c V_b L_a + L_{cb} L_a + L_{a\circ c} V_b - L_{(a\circ c)b}. \end{aligned}$$

Subtracting, we obtain (6). Rewriting (6), using (2)

$$\begin{aligned} [L_a, R_b]L_c &= -L_c[L_a, L_b] - L_c[L_a, R_b] - L_{[V_a,R_b]c} \\ &= -L_c L_{[a,b]} + L_c[L_a, R_b] - L_{[V_a,R_b]c}. \end{aligned}$$

Using (3)

$$\begin{aligned}[[L_a, R_b], L_c] &= -L_c L_{[a,b]} - L_{[L_a,R_b]c} - L_{[R_a,R_b]c} \\ &= -L_c L_{[a,b]} - L_{[L_a,R_b]c} + L_{R_{[a,b]}c} + L_{2[L_a,R_b]c} \\ &= -L_c L_{[a,b]} + L_{[a,b,c]} + L_{R_{[a,b]}c} \\ &= L_{[a,b,c]} - [L_{[a,b]}, R_c]\end{aligned}$$

since

$$\begin{aligned}-L_c L_{[a,b]}x + L_{R_{[a,b]}c}x &= -c([a,b]x) + (c[a,b])x \\ &= [c,[a,b],x] = [[a,b],x,c] = -[L_{[a,b]}, R_c]x.\end{aligned}$$

So we have (4). Reading it in the opposite algebra yields (5). Finally, using (6), (2) and (3),

$$\begin{aligned}[L_a, R_b](xy) &= -L_x[L_a, V_b]y - L_{[V_a,R_b]x}y \\ &= -L_x[L_a, L_b]y - L_x[L_a, R_b]y - L_{[L_a,R_b]x}y - L_{[R_a,R_b]x}y \\ &= -L_x L_{[a,b]}y + L_x[L_a, R_b]y - L_{[L_a,R_b]x}y + L_{R_{[a,b]}x}y + L_{2[L_a,R_b]x}y \\ &= ([L_a, R_b]x)y + x([L_a, R_b]y) + [x,[a,b],y]\end{aligned}$$

yielding (7).

48.6 Lie multiplication algebra. We define the *Lie multiplication algebra of* an algebra A, denoted by $\mathfrak{L}(A)$, to be the Lie subalgebra of $\mathfrak{gl}(A)$ generated by all left and right multiplications of A (see section 8.3). If A is an associative algebra then $\mathfrak{L}(A) = L_A + R_A$. If $2 \in k^\times$ and J is a linear Jordan algebra over k, then $\mathfrak{L}(J) = L_J + [L_J, L_J]$.

By (48.1.2) and (48.1.3),

$$[\mathrm{Der}(A), \mathfrak{L}(A)] \subseteq \mathfrak{L}(A).$$

48.7 Proposition (McCrimmon [176, Prop. 2.2])**.** *The Lie multiplication algebra of an alternative algebra A is*

$$\mathfrak{L}(A) = L_A + R_A + [L_A, R_A].$$

Proof By (48.5.2)–(48.5.5) it suffices to verify that

$$[[L_A, R_A], [L_A, R_A]] \subseteq L_A + R_A + [L_A, R_A].$$

This follows from the Jacobi identity and applying (48.5.4) and (48.5.5) twice. □

48.8 Lie multiplication derivations. We will assume from now on in this chapter that alternative algebras are unital. General results on derivations of

alternative algebras including not necessarily unital ones can be found in [176]. For a unital alternative algebra A, we define the *Lie multiplication derivation algebra* of A by

$$\mathrm{LMDer}(A) := \mathfrak{L}(A) \cap \mathrm{Der}(A)$$

and refer to its elements as *Lie multiplication derivations*. Thanks to [176, Prop 1.4], this definition is consistent with the corresponding one in [176, (1-7)].

48.9 Theorem (McCrimmon [176, Thm. 2.3])**.** *An endomorphism D of an alternative algebra A is a Lie multiplication derivation if and only if*

$$D = L_a - R_a + \sum_{i=1}^{m} [L_{a_i}, R_{b_i}] \tag{1}$$

for some $m \in \mathbb{N}$, a, a_i, $b_i \in A$ satisfying

$$3a + \sum_{i=1}^{m} [a_i, b_i] \in \mathrm{Nuc}(A). \tag{2}$$

Proof If D is a Lie multiplication derivation of A then $D = L_a + R_b + \sum_{i=1}^{m} [L_{a_i}, R_{b_i}]$ for some $m \in \mathbb{N}$, a, b, a_i, $b_i \in A$ and $b = -a$ since $D1_A = 0$. Therefore D is of the form (1). Now $(L_a - R_a)(xy) - ((L_a - R_a)x)y - x((L_a - R_a)y) = a(xy) - (xy)a - (ax)y + (xa)y - x(ay) + x(ya) = -[a, x, y] - [x, y, a] + [x, a, y] = [x, 3a, y]$.

On the other hand, (48.5.7) states

$$[L_a, R_b](xy) = ([L_a, R_b]x)y + x([L_a, R_b]y) + [x, [a, b], y].$$

Therefore for D as in (1),

$$D(xy) - D(x)y - xD(y) = [x, 3a + \sum_{i=1}^{m} [a_i, b_i], y]$$

for all x, $y \in A$ and (2) is equivalent to D being a derivation of A. □

48.10 Derivations of alternative algebras and exterior powers. We can restate Theorem 48.9 using exterior powers. Let

$$W(A) := A \oplus \bigwedge^2 A.$$

We introduce two linear maps on $W(A)$.

$$s\colon W(A) \to A, \qquad s((a, b \wedge c)) := 3a + [b, c] \quad a, b, c \in A.$$

By (13.1.3), the bilinear expression $[L_a, R_b]$ is alternating in a and b. Hence we can define the linear map

$$\Delta\colon W(A) \to \mathfrak{gl}(A), \quad \Delta((a, b \wedge c)) := L_a - R_a + [L_b, R_c], \quad a, b, c \in A.$$

For $x \in W(A)$, denote $\Delta(x)$ by Δ_x. In this notation, Theorem 48.9 implies

$$\mathrm{LMDer}(A) = \{\Delta_x \mid x \in W(A), s(x) \in \mathrm{Nuc}(A)\}. \tag{1}$$

Observe that every $g \in \mathfrak{gl}(A)$ induces a linear map

$$\hat{g}\colon W(A) \to W(A), \quad \hat{g}((a, b \wedge c)) := (g(a), g(b) \wedge c + b \wedge g(c))$$

for $a, b, c \in A$, thus providing an embedding of Lie algebras

$$\mathfrak{gl}(A) \to \mathfrak{gl}(W(A)).$$

48.11 Inner derivations. A homomorphism $f\colon A \to B$ of alternative algebras may fail to map the nucleus of A into the nucleus of B; for example, this happens for a quaternion subalgebra A of an octonion algebra B, with f being the inclusion (Exc. 19.32 (b)). It follows that Lie multiplication derivations of A do not necessarily extend to Lie multiplication derivations of B. We wish to avoid this difficulty by defining the *inner derivations* of A

$$\mathrm{InDer}_{\mathrm{alt}}(A) := \{\Delta_x \mid x \in W(A), s(x) = 0\}. \tag{1}$$

More explicitly they are the linear maps

$$L_a - R_a + \sum_{i=1}^{m} [L_{a_i}, R_{b_i}] \quad \text{with} \quad 3a + \sum_{i=1}^{m} [a_i, b_i] = 0.$$

48.12 Proposition (Schafer [254, p. 77])**.** *Let A be an alternative algebra and $a, b \in A$. Then*

$$\begin{aligned} D_{a,b} &:= [L_a, L_b] + [L_a, R_b] + [R_a, R_b] \\ &= L_{[a,b]} - R_{[a,b]} - 3[L_a, R_b] \\ &= \Delta([a, b], (-3a \wedge b)) \end{aligned} \tag{1}$$

is an inner derivation of A.

Proof If $x \in A$ then

$$\begin{aligned} D_{a,b}x &= a(bx) - b(ax) + a(xb) - (ax)b + (xb)a - (xa)b \\ &= -[a, b, x] + (ab)x + [b, a, x] - (ba)x - [a, x, b] \\ &\quad + [x, b, a] + x(ba) - [x, a, b] - x(ab) \\ &= L_{[a,b]}x - R_{[a,b]}x + 3[a, x, b] \end{aligned}$$

and the second equality of (1) holds. Since $s([a,b],(-3a \wedge b)) = 0$, $D_{a,b}$ is an inner derivation by Theorem 48.9. □

48.13 Various classes of inner derivations.

(a) *Commutator derivations*. Derivations of the form $L_a - R_a$ with $3a = 0$ are called *commutator derivations*. We put

$$\mathrm{ComDer}(A) = \{L_a - R_a \mid a \in A,\ 3a = 0\} = \{\Delta(a) \mid a \in A, s(a) = 0\}.$$

Nontrivial commutator derivations exist only in the presence of 3-torsion.

(b) *Associator derivations*. Derivations of the form $\sum_{i=1}^m [L_{a_i}, R_{b_i}]$ such that $\sum_{i=1}^m [a_i, b_i] = 0$ are called *associator derivations*. We put

$$\begin{aligned}\mathrm{AssDer}(A) &:= \{\sum_{i=1}^m [L_{a_i}, R_{b_i}] \mid m \in \mathbb{N},\ a_i, b_i \in A,\ \sum_{i=1}^m [a_i, b_i] = 0\} \\ &= \{\Delta(u) \mid u \in \bigwedge^2 A, s(u) = 0\}.\end{aligned}$$

Since $\sum_{i=1}^m [L_{a_i}, R_{b_i}]c = -\sum_{i=1}^m [a_i, c, b_i]$ up to a sign is a sum of associators, we have $\mathrm{AssDer}(A) = \{0\}$ if A is associative.

(c) *Standard derivations*. Linear combinations of derivations having the form $D_{a,b}$, $a, b \in A$, are called *standard derivations* of A. We denote by

$$\mathrm{StanDer}(A) = \{\sum_{i=1}^m D_{a_i,b_i} \mid m \in \mathbb{N},\ a_i, b_i \in A\} = \{\Delta(s(u), -3u) \mid u \in \bigwedge^2 A\}$$

the k-module of standard derivations of A.

48.14 Proposition. *The k-modules* $\mathrm{InDer}(A)$, $\mathrm{ComDer}(A)$, $\mathrm{AssDer}(A)$ *and* $\mathrm{StanDer}(A)$ *are ideals of* $\mathrm{Der}(A)$.

Proof This follows immediately from (48.1.2), (48.1.3), (48.1.4). □

48.15 Proposition (Schafer [254, pp. 77–78])**.** *If $D \in \mathrm{Der}(A)$ then $D_{b,a} = -D_{a,b}$ and*

$$[D, D_{a,b}] = D_{Da,b} + D_{a,Db}, \quad D_{ab,c} + D_{bc,a} + D_{ca,b} = 0$$

for all $a, b, c \in A$.

Proof The first two statements follow from (48.1.2), (48.1.3), (48.1.4). Let a, b, c, x be elements of an alternative algebra A. Then

$$[ab, c] + [bc, a] + [ca, b] = 3[a, b, c]. \tag{1}$$

Adding the following three versions of (7.5.2), using the fact that the associator is alternating,

$$\begin{aligned} x[a,b,c] + [x,a,b]c &= [xa,b,c] - [x,ab,c] + [x,a,bc], \\ -a[b,c,x] - [a,b,c]x &= -[ab,c,x] + [a,bc,x] - [a,b,cx], \\ a[x,b,c] + [a,x,b]c &= [ax,b,c] - [a,xb,c] + [a,x,bc], \end{aligned}$$

we obtain

$$[x,[a,b,c]] = [xa + ax,b,c] - 2[x,ab,c] - [x,bc,a] - [cx,a,b] - [xb,c,a].$$

Taking the sum over cyclic permutations of a, b, c, we get

$$3[x,[a,b,c]] = 3\sum_{(abc)}[ab,x,c],$$

hence

$$3[[a,b,c],x] + 3\sum_{(abc)}[ab,x,c] = 0.$$

Since $[ab,x,c] = -[L_{ab},R_c]x$, this amounts to

$$3(L_{[a,b,c]} - R_{[a,b,c]} - [L_{ab},R_c] - [L_{bc},R_a] - [L_{ca},R_b]) = 0. \tag{2}$$

Thus, (1) implies

$$\begin{aligned} D_{ab,c} + D_{bc,a} + D_{ca,b} &= L_{[ab,c]} - R_{[ab,c]} - 3[L_{ab},R_c] \\ &\quad + L_{[bc,a]} - R_{[bc,a]} - 3[L_{bc},R_a] \\ &\quad + L_{[ca,b]} - R_{[ca,b]} - 3[L_{ca},R_b] \\ &= 3L_{[a,b,c]} - 3R_{[a,b,c]} - 3[L_{ab},R_c] - 3[L_{bc},R_a] - 3[L_{ca},R_b], \end{aligned}$$

which is 0 by (2). □

It is well known that 3 plays a special role in alternative theory.

48.16 Proposition. *Let A be an alternative k-algebra.*

(a) *If* $3A = A$ *then* $\mathrm{InDer}(A) = \mathrm{StanDer}(A) + \mathrm{ComDer}(A)$.
(b) *If* $3 \in k^\times$ *then* $\mathrm{InDer}(A) = \mathrm{StanDer}(A)$.
(c) *If* $3A = \{0\}$ *then* $\mathrm{InDer}(A) = \mathrm{AssDer}(A) + \mathrm{ComDer}(A)$.

Proof Let $x = (a,u) \in W(A)$ with $s(x) = 0$. If $3A = A$ then $u = 3w$ for some $w \in \bigwedge^2 A$. So $s(u) = 3s(w)$ and $0 = s(x) = 3a + s(u) = 3a + 3s(w)$. Letting $b = a + s(w)$,

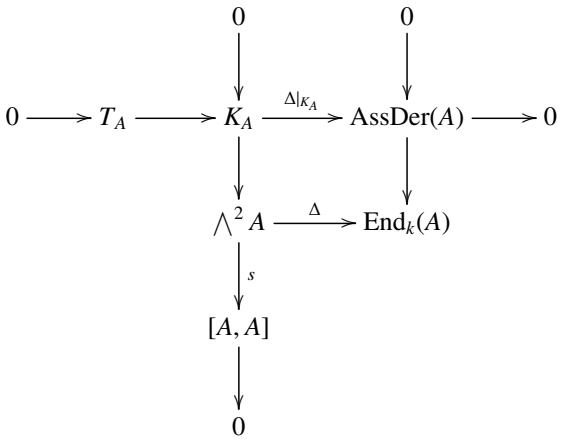
$$\Delta(x) = \Delta(-s(w),3w) + \Delta(b) \in \mathrm{StanDer}(A) + \mathrm{ComDer}(A).$$

If $3 \in k^\times$ there is no 3-torsion and $\mathrm{ComDer}(A) = \{0\}$ so $\mathrm{InDer}(A) = \mathrm{StanDer}(A)$. Finally if $3A = \{0\}$ then $s(x) = s(u) = 0$ and $\Delta(x) = \Delta(a)+\Delta(u) \in \mathrm{ComDer}(A)+\mathrm{AssDer}(A)$. □

If $3 \in k^\times$, for example if k is a field of characteristic not 3, then $\mathrm{InDer}(A) = \mathrm{StanDer}(A)$ and standard derivations suffice. In general we will need associator derivations. Let us first show that, under the identifications of 25.3, they are compatible with flat base change.

48.17 Proposition. *Let A be an alternative algebra that is finitely generated as a k-module. The associator derivations of A commute with flat base change, i.e., for all flat $R \in k$-**alg**, $\mathrm{AssDer}(A)_R = \mathrm{AssDer}(A_R)$.*

Proof Let $K_A := \mathrm{Ker}(s_A) \cap \bigwedge^2 A$ and $T_A = \mathrm{Ker}(\Delta_A)$. Taking exterior powers commutes with flat (even arbitrary) base change [28, III.7.5, Prop. 8], ergo so do the linear maps Δ_A and s_A as does $[A, A]$. By (25.3.2), $\mathrm{Ker}(s_A)$ commutes with flat base change. Therefore so does K_A. Since $\mathrm{AssDer}(A) = \{\Delta(u) \mid u \in \bigwedge^2 A, s(u) = 0\}$, Δ restricts to a surjection $\Delta|_{K_A} : K_A \to \mathrm{AssDer}(A)$ and we obtain the following commutative diagram with exact rows and columns:



Tensoring with R yields the desired result. □

The other classes of derivations we introduced also commute with flat base change, see Exc. 48.25.

48.18 Corollary. *Let A be an alternative algebra that is finitely generated as a k-module. If $\mathrm{Der}_R(A_R) = \mathrm{AssDer}_R(A_R)$ for a faithfully flat $R \in k$-**alg**, then $\mathrm{Der}_k(A) = \mathrm{AssDer}_k(A)$.*

Proof Both $\mathrm{Der}(A)$ and $\mathrm{AssDer}(A)$ are compatible with flat base change by Propositions 48.4 and 48.17, therefore

$$(\mathrm{Der}(A)/\mathrm{AssDer}(A))_R \cong \mathrm{Der}(A_R)/\mathrm{AssDer}(A_R) = 0.$$

Because R is faithfully flat, we conclude that $\mathrm{Der}(A) \cong \mathrm{AssDer}(A)$. □

To show that associator derivations arise naturally we need to consider gradings of alternative algebras.

48.19 3-gradings. Let Γ be a finite abelian group and $M = \oplus_{\gamma\in\Gamma} M_\gamma$ a Γ-graded k-module. Since Γ is finite, this induces a Γ-grading on the algebra $\mathrm{End}(M) = \oplus_{\gamma\in\Gamma}\mathrm{End}(M)_\gamma$, where $\mathrm{End}(M)_\gamma = \{f \in \mathrm{End}(M) \mid f(M_\beta) \subseteq M_{\beta+\gamma}, \forall \beta \in \Gamma\}$, and then on the Lie algebra $\mathfrak{gl}(M)$. Moreover, if M carries a non-associative k-algebra structure A, then $\mathrm{Der}(A)$ is easily seen to be a *graded* subalgebra of $\mathfrak{gl}(A)$. In particular if e is an idempotent of a unital alternative algebra A, letting $e_1 = e$, $e_2 = 1_A - e$ and $A = A_{11} \oplus A_{12} \oplus A_{21} \oplus A_{22}$ the Peirce decomposition of A with respect to e (cf. Exc. 14.12), then one checks that $A_0 = A_{11} \oplus A_{22}$, $A_1 = A_{12}$, $A_2 = A_{21}$ is a $\mathbb{Z}/3\mathbb{Z}$-grading of A. We refer to this as the *e-grading* of A and write

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$$

for the corresponding $\mathbb{Z}/3\mathbb{Z}$-grading of the derivation algebra $\mathfrak{g} = \mathrm{Der}(A)$ and call this the *e-grading* of $\mathfrak{g}$. Fixing $i, j \in \{1, 2\}$, $i \neq j$ and $u_{ij} \in A_{ij} = A_i$, it is straightforward to check, using the Peirce relations, that the derivation

$$D_i(u_{ij}) := -D_{e_i,u_{ij}} = D_{e_j,u_{ij}} \in \mathrm{StanDer}(A)$$

satisfies the relations

$$D_i(u_{ij})x_{ii} = x_{ii}u_{ij}, \tag{1}$$
$$D_i(u_{ij})x_{jj} = -u_{ij}x_{jj}, \tag{2}$$
$$D_i(u_{ij})x_{ij} = u_{ij}x_{ij}, \tag{3}$$
$$D_i(u_{ij})x_{ji} = -[u_{ij}, x_{ji}] \tag{4}$$

for all $x_{\lambda,\mu} \in A_{\lambda,\mu}$, $\lambda, \mu = 1, 2$. These and the Peirce relations yield $D_i(u_{ij}) \in \mathfrak{g}_i$, $i = 1, 2$. If $D \in \mathfrak{g}$ satisfies $D(e) = 0$ then $D(1_A - e) = 0$ and D stabilizes A_i, $i = 0, 1, 2$. So $D \in \mathfrak{g}_0$. In fact

48.20 Proposition. *Let $e \neq 0, 1$ be an idempotent of an alternative algebra A. The e-grading $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$ of $\mathfrak{g} = \mathrm{Der}(A)$ is given by*

$$\mathfrak{g}_0 = \{D \in \mathfrak{g} \mid De = 0\}, \quad \mathfrak{g}_i = \{D_i(u_{ij}) \mid u_{ij} \in A_{ij}\} \qquad (\{i, j\} = \{1, 2\}).$$

Moreover, the maps $u_{ij} \mapsto D_i(u_{ij})$ are k-module isomorphisms $A_{ij} \cong \mathfrak{g}_i$ for $i \neq j$.

Proof For any $D \in \mathfrak{g}$, $De = D(e^2) = (De)e + e(De)$. Therefore the 22 and hence the 11 Peirce components of De are 0 and $De = u_{12} + u_{21}$, for some $u_{12} \in A_{12}$, $u_{21} \in A_{21}$. Thus

$$D = D_0 + D_1 + D_2,$$

where

$$\begin{aligned} D_0 &:= D - D_1(u_{12}) + D_2(u_{21}), \\ D_1 &:= D_1(u_{12}), \\ D_2 &:= -D_2(u_{21}). \end{aligned}$$

Since $D_0(e) = 0$, we have $D_i \in \mathfrak{g}_i$, $i = 0, 1, 2$. Thus the first statement of the proposition holds. Finally, $D_i(u_{ij}) = 0$ implies $D_i(u_{ij})e_i = u_{ij} = 0$ by (48.19.1), proving the last statement. □

48.21 Corollary. *Let C be an associative composition algebra over k.*

(a) If $C = k$ or C is quadratic étale, then $\mathrm{Der}(C) = \{0\}$.

(b) If C is a quaternion algebra over k then

$$\mathrm{Der}(C) = \mathrm{InDer}_{\mathrm{ass}}(C) = \{L_a - R_a \mid a \in C\}.$$

Proof Suppose first that C is split. If $C = k$, $\mathrm{Der}(C) = \{0\}$ follows immediately from $D(1_C) = 0$. For C split quadratic étale, $C = k \times k$ and $C_{12} = \{0\} = C_{21}$. Therefore $\mathrm{Der}(C) = \mathfrak{g}_0 = \{0\}$ by Prop. 48.20.

If C is a split quaternion algebra over k, $C = \mathrm{Mat}_2(k)$. Letting $e = e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, we may consider the e-grading of C and of $\mathrm{Der}(C) = \mathfrak{g}$. For $i = 1$ or 2, $\mathfrak{g}_i = \{D_i(u_{ij}) \mid u_{ij} \in C_{ij}\}$ by Prop. 48.20. Since C is associative, up to sign, $D_i(u_{ij}) = D_{e_i,u_{ij}} = L_{[e_i,u_{ij}]} - R_{[e_i,u_{ij}]} = L_{u_{ij}} - R_{u_{ij}}$. Since $C_0 = ke_1 \oplus ke_2$, if $D \in \mathfrak{g}_0$ then the restriction $D|_{C_0} = 0$. So $D\left(\begin{smallmatrix} \alpha_1 & v \\ u & \alpha_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & D_1 v \\ D_2 u & 0 \end{smallmatrix}\right)$, where $D_i = L_{\lambda_i}$, $\lambda_i \in k$. Computing (48.1.1) for $x = \left(\begin{smallmatrix} 0 & 0 \\ u & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & v \\ 0 & 0 \end{smallmatrix}\right)$ yields $\lambda_2 = -\lambda_1$ and $D = L_{\lambda_1 e_1} - R_{\lambda_1 e_1}$. So $\mathrm{Der}(C) = \{L_a - R_a \mid a \in C\}$.

In the general case, let $R \in k$-**alg** be faithfully flat so that C_R is split. Since $\mathrm{Der}(C)$ and $\mathrm{InDer}_{\mathrm{ass}}(C)$ are compatible with flat base change (Prop. 48.4 and its proof) and R is faithfully flat, we are done by the split case. □

48.22 Remarks. (a) By Exc. 14.12, since any element $a_{ji} \in A_{ji}$, $\{i, j\} = \{1, 2\}$, squares to 0, any two elements of A_{ji} skew-commute.

(b) By left and right alternativity $a_{ij}(a_{ij}b) = a_{ij}^2 b = 0 = ba_{ij}^2 = (ba_{ij})a_{ij}$.

(c) By definition the 0-component $\mathfrak{g}_0$ is a subalgebra and $\mathfrak{g}_1, \mathfrak{g}_2$ are $\mathfrak{g}_0$-modules.

The elements of $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are obviously standard derivations. But in important cases they also turn out to be associator derivations. An explicit description of these cases will now be given.

48.23 Proposition. *Let A be a unital alternative algebra, e an idempotent of A and $A = A_0 \oplus A_1 \oplus A_2$ the e-grading of A. Let $i, j \in \{1, 2\}$ be distinct and $u_{ji}, v_{ji} \in A_{ji}$. Then the derivation $D_i(u_{ji}v_{ji})$ is in* AssDer(A).

Proof Let

$$D := 2[L_{e_i}, R_{u_{ji}v_{ji}}] - [L_{u_{ji}}, R_{v_{ji}}].$$

By Remark 48.22 (a),

$$2[e_i, u_{ji}v_{ji}] - [u_{ji}, v_{ji}] = 2u_{ji}v_{ji} - 0 - u_{ji}v_{ji} + v_{ji}u_{ji} = 0$$

and $D \in$ AssDer(A). To show that $D_i(u_{ji}v_{ji}) = D$ and hence that $D_i(u_{ji}v_{ji}) \in$ AssDer(A), it suffices to show that they have the same action on arbitrary elements of A_{lk}, $l, k \in \{1, 2\}$.

The identities (48.19.1)–(48.19.4) as well as the Peirce multiplication rules will be used throughout without further reference. The linearization of left alternativity (13.2.1) yields

$$\begin{aligned} Dx_{ii} &= 2e_i((x_{ii}(u_{ji}v_{ji})) - 2(e_ix_{ii})(u_{ji}v_{ji}) - u_{ji}(x_{ii}v_{ji}) + (u_{ji}x_{ii})v_{ji} \\ &= (u_{ji}x_{ii} + x_{ii}u_{ji})v_{ji} = u_{ji}(x_{ii}v_{ji}) + x_{ii}(u_{ji}v_{ji}) \\ &= D_i(u_{ji}v_{ji})x_{ii}. \end{aligned}$$

Similarly, using the linearization of right alternativity (13.2.2), we obtain

$$\begin{aligned} Dx_{jj} &= 2e_i(x_{jj}(u_{ji}v_{ji})) - 2(e_ix_{jj})(u_{ji}v_{ji}) - u_{ji}(x_{jj}v_{ji}) + (u_{ji}x_{jj})v_{ji} \\ &= -u_{ji}(x_{jj}v_{ji} + v_{ji}x_{jj}) = -(u_{ji}x_{jj})v_{ji} - (u_{ji}v_{ji})x_{jj} \\ &= D_i(u_{ji}v_{ji})x_{jj}. \end{aligned}$$

Using the linearization of Remark 48.22 (b),

$$\begin{aligned} Dx_{ji} &= 2e_i(x_{ji}(u_{ji}v_{ji})) - 2(e_ix_{ji})(u_{ji}v_{ji}) - u_{ji}(x_{ji}v_{ji}) + (u_{ji}x_{ji})v_{ji} \\ &= x_{ji}(u_{ji}v_{ji}) - (u_{ji}v_{ji})x_{ji} = -[u_{ji}v_{ji}, x_{ji}] \\ &= D_i(u_{ji}v_{ji})x_{ji}. \end{aligned}$$

Finally, using the fact that the associator is alternating and (13.2.2),

$$\begin{aligned} Dx_{ij} &= 2e_i(x_{ij}(u_{ji}v_{ji})) - 2(e_ix_{ij})(u_{ji}v_{ji}) - u_{ji}(x_{ij}v_{ji}) + (u_{ji}x_{ij})v_{ji} \\ &= -2x_{ij}(u_{ji}v_{ji}) - u_{ji}(x_{ij}v_{ji}) + (u_{ji}x_{ij})v_{ji} \\ &= -2(x_{ij}u_{ji})v_{ji} - 2(u_{ji}x_{ij})v_{ji} + 2u_{ji}(x_{ij}v_{ji}) - u_{ji}(x_{ij}v_{ji}) + (u_{ji}x_{ij})v_{ji} \\ &= u_{ji}(x_{ij}v_{ji}) - (u_{ji}x_{ij})v_{ji} = u_{ji}(v_{ji}x_{ij} + x_{ij}v_{ji}) - (u_{ji}x_{ij})v_{ji} = (u_{ji}v_{ji})x_{ij} \\ &= D_i(u_{ji}v_{ji})x_{ij}. \end{aligned}$$

Therefore $D_i(u_{ji}v_{ji}) = D$. □

48.24 Corollary. *The* $\mathfrak{g}_0$*-modules* $\mathfrak{g}_1$ *and* $\mathfrak{g}_2$ *are contained in* StanDer(A). *If* $A_{ij} = A_{ji}^2$, *then* $\mathfrak{g}_i \subseteq \mathrm{AssDer}(A)$ *for* $i = 1, 2$. □

Exercises

48.25. Show that if an alternative algebra A is finitely generated as a k-module the Lie algebras LMDer(A), InDer(A), ComDer(A) and StanDer(A) commute with flat base change. That is, show that for all flat $R \in k$-**alg**:

(a) $\mathrm{LMDer}(A)_R = \mathrm{LMDer}(A_R)$;
(b) $\mathrm{InDer}(A)_R = \mathrm{InDer}(A_R)$;
(c) $\mathrm{ComDer}(A)_R = \mathrm{ComDer}(A_R)$; and
(d) $\mathrm{StanDer}(A)_R = \mathrm{StanDer}(A_R)$.

49 Derivations of octonions

In 48.13, we have encountered various classes of inner derivations for unital alternative algebras. These classes will now be investigated more closely in the important special case of octonion algebras, where we will realize all derivations as inner derivations of a specific type. The idea to achieve this objective with standard derivations, however, is doomed to failure since, given an octonion algebra C over a field of characteristic 3, StanDer(C) turns out to be a seven-dimensional proper ideal in the full derivation algebra (49.7).

Associator derivations to the rescue! We will show in Thm. 49.5 below that every derivation of an octonion algebra over any commutative ring is an associator derivation. The proof will be based on our results on e-gradings, which can be achieved since any octonion algebra is split by a suitable faithfully flat extension (Cor. 26.9), and both the full derivation algebra and the algebra of associator derivations behave nicely under such extensions (Cor. 48.18).

49.1 Derivations and the norm. Let C be a conic algebra over k, $\mathfrak{g} = \mathrm{Der}(C)$,

$D \in \mathfrak{g}$ and $k[\varepsilon]$, the algebra of dual numbers. The map $\mathbf{1} + \varepsilon D$ is an automorphism of $C_{k[\varepsilon]}$ by Example 48.2, and hence leaves the norm and trace of $C_{k[\varepsilon]}$ invariant (Prop. 16.16). In particular

$$n_C(x, Dx) = 0 \quad \forall x \in C, \tag{1}$$
$$t_C(Dx) = 0 \quad \forall x \in C. \tag{2}$$

So $\mathfrak{g} \subseteq \mathfrak{o}(C, n_C)$, the orthogonal Lie algebra of (C, n_C). As in 16.6, let C^0 be the submodule of trace-zero elements in C . By (2), $\mathfrak{g}C^0 \subseteq C^0$ and, writing n_C^0 for $n_C|_{C^0}$, we have $\mathfrak{g} \subseteq \mathfrak{o}(C^0, n_C^0)$.

49.2 Reduced octonion algebras. Let C be a reduced octonion algebra over k. Then C is a twisted Zorn vector matrix algebra (22.14), that is,

$$C = \mathrm{Zor}(M, \theta) = \begin{pmatrix} k & M^* \\ M & k \end{pmatrix},$$

where M is a finitely generated projective k-module of rank 3, and θ is an orientation of M. The product is given by (22.14.3).

For $g \in \mathrm{End}_k(M)$, let $g^* \in \mathrm{End}_k(M^*)$ be the dual of g, so with respect to the canonical pairing

$$M^* \times M \longrightarrow k, \quad (x^*, y) \longmapsto \langle x^*, y \rangle,$$

we have $\langle g^*(w^*), x\rangle = \langle w^*, g(x)\rangle$, for all $x \in M$, $w^* \in M^*$. Then (22.14.2) implies

$$\begin{aligned} \langle g(x) \times_\theta g(y), g(z)\rangle &= \theta(g(x) \wedge g(y) \wedge g(z)) \\ &= \det(g)\theta(x \wedge y \wedge z) = \det(g)\langle x \times_\theta y, z\rangle \end{aligned}$$

for all $x, y, z \in M$. Differentiating at $\mathbf{1}_M$ in the direction $g \in \mathrm{End}_k(M)$ yields

$$\langle g(x) \times_\theta y, z\rangle + \langle x \times_\theta g(y), z\rangle + \langle x \times_\theta y, g(z)\rangle = \mathrm{tr}(g)\langle x \times_\theta y, z\rangle$$

or, since $\langle -, -\rangle$ is regular,

$$-g^*(x \times_\theta y) = g(x) \times_\theta y + x \times_\theta g(y) - \mathrm{tr}(g)x \times_\theta y. \tag{1}$$

Consider the canonical identification of $M^* \otimes M$ with $\mathrm{End}_k(M)$ via

$$(v^* \otimes u)(x) = \langle v^*, x\rangle u \qquad \text{for any } u, x \in M,\ v^* \in M^*, \tag{2}$$

and of $M \otimes M^*$ with $\mathrm{End}_k(M^*)$ via $u \otimes v^* \colon y^* \mapsto \langle y^*, u\rangle v^*$. One checks that $(v^* \otimes u)^* = u \otimes v^*$. Since

$$\mathrm{tr}(v^* \otimes u) = \langle v^*, u\rangle = \mathrm{tr}(u \otimes v^*), \tag{3}$$

we conclude

$$\operatorname{tr}(g) = \operatorname{tr}(g^*) \tag{4}$$

for any $g \in \operatorname{End}_k(M)$.

Now let $e = e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $e_2 = 1_C - e_1$. Consider the e-grading of $\operatorname{Der}(C) = \mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$.

49.3 Proposition. *If $C = \operatorname{Zor}(M, \theta)$ is a reduced octonion algebra over k and $\operatorname{Der}(C) = \mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$ as above, then the Lie subalgebra $\mathfrak{g}_0$ of $\mathfrak{g}$ is isomorphic to $\mathfrak{sl}(M) := \{g \in \operatorname{End}_k(M) \mid \operatorname{tr}(g) = 0\}$ via the map $\phi\colon \mathfrak{sl}(M) \to \mathfrak{g}_0$ given by*

$$\phi(g)\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} := \begin{pmatrix} 0 & -g^* v^* \\ gv & 0 \end{pmatrix}. \tag{1}$$

Proof For $D \in \mathfrak{g}_0$,

$$D\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} = \begin{pmatrix} 0 & D_1 v^* \\ D_2 v & 0 \end{pmatrix}, \tag{2}$$

where $D_1 \in \operatorname{End}(M^*)$ and $D_2 \in \operatorname{End}(M)$.

For $x = \left(\begin{smallmatrix} 0 & 0 \\ u & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & v^* \\ 0 & 0 \end{smallmatrix}\right)$, (48.1.1) and $De_2 = 0$ yield $0 = \langle v^*, D_2 u\rangle + \langle D_1 v^*, u\rangle$. Hence

$$D_1 = -D_2^*. \tag{3}$$

For $x = \left(\begin{smallmatrix} 0 & 0 \\ u & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & 0 \\ v & 0 \end{smallmatrix}\right)$, (48.1.1) yields

$$-D_2^*(u \times_\theta v) = (D_2 u) \times_\theta v + u \times_\theta D_2 v. \tag{4}$$

Comparing with (49.2.1), this is equivalent to $\operatorname{tr}(D_2) u \times_\theta v = 0$ for all $u, v \in M$. Recall from 22.14 that $\langle u \times_\theta v, w\rangle = \theta(u \wedge v \wedge w)$ and $\theta\colon \bigwedge^3 M \xrightarrow{\sim} k$. Therefore

$$\operatorname{tr}(D_2) = 0. \tag{5}$$

Note that if D_1, D_2 satisfy (3), (4) and (5) then to show that D as in (2) is a derivation of C we only need the relation $D_2(v^* \times_\theta w^*) = (D_1 v^*) \times_\theta w^* + v^* \times_\theta (D_1 w^*)$. This in turn will follow from (49.2.1) once we know $\operatorname{tr}(D_2^*) = 0$, which is clear since $\operatorname{tr}(g) = \operatorname{tr}(g^*)$ for all linear endomorphisms of a finitely generated projective k-module (49.2.4).

By definition $\phi(g)(e_i) = 0$ and $D = \phi(g)$ satisfies (3). Since $g \in \mathfrak{sl}(M)$, by (49.2.1) $\phi(g)$ satisfies (4) and therefore $\phi(g) \in \mathfrak{g}_0$. Bijectivity is obvious. □

49.4 Corollary. *For every octonion algebra C over a ring k, $\operatorname{Der}(C)$ is finitely generated projective of rank 14 as a k-module.*

Proof Making C reduced after a faithfully flat base change, combine Propositions 48.20 and 49.3 to see that $\mathrm{Der}(C) \cong \mathfrak{sl}_3(k) \oplus M \oplus M^*$ as a k-module. □

49.5 Theorem (Loos-Petersson-Racine [176, Thm. 5.1])**.** *Every derivation of an octonion algebra C is an associator derivation, i.e.,* $\mathrm{AssDer}(C) = \mathrm{Der}(C)$.

Proof By Corollaries 26.9 and 48.18, we may assume that C is split. The following argument works more naturally by merely assuming that C be reduced, as above. As shown in 22.14, locally, M is free and a basis can be chosen such that $\times_\theta$ is the classical vector product $\times$ and

$$C_{ji}^2 = C_{ij} \qquad \{i, j\} = \{1, 2\}.$$

So Cor. 48.24 holds and $\mathfrak{g}_i \subset \mathrm{AssDer}(C)$, $i = 1, 2$. Therefore it remains to prove that $\mathfrak{g}_0 \subset \mathrm{AssDer}(C)$. Recall the canonical identification of $M^* \otimes M$ with $\mathrm{End}(M)$ (49.2.2). Let

$$a = \begin{pmatrix} 0 & 0 \\ u & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & v^* \\ 0 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \in C. \tag{1}$$

Using (22.14.3) one computes

$$[a, b] = \langle v^*, u\rangle(e_1 - e_2),\ [L_a, R_b]e_1 = 0,\ [L_a, R_b]c = \begin{pmatrix} 0 & 0 \\ -(u \times_\theta x) \times_\theta v* & 0 \end{pmatrix}. \tag{2}$$

Now by the first of the Grassmann identities of Exc. 22.29,

$$-(u \times_\theta x) \times_\theta v* = \langle v^*, x\rangle u - \langle v^*, u\rangle x = (v^* \otimes u - \langle v^*, u\rangle \mathbf{1}_M)x \tag{3}$$

in the identification of (49.2.2). With the same identification, any $g \in \mathfrak{sl}(M)$ corresponds to some $\sum_i v_i^* \otimes u_i$ of trace 0 (49.2.3). Letting

$$a_i = \begin{pmatrix} 0 & 0 \\ u_i & 0 \end{pmatrix}, \quad b_i = \begin{pmatrix} 0 & v_i^* \\ 0 & 0 \end{pmatrix},$$

the derivation $\phi(g) = \sum_i [L_{a_i}, R_{b_i}]$ is an associator derivation by (2) and (3). □

49.6 Corollary. *If 3 is invertible in k, then every derivation of an octonion algebra C over k is standard, i.e., it is a sum of derivations $D_{a,b}$, $a, b \in C$.*

Proof We have in general $\mathrm{AssDer}(C) \subseteq \mathrm{InDer}(C) \subseteq \mathrm{Der}(C)$, with equality by the theorem and $\mathrm{InDer}(C) = \mathrm{StanDer}(C)$ by Prop. 48.16. □

Over fields of characteristic not 2 and 3, the preceding result is due to Schafer [254, III, Cor. 3.29].

49.7 Derivation algebra of octonions over a field. The derivation algebra

$\mathrm{Der}(C)$ of an octonion algebra C over a field k has been studied in many places. For example, using the language of octonion algebras, as we do here, see [132], [1], and [46]. An alternative is to use the language of group schemes, as we do in the next chapter, for which see [121], [123], and [233, §1]. (We will see in Thm. 53.1 and 53.14 that $\mathrm{Der}(C)$ is the Lie algebra of a simple group scheme of type G_2.) The group scheme results provide a general context for the fact that $\mathrm{Der}(C)$ is simple if and only if $\mathrm{char}(k) \neq 3$, which we now prove.

49.8 Proposition. *The derivation algebra* $\mathrm{Der}(C)$ *of an octonion algebra* C *over a field* k *of characteristic not 3 is a simple Lie algebra.*

Proof We may assume that $C = \mathrm{Zor}(k)$ is split so for $\mathfrak{g} := \mathrm{Der}(C)$,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$$

has a $\mathbb{Z}/3\mathbb{Z}$-grading (Prop. 48.20). By Exc. 49.11 and the characterization of $\mathfrak{g}_1$ and $\mathfrak{g}_2$ in the proof of Proposition 48.20, $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are irreducible $\mathfrak{g}_0$-modules and $\mathfrak{g}$ is a direct sum of inequivalent irreducible $\mathfrak{g}_0$-modules.

Let $\mathfrak{i}$ be an ideal of $\mathfrak{g}$. Since the characteristic is not 3, $\mathfrak{g}_0 \cong \mathfrak{sl}_3(k)$ is simple so if $\mathfrak{i} \cap \mathfrak{g}_0 \neq \{0\}$ then $\mathfrak{g}_0 \subseteq \mathfrak{i}$. In that case, using Exc. 49.11 and the characterization of $\mathfrak{g}_1$ and $\mathfrak{g}_2$, we have $\mathfrak{g}_1 \oplus \mathfrak{g}_2 \subseteq \mathfrak{i}$ and $\mathfrak{i} = \mathfrak{g}$. If $\mathfrak{i} \cap \mathfrak{g}_0 = \{0\}$, since $\mathfrak{i}$ is a $\mathfrak{g}_0$-submodule of $\mathfrak{g}$, $\mathfrak{i} = \mathfrak{g}_1$, $\mathfrak{g}_2$ or $\mathfrak{g}_1 \oplus \mathfrak{g}_2$. Since none of these are ideals, we are done. □

If k is of characteristic 3 then by Proposition 48.12, a standard derivation $D_{a,b}$ has the form

$$D_{a,b} = L_{[a,b]} - R_{[a,b]}$$

and $\mathrm{StanDer}(C)$ is an ideal of $\mathrm{Der}(C)$ of dimension 7 since $[C, C] = C^0$. Since $\mathrm{Der}(C)$ has dimension 14, this is a proper ideal and $\mathrm{Der}(C)$ is not simple. In fact one can show that $\mathrm{StanDer}(C)$ is a simple Lie algebra and that $\mathrm{Der}(C)/\mathrm{StanDer}(C) \cong \mathrm{StanDer}(C)$.

If k is a field of characteristic 2, the special linear Lie algebra $\mathfrak{sl}_{2n}(k)$ defined in Exc. 47.18 is not simple because $k\mathbf{1}$ is a central ideal. Instead, $\mathfrak{psl}_{2n}(k) := \mathfrak{sl}_{2n}(k)/k\mathbf{1}$ is simple for $n > 2$. It is sometimes called the classical Lie algebra of type A_{2n-1}.

49.9 Proposition. *The derivation algebra* $\mathrm{Der}(C)$ *of an octonion algebra* C *over a field* k *of characteristic 2 is isomorphic to* $\mathfrak{psl}_4(k)$ *and hence depends only on the field* k *and not on* C.

This can be seen by examining the multiplication table, which is the method suggested in [272, p. 1121]. Instead, we follow the argument from [46].

Proof Put $\mathfrak{g} := \mathrm{Der}(C)$. In general, $\mathfrak{g} \subseteq \mathfrak{o}(C^0, n_{C^0})$ (49.1). If the characteristic is 2, $1_C \in C^0$ and since $\mathfrak{g}(1_C) = \{0\}$, $\widetilde{C^0} := C^0/k1_C$ is also a $\mathfrak{g}$-module. Denote $D \in \mathfrak{g}$ acting on $\widetilde{C^0}$ by $\widetilde{D}$. The non-degenerate symmetric bilinear form $n_C(x, y)$ is alternating. Since $n_C(1_C, 1_C) = 0 = n_C(x, 1_C)$ for $x \in C^0$, the restriction of the bilinear form to C^0 has radical $k1_C$, and n_C induces an alternating form $\widetilde{n}_C$ on $\widetilde{C^0}$.

If C is split, then $C_{12} \oplus C_{21}$ is a hyperbolic space of dimension 6 isomorphic to $\widetilde{C^0}$ and $\widetilde{n}_C$ is non-degenerate. For general C, since $\widetilde{n}_C$ is non-degenerate over an extension field of k, it is non-degenerate over k. We obtain a map

$$\phi\colon \mathfrak{g} \to \mathfrak{sp}(\widetilde{C^0}, \widetilde{n}_C), \qquad D \mapsto \widetilde{D},$$

a homomorphism of Lie algebras, where the codomain was defined in Example 47.14. Now, $\widetilde{n}_C$ is a non-degenerate alternating bilinear form and all such forms are isomorphic, so $\mathfrak{sp}(\widetilde{C^0}, \widetilde{n}_C) \cong \mathfrak{sp}_6(k)$. Since $\mathfrak{g}$ is simple ϕ is injective and the second derived power $\mathfrak{g}^{(2)} := [[\mathfrak{g}, \mathfrak{g}], [\mathfrak{g}, \mathfrak{g}]]$ equals $\mathfrak{g}$. So

$$\phi(\mathfrak{g}) = \phi(\mathfrak{g}^{(2)}) \subseteq \mathfrak{sp}((\widetilde{C^0}, \widetilde{n}_C)^{(2)} \cong \mathfrak{sp}_6(k)^{(2)}.$$

This last algebra is isomorphic to $\mathfrak{psl}_4(k)$ by Exercises 47.19 and 47.20(c). Since $\mathfrak{g}$ is of dimension 14 (Cor. 49.4) while $\mathfrak{psl}_4(k)$ has dimension $15 - 1 = 14$ we obtain the desired isomorphism. □

In contrast to the conclusion of the proposition, if k has characteristic $\neq 2$, then the isomorphism class of $\mathrm{Der}(C)$ determines the octonion algebra C, see Prop. 55.7.

Exercises

49.10. Verify: For every octonion k-algebra C, the subspace $[C, C]$ generated by the commutators equals C^0, the trace 0 elements.

49.11. Let $C = \mathrm{Zor}(k)$, k a field of characteristic not 3, $e = e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\mathrm{Der}(C) = \mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2$ the e-grading of $\mathrm{Der}(C)$ as in Prop. 48.20. By Prop. 49.3, the Lie subalgebra $\mathfrak{g}_0$ of $\mathfrak{g}$ is isomorphic to $\mathfrak{sl}(M) := \{g \in \mathrm{End}_k(M) \mid \mathrm{tr}(g) = 0\}$ via the map $\phi\colon \mathfrak{sl}(M) \to \mathfrak{g}_0$ given by

$$\phi(g)\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} := \begin{pmatrix} 0 & -g^*v^* \\ gv & 0 \end{pmatrix}.$$

Show that the two representations of $\mathfrak{sl}_3(k)$ above are faithful irreducible and inequivalent.

50 Lie algebras obtained from a Jordan algebra

Our presentation of the results concerning Lie algebras obtained from Jordan algebras is inspired by Jacobson's books [138] and [140].

50.1 The structure Lie algebra of a Jordan algebra. We let J be a Jordan algebra over k and denote by $\mathfrak{str}(J)$, or by $\mathfrak{str}_k(J)$ to indicate dependence on k, the k-module of all k-linear maps $A\colon J \to J$ such that there exists a k-linear map $A'\colon J \to J$ satisfying

$$AU_x + U_xA' = U_{x,Ax} \tag{1}$$

for all $x \in J$. Letting $x = 1_J$, $A + A' = U_{1_J,A1_J}$. So

$$A' = V_{A1_J} - A \tag{2}$$

is uniquely determined by (1). Equation (1) linearizes to

$$AU_{x,y} + U_{x,y}A' = U_{Ax,y} + U_{x,Ay}. \tag{3}$$

which is equivalent to

$$[A, V_{x,z}] = V_{Ax,z} - V_{x,A'z}. \tag{4}$$

50.2 Proposition. *The k-module $\mathfrak{str}(J)$ is a subalgebra of $\mathfrak{gl}(J)$ and in particular a Lie algebra. Moreover, we have*

$$[A, B]' = -[A', B'] \qquad (A, B \in \mathfrak{str}(J)). \tag{1}$$

Proof For A, $B \in \mathfrak{str}(J)$ and $x \in J$, using (50.1.1) and (50.1.3),

$$\begin{aligned}[A, B]U_x &= U_x[A', B'] + AU_{x,Bx} + U_{x,Bx}A' - BU_{x,Ax} - U_{x,Ax}B'\\ &= U_x[A', B'] + U_{Ax,Bx} + U_{x,ABx} - U_{Bx,Ax} - U_{x,BAx}\\ &= U_x[A', B'] + U_{x,[A,B]x}.\end{aligned}$$

So $[A, B] \in \mathfrak{str}(J)$, and (1) holds. □

50.3 The Derivation Algebra of a Jordan algebra J. A *derivation* of J is an element $D \in \mathfrak{str}(J)$ such that $D1_J = 0$. By (50.1.2),

$$D' = -D \tag{1}$$

for a derivation D. Condition (50.1.1) becomes more suggestive if we write it

$$[D, U_x] = U_{Dx,x}, \tag{2}$$

$$D1_J = 0 \tag{3}$$

for all $x \in J$, which linearizes to

$$[D, U_{x,y}] = U_{Dx,y} + U_{x,Dy}. \tag{4}$$

So if D is a derivation, (4) can be written as

$$D\{x, z, y\} = \{Dx, z, y\} + \{x, Dz, y\} + \{x, z, Dy\} \tag{5}$$

and the derivation D behaves as one expects on the triple products. Putting $z = 1_J$,

$$D(x \circ y) = (Dx) \circ y + x \circ Dy \qquad \text{or} \qquad [D, V_x] = V_{Dx}. \tag{6}$$

Letting (2) act on 1_J,

$$D(x^2) = x \circ D(x). \tag{7}$$

Rewriting (5) in operator form, we obtain

$$[D, V_{x,z}] = V_{Dx,z} + V_{x,Dz}. \tag{8}$$

We put $\mathrm{Der}(J)$ for the subalgebra of $\mathfrak{str}(J)$ consisting of derivations.

Derivations were defined in §48 for arbitrary non-associative algebras over a ring k and hence for linear Jordan algebras. If $2 \in k^\times$ then $L_x := \frac{1}{2}V_x$ endows J with a linear Jordan algebra structure. If $D \in \mathrm{Der}(J)$ then (6) shows that D is a derivation of J as a linear Jordan algebra. Conversely if J is a linear Jordan algebra and $[D, L_x] = L_{Dx}$ for all $x \in J$ one checks that (2) holds for $U_x = 2(L_x)^2 - L_{x^2}$. So if $2 \in k^\times$, the above definition of a derivation of a quadratic Jordan algebra is equivalent to the usual definition for unital linear Jordan algebras.

In view of Proposition 48.4 one expects $\mathrm{Der}(J)$ and $\mathfrak{str}(J)$ to be compatible with flat base change.

50.4 Proposition. *Let J be a Jordan algebra over k. If J is finitely generated projective as a k-module and $R \in k$-**alg** a flat extension of k then $(\mathfrak{str}_k(J))_R \cong \mathfrak{str}_R(J_R)$ and $(\mathrm{Der}_k(J))_R \cong \mathrm{Der}_R(J_R)$.*

Proof Denote by $QL_k(J \times J)$ the k-module of quadratic-linear maps (over k) from $J \times J$ to J, i.e., maps that are quadratic in the first variable and linear in the second. Scalar extensions of quadratic-linear maps exist by Exc. 11.34.

Let $s : \mathrm{End}_k(J) \to QL_k(J \times J)$ be the unique linear map satisfying

$$s(f)(a, b) = f(U_a b) - U_a f(b) + U_a V_{f(1_J)} b - U_{a,f(a)} b.$$

By (50.1.1) and (50.1.2), we have $\mathrm{Ker}(f) = \mathfrak{str}_k(J)$, and (11.34.1) implies $s(f_R) = s(f)_R$. From (25.3.1) we therefore deduce $\mathfrak{str}_R(J_R) = \mathfrak{str}_k(J)_R$, as

claimed. Since $\mathrm{Der}_R(J_R) = \{f \in \mathfrak{str}_R(J_R) \mid f(1_{J_R}) = 0\}$ and $1_{J_R} = 1_J \otimes 1_R$ we also have the result for $\mathrm{Der}_k(J)$. □

We next identify a large class of elements of $\mathfrak{str}(J)$.

50.5 Proposition. *If J is a Jordan k-algebra then $V_{a,b} \in \mathfrak{str}(J)$ for any $a, b \in J$ with $V_{a,b}{}' := V_{b,a}$. In particular $V_a \in \mathfrak{str}(J)$ for all $a \in J$. If $A \in \mathfrak{str}(J)$ then $A' \in \mathfrak{str}(J)$ and $\theta\colon \mathfrak{str}(J) \to \mathfrak{str}(J)$ given by $A^\theta := -A'$ is an automorphism of period 2 of $\mathfrak{str}(J)$.*

Proof Letting $V_{a,b}{}' := V_{b,a}$, (29a.26) becomes (50.1.1) and $V_{a,b} \in \mathfrak{str}(J)$. If $A \in \mathfrak{str}(J)$ then $A' = V_{A1_J} - A \in \mathfrak{str}(J)$ since $V_{A1_J} = V_{1_J,A1_J} \in \mathfrak{str}(J)$, (50.1.2). The map θ is easily seen to be of period 2, and by (50.2.1) it is an automorphism. □

We denote by $\mathfrak{instr}(J)$ the submodule of $\mathfrak{str}(J)$ spanned by the $V_{a,b}$, $a, b \in J$. By (50.1.4), $\mathfrak{instr}(J)$ is an ideal of $\mathfrak{str}(J)$ called the *inner structure algebra* of J. Absorbing the coefficients in the a's, a typical element of $\mathfrak{instr}(J)$ can be written as $\sum_i V_{a_i,b_i}$. The element $\sum_i V_{a_i,b_i}$ annihilates 1_J if and only if $\sum_i a_i \circ b_i = 0$. By (50.3.8) these span an ideal of $\mathrm{Der}(J)$ the *inner derivation algebra*:

$$\mathrm{InDer}(J) = \{\textstyle\sum_i V_{a_i,b_i} \mid \sum_i a_i \circ b_i = 0\}. \tag{1}$$

50.6 Corollary. *If J is a Jordan k-algebra, then for any $a, b \in J$,*

$$D_{a,b} := V_{a,b} - V_{b,a}$$

is a derivation of J, and we have

$$[D, D_{a,b}] = D_{Da,b} + D_{a,Db}$$

for all $D \in \mathrm{Der}(J)$. In particular, the submodule $\mathrm{StanDer}(J)$ of $\mathrm{Der}(J)$ spanned by $D_{a,b}$, $a, b \in J$, is an ideal of $\mathrm{Der}(J)$. □

The elements of $\mathrm{StanDer}(J)$ are called *standard derivations*. Note that $D_{a,b} = [V_a, V_b]$ by (29a.12).

50.7 Examples. (1) If J is special, say J is a subalgebra of $A^{(+)}$, for A a unital associative algebra, then, for any $a, b \in J$, $D_{a,b} = L_{[a,b]} - R_{[a,b]}$ on J, so $D_{a,b}$ extends to a derivation of A. If $D \in \mathrm{Der}(A)$ stabilizes J then D restricts to a derivation of J. We will see in Cor. 51.3 that for an important class of special Jordan algebras, any $D \in \mathrm{Der}(J)$ extends to a unique derivation D' of the associative algebra A. In that case $\mathrm{Der}(J) = \{D'|_J \mid D' \in \mathrm{Der}(A),\ D'(J) \subseteq J\}$.

(2) If (A, ι) is an associative algebra with involution then $\mathrm{Sym}(A, \iota)$ is a subalgebra of $A^{(+)}$, $[\mathrm{Skew}(A, \iota), \mathrm{Sym}(A, \iota)] \subseteq \mathrm{Sym}(A, \iota)$, and $\{E_a \mid a \in \mathrm{Skew}(A, \iota)\} \subseteq \mathrm{Der}(\mathrm{Sym}(A, \iota))$.

(3) Just as the prime 3 gives rise to special behavior for derivations of alternative algebras, we expect that 2 will do so for derivations of Jordan algebras. In general $V_x \in \mathfrak{str}(J)$ (Prop. 50.5). If $2J = \{0\}$ then $V_x 1_J = 2x = 0$ for all $x \in J$ and $V_J \subseteq \mathrm{Der}(J)$. Since $V'_x = V_x$, if $D \in \mathrm{Der}(J)$, $[D, V_x] = [D, U_{x,1_J}] = U_{Dx,1_J} + U_{x,D1_J} = V_{Dx}$ by (50.3) and V_J is an ideal of $\mathrm{Der}(J)$.

(4) A *2-Lie algebra* [135, p. 187], is a Lie algebra $\mathfrak{L}$ over a ring k such that $2\mathfrak{L} = \{0\}$ endowed with an operation $^{[2]} : \mathfrak{L} \to \mathfrak{L}$, $x \mapsto x^{[2]}$ which is quadratic, i.e., for all $\alpha \in k$, $x, y \in \mathfrak{L}$

$$\begin{aligned} (\alpha x)^{[2]} &= \alpha^2 x^{[2]}, \\ (x+y)^{[2]} &= x^{[2]} + [x,y] + y^{[2]}, \quad \text{and} \\ [x^{[2]}, y] &= [x,[x,y]]. \end{aligned}$$

If $2J = \{0\}$ then J is not only a Jordan algebra but also a 2-Lie algebra [137, Thm. 4 in §1.4]. Let $L = L(J) = J$ as a k-module with $[x,y] := x \circ y$ and $x^{[2]} := x^2$, the square in J. The last equation follows from (29.2.10).

(5) Let $\mathbb{O}$ be the Graves-Cayley octonions and u_i, $0 \le i \le 7$ a Cartan-Schouten basis of $\mathbb{O}$ (2.1). Let D_{u_1,u_2} be the standard derivation of $\mathbb{O}^{(+)}$. One checks that

$$D_{u_1,u_2}(u_3u_5) - (D_{u_1,u_2}u_3)u_5 - u_3 D_{u_1,u_2}u_5 = -4u_1,$$

so D_{u_1,u_2} is a derivation of $\mathbb{O}^{(+)}$ but not a derivation of $\mathbb{O}$.

50.8 Proposition. *Let J be a Jordan k-algebra. If J is finitely generated projective as a k-module then the Lie algebras* $\mathfrak{instr}(J)$, $\mathrm{InDer}(J)$, *and* $\mathrm{StanDer}(J)$ *are compatible with flat base change.*

Proof The linear map $\nu\colon J \otimes J \to \mathrm{End}_k(J)$ given by $\nu(a \otimes b) := V_{a,b}$ has image $\mathfrak{instr}(J)$, so $\mathfrak{instr}(J)$ is compatible with flat base change by (25.3.3). Similarly, $\mathrm{StanDer}(J)$ is also the image of a linear map $J \otimes J \to \mathrm{End}_k(J)$, so it too is compatible with flat base change.

Let $c : J \otimes J \to J$ be the linear map defined by $c(a \otimes b) := a \circ b$. Then $\mathrm{Ker}(c)$ is compatible with flat base change, and $\mathrm{InDer}(J)$ is the image of $\nu\colon \mathrm{Ker}(c) \to \mathrm{End}_k(J)$, so $\mathrm{InDer}(J)$ is also compatible with flat base change. □

51 Derivations of Freudenthal algebras

In the preceding section, we defined a number of Lie algebras obtained from Jordan algebras. We are interested in identifying those Lie algebras when the Jordan algebra is a Freudenthal algebra. Since the derivation algebra of a Freudenthal algebra J is stable under flat base change (Prop. 50.4) and J can be split

by a faithfully flat base change (Cor. 39.32), many proofs can be reduced to the split case. For example:

51.1 Lemma. *If J is a Freudenthal algebra over k of rank* 1 *or* 3*, then* $\mathrm{Der}(J) = \{0\}$.

Proof A Freudenthal algebra of rank 1 is $k^{(+)}$, and it immediately follows from (50.3.3) that $\mathrm{Der}(k^{(+)}) = \{0\}$.

For the case of rank 3, we may assume that $J = (k \times k \times k)^{(+)}$. For any $D \in \mathrm{Der}(J)$, by (50.3.7), $De_i = D(e_i^2) = e_i \circ De_i$, and (32.2.7) implies $De_i \in J_1(e_i) = \{0\}$. □

To treat the Freudenthal algebras of rank 6, 9, or 15, we will need the following special case of a result of Martindale [180, Thm. 1].

51.2 Proposition. *Let $J = \mathrm{Her}_3(C)$, C an associative composition algebra, $A = \mathrm{Mat}_3(C)$ and τ the conjugate transpose involution as in 10.7. Then any homomorphism $f\colon J \to B^{(+)}$, B a unital associative algebra, such that $f(e_{ii}) \neq 0$, for all $i \in \{1,2,3\}$, factors through A, that is, there exists a unique unital homomorphism $f'\colon A \to B$ such that $f = f'|_J$.*

Proof Without loss of generality, we may assume that B is generated as an associative algebra by $f(J)$. We will abbreviate $e_i := e_{ii}$, use the notation of (36.2) and write e_{ij}, $i, j = 1, 2, 3$, for the standard matrix units of A. Let $\Omega := (f(e_1), f(e_2), f(e_3))$. By Exc. 28.25(b), Ω is a complete orthogonal system of idempotents in B and Exc. 32.22(d) implies $f(C[jl]) = B_{jl} + B_{lj}$. If f' exists, it must respect the Peirce decompositions. So it suffices to define f' on the Peirce components of A and extend by linearity. For arbitrary $x, y \in C$ and arbitrary i, $j \in \{1,2,3\}$, put $x_{ij} := xe_{ij}$. Assume f' exists. We first show it is then unique. Now $f'(x_{ij}) = f'(e_i x[ij]) = f(e_i)f(x[ij])$ and f determines a unique f' on off-diagonal elements of A. In other words, $f(x[ij]) \in B_{ij} \oplus B_{ji}$ and $f'(x_{ij})$ is the ij component of $f(x[ij])$. Since the x_{ij}'s generate A (as an associative algebra), the map f' is uniquely determined by f provided it is well-defined on A_{ii}. We must also show that f' is a homomorphism of associative algebras.

We start with the off-diagonal Peirce spaces,

$$\begin{aligned} f(x_{ij}y_{jl} + \bar{y}_{lj}\bar{x}_{ji}) &= f(x[ij] \circ y[jl]) = f(x[ij]) \circ f(y[ij]) \\ &= (f'(x_{ij}) + f'(\bar{x}_{ji})) \circ (f'(y_{jl}) + f'(\bar{y}_{lj})) \\ &= f'(x_{ij})f'(y_{jl}) + f'(\bar{y}_{lj})f'(\bar{x}_{ji}) \end{aligned}$$

and we obtain

$$f'(x_{ij}y_{jl}) = f'(x_{ij})f'(y_{jl}). \tag{1}$$

Consider $1[ij] = e_{ij} + e_{ji}$; $1[ij]^2 = e_i + e_j$ so $f(1[ij])^2 = f(e_i) + f(e_j)$ and $f'(e_{ij})f'(e_{ji}) = f(e_i)$. Using (1), $f'(e_{ij})f'(e_{ji}) = f'(e_{il})$ and the $f'(e_{ij})$'s form a set of matrix units of B. If $a, b \in B_{ij}$ then $af(1_{jl}) \in B_{il}$ and $f(e_{li})b \in B_{lj}$. Therefore $af'(e_{jl})f'(e_{li})b \in B_{ij}$ defines a product on B_{ij}. So $B = \mathrm{Mat}_3(F)$, for some unital associative algebra F over k.

Define $f'(x_{ii}) := f'(x_{ij})f'(e_{ji})$. To show that $f'(x_{ii})$ is well-defined, we must show that $f'(x_{il})f'(e_{li}) = f'(x_{ij})f'(e_{ji})$. By (1), $f'(x_{il})f'(e_{lj}) = f'(x_{ij})$ and $f'(x_{ij})f'(e_{ji}) = f'(x_{il})f'(e_{lj})f'(e_{ji}) = f'(x_{il})f'(e_{li})$. Therefore the definition does not depend on the choice of index other than i and we note

$$f'(x_{ii}) = f'(x_{ij})f'(e_{ji}) = f'(x_{il})f'(e_{li}). \tag{2}$$

We have shown that f', if it exists, is uniquely determined by f and have given explicit formulas for f'.

It remains to show that f' is a homomorphism of associative algebras in the few cases that are not already covered by (1) or automatically zero by Peirce considerations. Using (1) and (2),

$$\begin{aligned} f'(x_{ij})f'(y_{ji}) &= f'(x_{ij})f'(y_{jl}1_{li}) = f'(x_{ij})f'(y_{jl})f'(1_{li}) \\ &= f'(x_{ij}y_{jl})f'(e_{li}) \\ &= f'(x_{ij}y_{ji}). \end{aligned}$$

We have

$$\begin{aligned} f'(x_{ii})f'(y_{ii}) &= f'(x_{ij})f'(e_{ji})f'(y_{il})f'(e_{li}) = f'(x_{ij})f'(y_{jl})f'(e_{li}) \\ &= f'(xy_{il})f'(e_{li}) = f'(xy_{ii}) = f'(x_{ii}y_{ii}). \end{aligned}$$

Finally

$$\begin{aligned} f'(x_{ij})f'(y_{jj}) &= f'(x_{ij})f'(y_{jl})f'(e_{lj}) = f'(x_{ij}y_{jl})f'(e_{lj}) \\ &= f'(x_{ij}y_{jl})f'(1_{lj}) = f'(xy_{il}1_{lj}) \\ &= f'(x_{ij}y_{jj}) \end{aligned}$$

and

$$\begin{aligned} f'(x_{ii})f'(y_{ij}) &= f'(x_{il})f'(1_{li})f'(y_{ij}) = f'(x_{il}))f'(y_{lj}) \\ &= f'(x_{il}y_{lj}) = f'(x_{ii}y_{ij}). \end{aligned}$$

Thus f' is a homomorphism of associative algebras, completing the proof. □

51.3 Corollary. *Let C be an associative composition k-algebra. Then any derivation D of the Jordan algebra $J := \mathrm{Her}_3(C)$ extends to a unique derivation D' of the associative algebra $A := \mathrm{Mat}_3(C)$.*

Proof Let $R = k[\varepsilon]$, the algebra of dual numbers. Consider $J_R \subseteq A_R$ and write x for $x \otimes 1$ and $x\varepsilon$ for $x \otimes \varepsilon$. The map $f\colon J \to J_R$ given by $f(x) := x + D(x)\varepsilon$ is a k-module homomorphism which, by (50.3.2), is a homomorphism of Jordan algebras. Since $f(e_i) \neq 0$, Prop. 51.2 applies, so f extends to a unique homomorphism $f' : A \to A_R$ of associative algebras. We claim that

$$A' := \{x \in A \mid f'(x) - x \in \varepsilon A\} = A.$$

Indeed, A' is a k-submodule of A containing J and since J generates A as an associative algebra, it suffices to show that A' is closed under multiplication, so let $x, y \in A'$. Then there are $u, v \in A$ having $f'(x) = x+\varepsilon u$, $f'(y) = y+\varepsilon v$ and we conclude $f'(xy) = f'(x)f'(y) = xy+\varepsilon(uy+xv)$, hence $xy \in A'$, as claimed. Thus, for $x \in A$, $f'(x) = x + D'(x)\varepsilon$, where $D' : A \to A$ is a linear map which extends D. If $x, y \in A$ then $f'(xy) = xy+D'(xy)\varepsilon = f'(x)f'(y) = xy+(D'(x)y+xD'(y))\varepsilon$. Therefore $D'(xy) = D'(x)y + xD'(y)$ and D' is a derivation of the associative algebra A. Uniqueness of D' follows from the uniqueness of f'. □

We need to take a closer look at associative composition algebras. We begin by fixing some notation.

51.4 Notation. We fix a composition k-algebra C of rank $r \in \{1, 2, 4\}$ and put $A := \mathrm{Mat}_3(C)$, $J := \mathrm{Her}_3(C)$. In the case where C is split, we will determine $\mathrm{Der}(J)$ in Cor. 51.9, Prop. 51.11, or Prop. 51.13 respectively.

We write τ for the conjugate transpose involution of A and denote by $E_a = L_a - R_a$ as in 48.3 the inner derivation of A affected by $a \in A$.

51.5 Lemma. *Let C be a conic k-algebra and assume k has no 2-torsion. If C is projective as a k-module, then $H(C, \iota_C) = k1_C$*

Proof By Prop. 16.7, 1_C is unimodular. Hence there is a submodule $M \subseteq C$ satisfying $C = k1_C \oplus M$, and $x \in H(C, \iota_C)$ may be written $x = \xi 1_C + m$, $\xi \in k$, $m \in M$. We conclude $t_C(x)1_C = x + \bar{x} = 2x = 2\xi 1_C + 2m$, hence $2m = 0$. But M is projective and since 2 is not a zero divisor in k it is not one in M either (18.8). Thus, $m = 0$ and $x = \xi 1_C$. □

51.6 Lemma. *With the notation and assumptions of 51.4, let $a \in A$. The following conditions are equivalent.*

(i) $E_a J = \{0\}$.
(ii) $E_a = 0$.
(iii) $a \in \mathrm{Cent}(C)\mathbf{1}_3$.

Proof The implications (ii) ⇒ (iii) ⇒ (i) are obvious, while (i) ⇒ (ii) follows from the fact that J generates A as an associative algebra and the kernel of a derivation of A is a unital subalgebra. □

51.7 Proposition. *With the notation and assumptions of 51.4, we have*

$$\mathrm{Der}(J) = \{E_a|_J \mid a \in A, E_a J \subseteq J\}. \tag{1}$$

Moreover, if k has no 2-torsion, then for any $a \in A$ the following conditions are equivalent.

(i) $E_a J \subseteq J$.

(ii) $a + \bar{a}^\mathsf{T} \in \mathrm{Cent}(C)\mathbf{1}_3$.

(iii) *If* $a = (a_{ij})_{1\le i,j\le 3}$, $a_{ij} \in C$, *we have* $\bar{a}_{ji} = -a_{ij}$ *for* $i \neq j$, *and* $t_C(a_{11}) = t_C(a_{22}) = t_C(a_{33})$.

(iv) $2a \in t_C(C)\mathbf{1}_3 + \mathrm{Alt}(A,\tau)$.

Finally, assuming $2 \in k^\times$, these conditions are also equivalent to

(v) $a \in k\mathbf{1}_3 \oplus \mathrm{Skew}(A,\tau)$.

Proof By Cor. 51.3, every derivation of J extends to a derivation of A, and by Example 48.3, the derivations of A are all inner, i.e., have the form E_a for some $a \in A$. This proves (1). For the rest of the proof we may assume that k has no 2-torsion.

(i) $\Leftrightarrow$ (ii). By Lemma 51.5, $J = \mathrm{Sym}(A,\tau)$. Thus (i) holds if and only if, for all $x \in J$, $ax - xa = \overline{ax - xa}^\mathsf{T} = x\bar{a}^\mathsf{T} - \bar{a}^\mathsf{T}x$, which with $b := a + \bar{a}^\mathsf{T}$ is equivalent to $bx = xb$ for all $x \in J$, i.e., with $E_b J = \{0\}$. By Lemma 51.6, this in turn is equivalent to (ii).

(ii) $\Leftrightarrow$ (iii). Condition (ii) is equivalent to $a_{ji} = -\bar{a}_{ij}$ for $i \neq j$ and $t_C(a_{ii}1_C) = a_{ii} + \bar{a}_{ii}$ being independent of $i = 1,2,3$.

(iii) $\Leftrightarrow$ (iv). Condition (iii) implies $a + \bar{a}^\mathsf{T} \in t_C(C)\mathbf{1}_3$, and we conclude $2a = (a + \bar{a}^\mathsf{T}) + (a - \bar{a}^\mathsf{T})$, where the first summand belongs to $t_C(C)\mathbf{1}_3$ and the second one belongs to $\mathrm{Alt}(A,\tau)$. Thus (iv) holds. Conversely, (iv) implies $2a = t_C(u)\mathbf{1}_3 + b - \bar{b}^\mathsf{T}$ for some $u \in C$, $b \in A$, hence $2(a + \bar{a}^\mathsf{T}) = 2t_C(u)\mathbf{1}_3$, and the absence of 2-torsion combines with 18.8 to yield $a + \bar{a}^\mathsf{T} = t_C(u)\mathbf{1}_3$, so (iii) holds.

Finally, if 2 is invertible in k, then $t_C(C) = k$ and $\mathrm{Alt}(A,\tau) = \mathrm{Skew}(A,\tau)$, proving the equivalence of (iv) and (v). □

51.8 Corollary. *With the notation and assumption of 51.4, suppose 2 is invertible in k and put $K = \mathrm{Cent}(C)$. Then the assignment $a \mapsto E_a|_J$ defines a surjective homomorphism $\mathrm{Skew}(A,\tau) \to \mathrm{Der}(J)$ of Lie algebras with kernel $\mathrm{Skew}(K,\iota_K)\mathbf{1}_3$. In particular,*

$$\mathrm{Der}(J) \cong \mathrm{Skew}(A,\tau)/\,\mathrm{Skew}(K,\iota_K)\mathbf{1}_3.$$

Proof The map in question is clearly a homomorphism of Lie algebras. Thanks to Prop. 51.7, the elements of $\mathrm{Der}(J)$ have the form $E_a|_J$, with $a = \alpha\mathbf{1}_3 + b$, $\alpha \in k$, $b \in \mathrm{Skew}(A,\tau)$. Since $E_a = E_b$, the map in question is surjective and, by Lemma 51.6, has kernel $\mathrm{Skew}(K,\iota_K)\mathbf{1}_3$. □

We will now consider separately the various possibilities for the rank r of C.

51.9 Corollary. *In the situation of 51.4, assume k has no 2-torsion. Then the assignment $a \mapsto E_a|_J$ determines an isomorphism $\mathrm{Alt}_3(k) \xrightarrow{\sim} \mathrm{Der}(\mathrm{Her}_3(k))$ of Lie algebras.*

Proof It suffices to show that the map in question is bijective. Suppose $a \in \mathrm{Alt}_3(k)$ has $E_aJ = \{0\}$. Then $a \in k\mathbf{1}_3$ by Lemma 51.6. On the other hand, the diagonal entries of $a \in \mathrm{Alt}_3(k)$ are zero, and we conclude $a = 0$. Thus the map in question is injective. Furthermore, (51.7.1) implies that any derivation of J has the form $D = E_a|_J$, for some $a = (a_{ij}) \in A$ having $E_aJ \subseteq J$. From Prop. 51.7 (iii) for $C = k$ we conclude that the $2a_{ii} = t_k(a_{ii})$ are independent of $i = 1,2,3$. Since k has no 2-torsion, so are the a_{ii}, and we find an $\alpha \in k$ such that $b := a - \alpha\mathbf{1}_3 \in \mathrm{Alt}_3(k)$. Thus $D = E_b|_J$, and the map in question is surjective. □

We wish to derive an analogous result for the case $r = 2$ by specializing C to the split quadratic étale k-algebra. To this end, we need a preparation.

51.10. Let $C = k \times k$, the split quadratic étale k-algebra, and assume $2 \in k^\times$. Note that $C = K$ in the notation of Cor. 51.8. There is a natural identification

$$A = \mathrm{Mat}_3(C) = \mathrm{Mat}_3(k) \times \mathrm{Mat}_3(k)$$

matching

$$a = (a_{ij}) \in A,\ a_{ij} = (\alpha_{1ij}, \alpha_{2ij}) \in C$$

with

$$(a_1, a_2) \text{ where } a_r := (\alpha_{rij}) \text{ for } r = 1,2.$$

Under this identification we have

$$\overline{(a_1,a_2)}^{\mathsf{T}} = (a_2^{\mathsf{T}}, a_1^{\mathsf{T}}) \qquad (a_r \in \mathrm{Mat}_3(k),\ r = 1,2), \tag{1}$$

which implies

$$\mathrm{Her}_3(C) = \mathrm{Sym}(A,\tau) = \{(a_1, a_1^{\mathsf{T}}) \mid a_1 \in \mathrm{Mat}_3(k)\}, \tag{2}$$

$$\mathrm{Alt}(A,\tau) = \mathrm{Skew}(A,\tau) = \{(a_1, -a_1^{\mathsf{T}}) \mid a_1 \in \mathrm{Mat}_3(k)\}. \tag{3}$$

We also consider the first projection

$$\pi_1 : A = \mathrm{Mat}_3(k) \times \mathrm{Mat}_3(k) \to \mathrm{Mat}_3(k), \quad (a_1, a_2) \mapsto a_1. \tag{4}$$

51.11 Proposition. *Assume $2 \in k^\times$ and let $C = k \times k$, the split quadratic étale k-algebra. With the notation of 51.4 and 51.10, the first projection $\pi_1 : A \to \mathrm{Mat}_3(k)$ restricts to an isomorphism*

$$\varrho : \mathrm{Skew}(A, \tau) \xrightarrow{\sim} \mathfrak{gl}_3(k)$$

of Lie algebras sending $\mathrm{Skew}(C, \iota_C)\mathbf{1}_3$ to $k\mathbf{1}_3$. In particular,

$$\mathrm{Der}(\mathrm{Her}_3(C)) \cong \mathrm{Skew}(A, \tau)/\mathrm{Skew}(C, \iota_C)\mathbf{1}_3 \cong \mathfrak{gl}_3(k)/k\mathbf{1}_3.$$

If $3 \in k^\times$, then $\mathrm{Der}(\mathrm{Her}_3(C)) \cong \mathfrak{sl}_3(k)$.

Proof The first part follows by combining (51.10.3), (51.10.4) with the fact that the elements of $\mathrm{Skew}(C, \iota_C)\mathbf{1}_3$ have the form $(\alpha, -\alpha)\mathbf{1}_3 = (\alpha\mathbf{1}_3, -\alpha\mathbf{1}_3)$ for $\alpha \in k$. In the second displayed equation, the first isomorphism is Cor. 51.8 and the second follows from the isomorphism ϱ. For the final claim, since $3 \in k^\times$, $\mathfrak{gl}_3(k) = k\mathbf{1}_3 \oplus \mathfrak{sl}_3(k)$ as a direct sum of Lie ideals. □

51.12 A few facts concerning split symplectic involutions. Before tackling the last case, we recall a few facts concerning split symplectic involutions. Again we assume $2 \in k^\times$. In (10.10) (a), the split symplectic involution τ_{spl} is defined on $\mathrm{Mat}_{2l}(k)$. In fact, by (10.10.4), if $a, b, c, d \in \mathrm{Mat}_l(k)$,

$$\tau_{\mathrm{spl}}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} d^\mathsf{T} & -b^\mathsf{T} \\ -c^\mathsf{T} & a^\mathsf{T} \end{pmatrix}.$$

Since $2 \in k^\times$ we have $\mathrm{Mat}_{2l}(k) = \mathrm{Sym}(\mathrm{Mat}_{2l}(k), \tau_{\mathrm{spl}}) \oplus \mathrm{Skew}(\mathrm{Mat}_{2l}(k), \tau_{\mathrm{spl}})$. In (10.10) (b), it is noted that when $l = 1$ this involution coincides with the standard involution ι_C of $C = \mathrm{Mat}_2(k)$). Finally in (10.10) (c), it is explained that $(\mathrm{Mat}_l(C), \tau) \cong (\mathrm{Mat}_{2l}(k), \tau_{\mathrm{spl}})$ as algebras with involution, with an explicit isomorphism being given in Exc. 10.11 (b). The Lie algebras $\mathrm{Skew}(\mathrm{Mat}_{2l}(k), \tau_{\mathrm{spl}})$ are called symplectic Lie algebras and denoted $\mathfrak{sp}_l(k)$, see Ex. 47.14.

51.13 Proposition. *If $2 \in k^\times$, then $\mathrm{Der}(\mathrm{Her}_3(\mathrm{Mat}_2(k))) \cong \mathfrak{sp}_3(k)$.*

Proof Put $C := \mathrm{Mat}_2(k)$ and $J := \mathrm{Her}_3(C)$. We have the following isomorphisms of Lie algebras

$$\mathrm{Der}(J) \cong \mathrm{Skew}(A, \tau) \cong \mathrm{Skew}(\mathrm{Mat}_6(k), \tau_{\mathrm{spl}}) = \mathfrak{sp}_3(k).$$

Indeed, in the notation of Cor. 51.8, we have $K = k1_C$, so $\mathrm{Skew}(K, \iota_K) = \{0\}$.

Cor. 51.8 therefore implies that the assignment $a \mapsto E_a|_J$ gives an isomorphism $\mathrm{Skew}(A,\tau) \xrightarrow{\sim} \mathrm{Der}(J)$ of Lie algebras, hence the first isomorphism above. The second isomorphism arises from 51.12 for $l = 3$ via restriction of the isomorphism of algebras with involution to $\mathrm{Skew}(A,\tau)$, keeping in mind that $2 \in k^\times$. □

Before discussing derivations of Albert algebras, we need a few technical results.

51.14 Lemma. *Let J be a cubic Jordan k-algebra, $e \in J$ an elementary idempotent and $a \in J_1(e)$. Then*

$$D_{e,a}e = -a, \quad D_{e,a}x_1 = T_J(\{aex_1\}, e)e - \{aex_1\}, \quad D_{e,a}x_0 = \{eax_0\}$$

for all $x_i \in J_i(e)$, $i = 0, 1$. Moreover, $D_{e,x_0} = 0$.

Proof The Peirce rules of Thm. 32.2 and $J_2(e) = ke$ imply

$$V_{e,a}(e + x_1 + x_0) = \{eae\} + \{eax_1\} + \{eax_0\} = T_J(\{eax_1\}, e)e + \{eax_0\},$$
$$V_{a,e}(e + x_1 + x_0) = \{aee\} + \{aex_1\} + \{aex_0\} = a + \{aex_1\}.$$

Subtracting these relations from one another yields the displayed equation of the lemma. The final claim follows from the Peirce rules. □

51.15 Lemma. *Let J be a cubic Jordan algebra over k, $e \in J$ an elementary idempotent and $a, b \in J_1(e)$. Then*

$$V_{a,b}e = T_J(\{abe\}, e)e. \qquad D_{a,b}e = 0.$$

Proof The Peirce rules guarantee that $\{abe\} \in J_2(e) = ke$, hence the first equation. Since $D_{a,b} = V_{a,b} - V_{b,a}$, the second one now follows from (33a.32). □

51.16 Lemma. *Let J be a Freudenthal algebra over k. A k-linear map $D\colon J \to J$ is a derivation of J if and only if $D1_J = 0$ and the identity*

$$T_J(x^\sharp, Dx) = 0 \tag{1}$$

holds strictly. In this case,

$$T_J(Dx) = T_J(x, Dx) = 0$$

for all $x \in J$.

Proof Let $R := k[\varepsilon]$, $\varepsilon^2 = 0$, be the k-algebra of dual numbers. Arguing along the lines of Example 48.2, one checks that D is a derivation of J if and only if $\phi_D\colon J_R \to J_R$ defined by

$$\phi_D(x + \varepsilon y) := x + \varepsilon(Dx + y)$$

for all $x, y \in J$ is an automorphism of J_R as a para-quadratic R-algebra. By Cor. 39.13, this is equivalent to ϕ_D being an automorphism of J_R as a cubic Jordan R-algebra, i.e., to $\phi_D(1_J) = 1_J$ and to $N_{J_R} \circ \phi_D = N_{J_R}$ as polynomial laws over R. The former condition amounts to $D1_J = 0$, while the latter condition is equivalent to

$$N_{J_R}(x + \varepsilon(Dx + y)) = N_{J_R}(\phi_D(x + \varepsilon y)) = N_{J_R}(x + \varepsilon y)$$

for all $k' \in k$-**alg**, $x, y \in J_{k'}$, where $R' := R_{k'} = k'[\varepsilon]$ is the algebra of dual numbers over k'. Expanding both sides, strict validity of (1) follows. Linearizing we conclude $T_J(x \times y, Dx) + T_J(x^\sharp, Dy) = 0$ for all $x, y \in J$. Since $D1_J = 0$, setting $x := 1_J$ implies $T_J(Dy) = 0$, while setting $y = 1_J$ implies $T_J(x, Dx) = 0$. □

51.17. We now proceed to discuss derivations of Albert algebras and, unless stated otherwise, consider the following set-up. C is an octonion algebra over an arbitrary base ring k and $J := \mathrm{Her}_3(C)$ is the corresponding Albert algebra of un-twisted 3-by-3 hermitian matrices with entries in C and diagonal entries in k. Systematic use will be made of the ternary cyclicity convention 36.1, according to which an index $i = 1, 2, 3$ will always be thought of as the first component of the cyclic permutation (ijl) of (123) starting with i. Recall that this convention was employed extensively in connection with cubic Jordan matrix algebras (36.4). Recall also the diagonal frame $\Omega = (e_{11}, e_{22}, e_{33})$ of J whose off-diagonal Peirce components are given by $J_{jl}(\Omega) = J_1(e_{jj}) \cap J_1(e_{ll}) = C[jl]$ for all $i = 1, 2, 3$ (Prop. 37.8). Finally, since (C, n_C) is a quadratic space of constant even rank over k, we can form the orthogonal Lie algebra $\mathfrak{o}(n_C)$ in the sense of 47.4 and know from Prop. 47.8 that $\mathfrak{o}(n_C)$ is spanned as a k-module by the elementary orthogonal transformations $S_{a,b}$, $a, b \in C$ as defined in 47.7.

51.18 A four-group grading of $\mathrm{Der}(J)$**.** If G is a finite abelian group, and A a non-associative algebra over k, a *G-grading of A* is a decomposition $A = \oplus_{\gamma \in G} A_\gamma$ into submodules $A_\gamma \subseteq A$ such that $A_\gamma A_\delta \subseteq A_{\gamma+\delta}$ for all $\gamma, \delta \in G$; in this case, we also say that A is *graded by G*. In 48.19, we considered the case where A was graded by $\mathbb{Z}/3\mathbb{Z}$. Now we will consider an algebra graded by the Klein four-group $\mathcal{V} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is convenient to write the elements of $\mathcal{V}$ as $\{0, 1, 2, 3\}$ with the identity element $0 := (0, 0)$ and remaining elements $1 := (1, 0)$, $2 := (0, 1)$ and $3 := (1, 1)$.

51.19 Proposition. *With the notation and assumptions of 51.17, the Lie algebra* $\mathfrak{g} := \mathrm{Der}(J)$ *is graded by $\mathcal{V}$:*

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \mathfrak{g}_3, \tag{1}$$

where the graded components $\mathfrak{g}_i$, $0 \le i \le 3$, *are defined by*

$$\begin{aligned} \mathfrak{g}_0 &:= \{D \in \mathfrak{g} \mid De_{ii} = 0,\ i = 1,2,3\}, \\ \mathfrak{g}_i &:= \{D_{e_{ii},c_l[ij]} \mid c_l \in C\} \qquad\qquad (i = 1,2,3). \end{aligned}$$

$\mathfrak{g}_0$ *is a subalgebra of* $\mathfrak{g}$ *and the* $\mathfrak{g}_i$, $i = 1,2,3$, *are* $\mathfrak{g}_0$*-modules isomorphic to* C *as a* k*-modules. Moreover*

$$\mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \mathfrak{g}_3 \subseteq \mathrm{StanDer}(J).$$

Proof Given $\mathfrak{a} = (a_1, a_2, a_3) \in C^3$, we put $S_\mathfrak{a} := \sum D_{e_{ii},a_l[ij]} \in \sum_{i\ge1} \mathfrak{g}_i \subseteq \mathrm{StanDer}(J)$. For any cyclic permutation (mnp) of (123), Lemma 51.14 implies

$$S_\mathfrak{a} e_{mm} = \sum D_{e_{ii},a_l[ij]} e_{mm} = -a_p[mn] + a_n[pm]. \tag{2}$$

On the other hand, any $D \in \mathrm{Der}(J)$ satisfies $De_{mm} = D(e_{mm}^2) = e_{mm} \circ (De_{mm})$ by (50.3.7), hence $De_{mm} \in J_1(e_{mm}) = C[mn] \oplus C[pm]$, so De_{mm} can be written as

$$De_{mm} = a_{mp}[mn] + a_{mn}[pm] \tag{3}$$

for some $a_{mp}, a_{mn} \in C$. From

$$0 = D1_J = \sum_m De_{mm} = \sum_m a_{mp}[mn] + \sum_m a_{mn}[pm] = \sum_m (a_{mp} + a_{np})[mn]$$

we deduce $a_{mp} + a_{np} = 0$. Put $\mathfrak{a} := (a_1, a_2, a_3)$ with $a_p := -a_{mp} = a_{np}$. Then (2), (3) imply $S_\mathfrak{a} e_{mm} = a_{mp}[mn] + a_{mn}[pm] = De_{mm}$. Thus $D - S_\mathfrak{a} \in \mathfrak{g}_0$, and we have shown $\sum_{i\ge0} \mathfrak{g}_i = \mathrm{Der}(J)$. By (2), the sum is direct, and (1) holds.

If $D \in \mathfrak{g}_0$ it follows from (50.1.3) that D maps $J_{jl} = C[jl]$ to itself. By (50.1.4), the $\mathfrak{g}_i$'s are $\mathfrak{g}_0$ modules. Also, since $D_{e_{ii},e_{jj}} = 0$,

$$\begin{aligned} [D_{e_i,a[ij]}, D_{e_i,c[ij]}] &= D_{D_{e_i,a[ij]}e_i,c[ij]} + D_{e_i,D_{e_i,a[ij]}c[ij]} \\ &= D_{-a[ij],\,c[ij]} + D_{e_i,t_C(a\bar{c})(e_i-e_j)} \\ &= D_{-a[ij],\,c[ij]} + D_{e_i,-t_C(a\bar{c})e_j} \\ &= -D_{a[ij],\,c[ij]}, \end{aligned}$$

so $[\mathfrak{g}_l, \mathfrak{g}_l] \subseteq \mathfrak{g}_0$, for all $l \in \{1,2,3\}$.

By the Peirce rules $D_{e_{ii},c_l[ij]} e_{ll} = \{e_{ii}\ c_l[ij]\ e_{ll}\} - \{c_l[ij]\ e_{ii}\ e_{ll}\} = 0$ and $\mathfrak{g}_i$ annihilates e_{ll}. Moreover $D_{e_{ii},c_l[ij]} b_j[li] = \{e_{ii}\ c_l[ij]\ b_j[li]\} - \{c_l[ij]\ e_{ii}\ b_j[li]\} = -\{b_j[li]\ e_{ii}\ c_l[ij]\} = -\overline{b_j c_l}[jl]$ ((37.7.4)). Hence by (50.1.8) $[D_{e_{ii},c_l[ij]}, D_{e_{ll},b_j[li]}] = -D_{e_{ll},b_j c_l[jl]}$ and $[\mathfrak{g}_i, \mathfrak{g}_l] \subseteq \mathfrak{g}_j$. The same holds for cyclic permutations of the indices. Therefore the product of two distinct summands of $\mathfrak{g}$ with positive indices lands in the third, and $\mathfrak{g}$ has been endowed with a $\mathcal{V}$-grading. □

51.20 Lemma. *With the conventions of 51.17, the following conditions are equivalent, for all $u \in C$.*

(i) $L_u \in \mathfrak{o}(n_C)$.
(ii) $R_u \in \mathfrak{o}(n_C)$.
(iii) $t_C(u) = 0$.

Proof Since composition algebras are norm-associative (Prop. 17.2), they satisfy (16.12.1), (16.12.2), and we conclude $n_C(x, ux) = n_C(x, xu) = t_C(u)n_C(x)$. The assertion follows. □

The straightforward verification of the next lemma is left to the reader.

51.21 Lemma. *For $E \in \mathrm{End}_k(C)$ define $\bar{E} \in \mathrm{End}_k(C)$ by*

$$\bar{E}x := \overline{E\bar{x}} \qquad (x \in C). \tag{1}$$

Then, for $E, E_1, E_2 \in \mathrm{End}_k(C)$ and $u \in C$, we have

$$\bar{\bar{E}} = E, \quad \overline{E_1E_2} = \bar{E}_1\bar{E}_2, \tag{2}$$

$$\bar{L}_u = R_{\bar{u}}, \quad \bar{R}_u = L_{\bar{u}}, \tag{3}$$

$$E \in \mathfrak{o}(n_C) \iff \bar{E} \in \mathfrak{o}(n_C) \tag{4}$$

□

51.22 Lemma. *With the conventions of 51.17, let $D \in \mathfrak{g}_0$ relative to the $\mathcal{V}$-grading of $\mathfrak{g} = \mathrm{Der}(J)$. For $i = 1, 2, 3$, there are k-linear maps $D_i \colon C \to C$ such that*

$$D\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum(D_i u_i)[jl] \tag{1}$$

for all $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$.

Proof Since $De_{ii} = 0$ for all i, it suffices to show that D stabilizes the $C[jl]$, so let $x \in C[jl]$. By Prop. 37.8 and the Peirce rules,

$$C[jl] = J_1(e_{jj}) \cap J_1(e_{ll}) = \{y \in J \mid e_{jj} \circ y = y = e_{ll} \circ y\}.$$

This and (50.3.6) imply $Dx = D(e_{jj} \circ x) = (De_{jj}) \circ x + e_{jj} \circ (Dx) = e_{jj} \circ (Dx)$ and, similarly, $Dx = e_{ll} \circ (Dx)$. Thus $Dx \in C[jl]$. □

We ask for the converse of the preceding lemma: What conditions on three linear maps $D_i \colon C \to C$ are to be imposed that are necessary and sufficient for the map D defined by (51.22.1) to belong to $\mathfrak{g}_0$, equivalently, to be a derivation of J? The answer is given by the following theorem.

51.23 Theorem. *With the conventions of 51.17, consider three linear maps $D_i \colon C \to C$, $i = 1, 2, 3$. Then the following conditions are equivalent.*

(i) $D\colon C \to C$ *defined by*

$$D\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum(D_i u_i)[jl] \tag{1}$$

for all $\xi_i \in k$, $u_i \in C$, $i = 1,2,3$, *is a derivation of* J.

(ii) $D_i \in \mathfrak{o}(n_C)$ *for all* $i = 1,2,3$ *and*

$$\sum n_C(\overline{u_j u_l}, D_i u_i) = 0 \tag{2}$$

for all $u_i \in C$, $i = 1,2,3$.

(iii) $D_i \in \mathfrak{o}(n_C)$ *for all* $i = 1,2,3$ *and there exists* $i = 1,2,3$ *such that*

$$D_i(uv) = u\bar{D}_j v + (\bar{D}_l u)v \qquad (u, v \in C). \tag{3}$$

(iv) $D_i \in \mathfrak{o}(n_C)$ *and* (3) *holds for all* $i = 1,2,3$.

Proof Letting

$$x = \sum(\xi_i e_{ii} + u_i[jl]) \in J, \quad \xi_i \in k, \quad u_i \in C, \quad i = 1,2,3,$$

we use (36.4.4) and (36.4.7) to compute

$$T_J(x^\sharp, Dx) = \sum n_C(-\xi_i u_i + \overline{u_j u_l}, D_i u_i). \tag{4}$$

By Lemma 51.16, therefore, (i) holds if and only if this expression vanishes for all ξ_i, u_i in all scalar extensions. Fixing i and setting $\xi_i = 1$, $\xi_j = \xi_l = 0$, $u_j = u_l = 0$, we conclude $D_i \in \mathfrak{o}(n_C)$, and (4) collapses to (2). This shows that (i) and (ii) are equivalent. Since (2) is stable under cyclic permutations of the indices, (iii) and (iv) are equivalent once we have shown that (ii) and (iii) are. To this end, we may assume $D_i \in \mathfrak{o}(n_C)$ for all $i = 1,2,3$. For any such i, we consider the expression

$$n_C(\overline{u_j u_l}, D_i u_i) + n_C(\overline{u_l u_i}, D_j u_j) + n_C(\overline{u_i u_j}, D_l u_l) \tag{5}$$

and compute the individual summands by using the identities of Prop. 16.12 as follows.

$$\begin{aligned}
n_C(\overline{u_j u_l}, D_i u_i) &= -n_C(D_i(\bar{u}_l \bar{u}_j), u_i),\\
n_C(\overline{u_l u_i}, D_j u_j) &= n_C(\bar{u}_i \bar{u}_l, D_j u_j) = n_C(\bar{u}_i, (D_j u_j)u_l) = n_C(\bar{u}_l \overline{D_j u_j}, u_i),\\
n_C(\overline{u_i u_j}, D_l u_l) &= n_C(\bar{u}_j \bar{u}_i, D_l u_l) = n_C(\bar{u}_i, u_j(D_l u_l)) = n_C(\overline{D_l u_l}\bar{u}_j, u_i).
\end{aligned}$$

Replacing u_j, u_l by $\bar{u}_j, \bar{u}_l$, consulting Lemma 51.21, adding up and using regularity of n_C, we conclude that (3) holds if and only if (5) vanishes. This completes the proof. □

51.24 Corollary. *If conditions (i)–(iv) of Thm. 51.23 hold, then*

$$\bar{D}_i(uv) = (D_j u)v + u(D_l v)$$

for all $u, v \in C$ and all $i = 1, 2, 3$.

Proof Use the definition of $\bar{D}_i$ as in (51.21.1) and apply (51.23.3). □

51.25 Lemma. *With the conventions of 51.17, the k-module $\mathfrak{o}(n_C)$ is finitely generated projective of rank 28. Moreover, if 2 is invertible in k, then $\mathfrak{o}(n_C)$ is generated as a Lie algebra by the linear maps L_u, R_u for $u \in C^0$.*

Proof The first sentence holds if C is split by Example 47.13 for $l = 4$. The general case reduces to the split one by Lemma 47.5 and Exc. 26.12 (b)(i), because being projective of a certain rank descends from a faithfully flat extension (25.5(i)).

For the remainder of the proof, we recall that the elementary orthogonal transformations $S_{u,v}$ span $\mathfrak{o}(n_C)$ as a k-module (Prop. 47.8). In view of Lemma 51.20, it therefore suffices to verify the identity

$$[L_u + R_u, L_v + R_v] = 2S_{u,v} \qquad (u, v \in C^0). \tag{1}$$

Indeed, for $x \in C$ we apply the identities of 16.5 and Prop. 16.12 to conclude, since u and v have trace zero,

$$\begin{aligned}
[L_u + R_u, L_v + R_v]x &= u(vx) - v(ux) + u(xv) - (ux)v \\
&\quad + (vx)u - v(xu) + (xv)u - (xu)v \\
&= t_C(vx)u - n_C(vx, u)1_C - t_C(ux)v + n_C(ux, v)1_C \\
&\quad + t_C(xv)u - n_C(xv, u)1_C - t_C(xu)v + n_C(xu, v)1_C \\
&= -2n_C(v, x)u + 2n_C(u, x)v + n_C(x, vu - uv + uv - vu),
\end{aligned}$$

and (1) holds. □

51.26 Proposition. *With the assumptions and notation of Thm. 51.23, let $i = 1, 2, 3$. Then the i-th projection*

$$\pi_i \colon \mathfrak{g}_0 \longrightarrow \mathfrak{o}(n_C), \quad D \longmapsto D_i,$$

is a homomorphism of Lie algebras with kernel

$$\operatorname{Ker}(\pi_i) = \{D \in \mathfrak{g}_0 \mid \exists\, \alpha \in k : \ D_j = \alpha \mathbf{1}_C,\ D_l = -\alpha \mathbf{1}_C,\ 2\alpha = 0\}. \tag{1}$$

Moreover, π_i is

(a) injective if and only if k has no 2-torsion,

(b) bijective if 2 is invertible in k.

Proof π_i is clearly a Lie algebra homomorphism. If D belongs to the right-hand side of (1), then (51.23.3) for $v = 1_C$ shows that $D_i u = \alpha u - \alpha u = 0$, hence $D_i = 0$. Conversely, let $D \in \mathrm{Ker}(\pi_i)$. Then $D_i = 0$, and Cor. 51.24 implies

$$(D_j u)v + u(D_l v) = 0 \qquad (u, v \in C). \tag{2}$$

Setting $a := D_j 1_C$, $b := D_l 1_C$, we obtain $L_a = -D_l \in \mathfrak{o}(n_C)$ for $u = 1_C$, $R_b = -D_j \in \mathfrak{o}(n_C)$ for $v = 1_C$, and $a + b = 0$ for $u = v = 1_C$. Hence $a \in C^0$ by Lemma 51.20, and (2) implies $(ua)v - u(av) = 0$, Thus, $a \in \mathrm{Nuc}(C) = k1_C$ (by Exc. 19.32 (b)). We therefore have $a = \alpha 1_C$ for some $\alpha \in k$, and taking traces gives $2\alpha = 0$, so D belongs to the right-hand side of (1).

(a) follow immediately from (1).

(b) Since $2 \in k^\times$ and $\pi_i(\mathfrak{g}_0)$ is a Lie subalgebra of $\mathfrak{o}(n_C)$, it suffices to show, by Lemma 51.25, that it contains L_a, R_a, $a \in C^0$. From linearized left (resp. right) alternativity one concludes that

$$(D_i, D_j, D_l) := ((L_a, -(L_a + R_a), R_a)) \quad \text{and} \quad (D_i, D_j, D_l) := (R_a, -(L_a + R_a), L_a)$$

both satisfy (51.23.3), so by Thm. 51.23, L_a, R_a belong to the image of π_i. □

51.27 Corollary (Principle of local triality)**.** *If* 2 *is invertible in k, then for every* $E \in \mathfrak{o}(n_C)$*, there exist unique* $E_1, E_2 \in \mathfrak{o}(n_C)$ *such that*

$$E(uv) = (E_1 u)v + u(E_2 v) \qquad (u, v \in C).$$

Moreover, the assignments $E \mapsto E_1$ *and* $E \mapsto E_2$ *define automorphisms of* $\mathfrak{o}(n_C)$*.* □

51.28 Proposition. *With the notation and assumptions of 51.17, let* $i = 1, 2, 3$ *and* $a, b \in C$*. Then the standard derivation* $D_{a[jl],b[jl]}$ *belongs to* $\mathfrak{g}_0$ *and*

$$\pi_i(D_{a[jl],b[jl]}) = -2S_{a,b}$$

in the sense of Prop. 51.26.

Proof Put $D := D_{a[jl],b[jl]}$. Since $a[jl], b[jl]$ belong to $J_1(e_{jj}) \cap J_1(e_{ll})$, Lemma 51.15 implies $De_{jj} = De_{ll} = 0$, and $D1_J = 0$ also yields $De_{ii} = 0$. This proves $D \in \mathfrak{g}_0$. Put $D_i; = \pi_i(D) \in \mathfrak{o}(n_C)$. For all $c \in C$, linearizing (37.7.5) and (17.4.2)

implies

$$\begin{aligned}(D_i c)[jl] &= D_{a[jl],b[jl]}c[jl] = \{a[jl]b[jl]c[jl]\} - \{b[jl]a[[jl]c[jl]\}\\ &= U_{a[jl],c[jl]}b[jl] - U_{b[jl],c[jl]}a[jl]\\ &= ((a(\bar{b}c) + c(\bar{b}a) - b(\bar{a}c) - c(\bar{a}b))[jl]\\ &= (n_C(a,b)c + n_C(c,b)a - n_C(a,c)b - n_C(b,a)c\\ &\qquad - n_C(c,a)b + n_C(b,c)a)[jl]\\ &= 2(n_C(c,b)a - n_C(c,a)b)[jl] = (-2S_{a,b}c)[jl].\end{aligned}$$

The assertion follows. □

51.29 Corollary. *Let J be an Albert algebra over k. If $2 \in k^\times$, then*

(a) $\mathrm{Der}(J)$ *is finitely generated projective of rank* 52 *as a k-module.*

(b) $\mathrm{Der}(J) = \mathrm{StanDer}(J)$.

Proof Since $\mathrm{Der}(J)$ and $\mathrm{StanDer}(J)$ commute with flat base change (Prop. 50.4, 50.8), and the property of a module to be finitely generated projective of rank n is stable under faithfully flat descent, Cor. 39.32 allows us to assume $J = \mathrm{Her}_3(C)$ for some octonion algebra C over k. Then, by Prop. 51.19,

$$\mathrm{Der}(J) = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \mathfrak{g}_3, \quad \mathfrak{g}_1 \oplus \mathfrak{g}_2 \oplus \mathfrak{g}_3 \subseteq \mathrm{StanDer}(J), \tag{1}$$

and each $\mathfrak{g}_i$, $i > 0$, is isomorphic to C as a k-module, hence finitely generated projective of rank 8. By Prop. 51.26 (b), $\mathfrak{g}_0$ is isomorphic to $\mathfrak{o}(n_C)$, which by Lemma 51.25 is finitely generated projective of rank 28 as a k-module. Hence (1) implies that $\mathrm{Der}(J)$ is a finitely generated projective k-module of rank 52, proving (a). Then $\mathfrak{g}_0 \cong \mathfrak{o}(n_C)$ is spanned by elementary orthogonal transformations $S_{a,b}$, $a, b \in C$ (Prop. 47.8). By Prop. 51.28, $\pi_i(D_{a[jl],b[jl]}) = -2S_{a,b}$ so the standard derivations $D_{a[jl],b[jl]}$ span $\mathfrak{g}_0$ yielding (b). □

51.30 Derivation algebra of an Albert algebra over a field. The derivation algebra $\mathrm{Der}(J)$ of an Albert algebra J over a field F has been studied in many places. For example, using the language of Albert algebras, as we have done here, see [52], [138], and [2]. An alternative is to use the language of group schemes, as we do in the next chapter, for which see [121], [123], and [233, §1]. In summary, one finds:

51.31 Proposition. *The derivation algebra* $\mathrm{Der}(J)$ *of an Albert algebra J over a field F is a simple Lie algebra if and only if* $\mathrm{char}(F) \neq 2$. *If* $\mathrm{char}\, F = 2$, *it has a unique proper nonzero ideal V_J, which has dimension 26.* □

The case where $\mathrm{char}(F) \neq 2$ can be deduced from a combination of Propositions 51.19 and 51.26. We will see in the next chapter (Thm. 53.4 and 53.16) that $\mathrm{Der}(J)$ is the Lie algebra of a simple group scheme of type F_4.

We remark that one could deduce Cor. 51.29(b), about algebras over a ring, from Prop. 51.31, about algebras over a field.

Alternative proof of Cor. 51.29(b) It suffices to consider the case where $J = \mathrm{Her}_3(\mathrm{Zor}(k))$. To see this, pick a faithfully flat $R \in k$-**alg** that splits J. Since both kinds of derivation algebras are compatible with flat base change (Propositions 50.4 and 50.8), the split case and faithful flatness of R will imply equality over k.

Suppose $k \neq 0$, for otherwise there is nothing to prove. Picking distinct basis vectors $a, b \in C$, the elementary orthogonal transformation $S_{a,b}$ is not zero, and therefore by Prop. 51.28 the derivation $D_{a[jl],b[jl]} \in \mathrm{StanDer}(J)$ is not zero.

Suppose k is a local ring (e.g., a field), and write $\mathfrak{m}$ for its maximal ideal. Since $\mathrm{StanDer}(J)$ is an ideal in $\mathrm{Der}(J)$, so is $\mathrm{StanDer}(J)_{k(\mathfrak{m})}$ in $\mathrm{Der}(J)_{k(\mathfrak{m})}$. Since $\mathrm{StanDer}(J)_{k(\mathfrak{m})}$ is not the zero ideal (by the previous paragraph) and $\mathrm{Der}(J)_{k(\mathfrak{m})}$ is a simple algebra (Prop. 51.31), we have $\mathrm{StanDer}(J)_{k(\mathfrak{m})} = \mathrm{Der}(J)_{k(\mathfrak{m})}$. Now $\mathrm{Der}(J)$ is a finitely generated k-module (Cor. 51.29(a)), so by Nakayama's Lemma we conclude that $\mathrm{StanDer}(J) = \mathrm{Der}(J)$.

For general k, the inclusion $\mathrm{StanDer}(J) \hookrightarrow \mathrm{Der}(J)$ becomes an isomorphism after localizing at each maximal ideal of k by the preceding paragraph. So the inclusion itself is an isomorphism. □

Exercises

51.32. Let J be a split Albert algebra over a field k of characteristic 2. Use the Peirce decomposition to prove that $V_x = 0$ for $x \in J$ if and only if $x \in k1_J$.

51.33. Let J be a reduced Albert algebra over k. Therefore $J = \oplus J_{ij}$. Let $J_0 := J_{11} + J_{22} + J_{33}$. Prove that $J = J_0 + J_1 + J_2 + J_3$, where $J_i := J[jl]$ is a $\mathcal{V}$-grading of J in the sense that given any "product" involving 2 or 3 elements from these subspaces it lands in the subspace indexed by the sum of the indices.

IX

Group schemes

We now illuminate the connection between what has been proved for composition algebras, for Freudenthal algebras, and for Lie algebras with group schemes over the ring k. One highlight of this chapter is Theorem 57.4, which gives the classification of Albert algebras over $\mathbb{Z}$ by leveraging nonabelian H^1 and corresponding results for group schemes.

52 Background on group schemes

In this chapter, we will refer to results in the literature, especially concerning groups schemes over fields as in the books by Milne [195] or Waterhouse [293], as well as semisimple group schemes over rings as in SGA3 [101], [114] and [54]. In this section, we collect some of the results we will use. Some readers will prefer to skip past this section and use it as a reference.

52.1 Lie algebras of k-group schemes over a field. For the material in this subsection, we refer especially to [195, Ch. 10] or [100, Exp. II].

Suppose for the moment that k is a field and $\mathbf{G}$ is a k-group scheme. The dual numbers $k[\varepsilon]/(\varepsilon^2)$ have a natural map to k, namely the map sending ε to zero. The kernel of the homomorphism of ordinary groups $\mathbf{G}(k[\varepsilon]/(\varepsilon^2)) \to \mathbf{G}(k)$ is the *Lie algebra* of $\mathbf{G}$, denoted $\mathrm{Lie}(\mathbf{G})$. (We will only use this in the case where k is a field, although one could alternatively assume that G is smooth, see [100, §II.4.11] for more discussion.)

Suppose for the moment that $\mathbf{G}$ is a closed sub-functor of $\mathbf{GL}_n$ for some n, i.e., $\mathbf{G}(R)$ is the collection of matrices in $\mathrm{Mat}_n(R)$ satisfying a list of polynomials with coefficients in k. The elements of $\mathrm{Lie}(\mathbf{G})$ are of the form $\mathbf{1}_n + \varepsilon y$ for some $y \in \mathrm{Mat}_n(R)$ such that

$$0 = f_{k[\varepsilon]}(\mathbf{1}_n + \varepsilon y) = f(\mathbf{1}_n) + \varepsilon(Df)(\mathbf{1}_n, y)$$

for each of the polynomials f defining $\mathbf{G}$, in the notation of (12.15.5). Since $\mathbf{1}_n$ belongs to $\mathbf{G}(k)$, $f(\mathbf{1}_n) = 0$, so the condition reduces to

$$(Df)(\mathbf{1}_n, y) = 0,$$

which is linear in y, so $\mathrm{Lie}(\mathbf{G})$ is a k-module. Here are some specific examples.

(These **G** are evidently k-group functors. We refer ahead to Exercise 54.23 for the statement that they are k-group schemes.) We briefly focus on identifying Lie(**G**) as a k-module, ignoring for the moment its Lie product.

(a) Suppose A is a finite-dimensional non-associative k-algebra. Then **Aut**(A) has R-points the elements of $\mathrm{GL}(A_R)$ that preserve the multiplication on A and Lie(**Aut**(A)) consists of $x = \mathbf{1}_A + \varepsilon y$ for $y \in \mathrm{End}_{k\text{-}\mathbf{mod}}(A)$ such that x preserves the multiplication on $k[\varepsilon]$. We find, for $a, a' \in A_{k[\varepsilon]}$:

$$x(aa') - (xa)(xa') = \varepsilon\left[y(aa') - (ya)a' - a(ya')\right].$$

Taking $a, a' \in A$, we conclude that, if x is in Lie(**Aut**(A)), then y is in $\mathrm{Der}(A)$ as defined in 48.1. Conversely, if y is in $\mathrm{Der}(A)$, then y naturally acts as a derivation on A_R, and the displayed equation is satisfied for $a, a' \in A_{k[\varepsilon]}$; we have already observed this in Example 48.2. We conclude that Lie(**Aut**(A)) is identified with $\mathrm{Der}(A)$.

(b) Suppose J is a finite-dimensional para-quadratic k-algebra. Computations similar to the previous example (and already implicit in the proof of Lemma 51.16) show that $x = \mathbf{1}_J + \varepsilon y$ for $y \in \mathrm{End}_{k\text{-}\mathbf{mod}}(J)$ is an automorphism of $J_{k[\varepsilon]}$ if and only if

$$y1_J = 0 \quad \text{and} \quad yU_a b = U_a yb + U_{a,ya} b \quad \forall a, b \in J.$$

That is, the map $x \mapsto y$ identifies Lie(**Aut**(J)) with $\mathrm{Der}(J)$ as defined in 50.3.

(c) The k-group scheme $\mathbf{GL}_n$ has R-points the invertible $x \in \mathrm{Mat}_n(R)$. The Lie algebra of $\mathbf{GL}_n$ consists of matrices of the form $x = \mathbf{1}_n + \varepsilon y$ for $y \in \mathrm{Mat}_n(k)$ such that x is invertible. However, x always has an inverse, namely $\mathbf{1}_n - \varepsilon y$, and we conclude that Lie($\mathbf{GL}_n$) is identified with $\mathrm{Mat}_n(k)$, denoted by $\mathfrak{gl}_n(k)$ in Example 47.2(3). Similarly, for a finite dimensional vector space V, the Lie algebra of **GL**(V) is identified with $\mathrm{End}_{k\text{-}\mathbf{mod}}(V)$.

(d) The k-group scheme $\mathbf{SL}_n$ has R-points those $x \in \mathrm{Mat}_n(R)$ such that $\det x = 1$. (It is a k-group functor because the determinant of a product is the product of the determinants, and it is a closed subfunctor of $\mathbf{GL}_n$, so it is a k-group scheme.) The Lie algebra of $\mathbf{SL}_n$ consists of $x = \mathbf{1}_n + \varepsilon y$ for $y \in \mathrm{Mat}_n(k)$ such that $\det x = 1$. Expanding out the formula for the determinant in terms of the entries of x, we find that $\det x = 1 + \varepsilon \operatorname{tr} y$, so Lie($\mathbf{SL}_n$) is naturally identified with the set of trace zero matrices, denoted by $\mathfrak{sl}_n(k)$ in Exc. 47.18. Similarly, for a finite-dimensional vector space V, the Lie algebra of **SL**(V) is identified with the trace zero elements of $\mathrm{End}_{k\text{-}\mathbf{mod}}(V)$.

(e) Suppose that **G** is the closed subfunctor of $\mathbf{GL}_n$ fixing some element $v \in$

k^n. Then $\mathrm{Lie}(\mathbf{G})$ consists of those $x = \mathbf{1}_n + \varepsilon y$ for $y \in \mathrm{Mat}_n(k)$ such that $0 = xv - v = \varepsilon yv$. This identifies $\mathrm{Lie}(\mathbf{G})$ with the annihilator of v in $\mathrm{Mat}_n(k)$.

(f) Let $Q := (V, q)$ be a quadratic space over k. Then the orthogonal group $\mathbf{O}(Q)$ defined in 24.26, i.e., the subgroup of $\mathbf{GL}(V)$ stabilizing q, has Lie algebra consisting of $x = \mathbf{1}_V + \varepsilon y$ for $y \in \mathrm{End}_{k\text{-}\mathbf{mod}}(V)$ such that for all $v \in V$:

$$0 = q(xv) - q(v) = q(v + \varepsilon yv) - q(v) = \varepsilon q(v, yv),$$

i.e., such that $q(v, yv) = 0$. This Lie algebra was called $\mathfrak{o}(V, q)$ in 47.4.

In fact, Lie is a left-exact functor from the category of k-group schemes to k-**mod**.

Recall that there is a natural conjugation action of $\mathbf{G}$ on itself, namely

$$\mathrm{Int}\colon \mathbf{G} \to \mathbf{Aut}(\mathbf{G}) \quad \text{via } \mathrm{Int}_g(x) = gxg^{-1}. \tag{1}$$

This gives an action of $\mathbf{G}$ on $\mathrm{Lie}(\mathbf{G})$, which is called the *adjoint* action and is denoted

$$\mathrm{Ad}\colon \mathbf{G} \to \mathbf{GL}(\mathrm{Lie}(\mathbf{G})) \quad \text{via } \mathrm{Ad}_g(x) = gxg^{-1}. \tag{2}$$

Applying the functor Lie to this map, we find a k-linear map which is also called the adjoint action and is denoted

$$\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}).$$

Define a product $[-,-]\colon \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ via $[x, y] := \mathrm{ad}_x(y)$; it makes $\mathfrak{g}$ a Lie algebra as defined in 47.1. It is a fact that the bracket defined in this way on $\mathfrak{gl}_n$ agrees with the bracket in $\mathrm{Mat}_n(k)^{(-)}$. From this one can deduce that *the bracket just defined in terms of group schemes agrees with the familiar bracket from Chapter VIII* in the examples above.

52.2 Tori. A *split (k-)torus* is a k-group scheme that is isomorphic to a product $\mathbf{G}_\mathbf{m}^r$ of r copies of $\mathbf{G}_\mathbf{m}$ for some $r \geq 0$. The number r is the *rank* of the torus and the rank 0 torus is the trivial group scheme. A *(k-)torus* is a k-group scheme $\mathbf{T}$ such that there is a faithfully flat k-algebra R such that $\mathbf{T}_R$ is a split R-torus, i.e., $\mathbf{T}_R \cong \mathbf{G}_\mathbf{m}^r$ for some $r \geq 0$ [62, Def. IX.1.3]. If k is a field that is separably closed, then every k-torus is a split torus.

Let $\mathbf{T}$ be a k-torus. The morphisms of k-group schemes $\mathbf{T} \to \mathbf{G}_\mathbf{m}$ are called *characters*. The collection of all characters of $\mathbf{T}$ is typically denoted $\mathbf{T}^*$, rather than the more systematic notation $\mathrm{Hom}(\mathbf{T}, \mathbf{G}_\mathbf{m})$. Because $\mathbf{G}_\mathbf{m}$ is an abelian group, so is $\mathbf{T}^*$. Explicitly, $(\mathbf{G}_\mathbf{m}^r)^*$ is isomorphic to $\mathbb{Z}^r$ by identifying the vector $(n_1, \dots, n_r) \in \mathbb{Z}^r$ with the character $(t_1, \dots, t_r) \mapsto \prod t_i^{n_i}$.

In case k is a field and V is a k-vector space and $\rho\colon \mathbf{T} \to \mathbf{GL}(V)$ is a morphism of k-group schemes, for $\chi \in \mathbf{T}^*$ we set

$$V_\chi := \{v \in V \mid \rho(t)v = \chi(t)v \ \forall\, t \in \mathbf{T}(R) \ \forall\, R \in k\text{-}\mathbf{alg}\}.$$

It is a subspace of V. (It is a generalization of the notion of eigenspace for a diagonal matrix to the case of a collection of pairwise commuting diagonalizable matrices [29, VII.5.9, Prop. 19].) If $V_\chi \neq 0$, we say that χ is a *weight* of V and V_χ is a *weight space*. If $\mathbf{T}$ is a split k-torus, then

$$V = \oplus_{\chi \in \mathbf{T}^*} V_\chi. \tag{1}$$

It is known as the *weight space decomposition* of V.

52.3 Example. Let $c_1, \dots, c_r$ be a complete orthogonal system of idempotents in a unital associative k-algebra A, cf. Exercise 32.22,. For $R \in k$-**alg** and $t_1, \dots, t_r \in R^\times$, the element $c := \sum t_i c_i$ is invertible in A_R with inverse $c^{-1} := \sum t_i^{-1} c_i$ and for all $a, a' \in A_R$ we have

$$(c(aa'))c^{-1} = (cac^{-1})(ca'c^{-1}).$$

That is, the k-linear map $i_c\colon A_R \to A_R$ via $i_c(a) := cac^{-1}$ is an R-algebra automorphism of A_R. (This does not work when A is an octonion algebra, see Exc. 23.32.) Further, for $t_1', \dots, t_r' \in R^\times$ and $c' := \sum t_i' c_i$, we have $i_c i_{c'} = i_{cc'}$, so the map

$$(t_1, \dots, t_r) \mapsto i_{\sum t_i c_i}$$

defines a morphism of k-group schemes $\mathbf{G}_\mathbf{m}^r \to \mathbf{Aut}(A)$. Note that for a in the Peirce component A_{ij}, we have $i_c(a) = t_i t_j^{-1} a$. That is, in the weight space decomposition of A with respect to $\mathbf{G}_\mathbf{m}^r$ as in (52.2.1), A_{ij} is the weight space $A_{\chi_i - \chi_j}$ where χ_i denotes the character $\chi_i(t_1, \dots, t_r) = t_i$. In summary, the Peirce decomposition in Exercise 32.22 is the same as the weight space decomposition.

52.4 Semisimple group schemes over an algebraically closed field. For $\mathbf{G}$ an affine K-group scheme for K an algebraically closed field, the *radical* of $\mathbf{G}$, denoted $\mathrm{rad}(\mathbf{G})$, is defined to be the largest smooth closed connected solvable sub-group-scheme of $\mathbf{G}$ [101, XIX.1.2]. We say that $\mathbf{G}$ is *semisimple* if it is smooth, connected, and $\mathrm{rad}(\mathbf{G}) = 1$ [101, XIX.1.8].

Let $\mathbf{T}$ be a maximal torus in $\mathbf{G}$. That is, it is a torus, it is a closed sub-functor of $\mathbf{G}$, and it is not properly contained in any other torus that is also a closed sub-functor of $\mathbf{G}$. Since we have assumed that K is algebraically closed, $\mathbf{T}$ is a split torus and, if $\mathbf{T}'$ is another choice of maximal torus, then there is some $g \in \mathbf{G}(K)$ such that $g\mathbf{T}g^{-1} = \mathbf{T}'$.

We now apply the weight space decomposition to $\mathbf{T}$ acting on $\mathfrak{g} := \mathrm{Lie}(\mathbf{G})$ via the adjoint representation (52.1.2). Because $\mathbf{T}$ is abelian, the map $\mathrm{Int}\colon \mathbf{T} \to \mathbf{Aut}(\mathbf{T})$ is trivial and for all $t \in \mathbf{T}(R)$, $\mathrm{Ad}(t)$ fixes all the elements of $\mathrm{Lie}(\mathbf{T})$ in $\mathfrak{g}$. That is, the weight space $\mathfrak{g}_0$ with weight zero contains $\mathrm{Lie}(\mathbf{T})$. The set R of the non-zero $\chi \in \mathbf{T}^*$ such that $\mathfrak{g}_\chi \neq 0$, i.e., the non-zero weights of the adjoint representation, are called the *roots* of $\mathbf{G}$.

(This decomposition of $\mathrm{Lie}(\mathbf{G})$ into weight spaces under $\mathbf{T}$ is similar to the decomposition into weight spaces under $\mathrm{Lie}(\mathbf{T})$ as mentioned in 47.9. If $\mathrm{char}(K) = 0$, the two are equivalent. However, when $\mathrm{char}(K) \neq 0$, the two decompositions may differ, in which case the decomposition under $\mathbf{T}$ is finer.)

Suppose that $\mathbf{G}$ is semisimple. Then $(\mathbf{T}^* \otimes \mathbb{R}, R)$ is a root system in the sense of 47.11 [195, Cor. 21.12]. Recall that the root system is a finite sum of irreducible root systems. The *type* of $\mathbf{G}$ is the description of the root system as a sum of irreducible root systems, named as in 47.12. We say that $\mathbf{G}$ is *simple* if the root system is itself irreducible. The pair $(\mathbf{T}^*, R)$ is called a *root datum*, cf. [195, Appendix C.d]; this is equivalent to the notion of a semisimple root datum ("donnée radicielle semi-simple") from [101, Def. XXI.1.1.7], see [195, p. 615 and Prop. C.47].

Trivially, the roots generate a sublattice Q in $\mathbf{T}^*$. There is also a notion of weight in the context of root systems; this is a superlattice P of Q, and there are inclusions

$$Q \subseteq \mathbf{T}^* \subseteq P. \tag{1}$$

The extreme cases where one of the two containments is an equality have special names: We say that $\mathbf{G}$ is *adjoint* if $Q = \mathbf{T}^*$ (i.e., $\mathbf{T}^*$ is as small as possible) and $\mathbf{G}$ is *simply connected* if $\mathbf{T}^* = P$ (i.e., $\mathbf{T}^*$ is as large as possible). For a given semisimple $\mathbf{G}$, there are simple groups $\tilde{\mathbf{G}}$ and $\bar{\mathbf{G}}$ that are respectively simply connected and adjoint, both of which are unique up to isomorphism, together with morphisms

$$\tilde{\mathbf{G}} \to \mathbf{G} \to \bar{\mathbf{G}}.$$

The adjoint group $\bar{\mathbf{G}}$ is the quotient, in the sense of group schemes, of $\mathbf{G}$ modulo its center. The irreducible root systems of types G_2, F_4, and E_8 have $P = Q$, so a simple group of that type is always both adjoint and simply connected; whereas for $\mathbf{G}$ simple of one of the other types, the simply connected group $\tilde{\mathbf{G}}$ and the adjoint group $\bar{\mathbf{G}}$ are not isomorphic.

52.5 Semisimple group schemes over a ring k. In case $\mathbf{G}$ is an affine k-group scheme for k merely a ring, $\mathbf{G}$ is said to be *semisimple* if it is smooth and $\mathbf{G}_K$ is semisimple for every algebraically closed field $K \in k$-**alg** [101, XIX.2.7].

When $\mathbf{G}$ is semisimple, we can speak of the *root datum* of the root system

for $\mathbf{G}_K$; when the (isomorphism class of the) root datum is the same for all algebraically closed $K \in k$-**alg**, one says that it is the root datum of $\mathbf{G}$ (over k). Similarly, if the type (i.e., the root system) of $\mathbf{G}_K$ is the same for all algebraically closed $K \in k$-**alg**, we say that this is the type of $\mathbf{G}$. The *rank* of $\mathbf{G}$ is defined to be the rank of that root system, i.e., the dimension of a maximal torus in $\mathbf{G}_K$ for every algebraically closed field $K \in k$-**alg**.

52.6 Lemma. *Suppose* $\mathbf{G}$ *is a* k*-group scheme. If there is a faithfully flat* $R \in k$-**alg** *such that* $\mathbf{G}_R$ *is semisimple, then* $\mathbf{G}$ *is semisimple. If additionally* $\mathbf{G}_R$ *is simply connected (resp., adjoint; resp., of type* T_n*), then* $\mathbf{G}$ *is also simply connected (resp., adjoint; resp., of type* T_n*).*

Proof Since $\mathbf{G}_R$ is smooth and R is faithfully flat, $\mathbf{G}$ is smooth as in 25.25(iii).

For each $\mathfrak{p} \in \operatorname{Spec}(k)$, there is a $\mathfrak{q} \in \operatorname{Spec}(R)$ such that $\mathfrak{q} \cap k = \mathfrak{p}$. Then the field $k(\mathfrak{p})$ embeds in the field $R(\mathfrak{q})$, so the algebraic closure $\overline{k(\mathfrak{p})}$ includes in the algebraic closure $\overline{R(\mathfrak{q})}$. Because $\mathbf{G}_R$ is simply connected (resp., adjoint, resp. of type T_n) over $\overline{R(\mathfrak{q})}$ and this property is unchanged by replacing one algebraically closed field by a smaller one, the same holds over $\overline{k(\mathfrak{p})}$. □

52.7 Split semisimple group schemes over a ring k**.** Suppose now that $\mathbf{G}$ is semisimple and has a root datum as defined just before the lemma. We say that $\mathbf{G}$ is *split* if it is "déployable" in the sense of [101, Def. XXII.1.13]. In the case where k is a field, $\mathbf{G}$ is split if and only if it contains a split k-torus whose rank equals the rank of $\mathbf{G}$.

A split semisimple group scheme over a ring k is determined up to isomorphism by the isomorphism class of its root datum and the text of the final paragraph of 52.4 holds, see [101, §XXIII.5]. The split semisimple k-group scheme corresponding to a given root datum is obtained by base change from the split semisimple $\mathbb{Z}$-group scheme with that root datum. If $\mathbf{G}$ is a semisimple k-group scheme over a principal ideal domain k such that $\mathbf{G}_K$ is split for K the fraction field of k, then $\mathbf{G}$ is split [54, Prop. 1.3].

We now describe some examples of split semisimple groups.

(i) *Type* A: In the k-group scheme $\mathbf{SL}_n$ defined in 52.1(d), the diagonal matrices in $\mathbf{SL}_n$ make a rank $n-1$ split torus via

$$(t_1, t_2, \dots, t_{n-1}) \mapsto \operatorname{diag}(t_1, t_2, \dots, t_{n-1}, (\prod_{i=1}^{n-1} t_i)^{-1}).$$

Such an element of $\mathbf{SL}_n(k)$ acts on $\mathfrak{sl}_n$ by conjugation. It fixes the diagonal matrices in $\mathfrak{sl}_n$ elementwise and acts on a matrix with a 1 in the (i, j) entry and zeros elsewhere as $t_i t_j^{-1}$ where t_n is understood to mean $\prod_{i=1}^{n-1} t_i^{-1}$. Thus, the

roots of this representation are $\varepsilon_i - \varepsilon_j$ for $1 \le i \ne j \le n$, where $\varepsilon_i(t_1, \dots, t_{n-1}) = t_i$. The roots make up a copy of the root system A_{n-1}. It turns out that $\mathbf{SL}_n$ is simple and simply connected, see [42, §3.3].

The split adjoint simple group of type A_{n-1}, i.e., the quotient of $\mathbf{SL}_n$ by its center, is denoted $\mathbf{PGL}_n$. We mention that, if $R \in k\text{-}\mathbf{alg}$ has $\operatorname{Pic} R = 0$, then $\mathbf{PGL}_n(R) = \mathrm{GL}_n(R)/R^\times$.

What about groups of type A_{n-1} that are not split? Let A be an Azumaya k-algebra of degree n as defined in 42.6. We define $\mathbf{SL}_1(A)$ to be the k-group functor such that

$$\mathbf{SL}_1(A)(R) := \{x \in A_R \mid \mathrm{Nrd}_{A_R}(x) = 1\}.$$

It is a k-group scheme because it is a closed subfunctor of the k-group scheme $\mathbf{GL}_1(A)$ as in Example 24.23. Note that $\mathrm{Nrd}_{\mathrm{Mat}_n(k)} = \det$, so the k-group scheme $\mathbf{SL}_1(\mathrm{Mat}_n(k))$ is the same as $\mathbf{SL}_n$ from the previous paragraph. Because $A_R \cong \mathrm{Mat}_n(R)$ for some faithfully flat $R \in k\text{-}\mathbf{alg}$, we conclude by Lemma 52.6 that $\mathbf{SL}_1(A)$ is a simple and simply connected k-group scheme of type A_{n-1}.

(ii) *Type* C: For $n \ge 1$, consider the split symplectic involution τ on $\mathrm{Mat}_{2n}(k)$ as defined in 10.10. The k-group scheme $\mathbf{Aut}(\mathrm{Mat}_{2n}(k), \tau)$ whose R-points are the R-algebra automorphisms of $\mathrm{Mat}_{2n}(R)$ that preserve τ, is sometimes denoted $\mathbf{PGSp}_{2n}$; it is a split adjoint group of type C_n, compare [42, §7.1] or [160, 25.11].

Let S be the $2n$-by-$2n$ matrix I or J from 10.10. The bilinear form $s(x, y) := x^{\mathsf{T}} S y$ on k^n is alternating and regular. Define $\mathrm{Sp}(s)$ to be the automorphism group of s, i.e.,

$$\mathrm{Sp}(s) := \{f \in \mathrm{GL}_n(k) \mid s(fx, fy) = s(x, y)\ \forall x, y \in k^n\},$$

equivalently,

$$\mathrm{Sp}(s) = \{f \in \mathrm{GL}_n(k) \mid f^{\mathsf{T}} S f = S\}.$$

One obtains a k-group scheme $\mathbf{Sp}(s)$ by setting $\mathbf{Sp}(s)(R) := \mathrm{Sp}(s_R)$ for $R \in k\text{-}\mathbf{alg}$. It is split, simply connected, and simple of type C_n with associated adjoint group $\mathbf{PGSp}_{2n}$, compare [42, §7.2]. Computations like the ones in 52.1 verify that the Lie algebra $\mathrm{Lie}(\mathbf{Sp}(s))$ is the one denoted $\mathfrak{sp}(k^{2n}, s)$ in Example 47.14.

(iii) *Types* B *and* D: See especially [157, §V.5], [54, Appendix C], or [42] for details on the following. Let $Q := (M, q)$ be a non-singular quadratic module over k such that M is projective of constant rank $n \ge 1$. We have used $\mathbf{O}(Q)$ to denote the automorphism k-group scheme of Q. Except in the case where n is even and $2 \notin k^\times$, we define $\mathrm{SO}(Q_R)$ to be the kernel of the determinant $\mathrm{O}(Q_R) \to R^\times$ and define the *special orthogonal group* to be the functor

$\mathbf{SO}(Q)(R) := \mathrm{SO}(Q_R)$. We omit the definition of $\mathbf{SO}(Q)$ in the excluded case, which will not be used below.

For example, let $Q_n := (k^n, q_n)$ denote the quadratic form

$$q_{2\ell} = \sum_{i=1}^{\ell} x_{2i-1}x_{2i} \quad \text{and} \quad q_{2\ell+1} = x_0^2 + \sum_{i=1}^{\ell} x_{2i-1}x_{2i},$$

for $n = 2\ell$ or $2\ell + 1$, respectively. There is an fppf $R \in k$-**alg** such that $Q_R \cong (Q_n)_R$; if n is even or $2 \in k^\times$, then R may even be chosen to be an étale cover. (See Exercise 26.12 for the n even case.)

Now, $\mathbf{SO}(Q)$ is smooth. If $K \in k$-**alg** is an algebraically closed field, then $\mathbf{SO}(Q)_K \cong \mathbf{SO}(Q_n)_K$. One can calculate the roots of $\mathbf{SO}(Q_n)$ explicitly and find that it is semisimple and adjoint of type B_ℓ for $n = 2\ell + 1 \geq 3$. It is semisimple of type D_ℓ for $n = 2\ell \geq 4$, cf. Example 47.13, but neither adjoint nor simply connected.

52.8 Isotropic semisimple groups schemes over a field k. Suppose k is a field and $\mathbf{G}$ is a semisimple k-group scheme of rank r. We say that $\mathbf{G}$ is *isotropic* if it contains a copy of $\mathbf{G}_\mathbf{m}^s$ for some $s > 0$, and is *anisotropic* otherwise. As an example, a quadratic space Q is isotropic if and only if the k-group scheme $\mathbf{SO}(Q)$ is isotropic, see Exercises 52.10 and 54.24 or [25, §23.4]

One can make a more refined definition. Let s be the largest integer such that $\mathbf{G}$ contains a copy of $\mathbf{G}_\mathbf{m}^s$. The case $s = r$ is where $\mathbf{G}$ is split and the case $s = 0$ is where $\mathbf{G}$ is anisotropic. In this way, we see that anisotropic groups and split groups are opposite extremes.

We described split and anisotropic groups as opposite extremes. There is an asymmetry in this comparison in that there is a unique split adjoint semisimple k-group for each root system, but there can be zero or many anisotropic adjoint k-groups with that root system. There are no anisotropic groups if k is a separably closed field, because every maximal torus is split. If $k = \mathbb{R}$, then $\mathbf{G}(\mathbb{R})$ is compact if and only if $\mathbf{G}$ is anisotropic [25, §24.6], so there is a unique anisotropic adjoint $\mathbb{R}$-group with a given root system, cf. [33, §IX.3.3].

For another example, suppose k is a number field with n real embeddings. Then there are 2^n isomorphism classes of octonion k-algebras by Corollary 23.23. In Proposition 55.4 below, we will see that therefore there are 2^n isomorphism classes of semisimple k-group schemes of type G_2. Exactly one of these is split. It is a special fact about groups of type G_2 that those that are not split are anisotropic [269, 17.4.2], therefore the remaining $2^n - 1$ of them are all anisotropic.

52.9 Automorphisms of semisimple group schemes. For more details regard-

ing the following material, see [101, Th. XXIV.1.3, §XXIV.3.6], [269, §16.3], or [195, §23e].

For a k-group scheme $\mathbf{G}$, write $\mathrm{Aut}(\mathbf{G})$ for the ordinary group of automorphisms as a k-group scheme. Define a k-group functor $\mathbf{Aut}(\mathbf{G})$ by setting $\mathbf{Aut}(\mathbf{G})(R) := \mathrm{Aut}(\mathbf{G}_R)$ for $R \in k\text{-}\mathbf{alg}$, the collection of automorphisms of $\mathbf{G}_R$ as an R-group scheme. If $\mathbf{G}$ is semisimple, then $\mathbf{Aut}(\mathbf{G})$ is itself a smooth k-group scheme [101, Th. XXIV.1.3(i)]. Let $\bar{\mathbf{G}}$ denote the adjoint group, which is isomorphic to $\mathbf{G}$ modulo its center. Then $\bar{\mathbf{G}}$ is contained in $\mathbf{Aut}(\mathbf{G})$ via the map Int from (52.1.1), and the two groups are equal if $\mathbf{G}$ has a type whose Dynkin diagram has no nontrivial automorphisms, such as A_1, B_n, C_n, G_2, or F_4.

More generally, if $\mathbf{G}$ is semisimple, split, and simply connected (resp., adjoint), then $\bar{\mathbf{G}}$ is a closed normal subgroup of $\mathbf{Aut}(\mathbf{G})$ and $\mathbf{Aut}(\mathbf{G})/\bar{\mathbf{G}}$ is isomorphic to the group of automorphisms of the Dynkin diagram of the root system of $\mathbf{G}$.

Exercises

52.10. Suppose Q is a quadratic module over a ring k and write $\mathbf{h}$ for the split hyperbolic plane. Exhibit a copy of $\mathbf{G_m}$ in $\mathbf{O}(\mathbf{h} \perp Q)$.

53 Automorphism groups of composition algebras and Freudenthal algebras

One motivation for studying octonion algebras and Albert algebras is that the group scheme of automorphisms of such an algebra is interesting. In order to put this claim in context, we discuss the automorphism groups of composition algebras and Freudenthal algebras in general.

If a composition k-algebra C has rank 1, then $C = k$ and $\mathbf{Aut}(C)$ is the trivial k-group scheme 1.

If C has rank 2, then C is a quadratic étale k-algebra by 19.18, 19.19. The non-trivial conjugation is an element of order 2 in $\mathbf{Aut}(C)$, and it turns out that $\mathbf{Aut}(C)$ is the constant group scheme $\mathbb{Z}/2$, see Exercise 19.33. (Or see Exercises 24.29, 25.46 in case C is the split quadratic étale algebra $k \times k$.)

We describe $\mathbf{Aut}(C)$ for C a composition algebra of rank 4 or 8 using the notion of a semisimple group scheme from the preceding section. For the rank 8 case, see alternatively [54, Thm. B.14].

53.1 Theorem. *Let C be a composition algebra over k of rank 4 or 8. Then $\mathbf{Aut}(C)$ is a semisimple k-group scheme that is adjoint (i.e., its center is the*

trivial group scheme). The root system of $\mathbf{Aut}(C)$ *is irreducible of type* A_1 *if* $\operatorname{rk} C = 4$ *and type* G_2 *if* $\operatorname{rk} C = 8$. *If* C *is split, then* $\mathbf{Aut}(C)$ *is split.*

Proof In case k is an algebraically closed field, all three claims hold. See [270, Th. 2.3.5] for rank 8. For rank 4, C is $\mathrm{Mat}_2(k)$ and the Skolem-Noether Theorem as in [142, Cor. of Thm. 4.9] or [102, Thm. 2.4.2] says that all automorphisms of C are inner, i.e., $\mathbf{Aut}(C)$ is the group generally denoted by $\mathbf{PGL}_2$, the split adjoint semisimple group of type A_1 as in Example 52.7(i).

For general k, we know that $\mathbf{Aut}(C)$ is smooth by Corollary 26.10, verifying that it is semisimple. We checked in the preceding paragraph that $\mathbf{Aut}(C)_K$ is adjoint of the type claimed for every algebraically closed field $K \in k$-**alg**, so $\mathbf{Aut}(C)$ has the claimed root datum as a semisimple k-group scheme.

Finally, suppose C is split as a composition algebra. Then $C \cong (C_{\mathbb{Z}})_k$ for $C_{\mathbb{Z}}$ the split composition algebra over $\mathbb{Z}$ of the same rank and $\mathbf{Aut}(C) \cong \mathbf{Aut}(C_{\mathbb{Z}})_k$. We want to show that $\mathbf{Aut}(C)$ is split, for which it suffices to prove that the algebra $\mathbf{Aut}(C_{\mathbb{Z}})_{\mathbb{Q}} \cong \mathbf{Aut}((C_{\mathbb{Z}})_{\mathbb{Q}})$ is split. That is, it suffices to prove the claim in the case where $k = \mathbb{Q}$, where the claims were verified already by the references in the first paragraph of the proof. □

53.2 Automorphism groups of Freudenthal algebras. We now treat the automorphism group of a Freudenthal algebra J in a manner similar to what we have just done for composition algebras. For J of rank 1, $J = k$ and $\mathbf{Aut}(J)$ is the trivial group scheme.

For J the split Freudenthal algebra of rank 3, every automorphism of J as merely a Jordan algebra is an automorphism as a cubic Jordan algebra (Cor. 38.18). Therefore, the k-group scheme of automorphisms of the cubic Jordan algebra J is the same as that of the associative étale k-algebra $k \times k \times k$ (Exc. 29.24), i.e., is the constant group scheme corresponding to the symmetric group on three letters.

53.3 Relationship with J-structures. To address Freudenthal algebras of larger rank, we lean on Springer's book [268]. That book focuses on *J-structures*, which are triples (V, j, e), where V is a finite-dimensional vector space over an algebraically closed field K, j is a rational map from V to V of degree -1 (i.e., a ratio f/g where $f\colon V \to V$ is a homogeneous polynomial law of degree d and $g\colon V \to K$ is a homogeneous polynomial law of degree $d+1$), and e is an element of V. These must satisfy certain properties, which we elide here, but amount to Thm. 31.27. For J a Freudenthal algebra over K of dimension > 3, J is split, and 7.9 and 7.10(ii) in ibid. verify for those algebras that the triple $\mathcal{J} := (J, j, 1_J)$ where $j(x) := x^{-1}$ is a J-structure. For convenience of

cross-reference, we remark that Springer refers to the J-structure arising from J as $\mathcal{S}_3$, $\mathcal{M}_3$, $\mathcal{A}_3$, or $\mathcal{E}_3$ when J has rank 6, 9, 15, or 27 respectively.

This gives an important connection between various group schemes associated with J and $\mathcal{J}$. Springer notes (ibid., 1.1) that the collection

$$\{(g, g') \in \mathrm{GL}(J) \times \mathrm{GL}(J) \mid gj = jg'\}$$

is a group, which we will provisionally denote by $\tilde{G}$. He defines a group G to be the image of the map $\tilde{G} \to \mathrm{GL}(J)$ obtained by projecting on the first factor. In fact, the kernel of this projection is trivial (ibid., 1.2), so the projection is an isomorphism with G. Our structure group $\mathrm{Str}(J)$ naturally includes in $\tilde{G}$ via $\eta \mapsto (\eta^{\sharp -1}, \eta)$, by Thm. 31.22 (b). It is the group of similarities of N_J (Lemma 40.4), so the inclusion $\mathrm{Str}(J) \hookrightarrow \tilde{G}$ is an equality by 12.3 of ibid. Similarly, the automorphism group $\mathrm{Aut}(J)$, which is the stabilizer of 1_J in $\mathrm{Str}(J)$ (Thm. 31.22 (c)), equals the automorphism group of $\mathcal{J}$ denoted by H and defined on p. 50 of ibid. by Prop. 4.6.

We consider these isomorphisms not just as maps between (ordinary) groups, but as homomorphisms of group schemes. Specifically, define $\mathbf{Str}(J)$ to be the group scheme such that $\mathbf{Str}(J)(R) = \mathrm{Str}(J_R)$ for each $R \in K$-**alg** and define $\tilde{\mathbf{G}}$, $\mathbf{G}$, and $\mathbf{H}$ in an analogous way from $\tilde{G}$, G, and H. For each $R \in k$-**alg**, each element of $\mathrm{Str}(J_R)$ is an element of $\mathrm{GL}(J_R)$ that is an element of $\mathbf{G}(R)$, so the homomorphism of group schemes $\mathbf{Str}(J) \to \mathbf{G}$ is naturally a monomorphism. Since $\mathbf{Str}(J)(K) = \mathrm{Str}(J) = G = \mathbf{G}(K)$, if $\mathbf{G}$ is smooth then the natural inclusion $\mathbf{Str}(J) \to \mathbf{G}$ is an equality by [195, Prop. 5.47]. The same argument shows that, if $\mathbf{H}$ is smooth, then it is isomorphic to $\mathbf{Aut}(J)$. In this way, Springer's results describing $\mathbf{H}$, in the cases where that group scheme is smooth, translate to a description of $\mathbf{Aut}(J)$ in the case where k is an algebraically closed field.

53.4 Theorem. *Let J be a Freudenthal algebra of rank 15 or 27 over a ring k. Then $\mathbf{Aut}(J)$ is a semisimple k-group scheme that is adjoint (i.e., its center is the trivial group scheme). Its root system has type C_3 if J has rank 15 and type F_4 if J has rank 27. If J is the split Freudenthal algebra, then the group $\mathbf{Aut}(J)$ is split as a semisimple group.*

Proof The proof follows the same outline as Theorem 53.1. For the case where k is algebraically closed field, Springer shows in [268, 14.19, 14.24] that the group $\mathbf{H}$ for the corresponding J-structure is smooth and of the type claimed, which completes the proof of the first claim in that case as explained in 53.3. (For the case where k is an algebraically closed field of characteristic different from 2 and 3 and J has rank 27, we could instead refer to [270, Th. 7.2.1].)

For the fact that $\mathbf{Aut}(J)$ is smooth for arbitrary k, we refer to 39.33.

Finally, suppose J is split; we wish to prove that $\mathbf{Aut}(J)$ is split. As in the proof of Theorem 53.1, we may assume that $k = \mathbb{Q}$. If J has rank 15, then the proof of 14.19 in Springer's book shows that the automorphisms of J are exactly the automorphisms of the algebra $\mathrm{Mat}_6(k)$ with the split symplectic involution, which is the split adjoint group $\mathbf{PGSp}_6$ as noted in Example 52.7(ii). For J of rank 27, [138, §6] (written for Lie algebras), [85, Satz 4.11] (written for $\mathbb{R}$), and 53.16 below exhibit a weight space decomposition of $\mathrm{Der}(J)$ and a corresponding split maximal $\mathbb{Q}$-torus in $\mathbf{Aut}(J)$. □

53.5 Freudenthal algebras of rank 6. In order to describe Freudenthal algebras of rank 6, we introduce some notation under the assumption that k is a field of characteristic different from 2. For $\Gamma = \mathrm{diag}(\gamma_1, \dots, \gamma_n) \in \mathrm{GL}_n(k)$, we write $\mathbf{O}(\Gamma)$ for the orthogonal group scheme of the quadratic from $\langle\Gamma\rangle_{\mathrm{quad}}$ as defined in 11.7. The determinant gives a morphism of group schemes $\mathbf{O}(\Gamma) \to \mu_2$, and we define $\mathbf{SO}(\Gamma)$ to be the kernel, i.e.,

$$\mathbf{SO}(\Gamma)(R) = \{g \in \mathbf{O}(\Gamma)(R) \mid \det g = 1\}$$

for $R \in k$-**alg**. The groups $\mathbf{O}(\Gamma)$ and $\mathbf{SO}(\Gamma)$ are smooth by the references in Remark 25.22.

Note that μ_2 naturally embeds in $\mathbf{O}(\Gamma)$ as the scalar matrices. When n is odd this is a one-sided inverse for the determinant map, providing an isomorphism $\mathbf{O}(\Gamma) \cong \mathbf{SO}(\Gamma) \times \mu_2$.

We use the shorthand notations $\mathbf{O}(n)$ and $\mathbf{SO}(n)$ for $\mathbf{O}(\Gamma)$ and $\mathbf{SO}(\Gamma)$ in the special case where Γ is the identity matrix. Then $\mathbf{O}(n)(\mathbb{R})$ and $\mathbf{SO}(n)(\mathbb{R})$ are the groups commonly denoted by $O(n)$ and $SO(n)$.

53.6 Proposition. *Suppose that k is a field and let J be a split Freudenthal algebra over k as defined in 39.20.*

(i) *If J has rank 6 and $2 \in k^\times$, then $\mathbf{Aut}(J) \cong \mathbf{SO}(3)$.*

(ii) *Suppose J has rank 9 and view J as $\mathrm{Mat}_3(k)^{(+)}$. Then every automorphism of J arises from an automorphism or anti-automorphism of the associative algebra $\mathrm{Mat}_3(k)$, i.e., $\mathbf{Aut}(J) \cong \mathbf{PGL}_3 \rtimes \mathbb{Z}/2$.*

Proof We define a group scheme Y and a homomorphism $\phi\colon Y \to \mathbf{Aut}(J)$. For J of rank 6, take $Y := \mathbf{O}(3)$. For $y \in \mathbf{O}(3)(R)$, define $\phi_y \in \mathbf{Aut}(J)(R)$ via $\phi_h(x) = yxy^{-1}$. For J of rank 9, take $Y := \mathbf{GL}_3 \rtimes \mathbb{Z}/2$ where the semi-direct product acts via $(1,1)(g,0) = ((g^{-1})^{\mathsf{T}}, 0)(1,1)$ for $g \in \mathbf{GL}_3$. Define

$$\phi_{(g,0)}(x) = gxg^{-1} \quad \text{and} \quad \phi_{(1,1)}(x) = x^{\mathsf{T}}.$$

When $K \in k$-**alg** is an algebraically closed field, $\phi(Y(K)) = \mathbf{Aut}(J)(K)$

by 14.17 and 14.16 in [268], respectively, compare also [136, Ch. VI, Th. 8, Th. 12] or [133, Th. 9]. (Note that in the case of rank 6, [268] has a typo that conflates the group we denote here by Y and its image in $\mathbf{Aut}(J)$.) As $\mathbf{Aut}(J)$ is smooth (39.33) and K is a field, we deduce that $\mathbf{Aut}(J)$ is the image of ϕ as a group scheme. That is, by the usual homomorphism theorem [195, 5.74], $\mathbf{Aut}(J)$ is the quotient of the group scheme Y by the group scheme $\operatorname{Ker}\phi$.

For J of rank 9, the kernel of ϕ is the scalar matrices in $\mathbf{GL}_3$, a subgroup isomorphic to $\mathbf{G_m}$, therefore $\mathbf{Aut}(J) = (\mathbf{GL}_3/\mathbf{G_m}) \rtimes \mathbb{Z}/2 = \mathbf{PGL}_3 \rtimes \mathbb{Z}/2$.

For J of rank 6, the kernel of ϕ is the intersection of $\mathbf{O}(3)$ and the scalar matrices, i.e., μ_2. We find that $\mathbf{Aut}(J) \cong \mathbf{O}(3)/\mu_2 \cong \mathbf{SO}(3)$. □

53.7 Lemma. *Suppose k is a field of characteristic different from 2. Then for each diagonal $\Gamma \in \mathrm{GL}_3(k)$, the group $\mathbf{SO}(\Gamma)$ is isomorphic to the automorphism group of the rank 6 Freudenthal algebra $\mathrm{Her}_3(k,\Gamma)$.*

Proof For each $R \in k$-**alg**, $\mathrm{Her}_3(k,\Gamma) \otimes R$ is the collection of elements of $\mathrm{Mat}_3(R)$ fixed by $x \mapsto x^* := \Gamma^{-1}x^{\mathsf{T}}\Gamma$. If $g \in \mathrm{GL}_3(R)$ satisfies $g^{\mathsf{T}}\Gamma g = \Gamma$ — i.e., $g \in \mathbf{O}(\Gamma)(R)$ — then

$$(gxg^{-1})^* = \Gamma^{-1}(g^{\mathsf{T}})^{-1}x^{\mathsf{T}}g^{\mathsf{T}}\Gamma = g\Gamma^{-1}x^{\mathsf{T}}\Gamma g^{-1} = gx^*g^{-1}.$$

That is, the ordinary group $\mathbf{O}(\Gamma)(R)$ acts on $\mathrm{Her}_3(k,\Gamma)$ with kernel $\mu_2(R)$ as in the proof of 53.6, i.e., $\mathbf{SO}(\Gamma)(R)$ is contained in $\mathbf{Aut}(\mathrm{Her}_3(k,\Gamma))(R)$ and we find that $\mathbf{SO}(\Gamma)$ is a closed sub-group-scheme of $\mathbf{Aut}(\mathrm{Her}_3(k,\Gamma))$.

Now, $\mathbf{Aut}(\mathrm{Her}_3(k,\Gamma))$ is smooth and connected and for F an algebraic closure of k we have $\mathbf{SO}(\Gamma)(F) = \mathbf{Aut}(\mathrm{Her}_3(F,\Gamma))$ as in the proof of Proposition 53.6, so we conclude that the inclusion of k-group schemes is an equality. □

In the preceding material on Freudenthal algebras of rank 6, we restricted to the case where k is a field. We now relax that hypothesis.

53.8 Corollary. *If k is a ring and $2 \in k^\times$, then the automorphism group of $\mathrm{Her}_3(k, \mathrm{diag}(-1,1,-1))$ is the split adjoint group of type A_1.*

Proof Suppose first that $k = \mathbb{Q}$. The quadratic form $\langle -1,1,-1\rangle_{\mathrm{quad}}$ is isotropic (Exc. 11.31), so the group scheme $\mathbf{G} := \mathbf{SO}(\mathrm{diag}(-1,1,-1))$ is isotropic by Exc. 52.10. Since the group scheme is semisimple of type A_1, it is in fact split, as claimed.

For the algebra $J := \mathrm{Her}_3(\mathbb{Z}[1/2], \mathrm{diag}(-1,1,-1))$, we have $\mathbf{Aut}(J)_{\mathbb{Q}}$ is split of type A_1. Since $\mathbb{Z}[1/2]$ is a principal ideal domain, it follows that $\mathbf{Aut}(J)$ is split as a group scheme over $\mathbb{Z}[1/2]$ and therefore $\mathbf{Aut}(J)_k \cong \mathbf{Aut}(J_k)$ is a split group scheme for every ring k with $2 \in k^\times$. □

53.9 Example. Combining the two preceding results shows that the notion of the Freudenthal algebra J being split and the notion of the k-group scheme $\mathbf{Aut}(J)$ being split need not agree for rank 6 Freudenthal algebras. Indeed, when $k = \mathbb{R}$, $\mathrm{Her}_3(k, \mathrm{diag}(1,1,1))$ is the split Freudenthal algebra and it has automorphism group $\mathbf{SO}(3)$, the compact or anisotropic adjoint group of type A_1, whereas $\mathrm{Her}_3(k, \mathrm{diag}(-1,1,-1))$ has automorphism group the split adjoint group of type A_1.

53.10 Corollary. *Let J be a Freudenthal algebra of rank 6 over a ring k such that $2 \in k^\times$. Then $\mathbf{Aut}(J)$ is a semisimple k-group scheme that is adjoint (i.e., its center is the trivial group scheme) and has root system of type A_1.*

Proof Suppose first that J is split. The group $\mathbf{Aut}(J)$ is smooth by 39.33. For every algebraically closed field $K \in k\text{-}\mathbf{alg}$, $\mathbf{Aut}(J)_K = \mathbf{Aut}(J_K) \cong \mathbf{SO}(3)$ by Proposition 53.6(i), which is semisimple and adjoint of type A_1. This proves the claim for J split.

If J is not split, then there is an fppf $R \in k\text{-}\mathbf{alg}$ such that J_R is split by 39.32, and Lemma 52.6 finishes the proof. □

53.11 Remark. For the results in this section, we have relied on Corollaries 26.10 and 39.33 to see that the the automorphism group is smooth in each case. Alternatively, for Proposition 53.1 and Theorem 53.4, it would suffice to verify that the automorphism group of the split algebra over every algebraically closed field is smooth, to note that the split algebra is defined over $\mathbb{Z}$, and then to deduce that the automorphism group of the split algebra over $\mathbb{Z}$ is smooth by [87, Prop. 6.1] or [15, Lemma B.1]. That was the approach taken in [95].

So far, we have proved results of the type "the automorphism group of this kind of algebra looks like this". In the next section, we will develop the machinery of cohomology and descent, which will allow us to prove a tighter connection between algebras and their automorphism groups.

A root systems interlude

We now take a side trip to sketch the identification of root systems of type G_2 and F_4 for $\mathbf{Aut}(A)$ for A an octonion and Albert algebra, respectively. We do so because this material may be difficult to locate elsewhere in the literature. It is not used in the rest of the book.

53.12 An $\mathbf{SL}_3$ subgroup. Let C be a split octonion algebra, i.e., $C \cong \mathrm{Zor}(k)$. We claim that the sub-group-scheme of $\mathbf{Aut}(C)$ fixing the diagonal matrices in $\mathrm{Zor}(k)$ (equivalently, fixing the idempotent $e := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$) is isomorphic to $\mathbf{SL}_3$.

We need as a key point that for $\times$ the ordinary vector product and $h \in \mathrm{GL}_3(k)$, the identity

$$\det(u \wedge v \wedge w) = w^{\mathsf{T}}(u \times v)$$

for $u, v, w \in k^3$ implies that

$$hu \times hv = (\det h)h^{-\mathsf{T}}(u \times v), \tag{1}$$

compare (21.10.2). From this and the multiplication rule (22.14.3), it follows that, for $h \in \mathbf{SL}_3(R)$ for some $R \in k$-**alg**, the map

$$\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_1 & h^{-\mathsf{T}}v^* \\ hv & \alpha_2 \end{pmatrix}$$

is an automorphism of $\mathrm{Zor}(R)$. For the opposite containment, suppose $g \in \mathrm{Aut}(C)$ fixes e. Then, because g is an automorphism,

$$g\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & h'v^* \\ hv & \alpha_2 \end{pmatrix}$$

for some $h, h' \in \mathrm{GL}_3(R)$. Since $\langle h'v^*, hv\rangle = \langle v^*, v\rangle$ for all v, v^*, it follows that $h' = h^{-\mathsf{T}}$. Leveraging again the fact that g is an automorphism, we obtain $h^{-\mathsf{T}}(u \times v) = hu \times hv$, and (1) implies that $\det h = 1$, completing the proof.

Note that applying the functor Lie to the inclusion $\mathbf{SL}_3 \subset \mathbf{Aut}(C)$ immediately implies Prop. 49.3. Conversely, the proofs of the two results are practically the same.

53.13 Remark. We can now show: $\mathbf{Aut}(C)$ *is connected if* k *is a field*. To see this, recall that the notions of elementary and absolute idempotents agree in C (Prop. 22.7), so the scheme X of absolute idempotents consists of $e \in C$ such that $t_C(e) = 1$ and $n_C(e) = 0$. In particular, it is isomorphic to a dense open subscheme of the projective quadric $n_C = 0$ in $\mathbb{P}(C)$ defined by the condition $t_C \neq 0$. Since the projective quadric is irreducible, so is the affine scheme X. The stabilizer in $\mathbf{Aut}(C)$ of a point in X is isomorphic to $\mathbf{SL}_3$, which is connected. By [269, Ex. 5.5.9(1)], this gives the claim.

53.14 Exhibiting the G_2 root system. The proof of Thm. 53.1 that $\mathbf{Aut}(C)$ is simple of type G_2 for C an octonion algebra, which relies on [270], is somewhat indirect. It argues that $\mathbf{Aut}(C)$ is simple of dimension 14. (See Cor. 49.4 and Prop. 49.8 for similar statements about Lie algebras.) Let us now make this identification more explicit by exhibiting a root datum of type G_2 when C is split. We have just identified a subgroup of $\mathbf{Aut}(C)$ isomorphic to $\mathbf{SL}_3$. Let T denote the maximal torus in $\mathbf{SL}_3$ consisting of diagonal matrices. Because $\mathbf{Aut}(C)$ also has rank 2, T is also a maximal torus in $\mathbf{Aut}(C)$. We depict the simple root systems of type A_2 and G_2 in Figure 53a, where we follow the labeling for the simple roots of A_2 from 47.12 but we adopt a special choice for G_2 in order to avoid notational conflict between the two systems.

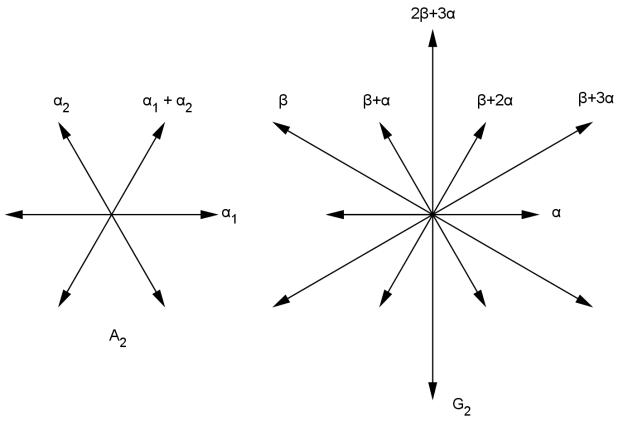


Figure 53a Root systems of type A_2 and G_2 in $\mathbb{R}^2$.

As a representation of $\mathbf{SL}_3$, $\mathrm{Der}(C)$ is a sum of the Lie algebra $\mathfrak{sl}_3$ of $\mathbf{SL}_3$, a copy of the natural representation k^3, and its dual, as in Prop. 48.20. The nonzero weights of $\mathfrak{sl}_3$ with respect to T consist of the roots of $\mathbf{SL}_3$, namely

$$\alpha_1, \quad \alpha_2, \quad \alpha_1 + \alpha_2 \tag{1}$$

and their negatives. The weights of T on k^3 or its dual are

$$\omega_1 = \tfrac{1}{3}(2\alpha_1 + \alpha_2), \quad \tfrac{1}{3}(-\alpha_1 + \alpha_2), \quad -\omega_2 = -\tfrac{1}{3}(\alpha_1 + 2\alpha_2) \tag{2}$$

and the other has an analogous list of weights where the subscripts 1 and 2 are swapped, i.e., the negatives of the weights in (2).

Let us define

$$\alpha := \tfrac{1}{3}(-\alpha_1 + \alpha_2) \quad \text{and} \quad \beta := \alpha_1.$$

With this notation, the weights in (1) are

$$\beta, \quad \beta + 3\alpha, \quad 2\beta + 3\alpha$$

and the weights in (2) are

$$\alpha + \beta, \quad \alpha, \quad -\beta - 2\alpha.$$

The nonzero weights of T on $\mathrm{Der}(C)$ are these and their negatives. We know by general theory [195, Cor. 21.12] that this collection of 12 weights is a root system. We have found that α and β are simple roots of that root system. The linear combinations of α and β that belong to the root system agree with those depicted for G_2 in Figure 53a so we have found the root system of type G_2.

Note that we have identified the roots of $\mathbf{SL}_3$ with the *long* roots of G_2 in $\mathbf{Aut}(C)$. This is an example of a general phenomenon: inside a split simple group scheme over a field, the long roots generate a sub-root-system and a corresponding semisimple subgroup.

Let's follow a similar procedure for F_4.

53.15 A $\mathbf{Spin}_8$ subgroup. In 53.12, we identified a copy of $\mathbf{SL}_3$ inside the split group of type G_2, which was itself an analogue for group schemes of an inclusion of Lie algebras proved in Chap. VIII. We now follow a similar recipe to exhibit inside the split group of type F_4 a copy of the split simply connected group scheme of type D_4, commonly denoted $\mathbf{Spin}_8$. Let $J := \mathrm{Her}_3(C)$ for C the split octonion algebra over k.

Write $\mathbf{H}$ for the affine group scheme whose R-points, for each $R \in k\text{-}\mathbf{alg}$, consists of the elements of $\mathbf{Aut}(J)(R) = \mathrm{Aut}(J_R)$ that fix the three diagonal idempotents e_{ii}. Every element $h \in H(k)$ must preserve the multiple Peirce decomposition as in Example 32.17, so we find that

$$h(\sum e_{ii} + u_i[jl]) = \sum e_{ii} + (h_i u_i)[jl],$$

where $h_i \in \mathrm{End}(C)$. Because $(hx)^\sharp = h(x^\sharp)$, we conclude from the formula for $\sharp$ in (36.4.4) that $h_i \in \mathrm{O}(n_C)$ for all i. Moreover, equating the $[jl]$ component of $(hx)^\sharp$ with that of $h(x^\sharp)$ shows that

$$h_i(\overline{u_j u_l}) = \overline{(h_j u_j)(h_l u_l)}.$$

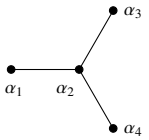
That is, $(h_i, h_j, h_l) \in \mathrm{O}(n_C)^3$ is a related triple in the sense of [69, §1]. The collection of such triples is isomorphic to $\mathbf{Spin}_8$, see Theorem 1.1 in ibid. This argument can be run in reverse and in that manner we identify $\mathbf{H}$ with $\mathbf{Spin}_8$ and we identify the three rank 8 subspaces $C[jl]$ of J with three inequivalent 8-dimensional representations of $\mathbf{Spin}_8$.

This description of the inclusion $\mathbf{Spin}_8 \subset \mathbf{Aut}(J)$ relied on the notion of triality on the level of groups. Applying the functor Lie then gives a notion of triality for Lie algebras, which we have already seen in Cor. 51.27. Changing to the setting of group schemes has allowed us to remove the hypothesis that 2 is invertible.

53.16 Exhibiting the F_4 root system. The proof in 53.4 that $\mathbf{Aut}(J)$ is simple of type F_4 for J an Albert algebra, which relies on [268], is somewhat indirect. It argues that the root system of $\mathbf{Aut}(J)$ is a subsystem of E_6 fixed by an automorphism. Let us now make the identification of the F_4 root system more explicit, following the same outline as we did in 53.14 for type G_2.

We have just identified a subgroup of $\mathbf{Aut}(J)$ isomorphic to $\mathbf{Spin}_8$. Pick a

maximal torus T in $\mathbf{Spin}_8$. The nonzero weights of T on the Lie algebra of $\mathbf{Spin}_8$ are the roots of a root system of type D_4; we follow the notation of 47.12 and write $\alpha_1, \ldots, \alpha_4$ for a choice of simple roots as in the diagram



Since $\mathbf{Aut}(J)$ has rank 4, T is also a maximal torus in $\mathbf{Aut}(J)$. As a representation of $\mathbf{Spin}_8$, $\mathrm{Der}(J)$ is a sum of the Lie algebra of $\mathbf{Spin}_8$ and the three 8-dimensional minuscule fundamental representations of $\mathbf{Spin}_8$. In order to simplify the notation, we write simply $abcd$ for the sum $a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4$, where $a, b, c, d \in \mathbb{Q}$. The roots of D_4 are:

(i) four simple roots 1000, 0100, 0010, 0001;
(ii) three roots of height 2: 1100, 0110, 0101;
(iii) three roots of height 3: 0111, 1101, 1110;
(iv) one root of height 4: 1111;
(v) the highest root: 1211

and their negatives. The weights of the minuscule representation with highest weight dual to the simple root 1000 can be found using the Weyl character formula, and therefore easily by computer. They are

$$11\tfrac{1}{2}\tfrac{1}{2}, \quad 01\tfrac{1}{2}\tfrac{1}{2}, \quad 00\tfrac{1}{2}\tfrac{1}{2}, \quad 00(-\tfrac{1}{2})\tfrac{1}{2}$$

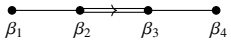
and their negatives. (Since -1 is in the Weyl group of type D_4, the lowest weight of each irreducible representation is the negative of the highest.) The weights of the other two minuscule representations are obtained by cyclically permuting the 1st, 3rd, and 4th coordinate, corresponding to the nontrivial automorphism of the Dynkin diagram. Our task is take this collection of 48 weights, which we know form a root system, and identify which root system it is.

Define

$$\beta_1 := 0100, \quad \beta_2 := 0010, \quad \beta_3 := 00(-\tfrac{1}{2})\tfrac{1}{2}, \quad \beta_4 := \tfrac{1}{2}00(-\tfrac{1}{2}).$$

Then each of the 48 weights we have exhibited can be expressed as an integral linear combination of the β_i, and for each weight the coefficients are all positive or all negative. That is, the β_i are a set of simple roots for the root system. By inspecting the linear combinations so obtained or by examining the inner

products of the β_i, we conclude that it has type F_4 as indicated in the diagram



54 Cohomology, twisted forms, and descent

In this technically demanding section, we define and prove basic results about the cohomology tools we will use in the remainder of the chapter. The culmination of this work is the Descent Theorem 54.15, which we apply to great effect in the next section.

54.1 Definition of cohomology. Given some $R \in k$-**alg**, we write $d^i\colon \otimes^n R \to \otimes^{n+1} R$ for $0 \le i \le n$ to be the map that inserts a 1 after the i-th place, i.e.,

$$d^i(r_1 \otimes \cdots \otimes r_i \otimes r_{i+1} \otimes \cdots \otimes r_n) = r_1 \otimes \cdots \otimes r_i \otimes 1 \otimes r_{i+1} \otimes \cdots \otimes r_n.$$

(In analogy with the terminology for simplicial sets, one might call the maps d^i *face maps*.) For each i, the map d^i is a homomorphism of k-algebras, so for any k-group functor $\mathbf{G}$ we obtain a homomorphism of ordinary groups $d^i\colon \mathbf{G}(\otimes^n R) \to \mathbf{G}(\otimes^{n+1} R)$. We have seen this homomorphism before in (25.6.1) and in Proposition 25.7.

Write $Z^1(R/k, \mathbf{G})$ for the collection of $g \in \mathbf{G}(R \otimes R)$ such that

$$d^1 g = (d^0 g)(d^2 g) \tag{1}$$

in $\mathbf{G}(R \otimes R \otimes R)$. Its elements are the *$R/k$-1-cocycles* with values in $\mathbf{G}$. Two 1-cocycles g, g' are said to be *equivalent* or *cohomologous*, written $g \sim g'$, if there is an element $h \in \mathbf{G}(R)$ such that

$$g' = (d^0 h) g (d^1 h)^{-1}$$

in $\mathbf{G}(R \otimes R)$. Because d^0 and d^1 are group homomorphisms, this defines an equivalence relation on $Z^1(R/k, \mathbf{G})$, and we define

$$H^1(R/k, \mathbf{G}) := Z^1(R/k, \mathbf{G})/\sim .$$

We can see that every morphism $\alpha\colon \mathbf{G} \to \mathbf{G}'$ of k-group functors induces a function $H^1(R/k, \mathbf{G}) \to H^1(R/k, \mathbf{G}')$ (directly from the definition of H^1), and we find that $H^1(R/k, -)$ is a functor from the category of k-group schemes to the category of sets.

54.2 Example: cocycles defined over k. Consider the case $R = k$. Then $\otimes^n k = \otimes^{n+1} k = k$ and $d^i = \mathbf{1}_k$. Therefore, the 1-cocycle condition (54.1.1) implies

that any $g \in Z^1(k/k, \mathbf{G})$ satisfies $g^2 = g$, i.e., g is the identity element in $\mathbf{G}$. It follows that $H^1(k/k, \mathbf{G}) = 1$.

Suppose now that $R \in k$-**alg** and $g \in Z^1(R/k, \mathbf{G})$ is the image of some $g_0 \in \mathbf{G}(k)$, i.e., $g = \vartheta(g_0)$. Then $d^i g = d^i\vartheta(g_0) = (\vartheta \otimes \vartheta \otimes \vartheta)d^i g_0$ does not depend on i, so $d^i g$ is the identity element as in the previous paragraph. When R is faithfully flat, the maps $d^i \colon R \otimes R \to R \otimes R \otimes R$ are injections by Proposition 25.7. So g is also the identity and $Z^1(R/k, \mathbf{G}) \cap \vartheta(\mathbf{G}(k)) = \{1_{\mathbf{G}}\}$.

54.3 Example: abelian G. Suppose now that $\mathbf{G}$ is abelian, meaning that the ordinary group $\mathbf{G}(R)$ is abelian for every $R \in k$-**alg**. Then for $g, g' \in Z^1(R/k, \mathbf{G})$, we have

$$d^1(gg') = (d^1 g)(d^1 g') = (d^0 g)(d^2 g)(d^0 g')(d^2 g') = d^0(gg')d^2(gg'),$$

so $Z^1(R/k, \mathbf{G})$ is itself an abelian group. Moreover, the group operation is compatible with the equivalence. For example, for $h \in \mathbf{G}(R)$ we have

$$g(d^0 h)g'(d^1 h)^{-1} = (d^0 h)gg'(d^1 h)^{-1}.$$

In summary, *if* $\mathbf{G}$ *is abelian, then* $H^1(R/k, \mathbf{G})$ *is an abelian group.*

54.4 Example: Galois cohomology. Suppose k is a field, K is a field that is a finite Galois extension of k, and $\mathbf{G}$ is a k-group functor. In that case, $H^1(K/k, \mathbf{G})$ can be viewed as a Galois cohomology set, which may be more amenable to concrete computation.

Specifically, put Γ for the group of k-automorphisms of K. We can view $\prod_\Gamma K$ as functions $\Gamma \to K$. The k-algebra homomorphism

$$w_2 \colon K \otimes K \to \prod_\Gamma K \quad \text{via } w_2(a \otimes b)(\gamma) = \gamma(a)b$$

is an isomorphism because $\dim_k K$ is finite [29, V.10.4, Cor.]. Using this identification, the homomorphisms $d^0, d^1 \colon K \to K \otimes K$ satisfy

$$d^0 a = 1 \otimes a = (\gamma \mapsto a) \quad \text{and} \quad d^1 a = a \otimes 1 = (\gamma \mapsto \gamma(a)).$$

Therefore, for $g \in \mathbf{G}(K)$, $d^i g \in \mathbf{G}(K \otimes K)$ is a function $\Gamma \to \mathbf{G}(K)$. It has

$$(d^0 g)(\gamma) = g \quad \text{and} \quad (d^1 g)(\gamma) = \gamma(g).$$

Tensoring with K, we identify $K \otimes K \otimes K$ with functions $\Gamma \times \Gamma \to K$ via $w_3(a \otimes b \otimes c)(\gamma, \delta) = \gamma(a)\delta(b)c$. We find that

$$\begin{aligned} d^0(a \otimes b) &= 1 \otimes a \otimes b = ((\gamma, \delta) \mapsto \delta(a)b), \\ d^1(a \otimes b) &= a \otimes 1 \otimes b = ((\gamma, \delta) \mapsto \gamma(a)b), \text{ and} \\ d^2(a \otimes b) &= a \otimes b \otimes 1 = ((\gamma, \delta) \mapsto \gamma(a)\delta(b)). \end{aligned}$$

Therefore, for $g \in \mathbf{G}(K \otimes K)$, equivalently $g\colon \Gamma \to \mathbf{G}(K)$, the element $d^i g\colon \Gamma \times \Gamma \to \mathbf{G}(K)$ satisfies

$$(d^0 g)(\gamma, \delta) = g(\delta), \quad (d^1 g)(\gamma, \delta) = g(\gamma), \quad \text{and} \quad (d^2 g)(\gamma, \delta) = \delta g(\delta^{-1}\gamma).$$

Putting this together, the 1-cocycle condition (54.1.1) amounts to $g(\gamma) = g(\delta) \cdot \delta g(\delta^{-1}\gamma)$ for $\gamma, \delta \in \Gamma$. Changing variables $\gamma \mapsto \gamma\delta$ and $\delta \mapsto \gamma$, we re-write the condition as

$$g(\gamma\delta) = g(\gamma) \cdot \gamma g(\delta) \tag{1}$$

for $\gamma, \delta \in \Gamma$. This formulation is the usual 1-cocycle condition from the cohomology of finite groups.

Another $g' \in Z^1(K/k, \mathbf{G})$ is equivalent to g if there is an $h \in \mathbf{G}(K)$ such that $g' = (d^0 h) g (d^1 h)^{-1}$, i.e., such that

$$g'(\gamma) = h \cdot g(\gamma) \cdot \gamma(h)^{-1}.$$

This description of $H^1(K/k, \mathbf{G})$ as equivalence classes of functions $\Gamma \to \mathbf{G}(K)$ satisfying (1) is the usual definition of Galois cohomology of the ordinary group $\mathbf{G}(K)$ with a Γ-action and is sometimes denoted $H^1(\Gamma, \mathbf{G}(K))$.

54.5 Twisted forms of modules. For a k-module M, the tensor product $M \otimes R \otimes R$ can be viewed as an $(R \otimes R)$-module in two ways, either in the natural way or through composing the natural way with a map θ defined via $\theta(m \otimes r_1 \otimes r_2) = m \otimes r_2 \otimes r_1$. When R is faithfully flat, M is identified with the submodule $M \otimes 1 \otimes 1$ of $M \otimes R \otimes R$ and Proposition 25.7 says that

$$M = \{y \in M \otimes R \mid \theta(y \otimes 1) = y \otimes 1\}.$$

We say that a k-module M' is an *$(R/k$-)twisted form* of another k-module M if there is an isomorphism of R-modules $f\colon M'_R \to M_R$. We will now relate the collection $E_M(R/k)$ of R/k-twisted forms M' of M, in case R is faithfully flat over k, with cohomology of $\mathbf{GL}(M)$ as we have just defined. Consider the diagram

$$\begin{array}{ccc} M' \otimes R \otimes R & \xrightarrow{\theta} & M' \otimes R \otimes R \\ {\scriptstyle f \otimes \mathbf{1}_R}\downarrow & & \downarrow{\scriptstyle f \otimes \mathbf{1}_R} \\ M \otimes R \otimes R & \xrightarrow{\theta} & M \otimes R \otimes R, \end{array}$$

where the θ on the top arrow is defined in a manner analogous to the one on the bottom. The diagram need not commute. Indeed, starting from the lower left corner and moving up, right, and down defines a map

$$\psi := (f \otimes \mathbf{1}_R)\theta(f \otimes \mathbf{1}_R)^{-1} \tag{1}$$

that need not equal the bottom θ. To say it differently, starting in the lower left corner and traversing the square clockwise, one finds a function $\phi := \theta\psi$ of $M \otimes R \otimes R$ that need not be the identity. Note that since the vertical arrows $f \otimes \mathbf{1}_R$ are $(R \otimes R)$-linear and the horizontal arrows θ are $(R \otimes R)$-semi-linear with respect to switching the two factors, ϕ is again $(R \otimes R)$-linear and belongs to $\mathrm{GL}(M_{R\otimes R})$.

54.6 Theorem. *The map $M' \mapsto \phi$ defined above is a function $E_M(R/k) \to H^1(R/k, \mathbf{GL}(M))$. If R is faithfully flat over k, then the map is a bijection and $E_M(R/k)$ is a set.*

Proof The crux is to verify that ϕ is a 1-cocycle. Define k-linear endomorphisms θ^e on $M' \otimes R \otimes R \otimes R$ for $e = 0, 1, 2$ instantiating the permutations (1 3), (1 2 3), (1 2) respectively of the three factors of R, i.e., for $r_1, r_2, r_3 \in R$ and $m' \in M'$, the element $m' \otimes r_1 \otimes r_2 \otimes r_3$ is sent to $m' \otimes r_3 \otimes r_2 \otimes r_1$ by θ^0, to $m' \otimes r_3 \otimes r_1 \otimes r_2$ by θ^1, and to $m' \otimes r_2 \otimes r_1 \otimes r_3$ by θ^2. Note that $\theta^1 = \theta^0\theta^2$.

Define $\psi^e := (f \otimes \mathbf{1}_R \otimes \mathbf{1}_R)\theta^e(f \otimes \mathbf{1}_R \otimes \mathbf{1}_R)^{-1}$. One finds that, if $\psi(m \otimes r \otimes a) = \sum m_i \otimes r_i \otimes a_i$, then

$$\begin{aligned}
\psi^0(m \otimes r \otimes u \otimes a) &= \sum m_i \otimes r_i \otimes u \otimes a_i, \\
\psi^1(m \otimes r \otimes u \otimes a) &= \sum m_i \otimes r_i \otimes a_i \otimes u, \\
\psi^2(m \otimes r \otimes a \otimes u) &= \sum m_i \otimes r_i \otimes a_i \otimes u.
\end{aligned} \tag{1}$$

(Note that the argument for ψ^2 is different from the others, and $\psi^2 = \psi \otimes \mathbf{1}_R$.) To see the equation involving ψ^1, for example, note that the u entry in the tensor product is not altered by $(f \otimes \mathbf{1}_R \otimes \mathbf{1}_R)^{-1}$, is moved to the last entry by θ^1, and is unchanged by $f \otimes \mathbf{1}_R \otimes \mathbf{1}_R$. Ignoring that one term, one sees that the remaining terms are mapped according to the formula (54.5.1).

Certainly

$$\psi^0\psi^2 = (f \otimes \mathbf{1}_R \otimes \mathbf{1}_R)\theta^0\theta^2(f \otimes \mathbf{1}_R \otimes \mathbf{1}_R)^{-1} = \psi^1.$$

One checks that $\psi^e = \theta^e(d^e\phi)$ for $e = 1, 2$ and $\psi^0 = \theta^1(d^0\phi)\theta^2$. Thus,

$$(d^0\phi)(d^2\phi) = \theta^1\psi^0\theta^2\theta^2\psi^2 = \theta^1\psi^1 = d^1\phi,$$

proving that ϕ is a 1-cocycle.

Now suppose that $f' \colon M' \otimes R \to M \otimes R$ is also an isomorphism. From it, we deduce $\psi' := (f' \otimes \mathbf{1}_R)\theta(f' \otimes \mathbf{1}_R)^{-1}$. Since $g := f'f^{-1}$ is an element of $\mathrm{GL}(M_R)$, $g \otimes 1 = d^1 g$, and $\theta(d^1 g)\theta = d^0 g$, we have

$$\psi' = (d^1 g)\psi(d^1 g)^{-1} \tag{2}$$

and

$$\theta\psi' = (d^0 g)\theta\psi(d^1 g)^{-1} \sim \phi. \tag{3}$$

That is, the equivalence class of ϕ depends only on M' and not on the choice of f. This proves that the map $M' \mapsto \phi$ is well defined.

Assume R is faithfully flat over k. Then $f|_{M'\otimes 1_R}$ is a k-module isomorphism between M' and $\{y \in M \otimes R \mid \theta\phi(y \otimes 1) = y \otimes 1\}$. That is, we can recover M' up to k-isomorphism from $M \otimes R$ and the 1-cocycle ϕ. If $\phi' \sim \phi$, i.e., there is a $g \in \mathrm{GL}(M_R)$ such that (3) holds, hence (2) holds, and we find that $d^1 g$ restricts to a k-module isomorphism

$$\{y \in M \otimes R \mid \psi(y \otimes 1) = y \otimes 1\} \xrightarrow{\sim} \{y' \in M \otimes R \mid \psi'(y' \otimes 1) = y' \otimes 1\}.$$

That is, the k-isomorphism class of M' depends only the equivalence class of ϕ, proving that the map $M' \mapsto \phi$ is injective.

For surjectivity, consider a 1-cocycle ϕ. Define $\psi := \theta\phi$, an $(R\otimes R)$-semilinear endomorphism of $M \otimes R \otimes R$. Define M', a k-submodule of $M \otimes R$ to make the sequence

$$0 \longrightarrow M' \longrightarrow M \otimes R \underset{\psi(\mathbf{1}_M \otimes d^1)}{\overset{\mathbf{1}_M \otimes d^1}{\rightrightarrows}} M \otimes R \otimes R \tag{4}$$

exact; we will show that $M' \mapsto \phi$. Define $\psi^e := \theta^e(d^e\phi)$ for $e = 1, 2$ and $\psi^0 = \theta^1(d^0\phi)\theta^2$ as above. Note that these definitions imply (1) and $\psi^0\psi^2 = \psi^1$.

Tensor sequence (4) with R to obtain a diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & M' \otimes R & \xrightarrow{\mathbf{1}_M \otimes d^1} & M \otimes R \otimes R & \underset{\psi^2(\mathbf{1}_M \otimes d^1)}{\overset{\mathbf{1}_M \otimes d^1}{\rightrightarrows}} & M \otimes R \otimes R \otimes R \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi^0} \\
0 & \longrightarrow & M \otimes R & \xrightarrow{\mathbf{1}_M \otimes d^1} & M \otimes R \otimes R & \underset{\mathbf{1}_M \otimes d^2}{\overset{\mathbf{1}_M \otimes d^1}{\rightrightarrows}} & M \otimes R \otimes R \otimes R
\end{array}$$

with exact rows. We check that the diagram commutes. Suppose $\mu \in M \otimes R$ and $a \in R$, and write $\psi(\mu \otimes a) = \sum \mu_i \otimes a_i$. For the box with the upper arrows, we find

$$\psi^0(\mathbf{1}_M \otimes d^1)(\mu \otimes a) = \psi^0(\mu \otimes 1_R \otimes a) = \sum \mu_i \otimes 1_R \otimes a = (1 \otimes d^1)\psi(\mu \otimes a).$$

For the box with the lower arrows, we find

$$\psi^0\psi^2(\mathbf{1}_M \otimes d^1)(\mu \otimes a) = \psi^1(\mu \otimes 1_R \otimes a) = (\mathbf{1}_M \otimes d^2)\psi(\mu \otimes a),$$

verifying the commutativity. Therefore, the vertical arrow ψ induces a unique vertical arrow f, which is an isomorphism. That is, the k-module M' constructed from ϕ maps to ϕ, verifying surjectivity.

For completeness, we note that for $\mu \in M' \subset M \otimes R$, we have

$$f(\mu \otimes a) = \psi((1_R \otimes a)(\mu \otimes 1_R)) = (a \otimes 1_R)(\mu \otimes 1_R) = a\mu \otimes 1_R.$$

That is, the R-module isomorphism $f\colon M' \otimes R \to M \otimes R$ is the obvious map arising from the fact that M' is a k-submodule of $M \otimes R$.

Finally, we note that $\mathbf{GL}(M)(R \otimes R) = \mathrm{GL}(M_{R\otimes R})$ is a set, so $Z^1(R/k, \mathbf{GL}(M))$ is a set, whence so is $H^1(R/k, \mathbf{GL}(M))$. □

54.7 Tensor systems. The same proof and statement immediately generalize to the case where M has some additional structure[1], which we now make precise. We describe various types of algebraic objects that have appeared in this text as a k-module M together with some k-linear maps between modules deduced from M, and we denote the total package by A and call such a thing a *tensor system* over k. We consider the following specific cases.

(a) A is a k-module; in this case $A = M$ and there are no additional linear maps.

(b) A is a non-associative k-algebra, as in Example 24.25. Such an algebra is determined by its multiplication, which is a linear map $M \otimes M \to M$.

(c) A is a unital non-associative k-algebra, as in 8.1. In addition to the information in (b), A has an additional linear map $k \to M$ defined by $\lambda \mapsto \lambda 1_A$, specifying 1_A.

This data is also sufficient to specify an element $A \in k$-**alg**. The additional axioms that A must satisfy to be an object of k-**alg** — namely, that the multiplication is commutative and associative — are not explicit in this setting.

(d) A is a k-group scheme $\mathbf{G}$. In this case, we take $M = k[\mathbf{G}]$. To specify the k-algebra structure on M, equivalently the scheme structure on A, we include the two linear maps from (c). To specify that $\mathbf{G}$ is a k-group functor, we add three linear maps $M \to k$, $M \to M$, and $M \to M \otimes M$ encoding the identity element, inversion, and multiplication in $\mathbf{G}$ as in Remark 24.18. (These three maps are usually called the counit, antipode, and comultiplication of $k[\mathbf{G}]$.)

(e) A is a $\mathbf{G}$-torsor $\mathbf{X}$ for a k-group scheme $\mathbf{G}$. In this case we take $M = k[\mathbf{X}]$. To specify the k-algebra structure on M, we use the two linear maps from (c). To specify the group action of $\mathbf{G} \times \mathbf{X} \to \mathbf{X}$, we add a third linear map $M \to k[\mathbf{G}] \otimes M$.

[1] Grothendieck described the situation in [110, p. 316] thusly: "On peut évidemment varier ad libitum le théorème... en introduisant des structures supplémentaires diverses sur les faisceaux (ou systèmes de faisceaux) quasi-cohérents envisagés."

The next few examples will only be considered in the case where the underlying k-module M is projective of finite constant rank, in which case $S^d(M^*)$ is naturally identified with the degree-d homogeneous forms in $\mathrm{Pol}(M,k)$, see Exc. 25.36.

(f) A is a quadratic space, as in Example 24.26. It is determined by a quadratic form q on its underlying k-module M. Viewing q as an element of $S^2(M^*)$, we may specify it via a k-linear map $k \to S^2(M^*)$ defined by $\lambda \mapsto \lambda q$.

(g) A is a conic algebra. In this case, there are three linear maps, the two from (c) encoding that it is a unital non-associative algebra and the one from (f) encoding the quadratic form. Note that the tensors for a conic algebra satisfy certain axioms, namely (16.1.1), which are not explicit in this setting.

(h) A is a para-quadratic algebra. There are two linear maps, one specifying the identity $1_A \in M$ and the other specifying the quadratic map U, which we encode as a k-linear map $k \to S^2(M^*) \otimes \mathrm{End}_k(M)$. As in the previous item, the axiom (28.1.2) that $U_{1_A} = \mathbf{1}_A$ is not explicit in this setting.

(i) A is a cubic Jordan algebra. In this case there are three linear maps, the two from (h) as well as a k-linear map $k \to S^3(M^*)$ encoding the cubic form N. Again, for a cubic Jordan algebra, there are relations among the tensors that are not explicit in this setting.

In summary, a tensor system A is a k-module M together with linear maps $\alpha_i \colon \sigma_i(M) \to \tau_i(M)$ for i in some index set I, where σ_i and τ_i are maps of the form $M \mapsto k$, $M \mapsto M \otimes M$, $M \mapsto S^d(M^*)$, or $M \mapsto M \otimes B$ for some $B \in k\text{-}\mathbf{alg}$ not depending on M. (This is the source of the name "tensor system": in the literature, one often finds the additional hypothesis that M, $\sigma_i(M)$, and $\tau_i(M)$ are finitely generated projective modules, in which case

$$\mathrm{Hom}_{k\text{-}\mathbf{mod}}(\sigma_i(M), \tau_i(M)) = \sigma_i(M)^* \otimes \tau_i(M) \tag{1}$$

by [28, II.4.2, Cor.], so α_i is an element of that module, i.e., a tensor.) We refer to σ_i, τ_i as *recipes*.

We treat tensor systems with different numbers of linear maps or different recipes as distinct kinds of objects. Suppose A' is another tensor system with the same recipes as A but with a possibly different underlying k-module M' and linear maps $\alpha_i' \colon \sigma_i(M') \to \tau_i(M')$. Each isomorphism of k-modules $f \colon M' \to M$ induces isomorphisms $\sigma_i(f) \colon \sigma_i(M') \to \sigma_i(M)$ and similarly for τ_i. We say

that f is an isomorphism $A' \xrightarrow{\sim} A$ if the diagram

$$\begin{array}{ccc} \sigma_i(M') & \xrightarrow{\alpha_i'} & \tau_i(M') \\ {\scriptstyle \alpha_i(f)}\downarrow & & \downarrow{\scriptstyle \tau_i(f)} \\ \sigma_i(M) & \xrightarrow{\alpha_i} & \tau_i(M) \end{array} \tag{2}$$

commutes for all i.

We define $\mathrm{Aut}(A)$ to be the collection of isomorphisms $A \xrightarrow{\sim} A$. It is a subset of $\mathrm{GL}(M)$ and in particular is a set. We obtain a k-group functor $\mathbf{Aut}(A)$ by setting $\mathbf{Aut}(A)(R) := \mathrm{Aut}(A_R)$ for $R \in k\text{-}\mathbf{alg}$.

54.8 Remark. For an (ordinary) group H, we can define its *opposite group* H^{op} to have the same underlying set as H but the opposite multiplication $\circ$ in the sense that $h_1 \circ h_2 := h_2 h_1$ for $h_1, h_2 \in H$. The two groups are isomorphic, via the map $H \to H^{\mathrm{op}}$ given by $h \mapsto h^{-1}$. We can imitate this construction also for a k-group functor $\mathbf{H}$ and again find an isomorphism of k-group functors $\mathbf{H} \xrightarrow{\sim} \mathbf{H}^{\mathrm{op}}$.

In particular, in cases (d) and (e) above, $\mathbf{Aut}(A)$ consists of automorphisms of the coordinate ring, whereas the automorphisms of the object viewed as a scheme are $\mathbf{Aut}(A)^{\mathrm{op}}$, compare Corollary 24.5. The previous paragraph suggests that this is only a minor distinction.

54.9 Example. Let $\mathbf{G}$ be a k-group scheme and take A to be the tensor system from case (e), obtained by regarding $\mathbf{G}$ as a $\mathbf{G}$-torsor. Then $\mathbf{Aut}(A) \cong \mathbf{G}$ by Exercise 25.45.

Let's repeat the work done for modules in 54.5, this time for tensor systems. We say that a tensor system A' is an *(R/k-)twisted form* of A if there is an isomorphism $f\colon A'_R \to A_R$ of tensor systems over R. We put $E_A(R/k)$ for the collection of isomorphism classes of R/k-twisted forms of A.

Given an element of $E_A(R/k)$, we pick a representative A' for it as well as an R-isomorphism $f\colon A'_R \to A_R$. As in 54.5, the element $\phi := \theta(f \otimes \mathbf{1}_R)\theta(f \otimes \mathbf{1}_R)^{-1}$ is in $\mathrm{GL}(A_{R\otimes R})$. But more is true. Since each α_i is k-linear, $\alpha_i \otimes \mathbf{1}_R \otimes \mathbf{1}_R$ commutes with θ. This together with commutativity of (2) gives that ϕ belongs to $\mathrm{Aut}(A_{R\otimes R})$.

54.10 Theorem. *For a tensor system A over k, the map $A' \mapsto \phi$ as just defined is a function $E_A(R/k) \to H^1(R/k, \mathbf{Aut}(A))$. If R is faithfully flat over k, the map is a bijection and $E_A(R/k)$ is a set.*

Proof Because ϕ is a 1-cocycle when viewed as an element of $\mathrm{GL}(M_{R\otimes R})$, it is also one when viewed as an element of $\mathrm{Aut}(A_{R\otimes R})$. To verify that the class

of ϕ does not depend on the choice of f, note that the element g produced in the proof of 54.6 belongs to $\mathrm{Aut}(A_R)$. This proves that the map is well defined.

As in the proof of 54.6, we note that given the 1-cocycle ϕ, the set $M'' := \{y \in M_R \mid \theta\phi(y \otimes 1) = y \otimes 1\}$ is a k-submodule. To argue that the map is an injection, we note that $f|_{M'\otimes 1_R}$ is an isomorphism $M' \xrightarrow{\sim} M''$. Repeating that argument from 54.6, the element g belongs to $\mathrm{Aut}(A_R)$ and so $d^1 g$ is an isomorphism of tensor systems over k.

For surjectivity, we suppose we are given a 1-cocycle ϕ and consider the fixed submodule M'' of M_R. For each recipe $\alpha\colon \sigma(M) \to \tau(M)$ of M, we obtain

$$\alpha''_R := \tau(f)^{-1}\alpha\sigma(f)\colon \sigma(M''_R) \to \tau(M''_R),$$

and we claim that α''_R comes from a unique $\alpha'' \in \mathrm{Hom}_{k\text{-}\mathbf{mod}}(\sigma(M''), \tau(M''))$. To see this, we compute

$$\begin{aligned}\theta(\alpha''_R \otimes \mathbf{1}_R)\theta &= \theta(\tau(f)^{-1} \otimes \mathbf{1}_R)(\alpha \otimes \mathbf{1}_R)(\sigma(f) \otimes \mathbf{1}_R)\theta \\ &= (\tau(f)^{-1} \otimes \mathbf{1}_R)\psi(\alpha \otimes \mathbf{1}_R)\psi(\sigma(f) \otimes \mathbf{1}_R) \\ &= (\tau(f)^{-1} \otimes \mathbf{1}_R)(\alpha \otimes \mathbf{1}_R)(\sigma(f) \otimes \mathbf{1}_R) = \alpha''_R \otimes \mathbf{1}_R,\end{aligned}$$

which proves the claim by Exercise 25.44. □

54.11 Lemma. *If $R \to S$ is a homomorphism of k-algebras and A is a tensor system, then $E_A(R/k)$ is naturally contained in $E_A(S/k)$.*

Proof For A a k-module,

$$A' \otimes_k S \cong A' \otimes_k (R \otimes_R S) \cong (A' \otimes_k R) \otimes_R S, \tag{1}$$

by 9.4. If $A' \otimes R \cong A \otimes R$, then applying (1) and running the same computation in reverse, we find that $A' \otimes S \cong A \otimes S$, proving the claim in this case. □

Each homomorphism of k-algebras $R \to S$ gives a map

$$\inf\colon H^1(R/k, \mathbf{G}) \to H^1(S/k, \mathbf{G})$$

known as *inflation*, which a priori depends on the homomorphism $R \to S$. We have:

54.12 Lemma. *If $R \to S$ is a homomorphism of faithfully flat k-algebras and A is a tensor system, then we have a commutative diagram of sets*

$$\begin{array}{ccc} E_A(R/k) & \longrightarrow & E_A(S/k) \\ \cong\downarrow & & \downarrow\cong \\ H^1(R/k, \mathbf{Aut}(A)) & \xrightarrow{\inf} & H^1(S/k, \mathbf{Aut}(A)) \end{array}$$

where the horizontal arrows are injective and do not depend on the choice of homomorphism $R \to S$.

Proof Tracking the proof of Theorem 54.10, we find that the bottom arrow is given by going up, right, and down, i.e., the diagram commutes. Because the top arrow does not depend on the homomorphism $R \to S$, neither does the bottom arrow. Injectivity of the top arrow (Lemma 54.11) gives injectivity of the bottom arrow. □

54.13 A set-theoretic excursion. Except in the trivial case where k is the zero ring, the category of k-algebras is not *small*, meaning that the collection of k-algebras is not a set, see Exercise 54.22. Consider instead the full subcategory C whose objects are finitely presented k-algebras. Each finitely presented k-algebra R is isomorphic to $k[\mathbf{t}_1, \dots, \mathbf{t}_n]/(f_1, \dots, f_r)$ for some $n, r \in \mathbb{N}$ and $f_1, \dots, f_r \in k[\mathbf{t}_1, \dots, \mathbf{t}_n]$. One may view the tuple $(f_1, \dots, f_r)$ as determining R up to isomorphism in C. In this way, we obtain every finitely presented k-algebra from an element of the *set*

$$\bigcup_{n\in\mathbb{N}} \bigcup_{r\in\mathbb{N}} k[\mathbf{t}_1, \dots, \mathbf{t}_n]^r.$$

Certainly multiple elements of this set will lead to the same isomorphism class of algebra. Using the Axiom of Choice, we may pick one element of the set for each isomorphism class of finitely presented k-algebras, showing that the collection of isomorphism classes of such algebras is a set. (The fancy language for this is that C "has a small skeleton.") One deduces from this that the collection of isomorphism classes of fppf k-algebras (resp. étale k-algebras; resp. étale covers of k) is also a set.

54.14 Twisted forms with no reference to R. Consider now a diagram of objects and arrows, where the objects are isomorphism classes of fppf k-algebras and one includes an arrow $R \to S$ if there is a k-algebra homomorphism $R \to S$. Note that the collection of objects in the diagram is a set as explained in 54.13. From this, we construct a new diagram by applying $E_A(-/k)$ to each of the objects, for some tensor system A over k. Note that for each homomorphism $R \to S$, there is an arrow $E_A(R/k) \to E_A(S/k)$ that does not depend on the specific choice of $R \to S$, and so the collection $\{E_A(R/k)\}$ forms a directed set (thanks to 54.13). We define

$$E_A(k) := \varinjlim_R E_A(R/k) \quad \text{for fppf } R \in k\text{-}\mathbf{alg},$$

which is a set [32, §III.7.6]. An element of $E_A(k)$ is called a *twisted form of A*.

Similarly, in view of Lemma 54.12, we may define

$$H^1(k, \mathbf{Aut}(A)) := \varinjlim_R H^1(R/k, \mathbf{Aut}(A)) \quad \text{for fppf } R \in k\text{-}\mathbf{alg}.$$

We call it the *fppf* or *flat cohomology* set of $\mathbf{Aut}(A)$. Combining Theorem 54.10 and Lemma 54.12 gives the result we have been aiming for.

54.15 Descent Theorem. *For every tensor system A over k, the map $E_A(k) \to H^1(k, \mathbf{Aut}(A))$ is a bijection and $E_A(k)$ is a set.* □

54.16 Example. The twisted forms of k^n are the rank n projective modules, for $n \in \mathbb{N}$, compare 25.5. The group scheme $\mathbf{Aut}(k^n)$ is $\mathbf{GL}_n$. Therefore:

(a) The case $n = 1$ concerns line bundles. We have $\mathbf{GL}_1 = \mathbf{G_m}$, and in this case the Descent Theorem says that $H^1(k, \mathbf{G_m}) = \mathrm{Pic}(k)$.

(b) If k is such that every rank n projective k-module is free (e.g., if k is an LG ring or a principal ideal domain), then by the Descent Theorem the set $H^1(k, \mathbf{GL}_n) = 1$.

54.17 Étale cohomology. Define

$$H^1_{\text{ét}}(k, \mathbf{G}) := \varinjlim_R H^1(R/k, \mathbf{G}) \quad \text{for étale covers } R \in k\text{-}\mathbf{alg}.$$

It too is a set by the same reasoning as for the fppf cohomology set $H^1(k, \mathbf{G})$. It is the *étale* 1-cohomology of $\mathbf{G}$, as opposed to the flat 1-cohomology set $H^1(k, \mathbf{G})$. Because every étale cover is faithfully flat, there is a natural inclusion $H^1_{\text{ét}}(k, \mathbf{G}) \subseteq H^1(k, \mathbf{G})$. We state:

54.18 Proposition. *For A a tensor system, the natural map $H^1_{\text{ét}}(k, \mathbf{Aut}(A)) \to H^1(k, \mathbf{Aut}(A))$ is injective. If $\mathbf{Aut}(A)$ is a smooth k-group scheme, then the map is an isomorphism.*

Proof Because étale covers are faithfully flat, the first claim is a consequence of Lemma 54.12. For the second claim, we need only show surjectivity. Given an element of $H^1(k, \mathbf{Aut}(A))$, by the Descent Theorem we may identify it with a $\mathbf{Aut}(A)$-torsor $\mathbf{X}$ over k in the flat topology. Since $\mathbf{Aut}(A)$ is smooth, $\mathbf{X}$ is also a torsor in the étale topology as explained in 25.26. That is, there is an étale cover R of k such that $\mathbf{X}(R)$ is nonempty, i.e., $\mathbf{X} \in H^1(k, \mathbf{Aut}(A))$ is in the image of $H^1_{\text{ét}}(R/k, \mathbf{Aut}(A)) \subseteq H^1_{\text{ét}}(k, \mathbf{Aut}(A))$. □

54.19 Cohomology over a field. In case $\mathbf{G}$ is a group scheme over a field F, we can describe the sets $H^1(F, \mathbf{G})$ and $H^1_{\text{ét}}(F, \mathbf{G})$ in a way that can be more

amenable to computation. Write $\bar{F}$ and F_s for the algebraic and separable closures of F, respectively. There is a natural commutative diagram

$$\begin{array}{ccc} H^1(F_s/F, \mathbf{G}) & \longrightarrow & H^1(\bar{F}/F, \mathbf{G}) \\ \downarrow & & \downarrow \\ H^1_{\text{ét}}(F, \mathbf{G}) & \longrightarrow & H^1(F, \mathbf{G}) \end{array} \tag{1}$$

where all the arrows come from the inflation map and are therefore injective by Lemma 54.12. In fact, *the vertical maps are isomorphisms*. To see this, view $H^1(F, \mathbf{G})$ as the collection of $\mathbf{G}$-torsors over F in the flat topology. For such a torsor $\mathbf{X}$, $\mathbf{X}(\bar{F})$ is nonempty by the Nullstellensatz (Proposition 25.28), so $\mathbf{X}$ is in the image of the right vertical arrow. The same argument using the separable Nullstellensatz shows that the left vertical arrow is a bijection.

54.20 Proposition. *Let* $\mathbf{G}$ *be a group scheme over a field* F *such that* $k[\mathbf{G}]$ *is finitely generated. If* $\mathbf{G}$ *is smooth or* F *is perfect, then*

$$H^1(F, \mathbf{G}) = H^1_{\text{ét}}(F, \mathbf{G}) = \varinjlim_K H^1(K/F, \mathbf{G})$$

where the limit runs over finite Galois extensions K *of* F.

Proof If $\mathbf{G}$ is smooth, then the bottom arrow in diagram (54.19.1) is a bijection (Prop. 54.18). If F is perfect, then $F_s = \bar{F}$ and the top arrow is a bijection. In either case, we conclude that all arrows in the diagram are bijections and we use them to identify the four sets, leading to $H^1(F, \mathbf{G}) = H^1_{\text{ét}}(F, \mathbf{G}) = H^1(F_s/F, \mathbf{G})$.

The inflation maps $H^1(K/F, \mathbf{G}) \to H^1(F_s/F, \mathbf{G})$ give by Lemma 54.12 a natural inclusion $\varinjlim_K H^1(K/F, \mathbf{G}) \subseteq H^1(F_s/F, \mathbf{G})$. Now, each $g \in Z^1(F_s/F, \mathbf{G})$ is an element of $\mathbf{G}(F_s \otimes F_s) = \operatorname{Hom}_{k\text{-}\mathbf{alg}}(k[\mathbf{G}], F_s \otimes F_s)$. For each element x of $k[\mathbf{G}]$, $g(x)$ is a sum of finitely many terms $y \otimes y'$ with $y, y' \in F_s$, and it follows that $g(k[\mathbf{G}])$ is contained in a finitely generated subfield L of F_s, which is necessarily finite dimensional over F. Taking K to be the Galois closure of L, we see that g belongs to the subset $H^1(K/F, \mathbf{G})$, proving the second claimed equality. □

Most of the group schemes we study in this chapter are smooth, so the proposition applies. This rephrases the problem of computing $H^1(F, \mathbf{G})$ into one of studying the sets $H^1(K/F, \mathbf{G})$, which can be viewed as the Galois cohomology sets from Example 54.4, where results from the literature are more readily available.

54.21 Bibliographic notes. The definition of cohomology in 54.1 follows

[110, p. 311], [103, III.3.6.1], and [293, 17.6]; it is a kind of Čech cohomology. The proof of Theorem 54.6 is a re-organization of arguments in [293, Ch. 17]; for a different view see for example [110, p. 312], [158, p. 36, Th. 3.2], or [290, Th. 4.23]. See [42, §2.1] for a different view on the notion of tensor system from 54.7. Theorem 54.10, proved here for tensor systems, can be found in the literature proved for k-algebras in [158, p. 38, Th. 3.4] or [290, Th. 4.29].

For other views on the material in this section, see [103] or [54, §3] (where k is replaced by a base scheme), [158] (for k a ring as here), or [260] or [160, 29.1] (for k a field).

Exercises

54.22. For each of the collections

- isomorphism classes of k-modules (i.e., objects in k-**mod**)
- isomorphism classes of k-algebras (i.e., objects in k-**alg**)

prove that the following are equivalent:

(i) The collection is a set.
(ii) The collection is a singleton.
(iii) The ring k is the zero ring.

54.23. Suppose A is a tensor system whose underlying k-module M and each of the $\sigma_i(M)$ and $\tau_i(M)$ are finitely generated projective. Prove that $\mathbf{Aut}(A)$ is a closed subfunctor of $\mathbf{GL}(M)$ (as defined in 24.15) and hence is a k-group scheme.

54.24. Suppose V is a finite-dimensional vector space over a field k and $f\colon V \to k$ is a homogeneous polynomial law of degree $d > 0$. The group functor $\mathbf{Aut}(f)$ such that

$$\mathbf{Aut}(f)(R) = \{g \in \mathrm{GL}(V \otimes R) \mid f_R \circ g = f_R\}$$

for all $R \in k$-**alg** is a closed sub-group-scheme of $\mathbf{GL}(V)$ by Exc. 54.23. Prove: If $\mathbf{Aut}(f)$ is isotropic, then there is a nonzero $v \in V$ such that $f_k(v) = 0$.

54.25. *Lang's Theorem.* Let F be the finite field with q elements. It is the collection of elements in its algebraic closure $\bar{F}$ fixed by the Frobenius automorphism $\sigma\colon x \mapsto x^q$. Lang's Theorem [269, Thm. 4.4.17] says that, for every finitely generated and connected group scheme $\mathbf{G}$ over F, every element of $\mathbf{G}(\bar{F})$ is of the form $\sigma(g)g^{-1}$ for some $g \in \mathbf{G}(\bar{F})$. Use this to prove that $H^1(F, \mathbf{G}) = 0$.

Remark. Sometimes this result is itself called "Lang's Theorem", see for example [293, §18.8].

54.26. Suppose k is a finite ring and $\mathbf{G}$ is a smooth and connected k-group scheme. Verify that $H^1(k, \mathbf{G}) = 0$.

(*Hint*: Compare Exercise 40.17.)

54.27. For any finite group Γ, the corresponding constant group scheme $\mathbf{X}_\Gamma$ from 24.20 is defined over $\mathbb{Z}$. The set $\mathbf{X}_\Gamma(\mathbb{Z}) \cong \Gamma$ has a canonical image in $\mathbf{X}_\Gamma(K)$ for every $K \in$

$\mathbb{Z}$-**alg**; call elements of this image *constant elements*. Let A be a tensor system over $k \in \mathbb{Z}$-**alg** and suppose there is a morphism of k-group functionrs $f\colon \mathbf{Aut}(A) \to \mathbf{X}_\Gamma$. Prove: If, for every $K \in k$-**alg**, the image of $f(K)\colon \mathrm{Aut}(A_K) \to \mathbf{X}_\Gamma(K)$ contains all the constant elements, then $f(K)$ is surjective for every $K \in k$-**alg**.

55 Applications of the Descent Theorem

In this and the following sections, we apply the Descent Theorem 54.15 to prove various classification results concerning the kinds of algebras studied elsewhere in the book. As a first example, let us consider a Jordan k-algebra J. We call J *étale* if there is a (finite) étale $E \in k$-**alg** such that $J \cong E^{(+)}$. We call J *split étale* if it is $E^{(+)}$ where E is a product of finitely many copies of k. (These definitions agree with the one in Ex. 34.17.) With this language, we now prove the following generalization of the result of Exercise 39.42(b).

55.1 Proposition. *(a) Let J be a Jordan k-algebra. If there is an fppf $R \in k$-**alg** such that the Jordan R-algebra J_R is étale, then J is étale.*

(b) If E, E' are finite étale k-algebras such that $E^{(+)} \cong E'^{(+)}$ as Jordan algebras, then $E \cong E'$.

Proof Suppose J_R is étale, so it is finitely generated projective as an R-module, and therefore J is finitely generated projective as a k-module, see 25.5.

Suppose k is connected, in which case J has constant rank, call it r. Put E for a product of r copies of k, the split étale k-algebra. There is an fppf $S \in R$-**alg** such that $J_S \cong (J_R)_S \cong (E_S)^{(+)}$; note that the composition $k \to R \to S$ is also fppf, see 25.3 and 25.15. Now, the natural map $\mathbf{Aut}(E) \to \mathbf{Aut}(E^{(+)})$ is an isomorphism of k-group schemes (Exercise 29.24), and the Descent Theorem 54.15 shows that the map $L \mapsto L^{(+)}$ defines a bijection between twisted forms of E (i.e., étale k-algebras by Exercise 25.47) and twisted forms of $E^{(+)}$, i.e., claim (b). As J is one of the latter, it is of the form $L^{(+)}$ for some étale $L \in k$-**alg**.

One reduces to the case where k is connected in the same manner as in the proof of 26.9, 26.10, completing the proof. □

For every Freudenthal k-algebra J of rank 3, there is an fppf $R \in k$-**alg** such that $J_R \cong (R \times R \times R)^{(+)}$ by Cor. 39.32, so the proposition gives the following, which we already knew from Exc. 39.42(b):

55.2 Corollary. *The map $E \mapsto E^{(+)}$ defines a bijection between the isomorphism classes of rank 3 (commutative, associative) étale k-algebras and the isomorphism classes of rank 3 Freudenthal k-algebras.* □

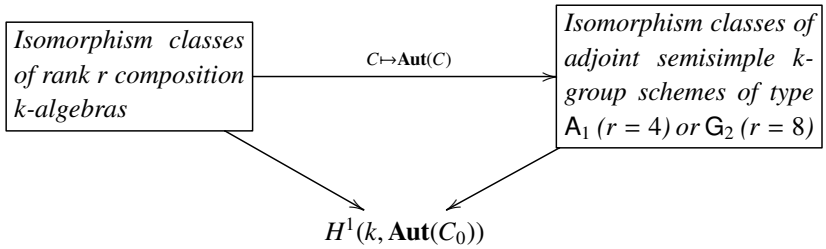
For A a composition algebra of rank > 2 or Freudenthal algebra of rank > 3, $\mathbf{Aut}(A)$ is either a semisimple group or closely related to one, and the following result highlights a major theme.

55.3 Lemma. *If* $\mathbf{G}$ *is a semisimple* k*-group scheme that is adjoint and whose Dynkin diagram has no nontrivial automorphisms, then the conjugation map* $\mathbf{G} \to \mathbf{Aut}(\mathbf{G})$ *is an isomorphism and* $H^1(k, \mathbf{G}) = E_{\mathbf{G}}(k)$.

Proof The claim that $\mathbf{G} \to \mathbf{Aut}(\mathbf{G})$ is an isomorphism is part of 52.9. The Descent Theorem gives the second claim. □

We immediately apply this to the case of composition algebras. Recall that, if A is a quaternion or octonion algebra, then $\mathbf{Aut}(A)$ is an adjoint semisimple group of type A_1 or G_2 respectively by Theorem 53.1. (Because all group schemes of type G_2 are adjoint, we may suppress the adjective in that case.)

55.4 Proposition. *Let* C_0 *be a composition algebra of rank* $r = 4$ *or* 8 *over* k. *In the diagram*



all arrows are bijections that are functorial in k. *In the top bijection, the split composition algebra in the sense of 39.20 corresponds to the split group scheme.*

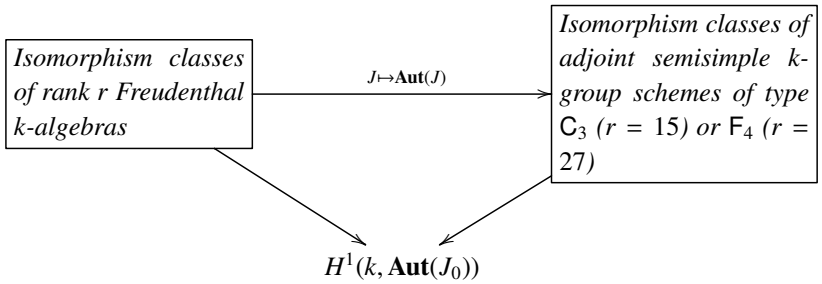
Proof Suppose C is a composition k-algebra of rank 4 or rank 8. Then $\mathbf{Aut}(C)$ is a group of the required type, by Theorem 53.1, and $\mathbf{Aut}(C)$ is split if C is split. The Dynkin diagrams of A_1 and G_2 have no nontrivial automorphisms, so by Lemma 55.3 $\mathbf{Aut}(\mathbf{Aut}(C)) = \mathbf{Aut}(C)$. Applying the Descent Theorem twice, we get bijections

$$E_C(k) \xrightarrow{\sim} H^1(k, \mathbf{Aut}(C)) = H^1(k, \mathbf{Aut}(\mathbf{Aut}(C))) \xleftarrow{\sim} E_{\mathbf{Aut}(C)}(k),$$

which is what was claimed. □

We now return to studying Freudenthal algebras. Recall that, if J is a Freudenthal algebra of rank 15 or 27, then $\mathbf{Aut}(J)$ is an adjoint semisimple group of type C_3 or F_4 respectively by Theorem 53.4. (Because all group schemes of type F_4 are adjoint, we may suppress the adjective in that case.)

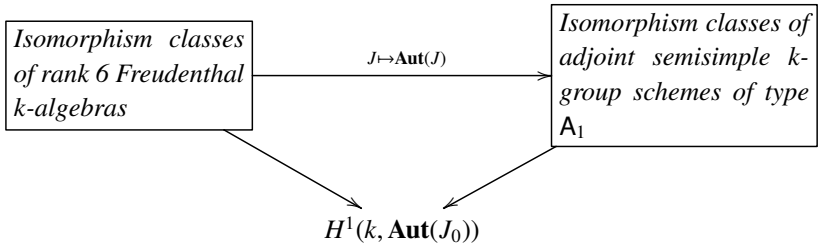
55.5 Proposition. *Let J_0 be a Freudenthal k-algebra of rank $r = 15$ or 27. In the diagram*



all arrows are bijections that are functorial in k. In the top bijection, the split Freudenthal algebra in the sense of 39.20 corresponds to the split group scheme.

Proof The proof proceeds in the same way as the proof of Proposition 55.4, referring to Proposition 53.4 for the fact that $\mathbf{Aut}(J)$ is a group scheme of the required type. The claim about split groups was already addressed in 53.4. □

55.6 Proposition. *Suppose k is a ring, 2 is invertible in k, and J_0 is a Freudenthal k-algebra of rank 6. In the diagram*



all arrows are bijections that are functorial in k. In the top bijection, the algebra $\mathrm{Her}_3(k, \mathrm{diag}(-1, 1, -1))$ corresponds to the split group.

Proof The proof proceeds in the same way as the proof of Proposition 55.4, referring to Corollary 53.10 for the fact that $\mathbf{Aut}(J)$ is a group scheme that is adjoint semisimple of type A_1. The claim about the split group is Corollary 53.8. □

We may use similar techniques to prove the following.

55.7 Proposition. *Suppose A and A' are both*

(1) Albert algebras over a ring k; or
(2) octonion algebras over a ring k such that $2 \in k^\times$.

Then:

(a) $\mathbf{Aut}(A) \cong \mathbf{Aut}(\mathrm{Der}(A))$.
(b) $A \cong A'$ *if and only if* $\mathrm{Der}(A) \cong \mathrm{Der}(A')$.

Proof We first claim that $\mathbf{Aut}(\mathrm{Der}(A))$ is a semisimple affine group scheme of type F_4 in case (1) or G_2 in case (2). Like in the previous proofs, it suffices to verify this in the case where A is split and $k = \mathbb{Z}$ for (1) or $\mathbb{Z}[1/2]$ for (2), in which case it suffices to verify the claim when k is replaced by an algebraically closed field. That case is verified in [272] and [123, esp. p. 456].

Now let us prove (a). Since $\mathrm{Der}(A) = \mathrm{Lie}(\mathbf{Aut}(A))$ by 52.1, the adjoint representation provides a natural homomorphism

$$\mathrm{Ad}\colon \mathbf{Aut}(A) \to \mathbf{Aut}(\mathrm{Der}(A)).$$

The kernel of this homomorphism is the (scheme-theoretic) center of $\mathbf{Aut}(A)$ [101, Prop. XXII.5.7.14], which is trivial for our particular choices of A. It follows that Ad is an isomorphism [101, Thm. XXIII.4.1], proving (a).

Claim (b) follows from (a) as in the proof of Prop. 55.4. □

The hypothesis "$2 \in k^\times$" in (2) cannot simply be dropped because (b) fails for octonion algebras over a field of characteristic 2 by Prop. 49.9. The proof breaks down in that case because $\mathbf{Aut}(\mathrm{Der}(C))$ has type C_3 [123] and therefore is of dimension 21 not 14.

We now combine very strong theorems about reductive group schemes with Propositions 55.4 and 55.5 to obtain classification results for the algebras we are interested in.

55.8 Corollary. *Let k be*

(i) *a regular local ring containing a field, or*
(ii) $k_0[\mathbf{t}]$ *for a field* k_0.

Write K for the field of fractions of k. If A and A' are both

- *composition k-algebras of rank 4 or rank 8, or*
- *Freudenthal k-algebras of rank 15 or rank 27*

and $A_K \cong A'_K$, then $A \cong A'$.

Proof Take $\mathbf{G} := \mathbf{Aut}(A)$. By Theorem 53.1 or 53.4, it is a simple k-group scheme that is adjoint of type A_1, G_2, C_3, or F_4. Propositions 55.4 and 55.5, combined with Lemma 55.3, show that the claim is equivalent to the statement that the natural map $H^1(k, \mathbf{G}) \to H^1(K, \mathbf{G})$ has trivial kernel. Because $\mathbf{G}$ is smooth, by Proposition 54.18 this map is the same as $H^1_{\text{ét}}(k, \mathbf{G}) \to H^1_{\text{ét}}(K, \mathbf{G})$,

which is injective by the hypotheses on k by [79] and [206] in case (i) and by [47, Lemma 3.5.4] in case (ii). □

In a similar vein, we can obtain classification results for composition algebras and Jordan algebras over special fields including those from 23.12–23.23 and 46.15–46.21 by using arguments in terms of semisimple group schemes and cohomology rather than dealing exclusively with algebras as was done in earlier chapters. For example, the argument of Exc. 40.17 for finite fields could be replaced by Exc. 54.26. For global fields, one could replace the role of the Hasse-Minkowski Theorem and Cor. 46.19 in the proof of the classification results 23.22 and 23.23 for octonions and 46.20 and 46.21 for Albert algebras by an appeal instead to the Local-Global Principle for Galois cohomology of simply connected semisimple groups over a global field that one can find in Theorem 6.6 on p. 286 of [234] (for algebraic number fields) or in [113] and [115].

55.9 Vista: fields of cohomological dimension ≤ 2. Several of the special kinds of fields discussed in this book belong to a broader class of fields where the classification results for Albert and octonion algebras still hold. Separably closed fields, finite fields, the C_2 fields of 46.15(e), local fields, and the global fields of Cor. 46.19 with no real embeddings are all examples of "fields of (separable) cohomological dimension ≤ 2". We omit the precise definition and refer the reader to [98, esp. §4.5] or [262, Ch. II]. For such a field F, one can prove that *every octonion or Albert F-algebra A is split*. Indeed, one observes that $\mathbf{G} := \mathbf{Aut}(A)$ is of type G_2 or F_4 respectively, and its subgroup $\mathbf{G}'$ corresponding to the long roots with respect to any maximal torus is simply connected of type A_2 or D_4. Then one shows that $H^1(F, \mathbf{G}') = 1$ and that this implies $H^1(F, \mathbf{G}) = 1$, see for example [98, p. 94] or [234, §6.8]. (Alternatively, the hypothesis on cohomological dimension implies that the cohomological invariants of degree ≥ 3 described in the next subsection all vanish, which implies the claim.)

The remaining kinds of special fields we have considered, namely $\mathbb{R}$ and number fields with a real embedding, are examples of "fields of virtual cohomological dimension ≤ 2". For such a field F, two octonion or Albert F-algebras A, A' are isomorphic if and only if $A_R \cong A'_R$ for every real closed field R containing F, see [20, §8, 9].

55.10 Vista: cohomological invariants. Given an F-group functor $\mathbf{G}$, we get a functor from the category of fields containing F (a full subcategory of F-**alg**) and **set** defined by $K \mapsto H^1(K, \mathbf{G})$, which we denote by $H^1(-, \mathbf{G})$. One can also define abelian groups $H^3(K, \mathbb{Z}/n\mathbb{Z}(2))$ for all n as in [94], which gives

another functor $K \mapsto H^d(-, \mathbb{Z}/n\mathbb{Z}(d-1))$ for $d \geq 0$. A morphism of functors $H^1(-, \mathbf{G}) \to H^d(-, \mathbb{Z}/n\mathbb{Z}(d-1))$ is sometimes called a *mod-n cohomological invariant of degree d*; it is *normalized* if it sends the trivial class to the zero element. For $\mathbf{G}$ the automorphism group of the split Albert F-algebra, there is a mod-6 cohomological invariant of degree 3. It was discovered by Markus Rost [250] and is a specific case of a general construction known as the Rost invariant, which is discussed in [94]. Because $H^d(K, \mathbb{Z}/n\mathbb{Z}(d-1))$ is an abelian group of exponent dividing n for all K, the Rost invariant of this choice of $\mathbf{G}$ is a sum of a mod-2 and mod-3 cohomological invariant, which can be viewed as associating with each Albert K-algebra J elements $f_3(J) \in H^3(K, \mathbb{Z}/2\mathbb{Z}(2))$ and $g_3(J) \in H^3(K, \mathbb{Z}/3\mathbb{Z}(2))$. Concrete descriptions of $f_3(J)$ and $g_3(J)$ in terms of Albert algebras can be found in [228], [229], and [231], and we have seen $f_3(J)$ in another guise already in 41.25(iii).

One key property of $g_3(J)$, proved using Albert algebras, is that J is division if and only if $g_3(J) \neq 0$. From this we trivially deduce: *If F is a field such that $H^3(F, \mathbb{Z}/3\mathbb{Z}(2)) = 0$, then every Albert F-algebra is reduced.* Since the familiar examples of fields F such as $\mathbb{R}$ and global fields have $H^3(F, \mathbb{Z}/3\mathbb{Z}(2)) = 0$, this viewpoint sheds light on the historical challenge — described in the introduction to §46 — that arose in trying to produce an example of an Albert division algebra.

These cohomological invariants have been leveraged to prove various isomorphism criteria for Albert algebras, see for example [50] or [112, Prop. 4.3.5].

Exercises

55.11. Suppose J is a rank 3 Freudenthal algebra over an infinite field k. Verify that the set $\{j \in J \mid k[j] = J\}$ is non-empty and Zariski-open in J.

55.12. *Freudenthal algebras of rank 9 over a field.* Suppose F is a field. Show that there are natural bijections between isomorphism classes of (a) involutorial systems as defined in 44.2 $(K, B, \tau, 1)$ where K is quadratic étale over F and the rank of B as a K-module is 9; (b) rank 9 Freudenthal F-algebras $H(B, \tau)$; and (c) adjoint semisimple F-group schemes of type A_2.

(*Hint*: Use Proposition 54.19 to connect the Descent Theorem with results for Galois cohomology in [160, p. 346 and §29.D].)

55.13. *Freudenthal algebras of rank 15 over a field.* Let A be an Azumaya algebra of degree d over a field F. An F-linear involution τ on A is *symplectic* if $\mathrm{Symd}(A, \tau)$ contains 1_A and has dimension $d(d-1)/2$. Recall from 29.8 that $\mathrm{Symd}(A, \tau)$ is a Jordan subalgebra of $A^{(+)}$ when τ is symplectic.

Show that the maps $(A, \tau) \mapsto \mathrm{Symd}(A, \tau)$ and $J \mapsto \mathbf{Aut}(J)$ define bijections of isomorphism classes between

(i) Azumaya F-algebras with symplectic involution (A, τ) where A has degree 6;
(ii) rank 15 Freudenthal F-algebras J; and

(iii) adjoint semisimple F-group schemes of type C_3.

Remark. The definition of symplectic involution given here agrees with the one in [160], see especially Proposition 2.6 in that reference. Indeed, if $\operatorname{char} F \neq 2$, the definition is that $\operatorname{Sym}(A,\tau)$ has dimension $d(d-1)/2$, and it is clear that 1_A is in $\operatorname{Sym}(A,\tau) = \operatorname{Symd}(A,\tau)$. If $\operatorname{char} F = 2$, then $\dim_F \operatorname{Alt}(A,\tau) = d(d-1)/2$ and the definition is that 1_A is in $\operatorname{Alt}(A,\tau)$, so it suffices to note that $\operatorname{Alt}(A,\tau) = \operatorname{Symd}(A,\tau)$.

56 Examples of Albert algebras over $\mathbb{Z}$

We now take a pause from group schemes to return to the setting of Albert algebras as in Chapter VI. Our aim is to exhibit two Albert algebras over $\mathbb{Z}$, Λ and Λ_0, and prove that they are not isomorphic (Thm. 56.6).

56.1 The cubic euclidean Jordan matrix algebras revisited. As in §5, we let $\mathbb{D}$ be one of the four real composition division algebras $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$, which by Thm. 5.10 gives rise to the cubic euclidean Jordan algebra $J := \operatorname{Her}_3(\mathbb{D})$. Being finite-dimensional as a real vector space, J carries the natural topology with respect to which $J^\times \subseteq J$ is an open subset. We denote by $\operatorname{Pos}(J)$ the connected component of 1_J in $J^\times$. and call it the *positive cone* of J because, by characterization (iii) of Exc. 56.7 (b) below, it is a cone in the sense of being stable under linear combinations with strictly positive real coefficients. Since $J^\times$ is locally connected, $\operatorname{Pos}(J)$ is not only closed but, in fact, also open in $J^\times$. The closure of $\operatorname{Pos}(J)$ in J will be called the *non-negative* cone of J, denoted by $\overline{\operatorname{Pos}}(J)$.

Since the bilinearized norm of $\mathbb{D}$ gives rise to a positive definite inner product (1.6), so does the bilinear trace of J (5a.3). Moreover, from (5.7.1) and (33a.24) we derive the relations

$$T(x \bullet y) = \frac{1}{2} T(x \circ y) = T(x,y)$$

for all $x, y \in J$, and we conclude from (33a.33) that the linear trace of J is an associative linear form relative to the bilinear Jordan product $x \bullet y$:

$$T(x \bullet y, z) = T(x, y \bullet z) \qquad (x,y,z \in J). \tag{1}$$

In order to carry out the transition from the euclidean Albert algebra over the reals to the one over the integers, we fix a Cartan-Schouten basis $E = (u_i)_{0 \leq i \leq 7}$ of $\mathbb{O}$ in the sense of 2.1. We then write $M := \operatorname{DiCo}(\mathbb{O})$ for the corresponding $\mathbb{Z}$-structure of Dickson-Coxeter octonions (Thm. 4.5). It follows from Ex. 6.6 that

$$\Lambda := \operatorname{Her}_3(M) \subseteq J := \operatorname{Her}_3(\mathbb{O}) \tag{2}$$

is a $\mathbb{Z}$-structure of the euclidean Albert algebra $\mathrm{Her}_3(\mathbb{O})$.

We proceed to the detailed study of some elements of Λ. The next few results, 56.2–56.5, re-interpret some clever computations from [71, §5] in the language of Jordan algebras and isotopes as developed in this book.

56.2 Lemma. *The algebra Λ contains exactly three elementary idempotents, namely e_{ii} for $1 \le i \le 3$.*

Proof Let e be an elementary idempotent in Λ, written in the form

$$e = \sum (\alpha_i e_{ii} + w_i[jl]) \qquad (\alpha_i \in \mathbb{Z}, \quad w_i \in M, \quad 1 \le i \le 3).$$

Then $e^\sharp = 0$ and e has trace 1, which by (36.4.4) and (36.4.8) amounts to

$$\alpha_j \alpha_l = n_{\mathbb{O}}(w_i), \quad \alpha_i w_i = \overline{w_j w_l}, \quad \alpha_1 + \alpha_2 + \alpha_3 = 1 \qquad (1 \le i \le 3). \tag{1}$$

From Exc. 56.7 (c) we deduce $e = e^2 \in \overline{\mathrm{Pos}}(J)$, and Exc. 56.10 (b) implies $\alpha_i \ge 0$ for $i = 1, 2, 3$. Thus the α_i, $1 \le i \le 3$, are non-negative integers adding up to 1, and hence there is a unique $i = 1, 2, 3$ such that $\alpha_i = 1$, $\alpha_j = \alpha_l = 0$. Since $n_{\mathbb{O}}$ is positive definite, (1) now implies $w_1 = w_2 = w_3 = 0$, hence $e = e_{ii}$. □

56.3 Proposition. *With the notation of 4.4, the element*

$$v := \frac{1}{2}(1_{\mathbb{O}} - \sum_{i=1}^{7} u_i) = u_1 - u_2 - u_4 - \mathbf{p} - u_1\mathbf{p} - u_2\mathbf{p} + u_4\mathbf{p} \tag{1}$$

belongs to M and satisfies the relations

$$n_{\mathbb{O}}(v) = 2, \quad t_{\mathbb{O}}(v) = 1, \quad v^2 = v - 2 \cdot 1_{\mathbb{O}}, \quad t_{\mathbb{O}}(v^3) = -5. \tag{2}$$

Proof Since E is an orthonormal basis of $\mathbb{O}$ (Exc. 2.8), the first three equations of (2) follow immediately from the definition of v. In order to establish the fourth one, we compute $v^3 = v^2 - 2v = v - 2 \cdot 1_{\mathbb{O}} - 2v = -v - 2 \cdot 1_{\mathbb{O}}$, and taking traces gives the assertion, hence completes the proof of (2). Since $(1_{\mathbb{O}}, u_1, u_2, u_4, \mathbf{p}, u_1\mathbf{p}, u_2\mathbf{p}, u_4\mathbf{p})$ is an $\mathbb{R}$-basis of $\mathbb{O}$ associated with M (Thm. 4.5), it therefore suffices to establish the final equation of (1). To this

end we apply (4.4.3)–(4.4.7) and compute

$$\begin{aligned} u_1 - u_2 - u_4 - \mathbf{p} - u_1\mathbf{p} - u_2\mathbf{p} + u_4\mathbf{p} &= \frac{1}{2}(2u_1 - 2u_2 - 2u_4 - 1_{\mathbb{O}} - u_1 - u_2 - u_3 \\ &\qquad + 1_{\mathbb{O}} - u_1 - u_4 - u_7 \\ &\qquad + 1_{\mathbb{O}} - u_2 + u_4 - u_5 \\ &\qquad - u_1 + u_2 + u_4 - u_6) \\ &= \frac{1}{2}(1_{\mathbb{O}} - u_1 - u_2 - u_3 - u_4 - u_5 - u_6 - u_7) \\ &= v. \end{aligned}$$

This completes the proof. □

56.4 Proposition. *With the notation of 56.1 and Prop. 56.3, the element*

$$q := \sum (2e_{ii} - v[jl]) \in \Lambda = \mathrm{Her}_3(M)$$

has norm 1 *and*

$$p := q^{-1} = q^\sharp = \sum (2e_{ii} - \bar{v}[jl]) \tag{1}$$

belongs to $\Lambda \cap \mathrm{Pos}(J)$.

Proof By Prop. 56.3 we have $q \in M$. Next we show $N_J(q) = 1$ and that $q^{-1} = q^\sharp$ has the form indicated in the final equation of the proposition. Consulting (36.4.5) and (56.3.2), we compute

$$N_J(q) = 2 \cdot 2 \cdot 2 - 3 \cdot 2n_C(v) - t_C(v^3) = 8 - 12 + 5 = 1.$$

In order to compute $p = q^\sharp$, we invoke (36.4.4) and (56.3.2) and obtain

$$\begin{aligned} q^\sharp &= \sum \big((2 \cdot 2 - n_{\mathbb{O}}(v))e_{ii} + (2v + \bar{v}^2)[jl]\big) \\ &= \sum \big(2e_{ii} + (2v + \bar{v} - 2 \cdot 1_{\mathbb{O}})[jl]\big) \\ &= \sum \big(2e_{ii} + (v + v + \bar{v} - 2(v + \bar{v}))[jl]\big) \\ &= \sum (2e_{ii} - \bar{v}[jl]), \end{aligned}$$

as claimed. Hence the proposition will follow once we have shown $p \in \mathrm{Pos}(J)$, equivalently (Exc. 56.10 (a)), that all its minors are strictly positive. This is obvious for the 1-minors and the 3-minor (since $N_J(p) = N_J(q)^{-1} = 1$), and follows from (1) for the two-minors as well. □

Write Λ_0 for the isotope $\Lambda^{(p)}$ of Λ for p as defined in the proposition. The subscript 0 is inspired by the following result.

56.5 Lemma. *The algebra* Λ_0 *does not contain any elementary idempotents.*

Proof Assume that

$$e = \sum (\alpha_i e_{ii} + w_i[jl]) \qquad (\alpha_i \in \mathbb{Z}, \quad w_i \in M, \quad 1 \le i \le 3) \tag{1}$$

is an elementary idempotent in Λ_0. We must show that this assumption leads to a contradiction. We do so in several steps.

1°. Since $e \in \Lambda_0$ is an elementary idempotent, 37.1 yields $e^{(\sharp,p)} = 0$ and $T^{(p)}(e) = 1$, which by (33.11.2) and (33.11.5) is equivalent to $e^\sharp = 0$ and $T(p,e) = 1$. Combining (1) with Exc. 39.39, Prop. 56.4 and (36.4.7), we therefore not only obtain

$$\alpha_j\alpha_l = n_{\mathbb{O}}(w_i), \quad (w_iw_j)w_l = \alpha_1\alpha_2\alpha_3 1_{\mathbb{O}} = w_i(w_jw_l) \qquad (i = 1,2,3) \tag{2}$$

but also $1 = \sum(2\alpha_i - n_{\mathbb{O}}(\bar{v}, w_i))$, and (16.12.5) yields

$$\sum (2\alpha_i - t_{\mathbb{O}}(vw_i)) = 1. \tag{3}$$

2°. Since $e = e^{(2,p)}$ is a square in $J^{(p)}$ for $J = \mathrm{Her}_3(\mathbb{O})$, we may combine Exc. 56.7 (c) with Exc. 56.8 (b) to conclude $e \in \overline{\mathrm{Pos}}(J^{(p)}) = \overline{\mathrm{Pos}}(J)$. Thus $\alpha_i \ge 0$ for $1 \le i \le 3$. On the other hand, Exc. 40.15(b) shows that

$$f^{(2,p)} = f := p^{-1} - e = q - e = \sum ((2-\alpha_i)e_{ii} - (v + w_i)[jl]) \tag{4}$$

has rank 2. By Exc. 56.7 (b), therefore, $f \in \overline{\mathrm{Pos}}(J^{(p)}) = \overline{\mathrm{Pos}}(J)$, so all minors of f are non-negative (Exc. 56.10 (b)). Summing up, we obtain

$$0 \le \alpha_i \le 2, \quad (2-\alpha_j)(2-\alpha_l) - n_{\mathbb{O}}(v + w_i) \ge 0 \qquad (1 \le i \le 3). \tag{5}$$

Next we claim

$$|\{i \mid 1 \le i \le 3,\ \alpha_i = 2\}| \le 1. \tag{6}$$

Otherwise, some $i = 1,2,3$ would have $\alpha_j = \alpha_l = 2$, and (5) would show $v + w_m = 0$ for all $m = 1,2,3$. But then $f = \sum_m (2-\alpha_m)e_{mm} = (2-\alpha_i)e_{ii}$ would have rank at most 1, a contradiction. Thus (6) holds.

3°. We now treat the case $\alpha_1\alpha_2\alpha_3 = 0$. Then there exists $i = 1,2,3$ such that $\alpha_j = 0$. In view of (2), this implies $w_l = w_i = 0$, and (3) reduces to

$$2\alpha_l + 2\alpha_i - t_{\mathbb{O}}(vw_j) = 1. \tag{7}$$

On the other hand, invoking (16.12.5), (56.3.2) and the Cauchy-Schwarz inequality, we obtain

$$|t_{\mathbb{O}}(vw_j)| = |n_{\mathbb{O}}(\bar{v}, w_j)| \le \sqrt{n_{\mathbb{O}}(v,v)n_{\mathbb{O}}(w_j,w_j)} = 2\sqrt{2n_{\mathbb{O}}(w_j)},$$

and (2) yields

$$|t_{\mathbb{O}}(vw_j)| \leq 2\sqrt{2\alpha_l\alpha_i}. \tag{8}$$

Now, if $\alpha_l\alpha_i = 0$, then $w_j = 0$ by (2), and (7) reduces to $2\alpha_l = 1$ or $2\alpha_i = 1$, a contradiction. On the other hand, if $\alpha_l = \alpha_i = 1$, then $|t_{\mathbb{O}}(vw_j)| \leq 2\sqrt{2} < 3$ by (8) (since $(2\sqrt{2})^2 = 4{\cdot}2 = 8 < 9 = 3^2$), and (7) yields $1 = 4-t_{\mathbb{O}}(vw_j) > 4-3 = 1$, again a contradiction. Finally, suppose $\alpha_l = 1$, $\alpha_i = 2$. Then $|t_{\mathbb{O}}(vw_j)| \leq 4$ by (8), so (7) implies with $1 = 2+4-t_{\mathbb{O}}(vw_j) \geq 6-4 = 2$ yet another contradiction. By symmetry and in view of (6), this concludes the case $\alpha_1\alpha_2\alpha_3 = 0$.

4°. Next we treat the case $\alpha_1 = \alpha_2 = \alpha_3 = 1$. Combining (2) with (5), we conclude $n_{\mathbb{O}}(w_i) = 1$ and $0 \leq n_{\mathbb{O}}(v + w_i) \leq 1$ for $1 \leq i \leq 3$. But v has norm 2 by (56.3.2), which implies $v + w_i \neq 0$, hence

$$n_{\mathbb{O}}(v + w_i) = 1 \qquad (1 \leq i \leq 3). \tag{9}$$

On the other hand, f, having rank 2 by 2°, cannot be invertible in J, so (4) and (9) yield

$$\begin{aligned} 0 &= N_J(f) \\ &= (2-\alpha_1)(2-\alpha_2)(2-\alpha_3) - \sum (2-\alpha_i) n_{\mathbb{O}}(v+w_i) \\ &\quad - t_{\mathbb{O}}((v+w_1)(v+w_2)(v+w_3)) \\ &= 1 - 3 - t_{\mathbb{O}}((v+w_1)(v+w_2)(v+w_3)) = -t_{\mathbb{O}}((v+w_1)(v+w_2)(v+w_3)) - 2. \end{aligned}$$

Thus $w := (v + w_1)((v + w_2)(v + w_3)) + 1_{\mathbb{O}} \in \mathbb{O}$ satisfies

$$(v + w_1)((v + w_2))(v + w_3)) = -1_{\mathbb{O}} + w, \quad w \in \mathbb{O}^0. \tag{10}$$

Taking norms in (10) and observing (9), we conclude $1 = n_{\mathbb{O}}(-1_{\mathbb{O}} + w) = 1 + n_{\mathbb{O}}(w)$, hence $w = 0$. But this means

$$(v + w_1)((v + w_2)(v + w_3)) = -1_{\mathbb{O}},$$

which combines with (4), (9) and Exc. 39.39 to show that f has rank 1, a contradiction.

5°. In view of (6), it remains to discuss the case $\alpha_i = 2$, $\alpha_j = \alpha_l = 1$ for some $i = 1, 2, 3$. Then (4) collapses to

$$f = e_{jj} + e_{ll} - (v + w_i)[jl] - (v + w_j)[li] - (v + w_l)[ij],$$

while (5) yields $1 - n_{\mathbb{O}}(v + w_i) \geq 0$, $v + w_j = v + w_l = 0$. Thus, by (1),

$$\begin{aligned} f &= e_{jj} + e_{ll} - (v + w_i)[jl], \\ e &= 2e_{ii} + e_{jj} + e_{ll} + w_i[jl] - v[li] - v[ij] \end{aligned}$$

Here the assumption $n_{\mathbb{O}}(v + w_i) = 1$ would imply $f^\sharp = 0$, in contradiction to f having rank 2. Hence $v + w_i = 0$, and we conclude

$$e = 2e_{ii} + e_{jj} + e_{ll} - v[jl] - v[li] - v[ij].$$

But e has rank 1 which by (2) implies $n_{\mathbb{O}}(v) = 1$, in contradiction to (56.3.2). This completes the proof. □

From this, we conclude that there are (at least) two non-isomorphic $\mathbb{Z}$-forms of $\mathrm{Her}_3(\mathbb{O})$:

56.6 Theorem. *For the Albert algebras Λ and Λ_0 over $\mathbb{Z}$,*

$$\Lambda \otimes F \cong \Lambda_0 \otimes F$$

for every field F, but

$$\Lambda \ncong \Lambda_0.$$

Proof The fact that $\Lambda \ncong \Lambda_0$ is an immediate consequence of Lemmas 56.2 and 56.5.

For the other claim when $F = \mathbb{Q}$, from Prop. 56.4 we know $p \in \mathrm{Pos}(J)$. By Exc. 56.8 (b), therefore, $\Lambda \otimes \mathbb{R} \cong \Lambda_0 \otimes \mathbb{R}$. Then it follows from Thm. 46.20 that $\Lambda \otimes \mathbb{Q} \cong \Lambda_0 \otimes \mathbb{Q}$. When F is a finite field, both algebras are split by Exc. 40.17. □

In contrast to this, there is only one $\mathbb{Z}$-form of $\mathbb{O}$, up to isomorphism, by Exc. 23.39. Compare Theorem 57.4.

Exercises

The following set of exercises paves the way for our brief investigation of the euclidean Albert algebra over the integers. These exercises are mainly concerned with properties of the positive cone as defined in 56.1. For an in-depth analysis of this important concept in the more general setting of arbitrary (finite-dimensional) euclidean Jordan algebras over the reals, see Braun-Koecher [36, Chap. X].

Unless explicitly stated otherwise, notation and conventions fixed in 56.1 will remain in force. In particular, $\mathbb{D}$ stands for one of the four division subalgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ of $\mathbb{O}$, and $J := \mathrm{Her}_3(\mathbb{D})$.

56.7. *Characterizations of the positive and the non-negative cone.* Let $x \in J$ and prove:

(a) There exist an elementary frame (c_1, c_2, c_3) in J and real numbers $\alpha_1, \alpha_2, \alpha_3$ satisfying

$$x = \sum_{i=1}^{3} \alpha_i c_i. \tag{1}$$

(b) The following conditions are equivalent.

(i) There exist an elementary frame (c_1, c_2, c_3) of J and *positive* real numbers $\alpha_1, \alpha_2, \alpha_3$ such that (1) holds.
(ii) $x = y^2$ for some $y \in J^\times$.
(iii) The left multiplication operator

$$L_x \colon J \longrightarrow J, \quad y \longmapsto x \bullet y,$$

is positive definite relative to the bilinear trace of J:

$$T(x \bullet z, z) > 0 \qquad (0 \neq z \in J). \tag{2}$$

(iv) $x \in \operatorname{Pos}(J)$.

In this case, x is said to be *positive*, and we write $x > 0$.

(c) The following conditions are equivalent.

(i) There exist an elementary frame (c_1, c_2, c_3) of J and *non-negative* real numbers $\alpha_1, \alpha_2, \alpha_3$ such that (1) holds.
(ii) $x = y^2$ for some $y \in J$.
(iii) The left multiplication operator

$$L_x \colon J \longrightarrow J, \quad y \longmapsto x \bullet y,$$

is positive semi-definite relative to the bilinear trace of J:

$$T(x \bullet z, z) \geq 0 \qquad (z \in J). \tag{3}$$

(iv) $x \in \overline{\operatorname{Pos}}(J)$.

In this case, x is said to be *non-negative*, and we write $x \geq 0$.

56.8. *Properties of the positive and the non-negative cone.* Prove:

(a) $U_p(\operatorname{Pos}(J)) = \operatorname{Pos}(J)$, $U_p(\overline{\operatorname{Pos}}(J)) = \overline{\operatorname{Pos}}(J)$ for all $p \in J^\times$.

(b) $J^{(p)} \cong J$, $p^{-1} \in \operatorname{Pos}(J)$ and

$$\operatorname{Pos}(J^{(p)}) = \operatorname{Pos}(J), \quad \overline{\operatorname{Pos}}(J^{(p)}) = \overline{\operatorname{Pos}}(J).$$

for all $p \in \operatorname{Pos}(J)$.

(c) For $\eta \in \operatorname{Aut}(J) \cup \operatorname{Str}^0(J)$, where $\operatorname{Str}^0(J)$ denotes the identity component of $\operatorname{Str}(J)$ as a topological group, we have

$$\eta(\operatorname{Pos}(J)) = \operatorname{Pos}(J), \quad \eta(\overline{\operatorname{Pos}}(J)) = \overline{\operatorname{Pos}}(J).$$

(d) Assume $\mathbb{D}' \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}\}$ is a subalgebra of $\mathbb{D}$ and put $J' := \operatorname{Her}_3(\mathbb{D}') \subseteq J$. Then

$$\operatorname{Pos}(J') = \operatorname{Pos}(J) \cap J'^\times = \operatorname{Pos}(J) \cap J', \quad \overline{\operatorname{Pos}}(J') = \overline{\operatorname{Pos}}(J) \cap J'.$$

56.9. *Positive definite elements.* Let n be a positive integer, $\mathbb{D} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$ (so $\mathbb{D}$ is associative) and $J := \operatorname{Her}_n(\mathbb{D})$ be the real Jordan algebra of n-by-n hermitian matrices with entries in $\mathbb{D}$ as defined in 5.3, 5.7).

(a) Show for $y \in \operatorname{GL}_n(\mathbb{D})$ that the $\mathbb{R}$-linear bijection

$$\Phi_y \colon J \longrightarrow J, \quad x \longmapsto \Phi_y(x) := \bar{y}^{\mathsf{T}} x y,$$

belongs to the structure group of J.

(b) Write $\mathrm{Tri}_n(\mathbb{D})$ for the group of upper triangular n-by-n matrices with entries in $\mathbb{D}$ and diagonal ones equal to $1_{\mathbb{D}}$. Then prove that the assignment $y \mapsto \Phi_y$ defines an anti-homomorphism from $\mathrm{Tri}_n(\mathbb{D})$ to the group $\mathrm{Str}^0(J)$ (in the sense of Exc. 56.8 (c)).

(c) Show for $x \in J$ that the following conditions are equivalent.

(i) x is *positive definite* in the sense that $\bar{u}^{\mathsf{T}} x u > 0$ for all $0 \neq u \in \mathbb{D}^n$.

(ii) There exists $y \in \mathrm{Tri}_n(\mathbb{D})$ such that $\bar{y}^{\mathsf{T}} x y$ is a diagonal matrix with strictly positive diagonal entries.

Moreover, for $n = 3$ these conditions are also equivalent to

(iii) $x \in \mathrm{Pos}(J)$.

(*Hint*: For the implication (i) $\Rightarrow$ (ii), argue by induction on n and use the formula

$$\overline{\begin{pmatrix} \mathbf{1}_p & -P^{-1}R \\ 0 & \mathbf{1}_q \end{pmatrix}}^{\mathsf{T}} \begin{pmatrix} P & R \\ \bar{R}^{\mathsf{T}} & Q \end{pmatrix} \begin{pmatrix} \mathbf{1}_p & -P^{-1}R \\ 0 & \mathbf{1}_q \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & -\bar{R}^{\mathsf{T}} P^{-1} R + Q \end{pmatrix} \tag{1}$$

for $p, q \in \mathbb{Z}$, $p > 0$, $q > 0$, $p + q = n$, $P = \bar{P}^{\mathsf{T}} \in \mathrm{GL}_p(\mathbb{D})$, $Q \in \mathrm{Mat}_q(\mathbb{D})$, $R \in \mathrm{Mat}_{pq}(\mathbb{D})$.)

56.10. *Minors and the positive cone.* As before, let $J := \mathrm{Her}_3(\mathbb{D})$ with $\mathbb{D} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}\}$ and write $x \in J$ as

$$x = \sum (\xi_i e_{ii} + u_i[jl]) \qquad (\xi_i \in \mathbb{R},\ u_i \in \mathbb{D},\ i = 1, 2, 3). \tag{1}$$

The quantities

$$T(x, e_{ii}), \quad T(x^\sharp, e_{ii}), \quad N(x) \qquad (1 \leq i \leq 3) \tag{2}$$

are called the *minors* of x, while

$$T(x, e_{11}), \quad T(x^\sharp, e_{33}), \quad N(x) \tag{3}$$

are called its *principal minors*. (Why?)

(a) Show that the following conditions are equivalent.

(i) $x \in \mathrm{Pos}(J)$.

(ii) The minors of x are all positive.

(iii) The principal minors of x are positive.

(*Hint*: Reduce the implication (iii) $\Rightarrow$ (i) to the case that $\mathbb{D}$ is associative by applying Exc. 5.18.)

(b) Conclude from (a) that the following conditions are equivalent.

(i) $x \in \overline{\mathrm{Pos}}(J)$.

(ii) The minors of x are all non-negative.

(iii) The principal minors of x are non-negative.

Remark. In Elkies-Gross [71, p. 668], the *exceptional cone* of the euclidean Albert algebra $J := \mathrm{Her}_3(\mathbb{O})$ is defined as the set of elements satisfying condition (b)(ii) above and hence agrees with $\overline{\mathrm{Pos}}(J)$, the closure of the positive cone of J.

57 Classification over $\mathbb{Z}$

In this section, we study octonion algebras and Albert algebras over $\mathbb{Z}$, or more generally over the ring of integers in a global field. Such a ring is a Dedekind domain.

57.1 Lemma. *Suppose k is a Dedekind domain with field of fractions K.*

(a) *Let A be an octonion or Albert k-algebra. Then A is split if and only if A_K is split.*

(b) *Let $\mathbf{G}$ be a semisimple k-group scheme of type G_2, F_4, or E_8. Then $\mathbf{G}$ is split if and only if $\mathbf{G}_K$ is split.*

Proof In both cases, the "only if" direction is obvious so we prove "if". We start with (b). Put $\mathbf{G}_0$ for the split form of $\mathbf{G}$ and suppose $\mathbf{G}_K$ is split. The natural map $\mathbf{G} \to \mathbf{Aut}(\mathbf{G})$ is an isomorphism, so by the Descent Theorem 54.15, there is an element $\gamma \in H^1(k, \mathbf{G}_0)$ corresponding to $\mathbf{G}$. Moreover, since k is Dedekind and $\mathbf{G}_0$ is simply connected, [114, Satz 3.3] says that $\gamma = 0$, i.e., $\mathbf{G} \cong \mathbf{G}_0$.

We deduce (a) from (b) using the correspondence between on the one hand Albert or octonion algebras and on the other hand groups of type F_4 or G_2 as in Propositions 55.5 or 55.4, which say in particular that the algebra is split if and only if its automorphism group is split. □

Regarding (b), recall from 52.7 that if k is a principal ideal domain, one can weaken the hypothesis on $\mathbf{G}$.

Part (a) of the lemma immediately gives the following.

57.2 Corollary. *Suppose k is a Dedekind domain with field of fractions K. If every Albert (resp., octonion) K-algebra is split, then the split Albert (resp., octonion) k-algebra is the only one.* □

Note that the hypothesis holds, for example, if K is a global field with no real embeddings, by Corollary 46.19 for Albert algebras and by Corollary 23.23 for octonions. Having addressed this case, we now focus on the case where K is a number field with at least one real embedding. We call a composition or Albert algebra A over K *definite* if A_{K_v} has no nilpotents for every real place v of K and K has at least one real place, and say that A is *indefinite* otherwise (e.g., if K has no real embeddings). Note that there is up to isomorphism only one Albert or octonion K-algebra A that is definite.

57.3 Proposition. *Suppose K is a number field and k is a localization of its*

ring of integers at finitely many primes. For every Albert (resp., octonion) K-algebra A that is indefinite, there is an Albert (resp., composition) k-algebra B such that $B_K \cong A$ and B is uniquely determined up to k-isomorphism.

Proof We may assume that K has at least one real embedding. Write $\mathbf{G}$ for the automorphism group of the split Albert (resp., octonion) k-algebra. Write $H^1_{\text{ind}}(k, \mathbf{G}) \subseteq H^1(k, \mathbf{G})$ for the isomorphism classes of k-algebras B such that B_K is indefinite. The reference [114] defines this symbol to mean the isomorphism classes of groups of type F_4 (resp. G_2) that are isotropic at at least one real place; the two definitions are equivalent by [43, p. 218]. Since $\mathbf{G}$ is simply connected, [114, Satz 4.4.2] says that the natural map $H^1_{\text{ind}}(k, \mathbf{G}) \to H^1_{\text{ind}}(K, \mathbf{G})$ is an isomorphism, which is what is claimed. □

Every Albert or octonion k-algebra B gives a K-algebra B_K by base change, and it only remains to describe those B such that B_K is the definite K-algebra. In the case of octonion algebras over the integers, this was already worked out in Exercise 23.39; we give a different proof here.

57.4 Theorem. *Over $\mathbb{Z}$:*

(a) There are exactly two isomorphism classes of octonion algebras: $\mathrm{Zor}(\mathbb{Z})$ *and* $\mathrm{DiCo}(\mathbb{O})$.

(b) There are exactly four isomorphism classes of Albert algebras, namely $\mathrm{Her}_3(\mathrm{Zor}(\mathbb{Z}))$, $\mathrm{Her}_3(\mathrm{DiCo}(\mathbb{O}), \langle 1, -1, 1\rangle)$, *and the algebras* Λ *and* Λ_0 *from §56.*

(c) There are exactly two isotopy classes of Albert algebras: $\mathrm{Her}_3(\mathrm{Zor}(\mathbb{Z}))$ *and* $\mathrm{Her}_3(\mathrm{DiCo}(\mathbb{O}))$.

Proof For (a) and (b), no pair of the listed algebras are isomorphic to another one. For Λ and Λ_0, this is Corollary 56.6. For any other pair, base change to $\mathbb{Q}$ yields non-isomorphic $\mathbb{Q}$-algebras. Therefore, it suffices to prove that there are no others.

Suppose that B is an octonion or Albert $\mathbb{Z}$-algebra. If B is indefinite, then it is determined by $B_{\mathbb{Q}}$ by Proposition 57.3. Since the indefinite octonion or Albert $\mathbb{Q}$-algebras are $\mathrm{Zor}(\mathbb{Q})$, $\mathrm{Her}_3(\mathrm{Zor}(\mathbb{Q}))$, and $\mathrm{Her}_3(\mathbb{O}, \langle 1, -1, 1\rangle)$, B is isomorphic to one of the algebras listed in the statement.

On the other hand, Gross's mass formula shows that there is only one group of type G_2 and two groups of type F_4 over $\mathbb{Z}$ whose base change to $\mathbb{Q}$ is anisotropic [105, Prop. 5.3], and therefore by Prop. 55.4 and 55.5, only one octonion $\mathbb{Z}$-algebra and two Albert $\mathbb{Z}$-algebras that are definite. This shows that we have captured all the definite algebras as well, completing the proof of (a) and (b).

For (c), note that the three algebras in (b) that are not $\mathrm{Her}_3(\mathrm{Zor}(\mathbb{Z}))$ are all isotopic, see Exercise 37.23, so the two algebras listed in (c) represent all of the isotopy classes of Albert $\mathbb{Z}$-algebras. After base change from $\mathbb{Z}$ to $\mathbb{Q}$, these two algebras have distinct co-ordinate algebras and therefore are not isotopic by Theorem 41.8, consequently they are not isotopic as $\mathbb{Z}$-algebras. □

This concludes our discussion of octonions and Albert algebras over $\mathbb{Z}$. We take this opportunity to prove a classification of Freudenthal algebras of rank 15 over $\mathbb{Z}$, which is somewhat trickier.

57.5 Proposition. *Up to isomorphism, the only quaternion $\mathbb{Z}$-algebra is the split one,* $\mathrm{Mat}_2(\mathbb{Z})$*, and the only rank 15 Freudenthal $\mathbb{Z}$-algebra is the split one,* $\mathrm{Her}_3(\mathrm{Mat}_2(\mathbb{Z}))$.

Sketch of proof We write the details for rank 15 Freudenthal algebras; the proof for quaternions is similar. Let $\mathbf{G}$ be a semisimple adjoint $\mathbb{Z}$-group scheme of type C_3, so $\mathbf{G} = \mathbf{Aut}(J)$ for a rank 15 Freudenthal $\mathbb{Z}$-algebra by Proposition 55.5. We wish to prove that $\mathbf{G}$ is split.

This is equivalent, as stated in 52.7, to the claim that $\mathbf{G}_{\mathbb{Q}}$ is split as a $\mathbb{Q}$-group scheme. Now, because $\mathbf{G}_{\mathbb{Q}}$ comes from $\mathbb{Z}$, the isomorphism class of $\mathbf{G}_{\mathbb{Q}}$ is determined by that of $\mathbf{G}_{\mathbb{R}}$ and moreover the isomorphism class of $\mathbf{G}_{\mathbb{R}}$ lies in the image of $H^1(\mathbb{R}, \mathbf{Sp}_6) \to H^1(\mathbb{R}, \mathbf{PGSp}_6)$, both by [54, Prop. 4.10]. (Recall that there is an element of $H^1(k, \mathbf{PGSp}_6)$ corresponding to the isomorphism class of $\mathbf{G}_k$ for all rings k by Lemma 55.3.) Yet $H^1(\mathbb{R}, \mathbf{Sp}_6) = 1$ because non-degenerate skew-symmetric bilinear forms on $\mathbb{R}^6$ are isomorphic, so $\mathbf{G}_{\mathbb{R}}$ is split. □

57.6 Remark. The claim that every quaternion algebra over $\mathbb{Z}$ is split was already proved via other means in Thm. 23.25. It is a special case of the more general statement that the Brauer group of $\mathbb{Z}$ is trivial, which is itself a corollary of the statement that $H^2(\mathbb{Z}, \mathbf{G_m}) = 0$ [109, p. 95].

58 Groups of type E_6

In this section, we re-cast the ordinary group $\mathrm{Inv}(J)$ for an Albert algebra J as a group scheme $\mathbf{Inv}(J)$, observe that it is simply connected of type E_6, and prove some basic facts about the correspondence between properties of the group scheme and properties of J.

Let's start with something slightly more general. Let J be a regular cubic Jordan algebra over a ring k. We define group schemes $\mathbf{Inv}(J)$ and $\mathbf{Str}(J)$ by setting

$$\mathbf{Inv}(J)(R) := \mathrm{Inv}(J_R) \quad \text{and} \quad \mathbf{Str}(J)(R) := \mathrm{Str}(J_R)$$

for all $R \in k$-**alg**. Recall from Lemma 40.4 that $\mathrm{Inv}(J)$ is the kernel of a homomorphism $\mu\colon \mathrm{Str}(J) \to k^\times$. Since the definition of μ is compatible with base change, we find a homomorphism of group schemes $\mathbf{Str}(J) \to \mathbf{G_m}$ — which we also denote by μ — with kernel $\mathbf{Inv}(J)$.

58.1 Lemma. *If J is a regular Freudenthal algebra, then the sequence*

$$0 \longrightarrow \mathbf{Inv}(J) \longrightarrow \mathbf{Str}(J) \xrightarrow{\mu} \mathbf{G_m} \longrightarrow 0$$

of sheaves of groups is exact in the étale topology.

The statement that the sequence is exact means that for every $R \in k$-**alg**, the sequence of groups

$$0 \to \mathrm{Inv}(J_R) \to \mathrm{Str}(J_R) \to R^\times$$

is exact, and for every $x \in R^\times$, there is some étale cover $S \in R$-**alg** such that x is the image of $\mathrm{Str}(J_S) \to S^\times$.

Proof The only thing that is not yet proved is the surjectivity of μ. That is, given $R \in k$-**alg** and $m \in R^\times$, we must show that there is an étale cover S of R such that m is in $\mu(\mathrm{Str}(J_S))$.

If J has rank 1, then $J = k^{(+)}$ and $3 \in k^\times$ because J is regular (Cor. 39.15). Therefore, $S := R[\mathbf{t}]/(\mathbf{t}^3 - x)$ is a finite étale k-algebra (Exc. 25.40). Since $\mu(\mathbf{t}\mathbf{1}_{J_S}) = \mathbf{t}^3 = x$ in S, this case is complete.

If J has rank > 3, then since J is regular, there is an étale cover S of R such that J_S is split (Cor. 39.32). Example 40.3 shows that $\mu(J_S) = S^\times$. The same argument also works when J has rank 3. □

We now focus our attention on Albert algebras.

58.2 Theorem. *If J is an Albert algebra over a ring k, then* $\mathbf{Inv}(J)$ *is a semisimple and simply connected group scheme of type* E_6. *If J is the split Albert algebra, then* $\mathbf{Inv}(J)$ *is split as a semisimple group scheme.*

Proof First suppose that $k = \mathbb{Z}$ and J is split. Then for every algebraically closed field F, the claim holds for $\mathbf{Inv}(J_F)$ by [268, 11.20, 12.4]. (Or see [270, Thm. 7.3.2] for the case where F is a field of characteristic $\neq 2, 3$.)

Note that $\mathbf{Inv}(J)_F$ is connected and smooth as a group scheme over F, and $\mathbf{Inv}(J)$ is finitely presented (because $\mathbb{Z}$ is noetherian and J is a finitely generated module), so it follows by [87, Prop. 6.1] or [15, Lemma B.1] that $\mathbf{Inv}(J)$ is smooth as a scheme over the Dedekind domain $\mathbb{Z}$. In summary, $\mathbf{Inv}(J)$ is semisimple and simply connected of the specified type. Moreover, because $\mathbf{Inv}(J)_{\mathbb{Q}}$ is split, $\mathbf{Inv}(J)$ is split as a group scheme over $\mathbb{Z}$. This handles the claim about split J.

In the case of general k and J, let $k' \in k$-**alg** be faithfully flat such that $J \otimes k'$ is split. Then $\mathbf{Inv}(J)_{k'}$ is semisimple simply connected of the specified type. Certainly, $\mathbf{Inv}(J)$ is also smooth. Moreover, for each field $K \in k$-**alg**, there is a field $K' \in k'$-**alg** such that K includes in K' as in Exc. 9.26. Since $\mathbf{Inv}(J)_{K'}$ has the claimed type, so does $\mathbf{Inv}(J)_K$. Since this holds for every K, the claim is verified. □

The above proof is essentially the same as the one in [14, §2.1]. A rather different proof can be found in [54, Th. C.2].

The group schemes $\mathbf{Inv}(J)$ for other kinds of Freudenthal algebras J can be described as part of a series, see for example the column labeled $\nu = 2$ in Table 1 of [59]; [289]; or Table 2 and §§8–10 in [106].

58.3 Example. (References: [271, Tag 03PK], [42, §2.4.3], [157, §III.3]) Suppose L is a line bundle and there is an isomorphism $h\colon L^{\otimes d} \to k$ for some $d \geq 1$. We call such a pair $[L, h]$ a *d-trivialized line bundle*. (In the case $d = 2$ they are sometimes called *discriminant modules*.) The group scheme μ_d of d-th roots of unity, viewed as a closed subgroup of $\mathbf{GL}(L)$, is the automorphism group of each $[L, h]$, where μ_d acts by multiplication on L. The set $H^1(k, \mu_d)$, which is an abelian group by Example 54.3, classifies pairs $[L, h]$ up to isomorphism.

If $L = k$, then every isomorphism $h\colon L^{\otimes d} \to k$ is of the form $h(\ell_1 \otimes \cdots \otimes \ell_d) = \alpha \prod \ell_i$ for some $\alpha \in k^\times$. We abbreviate this as $[k, \alpha]$ or simply α. If every d-torsion element of $\mathrm{Pic}(k)$ is zero — e.g., if k is an LG ring (Prop. 11.24) or a unique factorization domain [271, Tag 0BCH] — then every $[L, h]$ is of this form.

Suppose now that M and N are finitely generated projective k-modules. We may identify $(L^*)^{\otimes d} \cong S^d(L^*)$ and, via h, $(L^*)^{\otimes d} \cong k$. Therefore leveraging Exc. 25.36 we have:

$$\begin{aligned}\mathrm{Pol}^d(M, N) &\cong \mathrm{Pol}^d(M, N \otimes (L^*)^{\otimes d}) \\ &\cong S^d(M^*) \otimes S^d(L^*) \otimes N \cong \mathrm{Pol}^d(M \otimes L, N).\end{aligned}$$

Given an element $f \in \mathrm{Pol}^d(M, N)$, we write $[L, h] \cdot f$ for the corresponding element of $\mathrm{Pol}^d(M \otimes L, N)$. Note that in the special case $L = k$, where we have written $\alpha \in k^\times$ instead of $[L, h]$, the notation $\alpha \cdot f$ is the same as multiplying the polynomial law f by the scalar α.

We say that homogeneous degree d laws f and $[L, h] \cdot f$ for $[L, h] \in H^1(k, \mu_d)$ as in the preceding example are *similar*.

For $f \in \mathrm{Pol}^d(M, N)$, we define $\mathrm{Aut}(f)$ to be the subgroup of $\mathrm{GL}(M)$ consisting of elements g such that $f \circ g = f$ as polynomial laws. In case M and N are finitely generated projective, so is $\mathrm{Pol}^d(M, N)$ (cf. Exc. 25.36), whence

the functor $\mathbf{Aut}(f)$ from k-**alg** to groups defined by $\mathbf{Aut}(f)(T) := \mathrm{Aut}(f_T)$ is a closed sub-group-scheme of $\mathbf{GL}(M)$.

58.4 Lemma. *Let f and f' be homogeneous polynomial laws on finitely generated projective modules. If f and f' are similar, then their automorphism groups are isomorphic.*

Proof By hypothesis, $f \in \mathrm{Pol}^d(M,N)$ and $f' \in \mathrm{Pol}^d(M \otimes L, N)$ for some modules M and N; line bundle L; and $d \geq 0$. The group scheme $\mathbf{Aut}(f)$ is the closed sub-group-scheme of $\mathbf{GL}(M)$ stabilizing the element f in $S^d(M^*) \otimes N$. Now, any element of $\mathbf{GL}(M)$ acts on

$$S^d((M \otimes L)^*) \otimes (N \otimes L^{\otimes d}) \cong S^d((M \otimes L)^* \otimes N$$

by defining it to act as the identity on L. In this way, we find a homomorphism $\mathbf{Aut}(f) \to \mathbf{Aut}(f')$. Viewing M as $(M \otimes L) \otimes L^*$ and N as $(N \otimes L^{\otimes d}) \otimes (L^*)^{\otimes d}$, and repeating this construction, we find an inverse mapping $\mathbf{Aut}(f') \to \mathbf{Aut}(f)$. □

One could replace the hypothesis "similar" by a weaker property known as "projectively similar" in [17, §1.2] or "lax similar" in [19]. See [95, Lemma 3.6] for details.

58.5 Proposition. *Let J and J' be Albert k-algebras. Among the statements*

(i) $\mathbf{Inv}(J) \cong \mathbf{Inv}(J')$.

(ii) *There is a line bundle L and isomorphism $h\colon L^{\otimes 3} \to k$ such that $N_{J'} \cong [L,h] \cdot N_J$ for $\cdot$ as defined in Example 58.3.*

(iii) *J and J' are isotopic.*

we have the implications (i) $\Leftrightarrow$ (ii) $\Leftarrow$ (iii). If the only 3-torsion element of Pic k *is zero, then all three statements are equivalent.*

Proof Suppose (i); we prove (ii). The conjugation action gives a homomorphism $\mathbf{Inv}(J) \to \mathbf{Aut}(\mathbf{Inv}(J))$, which gives a map of pointed sets

$$H^1(k, \mathbf{Inv}(J)) \to H^1(k, \mathbf{Aut}(\mathbf{Inv}(J))), \tag{1}$$

where the second set is in bijection with isomorphism classes of group schemes over k that become isomorphic to $\mathbf{Inv}(J)$ after base change to an fppf k-algebra. By hypothesis, the class of $N_{J'} \in H^1(k, \mathbf{Inv}(J))$ is in the kernel of (1).

There is an exact sequence

$$1 \to \mathbf{Inv}(J)/\mu_3 \to \mathbf{Aut}(\mathbf{Inv}(J)) \to \mathbb{Z}/2 \to 1$$

of fppf sheaves as described in 52.9. From it, we obtain an exact sequence

$$\mathbf{Aut}(\mathbf{Inv}(J))(k) \to (\mathbb{Z}/2)(k) \to H^1(k, \mathbf{Inv}(J)/\mu_3) \to H^1(k, \mathbf{Aut}(\mathbf{Inv}(J))) \tag{2}$$

as proved in [103, III.3.2.2]. In the language of Exercise 54.27, $\mathbb{Z}/2$ has one nonidentity constant element, and it is the image of the map $\eta \mapsto \eta^{\sharp -1}$. (We observed already in 31.20 that this map is an automorphism of $\mathbf{Inv}(J)$ whose square is the identity, and Exc. 40.18 says that it is not an inner automorphism.) In (2), Exercise 54.27 shows that the first map is surjective, so the third map has zero kernel.

Consider next the exact sequence

$$1 \to \mu_3 \to \mathbf{Inv}(J) \to \mathbf{Inv}(J)/\mu_3 \to 1,$$

which gives an exact sequence

$$H^1(k, \mu_3) \to H^1(k, \mathbf{Inv}(J)) \to H^1(k, \mathbf{Inv}(J)/\mu_3). \tag{3}$$

Starting with $N_{J'} \in H^1(k, \mathbf{Inv}(J))$, we can map it first to $H^1(k, \mathbf{Inv}(J)/\mu_3)$ and then to $H^1(k, \mathbf{Aut}(\mathbf{Inv}(J)))$ where we obtain zero. Because the third map in (2) has zero kernel, the image of $N_{J'}$ is zero in $H^1(k, \mathbf{Inv}(J)/\mu_3)$. It follows that $N_{J'}$ is in the image of $H^1(k, \mu_3)$, which is the orbit of the zero class N_J under the action of the group $H^1(k, \mu_3)$ [103, Prop. III.3.4.5], which is (ii).

(ii) implies (i) by Lemma 58.4.

Corollary 40.5 says that (iii) is equivalent to $N_{J'} \cong [k, \alpha] \cdot N_J$ for some $\alpha \in k^\times$. Thus the claim about the implications between (iii) and (ii). □

58.6 Corollary. *Suppose every 3-torsion element of* $\operatorname{Pic} k$ *is zero. Then an Albert k-algebra J is split if and only if* $\mathbf{Inv}(J)$ *is split.*

Proof Combine Thm. 58.2 and Prop. 58.5 to see that $\mathbf{Inv}(J)$ is split if and only if J is isotopic to the split Albert algebra, which by Cor. 40.12 holds if and only if J is itself split. □

58.7 Classification of groups of type E_6 over $\mathbb{Z}$. Recall that there are two Albert algebras over $\mathbb{Z}$ up to isotopy, namely $\mathrm{Her}_3(C)$ for $C = \mathrm{Zor}(\mathbb{Z})$ or $\mathrm{DiCo}(\mathbb{O})$ (Thm. 57.4(c)). One of these algebras is split and the other is not, so by the corollary $\mathbf{Inv}(\mathrm{Her}_3(C))$ is split for one choice of C and not the other. Thus we have produced representatives of two distinct isomorphism classes of simply connected simple affine group schemes of type E_6 over $\mathbb{Z}$.

On the other hand, general arguments as in [114] and [54, §4] combined with the classification of real forms of E_6 show that there are exactly two isomorphism classes of simply connected group schemes of type E_6 over $\mathbb{Z}$, see [54, §7]. In conclusion, the groups $\mathbf{Inv}(\mathrm{Her}_3(C))$ for our two choices of C are a complete set of representatives for simply connected groups of type E_6 over $\mathbb{Z}$.

58.8 Vista: twisted forms of the the cubic norm. Consider now the case of

an Albert algebra J over a field F. Then, over an algebraic closure $\bar{F}$ of F, $\mathrm{Inv}(J_{\bar{F}})$ has an open orbit in $\mathbb{P}(J_{\bar{F}})$ consisting of the lines in $J_{\bar{F}}$ spanned by elements with nonzero norm (Exc. 40.16). This fact leads to a surjection in flat cohomology

$$H^1(F, \mathbf{Aut}(J)) \times H^1(F, \mu_3) \to H^1(F, \mathbf{Inv}(J)),$$

see [89, 9.12]. That is, every element of $H^1(F, \mathbf{Inv}(J))$ is the isomorphism class of a cubic form $\lambda N_{J'}$ for some $\lambda \in F^\times$ and Albert F-algebra J'. See [266] for a proof in the language of cubic forms under the additional hypothesis that $\mathrm{char}\, F \neq 2, 3$.

It follows from this that the groups in the image of

$$H^1(F, \mathbf{Inv}(J)) \to H^1(F, \mathbf{Aut}(\mathbf{Inv}(J))),$$

what Tits called in [282] the simply connected *strongly inner forms* E_6, are exactly the groups of the form $\mathrm{Inv}(J')$ for an Albert F-algebra J'. Compare [279, 6.4.2].

For a typical field F, there are simply connected semisimple groups of type E_6 that are not of the form $\mathbf{Inv}(J)$ for an Albert F-algebra J, i.e., are not strongly inner forms. See for example [279, §6.4], [91], and [88] for views on some additional groups of type E_6.

Results for groups of type E_7 — analogous to the results in this section for type E_6 — can be found in sections 16 and 17 of [95].

References

[1] Alberca Bjerregaard, P, Elduque, A., Martín González, C., and Navarro Márquez, F.J. 2002. On the Cartan-Jacobson theorem. *J. Algebra*, **250**(2), 397–407. 544

[2] Alberca Bjerregaard, P., Loos, O., and Martín González, C. 2005. Derivations and automorphisms of Jordan algebras in characteristic two. *J. Algebra*, **285**(1), 146–181. 563

[3] Albert, A.A. 1934. On a certain algebra of quantum mechanics. *Ann. of Math. (2)*, **35**(1), 65–73. vi, 31, 505

[4] Albert, A.A. 1942. Non-associative algebras. I. Fundamental concepts and isotopy. *Ann. of Math. (2)*, **43**, 685–707. 120

[5] Albert, A.A. 1946. On Jordan algebras of linear transformations. *Trans. Amer. Math. Soc.*, **59**, 524–555. 251

[6] Albert, A.A. 1947a. A structure theory for Jordan algebras. *Ann. of Math. (2)*, **48**, 546–567. 251

[7] Albert, A.A. 1947b. The Wedderburn principal theorem for Jordan algebras. *Ann. of Math. (2)*, **48**, 1–7. 251

[8] Albert, A.A. 1958. A construction of exceptional Jordan division algebras. *Ann. of Math. (2)*, **67**, 1–28. vi, 505, 516

[9] Albert, A.A. 1961. *Structure of algebras*. AMS Coll. Pub., vol. 24. Providence, RI: AMS. revised printing. 47, 517

[10] Albert, A.A. 1965. On exceptional Jordan division algebras. *Pacific J. Math.*, **15**, 377–404. vi, 516, 517

[11] Albert, A.A., and Jacobson, N. 1957. On reduced exceptional simple Jordan algebras. *Ann. of Math. (2)*, **66**, 400–417. 197, 441, 442, 514, 515

[12] Albert, N.E. 2005. *A^3 & his algebra: How a Boy from Chicago's West Side Became a Force in American Mathematics*. iUniverse. vi

[13] Allcock, D. 1999. Ideals in the integral octaves. *J. Algebra*, **220**(2), 396–400. 159

[14] Alsaody, S. 2021. Albert algebras over rings and related torsors. *Canad. J. Math.*, **73**(3), 875–898. 425, 614

[15] Alsaody, S., and Gille, P. 2019. Isotopes of octonion algebras, $\mathbf{G}_2$-torsors and triality. *Adv. Math.*, **343**, 864–909. 116, 193, 578, 613

[16] Asok, A., Hoyois, M., and Wendt, M. 2019. Generically split octonion algebras and $\mathbb{A}^1$-homotopy theory. *Algebra & Number Theory*, **13**(3), 695–747. 167, 187

[17] Auel, A., Bernardara, M., and Bolognesi, M. 2014. Fibrations in complete intersections of quadrics, Clifford algebras, derived categories, and rationality problems. *J. Math. Pures Appl.*, **102**, 249–291. 615

[18] Baeza, R. 1978. *Quadratic forms over semilocal rings*. Berlin: Springer-Verlag. Lecture Notes in Mathematics, Vol. 655. 81

[19] Balmer, P., and Calmès, B. 2012. Bases of total Witt groups and lax-similitude. *J. Algebra Appl.*, **11**(3), 1250045. 615

[20] Bayer-Fluckiger, E., and Parimala, R. 1998. Classical groups and the Hasse principle. *Ann. Math. (2)*, **147**, 651–693. 600

[21] Bayer-Fluckiger, E., First, U., and Parimala, R. 2022. On the Grothendieck-Serre conjecture for classical groups. *J. London Math. Soc.*, **106**, 2884–2926. 240

[22] Behrens, E.-A. 1954. Nichtassoziative Ringe. *Math. Ann.*, **127**, 441–452. 46

[23] Beli, C., Gille, P., and Lee, T.-Y. 2016. Examples of algebraic groups of type G_2 having the same maximal tori. *Proceedings of the Steklov Institute of Mathematics*, **292**(1), 10–19. 200

[24] Bix, R. 1981. Isomorphism theorems for octonion planes over local rings. *Trans. Amer. Math. Soc.*, **266**(2), 423–439. 191

[25] Borel, A. 1991. *Linear Algebraic Groups*. second edn. Graduate Texts in Mathematics, vol. 126. New York: Springer-Verlag. 572

[26] Bott, R., and Milnor, J. 1958. On the parallelizability of the spheres. *Bull. Amer. Math. Soc.*, **64**, 87–89. 8

[27] Bourbaki, N. 1972. *Commutative algebra: Chapters 1–7*. Elements of mathematics. Paris: Hermann. Translated from the French. x, 16, 40, 53, 56, 63, 79, 103, 189, 223, 226, 228, 229, 234, 519

[28] Bourbaki, N. 1974. *Algebra, Part I: Chapters 1–3*. Paris: Hermann. Translated from the French. x, xvi, 56, 57, 72, 98, 112, 139, 166, 217, 222, 229, 519, 520, 536, 589

[29] Bourbaki, N. 1981. *Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7]*. Masson, Paris. x, 36, 86, 240, 520, 568, 584

[30] Bourbaki, N. 1989. *Lie groups and Lie algebras: Chapters 1–3*. Berlin: Springer-Verlag. 522, 529

[31] Bourbaki, N. 2002. *Lie groups and Lie algebras: Chapters 4–6*. Berlin: Springer-Verlag. 26, 27, 518, 523

[32] Bourbaki, N. 2004. *Theory of sets*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin. Reprint of the 1968 English translation [Hermann, Paris]. 592

[33] Bourbaki, N. 2005. *Lie groups and Lie algebras: Chapters 7–9*. Berlin: Springer-Verlag. 518, 522, 523, 526, 572

[34] Bourbaki, N. 2012. *Algèbre. Chapitre 8. Modules et anneaux semi-simples*. Springer, Berlin. Second revised edition of the 1958 edition [MR0098114]. 79

[35] Brandt, H. 1943. Zur Zahlentheorie der Quaternionen. *Jber. Deutsch. Math. Verein.*, **53**, 23–57. 22

[36] Braun, H., and Koecher, M. 1966. *Jordan-Algebren*. Berlin: Springer-Verlag. 47, 84, 112, 176, 251, 299, 607

[37] Brown, E. 2015. Many more names of $(7, 3, 1)$. *Math. Mag.*, **8**(2), 103–120. 12

[38] Brown, E., and Rice, A. 2022. An accessible proof of Hurwitz's sums of squares theorem. *Math. Mag.*, **95**(5), 422–436. 8

[39] Brown, R.B. 1967. On generalized Cayley-Dickson algebras. *Pacific J. Math.*, **20**, 415–422. 157
[40] Bruck, R.H. 1958. *A survey of binary systems*. Reihe: Gruppentheorie. Springer-Verlag, Berlin-Göttingen-Heidelberg. 112
[41] Brühne, P. 2000. *Ordnungen und die Tits-Konstruktionen von Albert-Algebren*. Ph.D. thesis, Fernuniversität in Hagen. 327
[42] Calmès, B., and Fasel, J. 2015. Groupes classiques. *Panoramas & Synthèses*, **46**, 1–133. 83, 571, 595, 614
[43] Carr, M., and Garibaldi, S. 2006. Geometries, the principle of duality, and algebraic groups. *Expo. Math.*, **24**, 195–234. 442, 611
[44] Cartan, É. 1935. Sur les domaines bornés homogènes de l'espace de n variables complexes. *Abh. Math. Sem. Univ. Hamburg*, **11**(1), 116–162. viii
[45] Cartan, É., and Schouten, J. A. 1926. On Riemannian geometries admitting an absolute parallelism. *Proc. Akad. Wet. Amsterdam*, **29**, 933–946. 10
[46] Castillo-Ramirez, A., and Elduque, A. 2016. Some special features of Cayley algebras, and G_2, in low characteristics. *J. Pure Appl. Algebra*, **220**(3), 1188–1205. 544
[47] Cesnavicius, K. 2022. Problems about torsors over regular rings. *Acta Mathematica Vietnamica*, **47**, 39–107. with an appendix by Yifei Zhao. 600
[48] Chapman, A., Dolphin, A., and Laghribi, A. 2016. Total linkage of quaternion algebras and Pfister forms in characteristic two. *J. Pure Appl. Algebra*, **220**(11), 3676–3691. 200
[49] Chayet, M., and Garibaldi, S. 2021. A class of continuous non-associative algebras arising from algebraic groups including E_8. *Forum of Mathematics: Sigma*, **9**, e6. 252
[50] Chernousov, V., and Panin, I. 2013. Purity for Pfister forms and F_4-torsors with trivial g_3 invariant. *J. reine angew. Math.*, **2013**(685), 99–104. 601
[51] Chevalley, C. 1946 1957. *Theory of Lie groups. I*. Princeton University Press, Princeton, N. J. 12
[52] Chevalley, C., and Schafer, R.D. 1950. The exceptional simple Lie algebras F_4 and E_6. *Proc. Nat. Acad. Sci. U. S. A.*, **36**, 137–141. 563
[53] Conrad, B. 2014. Reductive group schemes. Pages 93–444 of: *Autour des schémas en groupes. Vol. I*. Panor. Synthèses, vol. 42/43. Soc. Math. France, Paris. 83, 235
[54] Conrad, B. 2015. Non-split reductive groups over $\mathbf{Z}$. Pages 193–253 of: *Autours des schémas en groupes. Vol. II*. Panor. Synthèses, vol. 46. Soc. Math. France, Paris. 565, 570, 571, 573, 595, 612, 614, 616
[55] Conway, J.H., and Smith, D.A. 2003. *On quaternions and octonions: their geometry, arithmetic, and symmetry*. A K Peters, Ltd., Natick, MA. 22, 25
[56] Coxeter, H.S.M. 1946. Integral Cayley numbers. *Duke Math. J.*, **13**, 561–578. x, 23
[57] Dahn, R. 2023. Nazis, émigrés, and abstract mathematics. *Physics Today*, **76**(1), 44–50. v
[58] Dam, E.B., Koch, M., and Lillholm, M. 1998 (July). *Quaternions, interpolation and animation*. Tech. rept. DIKU-TR-98/5. University of Copenhagen. 8
[59] Deligne, P., and Gross, B.H. 2002. On the exceptional series, and its descendants. *C. R. Math. Acad. Sci. Paris*, **335**(11), 877–881. 614

[60] Deligne, P., and Katz, N.M. 2006. *Groupes de Monodromie en Geometrie Algebrique: Seminaire de Geometrie Algebrique du Bois-Marie 1967–1969 (SGA 7 II)*. Vol. 340. Springer. 83

[61] Demazure, M., and Gabriel, P. 1970. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris. Avec un appendice *Corps de classes local* par Michiel Hazewinkel. 63, 204, 235, 238, 521

[62] Demazure, M., and Grothendieck, A. 1970. *Schémas en Groupes II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*. Lecture Notes in Mathematics, vol. 152. Springer. 567

[63] Dias, I. 1988 (October). *Formas quadráticas sobre LG-anéis*. Ph.D. thesis, Universidade Estadual de Campinas, Brazil. 81

[64] Dickson, L.E. 1923. A new simple theory of hypercomplex integers. *J. Math. Pures Appl.*, **2**, 281–326. x, 23

[65] Dickson, L.E. 1935. Linear algebras with associativity not assumed. *Duke Math. Journ.*, **1**, 113–125. 130

[66] Dieterich, E. 2005. Classification, automorphism groups and categorical structure of the two-dimensional real division algebras. *J. Algebra Appl.*, **4**(5), 517–538. 8

[67] Dieudonné, J. 1948. *Sur les groupes classiques*. Actualités Sci. Ind., no. 1040 = Publ. Inst. Math. Univ. Strasbourg (N.S.) no. 1 (1945). Hermann et Cie., Paris. 203

[68] Drucker, D. 1978. *Exceptional Lie algebras and the structure of Hermitian symmetric spaces*. Memoirs Amer. Math. Soc., no. 208. American Mathematical Soc. viii

[69] Elduque, A. 2000. On triality and automorphisms and derivations of composition algebras. *Linear Algebra Appl.*, **314**(1-3), 49–74. 581

[70] Elduque, A. 2018. Order 3 elements in G_2 and idempotents in symmetric composition algebras. *Canad. J. Math.*, **70**(5), 1038–1075. 148

[71] Elkies, N.D., and Gross, B.H. 1996. The exceptional cone and the Leech lattice. *Internat. Math. Res. Notices*, **1996**(14), 665–698. xiv, 603, 609

[72] Elman, R., Karpenko, N., and Merkurjev, A. 2008. *The algebraic and geometric theory of quadratic forms*. Coll. Publ., vol. 56. Providence, RI: Amer. Math. Soc. 78, 83, 103, 199, 343, 417, 427, 429, 434, 435, 436, 506, 516, 517

[73] Estes, D.R., and Guralnick, R.M. 1982. Module equivalences: local to global when primitive polynomials represent units. *J. Algebra*, **77**, 138–157. 79, 80

[74] Faulkner, J.R. 1970. *Octonion planes defined by quadratic Jordan algebras*. Memoirs of the American Mathematical Society, No. 104. Providence, R.I.: American Mathematical Society. 364, 377, 431

[75] Faulkner, J.R. 1988. Finding octonion algebras in associative algebras. *Proc. Amer. Math. Soc.*, **104**(4), 1027–1030. xiii

[76] Faulkner, J.R. 2000. Jordan pairs and Hopf algebras. *J. Algebra*, **232**(1), 152–196. 84, 104

[77] Faulkner, J.R. 2001. Generalized quadrangles and cubic forms. *Comm. Algebra*, **29**, 4641–4653. ix

[78] Faulkner, J.R. 2014. *The role of nonassociative algebra in projective geometry*. Graduate Studies in Mathematics, vol. 159. American Mathematical Society, Providence, RI. 10

[79] Fedorov, R., and Panin, I. 2015. A proof of the Grothendieck–Serre conjecture on principal bundles over regular local rings containing infinite fields. *Publications mathématiques de l'IHÉS*, **122**(1), 169–193. 600

[80] Fernández López, A. 2019. *Jordan structures in Lie algebras*. Math. Surveys and Monographs, no. 240. Amer. Math. Soc. vii

[81] Ferrar, J.C. 1967. Generic splitting fields of composition algebras. *Trans. Amer. Math. Soc.*, **128**, 506–514. 203

[82] Filippov, V.T. 1976. Central simple Mal'tsev algebras. *Algebra and Logic*, **15**(2), 147–151. 527

[83] Freudenthal, H. 1954. Beziehungen der E_7 und E_8 zur Oktavenebene. I. *Nederl. Akad. Wetensch. Proc. Ser. A.* **57** = *Indagationes Math.*, **16**, 218–230. 358

[84] Freudenthal, H. 1959. Beziehungen der E_7 und E_8 zur Oktavenebene. VIII. *Nederl. Akad. Wetensch. Proc. Ser. A.* **62** = *Indag. Math.*, **21**, 447–465. 358

[85] Freudenthal, H. 1985. Oktaven, Ausnahmegruppen und Oktavengeometrie. *Geom. Dedicata*, **19**, 7–63. (Reprint of Utrecht Lecture Notes, 1951). 443, 576

[86] Frobenius, G. 1878. Über lineare Substitutionen und bilineare Formen. *J. reine angew. Math.*, **84**, 1–63. 158

[87] Gan, W.T., and Yu, J.-K. 2003. Schémas en groupes et immeubles des groupes exceptionnels sur un corps local. Première partie: le groupe G_2. *Bull. Soc. Math. France*, **131**(3), 307–358. 578, 613

[88] Garibaldi, S. 2001. Structurable algebras and groups of type E_6 and E_7. *J. Algebra*, **236**(2), 651–691. 617

[89] Garibaldi, S. 2009. *Cohomological invariants: exceptional groups and spin groups*. Memoirs Amer. Math. Soc., no. 937. Providence, RI: Amer. Math. Soc. with an appendix by Detlev W. Hoffmann. 617

[90] Garibaldi, S., and Hoffmann, D.W. 2006. Totaro's question on zero-cycles on G_2, F_4, and E_6 torsors. *J. London Math. Soc.*, **73**, 325–338. 200

[91] Garibaldi, S., and Petersson, H.P. 2007. Groups of outer type E_6 with trivial Tits algebras. *Transf. Groups*, **12**(3), 443–474. 617

[92] Garibaldi, S., and Petersson, H.P. 2011. Wild Pfister forms over Henselian fields, K-theory, and conic division algebras. *J. Algebra*, **327**, 386–465. 122, 132, 136, 147, 195

[93] Garibaldi, S., and Saltman, D.J. 2010. Quaternion algebras with the same subfields. Pages 225–238 of: *Quadratic forms, linear algebraic groups, and cohomology*. Developments in Mathematics, vol. 18. Springer. 200

[94] Garibaldi, S., Merkurjev, A., and Serre, J-P. 2003. *Cohomological invariants in Galois cohomology*. University Lecture Series, vol. 28. Amer. Math. Soc. 439, 440, 600, 601

[95] Garibaldi, S., Petersson, H.P., and Racine, M.L. 2023. Albert algebras over $\mathbb{Z}$ and other rings. *Forum of Mathematics: Sigma*, **11**, e18. vii, xiv, 97, 103, 147, 226, 414, 416, 425, 578, 615, 617

[96] Garibaldi, S., Petersson, H.P., and Racine, M.L. 2024. *Solutions to the exercises from the book "Albert algebras over commutative rings"*. arXiv:2406.02933. x

[97] Gille, P. 2014. Octonion algebras over rings are not determined by their norms. *Canad. Math. Bull.*, **57**(2), 303–309. 192, 193, 201

[98] Gille, P. 2019. *Groupes algébriques semi-simples en dimension cohomologique* ≤ 2. Lecture Notes in Math., no. 2238. Springer. 600

[99] Gille, P., and Neher, E. 2021. Springer's odd degree extension theorem for quadratic forms over semilocal rings. *Indag. Math. (N.S.)*, **32**(6), 1290–1310. 77

[100] Gille, P., and Polo, P. (eds). 2011a. *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], vol. 7. Société Mathématique de France, Paris. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original. 565

[101] Gille, P., and Polo, P. (eds). 2011b. *Schémas en groupes (SGA 3). Tome III. Structure des schémas en groupes réductifs*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], vol. 8. Société Mathématique de France, Paris. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original. xiv, 565, 568, 569, 570, 573, 599

[102] Gille, P., and Szamuely, T. 2006. *Central simple algebras and Galois cohomology*. Cambridge studies in Advanced Math., vol. 101. Cambridge. 194, 195, 196, 204, 506, 513, 574

[103] Giraud, J. 1971. *Cohomologie non abélienne*. Springer-Verlag, Berlin-New York. Die Grundlehren der mathematischen Wissenschaften, Band 179. 595, 616

[104] Greenberg, M.J. 1969. *Lectures on forms in many variables*. W. A. Benjamin, Inc., New York-Amsterdam. 195, 513

[105] Gross, B.H. 1996. Groups over **Z**. *Invent. Math.*, **124**(1-3), 263–279. 611

[106] Gross, B.H., and Garibaldi, S. 2021. Minuscule embeddings. *Indag. Math.*, **32**(5), 987–1004. 614

[107] Grothendieck, A. 1960. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, **4**, 228. 63, 124

[108] Grothendieck, A. 1967. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, **32**, 361. 222, 231, 233, 234, 235

[109] Grothendieck, A. 1968. Le groupe de Brauer. III. Exemples et compléments. Pages 88–188 of: *Dix exposés sur la cohomologie des schémas*. Adv. Stud. Pure Math., vol. 3. North-Holland, Amsterdam. 612

[110] Grothendieck, A. 1995. Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats. Pages Exp. No. 190, 299–327 of: *Séminaire Bourbaki, Vol. 5*. Soc. Math. France, Paris. 236, 588, 595

[111] Hahn, A.J., and O'Meara, O.T. 1989. *The classical groups and K-theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of

Mathematical Sciences], vol. 291. Springer-Verlag, Berlin. With a foreword by J. Dieudonné. 161

[112] Harbater, D., Hartmann, J., and Krashen, D. 2014. Local-global principles for Galois cohomology. *Commentarii Mathematici Helvetici*, **89**(1), 215–253. 601

[113] Harder, G. 1966. Über die Galoiskohomologie halbeinfacher Matrizengruppen. II. *Math. Z.*, **92**, 396–415. 600

[114] Harder, G. 1967. Halbeinfache Gruppenschemata über Dedekindringen. *Invent. Math.*, **4**, 165–191. 565, 610, 611, 616

[115] Harder, G. 1975. Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III. *J. reine angew. Math.*, **274/275**, 125–138. 600

[116] Hartshorne, R. 1977. *Algebraic geometry*. New York: Springer-Verlag. Graduate Texts in Mathematics, No. 52. 63

[117] Henderson, A. 1911. *The twenty-seven lines upon the cubic surface*. Cambridge University Press. ix

[118] Hijikata, H. 1963. A remark on the groups of type G_2 and F_4. *J. Math. Soc. Japan*, **15**, 159–164. vii

[119] Hirzebruch, F. 1990. Division algebras and topology. Chap. 11, pages 281–302 of: *Numbers*. Graduate Texts in Mathematics, vol. 123. Springer. 8

[120] Hirzebruch, U. 1964. Halbräume und ihre holomorphen Automorphismen. *Math. Ann.*, **153**, 395–417. viii

[121] Hiss, G. 1984. Die adjungierten Darstellungen der Chevalley-Gruppen. *Arch. Math. (Basel)*, **42**, 408–416. 544, 563

[122] Hoffmann, D.W. 2022. Splitting of quadratic Pfister forms over purely inseparable extensions in characteristic 2. *J. Algebra*, **596**, 311–327. 200, 204

[123] Hogeweij, G.M.D. 1982. Almost-classical Lie algebras. I, II. *Nederl. Akad. Wetensch. Indag. Math.*, **44**(4), 441–460. 544, 563, 599

[124] Hopf, H. 1940/41. Ein topologischer Beitrag zur reellen Algebra. *Comm. Math. Helv.*, **13**, 219–239. 8

[125] Hübner, M., and Petersson, H.P. 2004. Two-dimensional real division algebras revisited. *Beiträge Algebra Geom.*, **45**(1), 29–36. 8

[126] Humphreys, J.E. 1980. *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics, vol. 9. Springer-Verlag. Third printing, revised. 518

[127] Hurwitz, A. 1896. Ueber die Zahlentheorie der Quaternionen. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, **1896**, 314–340. x, 20, 22

[128] Ikkink, T.J., and Boeve, H.M.B. 2009 (September). *Dental position tracking system for a toothbrush*. US Patent No. 8690579B2. 7

[129] Jacobi, C. G. J. 1828. Note sur la décomposition d'un nombre donné en quatre carrés. *J. Reine Angew. Math.*, **3**, 191. 21

[130] Jacobi, C. G. J. 1881. *Gesammelte Werke. I. Band. Herausgegeben von C. W. Borchardt.* Berlin. G. Reimer (1881). 21

[131] Jacobson, N. 1937. Abstract derivation and Lie algebras. *Trans. Amer. Math. Soc.*, **42**(2), 206–224. 529

[132] Jacobson, N. 1958. Composition algebras and their automorphisms. *Rend. Circ. Mat. Palermo (2)*, **7**, 55–80. 160, 164, 191, 544

[133] Jacobson, N. 1959. Some groups of transformations defined by Jordan algebras. I. *J. Reine Angew. Math.*, **201**, 178–195. 577

[134] Jacobson, N. 1961. Some groups of transformations defined by Jordan algebras. III. *J. Reine Angew. Math.*, **207**, 61–85. 421
[135] Jacobson, N. 1962. *Lie algebras*. Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers (a division of John Wiley & Sons), New York-London. 261, 518, 549
[136] Jacobson, N. 1968. *Structure and representations of Jordan algebras*. American Mathematical Society Colloquium Publications, Vol. XXXIX. American Mathematical Society, Providence, R.I. xi, 47, 84, 251, 254, 376, 431, 443, 577
[137] Jacobson, N. 1969. *Lectures on quadratic Jordan algebras*. Tata Institute of Fundamental Research, Bombay. Tata Institute of Fundamental Research Lectures on Mathematics, No. 45. xi, 376, 549
[138] Jacobson, N. 1971. *Exceptional Lie algebras*. Lecture notes in pure and applied mathematics, vol. 1. New York: Marcel-Dekker. vii, 546, 563, 576
[139] Jacobson, N. 1974. Abraham Adrian Albert: 1905–1972. *Bull. Amer. Math. Soc.*, **80**(6), 1075–1100. also reprinted in *Celebratio Mathematica: A.A. Albert* (2012). vi
[140] Jacobson, N. 1981. *Structure theory of Jordan algebras*. University of Arkansas Lecture Notes in Mathematics, vol. 5. Fayetteville, Ark.: University of Arkansas. ix, xi, 267, 280, 295, 314, 376, 380, 546
[141] Jacobson, N. 1985. *Basic algebra. I*. Second edn. W. H. Freeman and Company, New York. 18
[142] Jacobson, N. 1989. *Basic algebra. II*. Second edn. W. H. Freeman and Company, New York. 61, 574
[143] Jacobson, N., and Katz, J. 1973. Generically algebraic quadratic Jordan algebras. *Scripta Math.*, **29**(3-4), 215–227. 393
[144] Jacobson, N., and McCrimmon, K. 1971. Quadratic Jordan algebras of quadratic forms with base points. *J. Indian Math. Soc. (N.S.)*, **35**, 1–45. 315, 398
[145] Jacobson, N., and Rickart, C.E. 1950. Jordan homomorphisms of rings. *Trans. Amer. Math. Soc.*, **69**, 479–502. 201
[146] Jantzen, J.C. 2003. *Representations of algebraic groups*. second edn. Math. Surveys and Monographs, vol. 107. Amer. Math. Soc. 96, 204
[147] Jordan, P. 1949. Über eine nicht-desarguesche ebene projektive Geometrie. *Abh. Math. Sem. Univ. Hamburg*, **16**, 74–76. 443
[148] Jordan, P., von Neumann, J., and Wigner, E. 1934. On an algebraic generalization of the quantum mechanical formalism. *Ann. of Math. (2)*, **35**(1), 29–64. v, vi, 301
[149] Kaplansky, I. 1953. Infinite-dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.*, **4**, 956–960. 149
[150] Kervaire, M.A. 1958. Non-parallelizability of the n-sphere for $n > 7$. *Proc. Natl. Acad. Sci. USA*, **44**(3), 280–283. 8
[151] Kirkman, T.P. 1848. LXVI. On pluquaternions, and homoid products of sums of n squares. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, **33**(224), 447–459. 12
[152] Kirmse, J. 1924. Über die Darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten und über ein mit diesem Problem zusammenhängendes nichtkommutatives und nichtassoziatives Zahlensystem. *Sächs. Akad. Wissensch. Leipzig*, **76**, 63–82. 27, 28, 133

[153] Kleinfeld, E. 1963. A characteriziation of the Cayley numbers. Pages 126–143 of: Albert, A.A. (ed), *Studies in Modern Algebra*. Mathematical Association of America. 114

[154] Kleinfeld, E. 1968. On extensions of quaternions. *Indian J. Math.*, **9**, 443–446. 157

[155] Knebusch, M. 1965. Der Begriff der Ordnung einer Jordanalgebra. *Abh. Math. Sem. Univ. Hamburg*, **28**, 168–184. 36, 37, 38

[156] Kneser, M. 2002. *Quadratische Formen*. Springer-Verlag, Berlin. Revised and edited in collaboration with Rudolf Scharlau. 18, 24

[157] Knus, M.-A. 1991. *Quadratic and Hermitian forms over rings*. Vol. **294**. Springer-Verlag. 63, 65, 77, 81, 83, 122, 124, 155, 161, 192, 201, 447, 571, 614

[158] Knus, M.-A., and Ojanguren, M. 1974. *Théorie de la descente et algèbres d'Azumaya*. Lecture Notes in Mathematics, Vol. 389. Springer-Verlag, Berlin-New York. 46, 155, 158, 159, 226, 447, 529, 595

[159] Knus, M.-A., Parimala, R., and Sridharan, R. 1994. On compositions and triality. *J. Reine Angew. Math.*, **457**, 45–70. 156, 172

[160] Knus, M.-A., Merkurjev, A., Rost, M., and Tignol, J.-P. 1998. *The book of involutions*. Amer. Math. Soc. Coll. Publ., vol. 44. Providence, RI: American Mathematical Society. vii, 64, 66, 148, 345, 396, 439, 440, 490, 510, 571, 595, 601, 602

[161] Koecher, M., and Remmert, R. 1990. Composition algebras. Chap. 10, pages 265–280 of: *Numbers*. Graduate Texts in Mathematics, vol. 123. Springer. 8

[162] Korkine, A., and Zolotarev, G. 1877. Sur les formes quadratiques positives. *Math. Ann.*, **11**, 242–292. 25

[163] Krashen, D., and McKinnie, K. 2011. Distinguishing division algebras by finite splitting fields. *manuscripta math.*, **134**, 171–182. 200

[164] Krieg, A. 1985. *Modular forms on half-spaces of quaternions*. Lecture Notes in Mathematics, vol. 1143. Springer-Verlag, Berlin. 22

[165] Krutelevich, S. 2002. On a canonical form of a 3×3 Hermitian matrix over the ring of integral split octonions. *J. Algebra*, **253**, 276–295. 421, 425

[166] Kuipers, J.B. 2002. *Quaternions and rotation sequences: a primer with applications to orbits, aerospace, and virtual reality*. Princeton Univ. Press. 7

[167] Kuzmin, E.N. 2014. Structure and representations of finite dimensional Malcev algebras. *Quasigroups and Related Systems*, **22**, 97–132. English translation of *Akademiya Nauk SSSR, Sibirskoe Otdelenie, Trudy Instituta Matematiki (Novosibirsk), Issledovaniya po Teorii Kolets i Algebr* **16** (1989), 75–101. 527

[168] Landsberg, J.M., and Manivel, L. 2006. The sextonions and $E_{7\frac{1}{2}}$. *Adv. Math.*, **201**, 143–179. 157

[169] Lazarsfeld, R., and Van de Ven, A. 1984. *Topics in the geometry of projective space*. DMV Seminar, vol. 4. Birkhäuser Verlag, Basel. Recent work of F. L. Zak, With an addendum by Zak. viii

[170] Legrand, S. 1972. Généralisations d'un théorème sur les algèbres munies d'une forme quadratique multiplicative. *C. R. Acad. Sci. Paris Sér. A-B*, **274**, A231–A234. 153

[171] Loos, O. 1975. *Jordan pairs*. Lecture Notes in Mathematics, Vol. **460**. Springer-Verlag, Berlin-New York. vii, viii, 107, 301, 365
[172] Loos, O. 1977. *Bounded symmetric domains and Jordan pairs*. Mathematical lectures. University of California, Irvine, CA. viii
[173] Loos, O. 1978. Separable Jordan pairs over commutative rings. *Math. Ann.*, **233**(2), 137–144. 237
[174] Loos, O. 2006. Generically algebraic Jordan algebras over commutative rings. *J. Algebra*, **297**(2), 474–529. xii, 59, 204, 342, 383, 392, 393
[175] Loos, O. 2011. Algebras with scalar involution revisited. *J. Pure Appl. Algebra*, **215**(12), 2805–2828. 122, 129, 130
[176] Loos, O., Petersson, H.P., and Racine, M.L. 2008. Inner derivations of alternative algebras over commutative rings. *Algebra Number Theory*, **2**(8), 927–968. 240, 247, 248, 528, 531, 532, 543
[177] Maillot, P.-G. 1990. Using quaternions for coding 3D transformations. Pages 498–515 of: Glassner, A.S. (ed), *Graphics Gems*. Academic Press Inc. 8
[178] Manin, Yu.I. 1986. *Cubic forms: algebra, geometry, arithmetic*. second edn. North-Holland Mathematical Library, vol. 4. Amsterdam-New York: North-Holland Publishing Co. 112
[179] Manivel, L. 2006. Configurations of lines and models of Lie algebras. *J. Algebra*, **304**, 457–486. ix
[180] Martindale, III, W.S. 1967. Jordan homomorphisms of the symmetric elements of a ring with involution. *J. Algebra*, **5**, 232–249. 550
[181] McCrimmon, K. 1966. A general theory of Jordan rings. *Proc. Nat. Acad. Sci. U.S.A.*, **56**, 1072–1079. vi, 36, 267, 376
[182] McCrimmon, K. 1967. Generically algebraic algebras. *Trans. Amer. Math. Soc.*, **127**, 527–551. 84
[183] McCrimmon, K. 1969. The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras. *Trans. Amer. Math. Soc.*, **139**, 495–510. xi, xiii, 317, 323, 325, 326, 327, 358, 453
[184] McCrimmon, K. 1970. The Freudenthal-Springer-Tits constructions revisited. *Trans. Amer. Math. Soc.*, **148**, 293–314. 262, 263, 286
[185] McCrimmon, K. 1971a. Homotopes of alternative algebras. *Math. Ann.*, **191**, 253–262. 114, 115, 116, 120, 379
[186] McCrimmon, K. 1971b. Quadratic Jordan algebras and cubing operations. *Trans. Amer. Math. Soc.*, **153**, 265–278. 272
[187] McCrimmon, K. 1978a. Jordan algebras and their applications. *Bull. Amer. Math. Soc.*, **84**(4), 612–627. vii
[188] McCrimmon, K. 1978b. Peirce ideals in Jordan algebras. *Pacific J. Math.*, **78**(2), 397–414. 313
[189] McCrimmon, K. 1985. Nonassociative algebras with scalar involution. *Pacific J. Math.*, **116**(1), 85–109. 122, 135, 143, 148
[190] McCrimmon, K. 2004. *A taste of Jordan algebras*. Universitext. Springer-Verlag, New York. xi, 143, 251, 253, 256, 526
[191] McCrimmon, K., and Zel′manov, E. 1988. The structure of strongly prime quadratic Jordan algebras. *Adv. in Math.*, **69**(2), 133–222. vi, 267, 509
[192] McDonald, B.R., and Waterhouse, W.C. 1981. Projective modules over rings with many units. *Proc. Amer. Math. Soc.*, **83**(3), 455–458. 79, 80

[193] Meyberg, K. 1970. The fundamental-formula in Jordan rings. *Arch. Math. (Basel)*, **21**, 43–44. 256

[194] Meyer, Jeffrey S. 2014. Division algebras with infinite genus. *Bull. Lond. Math. Soc.*, **46**(3), 463–468. 200

[195] Milne, J.S. 2017. *Algebraic groups*. Cambridge Studies in Advanced Mathematics, vol. 170. Cambridge University Press, Cambridge. 565, 569, 573, 575, 577, 580

[196] Milne, J.S. 2020 (July). *Algebraic number theory*. available at https://www.jmilne.org/math/CourseNotes/ant.html. 195

[197] Milnor, J., and Husemoller, D. 1973. *Symmetric bilinear forms*. New York: Springer-Verlag. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. 24, 25, 71

[198] Moran, T., Moran, S., and Moran, S. 2021. Elementary derivations of the Euclidean Hurwitz algebras. *Amer. Math. Monthly*, **128**, 726–736. 8

[199] Moreno, G. 1998. The zero divisors of the Cayley-Dickson algebras over the real numbers. *Bol. Soc. Mat. Mexicana (3)*, **4**(1), 13–28. 202

[200] Mühlherr, B., and Weiss, R.M. 2019. Freudenthal triple systems in arbitrary characteristic. *J. Algebra*, **520**, 237–275. 340

[201] Mühlherr, B., and Weiss, R.M. 2022. Tits polygons. *Mem. Amer. Math. Soc.*, **275**(1352), xi+114. With an appendix by Holger P. Petersson. viii, 341

[202] Neher, E. 1987. *Jordan triple systems by the grid approach*. Lecture Notes in Mathematics, vol. 1280. Springer-Verlag, Berlin. ix

[203] Neukirch, J. 1999. *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322. Springer-Verlag, Berlin. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. 19

[204] O'Meara, O.T. 1963. *Introduction to quadratic forms*. Die Grundlehren der mathematischen Wissenschaften, Bd. 117. New York: Springer-Verlag. 78, 189, 194, 195, 196, 198, 515

[205] Osborn, J.M. 1962. Quadratic division algebras. *Trans. Amer. Math. Soc.*, **105**, 202–221. 130

[206] Panin, I. A. 2020. Proof of the Grothendieck–Serre conjecture on principal bundles over regular local rings containing a field. *Izvestiya: Mathematics*, **84**(4), 780–795. 600

[207] Parimala, R., Sridharan, R., and Thakur, M.L. 1999. Tits' constructions of Jordan algebras and F_4 bundles on the plane. *Compositio Math.*, **119**, 13–40. 503

[208] Peirce, B. 1882. *Linear associative algebra*. Van Nostrand. reproduced and edited version of 1870 original. 115

[209] Petersson, H.P. 1970. Borel subalgebras of alternative and Jordan algebras. *J. Algebra*, **16**, 541–560. 360

[210] Petersson, H.P. 1971. Quasi composition algebras. *Abh. Math. Sem. Univ. Hamburg*, **35**, 215–222. 8

[211] Petersson, H.P. 1973. Jordan-Divisionsalgebren und Bewertungen. *Math. Ann.*, **202**, 215–243. 299, 512

[212] Petersson, H.P. 1974. Composition algebras over a field with a discrete valuation. *J. Algebra*, **29**, 414–426. 147, 195, 199

[213] Petersson, H.P. 1978. The isotopy problem for Jordan matrix algebras. *Trans. Amer. Math. Soc.*, **244**, 185–197. 121, 433

[214] Petersson, H.P. 1979. Classification of locally compact Jordan division rings. *J. Algebra*, **58**(2), 350–360. 299

[215] Petersson, H.P. 1981. On linear and quadratic Jordan division algebras. *Math. Z.*, **177**(4), 541–548. 299

[216] Petersson, H.P. 1993. Composition algebras over algebraic curves of genus zero. *Trans. Amer. Math. Soc.*, **337**(1), 473–493. 147, 180, 183, 186

[217] Petersson, H.P. 2002. The structure group of an alternative algebra. *Abh. Math. Sem. Univ. Hamburg*, **72**, 165–186. 120, 121

[218] Petersson, H.P. 2004. Structure theorems for Jordan algebras of degree three over fields of arbitrary characteristic. *Comm. Algebra*, **32**(3), 1019–1049. ix, 439, 441

[219] Petersson, H.P. 2017. The non-orthogonal Cayley-Dickson construction and the octonionic structure of the E_8-lattice. *J. Algebra Appl.*, **16**(12), 1750230, 52. 25

[220] Petersson, H.P. 2019. A survey on Albert algebras. *Transform. Groups*, **24**(1), 219–278. ix, xiii, 448, 485, 506

[221] Petersson, H.P. 2021. Norm equivalences and ideals of composition algebras. *Münster J. of Math.*, **14**, 283–293. 159, 201

[222] Petersson, H.P., and Racine, M.L. 1984a. Cubic subfields of exceptional simple Jordan algebras. *Proc. Amer. Math. Soc.*, **91**(1), 31–36. 517

[223] Petersson, H.P., and Racine, M.L. 1984b. Springer forms and the first Tits construction of exceptional Jordan division algebras. *Manuscripta Math.*, **45**(3), 249–272. 203, 459

[224] Petersson, H.P., and Racine, M.L. 1985. Radicals of Jordan algebras of degree 3. Pages 349–377 of: *Radical theory (Eger, 1982)*. Colloq. Math. Soc. János Bolyai, vol. 38. Amsterdam: North-Holland. 265, 342, 344, 345

[225] Petersson, H.P., and Racine, M.L. 1986a. Classification of algebras arising from the Tits process. *J. Algebra*, **98**(1), 244–279. viii, 345, 352, 503, 504

[226] Petersson, H.P., and Racine, M.L. 1986b. Jordan algebras of degree 3 and the Tits process. *J. Algebra*, **98**(1), 211–243. xiii, 380, 487, 489, 510

[227] Petersson, H.P., and Racine, M.L. 1994. Albert algebras. Pages 197–207 of: Kaup, W., McCrimmon, K., and Petersson, H.P. (eds), *Jordan algebras*. Berlin: de Gruyter. (Proceedings of a conference at Oberwolfach, 1992). ix

[228] Petersson, H.P., and Racine, M.L. 1995. On the invariants mod 2 of Albert algebras. *J. Algebra*, **174**(3), 1049–1072. 344, 363, 516, 601

[229] Petersson, H.P., and Racine, M.L. 1996a. An elementary approach to the Serre-Rost invariant of Albert algebras. *Indag. Math. (N.S.)*, **7**(3), 343–365. 601

[230] Petersson, H.P., and Racine, M.L. 1996b. Reduced models of Albert algebras. *Math. Z.*, **223**(3), 367–385. 164, 440

[231] Petersson, H.P., and Racine, M.L. 1997. The Serre-Rost invariant of Albert algebras in characteristic three. *Indag. Math. (N.S.)*, **8**(4), 543–548. 601

[232] Petersson, H.P., and Thakur, M.L. 2004. The étale Tits process of Jordan algebras revisited. *J. Algebra*, **273**(1), 88–107. 504

[233] Pink, R. 1998. Compact subgroups of linear algebraic groups. *J. Algebra*, **206**(2), 438–504. 544, 563

[234] Platonov, V.P., and Rapinchuk, A. 1994. *Algebraic groups and number theory*. Boston: Academic Press. 600

[235] Pleasants, P.A.B. 1971. Forms over $\mathfrak{p}$-adic fields. *Acta Arithmetica*, **18**, 289–296. 512

[236] Pollak, B. 1970. Orthogonal groups over global fields of characteristic 2. *J. Algebra*, **15**, 585–595. 196

[237] Polster, B. 1999. Yea why try her raw wet hat: a tour of the smallest projective space. *Math. Intelligencer*, **21**(2), 38–43. 12

[238] Prasad, G., and Rapinchuk, A.S. 2009. Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. *Publ. Math. IHES*, **109**(1), 113–184. 200

[239] Premet, A., and Strade, H. 2006. Classification of finite dimensional simple Lie algebras in prime characteristics. *Contemporary Mathematics*, **413**, 185–214. 526

[240] Pumplün, D. 1999. *Elemente der Kategorientheorie*. Spektrum Hochschul-Taschenbuch. Spektrum Akademischer Verlag GmbH, Heidelberg. 227

[241] Pumplün, S. 1998. Quaternion algebras over elliptic curves. *Comm. Algebra*, **26**(12), 4357–4373. 164, 172

[242] Racine, M.L. 1972. A note on quadratic Jordan algebras of degree 3. *Trans. Amer. Math. Soc.*, **164**, 93–103. 148, 363, 384, 385, 386, 395, 396, 398, 427, 439

[243] Racine, M.L. 1973. *The arithmetics of quadratic Jordan algebras*. American Mathematical Society, Providence, R.I. Memoirs of the American Mathematical Society, No. 136. 40

[244] Racine, M.L. 1974. On maximal subalgebras. *J. Algebra*, **30**, 155–180. 157

[245] Racine, M.L., and Zel'manov, E.I. 2015. An octonionic construction of the Kac superalgebra K_{10}. *Proc. Amer. Math. Soc.*, **143**(3), 1075–1083. 160

[246] Rapinchuk, A.S., and Rapinchuk, I.A. 2010. On division algebras having the same maximal subfields. *Manuscripta Math.*, **132**(3–4), 273–293. 200

[247] Raussen, M., and Skau, C. 2009. Interview with John G. Thompson and Jacques Tits. *Notices Amer. Math. Soc.*, **56**(4), 471–478. vii

[248] Rehm, H.P. 1993. Prime factorization of integral Cayley octaves. *Ann. Fac. Sci. Toulouse Math. (6)*, **2**(2), 271–289. 25

[249] Roby, N. 1963. Lois polynomes et lois formelles en théorie des modules. *Ann. Sci. École Norm. Sup. (3)*, **80**, 213–348. x, 84, 102

[250] Rost, M. 1991. A (mod 3) invariant for exceptional Jordan algebras. *C. R. Acad. Sci. Paris Sér. I Math.*, **313**, 823–827. 601

[251] Rost, M. 2002. Norm varieties and algebraic cobordism. Pages 77–85 of: *Proceedings of the International Congress of Mathematicians*, vol. II. Beijing: Higher Education Press. arXiv:0304208. 456

[252] Schafer, R.D. 1943. Alternative algebras over an arbitrary field. *Bull. Amer. Math. Soc.*, **49**, 549–555. 120, 177

[253] Schafer, R.D. 1948. The exceptional simple Jordan algebras. *Amer. J. Math.*, **70**, 82–94. 505

[254] Schafer, R.D. 1995. *An introduction to nonassociative algebras*. New York: Dover Publications Inc. Corrected reprint of the 1966 original. 112, 115, 176, 313, 533, 534, 543

[255] Scharlau, W. 1985. *Quadratic and Hermitian forms*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 270. Berlin: Springer-Verlag. 25, 78, 194, 195, 196, 512, 513

[256] Schilling, O., and Hasse, H. 1936. Die Normen aus einer normalen Divisionsalgebra über einem algebraischen Zahlkörper. *J. Reine Angew. Math.*, **174**, 248–252. 513

[257] Seligman, G.B. 1967. *Modular Lie algebras*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40. Springer-Verlag New York, Inc., New York. 526

[258] Semenov, N. 2016. Motivic construction of cohomological invariants. *Comment. Math. Helv.*, **91**, 163–202. 456

[259] Serre, J-P. 1973. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg. Translated from the French, Graduate Texts in Mathematics, No. 7. 24

[260] Serre, J-P. 1979. *Local fields*. Graduate Texts in Mathematics, vol. 67. Springer-Verlag, New York-Berlin. Translated from the French by Marvin Jay Greenberg. 195, 595

[261] Serre, J-P. 1995. Cohomologie galoisienne: progrès et problèmes. *Astérisque*, **227**, 229–257. Séminaire Bourbaki, vol. 1993/94, Exp. 783. 439

[262] Serre, J-P. 2002. *Galois cohomology*. English edn. Springer Monographs in Mathematics. Springer-Verlag, Berlin. Translated from the French by Patrick Ion and revised by the author. 513, 600

[263] Smith, H.J.S. 1867. On the orders and genera of quadratic forms containing more than three indeterminates. *Proc. Royal Soc.*, **16**, 197–208. 25

[264] Springer, T. A. 1960a. The classification of reduced exceptional simple Jordan algebras. *Nederl. Akad. Wetensch. Proc. Ser.A 63 = Indag. Math.*, **22**, 414–422. 427, 439

[265] Springer, T.A. 1960b. The projective octave plane. I, II. *Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math.*, **22**, 74–101. 443

[266] Springer, T.A. 1962. Characterization of a class of cubic forms. *Nederl. Akad. Wetensch. Proc. Ser. A 65 = Indag. Math.*, **24**, 259–265. 327, 617

[267] Springer, T.A. 1963. *Oktaven, Jordan-Algebren und Ausnahmegruppen*. Universität Göttingen. 31, 104, 345, 459

[268] Springer, T.A. 1973. *Jordan algebras and algebraic groups*. Springer-Verlag, New York-Heidelberg. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band **75**. vii, 301, 574, 575, 577, 581, 613

[269] Springer, T.A. 1998. *Linear algebraic groups*. second edn. Birkhäuser. 572, 573, 579, 595

[270] Springer, T.A., and Veldkamp, F.D. 2000. *Octonions, Jordan algebras and exceptional groups*. Springer Monographs in Mathematics. Berlin: Springer-Verlag. vii, 147, 160, 345, 459, 574, 575, 579, 613

[271] Stacks Project Authors, The. 2018. *Stacks Project*. https://stacks.math.columbia.edu. x, 16, 35, 46, 55, 56, 79, 154, 226, 229, 231, 233, 234, 235, 614

[272] Steinberg, R. 1961. Automorphisms of classical Lie algebras. *Pacific J. Math.*, **11**, 1119–1129. [= Collected Papers, pp. 101–111]. 544, 599

[273] Strade, H. 2004. *Simple Lie algebras over fields of positive characteristic. I.* de Gruyter Expositions in Mathematics, vol. 38. Berlin: Walter de Gruyter & Co. 526

[274] Thakur, M.L. 1995. Cayley algebra bundles on $\mathbf{A}^2_K$ revisited. *Comm. Algebra*, **23**(13), 5119–5130. 156, 164, 169, 170, 172, 175

[275] Thakur, M.L. 2001. Kummer elements and the mod-3 invariant of Albert algebras. *J. Algebra*, **244**(2), 429–434. 449

[276] Thakur, M.L. 2021. The cyclicity problem for Albert algebras. *Israel J. Math.*, **241**(1), 139–145. 517

[277] Tits, J. 1957. Sur la géométrie des R-espaces. *J. Math. Pures Appl.*, **36**, 17–38. 442

[278] Tits, J. 1966. Algèbres alternatives, algèbres de Jordan et algèbres de Lie exceptionnelles. I. Construction. *Nederl. Akad. Wetensch. Proc. Ser. A 69 = Indag. Math.*, **28**, 223–237. vii

[279] Tits, J. 1971. Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque. *J. Reine Angew. Math.*, **247**, 196–220. 617

[280] Tits, J. 1974. *Buildings of spherical type and finite BN-pairs*. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin-New York. vii

[281] Tits, J. 1976. Classification of buildings of spherical type and Moufang polygons: a survey. Pages 229–246 of: *Colloquio Internazionale sulle Teorie Combinatorie (Roma, 1973), Tomo I*. Atti dei Convegni Lincei, no. 17. Accademia Nazionale dei Lincei. vii

[282] Tits, J. 1990. Strongly inner anisotropic forms of simple algebraic groups. *J. Algebra*, **131**, 648–677. 617

[283] Tits, J., and Weiss, R.M. 2002. *Moufang polygons*. Springer Monographs in Mathematics. Berlin: Springer-Verlag. viii, 340, 341

[284] Tkachev, V.G. 2014. A Jordan algebra approach to the cubic eiconal equation. *J. Algebra*, **419**, 34–51. 354

[285] Totaro, B. 2004. Splitting fields for E_8-torsors. *Duke Math. J.*, **121**, 425–455. 200

[286] Van der Blij, F., and Springer, T.A. 1959. The arithmetics of octaves and of the group G_2. *Nederl. Akad. Wetensch. Proc. Ser. A 62 = Indag. Math.*, **21**, 406–418. 25, 159, 186, 191, 203

[287] Vasconcelos, W.V. 1969a. On finitely generated flat modules. II. *An. Acad. Brasil. Ci.*, **41**, 503–504. 46

[288] Vasconcelos, W.V. 1969b. On projective modules of finite rank. *Proc. Amer. Math. Soc.*, **22**(2), 430–433. 56, 57

[289] Vinberg, E.B. 2017. Non-abelian gradings of Lie algebras. Pages 19–38 of: *50th Seminar "Sophus Lie"*. Banach Center Publications, vol. 113. Polish Academy of Sciences. 614

[290] Vistoli, A. 2005. Grothendieck topologies, fibered categories and descent theory. Pages 1–104 of: *Fundamental algebraic geometry*. Math. Surveys Monogr., vol. 123. Amer. Math. Soc., Providence, RI. 595

[291] Voight, J. 2021. *Quaternion algebras*. Springer. 155

[292] Warner, F.W. 1983. *Foundations of differentiable manifolds and Lie groups*. Graduate Texts in Mathematics, vol. 94. Springer-Verlag, New York-Berlin. Corrected reprint of the 1971 edition. 216

[293] Waterhouse, W.C. 1979. *Introduction to affine group schemes*. Graduate Texts in Mathematics, vol. 66. Springer-Verlag, New York-Berlin. 216, 217, 565, 595

[294] Weiss, R., et al. 2023. Jacques Tits (1930–2020). *Notices Amer. Math. Soc.*, **70**(1), 77–93. vii

[295] Westbury, B.W. 2006. Sextonions and the magic square. *J. London Math. Soc.*, **73**, 455–474. 157

[296] Witt, E., and Kersten, I. 2013. *Ernst Witt: Collected papers — Gesammelte Abhandlungen*. Springer Collected Works in Mathematics. Springer, Heidelberg. Reprint of the 1998 edition. 417

[297] Zak, F. L. 1981. Projections of algebraic varieties. *Mat. Sb. (N.S.)*, **116(158)**(4), 593–602, 608. viii

[298] Zhevlakov, K.A., Slin′ko, A.M., Shestakov, I.P., and Shirshov, A.I. 1982. *Rings that are nearly associative*. Pure and Applied Mathematics, vol. 104. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London. Translated from the Russian by Harry F. Smith. 112, 251

[299] Zorn, M. 1933. Alternativkörper und quadratische Systeme. *Abh. Math. Semin. Hamb. Univ.*, **9**, 395–402. 3, 193, 198

Index of notation

Subject index