Solutions to the exercises
from the book
# Albert algebras over commutative rings

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

# Contents

*Introduction* *page* 1
*Errata for the published edition of* Albert algebras over commutative rings 2
*Addenda to the published edition of* Albert algebras over commutative rings 6
A1 Albert algebras are exceptional 6
A2 Descent of algebras to Dedekind domains 9
A3 Splitting and reducing fields for Freudenthal algebras 15
A4 Describing Albert algebras by the Tits constructions 17
*Solutions for Chapter I* 23
Section 1 23
Section 2 30
Section 3 33
Section 4 33
Section 5 42
Section 6 48
*Solutions for Chapter II* 51
Section 7 51
Section 8 52
Section 9 57
Section 10 65
Section 11 66
Section 12 73
*Solutions for Chapter III* 96
Section 13 96
Section 14 96
Section 15 98

*Solutions for Chapter IV* 101
Section 16 101
Section 17 109
Section 18 114
Section 19 117
Section 20 130
Section 21 130
Section 22 137
Section 23 144
Section 24 156
Section 25 157
Section 26 168
*Solutions for Chapter V* 171
Section 27 171
Section 28 171
Section 29 176
Section 30 183
Section 31 185
Section 32 193
*Solutions for Chapter VI* 200
Section 33 200
Section 34 203
Section 35 220
Section 36 222
Section 37 225
Section 38 247
Section 39 251
Section 40 256
Section 41 261
*Solutions for Chapter VII* 265
Section 42 265
Section 43 281
Section 44 283
Section 45 298
Section 46 304
*Solutions for Chapter VIII* 307
Section 47 307
Section 48 310
Section 49 311
Section 50 311

Section 51 312
*Solutions for Chapter IX* 313
Section 52 313
Section 53 313
Section 54 313
Section 55 315
Section 56 316
Section 58 321

*References* 322
*Subject index* 325

# Introduction

What follows are errata, addenda, and solutions to the exercises in the book *Albert algebras over commutative rings* [17].

The current version of this document can be found on the arXiv at 2406.02933. A shorter text containing just the errata and addenda is also available at Skip's website garibaldibros.com; it may be updated more frequently then the text on the arxiv. There you can also find a current "draft" version of the book with the errata corrected. Please note that the draft version of the book preserves the numbering of theorems, definitions, and so on, but it has different page numbering.

### Equation numbering

In order to reduce ambiguity in cross-references, equations are numbered differently in the printed book from how they are numbered here. In the book, the equations are numbered (1), (2), etc., whereas here in the addenda we number them (a1), (a2), etc., and in the solutions we number them (s1), (s2), etc.

# Errata for the published edition of *Albert algebras over commutative rings*

Page numbers refer to the published/paper edition of the book, published by Cambridge in November 2024. These typos have been corrected in the online/"draft" version you can find on the web. The online/draft versions have a date on their front cover, and the "fixed" date says that the typo has been corrected in all online/draft versions starting with that date.

Thank you to Alberto Elduque, Darij Grinberg, and Eric Rains for identifying some of the following.

If you find other typos, please do tell us! You can send us an email or use the contact form on Skip's website at this link.

## Notation and conventions

*Page xxii, line -17 (fixed 20 Feb 2025)*: The $R$ in $M \times M \to R$ should be replaced by $k$.

## Chapter I: Prologue: the ancient protagonists

*Page 38, item 6.4, line 4 (fixed 16 Dec 2024)*: The $U$-operator maps $U : J \to \mathrm{End}(J)$. That is, the codomain is $\mathrm{End}(J)$ not $J$.

## Chapter II: Foundations

*Page 94, item 12.16, line -2 (fixed 9 Nov 2025)*: The $(Df)$ on this line should be $(Df)_R$.

*Page 95, item 12.17, line 1 after (8) (fixed 9 Nov 2025)*: Insert the following sentence before "Note": To verify each of (1)–(8), one can use (12.15.4) or (12.15.5) to expand both sides and equate coefficients of $\varepsilon$.

*Page 103, item 12.36, line -1 (fixed 26 Nov 2025)*: The lower bound on $p$ should read "$1 \leq p$" instead of "$0 \leq p$".

*Page 104, item 12.39, line 2 (fixed 2 Jan 2025)*: Insert after the first sentence: (See for example [27[1], §VI.3.6] for background on discrete valuations on fields.)

## Chapter IV: Composition algebras

*Page 157, item 19.24, line 5 (fixed 16 Dec 2024)*: Replace $\mathrm{Her}_r(\mathbb{D})$ with $\mathrm{Her}_r(\mathbb{O})$.

## Chapter V: Jordan algebras

*Page 275, item 29.11, line 3 (fixed 20 Feb 2025)*: Replace "that that" with a single "that".

## Chapter VI: Cubic Jordan algebras

*Page 344, item 34.25, line -2 (fixed 19 Jan 2026)*: Replace "in (c)" with "in (b)".

## Chapter VII: The two Tits constructions

*Page 458, item 42.18, line 1 (fixed 16 Jan 2025)*: The first sentence should read: Let $J = J(D, \mu)$ be an Albert algebra arising from a first Tits construction over a field $F$ of characteristic $\neq 3$.

*Page 495, item 45.1, line -2 (fixed 31 Dec 2025)*: Delete the phrase "of the second kind".

*Page 509, item 46.6 proof, line 3 (fixed 16 Dec 2024)*: Should refer to Lemma 46.5, not Proposition.

## Chapter VIII: Lie algebras

*Page 527, line 1 (fixed 20 Feb 2025)*: The first sentence should read: Let $V$ be the subspace of $E = \mathbb{R}^8$ whose points have coordinates $(\xi_i)$ such that $\xi_6 = \xi_7 = -\xi_8$.

[1] For the convenience of the reader: [27] in the printed book = [7].

(That is, replace every $\epsilon$ in the printed version with a $\xi$, to align with the notation in [10].)

*Page 529, item 47.17, line 4 of the remark (fixed 20 Feb 2025)*: Replace "very" with "every".

*Page 565, 51.29 (fixed 20 Feb 2025)*: The statement of part (a) should also include the hypothesis $2 \in k^\times$, in order for the proof provided to be sufficient. The proof needs that the map $\mathfrak{g}_0 \to \mathfrak{v}(n_C)$ is bijective from 51.26(b), which relies on $2 \in k^\times$.

The claim in part (a), that $\mathrm{Der}(J)$ is finitely generated projective of rank 52, does hold in greater generality. Here is a proof using the material from the next chapter, Chapter IX.

First suppose that $k$ is a field, in which case we only need to prove that $\dim(\mathrm{Der}(J)) = 52$. By 52.1(b), $\mathrm{Lie}(\mathbf{Aut}(J)) = \mathrm{Der}(J)$. By Theorem 53.4, $\mathbf{Aut}(J)$ is semisimple of type $\mathsf{F}_4$, so $\dim \mathrm{Lie}(\mathbf{Aut}(J)) = \dim \mathbf{Aut}(J)$ because $\mathbf{Aut}(J)$ is smooth and $\dim \mathbf{Aut}(J) = 52$ because type $\mathsf{F}_4$.

Next suppose that $J$ is the split Albert algebra $\mathrm{Her}_3(\mathrm{Zor}(k))$ over a principal ideal domain $k$. Since $\mathrm{Zor}(k)$ is a finitely generated free module, so is $\mathrm{End}(\mathrm{Zor}(k))$; since additionally $k$ is a principal ideal domain we conclude that the submodule $\mathrm{Der}(J)$ is also finitely generated and free [44, Tag 0AUW]. The field of fractions $F$ of $k$ is a flat extension of $k$, so $\mathrm{Der}(J)_F \cong \mathrm{Der}(J_F)$ by Prop. 50.4, and this has dimension 52 by the previous paragraph, hence $\mathrm{Der}(J)$ has rank 52 at the prime 0. Since $k$ is connected, $\mathrm{Der}(J)$ has constant rank 52.

If $J$ is any Albert algebra over a principal ideal domain $k$, then there is some faithfully flat $K \in k$-**alg** such that $J_K$ is split. Then $\mathrm{Der}(J)_K \cong \mathrm{Der}(J_K) \cong \mathrm{Der}(\mathrm{Her}_3(\mathrm{Zor}(K))) \cong \mathrm{Der}(\mathrm{Her}_3(\mathrm{Zor}(k))) \otimes K$ is finitely generated projective of rank 52 by the previous paragraph, and it follows that $\mathrm{Der}(J)$ is finitely generated projective of rank 52.

*Page 557, item (51.10.2), line 1 (fixed 16 Dec 2024)*: The right side of the equation should read $\{(a_1, a_1^\mathsf{T}) \mid a_1 \in \mathrm{Mat}_3(k)\}$.

*Page 566, alternative proof of 51.29(b), line 2 (fixed 20 Feb 2025)*: Replace $\mathrm{Zor}(k)$ with $\mathrm{Her}_3(\mathrm{Zor}(k))$.

## Chapter IX: Group schemes

*Page 567, item 52.1, paragraph 2, line -2 (fixed 22 Feb 2025)*: Replace $G$ with $\mathbf{G}$.

*Page 588, item proof of 54.6, line 3 (fixed 20 Feb 2025)*: Replace "(1 3 2)" by "(1 2)".

*Page 593, item 54.11, line 2 (fixed 20 Feb 2025)*: Replace "structure" by "system".

*Page 593, item 54.12, line 2 (fixed 20 Feb 2025)*: Replace "structure" by "system".

*Page 603, 55.12 (fixed 29 Mar 2025)*: Replace the statement of the exercise with the following, clearer, version:

Let $F$ be a field. Show that the maps $(A,\tau) \mapsto H(A,\tau)$ and $J \mapsto \mathbf{Aut}(J)$ define bijections between the isomorphism classes of

(i) Azumaya algebras $(A,\tau)$ of degree 3 with unitary involution over $F$, as in 44.23,
(ii) rank 9 Freudenthal $F$-algebras $J$, and
(iii) adjoint semi-simple $F$-group schemes of type $\mathsf{A}_2$.

*Page 619, bottom of page (fixed 20 Feb 2025)*: Insert new paragraph: Results for groups of type $\mathsf{E}_7$ — analogous to the results in this section for type $\mathsf{E}_6$ — can be found in sections 16 and 17 of [95[2]].

## Subject Index

*Page 648, middle of left column (fixed 1 Dec 2025)*: Insert line: balanced pair, 470

[2] For the convenience of the reader: [95] in the printed book = [16].

# Addenda to the published edition of *Albert algebras over commutative rings*

This chapter contains material that could have been in the book and does not require substantial extra background.

## A1 Albert algebras are exceptional

In his first paper on the subject of Jordan algebras, Albert [2] showed that (1) the euclidean Albert algebra $\mathrm{Her}_3(\mathbb{O})$ over the reals is a (linear) Jordan algebra and (2) that it is exceptional. We have shown (1) in Theorem 5.10. More generally, for every octonion algebra $C$ over every ring $k$, we have shown that $\mathrm{Her}_3(C)$ is a Jordan algebra in Theorem 36.5. (Note that Albert algebras are defined in the book to be cubic Jordan algebras, hence Jordan algebras.) In this addendum we would like to extend (2), the exceptionality of Albert algebras, to an arbitrary ring $k$. We prove the following slightly stronger result.

**A1.1 Theorem.** *Every Albert algebra over every non-zero ring is i-exceptional.*

We will define the term i-exceptional in a moment; it is stronger than the notion of exceptional defined in 29.9. When the ring is a field of characteristic different from 2, Theorem A1.1 was first proved in [3]. A proof of Theorem A1.1 for every field can be found in Jacobson's Arkansas notes [21, §2.5]. That proof considers separately the cases of fields of characteristic 2 and different from 2. We provide a proof that does not contain special considerations involving 2.

In the excluded case of the zero ring, all algebras are zero and so the notion of being exceptional or i-exceptional do not make sense.

Here is a beautiful application of the theorem.

**A1.2 Theorem.** *A central simple Jordan algebra over a field is exceptional if and only if it is an Albert algebra.*

*Proof* The central simple exceptional Jordan algebras over a field have been classified into types in §15 of [30]. One finds that each type is either special or an Albert algebra. Albert algebras are exceptional by Theorem A1.1. □

We now provide the promised definition.

**A1.3 Definition.** A Jordan algebra $J$ is *i-special* if $J$ is a homomorphic image of a special algebra and *i-exceptional* if it is not.

Clearly any special Jordan algebra is i-special. However P.M. Cohn has given an example of an i-special Jordan algebra that is exceptional [20, §I.3, Thm. 2]. Therefore being i-exceptional is stronger than being exceptional. We also have the following:

**A1.4 Lemma.** *Let $J$ be a Jordan $k$-algebra. If $J_R$ is i-exceptional for some flat $R \in k$-***alg***, then $J$ is i-exceptional.*

*Proof* We prove the contrapositive. Suppose that $J$ is not i-exceptional, i.e., there is a special Jordan algebra $J'$ and a (surjective) homomorphism $f\colon J' \to J$. Hence there exists a unital associative algebra $A$ and an injective Jordan homomorphism $j\colon J' \to A^{(+)}$. It follows that $f_R\colon J'_R \to J_R$ is still surjective and, by flatness, $j_R\colon J'_R \to (A_R)^{(+)}$ is still injective, i.e., $J_R$ is i-special. □

As a first step in the proof of Theorem A1.1, we note the following, which could have appeared in 37.7.

**A1.5 Lemma.** *For $J = \mathrm{Her}_3(C)$, $C$ a multiplicative conic alternative algebra, and $a[ij]$, $b[ji]$, $c[il] \in J$ with $\{i, j, k\} = \{1, 2, 3\}$,*

$$\{a[ij]\, b[ji]\, c[il]\} = a(bc)[il]. \tag{a1}$$

We remark that if $C$ is associative, then (a1) follows immediately from matrix multiplication.

*Proof* Using (33.6.2), (36.4.6), (36.4.7),

$$\begin{aligned}\{a[ij]\, b[ji]\, c[il]\} &= T_J(a[ij], \bar{b}[ij])c[il] - (c[il] \times a[ij]) \times b[ji] \\ &= n_C(a, \bar{b})c[il] - \bar{a}c[jl] \times b[ji] \\ &= (n_C(a, \bar{b})c - \bar{b}(\bar{a}c))[il].\end{aligned}$$

Replace $\bar{a}$ and $\bar{b}$ using (16.5.4) and expand. By (16.5.5), Proposition 16.10 and alternativity, we obtain (a1). □

The following polynomial map was introduced by Glennie [18]:

$$g_9(x,y,z) := U_x z \circ \{x\, U_z y^2\, y\} - U_y z \circ \{x\, U_z x^2\, y\} \\ - U_x U_z \{x\, U_y z\, y\} + U_y U_z \{x\, U_x z\, y\}.$$

It is homogeneous of degree 9 and skew-symmetric in $x$ and $y$.

**A1.6 Lemma.** *Let $C$ be a multiplicative conic alternative algebra. If $C$ is not associative, then $g_9$ is not identically zero on* $\mathrm{Her}_3(C)$.

*Proof* Consider the following substitution,

$$x = 1[12], \quad y = 1[23], \quad z = a[12] + b[23] + c[31], \quad x,y,z \in \mathrm{Her}_3(C),$$

for $a$, $b$, $c \in C$. Using (16.12.2), (17.4.2), the Peirce decomposition rules (32.15), the identities of 37.7 and Lemma A1.5, one computes

$$x^2 = e_{11} + e_{22}, \quad y^2 = e_{22} + e_{33}, \quad U_x z = \bar{a}[12], \quad U_y z = \bar{b}[23].$$

Futhermore

$$\begin{aligned}
U_z x^2 &= n_C(a)e_{11} + n_C(a)e_{22} + (n_C(b) + n_C(c))e_{33} + \bar{a}\,\bar{c}[23] + \bar{b}\,\bar{a}[31].\\
U_z y^2 &= n_C(b)e_{22} + n_C(b)e_{33} + (n_C(a) + n_C(c))e_{11} + \bar{c}\,\bar{b}[12] + \bar{b}\,\bar{a}[31].\\
\{x\, U_z y^2\, y\} &= t_C(ab)e_{22} + \bar{c}\,\bar{b}[23] + n_C(b)1[31].\\
\{x\, U_z x^2\, y\} &= t_C(ab)e_{22} + \bar{a}\,\bar{c}[12] + n_C(a)1[31].\\
U_x z \circ \{x\, U_z y^2\, y\} &= t_C(ab)\bar{a}[12] + n_C(b)a[23] + (bc)a[31].\\
U_y z \circ \{x\, U_z x^2\, y\} &= n_C(a)b[12] + t_C(ab)\bar{b}[23] + b(ca)[31].\\
\{x\, U_y z\, y\} &= \bar{b}[12],\\
U_z\{x\, U_y z\, y\} &= n_C(b)t_C(c)e_{33} + aba[12] + n_C(b)\bar{a}[23] + (c\bar{b})\bar{a}[31].\\
U_x U_z\{x\, U_y z\, y\} &= \overline{aba}[12].\\
\{x\, U_x z\, y\} &= \bar{a}[23].\\
U_z\{x\, U_x z\, y\} &= n_C(a)t_C(c)e_{11} + n_C(a)\bar{b}[12] + bab[23] + \bar{b}(\bar{a}c)[31].\\
U_y U_z\{x\, U_x z\, y\} &= \overline{bab}[23].
\end{aligned}$$

Therefore

$$g_3(x,y,z) = (t_C(ab)\bar{a} - n_C(a)b - \overline{aba})[12] + (n_C(b)a - t_C(ab)\bar{b} + \overline{bab})[23] \\ + [b,c,a][31].$$

The [12] and [23] entries are 0 by (17.4.2). If $C$ is not associative, one can choose $a$, $b$, $c \in C$ such that the associator $[a,b,c] \neq 0$, in which case the [31] entry is not 0. □

**A1.7 Lemma.** *The Glennie polynomial $g_9(x,y,z)$ vanishes on every i-special Jordan algebra.*

*Proof* A special Jordan algebra is a subalgebra of $A^{(+)}$ for some associative algebra $A$. Let $u, v, w \in A$. Substituting $x = u$, $y = v$, $z = w$ in $g_9(x,y,z)$, we obtain

$$\begin{aligned} &uwuuwv^2wv + uwuvwv^2wu + uwv^2wvuwu + vwv^2wuuwu \\ &\quad - vwvuwu^2wv - vwvvwu^2wu - uwu^2wvvwv - vwu^2wuvwv \\ &\quad - uwuvwvvwu - uwvvwvuwu + vwuuwuvwv + vwvuwuuwv = 0. \end{aligned}$$

If $J$ is an i-special Jordan algebra, then by definition there is a surjection $f\colon J' \to J$ such that $J'$ is special. Then $g_9$ on $J$ can be computed as the composition $g_9 f$ on $J'$, which is identically zero by the preceding paragraph. □

In fancier language, we have shown that $g_9$ is an *s-identity*, i.e., it is not identically zero for every Jordan algebra (Lemma A1.6) and it vanishes on every special Jordan algebra (Lemma A1.7).

*Proof of Theorem A1.1* If $J$ is an Albert algebra, by Corollary 39.32, there exists a faithfully flat extension $R \in k$-**alg** such that $J_R \cong \mathrm{Her}_3(\mathrm{Zor}(R))$. Since $\mathrm{Zor}(R)$ is not associative, Lemmas A1.6 and A1.7 show that $J_R$ is not i-special, i.e., is i-exceptional, and it follows (Lemma A1.4) that $J$ is i-exceptional. □

## A2 Descent of algebras to Dedekind domains

Chapter I of the book, especially section 6, addressed the question of what properties of a $\mathbb{Z}$-submodule of a real Jordan or Albert algebra correspond to it being a Jordan or Albert algebra over $\mathbb{Z}$. That part of the text, however, takes a naive view of the objects involved and therefore does not obviously give statements about the more sophisticated notions of cubic Jordan and Freudenthal algebras defined later in the text. We rectify that here.

The general setting we describe is some integral domain $k$ contained in a field $F$ and we wish to give properties of a $k$-submodule $M$ of some algebraic object over $F$ to guarantee that $M$ is also of the same type of object. We need the following basic tool.

**A2.1 Lemma.** *Let $M$, $N$ be $k$-modules for some integral domain $k$, and let $f\colon M \to N$ be a polynomial law. If there exists a field $F$ containing $k$ such that $f \otimes F = 0$, then $f = 0$ as a polynomial law.*

*Proof* If $k$ is itself a field, then $F$ is a faithfully flat $k$-algebra. Since $0 \otimes F = f \otimes F$, $f = 0$ by Exercise 25.35(b). If $k$ is not a field, then it is infinite, so $F$ is infinite. The Principle of Permanence [9, §IV.2.3, Scholium] then says that $f_R = 0$ for every $k$-algebra $R$ and therefore $f = 0$. □

## Jordan algebras

Recall from Definition 29.1 that a Jordan algebra is a para-quadratic algebra such that two identities concerning the $U$-operator hold strictly, meaning as polynomial laws.

**A2.2 Proposition** (Jordan algebras, first version)**.** *Let $A$ be a para-quadratic $k$-algebra where $k$ is an integral domain. If there is a field $F$ containing $k$ such that $A \otimes_k F$ is a Jordan $F$-algebra, then $A$ is a Jordan $k$-algebra.*

*Proof* We must verify that the polynomial laws $A \times A \times A \to A$ given by sending $(x, y, z)$ to

$$U_{U_x y} z - U_x U_y U_x z \quad \text{and} \quad U_x V_{y,x} z - V_{x,y} U_x z$$

are zero as polynomial laws. This follows from Lemma A2.1. □

We can rephrase this in terms of lattices. Let $M$ be a vector space over a field $F$. For an integral domain $k$ contained in $F$, a *$k$-lattice* $\Lambda$ in $M$ is a finitely generated $k$-submodule of $M$ such that the natural $F$-linear map $\Lambda \otimes_k F \to M$ is an isomorphism of $F$-modules.

**A2.3 Proposition** (Jordan algebras, second version)**.** *Suppose $J$ is a Jordan $F$-algebra for a field $F$, $k$ is an integral domain contained in $F$, and $\Lambda$ is a $k$-lattice $J$ that contains $1_J$. If*

*(1)* *$\Lambda$ is closed under the $U$-operator for $J$, or*
*(2)* *$2 \in k^\times$ and $x^2 \in \Lambda$ for every $x \in \Lambda$,*

*then the restriction of the $U$-operator of $J$ turns $\Lambda$ into a Jordan $k$-algebra.*

*Proof* Assume (1), i.e., the restriction of $U$ to $\Lambda$ defines a function $\Lambda \to \mathrm{End}_k(\Lambda)$. Since $U$ on $J$ is a quadratic map in the sense of 11.1, so is the restriction of $U$ to $\Lambda$. Therefore, $\Lambda$ together with $1_J$ and the restriction of $U$ is a para-quadratic $k$-algebra. Now apply Proposition A2.2.

Now assume (2). Since $2 \in k^\times$, we view $J$ as a linear Jordan algebra and write $xy$ for the product of $x, y \in J$. Again because $2 \in k^\times$, for $x, y \in \Lambda$, $xy := \frac{1}{2}((x+y)^2 - x^2 - y^2)$ belongs to $\Lambda$. It follows that $\Lambda$ is closed under the $U$-operator (27.10.1), and we are done by (1). □

## Jordan algebras of degree 3

Next we wish to treat Jordan algebras of degree 3, for which we will restrict to the case where $k$ is a Dedekind domain. In that case, because a $k$-lattice $\Lambda$ is necessarily torsion-free (and by definition finitely generated), it follows that $\Lambda$ is projective [44, Tags 00NX, 0AUW].

Recall that a cubic Jordan algebra can be defined as a Jordan algebra $J$ together with a cubic form $N$ on $J$ as in 34.1, or as a cubic norm structure meaning a module $J$ together with a base point $1_J$, quadratic map $\sharp$, and cubic form $N$ as in 33.1 and 33.4; the two notions are interchangeable by Corollary 34.6. Certain identities regarding these maps are required to hold as polynomial laws.

A Jordan algebra of degree 3 is defined in 38.1(b) as a cubic Jordan algebra $J$ such that the set map $J_K \to \wedge^3 J_K$ given by $x \mapsto 1_{J_K} \wedge x \wedge x^2$ is not the zero map for every algebraically closed field $K \in k$-**alg**.

**A2.4 Proposition** (Compare Theorem 6.11)**.** *Let $F$ be a field of characteristic $\neq 2$, and suppose $J$ is a Jordan algebra of degree 3 over $F$. Let $k$ be an infinite Dedekind domain contained in $F$. For a $k$-lattice $\Lambda$ in $J$ containing $1_J$, the following are equivalent:*

*(i)* *The restriction of the $U$-operator and $N$ turn $\Lambda$ into a cubic Jordan algebra.*
*(ii)* *$x^2 \in \Lambda$ for all $x \in \Lambda$.*
*(iii)* *$x^\sharp \in \Lambda$ for all $x \in \Lambda$.*

*Proof* It is trivial that (i) implies (ii) and (iii), so the work is in proving the opposite implications. The idea is to imitate the proof of Theorem 6.11 in the book, substituting items according to the following table, where $K$ denotes the fraction field of $k$:

| book | $\mathbb{Z}$ | $\mathbb{Q}$ | $\mathbb{R}$ | $\mathrm{Her}_3(\mathbb{D})$ |
|---|---|---|---|---|
| here | $k$ | $K$ | $F$ | $J$ |

We also replace various identities regarding $\mathrm{Her}_3(\mathbb{D})$ from Chapter I with the corresponding properties for cubic Jordan algebras from Chapter VI, for example: (5a.8) is replaced by (34.1.4); Exercise 6.16 is replaced by (33a.6); and Exercise 6.12(b) is replaced by (33.6.1) and (33.24). We now step through the various arguments leading up to Theorem 6.11, and comment on what further changes are required.

The proof of Proposition 3.5 goes through, using that a Dedekind domain is integrally closed. Lemma 3.7, Proposition 3.8, and Exercises 3.19 and 6.15 go through.

Lemma 6.7 shows that (ii) implies that the trace $T$, quadratic trace $S$, and norm $N$ of $J$ restrict to maps $\Lambda \otimes K \to K$. In the proof, we use that $K$ has characteristic $\neq 2$ so that we can work with linear Jordan algebras, and so that (ii) gives that $\Lambda \otimes K$ is a $K$-algebra. For the Zariski-density argument following equation (1) in the proof of Lemma 6.7, we require $J$ to be a Jordan algebra of degree 3 and not merely a cubic Jordan algebra in order that the set of elements in $k$ with minimal polynomial of degree 3 is not empty.[3] We require $k$ to be infinite so that the Zariski-open set constructed there has a $k$-point.

Remark 6.8 observes that every $K$-subspace $B$ of $J$ that is closed under squaring is a $K$-subalgebra, because $\operatorname{char} K \neq 2$.

Proposition 6.9 shows that, if $\Lambda$ is closed under taking powers $x \mapsto x^n$ for $n \in \mathbb{N}$, then every $x \in \Lambda$ is integral over $k$ and has $T(x), S(x), N(x) \in k$. In the proof, when Cor. 5.14 is invoked to produce elements $c_1, c_2 \in \mathbb{R}[x]$, we instead produce elements in $\bar{F}[x]$, where $\bar{F}$ denotes the algebraic closure of $F$.

Assuming (ii), the argument in the proof of Theorem 6.11 gives (iii), where Lemma 6.10 is replaced by Lemma A2.5 below.

Assuming (iii), the argument in the proof of Theorem 6.11 shows that the adjoint $\sharp$ and norm $N$ on $J$ restrict to $\Lambda$ to give $\Lambda$ the structure of a cubic array as defined in 33.1. To be a cubic array requires that the element $1_J$ be unimodular, but that is automatic by Exercise 12.44 since $\Lambda$ is a projective $k$-module.

For this cubic array to be a cubic norm structure, certain identities must hold strictly, i.e., as polynomial laws. For each such polynomial law $f$ that we wish to prove is zero, we use Lemma A2.1 to reduce to checking it over $F$, where it holds by hypothesis. The equivalence between cubic norm structures and cubic Jordan algebras (Cor. 34.6) completes the proof of (i). □

Here is the promised generalization of Lemma 6.10 about $\mathbb{Z}$ to the case of a Dedekind domain.

**A2.5 Lemma** (Compare Lemma 6.10)**.** *Let $k$ be a Dedekind domain with quotient field $F$ and suppose $X \subseteq F$ is closed under squaring (i.e., $\xi \in X \Rightarrow \xi^2 \in X$). If the $k$-submodule of $F$ generated by $X$ is finitely generated, then $X \subseteq k$.*

The proof is only cosmetically different from the one in the book.

*Proof* For any $\xi \in F$, we denote by

$$\mathfrak{d}_\xi := \{b \in k \mid b\xi \in k\} \subseteq k$$

the *denominator ideal* of $\xi$. These ideals satisfy the following obvious relations

[3] Note that this property is lacking for the example in Exercise 34.27 that shows that cubic Jordan algebras are not stable under faithfully flat descent.

for all $\xi, \eta \in F$ and $a \in k$:

$$\mathfrak{d}_\xi = k \iff \xi \in k, \quad \mathfrak{d}_\xi \mathfrak{d}_\eta \subseteq \mathfrak{d}_\xi \cap \mathfrak{d}_\eta \subseteq \mathfrak{d}_{\xi+\eta}, \quad \mathfrak{d}_\xi \subseteq \mathfrak{d}_{a\xi}. \tag{a1}$$

Slightly less obvious is

$$\mathfrak{d}_\xi = \prod_{\mathfrak{p}, v_\mathfrak{p}(\xi)<0} \mathfrak{p}^{-v_\mathfrak{p}(\xi)}. \tag{a2}$$

In order to see this, let $b \in k$. Then $b \in \mathfrak{d}_\xi$ if and only if $v_\mathfrak{p}(b) \geq -v_\mathfrak{p}(\xi)$ for all $\mathfrak{p}$, which holds trivially for $v_\mathfrak{p}(\xi) \geq 0$ and thus is equivalent to its validity for all $\mathfrak{p}$ having $v_\mathfrak{p}(\xi) < 0$, that is, to $b$ belonging to the right-hand side of (a2). This verifies (a2). As an immediate consequence, we conclude

$$\mathfrak{d}_{\xi^2} = \mathfrak{d}_\xi^2. \tag{a3}$$

Now let $\xi_1, \ldots, \xi_n$ be a finite sequence in $X$ generating the $k$-submodule of $F$ generated by $X$. Then any $\xi \in X$ may be written as $\xi = \sum_{i=1}^n a_i \xi_i$, for some $a_1, \ldots, a_n \in k$, which by (a1) implies

$$\mathfrak{d}_\xi \supseteq \prod_{i=1}^n \mathfrak{d}_{a_i \xi_i} \supseteq \mathfrak{d} := \prod_{i=1}^n \mathfrak{d}_{\xi_i},$$

the latter being a fractional ideal of $F$ depending only on $X$. Thus $\mathfrak{d}_\xi$ divides $\mathfrak{d}$ for all $\xi \in X$. But $\mathfrak{d}$ has only finitely many divisors, so $\{\mathfrak{d}_\xi \mid \xi \in X\}$ is a finite set. On the other hand, the fractional ideals of $F$ form a free, hence torsion-free, abelian group, and for any $\xi \in X$ having $\mathfrak{d}_\xi \neq (1) = k$, the hypothesis of the lemma would yield a sequence $(\xi^{2^n})_{n\geq 0}$ of elements in $X$ such that the $\mathfrak{d}_{\xi^{2^n}}$, $n = 0, 1, 2, \ldots$, by (a3) would be mutually distinct, a contradiction. Thus $\mathfrak{d}_\xi = k$ for all $\xi \in X$, and (a1) implies $X \subseteq k$. □

## Albert algebras

Next we wish to give a result for Albert algebras that is similar to Propositions A2.2, which we will do in Theorem A2.7. Recall that an Albert $k$-algebra $J$ is a cubic Jordan algebra whose underlying module is finitely generated projective[4] and such that $J_K$ is simple of rank 27 for every field $K \in k$-**alg**.

The heavy lifting for this is done by the following lemma, which encapsulates arguments by Racine and van der Blij–Springer.

**A2.6 Lemma.** *Let $F$ be a field that is complete with respect to a discrete*

[4] The definition in 39.8 has that the module is projective and its rank is locally constant, which is a priori a weaker condition, yet Corollary 39.11 proves that the module is finitely generated. Conversely, a finitely generated projective module has locally constant rank [44, Tag 00NX].

*valuation and let $J$ be a cubic Jordan algebra over the valuation ring $k$ of $F$. Then $J$ is the split Albert $k$-algebra if and only if*

*(i)* $J \otimes_k F$ *is the split Albert $F$-algebra and*
*(ii)* *the trace bilinear form on $J$ is regular.*

*Proof* Since the trace bilinear form on an Albert algebra is regular (39.19(b)) and split Albert algebras remain so after base change, the two conditions are clearly necessary.

Conversely, given the two conditions and since $k$ is a Dedekind domain, [41, p. 115, §IV.4, Prop. 5] says that $J$ is isomorphic to $\mathrm{Her}_3(C)$ for $C$ a maximal order in the split octonions over $F$. (We note that while the isomorphism statements for $J$ in [41] are as quadratic Jordan algebras, such isomorphisms are isomorphisms also as cubic Jordan algebras by Cor. 38.18.) Since $k$ is a complete discrete valuation ring, all maximal orders in the split octonions are isomorphic [5, (3.4)], so we may assume that $C$ is the split octonions over $k$, ergo $J$ is itself the split Albert algebra. □

**A2.7 Theorem.** *Let $k$ be a Dedekind domain and suppose $J$ is a cubic Jordan algebra over $k$ that is regular. If there is a field $F \supseteq k$ such that $J \otimes_k F$ is an Albert algebra, then $J$ is an Albert algebra.*

Recall from 33.3 that $J$ is defined to be regular if its underlying $k$-module is finitely generated projective and the bilinear trace form is regular as a symmetric bilinear form.

*Proof* Because the rank of $J$ is locally constant and $k$ is an integral domain, the rank of $J$ at every prime equals $\dim_F(J_F) = 27$. Consequently, it suffices to prove that $J_K$ is an Albert algebra for every field $K \in k$-**alg**. So suppose that $K = k(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of $k$.

If $\mathfrak{p} = 0$, then $K$ is the fraction field of $k$. Since $F$ is faithfully flat over $K$, the base change $J_K$ is an Albert algebra by Cor. 39.32.

Assume $\mathfrak{p} \neq 0$, and write $E$ for the completion of $F$ with respect to the discrete valuation defined by $\mathfrak{p}$. Now $J_E$ is an Albert algebra so there is a finite[5] extension $E'$ of $E$ that splits $J_E$ by Cor. 54.19 and Prop. 55.5. The discrete valuation on $E$ extends to one on $E'$ and we take $R$ to be the valuation ring of $E'$ with respect to that extension. Since $E'$ is finite over $E$, it is complete with respect to the valuation. Now $J_R$ is regular because $J$ is, and $J_{E'}$ is the split Albert algebra, so $J_R$ is the split Albert algebra by Lemma A2.6. For $\ell$ the residue field of $R$, then, $J_\ell$ is the split Albert algebra. But $\ell$ is a finite extension of $K$, so we deduce that $J_K$ is also an Albert algebra.

[5] In fact, separable of dimension dividing 6, by Proposition A3.3.

For any $K \in k$-**alg**, there is some prime ideal $\mathfrak{p}$ (possibly zero) such that $K \supseteq k(\mathfrak{p})$. Since $J_{k(\mathfrak{p})}$ is an Albert algebra, so is $J_K$. □

**A2.8 Application.** Pick $k$ to be an infinite Dedekind domain of characteristic $\neq 2$. Let $F$ be any field containing $k$, and let $A$ be an Albert algebra over $F$. For example, you could take $k$ to be the ring of integers in a number field with a real embedding, $F = \mathbb{R}$, and $A$ to be the euclidean Albert algebra.

If you pick any $k$-lattice $J$ in $A$ that contains $1_J$ and is closed under the $\sharp$ operator in $A$, then by Theorem A2.4 $J$ is a cubic Jordan algebra. If furthermore the bilinear trace form on $J$ (the restriction of the bilinear form on $A$) is regular, then Theorem A2.7 gives that $J$ is an Albert algebra over $k$ as defined in 39.18.

## A3 Splitting and reducing fields for Freudenthal algebras

In this section, we consider a Freudenthal algebra $J$ over a field $F$ and prove the existence of separable extensions $K \supseteq L \supseteq F$ of small dimension such that $J_K$ is split (as defined in 39.20) and $J_L$ is reduced (as defined in 41.1).

### Dimensions 1 and 3

If $\dim_F J = 1$, then $J \cong k^{(+)}$, so $J$ is split and we may take $K = F$.

If $\dim_F J = 3$, then $J \cong E^{(+)}$ for a cubic étale $F$-algebra $E$ that is uniquely determined up to isomorphism, see Cor. 55.2 or Exercise 39.42(b). For such a $J$, being reduced is equivalent to being split — i.e., $J \cong (F \times F \times F)^{(+)}$ — which is equivalent to $E \cong F \times F \times F$. If $E \cong F \times K$ for a field $K$, then $E \otimes_F K$ is split. Otherwise, $E$ is a field, and the normal closure $K$ of $E$ has dimension 3 or 6 and $E \otimes_F K$ is split. In summary, one can take $L = K$ and $K$ of dimension dividing 6.

### Dimensions 9, 15, and 27

**A3.1 Lemma.** *Suppose $J$ is a Freudenthal $F$-algebra of rank $\geq 9$. If $J$ is reduced, then there is a separable extension $K$ of $J$ of degree dividing 2 such that $J_K$ is split.*

*Proof* The hypothesis that $J$ is reduced says that $J \cong \mathrm{Her}_3(C, \Gamma)$ for some composition algebra $C$ (Prop. 39.17) of rank $\geq 2$. If $C$ is split, then $J$ is split (Prop. 40.6), and we take $K = F$. Otherwise, there is a separable quadratic extension $K$ of $F$ contained in $C$ and $C \otimes_F K$ is split (Prop. 22.20, Cor. 22.16). □

Because every Freudenthal algebra of dimension 15 is reduced (Th. 46.8), we obtain:

**A3.2 Corollary.** *If $J$ is a Freduenthal $F$-algebra of dimension 15, then there is a separable extension $K$ of $F$ of dimension dividing 2 such that $J_K$ is split.* □

**A3.3 Proposition.** *Let $J$ be a Freudenthal $F$-algebra of dimension 9 or 27. There exist separable extensions $K \supseteq L \supseteq F$ such that $[K : L]$ divides 2, $[L : F]$ divides 3, $J_K$ is split, and $J_L$ is reduced.*

*Proof #1* If $J$ is reduced, take $L = F$. Otherwise, $J$ is a division algebra (Prop. 39.17), so it contains a a separable cubic subfield $L$ (Cor. 46.7). Since $L \otimes_F L$ is not a field, $(L \otimes_F L)^{(+)}$ contains a nonzero element of norm zero, ergo so does $J_L$, and we conclude that $J_L$ is reduced (Prop. 39.17).

Applying Lemma A3.1 to $J_L$ provides $K$. □

*Proof #2 (sketch)* To produce $K$, use Exercise 55.12 or Prop. 55.5 to translate the problem into producing a field $K$ that splits an absolutely simple algebraic group of type $\mathsf{A}_2$ or $\mathsf{F}_4$. Then apply the main result of [45]. □

**A3.4 Example.** We sketch an example of a field $F$ and an Albert $F$-algebra $J$ that shows that the dimensions in Prop. A3.3 are best possible.

Pick a field $k$. There exists a field $F \supseteq k$ and an Albert $F$-algebra $J$ such that the Rost invariant $r(J)$ of $J$ as described in 55.10 has order 6 as an element of the abelian group $H^3(F, \mathbb{Z}/6\mathbb{Z}(2))$. Here are two ways to produce $F$ and $J$:

(1) Do it explicitly, using the second Tits construction and the formulas for $r(J)$ provided in [38], [37], [39], and [25, §40].

(2) Take $\mathbf{G}$ to be the automorphism group of the split Albert algebra, which is a split semi-simple group scheme of type $\mathsf{F}_4$. Find a versal $\mathbf{G}$-torsor $\mathbf{X}$, which exists by [15, p. 12] and is defined over some extension field $F$ of $k$. Take $J$ to be the Albert $F$-algebra corresponding to $\mathbf{X}$ by Prop. 55.5. The fact that $r(J)$ has order 6 follows from [15, pp. 31, 135].

Suppose now that $K$ is a finite separable extension of $F$ such that $J_K$ is split. Then the restriction $\operatorname{res}_{K/F}(r(J)) \in H^3(K, \mathbb{Z}/6\mathbb{Z}(2))$ is zero, consequently the corestriction satisfies

$$[K : F]\, r(J) = \operatorname{cor}_{K/F} \operatorname{res}_{K/F}(r(J)) = \operatorname{cor}_{K/F}(0) = 0 \tag{a1}$$

in $H^3(F, \mathbb{Z}/6\mathbb{Z}(2))$, ergo 6 divides $[K : F]$. A similar argument shows that every separable extension $L$ of $F$ such that $J_L$ is reduced has dimension divisible by 3.

The argument in the example works with essentially no changes also for dimension 9.

The restriction/corestriction argument around (a1) gives a converse to Proposition A3.3: *If $J$ is an Albert $F$-algebra that is not reduced and $L$ is a separable extension of $F$ such that $J_L$ is reduced, then 3 divides* $[L : F]$. (Compare Exercise 12.41.)

Using the same restriction/corestriction argument or combining Th. 41.26 and Springer's theorem on quadratic forms under odd-degree extensions [14, Cor. 18.5, 18.6] completes the converse: *If $J$ is an Albert $F$-algebra in which every nilpotent element is zero and $K$ is a separable extension of $F$ such that $J_K$ does contain nonzero nilpotents, then 2 divides* $[K : F]$.

### Dimension 6

It remains to treat the case of a Freudenthal algebra $J$ of rank 6. We will assume that $J$ is regular, equivalently (by Cor. 39.15) that $\operatorname{char} F \neq 2$. By Th. 46.8, any such $J$ is reduced, i.e., of the form $\mathrm{Her}_3(F, \Gamma)$ for some $\Gamma = \operatorname{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathbf{GL}_3(F)$. The algebra $J$ that is defined to be split in 39.20 has $\Gamma = \operatorname{diag}(1, 1, 1)$, whereas the $J$ that has $\mathbf{Aut}(J)$ split has $\Gamma = \operatorname{diag}(1, -1, -1)$ (Prop. 55.6). Example 39.35 provides an example of a $J$ that is not split by any separable extension of $F$. Consequently, rather than splitting $J$, we instead split $\mathbf{Aut}(J)$.

**A3.5 Lemma.** *Let $J$ be a Freudenthal $F$-algebra of dimension 6 and suppose that* $\operatorname{char} F \neq 2$. *Then there exists a separable extension $K$ of $F$ of dimension dividing 2 such that $J_K \cong \mathrm{Her}_3(F, \operatorname{diag}(1, -1, -1))$.*

*Proof* There is a 3-dimensional regular quadratic form $Q_J$ defined in (41.5.1). Adjoining a square root (which would be a separable extension) is sufficient to make $Q_J$ isotropic, which implies the necessary isomorphism by Th. 41.26. □

## A4 Describing Albert algebras by the Tits constructions

The classical treatment of the two Tits constructions as set forth in Jacobson [20, IX.12] and McCrimmon [28, 29], culminates in the following result ([20, Thm. IX.22], [29, Thm. 8]): If $J$ is an Albert algebra over a field $F$ and $A$ is a central simple associative $F$-algebra of degree 3 making $A^{(+)}$ a subalgebra of $J$, then there exists a scalar $\lambda \in F^\times$ such that the inclusion $A^{(+)} \hookrightarrow J$ can be extended to an isomorphism from the first Tits construction $J(A, \lambda)$ onto $J$. As an immediate corollary, basically the same conclusion can be drawn after

replacing $A^{(+)}$ by the Jordan algebra of symmetric elements of a central simple associative $F$-algebra of degree 3 with unitary involution.

These results are quick to derive, given the approach to the Tits constructions as described in Chap. VII, so we give a proof here. The approach adopted here is different from that taken by Jacobson and McCrimmon. They relied on properties of the special universal envelope of $A^{(+)}$, where $A$ is a central simple associative algebra of degree 3, whereas we combine results from the book with [24].

Throughout we let $F$ be an arbitrary field.

**A4.1 Proposition.** *For a central simple associative $F$-algebra $(B, \tau)$ of degree 3 with unitary involution, the following conditions are equivalent.*

(i) *The center of $B$ is not a field.*

(ii) *$B$ is not simple.*

(iii) *There exists a central simple associative $F$-algebra $A$ of degree 3 such that $H(B, \tau) \cong A^{(+)}$.*

*Proof* Put $K := \mathrm{Cent}(B)$, a quadratic étale $F$-algebra.

(i)⇒(ii). The center of a unital simple algebra is a field (Cor. 9.20).

(ii)⇒(iii). Since $(B, \tau)$ is simple but $B$ is not, Prop. 10.5 yields a simple associative $F$-algebra $A$ having $(B, \tau) \cong (A \times A^{\mathrm{op}}, \varepsilon_A)$ where $\varepsilon_A$ is the exchange involution. We conclude $H(B, \tau) \cong A^{(+)}$ from (29.8.1) and with $L := \mathrm{Cent}(A)$ have $L \times L = K$, hence $L = F$. Thus $A$ is central, while a dimension count shows that $A$ has degree 3.

(iii)⇒(i). Suppose (iii) and not (i), i.e., that $K$ is a field. From Exc. 44.29 (a) we deduce $A_K^{(+)} \cong H(B, \tau)_K = B^{(+)}$, where $A_K$ and then $B$ are both central simple over $K$ (Cor. 9.23 (a)). By [24, Cor. of Thm. 21], therefore, either $A_K \cong B$ or $A_K^{\mathrm{op}} \cong B$. Replacing $A$ by $A^{\mathrm{op}}$ if necessary, we may assume $A_K \cong B$. The action of $\tau$ on $A_K$ induced by any such isomorphism fixes $A$ since $A^{(+)} \cong H(B, \tau)$ and is the conjugation on $K$, hence an automorphism on all of $A_K$, a contradiction to $\tau$ being an anti-automorphism on $B$. □

**A4.2 Corollary.** *For $i = 1, 2$, let $(B_i, \tau_i)$ be central simple associative $F$-algebras of degree 3 with unitary involutions and $K_i := \mathrm{Cent}(B_i)$. If $H(B_1, \tau_1) \cong H(B_2, \tau_2)$, then $K_1 \cong K_2$ over $F$.*

*Proof* If $K_1$ is split, then Prop. A4.1 yields a central simple associative $F$-algebra $A_1$ of degree 3 such that $H(B_2, \tau_2) \cong A_1^{(+)}$. Hence $K_2$ is split as well. By symmetry, we may therefore assume that $K_1, K_2$ are both fields. Then

$$H((B_1)_{K_2}, (\tau_1)_{K_2}) \cong B_2^{(+)},$$

so $(K_1)_{K_2}$ by Prop. A4.1 is a split quadratic étale $K_2$-algebra. By Exc. 23.40, this implies $K_1 \cong K_2$ over $F$. □

**A4.3 Lemma.** *Let $\mathcal{B} = (K, B, \tau, p)$ be an involutorial system of the second kind over $F$ such that $H(\mathcal{B})$ is a Freudenthal $F$-algebra of dimension 9. Then $(B, \tau)$ is a central simple associative $F$-algebra of degree 3 with unitary involution and $K = \mathrm{Cent}(B)$.*

*Proof* $B^{(+)} = H(\mathcal{B})_K$ (by Exc. 44.29 (a)) is a Freudenthal $K$-algebra of constant rank 9 as a $K$-module. If $K$ is a field, we therefore conclude that $B^{(+)}$ is simple. Hence so is $B$, and Exc. 42.21 implies that $B$ is, in fact, a central simple associative $K$-algebra of degree 3 on which $\tau$ acts as a $K/F$-involution. On the other hand, if $K = F \times F$ is split, Exc. 44.31 (a) yields a pointed cubic alternative $F$-algebra $(A, q)$ such that $B = A \times (A^q)^{\mathrm{op}}$, $\tau = \varepsilon_A$ is the switch and $p = (q, q)$. Letting $K$ act on $F$ through the first factor, we obtain $F \in K$-**alg** and, for the same reason as before, $A = B_F$ is a central simple associative $F$-algebra of degree 3. In both cases, therefore, $(B, \tau)$ is a central simple associative $F$-algebra of degree 3 with unitary involution having $K = \mathrm{Cent}(B)$. □

We can now prove the results announced at the beginning of this section, albeit in the reverse order.

**A4.4 Theorem.** *Let $J$ be an Albert $F$-algebra and $(B, \tau)$ a central simple associative algebra of degree 3 with unitary involution over $F$ making $J_0 := H(B, \tau)$ a Freudenthal subalgebra of $J$. Then there exists an admissible scalar $(p, \mu)$ for $(B, \tau)$ such that the inclusion $J_0 \hookrightarrow J$ can be extended to an isomorphism from the second Tits construction $J(B, \tau, p, \mu)$ onto $J$.*

*Proof* We first assume that $F$ is finite. Then $J$ is split (Exc. 40.17 (b)). But $J' := J(B, \tau, 1, 1)$ is a split Albert $F$-algebra as well, so there is an isomorphism $\Psi\colon J' \xrightarrow{\sim} J$, and this isomorphism maps the subalgebra $J_0 \subseteq J'$ onto a subalgebra $J_0' \subseteq J$. Since $F$ is finite, both $J_0$ and $J_0'$ are reduced simple Freudenthal subalgebras of $J$, and $\Psi$ induces an isomorphism $\varphi\colon J_0 \xrightarrow{\sim} J_0'$. By the Skolem-Noether theorem (Exc. 41.34), $\varphi$ can be extended to an automorphism $\Phi$ of $J$. Hence $\Phi^{-1} \circ \Psi\colon J' \xrightarrow{\sim} J$ is an isomorphism of the desired kind.

Next assume that $F$ is infinite. Applying Thm. 45.10, we find an étale element of $J$ relative to $J_0$[6]. Hence Cor. 44.17 yields an involutorial system

[6] The full force of the difficult Thm. 45.10 will not be needed here. Instead, by a Zariski density argument, we are reduced to the case that $F$ is algebraically closed. Then $J = \mathrm{Her}_3(C)$, $C := \mathrm{Zor}(F)$, is split, and, again by the Skolem-Noether theorem, we may assume $J_0 = \mathrm{Her}_3(D)$, $D$ being the diagonal of $\mathrm{Zor}(F)$. Since $D^\perp \subseteq \mathrm{Zor}(F)$ is a free right $D$-module of rank 3, étale elements of $J$ relative to $J_0$ exist, thanks to Exc. 45.17 (b).

$\mathcal{A} = (K, A, \sigma, p)$ of the second kind over $F$ as well as an admissible scalar $\mu \in K^\times$ such that

$$H(A, \sigma) = H(\mathcal{A}) = H(B, \tau) \tag{a1}$$

and the inclusion $J_0 \hookrightarrow J$ can be extended to an isomorphism from $J(\mathcal{A}, \mu)$ onto $J$. By Lemma A4.3, $(A, \sigma)$ is a central simple associative $F$-algebra of degree 3 with unitary involution and $K = \mathrm{Cent}(A)$. From Cor. A4.2 we deduce $K = \mathrm{Cent}(B)$, while (a1) implies

$$A^{(+)} = H(A, \sigma) \otimes_F K = H(B, \tau) \otimes_F K = B^{(+)},$$

hence $A = B$ by [24, Cor. of Thm. 21], after replacing $A$ by $A^{\mathrm{op}}$ if necessary. But $\sigma$ acts on $H(A, \sigma) = H(B, \tau)$ as the identity and on $K$ by conjugation. Hence $\sigma = \tau$, and the proof is complete. □

**A4.5 Corollary.** *Let $J$ be an Albert $F$-algebra and $A$ a central sinple associative algebra of degree* 3 *over $F$ making $A^{(+)}$ a subalgebra of $J$. Then there exists a $\lambda \in F^\times$ such that the inclusion $A^{(+)} \hookrightarrow J$ can be extended to an isomorphism from the first Tits construction $J(A, \lambda)$ onto $J$.*

*Proof* Put $(B, \tau) := (A \times A^{\mathrm{op}}, \varepsilon_A)$, $\varepsilon_A$ being the exchange involution, and identify $A^{(+)} = H(B, \tau)$ canonically. By Thm. A4.4, there exists an admissible scalar $(p, \mu)$ for $(B, \tau)$ such that the inclusion $A^{(+)} \hookrightarrow J$ can be extended to an isomorphism $\Psi\colon J(B, \tau, p, \mu) \xrightarrow{\sim} J$. Write $p = (q, q)$ with $q \in A^\times$, and $\mu = (\lambda, \lambda')$ with $\lambda, \lambda' \in F^\times$. Applying Thm. 44.19, we find an isomorphism $\Phi\colon J(B, \tau, p, \mu) \xrightarrow{\sim} J(A, \lambda)$ extending the identity of $A^{(+)}$. Thus $\Psi \circ \Phi^{-1}\colon J(A, \lambda) \xrightarrow{\sim} J$ is an isomorphism of the desired kind. □

## A counter example to the Skolem-Noether theorem

The Skolem-Noether theorem in its classical form may be phrased as follows [23, Thm. 4.9]: if $A$ is a central simple associative algebra of finite dimension over a field $F$, then any isomorphism between simple subalgebras of $A$ can be extended to an (inner) automorphism of $A$. This result survives in many different settings. In the present one, we will be concerned with Albert algebras. Given an Albert $F$-algebra $J$, its most important class of subalgebras is provided by the Freudenthal subalgebras of dimension 9, and, indeed, the Skolem-Noether theorem does hold in this particular setting ([33, Thm. 2.7], [35, Thm. 5.2]).

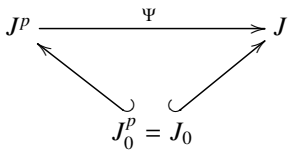
Replacing the base field $F$ by an arbitrary commutative ring, and passing to Azumaya algebras from central simple ones in the process, a straightforward extension of the Skolem-Noether theorem in its classical form to this more

general setting is hardly conceivable[7]. A similar extension of its version for Albert algebras alluded to above seems to be even less likely. In the present note, we will confirm this suspicion. More precisely, we will establish the following result.

**A4.6 Theorem.** *Let $k$ be a commutative ring whose split octonion algebra of Zorn vector matrices, $C := \mathrm{Zor}(k)$, contains an invertible element $p$ such that $C^p$, the unital $p$-isotope of $C$, is not split. Then the split Albert $k$-algebra $J := \mathrm{Her}_3(C)$ admits two split Freudenthal subalgebras of rank 9 as $k$-modules as well as an isomorphism between them that cannot be extended to an automorphism of $J$.*

*Proof* Before proving this result, we should convince ourselves that commutative rings satisfying the hypothesis of the theorem do in fact exist. This follows from Thm. 23.9 and Cor. 23.11.

Entering into the proof proper, we denote by $D$ the diagonal of $C = \mathrm{Zor}(k)$, which is a split quadratic étale subalgebra. After the natural identifications of Prop. 36.9, therefore, $J_0 := \mathrm{Mat}_3(k)^{(+)} = \mathrm{Her}_3(D) \subseteq J$ is a split Freudenthal subalgebra of rank 9. Note that $C^p$ is an octonion algebra which, though no longer split by hypothesis, has the same norm, trace and unit element as $C$ (15.9 and Exc. 17.12). In particular, the diagonal idempotent $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathrm{Zor}(k)$ is elementary not only in $C$ but also in $C^p$. It follows that $D$ is a split quadratic étale subalgebra not only of $C$ but also of $C^p$. Hence $J_0$ may be viewed not only as a split Freudenthal subalgebra of $J$ but also as one of $J^p := \mathrm{Her}_3(C^p)$. In the latter capacity, it will be denoted by $J_0^p$, so we have $J_0^p \subseteq J^p$ as a split Freudenthal subalgebra of rank 9 and $J_0^p = J_0$ as cubic Jordan algebras. Since the Albert algebra $J^p$ is split (Exc. 42.27 (b)), there exists an isomorphism $\Phi\colon J^p \to J$. Hence $J_0' := \Phi(J_0^p) \subseteq J$ is a split Freuidenthal subalgebra of rank 9, and the restriction of $\Phi$ to $J_0^p$ may be regarded as an isomorphism $\varphi\colon J_0 \to J_0'$. We claim that $\varphi$ cannot be extended to an automorphism of $J$. Arguing indirectly, assume that $\eta \in \mathrm{Aut}(J)$ is such an extension. Then $\Psi := \eta^{-1} \circ \Phi\colon J^p \to J$ is an isomorphism rendering the diagram




commutative. Now let $\mathfrak{S} := (e_{11}, e_{22}, e_{33}, u_{23}, u_{31})$ be the diagonal coordinate system of $J_0$, so $u_{jl} = 1_D[jl] = 1_C[jl] = 1_{C^p}[jl]$ for $i = 1, 2$, and write $\mathfrak{S}^p$ for $\mathfrak{S}$

[7] *To do:* Give a precise reference for this.

regarded as a coordinate system of $J_0^p$. Then $\mathfrak{S}$, $\mathfrak{S}^p$ are coordinate systems for $J$, $J^p$, respectively, and $\Psi$, by the diagram above, maps $\mathfrak{S}^p$ to $\mathfrak{S}$. Since $\Psi$ fixes $u_{23}$ and $u_{31}$, it follows from (37.15.3), (37.15.6) that the restriction of $\Psi$ to $J_{12}^p$ gives an isomorphism $\Psi_{12}\colon C_{J^p,\mathfrak{S}^p} \to C_{J,\mathfrak{S}}$ of octonion algebras. On the other hand, since $\mathfrak{S}$ (resp., $\mathfrak{S}^p$) is the *diagonal* coordinate system of $J$ (resp., of $J^p$), Ex. 37.16 implies $C_{J,\mathfrak{S}} \cong C$, $C_{J^p,\mathfrak{S}^p} \cong C^p$, and we arrive at the contradiction that $C$ and $C^p$ are isomorphic. □

# Solutions for Chapter I

## Solutions for Section 1

**1.15** Suppose $A$ is a finite-dimensional real algebra of odd dimension $> 1$. Then there exists $x, y \in A$ that are linearly independent. Put $L_x$ for the linear transformations that is left multiplication by $x$ and similarly for $y$. For $\mathbf{t}$ an indeterminate, $\det(L_x + \mathbf{t}L_y)$ is a polynomial in $\mathbb{R}[\mathbf{t}]$ of odd degree $\dim A$, and therefore it has a nontrivial root in $\mathbb{R}$. That is, there is some $\alpha \in \mathbb{R}$ such that $L_{x+\alpha y} = L_x + \alpha L_y$ is not invertible. Since $x + \alpha y \neq 0$, $A$ is not division.

(This observation, under the additional hypothesis that $A$ is unital, can be found in the entertaining paper [42].)

**1.16** Putting $[x_1, x_2, x_3] =: (a, u)$ for some $a \in \mathbb{C}$, $u \in \mathbb{C}^3$ and using (1.5.1), we obtain

$$\begin{aligned}(a,u) &= [(a_1,u_1),(a_2,u_2),(a_3,u_3)]\\ &= ((a_1,u_1)(a_2,u_2))(a_3,u_3) - (a_1,u_1)((a_2,u_2)8a_3,u_3))\\ &= ((a_1a_2 - \bar{u}_1^{\mathsf{T}}u_2, u_2\bar{a}_1 + u_1a_2 + \bar{u}_1\times\bar{u}_2))(a_3,u_3)\\ &\quad - (a_1,u_1)((a_2a_3 - \bar{u}_2^{\mathsf{T}}u_3, u_3\bar{a}_2 + u_2a_3 + \bar{u}_2\times\bar{u}_3)),\end{aligned}$$

and an application of (1.1.1) combined with the Grassmann identity (1.1.3) yields

$$\begin{aligned}a &= a_1a_2a_3 - \bar{u}_1^{\mathsf{T}}u_2a_3 - a_1\bar{u}_2^{\mathsf{T}}u_3 - \bar{a}_2\bar{u}_1^{\mathsf{T}}u_3 - (u_1\times u_2)^{\mathsf{T}}u_3 - a_1a_2a_3\\ &\quad + a_1\bar{u}_2^{\mathsf{T}}u_3 + \bar{u}_1^{\mathsf{T}}u_3\bar{a}_2 + \bar{u}_1^{\mathsf{T}}u_2a_3 + \overline{u_1^{\mathsf{T}}(u_2\times u_3)}\\ &= \overline{\det(u_1,u_2,u_3)} - \det(u_1,u_2,u_3),\\ x &= u_3\overline{a_1a_2} - u_3\bar{u}_2^{\mathsf{T}}u_1 + u_2\bar{a}_1a_3 + u_1a_2a_3 + (\bar{u}_1\times\bar{u}_2)a_3 + (\bar{u}_2\times\bar{u}_3)a_1\\ &\quad + (\bar{u}_1\times\bar{u}_3)\bar{a}_2 + (u_1\times u_2)\times\bar{u}_3 - u_3\bar{a}_2\bar{a}_1 - u_2a_3\bar{a}_1 - (\bar{u}_2\times\bar{u}_3)\bar{a}_1\\ &\quad - u_1a_2a_3 + u_1\bar{u}_2^{\mathsf{T}}u_3 - (\bar{u}_1\times\bar{u}_3)a_2 - (\bar{u}_1\times\bar{u}_2)\bar{a}_3 - \bar{u}_1\times(u_2\times u_3)\end{aligned}$$

$$\begin{aligned} &= -u_3\bar{u}_2^{\mathsf{T}}u_1 + (\bar{u}_1\times\bar{u}_2)(a_3-\bar{a}_3) + (\bar{u}_2\times\bar{u}_3)(a_1-\bar{a}_1) + (\bar{u}_3\times\bar{u}_1)(a_2-\bar{a}_2)\\ &\quad + (u_1\times u_2)\times\bar{u}_3 + u_1\bar{u}_2^{\mathsf{T}}u_3 + (u_2\times u_3)\times\bar{u}_1\\ &= \sum(\bar{u}_i\times\bar{u}_j)(a_k-\bar{a}_k) + \sum(u_i\times u_j)\times\bar{u}_k. \end{aligned}$$

Thus the associator formula holds, While the $\mathbb{C}$-component of the right-hand side is trivially alternating in $x_1, x_2, x_3$, so is its $\mathbb{C}^3$-component since it is the sum over all cyclic permutations of (123) of a trilinear expression, namely, $(u_1\times u_2)\times\bar{u}_3 + (\bar{u}_1\times\bar{u}_2)(a_3-\bar{a}_3)$, that vanishes for $x_1 = x_2$.

**1.17** Let $x = (a,u), y = (b,v)$ with $a, b \in \mathbb{C}$, $u, v \in \mathbb{C}^3$ and assume $x \neq 0 = xy$. We must show $y = 0$. First of all, (1.5.1) implies

$$ab = \bar{u}^{\mathsf{T}}v, \quad v\bar{a} + ub + \bar{u}\times\bar{v} = 0. \tag{s1}$$

Multiplying the second equation with $\bar{u}^{\mathsf{T}}$ from the left and applying the first combined with (1.1.1), (1.6.4), we obtain

$$0 = \bar{u}^{\mathsf{T}}(\bar{u}\times\bar{v}) + \bar{u}^{\mathsf{T}}ub + \bar{u}^{\mathsf{T}}v\bar{a} = (\|u\|^2 + \|a\|^2)b = \|x\|^2 b,$$

hence $b = 0$. Thus (s1) reduces to

$$u^{\mathsf{T}}\bar{v} = 0, \quad \bar{u}\times\bar{v} = -v\bar{a}. \tag{s2}$$

Here the second equation gives $0 = \bar{v}^{\mathsf{T}}(\bar{u}\times\bar{v}) = -\|v\|^2\bar{a}$, so if $a \neq 0$ then $v = 0$. Hence we are left with the case $a = 0$, which implies $u \neq 0$. On the other hand, (s2) yields $(\bar{u}\times\bar{v})\times u = \bar{v}u^{\mathsf{T}}\bar{u} - \bar{u}u^{\mathsf{T}}\bar{v} = \|u\|^2\bar{v}$, hence again $v = 0$.

**1.18** a) For $a, b \in \mathbb{C}$, $u, v \in \mathbb{C}^3$, $x = (a,u), y = (b,v) \in \mathbb{O}$, we apply (1.5.1), (1.6.7) and conclude

$$\begin{aligned} \overline{xy} &= \overline{(ab - \bar{u}^{\mathsf{T}}v, v\bar{a} + ub + \bar{u}\times\bar{v})} = (\overline{ab - \bar{u}^{\mathsf{T}}v}, -v\bar{a} - ub - \bar{u}\times\bar{v})\\ &= (\bar{b}\bar{a} - \overline{(-v)}^{\mathsf{T}}(-u), (-u)\bar{\bar{b}} + (-v)\bar{a} + (-\bar{v})\times(-\bar{u}))\\ &= (\bar{b}, -v))(\bar{a}, -u) = \bar{y}\bar{x}, \end{aligned}$$

which proves (a).

(b) Let $x = (a,u)$, $y = (b,v)$, with $a, b \in \mathbb{C}$, $u, v \in \mathbb{C}^3$. From (1.5.1) and (1.5.5) we conclude that $t_{\mathbb{O}}(xy) = ab + \bar{a}\bar{b} - \bar{u}^{\mathsf{T}}v - u^{\mathsf{T}}\bar{v} = ab + \bar{a}\bar{b} - \bar{u}^{\mathsf{T}}v - \bar{v}^{\mathsf{T}}u$ is symmetric in $x, y$, giving the first equation. Moreover, the $\mathbb{C}$-component of the associator $[x_1, x_2, x_3]$ in Exc. 1.16 is purely imaginary. Hence the second equation follows from (1.6.5). Combined with (1.6.13) and (a) it implies

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

hence the first of the remaining equations. The second one follows analogously.

(c) The first set of equations follows immediately from (1.6.10) and the definition of the conjugation. As to the remaining ones, we apply alternativity, (1.6.12), (1.6.10), (1.6.6) to deduce

$$\begin{aligned} xyx &= x(x \circ y) - x^2 y = t_{\mathbb{O}}(x)xy + t_{\mathbb{O}}(y)x^2 - n_{\mathbb{O}}(x,y)x - t_{\mathbb{O}}(x)xy + n_{\mathbb{O}}(x)y \\ &= t_{\mathbb{O}}(x)t_{\mathbb{O}}(y)x - n_{\mathbb{O}}(x)t_{\mathbb{O}}(y)1_{\mathbb{O}} - n_{\mathbb{O}}(x,y)x + n_{\mathbb{O}}(x)y \\ &= n_{\mathbb{O}}(x, t_{\mathbb{O}}(y)1_{\mathbb{O}} - y)x - n_{\mathbb{O}}(x)(t_{\mathbb{O}}(y)1_{\mathbb{O}} - y) = n_{\mathbb{O}}(x,\bar{y})x - n_{\mathbb{O}}(x)\bar{y}, \end{aligned}$$

which completes the proof of (c).

**1.19** We begin by proving (1). If tr stands for the trace form of $\mathrm{Mat}_3(\mathbb{C})$, then for any $A \in \mathrm{Mat}_3(\mathbb{C})$, we find a scalar $\lambda(A) \in \mathbb{C}$ such that

$$\mathrm{tr}\Big(((u \times v)w^{\mathsf{T}} + (v \times w)u^{\mathsf{T}} + (w \times u)v^{\mathsf{T}})A\Big) = \lambda(A)\det(u,v,w) \quad (u,v,w \in \mathbb{C}^3) \tag{s1}$$

since the left-hand side is an alternating trilinear function of its arguments $u, v, w \in \mathbb{C}^3$. Specializing $u := e_1$, $v := e_2$, $w := e_3$ and observing $e_i e_i^{\mathsf{T}} = e_{ii}$ in terms of the ordinary matrix units for $1 \leq i \leq 3$, we deduce $\lambda(A) = \mathrm{tr}(A)$, hence

$$\mathrm{tr}\Big(((u \times v)w^{\mathsf{T}} + (v \times w)u^{\mathsf{T}} + (w \times u)v^{\mathsf{T}})A\Big) = \mathrm{tr}\Big(\det(u,v,w)\mathbf{1}_3)A\Big).$$

Since the symmetric bilinear form $(X, Y) \mapsto \mathrm{tr}(XY)$ on $\mathrm{Mat}_3(\mathbb{C})$ is easily seen to be non-degenerate, (1) holds.

It remains to prove the Moufang identities. Since the conjugation of $\mathbb{O}$ is an algebra involution (Exc. 1.18 (a)), the third Moufang identity immediately follows from the first.

We begin by proving the first Moufang identity, which by Exc. 1.18 (c) comes down to showing

$$x(y(xz)) = n_{\mathbb{O}}(x,\bar{y})xz - n_{\mathbb{O}}(x)\bar{y}z. \tag{s2}$$

Since this relation is bilinear in $(y, z)$, it suffices to put $x = a \oplus u$, $a \in \mathbb{C}$, $u \in \mathbb{C}^3$, and to consider the following cases.

*Case 1:* $y = (b, 0)$, $z = (c, 0)$, $b, c \in \mathbb{C}$. Then (1.5.1) yields

$$\begin{aligned} x(y(xz)) &= x\Big(y((a,u)(c,0))\Big) = x((b,0)(ac,uc)) = (a,u)(abc, u\bar{b}c) \\ &= (a^2bc - \bar{u}^{\mathsf{T}}u\bar{b}c, u(ab + \bar{a}\bar{b})c). \end{aligned}$$

On the other hand, applying (1.6.1), (1.6.2) and (1.6.7) we obtain

$$\begin{aligned} n_{\mathbb{O}}(x,\bar{y})xz - n_{\mathbb{O}}(x)\bar{y}z &= n_{\mathbb{O}}((a,u),(\bar{b},v))(a,u)(c,0) - n_{\mathbb{O}}((a,u))(\bar{b},0)(c,0) \\ &= (\bar{a}\bar{b}+ab)(ac,uc) - (\bar{a}a + \bar{u}^{\mathsf{T}}u)(\bar{b}c,0) \\ &= (\bar{a}a\bar{b}c + a^2bc - \bar{a}a\bar{b}c - \bar{u}^{\mathsf{T}}u\bar{b}c, u(abc+\bar{a}\bar{b}c)) \\ &= (a^2bc - \bar{u}^{\mathsf{T}}u\bar{b}c, u(ab+\bar{a}\bar{b})c). \end{aligned}$$

Thus (s2) holds.

*Case 2:* $y = (b,0)$, $z = (0,w)$, $b \in \mathbb{C}$, $w \in \mathbb{C}^3$. Basically arguing as before, we obtain

$$\begin{aligned} x(y(xz)) &= x\Big(y((a,u)(0,w))\Big) = x((b,0)(-\bar{u}^{\mathsf{T}}w, w\bar{a} + \bar{u}\times\bar{w})) \\ &= (a,u)(-b\bar{u}^{\mathsf{T}}w, w\bar{a}\bar{b} + (\bar{u}\times\bar{w})\bar{b}) \\ &= (-ab\bar{u}^{\mathsf{T}}w - \bar{u}^{\mathsf{T}}w\bar{a}\bar{b} - \bar{u}^{\mathsf{T}}(\bar{u}\times\bar{w})\bar{b}, \\ &\quad w\bar{a}^2\bar{b} + (\bar{u}\times\bar{w})\bar{a}\bar{b} - ub\bar{u}^{\mathsf{T}}w + (\bar{u}\times\bar{w})ab + \bar{u}\times(u\times w)b). \end{aligned}$$

Here (1.1.1) and the Grassmann identity (1.1.3) imply $\bar{u}^{\mathsf{T}}(\bar{u}\times\bar{w}) = 0$ as well as $\bar{u}\times(u\times w) = (w\times u)\times\bar{u} = u\bar{u}^{\mathsf{T}}w - w\bar{u}^{\mathsf{T}}u$, hence

$$x(y(xz)) = -\bar{u}^{\mathsf{T}}w(ab+\bar{a}\bar{b}) \oplus (w\bar{a}^2\bar{b} + (\bar{u}\times\bar{w})(ab+\bar{a}\bar{b}) - w(\bar{u}^{\mathsf{T}}u)b)$$

On the other hand,

$$\begin{aligned} n_{\mathbb{O}}(x,\bar{y})xz - n_{\mathbb{O}}(x)\bar{y}z &= n_{\mathbb{O}}((a,u),(\bar{b},0))(a,u)(0,w) - n_{\mathbb{O}}((a,u))(\bar{b},0)(0,w) \\ &= (\bar{a}\bar{b}+ab)(-\bar{u}^{\mathsf{T}}w, w\bar{a}+\bar{u}\times\bar{w}) - (\bar{a}a+\bar{u}^{\mathsf{T}}u)(0,wb) \\ &= -((\bar{u}^{\mathsf{T}}w)(ab+\bar{a}\bar{b}), w(\bar{a}ab + \bar{a}^2\bar{b}) \\ &\quad + (\bar{u}\times\bar{w})(ab+\bar{a}\bar{b}) - w\bar{a}ab - w\bar{u}^{\mathsf{T}}ub) \\ &= (-(\bar{u}^{\mathsf{T}}w)(ab+\bar{a}\bar{b}), w\bar{a}^2\bar{b} + (\bar{u}\times\bar{w})(ab+\bar{a}\bar{b}) - w\bar{u}^{\mathsf{T}}ub) \end{aligned}$$

Comparing with the preceding expression for $x(y(xz))$ settles Case 2.

*Case 3:* $y = (0,v)$, $z = (c,0)$, $v \in \mathbb{C}^3$, $c \in \mathbb{C}$. Then

$$\begin{aligned} x(y(xz)) &= x\Big(y((a,u)(c,0))\Big) = x((0,v)(ac,uc)) = (a,u)(-\bar{v}^{\mathsf{T}}uc, vac + (\bar{v}\times\bar{u})\bar{c}) \\ &= (-a\bar{v}^{\mathsf{T}}uc - \bar{u}^{\mathsf{T}}vac - \bar{u}^{\mathsf{T}}(\bar{v}\times\bar{u})\bar{c}, \\ &\quad v\bar{a}ac + (\bar{v}\times\bar{u})\bar{a}\bar{c} - u\bar{v}^{\mathsf{T}}uc + (\bar{u}\times\bar{v})\bar{a}\bar{c} + \bar{u}\times(v\times u)c). \end{aligned}$$

Here $\bar{u}^{\mathsf{T}}(\bar{v}\times\bar{u}) = 0$ and $\bar{u}\times(v\times u) = (u\times v)\times\bar{u} = v\bar{u}^{\mathsf{T}}u - u\bar{u}^{\mathsf{T}}v$, which implies

$$x(y(xz)) = (-ac(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u), v(\bar{a}a + \bar{u}^{\mathsf{T}}u)c - u(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u)c).$$

On the other hand,

$$\begin{aligned} n_{\mathbb{O}}(x,\bar{y})xz - n_{\mathbb{O}}(x)\bar{y}z &= -n_{\mathbb{O}}((a,u),(0,v))(a,u)(c,0) + n_{\mathbb{O}}((a,u))(0,v)(c,0) \\ &= -(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u)(ac,uc) + (\bar{a}a + \bar{u}^{\mathsf{T}}u)(0,vc) \\ &= (-ac(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u), -u(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u)c + v(\bar{a}a + \bar{u}^{\mathsf{T}}u)c), \end{aligned}$$

and the discussion of Case 3 is complete.

*Case 4:* $y = (0,v)$, $z = (0,w)$, $v,w \in \mathbb{C}^3$. This is the most delicate case of them all.

$$\begin{aligned} x(y(xz)) &= x\Big(y((a,u)(0,w))\Big) = x((0,v)(-\bar{u}^{\mathsf{T}}w, w\bar{a} + \bar{u}\times\bar{w})) \\ &= (a,u)(-\bar{v}^{\mathsf{T}}w\bar{a} - \bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}), -v\bar{u}^{\mathsf{T}}w + (\bar{v}\times\bar{w})a + \bar{v}\times(u\times w)). \end{aligned}$$

Since $\bar{v}\times(u\times w) = (w\times u)\times\bar{v} = u\bar{v}^{\mathsf{T}}w - w\bar{v}^{\mathsf{T}}u$, we conclude

$$\begin{aligned} x(y(xz)) &= (a,u)(-\bar{v}^{\mathsf{T}}w\bar{a} - \bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}), u\bar{v}^{\mathsf{T}}w - w\bar{v}^{\mathsf{T}}u - v\bar{u}^{\mathsf{T}}w + (\bar{v}\times\bar{w})a) \\ &= (-\bar{a}a\bar{v}^{\mathsf{T}}w - a\bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}) - \bar{u}^{\mathsf{T}}u\bar{v}^{\mathsf{T}}w + \bar{u}^{\mathsf{T}}w\bar{v}^{\mathsf{T}}u + \bar{u}^{\mathsf{T}}v\bar{u}^{\mathsf{T}}w - \bar{u}^{\mathsf{T}}(\bar{v}\times\bar{w})a), \\ &\quad u\bar{v}^{\mathsf{T}}w\bar{a} - w\bar{v}^{\mathsf{T}}u\bar{a} - v\bar{u}^{\mathsf{T}}w\bar{a} + (\bar{v}\times\bar{w})\bar{a}a - u\bar{v}^{\mathsf{T}}w\bar{a} - u\bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}) \\ &\quad + (\bar{u}\times\bar{u})v^{\mathsf{T}}\bar{w} - (\bar{u}\times\bar{w})v^{\mathsf{T}}\bar{u} - (\bar{u}\times\bar{v})u^{\mathsf{T}}\bar{w} + \bar{u}\times(v\times w)\bar{a}). \end{aligned}$$

Here $\bar{u}\times(v\times w) = (w\times v)\times\bar{u} = v\bar{u}^{\mathsf{T}}w - w\bar{u}^{\mathsf{T}}v$, so that we obtain

$$\begin{aligned} x(y(xz)) &= (\bar{u}^{\mathsf{T}}v\bar{u}^{\mathsf{T}}w + \bar{u}^{\mathsf{T}}w\bar{v}^{\mathsf{T}}u - \bar{u}^{\mathsf{T}}u\bar{v}^{\mathsf{T}}w - \bar{a}a\bar{v}^{\mathsf{T}}w, -w\bar{v}^{\mathsf{T}}u\bar{a} - w\bar{u}^{\mathsf{T}}v\bar{a} \\ &\quad + (\bar{v}\times\bar{w})\bar{a}a - u\bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}) - (\bar{u}\times\bar{v})u^{\mathsf{T}}\bar{w} - (\bar{u}\times\bar{w})v^{\mathsf{T}}\bar{u}). \end{aligned} \tag{s3}$$

On the other hand,

$$\begin{aligned} n_{\mathbb{O}}(x,\bar{y})xz - n_{\mathbb{O}}(x)\bar{y}z &= -n_{\mathbb{O}}((a,u),(0,v))(a,u)(0,w) + n_{\mathbb{O}}((a,u))(0,v)(0,w) \\ &= -(\bar{u}^{\mathsf{T}}v + \bar{v}^{\mathsf{T}}u)(-\bar{u}^{\mathsf{T}}w, w\bar{a} + \bar{u}\times\bar{w}) + (\bar{a}a + \bar{u}^{\mathsf{T}}u)(-\bar{v}^{\mathsf{T}}w, \bar{v}\times\bar{w}) \\ &= (\bar{u}^{\mathsf{T}}v\bar{u}^{\mathsf{T}}w + \bar{v}^{\mathsf{T}}u\bar{u}^{\mathsf{T}}w - \bar{a}a\bar{v}^{\mathsf{T}}w - \bar{u}^{\mathsf{T}}u\bar{v}^{\mathsf{T}}w, -w\bar{u}^{\mathsf{T}}v\bar{a} - w\bar{v}^{\mathsf{T}}u\bar{a} \\ &\quad - (\bar{u}\times\bar{w})\bar{u}^{\mathsf{T}}v - (\bar{u}\times\bar{w})\bar{v}^{\mathsf{T}}u + (\bar{v}\times\bar{w})\bar{a}a + \bar{u}^{\mathsf{T}}u(\bar{v}\times\bar{w})). \end{aligned}$$

Comparing this with (s3) we see that the $\mathbb{C}$-components are the same. Since $u^{\mathsf{T}}\bar{w} = \bar{w}w^{\mathsf{T}}u$ and $v^{\mathsf{T}}\bar{u} = \bar{u}^{\mathsf{T}}v$, equality of the $\mathbb{C}^3$-components is equivalent to

$$-u\bar{v}^{\mathsf{T}}(\bar{u}\times\bar{w}) - (\bar{u}\times\bar{v})\bar{w}^{\mathsf{T}}u - (\bar{u}\times\bar{w})\bar{u}^{\mathsf{T}}v = -(\bar{u}\times\bar{w})\bar{u}^{\mathsf{T}}v - (\bar{u}\times\bar{w})\bar{v}^{\mathsf{T}}u + (\bar{v}\times\bar{w})\bar{u}^{\mathsf{T}}u,$$

which in turn is equivalent to

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

But this relation holds by (1), and the discussion of Case 4 is complete.

We now turn to the second Moufang identity. Arguing as before, it will be enough to consider the following cases.

*Case 1:* $y = (b,0)$, $z = (c,0)$, $b, c \in \mathbb{C}$. Then (1.5.1) yields

$$\begin{aligned}(xy)(zx) &= \big((a,u)(b,0)\big)\big((c,0)(a,u)\big) = (ab, ub)(ca, u\bar{c})\\ &= (a^2bc - \bar{b}\bar{c}\bar{u}^{\mathsf{T}}u, u\bar{a}\bar{b}\bar{c} + uabc),\\ x(yz)x &= \big((a,u)(bc,0)\big)x = (abc, ubc)(a,u)\\ &= (a^2bc - \overline{bc}\bar{u}^{\mathsf{T}}u, u\overline{abc} + uabc),\end{aligned}$$

hence the assertion.

*Case 2:* $y = (b,0)$, $z = (0,w)$, $b \in \mathbb{C}$, $w \in \mathbb{C}^3$. Then (1.5.1) and (1.1.1) yield

$$\begin{aligned}(xy)(zx) &= \big((a,u)(b,0)\big)\big((0,w)(a,u)\big) = (ab, ub)(-\bar{w}^{\mathsf{T}}u, wa + \bar{w}\times\bar{u})\\ &= \big( - ab\bar{w}^{t}u - a\bar{b}\bar{u}^{t}w - \bar{b}\bar{u}^{\mathsf{T}}(\bar{w}\times\bar{u}),\\ &\quad wa\bar{a}\bar{b} + (\bar{w}\times\bar{u})\bar{a}\bar{b} - ub\bar{w}^{t}u + (\bar{u}\times\bar{w})\bar{a}\bar{b} + \bar{u}\times(w\times u)\bar{b}\big)\\ &= \big( - ab\bar{w}^{\mathsf{T}}u - a\bar{b}\bar{u}^{\mathsf{T}}w, wa\bar{a}\bar{b} - ub\bar{w}^{\mathsf{T}}u + \bar{u}\times(w\times u)\bar{b}\big),\\ x(yz)x &= \Big((a,u)\big((b,0)(0,w)\big)\Big)x = \big((a,u)(0,w\bar{b})\big)x\\ &= \big( - \bar{b}\bar{u}^{\mathsf{T}}w, w\bar{a}\bar{b} + (\bar{u}\times\bar{w})b\big)(a,u)\\ &= \big( - a\bar{b}\bar{u}^{\mathsf{T}}w - ab\bar{w}^{\mathsf{T}}u - \bar{b}(u\times w)^{\mathsf{T}}u,\\ &\quad - ub\bar{w}^{\mathsf{T}}u + wa\bar{a}\bar{b} + (\bar{u}\times\bar{w})ab + (\bar{w}\times\bar{u})ab + (u\times w)\times\bar{u}\bar{b}\big)\\ &= \big( - a\bar{b}\bar{u}^{\mathsf{T}}w - ab\bar{w}^{\mathsf{T}}u, -ub\bar{w}^{\mathsf{T}}u + wa\bar{a}\bar{b} + \bar{u}\times(w\times u)\bar{b}\big),\end{aligned}$$

and a comparison gives the assertion.

Since $\iota_{\mathbb{O}}$ is an algebra involution by Exc. 1.18 (a), the case $y = (0,v)$, $z = (c,0)$ with $v \in \mathbb{C}^3$, $c \in \mathbb{C}$ immediately reduces to Case 2. Thus we are left with

*Case 3:* $y = (0,v)$, $z = (0,w)$, $v, w \in \mathbb{C}^3$. Then we put

$$(xy)(zx) = (a_0, u_0), \quad x(yz)x = (a_1, u_1) \quad (a_i \in \mathbb{C},\ u_i \in \mathbb{C}^3,\ i = 1,2) \tag{s4}$$

and must show $a_0 = a_1$, $u_0 = u_1$. Since

$$xy = (a,u)(0,v) = (-\bar{u}^{\mathsf{T}}v, v\bar{a} + \bar{u}\times\bar{v}), \tag{s5}$$

$$zx = (0,w)(a,u) = (-\bar{w}^{\mathsf{T}}u, wa + \bar{w}\times\bar{u}), \tag{s6}$$

we conclude

$$a_0 = \bar{u}^{\mathsf{T}}v\bar{w}^{\mathsf{T}}u - a^2\bar{v}^{\mathsf{T}}w - a\bar{v}^{\mathsf{T}}(\bar{w}\times\bar{u}) - a(u\times v)^{\mathsf{T}}w - (u\times v)^{\mathsf{T}}(\bar{w}\times\bar{u}),$$

where the last summand may be written as

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

Thus

$$a_0 = \bar{u}^{\mathsf{T}}u\bar{w}^{\mathsf{T}}v - a^2\bar{v}^{\mathsf{T}}w - a\big(\det(u,v,w) + \overline{\det(u,v,w)}\big). \tag{s7}$$

Using (s5), (s6) to compute the $\mathbb{C}^3$-component of $(xy)(zx)$, we obtain

$$\begin{aligned} u_0 = & -wa\bar{v}^{\mathsf{T}}u - (\bar{w}\times\bar{u})\bar{v}^{\mathsf{T}}u - v\bar{a}\bar{w}^{\mathsf{T}}u - (\bar{u}\times\bar{v})\bar{w}^{\mathsf{T}}u + (\bar{v}\times\bar{w})a\bar{a} \\ & + \bar{v}\times(w\times u)a + (u\times v)\times\bar{w}\bar{a} + (u\times v)\times(w\times u). \end{aligned}$$

Here the last three terms may be written as

$$\begin{aligned} \bar{v}\times(w\times u)a &= (u\times w)\times\bar{v}a = w\bar{v}^{\mathsf{T}}ua - u\bar{v}^{\mathsf{T}}wa, \\ (u\times v)\times\bar{w}\bar{a} &= v\bar{w}^{\mathsf{T}}u\bar{a} - u\bar{w}^{\mathsf{T}}v\bar{a}, \\ (u\times v)\times(w\times u) &= v(w\times u)^{\mathsf{T}}u - u(w\times u)^{\mathsf{T}}v = -u\det(u,v,w). \end{aligned}$$

Thus

$$u_0 = -u\bar{v}^{\mathsf{T}}wa - u\bar{w}^{\mathsf{T}}v\bar{a} + (\bar{v}\times\bar{w})a\bar{a} - ((\bar{u}\times\bar{v})\bar{w}^{\mathsf{T}} + (\bar{w}\times\bar{u})\bar{v}^{\mathsf{T}})u - u\det(u,v,w). \tag{s8}$$

We now apply Exc. 1.18 (c) to tackle the expression

$$x(yz)x = n_{\mathbb{O}}(x,\overline{yz})x - n_{\mathbb{O}}(x)\overline{yz}. \tag{s9}$$

Since $yz = (-\bar{v}^{\mathsf{T}}w, \bar{v}\times\bar{w})$, we deduce from (1.6.7) that

$$\overline{yz} = (-\bar{w}^{\mathsf{T}}v, -\bar{v}\times\bar{w}). \tag{s10}$$

When combined with (1.6.2), this implies

$$\begin{aligned} n_{\mathbb{O}}(x,\overline{yz}) = n_{\mathbb{O}}(\overline{yz},x) &= -\bar{v}^{\mathsf{T}}wa - \bar{w}^{\mathsf{T}}v\bar{a} - (v\times w)^{\mathsf{T}}u - (\bar{v}\times\bar{w})^{\mathsf{T}}\bar{u} \\ &= -\bar{v}^{\mathsf{T}}wa - \bar{w}^{\mathsf{T}}v\bar{a} - \det(u,v,w) - \overline{\det(u,v,w)}, \end{aligned} \tag{s11}$$

hence, in view of (s9), (s10), (s7)

$$\begin{aligned} a_1 &= n_{\mathbb{O}}(x,\overline{yz})a + n_{\mathbb{O}}(x)\bar{w}^{\mathsf{T}}v \\ &= -\bar{v}^{\mathsf{T}}wa^2 - \bar{w}^{\mathsf{T}}v\bar{a}a - \det(u,v,w)a - \overline{\det(u,v,w)}a + \bar{w}^{\mathsf{T}}va\bar{a} + \bar{w}^{\mathsf{T}}v\bar{u}^{\mathsf{T}}u = a_0, \end{aligned}$$

giving our first claim. It remains to prove the second, i.e., $u_0 = u_1$. Again by (s9), (s10), we obtain

$$\begin{aligned} u_1 &= n_{\mathbb{O}}(x,\overline{yz})u + n_{\mathbb{O}}(x)(\bar{v}\times\bar{w}) \\ &= -u\bar{v}^{\mathsf{T}}wa - u\bar{w}^{\mathsf{T}}v\bar{a} - u\det(u,v,w) - u\overline{\det(u,v,w)} + (\bar{v}\times\bar{w})\bar{a}a + (\bar{v}\times\bar{w})\bar{u}^{\mathsf{T}}u, \end{aligned}$$

and comparing with (s8) yields

$$u_1 - u_0 = ((\bar{u}\times\bar{v})\bar{w}^{\mathsf{T}} + (\bar{v}\times\bar{w})\bar{u}^{\mathsf{T}} + (\bar{w}\times\bar{u})\bar{v}^{\mathsf{T}} - \det(\bar{u},\bar{v},\bar{w})\mathbf{1}_3)u,$$

which is zero by (1), and the assertion follows.

**1.20** (a): Since

$$n_{\mathbb{H}}(v) = \cos^2(\theta/2) + \|\sin(\theta/2)u\|^2 = \cos^2(\theta/2) + \sin^2(\theta/2) = 1,$$

$v$ is a versor.

Conversely, if $v = \alpha \oplus t \in \mathbb{H}$ is a versor, then since

$$1 = n_{\mathbb{H}}(v) = \alpha^2 + \|t\|^2,$$

$\alpha = \cos(\theta/2)$ for some angle $\theta$. If $\alpha = 1$, then we can take $\theta = 0$ and $u$ any unit vector and we have verified the claim. Similarly if $\alpha = -1$. Thus we may assume that $\sin(\theta/2) \neq 0$ and set $u = (1/\sin(\theta/2))t$ to obtain the required expression

$$\cos(\theta/2) \oplus \sin(\theta/2)u = \alpha \oplus t = v.$$

(b): We use $v^{-1} = \bar{v} = \cos(\theta/2) \oplus -\sin(\theta/2)u$ and expand the product $vsv^{-1}$ using the multiplication formula (1.11.1) and trigonometric double angle identities to find:

$$vsv^{-1} = \frac{1-\cos\theta}{2}(u \cdot s)u + \frac{1+\cos\theta}{2}s + (\sin\theta)u \times s - \frac{1-\cos\theta}{2}(u \times s) \times u.$$

Applying now $(u \times s) \times u = (u \cdot u)s - (u \cdot s)u$ simplifies the expression to the one given by Rodrigues' Formula.

## Solutions for Section 2

**2.7** Put $N := \{(s,t) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq s,t \leq 7,\ s \neq t\}$ and note that $M$ (resp. $N$) has 21 (resp. 42) elements. Defining maps $\varphi_{\pm} \colon M \to N$ by

$$\varphi_+(r,i) := (r+i, r+3i), \quad \varphi_-(r,i) := (r+3i, r+i) \quad ((r,i) \in M, \text{ integers mod } 7), \tag{s1}$$

it suffices to show that (i) the assignments (s1) for $\varphi_{\pm}$ do indeed take values in $N$, (ii) $\varphi_{\pm}$ are both injective, and (iii) their images in $N$ are disjoint. We prove these assertions one at a time.

(i) Let $(r,i) \in M$ and assume $r+i \equiv r+3i \bmod 7$. Then $2i \equiv 0 \bmod 7$, hence $i \equiv 0 \bmod 7$, a contradiction.

(ii) Let $(r,i),(s,j) \in M$. If $\varphi_+(r,i) = \varphi_+(s,j)$, then $r+i \equiv s+j \bmod 7$ and $r+3i \equiv s+3j \bmod 7$. Taking differences, we conclude $2i \equiv 2j \bmod 7$, hence $i \equiv j \bmod 7$ and then $i = j$. This implies $r \equiv s \bmod 7$, hence $r = s$, and we have show that $\varphi_+$ is injective. But $\varphi_-$ agrees with the switch $(s,t) \mapsto (t,s)$ of $N$, which is bijective, composed with $\varphi_+$. Thus $\varphi_-$ is injective as well, which completes the proof of (ii).

(iii) Let $(r,i),(s,j) \in M$ and suppose $\varphi_+(r,i) = \varphi_-(s,j)$. Then $r+i \equiv s+3j \bmod 7$, $r+3i \equiv s+j \bmod 7$, and taking differences yields $2i \equiv -2j \bmod 7$, hence $i+j \equiv 0 \bmod 7$, a contradiction. This proves (iii).

**2.8** (i) ⇒ (iii). Combining (1.6.10) with (2.1.1), we deduce $t_{\mathbb{O}}(u_r) = 0$, $n_{\mathbb{O}}(u_r) = 1$ for $1 \le r \le 7$, so $u_r \in \mathbb{O}^0$ has euclidean norm 1, while (2) follows immediately from (2.1.2). Thus (iii) holds.

(iii) ⇒ (iv). For $1 \le r \le 7$, $i = 1, 2, 4$, indices mod7, we combine (2) with (1.6.13), (1.6.9) and obtain $n_{\mathbb{O}}(u_{r+i}, u_{r+3i}) = t_{\mathbb{O}}(u_{r+i}\bar{u}_{r+3i}) = -t_{\mathbb{O}}(u_{r+i}u_{r+3i}) = -t_{\mathbb{O}}(u_r) = 0$. By Exc. 2.7, therefore, $(u_r)_{1\le r\le 7}$ forms an orthonormal basis of $\mathbb{O}^0$, giving the final assertion of the problem. The second set of equations in (3) is just (2) for $r \ge 4$, $i = 4$, and implies $n_{\mathbb{O}}(u_1u_2, u_3) = n_{\mathbb{O}}(u_4, u_3) = 0$. Thus (iv) holds.

(iv) ⇒ (i). Systematically counting indices mod 7, we establish the desired implication by proving the following intermediate assertions.

1°. $n_{\mathbb{O}}(u_r) = 1$ *for* $1 \le r \le 7$. By (iv) this is clear for $r \le 3$, and for $r \ge 4$ follows from (3) by induction since the norm of $\mathbb{O}$ by Theorem 1.8 permits composition.

2°. $n_{\mathbb{O}}(u_r, u_s) = 0$ *for* $1 \le r, s \le 4$ *distinct.* By (iv), we may assume $s = 4$, $r \le 2$. Then 1.9 implies $n_{\mathbb{O}}(u_r, u_4) = n_{\mathbb{O}}(u_r, u_1u_2) = n_{\mathbb{O}}(u_r)t_{\mathbb{O}}(u_{3-r}) = 0$, as claimed.

3°. *Let* $1 \le r \le 7$ *and* $i = 1, 2, 4$ *such that* $u_r = u_{r+i}u_{r+3i}$. *If* $u_{r+i}$ *has trace zero, then* $u_r$ *has trace zero if and only if* $u_{r+i}, u_{r+3i}$ *are orthogonal. Moreover, if this is so and* $u_{r+i}$ *as well as* $u_{r+3i}$ *both have trace zero, then* $u_r = -u_{r+3i}u_{r+i}$. Since $\bar{u}_{r+i} = -u_{r+i}$, we deduce from (1.6.13) that $t_{\mathbb{O}}(u_r) = -n_{\mathbb{O}}(u_{r+i}, u_{r+3i})$, giving the first assertion. Since, under the final conditions stated, $u_r, u_{r+i}, u_{r+3i}$ are all skew relative to the conjugation of $\mathbb{O}$, and since this is an algebra involution, we conclude $u_r = -\bar{u}_r = -\bar{u}_{r+3i}\bar{u}_{r+i} = -u_{r+3i}u_{r+i}$, as claimed.

4°. $u_r \in \mathbb{O}^0$ *for* $1 \le r \le 7$. By (iv), this is automatic for $r \le 3$, while it follows immediately from 2°, 3° (with $i = 4$) for $r = 4, 5, 6$. It remains to discuss the case $r = 7$. We have $u_7 = u_4u_5$, and 3° combined with 1.9 yields $n_{\mathbb{O}}(u_4, u_5) = n_{\mathbb{O}}(u_1u_2, u_2u_3) = -n_{\mathbb{O}}(u_2u_1, u_2u_3) = -n_{\mathbb{O}}(u_2)n_{\mathbb{O}}(u_1, u_3) = 0$. Hence the first part of 3° yields $t_{\mathbb{O}}(u_7) = 0$.

5°. $(u_r)_{1\le r\le 7}$ *is an orthonormal basis of* $\mathbb{O}^0$ *and* $u_r^2 = -u_0$, $u_ru_s = -u_su_r$ *for* $1 \le r, s \le 7$ *distinct.* The first part follows immediately from 1°, 3°, 4° combined with Exc. 2.7, while the second part is now a consequence of 1° and (1.6.10), (1.6.12).

6°. *Let* $1 \le r \le 7$ *and* $i = 1, 2, 4$ *such that* $u_{r+i}u_{r+3i} = u_r$. *Then*

$$u_{s+j}u_{s+3j} = u_s \qquad (s = r + i,\ j \in \{1, 2, 4\},\ j \equiv 2i \bmod 7), \tag{s1}$$

$$u_{s+j}u_{s+3j} = u_s \qquad (s = r + 3i,\ j \in \{1, 2, 4\},\ j \equiv 4i \bmod 7). \tag{s2}$$

Since $u_{r+3i}u_{r+i} = -u_r$ by 5° and $\mathbb{O}$ is an alternative algebra, $u_{r+3i}u_r = -u_{r+3i}^2 u_{r+i} = u_{r+i}$, and (s1) follows. (s2) is proved similarly.

The proof of the implication (iv) ⇒ (i) will be complete once we have shown that the hypothesis of 6° holds for all $r = 1, \dots, 7$ and $i = 4$. Hence it suffices to establish

7°. $u_{r+4}u_{r+5} = u_r$ *for* $1 \le r \le 7$. By (3), this is clear for $4 \le r \le 7$, and 6° yields

$$u_{s+1}u_{s+3} = u_s \qquad (1 \le s \le 4), \tag{s3}$$

$$u_{s+2}u_{s+6} = u_s \qquad (2 \le s \le 5). \tag{s4}$$

Now let $1 \le r \le 2$. Then (3) combined with 5°, the middle Moufang identity (cf. Exc. 1.19) and (s3) yields

$$\begin{aligned} u_{r+4}u_{r+5} &= (u_{r+1}u_{r+2})(u_{r+2}u_{r+3}) = (u_{r+2}u_{r+1})(u_{r+3}u_{r+2}) = u_{r+2}(u_{r+1}u_{r+3})u_{r+2} \\ &= u_{r+2}u_r u_{r+2} = -u_{r+2}(u_{r+2}u_r) = -u_{r+2}^2 u_r = u_r, \end{aligned}$$

so we are left with the case $r = 3$. Applying (s3) for $s = 1$ and (s4) for $s = 3$, we obtain

$$\begin{aligned} u_7u_8 &= (u_4u_5)u_1 = (u_4u_5)(u_2u_4) = u_4(u_5u_2)u_4 = u_4(u_{3+2}u_{3+6})u_4 \\ &= u_4u_3u_4 = -u_4(u_4u_3) = -u_4^2u_3 = u_3, \end{aligned}$$

as claimed.

Summing up, we have shown not only that conditions (i), (iii), (iv) are equivalent but also the final statement of the problem. It remains to establish (i) ⇔ (ii). The first equation of (1) is the same as (2.1.1). As to the second, the alternative laws combined with the fact that $\mathbb{O}$ is a division algebra yield the following chain of equivalent conditions.

$$\begin{aligned} (u_ru_{r+1})u_{r+3} = -1_{\mathbb{O}} &\iff (u_ru_{r+1})u_{r+3}^2 = -u_{r+3} \iff u_ru_{r+1} = u_{r+3} \\ &\iff u_{(r+3)+4}u_{(r+3)+3\cdot 4} = u_{r+3}. \end{aligned} \tag{s5}$$

Similarly, the third equation of (1) may be rephrased as

$$u_r(u_{r+1}u_{r+3}) = -1_{\mathbb{O}} \iff u_r^2(u_{r+1}u_{r+3}) = -u_r \iff u_{r+1}u_{r+3} = u_r. \tag{s6}$$

Hence (i) implies (ii). Conversely, suppose (ii) holds. Then the first equation of (1) combined with (1.6.10) shows that the elements $u_r$, $1 \le r \le 7$, belong to $\mathbb{O}^0$ and have length 1, while (s5), (s6) yield $u_ru_{r+1} = u_{r+3}$, $u_{r+1}u_{r+3} = u_r$. Combining with (1.6.9), (1.6.13) we deduce $n_{\mathbb{O}}(u_r, u_{r+1}) = t_{\mathbb{O}}(u_r\bar{u}_{r+1}) = -t_{\mathbb{O}}(u_ru_{r+1}) = t_{\mathbb{O}}(u_{r+3}) = 0$ and, similarly, $n_{\mathbb{O}}(u_{r+1}, u_{r+3}) = 0$. In particular, $u_1, u_2, u_3$ form an orthonormal system in $\mathbb{O}^0$ such that $n_{\mathbb{O}}(u_1u_2, u_3) = n_{\mathbb{O}}(u_3, u_4) = 0$, and we have $u_r = u_{r-3}u_{r-2}$ for $4 \le r \le 7$. Since, therefore, condition (iv) holds, so does (ii).

**2.9** $\mathbb{O}^+$ is clearly a commutative real algebra with identity element $1_{\mathbb{O}^+} = 1_{\mathbb{O}}$. Moreover, the squarings in $\mathbb{O}$ and $\mathbb{O}^+$ coincide. Hence any $\varphi \in \mathrm{Aut}(\mathbb{O}^+)$ fixes $1_{\mathbb{O}}$ and preserves squares in $\mathbb{O}$. From (1.6.10) we therefore deduce $t(x)x = n(x)1_{\mathbb{O}}$ for all $x \in \mathbb{O}$, where $t := t_{\mathbb{O}} \circ \varphi - t_{\mathbb{O}}$, $n := n_{\mathbb{O}} \circ \varphi - n_{\mathbb{O}}$. Thus $\mathbb{O}$ is the *union* of the subspaces $\mathrm{Ker}(t)$ and $\mathbb{R}1_{\mathbb{O}}$. This implies first $t = 0$ and then $n = 0$, so $\varphi$ is an orthogonal transformation of $\mathbb{O}$ fixing $1_{\mathbb{O}}$, hence stabilizing $\mathbb{O}^0 = (\mathbb{R}1_{\mathbb{O}})^\perp$. The assignment $\varphi \mapsto \varphi|_{\mathbb{O}^0}$ clearly gives an injective group homomorphism from $\mathrm{Aut}(\mathbb{O}^+)$ to $\mathrm{O}(\mathbb{O}^0)$. Conversely, the unique linear extension fixing $1_{\mathbb{O}}$ of $\psi \in \mathrm{O}(\mathbb{O}^0)$ belongs to the orthogonal group of $\mathbb{O}$ and leaves the trace invariant, hence is an automorphism of $\mathbb{O}^+$. Moreover, the maps in question are inverse isomorphisms not only of abstract groups but, in fact, of topological ones since both are restrictions of linear maps and hence automatically continuous. Finally, $\mathrm{Aut}(\mathbb{O})$ is trivially a subgroup of $\mathrm{Aut}(\mathbb{O}^+)$ which is closed since it may be realized via

$$\mathrm{Aut}(\mathbb{O}) = \bigcap_{x,y \in \mathbb{O}} \{\varphi \in \mathrm{GL}(\mathbb{O}) \mid \varphi(xy) = \varphi(x)\varphi(y)\}$$

as the intersection of a family of closed subsets of $\mathrm{GL}(\mathbb{O})$.

## Solutions for Section 3

**3.17** Put $n := \dim_{\mathbb{R}}(V)$.

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

(iii) $\Rightarrow$ (ii). Since $L_0$ spans $V$ as a real vector space, so does $L$. Since $L$ is an additive subgroup of $L_1$, it is finitely generated and torsion-free, hence free of finite rank with $\mathrm{rk}(L) \leq \mathrm{rk}(L_1) = n$.

(ii) $\Rightarrow$ (i). Let $\varepsilon = (e_1, \ldots, e_r)$, $r \leq n$, be a $\mathbb{Z}$-basis of $L$. Since $L$ spans $V$, so does $\varepsilon$, and we conclude that $\varepsilon$ is an $\mathbb{R}$-basis of $V$, forcing $L \subseteq V$ to be a lattice.

**3.18** $M + \sqrt{2}M \subseteq \mathbb{D}$ is a free abelian subgroup of rank $2\dim_{\mathbb{R}}(\mathbb{D})$ which is obviously closed under multiplication but not a lattice, hence not a $\mathbb{Z}$-structure of $A$.

**3.19** Since $M$ is clearly a discrete additive subgroup of $\mathbb{D}$, it follows that $M' := M \cap \mathbb{R}$ is a discrete additive subgroup of $\mathbb{R}$ containing 1. Thus $M' = \mathbb{Z}v$ for some $0 \neq v \in \mathbb{R}$. Hence $M'$ is a $\mathbb{Z}$-structure of $\mathbb{R}$. As such it contains $\mathbb{Z}$. On the other hand, $v^2 \in M'$ implies $v^2 = rv$ for some integer $r$, hence $v = r \in \mathbb{Z}$, and we also conclude $M' \subseteq \mathbb{Z}$, as desired.

## Solutions for Section 4

**4.8** By Thm. 4.2, $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{h})$ is an $\mathbb{R}$-basis of $\mathbb{H}$ that is associated with $\mathrm{Hur}(\mathbb{H})$. Hence $\mathrm{Hur}(\mathbb{H})$ consists of all linear combinations

$$m1_{\mathbb{H}} + n\mathbf{i} + p\mathbf{j} + q\mathbf{h} = (m + \frac{q}{2})1_{\mathbb{H}} + (n + \frac{q}{2})\mathbf{i} + (p + \frac{q}{2})\mathbf{j} + \frac{q}{2}\mathbf{k}$$

with $m, n, p, q \in \mathbb{Z}$. Since the coefficients of the linear combination on the right either all belong to $\mathbb{Z}$ or to $\frac{1}{2} + \mathbb{Z}$ depending on whether $q$ is even or odd, the assertion follows.

**4.9** Write $x \in L$ in the form $x = \alpha 1_{\mathbb{H}} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{h}$ with $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. We must show $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Replacing $x$ by $x - \lfloor x \rfloor$, $\lfloor x \rfloor := \lfloor \alpha \rfloor 1_{\mathbb{H}} + \lfloor \beta \rfloor \mathbf{i} + \lfloor \gamma \rfloor \mathbf{j} + \lfloor \delta \rfloor \mathbf{h} \in \mathrm{Hur}(\mathbb{H}) \subseteq L$, if necessary, we may assume $0 \leq \alpha, \beta, \gamma, \delta < 1$ and then must show $\alpha = \beta = \gamma = \delta = 0$. By hypothesis and (4.1,2), the quantities

$$n_{\mathbb{H}}(x) = \alpha^2 + \beta^2 + \gamma^2 + (\alpha + \beta + \gamma + \delta)\delta, \tag{s1}$$
$$t_{\mathbb{H}}(x) = 2\alpha + \delta, \tag{s2}$$
$$n_{\mathbb{H}}(\mathbf{i}, x) = 2\beta + \delta, \tag{s3}$$
$$n_{\mathbb{H}}(\mathbf{j}, x) = 2\gamma + \delta, \tag{s4}$$
$$n_{\mathbb{H}}(\mathbf{h}, x) = \alpha + \beta + \gamma + 2\delta \tag{s5}$$

are all integers. Multiplying (s5) by 2 and subtracting the sum of (s2), (s3), (s4) from the result, we conclude $\delta \in \mathbb{Z}$, hence $\delta = 0$, and then $2\alpha, 2\beta, 2\gamma, \alpha^2 + \beta^2 + \gamma^2 \in \mathbb{Z}$ by (s1)–(s4). Thus $\alpha, \beta, \gamma \in \{0, \frac{1}{2}\}$, forcing $\alpha = \beta = \gamma = 0$ as well.

**4.10** We begin by deriving a general formula for the determinant of a block matrix. Let $A \in \mathrm{GL}_p(\mathbb{R})$, $B \in \mathrm{Mat}_{p,q}(\mathbb{R})$, $C \in \mathrm{Mat}_{q,p}(\mathbb{R})$ and $D \in \mathrm{Mat}_q(\mathbb{R})$. Then we claim

$$\det(\begin{pmatrix} A & B \\ C & D \end{pmatrix}) = \det(A)\det(D - CA^{-1}B). \tag{s1}$$

To see this, we make use of the well known fact that (s1) holds for $B = 0$ or $C = 0$. Hence

$$\begin{aligned}
\det(\begin{pmatrix} A & B \\ C & D \end{pmatrix}) &= \det(A)\det(\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A^{-1} & 0 \\ 0 & \mathbf{1}_q \end{pmatrix}) = \det(A)\det(\begin{pmatrix} \mathbf{1}_p & B \\ CA^{-1} & D \end{pmatrix}) \\
&= \det(A)\det(\begin{pmatrix} \mathbf{1}_p & 0 \\ -CA^{-1} & \mathbf{1}_q \end{pmatrix}\begin{pmatrix} \mathbf{1}_p & B \\ CA^{-1} & D \end{pmatrix}) = \det(A)\det(\begin{pmatrix} \mathbf{1}_p & B \\ 0 & -CA^{-1}B + D \end{pmatrix}) \\
&= \det(A)\det(D - CA^{-1}B),
\end{aligned}$$

as claimed. Turning to the matrix $S$ of our problem, we now conclude

$$\begin{aligned}\det(S) &= \det(r\cdot\mathbf{1}_p)\det\left(s\cdot\mathbf{1}_q - T_2(r^{-1}\cdot\mathbf{1}_p)T_1\right) = r^p\det(s\cdot\mathbf{1}_q - r^{-1}T_2T_1)\\ &= r^{p-q}\det(rs - T_2T_1) = r^{p-q}\,\mathrm{char}_{T_2T_1}(rs),\end{aligned}$$

as claimed. Next suppose $T_1 = T$, $T_2 = T^{\mathsf{T}}$, with $T \in \mathrm{Mat}_{p,q}(\mathbb{R})$ being comprised of column vectors $v_1,\dots,v_q \in \mathbb{R}$ that are mutually orthogonal but may have different euclidean lengths. Then

$$T_2T_1 = T^{\mathsf{T}}T = \begin{pmatrix} v_1^{\mathsf{T}} \\ \vdots \\ v_q^{\mathsf{T}}\end{pmatrix}(v_1,\dots,v_q) = (v_i^{\mathsf{T}}v_j)_{1\le i,j\le q} = \mathrm{diag}(\|v_1\|^2,\dots,\|v_q\|^2).$$

Thus the preceding determinant formula reduces to

$$\det(S) = r^{p-q}\prod_{i=1}^{q}(rs - \|v_i\|^2).$$

In particular, if $\|v_i\| = \sqrt{a}$ for some $a > 0$ and all $i = 1,\dots,q$, the second assertion stated in our problem drops out. Finally, assuming $\|v_i\|^2 < rs$ for all $i = 1,\dots,q$, we claim that the matrix $S$ is positive definite. Since it is symmetric, it will be enough to show that all its principal minors are positive. Let $1 \le i \le p+q$. For $i \le p$, the the $i$-th principal minor of $S$ is 1, while for $p < i \le p+q$, it is the determinant of the matrix

$$S' := \begin{pmatrix} r\cdot\mathbf{1}_p & T' \\ (T')^{\mathsf{T}} & s\cdot\mathbf{1}_{i-p}\end{pmatrix},$$

where $T' = (v_1,\dots,v_{i-p}) \in \mathrm{Mat}_{p,i-p}(\mathbb{R})$. But by what we have just seen, $S'$ has determinant

$$\det(S') = r^{p-q}\prod_{j=1}^{p-i}(rs - \|v_j\|^2) > 0,$$

and the assertion follows. Since the final statement of the problem is a special case of this assertion, the solution is complete.

**4.11** (a) If (iii) holds, then (1.6.11) implies $u\bar{u} = n_{\mathbb{D}}(u)1_{\mathbb{D}} = 1_{\mathbb{D}} = \bar{u}u$. Thus (iii) implies (i) and (ii). Conversely, suppose (i) holds. Then $1 = n_{\mathbb{D}}(uv) = n_{\mathbb{D}}(u)n_{\mathbb{D}}(v)$, and since both factors on the right are integers, (iii) holds. This shows that (i) and (iii) are equivalent. The equivalence of (ii) and (iii) is proved similarly. Moreover, for any $v$ satisfying (i) we apply Exc. 1.18 (c) and obtain $\bar{u} = 1_{\mathbb{D}}\bar{u} = (vu)\bar{u} = n_{\mathbb{D}}(u)v = v$ (by (iii)). Reading this in $\mathbb{D}^{\mathrm{op}}$ shows that $v$ as in (ii) is unique and equal to $\bar{u}$. Since the norm of $\mathbb{D}$ permits composition by Thm. 1.8, the set of units in $M$ is closed under multiplication and contains $1_{\mathbb{D}}$.

Finally, by (1.6.8), if $n_{\mathbb{D}}(u) = 1$, then $n_{\mathbb{D}}(\bar{u}) = 1$, so $M^\times$ is also closed under taking inverses.

(b) $(1, i)$ is an orthonormal basis of $\mathbb{C}$ associated with $\mathrm{Ga}(\mathbb{C})$. Hence $\mathrm{Ga}(\mathbb{C})^\times = \{\pm 1, \pm i\}$. Similarly, $(1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ is an orthonormal basis of $\mathbb{H}$ associated with $\mathrm{Ga}(\mathbb{H})$. Hence $\mathrm{Ga}(\mathbb{H})^\times = \{\pm 1_{\mathbb{H}}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. And, finally, any Cartan-Schouten basis $E = (u_r)_{0\le r\le 7}$ of $\mathbb{O}$ is an orthonormal basis associated with $\mathrm{Ga}_\varepsilon(\mathbb{O})$. Hence $\mathrm{Ga}_E(\mathbb{O})^\times = \{\pm u_r \mid 0 \le r \le 7\}$. Now we claim

$$\mathrm{Hur}(\mathbb{H})^\times = \{\pm 1_{\mathbb{H}}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}, \frac{1}{2}(\pm 1_{\mathbb{H}} \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})\}. \tag{s1}$$

To prove this, we note that the first eight elements of the right-hand side belong to $\mathrm{Ga}(\mathbb{H})^\times \subseteq \mathrm{Hur}(\mathbb{H})^\times$. The remaining sixteen may all be obtained from adding a unit of $\mathrm{Ga}(\mathbb{H})$ to $\mathbf{h}$, hence belong to $\mathrm{Hur}(\mathbb{H})$. Since they also have norm 1, the right-hand side of (s1) belongs to the left. Conversely, suppose $u = \alpha_0 1_{\mathbb{H}} + \alpha_1\mathbf{i} + \alpha_2\mathbf{j} + \alpha_3\mathbf{k}$ with $\alpha_i \in \mathbb{R}$, $0 \le i \le 3$, is invertible in $\mathrm{Hur}(\mathbb{H})$. By Exc. 4.8, there are two cases.

*Case 1:* $\alpha_i \in \mathbb{Z}$, $0 \le i \le 3$. Then $u \in \mathrm{Ga}(\mathbb{H})^\times \subseteq \mathrm{Hur}(\mathbb{H})^\times$.

*Case 2:* $\alpha_i = \frac{1}{2} + \beta_i$, $\beta_i \in \mathbb{Z}$, $0 \le i \le 3$. Then

$$1 = n_{\mathbb{H}}(u) = \sum_{i=0}^{3}(\frac{1}{4} + \beta_i + \beta_i^2) = 1 + \sum_{i=0}^{3}(\beta_i^2 + \beta_i),$$

and we conclude $\sum_{i=0}^{3}(\beta_i^2 + \beta_i) = 0$, where the summands are all non-negative. Thus $\beta_i^2 = -\beta_i$, i.e., $\beta_i = -1, 0$ for $0 \le i \le 3$. But this means $\alpha_i = \pm\frac{1}{2}$ for $0 \le i \le 3$, and $u$ belongs to the right-hand side of (s1).

**4.12** That the $\varepsilon_i$, $1 \le i \le 4$, form an orthonormal basis of $\mathbb{H}$ relative to $2\langle x, y\rangle$ follows immediately from the fact that the vectors $1_{\mathbb{H}}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ of $\mathbb{H}$ are orthogonal of norm 1. Moreover, the latter vectors can be linearly expressed by the former according to the formulas

$$\varepsilon_1 - \varepsilon_2 = \mathbf{j}, \quad \varepsilon_2 - \varepsilon_3 = -\mathbf{h}, \quad \varepsilon_3 - \varepsilon_4 = 1_{\mathbb{H}}, \quad \varepsilon_3 + \varepsilon_4 = \mathbf{i}.$$

In particular, the second equation of the problem holds. Given $\xi_i \in \mathbb{R}$, $1 \le i \le 4$, we also obtain

$$\begin{aligned}\sum_{i=1}^{4}\xi_i\varepsilon_i &= \frac{1}{2}(\xi_1\mathbf{j} - \xi_1\mathbf{k} - \xi_2\mathbf{j} - \xi_2\mathbf{k} + \xi_3 1_{\mathbb{H}} + \xi_3\mathbf{i} - \xi_4 1_{\mathbb{H}} + \xi_4\mathbf{i})\\ &= \frac{1}{2}((\xi_3 - \xi_4)1_{\mathbb{H}} + (\xi_3 + \xi_4)\mathbf{i} + (\xi_1 - \xi_2)\mathbf{j} - (\xi_1 + \xi_2)\mathbf{k}).\end{aligned}$$

Using (4.1.1), we therefore deduce

$$\begin{aligned}\sum_{i=1}^{4}\xi_i\varepsilon_i &= \frac{1}{2}((\xi_3-\xi_4)1_{\mathbb{H}}+(\xi_3+\xi_4)\mathbf{i}+(\xi_1-\xi_2)\mathbf{j}-(\xi_1+\xi_2)(2\mathbf{h}-1_{\mathbb{H}}-\mathbf{i}-\mathbf{j}))\\ &= \frac{1}{2}((\xi_1+\xi_2+\xi_3-\xi_4)1_{\mathbb{H}}+(\xi_1+\xi_2+\xi_3+\xi_4)\mathbf{i}+2\xi_1\mathbf{j})-(\xi_1+\xi_2)\mathbf{h}\\ &= \frac{1}{2}(\xi_1+\xi_2+\xi_3-\xi_4)1_{\mathbb{H}}+\frac{1}{2}(\xi_1+\xi_2+\xi_3+\xi_4)\mathbf{i}+\xi_1\mathbf{j}-(\xi_1+\xi_2)\mathbf{h},\end{aligned}$$

which by Thm. 4.2 yields the following chain of equivalent conditions.

$$\begin{aligned}\sum_{i=1}^{4}\xi_i\varepsilon_i\in\mathrm{Hur}(\mathbb{H}) \quad &\Longleftrightarrow \quad \xi_1,\xi_1+\xi_2\in\mathbb{Z},\quad \xi_1+\xi_2+\xi_3\pm\xi_4\in 2\mathbb{Z}\\ &\Longleftrightarrow \quad \xi_1,\xi_2\in\mathbb{Z},\quad \sum_{i=1}^{4}\xi_i\in 2\mathbb{Z},\quad 2\xi_4\in 2\mathbb{Z}\\ &\Longleftrightarrow \quad \xi_1,\xi_2,\xi_3,\xi_4\in\mathbb{Z},\quad \sum_{i=1}^{4}\xi_i\in 2\mathbb{Z}.\end{aligned}$$

Thus the second equation of the problem holds. Finally, we note $n_{\mathbb{H}}(\varepsilon_i)=\frac{1}{2}$ for $1\le i\le 4$, so for $\xi_i\in\mathbb{Z}$, $\sum\xi_i\in 2\mathbb{Z}$, we obtain

$$\sum_{i=1}^{4}\xi_i\varepsilon_i\in\mathrm{Hur}(\mathbb{H})^{\times} \quad\Longleftrightarrow\quad \frac{1}{2}\sum_{i=1}^{4}\xi_i^2=1 \quad\Longleftrightarrow\quad \sum_{i=1}^{4}\xi_i^2=2,$$

which amounts to $\xi_i=\pm 1$ for precisely two indices $i=1,2,3,4$ and $\xi_i=0$ for the remaining ones. But this means the units of $\mathrm{Hur}(\mathbb{H})$ have the form stated at the very end of the problem.

**4.13** (a) This follows immediately from the fact that Cartan-Schouten bases are orthonormal relative to the scalar product $\langle x,y\rangle$. (Exc. 2.8). For example, $n_{\mathbb{O}}(\varepsilon_1)=\frac{1}{4}(n_{\mathbb{O}}(u_0)+n_{\mathbb{O}}(u_2)=\frac{1}{2}$, which implies $2\langle\varepsilon_1,\varepsilon_1\rangle=2n_{\mathbb{O}}(\varepsilon_1)=1$.

(b) We write $L$ for the additive subgroup of $\mathbb{O}$ generated by the quantities assembled in (1). We claim

$$\mathrm{DiCo}(\mathbb{O})\subseteq L\subseteq\frac{1}{2}\sum_{i=1}^{8}\mathbb{Z}\varepsilon_i, \tag{s1}$$

where the second inclusion is obvious. In order to prove the first, we note that

$$\begin{aligned}u_0 &= -\varepsilon_1+\varepsilon_2, \quad u_1=-\varepsilon_3+\varepsilon_4, \quad u_2=\varepsilon_1+\varepsilon_2, \quad u_3=-\varepsilon_3-\varepsilon_4, \qquad \text{(s2)}\\ u_4 &= -\varepsilon_5+\varepsilon_6, \quad u_5=\varepsilon_5+\varepsilon_6,, \quad u_6=\varepsilon_7+\varepsilon_8, \quad u_7=-\varepsilon_7+\varepsilon_8\end{aligned}$$

all belong to $L$. Moreover, (s2) and (4.4.3)–(4.4.7) imply

$$\mathbf{p} = \frac{1}{2}(-\varepsilon_1 + \varepsilon_2 - \varepsilon_3 + \varepsilon_4 + \varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_4) = \varepsilon_2 - \varepsilon_3 \in L, \tag{s3}$$

$$u_1\mathbf{p} = \frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4 - \varepsilon_5 + \varepsilon_6 - \varepsilon_7 + \varepsilon_8) \in L, \tag{s4}$$

$$u_2\mathbf{p} = \frac{1}{2}(\varepsilon_1 - \varepsilon_2 + \varepsilon_1 + \varepsilon_2 + \varepsilon_5 - \varepsilon_6 + \varepsilon_5 + \varepsilon_6) = \varepsilon_1 + \varepsilon_5 \in L, \tag{s5}$$

$$u_4\mathbf{p} = \frac{1}{2}(\varepsilon_3 - \varepsilon_4 + \varepsilon_1 + \varepsilon_2 - \varepsilon_5 + \varepsilon_6 - \varepsilon_7 - \varepsilon_8) \in L. \tag{s6}$$

Thus the basis $E'$ exhibited in (4.5.2), which is associated with DiCo($\mathbb{O}$) by Thm. 4.5, is entirely contained in $L$, and the first inclusion of (s1) holds. From this and Exc. 3.17 we deduce that $L$ is a lattice in $\mathbb{O}$. Since DiCo($\mathbb{O}$) is unimodular by Thm. 4.5, the proof of (b) will be complete once we have shown that the lattice $L$ is integral quadratic (Cor. 3.14). Since $n_{\mathbb{O}}(\varepsilon_i) = \frac{1}{2}$ for $1 \le i \le 8$ by (a), equation (1) yields

$$n_{\mathbb{O}}(\pm\varepsilon_i \pm \varepsilon_j) = n_{\mathbb{O}}(\frac{1}{2}\sum_{i=1}^{8} s_i\varepsilon_i) = 1 \tag{s7}$$

for $1 \le i < j \le 8$ and all families $s = (s_i) \in \{\pm 1\}^8$. Writing $M := \{1, 2, \dots, 8\}$ and $M_s^{\pm} := \{i \in M \mid s_i = \pm 1\}$, it remains to show

$$n_{\mathbb{O}}(\pm\varepsilon_i \pm \varepsilon_j, \pm\varepsilon_k \pm \varepsilon_l) \in \mathbb{Z}, \quad n_{\mathbb{O}}(\frac{1}{2}\sum_{i=1}^{8} s_i\varepsilon_i, \frac{1}{2}\sum_{i=1}^{8} t_i\varepsilon_i) \in \mathbb{Z} \tag{s8}$$

for all $1 \le i < j \le 8$, $1 \le k < l \le 8$ and all families $s = (s_i), t = (t_i) \in \{\pm 1\}^8$ such that $|M_s^-|$ and $|M_t^-|$ are both even. The first relation of (s8) is obvious. In order to prove the second, we let $s = (s_i) \in \{\pm 1\}^8$ be arbitrary and note $|M_s^+| + |M_s^-| = 8$, so $|M_s^{\pm}|$ are either both even or both odd. Moreover, $-s := (-s_i) \in \{\pm 1\}^8$ and $M_{-s}^{\pm} = M_s^{\mp}$. Now, letting also $t = (t_i) \in \{\pm 1\}^8$ be arbitrary and setting $st := (s_i t_i) \in \{\pm 1\}^8$, we obtain

$$n_{\mathbb{O}}(\frac{1}{2}\sum_{i=1}^{8} s_i\varepsilon_i, \frac{1}{2}\sum_{i=1}^{8} t_i\varepsilon_i) = \frac{1}{4}\sum_{i=1}^{8} s_i t_i = \frac{1}{4}(|M_{st}^+| - |M_{st}^-|) = 2 - \frac{1}{2}|M_{st}^-|,$$

and must show that if $|M_s^{\pm}|$ and $|M_t^{\pm}|$ are even, then so is $|M_{st}^{\pm}|$. Suppose not. Then

$$|M_{st}^+| = |M_s^+ \cup M_t^+| + |M_s^- \cup M_t^-|$$

is odd. Replacing $s$ by $-s$, $t$ by $-t$ if necessary, we may assume that $|M_s^+ \cup M_t^+|$ is odd and $|M_s^- \cup M_t^-|$ is even. But then

$$|M_s^+| = |M_s^+ \cup M_t^+| + |M_s^+ \cup M_t^-|$$

shows that $|M_s^+ \cup M_t^-|$ is odd, whence

$$|M_t^-| = |M_s^+ \cup M_t^-| + |M_s^- \cup M_t^-|$$

is odd as well, a contradiction.

(c) Write $L'$ for the right-hand side of (2). Inspecting (s2)–(s6), we conclude $\mathrm{DiCo}(\mathbb{O}) \subseteq L' \subseteq \frac{1}{2}\sum \mathbb{Z}\varepsilon_i$, so $L'$ is a lattice in $\mathbb{O}$ by Exc. 3.17. As before, we will be through once we have shown that $L'$ is integral quadratic. Let $x = \sum \xi_i\varepsilon_i \in L'$ with $\xi_1, \dots, \xi_8 \in \mathbb{R}$. Then (2) implies $2\xi_1 \in \mathbb{Z}$, $\xi_i = \xi_1 + n_i$, $n_i \in \mathbb{Z}$ for $1 \le i \le 8$, and

$$\sum_{i=1}^{8} \xi_i = \sum_{i=1}^{8} (\xi_1 + n_i) = 4(2\xi_1) + \sum_{i=1}^{8} n_i$$

belongs to $2\mathbb{Z}$. Thus $\sum n_i \in 2\mathbb{Z}$, and $N := \{i \in M \mid n_i \equiv 1 \bmod 2\}$ contains an even number of elements. Now $n_{\mathbb{O}}(x) = \frac{1}{2}\sum \xi_i^2$ and

$$\begin{aligned}\sum_{i=1}^{8} \xi_i^2 &= \sum_{i=1}^{8} (\xi_1 + n_i)^2 = \sum_{i=1}^{8} (\xi_1^2 + 2\xi_1 n_i + n_i^2) = 2(2\xi_1)^2 + 2\xi_1 \sum_{i=1}^{8} n_i + \sum_{i=1}^{8} n_i^2 \\ &\equiv \sum_{i=1}^{8} n_i^2 \equiv \sum_{i \in N} n_i^2 \equiv |N| \equiv 0 \bmod 2.\end{aligned}$$

Hence $n_{\mathbb{O}}(x) \in \mathbb{Z}$, as claimed.

(d) By (b), (c) and (s7), the quantities in (1) are all units in $\mathrm{DiCo}(\mathbb{O})$. Conversely, suppose $u = \sum_{i=1}^{8} \xi_i\varepsilon_i$, $\xi_i \in \mathbb{R}$, $1 \le i \le 8$, is invertible in $\mathrm{DiCo}(\mathbb{O})$. Then (a) implies

$$\sum_{i=1}^{8} \xi_i^2 = 2n_{\mathbb{O}}(u) = 2. \tag{s9}$$

If $\xi_1$ is an integer, then all $\xi_i$, $1 \le i \le 8$, are, and (s9) shows that $u$ belongs to the first type of (1). On the other hand, if $\xi_1$ belongs to $\frac{1}{2} + \mathbb{Z}$, then all $\xi_i$, $1 \le i \le 8$, do, and (s9) shows $\xi_i^2 = \frac{1}{4}$, hence $\xi_i = \pm\frac{1}{2}$ for all $i = 1, \dots, 8$. Since $\sum \xi_i \in 2\mathbb{Z}$ by (2) the number if indices $i = 1, \dots, 8$ having $\xi_i$ negative must be even, so $u$ is of the second type in (1).

The units of $\mathrm{DiCo}(\mathbb{O})$ belonging to the first type of (1) are in bijective correspondence with the quadruples of subsets of $M$ consisting of two elements, hence are $4 \cdot \binom{8}{2} = 4 \cdot \frac{8\cdot 7}{2} = 4 \cdot 28 = 112$ in number. On the other hand, the units of $\mathrm{DiCo}(\mathbb{O})$ belonging to the second type of (1) are in bijective correspondence with the subsets of $M$ consisting of an even number of elements, hence are $\frac{2^8}{2} = 2^7 = 128$ in number. All in all, therefore, $\mathrm{DiCo}(\mathbb{O})$ has exactly $112 + 128 = 240$ units.

**4.14** The inclusions $\mathrm{Ga}(\mathbb{O}) \subseteq \mathrm{Kir}(\mathbb{O}) \subseteq \frac{1}{2}\,\mathrm{Ga}(\mathbb{O})$ follow immediately from the definition and show by Exc. 3.17 that $L := \mathrm{Kir}(\mathbb{O})$ is a lattice in $\mathbb{O}$.

Since $(u_r)_{0\le r\le 7}$ is an orthonormal basis of $\mathbb{O}$, we have $n_{\mathbb{O}}(\mathrm{Ga}(\mathbb{O}), v_i) \subseteq \mathbb{Z}$ for $1 \le i \le 4$, and a straightforward verification shows

$$n_{\mathbb{O}}(v_i) = 1, \quad n_{\mathbb{O}}(v_1, v_2) = 0, \quad n_{\mathbb{O}}(v_j, v_k) = 1 \tag{s1}$$

for $1 \le i, j, l \le 4$, $j \ne l$, $\{j, l\} \ne \{1, 2\}$. Combining this with the definition of $L$, we conclude $n_{\mathbb{O}}(L) \subseteq \mathbb{Z}$, so $L$ is a unital integral quadratic lattice in $\mathbb{O}$.

Next we consider the family

$$E_1 := (1_{\mathbb{O}}, u_1, u_2, u_3, v_1, v_2, v_3, v_4)$$

of elements in $L$. From $u_4 = 2v_1 - 1_{\mathbb{O}} - u_1 - u_2$, $u_5 = 2v_4 - 1_{\mathbb{O}} - u_2 - u_3$, $u_7 = -2v_3 + 1_{\mathbb{O}} + u_1 + u_3$, $u_6 = -2v_2 + u_3 + u_5 - u_7$ we deduce that $E_1$ spans $\mathbb{O}$ as a real vector space, hence is a basis, and that the additive map from $\mathbb{Z}^8$ to $L$ determined by $E_1$ is surjective, hence bijective. Thus $E_1$ is an $\mathbb{R}$-basis of $\mathbb{O}$ associated with $L$.

We now proceed to determine the discriminant of $L$ by computing the determinant of $Dn_{\mathbb{O}}(E_1)$. A straightforward verification using (s1) shows

$$Dn_{\mathbb{O}}(E_1) = \begin{pmatrix} 2 \cdot \mathbf{1}_4 & B \\ B^{\mathsf{T}} & D \end{pmatrix},$$

where

$$B = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$

Now we use (s1) in the solution to Exc. 4.10 and obtain

$$\begin{aligned} \det\left(Dn_{\mathbb{O}}(E_1)\right) &= \det(2 \cdot \mathbf{1}_4) \det\left(D - B^{\mathsf{T}}(\frac{1}{2} \cdot \mathbf{1}_4)B\right) = \det(2 \cdot D - B^t B) \\ &= \det\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 3 - 1 - 1 = 1. \end{aligned}$$

Thus $L$ is a unimodular integral quadratic lattice in $\mathbb{O}$.

It remains to show that $L$ is *not* a $\mathbb{Z}$-structure of $\mathbb{O}$, equivalently, that it is not closed under multiplication. To this end, we consider the product $v_1 v_3$. A short computation gives

$$v_1 v_3 = \frac{1}{2}(u_1 + u_2 + u_3 + u_5). \tag{s2}$$

Assuming $v_1v_3 \in \mathrm{Kir}(\mathbb{O})$, we would find integers $\alpha_r, \beta_i$, $0 \le r \le 3$, $1 \le i \le 4$, such that

$$v_1v_3 = \sum_{r=0}^{3} \alpha_r u_r + \sum_{i=1}^{4} \beta_i v_i. \tag{s3}$$

Comparing coefficients of $u_4$, we obtain $\beta_1 = 0$; comparing coefficients of $u_1$, we obtain $\frac{1}{2} = \alpha_1 + \frac{1}{2}\beta_3$, hence $\alpha_1 = \frac{1-\beta_3}{2}$, *and* $\beta_3$ *is odd.* Comparing coefficients of $u_2$, we obtain $\frac{1}{2} = \alpha_2 + \frac{1}{2}\beta_4$, hence $\alpha_2 = \frac{1-\beta_4}{2}$, *and* $\beta_4$ *is odd.* Comparing coefficients of $u_3$, we obtain $\frac{1}{2} = \alpha_3 + \frac{1}{2}(\beta_2 + \beta_3 + \beta_4)$, hence $\alpha_3 = -\frac{1}{2}(\beta_3 + \beta_4) + \frac{1-\beta_2}{2}$, *and* $\beta_2$ *is odd* since both $\beta_3, \beta_4$ are odd. And, finally, comparing coefficients of $u_5$, we obtain $\frac{1}{2} = \frac{1}{2}(\beta_2 + \beta_4)$, hence $\beta_2 + \beta_4 = 1$, which is a contradiction since $\beta_2, \beta_4$ are both odd. Thus $v_1v_3$ does not belong to $\mathrm{Kir}(\mathbb{O})$, as desired.

**4.15** The idea of the solution is to imitate our construction of the Dickson-Coxeter octonions with a different model of the Hamiltonian quaternions inside $\mathbb{O}$ and a different vector $\mathbf{q} \in \mathbb{O}$ in place of $\mathbf{p}$ such that the resulting $\mathbb{Z}$-structure agrees with $R$. In doing so, repeated use will be made of the multiplcation rules for Cartan-Shouten bases as depicted in Fig. 2a on page 12.

On a more formal level, these multiplication rules as described in (2.1.1) and (2.1.2) show that the linear bijection $\varphi\colon \mathbb{O} \to \mathbb{O}$ determined by

$$\varphi(1_{\mathbb{O}}) = 1_{\mathbb{O}}, \quad \varphi(u_r) = u_{r+2} \qquad (1 \le r \le 7, \text{ indices mod } 7)$$

is an automorphism of $\mathbb{O}$. With $\mathbb{H} \subseteq \mathbb{O}$ as given in (4.4.1) we therefore conclude that

$$B := \varphi(\mathbb{H}) = \mathbb{R}1_{\mathbb{O}} + \mathbb{R}u_3 + \mathbb{R}u_4 + \mathbb{R}u_6 \subseteq \mathbb{O}$$

is a model of the Hamiltonian quaternions matching $1_{\mathbb{H}} = 1_{\mathbb{O}}$, $\mathbf{i} = u_3$, $\mathbf{j} = u_4$, $\mathbf{k} = u_6$ and

$$\mathrm{Ga}(B) := \varphi(\,\mathrm{Ga}(\mathbb{H})) = \mathbb{Z}1_{\mathbb{O}} + \mathbb{Z}u_3 + \mathbb{Z}u_4 + \mathbb{Z}u_6.$$

Observing (4.4.3), we also put

$$\mathbf{q} := \varphi(\mathbf{p}) = \frac{1}{2}(1_{\mathbb{O}} + u_3 + u_4 + u_5) \tag{s1}$$

and deduce from Thm. 4.5 that

$$R' := \varphi(\,\mathrm{DiCo}(\mathbb{O})) = \mathrm{Ga}(B) + \mathrm{Ga}(B)\mathbf{q}$$

is a $\mathbb{Z}$-structure of $\mathbb{O}$ isomorphic to $\mathrm{DiCo}(\mathbb{O})$. It therefore remains to show $R' = R$.

We first note that $\mathrm{Ga}(\mathbb{O})$ is contained in $R$ (by definition) but also in $R'$ (by Thm. 4.5). Moreover, invoking (4.4.4)–(4.4.7), we deduce

$$\begin{aligned} u_3\mathbf{q} = \varphi(u_1\mathbf{p}) &= \frac{1}{2}(-1_{\mathbb{O}} + u_2 + u_3 + u_6), \\ u_4\mathbf{q} = \varphi(u_2\mathbf{p}) &= \frac{1}{2}(-1_{\mathbb{O}} + u_4 - u_6 + u_7), \\ u_6\mathbf{q} = \varphi(u_4\mathbf{p}) &= \frac{1}{2}(-u_1 - u_3 + u_4 + u_6). \end{aligned}$$

Now an inspection shows

$$\begin{aligned} v_1 + v_4 &\equiv \frac{1}{2}(1_{\mathbb{O}} + u_3 + u_4 + u_5) \equiv \mathbf{q} \bmod \mathrm{Ga}(\mathbb{O}), \\ v_2 + v_4 &\equiv \frac{1}{2}(1_{\mathbb{O}} + u_2 + u_3 + u_6) \equiv u_3\mathbf{q} \bmod \mathrm{Ga}(\mathbb{O}), \\ v_1 + v_2 + v_3 + v_4 &\equiv \frac{1}{2}(1_{\mathbb{O}} + u_4 + u_6 + u_7) \equiv u_4\mathbf{q} \bmod \mathrm{Ga}(\mathbb{O}), \\ v_1 + v_2 + v_4 &\equiv \frac{1}{2}(u_1 + u_3 + u_4 + u_6) \equiv u_6\mathbf{q} \bmod \mathrm{Ga}(\mathbb{O}). \end{aligned}$$

Since

$$\varphi(E') = (1_{\mathbb{O}}, u_3, u_4, u_6, \mathbf{q}, u_3\mathbf{q}, u_4\mathbf{q}, u_6\mathbf{q})$$

by (4.5.2) is a basis of $\mathbb{O}$ associated with $R'$, the preceding relations imply $R' \subseteq R$. But they also yield

$$\begin{aligned} u_4\mathbf{q} - u_6\mathbf{q} &\equiv v_3 \bmod \mathrm{Ga}(\mathbb{O}), \\ u_6\mathbf{q} - u_3\mathbf{q} &\equiv v_1 \bmod \mathrm{Ga}(\mathbb{O}), \\ u_6\mathbf{q} - \mathbf{q} &\equiv v_2 \bmod \mathrm{Ga}(\mathbb{O}), \\ \mathbf{q} + u_3\mathbf{q} - u_6\mathbf{q} &\equiv v_4 \bmod \mathrm{Ga}(\mathbb{O}) \end{aligned}$$

and hence imply $R \subseteq R'$. This shows $R = R'$ and the proof is complete.

**4.16** Let $(u_r)_{0\le r\le 7}$ be a Cartan-Schouten basis of $\mathbb{O}$. In the language of Exc. 4.13 we have

$$\mathbf{q} := \frac{1}{2}(1_{\mathbb{O}} + u_3 + u_4 + u_6) = \frac{1}{2}(-\varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_4 - \varepsilon_5 + \varepsilon_6 + \varepsilon_7 + \varepsilon_8),$$

whence part (d) of that exercise shows that $\mathbf{q}$ is invertible in $\mathrm{DiCo}(\mathbb{O})$. Since a straightforward verification yields $u_3u_4 = u_6$, $u_4u_6 = u_3$, $u_6u_3 = u_4$, we conclude from Thm. 4.2 that the assignments $1_{\mathbb{H}} \mapsto 1_{\mathbb{O}}$, $\mathbf{i} \mapsto u_3$, $\mathbf{j} \mapsto u_4$, $\mathbf{h} \mapsto \mathbf{q}$ determine an additive embedding $\mathrm{Hur}(\mathbb{H}) \hookrightarrow \mathrm{DiCo}(\mathbb{O})$ that preserves multiplication, hence is an embedding of $\mathbb{Z}$-algebras.

## Solutions for Section 5

**5.15** Computing the square of the matrix (5.4.2) in a straighforward manner yields (5a.1). Linearizing and dividing by 2 immediately yields (5a.2). Taking the trace of (5a.2) and applying (5.8.3), we obtain

$$\begin{aligned} T(x \bullet y) &= \sum (\alpha_i\beta_i + \frac{1}{2}n_{\mathbb{O}}(u_j, v_j) + \frac{1}{2}n_{\mathbb{O}}(u_l, v_l)) \\ &= \sum \alpha_i\beta_i + \frac{1}{2}(\sum n_{\mathbb{O}}(u_i, v_i) + \sum n_{\mathbb{O}}(u_i, v_i)), \end{aligned}$$

and (5a.3) follows. Writing

$$z = \sum (\gamma_i e_{ii} + w_i[jl]) \qquad (\gamma_i \in \mathbb{R}, \quad w_i \in \mathbb{O}, \quad 1 \le i \le 3),$$

we first note by (1.6.13) and Exc. 1.18 (b) that, for all $u, v, w \in \mathbb{O}$, the expression

$$n_{\mathbb{O}}(\overline{uv}, w) = t_{\mathbb{O}}(uvw) \text{ is invariant under cyclic permutations of the variables.} \tag{s1}$$

Combining (5a.2) with (5a.3), we therefore obtain

$$\begin{aligned} T((x \bullet y) \bullet z) = &\sum \Big((\alpha_i\beta_i + \frac{1}{2}n_{\mathbb{O}}(u_j, v_j) + \frac{1}{2}n_{\mathbb{O}}(u_l, v_l))\gamma_i \\ &+ \frac{1}{2}n_{\mathbb{O}}((\alpha_j + \alpha_l)v_i + (\beta_j + \beta_l)u_i + \overline{u_jv_l + v_ju_l}, w_i)\Big) \\ = &\sum \Big(\alpha_i\beta_i\gamma_i + \frac{1}{2}(\gamma_j + \gamma_l)n_{\mathbb{O}}(u_i, v_i) + \frac{1}{2}(\alpha_j + \alpha_l)n_{\mathbb{O}}(v_i, w_i) \\ &+ \frac{1}{2}(\beta_j + \beta_l)n_{\mathbb{O}}(w_i, u_i) + \frac{1}{2}\big(t_{\mathbb{O}}(u_iv_jw_l) + t_{\mathbb{O}}(w_iv_ju_l)\big)\Big). \end{aligned}$$

This expression obviously being symmetric in $x, z$, we end up with (5.9.4).

We now turn to (5.9.5). Combining (5.8.3) with (5.9.3) we deduce

$$\begin{aligned} T(x)T(y) - T(x \bullet y) &= (\sum \alpha_i)(\sum \beta_i) - \sum (\alpha_i\beta_i + n_{\mathbb{O}}(u_i, v_i)) \\ &= \sum (\alpha_i\beta_j + \beta_i\alpha_j - n_{\mathbb{O}}(u_i, v_i)), \end{aligned}$$

which by (5.8.7) agrees with $S(x, y)$. Similarly, by (5.9.1), (5.8.3), 5.8.6) and

(5.8.4) we obtain

$$\begin{aligned} x^2 - T(x)x + S(x)\mathbf{1}_3 &= \sum \Big( (\alpha_i^2 + n_{\mathbb{O}}(u_j) + n_{\mathbb{O}}(u_l))e_{ii} + ((\alpha_j + \alpha_l)u_i + \overline{u_j u_l})[jl] \Big) \\ &\quad - (\sum \alpha_i) \sum (\alpha_i e_{ii} + u_i[jl]) + \sum (\alpha_j\alpha_l - n_{\mathbb{O}}(u_i))(\sum e_{ii}) \\ &= \sum \Big( (\alpha_i^2 + n_{\mathbb{O}}(u_j) + n_{\mathbb{O}}(u_l) - \alpha_i^2 - \alpha_i\alpha_j - \alpha_l\alpha_i \\ &\quad + \alpha_i\alpha_j + \alpha_j\alpha_l + \alpha_l\alpha_i - n_{\mathbb{O}}(u_i) - n_{\mathbb{O}}(u_j) - n_{\mathbb{O}}(u_l))e_{ii} \\ &\quad + ((\alpha_j + \alpha_l)u_i + \overline{u_j u_l} - \alpha_i u_i - \alpha_j u_i - \alpha_l u_i)[jl] \Big) \\ &= \sum \Big( (\alpha_j\alpha_l - n_{\mathbb{O}}(u_i))e_{ii} + (-\alpha_i u_i + \overline{u_j u_l})[jl] \Big) = x^\sharp, \end{aligned}$$

which completes the proof of (5.9.6).

Differentiating (5.8.2) at $x$ in the direction $y$ and observing (s1), we obtain

$$\begin{aligned} DN(x)(y) &= \beta_1\alpha_2\alpha_3 + \alpha_1\beta_2\alpha_3 + \alpha_1\alpha_2\beta_3 - \sum (\beta_i n_{\mathbb{O}}(u_i) + \alpha_i n_{\mathbb{O}}(u_i, v_i)) \\ &\quad + t_{\mathbb{O}}(v_1u_2u_3) + t_{\mathbb{O}}(u_1v_2u_3) + t_{\mathbb{O}}(u_1u_2v_3) \\ &= \sum (\alpha_j\alpha_l\beta_i - n_{\mathbb{O}}(u_i)\beta_i - \alpha_i n_{\mathbb{O}}(u_i, v_i) + t_{\mathbb{O}}(u_j u_l v_i)), \end{aligned}$$

while combining (5.9.3) with (5.8.4) and (s1) yields

$$\begin{aligned} T(x^\sharp \bullet y) &= \sum \Big( (\alpha_j\alpha_l - n_{\mathbb{O}}(u_i))\beta_i + n_{\mathbb{O}}(-\alpha_i u_i + \overline{u_j u_l}, v_i) \Big) \\ &= \sum (\alpha_j\alpha_l\beta_i - n_{\mathbb{O}}(u_i)\beta_i - \alpha_i n_{\mathbb{O}}(u_i, v_i + t_{\mathbb{O}}(u_j u_l v_i)), \end{aligned}$$

which proves the first equation of (5.9.7), while the second one follows from (5.9.6).

In order to prove (5a.8), we apply (5a.2) and (5.8.4) to compute

$$\begin{aligned} x \bullet x^\sharp = \sum \Big( &(\alpha_i[\alpha_j\alpha_l - n_{\mathbb{O}}(u_i)] + \frac{1}{2}n_{\mathbb{O}}(u_j, -\alpha_j u_j + \overline{u_l u_i}) + \frac{1}{2}n_{\mathbb{O}}(u_l, -\alpha_l u_l + \overline{u_i u_j}))e_{ii} \\ &+ \frac{1}{2}((\alpha_j + \alpha_l)[-\alpha_i u_i + \overline{u_j u_l}] + [\alpha_l\alpha_i - n_{\mathbb{O}}(u_j) + \alpha_i\alpha_j - n_{\mathbb{O}}(u_l)]u_i \\ &+ \overline{u_j[-\alpha_l u_l + \overline{u_i u_j}] + [-\alpha_j u_j + \overline{u_l u_i}]u_l})[jl] \Big). \end{aligned}$$

Since the conjugation of $\mathbb{O}$ is an involution and $(u_iu_j)\bar{u}_j = n_{\mathbb{O}}(u_j)u_i$, $\bar{u}_l(u_lu_i) = n_{\mathbb{O}}(u_l)u_i$ by Exc. 1.18 (c), we conclude

$$x \bullet x^\sharp = \sum (\alpha_1\alpha_2\alpha_3 - \sum_{r=1}^{3} \alpha_r n_{\mathbb{O}}(u_r) + t_{\mathbb{O}}(u_1u_2u_3))e_{ii} = N(x)\mathbf{1}_3,$$

and plugging in (5a.6) gives (5a.8).

Finally, differentiating $x^3 = (x \bullet x) \bullet x$ at $x$ in the direction $y$, we find $(y \bullet x) \bullet x + (x \bullet y) \bullet x + (x \bullet x) \bullet y = 2x \bullet (x \bullet y) + x^2 \bullet y$. Performing the same procedure on the right-hand side of (5a.8), we therefore get (5a.9).

**5.16** We have $\mathrm{Her}_1(\mathbb{O}) \cong \mathbb{R}^+$, while $\mathrm{Her}_2(\mathbb{O})$ sits in the euclidean Albert algebra via

$$\mathrm{Her}_2(\mathbb{O}) \cong \left\{ \begin{pmatrix} \alpha_1 & u_3 & 0 \\ \bar{u}_3 & \alpha_2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid \alpha_1, \alpha_2 \in \mathbb{R},\ u_3 \in \mathbb{O} \right\}$$

as a non-unital subalgebra. By Thm. 5.10, therefore, $\mathrm{Her}_n(\mathbb{O})$ is a Jordan algebra for $1 \leq n \leq 3$. It remains to show that it is *not* a Jordan algebra for $n \geq 4$. We begin by differentiating the Jordan identity $u(u^2v) = u^2(uv)$ at $u$ in the direction $w$ and obtain

$$w(u^2v) + 2u((uw)v) = 2(uw)(uv) + u^2(wv).$$

Differentiating at $u$ again, this time in the direction $x$, changing notation and rearranging terms, we end up with the fully linearized Jordan identity, which therefore holds in arbitrary real Jordan algebras.

Now consider the commutative real algebra $J := \mathrm{Her}_n(\mathbb{O})$ for some integer $n \geq 4$. For $1 \leq i, j, l, m \leq n$ satisfying $i \neq j$, $l \neq m$ and $u, v \in \mathbb{O}$, we will make use of the obvious relations

$$\begin{aligned} e_{ii} \bullet u[lm] &= \frac{1}{2}(\delta_{il} + \delta_{im})u[lm] = u[lm] \bullet e_{ii}, \\ u[ij] &= \bar{u}[ji], \\ u[ij] \bullet v[jl] &= \frac{1}{2}(uv)[il] && (j \neq l \neq i), \\ u[ij] \bullet v[lm] &= 0 && (\{i,j\} \cap \{l,m\} = \emptyset). \end{aligned}$$

Assuming now $J$ is a Jordan algebra, we combine the preceding relations with the fully linearized Jordan identity and conclude

$$\begin{aligned} \frac{1}{4}((uv)w)[14] &= (u[12] \bullet v[23]) \bullet ((e_{33} + e_{44}) \bullet w[34]) \\ &= -(v[23] \bullet (e_{33} + e_{44})) \bullet (u[12] \bullet w[34]) - ((e_{33} + e_{44}) \bullet u[12]) \bullet (v[23] \bullet w[34]) \\ &\quad + u[12] \bullet \Big((v[23] \bullet (e_{33} + e_{44})) \bullet w[34]\Big) + v[23] \bullet \Big(((e_{33} + e_{44}) \bullet u[12]) \bullet w[34]\Big) \\ &\quad + (e_{33} + e_{44}) \bullet ((u[12] \bullet v[23]) \bullet w[34]) \\ &= \frac{1}{8}(u(vw))[14] + \frac{1}{8}((uv)w)[14]. \end{aligned}$$

Thus we obtain the contradiction that $\mathbb{O}$ is associative. Hence $J$ cannot be a Jordan algebra.

**5.17** (a) By hypothesis, $\deg(\mu_x) = \dim_{\mathbb{R}}(\mathbb{R}[x]) = 3$. Hence $\mu := \det(\mathbf{t}\mathbf{1}_{\mathbb{R}[x]} - L_x^0)$ is monic of degree 3 as well. Moreover, $\mu(x) = \mu(L_x^0)\mathbf{1}_3 = 0$, which proves the first assertion. The remaining ones now follow from (5.13.1).

(b) Using the polynomial map

$$f\colon J \longrightarrow \bigwedge^3(J), \quad x \longmapsto \mathbf{1}_3 \wedge x \wedge x^2,$$

we consider the set $X$ of all septuples

$$(\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2, x) \in \mathbb{R}^6 \times J \tag{s1}$$

such that, setting $u := \sum_{r=0}^{2} \alpha_r x^r$, $v := \sum_{r=0}^{2} \beta_r x^r$, the quantities $f(x), f(u), f(v), f(u \bullet v)$ are all different from zero. Note that this condition is equivalent to $\mathbb{R}[x] = \mathbb{R}[u] = \mathbb{R}[v] = \mathbb{R}[u \bullet v]$ having dimension 3. We claim that $X \subseteq \mathbb{R}^6 \times J$, which is obviously Zariski-open, is also not empty, hence Zariski-dense. Indeed, let $\xi_i, \eta_i, \zeta_i \in \mathbb{R}$ for $i = 1, 2, 3$ such that the sets

$$\{\xi_1, \xi_2, \xi_3\}, \quad \{\eta_1, \eta_2, \eta_3\}, \quad \{\zeta_1, \zeta_2, \zeta_3\}, \quad \{\eta_1\zeta_1, \eta_2\zeta_2, \eta_3\zeta_3\}$$

all have cardinality 3. Setting $x := \sum \xi_i e_{ii}$, $u := \sum \eta_i e_{ii}$, $v := \sum \zeta_i e_{ii}$, we conclude $\mathbb{R}[x] = \mathbb{R}[u] = \mathbb{R}[v] = \mathbb{R}[u \bullet v] = \sum \mathbb{R} e_{ii}$, allowing us to write $u = \sum_{r=0}^{2} \alpha_r x^r$, $v = \sum_{r=0}^{2} \beta_r x^r$ for some $\alpha_r, \beta_r \in \mathbb{R}$, $0 \le r \le 2$, and it follows that the quantity (s1) belongs to $X$.

Hence it suffices to prove the first claim under the additional hypothesis that $\mathbb{R}[x] = \mathbb{R}[u] = \mathbb{R}[v] = \mathbb{R}[u \bullet v]$ is three-dimensional. But then, since $\mathbb{R}[x]$ is commutative associative, (a) gives

$$N(u \bullet v) = \det(L^0_{u \bullet v}) = \det(L^0_u L^0_v) = \det(L^0_u)\det(L^0_v) = N(u)N(v).$$

It remains to show that the equation $N(x \bullet y) = N(x)N(y)$ does not hold for all $x, y \in J$. To this end, put

$$x := \sum \alpha_i e_{ii}, \quad y := \sum v_i [jl] \qquad (\alpha_i \in \mathbb{R},\ v_i \in \mathbb{D},\ 1 \le i \le 3).$$

Then (5.8.2) and (5a.2) imply

$$\begin{aligned} N(x) &= \alpha_1\alpha_2\alpha_3, \\ N(y) &= t_{\mathbb{D}}(v_1 v_2 v_3), \\ x \bullet y &= \frac{1}{2} \sum (\alpha_j + \alpha_l) v_i [jl] \end{aligned}$$

hence

$$N(x \bullet y) = \frac{1}{8}(\alpha_2 + \alpha_3)(\alpha_3 + \alpha_1)(\alpha_1 + \alpha_2) t_{\mathbb{D}}(v_1 v_2 v_3),$$

which in general will be distinct from $N(x)N(y) = \alpha_1\alpha_2\alpha_3 t_{\mathbb{D}}(v_1 v_2 v_3)$.

(c) If $x$ is invertible in $J$, then, by definition, it is so in $\mathbb{R}[x]$, and $x^{-1} \in \mathbb{R}[x]$ satisfies $x \bullet x^{-1} = \mathbf{1}_3$. Now (b) implies $N(x)N(x^{-1}) = 1$, hence $N(x) \neq 0$ as well as $N(x^{-1}) = N(x)^{-1}$. Conversely, let $N(x) \neq 0$. Combining (5a.6) with (5a.8),

we obtain $x^\sharp \in \mathbb{R}[x]$ and $x \bullet x^\sharp = N(x)\mathbf{1}_3$. But this implies $x \bullet y = \mathbf{1}_3$ with $y := N(x)^{-1}x^\sharp \in \mathbb{R}[x]$, so $x$ is invertible in $J$, and the inverse has the desired form.

(d) By Zariski density and (c), it suffices to prove both identities for $x$ invertible. Taking norms on both sides of the displayed equation in (c), we obtain $N(x)^{-1} = N(x^{-1}) = N(x)^{-3}N(x^\sharp)$, hence $N(x^\sharp) = N(x)^2$. In particular, $x^\sharp$ is invertible with inverse $x^{\sharp-1} = N(x^\sharp)^{-1}x^{\sharp\sharp} = N(x)^{-2}x^{\sharp\sharp}$. Hence

$$x = (x^{-1})^{-1} = (N(x)^{-1}x^\sharp)^{-1} = N(x)x^{\sharp-1} = N(x)^{-1}x^{\sharp\sharp},$$

and also the adjoint identity follows.

**5.18** First let $\varphi$ be an automorphism of $J$. Then $\varphi$ fixes $\mathbf{1}_3$ and in order to prove $N(\varphi(x)) = N(x)$ for $x \in J$, we may assume, by Zariski densitiy, that $\mathbf{1}_3 \wedge x \wedge x^2 \neq 0$ in $\bigwedge^3(J)$. Since $\varphi$ preserves powers, (5a.8) implies

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

and since $\mathbf{1}_3, \varphi(x), \varphi(x)^2$ are linearly independent, we conclude $N(\varphi(x)) = N(x)$, as claimed.

Conversely, suppose $\varphi$ preserves $\mathbf{1}_3$ and $N$. Then $\varphi$ also preserves the directional derivative of $N$ at $x$ in the direction $y$, i.e., in view (5a.7) we have

$$T(\varphi(x)^\sharp \bullet \varphi(y) = DN(\varphi(x))(\varphi(y)) = DN(x)(y) = T(x^\sharp \bullet y). \tag{s1}$$

Setting $x = \mathbf{1}_3$ implies $T \circ \varphi = T$, while setting $y = \mathbf{1}_3$ implies $S \circ \varphi = S$. Taking traces in (5a.6), on the other hand, we conclude $T(x^2) = T(x)^2 - 2S(x)$. Replacing $x$ by $\varphi(x)$ and applying what we have just proved yields $T(\varphi(x)^2) = T(x^2)$, hence $T(\varphi(x) \bullet \varphi(y)) = T(x \bullet y)$ after linearization. Substituting $x^\sharp$ for $x$ and combining with (s1), we deduce $T(\varphi(x)^\sharp \bullet \varphi(y)) = T(x^\sharp \bullet y) = T(\varphi(x^\sharp) \bullet \varphi(y))$. But (5a.3) shows that the bilinear form $T(x \bullet y)$ is positive definite, hence nondegenerate, and we conclude that $\varphi$ preserves adjoints. By (5a.6), therefore, $\varphi$ preserves squares, and since the algebra $J$ is commutative, it must be an isomorphism.

As to the second part, the linear map $\varphi$ is clearly bijective and preserves the unit. Assume that $\varphi$ is an automorphism of $J$. Then (5a.1) yields

$$e_{22} + e_{33} = \varphi(1_{\mathbb{D}}[23]^2) = \varphi(1_{\mathbb{D}}[23])^2 = u^{-1}[23]^2 = n_{\mathbb{D}}(u)^{-1}(e_{22} + e_{33}),$$

and we conclude $n_{\mathbb{D}}(u) = 1$. Conversely, let this be so. By the first part of the

problem, it suffices to show that $\varphi$ preserves the norm. To this end, we compute

$$\begin{aligned} N(\varphi(x)) &= N\Big(\sum \alpha_i e_{ii} + (u^{-1}u_1)[23] + (u_2u^{-1})[31] + (uu_3u)[12]\Big) \\ &= \alpha_1\alpha_2\alpha_3 - \alpha_1 n_{\mathbb{D}}(u^{-1}u_1) - \alpha_2 n_{\mathbb{D}}(u_2u^{-1}) - \alpha_3 n_{\mathbb{D}}(uu_3u) + \\ &\quad t_{\mathbb{D}}((u^{-1}u_1)(u_2u^{-1})(uu_3u)). \end{aligned}$$

But $u$ has norm 1, $n_{\mathbb{D}}$ permits composition, and the Moufang identities (Exc. 1.19) combined with Exc. 1.18 (b), (c) give

$$\begin{aligned} t_{\mathbb{D}}((u^{-1}u_1)(u_2u^{-1})(uu_3u)) &= t_{\mathbb{D}}\Big((u^{-1}(u_1u_2)u^{-1})(uu_3u)\Big) \\ &= t_{\mathbb{D}}\Big(u^{-1}((u_1u_2)[u^{-1}(uu_3u)])\Big) \\ &= t_{\mathbb{D}}\Big(u^{-1}((u_1u_2)(u_3u))\Big) = t_{\mathbb{D}}\Big((u^{-1}(u_1u_2))(u_3u)\Big) \\ &= t_{\mathbb{D}}\Big(([u^{-1}(u_1u_2)]u_3)u\Big) = t_{\mathbb{D}}\Big(u([u^{-1}(u_1u_2)]u_3)\Big) \\ &= t_{\mathbb{D}}\Big((u[\bar{u}(u_1u_2)])u_3\Big) = t_{\mathbb{D}}(u_1u_2u_3). \end{aligned}$$

Hence $N(\varphi(x)) = N(x)$, and the problem is solved.

## Solutions for Section 6

**6.12** (a) This follows by a straightforward computation.

(b) Linearizing (5a.6) and applying (5a.5), we obtain

$$x \times y = 2x \bullet y - T(x)y - T(y)x + T(x)T(y)\mathbf{1}_3 - T(x \bullet y)\mathbf{1}_3,$$

and combining this with (5a.6), (5a.7), (5a.9) yields

$$\begin{aligned} x^\sharp \times y &= 2x^\sharp \bullet y - T(x^\sharp)y - T(y)x^\sharp + T(x^\sharp)T(y)\mathbf{1}_3 - T(x^\sharp \bullet y)\mathbf{1}_3 \\ &= 2x^2 \bullet y - 2T(x)x \bullet y + 2S(x)y - S(x)y - T(y)x^\sharp + S(x)T(y)\mathbf{1}_3 - DN(x)(y)\mathbf{1}_3 \\ &= 2x^2 \bullet y - 2T(x)x \bullet y + S(x)y - T(y)x^2 + T(x)T(y)x - S(x)T(y)\mathbf{1}_3 \\ &\quad + S(x)T(y)\mathbf{1}_3 - x^2 \bullet y + 2T(x)x \bullet y + T(y)x^2 - S(x)y - S(x,y)x - 2x \bullet (x \bullet y) \\ &= -U_x y + T(x \bullet y)x, \end{aligned}$$

as claimed.

**6.13** Let $A, B$ be commutative real algebras and $\varphi\colon A \to B$ a linear map. If $\varphi$ is a homomorphism, then it clearly preserves squares. Conversely, let this be so. Then $\varphi(x^2) = \varphi(x)^2$ for all $x \in A$, and linearizing gives

$$\varphi(xy) = \frac{1}{2}\Big(\varphi((x+y)^2 - x^2 - y^2)\Big) = \frac{1}{2}\Big((\varphi(x)+\varphi(y))^2 - \varphi(x)^2 - \varphi(y)^2\Big) = \varphi(x)\varphi(y).$$

Thus $\varphi$ is a homomorphism.

Now define the *left multiplication* of $\mathbb{O}$ as the linear map $L\colon \mathbb{O}^+ \to \mathrm{End}_{\mathbb{R}}(\mathbb{O})^+$ sending $x \in \mathbb{O}^+$ to $L_x\colon \mathbb{O} \to \mathbb{O}$, $y \mapsto xy$. Since $L_{x^2} = L_x^2$ for all $x \in \mathbb{O}$ by 1.7, $L$ preserves squares and hence is a homomorphism of commutative algebras. It is also injective since $L_x = 0$ implies $x = L_x 1_{\mathbb{O}} = 0$. Thus $L$ maps $\mathbb{O}^+$ isomorphically onto a subalgebra of $\mathrm{End}_{\mathbb{R}}(\mathbb{O})^+$, and we conclude from 5.7 (a) that $\mathbb{O}^+$ is a special Jordan algebra. As in Exc. 6.12 (a), the verification of the formula for the $U$-operator is straightforward: for $x, y \in \mathbb{O}$ we obtain, using alternativity 1.7,

$$\begin{aligned} U_x y &= 2x \bullet (x \bullet y) - x^2 \bullet y = \frac{1}{2}\big(x(xy + yx) + (xy + yx)x - x^2 y - yx^2\big) \\ &= \frac{1}{2}\big(x(xy) - x^2 y + x(yx) + (xy)x + (yx)x - yx^2\big) = xyx, \end{aligned}$$

as claimed. Finally, the Jordan algebra $\mathbb{O}^+$ is *not* euclidean since, given a Cartan-Shouten basis $(u_i)_{0 \le i \le 7}$ of $\mathbb{O}$, we have $1_{\mathbb{O}}^2 + u_i^2 = 0$ for $i = 1, \dots, 7$.

**6.14** For $0 \le i \le n$ we have $e_0 \bullet e_i = \frac{1}{2}(1_A e_i + e_i 1_A) = e_i$. Now let $1 \le i, j \le n$, $i \ne j$. By orthnormality, $e_i$ has trace 0 and norm 1, which by (1.6.10) implies $e_i \bullet e_i = e_i^2 = -1_A = -e_0$, while (1.6.12) implies

$$e_i \bullet e_j = \frac{1}{2} e_i \circ e_j = \frac{1}{2}\big(t_{\mathbb{D}}(e_i)e_j + t_{\mathbb{D}}(e_j)e_i - n_{\mathbb{D}}(e_i, e_j)\big) = 0.$$

Thus $\Lambda$ is closed under the multiplication of $\mathbb{D}^+$ and hence is a linear $\mathbb{Z}$-structure of that algebra. But note that, in general, $\Lambda$ will not be closed under the multiplication of $\mathbb{D}$. Finally, by Ex. 3.16 and Exc. 2.8, the Gaussian integers of $\mathbb{D}$ are the $\mathbb{Z}$-linear span of some orthonormal basis of $\mathbb{D}$, yielding the final assertion of the problem.

**6.15** Exc. 5.17 (b) implies $N(c) = N(c^2) = N(c)^2$, hence $N(c) \in \{0, 1\}$. If $N(c) = 1$, then $c$ is invertible (Exc. 5.17 (c)), and the relations $\mathbf{1}_3 - c \in \mathbb{R}[c]$, $c(\mathbf{1}_3 - c) = 0$ yield $c = \mathbf{1}_3$, a contradiction. Thus $N(c) = 0$. Using this and (5a.8), we deduce $c = c^3 = (T(c) - S(c))c$, hence

$$S(c) = T(c) - 1. \tag{s1}$$

Now (5a.6) yields $c^\sharp = (1 - T(c))c + S(c)\mathbf{1}_3 = S(c)(\mathbf{1}_3 - c)$, hence $S(c) = T(c^\sharp) = S(c)(3 - T(c)) = -S(c)^2 + 2S(c)$. Thus $S(c)^2 = S(c)$, forcing $S(c) \in \{0, 1\}$, and (s1) implies the assertion.

**6.16** Setting

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

with $\alpha_i, \beta_i \in \mathbb{R}$, $u_i, v_i \in \mathbb{D}$, $1 \le i \le 3$ and applying (5.8.2), (5.8.3), (5a.3) and

the fact that the expression $t_{\mathbb{O}}(uvw) = n_{\mathbb{O}}(\overline{uv}, w)$ remains invariant under cyclic permutations of the variables, we compute

$$\begin{aligned}
N(x+y) &= (\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3) - \sum(\alpha_i+\beta_i)n_{\mathbb{O}}(u_i+v_i) \\
&\quad + t_{\mathbb{O}}((u_1+v_1)(u_2+v_2)(u_3+v_3)) \\
&= \alpha_1\alpha_2\alpha_3 + \sum \alpha_j\alpha_l\beta_i + \sum \alpha_i\beta_j\beta_l + \beta_1\beta_2\beta_3 \\
&\quad - \sum (\alpha_i n_{\mathbb{O}}(u_i) + \alpha_i n_{\mathbb{O}}(u_i, v_i) + \alpha_i n_{\mathbb{O}}(v_i) + \beta_i n_{\mathbb{O}}(u_i) + \beta_i n_{\mathbb{O}}(u_i, v_i) \\
&\quad + \beta_i n_{\mathbb{O}}(v_i)) + t_{\mathbb{O}}(u_1u_2u_3) + \sum t_{\mathbb{O}}(u_ju_lv_i) + \sum t_{\mathbb{O}}(u_iv_jv_l) + t_{\mathbb{O}}(v_1v_2v_3) \\
&= (\alpha_1\alpha_2\alpha_3 - \sum \alpha_i n_{\mathbb{O}}(u_i) + t_{\mathbb{O}}(u_1u_2u_3)) \\
&\quad + \sum \Big((\alpha_j\alpha_l - n_{\mathbb{O}}(u_i))\beta_i + n_{\mathbb{O}}(-\alpha_i u_i + \overline{u_ju_l}, v_i)\Big) \\
&\quad + \sum \Big(\alpha_i(\beta_j\beta_l - n_{\mathbb{O}}(v_i)) + n_{\mathbb{O}}(u_i, -\beta_i v_i + \overline{v_jv_l})\Big) \\
&\quad + (\beta_1\beta_2\beta_3 - \sum \beta_i n_{\mathbb{O}}(v_i) + t_{\mathbb{O}}(v_1v_2v_3)) \\
&= N(x) + T(x^\sharp \bullet y) + T(x \bullet y^\sharp) + N(y),
\end{aligned}$$

as desired.

# Solutions for Chapter II

## Solutions for Section 7

**7.12** For $x \in A$ and $\varepsilon = \pm$, we put

$$M_\varepsilon(x) := \{y \in A \mid f(xy) = \varepsilon f(x)f(y)\},$$

which is a submodule of $A$. By hypothesis we have $A = M_+(x) \cup M_-(x)$, so some $\varepsilon = \pm$ has $M_\varepsilon(x) = A$. Now put

$$N_\varepsilon := \{x \in A \mid \forall y \in A \,:\, f(xy) = \varepsilon f(x)f(y)\} = \{x \in A \mid M_\varepsilon(x) = A\},$$

which is again a submodule of $A$, and from what we have just proved, we obtain $A = N_+ \cup N_-$. This gives $N_\varepsilon = A$ for some $\varepsilon = \pm$, and if $\varepsilon = +$ (resp. $\varepsilon = -$), $f$ (resp. $-f$) is a homomorphism from $A$ to $B$.

**7.13** For any subset $X \subseteq A$ and any homomorphism $\varphi\colon A \to B$ of $k$-algebras, one makes the following observations by straightforward induction:

(a) $\varphi(\mathrm{Mon}_m(X)) = \mathrm{Mon}_m(\varphi(X))$ for all integers $m > 0$.
(b) $\mathrm{Mon}_m(Y) \subseteq \mathrm{Mon}_{mn}(X)$ for all $Y \subseteq \mathrm{Mon}_n(X)$ and all integers $m, n > 0$.

If $x \in A$ is nilpotent, then (a) implies that $\varphi(x) \in B$ is nilpotent. Hence if $A$ is nil, so are $I$ and $A' := A/I$. Conversely, suppose $I$ and $A'$ are nil. Writing $\pi\colon A \to A'$ for the canonical epimorphism, any $x \in A$ makes $\pi(x) \in A'$ nilpotent, so by (a), $\mathrm{Mon}_n(\{x\})$ meets $I$ for some integer $n > 0$. But since $I$ is nil, we conclude that some $y \in \mathrm{Mon}_n(\{x\})$ is nilpotent, leading to a positive integer $m$ such that $0 \in \mathrm{Mon}_{mn}(\{x\})$ by (b). Thus $x$ is nilpotent, forcing $A$ to be a nil algebra. Now write $\mathfrak{n} := \mathrm{Nil}(A)$ for the sum of all nil ideals in $A$. Given $x \in \mathfrak{n}$, there are finitely many nil ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_r \subseteq A$ such that $x \in \mathfrak{n}_1 + \cdots + \mathfrak{n}_r$. Thus we only have to show that the sum of finitely many nil ideals in $A$ is nil. Arguing by induction, we are actually reduced to the case $r = 2$. But then the isomorphism

$(\mathfrak{n}_1+\mathfrak{n}_2)/\mathfrak{n}_1 \cong \mathfrak{n}_2/(\mathfrak{n}_1\cap\mathfrak{n}_2)$ combines with what we have proved earlier to yield the assertion. To establish the final statement of the problem, we require the following standard result.

**Lemma.** *Every finitely generated nil ideal $I \subseteq k$ is nilpotent, i.e., there exists a positive integer $n$ such that $I^n = \{0\}$.*

*Proof* Assume $\alpha_1, \dots, \alpha_m \in I$ generate $I$ as an ideal and let $p \in \mathbb{Z}$, $p > 0$, satisfy $\alpha_i^p = 0$ for all $i = 1, \dots, m$. For any positive integer $n$, the ideal $I^n \subseteq k$ is generated by the expressions $\alpha_{i_1} \cdots \alpha_{i_n}$, where $1 \le i_1 \le \cdots \le i_n \le m$. If for all $i = 1, \dots, m$,

$$q_i := |\{j \in \mathbb{Z} | 1 \le j \le n,\ i_j = i\}| \le p-1,$$

then $n = \sum_{i=1}^m q_i \le m(p-1)$. Thus for $n > m(p-1)$, some $i = 1, \dots, m$ has $q_i \ge p$. But this implies first $\alpha_{i_1} \cdots \alpha_{i_n} = 0$ and then $I^n = \{0\}$. □

Since $\mathrm{Nil}(k)A \subseteq A$ is an ideal, it suffices to show that it consists entirely of nilpotent elements, so let $x \in \mathrm{Nil}(k)A$. Then $x \in IA$ for some finitely generated nil ideal $I \subseteq A$, and the lemma implies $x^n \in I^n A = \{0\}$ for some positive integer $n$. The assertion follows.

**7.14** (a) Since $x^n$ is a linear combination of powers $x^i$, $d \le i < n$, the $k$-module $k_d[x]$ is finitely generated. Moreover, right multiplication by $x$ in the power associative algebra $A$ gives a linear map $\varphi\colon k_d[x] \to k_d[x]$ whose image is $k_{d+1}[x]$. But $k_{d+1}[x] = k_d[x]$ since $\alpha_d \in k^\times$. Therefore, $\varphi$ is surjective, hence bijective (by Prop. 7.11), and so is $\varphi^d$. This proves existence and uniqueness of $c \in k_d[x]$ satisfying $cx^d = x^d$, and the relation $c^2x^d = c(cx^d) = cx^d$ shows that $c$ is an idempotent.

(b) Let $x \in A$ be a pre-image of $c'$ under $\varphi$. Then $x^2 - x$ is nilpotent, so some integer $n > 0$ has $0 = (x^2-x)^n = x^{2n} - \cdots + (-1)^n x^n$. Now (a) yields an idempotent $c \in k_n[x]$ satisfying $cx^n = x^n$. Writing $\bar{u} := \varphi(u)$ for $u \in A$, we conclude $\bar{c}c' = \bar{c}c'^n = \bar{c}\bar{x}^n = \bar{x}^n = c'$. On the other hand, $c = \sum_{i\ge n} \alpha_i x^i$ for some scalars $\alpha_i \in k$, $i \ge n$, so with $\alpha := \sum_{i\ge n}\alpha_i$ we obtain $\bar{c} = \bar{\alpha}c' = \bar{\alpha}c'^2 = \bar{c}c' = c'$.

## Solutions for Section 8

**8.10** If $I_j$ are ideals in $A_j$ for $1 \le j \le n$, then $I := I_1 \times \cdots \times I_n$ is an ideal in $A$ since $AI + IA = \prod_j (A_j I_j + I_j A_j) \subseteq \prod_j I_j = I$. Conversely, let $I$ be an ideal in $A$ and $e_j$ the identity element of $A_j$ for $1 \le j \le n$. If we identify $A_j \subseteq A$ through the $j$-th factor, then $I_j = e_j I = I e_j$ is clearly an ideal in $A_j$ such that $I = \prod_j I_j$.

The assertion *fails* without the assumption that $A$ be unital: suppose the $A_j$ have trivial multiplication. Then so has $A$, and *any* decomposition of $A$ into the direct product of $n$ submodules not related to the $A_j$ in any way is a decomposition into a direct product of ideals.

To complete the solution, let us assume that the $A_j$, $1 \le j \le n$, are simple $k$-algebras. By the first part of the exercise, the ideals of $A$ have the form $\prod_{j=1}^{n} I_j$, where either $I_j = A_j$ or $I_j = \{0\}$, for all $j = 1, \dots, n$. Hence the $A_j$, $1 \le j \le n$, are precisely the minimal ideals of $A$. This description being independent of the decomposition chosen, the assertion follows.

**8.11** (a) The polynomials $\mu_1, \dots, \mu_r$ have greatest common divisor 1. Hence $f_1, \dots, f_r \in F[\mathbf{t}]$ with the desired properties exist. We therefore conclude $\sum_{i=1}^{r} c_i = 1_A$. Moreover, for $1 \le i, j \le r$, $i \ne j$, the polynomial $\mu_i \mu_j$ is a multiple of $\mu_x$, hence kills $x$. This proves $c_i c_j = 0$ and then $c_i = c_i 1_A = \sum_{l=1}^{r} c_i c_l = c_i^2$. Thus $(c_1, \dots, c_r)$ is a complete orthogonal system of idempotents in $R := F[x]$. Now put

$$v := x - \sum_{i=1}^{r} \alpha_i c_i = \sum_{i=1}^{r} (x - \alpha_i 1_A) c_i \in R. \tag{s1}$$

Then the first relation of (2) (in the exercise) trivially holds and

$$v^n = \sum_{i=1}^{r} (x - \alpha_i 1_A)^n c_i = \Big( \sum_{i=1}^{r} (\mathbf{t} - \alpha_i)^n \mu_i f_i \Big)(x).$$

For $1 \le i \le r$,

$$(\mathbf{t} - \alpha_i)^n \mu_i f_i = (\mathbf{t} - \alpha_i)^{n_i} \mu_i (\mathbf{t} - \alpha_i)^{n - n_i} f_i = \mu_x (\mathbf{t} - \alpha_i)^{n - n_i} f_i$$

is a multiple of $\mu_x$ and hence kills $x$. This shows $v^n = 0$, and the proof of (2) (in the exercise) is complete.

(b) For $I \subseteq \{1, \dots, r\}$, the quantity $c_I$ is clearly an idempotent in $R$. Conversely, let $c$ be an idempotent in $R$. Then $c = f(x)$ for some $f \in F[\mathbf{t}]$. Since $R$ is commutative associative, we have

$$\mathrm{Nil}(R) = \{u \in R \mid u \text{ is nilpotent}\}. \tag{s2}$$

Hence (2) (in the exercise) implies, for all $m \in \mathbb{N}$,

$$x^m = \sum_{i=1}^{m} \alpha_i^m c_i + v_m, \quad v_m \in \mathrm{Nil}(R)$$

and then

$$g(x) = \sum_{i=1}^{r} g(\alpha_i) c_i + v_g, \quad v_g \in \mathrm{Nil}(R),$$

for all $g \in F[\mathbf{t}]$. In particular, setting $\beta_i := f(\alpha_i)$ for $1 \leq i \leq r$,

$$c = f(x) = \sum_{i=1}^{r} \beta_i c_i + v_f, \quad c^2 = f^2(x) = \sum_{i=1}^{r} \beta_i^2 c_i + v_{f^2}.$$

But $c = c^2$, so $\sum(\beta_i^2 - \beta_i)c_i = v_{f^2} - v_f$ is nilpotent, which obviously implies $\beta_i^2 = \beta_i$, hence $\beta_i \in \{0, 1\}$ for $1 \leq i \leq r$. Put

$$I := \{i \in \mathbb{Z} \mid 1 \leq i \leq r,\ \beta_i = 1\}.$$

Then, setting $w := v_f \in \mathrm{Nil}(R)$,

$$c_I + w = c = c^2 = c_I + 2c_I w + w^2,$$

and we conclude

$$(1_A - 2c_I)w = w^2, \quad (1_A - 2c_I)^2 = 1_A. \tag{s3}$$

In particular, $1_A - 2c_I$ is invertible in $R$. Let $m \in \mathbb{Z}$ satisfy $m \geq 1$ and $w^m = 0 \neq w^{m-1}$. Assuming $m \geq 2$, we conclude from (s3) (in the solution) that $(1 - 2c_I)w^{m-1} = w^m = 0$, hence $w^{m-1} = 0$, a contradiction. Thus $m = 1$, forcing $w = 0$ and $c = c_I$.

(c) (i) $\Rightarrow$ (ii). Let $1 \leq i \leq r$ and put $v := ((\mathbf{t} - \alpha_i)\mu_i)(x) \in R$. Then

$$v^{n_i} = ((\mathbf{t} - \alpha_i)^{n_i}\mu_i^{n_i})(x) = (\mu_x \mu_i^{n_i - 1})(x) = 0,$$

and (i) implies $v = 0$.Thus $\mu_x = (\mathbf{t} - \alpha_i)^{n_i}\mu_i$ divides $(\mathbf{t} - \alpha_i)\mu_i$, forcing $n_i = 1$ since $\mu_i$ is not divisible by $\mathbf{t} - \alpha_i$.

(ii) $\Rightarrow$ (iii). This follows immediately from (2) (in the exercise).

(iii) $\Rightarrow$ (i). Let $v \in \mathrm{Nil}(R)$. Then

$$v = f(x) = \sum_{i=1}^{r} f(\alpha_i)c_i$$

for some $f \in F[\mathbf{t}]$ is nilpotent, which can happen only if $f(\alpha_1) = \cdots = f(\alpha_r) = 0$ and hence amounts to $v = 0$.

(d) Write $\mu_x = \sum_{j=0}^{d} \gamma_j \mathbf{t}^j$ with $d = \sum_{i=1}^{r} n_i$ and $\gamma_0, \ldots, \gamma_d \in F$. Then the condition $\alpha_i \neq 0$ for all $i = 1, \ldots, r$ is equivalent to $\gamma_0 = \mu_x(0) \neq 0$, hence implies $xy = 1_A$ with $y = -\gamma_0^{-1} \sum_{j=1}^{d} \gamma_j x^{j-1} \in R$, so $x$ is invertible in $R$. Conversely, let this be so and assume $\gamma_0 = 0$. Then $x \sum_{j=1}^{d} \gamma_j x^{j-1} = \mu_x(x) = 0$, and since $x$ is invertible in $R$, the polynomial $\sum_{j=1}^{d} \gamma_j \mathbf{t}^{j-1} \in F[\mathbf{t}]$ of degree at most $d - 1$ kills $x$, in contradiction to $\mu_x$ being the minimum polynomial of $x$. Thus $\gamma_0 \neq 0$.

(e) Let $\beta_i \in F^\times$ satisfy $\beta_i^2 = \alpha_i$ for $1 \leq i \leq r$. Setting $z := \sum_{i=1}^{r} \beta_i c_i$, we obtain $z^{-2}x = 1_A + w$, for some $w \in \mathrm{Nil}(R)$. Thus we may assume $x = 1_A + w$ and

$w^m = 0 \neq w^{m-1}$ for some positive integer $m$. The case $m = 1$ being obvious, we may actually assume $m \geq 2$. Let

$$y = \sum_{j=0}^{m-1} \gamma_j w^j \in R \qquad (\gamma_0 \ldots, \gamma_{m-1} \in F).$$

The minimum polynomial of $w$ is $\mathfrak{t}^m$, and we conclude that $1_A, w, \ldots, w^{m-1}$ are linearly independent over $F$. Hence $y^2 = x$ if and only if

$$1_A + w = \sum_{j=0}^{m-1} (\sum_{l=0}^{j} \gamma_l \gamma_{j-l}) w^j,$$

which in turn is equivalent to

$$\gamma_0^2 = 2\gamma_0\gamma_1 = 1, \quad \sum_{l=0}^{j} \gamma_l \gamma_{j-l} = 0 \qquad (2 \leq j < m).$$

This system of quadratic equations can be solved recursively by

$$\gamma_0 = 1, \quad \gamma_1 = \frac{1}{2}, \quad \gamma_j = -\frac{1}{2} \sum_{l=1}^{j-1} \gamma_l \gamma_{j-l} \qquad (2 \leq j < m).$$

This proves the assertion.

*A4.7 Remark.* The equation $y^2 = x = 1_A + w$, $w \in R$ nilpotent, can be solved more concisely by

$$y = \sum_{l=0}^{\infty} \binom{\frac{1}{2}}{l} w^l,$$

combined with the observation that $\binom{\frac{1}{2}}{l} \in \mathbb{Q}$ has exact denominator a power of 2 (depending on $l$).

**8.12** We write $\mathfrak{D}$ (resp. $\mathfrak{E}$) for the set of decompositions of $A$ into the direct sum of $n$ complementary ideals (resp. of complete orthogonal systems of $n$ central idempotents) in $A$. Let $(e_j)_{1 \leq j \leq n} \in \mathfrak{E}$. For $1 \leq j, l \leq n$, centrality implies $(Ae_j)(Ae_l) = A^2(e_j e_l)$, which is zero for $j \neq l$ and $Ae_j$ for $j = l$. Moreover, $x = \sum xe_j \in \sum Ae_j$ for every $x \in A$, and given $x_j \in A$ for $1 \leq j \leq n$ satisfying $\sum x_j e_j = 0$, we multiply with $e_l$, $1 \leq l \leq n$, and deduce $x_l e_l = 0$. All this boils down to $A = (Ae_1) \oplus \cdots \oplus (Ae_n)$ as a direct sum of ideals. Thus the assignment $(e_j) \mapsto (Ae_j)$ gives a map from $\mathfrak{E}$ to $\mathfrak{D}$.

Conversely, let $(I_j)_{1 \leq j \leq n} \in \mathfrak{D}$. Then each $I_j$, $1 \leq j \leq n$, is a unital $k$-algebra in its own right, and setting $e_j := 1_{A_j}$, we deduce $\sum e_j = 1_A$, $e_j e_l = \delta_{jl} e_j$ for $1 \leq j, l \leq n$, so $(e_j)_{1 \leq j \leq n}$ is a complete orthogonal system of idempotents in

$A$, which are clearly central since $\mathrm{Cent}(A) = \mathrm{Cent}(I_1) \oplus \cdots \oplus \mathrm{Cent}(I_n)$ as a direct sum of ideals. Thus the assignment $(I_j)_{1\le j\le n} \mapsto (e_j)_{1\le j\le n}$ determines a map from $\mathfrak{D}$ to $\mathfrak{E}$, and it is readily checked that the two maps constructed are inverse to each other.

**8.13** (a) (i) $\Rightarrow$ (ii). Let $d \in Rc$ be a non-zero idempotent. Then $cd = d$ and $c = d + d'$, where $d' := c - d \in Rc$ is an idempotent orthogonal to $d$. Since $c$ is primitive, this implies $d' = 0$, i.e., $d = c$.

(ii) $\Rightarrow$ (iii). Suppose $x \in Rc$ is not nilpotent. Since $F$ is a field, we conclude from Exc. 7.14 (a) that $F_1[x] \subseteq Rc$ contains a non-zero idempotent. By (ii), therefore, $c \in F_1[x]$, and there are $n \in \mathbb{Z}$, $n > 0$, as well as $\alpha_1, \ldots, \alpha_n \in F$ satisfying $c = \sum_{i=1}^{n} \alpha_i x^i = xy$, $y := \alpha_1 c + \sum_{i=1}^{n-1} \alpha_{i+1} x^i \in Rc$. Hence $x$ is invertible in $Rc$.

(iii) $\Rightarrow$ (i). Assume $c_1, c_2 \in R$ are non-zero orthogonal idempotents having $c = c_1 + c_2$. Then $cc_i = c_i$, hence $c_i \in Rc$, for $i = 1, 2$. But $c_i$, being a non-zero idempotent, cannot be nilpotent. By (iii), therefore, $c_i$ is invertible in $Rc$, which contradicts the relation $c_1 c_2 = 0$.

(b) Non-zero orthogonal idempotents are linearly independent. Hence, as $R$ is finite-dimensional over $F$, there exists a unique maximal number $n$ such that $c$ splits into the orthogonal sum of $n$ non-zero idempotents: $c = \sum_{i=1}^{n} c_i$. Assume $c_n$, say, is not primitive. Then $c_n = d_n + d_{n+1}$, for some non-zero orthogonal idempotents $d_n, d_{n+1}$. For $1 \le i < n$ and $j = n, n+1$, we conclude $c_i d_j = c_i c_n d_j = 0$, and $c = \sum_{i=1}^{n-1} c_i + d_n + d_{n+1}$ decomposes into the orthogonal sum of $n+1$ non-zero idempotents, a contradiction. Thus $c_n$, hence (by symmetry) each $c_i$, $1 \le i \le n$, is primitive.

(c) Let $c, d \in R$ be distinct primitive idempotents. Then $cd \in Rc \cap Rd$ is an idempotent. Assuming $cd \neq 0$, condition (ii) in (a) would imply $c = cd = d$, a contradiction. Hence $cd = 0$. Summing up, the primitive idempotents of $R$ are mutually orthogonal and thus finite in number since $R$ is finite-dimensional over $F$. We may therefore form the orthogonal system $(c_1, \ldots, c_n)$ of *all* primitive idempotents in $R$. Put $c := \sum_{i=1}^{n} c_i$ and $R_0 := \{x \in R \mid cx = 0\}$. Then Exc. 8.12 implies

$$R = Rc \oplus R_0 = \bigoplus_{i=1}^{n} Rc_i \oplus R_0 \tag{s1}$$

as direct sums of ideals. Assuming $R_0 \neq \{0\}$, Exc. 7.14 would yield a non-zero idempotent in $R_0$, hence also a primitive one by (b). Using (s1), one checks that a primitive idempotent in $R_0$ stays primitive in $R$, and we have arrived at a contradiction. Thus $R_0 = \{0\}$, i.e., $R$ is unital with identity element $c$. From

condition (iii) in (a) we conclude that $K_i := Rc_i$ $(1 \le i \le n)$ are finite algebraic field extensions of $F$, and (s1) yields $R \cong \prod_{i=1}^{n} K_i$.

**8.14** Let $(c_i)_{i\in I}$ be an orthogonal system of non-zero idempotents in $R$, indexed by an infinite set $I$. Pick a countably infinite ascending chain

$$I_0 \subset I_1 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots$$

of finite subsets of $I$ and put $\mathfrak{a}_n := \sum_{i\in I_n} Rc_i$ for all $n \in \mathbb{N}$. Then

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_n \subset \mathfrak{a}_{n+1} \subset \cdots$$

is a countably infinite ascending chain of ideals in $R$. If $R$ were finitely generated as a $k$-algebra, it would be noetherian (since $k$ is) and the aforementioned chain would become stationary eventually, a contradiction.

**8.15** For $1 \le i, j, l, m, p, q \le n$, a straightforward verification shows

$$[ae_{ij}, be_{lm}, ce_{pq}] = \delta_{jl}\delta_{mp}[a, b, c]e_{iq}, \tag{s1}$$

$$[ae_{ij}, be_{lm}] = \delta_{jl}(ab)e_{im} - \delta_{im}(ba)e_{lj}. \tag{s2}$$

The inclusion $\mathrm{Mat}_n(\mathrm{Nuc}(A)) \subseteq \mathrm{Nuc}(\mathrm{Mat}_n(A))$ follows immediately from (s1). Conversely, let $x = (a_{ij}) = \sum a_{ij}e_{ij} \in \mathrm{Nuc}(\mathrm{Mat}_n(A))$. Then (s1) for $m = p$ implies $0 = [x, be_{lm}, c_{mp}] = \sum_i [a_{il}, b, c]e_{iq}$, hence $[a_{il}, A, A] = \{0\}$. Similarly, $0 = [be_{lm}, ce_{mq}, x] = \sum_j [b, c, a_{qj}]e_{lj}$, forcing $[A, A, a_{qj}] = \{0\}$. And, finally, $0 = [be_{lm}, x, ce_{pq}] = [b, a_{mp}, c]e_{lq}$ implies $[b, a_{mp}, c] = 0$. Summing up, we conclude $a_{ij} \in \mathrm{Nuc}(A)$ for $1 \le i, j \le n$, solving the first part of the problem.

Concerning the second one, let $x = (a_{ij}) = \sum a_{ij}e_{ij} \in \mathrm{Cent}(\mathrm{Mat}_n(A))$. By the first part, $a_{ij} \in \mathrm{Nuc}(A)$ for $1 \le i, j \le n$. Moreover, (s2) for $l = m$ yields $0 = [x, e_{ll}] = \sum_i a_{il}e_{il} - \sum_j a_{lj}e_{lj}$, hence $a_{ij} = 0$ for $1 \le i, j \le n$, $i \ne j$. Now let $l \ne m$ in (s2). Then $[x, be_{lm}] = (a_{ll}b)e_{lm} - (ba_{mm})e_{lm}$, forcing $a_{ll} = a_{mm} \in \mathrm{Cent}(A)$, and we conclude $x \in \mathrm{Cent}(A)\mathbf{1}_n$. Conversely, it is clear that every element of $\mathrm{Cent}(A)\mathbf{1}_n$ belongs to $\mathrm{Cent}(\mathrm{Mat}_n(A))$.

**8.16** Let $D$ be a finite-dimensional non-associative division algebra over $F$ and suppose $D$ has dimension $n > 1$. Picking linearly independent vectors $x, y \in D$, the polynomial $\det(L_{x+\mathbf{t}y}) \in F[\mathbf{t}]$ has degree $n$, hence a root $\alpha \in F$. But then left multiplication by the non-zero element $x + \alpha y \in D$ is not bijective, contradicting the property of $D$ being a division algebra. Thus $n = 1$, and we conclude $D = Fe$ for some non-zero element $e \in D$. Therefore $e^2 = \alpha e$ for some $\alpha \in F^\times$, and it is readily checked that $F \to D$, $\xi \mapsto \alpha^{-1}\xi e$ is an isomorphism of $F$-algebras.

## Solutions for Section 9

**9.24** Let $m, n \in \mathbb{Z}$ such that $u := mx + ny \in \mathrm{Nuc}(A)$. Then $0 = [u, x, x] = m(x^2x - xx^2) + n((yx)x - yx^2) = 2m(x - x) - 2ny = -2ny$, hence $n = 0$, and $0 = [u, x, y] = m(x^2y - x(xy)) = 2my$, hence $m = 0$. Thus $\mathrm{Cent}(A) = \mathrm{Nuc}(A) = \mathbb{Z}1_A$; in particular, $A$ is central. On the other hand, passing to the base change $A_R$, $R = \mathbb{Z}/2\mathbb{Z}$, which by 9.3 agrees with $A/2A$, and setting $\bar{u} := u_R$ for $u \in A$, we conclude that $1_{\bar{A}}, \bar{x}, \bar{y}$ is an $R$-basis of $A_R$ with multiplication table $\bar{x}^2 = \bar{x}\bar{y} = \bar{y}\bar{x} = \bar{y}^2 = 0$. It follows from this at once that $A_R$ is commutative associative, so while $\mathrm{Cent}(A_R) = \mathrm{Nuc}(A_R) = A_R$ is a free $R$-module of rank 3, $(\mathrm{Cent}(A))_R = (\mathrm{Nuc}(A))_R = R1_{\bar{A}}$ is a free $R$-module of rank 1.

**9.25** (a): Suppose $0 \neq x \in A$. If $y \in A$ is such that $0 = xy$, then $y = 0$ by hypothesis on $A$. That is, the linear transformation $L_x \colon A \to A$ is injective. Since $A$ is finite-dimensional, $L_x$ is bijective. Similarly, $R_x$ is bijective. This verifies the claim.

(b): Since $F(\mathbf{t}) \subset F((\mathbf{t}))$, $A_{F(\mathbf{t})} \subset A_{F((\mathbf{t}))}$, so it suffices to treat the case $K = F((\mathbf{t}))$.

Since $A$ is a division algebra, it has no zero divisors. Applying Exc. 18.21 with $k = F$ and $R = F[[\mathbf{t}]]$, we find that $A_R$ has no zero divisors.

Every element of $A_K$ can be written as $a\mathbf{t}^{-m}$ for some $a \in A_R$ and $m \geq 0$. Suppose $b\mathbf{t}^{-n} \in A_K$ for $b \in A_R$ and $n \geq 0$ is such that $0 = (a\mathbf{t}^{-m})(b\mathbf{t}^{-n})$. Then $0 = (ab)\mathbf{t}^{-m-n}$, i.e., $ab = 0$ in $A_R$, so $a = 0$ or $b = 0$, ergo $a\mathbf{t}^{-m} = 0$ or $b\mathbf{t}^{-n} = 0$.

**9.26** Put $\mathfrak{p}$ for the prime ideal that is the kernel of the unit morphism $\vartheta \colon k \to K$. By hypothesis, there is a prime ideal $\mathfrak{p}' \in \mathrm{Spec}(k')$ such that $\mathfrak{p} = \vartheta^{-1}(\mathfrak{p}')$. This provides a commutative diagram as in (9.5.6) and in particular the field $k(\mathfrak{p})$ is contained in both $K$ and $k'(\mathfrak{p}')$. It suffices to take $K'$ to be any field containing both $K$ and $k'(\mathfrak{p}')$ (called a "compositum" of the two fields), which exists by an argument as in [23, p. 552].

**9.27** We proceed in several steps.

1°. Let $\mathrm{can} = \mathrm{can}_{k,k(\mathfrak{p})} \colon k \to k(\mathfrak{p})$, $\alpha \mapsto \alpha(\mathfrak{p})$, be the natural map. Then the diagram

$$\begin{array}{ccc} k & \xrightarrow[\mathrm{can}]{} & k(\mathfrak{p}) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi(\mathfrak{p})} \\ k' & \xrightarrow[\mathrm{can}(\mathfrak{p})]{} & k'(\mathfrak{p}) \end{array}$$

commutes since

$$\begin{aligned}\varphi(\mathfrak{p})\circ\mathrm{can}(\alpha) &= (\varphi\otimes\mathbf{1}_{k(\mathfrak{p})})(1\otimes\alpha(\mathfrak{p})) = 1_{k'}\otimes\alpha(\mathfrak{p}) = 1_{k'}\otimes(\alpha\cdot 1_{k(\mathfrak{p})})\\ &= (\alpha\cdot 1_{k'})\otimes 1_{k(\mathfrak{p})} = \varphi(\alpha)\otimes 1_{k(\mathfrak{p})} = \varphi(\alpha)(\mathfrak{p}) = \mathrm{can}(\mathfrak{p})\circ\varphi(\alpha)\end{aligned}$$

for all $\alpha \in k$. Applying the contra-variant functor Spec to this diagram, we conclude that also

$$\begin{array}{ccc}\mathrm{Spec}\,(k'(\mathfrak{p})) & \xrightarrow[\mathrm{Spec}(\mathrm{can}(\mathfrak{p}))]{} & \mathrm{Spec}(k')\\ {\scriptstyle\mathrm{Spec}(\varphi(\mathfrak{p}))}\downarrow & & \downarrow{\scriptstyle\mathrm{Spec}(\varphi)}\\ \mathrm{Spec}\,(k(\mathfrak{p})) & \xrightarrow[\mathrm{Spec}(\mathrm{can})]{} & \mathrm{Spec}(k)\end{array}$$

commutes. But $\mathrm{Spec}(k(\mathfrak{p}))$ consists of a single point sent by Spec(can) to $\mathrm{can}^{-1}(\{0\}) = \mathrm{Ker}(\mathrm{can}) = \mathfrak{p}$. Hence the image of $\mathrm{Spec}(\mathrm{can}(\mathfrak{p}))$ belongs to the fiber $\mathrm{Spec}(\varphi)^{-1}(\mathfrak{p})$. Thus $\mathrm{Spec}(\mathrm{can}(\mathfrak{p}))$ *induces canonically a continuous map*

$$\Psi\colon\ \mathrm{Spec}\,(k'(\mathfrak{p})) \longrightarrow \mathrm{Spec}(\varphi)^{-1}(\mathfrak{p}).$$

2°. Let $\mathfrak{p}' \in \mathrm{Spec}(\varphi)^{-1}(\mathfrak{p})$. Then $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$, and consulting (9.5.6), we find a unique homomorphism

$$\sigma_{\mathfrak{p}'}\colon k'(\mathfrak{p}) \longrightarrow k'(\mathfrak{p}')$$

of $k(\mathfrak{p})$-algebras making a commutative diagram

$$\begin{array}{ccccc}k & \xrightarrow{\varphi} & k' & \xrightarrow{\mathrm{can}(\mathfrak{p})} & k'(\mathfrak{p})\\ {\scriptstyle\mathrm{can}_{\mathfrak{p}}}\downarrow & & {\scriptstyle\mathrm{can}_{\mathfrak{p}'}}\downarrow & & \\ k_{\mathfrak{p}} & \xrightarrow{\varphi'} & k'_{\mathfrak{p}'} & \overset{\sigma_{\mathfrak{p}'}}{\searrow} & \\ {\scriptstyle\varrho(\mathfrak{p})}\downarrow & & {\scriptstyle\varrho(\mathfrak{p}')}\downarrow & & \\ k(\mathfrak{p}) & \xrightarrow[\bar{\varphi}]{} & k'(\mathfrak{p}'). & & \end{array}\qquad\text{(s1)}$$

Thus $\mathrm{Ker}(\sigma_{\mathfrak{p}'}) \in \mathrm{Spec}(k'(\mathfrak{p}))$, and we obtain a map

$$\Phi\colon\ \mathrm{Spec}(\varphi)^{-1}(\mathfrak{p}) \longrightarrow \mathrm{Spec}\,(k'(\mathfrak{p}))$$

given by

$$\Phi(\mathfrak{p}') := \mathrm{Ker}(\sigma_{\mathfrak{p}'}) \qquad\qquad (\mathfrak{p}' \in \mathrm{Spec}(\varphi)^{-1}(\mathfrak{p})).$$

The definitions and (s1) imply

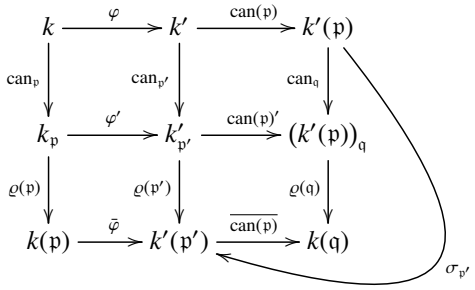
$$\Psi\circ\Phi(\mathfrak{p}') = \mathrm{can}(\mathfrak{p})^{-1}(\sigma_{\mathfrak{p}'}^{-1}(\{0\})) = (\sigma_{\mathfrak{p}'}\circ\mathrm{can}(\mathfrak{p})^{-1})(\{0\}) = \{\alpha' \in k' \mid \alpha'(\mathfrak{p}') = 0\} = \mathfrak{p}'$$

for all $\mathfrak{p}' \in \operatorname{Spec}(\varphi)^{-1}(\mathfrak{p})$, hence $\Psi \circ \Phi = \mathbf{1}_{\operatorname{Spec}(\varphi)^{-1}(\mathfrak{p})}$.

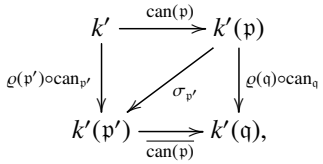
3°. Let $\mathfrak{q} \in \operatorname{Spec}(k'(\mathfrak{p}))$. Then

$$\Phi \circ \Psi(\mathfrak{q}) = \Phi(\mathfrak{p}') = \operatorname{Ker}(\sigma_{\mathfrak{p}'}), \quad \mathfrak{p}' := \operatorname{can}(\mathfrak{p})^{-1}(\mathfrak{q}) \in \operatorname{Spec}(\varphi)^{-1}(\mathfrak{p}).$$

By (9.5.6) again, we obtain a diagram




where the four squares commute. But so does the diagram




which by (s1) is clear for the upper triangle but holds true also for the lower one because $\overline{\operatorname{can}(\mathfrak{p})} \circ \sigma_{\mathfrak{p}'}$ and $\varrho(\mathfrak{q}) \circ \operatorname{can}_{\mathfrak{q}}$ are both $k(\mathfrak{p})$-linear satisfying $\overline{\operatorname{can}(\mathfrak{p})} \circ \sigma_{\mathfrak{p}'} \circ \operatorname{can}(\mathfrak{p}) = \varrho(\mathfrak{q}) \circ \operatorname{can}_{\mathfrak{q}} \circ \operatorname{can}(\mathfrak{p})$, hence $\overline{\operatorname{can}(\mathfrak{p})} \circ \sigma_{\mathfrak{p}'} = \varrho(\mathfrak{q}) \circ \operatorname{can}_{\mathfrak{q}}$. Since $\overline{\operatorname{can}(\mathfrak{p})}$ as a field homomorphism is injective, we therefore conclude

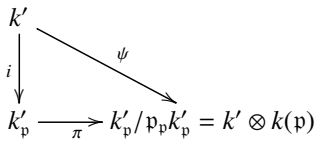
$$\Phi \circ \Psi(\mathfrak{q}) = \operatorname{Ker}(\sigma_{\mathfrak{p}'}) = \operatorname{Ker}(\overline{\operatorname{can}(\mathfrak{p})} \circ \sigma_{\mathfrak{p}'}) = \operatorname{Ker}\left(\varrho(\mathfrak{q}) \circ \operatorname{can}_{\mathfrak{q}}\right) = \mathfrak{q}.$$

Summing up we have shown that $\Psi$ *is bijective with inverse* $\Phi$.

4°. By 1° and 3°, it remains to show that $\Phi$ is continuous, equivalently, that $\Psi$ is open. In order to see this, we first deduce from (9.4.1) and 9.3 the natural identifications

$$k'(\mathfrak{p}) = (k' \otimes k_{\mathfrak{p}}) \otimes_{k_{\mathfrak{p}}} (k_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}) = k'_{\mathfrak{p}} \otimes_{k_{\mathfrak{p}}} (k_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}) = k'_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}k'_{\mathfrak{p}}$$

such that, with the natural maps $i\colon k' \to k'_{\mathfrak{p}}$, $\pi\colon k'_{\mathfrak{p}} \to k'_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}k'_{\mathfrak{p}}$, the triangle



commutes. The proof will be complete once we have shown

$$\Psi\big(D(\pi(f/s))\big) = D(f) \cap \operatorname{Spec}(\varphi)^{-1}(\mathfrak{p}) \tag{s2}$$

for all $f \in k'$, $s \in k \setminus \mathfrak{p}$. Let $\mathfrak{q} \in \operatorname{Spec}(k'(\mathfrak{p})) = \operatorname{Spec}(k'_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}k'_{\mathfrak{p}})$. Then the chain of equivalent conditions

$$\begin{aligned} \mathfrak{q} \in D(\pi(f/s)) &\iff \pi(f/s) \notin \mathfrak{q} \iff f/s \notin \pi^{-1}(\mathfrak{q}) \\ &\iff f \notin i^{-1}(\pi^{-1}(\mathfrak{q})) = \psi^{-1}(\mathfrak{q}) \iff \operatorname{can}(\mathfrak{p})^{-1}(\mathfrak{q}) \in D(f) \end{aligned} \tag{s3}$$

shows that the left-hand side of (s2) is contained in the right. Conversely, let $\mathfrak{p}' \in D(f) \cap \operatorname{Spec}(\varphi)^{-1}(\mathfrak{p})$. Then $\mathfrak{q} := \Psi^{-1}(\mathfrak{p}') \in \operatorname{Spec}(k'(\mathfrak{p}))$ and $\operatorname{can}(\mathfrak{p})^{-1}(\mathfrak{q}) = \mathfrak{p}' \in D(f)$. Consulting (s3), we conclude $\mathfrak{q} \in D(\pi(f/s))$, hence $\mathfrak{p}' = \Psi(\mathfrak{q}) \in \Psi(D(\pi(f/s)))$, and the proof of (s2) is complete.

**9.28** (a) We may assume $\chi = 0$. Pick $\mathfrak{p} \in U$. Let $u_1, \dots, u_m$ be a finite set of generators for the $k$-module $M$. For each $1 \le i \le m$, we have $\psi(u_i)/1 = \psi(u_i)_{\mathfrak{p}} = \psi_{\mathfrak{p}}(u_{i\mathfrak{p}}) = 0$ in $N_{\mathfrak{p}}$. Hence there are $f_i \in k \setminus \mathfrak{p}$ such that $f_i\psi(u_i) = 0$ in $N$. But this means $\psi(u_i)/1 = 0$ in $N_{f_i}$, which in turn, by 9.6, amounts to $\psi_{\mathfrak{q}} = 0$ for all $\mathfrak{q} \in \cap_{i=1}^m D(f_i) = D(f)$ for $f = f_1 f_2 \cdots f_m$. Hence we have shown $\mathfrak{p} \in D(f) \subseteq U$, and $U$ is Zariski-open in $X$.

(b) Again let $u_1, \dots, u_m$ be a finite set of generators for $A$ as a $k$-module. Given $i = 1, \dots, m$, we define $k$-linear maps $\psi_i, \chi_i \colon A \to B$ by $\psi_i(v) := \varphi(u_i v)$, $\chi_i(v) := \varphi(u_i)\varphi(v)$, $v \in A$. By (a),

$$U_i := \{\mathfrak{p} \in X \mid \psi_{i\mathfrak{p}} = \chi_{i\mathfrak{p}}\}$$

is Zariski-open in $X$. Hence so is $V = \bigcap_{i=1}^m U_i$.

**9.29** In the solution to this problem, free use will be made of the formalism for the Zariski topology as explained, for example, in [7, II, §4.3].

(a) For $\mathfrak{p} \in X$, the chain of equivalent conditions

$$\begin{aligned} \mathfrak{p} \in D(\varepsilon) &\iff \varepsilon \notin \mathfrak{p} \iff \varepsilon_{\mathfrak{p}} \notin \mathfrak{p}_{\mathfrak{p}} \iff \varepsilon_{\mathfrak{p}} \in k_{\mathfrak{p}}^{\times} \\ &\iff \varepsilon_{\mathfrak{p}} = 1_{\mathfrak{p}} \iff (1-\varepsilon)_{\mathfrak{p}} = 0 \end{aligned}$$

gives the first displayed equality, while the second one follows from the first and the fact that local rings are *connected*, i.e., contain only the trivial idempotents 0 and 1. The third equality is now obvious. To establish the final assertion of (a), we note for $\mathfrak{p} \in X$ that $(e_{i\mathfrak{p}})_{i\in I}$ is an orthogonal system of idempotents in $k_{\mathfrak{p}}$, whence $(\sum e_i)_{\mathfrak{p}} \neq 0$ if and only if $e_{i\mathfrak{p}} \neq 0$ for some $i = 1, \dots, r$. This proves $\bigcup D(\varepsilon_i) = D(\sum \varepsilon_i)$, and the union on the left is disjoint since $D(\varepsilon_i) \cap D(\varepsilon_j) = D(\varepsilon_i\varepsilon_j) = D(0) = \emptyset$ for $i, j \in I$, $i \neq j$.

(b) Given a complete system $(\varepsilon_i)_{i\in I}$ of orthogonal idempotents in $k$, the subsets $U_i := D(\varepsilon_i) \subseteq X$, $i \in I$, are open in $X$ and by (a) satisfy $\bigcup U_i = D(\sum e_i) =$

$D(1) = X$, where the union on the very left is disjoint and the $U_i$ are empty for almost all $i \in I$. Thus the assignment $(\varepsilon_i) \mapsto (U_i)$ gives a map of the right kind, which is injective since the $U_i$ by (a) determine the $\varepsilon_i$ locally, hence globally. It remains to show that the map in question is surjective, so let $(U_i)_{i\in I}$ be a decomposition of $X$ into disjoint open subsets almost all of which are empty.

First, view $X$ as a geometric space with structure sheaf $\mathcal{O}$. Since the $U_i$ form a disjoint open cover of $X$, we may apply the sheaf axioms to find, for each $i \in I$, a unique global section $\varepsilon_i \in H^0(X, \mathcal{O}) = k$ which restricts to the identity element of $H^0(U_i, \mathcal{O})$ and to zero on $H^0(U_j, \mathcal{O})$ for all $j \in I$, $j \neq i$. It is then readily checked that the $\varepsilon_i$ form a complete orthogonal system of idempotents in $k$, forcing the $D(\varepsilon_i)$ to be an open disjoint cover of $X$. On the other hand, given $\mathfrak{p} \in U_i$, we obtain $\varepsilon_{i\mathfrak{p}} = 1_{\mathfrak{p}}$, which implies $U_i \subseteq D(\varepsilon_i)$ by (a). Summing up, we have equality and surjectivity is proved.

Adopting a more direct approach based on the proof of [7, II.4, Prop. 15], let $i \in I$. Then $U_i$ and $Y_i := \bigcup_{j\neq i} U_j$ are closed subsets of $X$, hence may be written in the form $U_i = V(\mathfrak{a}_i)$, $Y_i = V(\mathfrak{b}_i)$ for some ideals $\mathfrak{a}_i, \mathfrak{b}_i \subseteq k$. Since $V(\mathfrak{a}_i + \mathfrak{b}_i) = V(\mathfrak{a}_i) \cap V(\mathfrak{b}_i) = U_i \cap Y_i = \emptyset$, we conclude $\mathfrak{a}_i + \mathfrak{b}_i = k$, hence $\alpha_i + \beta_i = 1$ for some $\alpha_i \in \mathfrak{a}_i$, $\beta_i \in \mathfrak{b}_i$. This implies $\alpha_i = \alpha_i(\alpha_i + \beta_i) = \alpha_i^2 + \alpha_i\beta_i \equiv \alpha_i^2 \bmod \mathfrak{a}_i\mathfrak{b}_i$, so $\alpha_i \in \mathfrak{a}_i$ becomes an idempotent modulo $\mathfrak{a}_i\mathfrak{b}_i$. On the other hand, $X = U_i \cup Y_i = V(\mathfrak{a}_i) \cup V(\mathfrak{b}_i) = V(\mathfrak{a}_i\mathfrak{b}_i)$, so $\mathfrak{a}_i\mathfrak{b}_i \subseteq k$ is a nil ideal. Now Exc. 7.14 (b) yields an idempotent $\varepsilon_i' \in \mathfrak{a}_i$ such that $\varepsilon_i' \equiv \alpha_i \bmod \mathfrak{a}_i\mathfrak{b}_i$. Thus $\varepsilon_i := 1 - \varepsilon_i' \in k$ is an idempotent as well satisfying $\varepsilon_i \equiv \beta_i \bmod \mathfrak{a}_i\mathfrak{b}_i$, hence $\varepsilon_i' \in \mathfrak{b}_i$. We conclude $U_i = V(\mathfrak{a}_i) \subseteq V(\varepsilon_i') = D(\varepsilon_i)$, $Y_i = V(\mathfrak{b}_i) \subseteq V(\varepsilon_i) = D(\varepsilon_i')$ and $D(\varepsilon_i) \cap D(\varepsilon_i') = \emptyset$ by (a). Therefore $U_i = D(\varepsilon_i)$, and it remains to show that $(\varepsilon_i)_{i\in I}$ is a complete orthogonal system of idempotents. For $i, j \in I$, $i \neq j$, we deduce $D(\varepsilon_i\varepsilon_j) = D(\varepsilon_i) \cap D(\varepsilon_j) = U_i \cap U_j = \emptyset$, so the idempotent $\varepsilon_i\varepsilon_j$ is also nilpotent, hence zero. Thus the $\varepsilon_i$ are orthogonal. For the same reason, $\varepsilon_i = 0$ for almost all $i \in I$ Now (a) gives

$$X = \bigcup U_i = \bigcup D(\varepsilon_i) = \bigcup V(1 - \varepsilon_i) = V(\prod (1 - \varepsilon_i)) = V(1 - \sum \varepsilon_i),$$

forcing the idempotent $1 - \sum \varepsilon_i$ to be nilpotent, hence zero.

**9.30** By [7, §II.3.3, Thm. 1], it suffices to prove that the map $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ induced by $f$ is an isomorphism for every $\mathfrak{m}$, so we may replace $k$ by $k_{\mathfrak{m}}$ and assume $k$ is local. Then $M$ and $N$ are free modules, and $M$ has finite rank. Since they have the same rank, they are isomorphic. Let $g\colon N \to M$ be an isomorphism. Then $g \circ f\colon M \to M$ is a $k$-linear surjection, and Prop. 7.11 shows that it is, in fact, a bijection. Hence so is $f$.

**9.31** Setting $X := \operatorname{Spec}(k)$, the subsets

$$U_i := \{\mathfrak{p} \in \operatorname{Spec}(k) \mid \operatorname{rk}_{\mathfrak{p}}(M) = i\} \subseteq X \qquad (i \in \mathbb{N}) \qquad \text{(s1)}$$

form an open disjoint cover of $X$ and since $X$ is quasi-compact [7, II.4, Prop. 12], $U_i$ is empty for almost all $i \in \mathbb{N}$. This proves (a) while, in order to prove (b), we apply Exc. 9.29 to obtain a complete orthogonal system $(\varepsilon_i)_{i\in\mathbb{N}}$ of idempotents in $k$ such that $U_i = D(\varepsilon_i)$ for all $i \in \mathbb{N}$. Given $j \in \mathbb{N}$, let $\pi_j \colon k \to k_j$ be the canonical projection induced by (1) and let $\mathfrak{p}_j \in \operatorname{Spec}(k_j)$. Then

$$\mathfrak{p} := \operatorname{Spec}(\pi_j)(\mathfrak{p}_j) = \pi_j^{-1}(\mathfrak{p}_j) = \mathfrak{p}_j \times \prod_{i\neq j} k_i \in X,$$

and (9.5.7) shows

$$M_{j\mathfrak{p}_j} = M_{\mathfrak{p}} \otimes_{k_{\mathfrak{p}}} k_{j\mathfrak{p}_j}.$$

Since $M_{\mathfrak{p}}$ is free of rank $j$ over $k_{\mathfrak{p}}$, it follows that $M_{j\mathfrak{p}_j}$ is free of rank $j$ over $k_{j\mathfrak{p}_j}$. This proves existence. In order to establish uniqueness, let $(\eta_i)_{i\in\mathbb{N}}$ be any complete orthogonal system of idempotents in $k$, giving rise, in analogy to (1), (2), to the decompositions

$$k = \prod_{i\in\mathbb{N}} l_i, \quad l_i = k\eta_i \qquad (i \in \mathbb{N}), \qquad \text{(s2)}$$

$$M = \prod_{i\in\mathbb{N}} N_i, \quad N_i = N \otimes l_i \qquad (i \in \mathbb{N}), \qquad \text{(s3)}$$

and making each $N_i$ a projective $l_i$-module of rank $i$. Again by Exc. 9.29, the $V_i := D(\eta_i)$ are empty for almost all $i \in I$ and form an open disjoint cover of $X$, so it suffices to show $V_i \subseteq U_i$ for all $i \in \mathbb{N}$. Fixing $j \in \mathbb{N}$ and $\mathfrak{q} \in V_j$, we apply Exc. 8.10, and find a decomposition $\mathfrak{q} = \prod_{i\in\mathbb{N}} \mathfrak{q}_i$, where $\mathfrak{q}_i = \mathfrak{q} \cap l_i$ is an ideal in $l_i$. But $\eta_j \notin \mathfrak{q}$ while $\eta_i\eta_j = 0 \in \mathfrak{q}$ for all $i \neq j$, forcing $\eta_i \in \mathfrak{q} \cap l_i = \mathfrak{q}_i$ and then $\mathfrak{q}_i = l_i$. Summing up we have shown

$$\mathfrak{q} = \mathfrak{q}_j \times \prod_{i\neq j} l_i,$$

so $\mathfrak{q}_j$ is a prime ideal in $l_j$ and $\operatorname{Spec}(\rho_j)(\mathfrak{q}_j) = \mathfrak{q}$, where $\rho_j \colon k \to l_j$ is the canonical projection induced by (s2). Since

$$N_{j\mathfrak{q}_j} = M_{\mathfrak{q}} \otimes_{k_{\mathfrak{q}}} l_{j\mathfrak{q}_j}$$

has rank $j$ over $l_{j\mathfrak{q}_j}$, the free $k_{\mathfrak{q}}$-module $M_{\mathfrak{q}}$ must have rank $j$ over $k_{\mathfrak{q}}$. This proves $\mathfrak{q} \in U_j$ by (s1), and the solution is complete.

**9.32** If $\varphi \colon A \to A'$ is a unital algebra homomorphism, then so is $\varphi(\mathfrak{p}) \colon A(\mathfrak{p}) \to A'(\mathfrak{p})$, for each $\mathfrak{p} \in \operatorname{Spec}(k)$. But since $A(\mathfrak{p})$ is simple by hypothesis, $\varphi(\mathfrak{p})$ is injective and a dimension argument shows that it is, in fact, an isomorphism.

Hence, by Nakayama's lemma [27, X, Prop. 4.5] or [44, Tag 07RC], $\varphi_\mathfrak{p}\colon A_\mathfrak{p} \to A'_\mathfrak{p}$ is an isomorphism, whence $\varphi$ is one [7, II.3, Thm. 1].

**9.33** (a) The right-hand side is clearly contained in the left, so it remains to establish the reverse inclusion. To this end, put $(A', G') = (A, G) \otimes F'$ and write $a' \in \mathrm{Cent}(A', G')$ in the form $a' = \sum a_i \otimes \alpha'_i$ with $a_i \in A$ and $\alpha'_i \in F'$ linearly independent over $F$. For $x, y \in A$, we have $\sum [a_i, x, y] \otimes \alpha'_i = [a', x \otimes 1_{F'}, y \otimes 1_{F'}] = 0$ and, similarly, $\sum [x, a_i, y] \otimes \alpha'_i = \sum [x, y, a_i] \otimes \alpha'_i = \sum [x, a_i] \otimes \alpha'_i = 0$. Moreover, for $g \in G$, $\sum g(a_i) \otimes \alpha'_i = (g \otimes \mathbf{1}_{F'})(a') = a' = \sum a_i \otimes \alpha'_i$. Since the $\alpha'_i$ are linearly independent over $F$, we therefore obtain $[a_i, x, y] = [x, a_i, y] = [x, y, a_i] = [a_i, x] = 0$, $g(a_i) = a_i$, hence $a_i \in \mathrm{Cent}(A, G)$ for all $i$, which implies $a' \in \mathrm{Cent}(A', G')$, as claimed.

(b) By Prop. 9.19, the right multiplication of $A$ induces an isomorphism $R : \mathrm{Cent}(A) \to \mathrm{End}_{\mathrm{Mult}(A)}(A)$. Hence it suffices to show that the elements of $\mathrm{Cent}(A, G)$ correspond to the $\mathrm{Mult}(A, G)$-linear maps $A \to A$ under this isomorphism, which follows from the relations $R_{g(a)} g = g R_a$ for all $a \in \mathrm{Cent}(A)$, $g \in G$.

(c) If $(A, G)$ is a simple $F$-algebra with a group of antomorphisms, then $M(A, G)$ acts irreducibly on $A$, so Schur's lemma and (b) yield the assertion.

(d) Since $A$, by simplicity of $(A, G)$, is an irreducible faithful $M(A, G)$-module, $M(A, G)$ is a primitive left-artinian $F$-algebra, hence simple [23, Thm. 4.2]. The first assertion now follows from the double centralizer theorem [23, Thm. 4.10]. It immediately implies necessity in the second part. Conversely, suppose $A \neq \{0\}$ and $M(A, G) = \mathrm{End}_F(A)$. Then $A$ is an irreducible $M(A, G)$-module, forcing $(A, G)$ to be simple and $\mathrm{Cent}(A, G)$ to be a field. Also, by (b), $\mathrm{End}_F(A) = M(A, G) = \mathrm{End}_{\mathrm{Cent}(A,G)}(A)$ and a dimension count yields sufficiency as well.

**9.34** (i) $\Rightarrow$ (ii). Let $F'$ be any extension field of $F$ and put $(A', G') = (A, G) \otimes F'$ as an $F'$-algebra with a group of antomorphisms. A moment's reflection shows $M(A', G') = M(A, G) \otimes F'$. Now the assertion follows from the second part of Exc. 9.33 (d).

(ii) $\Rightarrow$ (iii). Obvious.

(iv) $\Rightarrow$ (i). This follows immediately from Exc. 9.33 (a), (c).

**9.35** We follow standard arguments, reproduced in [12, I Satz 5.5], for example. Let $J \subseteq A \otimes A'$ be a non-zero ideal of $(A, G) \otimes (A', G')$ and consider the least positive integer $n$ such that there exist elements $x_1, \ldots, x_n \in A, x'_1, \ldots, x'_n \in A'$ satisfying

$$0 \neq x := \sum_{i=1}^{n} x_i \otimes x'_i \in J. \tag{s1}$$

Then the elements $x'_1, \dots, x'_n$ are linearly independent over $F$. Furthermore, a straightforward verification shows that the totality of elements $u_1 \in A$ such that

$$\sum_{i=1}^{n} u_i \otimes x'_i \in J$$

for some $u_2, \dots, u_n \in A$ forms an ideal $I$ of $(A, G)$ which is non-zero since $x_1 \in I$ and $x_1 \neq 0$ by minimality of $n$. Simplicity of $(A, G)$ therefore implies $I = A$, so in (s1) we may assume $x_1 = 1$. But then, for all $u, v \in A$,

$$\sum_{i=2}^{n} [x_i, u, v] \otimes x'_i = [x, u \otimes 1, v \otimes 1] \in J.$$

Again minimality of $n$ yields $[x, u \otimes 1, v \otimes 1] = 0$ and then $[x_i, u, v] = 0$ for $2 \leq i \leq n$. Similarly, $[u, x_i, v] = [u, v, x_i] = [x_i, u] = 0$, forcing $x_i \in \mathrm{Cent}(A)$ for $2 \leq i \leq n$. Applying $g \otimes \mathbf{1}$ for any $g \in G$ to (s1) and again observing $x_1 = 1$, we conclude

$$\sum_{i=2}^{n} (x_i - g(x_i)) \otimes x'_i = x - (g \otimes \mathbf{1})(x) \in J\,,$$

and minimality of $n$ implies $\sum_{i=2}^{n} (x_i - g(x_i)) \otimes x'_i = 0$, hence $x_i \in \mathrm{Cent}(A, G)$ for $2 \leq i \leq n$. But $(A, G)$ was assumed to be central simple, so $\mathrm{Cent}(A, G) = k1_A$, and we conclude $x = 1_A \otimes x' \in J$ for some $x' \in A'$. Now put

$$I' = \{u' \in A' \mid 1_A \otimes u' \in J\}.$$

Again it is straightforward to check that $I'$ is an ideal in $(A', G')$ which is non-zero since it contains $x' \neq 0$. Simplicity of $(A', G')$ therefore implies $I' = A'$, hence $1_{A \otimes A'} = 1_A \otimes 1_{A'} \in J$ and $J = A$, as claimed.

## Solutions for Section 10

**10.11** (a) We must show $P_\pi = \mathbf{1}_m \Rightarrow \pi = 1_{S_m}$, $P_{\pi\varrho} = P_\pi P_\varrho$ and $P_\pi^{-1} = P_\pi^{\mathsf{T}}$ for all $\pi, \varrho \in S_m$. The first statement is obvious, while the second one follows from

$$P_\pi P_\varrho = \sum_{i,j=1}^{m} e_{\pi(i),i} e_{\varrho(j),j} = \sum_{i=1}^{m} e_{\pi(i),\varrho^{-1}(i)} = \sum_{i=1}^{m} e_{\pi\varrho(i),i} = P_{\pi\varrho}.$$

And, finally, $P_\pi^{\mathsf{T}} = \sum e_{i,\pi(i)} = \sum e_{\pi^{-1}(i),i} = P_{\pi^{-1}} = P_\pi^{-1}$. Thus (a) is proved. In addition, we have

$$P_\pi e_{rs} P_\pi^{\mathsf{T}} = e_{\pi(r),\pi(s)} \qquad (1 \leq r, s \leq m) \qquad \text{(s1)}$$

since the left-hand side equals $\sum_{i,j} e_{\pi(i),i} e_{rs} e_{j,\pi(j)} = e_{\pi(r),\pi(r)}$, as desired.

(b) In terms of matrix units, the quantities $I, J$ of 10.10 may be written as

$$I = \sum_{i=1}^{n} (e_{i,i+n} - e_{i+n,i}), \quad J = \sum_{i=1}^{n} (e_{2i-1,2i} - e_{2i,2i-1}).$$

Hence (s1) implies $P_\pi I P_\pi^\mathsf{T} = J$, and setting $\tau := \tau_{\mathrm{ort}}^J$, we conclude

$$\tau(P_\pi S P_\pi^\mathsf{T}) = J^{-1}(P_\pi S P_\pi^\mathsf{T})^\mathsf{T} J = J^{-1} P_\pi S^\mathsf{T} P_\pi^\mathsf{T} J = P_\pi I^{-1} S^\mathsf{T} I P_\pi^\mathsf{T} = P_\pi \tau_{\mathrm{spl}}(S) P_\pi^\mathsf{T}$$

for all $S \in \mathrm{Mat}_{2n}(k)$, and the assertion follows.

## Solutions for Section 11

**11.28** Let $t\colon A \to k$ be an associative linear form and suppose the corresponding bilinear form $\sigma := \sigma_t$ (cf. 7.9) is regular (cf. 11.9). By hypothesis, there exists a unique element $e \in A$ such that $t(x) = \sigma(e, x) = t(ex)$ for all $x \in A$. Now the relations $t((ex)y) = t(e(xy)) = t(xy)$ and $t((xe)y) = t(y(xe)) = t((yx)e) = t(e(yx)) = t(yx) = t(xy)$ for all $x, y \in A$ combined with regularity of $\sigma$ imply $ex = x = xe$ for all $x \in A$. Hence $A$ is unital with $1_A = e$.

**11.29** Let $\alpha_1, \ldots, \alpha_n \in k$ satisfy $\sum_{i=1}^n \alpha_i m_i = 0$ and put $x := (\alpha_1, \ldots, \alpha_n) \in k^n$. Then

$$\sum_{i=1}^{n} \alpha_i \sigma(m_i, m_j) = \sigma(\sum_{i=1}^{n} \alpha_i m_i, m_j) = 0$$

for $1 \le j \le n$, hence $xS = 0$. Applying the adjoint of $S$ yields $0 = xSS^\sharp = \det(S)x$, and since $\det(S)$ is not a zero divisor in $k$, we conclude $x = 0$, i.e., $\alpha_i = 0$ for $1 \le i \le n$, as desired.

**11.30** The implications (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) being obvious, it suffices to prove (ii) $\Rightarrow$ (iii), which we do by following a suggestion of O. Loos. Letting $(e_+, e_-)$ be a hyperbolic pair of $\mathbf{h}_L$ and writing $e_\pm = (v_\pm^*, v_\pm)$, $v_\pm \in L$, $v_\pm^* \in L^*$, we apply (11.18.1) and obtain $\langle v_+^* + v_-^*, v_+ + v_- \rangle = \mathbf{h}_L(e_+ + e_-) = 1$. Therefore $v_+ + v_- \in L$ is a unimodular vector, hence a basis of $L$ over $k$, and (iii) follows.

**11.31** (i) $\Rightarrow$ (ii). Clear.

(ii) $\Rightarrow$ (iii). We have $q = \langle S \rangle_{\mathrm{quad}}$ with $S := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, hence $Dq = \langle S + S^\mathsf{T} \rangle$ with $S + S^\mathsf{T} = \left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ having determinant $-4$. Since $q$ is regular, $2 \in k$ is a unit.

(iii) $\Rightarrow$ (i). With the canonical basis $e_1, e_2$ of $k^2$, we have $q(e_1) = 1$, $q(e_2) = -1$, $q(e_1, e_2) = 0$. One checks that $(u_+, u_-)$ with $u_\pm := \frac{1}{2}(e_1 \pm e_2)$ is a hyperbolic

pair relative to $q$, and since $e_1 = u_+ + u_-$, $e_2 = u_+ - u_-$, it follows that $q$ is a hyperbolic plane.

**11.32** Because the base ring is a field of characteristic $\neq 2$, $q$ is isomorphic to a form $\langle \alpha_1, \alpha_2 \rangle_{\text{quad}}$ for some $\alpha_1, \alpha_2 \in F^\times$. By hypothesis on the discriminant, $\alpha_1 \cong -\alpha_2$ and we find $q \cong \langle \alpha_1 \rangle \otimes \langle 1, -1 \rangle_{\text{quad}}$. It suffices now to note that $\langle 1, -1 \rangle_{\text{quad}}$ is a split hyperbolic plane by Exercise 11.31, so tensoring with $\langle \alpha_1 \rangle$ does not change its isomorphism class (11.19).

**11.33** The implications (ii) $\Rightarrow$ (i) being obvious, let us assume that $(u_1, u_2)$ is a hyperbolic pair in $\mathbf{h}$. Writing $u_j = \alpha_{1j} e_1 + \alpha_{2j} e_2$ ($\alpha_{ij} \in k$, $i, j = 1, 2$), we conclude

$$\alpha_{1j}\alpha_{2j} = 0, \quad \alpha_{11}\alpha_{22} + \alpha_{21}\alpha_{12} = 1 \qquad (j = 1, 2). \tag{s1}$$

Thus $(\varepsilon_+, \varepsilon_-)$, $\varepsilon_+ := \alpha_{11}\alpha_{22}$, $\varepsilon_- := \alpha_{21}\alpha_{12}$, is a complete orthogonal system of idempotents in $k$, giving rise to a decomposition of $k$ as in (ii) such that (1) holds. Moreover, setting $\gamma_+ := \alpha_{11}\varepsilon_+ \in k_+^\times$ with inverse $\gamma_+^{-1} = \alpha_{22}\varepsilon_+$, $\gamma_- := \alpha_{21}\varepsilon_- \in k_-^\times$ with inverse $\gamma_-^{-1} = \alpha_{12}\varepsilon_-$, we apply (s1) and obtain

$$\begin{aligned}
u_{1+} &= \varepsilon_+ u_1 = \alpha_{11}\alpha_{22}(\alpha_{11}e_1 + \alpha_{21}e_2) = \gamma_+ e_{1+}, \\
u_{2+} &= \varepsilon_+ u_2 = \alpha_{11}\alpha_{22}(\alpha_{12}e_1 + \alpha_{22}e_2) = \gamma_+^{-1} e_{2+}, \\
u_{1-} &= \varepsilon_- u_1 = \alpha_{21}\alpha_{12}(\alpha_{11}e_1 + \alpha_{21}e_2) = \gamma_- e_{2-}, \\
u_{2-} &= \varepsilon_- u_2 = \alpha_{21}\alpha_{12}(\alpha_{12}e_1 + \alpha_{22}e_2) = \gamma_-^{-1} e_{1-},
\end{aligned}$$

hence (2), (3).

**11.34** Uniqueness is clear, so it suffices to prove existence. Setting

$$\operatorname{Quad}_k(M, P) := \{Q \mid Q\colon M \to P \text{ is } k\text{-quadratic}\}$$

as a $k$-module, the map

$$h\colon N \longrightarrow \operatorname{Quad}_k(M, P), \quad y \longmapsto h(y) := g(-, y)$$

is $k$-linear and hence induces a $k$-linear map

$$h_1\colon N \longrightarrow \operatorname{Quad}_R(M_R, P_R), \quad y \longmapsto h_1(y) := h(y)_R,$$

$h(y)_R$ being the $R$-quadratic extension of $h(y)$ is the sense of Corollary 11.5. Applying (9.2.5), we obtain an $R$-linear map

$$h_1'\colon N_R \longrightarrow \operatorname{Quad}_R(M_R, P_R)$$

such that

$$h_1'(y_R) = h(y)_R \tag{s1}$$

for all $y \in N$. Now define $g_R\colon M_R \times N_R \to P_R$ by

$$g_R(u, v) := h_1'(v)(u) \tag{s2}$$

for all $u \in M_R$, $v \in N_R$. Combining (s2) with (s1) and (11.5.1), one checks that (1) is commutative.

**11.35** We argue by induction on $n$. The case $n = 1$ has been settled in Cor. 11.5. Now suppose $n > 1$ and assume that the assertion holds for $n - 1$. For any $u_n \in M_n$, the map

$$F_{u_n}\colon M_1 \times \cdots \times M_{n-1} \longrightarrow M, \quad (u_1, \ldots, u_{n-1}) \longmapsto F(u_1, \ldots, u_{n-1}, u_n) \tag{s1}$$

is obviously $k$-$(n-1)$-quadratic. Hence by the induction hypothesis, it has a unique $R$-$(n-1)$-quadratic extension

$$(F_{u_n})_R\colon M_{1R} \times \cdots \times M_{n-1,R} \longrightarrow M_R.$$

Now let $x_i \in M_{iR}$ be arbitrary for $1 \le i < n$ and put $x := (x_1, \ldots, x_{n-1})$. We claim that *the map*

$$F_x\colon M_n \longrightarrow M_R, \quad u_n \longmapsto F_x(u_n) := (F_{u_n})_R(x). \tag{s2}$$

*is $k$-quadratic*. In order to see this, we put

$$V := \mathrm{Quad}(M_1, \ldots, M_{n-1}; M)$$

and conclude from (s1) that the map $Q\colon M_n \to V$, $u_n \mapsto F_{u_n}$ is $k$-quadratic. On the other hand, (s2) implies $F_x(u_n) = Q(u_n)_R(x)$, so $F_x$ is $Q$ composed with two $k$-linear maps: the natural map

$$\mathrm{Quad}(M_1, \ldots, M_{n-1}; M) \longrightarrow \mathrm{Quad}(M_{1R}, \ldots, M_{n-1,R}; M_R), \quad G \longmapsto G_R,$$

given and $k$-linear by the induction hypothesis, and the evaluation at $x$. This proves our claim.

By Cor. 11.5 we therefore obtain an $R$-quadratic map

$$(F_x)_R\colon M_{nR} \longrightarrow (M_R)_R := M \otimes R \otimes R,$$

which composes with the $R$-linear map

$$\mu\colon M \otimes R \otimes R \longrightarrow M \otimes R = M_R, \quad u \otimes r \otimes s \longmapsto u \otimes rs \tag{s3}$$

to yield a map $F_R\colon M_{1R} \times \cdots \times M_{n-1,R} \times M_{nR} \to M_R$ via

$$F_R(x_1, \ldots, x_{n-1}, x_n) := \mu((F_{x_1,\ldots,x_{n-1}})_R(x_n)) \tag{s4}$$

for $x_i \in M_{iR}$, $1 \le i \le n$. By construction, $F_R$ is $R$-quadratic in $x_n$. Hence,

writing $x_n = \sum r_l u_{lnR}$, $r_l \in R$, $u_{ln} \in M_n$, we obtain, after a straightforward computation,

$$(F_R)_{x_n} = \sum r_l^2 (F_{u_{ln}})_R + \sum_{l<m} r_l r_m ((F_{u_{ln}+u_{mn}})_R - (F_{u_{ln}})_R - (F_{u_{mn}})_R),$$

which shows that the left-hand side of (s4) is $R$-quadratic in $x_i$, $1 \leq i < n$. Thus $F_R$ is an $R$-$n$-quadratic map. Next we show that (1) commutes. Indeed, given $u_i \in M_i$, $1 \leq i \leq n$, we apply (s4), Cor. 11.5, (s3), (s2), the induction hypothesis and (s1) to obtain

$$\begin{aligned} F_R(u_{1R}, \ldots, u_{n-1,R}, u_{nR}) &= \mu((F_{u_{1R},\ldots,u_{n-1,R}})_R(u_{nR})) = \mu\Big((F_{u_{1R},\ldots,u_{n-1,R}}(u_n))_R\Big) \\ &= F_{u_{1R},\ldots,u_{n-1,R}}(u_n) = (F_{u_{nR}})_R(u_{1R}, \ldots, u_{n-1,R}) \\ &= F_{u_n}(u_1, \ldots, u_{n-1})_R = F(u_1, \ldots, u_{n-1}, u_n)_R, \end{aligned}$$

and commutativity of (1) is proved.

It remains to establish uniqueness. Let $G, H\colon M_{1R} \times \cdots \times M_{nR} \to M_R$ be $R$-$n$-quadratic maps both rendering the diagram

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{F} & M \\ {\scriptstyle \text{can}}\downarrow & & \downarrow{\scriptstyle \text{can}} \\ M_{1R} \times \cdots \times M_{nR} & \xrightarrow[G,H]{} & M_R. \end{array} \tag{s5}$$

commutative. For $u_n \in M_n$, using obvious notation, both

$$G_{u_{nR}}, H_{u_{nR}}\colon M_{1R} \times \cdots \times M_{n-1,R} \longrightarrow M_R$$

are $R$-$(n-1)$-quadratic maps rendering the diagram

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{F} & M \\ {\scriptstyle \text{can}}\downarrow & & \downarrow{\scriptstyle \text{can}} \\ M_{1R} \times \cdots \times M_{nR} & \xrightarrow[G_{u_{nR}}, H_{u_{nR}}]{} & M_R. \end{array}$$

commutative. From the uniqueness part of the induction hypothesis, we therefore conclude $G_{u_{nR}} = H_{u_{nR}}$. Now let $x_i \in M_{iR}$ for $1 \leq i \leq n$ and write

$x_n = \sum r_l u_{nlR}$, $r_l \in R$, $u_{ln} \in M_n$. Then what we have just shown implies

$$\begin{aligned} G(x_1, \dots, x_{n-1}, x_n) = & \sum r_l^2 G(x_1, \dots, x_{n-1}, u_{nlR}) + \sum_{l<m} (G(x_1, \dots, x_{n-1}, u_{lnR} + u_{mnR}) \\ & - G(x_1, \dots, x_{n-1}, u_{lnR}) - G(x_1, \dots x_{n-1}, u_{mnR})) \\ = & \sum r_l^2 G_{u_{nlR}}(x_1, \dots, x_{n-1}) + \sum_{l<m} (G_{(u_{ln}+u_{mn})_R}(x_1, \dots, x_{n-1}) \\ & - G_{u_{lnR}}(x_1, \dots, x_{n-1}) - G_{u_{mnR}}(x_1, \dots, x_{n-1}) \\ = & H(x_1, \dots, x_{n-1}, x_n) \end{aligned}$$

This proves uniqueness and completes the induction. Finally, a straightforward verification using uniqueness of $F_R$ shows that the assignment $F \mapsto F_R$ is $k$-linear.

**11.36** We first assume that $M$ is free and let $(e_i)_{i\in I}$ be a basis of $M$. By the Axiom of Choice, we may choose a well-ordering on $I$. Let $B\colon M \times M \to N$ be the unique bilinear map from $M$ to $N$ given by the values

$$B(e_i, e_j) = \begin{cases} Q(e_i) & \text{for } i = j \in I, \\ Q(e_i, e_j) & \text{for } i, j \in I, i < j, \\ 0 & \text{for } i, j \in I, i > j \end{cases}$$

on the basis vectors. Then, for any $x = \sum \xi_i e_i \in M$, $\xi_i \in k$, we have

$$\begin{aligned} B(x, x) = B(\sum \xi_i e_i, \sum \xi_i e_i) = & \sum_{i,j\in I} \xi_i \xi_j B(e_i, e_j) \\ = & \sum \xi_i^2 Q(e_i) + \sum_{i<j} \xi_i \xi_j Q(e_i, e_j) = Q(x), \end{aligned}$$

as claimed. Now let $M$ be an arbitrary projective module. Then there exists a $k$-module $M'$ making $M_0 := M \oplus M'$ free. Let $Q'\colon M' \to N$ be the zero quadratic map on $M'$ with values in $N$ and consider the quadratic map $Q_0\colon M_0 \to N$ canonically induced by $Q$ and $Q'$. By the special case just treated we find a bilinear map $B_0\colon M_0 \times M_0 \to N$ such that $Q_0(x_0) = B_0(x_0, x_0)$ for all $x_0 \in M_0$. But this implies $Q(x) = B(x, x)$ for all $x \in M$, where $B\colon M \times M \to N$ is the restriction of $B_0$ to $M \times M$.

**11.37** (i) $\Rightarrow$ (iv) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (ii). If $x \in V$ satisfies $q(x) = q(x, y) = 0$ for all $y \in V$, then by linearity $x_K \in V_K$ satisfies $(q_K)(x_K) = (q_K)(x_K, y') = 0$ for all $y' \in V_K$, and (iii) gives $x_K = 0$, hence $x = 0$. Thus $q$ is non-degenerate, and it remains to show $\dim_F(\mathrm{Rad}(Dq)) \le 1$. Since the radical of a symmetric or skew-symmetric bilinear form *over a field* is compatible with base change, it suffices to show

$\dim_K(\mathrm{Rad}(Dq_K)) \leq 1$. But $q_K$ is non-degenerate by hypothesis, so its restriction to $\mathrm{Rad}(Dq_K)$ is anisotropic. On the other hand, $K$ being algebraically closed, all quadratic forms of (possibly infinite) dimension $> 1$ over $K$ are isotropic. The assertion follows.

(ii) $\Rightarrow$ (i). By hypothesis, there exists an element $u \in V$ satisfying $\mathrm{Rad}(Dq) = Fu$, and if $u \neq 0$, then $q(u) \neq 0$ since $q$ is non-degenerate. Now let $L$ be any field containing $F$. Then $\mathrm{Rad}(Dq_L) = Lu_L$. If $x' \in V_L$ satisfies $(q_L)(x') = (q_L)(x', y') = 0$ for all $y' \in V_L$ then, in particular, $x' \in \mathrm{Rad}(Dq_L) = Lu_L$, so some $a \in L$ has $x' = a(u_L)$. This implies $0 = q_L(x') = a^2 q(u)$, hence $a = 0$ or $q(u) = 0$, which in turn yields $a = 0$ or $u = 0$, hence $x' = 0$. Therefore $q_L$ is non-degenerate, and $q$ is non-singular.

**11.38** (a) Let $x \in V$. The assertion is obvious if $x = 0$ or $x$ is anisotropic. Hence we may assume that $x$ is isotropic. Then there is a hyperbolic plane $H \subseteq V$ containing $x$, and the assumption $n \geq 3$ implies that $H^\perp \neq \{0\}$ is a quadratic space in its own right. Let $y \in H^\perp$ be anisotropic. Then so are $-y$ and $x + y$, and $x = (x + y) - y$ is a decomposition of the desired kind.

(b) We may assume $q(x_1, x_2) = 0$. Let $H \subseteq V$ be a hyperbolic subspace of dimension 4. By hypothesis, $q$ is regular and isotropic, hence universal, on $H^\perp \neq \{0\}$. There are two cases, depending on $x_1$ and $x_2$ are linearly dependent.

Suppose first that $x_1$ and $x_2$ are linearly dependent. Then $x_2 = \alpha x_1$ for some $\alpha \in F^\times$, and we are in characteristic 2. The Witt Extension Theorem [14, Thm. 8.3] allows us to assume $x_1 \in H$. Pick $y_1 \in H$ such that $q(x_1, y_1) \neq 0$, and $y_3 \in H^\perp$ such that $y := y_1 + y_3 \in V$ is anisotropic. Then $q(x_1, y \neq 0 \neq q(y, x_2)$.

Suppose now that $x_1$ and $x_2$ are linearly independent. Write $H = H_1 \perp H_2$ with hyperbolic planes $H_1, H_2$. Since $q$ is universal on each of the subspaces $H_1, H_2$, the Witt Extension Theorem again justifies the assumption $x_i \in H_i$ for $i = 1, 2$. Pick $y_i \in H_i$ such that $q(x_i, y_i) \neq 0$ for $i = 1, 2$ and $y_3 \in H^\perp$ such that $y := y_1 + y_2 + y_3$ is anisotropic. Then $q(x_1, y) = q(x_1, y_1) \neq 0 \neq q(y_2, x_2) = q(y, x_2)$, as desired.

We now show that *in* (a) *the assumption $n \geq 3$ cannot be avoided.* Indeed, let $(V, q)$ be the hyperbolic plane over $\mathbb{F}_2$, the field with two elements. $V$ contains precisely two isotropic vectors relative to $q$, denoted by $e_1, e_2$, which form a hyperbolic pair, and precisely one anisotropic one, denoted by $a = e_1 + e_2$. Hence any finite sum of anisotropic vectors in $(V, q)$ is either zero or equal to $a$, so neither $e_1$ nor $e_2$ can be written in this form.

Finally, we show that *in* (b) *the assumption of a hyperbolic subspace of dimension at least 6 cannot be avoided.* Indeed, with $(V, q)$ as in the previous paragraph, put $(W, Q) = (V, q) \perp (V, q)$. Then $W$ contains precisely four anisotropic vectors relative to $Q$, namely $(a, e_i)$, $(e_j, a)$ for $i, j = 1, 2$. More-

over, $Q((a,e_i),(a,e_j)) = 1-\delta_{ij}$ and $Q((a,e_i),(e_j,a)) = 0$. Hence $x_1 := (a,e_1)$ and $x_2 := (e_1,a)$ are anisotropic as well as orthogonal, and there is a unique anisotropic vector $y \in W$ satisfying $Q(x_1,y) \neq 0$, namely, $y = (a,e_2)$. But $Q(y,x_2) = 0$, so the conclusion of (b) does not hold.

**11.39** Suppose first that $k$ is local, i.e., has a unique maximal ideal $\mathfrak{m}$. Then $M \cong k^n$ for some $n$ and $Dq$ is identified with a symmetric $S \in \mathrm{Mat}_n(k)$. By hypothesis, $q_{k(\mathfrak{m})}$ is non-singular, so by the remark after Exc. 11.37 it is regular. Therefore $\det S$ is not zero in $k/\mathfrak{m}$, i.e., $\det S$ is invertible in $k$ and the map $M \to M^*$ induced by $Dq$ is an isomorphism.

For general $k$, the map $M \to M^*$ induced by $Dq$ has the property that it is an isomorphism after base change to $k_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of $k$, so it is an isomorphism by [7, II.3, Thm. 1].

**11.40** (a): For each $v \in \mathrm{Rad}(Dq)$, we have $q(v) = \frac{1}{2}Dq(v,v) = 0$.

(b): Replace $(M,q)$ with $(M',q|_{M'})$ and so assume that $M$ is free of finite rank, $Dq$ is identically zero, and $q$ is anisotropic. Pick a basis $m_1,\dots,m_r$ of $M$ and define $\alpha_i := q(m_i)$. Then for $c_1,\dots,c_r \in k$ we have $q(\sum c_i m_i) = \sum q(c_i m_i) = c_i^2\alpha_i$, as required. Finally, if $\alpha_i = \alpha_j\beta^2$ for some $i \neq j$ and $\beta \in k^\times$, then $q(m_i+\beta m_j) = \alpha_i + \alpha_j\beta^2 = 0$, whence $m_i + \beta m_j = 0$, a contradiction.

**11.41** (i): We may identify each $x \in \mathrm{Hom}_{k\text{-}\mathbf{mod}}(M/\mathrm{Rad}(q), \mathrm{Rad}(q))$ with an element of $\mathrm{Hom}_{k\text{-}\mathbf{mod}}(M,M)$ by composing it with the natural maps $M \to M/\mathrm{Rad}(q)$ and $\mathrm{Rad}(q) \to M$. For such an $x$, define $g_x := x + \mathbf{1}_M \in \mathrm{Hom}_{k\text{-}\mathbf{mod}}(M,M)$. Then, for $m \in M$,

$$q(g_x(m)) = q(m+x(m)) = q(m) + q(x(m)) + q(m,x(m)) = q(m),$$

so $q \circ g_x = q$.

Also, $x \in \mathrm{Hom}_{k\text{-}\mathbf{mod}}(M,M)$ vanishes on $\mathrm{Rad}(q)$ so $x^2 = 0$ and we have $g_x(\mathbf{1}_M - x) = \mathbf{1}_M - x^2 = \mathbf{1}_M$ and similarly $(\mathbf{1}_M - x)g_x = \mathbf{1}_M$. That is, $g_x$ is invertible, so it belongs to $\mathrm{O}(Q)$.

Evidently the map $x \mapsto g_x$ is injective. For $x,y \in \mathrm{Hom}_{k\text{-}\mathbf{mod}}(M,\mathrm{Rad}(q))$, we have $g_x g_y = g_{xy+x+y}$, so the image $R$ of $\mathrm{Hom}_{k\text{-}\mathbf{mod}}(M,\mathrm{Rad}(q))$ in $\mathrm{O}(Q)$ is a subgroup.

For $\eta \in \mathrm{O}(Q)$ and $m \in M$, we have

$$\eta g_x \eta^{-1}(m) = \eta x \eta^{-1}(m) + m = g_{\eta x \eta^{-1}}(m),$$

so $R$ is a normal subgroup.

(ii): Every $\eta \in \mathrm{O}(Q)$ maps $\mathrm{Rad}(q)$ to itself, whence restriction gives a well-defined homomorphism $\phi$. Now suppose that $\eta \in \mathrm{Ker}\,\phi$ and set $x := \eta - \mathbf{1}_M$. Since $\eta$ maps to the identity in $\mathrm{O}(\overline{Q})$, it follows that $\eta m - m \in \mathrm{Rad}(q)$ for all $m \in$

$M$, i.e., $x\colon M \to \mathrm{Rad}(q)$. Since $\eta$ maps to the identity in $\mathrm{GL}(\mathrm{Rad}(q))$, it follows that for $m \in \mathrm{Rad}(q)$ we have $xm = \eta m - m = 0$. That is, $x\colon M/\mathrm{Rad}(q) \to \mathrm{Rad}(q)$ and $\eta$ is in $R$.

(iii): The quotient map $M \to M/\mathrm{Rad}(q)$ identifies the quadratic module $(M', q|_{M'})$ with $(M/\mathrm{Rad}(q), \overline{q})$, providing a recipe that takes an element of $\mathrm{GL}(\mathrm{Rad}(q))\times\mathrm{O}(\overline{Q})$ and identifies it with an element of $\mathrm{GL}(\mathrm{Rad}(q))\times\mathrm{O}(M', q|_{M'}) \subseteq \mathrm{O}(Q)$. This shows that the map $\phi$ is surjective.

**11.42** We first claim: *If a ring $k$ is LG, then for every $c \in k$ the polynomial $x^2 + c$ represents a unit.* By the LG property, it suffices to verify this in case $k$ is a field. In that case: If $c \neq -1$, take $x = 1$. If $c = -1$, take $x = 0$.

(a): For $k = \mathbb{Z}$, take $f = x^2 + 2$. Then for every $z \in \mathbb{Z}$, $f(z) = z^2 + 2 \geq 2$, so $f(z)$ is not a unit. The previous paragraph shows that $\mathbb{Z}$ is not LG.

(b): For $k = R[\mathbf{t}]$, we have $k^\times = R^\times$ since $R$ is an integral domain. Then $x^2 + \mathbf{t}$ represents polynomials of degree $\geq 1$, hence non-units, and we again conclude that $k$ is not LG.

**Extension.** Part (b) of this exercise can be generalized in the following way. *Suppose $k$ is a ring with a discrete valuation $v$. If there exists an element $c \in k$ such that $v(c)$ is odd and negative, then $k$ is not an LG ring.*

A discrete valuation on a ring $k$ is defined in [9, §VI.3.1, Def. 1]. It is a $v\colon k \to \mathbb{Z} \cup \{\infty\}$ such that following axioms hold for all $x, y \in k$:

(I) $v(xy) = v(x) + v(y)$.
(II) $v(x + y) \geq \min\{v(x), v(y)\}$.
(III) $v(1) = 0$ and $v(0) = \infty$.

For such a $v$, we have equality in (II) if $v(x) \neq v(y)$ [9, §VI.3.1, Prop. 1].

The italicized claim generalizes part (b) by taking the valuation to be $v(f) = -\deg f$ (the "$1/\mathbf{t}$-adic valuation") and $c = \mathbf{t}$, which has $v(c) = -1$.

*Proof* Assume $c \in k$ has $v(c)$ odd and negative. Assume further for some $x \in k$ that $x^2 + c$ is a unit. Since $v(x^2) = 2v(x)$ is even and hence distinct from $v(c)$, we conclude $0 = v(x^2 + c) = \min\{2v(x), v(c)\}$, which cannot be $v(c)$ since this is negative, hence must be $2v(x)$, forcing the minimum in question to be $0 = v(c)$, a contradiction. □

## Solutions for Section 12

**12.30** Setting $\mathbf{T} = (\mathbf{t}_1, \dots, \mathbf{t}_n)$ as usual, $x = (x_1, \dots, x_n)$, $y = (x_{n+1}, \dots, x_{n+p})$, $x_i \in M_R$ for $1 \le i \le n+p$ and applying Thm. 12.9, we obtain

$$\begin{aligned}\sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu(\Pi^{(\nu,0)}f)_R(x,y) &= \sum_{(\nu,\nu')\in\mathbb{N}^{n+p}} \mathbf{t}_1^{\nu_1}\cdots\mathbf{t}_n^{\nu_n}0^{\nu_{n+1}}\cdots 0^{\nu_{n+p}}(\Pi^{(\nu,\nu')}f)_R(x,y)\\ &= f_{R[\mathbf{T}]}\Big(\sum_{i=1}^n \mathbf{t}_i x_i + \sum_{i=1}^p 0x_{n+i}\Big) = f_R\Big(\sum_{i=1}^n \mathbf{t}_i x_i\Big)\\ &= \sum_{\nu\in\mathbb{N}^n} \mathbf{T}^\nu(\Pi^\nu f)_R(x),\end{aligned}$$

and comparing coefficients, the assertion follows.

**12.31** For $d \in \mathbb{N}$ define $f_d := \Pi^{(d)}f$, which by Thm. 12.9 and 12.10 (a) is a homogeneous polynomial law $M \to N$ of degree $d$ over $k$. Moreover, the family $(f_d)_{d\ge0}$ is locally finite, and (12.9.1) for $n = 1$, $r_1 = 1_R$ implies $f = \sum_{d\ge0} f_d$. This proves existence. Conversely, let $(f_d)_{d\ge0}$ be any family of polynomial laws over $k$ with the desired properties. For $R \in k\text{-}\mathbf{alg}$, $r \in R$, $x \in M_R$ we deduce

$$f_R(rx) = \sum_{d\ge0} f_{dR}(rx) = \sum_{d\ge0} r^d f_{dR}(x),$$

and the uniqueness property of Thm. 12.9 yields $f_d = \Pi^{(d)}f$ for all $d \in \mathbb{N}$. This shows uniqueness and solves the first part of the problem.

It remains to exhibit an example of a polynomial law $f$ having $f_d \ne 0$ for all $d \in \mathbb{N}$. To this end, consider a free $k$-module $M$ of countably infinite rank and let $(e_i)_{i\in\mathbb{N}}$ be a basis of $M$ over $k$. For $d \in \mathbb{N}$ and $R \in k\text{-}\mathbf{alg}$, define a set map $f_{dR}\colon M_R \to R$ by

$$f_{dR}\Big(\sum_{i\in\mathbb{N}} r_i e_{iR}\Big) := r_d^d,$$

where $(r_i)_{i\in\mathbb{N}}$ is an arbitrary sequence of finite support in $R$. The family $(f_{dR})_{R\in k\text{-}\mathbf{alg}}$ is clearly a homogeneous polynomial law $f_d\colon M \to k$ of degree $d$ over $k$, and the family $(f_d)_{d\ge0}$ is locally finite. Hence, by 12.8, $f := \sum_{d\ge0} f_d\colon M \to k$ exists as a polynomial law over $k$ and has the desired property.

**12.32** The family of set maps $\hat{w}_R\colon M_R \to N_R$ for $w \in N$ clearly varies functorially with $R \in k\text{-}\mathbf{alg}$ and hence is a polynomial law $\hat{w}\colon M \to N$ such that $\hat{w}_R(rx) = w_R = r^0\hat{w}_R(x)$ for all $r \in R$, $x \in M_R$. Thus $\hat{w}$ is homogeneous of degree 0. Conversely, let $f\colon M \to N$ be any homogeneous polynomial law of degree 0 over $k$. Then $w := f_k(0) \in N$, and for all $R \in k\text{-}\mathbf{alg}$, $x \in M_R$, we apply

(12.2.2) to obtain $w_R = f_k(0)_R = f_R(0) = f_R(0x) = 0^0 f_R(x) = f_R(x)$, hence $\hat{w}_R = f_R$ and then $\hat{w} = f$.

**12.33** (a) The first part is obvious. To establish the second, we begin by treating the case $n = 1$, so let $f\colon M \to N$ be a homogeneous polynomial law of degree 1. Then 12.10 (c) implies $\Pi^\nu f = 0$ for all $\nu \in \mathbb{N}^2 \setminus \{(1,0),(0,1)\}$, and (12.14.1) yields

$$f_k(\alpha x + \beta y) = \alpha(\Pi^{(1,0)} f)_k(x,y) + \beta(\Pi^{(0,1)} f)_k(x,y)$$

for all $\alpha, \beta \in k$ and all $x, y \in M$. Specializing $\alpha = 1$, $\beta = 0$ and $\alpha = 0$, $\beta = 1$, we conclude $(\Pi^{(1,0)} f)_k(x,y) = f_k(x)$, $(\Pi^{(0,1)} f)_k(x,y) = f_k(y)$. Hence $f_k\colon M \to N$ is a $k$-linear map. Since $f \otimes R\colon M_R \to N_R$, for $R \in k$-**alg**, is a homogeneous polynomial law of degree 1 over $R$, it follows, therefore, that $f_R\colon M_R \to N_R$ is an $R$-linear map. Moreover, for $r \in R$, $x \in M$, we deduce $f_R(x \otimes r) = f_R(rx_R) = r f_R(x_R) = r f_k(x)_R = f_k(x) \otimes r = (f_k \otimes \mathbf{1}_R)(x \otimes r)$, hence $f_R = (f_k)_R$. Thus $f$ is the polynomial law derived from the scalar extensions of the linear map $f_k$. This settles the case $n = 1$.

Now let $n$ be arbitrary and $\mu\colon M_1 \times \cdots \times M_n \to N$ be a multi-homogeneous polynomial law of multi-degree $\hat{1} = (1, \ldots, 1)$. For $1 \le i \le n$ and fixed $v_j \in M_j$ $(1 \le j \le n,\ j \ne i)$, it is straightforward to verify, using (12.6.1), that $f_i\colon M_i \to N$ defined by

$$f_{iR}(x) := \mu_R(v_{1R}, \ldots, v_{i-1,R}, x, v_{i+1,R}, \ldots, v_{nR})$$

for $R \in k$-**alg**, $x \in M_R$, is a homogeneous polynomial law of degree 1. Therefore, by the special case treated above, $f_{ik}\colon M_i \to N$ is a $k$-linear map, forcing $\mu_k\colon M_1 \times \cdots \times M_n \to N$ to be $k$-multi-linear. Applying this to the extended polynomial law $\mu \otimes R\colon M_{1R} \times \cdots \times M_{nR} \to N_R$ over $R$, we conclude that $\mu_R\colon M_{1R} \times \cdots \times M_{nR} \to N_R$ is an $R$-multi-linear map. Hence, given $r_{ij} \in R$, $v_{ij} \in M_j$ for $1 \le j \le n$ and finitely many indices $i$, we obtain

$$\begin{aligned}\mu_R\Big(\sum_i r_{i1} v_{i1R}, \ldots, \sum_i r_{in} v_{inR}\Big) &= \sum_{i_1,\ldots,i_n} r_{i_1 1} \cdots r_{i_n n} \mu_k(v_{i_1 1}, \ldots, v_{i_n n})_R \\ &= (\mu_k \otimes R)\Big(\sum_i r_{i1} v_{i1R}, \ldots, \sum_i r_{in} v_{inR}\Big).\end{aligned}$$

This proves $\mu_R = \mu_k \otimes R$ and completes the solution of (a).

(b) Let $Q\colon M \to N$ be a quadratic map. We show that $\tilde{Q}\colon M \to N$ is a polynomial law over $k$ by letting $\varphi\colon R \to S$ be a morphism in $k$-**alg** and $x, x' \in$

$M, r, r' \in R$. The Cor. 11.5 implies

$$\begin{aligned}(\mathbf{1}_N \otimes \varphi) \circ Q_R(x \otimes r) &= (\mathbf{1}_N \otimes \varphi) \circ Q_R(rx_R) = (\mathbf{1}_N \otimes \varphi)(r^2 Q(x)_R) = (\mathbf{1}_N \otimes \varphi)(Q(x) \otimes r^2)\\ &= Q(x) \otimes \varphi(r)^2 = \varphi(r)^2 Q(x)_S = \varphi(r)^2 Q_S(x_S)\\ &= Q_S(\varphi(r)x_S) = Q_S(x \otimes \varphi(r)) = Q_S \circ (\mathbf{1}_M \otimes \varphi)(x \otimes r)\end{aligned}$$

and, similarly, $(\mathbf{1}_N \otimes \varphi) \circ Q_R(x \otimes r, x' \otimes r') = Q_S \circ (\mathbf{1}_M \otimes \varphi)(x \otimes r, x' \otimes r')$. This proves that $\tilde{Q}$ is indeed a polynomial law over $k$ and obviously homogeneous of degree 2. Conversely, let $f\colon M \to N$ be a homogeneous polynomial law of degree 2 over $k$ and consider the set map $Q := f_k\colon M \to N$. By 12.10 (c) and (12.14.1), we have

$$Q(\alpha x + \beta y) = \alpha^2(\Pi^{(2,0)}f)_k(x, y) + \alpha\beta(\Pi^{(1,1)}f)_k(x, y) + \beta^2(\Pi^{(0,2)}f)_k(x, y)$$

for all $\alpha, \beta \in k$ and all $x, y \in M$. After specializing $\alpha = 1, \beta = 0$ and $\alpha = 0$, $\beta = 1$ and observing (12.16.1), this may be rewritten as

$$Q(\alpha x + \beta y) = \alpha^2 Q(x) + \alpha\beta(Df)_k(x, y) + \beta^2 Q(y),$$

where $(Df)_k = (\Pi^{(1,1)}f)_k$ is $k$-bilinear by 12.10 (a) and (a). This shows that $Q$ is a quadratic map with $DQ = (Df)_k$. For $R \in k$-**alg**, the $R$-quadratic map $Q_R\colon M_R \to N_R$ is uniquely determined by (11.5.1), which proves $Q_R = f_R$, hence $\tilde{Q} = f$.

**12.34** (a) Applying Thm. 12.9, we deduce

$$\begin{aligned}&\sum_{\nu_1,\dots,\nu_p \geq 0} \mathbf{t}_1^{\nu_1} \cdots \mathbf{t}_p^{\nu_p} \Big( \sum_{\nu_{p+1},\dots,\nu_n \geq 0} \mathbf{t}_{p+1}^{\nu_{p+1}} \cdots \mathbf{t}_n^{\nu_n} (\Pi^{(\nu_1,\dots,\nu_n)}f)_R(x_1, \dots, x_p, x, \dots, x) \Big)\\ &\quad = \sum_{\nu \in \mathbb{N}^n} \mathbf{T}^\nu (\Pi^\nu f)(x_1, \dots, x_p, x, \dots, x) = f_{R[\mathbf{T}]}\Big( \sum_{j=1}^{p} \mathbf{t}_j x_j + \big( \sum_{j=p+1}^{n} \mathbf{t}_j \big) x \Big)\\ &\quad = \sum_{\nu_1,\dots,\nu_p,\nu_{p+1} \geq 0} \mathbf{t}_1^{\nu_1} \cdots \mathbf{t}_p^{\nu_p} \big( \sum_{j=p+1}^{n} \mathbf{t}_j \big)^{\nu_{p+1}} (\Pi^{(\nu_1,\dots,\nu_p,\nu_{p+1})}f)_R(x_1, \dots, x_p, x)\\ &\quad = \sum_{\nu_1,\dots,\nu_p \geq 0} \mathbf{t}_1^{\nu_1} \cdots \mathbf{t}_p^{\nu_p} \Big( \sum_{i \geq 0} \big( \sum_{j=p+1}^{n} \mathbf{t}_j \big)^i (\Pi^{(\nu_1,\dots,\nu_p,i)}f)_R(x_1, \dots, x_p, x) \Big).\end{aligned}$$

Comparing coefficients and using the multi-nomial formula (Abramowitz-Segun

[1, p. 823]), this implies, for all $\nu_1, \dots, \nu_p \in \mathbb{N}$,

$$\begin{aligned}
&\sum_{\nu_{p+1},\dots,\nu_n \geq 0} \mathbf{t}_{p+1}^{\nu_{p+1}} \cdots \mathbf{t}_n^{\nu_n} (\Pi^{(\nu_1,\dots,\nu_n)} f)_R(x_1, \dots, x_p, x, \dots, x) \\
&\quad = \sum_{i \geq 0} \Big( \sum_{j=p+1}^{n} \mathbf{t}_j \Big)^i (\Pi^{(\nu_1,\dots,\nu_p,i)} f)_R(x_1, \dots, x_p, x) \\
&\quad = \sum_{i \geq 0} \Big( \sum_{\nu_{p+1},\dots,\nu_n \geq 0, \nu_{p+1}+\cdots+\nu_n = i} \frac{i!}{\nu_{p+1}! \cdots \nu_n!} \mathbf{t}_{p+1}^{\nu_{p+1}} \cdots \mathbf{t}_n^{\nu_n} (\Pi^{(\nu_1,\dots,\nu_p,i)} f)_R(x_1, \dots, x_p, x) \Big) \\
&\quad = \sum_{\nu_{p+1},\dots,\nu_n \geq 0} \mathbf{t}_{p+1}^{\nu_{p+1}} \cdots \mathbf{t}_n^{\nu_n} \frac{(\nu_{p+1} + \cdots + \nu_n)!}{\nu_{p+1}! \cdots \nu_n!} (\Pi^{(\nu_1,\dots,\nu_p,\nu_{p+1}+\cdots+\nu_n)} f)_R(x_1, \dots, x_p, x),
\end{aligned}$$

and comparing coefficients again completes the proof of (a).

(b) Let $\varphi\colon R \to S$ be a morphism in $k$-**alg** and $x \in M_R$. Since $D^p f$ is a polynomial law over $k$, an application of (12.6.2) yields

$$\begin{aligned}
(\partial_y^{[p]} f)_S \circ (\mathbf{1}_M \otimes \varphi)(x) &= (D^p f)_S((\mathbf{1}_M \otimes \varphi)(x), y_S) = (D^p f)_S((\mathbf{1}_M \otimes \varphi)(x), (\mathbf{1}_M \otimes \varphi)(y_R)) \\
&= (D^p f)_S \circ (\mathbf{1}_{M\times M} \otimes \varphi)(x, y_R) = (\mathbf{1}_N \otimes \varphi) \circ (D^p f)_R(x, y_R) \\
&= (\mathbf{1}_N \otimes \varphi) \circ (\partial_y^{[p]})_R(x).
\end{aligned}$$

Thus $\partial_y^{[p]} f$ is a polynomial law over $k$ and the map $\partial_y^{[p]}\colon \operatorname{Pol}_k(M,N) \to \operatorname{Pol}_k(M,N)$ is clearly $k$-linear.

Next combine Prop. 12.21 for $y_1 = \cdots = y_p = y$ with (a) to conclude

$$\begin{aligned}
((\partial_y)^p f)_R(x) = (\partial_y \cdots \partial_y f)_R(x) &= \sum_{i \geq 0} (\Pi^{(i,1,\dots,1)} f)_R(x, y_R, \dots, y_R) = p! \sum_{i \geq 0} (\Pi^{(i,p)} f)_R(x, y_R) \\
&= p!(D^p f)_R(x, y_R) = p!(\partial_y^{[p]} f)_R(x),
\end{aligned}$$

which implies $(\partial_y)^p = p!\partial_y^{[p]}$ as linear maps $\operatorname{Pol}_k(M,N) \to \operatorname{Pol}_k(M,N)$. This completes the solution of (b).

(c) Let $R \in k$-**alg**, $\mathbf{t}, \mathbf{t}_1, \mathbf{t}_2$ be independent variables and $\mathbf{T} = (\mathbf{t}_1, \mathbf{t}_2)$. For $x, y_1, y_2 \in M_R$ we combine the Taylor expansion formula (12.15.3) with Thm. 12.9 and obtain

$$\begin{aligned}
\sum_{n \geq 0} \mathbf{t}^n (D^n f)_{R[\mathbf{T}]}(x, \mathbf{t}_1 y_1 + \mathbf{t}_2 y_2) &= f_{R[\mathbf{t},\mathbf{T}]}(x + \mathbf{t}(\mathbf{t}_1 y_1 + \mathbf{t}_2 y_2)) = f_{R[\mathbf{t},\mathbf{T}]}(x + (\mathbf{t}\mathbf{t}_1) y_1 + (\mathbf{t}\mathbf{t}_2) y_2) \\
&= \sum_{\nu_0,\nu_1,\nu_2 \geq 0} 1^{\nu_0} (\mathbf{t}\mathbf{t}_1)^{\nu_1} (\mathbf{t}\mathbf{t}_2)^{\nu_2} (\Pi^{(\nu_0,\nu_1,\nu_2)} f)_R(x, y_1, y_2) \\
&= \sum_{\nu_1,\nu_2 \geq 0} \mathbf{t}^{\nu_1+\nu_2} \mathbf{t}_1^{\nu_1} \mathbf{t}_2^{\nu_2} \sum_{i \geq 0} (\Pi^{(i,\nu_1,\nu_2)} f)_R(x, y_1, y_2) \\
&= \sum_{n \geq 0} \mathbf{t}^n \sum_{j=0}^{n} \mathbf{t}_1^j \mathbf{t}_2^{n-j} \sum_{i \geq 0} (\Pi^{(i,j,n-j)} f)_R(x, y_1, y_2)
\end{aligned}$$

Comparing coefficients of $\mathbf{t}^n$, we therefore end up with the formula

$$(D^n f)_{R[\mathbf{T}]}(x, \mathbf{t}_1 y_1 + \mathbf{t}_2 y_2) = \sum_{j=0}^{n} \mathbf{t}_1^j \mathbf{t}_2^{n-j} \sum_{i\geq 0} (\Pi^{(i,j,n-j)} f)_R(x, y_1, y_2) \tag{s1}$$

This formula will now be applied in the special case $n = 2$. From Exc. 12.30 combined with 12.10 (b) we deduce, for all $i \in \mathbb{N}$,

$$\begin{aligned}(\Pi^{(i,2,0)} f)_R(x, y_1, y_2) &= (\Pi^{(i,2)} f)_R(x, y_1),\\ (\Pi^{(i,0,2)} f)_R(x, y_1, y_2) &= (\Pi^{(i,2,0)} f)_R(x, y_2, y_1) = (\Pi^{(i,2)} f)_R(x, y_2).\end{aligned}$$

Hence (s1) for $n = 2$ implies

$$\begin{aligned}(D^2 f)_{R[\mathbf{T}]}(x, \mathbf{t}_1 y_1 + \mathbf{t}_2 y_2) &= \mathbf{t}_1^2 \sum_{i\geq 0} (\Pi^{(i,2)} f)_R(x, y_1) + \mathbf{t}_1 \mathbf{t}_2 \sum_{i\geq 0} (\Pi^{(i,1,1)} f)_R(x, y_1, y_2)\\ &\quad + \mathbf{t}_2^2 \sum_{i\geq 0} (\Pi^{(i,2)} f)_R(x, y_2)\\ &= \mathbf{t}_1^2 (D^2 f)_R(x, y_1) + \mathbf{t}_1 \mathbf{t}_2 \sum_{i\geq 0} (\Pi^{(i,1,1)} f)_R(x, y_1, y_2) + \mathbf{t}_2^2 (D^2 f)_R(x, y_2).\end{aligned}$$

In particular, applying Prop. 12.21,

$$\begin{aligned}(\partial^{[2]}_{y+z} f)_R(x) &= (D^2 f)_R(x, y_R + z_R)\\ &= (D^2 f)_R(x, y_R) + \sum_{i\geq 0} (\Pi^{(i,1,1)} f)_R(x, y_R, z_R) + (D^2 f)_R(x, z_R)\\ &= \Big((\partial^{[2]}_y f)_R + (\partial_y \partial_z f)_R + (\partial^{[2]}_z f)_R\Big)(x),\end{aligned}$$

which completes the proof of (c).

**12.35** (a) Let $R \in K$-**alg** and $x \in V_R$. We must show $f_R(x) = 0$. To this end, pick $K$-bases $(v_i)_{i\in I}$ of $V$, $(w_j)_{j\in J}$ of $W$. and write

$$x = \sum_{i\in I} r_i v_{iR}, \quad f_R(x) = \sum_{j\in J} s_j w_{jR} \tag{s1}$$

with $r_i, s_j \in R$, $i \in I$, $j \in J$. Then

$$I_0 := \{i \in I \mid r_i \neq 0\} \subseteq I, \quad J_0 := \{j \in J \mid s_j \neq 0\} \subseteq J$$

are finite subsets, forcing

$$V_0 := \sum_{i\in I_0} K v_i \subseteq V, \quad W_0 := \sum_{j\in J_0} K w_j \subseteq W \tag{s2}$$

to be finite-dimensional subspaces of $V, W$, respectively. Writing $\varepsilon_0 \colon V_0 \to V$ for the inclusion and $\pi_0 \colon W \to W_0$ for the projection along $\sum_{j\notin J_0} K w_j$,

$$f_0 := \pi_0 \circ f \circ \varepsilon_0 \colon V_0 \longrightarrow W_0$$

is a polynomial law over $K$ such that $f_{0K} = \pi_{0K} \circ f_K \circ \varepsilon_{0K} = 0$ as a set map from $V_0$ to $W_0$. Since $V_0$ and $W_0$ are both finite-dimensional, we conclude from Corollary 12.13 that $f_0 = 0$ as a polynomial law over $K$. On the other hand, $x \in V_{0R}$, $f_R(x) \in W_{0R}$ by (s1), (s2), which implies $f_R(x) = f_{0R}(x) = 0$, as claimed.

(b) By (a) we may assume $f_K \neq 0$ and must show $\varphi_K = 0$. Let $(v_i)_{i\in I}$, $(w_j)_{j\in J}$ be $K$-bases of $V, W$, respectively, and choose $x \in V$ such that

$$f_K(x) \neq 0. \tag{s3}$$

Write

$$x = \sum_{i\in I} \alpha_i v_i, \quad f_K(x) = \sum_{j\in J} \beta_j w_j \qquad (\alpha_i, \beta_j \in K, i \in I, j \in J). \tag{s4}$$

For any $y \in V$, we have

$$y = \sum_{i\in I} \gamma_i v_i, \quad f_K(y) = \sum_{j\in J} \delta_j w_j \qquad (\gamma_i, \delta_j \in K, i \in I, j \in J) \tag{s5}$$

and must show $\varphi_K(y) = 0$. Consider the finite subsets

$$I_0 := \{i \in I \mid \alpha_i \neq 0 \text{ or } \gamma_i \neq 0\} \subseteq I, \quad J_0 := \{j \in J \mid \beta_j \neq 0\} \subseteq J,$$

making

$$V_0 := \sum_{i\in I_0} Kv_i, \quad W_0 = \sum_{j\in J_0} Kw_j \tag{s6}$$

finite-dimensional subspaces of $V, W$, respectively, such that

$$x, y \in V_0, \quad f_K(x) \in W_0. \tag{s7}$$

Writing as before $\varepsilon_0 \colon V_0 \to V$ for the inclusion and $\pi_0 \colon W \to W_0$ for the projection along $\sum_{j\notin J_0} Kw_j$, it follows that $f_0 := \pi_0 \circ f \circ \varepsilon_0 \colon V_0 \to W_0$ is a polynomial law over $K$ having $f_{0K}(x) \neq 0$; in particular, $f_{0K} \neq 0$. On the other hand, $\varphi_0 := \varphi \circ \varepsilon_0 \colon V_0 \to K$ is a scalar polynomial law over $K$, and one checks that $(\varphi_0 f_0)_K = 0$, which implies $\varphi_{0K}(z_0) = 0$ for all $z_0 \in V_0$ having $f_{0K}(z_0) \neq 0$. But Corollary 12.13 guarantees that $f_{0K} \colon V_0 \to W_0$ is a non-zero polynomial map. By Zariski density, therefore, we obtain $\varphi_K(z_0) = \varphi_{0K}(z_0) = 0$ for all $z_0 \in V_0$; in particular, (s7) yields $\varphi_K(y) = 0$, as desired.

**12.36** (a) $f = 0$ clearly implies $f_\mathfrak{p} := f \otimes k_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Before proving the converse, we show

(∗) If $f_{k_\mathfrak{p}} = 0$ as a set map $M_\mathfrak{p} \to N_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$, then $f_k = 0$ as a set map $M \to N$.

Indeed, by the very definition of a polynomial law, the diagram

$$\begin{array}{ccc} M & \xrightarrow{f_k} & N \\ {\scriptstyle \mathrm{can_M}}\downarrow & & \downarrow{\scriptstyle \mathrm{can_N}} \\ M_\mathfrak{p} & \xrightarrow[f_{k_\mathfrak{p}}=0]{} & N_\mathfrak{p} \end{array}$$

commutes for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Hence for all $x \in M$ we have $f_k(x)/1 = 0$ in $N_\mathfrak{p}$, which means $s_\mathfrak{p} f_k(x) = 0$ for some $s_\mathfrak{p} \in k \setminus \mathfrak{p}$. It follows that the ideal generated by the $s_\mathfrak{p}$, $\mathfrak{p} \in \operatorname{Spec}(k)$, is all of $k$, since it cannot be contained in any prime ideal of $k$. Thus there exists a family $(\alpha_\mathfrak{p})_{\mathfrak{p}\in\operatorname{Spec}(k)}$ with finite support such that $\sum_\mathfrak{p} \alpha_\mathfrak{p} s_\mathfrak{p} = 1$. But this implies $f_k(x) = \sum \alpha_\mathfrak{p} s_\mathfrak{p} f_k(x) = 0$, and (∗) is proved.

Now assume $f_\mathfrak{p} = 0$ as a polynomial law $M_\mathfrak{p} \to N_\mathfrak{p}$ over $k_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Let $R \in k$-**alg** and $\mathfrak{P} \in \operatorname{Spec}(R)$. Then $\mathfrak{p} := i^{-1}(\mathfrak{P}) \in \operatorname{Spec}(k)$, where $i$ stands for the unit homomorphism $k \to R$, and we derive from (9.5.6) the commutative diagram

$$\begin{array}{ccc} k & \xrightarrow{i} & R \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}_R} \\ k_\mathfrak{p} & \xrightarrow[j]{} & R_\mathfrak{P} \end{array}$$

with a local homomorphism $j$ of local $k$-algebras, making $R_\mathfrak{P}$ a $k_\mathfrak{p}$-algebra compatible with its $k$-algebra structure. Since $f_\mathfrak{p} = 0$ as a polynomial law $M_\mathfrak{p} \to N_\mathfrak{p}$ over $k_\mathfrak{p}$ by hypothesis, we therefore conclude $(f_R)_{R_\mathfrak{P}} = f_{R_\mathfrak{P}} = (f_\mathfrak{p})_{R_\mathfrak{P}} = 0$ as a set map $(M_R)_\mathfrak{P} \to (N_R)_\mathfrak{P}$. Now (∗) for $R$ in place of $k$ and $f_R$ in place of $f$ shows $f_R = 0$ as a set map $M_R \to N_R$.

(b) We must show that the conjunction of (i) $f_k = 0$ and (ii) $D^p f = 0$ for $1 \le p \le \lfloor \frac{d}{2} \rfloor$ implies $f = 0$. For $d = 0, 1$, condition (ii) is void, so we must show that $f_k = 0$ implies $f = 0$. But this is clear since $f$ for $d = 0$ is a constant polynomial law (Exc. 12.32), while for $d = 1$ it is basically a linear map (Exc. 12.33 (a)). We may therefore assume $d \ge 2$. In order to prove $f = 0$, it suffices to show, by Corollary 12.11, that $(\Pi^\nu f)_k = 0$ for all $\nu \in \mathbb{N}^n$, $n \in \mathbb{Z}$, $n > 0$. By 12.10 (c), we may assume $|\nu| = d$. For $n = 1$, we therefore have $\nu = d$, and (12.9.2) for $R = k$ and $n = 1$ yields $(\Pi^d f)_k = f_k = 0$. For $n > 1$, we put

$$m := \max\{i \in \mathbb{Z} \mid 1 \le i \le n,\ \nu_i \ne 0\}.$$

Hence $\nu = (\mu, 0, \dots, 0)$, $\mu = (\nu_1, \dots, \nu_m)$, and if $m < n$, then Exc. 12.30 implies $(\Pi^\nu f)_R(x, y) = (\Pi^\mu f)_R(x)$ for all $R \in k$-**alg**, $x \in M_R^m$, $y \in M_R^{n-m}$. We are thus reduced to the case $\nu_n \ne 0$. Simplifying notation, we conclude $\nu = (\varrho, p)$ for

some $\varrho \in \mathbb{N}^{n-1}$, $p \in \mathbb{N}$ having $p \geq 1$ and $|\varrho| + p = n$. Applying 12.10 (b) with an appropriate permutation, we may assume $1 \leq p \leq \lfloor \frac{d}{2} \rfloor$. Now Lemma 12.19 combined with $D^p f = 0$ yields

$$0 = (D^p f)_{k[\mathbf{T}]}(\sum_{i=1}^{n-1} \mathbf{t}_i x_i, x_n) = \sum_{\lambda \in \mathbb{N}^{n-1}} \mathbf{T}^\lambda (\Pi^{(\lambda,p)} f)_k(x_1, \ldots, x_{n-1}, x_n)$$

for all $x_1, \ldots, x_{n-1}, x_n \in M$. Applying (12.4.1), we conclude $(\Pi^{(\lambda,p)} f)_k = 0$ for all $\lambda \in \mathbb{N}^{n-1}$. Specializing $\lambda$ to $\varrho$, we obtain $(\Pi^\nu f)_k = 0$, as claimed.

**12.37** Let $F \in k$-**alg** be a field. By hypothesis, $f_F(m_F) = f_k(m)_F \in N$ is unimodular, hence not zero. Since $f_F(0) = f_k(0)_F = 0$, we conclude $m_F \neq 0$, whence $m \in M$ is unimodular (Lemma 9.17).

**12.38** (a) Let $m \in M_R$ be nonzero, so $m = \sum_{j \geq j_0} m_j \mathbf{t}^j$ for some $j_0 \geq 0$ with $m_{j_0} \neq 0$.

Suppose that $j_0 = 0$. Then the homomorphism $R \to k$ defined by sending $\mathbf{t} \mapsto 0$ sends $m \mapsto m_0$ and $f_R(m) \mapsto f(m_0)$. Since $f$ does not represent zero on $M$, $f(m_0) \neq 0$, whence $f_R(m) \neq 0$ and indeed $f_R(m)$ has lowest degree term $f(m_0)t^0$.

Suppose $j_0 > 0$. Then

$$f_R(m) = f_R(t^{j_0}(mt^{-j_0})) = t^{d j_0}(f(m_{j_0})t^0 + \cdots),$$

proving the claim.

(b) Suppose there is a nonzero $m \in M$ such that $f_k(m) = 0$. Because $M$ is torsion-free, $m \otimes 1$ is not zero in $M_R$ [7, II.2, Prop. 4] and $f_R(m \otimes 1) = f_k(m) \otimes 1_R = 0$.

Conversely, suppose $f_R$ represents zero. Then by combining denominators, there is a nonzero $m \in M$ and $s \in S$ such that $f_R(m \otimes 1/s) = 0$. Whence

$$0 = (1 \otimes s^{-d}) f_R(m \otimes 1) = (1 \otimes s^{-d})(f_k(m) \otimes 1),$$

and $f_k(m) \otimes 1 = 0$ in $R$. Since $S$ contains no zero divisors, $f_k(m) = 0$.

(c): By hypothesis, there is a nonzero $m \in M$ such that $f_k(m) = 0$. Identify $M = k^r$ for some $r \in \mathbb{N}$. The ideal of $k$ generated by the coordinates $m_i$ of $m$ for all $i$ is generated by a $g \neq 0$, and $g$ divides $m_i$ in $k$ for all $i$. Defining $m' \in M$ via $gm'_i = m_i$ for each $i$, we find that $gm' = m$ and the coordinates of $m'$ generate the unit ideal in $k$ so $m'$ is unimodular. Finally, $0 = f_k(m) = g^d f_k(m')$, whence $f_k(m') = 0$.

**12.39** The argument is similar to that of Exercise 12.38 (a). Put $v$ for the value function on $R$, so in particular $v(\pi) = 1$. If $M$ is a finitely generated free $R$-module, then the unimodular elements are exactly those $m \in M$ whose image

$\bar{m} \in M \otimes k$ is not zero. With respect to a basis of $M$, the unimodular elements are the ones with at least one coordinate in $R^\times$. For any nonzero $m \in M$, we have $m = \pi^e m'$ for uniquely determined $e \geq 0$ and $m' \in M$ unimodular.

For $m \in M_i$, if $\bar{m} \in M_i \otimes k$ is not zero, then $\overline{f_i(m)} = \overline{f_i}(\bar{m}) \neq 0$, whence $v(f_i(m)) = 0$. Otherwise, if $m \neq 0$, because $M_i$ is free and finitely generated it can be written as $m = \pi^e m'$ for some $e > 0$ and $m' \in M$ whose image in $M \otimes k$ is not zero. Then $f_i(m) = \pi^{de} f_i(m')$, so $v(f_i(m)) = de$. In summary, for all $m \in M_i$, $v(f_i(m))$ is divisible by $d$. (If $m = 0$, then $f_i(m) = 0$ and $v(f_i(m)) = \infty$, which is divisible by $d$.) Note that this argument shows that $f_i$ does not represent zero.

To prove the claim, pick $m_i \in M_i$ for all $i$ such that $m := \sum m_i$ is not zero. By the preceding paragraph, $v(\pi^i f_i(m_i)) = i + v(f_i(m_i)) \equiv i \mod d$. Since these represent distinct residue classes mod $d$, the one of smallest valuation, call it $i_0$, is the only one with that valuation. It follows that $v(m) = i_0 + v(f_{i_0}(m_{i_0}))$, the value of the smallest term. In particular, $\sum_i \pi^i f_i(m_i) \neq 0$.

**12.40** By (12.16.1) we have $D^2 f = \Pi^{(1,2)} f$, and (12.10.1) implies $(D^2 f)(x, y) = \Pi^{(1,2)} f)(x, y) = (\Pi^{(2,1)} f)(y, x) = (Df)(y, x)$, hence

$$f(y, x) = (D^2 f)(x, y). \tag{s1}$$

Combining (12.16.2) for $d = 3$ with (12.15.3) and (1), (s1), we obtain (2). In order to derive (3), we first let $x, y \in M$. Then (s1), Exc. 12.34 (c) and Prop. 12.21 imply

$$\begin{aligned} f(x + y, z) &= (D^2 f)(z, x + y) = (\partial^{[2]}_{x+y} f)(z) \\ &= (\partial^{[2]}_x f)(z) + (\partial_x \partial_y f)(z) + (\partial^{[2]}_y f)(z) \\ &= (D^2 f)(z, x) + (\Pi^{(1,1,1)} f)(x, y, z) + (D^2 f)(z, y) \\ &= f(x, z) + f(x, y, z) + f(y, z), \end{aligned}$$

as claimed. The general case $x, y \in M_R$ now follows by looking at $f \otimes R$ rather than $f$. Combining (2) for $\mathbf{t} = 1$ and (3), we now obtain

$$\begin{aligned} f(x + y + z) &\; - f(x + y) - f(y + z) - f(z + x) + f(x) + f(y) + f(z) \\ &= f(x + y) + f(x + y, z) + f(z, x + y) + f(z) - f(x + y) - f(y) - f(y, z) \\ &\quad - f(z, y) - f(z) - f(z) - f(z, x) - f(x, z) - f(x) + f(x) + f(y) + f(z) \\ &= f(x, z) + f(x, y, z) + f(y, z) + f(z, x) + f(z, y) + f(z) - f(y) - f(y, z) - f(z, y) \\ &\quad - f(z) - f(z) - f(z, x) - f(x, z) - f(x) + f(x) + f(y) + f(z) \\ &= f(x, y, z), \end{aligned}$$

and this is (4). Before dealing with (5), we prove

$$f(\sum_{i=1}^{n} r_i x_i, x) = \sum_{i=1}^{n} r_i^2 f(x_i, x) + \sum_{1\le i<j\le n} r_i r_j f(x_i, x_j, x) \tag{s2}$$

for $x \in M_R$ by induction on $n$. For $n = 1$ there is nothing to prove. For $n > 1$, the induction hypothesis and (3) imply

$$\begin{aligned} f(\sum_{i=1}^{n} r_i x_i, x) &= f(\sum_{i=1}^{n-1} r_i x_i, x) + f(\sum_{i=1}^{n-1} r_i x_i, r_n x_n, x) + f(r_n x_n, x) \\ &= \sum_{i=1}^{n-1} r_i^2 f(x_i, x) + \sum_{1\le i<j<n} r_i r_j f(x_i, x_j, x) + \sum_{i=1}^{n-1} r_i r_n f(x_i, x_n, x) + r_n^2 f(x_n, x) \\ &= \sum_{i=1}^{n} r_i^2 f(x_i, x) + \sum_{1\le i<j\le n} r_i r_j f(x_i, x_j, x), \end{aligned}$$

as claimed. Now we can prove (5), again by induction on $n$. The case $n = 1$ again being obvious, let us assume $n > 1$ and that (5) holds for $n - 1$. Then this and (s2) yield

$$\begin{aligned} f(\sum_{i=1}^{n} r_i x_i) &= f(\sum_{i=1}^{n-1} r_i x_i) + f(\sum_{i=1}^{n-1} r_i x_i, r_n x_n) + f(r_n x_n, \sum_{i=1}^{n-1} r_i x_i) + f(r_n x_n) \\ &= \sum_{i=1}^{n-1} r_i^3 f(x_i) + \sum_{1\le i,j<n, i\ne j} r_i^2 r_j f(x_i, x_j) + \sum_{1\le i<j<l<n} r_i r_j r_l f(x_i, x_j, x_l) \\ &\quad + \sum_{i=1}^{n-1} r_i^2 r_n f(x_i, x_n) + \sum_{1\le i<j<n} r_i r_j r_n f(x_i, x_j, x_n) + \sum_{j=1}^{n-1} r_n^2 r_j f(x_n, x_j) + r_n^3 f(x_n) \\ &= \sum_{i=1}^{n} r_i^3 f(x_i) + \sum_{1\le i,j\le n, i\ne j} r_i^2 r_j f(x_i, x_j) + \sum_{1\le i<j<l\le n} r_i r_j r_l f(x_i, x_j, x_l). \end{aligned}$$

This completes the induction and the proof of (a).

(b) (i) $\Rightarrow$ (ii). From (i) we deduce $g_F(e_i) = 0$ for $1 \le i \le n$, while (4) implies $g_F(x, y, z) = 0$ for all $x, y, z \in F^n$. Moreover, from Euler's differential equation (12.16.3 we conclude $g_F(x, x) = (Dg)_F(x, x) = 3g_F(x) = 0$. It remains to show that $F$ consists of two elements and $g_F(x_0, y_0) \ne 0$ for some $x_0, y_0 \in F^n$. Replacing $f$ by $g$ and specializing $\mathbf{t} \mapsto \alpha \in F^\times$ in (2), we conclude $g_F(x, y) + \alpha g_F(y, x) = 0$. Assuming $|F| > 2$, this implies $g_F(x, y) = 0$ for all $x, y \in F^n$. But If $g_F(x, y) = 0$ for all $x, y \in F^n$, then (6) and (5) for $g$ in place of $f$ and $e_{iR}$ in place of $x_i$ for $1 \le i \le n$ would lead to the contradiction $g = 0$ as a polynomial law over $F$. Thus (ii) holds.

(ii) ⇒ (iii). By (6) and (s2) for $g$ in place of $f$, the map $F^n \times F^n \to F$, $(x, y) \mapsto g_F(x, y)$ is an alternating $F$-bilinear form, forcing

$$S := (g_F(e_i, e_j))_{1\le i,j\le n} \in \mathrm{Mat}_n(F)$$

to be an alternating matrix and $S \neq 0$ by (ii). Now let

$$x = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \sum_{i=1}^{n} r_i e_{iR} \in R^n = (F^n)_R \qquad (r_1, \dots, r_n \in R).$$

Then (5) and (6) imply

$$\begin{aligned} g_R(x) = g_R(\sum_{i=1}^{n} r_i e_{iR}) &= \sum_{i=1}^{n} r_i^3 g_F(e_i) + \sum_{1\le i,j\le n, i\neq j} r_i^2 r_j g_F(e_i, e_j) + \sum_{1\le i<j<l\le n} r_i r_j r_l g_F(e_i, e_j, e_l) \\ &= \sum_{1\le i,j\le n} r_i g_F(e_i, e_j) r_j^2 = x^{\mathsf{T}} S\, x^2, \end{aligned}$$

as claimed.

(iii) ⇒ (i). Since $F \cong \mathbb{F}_2$ consists of two elements, the elements of $F^n$ as an $F$-algebra are all idempotents. Hence $g_F(x) = x^{\mathsf{T}} S\, x = 0$ for all $x \in F^n$, whence the set map $g_F \colon F^n \to F$ is identically zero. On the other hand, since $S \neq 0$, there are elements $x_0, y_0 \in F^n$ such that $x_0^{\mathsf{T}} S\, y_0 \neq 0$, and passing from $F \cong \mathbb{F}^2$ to the separable quadratic extension $K = F(\theta) \cong \mathbb{F}_4$ with $\theta \in K$ satisfying $\theta^2 = \theta + 1$, we deduce

$$\begin{aligned} g_K(x_0 + \theta y_0) &= (x_0 + \theta y_0)^{\mathsf{T}} S\, (x_0^2 + \theta^2 y_0^2) \\ &= (x_0 + \theta y_0)^{\mathsf{T}} S\, (x_0 + \theta^2 y_0) = (x_0 + \theta y_0)^{\mathsf{T}} S\, (x_0 + \theta y_0) + (x_0 + \theta y_0)^{\mathsf{T}} S\, y_0 \\ &= x_0^{\mathsf{T}} S\, y_0 \neq 0. \end{aligned}$$

Thus $g_K \neq 0$, so $g \colon F^n \to F$ is a non-zero cubic form.

**12.41** Identifying $V \subseteq V_K$ canonically and picking a basis $(1, \xi)$ of $K$ as a vector space over $F$, we have $V_K = V \oplus \xi V$ as a direct sum of $F$-subspaces. Arguing indirectly, we assume that $f \otimes K$ does represent zero. Then $f_K(v + \xi w) = 0$ for some $v, w \in V$ not both zero. If $w = 0$, then $f_F(v) = 0$, hence $v = 0$ (since $f$ does not represenr zero), a contradiction. Thus $w \neq 0$ and then $f_F(w) \neq 0$. Consulting eqn. (2) of Exc. 12.40, we conclude that $\mu := f_{F[\mathbf{t}]}(v + \mathbf{t}w) \in F[\mathbf{t}]$ is a cubic polynomial having the root $\xi$ in $K$ but no root in $F$ (since $f_F$ is does not represent zero). Thus $\mu$ is irreducible and hence the minimum polynomial of $\xi$. On the other hand, the minimum polynomial of any element in the quadratic field extension $K$ of $F$ has degree at most 2. This contradiction proves our claim.

**12.42** Passing to $R[\varepsilon]$, $\varepsilon^4 = 0$, the Taylor expansion (12.15.4) yields

$$\begin{aligned}(D^0(g\circ f))(x,y)+\ &\varepsilon(D(g\circ f))(x,y)+\varepsilon^2(D^2(g\circ f))(x,y)+\varepsilon^3(D^3(g\circ f))(x,y)\\ &= (g\circ f)(x+\varepsilon y)\\ &= g(f(x)+\varepsilon(Df)(x,y)+\varepsilon^2(D^2f)(x,y)+\varepsilon^3(D^3f)(x,y))\\ &= g(f(x))+\varepsilon(Dg)(f(x),(Df)(x,y)+\varepsilon(D^2f)(x,y)+\varepsilon^2(D^3f)(x,y))\\ &\quad+\varepsilon^2(D^2g)(f(x),(Df)(x,y)+\varepsilon(D^2f)(x,y)+\varepsilon^2(D^3f)(x,y))\\ &\quad+\varepsilon^3(D^3g)(f(x),(Df)(x,y)+\varepsilon(D^2f)(x,y)+\varepsilon^2(D^3f)(x,y)).\end{aligned}$$

Comparing coefficients of $\varepsilon^3$ by combining (1) with (5) of Exercise 12.40, the assertion follows.

**12.43** (a) If $f\colon M\to N$ and $f'\colon M'\to N'$ are polynomial laws over $k$, a *morphism* from $f$ to $f'$ in $k$-**polaw** is defined as a pair of linear maps $\varphi\colon M\to M'$, $\psi\colon N\to N'$ making a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M' & \xrightarrow[f']{} & N' \end{array} \tag{s1}$$

of polynomial laws over $k$.

(b) Since $g$ is quadratic in the first variable, the expression $g(x,y,z)$ is surely trilinear. Moreover, for $x,y,z\in M$, we repeatedly use condition (iii) to compute

$$\begin{aligned}f(x+y+z)-\ &f(x+y)-f(y+z)-f(z+x)+f(x)+f(y)+f(z)\\ &= g(x+y,z)+g(z,x+y)+f(z)-f(y)-g(y,z)-g(z.y)-f(z)\\ &\quad -f(z)-g(z,x)-g(x,z)-f(x)+f(x)+f(y)+f(z)\\ &= g(x,y,z),\end{aligned}$$

and since the very left-hand side is totally symmetric in $x,y,z$, so is the right. This proves the first part of (a). As to the second, (3) follows immediately by linearizing $g(y,x)=0$ for $x\in\mathrm{Rad}(f,g)$ with respect to $y\in M$ and using the total symmetry of (1). Hence (iii) implies that $\mathrm{Rad}(f,g)$ is a submodule of $M$. Finally, for a linear map $\pi$ as indicated, the maps $f_1\colon M_1\to N$ and $g_1\colon M_1\times M_1\to N$ given by $f_1(\pi(x)):=f(x)$ and $g_1(\pi(x),\pi(y)):=g(x,y)$, respectively, for $x,y\in M$ in view of (2) are well-defined, and it is straightforward to check that $(f_1,g_1)\colon M_1\to N_1$ is a cubic map with the desired properties. This completes the proof of (c).

(c) Combining (iii) with the fact that $g$ is quadratic-linear, (4) follows by a straightforward induction. (4) and the commutativity of (5) immediately imply

uniqueness of the $R$-cubic extension. To prove its existence, let $R \in k$-**alg** and assume first that $M$ is a free $k$-module, with basis $(e_i)_{i\in I}$. Write $g_R\colon M_R \times M_R \to N_R$ for the $R$-quadratic-linear extension of $g$ in the sense of Exercise 11.34. In the spirit of (4), we define a set map $f_R\colon M_R \to N_R$ by

$$f_R(\sum_{i\in I} r_i e_{iR}) := \sum_i r_i^3 f(e_i)_R + \sum_{i\neq j} r_i^2 r_j g(e_i, e_j)_R + \sum_{|i<j<l} r_i r_j r_l g(e_i, e_j, e_l)_R \quad \text{(s2)}$$

for all families $(r_i)_{i\in I}$ with finite support in $R$. Putting $x := \sum r_i e_{iR}$, $y := \sum s_i e_{iR}$ with another such family $(s_i)_{i\in I}$, we obtain

$$g_R(x, y) = \sum_{i,l} r_i^2 s_l g(e_i, e_l)_R + \sum_{i<j,l} r_i r_j r_l g(e_i, e_j, e_l)_R, \quad \text{(s3)}$$

and using (s2), (s3), (iv), one checks that $(f, g)_R := (f_R, g_R)$ is indeed an $R$-cubic extension of $(f, g)$.

Now assume that $M$ is arbitrary. Since the functor $- \otimes R$ is right exact, we obtaina commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow[i]{} & M' & \xrightarrow[\pi]{} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{can}} & & \\ & & L_R & \xrightarrow[i_R]{} & M'_R & \xrightarrow[\pi_R]{} & M_R & \longrightarrow & 0 \end{array} \quad \text{(s4)}$$

of $k$- (resp. $R$-)modules, with exact rows and $M$ a free $k$-module. By the special case just treated, the cubic map

$$(f', g') := (f \circ \pi, g \circ (\pi \times \pi))\colon M' \longrightarrow N \quad \text{(s5)}$$

over $k$ extends to a cubic map

$$(f', g')_R := (f'_R, g'_R)\colon M'_R \longrightarrow N_R \quad \text{(s6)}$$

over $R$. We claim

$$\mathrm{Ker}(\pi_R) \subseteq \mathrm{Rad}\,((f', g')_R). \quad \text{(s7)}$$

Exactness of the second row in (s4) implies that any element of $\mathrm{Ker}(\pi_R)$ can be written as $i_R(z)$, for some $z = \sum r_j u_{jR} \in L_R$, $r_j \in R$, $u_j \in L$. Applying (4) to $(f', g')_R$, we conclude

$$\begin{aligned} f'_R(i_R(z)) &= f'_R(\sum r_j i(u_j)_R) \\ &= \sum_j r_j^3 f'(i(u_j))_R + \sum_{j\neq l} r_j^2 r_l g'(i(u_j), i(u_l))_R + \sum_{j<l<m} r_j r_l r_m g'(i(u_j), i(u_l), i(u_m))_R, \end{aligned}$$

where (s6) implies $f'(i(u_j)) = (f \circ \pi \circ i)(u_j) = 0$, $g'(i(u_j), i(u_l)) = g((\pi \circ i)(u_j)$,

$(\pi \circ i)(u_l)) = 0$ and, similarly, $g'(i(u_j), i(u_l), i(u_m)) = 0$. Since $g'$ is $R$-quadratic-linear, we also have $g'_R(i_R(z), y) = g'_R(y, i_R(z)) = 0$ for all $y \in M$. Summing up, we conclude $i_R(z) \in \mathrm{Rad}((f', g')_R)$, and (s7) follows. By (c), therefore, we find a cubic map

$$(f, g)_R := (f_R, g_R) \colon M_R \longrightarrow N \tag{s8}$$

over $R$ such that

$$f_R \circ \pi_R = f'_R, \quad g_R \circ (\pi_R \times \pi_R) = g'_R. \tag{s9}$$

Since $\pi$ and $\pi_R$ are both surjective, one checks that (5) commutes, so $(f, g)_R$ is indeed an $R$-cubic extension of $(f, g)$.

(d) If $(f, g) \colon M \to N$ and $(f', g') \colon M' \to N'$ are cubic maps over $k$, a *morphism* from $(f, g)$ to $(f', g')$ in $k$-**cumap** is defined as a pair of linear maps $\varphi \colon M \to M', \psi \colon N \to N'$ making commutative diagrams

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M' & \xrightarrow[f']{} & N', \end{array} \qquad \begin{array}{ccc} M \times M & \xrightarrow{g} & N \\ {\scriptstyle\varphi\times\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M' \times M' & \xrightarrow[g']{} & N' \end{array} \tag{s10}$$

of set maps.

Now let $f \colon M \to N$ be a homogeneous polynomial law of degree 3 over $k$. We combine equations (2), (3) of Exc. 12.40 with Euler's differential equation (12.16.3) to conclude that $(f_k, (Df)_k)$ is a cubic map from $M$ to $N$. If $(\varphi, \psi) \colon f \to f'$ is a morphism in $k3$-**holaw**, then the chain rules (12.17.4), (12.17.5) applied to the commutative diagram (s1) show that $(\varphi, \psi)$ is also a morphism from $(f_k, (Df)_k)$ to $(f'_k, (Df')_k)$ in $k$-**cumap**. Thus we have obtained a functor from $k3$-**holaw** to $k$-**cumap**.

Conversely, let $(f, g) \colon M \to N$ be a cubic map over $k$. We claim that *the family of set maps*

$$(f * g)_R := f_R \colon M_R \longrightarrow N_R \tag{s11}$$

*defined for $R \in k$-**alg** as the first component of the $R$-cubic extension of $(f, g)$ is a polynomial law over $k$.* Indeed, given a morphism$\varphi \colon R \to S$ in $k$-**alg**, we replace $f$ by $f_R$ and $R$ by $S$ in (5), observe $(f_R)_S = f_S$ and conclude from (9.4.2) that (12.2.1) commutes, as desired. Note that the polynomial law $f * g \colon M \to N$ by definition is homogeneous of degree 3, hence an object of the category $k3$-**holaw**. If $(\varphi, \psi) \colon (f, g) \to (f', g')$ is a morphism of cubic maps $(f, g) \colon M \to N$, $(f', g') \colon M' \to N'$ over $k$, one checks that $f'_R(\varphi(x_R)) = \psi_R(f_R(x_R))$, $g'_R(\varphi_R(x_R), \varphi(y_R)) = \psi_R(g_R(x_R, y_R))$ for all $R \in k$-**alg**,

$x, y \in M$, and we conclude from (s11) that $(\varphi_R, \psi_R)\colon (f,g)_R \to (f',g')_R$ is a morphism of cubic maps over $R$. Hence $(\varphi,\psi)\colon f * g \to f' * g'$ is a morphism in $k3$-**holaw**., thus defining a functor from $k$-**cumap** to $k3$-**holaw**. It remains to show that the two functors are inverse to one another. Let $f\colon M \to N$ be a homogeneous poynomial law of degree 3 over $k$. For $R \in k$-**alg**, the diagrams

$$\begin{array}{ccc} M & \xrightarrow{f_k} & N \\ {\scriptstyle\text{can}}\downarrow & & \downarrow{\scriptstyle\text{can}} \\ M_R & \xrightarrow[f_R]{} & N_R, \end{array} \qquad \begin{array}{ccc} M\times M & \xrightarrow{(Df)_k} & N \\ {\scriptstyle\text{can}}\downarrow & & \downarrow{\scriptstyle\text{can}} \\ M_R\times M_R & \xrightarrow[(Df)_R]{} & N_R \end{array}$$

commute, and we conclude $f_R = (f_k)_R$, $(Df)_R = ((Df)_k)_R$, so $(f_R, (Df)_R)$ is the $R$-cubic extension of $(f_k, (Df)_k)$. Hence $f_k * (Df)_k = f$ as polynomial laws over $k$. Conversely, let $(f,g)\colon M \to N$ be a cubic map over $k$ and write $R := k[\varepsilon]$, $\varepsilon^2 = 0$, for the $k$-algebra of dual numbers. Since $g$ is quadratic-linear, condition (iii) in the definition of a cubic map implies

$$f_R(x_1 + \varepsilon x_2) = f(x_1 + \varepsilon g(x_1, x_2))$$

for all $x_1, x_2 \in M$, and comparing with the Taylor expansion (12.15.5) we conclude $((f*g)_k, (D(f*g))_k) = (f,g)$. This completes the proof.

**12.44** Arguing as in the solution to Exercise 11.36, we first assume that $M$ is free, let $(e_i)_{i\in I}$ be a basis of $M$, and choose a total order on $I$. By Exercise 12.43 (d), we may write $F = f * g$, where $(f,g)\colon M \to N$ is a cubic map in the sense of Exercise 12.43. Let $T\colon M\times M\times M \to N$ be the unique trilinear map from $M\times M\times M$ to $N$ given by the values

$$T(e_i,e_j,e_l) = \begin{cases} f(e_i) & \text{for } i=j=l\in I, \\ g(e_i,e_l) & \text{for } i,j,l\in I, i=j\neq l, \\ g(e_i,e_j,e_l) & \text{for } i,j,l\in I, i<j<l, \\ 0 & \text{otherwise} \end{cases}$$

on the basis vectors. Then, for any $x = \sum \xi_i e_i \in M$, $\xi_i \in k$, we have

$$\begin{aligned} T(x,x,x) &= T\Big(\sum \xi_i e_i, \sum \xi_i e_i, \sum \xi_i e_i\Big) = \sum_{i,j,l\in I} \xi_i\xi_j\xi_l T(e_i,e_j,e_l) \\ &= \sum_{i\in I} \xi_i^3 T(e_i,e_i,e_i) + \sum_{i,l\in I, i\neq l} \xi_i^2\xi_l \big(T(e_i,e_i,e_l) + T(e_i,e_l,e_i) + T(e_l,e_i,e_i)\big) \\ &\quad + \sum_{i,j,l\in I, i<j<l} \xi_i\xi_j\xi_l \big(T(e_i,e_j,e_l) + T(e_j,e_l,e_i) + T(e_l,e_i,e_j) \\ &\quad + T(e_j,e_i,e_l) + T(e_i,e_l,e_j) + T(e_l,e_j,e_i)\big) \end{aligned}$$

$$= \sum \xi_i^3 f(e_i) + \sum_{i\neq j} g(e_i, e_j) + \sum_{i<j<l} \xi_i\xi_j\xi_l g(e_i, e_j, e_l) = f(\sum \xi_i e_i)$$

by Exercise (12.43.4) Since the identification $F = f * g$ is compatible with base change, the assertion follows if $M$ is free. Now let $M$ be an arbitrary projective module. Then there exists a $k$-module $M'$ making $M_0 := M \oplus M'$ free. Let $F'\colon M' \to N$ be the zero polynomial law on $M'$ with values in $N$ and consider the homogeneous polynomial law $F_0\colon M_0 \to N$ of degree 3 canonically induced by $F$ and $F'$. By the special case just treated we find a trilinear map $T_0\colon M_0 \times M_0 \times M_0 \to N$ such that $F_0(x_0) = T_0(x_0, x_0, x_0)$ for all $x_0 \in M_{0R}$, $R \in k$-**alg**. But this implies $F(x) = T(x, x, x)$ for all $x \in M_R$, where $T\colon M \times M \times M \to N$ is the restriction of $T_0$ to $M \times M \times M$.

**12.45** Let $f\colon M \to N$ be a polynomial law over $K$. Letting $S \in K$-**alg** and setting $R := {}_kS$, the map $\mathbf{1}_S\colon R \to S$ is a morphism of $k$-algebras, giving rise to a *surjective* morphism $\varphi\colon R_K \to S$ of $K$-algebras and hence, in view of (12.27.1), to a commutative diagram with exact columns

$$\begin{array}{ccc}
({}_kM)_R & \xrightarrow[({}_kf)_R]{} & ({}_kN)_R \\
\downarrow{\scriptstyle \mathbf{1}_M\otimes\varphi} & & \downarrow{\scriptstyle \mathbf{1}_N\otimes\varphi} \\
M_S & \xrightarrow[f_S]{} & N_S \\
\downarrow & & \downarrow \\
0 & & 0,
\end{array}$$

which shows that $f_S$ is uniquely determined by $({}_kf)_R$, so $f$ is uniquely determined by ${}_kf$, as claimed.

**12.46** Let $R \in k$-**alg**.

(a) Using (12.27.4), we obtain $(g \circ f)_R = (g \circ f)_{R_K} = (g_{R_K}) \circ (f_{R_K}) = ({}_kg)_R \circ ({}_kf)_R = ({}_kg \circ {}_kf)_R$.

(b) For $r, r_i \in R$, $x_i \in M$, we recall $({}_kN)_R = N_{R_K}$ as $R_K$-modules and compute $({}_kf)_R(r\sum x_i\otimes r_i) = ({}_kf)_R(\sum x_i\otimes rr_i) = f_{R_K}(\sum x_i\otimes_K(rr_i\otimes 1_K)) = f_{R_K}(\sum x_i\otimes_K((r\otimes 1_K)(r_i\otimes 1_K))) = f_{R_K}((r\otimes 1_K)\sum x_i\otimes_K(r_i\otimes 1_K)) = (r\otimes 1_K)^d f_{R_K}(\sum x_i\otimes_K(r_i\otimes 1_K)) = r^d({}_kf)_R(\sum x_i\otimes r_i)$, where the last equality is justified by (12.27.4) for $a = 1_K$.

(c) For a finite chain $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ of independent indeterminates, we make use of the identification

$$R[\mathbf{T}]_K = R_K[\mathbf{T}] \tag{s1}$$

via

$$(r\mathbf{T}^\nu)\otimes a = (r\otimes a)\mathbf{T}^\nu, \quad \mathbf{T}^\nu\otimes 1_K = \mathbf{T}^\nu \qquad (r \in R,\ a \in K,\ \nu \in \mathbb{N}^n) \tag{s2}$$

Combining this identification with 12.27, we find

$$((_kM)_R)_{R[\mathbf{T}]} = (_kM)_{R[\mathbf{T}]} = M_{R[\mathbf{T}]_K} = M_{R_K[\mathbf{T}]} = (M_{R_K})_{R_K[\mathbf{T}]} \tag{s3}$$

and claim

$$z \otimes_R \mathbf{T}^\nu = z \otimes_{R_K} \mathbf{T}^\nu \qquad (z \in (_kM)_R = M_{R_K}, \nu \in \mathbb{N}_0^n). \tag{s4}$$

In order to prove (s4), additivity in the first variable allows us to assume $z = x \otimes r = x \otimes_K (r \otimes 1_K)$ with $x \in M$, $r \in R$, and following the chain of identifications presented in (s3), we conclude $z \otimes_R \mathbf{T}^\nu = (x \otimes r) \otimes_R \mathbf{T}^\nu = x \otimes (r\mathbf{T}^\nu) = x \otimes_K ((r\mathbf{T}^\nu) \otimes 1_K) = x \otimes_K ((r \otimes 1_K)\mathbf{T}^\nu) = (x \otimes_K (r \otimes 1_K)) \otimes_{R_K} \mathbf{T}^\nu = z \otimes_{R_K} \mathbf{T}^\nu$, and (s4) follows. Now let $x_1, \ldots, x_n \in (_kM)_R = M_{R_K}$. Then we combine (s3) with the identifications of (12.5.1) and Theorem 12.9 to obtain

$$\begin{aligned}
\sum_{\nu \in \mathbb{N}_0^n} \Big( (\Pi^\nu {}_kf)_R(x_1, \ldots, x_n) \Big) \otimes_R \mathbf{T}^\nu &= (_kf)_{R[\mathbf{T}]}\Big(\sum_{j=1}^n x_j \otimes_R \mathbf{t}_j\Big) \\
&= f_{R_K[\mathbf{T}]}\Big(\sum_{j=1}^n x_j \otimes_{R_K} \mathbf{t}_j\Big) \\
&= \sum_{\nu \in \mathbb{N}_0^n} (\Pi^\nu f)_{R_K}(x_1, \ldots, x_n) \otimes_{R_K} \mathbf{T}^\nu \\
&= \sum_{\nu \in \mathbb{N}_0^n} \Big( (_k(\Pi^\nu f))_R(x_1, \ldots, x_n) \Big) \otimes_R \mathbf{T}^\nu,
\end{aligned}$$

and a comparison yields $(\Pi^\nu (_kf))_R(x_1, \ldots, x_n) = (_k(\Pi^\nu f))_R(x_1, \ldots, x_n)$, hence (c).

(d) Let $x \in (_kM)_R = M_{R_K}$. Then $(_kf_i)_R(x) = (f_i)_{R_K}(x) = 0$ for almost all $i \in I$, showing that the family $(_kf_i)_{i \in I}$ is locally finite. Moreover, $(\sum_{i \in I} (_kf_i)_R)(x) = \sum_{i \in I} (_kf_i)_R(x) = \sum_{i \in I} (f_i)_{R_K}(x) = (\sum_{i \in I} f_i)_{R_K}(x) = (_k(\sum_{i \in I} f_i))_R(x)$, and (d) follows.

(e) Combining (c) with (d) and (12.15.1) yields

$$_k(D^n f) = {}_k\Big(\sum_{p \geq 0} \Pi^{(p,n)} f\Big) = \sum_{p \geq 0} {}_k(\Pi^{(p,n)} f) = \sum_{p \geq 0} \Pi^{(p,n)}(_kf) = D^n(_kf)$$

for all $n \in \mathbb{N}^0$.

(f) For $R \in k$-**alg**, $x \in (_kM)_R = M_{R_K}$, we apply (e) and obtain

$$\begin{aligned}
(\partial_y (_kf))_R(x) &= (D(_kf))_R(x, y_R) = (_k(Df))_R(x, y_R) \\
&= (Df)_{R_K}(x, y_{R_K}) = (\partial_y f)_{R_K}(x) = (_k(\partial_y f))_R(x),
\end{aligned}$$

as claimed.

**12.47** *Existence*. Let $R \in K$-**alg** $\subseteq k$-**alg**. There is a natural surjection

$$\omega_R \colon ({}_kN)_R \longrightarrow N_R, \quad \omega_R(y \otimes r) = y \otimes_K r \qquad (y \in N, r \in R). \tag{s1}$$

Combining this with (9.4.1), we obtain a set map

$$g_R := \omega_R \circ f_R \colon (M_K)_R = M_R \xrightarrow[f_R]{} ({}_kN)_R \xrightarrow[\omega_R]{} N_R. \tag{s2}$$

We claim that the totality of set maps $g_R$, $R \in K$-**alg**, is a polynomial law over $K$. To see this, suppose $\varphi \colon R \to S$ is a morphism in $K$-**alg**. In the diagram

$$\begin{array}{ccccccc}
(M_K)_R & \xrightarrow[\mathbf{1}]{} & M_R & \xrightarrow[f_R]{} & ({}_kN)_R & \xrightarrow[\omega_R]{} & N_R \\
\downarrow{\scriptstyle \mathbf{1}_{M_K} \otimes_K \varphi} & & \downarrow{\scriptstyle \mathbf{1}_M \otimes \varphi} & & \downarrow{\scriptstyle \mathbf{1}_N \otimes \varphi} & & \downarrow{\scriptstyle \mathbf{1}_N \otimes_K \varphi} \\
(M_K)_S & \xrightarrow[\mathbf{1}]{} & M_S & \xrightarrow[f_S]{} & ({}_kN)_S & \xrightarrow[\omega_S]{} & N_S,
\end{array}$$

the left-hand square commutes by (9.4.1), the middle square commutes because $f$ is a polynomial law over $k$, while the right-hand square commutes by virtue of (s1). Combining we obtain a commutative diagram

$$\begin{array}{ccc}
(M_K)_R & \xrightarrow[g_R]{} & N_R \\
\downarrow{\scriptstyle \mathbf{1}_{M_K} \otimes_K \varphi} & & \downarrow{\scriptstyle \mathbf{1}_N \otimes_K \varphi} \\
(M_K)_S & \xrightarrow[g_S]{} & N_S,
\end{array}$$

which shows that $g$ is indeed a polynomial law over $K$. To complete the existence part of the proof, it remains to show that the diagram (1) commutes, so let $R \in k$-**alg**. Then $({}_kN)_R = N_{R_K}$ by (12.27.1), leading to a composition of additive maps as

$$({}_kN)_R \xrightarrow[\mathbf{1}_{({}_kN)} \otimes \mathrm{can}_{R,K}]{} ({}_kN)_{R_K} \xrightarrow[\omega_{R_K}]{} N_{R_K} = ({}_kN)_R,$$

where $\mathrm{can}_{R,K} \colon R \to R_K$ is the natural map of (9.2.3). For $y \in N$, $r \in R$, we obtain $\omega_{R_K} \circ (\mathbf{1}_{({}_kN)} \otimes \mathrm{can}_{R,K})(x \otimes r) = \omega_{R_K}(x \otimes (r \otimes 1_K)) = x \otimes_K (r \otimes 1_K) = x \otimes r$, so

$$\omega_{R_K} \circ (\mathbf{1}_{({}_kN)} \otimes \mathrm{can}_{R,K}) = \mathbf{1}_{({}_kN)_R}. \tag{s3}$$

We must show $({}_kg)_R \circ ({}_k(\mathrm{can}_{M,K}))_R = f_R$. Under the natural identification $({}_k(M_K))_R = (M_K)_{R_K} = M_{R_K}$, we have $({}_k(\mathrm{can}_{M,K}))_R = \mathbf{1}_M \otimes \mathrm{can}_{R,K}$, so we must show $g_{R_K} \circ (\mathbf{1}_M \otimes \mathrm{can}_{R,K}) = f_R$. But $f$ is a polynomial law over $k$, so the

diagram

$$\begin{array}{ccc} M_R & \xrightarrow[f_R]{} & ({}_kN)_R \\ {\scriptstyle \mathbf{1}_M\otimes \mathrm{can}_{R,K}}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_{({}_kN)}\otimes \mathrm{can}_{R,K}} \\ M_{R_K} & \xrightarrow[f_{R_K}]{} & ({}_kN)_{R_K} \end{array}$$

commutes. Hence (s2),(s3) imply $g_{R_K} \circ (\mathbf{1}_M \otimes i_{R,K}) = \omega_{R_K} \circ f_{R_K} \circ (\mathbf{1}_M \otimes i_{R,K}) = \omega_{R_K} \circ (\mathbf{1}_{({}_kN)} \otimes i_{R,K}) \circ f_{R_K} = f_{R_K}$, as desired.

*Uniqueness.* Suppose $g, h\colon M_K \to N$ are two polynomial laws over $K$ making the diagram (1) commutative. We must show $g = h$. Thanks to Exercise 12.45, it actually suffices to show ${}_kg = {}_kh$, i.e., $g_{R_K} = h_{R_K}$ for all $R \in k$-**alg**. In order to do so, let $x_1, \ldots, x_n \in M$, $r_1, \ldots, r_n \in R$, $a_1, \ldots, a_n \in K$ and $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ a finite chain of independent indeterminates. Write $\varphi\colon R_K[\mathbf{T}] \to R_K$ for the unique homomorphism of $R_K$-algebras sending $\mathbf{t}_\nu$ to $r_\nu \otimes a_\nu$ $(1 \le \nu \le n)$. Since $g, h$ are polynomial laws over $K$, the squares of the diagram

$$\begin{array}{ccccc} M_{R_K[\mathbf{T}]} & \xrightarrow[\mathbf{1}]{} & (M_K)_{R_K[\mathbf{T}]} & \xrightarrow[g_{R_K[\mathbf{T}]},h_{R_K[\mathbf{T}]}]{} & N_{R_K[\mathbf{T}]} \\ {\scriptstyle \mathbf{1}_M\otimes\varphi}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_{M_K}\otimes_K\varphi} & & \downarrow{\scriptstyle \mathbf{1}_N\otimes_K\varphi} \\ M_{R_K} & \xrightarrow[\mathbf{1}]{} & (M_K)_{R_K} & \xrightarrow[g_{R_K},h_{R_K}]{} & N_{R_K} \end{array}$$

commute, and using (9.4.1) we conclude, for $p \in \{g, h\}$,

$$\begin{aligned} p_{R_K}\Big(\sum x_\nu \otimes (r_\nu \otimes a_\nu)\Big) &= p_{R_K}\Big(\sum (x_\nu \otimes 1_K) \otimes_K (r_\nu \otimes a_\nu)\Big) \\ &= (p_{R_K} \circ (\mathbf{1}_{M_K} \otimes_K \varphi))\Big(\sum (x_\nu \otimes 1_K) \otimes_K \mathbf{t}_\nu\Big) \\ &= (p_{R_K} \circ (\mathbf{1}_M \otimes \varphi))\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big) \\ &= ((\mathbf{1}_N \otimes_K \varphi) \circ p_{R_K[\mathbf{T}]}\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big), \end{aligned}$$

which shows that it will be enough to prove

$$g_{R_K[\mathbf{T}]}\Big(\sum x_\nu \otimes t_\nu\Big) = h_{R_K[\mathbf{T}]}\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big).$$

Combining our previous identifications with the fact that (1) holds for $p$ and $R[\mathbf{T}]_K = R_K[\mathbf{T}]$ under the identification $\mathbf{t}_\nu \otimes 1_K = \mathbf{t}_\nu$ for all $\nu = 1, \ldots, n$ , this follows from

$$\begin{aligned} f_{R[\mathbf{T}]}\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big) &= ({}_kp)_{R[\mathbf{T}]} \circ ({}_k(\mathrm{can}_{M,K}))_{R[\mathbf{T}]}\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big) \\ &= p_{R[\mathbf{T}]_K} \circ (\mathbf{1}_M \otimes \mathrm{can}_{R[\mathbf{T}],K})\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big) \\ &= p_{R[\mathbf{T}]_K}\Big(\sum x_\nu \otimes (\mathbf{t}_\nu \otimes 1_K)\Big) \\ &= p_{R_K[\mathbf{T}]}\Big(\sum x_\nu \otimes \mathbf{t}_\nu\Big). \end{aligned}$$

**12.48** (a) Put $H := f * g\colon M \to N$ as a polynomial law over $K$ and $H' := ({}_kf, {}_kg)\colon {}_kM \to {}_kN$ as a polynomial law over $k$. We must show ${}_kH = H'$. For any polynomial law $h$ over $K$, we apply (12.27.4) and obtain $({}_kh)_k = h_{k\otimes K} = h_K$. Hence

$$({}_kH)_k = H_K(f * g)_K = f_K = f$$

as a set map $M \to N$, which is the same as

$${}_kf = ({}_kf)_k(({}_kf) = *({}_kg))_k = H'_k$$

as a set map ${}_kM \to {}_kN$, and we have shown $({}_kH)_k = H'_k$. Similarly, by Exercise 12.46 (e),

$$\big(D({}_kH)\big)_k = \big({}_k(DH)\big)_k = (DH)_K = g_K = g$$

as a set map $M \times M \to N$, which is the same as

$${}_kg = ({}_kg)_k = \Big(D(({}_kf) * ({}_kg))\Big)_k = (DH')_k$$

as a set map ${}_kM \times {}_kM \to {}_kN$. Thus $\big(D({}_kH)\big)_k = H'_k$, and from Exercise 12.43 (d) we conclude ${}_kH = H'$, as claimed.

(b) By definition, (2) commutes as a $\sigma$-semi-linear polynomial square if and only if

$$\begin{array}{ccc} {}_kM & \xrightarrow[{}_k\varphi]{} & {}_kM' \\ {\scriptstyle {}_k(f*g)}\downarrow & & \downarrow{\scriptstyle {}_k(f'*g')} \\ {}_kN & \xrightarrow[{}_k\psi]{} & {}_kN' \end{array} \tag{s1}$$

does as a diagram of polynomial laws over $k$. But (s1), thanks to (a), is the same as

$$\begin{array}{ccc} {}_kM & \xrightarrow[{}_k\varphi]{} & {}_kM' \\ {\scriptstyle ({}_kf)*({}_kg)}\downarrow & & \downarrow{\scriptstyle ({}_kf')*({}_kg')} \\ {}_kN & \xrightarrow[{}_k\psi]{} & {}_kN' \end{array}$$

By the solution to Exercise 12.43 (a), therefore,

$$({}_k\varphi, {}_k\psi)\colon ({}_kf) * ({}_kg) \longrightarrow ({}_kf') * ({}_kg')$$

is a morphism in the category $k3$-**holaw**. Thus Exercise 12.43 (d) and (1) imply that

$$({}_k\varphi, {}_k\psi)\colon ({}_kf, {}_kg) \longrightarrow ({}_kf', {}_kg')$$

is a morphism in the category $k$-**cumap**, which in turn is equivalent to the diagrams (3) of set maps being commutative.

**12.49** Fixing $R \in k$-**alg**, there is clearly a unique $k$-linear map

$$\Psi_R \colon N \otimes \mathrm{Pol}(M,k) \longrightarrow \mathrm{Map}(M_R, N_R)$$

given by

$$\Psi_R(v \otimes f)(x) = v \otimes f_R(x)$$

for $v \in N$, $f \in \mathrm{Pol}(M,k)$, $x \in M_R$. For the first part of the problem, it will be enough to show that $\Psi_R$ varies functorially with $R$, so let $\varphi \colon R \to S$ be a morphism in $k$-**alg**. Since $f$ is a scalar polynomial law, hence the diagram

$$\begin{array}{ccc} M_R & \xrightarrow[f_R]{} & R \\ {\scriptstyle \mathbf{1}_M \otimes \varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ M_S & \xrightarrow[f_S]{} & S \end{array}$$

commutes, so does

$$\begin{array}{ccc} M_R & \xrightarrow[\Psi_R(v\otimes f)]{} & N_R \\ {\scriptstyle \mathbf{1}_M \otimes \varphi}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_N \otimes \varphi} \\ M_S & \xrightarrow[\Psi_S(v\otimes f)]{} & N_S\,. \end{array}$$

Hence we have shown that a $k$-linear map $\Psi \colon N \otimes \mathrm{Pol}(M,k) \to \mathrm{Pol}(M,N)$ satisfying (1) does indeed exist and is obviously unique. It remains to prove that $\Psi$ is an isomorphism if $N$ is finitely generated projective.

To this end, $N$ still being arbitrary, we write $\Psi^N := \Psi$ to indicate dependence on $N$ and consider another $k$-module $N'$. Then the linear projections $\pi \colon N \oplus N' \to N$, $\pi' \colon N \oplus N' \to N'$, canonically regarded as homogeneous polynomial laws of degree 1 via Exercise 12.33, induce $k$-linear maps

$$\pi_* \colon \mathrm{Pol}(M, N \oplus N') \longrightarrow \mathrm{Pol}(M,N), \quad \pi'_* \colon \mathrm{Pol}(M, N \oplus N') \longrightarrow \mathrm{Pol}(M,N')$$

given by $f \mapsto \pi \circ f$, $f \mapsto \pi' \circ f$, respectively, which in turn yield an isomorphism

$$\pi_* \oplus \pi'_* \colon \mathrm{Pol}(M, N \oplus N') \xrightarrow{\sim} \mathrm{Pol}(M,N) \oplus \mathrm{Pol}(M,N').$$

After the natural identification $M \otimes (N \oplus N') = M \otimes N \oplus M \otimes N'$, it is straight-

forward to check that the diagram

$$\begin{array}{ccc} (N \oplus N') \otimes \mathrm{Pol}(M,k) & \xrightarrow{\Psi^{N\oplus N'}} & \mathrm{Pol}(M, N \oplus N') \\ {\scriptstyle \mathrm{can}}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \pi_*\oplus\pi'_*} \\ (N \otimes \mathrm{Pol}(M,k)) \oplus (N' \otimes \mathrm{Pol}(M,k)) & \xrightarrow[\Psi^N\oplus\Psi^{N'}]{} & \mathrm{Pol}(M,N) \oplus \mathrm{Pol}(M,N') \end{array} \tag{s1}$$

commutes. Now suppose $N$ is finitely generated projective and choose a $k$-module $N'$ making $N \oplus N'$ free of finite rank. By a repeated application of (s1), we are reduced to the case $N = k$. But then $\Psi = \Psi^k = \mathbf{1}_{\mathrm{Pol}(M,k)}$, and the problem is solved.

*Remark.* In [16, Lemma 3.3], the result in this exercise is obtained as a consequence of 25.5 (iii).

# Solutions for Chapter III

## Solutions for Section 13

This section contains no exercises.

## Solutions for Section 14

**14.7** Since the associator of $A$ is alternating, the first part follows immediately from (7.5.1). The second part is now obvious.

**14.8** A multilinear map is alternating if and only if it vanishes provided two adjacent components of the argument are equal; hence, after linearizing, it changes signs when two adjacent components are switched. For an alternative $k$-algebra $A$, we therefore have to prove

$$f(w,x,y,y) = 0 = f(w,x,x,z) = f(x,x,y,z)$$

for all $w,x,y,z \in A$. The first equation follows from the fact that the associator of $A$ is alternating by definition. Combined with the left Moufang identity and the linearized left alternative law, this also gives

$$\begin{aligned} f(w,x,x,z) &= [wx,x,z] - x[w,x,z] = ((wx)x)z - (wx)(xz) - x\big((wx)z\big) + x\big(w(xz)\big) \\ &= ((wx)x + x(wx))z - \Big(((wx)(xz) + x\big((wx)z\big)\Big) = 0, \end{aligned}$$

hence the second equation. As to the third, we write $f^{\mathrm{op}}$ for the Kleinfeld function of $A^{\mathrm{op}}$, and since $A$ and $A^{\mathrm{op}}$ have the same associator, we conclude

$$f^{\mathrm{op}}(w,x,y,z) = f(x,w,y,z),$$

hence $f(x,x,y,z) = -f(x,y,x,z) = -f^{\mathrm{op}}(y,x,x,z) = 0$, as desired.

**14.9** The implications (i)⇒(ii)⇒(iii)⇒(iv) and (i)⇒(v) are obvious, while

(iv)⇒(iii) follows from the fact that $L_x$, $R_x$, $U_x = L_xR_x$ pairwise commute. We are thus left with the following implications.

(iv)⇒(i). Given $y \in A$, we find an element $z \in A$ satisfying $xzx = y$. Moreover, since (iii) holds by what we have just seen, there are $e, f \in A$ such that $ex = x = xf$. Now the Moufang identities yield $ey = e(xzx) = ((ex)z)x = xzx = y$, $yf = (xzx)f = x(z(xf)) = xzx = y$, so $e$ (resp. $f$) is a left (resp. right) unit for $A$. Hence $A$ is unital with $1_A = e = f$.

(v)⇒(i). Since $L_x$ is surjective, some $e \in A$ has $xe = x$ and any $z \in A$ can be written as $z = xw$ for some $w \in A$. Hence $x(ez) = x(e(xw)) = (xex)w = x^2w = x(xw) = xz$, forcing $e$ to be a left unit for $A$ since $L_x$ is also injective. Passing to $A^{\mathrm{op}}$, we find a right unit for $A$ as well, and (i) holds.

**14.10** (a) The implication (ii)⇒(i) is obvious, while (i)⇔(iii) becomes (i)⇔(ii) in $A^{\mathrm{op}}$. Thus we only have to prove (i)⇒(ii). Using the Moufang identities in operator form (13.3.4), (13.3.5), we obtain $E^2 = L_xL_yL_xL_y = L_{xyx}L_y = L_xL_y = E$ and, similarly, $F^2 = F$. Furthermore, by (13.5.4), $EF = L_xL_yR_yR_x = L_xU_yR_x = U_{xy} = U_{1_A} = \mathbf{1}_A$, hence $\mathbf{1}_A = E^2F = EEF = E$, and this is (ii).

(b) Assume $x \in A$ is right invertible, so some $y \in A$ has $xy = 1_A$. Then $L_xL_y = \mathbf{1}_A$ by (a)(ii), so $L_x\colon A \to A$ is surjective. But $A$ is a finitely generated $k$-module, forcing $L_x$ to be bijective (Prop. 7.11), hence $x$ to be invertible (Prop. 13.6) and $y = x^{-1}$ to be its two-sided inverse. The case of a left invertible element is treated analogously.

(c) Take $V$ to be the $k$-vector space of all sequences $a_0, a_1, \ldots$ of elements of $k$ with coordinatewise addition, $A := \mathrm{End}_k(V)$, $y$ to be the map that shifts the sequence right by one place and puts a zero in the first coordinate, and $x$ to be the map that shifts the sequence left by one place and drops the first coordinate. Then $xy = 1_A$, but neither $x$ nor $y$ is invertible because $x$ is not injective and $y$ is not surjective.

**14.11** Since $xy \in A$ is invertible, so is the linear operator $U_{xy}$, by Prop. 13.6. But $U_{xy} = R_yU_xL_y$ by (13.5.4), so $L_y$ is injective. On the other hand, the left Moufang identity and (13.6.2) imply $L_y(x(y(xy)^{-1})) = y[x(y(xy)^{-1})] = [y(xy)](xy)^{-1} = y = L_y1_A$, and since $L_y$ is injective, we conclude $x(y(xy)^{-1}) = 1_A$, so $x$ is right invertible with $y(xy)^{-1}$ as a right inverse. Reading this in $A^{\mathrm{op}}$ shows that $y$ is left invertible with $(xy)^{-1}x$ as a left inverse.

**14.12** For $i, j = 1, 2$ and $x \in A$, the expression $c_ixc_j$ is unambiguous since it takes place in the unital subalgebra of $A$ generated by $c$ and $x$, which is associative by Cor. 14.5. We now claim that the following relations hold.

$$L_{c_i}L_{c_j} = \delta_{ij}L_{c_i}, \quad R_{c_i}R_{c_j} = \delta_{ij}R_{c_i}, \quad L_{c_i}R_{c_j} = R_{c_j}L_{c_i}. \tag{s1}$$

For $i = j$, this follows immediately from (13.1.4)–(13.1.2), while for $i \neq j$

it suffices to observe $L_{c_j} = \mathbf{1}_A - L_{c_i}$, $R_{c_j} = \mathbf{1}_A - R_{c_i}$ to arrive at the desired conclusion. Now let $i, j, l, m = 1, 2$ and put $E_{ij} := L_{c_i} R_{c_j}$. Then (s1) yields $E_{ij}E_{lm} = L_{c_i}R_{c_j}L_{c_l}R_{c_m} = L_{c_i}L_{c_l}R_{c_j}R_{c_m} = \delta_{il}\delta_{jm}L_{c_i}R_{c_j} = \delta_{il}\delta_{jm}E_{ij}$, so the $E_{ij}$ are indeed orthogonal projections that add up to $\sum_{i,j=1,2} E_{ij} = \sum_{i,j=1,2} L_{c_i}R_{c_j} = U_{c_1+c_2} = U_{1_A} = \mathbf{1}_A$. This proves (1), where the $A_{ij} = A_{ij}(c)$ are defined by the first among the relations in (2). The remaining ones are now obvious. Next we establish (3)–(5). In order to do so, we let $x_{ij} \in A_{ij}$, $y_{lm} \in A_{lm}$ etc. and first prove

$$c_i x_{jl} = \delta_{ij} x_{jl}, \quad x_{ij} c_l = \delta_{jl} x_{ij}. \tag{s2}$$

Indeed, by (2) the first relation is clear for $i = j$, while for $i \neq j$ we obtain $c_i x_{jl} = x_{jl} - c_j x_{jl} = x_{jl} - x_{jl} = 0$, as claimed. The second relation is proved analogously. Combining now the linearized right alternative law (13.2.2) with (s2), we obtain $(x_{ij}y_{jl})c_l = x_{ij}(y_{jl}c_l + c_l y_{jl}) - (x_{ij}c_l)y_{jl} = x_{ij}y_{jl} + \delta_{jl}x_{ij}y_{jl} - \delta_{jl}x_{ij}y_{jl} = x_{ij}y_{jl}$ and, similarly, $c_i(x_{ij}y_{jl}) = x_{ij}y_{jl}$. This proves (3). Furthermore, for $i \neq j$, the left Moufang identity and (s2) yield $x_{ii}y_{jl} = (c_i x_{ii} c_i)y_{jl} = c_i(x_{ii}(c_i y_{jl})) = 0$ and, similarly, $y_{lj}x_{ii} = 0$. Thus (4) holds. Finally, since $c_j(x_{ij}y_{ij}) = (c_j x_{ij} + x_{ij}c_j)y_{ij} - x_{ij}(c_j y_{ij}) = x_{ij}y_{ij} = (x_{ij}y_{ij})c_i$, we also have (5). In particular, $x_{ij}^2 = c_j x_{ij}^2 = (c_j x_{ij})x_{ij} = 0$, while the remaining assertion $A_{ij}^2 = \{0\}$ for $A$ associative is obvious.

## Solutions for Section 15

**15.13** By Prop. 13.6, $x \in A$ is invertible in $A^{(p,q)}$ iff $U_x^{(p,q)} = U_x U_{pq}$ (by (15.5.1)) is bijective iff $U_x$ is bijective iff $x$ is invertible in $A$, in which case its inverse in $A^{(p,q)}$ is $x^{(-1,p,q)} = (U_x^{(p,q)})^{-1}x = U_{pq}^{-1}U_x^{-1}x = U_{pq}^{-1}x^{-1}$.

**15.14** By definition, $f, g, h$ are linear bijections from $A$ to $B$ satisfying $f(xy) = g(x)h(y)$ for all $x, y \in A$. Setting $u := g^{-1}(1_B)$, $v := h^{-1}(1_B)$, we conclude $f(uy) = h(y)$, $f(xv) = g(x)$, equivalently, $f \circ L_u = h$, $f \circ R_v = g$. Thus $L_u, R_v \colon A \to A$ are linear bijections, forcing $A$ to be unital (Exc. 14.9) and $u, v \in A$ to be invertible (Prop. 13.6), with inverses $p := v^{-1}$, $q := u^{-1}$ This implies $f((xp)(qy)) = g(xp)h(qy) = f((xv^{-1})v)f(u(u^{-1}y)) = f(x)f(y)$. Thus $f \colon A^{(p,q)} \to B$ is an isomorphism; in particular, $B$ is alternative.

**15.15** See [34, 2.2-2.8]. In particular $1_{\mathrm{Str}(A)} = (1_A.1_A, \mathbf{1}_A)$ is the unit element of $\mathrm{Str}(A)$ and $(p, q, g)^{-1} = (g^{-1}(q^{-1}p^{-2}), g^{-1}(q^{-2}p^{-1}), g^{-1})$ is the inverse of $(p, q, g) \in \mathrm{Str}(A)$.

**15.16** The equation $(L_u x)u \cdot u^{-2}(L_u y) = uxu \cdot u^{-2}(uy) = u(x(u(u^{-1}y))) =$

$u(xy) = L_u(xy)$ for all $x, y \in A$ shows that $L_u\colon A \to A^{(u,u^{-2})}$ is an isomorphism. Hence $\tilde{L_u} \in \mathrm{Str}(A)$. Reading this in $A^{op}$ also yields $\tilde{R_u} \in \mathrm{Str}(A)$. Invoking (15.15.1) and Cor. 14.5, we now compute

$$\begin{aligned}\tilde{L_u}\tilde{L_v}\tilde{L_u} &= (u, u^{-2}, L_u)(v, v^{-2}, L_v)\tilde{L_u} = (uu^{-2}uvu, u^{-2}uv^{-2}uu^{-2}, L_uL_v)\tilde{L_u}\\ &= (vu, u^{-1}v^{-2}u^{-1}, L_uL_v)(u, u^{-2}L_u) = (w, z, L_uL_vL_u) = (w, z, L_{uvu}),\end{aligned}$$

where

$$\begin{aligned}w &= vuu^{-1}v^{-2}u^{-1}uvuvu = uvu,\\ z &= u^{-1}v^{-2}u^{-1}uvu^{-2}vuu^{-1}v^{-2}u^{-1} = u^{-1}v^{-1}u^{-2}v^{-1}u^{-1} = (uvu)^{-2}.\end{aligned}$$

Thus $\tilde{L_u}\tilde{L_v}\tilde{L_u} = (uvu, (uvu)^{-2}, L_{uvu}) = \tilde{L}_{uvu}$. Reading this in $A^{\mathrm{op}}$, we also obtain $\tilde{R_u}\tilde{R_v}\tilde{R_u} = \tilde{R}_{uvu}$. Since $\tilde{L}_{1_A} = 1_{\mathrm{Str}(A)} = \tilde{R}_{1_A}$, the relations $(\tilde{L_u})^{-1} = \tilde{L}_{u^{-1}}$, $(\tilde{R_u})^{-1} = \tilde{R}_{u^{-1}}$ are now clear. Next we compute

$$\begin{aligned}\tilde{L_u}\tilde{R_v} &= (u, u^{-2}, L_u)(v^{-2}, v, R_v) = (uu^{-2}uv^{-2}u, u^{-2}uvuu^{-2}, L_uR_v)\\ &= (v^{-2}u, u^{-1}vu^{-1}, L_uR_v),\end{aligned}$$

as claimed. A similar computation or passing to $A^{\mathrm{op}}$ yields the analogous equation for $\tilde{R_v}\tilde{L_u}$. The rest is clear.

**15.17** See [34, 3.2, 3.3].

**15.18** (a) The extended right multiplication by $pq$ as defined in Exc. 15.16 yields an isomorphism

$$R_{pq}\colon A \xrightarrow{\sim} A^{((pq)^{-2},pq)},$$

which by functoriality 15.4 and Prop. 15.3 may also be regarded as an isomorphism

$$R_{pq}\colon A^{(p,q)} \xrightarrow{\sim} (A^{((pq)^{-2},pq)})^{(p^2q,qpq)} = A^{(p',q')}$$

with

$$\begin{aligned}p' &= (pq)^{-2}(pq)p^2q(pq)^{-2} = q^{-1}p^{-1}pq^{-1}p^{-1} = q^{-2}p^{-1},\\ q' &= (pq)(qpq)(pq)^{-2}(pq) = pq^2.\end{aligned}$$

Thus $R_{pq}\colon A^{(p,q)} \to A^{pq^2}$ is an isomorphism, which may also be verified di-

rectly, using (13.7.1) and the Moufang identities:

$$\begin{aligned}(R_{pq}x)(pq^2)^{-1}\cdot(pq^2)R_{pq}y &= (x(pq))(q^{-2}p^{-1})\cdot((pq)q)(y(pq))\\ &= (x(pq))(q^{-2}p^{-1})\cdot(pq)(qy)(pq)\\ &= \Big[\Big([(x(pq))(q^{-2}p^{-1})](pq)\Big)(qy)\Big](pq)\\ &= \Big[\Big(x((pq)(q^{-2}p^{-1})(pq))\Big)(qy)\Big](pq)\\ &= ((xp)(qy))(pq) = R_{pq}((xp)(qy)).\end{aligned}$$

(b) The argument uses (15.9.3) to conclude $A^{(pq)r} = (A^{pq})^r = ((A^p)^q)^r = (A^p)^{qr} = A^{p(qr)}$, which by (15.9.4) yields $(pq)r = up(qr)$ for some $u \in \mathrm{Nuc}(A)^\times$. But the argument is faulty since with $B := A^p$ we have $((A^p)^q)^r = (B^q)^r = B^s$, where $s$ is the product of $q$ and $r$ *not in* $A$ *but in* $B = A^p$: $s = (qp^{-1})(pr)$, forcing $B^s = (A^p)^{(qp^{-1})(pr)} = A^\mathsf{T}$, $t = p[(qp^{-1})(pr)] = [p(qp^{-1})p]r = (pq)r$, in complete agreement with the previous computation. Moreover, the conclusion does not hold, which follows from looking at the real octonions ....

**15.19** The solution to Exc. 15.18 shows that right multiplication by $pq$ yields an isomorphism from $A^{(p,q)}$ to an appropriate unital isotope of $A$. It therefore suffices to show $\mathrm{Nuc}(A^p) = \mathrm{Nuc}(A)$ and $\mathrm{Cent}(A^p) = \mathrm{Cent}(A)$ for all $p \in A^\times$; actually, since $A = (A^p)^{p^{-1}}$, it will be enough to verify the inclusions $\mathrm{Nuc}(A) \subseteq \mathrm{Nuc}(A^p)$, $\mathrm{Cent}(A) \subseteq \mathrm{Cent}(A^p)$. Writing $[-,-,-]^p$ (resp. $[-,-]^p$) for the associator (resp. the commutator) of $A^p$, this will follow once we have shown

$$\begin{aligned}[x,y,z]^p &= [x,yp^{-1},pz] - [x,p^{-1},(py)z] \quad \text{and}\\ [x,y]^p &= [x,y] + [x,p^{-1},py] - [y,p^{-1},px]\end{aligned} \tag{s1}$$

for all $x, y \in A$. In order to derive the first relation of (s1), we compute

$$\begin{aligned}[x,y,z]^p &= \Big(((xp^{-1})(py))p^{-1}\Big)(pz) - (xp^{-1})\Big(p((yp^{-1})(pz))\Big)\\ &= (x(yp^{-1})(pz) - (xp^{-1})((py)z)\\ &= [x,yp^{-1},pz] + x((yp^{-1})(pz)) - (xp^{-1})((py)z),\end{aligned}$$

where the second summand on the right agrees with

$$x\Big[p^{-1}\Big(p((yp^{-1})(pz))\Big)\Big] = x\Big(p^{-1}((py)z)\Big) = -[x,p^{-1},(py)z] + (xp^{-1})((py)z).$$

Inserting this into the previous equation yields the first relation of (s1). For the second, we obtain $[x,y]^p = (xp^{-1})(py) - (yp^{-1})(px) = [x,p^{-1},py] + xy - [y,p^{-1},px] - yx = [x,y] + [x,p^{-1},py] - [y,p^{-1},px]$, as claimed.

# Solutions for Chapter IV

## Solutions for Section 16

**16.18** (a) We begin by deriving the following identities:

$$n_C(x^2) = n_C(x)^2, \tag{s1}$$
$$n_C(x, x^2) = t_C(x)n_C(x), \tag{s2}$$
$$t_C(x^2) = t_C(x)^2 - 2n_C(x). \tag{s3}$$

Indeed, the identities of 16.5 yield $n_C(x^2) = n_C(t_C(x)x - n_C(x)1_C) = t_C(x)^2 n_C(x) - t_C(x)^2 n_C(x) + n_C(x)^2$, hence (s1), while $n_C(x, x^2) = n_C(x, t_C(x)x - n_C(x)1_C = 2t_C(x)n_C(x) - t_C(x)n_C(x)$ yields (s2) and $t_C(x^2) = t_C(t_C(x)x - n_C(x)1_C) = t_C(x)^2 - 2n_C(x)$ is (s3). Combining these identities with those of (16.5) and writing $y, z \in k[x]$ as $y = \alpha_0 1_C + \alpha_1 x$, $y = \beta_0 1_C + \beta_1 x$ with $\alpha_0, \alpha_1, \beta_0, \beta_1 \in k$, we now compute

$$\begin{aligned}
n_C(yz) - n_C(y)n_C(z) &= n_C((\alpha_0 1_C + \alpha_1 x)(\beta_0 1_C + \beta_1 x)) \\
&\quad - n_C(\alpha_0 1_C + \alpha_1 x)n_C(\beta_0 1_C + \beta_1 x) \\
&= n_C(\alpha_0\beta_0 1_C + (\alpha_0\beta_1 + \alpha_1\beta_0)x + \alpha_1\beta_1 x^2) \\
&\quad - (\alpha_0^2 + \alpha_0\alpha_1 t_C(x) + \alpha_1^2 n_C(x))(\beta_0^2 + \beta_0\beta_1 t_C(x) + \beta_1^2 n_C(x)) \\
&= \alpha_0^2\beta_0^2 + \alpha_0\beta_0(\alpha_0\beta_1 + \alpha_1\beta_0)t_C(x) + \alpha_0\beta_0\alpha_1\beta_1 t_C(x^2) \\
&\quad + (\alpha_0\beta_1 + \alpha_1\beta_0)^2 n_C(x) + (\alpha_0\beta_1 + \alpha_1\beta_0)\alpha_1\beta_1 n_C(x, x^2) + \alpha_1^2\beta_1^2 n_C(x^2) \\
&\quad - (\alpha_0^2 + \alpha_0\alpha_1 t_C(x) + \alpha_1^2 n_C(x))(\beta_0^2 + \beta_0\beta_1 t_C(x) + \beta_1^2 n_C(x)) \\
&= \alpha_0^2\beta_0^2 + \alpha_0\beta_0(\alpha_0\beta_1 + \alpha_1\beta_0)t_C(x) + \alpha_0\alpha_1\beta_0\beta_1 t_C(x)^2 - 2\alpha_0\alpha_1\beta_0\beta_1 n_C(x) \\
&\quad + (\alpha_0\beta_1 + \alpha_1\beta_0)^2 n_C(x) + (\alpha_0\beta_1 + \alpha_1\beta_0)\alpha_1\beta_1 t_C(x)n_C(x) + \alpha_1^2\beta_1^2 n_C(x)^2 \\
&\quad - (\alpha_0^2 + \alpha_0\alpha_1 t_C(x) + \alpha_1^2 n_C(x))(\beta_0^2 + \beta_0\beta_1 t_C(x) + \beta_1^2 n_C(x)) \\
&= \alpha_0^2\beta_0^2 + \alpha_0^2\beta_0\beta_1 t_C(x) + \alpha_0\alpha_1\beta_0^2 t_C(x) + \alpha_0\alpha_1\beta_0\beta_1 t_C(x)^2 + \alpha_0^2\beta_1^2 n_C(x)
\end{aligned}$$

$$\begin{aligned} &+ \alpha_1^2\beta_0^2 n_C(x) + \alpha_0\alpha_1\beta_1^2 t_C(x)n_C(x) + \alpha_1^2\beta_0\beta_1 t_C(x)n_C(x) + \alpha_1^2\beta_1^2 n_C(x)^2 \\ &- (\alpha_0^2 + \alpha_0\alpha_1 t_C(x) + \alpha_1^2 n_C(x))(\beta_0^2 + \beta_0\beta_1 t_C(x) + \beta_1^2 n_C(x)) \\ = \;& 0. \end{aligned}$$

This completes the proof of (a).

(b) If $x$ is invertible in $k[x]$ with inverse $x^{-1} \in k[x]$, then (a) yields

$$n_C(x)n_C(x^{-1}) = n_C(xx^{-1}) = n_C(1_C) = 1,$$

hence $n_C(x) \in k^\times$ and $n_C(x^{-1}) = n_C(x)^{-1}$. Conversely, if $n_C(x) \in k^\times$, then $y := n_C(x)^{-1}\bar{x}$ by (16.5.6) satisfies $xy = 1_C = yx$. Thus $x$ is invertible in $k[x]$ with inverse $y$.

(c) If $t_C(x), n_C(x) \in \mathrm{Nil}(k)$, the elements $t_C(x)x, n_C(x)1_C \in k[x]$ are nilpotent and commute. But then $x^2 = t_C(x)x - n_C(x)1_C$ is nilpotent. Hence so is $x$. Conversely, assume $x$ is nilpotent. Then $x^n = 0$ for some positive integer $n$, and we show by induction on $n$ that $t_C(x)$ and $n_C(x)$ are nilpotent. If $n = 1$, there is nothing to prove. If $n > 1$, then we put $m := 1$ for $n = 2$ and $m := \lfloor \frac{n}{2} \rfloor + 1 > \frac{n}{2}$ for $n > 2$. This implies $2m \geq n$, hence $(x^2)^m = 0$, and $m < n$. Thanks to the induction hypothesis, therefore, the scalars $t_C(x^2) = t_C(x)^2 - 2n_C(x)$ (by (s3)) and $n_C(x^2) = n_C(x)^2$ (by (s1)) are both nilpotent. Hence $n_C(x)$ is nilpotent and so is $t_C(x)^2 = t_C(x^2) + 2n_C(x)$. But then $t_C(x)$ itself must be nilpotent, which completes the induction.

**16.19** $n := n_{C'} \circ \varphi \colon C \to k$ is a quadratic form such that $Dn = (Dn_{C'}) \circ (\varphi \times \varphi)$. Since $\varphi$ preserves units, we conclude $n(1_C) = 1$ and $t := (Dn)(1_C, -) = t_{C'} \circ \varphi$. Now let $x \in C$. Then

$$\varphi(t(x)x - n(x)1_C) = t_{C'}(\varphi(x))\varphi(x) - n_{C'}(\varphi(x))1_{C'} = \varphi(x)^2 = \varphi(x^2),$$

and since $\varphi$ is injective, $x^2 = t(x)x - n(x)1_C$. Thus not only $n_C$ but also $n$ is a norm for the conic algebra $C$. But by the hypotheses on $C$, its norm is unique (Prop. 16.16), which implies $n_C = n = n_{C'} \circ \varphi$, as desired.

If we drop the assumption that $\varphi$ be injective, the asserted conclusion is false: let $C := k \times k$, $C' := k$ and $\varphi \colon k \times k \to k$ be the projection onto the first factor. Then 16.2 (c),(d) yields $n_k(\varphi((\alpha, \beta))) = n_k(\alpha) = \alpha^2$ for all $\alpha, \beta \in k$, while $n_{k\times k}((\alpha, \beta)) = \alpha\beta$. Thus $\varphi$ does not preserve norms, hence, though being a unital algebra homomorphism, is *not* one of conic algebras.

**16.20** (a) One verifies immediately that $C$ is unital with identity element $e$. Defining $n_C \colon C \to k$ by

$$n_C(\alpha e + x) := \alpha^2 + \alpha T(x) + B(x, x)$$

for $\alpha \in k$, $x \in M_\lambda$, we obviously obtain a quadratic form with bilinearization

$$n_C(\alpha e + x, \beta e + y) = 2\alpha\beta + \alpha T(y) + \beta T(x) + B(x, y) + B(y, x)$$

for $\alpha, \beta \in k$, $x, y \in M_\lambda$. We have $n_C(e) = 1$, while $t_C := (Dn_C)(-, e)$ satisfies

$$t_C(\alpha e + x) = 2\alpha + T(x)$$

for $\alpha \in k$, $x \in M_\lambda$. Hence

$$\begin{aligned} t_C(\alpha e + x)(\alpha e + x) - n_C(\alpha e + x)e &= (2\alpha + T(x))(\alpha e + x) \\ &\quad - (\alpha^2 + \alpha T(x) + B(x, x))e \\ &= (\alpha^2 - B(x, x))e + \big((\alpha + T(x))x + \alpha x\big) \\ &= (\alpha e + x)^2, \end{aligned}$$

which shows that $C$ is a conic $k$-algebra with norm $n_C$ and trace $t_C$.

(b) We first show that $(T, B, K)$ is a conic co-ordinate system. The defining conditions of such a system are obviously fulfilled, with the following two exceptions. (i) the bilinear map $K$ takes values in $M_\lambda$, and (ii) $K$ is alternating. In order to establish (i), we let $x, y \in M_\lambda = \mathrm{Ker}(\lambda)$ and obtain

$$\lambda(x \times y) = t_C(x)\lambda(y) - \lambda(xy) + \lambda(xy)\lambda(e) = -\lambda(xy) + \lambda(xy) = 0,$$

hence $x \times y \in M_\lambda$. In order to establish (ii), we compute

$$x \times x = t_C(x)x - x^2 + \lambda(x^2)e = n_C(x)e + \lambda\big(t_C(x)x - n_C(x)e\big)e = n_C(x)e - n_C(x)e = 0,$$

so $K$ is indeed alternating. We now denote by "$\cdot$" the product in the conic algebra $C' := \mathrm{Con}(T, B, K)$ and obtain, for $\alpha, \beta \in k$, $x, y \in M_\lambda$,

$$\begin{aligned} (\alpha e + x) \cdot (\beta e + y) &= (\alpha\beta + \lambda(xy))e + \big((\alpha + t_C(x))y \\ &\quad + \beta x - t_C(x)y + xy - \lambda(xy)e\big) \\ &= \alpha\beta e + \alpha y + \beta x + xy = (\alpha e + x)(\beta e + y), \\ n_{C'}(\alpha e + x) &= \alpha^2 + \alpha t_C(x) - \lambda(x^2) = \alpha^2 \\ &\quad + \alpha t_C(x) - t_C(x)\lambda(x) + n_C(x)\lambda(e) \\ &= \alpha^2 + \alpha t_C(x) + n_C(x) = n_C(\alpha e + x). \end{aligned}$$

Summing up, we have proved $C = \mathrm{Con}(T_C, B_C, K_C)$. Finally, let $(T, B, K)$ be a conic co-ordinate system and $C := \mathrm{Con}(T, B, K)$. Consulting the multiplication

formula for $C$ (resp. the formula for the trace of $C$), we conclude

$$\begin{aligned} T_C(x) &= t_C(x) = T(x), \\ B_C(x,y) &= -\lambda(xy) = B(x,y) \\ K_C(x,y) &= t_C(x)y - xy + \lambda(xy)e = T(x)y - xy + \lambda(xy)e \\ &= (B(x,y+\lambda(xy))e + (T(x)y - T(x)y + K(x,y)) = K(x,y). \end{aligned}$$

Thus $(T_C, B_C, K_C) = (T, B, K)$ and we have proved that the two constructions in (a), (b) are inverse to each other.

**16.21** By assumption we have $1_C \wedge x \wedge x^2 = 0$ for all $x \in C$. Replacing $x$ by $x + \alpha y$, $x, y \in C$, $\alpha \in k$, we obtain (since $k$ contains more than two elements)

$$1_C \wedge y \wedge x^2 + 1_C \wedge x \wedge (x \circ y) = 0 \qquad (x, y \in C). \tag{s1}$$

Now put

$$U := \{0\} \cup \{u \in C \setminus k1_C \mid u^2 \in k1_C\} \tag{s2}$$

We claim that $U$ *is a vector subspace of* $C$. Clearly being closed under scalar multiplication, we must show $u+v \in U$ for all $u, v \in U$ such that $u, v$ are linearly independent. Then $1_C, u$ are linearly independent, and assuming $v = \alpha 1_C + \beta u$ for some $\alpha, \beta \in k$, we obtain $\alpha^2 1_C + 2\alpha\beta u + \beta^2 u^2 = v^2 \in k1_C$, hence $\alpha = 0$ or $\beta = 0$, a contradiction. Thus $1_C, u, v$ are linearly independent. On the other hand, setting $x = u$, $y = v$ (resp. $x = v$, $y = u$) in (s1), and observing (s2), we obtain $u \circ v = \alpha 1_C + \beta u = \gamma 1_C + \delta v$ for some $\alpha, \beta, \gamma, \delta \in k$, hence $u \circ v \in k1_C$. But this amounts to $(u+v)^2 \in k1_C$, so we have proved that $U$ is closed under addition and thus, altogether, a vector subspace of $C$.

Now let $x \in C \setminus k1_C$. Then $x^2 = \alpha 1_C + \beta x$ for some $\alpha, \beta \in k$, which implies $(x - \frac{\beta}{2}1_C)^2 \in k1_C$, hence $x - \frac{\beta}{2}1_C \in U$, and we have shown $C = k1_C \oplus U$ as a direct sum of subspaces. Now define a quadratic form $n_C \colon C \to k$ by $n_C(\alpha 1_C + u) := \alpha^2 + n_C(u)$ for $\alpha \in k$, $u \in U$, where $n_C(u) \in k$ is determined by $u^2 = -n_C(u)1_C$. This implies

$$\begin{gathered} n_C(\alpha 1_C + u, \beta 1_C + v) = 2\alpha\beta + n_C(u,v), \quad u \circ v = -n_C(u,v)1_C, \\ (\alpha, \beta \in k,\ u, v \in U), \end{gathered}$$

hence $t_C(\alpha 1_C + u) := n_C(1_C, \alpha 1_C + u) = 2\alpha$. Summing up, we obtain

$$\begin{aligned} (\alpha 1_C + u)^2 &= \alpha^2 1_C + 2\alpha u + u^2 = 2\alpha(\alpha 1_C + u) - (\alpha^2 + n_C(u))1_C \\ &= t_C(\alpha 1_C + u)(\alpha 1_C + u) - n_C(\alpha 1_C + u)1_C. \end{aligned}$$

Thus $C$ is a conic algebra over $k$ with norm $n_C$.

**16.22** Since conic algebras are stable under base change, they clearly satisfy

the Dickson condition. Conversely, suppose $C$ satisfies the Dickson condition. By hypothesis, the vector $1_C \in C$ is unimodular, so we find a submodule $M \subseteq C$ such that

$$C = k1_C \oplus M \tag{s1}$$

as a direct sum of $k$-modules. Since the assignment $x \mapsto x^2$ defines a quadratic map $M \to C$, the projections to the direct summands $k1_C \cong k$ and $M$ of the decomposition (s1) give rise to quadratic maps $n\colon M \to k$ and $s\colon M \to M$ such that

$$x^2 = s(x) - n(x)1_C \qquad (x \in M). \tag{s2}$$

In particular, $n$ is a quadratic form over $k$ that will eventually become the norm (restricted to $M$) of the prospective conic $k$-algebra $C$. On the other hand, by the Dickson condition, we also have $s(x) \in kx$ for $x \in M$, and we would like to think of $s(x)$ as $t(x)x$ with $t(x) \in k$ becoming the trace of $x$ in the prospective conic $k$-algebra $C$. But since the annihilator of $x$ may not be zero, we don't even know at this stage how to make $t(x)$ a quantity that is well defined, let alone a linear form. For this reason, we bring the hypotheses on the module structure of $C$ and the *strict* Dickson condition into play.

Let us first reduce to the case that $M$ is a free $k$-module. Otherwise, $M$ is finitely generated projective by hypothesis, so there exists a finite family of elements $f \in k$ that generate the unit ideal in $k$ and make $M_f$ a free $k_f$-module of finite rank, for each such $f$. Assuming the free case has been settled, it follows that all $C_f$ are conic, and Prop. 16.16 ensures that the norms $n_{C_f}$ glue to give a quadratic form $n\colon C \to k$. It is then clear that $C$ is a conic algebra with norm $n$ since this is so after changing scalars from $k$ to each $k_f$.

For the rest of the proof, we may therefore assume that $M$ is a free $k$-module, possibly of infinite rank, with basis $(e_i)_{i\in I}$. We let $\mathbf{T} = (\mathbf{t}_i)_{i\in I}$ be a family of independent variables and write $k[\mathbf{T}]$ for the corresponding polynomial ring. For a *non-empty finite* subset $E \subseteq I$, we consider the submodule

$$M^E := \sum_{i\in E} ke_i \subseteq M, \tag{s3}$$

which is a direct summand, and the element

$$\mathbf{x}^E := \sum_{i\in E} e_i \otimes \mathbf{t}_i \in M^E_{k[\mathbf{T}]} \subseteq M_{k[\mathbf{T}]}. \tag{s4}$$

We claim the annihilator of $\mathbf{x}^E$ in $k[\mathbf{T}]$ is zero; indeed, for $f(\mathbf{T}) \in k[\mathbf{T}]$ the relation $f(\mathbf{T})\mathbf{x}^E = 0$ implies $\sum e_i \otimes (\mathbf{t}_i f(\mathbf{T})) = 0$, hence $\mathbf{t}_i f(\mathbf{T}) = 0$ for all $i \in E$ and then $f(\mathbf{T}) = 0$ since $\mathbf{t}_i$ is not a zero divisor in $k[\mathbf{T}]$. Invoking the strict

Dickson condition, we therefore find a unique polynomial $g(\mathbf{T}) \in k[\mathbf{T}]$ such that

$$s(\mathbf{x}^E) = g(\mathbf{T})\mathbf{x}^E.$$

Specializing this relation with an additional variable $\mathbf{u}$ to $\mathbf{uT}$, we obtain $g(\mathbf{uT})\mathbf{ux}^E = s(\mathbf{ux}^E) = \mathbf{u}^2 s(\mathbf{x}^E) = (\mathbf{u}g(\mathbf{T}))\mathbf{ux}^E$, so the polynomial $g(\mathbf{T}) \in k[\mathbf{T}]$ is homogeneous of degree 1. Thus there exists a unique linear form $t^E\colon M^E \to k$ satisfying the relation $s(x) = t^E(x)x$ for all $x \in M^E$ because any such $t^E$ will be converted into the linear homogeneous polynomial $g(\mathbf{T})$ after extending scalars from $k$ to $k[\mathbf{T}]$. Here the uniqueness condition implies that the linear forms $t^E$ as $E$ varies over the non-empty finite subsets of $I$ glue to give a linear form $t\colon M \to k$ such that $s(x) = t(x)x$ for all $x \in M$. Combining with (s2), we obtain the relation

$$x^2 - t(x)x + n(x)1_C = 0 \tag{s5}$$

for all $x \in M$. We now extend $t, n$ as given on $M$ to all of $C$ by

$$t(\alpha 1_C + x) = 2\alpha + t(x), \quad n(\alpha 1_C + x) = \alpha^2 + \alpha t(x) + n(x) \quad (\alpha \in k,\ x \in M)$$

and then conclude from a straightforward computation that (s5) holds for all $x \in C$. Since we also have $t = n(1_C, -)$, it follows that $C$ is a conic algebra.

**16.23** For the first part, assume $k \neq \{0\}$ is connected and let $c \in C$. If $n_C(c) = 0$ and $t_C(c) = 1$, then $c$ is an idempotent by (16.5.1) which cannot be zero since $t_C(c) = 1$, and cannot be 1 since $n_C(c) = 0$. Conversely, let $c \in C$ be an idempotent $\neq 0, 1_C$. From Exc. 16.18 (a) we deduce that $n_C(c) \in k$ is an idempotent. If $n_C(c) = 1$, then $c$ is invertible in $k[c]$ (Exc. 16.18 (b)), whence the relation $c(1_C - c) = 0$ implies $c = 1_C$, a contradiction. Hence $n_C(c) = 0$, and (16.5.1) reduces to $c = c^2 = t_C(c)c$. Taking traces, we conclude that $t_C(c) \in C$ is an idempotent, which cannot be zero since this would imply $c = 0$. Thus $t_C(c) = 1$. We now proceed to establish the equivalence of (i)–(iv).

(i) $\Rightarrow$ (ii). This is clear.

(ii) $\Rightarrow$ (iii). For any prime ideal $\mathfrak{p} \subseteq k$, the ring $k_\mathfrak{p}$ is local, hence connected, and the first part of the problem yields $n_C(c)_\mathfrak{p} = n_{C_\mathfrak{p}}(c_\mathfrak{p}) = 0$, $t_C(c)_\mathfrak{p} = t_{C_\mathfrak{p}}(c_\mathfrak{p}) = 1_\mathfrak{p}$, and since this holds true for all $\mathfrak{p} \in \operatorname{Spec}(k)$, condition (iii) follows.

(iii) $\Rightarrow$ (iv). $c$ is clearly an idempotent. Moreover, the second condition of (iii) shows that $c$ is unimodular, and since $t_C(1_C - c) = 2 - 1 = 1$, so is $1_C - c$.

(iv) $\Rightarrow$ (i). Unimodularity is stable under base change, so for $R \in k$-**alg**, $R \neq \{0\}$, the elements $c_R$ and $1_{C_R} - c_R$ are both different from zero. Hence (i) holds.

**16.24** (a) Let $\mathfrak{a}$ be an ideal in $k$. An element of the ideal $\mathfrak{a}C \subseteq C$ has the form

$x = \sum \alpha_i x_i$, $\alpha_i \in \mathfrak{a}$, $x_i \in C$, and expanding $n_C(x)$ accordingly, we conclude $n_C(x) \in \mathfrak{a}$; the relation $n_C(x,y) \in \mathfrak{a}$ for $y \in C$ is even more obvious. Thus $(\mathfrak{a}, \mathfrak{a}C)$ is a conic ideal in $C$. By definition, the ideal $\mathfrak{a}C \subseteq C$ is the smallest one with this property. Now let $I$ be an ideal in $C$ and write $\mathfrak{a}$ for the ideal in $k$ generated by the expressions $n_C(x)$, $n_C(x,y)$ for $x \in I$, $y \in C$. By (1), the solution of (a) will be complete once we have shown that $(\mathfrak{a}, I)$ is a conic ideal in $C$. Since $n_C(x)1_C = x\bar{x}$ and $n_C(x,y)1_C = x\bar{y} + y\bar{x}$ by (16.5.6) and its bilinearization, we clearly have $\mathfrak{a}C \subseteq I$, while (1) is trivially fulfilled.

(b) follows from a straightforward computation using (16.17.2).

(c) Since $\mathfrak{a}C \subseteq I$, the $k$-algebra $C_0 := C/I$ carries a unique $k_0$-algebra structure making $\pi$ a $\sigma$-semi-linear homomorphism of unital algebras. From (1) we deduce that there is a unique set map $n_{C_0} : C_0 \to k_0$ making a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\pi} & C_0 \\ {\scriptstyle n_C}\downarrow & & \downarrow{\scriptstyle \exists!\, n_{C_0}} \\ k & \xrightarrow[\sigma]{} & k_0. \end{array} \tag{s1}$$

Since $\sigma$ and $\pi$ are both surjective, one checks that $n_{C_0}$ is, in fact, a quadratic form over $k_0$ making $C_0$ a conic $k_0$-algebra. Now (s1) , being a commutative diagram of set maps, shows that $\pi : C \to C_0$ is a $\sigma$-semi-linear homomorphism of conic algebras having $\mathrm{Ker}(\sigma, \pi) = (\mathfrak{a}, I)$, as claimed.

**16.25** (a) Suppose first that $\mathfrak{a}$ is a nil ideal in $k$. For $x \in I$, we deduce from (1) in Exc. 16.24 that $n_C(x)$ and $t_C(x) = n_C(x, 1_C)$ both belong to $\mathfrak{a}$, so $x$ by Exc. 16.18 (c) is nilpotent. Thus $I$ is a nil ideal in $C$. Conversely, let this be so. Then $\mathfrak{a}C \subseteq I$ is a nil ideal in $C$, forcing in particular $\alpha 1_C$ to be nilpotent for all $\alpha \in \mathfrak{a}$. By Exc. 16.18 (c) again, this implies that $\alpha^2 = n_C(\alpha 1_C)$ is nilpotent, so $\mathfrak{a}$ is a nil ideal in $k$.

(b) We have $\mathrm{Nil}(k)C \subseteq \mathrm{Nil}(C)$ by Exc. 7.13, so we need only show $n_C(x)$, $n_C(x,y) \in \mathfrak{a} := \mathrm{Nil}(k)$ for all $x \in I := \mathrm{Nil}(C)$, $y \in C$. The first inclusion being obvious, we turn to the second by combining the ideal property of $I$ with (16.5.5):

$$I \ni xy + yx = t_C(x)y + t_C(y)x - n_C(x,y)1_C,$$

where $t_C(x)y \in \mathfrak{a}C \subseteq I$ by hypothesis and $t_C(y)x \in I$ for trivial reasons. Thus $n_C(x,y)1_C \in I$, and we conclude $n_C(x,y)^2 = n_C(n_C(x,y1)_C) \in \mathfrak{a}$, hence $n_C(x,y) \in \mathfrak{a}$.

(c) Let $c \in \pi^{-1}(c_0)$ be an idempotent in $C$. Then $\pi(c) = c_0$, and (16.17.2) shows $\sigma(n_C(c)) = n_{C_0}(c_0) = 0$, so $n_C(c) \in \mathfrak{a}$ is nilpotent. But by Exc. 16.18 (a), it is also an idempotent, and we conclude $n_C(c) = 0$. Similarly, $\sigma(t_C(c)) =$

$t_{C_0}(c_0) = 1$, forcing $t_C(c) \in 1 + \mathfrak{a}$ to be invertible. On the other hand, applying $t_C$ to the equation $c = c^2 = t_C(c)c$ (by (16.5.1)), it follows that $t_C(c)$ is an idempotent. Thus $t_C(c) = 1$, and we have shown that the idempotent $c \in C$ is elementary.

**16.26** Recall from (9.7.1), (9.7.2) that there is a natural identification $M_R = \varepsilon M$ as $R$-modules such that $x_R = x \otimes \varepsilon = \varepsilon x$ for all $x \in M$.

(ii) $\Leftarrow$ (i). Obvious.

(i) $\Rightarrow$ (ii). If $c \in C$ is an idempotent, then (16.5.8) implies $t_C(c) = t_C(c^2) = t_C(c)^2 - 2n_C(c)$, hence

$$t_C(c)(1 - t_C(c)) = -2n_C(c). \tag{s1}$$

The quantities $\varepsilon^{(i)}$, $i = 0, 1, 2$, as defined in (1) obviously satisfy $\sum \varepsilon^{(i)} = 1$, while the fact that $n_C(c) \in C$ is an idempotent by Exc. 16.18 (a) combined with (s1) implies $\varepsilon^{(i)}\varepsilon^{(j)} = 0$ for $i, j = 0, 1, 2$ distinct. Thus they form a complete orthogonal system of idempotents in $k$. Our preliminary remark shows $C^{(i)} = C_{k^{(i)}}$ and $c = \sum c^{(i)}$, where $c^{(i)} = c_{k^{(i)}} = \varepsilon^{(i)}c$ for $i = 0, 1, 2$. We now compute $c^{(0)} = \varepsilon^{(0)}c = (1-n_C(c))(1-t_C(c))c$, where $(1-t_C(c))c = c^2-t_C(c)c = -n_C(c)1_C$, which implies $c^{(0)} = 0$. Next we turn to

$$c^{(1)} = \varepsilon^{(1)}c = (1 - n_C(c))t_C(c)c = (1 - n_C(c))(c + n_C(c)1_C) = (1 - n_C(c))c,$$

which together with (s1) implies

$$\begin{aligned} t_C(c^{(1)}) &= \varepsilon^{(1)}t_C(c) = (1 - n_C(c))t_C(c)^2 = (1 - n_C(c))(t_C(c) + 2n_C(c)) \\ &= (1 - n_C(c))t_C(c) = \varepsilon^{(1)} = 1_{k^{(1)}}, \\ n_C(c^{(1)}) &= \varepsilon^{(1)}n_C(c) = (1 - n_C(c))t_C(c)n_C(c) = 0. \end{aligned}$$

Thus $c^{(1)} \in C^{(1)}$ is an elementary idempotent. Finally,

$$c^{(2)} = \varepsilon^{(2)}c = n_C(c)c,$$

which implies $n_C(c^{(2)}) = \varepsilon^{(2)}n_C(c) = \varepsilon^{(2)} = 1_{C^{(2)}}$. Thus $c^{(2)} \in C^{(2)}$ is an invertible idempotent in the sense of Exc. 16.18 (b), forcing $c^{(2)} = 1_{C^{(2)}}$, as claimed. The statement just proved implies $t_C(c^{(2)}) = 2$ in $k^{(2)}$. This can also be proved directly by noting

$$(2 - t_C(c))\varepsilon^{(2)} = 2n_C(c) - t_C(c)n_C(c) = n_C(c, c^2) - t_C(c)n_C(c)$$

which is zero by (s2) of the solution to Exc. 16.18.

It remains to prove uniqueness of the $\varepsilon^{(i)}$, so let $\eta^{(i)}$, $i = 0, 1, 2$, be any complete orthogonal system of idempotents in $C$ satisfying mutatis mutandis the conditions of (ii), and define the $\varepsilon^{(i)}$, $i = 0, 1, 2$, as in (1). Then $n_C(c^{(i)}) = n_C(\eta^{(i)}c) = \eta^{(i)}n_C(c) = n_C(c)_{k^{(i)}} = n_{C^{(i)}}(c^{(i)})$ and, similarly, $t_C(c^{(i)}) = t_{C^{(i)}}(c^{(i)})$

for $i = 0, 1, 2$. Since $c^{(1)} \in C^{(1)}$ is an elementary idempotent and $c^{(2)} = 1_{C^{(2)}}$ by hypothesis, this implies

$$n_C(c) = (0, n_{C^{(1)}}(c^{(1)}), n_{C^{(2)}}(c^{(2)})) = (0, 0, 1_{k^{(2)}}) = \eta^{(2)},$$
$$t_C(c) = (0, t_{C^{(1)}}(c^{(1)}), t_{C^{(2)}}(c^{(2)})) = (0, 1_{k^{(1)}}, 2 \cdot 1_{k^{(2)}}) = \eta^{(1)} + 2\eta^{(2)},$$

hence $\eta^{(2)} = n_C(c) = \varepsilon^{(2)}$ and $\eta^{(1)} = t_C(c) - 2n_C(c)$. But the idempotents $\eta^{(1)}, \eta^{(2)}$ are orthogonal, which implies $t_C(c)n_C(c) = 2n_C(c)$, and we conclude $\eta^{(1)} = t_C(c)(1 - n_C(c)) = \varepsilon^{(1)}$ by (1). Since the orthogonal systems formed by the $\eta$'s and by the $\varepsilon$'s are both complete, we also have $\eta^{(0)} = \varepsilon^{(0)}$, as claimed.

**16.27** If $C$ is a conic $k$-algebra with trivial conjugation, then $2x = t_C(x)1_C$ for all $x \in C$ by (16.5.4). Since the trace form of $C$ is surjective, we find an element $u \in C$ satisfying $t_C(u) = 1$. This implies $2u = 1_C$, hence $x = 2ux = t_C(ux)1_C$. But $C$ is a faithful $k$-module. Hence $C \cong k$ as conic algebras. The converse is obvious.

**16.28** For the first part we have to show $n_C(x, [y, y]) = 0 = n_C(x, [x, y])$ for all $x, y \in C$. The first assertion is obvious, while the second one follows from $n_C(x, [x, y]) = n_C(x, xy) - n_C(x, yx)$ and (16.12.2), (16.12.1). In order to establish (1), (2), we expand $n_C(x \circ y)$ by using (16.5.5), (16.5.2) to obtain

$$\begin{aligned} n_C(x \circ y) &= n_C(t_C(x)y + t_C(y)x - n_C(x, y)1_C) \\ &= t_C(x)^2 n_C(y) + t_C(x)t_C(y)n_C(x, y) - t_C(x)t_C(y)n_C(x, y) \\ &\quad + t_C(y)^2 n_C(x) - t_C(x)t_C(y)n_C(x, y) + n_C(x, y)^2 \\ &= t_C(x)^2 n_C(y) + t_C(y)^2 n_C(x) + n_C(x, y)^2 - t_C(x)t_C(y)n_C(x, y), \end{aligned}$$

and (16.5.10) yields

$$n_C(x \circ y) = t_C(x)^2 n_C(y) + t_C(y)^2 n_C(x) - n_C(x, y)n_C(x, \bar{y}). \tag{s1}$$

Now let $\varepsilon = \pm 1$. From (16.5.5), (16.12.2), (16.12.1), (16.12.5) we deduce

$$\begin{aligned} n_C(xy + \varepsilon yx) &= n_C(xy) + \varepsilon n_C(xy, yx) + n_C(yx) \\ &= n_C(xy) + (1 - 2\varepsilon)n_C(yx) + \varepsilon n_C(x \circ y, yx) \\ &= n_C(xy) + (1 - 2\varepsilon)n_C(yx) \\ &\quad + \varepsilon(t_C(x)^2 n_C(y) + t_C(y)^2 n_C(x) - n_C(x, y)n_C(x, \bar{y})), \end{aligned}$$

and (s1) implies

$$n_C(xy + \varepsilon yx) = n_C(xy) + (1 - 2\varepsilon)n_C(yx) + \varepsilon n_C(x \circ y).$$

Setting $\varepsilon = 1$ in the last equation yields (1), while setting $\varepsilon = -1$ and using (1), (s1) yields (2).

## Solutions for Section 17

**17.8** For the subsequent computations it is important to note

$$(\alpha.\beta_0)\varepsilon = (\alpha\beta_0)\varepsilon \qquad (\alpha \in k,\ \beta_0 \in k_0) \tag{s1}$$

since, for $\alpha = \alpha_0 + \alpha_0'\varepsilon$, $\alpha_0, \alpha_0' \in k_0$, the right-hand side becomes $(\alpha_0\beta_0 + (\alpha_0'\beta_0)\varepsilon)\varepsilon = (\alpha_0\beta_0)\varepsilon = (\alpha.\beta_0)\varepsilon$, as claimed.

Turning to the exercise itself, we begin by showing associativity. Writing $(e_i)_{1\le i\le 3}$ for the canonical basis of $k_0^3$ over $k_0$, we deduce from (1) that $[k_0^3, k_0^3] = k_0 e_3$ and $[e_3, k_0^3] = \{0\}$, hence $[[k_0^3, k_0^3], k_0^3] = \{0\} = [k_0^3, [k_0^3, k_0^3]]$. Now let $\alpha, \beta, \gamma \in k$ and $u, v, w \in k_0^3$. Then

$$\begin{aligned}
((\alpha,u)(\beta,v))(\gamma,w) &= (\alpha\beta, \alpha.v + \beta.u + [u,v])(\gamma,w)\\
&= (\alpha\beta\gamma, (\alpha\beta).w + (\gamma\alpha).v + (\beta\gamma).u + \gamma.[u,v]\\
&\quad + \alpha.[v,w] + \beta.[u,w] + [[u,v],w]),\\
(\alpha,u)((\beta,v)(\gamma,w)) &= (\alpha,u)(\beta\gamma, \beta.w + \gamma.v + [v,w])\\
&= (\alpha\beta\gamma, (\alpha\beta).w + (\gamma\alpha).v + \alpha.[v,w]\\
&\quad + (\beta\gamma).u + \beta.[u,w] + \gamma.[u,v] + [u,[v,w]]),
\end{aligned}$$

and the preceding observation shows $[[u,v],w] = [u,[v,w]] = 0$. Hence $C$ is associative.

The algebra $C$ is obviously unital with identity element $1_C = (1,0)$, and the quadratic form $n_z$ obviously satisfies $n_z(1_C) = 1$. Moreover, (s1) yields

$$n_z((\alpha,u)) = \alpha^2 + (\alpha z^{\mathsf{T}} u)\varepsilon \qquad (\alpha \in k,\ u \in k_0^3),$$

and we have

$$n_z((\alpha,u),(\beta,v)) = 2\alpha\beta + (\alpha z^{\mathsf{T}} v + \beta z^{\mathsf{T}} u)\varepsilon \qquad (\alpha,\beta \in k,\ u,v, \in k_0^3),$$

hence

$$t_z((\alpha,u)) := n_z(1_C,(\alpha,u)) = 2\alpha + (z^{\mathsf{T}} u)\varepsilon.$$

Comparing

$$(\alpha,u)^2 = (\alpha^2, 2\alpha.u)$$

with

$$\begin{aligned}
t_z((\alpha,u))(\alpha,u) - n_z((\alpha,u))1_C &= (2\alpha + (z^{\mathsf{T}} u)\varepsilon)(\alpha,u) - (\alpha^2 + (\alpha z^{\mathsf{T}} u)\varepsilon)(1,0)\\
&= (2\alpha^2 + (\alpha z^{\mathsf{T}} u)\varepsilon - \alpha^2 - (\alpha z^{\mathsf{T}} u)\varepsilon,\\
&\quad (2\alpha + (z^{\mathsf{T}} u)\varepsilon).u)\\
&= (\alpha^2, 2\alpha.u),
\end{aligned}$$

we see that $C$ is indeed a conic $k$-algebra with norm $n_z$ and trace $t_z$. We now turn to the equivalence of (i)–(iv). By Props. 17.2 and 16.14, we have (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Thus it remains to show (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

(iii) $\Rightarrow$ (iv). Since the conjugation of $C$ is an involution and $\mathrm{Ann}(C) = \{0\}$, we conclude from Prop. 16.10 that $t_z(xy) = n_z(x, \bar{y})$ for all $x, y \in C$. Writing $x = \alpha \oplus u$, $y = \beta \oplus v$, $\alpha, \beta \in k$, $u, v \in k_0^3$, we apply (s1) and obtain

$$\begin{aligned}
t_z(xy) &= t_z((\alpha\beta, \alpha.v + \beta.u + [u, v])) = 2\alpha\beta + (z^{\mathsf{T}}(\alpha.v + \beta.u + [u, v]))\varepsilon \\
&= 2\alpha\beta + (\alpha.(z^{\mathsf{T}}v) + \beta.(z^{\mathsf{T}}u) + z^{\mathsf{T}}[u, v])\varepsilon \\
&= 2\alpha\beta + (\alpha z^{\mathsf{T}}v + \beta z^{\mathsf{T}}u + z^{\mathsf{T}}[u, v])\varepsilon, \\
\bar{y} &= t_z((\beta, v))1_C - (\beta, v) = (2\beta + (z^t v)\varepsilon)(1, 0) - (\beta, v) = (\beta + (z^t v)\varepsilon, -v), \\
n_z(x, \bar{y}) &= n_z\Big((\alpha, u), (\beta + (z^{\mathsf{T}}v)\varepsilon, , -v)\Big) \\
&= 2\alpha\beta + 2\alpha z^{\mathsf{T}}v\varepsilon + ( - \alpha z^t v + \beta z^{\mathsf{T}}u + (z^t v)\varepsilon u)\varepsilon \\
&= 2\alpha\beta + (\alpha z^{\mathsf{T}}v + \beta z^{\mathsf{T}}u)\varepsilon.
\end{aligned}$$

Comparing, we conclude $z^{\mathsf{T}}[u, v] = 0$ for all $u, v \in k_0^3$, and specializing $u = e_1$, $v = e_2$, $(e_i)_{1 \le i \le 3}$ being the $k_0$-basis of unit vectors in $k_0^3$, yields $\delta_3 = 0$, hence (iv).

(iv) $\Rightarrow$ (i). For $\alpha, \beta \in k$, $u, v \in k_0^3$, we compute

$$\begin{aligned}
n_z((\alpha, u)(\beta, v)) &= n_z((\alpha\beta, \alpha.v + \beta.u + [u, v])) \\
&= (\alpha\beta)^2 + ((\alpha^2\beta)z^{\mathsf{T}}v + (\alpha\beta^2)z^{\mathsf{T}}u + (\alpha\beta)z^{\mathsf{T}}[u, v])\varepsilon, \\
n_z((\alpha, u))n_z((\beta, v)) &= (\alpha^2 + (\alpha z^{\mathsf{T}}u)\varepsilon)(\beta^2 + (\beta z^{\mathsf{T}}v)\varepsilon) \\
&= \alpha^2\beta^2 + (\alpha^2\beta z^{\mathsf{T}}v + \alpha\beta^2 z^{\mathsf{T}}u)\varepsilon.
\end{aligned}$$

By definition of the algebra $A$, the $e_1$- and $e_2$-components of $[u, v]$ are both zero, as is the $e_3$-component of $z$, by (iv). Hence $z^{\mathsf{T}}[u, v] = 0$, and we conclude that $n_z$ permits composition, i.e., the conic algebra $C$ with norm $n_z$ is multiplicative.

**17.9** By Prop. 17.2 (a), $C$ is norm-associative. We put

$$N := \{x \in C \mid n_C(x), n_C(x, y) \in \mathrm{Nil}(k) \text{ for all } y \in C\}$$

It is straightforward to check that $N \subseteq C$ is a $k$-submodule. We claim that it is, in fact, an ideal. In order to see this, let $x \in N$ and $y, z \in C$. By multiplicativity, $n_C(xy) = n_C(x)n_C(y) = n_C(yx)$ is nilpotent, while norm-associativity yields the same for $n_C(xz, y) = n_C(x, y\bar{z})$ and $n_C(zx, y) = n_C(x, \bar{z}y)$. Thus $xz$ and $zx$ both belong to $N$, forcing $N$ to be an ideal in $C$. Since $n_C(x)$ and $t_C(x) = n_C(x, 1_C)$ are nilpotent, so is $x$ by Exc. 16.18 (c). Hence $N \subseteq C$ is a nil ideal and as such contained in the nil radical of $C$. Conversely, let $x \in \mathrm{Nil}(C)$. Then $x$ is

nilpotent, as is $x\bar{y} \in \mathrm{Nil}(C)$ for all $y \in C$. Consulting Exc. 16.18 (c) again, we see that $n_C(x)$ and $n_C(x,y) = t_C(x\bar{y})$ belong to $\mathrm{Nil}(k)$, which implies $x \in N$ and completes the proof.

**17.10** For the first part we must show that the submodule $M$ of $C$ spanned by the elements $1_C, x, y, xy$ is, in fact, a subalgebra, i.e., it is closed under multiplication. In order to see this, we apply the alternative laws, the identities of 16.5, and (17.4.2) to obtain

$$\begin{aligned} z^2 &= t_C(z)z - n_C(z)1_C \in M && (z \in \{x, y, xy\}),\\ x(xy) &= x^2y = t_C(x)xy - n_C(x)y \in M,\\ (xy)x &= n_C(x,\bar{y})x - n_C(x)\bar{y} = n_C(x,\bar{y})x - n_C(x)t_C(y)1_C + n_C(x)y,\\ yx &= x \circ y - xy = t_C(x)y + t_C(y)x - n_C(x,y)1_C - xy \in M. \end{aligned}$$

By symmetry, therefore, $M$ is closed under multiplication, giving the first part of the problem. As to the second, it suffices to verify the associative law on the generators of $M$, which is straightforward.

**17.11** Abbreviating $1 := 1_C$, $n := n_C$, $t := t_C$ and expanding the norm of an associator, we obtain

$$n([x_1,x_2,x_3]) = n((x_1x_2)x_3) - n((x_1x_2)x_3, x_1(x_2x_3)) + n(x_1(x_2x_3)),$$

where multiplicativity of the norm yields

$$n([x_1,x_2,x_3]) = 2n(x_1)n(x_2)n(x_3) - n((x_1x_2)x_3, x_1(x_2x_3)). \tag{s1}$$

Turning to the second summand on the right of (s1), we obtain, by (17.1.4),

$$n((x_1x_2)x_3, x_1(x_2x_3)) = n(x_1x_2, x_1)n(x_3, x_2x_3) - n((x_1x_2)(x_2x_3), x_1x_3).$$

Since $C$ is norm associative by Prop. 17.2, we may apply apply (16.12.2) to the first summand on the right, which yields

$$n((x_1x_2)x_3, x_1(x_2x_3)) = t(x_2)^2n(x_3)n(x_1) - n((x_1x_2)(x_2x_3), x_1x_3). \tag{s2}$$

Manipulating the expression $(x_1x_2)(x_2x_3)$ by means of (16.5.5) and the middle Moufang identity (13.3.3), we obtain

$$\begin{aligned} (x_1x_2)(x_2x_3) &= (x_1x_2) \circ (x_2x_3) - (x_2x_3)(x_1x_2)\\ &= t(x_1x_2)x_2x_3 + t(x_2x_3)x_1x_2 - n(x_1x_2, x_2x_3)1 - x_2(x_3x_1)x_2, \end{aligned}$$

where associativity of the trace (16.13.1) and (16.12.5),(17.4.2) yield

$$\begin{aligned} (x_1x_2)(x_2x_3) = {} & t(x_1x_2)x_2x_3 + t(x_2x_3)x_1x_2 - n(x_1x_2, x_2x_3)1 - \\ & t(x_1x_2x_3)x_2 + n(x_2)\overline{x_3x_1}. \end{aligned} \tag{s3}$$

Here we use (16.12.3),(16.5.4) to compute

$$n(x_1x_2, x_2x_3) = n(x_1, x_2x_3\bar{x}_2) = t(x_2)n(x_1, x_2x_3) - n(x_1, x_2x_3x_2),$$

and (16.12.5),(17.4.2) give

$$\begin{aligned} n(x_1x_2, x_2x_3) &= t(x_2)n(x_1, x_2x_3) - t(x_2x_3)n(x_1, x_2) + t(x_3x_1)n(x_2) \\ &= t(x_1)t(x_2)t(x_2x_3) - t(x_2)t(x_1x_2x_3) - t(x_1)t(x_2)t(x_2x_3) + \\ &\quad t(x_1x_2)t(x_2x_3) + t(x_3x_1)n(x_2), \end{aligned}$$

hence

$$n(x_1x_2, x_2x_3) = t(x_1x_2)t(x_2x_3) - t(x_2)t(x_1x_2x_3) + t(x_3x_1)n(x_2).$$

Inserting this into (s3), and (s3) into the second term on the right of (s2), we conclude

$$\begin{aligned} n\big((x_1x_2)(x_2x_3), x_1x_3\big) &= t(x_1x_2)n(x_2x_3, x_1x_3) + t(x_2x_3)n(x_1x_2, x_1x_3) - \\ &\quad t(x_1x_2)t(x_2x_3)t(x_3x_1) + t(x_2)t(x_3x_1)t(x_1x_2x_3) - \\ &\quad t(x_3x_1)^2n(x_2) - t(x_1x_2x_3)n(x_2, x_1x_3) + \\ &\quad n\big((x_3x_1)^*, x_1x_3\big)n(x_2) \\ &= t(x_1x_2)t(x_1x_2^*)n(x_3) + t(x_2x_3)t(x_2x_3^*)n(x_1) - \\ &\quad t(x_1x_2)t(x_2x_3)t(x_3x_1) + t(x_2)t(x_3x_1)t(x_1x_2x_3) - \\ &\quad t(x_3x_1)^2n(x_2) - t(x_2)t(x_3x_1)t(x_1x_2x_3) + \\ &\quad t(x_1x_2x_3)t(x_2x_1x_3) + t(x_3x_1^2x_3)n(x_2), \end{aligned}$$

where we may use (16.13.1), (16.5.1), (16.12.5) to expand

$$\begin{aligned} t(x_3x_1^2x_3)n(x_2) - t(x_3x_1)^2n(x_2) &= t(x_3^2x_1^2)n(x_2) - t(x_3x_1)^2n(x_2) \\ &= t\big([t(x_3)x_3 - n(x_3)1][t(x_1)x_1 - n(x_1)1]\big)n(x_2) - \\ &\quad t(x_3x_1)^2n(x_2) \\ &= t(x_3)t(x_1)t(x_3x_1)n(x_2) - t(x_1)^2n(x_2)n(x_3) - \\ &\quad t(x_3)^2n(x_1)n(x_2) + 2n(x_1)n(x_2)n(x_3) - \\ &\quad t(x_3x_1)^2n(x_2) \\ &= t(x_3x_1)t(x_3\bar{x}_1)n(x_2) - t(x_1)^2n(x_2)n(x_3) - \\ &\quad t(x_3)^2n(x_1)n(x_2) + 2n(x_1)n(x_2)n(x_3). \end{aligned}$$

Inserting the resulting expression

$$n((x_1x_2)(x_2x_3), x_1x_3) = \sum t(x_ix_j)t(x_ix_j^*)n(x_l) - t(x_1x_2)t(x_2x_3)t(x_3x_1) + t(x_1x_2x_3)t(x_2x_1x_3) - t(x_1)^2n(x_2)n(x_3) - t(x_3)^2n(x_1)n(x_2) + 2n(x_1)n(x_2)n(x_3)$$

into (s2) and (s2) into (s1), the assertion follows.

**17.12** From Prop. 15.3 combined with 15.7 we deduce that $C^{(p,q)}$ is a unital alternative $k$-algebra with identity element $1_C^{(p,q)} = (pq)^{-1}$. Defining $n_{C^{(p,q)}} := n_C(pq)n_C$, Prop. 17.5 yields $n_{C^{(p,q)}}(1_C^{(p,q)}) = 1$, and we have $n_{C^{(p,q)}}(x, y) = n_C(pq)n_C(x, y)$ for all $x, y \in C$, which implies

$$t_{C^{(p,q)}}(x) := n_{C^{(p,q)}}(1_C^{(p,q)}, x) = n_C(pq)n_C((pq)^{-1}, x) = n_C(\overline{pq}, x).$$

Writing $x^{(m,p,q)}$ for the $m$-th power of $x \in C$ in $C^{(p,q)}$, we apply (15.2.1), the middle Moufang identity (13.3.3) and (17.4.2) to conclude

$$\begin{aligned} x^{(2,p,q)} &= (xp)(qx) = x(pq)x = n_C(x, \overline{pq})x - n_C(x)\overline{pq} \\ &= t_{C^{(p,q)}}(x)x - n_{C^{(p,q)}}(x)(pq)^{-1} = t_{C^{(p,q)}}(x)x - n_{C^{(p,q)}}(x)1_C^{(p,q)}. \end{aligned}$$

Thus $C^{(p,q)}$ is a conic alternative $k$-algebra with norm and trace as indicated. Moreover,

$$\begin{aligned} \iota_{C^{(p,q)}}(x) &= t_{C^{(p,q)}}(x)1_C^{(p,q)} - x = n_C(\overline{pq}, x)(pq)^{-1} - x \\ &= n_C(pq)^{-1}(n_C(\overline{pq}, x)\overline{pq} - n_C(\overline{pq})x) = n_C(pq)^{-1}\overline{pq}\bar{x}\,\overline{pq}, \end{aligned}$$

giving the desired formula for the conjugation of $C^{(p,q)}$. Finally, if $C$ is multiplicative, then

$$\begin{aligned} n_{C^{(p,q)}}(x \cdot_{p,q} y) &= n_C(pq)n_C((xp)(qy)) = n_C(pq)n_C(x)n_C(p)n_C(q)n_C(y) \\ &= n_C(pq)n_C(x)n_C(pq)n_C(y) = n_{C^{(p,q)}}(x)n_{C^{(p,q)}}(y) \end{aligned}$$

for all $x, y \in C$, and $C^{(p,q)}$ is multiplicative as well.

## Solutions for Section 18

**18.18** We put $C := \mathrm{Cay}(B, \mu)$ and let $u_1, u_2, v_1, v_2 \in B$. Using the fact that $B$ is norm associative by Prop. 17.2 (a) and applying (18.4.1), (18.4.3) we obtain

$$\begin{aligned} n_C((u_1 + v_1 j)(u_2 + v_2 j)) &= n_C((u_1u_2 + \mu\bar{v}_2v_1) + (v_1\bar{u}_2 + v_2u_1)) \\ &= n_B(u_1u_2 + \mu\bar{v}_2v_1) - \mu n_C(v_1\bar{u}_2 + v_2u_1) \\ &= n_B(u_1)n_B(u_2) + \mu n_B(u_1u_2, \bar{v}_2v_1) + \mu^2 n_B(v_2)n_B(v_1) \\ &\quad - \mu n_B(v_1)n_B(u_2) - \mu n_B(v_1\bar{u}_2, v_2u_1) - \mu n_B(v_2)n_B(u_1) \\ &= (n_B(u_1) - \mu n_B(v_1))(n_B(u_2) - \mu n_B(v_2)) \\ &\quad + \mu n_B(v_2(u_1u_2), v_1) - \mu n_B(v_1, (v_2u_1)u_2)) \\ &= n_B(u_1 + v_1 j)n_B(u_2 + v_2 j) - \mu n_B([v_2, u_1, u_2], v_1), \end{aligned}$$

from which the assertion can be read off immediately.

**18.19** For $u_1, u_2, v_1, v_2 \in B$, we combine the hypothesis that $a$ belongs to the nucleus of $B$ with the fact that the conjugation of $B$ is an involution (Prop. 17.2) (a) to compute

$$\begin{aligned} \varphi(u_1 + v_1 j)\varphi(u_2 + v_2 j) &= (u_1 + (av_1)j)(u_2 + (av_2)j) \\ &= (u_1u_2 + \mu\overline{av_2}av_1) + ((av_2)u_1 + (av_1)\bar{u}_2)j \\ &= (u_1u_2 + \mu\bar{v}_2(\bar{a}a)v_1) + (a(v_2u_1 + v_1\bar{u}_2))j \\ &= (u_1u_2 + n_B(a)\mu\bar{v}_2v_1) + (a(v_2u_1 + v_1\bar{u}_2))j \\ &= \varphi\Big((u_1u_2 + n_B(a)\mu\bar{v}_2v_1) + (v_2u_1 + v_1\bar{u}_2)j\Big) \\ &= \varphi((u_1 + v_1 j)(u_2 + v_2 j)). \end{aligned}$$

Thus $\varphi$ is an obviously unital algebra homomorphism. Moreover, setting $C := \mathrm{Cay}(B, n_B(a)\mu)$, $C' := \mathrm{Cay}(B, \mu)$, we have, for all $u, v \in B$,

$$\begin{aligned} n_{C'} \circ \varphi(u + vj) = n_{C'}(u + (av)j) &= n_B(u) - \mu n_B(av) = n_B(u) - n_B(a)\mu n_B(v) \\ &= n_C(u + vj) \end{aligned}$$

since $B$ is multiplicative. Thus $\varphi$ is a homomorphism of conic algebras. The final statement is obvious.

**18.20** (iii) means the same in $C$ as in $C^{\mathrm{op}}$, while (i) in $C$ is equivalent to (ii) in $C^{\mathrm{op}}$. Hence it suffices to show (i) $\Leftrightarrow$ (iii).

(i) $\Rightarrow$ (iii). Assume $f := n_C(x)$ is not a zero divisor in $k$. We must show that $x$ is not a right zero divisor in $C$. By 18.8, $f$ is not a zero divisor in $C$, whence it follows from Bourbaki [7, II.2, Prop. 4] that the natural map $z \mapsto z_f = z/1$ from $C$ to $C_f$ is injective. On the other hand, $n_{C_f}(x_f) = n_C(x)_f = f_f \in k_f^\times$,

forcing $x_f$ to be invertible in $C_f$ (Prop. 17.5). Now suppose $y \in C$ satisfies $xy = 0$. Then $x_f y_f = (xy)_f = 0$ in $C_f$, hence $y_f = 0$, which by what we have just seen implies $y = 0$. Thus $x$ is not a right zero divisor of $C$.

(iii) $\Rightarrow$ (i). Assume $x$ is not a right zero divisor of $C$. We must show that $n_C(x)$ is not a zero divisor in $k$, so let $\alpha \in k$ satisfy $\alpha n_C(x) = 0$. Then $0 = \alpha x\bar{x} = x(\alpha\bar{x})$ implies $\alpha\bar{x} = 0$, hence $\alpha x = \overline{\alpha\bar{x}} = 0$. But this means $x(\alpha 1_C) = 0$, hence $\alpha 1_C = 0$, and since $1_C \in C$ is unimodular, we conclude $\alpha = 0$, as desired.

**18.21** We prove it for $R = k[\mathbf{t}]$. A nonzero element $f$ of $A_R$ can be written uniquely as $f = \sum_{i=0}^{m} f_i \mathbf{t}^i$ where $f_i \in A$ and $f_m \neq 0$. The element $f_m$ is called the leading coefficient of $f$. Let $g$ also be a nonzero element of $A_R$ and write $g = \sum_{i=0}^{n} g_i \mathbf{t}^i$ where $g_n \neq 0$. The product $fg$ has leading coefficient, the coefficient of $t^{m+n}$, $f_m g_n$.

Therefore, if $A_R$ has zero divisors $f$, $g$ such that $fg = 0$, then $f_m g_n = 0$ and $f_m$ is a zero divisor in $A$.

The converse is trivial. The $k[[\mathbf{t}]]$-case is similar

**18.22** We put $C := \mathrm{Cay}(B^{\mathrm{op}}, \mu)$, $C' := \mathrm{Cay}'(B, \mu)$ and define $\varphi\colon C \to C'^{\,\mathrm{op}}$ by

$$\varphi(u + vj) := u + j'v \qquad\qquad (u, v \in B).$$

Then $\varphi$ is a $k$-linear bijection, and indicating the products in $B^{\mathrm{op}}$ as well as in $C'^{\,\mathrm{op}}$ by "$\cdot$", but the ones in $B, C$ and $C'$ by juxtaposition, we obtain, for all $u_1, u_2, v_1, v_2 \in B$,

$$\begin{aligned}
\varphi(u_1 + v_1 j) \cdot \varphi(u_2 + v_2 j) &= (u_2 + j'v_2)(u_1 + j'v_1) \\
&= (u_2 u_1 + \mu v_1 \bar{v}_2) + j'(\bar{u}_2 v_1 + u_1 v_2) \\
&= (u_1 \cdot u_2 + \mu \bar{v}_2 \cdot v_1) + j'(v_1 \cdot \bar{u}_2 + v_2 \cdot u_1) \\
&= \varphi((u_1 \cdot u_2 + \mu \bar{v}_2 \cdot v_1) + (v_1 \cdot \bar{u}_2 + v_2 \cdot u_1) j) \\
&= \varphi((u_1 + v_1 j)(u_2 + v_2 j)).
\end{aligned}$$

Hence $\varphi$ is an algebra isomorphism. Transporting the norm of $C$ to $C'$ by means of $\varphi$, therefore, gives a quadratic form $n_{C'}$ on $C'$ making it a conic algebra isomorphic to $C$ under $\varphi$. Since the norms of $B$ and $B^{\mathrm{op}}$ coincide, we have $n_C = n_B \perp (-\mu) n_B$, which obviously implies

$$\begin{aligned}
n_{C'}(u + j'v) &= n_B(u) - \mu n_B(v), \\
t_{C'}(u + j'v) &= t_B(u), \\
\overline{u + j'v} &= \bar{u} - j'v
\end{aligned}$$

for all $u, v \in B$.

Finally, let us assume that the conjugation of $B$ is an involution. Then we

claim that

$$\psi\colon \operatorname{Cay}(B,\mu)^{\mathrm{op}} \xrightarrow{\sim} \operatorname{Cay}(B^{\mathrm{op}},\mu), \quad u+vj \longmapsto u+\bar{v}j,$$

is an isomorphism of conic algebras. Since $\psi$ is obviously bijective and preserves norms, it will be enough to show that it is an algebra homomorphism. Indeed, extending the previous conventions to $\operatorname{Cay}(B,\mu)^{\mathrm{op}}$, we obtain, for all $u_1,u_2,v_1,v_2 \in B$,

$$\begin{aligned}
\psi(u_1+v_1j)\psi(u_2+v_2j) &= (u_1+\bar{v}_1j)(u_2+\bar{v}_2j)\\
&= (u_1\cdot u_2+\mu v_2\cdot\bar{v}_1)+(\bar{v}_2\cdot u_1+\bar{v}_1\cdot\bar{u}_2)j\\
&= (u_2u_1+\mu\bar{v}_1v_2)+(u_1\bar{v}_2+\bar{u}_2\bar{v}_1)j\\
&= (u_2u_1+\mu\bar{v}_1v_2)+\overline{v_2\bar{u}_1+v_1u_2}\,j\\
&= \psi\big((u_2u_1+\mu\bar{v}_1v_2)+(v_2\bar{u}_1+v_1u_2)j\big)\\
&= \psi\big((u_2+v_2j)(u_1+v_1j)\big) = \psi\big((u_1+v_1j)\cdot(u_2+v_2j)\big),
\end{aligned}$$

as claimed. Combining we obtain an isomorphism $\varphi\circ\psi\colon \operatorname{Cay}(B,\mu)^{\mathrm{op}} \to \operatorname{Cay}'(B,\mu)^{\mathrm{op}}$, hence an isomorphism

$$\varphi\circ\psi\colon \operatorname{Cay}(B,\mu) \xrightarrow{\sim} \operatorname{Cay}'(B,\mu), \quad u+vj \longmapsto u+j'\bar{v},$$

of conic algebras.

## Solutions for Section 19

**19.26** (i) $\Rightarrow$ (ii). Since $(C,n,1_C)$ by (19.1.1) is a pointed quadratic module, the implication follows from Lemma 11.15.

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (i). By (19.1.2), (17.1.3), the quantity $\varepsilon := n(1_C) \in k$ is an idempotent with $\varepsilon n(x) = n(x)$, $\varepsilon n(x,y) = n(x,y)$ for all $x,y \in C$. Therefore the idempotent $\varepsilon' := 1-\varepsilon \in k$ satisfies $n(\varepsilon' 1_C) = \varepsilon'\varepsilon = 0$, $n(\varepsilon' 1_C, y) = \varepsilon'\varepsilon n(1_C,y) = 0$ for all $y \in C$, which implies $\varepsilon' 1_C = 0$ by non-degeneracy of $n$, hence $\varepsilon' = 0$ by (iii). Thus $n(1_C) = 1$.

**19.27** Let $K$ be a unital $F$-algebra of dimension 2. Then $K$ is quadratic, hence commutative associative (16.4), and we have $K = F[u]$ for any $u \in K \setminus F1_K$. Writing $\mu_u \in F[\mathbf{t}]$ for the minimum polynomial of $u$ over $F$, which is monic of degree 2, we have the following possibilities.

1°. $\mu_u$ is irreducible and separable. The $K/F$ is a separable quadratic field extension, and we are in Case (i).

2°. $\mu_u$ is reducible and separable. Then $\mu_u = (\mathbf{t}-\alpha)(\mathbf{t}-\beta)$ for some $\alpha, \beta \in F$, $\alpha \neq \beta$. Here the Chinese Remainder Theorem implies

$$K \cong F[\mathbf{t}]/(\mu_u) \cong F[\mathbf{t}]/(\mathbf{t}-\alpha) \times F[\mathbf{t}]/(\mathbf{t}-\beta) \cong F \oplus F$$

as a direct product of ideals, and we are in Case (ii).

3°. $\mu_u$ is irreducible and inseparable. Then $\mathrm{char}(F) = 2$ and $K/F$ is an inseparable quadratic field extension. Hence we are in Case (iii).

4°. $\mu_u$ is reducible and inseparable. Then $\mu_u = (\mathbf{t}-\alpha)^2$ for some $\alpha \in F$, which implies $K = F[v]$, where $v := u - \alpha 1_K$ satisfies $v^2 = 0 \neq v$. Hence the map $F[\varepsilon] \to K$ sending $\varepsilon$ to $v$ is an isomorphism of $F$-algebras, and we are in Case (iv).

For the second part of the problem, assume that $F$ is perfect of characteristic 2 and let $C$ be a conic $F$-algebra without nilpotent elements $\neq 0$. It will be enough to prove $\mathrm{Ker}(t_C) = F1_C$, where the inclusion "$\supseteq$" is obvious. Conversely, let $u \in \mathrm{Ker}(t_C)$ and assume $u \notin F1_C$. Then $K := F[u] \subseteq C$ is a two-dimensional subalgebra, so by what we have just proved, it satisfies one of the conditions (i)–(iv) above. If (i) or (ii) holds, then the trace of $K$ kills $1_K = 1_C$ but is not identically zero. Thus $\mathrm{Ker}(t_K) = F1_C$, forcing $t_C(u) = t_K(u) \neq 0$, a contradiction. Case (iii) cannot hold since $F$ is perfect, but neither can Case (iv) since $C$ does not contain nilpotent elements different from zero. This completes the proof.

**19.28** Let $I \neq C$ be a two-sided ideal of $(C, \iota_C)$. For $x \in C$ we obtain $n_C(x)1_C = x\bar{x} \in I$, which implies $n_C(x) = 0$. Moreover, for $y \in C$ we obtain $n_C(x,y)1_C = x\bar{y} + y\bar{x} \in I$, which implies $n_C(x,y) = 0$. But $n_C$ is non-degenerate. Thus $x = 0$, and we have shown $I = \{0\}$, so $(C, \iota_C)$ is simple as an algebra with involution. Here Prop. 10.5 shows that either $C$ is simple, or $(C, \iota_C) \cong (A \times A^{\mathrm{op}}, \varepsilon)$ for some simple unital $F$-algebra $A$, where $\varepsilon$ stands for the exchange involution. Identifying $C = A \times A^{\mathrm{op}}$ by means of this isomorphism and $A, A^{\mathrm{op}} \subseteq C$ canonically, we put $c := 1_A$, $c' := 1_{A^{\mathrm{op}}}$ and conclude from Exc. 16.23 that $c, c'$ are elementary idempotents in $C$ such that $1_C = c + c'$. For $x \in A$, we now obtain $2x = c \circ x = t_C(c)x + t_C(x)c - n_C(c,x)1_C = x + t_C(x)c - n_C(c,x)1_C$, hence

$$x = (t_C(x) - n_C(c,x))c - n_C(c,x)c'.$$

This shows $n_C(c,x) = 0$ and $x = t_C(x)c \in Fc$, and we have proved $A \cong F$, hence $A^{\mathrm{op}} \cong F$ as well. Thus $C \cong F \times F$ is split quadratic étale.

**19.29** We first show that *the norm of a conic divsion algebra over a field $F$ is anisotropic.* Indeed, let $C$ be a conic division algebra over $F$ and $0 \neq x \in C$.

Then $F[x] \subseteq C$ is a unital subalgebra of dimension at most 2, and left multiplication by $x$ gives a linear injection from $F[x]$ to itself, which therefore is a bijection. Hence $x$ is invertible in $F[x]$, which implies $n_C(x) \neq 0$ by Exc. 16.18 (b) and proves our claim. For the rest of the proof, we assume that $F$ is a field of arbitrary characteristic, $\mu \in F$ is a non-zero scalar, $B$ is an octonion algebra over $F$ and $C = \mathrm{Cay}(B, \mu) = B \oplus Bj$.

(a) Isotropic regular quadratic forms over $F$ are known to be universal. The assumption $\mu \notin n_B(B^\times)$ therefore implies that $n_B$ is anisotropic, forcing $B$ to be an octonion division algebra by Thm. 19.13 combined with Prop. 17.5. Now (18.4.1) implies

$$x_1x_2 = (u_1u_2 + \mu\bar{v}_2v_1) + (v_2u_1 + v_1\bar{u}_2)j,$$

and we conclude

$$x_1x_2 = 0 \quad \Longleftrightarrow \quad u_1u_2 = -\mu\bar{v}_2v_1, \;\; v_2u_1 = -v_1\bar{u}_2. \tag{s1}$$

Suppose first $x_1x_2 = 0$. If $u_1 = 0$, then $v_1 \neq 0$ and (s1) implies $v_2 = u_2 = 0$, hence $x_2 = 0$, a contradiction. Thus $u_1 \neq 0$. If $u_2 = 0$, then (s1) again implies $v_2 = 0$. This contradiction shows $u_2 \neq 0$. Since $B$ is a division algebra, the first equation of (s1) now implies $v_1 \neq 0 \neq v_2$. We have thus shown $u_i \neq 0 \neq v_i$ for $i = 1, 2$. Next, since the norm of $B$ is multiplicative, (s1) yields first $n_B(u_1)n_B(u_2) = \mu^2 n_B(v_1)n_B(v_2)$ and then

$$n_B(u_1)^2 n_B(u_2) = \mu^2 n_B(v_1)n_B(v_2)n_B(u_1) = \mu^2 n_B(v_1)^2 n_B(u_2).$$

Thus $n_B(u_1) = \pm\mu n_B(v_1)$. But $n_B(u_1) = \mu n_B(v_1)$ is impossible since this and multiplicativity of $n_B$ would yield the contradiction $\mu \in n_B(B^\times)$. Hence (i) holds. Turning to (ii), we use (s1), (i) and Kirmse's identities (17.4.1) to compute

$$\begin{aligned}(u_1u_2)\bar{v}_1 &= -\mu(\bar{v}_2v_1)\bar{v}_1 = -\mu n_B(v_1)\bar{v}_2 = n_B(u_1)\bar{v}_2 = u_1(\bar{u}_1\bar{v}_2)\\ &= -u_1\overline{v_1\bar{u}_2} = -u_1(u_2\bar{v}_1),\end{aligned}$$

and this is (ii). Finally, (iii) is equivalent to the second equation of (s1). Conversely, suppose $u_i \neq 0 \neq v_i$ for $i = 1, 2$ and (i)–(iii) hold. Then so does the second equation of (s1), and (i), (ii) imply

$$\begin{aligned}(u_1u_2)\bar{v}_1 &= -u_1(u_2\bar{v}_1) = -u_1\overline{v_1\bar{u}_2} = u_1(\bar{u}_1\bar{v}_2) = n_B(u_1)\bar{v}_2\\ &= -\mu n_B(v_1)\bar{v}_2 = -\mu(\bar{v}_2v_1)\bar{v}_1.\end{aligned}$$

But $\bar{v}_1$, being different from zero, is invertible in $B$. Hence the first equation of (s1) holds as well. This completes the proof of (a).

(b) We know already that if $C$ is a division algebra, then $n_C$ is anisotropic.

Conversely, suppose $n_C = n_B \perp (-\mu)n_B$ (cf. Remark 18.5) is anisotropic. Assuming $\mu = n_B(u)$ for some $u \in B^\times$ would lead to the contradiction $n_C(u + j) = 0$. Thus $\mu \notin n_B(B^\times)$. If $C$ were not a division algebra, some $x_i = u_i + v_i j$, $u_i, v_i \in B$, $i = 1, 2$, would satisfy the conditions of (a). In particular, since we are in characteristic 2, condition (i) would imply $n_C(x_1) = n_B(u_1) + \mu n_B(v_1) = 0$, in contradiction to $n_C$ being anisotropic. Hence $C$ is a division algebra.

(c) Suppose first $x, y \in A$, $z \in A^\perp$ for some quaternion subalgebra $A \subseteq B$ and $x \circ y = 0$, equivalently, $xy = -yx$. Then we may identify $B = \mathrm{Cay}(A, \nu) = A \perp Ai$ for some non-zero scalar $\nu \in F$ (Thm. 19.16 (a)) and have $A^\perp = Ai$, hence $z = ui$ for some $u \in A$. Now we use (18.4.1) and compute

$$\begin{aligned}(xy)z &= (xy)(ui) = (uxy)i,\\ x(yz) &= x(y(ui)) = x((uy)i) = (uyx)i = -(uxy)i.\end{aligned}$$

Hence $(xy)z = -x(yz)$, as desired. Conversely, let this be so. Since $\mathrm{char}(F) \neq 2$ and $B$ is alternative, we have $x \notin F1_B$, $y \notin F[x]$. Let $A$ be the (unital) subalgebra of $B$ generated by $x, y$. Since $B$ is a division algebra, so is $A$, forcing its norm to be anisotropic, hence regular. Since, therefore, $A$ is a composition algebra of dimension at least 3 and at most 4 (Exc. 17.10), it must, in fact, be a quaternion algebra. As before, we may assume $B = \mathrm{Cay}(A, \nu) = A \perp Ai$ for some $\nu \in F^\times$. Then $z = u + vi$, $u, v \in A$, and we conclude

$$\begin{aligned}(xy)z &= xyu + (\nu xy)i,\\ -x(yz) &= -x(yu + (vy)i) = -xyu - (vyx)i.\end{aligned}$$

Comparing coefficients, this implies $xyu = \nu(x \circ y) = 0$, hence $u = 0$. But then $\nu \neq 0$, forcing $x \circ y = 0$ and $z = vi \in A^\perp$.

(d) Suppose first that $C$ is a division algebra. Then its norm is anisotropic, and we have seen in (b) that this implies $\mu \notin n_B(B^\times)$. Assume now $-\mu = n_B(z)$ for some element $z \in B$ of trace zero. Pick any non-zero element $y \in F[z]^\perp$ and write $A'$ for the subalgebra of $B$ generated by $y, z$. The argument produced in the proof of (c) shows that $A'$ is a quaternion subalgebra of $B$. Pick any non-zero element $x \in A'^\perp \subseteq F[y]^\perp$. Then the subalgebra $A$ of $B$ generated by $x, y$ is again a quaternion algebra, and we have not only $n_B(z, 1_B) = n_B(z, x) = n_B(z, y) = 0$ but also (by norm associativity) $n_B(z, xy) = n_B(z\bar{y}, x) \in n_B(A', x) = \{0\}$. Thus $z \in A^\perp$, while (16.5.5) yields $x \circ y = 0$. Setting $u_1 := x$, $u_2 := y$, $v_1 := u_1 z^{-1} = -n_B(z)^{-1} u_1 z \in A^\perp$, $v_2 := -(v_1 \bar{u}_2)u_1^{-1}$, we have $\bar{v}_1 = -v_1 \in A^\perp$, whence (c) implies that conditions (i)–(iii) of (a) hold. Hence (a) produces zero divisors in $C$, a contradiction. Conversely, suppose $\mu \notin n_B(B^\times)$, $-\mu \notin n_B(B^0 \cap B^\times)$. If $C$ were not a division algebra, we would find elements $u_i, v_i \in B$, $i = 1, 2$ satisfying the conditions of (a). Then (c) would lead to a quaternion

subalgebra $A \subseteq B$ such that $u_1, u_2 \in A$, $\bar{v}_1 \in A^\perp$ and $u_1 \circ u_2 = 0$. This would imply $\bar{v}_1 = -v_1 \in A^\perp$ and $-\mu = n_B(z)$, $z := u_1 v_1^{-1} \in A^\perp$ and, in particular, $t_B(z) = 0$. This contradiction completes the proof.

(e) The norm of $\mathbb{O}$ is positive definite, and so is its restriction to the trace zero elements. Hence $1 = -(-1)$ cannot avoid being the norm of a trace zero element of $\mathbb{O}$.

**19.30** Let $C$ be a finite-dimensional alternative division algebra over $\mathbb{R}$. Then Exc. 14.9 shows that $C$ is unital. Moreover, for $0 \neq x \in C$, the unital subalgebra $\mathbb{R}[x] \subseteq C$ is finite-dimensional, commutative associative and without zero divisors. Thus $\mathbb{R}[x]/\mathbb{R}$ is a finite algebraic field extension, which implies $\mathbb{R}[x] = \mathbb{R}1_C$ or $\mathbb{R}[x] \cong \mathbb{C}$ as $\mathbb{R}$-algebras. In particular, the elements $1_C, x, x^2$ are linearly dependent over $\mathbb{R}$, and we deduce from Exc. 16.21 that $C$ is a conic algebra. Since the non-zero elements of $C$ are invertible, Prop. 17.5 shows that the norm of $C$ is anisotropic. On the other hand, it represents 1 and hence (by the intermediate value theorem) must be positive definite. Now Thm. 19.13 shows that $C$ is a composition division algebra over $\mathbb{R}$. By Cor. 19.17, therefore, $C \cong \mathrm{Cay}(\mathbb{R}, \alpha_1, \ldots, \alpha_n)$ for some $n = 0, 1, 2, 3$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{R}^\times$. Here the assumption $\alpha_i > 0$ for some $i = 0, \ldots, n$ would contradict Remark 18.5 in conjunction with the property of $n_C$ to be positive definite. Thus $\alpha_i < 0$ for $0 \leq i \leq n$, and invoking Exc. 18.19, we are actually reduced to the case $\alpha_i = -1$, $0 \leq i \leq n$, which means $C \cong \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ for $n = 0, 1, 2, 3$, respectively.

**19.31** For the first part of the problem, put $C := \mathrm{Cay}(B, \mu)$ and write $\varphi\colon C \to C^p$ for the map defined by

$$\varphi(u + vj) := (p^{-1}up) + vj \qquad (u, v \in B),$$

which is obviously a linear bijection preserving units but also norms since $B$ was assumed to be multiplicative. It therefore suffices to show that $\varphi$ is an algebra homomorphism. In order to do so, write "$\cdot$" for the product in $C^p$ and let $u_1, u_2, v_1, v_2 \in B$. Combining (18.4.1) and associativity of $B$ with the fact that its conjugation is an involution (Prop. 17.2 (a)), we obtain

$$\begin{aligned}
\varphi(u_1 + v_1 j) \cdot \varphi(u_2 + v_j) &= ((p^{-1}u_1 p) + v_1 j) \cdot ((p^{-1}u_2 p) + v_2 j) \\
&= \Big(((p^{-1}u_1 p) + v_1 j)p^{-1}\Big)\Big(p((p^{-1}u_2 p) + v_2 j)\Big) \\
&= (p^{-1}u_1 + (v_1 \bar{p}^{-1})j)(u_2 p + (v_2 p)j) \\
&= (p^{-1}u_1 u_2 p + \mu \bar{p}\bar{v}_2 v_1 \bar{p}^{-1}) + (v_2 p p^{-1}u_1 + v_1 \bar{p}^{-1}\bar{p}\bar{u}_2)j.
\end{aligned}$$

But $\bar{p} = n_B(p)p^{-1}$, $\bar{p}^{-1} = n_B(p)^{-1}p$. Hence

$$\begin{aligned}\varphi(u_1 + v_1 j) \cdot \varphi(u_2 + v_j) &= \big(p^{-1}(u_1u_2 + \mu\bar{v}_2v_1)p\big) + (v_2u_1 + v_1\bar{u}_2)j \\ &= \varphi\big((u_1u_2 + \mu\bar{v}_2v_1) + (v_2u_1 + v_1\bar{u}_2)j\big) \\ &= \varphi((u_1 + v_1 j)(u_2 + v_2 j)),\end{aligned}$$

as desired.

Turning to the second part of the problem, let $C$ be an octonion algebra over $k$ and suppose $p, q \in C^\times$ have the property that $pq^2$ belongs to some quaternion subalgebra $B \subseteq C$. By Exc. 15.18 (a) and its solution, it will be enough to show for $p \in B^\times$ and $B$ as above that $C$ and $C^p$ are isomorphic. In order to do so, we note $C = B \oplus B^\perp$ as a direct sum of submodules (Lemma 11.10) and define $\varphi\colon C \to C^p$ by $\varphi(u + v) := (p^{-1}up) + v$ for $u \in B$, $v \in B^\perp$. We claim that $\varphi$ is an isomorphism of conic algebras. This assertion is local on $k$, so we may assume that $k$ is a local ring. By Thm. 19.16 (a), we may identify $C = \mathrm{Cay}(B, \mu) = B \oplus Bj$, where the relation $B^\perp = Bj$ can be read off from (18.4.4) and the regularity of $n_B$. Thus our new map $\varphi$ agrees with the one defined in the first part and hence must be an isomorphism of conic algebras.

**19.32** (a) We begin by showing that *for a quadratic $k$-algebra $R$ and $u \in R$,*

$$n_R(u - \bar{u}) = 4n_R(u) - t_R(u)^2, \tag{s1}$$

which follows from

$$n_R(u-\bar{u}) = n_R(u)-n_R(u,\bar{u})+n_R(\bar{u}) = 2n_R(u)-t_R(u)^2+n_R(u,u) = 4n_R(u)-t_R(u)^2.$$

Assume first that $R$ is étale and $u$ generates $R$ as a $k$-algebra. Combining Prop. 19.8 with (s1), we conclude that $u - \bar{u}$ is invertible. Conversely, suppose that $u - \bar{u}$ is invertible in $R$. Again by Prop. 19.8 and (s1), $D := k[u] \subseteq R$ is a quadratic étale subalgebra. By Lemma 11.10, therefore, we obtain the decomposition $R = D \oplus D^\perp$ as $k$-modules and conclude, by comparing ranks, that $R = D$ is quadratic étale.

Next suppose $k$ is an LG ring and $D$ is a quadratic étale $k$-algebra. By Prop. 11.24, $D$ is a free $k$-module of rank 2 containing $1_D$ as a unimodular element (16.4), which therefore can be extended to a basis $(1_D, u)$ of $D$. Thus $D = k[u]$, and Prop. 19.8 combined with (s1) shows $n_D(u - \bar{u}) \in k^\times$, hence $u - \bar{u} \in D^\times$.

Finally, returning to an arbitrary base ring $k$ and a quadratic étale $k$-algebra $D$, it remains to show $H(D, \iota_D) = k1_D$. In order to do so, we may assume $D = k[u]$ for some $u \in D$ such that $u - \bar{u} \in D^\times$. In particular, by Prop. 19.8, $D$ is free (of rank 2) as a $k$-module with basis $1_D, u$. We clearly have $k1_D \subseteq H(D, \iota_D)$. Conversely, write $x \in H(D, \iota_D)$ as $x = \alpha 1_D + \beta u$ for some $\alpha, \beta \in k$. Then

$x = \bar{x} = \alpha 1_D + \beta\bar{u}$ implies $\beta(u - \bar{u}) = 0$, hence $\beta = 0$ (since invertible elements, being the image of $1_D$ under a linear bijection, are unimodular), and we end up with $x = \alpha 1_D \in k1_D$.

(b) Let $B$ be a quaternion algebra over $k$. We must show that an element $x \in B$ satisfying $[x, y] = 0$ for all $y \in B$ is a scalar multiple of $1_C$. This assertion being local on $k$, we may assume that $k$ is a local ring. By Cor. 19.17, we may further assume $B = \mathrm{Cay}(D, \mu) = B \oplus Bj$ for some quadratic étale $k$-algebra $D$ and some $\mu \in k$. From Thm. 19.14 we deduce $\mu \in k^\times$, while part (a) of our problem yields an element $u \in D$ making $u - \bar{u}$ invertible. Now write $x = u_1 + v_1 j$, $u_1, v_1 \in D$. By hypothesis we have $[x, u_2 + v_2 j] = 0$ for all $u_2, v_2 \in D$, which by (18.13.1) implies

$$0 = [u_1, u_2] + \mu(\bar{v}_2 v_1 - \bar{v}_1 v_2) = \mu(\bar{v}_2 v_1 - \bar{v}_1 v_2).$$

Since $\mu$ is invertible, we conclude $\bar{v}_2 v_1 = \bar{v}_1 v_2$ for all $v_2 \in D$. Setting $v_2 = 1_B$ gives $\bar{v}_1 = v_1$, while setting $v_2 = u$ now gives $(u - \bar{u})v_1 = 0$, hence $v_1 = 0$ since $u - \bar{u}$ is invertible. Next applying (18.13.2), we obtain $0 = v_2(u_1 - \bar{u}_1) - v_1(u_2 - \bar{u}_2) = v_2(u_1 - \bar{u}_1)$ for all $v_2 \in B$, which for $v_2 = 1_B$ amounts to $u_1 = \bar{u}_1$, hence by (a) to $u_1 \in k1_B$. Thus we have $x \in k1_C$, as desired.

Finally, let $C$ be an octonion algebra over $k$. We have

$$k1_C \subseteq \{x \in C \mid \forall y \in C : \ xy = yx\} \cap \mathrm{Nuc}(C),$$

so it remains to show that both sets taking part in the intersection on the right-hand side belong to $k1_C$. Since these are local questions, we may assume that $k$ is a local ring and then obtain, by Cor. 19.17, $C = \mathrm{Cay}(B, \mu) = B \oplus Bj$ up to isomorphism, for some quaternion subalgebra $B \subseteq C$ and some scalar $\mu \in k^\times$ (Thm. 19.14). Now let $x = u_1 + v_1 j \in C$ with $u_1, v_1 \in B$ and first assume $[x, u_2 + v_2 j] = 0$ for all $u_2, v_2 \in B$. From (18.13.1), (18.13.2), we conclude

$$[u_1, u_2] + \mu(\bar{v}_2 v_1 - \bar{v}_1 v_2) = 0 = v_2(u_1 - \bar{u}_1) - v_1(\bar{u}_2 - u_2) \tag{s2}$$

for all $u_2, v_2 \in B$. By what we have seen before, the first of these equations for $v_2 = 0$ shows $u_1 \in \mathrm{Cent}(B) = k1_B$. Now the second one implies $v_1(u_2 - \bar{u}_2) = 0$ for all $u_2 \in B$. By Thm. 19.16 (b), we find a quadratic étale subalgebra $D \subseteq B$, which in turn, by part (a) of this exercise, contains an element $u_2$ making $u_2 - \bar{u}_2$ invertible. Hence $v_1 = 0$ and thus $x \in k1_C$. Next assume $x \in \mathrm{Nuc}(C)$. Applying (18.13.3), for $u_2 = v_3 = 0$, we obtain $(\bar{v}_2 v_1)u_3 = (u_3 \bar{v}_2)v_1$ for all $v_2, u_3 \in B$. Setting $v_2 = 1_B$, this implies $v_1 u_3 = u_3 v_1$ for all $u_3 \in B$, hence $v_1 \in \mathrm{Cent}(B) = k1_B$. Thus $v_1 = \beta 1_B$ for some $\beta \in k$, and our original equation reduces to $(\beta\bar{v}_2)u_3 = u_3(\beta\bar{v}_2)$ for all $v_2, u_3 \in B$ This means $\beta v_2 \in \mathrm{Cent}(B) = k1_B$ for all $v_2 \in B$. But $1_B$, being unimodular, may be extended to basis of $B$ as a $k$-module, and picking for $v_2$ one of the basis vectors distinct from $1_B$, we

conclude $\beta = 0$, hence $v_1 = 0$. Now we consider (18.13.4) for $u_2 = u_3 = v_2 = 0$ and $v_3 = 1_B$. Then $[u_1, u_2] = 0$ for all $u_2 \in B$, which yields $u_1 \in \mathrm{Cent}(B) = k1_B$, hence $x \in k1_C$, and completes the proof.

**19.33** (a) Assume first $2 \in k^\times$. Then $k1_D \subseteq D$ is a regular composition subalgebra, and Thm. 19.16 yields an identification $D = \mathrm{Cay}(k, \mu) = k \oplus kj$, for some $\mu \in k^\times$. By (18.4.3), therefore, $u := \frac{1}{2} \cdot 1_D + j$ does the job. We are left with the case $2 \in \mathfrak{m}$, where $\mathfrak{m}$ stands for the maximal ideal of $k$. Since all finitely generated projectives over $k$ are free and $1_D \in D$ is unimodular, some $v \in D$ makes $(1_D, v)$ a basis of $D$ over $k$. Now Prop. 19.8 implies $\mu := t_D(v)^2 - 4n_D(v) \in k^\times$. Since $2 \in \mathfrak{m}$, we conclude $t_D(v) \in k^\times$ and $u := t_D(v)^{-1}v$ does the job.

(b) If $k$ allows a decomposition of the desired kind, then $\varphi$ is clearly an automorphism of $D$. Conversely, let this be so. We first treat the case that $k$ is a local ring. By (a), $D = k[u]$ for some element $u \in D$ of trace 1. By Prop. 19.8, therefore, $(1_D, u)$ is a basis of $D$, and there are $\alpha, \beta \in k$ such that $\varphi(u) = \alpha 1_D + \beta u$. But $\varphi$, being an automorphism of $D$, preserves norms, traces and unit. Hence

$$2\alpha + \beta = t_D(\varphi(u)) = t_D(u) = 1,$$
$$\alpha^2 + \alpha\beta + \beta^2 n_D(u) = n_D(\varphi(u)) = n_D(u),$$

and we conclude $\beta = 1 - 2\alpha$,

$$\alpha^2 + \alpha - 2\alpha^2 + (1 - 4\alpha + 4\alpha^2)n_D(u) = n_D(u).$$

Thus $(\alpha - \alpha^2)(1 - 4n_D(u)) = 0$. On the other hand, since $D$ is quadratic étale, Prop. 19.8 shows $1 - 4n_D(u) \in k^\times$. Hence $\alpha \in k$ is an idempotent. But as a local ring, $k$ is connected. We therefore conclude $\alpha = 0, \beta = 1$ or $\alpha = 1, \beta = -1$, which implies $\varphi = \mathbf{1}_D$ in the first case, $\varphi = \iota_D$ in the second.

Now let $k$ be arbitrary and put $X := \mathrm{Spec}(k)$. Since $D$ is finitely generated as a $k$-module,

$$X_+ := \{\mathfrak{p} \in X \mid \varphi_\mathfrak{p} = \mathbf{1}_{D_\mathfrak{p}}\}, \quad X_- := \{\mathfrak{p} \in X \mid \varphi_\mathfrak{p} = \iota_{D_\mathfrak{p}}\}$$

by Exc. 9.28, are Zariski-open subsets of $X$. Moreover, they are disjoint by Exc. 19.32 (a) and cover $X$ by the special case just treated. Hence Exc. 9.29, yields a complete orthogonal system $(\varepsilon_+, \varepsilon_-)$ of idempotents in $k$ such that $X_\pm = D(\varepsilon_\pm)$. Put $k_\pm := \varepsilon_\pm k$. Then $k = k_+ \times k_-$ as a direct product of ideals, and with the canonical projection $\pi_+ \colon k \to k_+$, we consult (9.7.5) to conclude $\mathfrak{p} := \mathrm{Spec}(\pi_+)(\mathfrak{p}_+) = \mathfrak{p}_+ \times k_- \in D(\varepsilon_+)$ for any prime ideal $\mathfrak{p}_+ \subseteq k_+$. Now 9.6, 9.7 show that $\varphi_{+\mathfrak{p}_+} = \varphi_\mathfrak{p} \otimes_{k_\mathfrak{p}} k_{+\mathfrak{p}_+} = \mathbf{1}_{D_{+\mathfrak{p}_+}}$. Thus $\varphi_+ = \mathbf{1}_{D_+}$ and, similarly, $\varphi_- = \iota_{D_-}$.

**19.34** See [36, pp. 290-291]

**19.35** We begin by proving (1) and first note that not only $c_1 = c$ but also $c_2 = 1_C - c$ is an elementary idempotent (cf. Exc. 16.23, particularly (iv)). Let $i = 1, 2$ and $x \in C_{ii}$. Then $c_i x = x = xc_i$, and (17.4.2) yields $x = c_i x c_i = n_C(c_i, \bar{x})c_i - n_C(c_i)\bar{x} = n_C(c_i, \bar{x})c_i \in kc_i$, and (1) holds. In view of this, arbitrary elements $x, y \in C$ can be written as in (2). Expanding the norm of $x$ in the obvious manner, we obtain

$$\begin{aligned} n_C(x) &= n_C(\alpha_1 c_1 + x_{12} + x_{21} + \alpha_2 c_2) \\ &= \alpha_1^2 n_C(c_1) + \alpha_1 n_C(c_1, x_{12}) + \alpha_1 n_C(c_1, x_{21}) + \alpha_1\alpha_2 n_C(c_1, c_2) + n_C(x_{12}) \\ &\quad + n_C(x_{12}, x_{21}) + \alpha_2 n_C(x_{12}, c_2) + n_C(x_{21}) + \alpha_2 n_C(x_{21}, c_2) + \alpha_2^2 n_C(c_2). \end{aligned}$$

Applying (17.1.3), (17.1.2) and observing $n_C(c_1) = n_C(c_2) = 0$, we obtain, for $\{i, j\} = \{1, 2\}$,

$$\begin{aligned} n_C(c_i) &= 0, \\ n_C(c_i, x_{ij}) &= n_C(c_i c_i, c_i x_{ij}) = n_C(c_i) n_C(c_i, x_{ij}) = 0, \\ n_C(c_i, x_{ji}) &= n_C(c_i c_i) n_C(x_{ji} c_i) = n_C(c_i, x_{ji}) n_C(c_i) = 0, \\ n_C(c_1, c_2) &= n_C(c, 1_C - c) = t_C(c) - 2n_C(c) = 1, \\ n_C(x_{ij}) &= n_C(c_i x_{ij}) = n_C(c_i) n_C(x_{ij}) = 0. \end{aligned}$$

Inserting these relations into the preceding equation, we end up with (3), while linearizing (3) gives (4), which for $y = 1_C$ yields (5). Finally, (6) follows immediately from the definition.

Now let $C$ be a composition algebra. We must show for $\{i, j\} = \{1, 2\}$ that $Dn_C$ determines a duality between $C_{ij}$ and $C_{ji}^*$. Let $x_{ij} \in C_{ij}$ and suppose $n_C(x_{ij}, C_{ji}) = \{0\}$. Then (4) yields

$$n_C(x_{ij}, C) = n_C(x_{ij}, kc_i + C_{ij} + C_{ji} + kc_j) = n_C(x_{ij}, C_{ji}) = \{0\}$$

hence $x_{ij} = 0$ since $n_C$ is non-singular. Next let $\lambda_{ji} \colon C_{ji} \to k$ be a linear form and $\lambda \colon C \to k$ the linear extension of $\lambda_{ji}$ that kills $kc_1 \oplus C_{ij} \oplus kc_2$. By non-singularity of $n_C$, there exists $x \in C$ such that $\lambda = n_C(x, -)$. Writing $x$ in the form (2) and choosing $y_{ji} \in C_{ji}$, we apply (4) and obtain $\lambda_{ji}(y_{ji}) = \lambda(y_{ji}) = n_C(x, y_{ji}) = n_C(x_{ij}, y_{ji})$. Summing up, $Dn_C$ does indeed determine a duality between $C_{ij}$ and $C_{ji}$. In order to prove the final statement, we must show $t_C(x^2 z) = t_C(xy^2) = 0$ for all $x, y, z \in C_{ij}$. This follows from the final statement in Exercise 14.12.

**19.36** (a) Since scalar multiplication by $D$ acts on the second factor of $D \otimes D$, the map $\varphi$ is a unital homomorphism of $D$-algebras. Moreover, for $u \in D$ we

have

$$\varphi(u \otimes 1_D - 1_D \otimes \bar{u}) = (u, \bar{u}) - (\bar{u}, \bar{u}) = (u - \bar{u}, 0),$$
$$\varphi(1_D \otimes u - u \otimes 1_D) = (u, u) - (u, \bar{u}) = (0, u - \bar{u}).$$

In order to prove that $\varphi$ is an isomorphism, we may assume that $k$ is a local ring. By Exc. 19.32 (a), the element $u$ may be so chosen that $u - \bar{u} \in D^\times$. The preceding equations therefore show that $(1_D, 0)$ and $(0, 1_D)$ both belong to $\mathrm{Im}(\varphi)$. But $D \times D$ is generated by these elements as a $D$-algebra. Hence $\varphi$ is surjective. On the other hand, $D \otimes D$ and $D \times D$ are finitely generated projective $D$-modules of rank 2. Hence $\varphi$ is an isomorphism by Exc. 9.30.

(b) By definition, we have $\sigma' \circ \varphi = \varphi \circ \sigma'$. Hence, for $x, d \in D$,

$$\sigma'((xd, \bar{x}d)) = \sigma'(\varphi(x \otimes d)) = \varphi(\sigma(x \otimes d)) = \varphi(x \otimes \bar{d}) = (x\bar{d}, \bar{x}\bar{d}) = (\overline{\bar{x}d}, \overline{xd}),$$

which proves the assertion since, by (a), any element of $D \times D$ can be written as a finite sum of expressions of the form $(xd, \bar{x}d)$ with $x, d \in D$.

**19.37** (a) Let $x, y \in R$. Since $R$ by Prop. 17.2 (b) is a multiplicative conic algebra, we may apply (16.12.5), (16.5.10) and (17.1.3) to obtain

$$\begin{aligned} t_R(e(xy)) &= t_R((ex)(ey)) = t_R(ex)t_R(ey) - n_R(ex, ey) \\ &= t_R(ex)t_R(ey) - n_R(e)n_R(x, y) = t_R(ex)t_R(ey). \end{aligned}$$

Hence $t_R \circ L_e \colon R \to k$ is an algebra homomorphism, which by Exc. 16.23 is unital if and only if $e$ is an elementary idempotent.

(b) For $x, y \in R$, we combine (a) with the multiplicativity of $n_R$ and obtain

$$\begin{aligned} q(x)q(y) &= (t_R(ex^2) + \varepsilon n_R(x))(t_R(ey^2) + \varepsilon n_R(y)) \\ &= t_R(ex^2)t_R(ey^2) + \varepsilon t_R(ex^2)n_R(y) + \varepsilon n_R(x)t_R(ey^2) + \varepsilon^2 n_R(xn_R(y) \\ &= t_R(e(xy)^2) + t_R(\varepsilon ex^2)n_R(y) + n_R(x)t_R(\varepsilon ey^2) + \varepsilon n_R(xy) \\ &= t_R(e(xy)^2) + \varepsilon n_R(xy) = q(xy). \end{aligned}$$

Hence $q$ permits composition.

(c) The condition is clearly sufficient. Conversely, suppose $q$ permits composition. We put $e_1 := (1, 0)$, $e_2 := (0, 1)$ and

$$\varepsilon_1 := q(e_1), \quad \varepsilon_2 := q(e_1, e_2), \quad \varepsilon_3 := q(e_2).$$

Then (1) holds. Moreover, since $q$ permits composition, $(\varepsilon_1, \varepsilon_3)$ is an orthogonal system of idempotents such that $\varepsilon_1\varepsilon_2 = q(e_1)q(e_1, e_2) = q(e_1^2, e_1e_2) = 0$ and, similarly, $\varepsilon_3\varepsilon_2 = 0$. On the other hand, $\varepsilon := q(1_D) = \sum \varepsilon_i$ is an idempotent in $k$ satisfying $q(x) = \varepsilon q(x)$, $q(x, y) = \varepsilon q(x, y)$ for all $x, y \in D$. In particular, we

have $\varepsilon\varepsilon_i = \varepsilon_i$ for $i = 1, 2, 3$, whence $\varepsilon_2 = \varepsilon - \varepsilon_1 - \varepsilon_3$ must be an idempotent as well.

(d) Let $q\colon D \to k$ be a quadratic form permitting composition. Since, therefore, its scalar extension $q_D\colon D \otimes D \to D$ permits composition, so does $q' := q_D \circ \varphi^{-1}\colon D \times D \to D$, where $\varphi$ is the isomorphism of Exc. 19.36 (a). Hence (c) yields an orthogonal system $(d_1, d_2, d_3)$ of idempotents in $D$ such that

$$q((a, b)) = d_1 a^2 + d_2 ab + d_3 b^2$$

for all $a, b \in D$. With $\sigma$ as in Exc. 19.36 (b), we now claim

$$q_D \circ \sigma = \iota_D \circ q_D. \tag{s1}$$

In order to prove this, we let $x, x', d, d' \in D$ and compute

$$\begin{aligned}
(q_D \circ \sigma)(x \otimes d) &= q_D(x \otimes \bar{d}) = q(x)\bar{d}^2,\\
(\iota_D \circ q_D)(x \otimes d) &= \overline{q_D(x \otimes d)} = \overline{q(x)d^2} = q(x)\bar{d}^2,\\
(q_D \circ (\sigma \times \sigma))(x \otimes d, x' \otimes d') &= q_D(x \otimes \bar{d}, x' \otimes \bar{d}') = q(x, x')\bar{d}\bar{d}',\\
(\iota_D \circ q_D)(x \otimes d, x' \otimes d') &= \overline{q(x, x')dd'} = q(x, x')\bar{d}d'.
\end{aligned}$$

Hence (s1) holds. Using this, and keeping the notation of Exc. 19.36 (b), we conclude

$$q' \circ \sigma' = q_D \circ \varphi^{-1} \circ \varphi \circ \sigma \circ \varphi^{-1} = q_D \circ \sigma \circ \varphi^{-1} = \iota_D \circ q_D \circ \varphi^{-1} = \iota_D \circ q'.$$

deviating slightly from the notation used in (c), we now put $e_1 := (1_D, 0)$, $e_2 := (0, 1_D$ and obtain

$$\bar{d}_1 = \overline{q'(e_1)} = (\iota_D \circ q')(e_1) =$$

hence $\bar{d}_3 = d_1$. Similarly,

$$\bar{d}_2 = (\iota_D \circ q')(e_1, e_2) = q'(\sigma'(e_1), \sigma'(e_2)) = q'(e_2, e_1) = d_2.$$

Thus $d_2 \in H(D, \iota_D) = k1_D$ (by Exc. 19.32 (a)). Since $1_D$ is unimodular, we find a unique idempotent $\varepsilon \in k$ such that $d_2 = \varepsilon 1_D$. Then $e := d_1$ is an idempotent in $D$ such that $\varepsilon e = d_2 d_1 = 0$, while the relation $n_D(e)1_D = e\bar{e} = d_1 d_3 = 0$ implies $n_D(e) = 0$. Finally, for $x \in D$, we compute

$$\begin{aligned}
q(x)1_D &= q_D(x \otimes 1_D) = (q' \circ \varphi)(x \otimes 1_D) = q'(x \oplus \bar{x}) = ex^2 + \varepsilon x\bar{x} + \bar{e}\bar{x}^2\\
&= (t_D(ex^2) + \varepsilon n_D(x))1_D,
\end{aligned}$$

and the assertion follows.

**19.38** We begin by reducing to the case that $k$ is a field. Since all finitely generated projectives over $k$ are free and $1_C \in R$ is unimodular, it can be extended

to a basis $(1_C, v)$ of $R$ as a $k$-module. Moreover, the $k$-module $k \times k \times C$ is free, so the polynomial law $f\colon k \times k \times C \to k$ given by the set maps

$$f_S : S \times S \times C_S \longrightarrow S, (s_1, s_2, u) \longmapsto s_2 \det\left((n_{C_S}(u_i, u_j))_{0\le i,j\le 3}\right)$$

for $S \in k$-**alg**, where $u_0 := 1_{C_S}$, $u_1 := s_1 1_{C_S} + s_2 v_S$, $u_2 := u$, $u_3 := u_1 u_2$, may be regarded as a polynomial $f \in k[\mathbf{t}_1, \ldots, \mathbf{t}_{10}]$ (Cor. 12.12). This polynomial represents a unit over $k$ if and only if, for some $\xi_1, \xi_2 \in k$, $u \in C$, both $\xi_2$ and $\det(((n_C(u_i, u_j))_{0\le i,j\le 3})$ with $u_0 := 1_C$, $u_1 = \xi_1 1_C + \xi_2 v$, $u_2 := u$, $u_3 = u_1 u_2$ belong to $k^\times$, equivalently, $R = k[u_1]$ and $B := \sum_{i=0}^{3} k u_i$ is a quaternion subalgebra of of $C$ (Exc. 17.10) (which, in addition, contains $R$). Hence the proof will be complete once we have shown that $f$ represents a unit over $k$. But $k$ is LG, so it suffices to show that $F$ represents a unit over every field in $k$-**alg**. This completes the reduction to the field case.

From now on, therefore, let $k = F$ be a field. Then $R$ is a two-dimensional $F$-algebra. If $R$ is quadratic étale, then Thm. 19.16 (a) yields a scalar $\mu \in k^\times$ such that the inclusion $R \hookrightarrow C$ extends to an embedding $\varphi\colon \mathrm{Cay}(R, \mu) = R \oplus Rj \to C$. Its image, therefore, is a quaternion subalgebra of $C$ generated by $R$ and $\varphi(j)$ in $C$, and we conclude $f(0, 1, \varphi(j)) \neq 0$. Hence we may assume that $R$ is not quadratic étale. Then Exc. 19.27 implies that $R/F$ is either an inseparable quadratic field extension of characteristic 2 or the $F$-algebra of dual numbers. In any event, setting $u_0 := 1_C$, there is an element $u_1 \in C$ such that $R = Fu_0 \oplus Fu_1$ and $n_C(u_0, u_1) = t_C(u_1) = 2\alpha = 0$, where $\alpha := n_C(u_1)$. Since $u_0, u_1$ are linearly independent, any $\beta \in k$ yields a linear form $\lambda$ on $C$ having $\lambda(u_0) = 1$, $\lambda(u_1) = \beta$, and by regularity of $n_C$ we obtain $\lambda = n_C(-, u_2)$ for some $u_2 \in C$. Thus $n_C(u_0, u_2) = t_C(u_2) = 1$ and $n_C(u_1, u_2) = \beta$. Setting $\gamma := n_C(u_2)$ and $u_3 := u_1 u_2$, we conclude

$$\begin{aligned}
n_C(u_0, u_3) &= n_C(1_C, u_1 u_2) = n_C(\bar{u}_1, u_2) = -n_C(u_1, u_2) = -\beta,\\
n_C(u_1, u_1) &= 2\alpha = 0,\\
n_C(u_1, u_3) &= n_C(u_1, u_1 u_2) = n_C(u_1) t_C(u_2) = \alpha,\\
n_C(u_2, u_2) &= 2n_C(u_2) = 2\gamma,\\
n_C(u_2, u_3) &= n_C(u_2, u_1 u_2) = n_C(u_2) t_C(u_1) = 0,\\
n_C(u_3, u_3) &= 2n_C(u_1 u_2) = 2n_C(u_1) n_C(u_2) = 2\alpha n_C(u_2) = 0.
\end{aligned}$$

This implies

$$\det\left((n_C(u_i, u_j))_{0\le i,j\le 3}\right) = \det\begin{pmatrix} 2 & 0 & 1 & -\beta \\ 0 & 0 & \beta & \alpha \\ 1 & \beta & 2\gamma & 0 \\ -\beta & \alpha & 0 & 0 \end{pmatrix}$$

$$= \det\begin{pmatrix} 0 & -2\beta & 1-4\gamma & -\beta \\ 0 & 0 & \beta & \alpha \\ 1 & \beta & 2\gamma & 0 \\ 0 & \alpha+\beta^2 & 2\beta\gamma & 0 \end{pmatrix}$$

$$= \det\begin{pmatrix} -2\beta & 1-4\gamma & -\beta \\ 0 & \beta & \alpha \\ \alpha+\beta^2 & 2\beta\gamma & 0 \end{pmatrix}$$

$$= \alpha(\alpha+\beta^2)(1-4\gamma) + (\alpha+\beta^2)\beta^2 + 4\alpha\beta^2\gamma$$

$$= (\alpha+\beta^2)(\alpha+\beta^2) = (\alpha+\beta^2)^2$$

since $2\alpha = 0$. Setting $\beta = 1$ (resp. $\beta = 0$) for $\alpha = 0$ (resp. $\alpha \neq 0$), the above determinant will be different from zero. Writing $u_1 = \xi_1 1_C + \xi_2 v$ for some $\xi_1, \xi_2 \in F$, we conclude $\xi_2 \neq 0$ (since $u_0, u_1$ are linearly independent), hence $f(\xi_1, \xi_2, u_2) \neq 0$, as desired.

**19.39** (a) Let $\sigma$ be a reflection of $C$ and write $B^{\pm} := \{x \in C \mid \sigma(x) = \pm x\}$. Then $B^+ = \mathrm{Fix}(\sigma) \subseteq C$ is a unital subalgebra and since $\frac{1}{2} \in k$, we have $C = B^+ \oplus B^-$ as a direct sum of submodules. In fact, this sum is even an orthogonal one since $\sigma$ preserves $n_C$ (Exc. 16.19), so for $x^{\pm} \in B^{\pm}$ we obtain $n_C(x^+, x^-) = n_C(\sigma(x^+), \sigma(x^-)) = -n_C(x^+, x^-)$, forcing $n_C(x^+, x^-) = 0$. It follows that $\mathrm{Fix}(\sigma) = B^+ \subseteq C$ is a composition subalgebra. In order to prove that its rank is $\frac{r}{2}$, we may assume that $k$ is a local ring. Then Thm. 19.16 (a) yields an element $\mu \in k^\times$ such that $\mathrm{Cay}(B^+, \mu) = B^+ \oplus B^+ j$ may be viewed as a subalgebra of $C$. In particular, $j \in C^\times$, and since $\sigma$ is an automorphism of $C$, we conclude $jB^{\pm} \subseteq B^{\mp}$. This shows that $B^+$ and $B^-$ have the same rank. But the sum of the two ranks is $r$. Thus $\mathrm{rk}(B^{\pm}) = \frac{r}{2}$.

Conversely, suppose $B \subseteq C$ is a composition subalgebra of rank $\frac{r}{2}$, automatically regular since $\frac{1}{2} \in k$. Hence $C = B \oplus B^\perp$ as direct sum of submodules, and we have

$$BB \subseteq C, \quad BB^\perp \subseteq B^\perp, \quad B^\perp B \subseteq B^\perp, \quad B^\perp B^\perp \subseteq B. \tag{s1}$$

Here the first inclusion is obvious, while the second and third one follow from the fact that $C$ is norm associative, particularly from (16.12.3), (16.12.4). Finally, in order to establish the fourth inclusion, we may assume that $k$ is a local ring, in which case Thm. 19.16 (a) yields an identification $C = \mathrm{Cay}(B, \mu) = B \oplus Bj$ for some $\mu \in k^\times$ and then $B^\perp = Bj$ by (18.4.4). But now the assertion follows from (18.4.1). By (s1), the map $\sigma_B := \mathbf{1}_B \oplus (-\mathbf{1}_{B^\perp})$ is a reflection of $C$, and it is straightforward to check that the assignments $\sigma \mapsto \mathrm{Fix}(\sigma)$, $B \mapsto \sigma_B$ define inverse bijections between the set of reflections of $C$ and the set of composition subalgebras of $C$ having rank $\frac{r}{2}$.

Let $\rho \in \mathrm{Aut}(C)$. If $\sigma$ is a reflection of $C$, then so is $\sigma^\rho := \rho^{-1} \circ \sigma \circ \rho$ and $\mathrm{Fix}(\sigma^\rho) = \rho^{-1}(\mathrm{Fix}(\sigma))$. On the other hand, if $B \subseteq C$ is a composition subalgebra of rank $\frac{r}{2}$, then $\sigma_{\rho^{-1}(B)} = (\sigma_B)^\rho$. This shows that two reflections of $C$ are conjugate under $\mathrm{Aut}(C)$ if and only if their fixed algebras are, and the proof of (a) is complete.

(b) Let $\tau$ be an involution of $C$. Since $C$ and $C^{\mathrm{op}}$ have the same unit, norm and trace, Exc. 16.19 shows that they are preserved by $\tau$. For $x \in C$, this implies

$$\tau(\bar{x}) = \tau\big(t_C(x)1_C - x\big) = t_C\big(\tau(x)\big)1_C - \tau(x) = \overline{\tau(x)}.$$

Thus $\tau$ commutes with $\iota_C$.

Now let $\tau$ be an involution of $C$ distinct from $\iota_C$. Since $\tau$, as we have just seen, commutes with $\iota_C$, the map $\sigma_\tau := \tau \circ \iota_C = \iota_C \circ \tau$ is a reflection of $C$. Conversely, let $\sigma$ be a reflection of $C$. Being an automorphism of $C$, $\sigma$ preserves conjugation, forcing $\tau_\sigma := \sigma \circ \iota_C = \iota_C \circ \sigma$ to be an involution other than $\iota_C$. It is clear that the assignments $\tau \mapsto \sigma_\tau$ and $\sigma \mapsto \tau_\sigma$ define inverse bijections between the set of involutions of $C$ distinct from $\iota_C$ and the set of reflections of $C$. Moreover, the identities $\tau_{\sigma^\rho} = \rho^{-1} \circ \tau_\sigma \circ \rho$ and $\sigma_{\rho^{-1}\circ\tau\circ\rho} = (\sigma_\tau)^\rho$ are immediately verified. Invoking (a), the aforementioned bijections, therefore, induce canonically inverse bijections between the isomorphism classes of involutions of $C$ other than $\iota_C$ and the conjugacy classes under $\mathrm{Aut}(C)$ of the composition subalgebras of $C$ having rank $\frac{r}{2}$.

Finally, let $\tau \neq \iota_C$ be an involution of $C$ and $B \subseteq C$ the corresponding composition subalgebra of rank $\frac{r}{2}$. Then $\tau = \sigma_B \circ \iota_C$, and for $x \in B$, $y \in B^\perp$, we obtain $\tau(x + y) = \sigma_B(\bar{x} - y) = \bar{x} + y$, hence

$$H(C, \tau) = H(B, \iota_B) \oplus B^\perp = k1_B \oplus B^\perp \cong k \oplus B^\perp,$$

and since $B^\perp$ is finitely generated projective of rank $\frac{r}{2}$, the final assertion follows.

## Solutions for Section 20

This section contains no exercises.

## Solutions for Section 21

**21.20** Let $x_1, \dots, x_n \in M$, $y_1, \dots, y_n \in N$, $r_1, \dots, r_n, s_1, \dots, s_n \in R$. We put $r := r_1 \cdots r_n$, $s := s_1 \cdots s_n \in R$, $A := \mathrm{diag}(r_1, \dots, r_n)$, $B := \mathrm{diag}(s_1, \dots, s_n) \in$

$\mathrm{Mat}_n(R)$ and obtain

$$
\begin{aligned}
(\bigwedge^n h)_R((x_1 \otimes r_1) \wedge \cdots \wedge (x_n \otimes r_n), (y_1 \otimes s_1) \wedge \cdots \wedge (y_n \otimes s_n)) \\
&= (\bigwedge^n h)_R((x_1 \wedge \cdots \wedge x_n) \otimes r, (y_1 \wedge \cdots \wedge y_n) \otimes s) \\
&= ((\bigwedge^n h)(x_1 \wedge \cdots \wedge x_n, y_1 \wedge \cdots \wedge y_n)) \otimes rs \\
&= \det\left((h(x_i, y_j))_{1 \le i,j \le n}\right) \otimes rs \\
&= rs \det\left((h(x_i, y_j))_{1 \le i,j \le n}\right)_R \\
&= rs \det\left((h(x_i, y_j)_R)_{1 \le i,j \le n}\right) \\
&= rs \det\left((h_R(x_{iR}, y_{jR}))_{1 \le i,j \le n}\right) \\
&= \det(A) \det\left((h_R(x_{iR}, y_{jR}))_{1 \le i,j \le n}\right) \det(B) \\
&= \det\left((r_i s_j h_R(x_{iR}, y_{jR}))_{1 \le i,j \le n}\right) \\
&= \det\left((h_R(x_i \otimes r_i, y_j \otimes s_j))_{1 \le i,j \le n}\right) \\
&= \bigwedge^n (h_R)((x_1 \otimes r_1) \wedge \cdots \wedge (x_n \otimes r_n), (y_1 \otimes s_1) \wedge \cdots \wedge (y_n \otimes s_n)),
\end{aligned}
$$

which completes the proof.

**21.21** (a) We begin with the following:

**Claim.** *If $k = F$ is a field and $M \neq \{0\}$, then the map $M \to F$, $x \mapsto h(x, x)$, is not identically zero.*

*Proof* We argue indirectly and assume $h(x, x) = 0$ for all $x \in M$. Linearizing this relation yields

$$t_D(h(x, y)) = h(x, y) + \overline{h(x, y)} = h(x, y) + h(y, x) = 0$$

for all $x, y \in M$, where we may replace $x$ by $xa$, $a \in D$, to obtain $n_D(a, h(x, y)) = t_D(\bar{a}h(x, y)) = t_D(h(xa, y)) = 0$ for all $a \in D$, $x, y \in M$. But since the norm of $D$ is non-singular, this leads to the contradiction $h = 0$ and proves our claim. □

Returning to our LG ring $k$, we argue by induction on $n$ and have nothing to prove for $n = 0$. If $n > 0$, our claim shows that the scalar polynomial law $x \mapsto h(x, x)$ over k represents a unit over any field in $k$-**alg**. Hence it represents a unit over our LG ring $k$: we deduce $\alpha_1 := h(e_1, e_1) \in k^\times$ for some $e_1 \in M$. Now we put

$$N := (e_1 D)^\perp = \{y \in | \, h(e_1, y) = 0\} = \{x \in M \mid h(x, e_1) = 0\}$$

and see by a straightforward verification that $M = (e_1D) \oplus N = (e_1D) \perp N$ relative to $h$. It follows that $(N, h|_{N\times N})$ is a hermitian space of rank $n-1$ over $D$, and applying the induction hypothesis completes the proof.

(b) We may clearly assume that $k$ is a local ring. Let the $e_i \in M$, $\alpha_i \in k$, $1 \le i \le n$, be as in (a). Then

$$M = (e_1D) \oplus \cdots \oplus (e_nD)$$

as a direct sum of free $D$-submodules of rank 1. Since $D$ is a free $k$-module of rank 2, this shows that $M$ is a free $k$-module of rank $2n$. On the other hand, the relations $h(e_id, e_jd') = \delta_{ij}\alpha_i\bar{d}d'$ for $d, d' \in D$, $1 \le i, j \le n$ show that the preceding decomposition is an orthogonal one relative to $h$, hence relative to $q$ as well, and $q(e_id) = h(e_id, e_id) = \alpha_i\bar{d}d = \alpha_i n_D(d)$ for $d \in D$, $1 \le i \le n$. Thus

$$q \cong \alpha_1 n_D \perp \cdots \perp \alpha_n n_D \cong \langle \alpha_1, \ldots, \alpha_n \rangle \otimes n_D$$

is the finite orthogonal sum of of regular quadratic forms over $k$, hence must be regular itself.

**21.22** We put $C := \mathrm{Ter}(D; M, h, \Delta)$ and have $C = D \times M$ as $k$-modules. After the natural identification $D \subseteq C$, we obtain $p^{\pm 1} = (p^{\pm 1}, 0)$, and writing "$\cdot$" for the product in $C^p$, we conclude, for $a, b \in D$, $x, y \in M$,

$$\begin{aligned}(a, x) \cdot (b, y) &= ((a, x)(p^{-1}, 0))((p, 0)(b, y)) \\ &= (ap^{-1}, xp^{-1})(pb, y\bar{p}) \\ &= (ap^{-1}pb - h(xp^{-1}, y\bar{p}), y\bar{p}\overline{ap^{-1}} + xp^{-1}pb + (xp^{-1}) \times_{h,\Delta} (y\bar{p})) \\ &= (ab - \bar{p}^{-1}h(x, y)\bar{p}, y\bar{a} + xb + (x \times_{h,\Delta} y)\bar{p}^{-1}p)\end{aligned}$$

Hence

$$(a, x) \cdot (b, y) = (ab - h(x, y), y\bar{a} + xb + (x \times_{h,\Delta} y)\bar{p}^{-1}p) \quad (a, b \in D,\ x, y \in M). \tag{s1}$$

We will now be able to compute the constituents of $C^p = \mathrm{Ter}(D; M^p, h^p, \Delta^p)$ by appealing to Thm. 21.12 as follows.

As a $k$-module, $M^p$ is the orthogonal complement of $D = D^p$ in $C^p$ relative to the bilinearized norm of $C^p$, which by Exc. 17.12 agrees with the bilinearized norm of $C$. Thus $M^p = M$ as $k$-modules. Consulting (s1), the right action of $D^p = D$ on $M^p = M$ may be read off from

$$(x, a) \longmapsto (0, x) \cdot (a, 0) = (0, xa),$$

which amounts to $M^p = M$ as right $D$-modules.

For $x, y \in M$, we deduce from (s1) that $h^p(x,y)$ is the negative of the $D$-component of

$$(0,x)\cdot(0,y) = (-h(x,y), (x \times_{h,\Delta} y)\bar{p}^{-1}p), \tag{s2}$$

hence agrees with $h(x,y)$. Thus $h^p = h$.

Finally, let $a \in D^\times$. Then $a\Delta\colon \bigwedge^3 M \xrightarrow{\sim} D$ is an orientation of $M$, and 21.9 shows

$$h(x \times_{h,a\Delta} y, z) = a\Delta(x \wedge y \wedge z) = ah(x \times_{h,\Delta} y, z) = h((x \times_{h,\Delta} y)\bar{a}, z)$$

for all $x, y, z \in M$, which is equivalent to

$$x \times_{h,a\Delta} y = (x \times_{h,\Delta} y)\bar{a} \qquad (x, y \in M,\ a \in D^\times). \tag{s3}$$

Now by Thm. 21.12, $x \times_{h,\Delta^p} y$ is the $M$-component of $(0,x)\cdot(0,y)$, hence by (s2) agrees with $(x \times_{h,\Delta} y)\bar{p}^{-1}p$. Since, fixing $h$, the hermitian vector product uniquely determines the orientation it corresponds to, we conclude from this and (s3) that $\Delta^p = \bar{p}p^{-1}\Delta$.

Summing up, we have proved

$$C^p = \mathrm{Ter}(D; M, h, \bar{p}p^{-1}\Delta). \tag{s4}$$

Finally, we wish to understand what all this means for the algebra $C = \mathrm{Zor}(k)$ of Zorn vector matrices over $k$. By 21.18, we have

$$C = \mathrm{Ter}(D; D^3, h, \Delta), \quad D = k \times k, \quad D^3 = k^3 \times k^3, \quad h = \langle \mathbf{1}_3 \rangle_{\mathrm{sesq}},$$
$$\Delta(\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3) = 1, \quad \mathbf{e}_i = (e_i, e_i)\ \ (1 \le i \le 3),$$

where $(e_i)_{1\le i\le 3}$ is the canonical basis of unit vectors in $k^3$. The quantity $\bar{p}^{-1}p$ is essentially an arbitrary element of $D$ having norm 1, hence can be written in the form $\gamma \oplus \gamma^{-1}$ for some $\gamma \in k^\times$. Writing $x, y \in M$ as $x = u_1 \oplus u_2$, $y = v_1 \oplus v_2$, we may apply (21.18.3) and obtain

$$\begin{aligned}(x \times_{h,\Delta^p} y) &= (x \times_{h,\Delta} y)\bar{p}^{-1}p = ((u_2 \times v_2) \oplus (u_1 \times v_1))(\gamma \oplus \gamma^{-1}) \\ &= (\gamma(u_2 \times v_2)) \oplus (\gamma^{-1}(u_1 \times v_1)).\end{aligned}$$

Repeating the computations of 21.18, we therefore conclude that $\mathrm{Zor}(k)^p$ is the $k$-module

$$\begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix}$$

under the multiplication

$$\begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix}\begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 - u_2^{\mathsf{T}}v_1 & \alpha_1 v_2 + \beta_2 u_2 + \gamma^{-1}(u_1 \times v_1) \\ \beta_1 u_1 + \alpha_2 v_1 + \gamma(u_2 \times v_2) & \alpha_2\beta_2 - u_1^{\mathsf{T}}v_2 \end{pmatrix}$$

for $\alpha_i, \beta_i \in k$, $u_i, v_i \in k^3$, $i = 1, 2$. Since $p$ belongs to the split quaternion subalgebra

$$\begin{pmatrix} k & ke_1 \\ ke_1 & k \end{pmatrix} \subseteq \mathrm{Zor}(k),$$

it follows from Exc. 19.31 that $\mathrm{Zor}(k)$ and $\mathrm{Zor}(k)^p$ are isomorphic.

**21.23** (i) $\Leftrightarrow$ (ii). Let $\chi\colon (M_1, h_1) \to (M_2, h_2)$ be an isometry and $x, y, z \in M_1$. Then

$$h_2(\chi(x) \times_{h_2,\Delta_2} \chi(y), \chi(z)) = \Delta_2(\chi(x) \wedge \chi(y) \wedge \chi(z)) = (\Delta_2 \circ \textstyle\bigwedge^3 \chi)(x \wedge y \wedge z),$$
$$h_2(\chi(x \times_{h_1,\Delta_1} y), \chi(z)) = h_1(x \times_{h_1,\Delta_1} y, z) = \Delta_1(x \wedge y \wedge z),$$

and comparing yields the asserted equivalence.

(ii) $\Leftrightarrow$ (iii). Apply (21.12.1).

**21.24** We proceed in several steps.

We write $(e_i)_{1 \le i \le 3}$ for the canonical basis of unit vectors in $k^3$ and put

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_1 := \begin{pmatrix} 0 & -e_1 \\ e_1 & 0 \end{pmatrix}, \quad X_2 := \begin{pmatrix} 0 & -e_2 \\ e_2 & 0 \end{pmatrix}.$$

Then (21.18.4) implies

$$X_3 := X_1 X_2 = \begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix}, \quad X_1^2 = \begin{pmatrix} 1 & 0, \\ 0 & 1 \end{pmatrix} = 1_C = X_2^2,$$
$$X_1 X_2 X_1 = X_3 X_1 = \begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix} \begin{pmatrix} 0 & -e_1 \\ e_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & e_2 \\ -e_2 & 0 \end{pmatrix} = -X_2.$$

Moreover, since $E$ is an elementary idempotent, we have

$$\bar{E} = 1_C - E = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

and using (17.4.2), we see $X_i E X_i = n_C(X_i, \bar{E}) X_i - n_C(X_i) \bar{E}$ which is $\bar{E}$ for $i = 1, 2$ and $-\bar{E}$ for $i = 3$. We have thus established all the relations of (1). Now observe that an easy computation yields

$$EX_i = \begin{pmatrix} 0 & -e_i \\ 0 & 0 \end{pmatrix}, \quad EX_3 = \begin{pmatrix} 0 & e_3 \\ 0 & 0 \end{pmatrix} \qquad (i = 1, 2),$$

which shows that the quantities

$$E, \bar{E}, X_1, X_2, X_3, EX_1, EX_2, EX_3$$

form a basis of $C$ as a $k$-module. In particular, $C$ is generated by $E, X_1, X_2$ as a $k$-algebra.

2°. Now let $A$ be any unital $k$-algebra and suppose that $e, x_1, x_2 \in A$ satisfy the relations

$$e^2 = e, \quad x_1^2 = x_2^2 = 1_A, \quad x_1x_2x_1 = -x_2, \tag{s1}$$
$$x_1ex_1 = x_2ex_2 = \bar{e} := 1_A - e, \quad (x_1x_2)e(x_1x_2) = -\bar{e}.$$

Then we put

$$\varepsilon_{12} := 1, \quad \varepsilon_{21} := -1, \quad x_3 := x_1x_1. \tag{s2}$$

Since (s1), (s2) yield $x_2x_1x_2 = x_2x_1x_2x_1^2 = -x_2x_2x_1 = -x$ and $x_2x_1 = x_1^2x_2x_1 = -x_1x_2 = -x_3$, we obtain

$$\varepsilon_{ji} = -\varepsilon_{ij}, \quad e^2 = e, \quad x_i^2 = 1_A, \quad x_ix_jx_i = -x_j, \tag{s3}$$
$$x_iex_i = \bar{e}, \quad (x_ix_j)e(x_ix_j) = -\bar{e}, \quad x_ix_j = \varepsilon_{ij}x_3 \qquad (\{i,j\} = \{1,2\}).$$

Next we put

$$B := ke + k\bar{e} + \sum_{i=1}^{3} kx_i + \sum_{i=1}^{3} ky_i \subseteq A \qquad (y_i := ex_i,\ 1 \le i \le 3) \tag{s4}$$

and claim that *the spanning elements of $B$ as a $k$-module displayed in* (s4) *satisfy the following multiplication rules.*

$$e^2 = e, \quad \bar{e}^2 = \bar{e}, \quad x_i^2 = 1_C, \quad x_3^2 = -1_C, \quad y_i^2 = y_3^2 = 0 \qquad (i = 1,2), \tag{s5}$$

$$x_iy_i = \bar{e}, \quad y_ix_i = e, \quad x_3y_3 = -\bar{e}, \quad y_3x_3 = -e \qquad (i = 1,2), \tag{s6}$$

$$e\bar{e} = 0, \quad ex_i = y_i, \quad ey_i = y_i \qquad (1 \le i \le 3), \tag{s7}$$

$$\bar{e}e = 0, \quad x_ie = x_i - y_i, \quad y_ie = 0 \qquad (1 \le i \le 3), \tag{s8}$$

$$\bar{e}x_i = x_i - y_i, \quad \bar{e}y_i = 0 \qquad (1 \le i \le 3), \tag{s9}$$

$$x_i\bar{e} = y_i, \quad y_i\bar{e} = y_i \qquad (1 \le i \le 3), \tag{s10}$$

$$x_ix_j = \varepsilon_{ij}x_3, \quad x_ix_3 = \varepsilon_{ij}x_j, \quad x_iy_j = \varepsilon_{ij}(x_3 - y_3), \quad x_iy_3 = \varepsilon_{ij}(x_j - y_j) \qquad (\{i,j\} = \{1,2\}), \tag{s11}$$

$$x_3x_i = -\varepsilon_{ij}x_j, \quad y_jx_i = -\varepsilon_{ij}(x_3 - y_3), \quad y_3x_i = -\varepsilon_{ij}(x_j - y_j) \qquad (\{i,j\} = \{1,2\}), \tag{s12}$$

$$x_3y_i = -\varepsilon_{ij}(x_j - y_j), \quad y_ix_3 = \varepsilon_{ij}(x_j - y_j) \qquad (\{i,j\} = \{1,2\}), \tag{s13}$$

$$y_iy_j = \varepsilon_{ij}(x_3 - y_3), \quad y_iy_3 = \varepsilon_{ij}(x_j - y_j), \quad y_3y_i = -\varepsilon_{ij}(x_j - y_j) \qquad (\{i,j\} = \{1,2\}). \tag{s14}$$

Suppose these relations have been proved. Then they hold, mutatis mutandis, for $E, X_1, X_2 \in C$ as well, and it follows that the linear map $C \to A$ acting on the basis vectors of $C$ exhibited in $1^0$ according to

$$E \mapsto e, \quad \bar{E} \mapsto \bar{e}, \quad X_i \mapsto x_i, \quad EX_i \mapsto y_i \qquad (1 \le i \le 3)$$

is the unique unital homomorphism satisfying the conditions of the problem. The kernel of this homomorphism is an ideal in $C$, which, by Exc. 19.34, has the form $\mathfrak{a}C$ for some ideal $\mathfrak{a} \subseteq k$. Hence $B \cong C/\mathfrak{a}C \cong C \otimes (k/\mathfrak{a}) \cong \mathrm{Zor}(k/\mathfrak{a})$ as $k$-algebras.

3°. It remains to establish (s5)–(s14), which we now proceed to do by making use, among other things, of Artin's theorem (Cor. 14.5) allowing us to drop parentheses in products with at most two distinct factors.

*Proof of* (s5). The first four relations are clear in view of (s3). Moreover, by (s1), (s2), $x_3^2 = x_1x_2x_1x_2 = -x_2^2 = -1_C$, $y_i^2 = ex_iex_i = e\bar{e} = 0$ for $i = 1, 2$ and $y_3^2 = ex_3ex_3 = -e\bar{e} = 0$, which completes the proof.

*Proof of* (s6). For $i = 1, 2$, the definitions and (s3) yield $x_iy_i = x_iex_i = \bar{e}$, $y_ix_i = ex_i^2 = e$, $x_3y_3 = x_3ey_3 = -\bar{e}$, $y_3x_3 = ex_3^2 = -e$, as desired.

*Proof of* (s7). The first relation is obvious, the next three hold by definition (cf. (s4)), while the remaining ones follow from $ey_i = eex_i = ex_i = y_i$ for $i = 1, 2, 3$.

*Proof of* (s8). The first equation is again obvious. As to the next three, we apply (s3), (s5) to obtain $x_ie = x_iex_i^2 = \bar{e}x_i = x_i - ex_i = x_i - y_i$ for $i = 1, 2$ and $x_3e = -x_3ex_3^2 = \bar{e}x_3 = x_3 - ex_3 = x_3 - y_3$, as claimed.

*Proof of* (s9) We have $\bar{e}x_i = x_i - ex_i$ for $1 \le i \le 3$, hence the first three equations of (s9), while (s8) yields $y_i\bar{e} = y_i - y_ie = y_i$ for $1 \le i \le 3$, which completes the proof.

*Proof of* (s10). From (s8) we deduce $x_i\bar{e} = x_i - x_ie = y_i$, $y_i\bar{e} = y_i - y_ie = y_i$ for $1 \le i \le 3$, and the assertion follows.

*Proof of* (s11). Let $\{i, j\} = \{1, 2\}$. The first equation is already in (s3). By the same token, $x_ix_3 = \varepsilon_{ij}x_ix_ix_j = \varepsilon_{ij}x_j$ yields the second equation. Applying (s3), (s9) and the left Moufang identity, we obtain $x_iy_j = x_i(ex_j) = \varepsilon_{ij}x_i(e(x_ix_3)) = \varepsilon_{ij}(x_iex_i)x_3 = \varepsilon_{ij}\bar{e}x_3 = \varepsilon_{ij}(x_3 - y_3)$ and $x_iy_3 = x_i(ex_3) = \varepsilon_{ij}x_i(e(x_ix_j)) = \varepsilon_{ij}(x_iex_i)x_j = \varepsilon_{ij}\bar{e}x_j = \varepsilon_{ij}(x_j - y_j)$, which completes the proof of (s11).

*Proof of* (s12). Let $i, j = \{1, 2\}$. Then (s11) yields $x_3x_i = \varepsilon_{ij}x_ix_jx_i = -\varepsilon_{ij}x_j$, while this, (s8), (s3), (s11), (s10) imply $y_jx_i = x_jx_i - (x_je)x_i = \varepsilon_{ji}x_3 +$

$\varepsilon_{ij}((x_3x_i)e)x_i = \varepsilon_{ij}(x_3(x_iex_i) - x_3) = \varepsilon_{ij}(x_3\bar{e} - x_3) = -\varepsilon_{ij}(x_3 - y_3)$. Finally, applying (s8), (s12), (s11), (s10), we obtain $y_3x_i = x_3x_i - (x_3e)x_i = -\varepsilon_{ij}x_j - \varepsilon_{ji}((x_jx_i)e)x_i = \varepsilon_{ij}(x_j(x_iex_i) - x_j) = \varepsilon_{ij}(x_j\bar{e} - x_j) = -\varepsilon_{ij}(x_j - y_j)$.

*Proof of* (s13). Let $\{i, j\} = \{1, 2\}$. Then (s5), (s11), (s8), (s12) yield

$$\begin{aligned}
x_3y_i &= -x_3(ex_i)x_3^2 = -[x_3(ex_i)x_3]x_3 = -[(x_3e)(x_ix_3)]x_3 = -\varepsilon_{ij}[(x_3e)x_j]x_3\\
&= -\varepsilon_{ij}x_3x_jx_3 + \varepsilon_{ij}[(ex_3)x_j]x_3 = \varepsilon_{ij}\varepsilon_{ji}x_ix_3 + \varepsilon_{ij}e(x_3x_jx_3)\\
&= = -\varepsilon_{ij}x_j - \varepsilon_{ij}\varepsilon_{ji}e(x_ix_3) - \varepsilon_{ij}x_j + \varepsilon_{ij}ex_j = -\varepsilon_{ij}(x_j - y_j),\\
y_ix_3 &= [x_i(x_ie)x_i]x_3 = x_i[(x_ie)(x_ix_3)] = \varepsilon_{ij}x_i[(x_ie)x_j] = \varepsilon_{ij}x_i[(x_i - y_i)x_j]\\
&= \varepsilon_{ij}(x_i^2x_j - x_i(y_ix_j)) = \varepsilon_{ij}(x_j + \varepsilon_{ji}x_i(x_3 - y_3)) = \varepsilon_{ij}x_j - x_ix_3 + x_iy_3\\
&= \varepsilon_{ij}x_j - \varepsilon_{ij}x_j + \varepsilon_{ij}(x_j - y_j) = \varepsilon_{ij}(x_j - y_j),
\end{aligned}$$

hence (s13).

*Proof of* (s14). Again, let $\{i, j\} = \{1, 2\}$. Then (s8), (s12), (s7) yield $y_iy_j = y_ix_j - (ex_i)(x_je) = \varepsilon_{ij}(x_3 - y_3) - e(x_ix_j)e = \varepsilon_{ij}(x_3 - y_3 - ex_3e) = \varepsilon_{ij}(x_3 - y_3)$, giving the first equation of (s14). Similarly, $y_iy_3 = y_ix_3 - (ex_i)(x_3e) = \varepsilon_{ij}(x_j - y_j) - e(x_ix_3)e = \varepsilon_{ij}(x_j - y_j - ex_je) = \varepsilon_{ij}(x_j - y_j)$. And finally, $y_3y_i = y_3(x_i - x_ie) = y_3x_i - (ex_3)(x_ie) = -\varepsilon_{ij}(x_j - y_j) - e(x_3x_i)e = -\varepsilon_{ij}(x_j - y_j) + \varepsilon_{ij}ex_je = -\varepsilon_{ij}(x_j - y_j)$, which completes the entire proof.

## Solutions for Section 22

**22.22** (i) $\Rightarrow$ (ii). $c \neq 0$ implies $k \neq \{0\}$, and if $k^\pm \neq \{0\}$, then $c^\pm = c_{k^\pm} \in A_{k^\pm} = A^\pm$ is an absolutely primitive idempotent by definition.

(ii) $\Rightarrow$ (i). For each sign $\pm$, $c^\pm \in A^\pm$ is an idempotent, and for some sign $\pm$, we have $c^\pm \neq 0$. Hence $c \neq 0$ is an idempotent in $A$. Now assume we are given orthogonal idempotents $d = (d^+, d^-), e = (e^+, e^-) \in A$ such that $c = d + e$. Then $d^\pm, e^\pm$ are orthogonal idempotents in $A^\pm$, $c^\pm = d^\pm + e^\pm$, and since $k^\pm = \{0\}$ or $c^\pm$ is primitive, we find complete orthogonal systems $(\varepsilon_1^\pm, \varepsilon_2^\pm)$ of idempotents in $k^\pm$ such that $d^\pm = \varepsilon_1^\pm c^\pm$, $e^\pm = \varepsilon_2^\pm c^\pm$. Hence $(\varepsilon_1, \varepsilon_2)$, $\varepsilon_1 = (\varepsilon_1^+, \varepsilon_1^-)$, $\varepsilon_2 = (\varepsilon_2^+, \varepsilon_2^-)$, is a complete orthogonal system of idempotents in $k$ satisfying $d = \varepsilon_1 c$, $e = \varepsilon_2 c$. Thus $c$ is a primitive idempotent in $A$.

It remains to show that the same conclusion holds under every non-zero base change of $A$, equivalently, that condition (ii) is stable under such a non-zero base change, so let $R \in k$-**alg**, $R \neq \{0\}$. Setting $\varepsilon^+ := (1, 0)$, $\varepsilon^- := (0, 1) \in k$ and applying 9.7, we conclude $R^+ \times R^-$, $R^\pm = \varepsilon^\pm R = R_{k^\pm}$, $A_R = A_R^+ \times A_R^-$, $A_R^\pm = (A_R)_{R^\pm} = A_{R^\pm} = (A_{k^\pm})_{R^\pm} = A_{R^\pm}^\pm$. We have $c_R = (c_{R^+}^+, c_{R^-}^-)$, and $R^\pm \neq \{0\}$ for some sign $\pm$ implies $k^\pm \neq \{0\}$, hence by (ii) that $c^\pm$ is an absolutely primitive

idempotent of $A^{\pm}$. But then $c^{\pm}_{R^{\pm}}$ must be an absolutely primitive idempotent of $A^{\pm}_{R^{\pm}}$, and we have shownn that (ii) is indeed stable under non-zero base change.

**22.23** (i) $\Rightarrow$ (ii). We clearly have $k \neq \{0\}$. Assuming $k^{(0)} \neq \{0\}$ in the decomposition (ii) of Exc. 16.26, the base change $0 = c_{k^{(0)}} \in C^{(0)} = C_{k^{(0)}}$ would be primitive, a contradiction. Hence $k^{(0)} = \{0\}$. Similarly, if $k^{(2)} \neq \{0\}$, then $1_{C^{(2)}} = c_{k^{(2)}}$ is absolutely primitive in $C^{(2)} = C_{k^{(2)}}$. Hence every composition algebra appearing in the rank decomposition of $C_{k^{(2)}}$ (Exc. 9.31) contains its identity element as an absolutely primitive idempotent and thus, by Prop. 22.7, has rank 1. We conclude $C^{(2)} \cong k^{(2)}$ and have established decompositions (1), (2).

(ii) $\Rightarrow$ (i). If $k^{(1)} \neq \{0\}$, then $c^{(1)}$ is absolutely primitive in $C^{(1)}$ by Prop. 22.7, and if $k^{(2)} \neq \{0\}$, then $1_{k^{(2)}}$ is an absolutely primitive idempotent of $k^{(2)}$. Thus (i) follows from Exc. 22.22.

The final statement of the exercise is now obvious.

**22.24** (a) (i) $\Rightarrow$ (ii). We view $c$ canonically as an idempotent linear map $c\colon k \oplus L_0 \to k \oplus L_0$. With $L_c := \mathrm{Im}(c)$, $\bar{L}_c := \mathrm{Ker}(c) = L_{\bar{c}}$, we then have

$$k \oplus L_0 = L_c \oplus \bar{L}_c = L_c \oplus L_{\bar{c}} \tag{s1}$$

as a directi sum of submodules. Hence $L_c$ and $L_{\bar{c}}$ are both finitely generated projective $k$-modules. For $\mathfrak{p} \in \mathrm{Spec}(k)$, we have $c_{\mathfrak{p}} \neq 0 \neq \bar{c}_{\mathfrak{p}}$ since $c$ is elementary, so $(L_c)_{\mathfrak{p}} = L_{c_{\mathfrak{p}}}$ and $(L_{\bar{c}})_{\mathfrak{p}} = L_{\bar{c}_{\mathfrak{p}}}$ are both free $k_{\mathfrak{p}}$-modules of positive rank. On the other hand, (s1) yields $\mathrm{rk}_{\mathfrak{p}}(L_c) + \mathrm{rk}_{\mathfrak{p}}(L_{\bar{c}}) = 2$, which altogether implies $\mathrm{rk}_{\mathfrak{p}}(L_c) = \mathrm{rk}_{\mathfrak{p}}(L_{\bar{c}}) = 1$. Hence $L_c$ is a line bundle, as claimed.

(ii) $\Rightarrow$ (iii). Regardless of whether the idempotent $c$ is elementary or not, (s1) holds, forcing $L_c$ and $L_{\bar{c}}$ to be finitely generated projective $k$-modules. Now suppose as in (ii) that $L_c$ is a line bundle. Then [8, III.7, Cor. of Prop. 10] implies

$$L_0 \cong k \otimes L_0 \cong \bigwedge^2 (k \oplus L_0) \cong \bigwedge^2 (L_c \oplus L_{\bar{c}}) \cong L_c \otimes L_{\bar{c}}.$$

Thus $L_{\bar{c}} \cong L_0 \otimes L_c^*$ is a line bundle as well, and we have established (1). At this stage, we require the following well-known fact:

**fact.** *Let $M, N$ be finitely generated projective $k$-modules. Then there is a natural identification $\mathrm{Hom}_k(M,N) = N \otimes M^*$ such that $(y \otimes x^*)(x') = \langle x^*, x' \rangle y$ for all $x' \in M$, $y \in N$, $x^* \in M^*$.*

Using this and (1), we now obtain a chain of natural isomorphism as follows:

$$\begin{aligned} B &\cong \operatorname{End}_k(k \oplus L_0) \cong \operatorname{End}_k(L_c \oplus L_{\bar{c}}) \cong \operatorname{End}_k \begin{pmatrix} L_c \\ L_{\bar{c}} \end{pmatrix} \\ &\cong \begin{pmatrix} \operatorname{Hom}_k(L_c, L_c) & \operatorname{Hom}_k(L_{\bar{c}}, L_c) \\ \operatorname{Hom}_k(L_c, L_{\bar{c}}) & \operatorname{Hom}_k(L_{\bar{c}}, L_{\bar{c}}) \end{pmatrix} \cong \begin{pmatrix} L_c \otimes L_c^* & L_c \otimes L_{\bar{c}}^* \\ L_{\bar{c}} \otimes L_c^* & L_{\bar{c}} \otimes L_{\bar{c}}^* \end{pmatrix} \\ &\cong \begin{pmatrix} k & L_0^* \otimes L_c^{\otimes 2} \\ L_0 \otimes L_c^{*\otimes 2} & k \end{pmatrix} \cong B' := \operatorname{End}_k(k \oplus L) \end{aligned}$$

with $L := L_0 \otimes L_c^{*\otimes 2}$ an appropriate line bundle over $k$. Writing $\Phi\colon B \to B'$ for the composite of these isomorphisms, and following step-by-step their effect on the idempotent $c$, we conclude

$$\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{s2}$$

which completes the proof of (iii). Now suppose $L$ is any line bundle over $k$ such that there exists an isomorphism $\Phi\colon B \to B' := \operatorname{End}_k(k \oplus L)$ satisfying (s2). Then $L \cong B'_{21}(\Phi(c)) \cong B_{21}(c)$, $L^* \cong B'_{12}(\Phi(c)) \cong B_{12}(c)$, which not only shows that $L$ is unique up to isomorphism but also completes the proof of (2).

(iii) $\Rightarrow$ (i). Since $\Phi(c)$ is obviously elementary, so is $c$.

(b) Let $g \in \mathrm{GL}(k \oplus L_0) = B^\times$ such that $d = gcg^{-1}$. Then

$$L_d = d \begin{pmatrix} k \\ L_0 \end{pmatrix} = gcg^{-1} \begin{pmatrix} k \\ L_0 \end{pmatrix} = gc \begin{pmatrix} k \\ L_0 \end{pmatrix} = g(L_c).$$

Hence $g$ determines via restriction an isomorphism $L_c \xrightarrow{\sim} L_d$. Conversely, suppose $L_c$ and $L_d$ are isomorphic. Then, by (1), so are $L_{\bar{c}}$ and $L_{\bar{d}}$. Let

$$\rho\colon L_c \xrightarrow{\sim} L_d, \quad \bar{\rho}\colon L_{\bar{c}} \xrightarrow{\sim} L_{\bar{d}}$$

be isomorphisms. Then so is

$$g := \rho \oplus \bar{\rho}\colon k \oplus L_0 = L_c \oplus L_{\bar{c}} \xrightarrow{\sim} L_d \oplus L_{\bar{d}} = k \oplus L_0,$$

which amounts to $g \in \mathrm{GL}(k \oplus L_0) = B^\times$. Moreover, for $x \in L_d$, $y \in L_{\bar{d}}$ we have $\rho^{-1}(x) \in L_c$, $\bar{\rho}^{-1}(y) \in L_{\bar{c}}$, hence

$$gcg^{-1}(x + y) = gc(\rho^{-1}(x) + \bar{\rho}^{-1}(y)) = (\rho \oplus \bar{\rho})(\rho^{-1}(x)) = x.$$

But this means $gcg^{-1} = d$, and $c, d$ are conjugate under inner automorphisms of $B$. Now suppose $\varphi(c) = d$ for some automorphism $\varphi$ of $B$. Then $B_{12}(c) \cong B_{12}(d)$, which by (2) implies $L_c^{\otimes 2} \cong L_d^{\otimes 2}$. Conversely, let this be so and put

$L := L_0 \otimes L_c^{*\otimes 2}$. Then (iii) yields isomorphisms $\Phi\colon B \xrightarrow{\sim} B' := \mathrm{End}_k(k \oplus L)$, $\Psi\colon B \xrightarrow{\sim} B'$ such that

$$\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \Psi(d).$$

Hence $\varphi := \Psi^{-1} \circ \Phi$ is an automorphism of $B$ sending $c$ to $d$.

(c) By (1), the line bundle $L_c$ is a direct summand of $k \oplus L_0$. Conversely, let $L$ be a direct summand of $k \oplus L_0$, so $k \oplus L_0 = L \oplus L'$ for some submodule $L' \subseteq k \oplus L_0$. Then the projection from $k \oplus L_0$ onto $L$ alongside $L'$ yields an idempotent $c \in B$ such that $L = L_c$, and by (a), $c$ is elementary.

**22.25** (a) Let $x_i/1$ be a basis of $L_{f_i}$ over $k_{f_i}$, for $i = 1, \dots, n$. Given $x \in L$, there exist $m \in \mathbb{N}$ and $\alpha_1, \dots, \alpha_n \in k$ such that $x/1 = (\alpha_i/f_i^m)(x_i/1) = (\alpha_i x_i)/f_i^m$ in $L_{f_i}$ for all $i = 1, \dots, n$. Hence for some integer $p \geq m$ and all $i = 1, \dots, n$, $f_i^p x = \beta_i x_i$, $\beta_i := f_i^{p-m}\alpha_i$. Since the $f_1^p, \dots, f_n^p$ continue to generate $k$ as an ideal, we find $g_1, \dots, g_n \in k$ such that $\sum f_i^p g_i = 1$. But this implies $x = \sum \beta_i g_i x_i$, so $L = \sum k x_i$ is generated by $x_1, \dots, x_n$.

(b) (i) $\Rightarrow$ (ii). Since $L$ is generated by two elements, we obtain a short exact sequence

$$0 \longrightarrow L' \longrightarrow k \oplus k \longrightarrow L \longrightarrow 0$$

of $k$-modules, which splits since $L$ is projective. Thus $L \oplus L' \cong k \oplus k$ is free of rank 2, and taking determinants (= second exterior powers), we obtain $L \otimes L' \cong k$, i.e., $L' \cong L^*$.

(ii) $\Rightarrow$ (iii). This is Exc. 22.24 for $L_0 := k$.

(iii) $\Rightarrow$ (iv). Write

$$c = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

with $\alpha, \beta, \gamma, \delta \in k$. Since $c$ has trace 1 and determinant 0, we have

$$\alpha + \delta = 1, \quad \alpha\delta = \beta\gamma. \tag{s1}$$

From Exc. 22.24 we deduce

$$L \cong L_c = \mathrm{Im}(c) = k\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} + k\begin{pmatrix} \beta \\ \delta \end{pmatrix}.$$

Observing

$$\beta\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \alpha\begin{pmatrix} \beta \\ \delta \end{pmatrix}, \quad \delta\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \gamma\begin{pmatrix} \beta \\ \delta \end{pmatrix}, \tag{s2}$$

we now put $f_1 = \alpha$, $f_2 = \delta$. Then $kf_1 + kf_2 = k$ by (s1), and (s2) shows that $L_{f_1}$ is

the free $k_{f_1}$-module of rank 1 with basis $\binom{\alpha/1}{\beta/1}$, while $L_{f_2}$ is the free $k_{f_2}$-module of rank 1 with basis $\binom{\beta/1}{\delta/1}$. Thus (iv) holds.

(iv) $\Rightarrow$ (i). This is just a special cse of (a).

Now suppose $L$ satisfies one (hence all) of the preceding four conditions. Then, by (ii), so does $L^*$, allowing us to assume $n > 0$. But then (iv) holds for $L^{\otimes n}$. In partiuclar, by (ii), an elementary idempotent $c^{(n)} \in \mathrm{Mat}_2(k)$ satisfying $L^{\otimes n} \cong L_{c^{(n)}}$ exists for any $n \in \mathbb{Z}$ and is unique up to conjugation by inner automorphisms (Exc. 22.24 (b)). Since $L^{\otimes 0} \cong k$ is free of rank 1, we may put $c^{(0)} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Moreover, combining (ii) with (1) in Exc. 22.24, we may also put $c^{(-1)} := \bar{c} = \mathbf{1}_2 - c$, and it will be enough to treat the case $n > 0$. Writing $c$ as in the proof of the implication (iii)$\Rightarrow$(iv), we claim that

$$\alpha^n \alpha_n + \delta^n \delta_n = 1, \tag{s3}$$

*where*

$$\alpha_n := \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{n-1-i} \delta^i, \quad \delta_n := \sum_{i=0}^{n-1} \binom{2n-1}{n+i} \alpha^{n-1-i} \delta^i,$$

*and*

$$c^{\langle n \rangle} := \begin{pmatrix} \alpha^n \alpha_n & \beta^n \delta_n \\ \gamma^n \alpha_n & \delta^n \delta_n \end{pmatrix} \in \mathrm{Mat}_2(k) \tag{s4}$$

*is an elementary idempotent satisfying* $L_{c^{\langle n \rangle}} \cong L_c^{\otimes n}$.

We begin by proving (s3), which follows from the computation

$$\begin{aligned} \alpha^n \alpha_n + \delta^n \delta_n &= \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i + \sum_{i=0}^{n-1} \binom{2n-1}{n+i} \alpha^{n-1-i} \delta^{n+i} \\ &= \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i + \sum_{j=n}^{2n-1} \binom{2n-1}{j} \alpha^{2n-1-j} \delta^j \\ &= \sum_{i=0}^{2n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i = (\alpha + \delta)^{2n-1} = 1. \end{aligned}$$

Combining (s3) with (s2), we conclude that $c^{(n)}$ as defined in (s4) has trace 1 and determinant 0, hence is an elementary idempotent. Moreover,

$$\beta^n \begin{pmatrix} \alpha^n \\ \gamma^n \end{pmatrix} = \alpha^n \begin{pmatrix} \beta^n \\ \delta^n \end{pmatrix}, \quad \delta^n \begin{pmatrix} \alpha^n \\ \gamma^n \end{pmatrix} = \gamma^n \begin{pmatrix} \beta^n \\ \delta^n \end{pmatrix}. \tag{s5}$$

We now put

$$f^{(n)} := \alpha^n \alpha_n, \quad g^{(n)} := \delta^n \delta_n \tag{s6}$$

and have $f^{(n)}+g^{(n)}=1$ by (s3). Setting $L:=L_c$, $L_{c^{(n)}}$, we must show $L^{\otimes n}\cong L^{(n)}$. To this end, we examine the situation of $k_{f^{(n)}}$ and $k_{g^{(n)}}$.

Over $k_{f^{(n)}}$, the quantities $\alpha,\alpha_n$ are both invertible. By (s2), therefore, $L_{f^{(n)}}$ is the free $k_{f^{(n)}}$- module with basis $\left(\begin{smallmatrix}\alpha\\ \gamma\end{smallmatrix}\right)$. Consequently, $(L^{\otimes n})_{f^{(n)}}=(L_{f^{(n)}})^{\otimes n}$ is the free $k_{f^{(n)}}$-module with basis $\left(\begin{smallmatrix}\alpha\\ \gamma\end{smallmatrix}\right)^{\otimes n}$. By the same token, $(L^{(n)})_{f^{(n)}}$ is the free $k_{f^{(n)}}$-module with basis $\left(\begin{smallmatrix}\alpha^n\alpha_n\\ \gamma^n\alpha_n\end{smallmatrix}\right)=\left(\begin{smallmatrix}\alpha^n\\ \gamma^n\end{smallmatrix}\right)\alpha_n$, which is the same as the free $k_{f^{(n)}}$-module with basis $\left(\begin{smallmatrix}\alpha^n\\ \gamma^n\end{smallmatrix}\right)$. Summing up, we find a unique isomorphism

$$\Phi^{(n)}\colon (L^{\otimes n})_{f^{(n)}}\xrightarrow{\sim}(L^{(n)})_{f^{(n)}}\quad\text{such that}\quad \Phi^{(n)}\Big(\begin{pmatrix}\alpha\\ \gamma\end{pmatrix}^{\otimes n}\Big)=\begin{pmatrix}\alpha^n\\ \gamma^n\end{pmatrix}.$$

Similarly, by (s6), the quantities $\delta,\delta^{(n)}$ are invertible over $k_{g^{(n)}}$, and there is a unique isomorphism

$$\Psi^{(n)}\colon (L^{\otimes n})_{g^{(n)}}\xrightarrow{\sim}(L^{(n)})_{g^{(n)}}\quad\text{such that}\quad \Psi^{(n)}\Big(\begin{pmatrix}\beta\\ \delta\end{pmatrix}^{\otimes n}\Big)=\begin{pmatrix}\beta^n\\ \delta^n\end{pmatrix}.$$

Over $k_{f^{(n)}g^{(n)}}$, all the quantities $\alpha,\alpha_n,\delta,\delta_n,\beta,\gamma$ become invertible, and we have $\left(\begin{smallmatrix}\beta\\ \delta\end{smallmatrix}\right)=\gamma^{-1}\delta\left(\begin{smallmatrix}\alpha\\ \gamma\end{smallmatrix}\right)$, hence $\left(\begin{smallmatrix}\beta\\ \gamma\end{smallmatrix}\right)^{\otimes n}=\gamma^{-n}\delta^n\left(\begin{smallmatrix}\alpha\\ \gamma\end{smallmatrix}\right)^{\otimes n}$, but also $\left(\begin{smallmatrix}\beta^n\\ \delta^n\end{smallmatrix}\right)=\gamma^{-n}\delta^n\left(\begin{smallmatrix}\alpha^n\\ \gamma^n\end{smallmatrix}\right)$. Hence the isomorphisms $\Phi^{(n)}$, $\Psi^{(n)}$ agree over $k_{f^{(n)}g^{(n)}}$ and thus glue to an isomorphism $L^{\otimes n}\xrightarrow{\sim}L^{(n)}$. This completes the proof.

*A4.8 Remark.* The final proof of this exercise would have become much more natural if we had used the identification of $\mathrm{Pic}(k)$ with $H^1_{\mathrm{Zar}}(k,\mathrm{GL}_1)$, compare Example 54.16.

**22.26** (i) $\Rightarrow$ (ii). Let $L$ be any line bundle over $k$ that is a direct summand of $k\oplus L_0$. By Exc. 22.24 (c), there exists an elementary idempotent $c\in B$ such that $L\cong L_c$. Using (i) to select an isomorphism $\Phi\colon B\xrightarrow{\sim}B'$, we obtain an elementary idempotent $c':=\Phi(c)\in B'$ and, again by Exc. 22.24, we find in $L':=L_{c'}$ a line bundle over $k$ that is a direct summand of $k\oplus L'_0$. Now (2) of Exc. 22.24

$$L_0^*\otimes L^{\otimes 2}\cong L_0^*\otimes L_c^{\otimes 2}\cong B_{12}(c)\cong B'_{12}(c')\cong L_0'^*\otimes L'^{\otimes 2},$$

and (1) holds.

(ii) $\Rightarrow$ (iii). This is clear since line bundles $L$ over $k$ satisfying the requirements of (ii) exist, e.g., $L:=k\oplus\{0\}\subseteq k\oplus L_0$.

(iii) $\Rightarrow$ (i). Let $L$, $L'$ be line bundles over $k$ that are direct summands of $k\oplus L_0$, $k\oplus L'_0$, respectively, and satisfy (1). By Exc. 22.24 (c), there exist elementary idempotents $c\in B$, $c'\in B'$ such that $L\cong L_c$, $L'\cong L_{c'}$. Now (1) yields

$$M:=L_0^*\otimes L_c^{\otimes 2}\cong L_0'^*\otimes L_{c'}^{\otimes 2},$$

and Exc. 22.24 (a) produces isomorphisms $\Phi\colon B \xrightarrow{\sim} C := \mathrm{End}_k(k \oplus M)$, $\Phi'\colon B' \xrightarrow{\sim} C$ sending $c, c'$ to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, respectively. In particular, $\Phi'^{-1} \circ \Phi$ is an isomorphism from $B$ to $B'$, and (i) holds.

**22.27** We apply Exc. 22.26 to $B := \mathrm{End}_k(k \oplus L_0)$, $L_0 := L$, and $B' := \mathrm{Mat}_2(k) = \mathrm{End}_k(k \oplus L_0')$, $L_0' := k$. Then $M := k \oplus \{0\} \subseteq k \oplus L_0$ is a free submodule of rank 1 and a direct summand at the same time. If $B$ is split, then $B \cong B'$ and condition (ii) of Exc. 22.26 yields a line bundle $M' \subseteq k \oplus L_0' = k \oplus k$ which is a direct summand of $k \oplus k$ and satisfies $L_0 \otimes M'^{\otimes 2} \cong L_0' \otimes M^{\otimes 2}$. This means $L_0 \cong M'^{* \otimes 2}$. Moreover, $k \oplus k \cong M' \oplus M''$ for some line bundle $M''$, and taking determinants (= second exterior powers), we obtain $M' \otimes M'' \cong k$. Hence $M'^* \cong M''$, being a homomorphic image of $k \oplus k$, is generated by two elements.

Conversely, suppose $L_0 = L \cong M'^{\otimes 2}$ for some line bundle $M'$ on two generators over $k$. Then Exc. 22.25 (b) implies $M' \oplus M'^* \cong k \oplus k$. Since $L_0 \otimes M'^{* \otimes 2} \cong L \otimes M'^{* \otimes 2} \cong k \cong L_0' \otimes M^{\otimes 2}$, we deduce from Exc. 22.26 that $B$ and $B' = \mathrm{Mat}_2(k)$ are isomorphic, i.e., $B$ is split.

Finally, suppose we are given a line bundle $L$ on two generators over $k$ that is not a square in $\mathrm{Pic}(k)$. (For example, take $k$ to be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-14})$. Then $\mathrm{Pic}(k) \cong \mathbb{Z}/4$ and we take $L$ to be a generator. It is generated by 2 elements because $k$ is Dedekind.) By what we have just shown, the quaternion algebra

$$B := \mathrm{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}$$

is reduced but not split. It will be free as a $k$-module once we have shown that $L \oplus L^*$ is a free $k$-module. But this follows immediately from Exc. 22.25 (b).

**22.28** By Exc. 22.27, the quaternion algebra

$$B := \mathrm{End}_k(k \oplus L') = \begin{pmatrix} k & L'^* \\ L' & k \end{pmatrix}$$

is split since $L'$ is the square (in $\mathrm{Pic}(k)$) of some line bundle on two generators over $k$. Computing the norm of $B$ in two ways by means of (22.12.1), we deduce $\mathbf{h} \perp \mathbf{h} \cong n_B \cong \mathbf{h} \perp (-\mathbf{h}_{L'}) \cong \mathbf{h} \perp \mathbf{h}_{L'}$ and hence obtain the first assertion. As to the second, it suffices to consult Exc. 11.30, which shows that the hyperbolic plane $\mathbf{h}_{L'}$ is not split.

**22.29** Localizing if necessary, we may assume that $M$ is free (of rank 3). Let $(e_i)_{1 \le i \le 3}$ be a basis of $M$ and $(e_i^*)_{1 \le i \le 3}$ the corresponding dual basis of $M^*$. Setting $\alpha := \theta(e_1 \wedge e_2 \wedge e_3)$, $\beta := \theta^{*-1}(e_1^* \wedge e_2^* \wedge e_3^*)$, we apply (22.14.1) to conclude $\alpha\beta = 1$. In particular, $\alpha$ and $\beta$ are both invertible.

Letting $(ijl)$ vary over the cyclic permutations of (123) and $s = 1, 2, 3$, we

now apply (22.14.2) to obtain $\langle e_i \times_\theta e_j, e_s\rangle = \theta(e_i \wedge e_j \wedge e_s) = \alpha\delta_{ls} = \langle \alpha e_l^*, e_s\rangle$ and $\langle e_s^*, e_i^* \times_\theta e_j^*\rangle = \theta^{*-1}(e_i^* \wedge e_j^* \wedge e_s^*) = \beta\delta_{ls} = \langle e_s^*, \beta e_l\rangle$, which amounts to

$$e_i \times_\theta e_j = \alpha e_l^*, \quad e_i^* \times_\theta e_j^* = \beta e_l. \tag{s1}$$

Now observe that our asserted equations are alternating in $u, v$ (resp. $u^*, v^*$). For the first equation, we may therefore assume $u = e_i$, $v = e_j$, $w^* = e_s^*$. Then (s1) yields

$$\begin{aligned}(e_i \times_\theta e_j) \times_\theta e_s^* = \alpha e_l^* \times_\theta e_s^* &= \begin{cases} \alpha\beta e_j & \text{for } s = i,\\ -\alpha\beta e_i & \text{for } s = j,\\ 0 & \text{for } s = l \end{cases}\\ &= \begin{cases} e_j & \text{for } s = i,\\ -e_i & \text{for } s = j,\\ 0 & \text{for } s = l \end{cases}\\ &= \langle e_s^*, e_i\rangle e_j - \langle e_s^*, e_j\rangle e_i,\end{aligned}$$

as claimed. Similarly, for the second equation, we may assume $u^* = e_i^*$, $v^* = e_j^*$, $w = e_s$ and obtain

$$\begin{aligned}(e_i^* \times_\theta e_j^*) \times_\theta e_s = \beta e_l \times_\theta e_s &= \begin{cases} \alpha\beta e_j^* & \text{for } s = i,\\ -\alpha\beta e_i^* & \text{for } s = j,\\ 0 & \text{for } s = l \end{cases}\\ &= \begin{cases} e_j^* & \text{for } s = i,\\ -e_i^* & \text{for } s = j,\\ 0 & \text{for } s = l \end{cases}\\ &= \langle e_i^*, e_s\rangle e_j^* - \langle e_j^*, e_s\rangle e_i^*.\end{aligned}$$

This completes the proof.

**22.30** Let $C$ be a reduced octonion algebra over the Dedekind domain $k$. By Thm. 22.15, there exist a finitely generated projective $k$-module $M$ of rank 3 and an orientation $\theta$ of $M$ such that $C \cong \mathrm{Zor}(M, \theta)$ in the sense of 22.14. By [7, §VII.4.10, Prop. 24], we can find an ideal $\mathfrak{a} \subseteq k$ satisfying $M \cong k^2 \oplus \mathfrak{a}$. But $\bigwedge^3(M) \cong k$ by means of $\theta$. By [8, III, §7.7, Cor. of Prop. 10], therefore, $\bigwedge^2(k^2) \otimes \mathfrak{a} \cong k \otimes \mathfrak{a} \cong \mathfrak{a}$ is free of rank 1, forcing $M$ to be free of rank 3. Now Thm. 22.15 shows that $C \cong \mathrm{Zor}(M, \theta) \cong \mathrm{Zor}(k)$ is split.

## Solutions for Section 23

**23.28** The cases $s = 1$ and $s = r$ are obvious. Hence we may assume $1 < s < r$, which by Cor. 19.11 implies that $C, B, B'$ are all regular. Arguing by induction on $r - s$, we let $\varphi\colon B \xrightarrow{\sim} B'$ be an isomorphism. Then $C = B \perp B^\perp = B' \perp B'^\perp$, hence

$$n_B \perp n_C|_{B^\perp} \cong n_C \cong n_{B'} \perp n_C|_{B'^\perp}$$

On the other hand, $\varphi$ is an isometry from $n_B$ onto $n_{B'}$. Thus, by Witt cancellation (Thm. 11.27), $n_C|_{B^\perp}$ and $n_C|_{B'^\perp}$ are isometric. Since $s < r$, applying Lemma 11.26 yields an element $l \in B^\perp$ such that $n_C(l) \in k^\times$, which in turn leads to an element $l' \in B'^\perp$ satisfying $n_C(l') = n_C(l) =: -\mu$. Write $B_1$ (resp. $B'_1$) for the subalgebra of $C$ generated by $B$ (resp. $B'$) and $l$ (resp. $l'$). Then Cor. 18.9 yields unique isomorphisms $h\colon \operatorname{Cay}(B,\mu) = B \oplus Bj \xrightarrow{\sim} B_1$ (resp. $h'\colon \operatorname{Cay}(B',\mu) = B' \oplus B'j' \xrightarrow{\sim} B'_1$) extending the identity of $B$ (resp. $B'$) and sending $j$ (resp. $j'$) to $l$ (resp. $l'$). The isomorphisms thus obtained fit into the diagram

$$\begin{array}{ccc} \operatorname{Cay}(B,\mu) & \xrightarrow[\cong]{h} & B_1 \\ {\scriptstyle \operatorname{Cay}(B,\varphi)}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\vdots{\scriptstyle \varphi_1} \\ \operatorname{Cay}(B',\mu) & \xrightarrow[h']{\cong} & B'_1, \end{array}$$

which can be completed uniquely to a commutative square by the dotted isomorphism $\varphi_1\colon B_1 \xrightarrow{\sim} B'_1$ as indicated. Since $B_1$ and $B'_1$ both have rank $2s$, the induction hypothesis applies to $\varphi_1$ and completes the proof. To conclude the solution to the problem, let $B \subseteq \mathbb{O}$ be a non-zero subalgebra and let $0 \neq x \in B$. Then $n_\mathbb{O}(x) \neq 0$ and $B$ contains the element $x^2 = t_\mathbb{O}(x)x - n_\mathbb{O}(x)1_\mathbb{O}$, hence $1_\mathbb{O}$. Thus $B$ is a unital subalgebra of $\mathbb{O}$ on which $n_\mathbb{O}$ continues to permit composition and to be anisotropic, hence regular as well since the characteristic is not 2. Summing up, therefore, $B \subseteq \mathbb{O}$ is a composition division subalgebra. From 23.13 we now conclude that $B$ is isomorphic to one of the algebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$, and the Skolem-Noether theorem completes the proof.

**23.29** By Prop. 23.2 (b), $f$ preserves not only norms and units, but also traces and conjugations.

(a) Applying (17.4.2), we obtain

$$\begin{aligned} f(U_x y) &= n_C(x,\bar{y})f(x) - n_C(x)f(\bar{y}) = n_C\big(f(x),\overline{f(y)}\big)f(x) - n_C\big(f(x)\big)\overline{f(y)} \\ &= U_{f(x)}f(y), \end{aligned}$$

hence (1). In order to prove (2), we first note

$$x^2 = U_x 1_C, \quad (U_{x+y} - U_x - U_y)z = x(yz) + z(yx),$$

so by (1), $f$ preserves squares and the expression $x(yz) + z(yx)$. Abbreviating the left-hand side of (2) by $A$ and using the fact that the associator of $C$ is alternating, we can now compute

$$\begin{aligned} A &= f(xy)^2 - f(xy)(f(y)f(x)) - (f(x)f(y))f(xy) + f(x)f(y)^2 f(x) \\ &= f((xy)^2) - f(xy)(f(y)f(x)) - f(x)(f(y)f(xy)) - [f(x), f(y), f(xy)] \\ &\quad + f(xy^2x) \\ &= [f(x), f(xy), f(y)] + f\Big((xy)^2 - (xy)(yx) - x(y(xy)) + xy^2x\Big) \\ &= [f(x), f(xy), f(y)] \end{aligned}$$

since, thanks to Artin's Theorem (Cor. 14.5), the subalgebra of $C$ generated by two elements is associative. This completes the proof of (2). In order to complete the proof of (a), it will therefore suffice to show that the *right*-hand side of (2) is symmetric in $x, y$. To see this, we note that, since squares are preserved by $f$, so is the circle product. Hence $f(x \circ y) = f(x) \circ f(y)$, which implies

$$\begin{aligned} [f(y), f(yx), f(x)] &= [f(y), f(x \circ y), f(x)] - [f(y), f(xy), f(x)] \\ &= [f(y), f(x) \circ f(y), f(y)] + [f(x), f(xy), f(y)] \\ &= [f(x), f(xy), f(y)], \end{aligned}$$

again by Artin's Theorem, and the assertion follows.

(b) Since $f$ preserves norms and traces, we have $t_{C'}(c') = t_{C'}(f(c)) = t_C(c) = 1$, $n_{C'}(c') = n_{C'}(f(c)) = n_C(c) = 0$, so $c' \in C'$ is an elementary idempotent. Now, as we have seen in (a), $f$ preserves the circle product: $f(x \circ y) = f(x) \circ f(y)$ for all $x, y \in C$. In particular, $f(c \circ y) = c' \circ f(y)$. Hence, writing $C_{ij}$, $i, j = 1, 2$, for the Peirce components of $C$ relative to $c$, it will be enough to show

$$C_{12} + C_{21} = \{x \in C \mid c \circ x = x\}. \tag{s1}$$

For $x \in C$, we let $x = x_{11} + x_{12} + x_{21} + x_{22}$ be its Peirce decomposition relative to $c$. Then

$$c \circ x = cx + xc = x_{11} + x_{12} + x_{11} + x_{21} = 2x_{11} + x_{12} + x_{21},$$

and comparing Peirce components we see that $c \circ x = x$ if and only if $x_{11} = x_{22} = 0$. Hence (s1) is proved.

**23.30** (a) We begin by assuming that the case of a local ring has been settled

and then let $k$ be arbitrary. We put $X := \mathrm{Spec}(k)$ and deduce from Exc. 9.28 (b) that

$$X_+ := \{\mathfrak{p} \in X \mid f_\mathfrak{p} \colon B_\mathfrak{p} \to B'_\mathfrak{p} \text{ is an isomorphism}\},$$
$$X_- := \{\mathfrak{p} \in X \mid f_\mathfrak{p} \colon B_\mathfrak{p} \to B'_\mathfrak{p} \text{ is an anti-isomorphism}\}$$

are Zariski-open subsets of $X$. Since a quaternion algebra is not commutative, they are also disjoint, and our assumption implies that they cover $X$. Hence Exc. 9.29, yields a complete orthogonal system $(\varepsilon_+, \varepsilon_-)$ of idempotents in $k$ satisfying $X_\pm = D(\varepsilon_\pm)$. Now it suffices to put $k_\pm = k\varepsilon_\pm$ and to invoke (9.7.5), which implies for any $\mathfrak{p}_+ \in \mathrm{Spec}(k_+)$ that $\mathfrak{p} := \mathfrak{p}_+ \times k_- \in D(\varepsilon_+)$ makes $f_{+\mathfrak{p}_+} = (f_\mathfrak{p})_{k_{+\mathfrak{p}_+}} \colon B_{+\mathfrak{p}_+} \to B'_{+\mathfrak{p}_+}$ (by (9.5.7)) an isomorphism. Similarly, for $\mathfrak{p}_- \in \mathrm{Spec}(k_-)$, $f_{-\mathfrak{p}_-} \colon B_{-\mathfrak{p}_-} \to B'_{-\mathfrak{p}_-}$ turns out to be an anti-isomorphism. Hence $f_+$ is an isomorphism and $f_-$ is an anti-isomorphism.

We are thus left with the case that $k$ is a local ring and must show that $f$ is either an isomorphism or an anti-isomorphism. Thm. 19.16 (b) and Exc. 19.33 (a) yield a quadratic étale subalgebra $D = k[u] \subseteq B$, for some $u \in B$ having trace 1. Since $f$ preserves units, norms, and traces by Prop. 23.2, we conclude that $D' := f(D) = k[u']$, $u' := f(u)$, is a quadratic étale subalgebra of $B'$ (Prop. 19.8), and $f|_D \colon D \to D'$ is an isomorphism (Prop. 23.4). Now apply Thm. 19.16 (a) to reach $B$ from $D$ by means of the Cayley-Dickson construction: there exists a unit $\mu \in k^\times$ such that the inclusion $D \hookrightarrow B$ extends to an identification $B = \mathrm{Cay}(D, \mu) = D \oplus Dj$, $j \in D^\perp$, $n_B(j) = -\mu$. Setting $j' := f(j) \in D'^\perp \subseteq B'$, we obtain $n_{B'}(j') = -\mu$, and from Prop. 18.7 we conclude that $f|_D$ extends to a homomorphism $g \colon B \to B'$ of conic algebras satisfying $g(j) = j'$. By Cor. 18.9, therefore, $g$ is an isomorphism from $B$ onto the subalgebra of $B'$ generated by $D'$ and $j'$. Counting ranks we conclude that $g$ is in fact an isomorphism from $B$ onto $B'$. Hence $f_1 := g^{-1} \circ f \colon B \to B$ is a unital norm equivalence inducing the identity on $D$ and satisfying $f_1(j) = j$. Since $f_1$ stabilizes $D^\perp = Dj$, we find a $k$-linear bijection $\varphi \colon D \to D$ such that $f_1(vj) = \varphi(v)j$ for all $v \in D$. Then $\varphi(1_D) = 1_D$, and since $n_B$ permits composition, $\varphi$ leaves $n_D$ invariant and is thus a unital norm equivalence of $D$, hence an automorphism (Prop. 23.4 (b)). By Exc. 19.33, therefore, we are left with two cases depending on $\varphi$.

Suppose first that $\varphi = \mathbf{1}_D$. Then $f_1 = \mathbf{1}_B$, and $f = g \colon B \to B'$ is an isomorphism.

Suppose next that $\varphi = \iota_D$. By Exc. 18.19, the map $\psi \colon B \to B$ defined by $\psi(v + wj) := v - wj$ for all $v, w \in D$ is an automorphism, and one checks that $f_1 = \psi \circ \mathrm{Int}(j) \circ \iota_B$, where $\mathrm{Int}(j)$ stands for the inner automorphism $x \mapsto jxj^{-1}$ of $B$ affected by $j$. Hence $f = g \circ \psi \circ \mathrm{Int}(j) \circ \iota_B \colon B \to B'$ is an anti-isomorphism.

(b) The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are obvious, so let us prove (i) under the assumption (iii). By Cor. 23.3, there exists a unital norm equivalence $f\colon B \to B'$. With the notation of (1), we apply (a) to conclude that $g := f_+ \times (f_- \circ \iota_{B_-})\colon B \to B'$ is an isomorphism.

**23.31** By Prop. 23.4 (a), every automorphism of $B$ is a unital norm equivalence. Hence it suffices to show that, conversely, if $f\colon B \to B$ is a unital norm equivalence sending $e_{11}$ to $c$, then an automorphism of $B$ exists having the same property. From Exc. 23.29 (b) we deduce that $c$ is an elementary idempotent in $B$. Hence Exc. 22.24 (a) yields a line bundle $L$ over $k$ and an isomorphism

$$\Phi\colon B \xrightarrow{\sim} B' := \mathrm{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix} \quad \text{such that} \quad \Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Viewing $B_{12}(c) \oplus B_{21}(c)$ (resp. $L^* \oplus L$) canonically as quadratic submodules of $(B, n_B)$ (resp. $(B', n_{B'})$),

$$\Phi\colon B_{12}(c) \oplus B_{21}(c) \xrightarrow{\sim} L^* \oplus L$$

is an isometry and by (22.12.1), (11.18.1), there is a natural identification of $L^* \oplus L$ with the hyperbolic plane $\mathbf{h}_L$. On the other hand, $f$, being a unital norm equivalence, by Exc. 23.29 (b) induces an isometry from the split hyperbolic plane $k \oplus k \cong B_{12}(e_{11}) \oplus B_{21}(e_{11})$ onto $B_{12}(c) \oplus B_{21}(c)$. Hence the hyperbolic plane $\mathbf{h}_L$ is split, which by Exc. 11.30 forces the line bundle $L$ to be free of rank 1. Thus we may identify $L = k$ and in this way view $\Phi$ as an automorphism of $B$ sending $e_{11}$ to $c$.

**23.32** By Exc. 15.17, $\varphi := L_p R_{p^{-1}}$ is an isomorphism from $C$ to $C^q$ with $q := p^{-3}$.

(a) By Prop. 23.2 (a), $\varphi$ is a norm similarity fixing $1_C$ and hence a unital norm equivalence.

(b) $\varphi$ is an automorphism of $C$ if and only if $C = C^q$, which by (15.9.4) is equivalent to $q \in \mathrm{Nuc}(C) = k1_C$ (Exc. 19.32 (b)), hence to $p^3 = q^{-1} \in k1_C$.

(c) Assume $\varphi$ is an anti-automorphism of $C$. Then $C^{\mathrm{op}} = C^q$, so we have $yx = (xq^{-1})(qy)$, equivalently, $y(xq) = x(qy)$, for all $x, y \in C$. Setting $x = 1_C$ gives $yq = qy$ for all $y \in C$. By Exc. 19.32 (b), this implies $q \in k1_C$ and then $xy = yx$ for all $x, y \in C$, a contradiction.

**23.33** Let $p, q \in C^\times$. By Exc. 17.12, $C^{(p,q)}$ is a multiplicative conic alternative $k$-algebra with norm $n_{C^{(p,q)}} = n_C(pq)n_C$. By multiplicativity, $L_{pq}$ is an isometry from $n_{C^{(p,q)}}$ to $n_C$. Hence $C^{(p,q)}$ is a composition algebra which is regular if $C$ is. Moreover, if $C$ is associative, then $L_{pq}\colon C^{(p,q)} \to C$ is an isomorphism. And finally, if $k$ is LG, the norm equivalence theorem 23.5 shows that $C$ and $C^{(p,q)}$ are isomorphic.

**23.34** Let $x_i = u_i + v_i j$, $u_i, v_i \in \mathbb{O}$, $i = 1, 2$ be non-zero elements of $\mathbb{S}$, Then Exc. 19.29 (a) for $\mu = -1$ shows that $x_1 x_2 = 0$ if and only if $u_i \neq 0 \neq v_i$ for $i = 1, 2$ and

$$n_{\mathbb{O}}(u_1) = n_{\mathbb{O}}(v_1), \quad (u_1 u_2)\bar{v}_1 = -u_1(u_2 \bar{v}_1), \quad v_2 = -(v_1 \bar{u}_2)u_1^{-1}. \tag{s1}$$

Now let $(w_i)_{1 \leq i \leq 7}$ be a Cartan-Shouten basis of $\mathbb{O}$ in the sense of 2.1. Combining (18.4.1) with Fig. 2a on page 12, we compute

$$\begin{aligned}(w_1 + w_3 j)(w_2 - w_6 j) &= (w_1 w_2 - (-\bar{w}_6)w_3) + (w_3 \bar{w}_2 - w_6 w_1)j \\ &= (w_1 w_2 - w_6 w_3) + (-w_3 w_2 - w_6 w_1)j,\end{aligned}$$

where $w_6 w_3 = w_4 = w_1 w_2$ and $w_6 w_1 = w_5 = -w_3 w_2$. Thus the quantities $a := w_1 + w_3 j$, $b := w_2 - w_6 j$ have $\mathbb{S}$-norm 2 and satisfy $ab = 0$, so we conclude $(a, b) \in \mathrm{Zer}(\mathbb{S})$, while (s1) (or the property of $(w_i)$ being a Cartan-Shouten basis) yields

$$w_6 = (w_3 \bar{w}_2)w_1^{-1} = (w_3 w_2)w_1. \tag{s2}$$

We must show that the action of $G$ on $\mathrm{Zer}(\mathbb{S})$ is simply transitive. Let $(x_1, x_2) \in \mathrm{Zer}(\mathbb{S})$ and write $x_i = u_i + v_i j$ with $u_i, v_i \in \mathbb{O}$ for $i = 1, 2$ as before. Then (s1) shows $n_{\mathbb{O}}(u_i) = n_{\mathbb{O}}(v_i)$ for $i = 1, 2$, whence the relations $n_{\mathbb{S}}(x_i) = 2$ imply $n_{\mathbb{O}}(u_i) = n_{\mathbb{O}}(v_i) = 1$. From Exc. 19.29 and (16.5.5) we deduce $0 = x := u_1 \circ u_2 = \alpha 1_{\mathbb{O}} + \alpha_1 u_1 + \alpha_2 u_2$, $\alpha := -n_{\mathbb{O}}(u_1, u_2)$, $\alpha_i := t_{\mathbb{O}}(u_{3-i})$, $i = 1, 2$, hence $0 = u_1 \circ x = 2\alpha u_1 + 2\alpha_1 u_1^2 = 2u_1(\alpha 1_{\mathbb{O}} + \alpha_1 u_1)$. Thus $0 = y := \alpha 1_{\mathbb{O}} + \alpha_1 u_1$, which implies $0 = y \circ u_2 = 2\alpha 1_{\mathbb{O}}$, and we conclude $0 = \alpha = \alpha_1 = \alpha_2$. Summing up, we have shown that $(u_1, u_2)$ is an orthonormal system in the euclidean space $\mathbb{O}^0$. Consulting Exc. 19.29 (b) again, we also get $n_{\mathbb{O}}(u_1 u_2, v_1) = 0$. By Exc. 2.8, therefore, the quantities $u_1, u_2, v_1$ can be extended to a Cartan-Shouten basis of $\mathbb{O}$. Hence there exists an automorphism $\sigma$ of $\mathbb{O}$ sending $u_1, u_2, v_1$ respectively to $w_1, w_2, w_3$. Consulting (s1), (s2), we conclude that $\sigma$ also sends $v_2$ to $-w_6$. But this means $\sigma((x_1, x_2)) = (a, b)$, and we have proved that the action is transitive. It remains to show that $\sigma(a) = a$, $\sigma(b) = b$ implies $\sigma = \mathbf{1}_{\mathbb{O}}$. But this is clear since we then have $\sigma(w_i) = w_i$ for $i = 1, 2, 3$, and $w_1, w_2, w_3$ by Exc. 2.8 generate the octonion algebra $\mathbb{O}$.

**23.35** We begin by proving the following general statement.

**Claim.** *Let $(V, Q)$ be a hyperbolic quadratic space of dimension $2n$ over $\mathbb{F}_q$. Then the number of anisotropic vectors in $(V, Q)$ is*

$$q^{n-1}(q - 1)(q^n - 1).$$

*Proof* We identify $(V, Q) = (\mathbb{F}_q^n \times \mathbb{F}_q^n, (x, y) \mapsto x^\mathsf{T} y)$ and note for $x \in \mathbb{F}_q^n$ that

$$|\{y \in \mathbb{F}_q^n \mid x^\mathsf{T} y = 0\}| = \begin{cases} q^n & \text{for } x = 0, \\ q^{n-1} & \text{for } x \neq 0. \end{cases}$$

Thus $|\{v \in V \mid Q(v) = 0\}| = q^n + (q^n - 1)q^{n-1}$, and we conclude that $(V, Q)$ contains precisely

$$\begin{aligned} q^{2n} - q^n - (q^n - 1)q^{n-1} &= q^n(q^n - 1) - (q^n - 1)q^{n-1} = (q^n - q^{n-1})(q^n - 1) \\ &= q^{n-1}(q - 1)(q^n - 1) \end{aligned}$$

anisotropic vectors. □

We now turn to the assertions of our problem. Since the anisotropic vectors of $C$ relative to $n_C$ are just its invertible elements (Prop. 17.5), and the norm of the split octonions is hyperbolic (Cor. 22.18), the preceding claim reduces to the first equation for $n = 3$.

To prove the second equation, we note that $n\colon C^\times \to \mathbb{F}_q^\times, x \mapsto n(x) := n_C(x)$, is a surjective multiplicative map. Writing $N := \{x \in C \mid n_C(x) = 1\}$ for its "kernel", we let $x, y \in C^\times$, use Prop. 13.6 and obtain

$$y \in n^{-1}(n(x)) \Leftrightarrow n(y) = n(x) \Leftrightarrow n(x^{-1}y) = 1 \Leftrightarrow x^{-1}y \in N \Leftrightarrow y \in xN,$$

so the fibers of $n$ all have the same cardinality. This shows $|N| = |C^\times|/|\mathbb{F}_q^\times| = q^3(q^4 - 1)$.

**23.36** (a) is trivial: if $x \in M$ is not minimal, then $x = y + z$ for some $y, z \in M$ such that $Q(y) < Q(x)$ and $Q(z) < Q(x)$. Proceeding with $y, z$ in the same manner, we eventually arrive at a decomposition of $x$ as a finite sum of minimal elements.

(b) Again this is trivial, demanding not even the *sketch* of a proof.

(c) We begin with a simple lemma.

**Lemma.** *(i) If $N \subseteq M$ is a submodule, then* $\mathrm{Min}(M, Q) \cap N \subseteq \mathrm{Min}(N, Q|_N)$.

*(ii) If $M = N \perp N'$ is a decomposition of $M$ into the orthogonal sum (relative to $Q$) of two submodules $N, N' \subseteq M$, then* $\mathrm{Min}(M, Q) = \mathrm{Min}(N, Q|_N) \cup \mathrm{Min}(N', Q|_{N'})$.

*Proof* In order to prove (i), let $x \in \mathrm{Min}(M, Q) \cap N$ and suppose we have a decomposition $x = y + z$ with $y, z \in N$, $Q(y) < Q(x)$, $Q(z) < Q(x)$. Then this decomposition takes place also in $M$, contradicting minimality of $x$ in $(M, Q)$. Thus $x \in \mathrm{Min}(N, Q|_N)$. But note for $x \in \mathrm{Min}(N, Q|_N)$, that it is conceivable to have a decomposition $x = y+z$ with $y, z \in M \setminus N$ and $Q(y) < Q(x)$, $Q(z) < Q(x)$, so in general we won't have equality in (i).

In order to prove (ii), let $x \in \mathrm{Min}(M,Q)$ and write $x = y + y'$ with $y \in N$, $y' \in N'$. Then $Q(x) = Q(y) + Q(y')$, and since $x$ is minimal in $M$, we conclude $Q(y) = 0$ or $Q(y') = 0$, hence $y = 0$ or $y' = 0$. Thus $\mathrm{Min}(M,Q) \subseteq N \cup N'$, which implies

$$\begin{aligned}\mathrm{Min}(M,Q) &= \mathrm{Min}(M,Q) \cap (N \cup N') \\ &= (\mathrm{Min}(M,Q) \cap N) \cup (\mathrm{Min}(M,Q) \cap N')\,.\end{aligned}$$

By symmetry and (i), it therefore suffices to show $\mathrm{Min}(N, Q|_N) \subseteq \mathrm{Min}(M,Q)$. Let $x \in \mathrm{Min}(N, Q|_N)$ and suppose $x = y + z$ for some $y, z \in M$, $Q(y) < Q(x)$, $Q(z) < Q(x)$. Write $y = u + u'$, $z = v + v'$ with $u, v \in N$, $u', v' \in N'$. Since $x$ belongs to $N$, this implies $x = u + v$ and $Q(u) \leq Q(y) < Q(x)$, $Q(v) \leq Q(z) < Q(x)$, in contradiction to $x$ being a minimal vector of $(N, Q|_N)$. Thus $x \in \mathrm{Min}(M,Q)$. □

We can now prove (c). Let $x, y \in \mathrm{Min}(M,Q)$ be inequivalent. For $u \in [x]$, $v \in [y]$, the assumption $Q(u,v) \neq 0$ would imply that $u, v \in \mathrm{Min}(M,Q)$ are equivalent. Since $M_{[x]}$ is spanned as a $\mathbb{Z}$-module by the minimal elements of $(M,Q)$ belonging to $[x]$, ditto for $M_{[y]}$, this contradiction shows that $M_{[x]}$ and $M_{[y]}$ are orthogonal. But every $x \in \mathrm{Min}(M,Q)$ belongs to $M_{[x]}$, and $M$ is spanned by $\mathrm{Min}(M,Q)$ as a $\mathbb{Z}$-module. Thus $M$ is the orthogonal sum of the distinct $M_{[x]}$'s, $x \in \mathrm{Min}(M,Q)$, and it remains to show that each $M_{[x]}$ is indecomposable. Thanks to the obvious extension of (b) in the preceding lemma to more than two orthogonal summands, it will actually be enough to show that every positive definite integral quadratic module $(M,Q)$ all of whose minimal elements are equivalent is indecomposable. Indeed, suppose we have an orthogonal decomposition $M = N \perp N'$ relative to $Q$, with submodules $N, N' \subseteq M$, and let $x, y \in \mathrm{Min}(M,Q)$. By part (b) of the lemma, we may assume $x \in \mathrm{Min}(N, Q|_N)$, and by definition, there is a finite sequence $x = x_0, x_1, \ldots, x_{k-1}, x_k = y$ of minimal vectors in $(M,Q)$ such that $Q(x_{i-1}, x_i) \neq 0$ for $1 \leq i \leq k$. We claim $x_i \in \mathrm{Min}(N, Q|_N)$ for all $i = 0, \ldots, k$ and argue by induction. For $i = 0$, there is nothing to prove. If $i > 0$ and the assertion holds for $i - 1$, then $x_i \notin N'$ since $x_{i-1} \in N$ by the induction hypothesis and $Q(x_{i-1}, x_i) \neq 0$, whence aprt (b) of the lemma implies $x_i \in \mathrm{Min}(N, Q|_N)$, and the induction is complete. In particular, $y \in \mathrm{Min}(N, Q|_N)$, and we have shown $\mathrm{Min}(M,Q) = \mathrm{Min}(N, Q|_N)$, which obviously implies $M = N$, $N' = \{0\}$.

**23.37** We put $C^\dagger = C/2C = C \otimes_{\mathbb{Z}} \mathbb{F}_2$ as a conic algebra over $\mathbb{F}_2$ and write $x \mapsto x^\dagger$ for the natural epimorphism from $C$ to $C^\dagger$. This epimorphism canonically induces a map from $C^\times$ to $C^{\dagger\times}$, which may or may not be surjective. Note that, since the discriminant of $C$ is odd, $C^\dagger$ is a composition algebra of di-

mension 8 over $\mathbb{F}_2$, hence an octonion algebra and thus isomorphic to $\mathrm{Zor}(\mathbb{F}_2)$ (Cor. 22.18).

**Lemma.** *For $x, y \in C^\times$ we have $x^\dagger = y^\dagger$ if and only if $y = \pm x$.*

*Proof* $y = \pm x$ clearly implies $x^\dagger = y^\dagger$. Conversely, let this be so. Then $y = x + 2z$ for some $z \in C$. If $z = 0$, we are done, so we may assume $z \neq 0$. Since $x, y \in C$ are both units, we obtain $1 = n_C(x + 2z) = 1 + 2n_C(x, z) + 4n_C(z)$, hence $n_C(x, z) = -2n_C(z)$, and applying the Cauchy-Schwarz inequality yields

$$4n_C(z)^2 = n_C(x, z)^2 \leq n_C(x, x)n_C(z, z) = 4n_C(z).$$

But $n_C(z)$ is a positive integer, forcing $n_C(z) = 1$. Thus the above inequality is, in fact, an equality, which implies $z = \alpha x$ for some $\alpha \in \mathbb{Q}$. Taking norms, we deduce $\alpha^2 = 1$, hence $\alpha = \pm 1$, where the assumption $\alpha = 1$ would lead to the contradiction that $y = 3x$ is not invertible in $C$. Hence $\alpha = -1$ and $y = -x$. □

We can now establish the first part of the problem. By Exc. 23.35 for $q = 2$, we have $|C^{\dagger\times}| = 120$, while by the lemma, the fiber of an arbitrary element $u \in C^{\dagger\times}$ under the natural map $C^\times \to C^{\dagger\times}$ is either empty or consists of two elements. Hence $|C^\times| \leq 240$.

For the rest of the proof, we may assume that $|C^\times| = 240$. Writing $C^{\times\dagger}$ for the image of $C^\times$ under the natural map $C^\times \to C^{\dagger\times}$, and putting $r := |C^{\times\dagger}|$, we note that the fiber of any point in $C^{\times\dagger}$ consists of two elements. Thus $2r = 240$, hence $r = 120 = |C^{\dagger\times}|$, and we conclude $C^{\times\dagger} = C^{\dagger\times}$. In other words, *the natural map $C^\times \to C^{\dagger\times}$ is surjective.*

We can now prove that the positive definite integral quadratic lattice $(C, n_C)$ is indecomposable. We have $C^\times = \{x \in C \mid n_C(x) = 1\} \subseteq \mathrm{Min}(C, n_C)$, and for $x, y \in C^\times$, Exc. 11.38 (b) yields a sequence $x^\dagger = x'_0, x'_1, \ldots, x'_k = y^\dagger$ of elements in $C^{\dagger\times}$ such that $k \leq 2$ and $n_{C^\dagger}(x'_{i-1}, x'_i) \neq 0$ for $1 \leq i \leq k$. Since the natural map $C^\times \to C^{\dagger\times}$ is surjective, each $x'_i$, $1 \leq i < k$, lifts to an invertible element $x_i \in C$, so we have got a sequence $x =: x_0, x_1, \ldots, x_k := y$ of elements in $C^\times$, hence of minimal vectors in $(C, n_C)$, such that $n_C(x_{i-1}, x_i)$ is an odd integer and, in particular, different from 0, for $1 \leq i \leq k$. This shows that the minimal vectors $x$ and $y$ of $(C, n_C)$ are equivalent, in other words, the invertible elements of $C$ all belong to a single equivalence class of minimal vectors, which may also be expressed by saying that $C^\times \subseteq C_{[1_C]}$. Now suppose that $x \in \mathrm{Min}(C, n_C)$ is *not* equivalent to $1_C$. From Exc. 23.36 (c) we deduce $n_C(C^\times, x) = \{0\}$, which implies $n_{C^\dagger}(C^{\dagger\times}, x^\dagger) = n_{C^\dagger}(C^{\times\dagger}, x^\dagger) = \{0\}$. But $C'$ is an octonion algebra over $\mathbb{F}_2$ that is spanned as a vector space by $C^{\dagger\times}$ (Exc. 11.38 (a) and Prop. 17.5). Thus $x^\dagger = 0$, hence $x \in 2C$, and we conclude that the indecomposable submodules $C_{[x]} \subseteq C$, with $x \in \mathrm{Min}(C, n_C)$ not equivalent to $1_C$, all belong to $2C$; in

particular, they have even discriminant. But the discriminant of $(C, n_C)$ is odd by hypothesis, which, thanks to Exc. 23.36 (c), implies that $(C, n_C) = C_{[1_C]}$ is indeed indecomposable.

**23.38** Let $R$ be a quadratic étale $\mathbb{Z}$-algebra. Then $R$ is a free $\mathbb{Z}$-module of rank 2, and since $1_R \in R$ is unimodular, it can be extended to a basis $(1_R, u)$ of $R$. By Lemma 19.15, the trace form of $R$ is surjective. Since $t_R(1_R) = 2$, we conclude that $t_C(u) = 2n + 1$ (for some integer $n$) is odd. In fact, replacing $u$ by $u - n \cdot 1_R$, we may assume $t_R(u) = 1$. Now Prop. 19.8 shows $1 - 4n_C(u) = \pm 1$, which implies $n_C(u) = 0$ or $n_C(u) = \frac{1}{2}$. The latter option obviously being impossible, we conclude that $R$ has zero divisors (Exc. 18.20), hence is split (Cor. 22.19). This solves the first part of the problem.

As to the second, assume $\mathrm{Hur}(\mathbb{H}) \cong \mathrm{Cay}(R, \mu)$ for some quadratic $\mathbb{Z}$-algebra $R$ and some $\mu \in \mathbb{Z}$. Combining the definition of the discriminant (3.12) with (4.2.2) and Remark 18.5, we conclude with $d := \mathrm{disc}(R)$ that $4 = d^2\mu^2$. On the other hand, since the norm of $R \subseteq \mathrm{Hur}(\mathbb{H})$ is positive definite, and $R$ itself by the first part of this exercise is not étale, we have $d \geq 2$ and hence $d = 2$, $\mu = -1$. Extending $1_R$ to a basis $(1_R, u)$ of $R$ over $\mathbb{Z}$, we thus obtain $2 = t_C(u)^2 - 4n_R(u)$ from Prop. 19.8, where the left-hand side is $\equiv 2 \bmod 4$, while the right-hand is $\equiv 0$ or $\equiv 1 \bmod 4$, a contradiction.

**23.39** (a) Since $C$ is not split, it has no zero divisors (Cor. 22.19). Hence neither has $C_{\mathbb{Q}}$, whence $C_{\mathbb{Q}}$ is an octonion division algebra over the rationals, up to isomorphism actually the only one (Cor. 23.23). This shows $C_{\mathbb{Q}} \cong \mathrm{Cay}(\mathbb{Q}; -1, -1, -1)$. In particular, the norm of $C_{\mathbb{Q}}$ is positive definite. Hence so is the norm of $C$. Summing up we have shown that $(C, n_C)$ is a positive definite inner product space of rank 8 over $\mathbb{Z}$. But by 4.6 (c), up to isometry there is only one. Hence, by Cor. 23.3, there exists a unital norm equivalence $f\colon C \to \mathrm{DiCo}(\mathbb{O})$. Transferring the unit element, norm and multiplication of $C$ to $\mathrm{DiCo}(\mathbb{O})$ by means of $f$, we may actually assume $C = \mathrm{DiCo}(\mathbb{O})$ as additive groups with $1_C = 1_{\mathbb{O}}$ and $n_C = n_{\mathrm{DiCo}(\mathbb{O})}$. In particular $|C^\times| = 240$ (Exc. 4.13 (d)).

(b) Put $D := \mathrm{DiCo}(\mathbb{O})$. Then $C^\dagger := C/2C = C \otimes_{\mathbb{Z}} \mathbb{F}_2$ and $D^\dagger = D/2D = D \otimes_{\mathbb{Z}} \mathbb{F}_2$ are both octonion algebras over $\mathbb{F}_2$, hence split (23.14) and, in particular, isomorphic. We therefore find an isomorphism $\psi\colon C^\dagger \xrightarrow{\sim} D^\dagger$ of $\mathbb{F}_2$-algebras. Note by the normalization provided in (a) that $(C^\dagger, n_{C^\dagger}, 1_{C^\dagger}) = (D^\dagger, n_{D^\dagger}, 1_{D^\dagger})$ as "pointed" quadratic spaces over $\mathbb{F}_2$. In particular, $\psi$ is an orthogonal transformation of the quadratic space $(C^\dagger, n_{C^\dagger})$. Applying [13, Prop. 14], we see that the orthogonal group of this space is generated by the orthogonal transvections

$$\tau_a\colon \quad x \longmapsto x - \frac{n_{C^\dagger}(a, x)}{n_{C^\dagger}(a)} a \qquad\qquad (a \in C^{\dagger\times}),$$

each of which can be lifted to an orthogonal transformation from $(C, n_C)$ onto itself since, as we have seen in the solution to Exc. 23.37, the natural map from $C^\times$ to $C^{\dagger\times}$ is surjective. Hence we can also lift $\psi$ to an orthogonal transformation $\varphi$ of $(C, n_C)$. In other words, $\varphi\colon C \to \mathrm{DiCo}(\mathbb{O})$ is a linear bijection preserving norms such that the diagram

$$\begin{array}{ccc} C & \xrightarrow{\varphi} & \mathrm{DiCo}(\mathbb{O}) \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}} \\ C/2C & \xrightarrow[\psi]{} & \mathrm{DiCo}(\mathbb{O})/2\,\mathrm{DiCo}(\mathbb{O}), \end{array}$$

commutes. Writing $x^\dagger := \mathrm{can}(x)$ for $x \in C^\times$ and using the fact that $\psi$ is an algebra isomorphism, we therefore obtain, for all $x, y \in C^\times$,

$$(\varphi(x \cdot y))^\dagger = \psi((x \cdot y)^\dagger) = \psi(x^\dagger \cdot y^\dagger) = \psi(x^\dagger)\psi(y^\dagger) = (\varphi(x))^\dagger(\varphi(y))^\dagger = (\varphi(x)\varphi(y))^\dagger.$$

But for $x \in C^\times$, the fiber of $x^\dagger \in C^{\dagger\times}$ under the vertical arrows in the above diagram consists of the elements $\pm x$. Thus $\varphi(x \cdot y) = \pm\varphi(x)\varphi(y)$.

(c) According to (b), there exists a map $\varepsilon\colon C^\times \times C^\times \to \{\pm 1\}$ such that $\varphi(x \cdot y) = \varepsilon(x, y)\varphi(x)\varphi(y)$ for all $x, y \in C^\times$. We claim that $\varepsilon$ *is constant*. Indeed, let $x, y, z \in C^\times$. Since $\varphi$ preserves norms, and these are the same for $C$ and $\mathrm{DiCo}(\mathbb{O})$, an application of (17.1.3) yields

$$\begin{aligned} \varepsilon(x, y)\varepsilon(x, z)n_C(x)n_C(y, z) &= \varepsilon(x, y)\varepsilon(x, z)n_C(\varphi(x))n_C(\varphi(y), \varphi(z)) \\ &= \varepsilon(x, y)\varepsilon(x, z)n_C(\varphi(x)\varphi(y), \varphi(x)\varphi(z)) \\ &= n_C(\varphi(x \cdot y), \varphi(x \cdot z)) \\ &= n_C(x \cdot y, x \cdot z) = n_C(x)n_C(y, z). \end{aligned}$$

Hence $\varepsilon(x, y) = \varepsilon(x, z)$ provided $n_C(y, z) \neq 0$. On the other hand, if $n_C(y, z) = 0$, then Exc. 11.38 (b) combined with the surjectivity of the natural map $C^\times \to C^{\dagger\times}$ yields a $w \in C^\times$ satisfying $n_C(y, w) \neq 0 \neq n_C(w, z)$, which in turn implies $\varepsilon(x, y) = \varepsilon(x, w) = \varepsilon(x, z)$. Thus $\varepsilon(x, y)$ does not depend on $y \in C^\times$. Interchanging the role of $x$ and $y$, and replacing (17.1.3) by (17.1.2) in the process, the same argument shows that $\varepsilon(x, y)$ is also independent of $x \in C^\times$, showing that the map $\varepsilon$ is indeed constant. Finally, replacing $\varphi$ by $-\varphi$ if necessary, we may assume $\varphi(x \cdot y) = \varphi(x)\varphi(y)$ for all $x, y \in C^\times = \mathrm{DiCo}(\mathbb{O})^\times$. But since $C$ is generated by $C^\times$ as an additive group (Exc. 4.13) (b),(d)), this means that $\varphi\colon C \xrightarrow{\sim} \mathrm{DiCo}(\mathbb{O})$ is an isomorphism of octonion algebras.

**23.40** (a) We begin by proving sufficiency The assertion is clear if (i) or (ii) holds. As to (iii), assuming there exists an $F$-embedding $K \hookrightarrow C$, we obtain an induced $K$-embedding $K_K \hookrightarrow C_K$. If we can show that $K_K$ is not a division

algebra, then neither is $C_K$, forcing $C_K$ to be split by Cor. 22.18. Hence it suffices to show that $K_K = K \otimes K$ contains zero divisors. If $K/F$ is separable, this follows from Exc. 19.36 (a). On the other hand, if $K/F$ is inseparable, then $\mathrm{char}(F) = 2$ and $\xi^2 \in F$ for all $\xi \in K \setminus F$. This implies $0 \neq u := 1_K \otimes \xi + \xi \otimes 1_K \in K \otimes K$ and $u^2 = 1_K \otimes \xi^2 + \xi^2 \otimes 1_K = 2\xi^2 1_{K\otimes K} = 0$. Thus $K_K$ contains non-zero nilpotent elements, and we are done.

In order to prove necessity, let us assume that $K$ is a splitting field of $C$ and (i), (ii) do not hold. If $C$ is split, then it has dimension 4 or 8, and $C_1 := \mathrm{Cay}(K, 1)$ in the first case, $C_2 := \mathrm{Cay}(K; 1, 1)$ in the second, is a split composition algebra over $F$ of the same dimension as $C$. Thus $C \cong C_i$ for some $i = 1, 2$, and since $C_i$ contains an isomorphic copy of $K$, so does $C$. We are left with the case that $C$ is a division algebra, so by Cor. 22.18 its norm is anisotropic. Pick any $\xi \in K \setminus F$. Then $\xi^2 = \alpha\xi - \beta$ with $\alpha := t_K(\xi), \beta := n_K(\xi)$. Since $C_K = C \oplus (C \otimes \xi)$ is split over $K$, we find elements $u, v \in C$ not both zero such that

$$\begin{aligned} 0 = n_C(u - v \otimes \xi) &= n_C(u) - \xi n_C(u, v) + \xi^2 n_C(v) \\ &= (n_C(u) - \beta n_C(v)) + (\alpha n_C(v) - n_C(u, v))\xi, \end{aligned}$$

hence $n_C(u) = \beta n_C(v)$ and $n_C(u, v) = \alpha n_C(v)$. This implies $v \in C^\times$ and with $x := uv^{-1}$ we deduce $\beta = n_C(x)$, $\alpha = n_C(u, n_C(v)^{-1}v) = n_C(u, \bar{v}^{-1}) = t_C(x)$. Summing up, $F[x] \subseteq C$ is a subalgebra isomorphic to $K$, and we have found an embedding $K \hookrightarrow C$.

(b) We claim that the given quadratic form $q$ is isotropic iff there exists $x \in C^0$ such that $n_C(x) = -\alpha$. The "if" direction is obvious. For "only if", suppose $c = \beta 1_C + y$ for $\beta \in k$ and $y \in C^0$ such that $c \neq 0$ but $q(c) = \alpha\beta^2 + n_C(y) = 0$. If $\beta = 0$, then $n_C|_{C^0}$ is isotropic, so it contains a hyperbolic plane and such an $x$ exists. If $\beta \neq 0$, then $n_C(y/\beta) = n_C(y)/\beta^2 = -\alpha$. This verifies the claim.

For $x \in C^0$, we have $n_C(x) = -\alpha$ if and only if $x^2 = \alpha$. By part (a), such an $x$ exists iff there is an $F$-embedding $K \hookrightarrow C$.

**23.41** Write $C \cong F[\mathbf{t}]/(f)$ for some irreducible polynomial $f \in F[\mathbf{t}]$. By hypothesis, $K[\mathbf{t}]/(f) \cong C_K$ is not a field, so $f$ is reducible in $K[\mathbf{t}]$. Because $f$ has degree 2 or 3, one of the factors of $f$ has degree 1, i.e., $f$ has a root $\alpha \in K$. Then $F[\alpha]$ is a subfield of $K$ isomorphic to $C$.

**23.42** $C_{\mathbb{R}} \cong \mathbb{H}$ is division, so $C$ is division. Since

$$1 + 7 \cdot i^2 + 15 \cdot i^2 + 7 \cdot 15 \cdot (1/\sqrt{5})^2 = 0,$$

$(n_C)_K$ is isotropic, so $C_K$ is split.

A subalgebra $E$ of $K$ properly containing $\mathbb{Q}$ is a quadratic field extension

of $\mathbb{Q}$. Now $K$ is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$, so the three possibilities for $E$ are $\mathbb{Q}(\sqrt{d})$ for $d = 5, -1$, or $-5$.

By Exc. 23.40, it suffices to show that $q_d := \langle d, 7, 15, 7\cdot 15\rangle_{\text{quad}}$ is anisotropic over $\mathbb{Q}$. For $d = 5$, we have $(q_5)_{\mathbb{R}} \cong (n_C)_{\mathbb{R}}$, which is anisotropic. For $d = -1$ or $-5$, we verify that $(q_d)_{\mathbb{Q}_p}$ is anisotropic, where $\mathbb{Q}_p$ denotes the $p$-adic numbers with $p = 5$ or 3, respectively.

We have $q_{-1} \cong \langle -1, 7\rangle_{\text{quad}} \perp 5\langle 3, 21\rangle_{\text{quad}}$. We apply Exc. 12.39 or [14, Lemma 19.5], to see that $q_{-1}$ is anisotropic over $\mathbb{Q}_5$ if the residue forms $\langle -1, 7\rangle_{\text{quad}}$ and $\langle 3, 21\rangle_{\text{quad}}$ are anisotropic over $\mathbb{F}_5$. To check this, by Exc. 11.32 it suffices to note that the forms have determinant 3 and 2, respectively, which are not congruent to $-1$ mod squares.

We have $q_{-5} \cong \langle -5, 7\rangle_{\text{quad}} \perp 3\langle 5, 35\rangle_{\text{quad}}$. For $(q_{-5})_{\mathbb{Q}_3}$, the residue forms are $\langle -5, 7\rangle_{\text{quad}} \cong \langle 1, 1\rangle_{\text{quad}}$ and $\langle 2, 2\rangle_{\text{quad}}$ over $\mathbb{F}_3$, which both have determinant a square. Since $-1$ is not a square in $\mathbb{F}_3$, these forms are anisotropic, whence so is $q_{-5}$.

## Solutions for Section 24

**24.29** Let $R$ be a $k$-algebra and suppose $R \cong R_0 \times R_1$ for $k$-algebras $R_i$. Then we obtain an element of $\mathrm{Aut}(D_R)$ that acts as the identity on $D_{R_0}$ and as conjugation on $D_{R_1}$. Exercise 19.33 says that every element of $\mathrm{Aut}(D_R)$ arises in this way and conversely each expression $R \cong R_0 \times R_1$ gives an automorphism of $D_R$. In this way, we may identify $\mathrm{Aut}(D_R)$ as a set with the collection of complete orthogonal system of idempotents $e_0, e_1$ in $R$, i.e., with the set of $k$-algebra homomorphisms $\mathrm{Hom}(k \times k, R)$.

Thus we have defined a bijection $\mathrm{Aut}(D_R)$ between and $(\mathbb{Z}/2)(R)$ as sets, in a way that is functorial in $R$. We check that this bijection is compatible with the group operation. Let $(c_0, c_1)$, $(d_0, d_1)$ be complete orthogonal systems of idempotents in $R$. Then $(c_0d_0, c_0d_1, c_1d_0, c_1d_1)$ is a complete orthogonal system of idempotents, giving rise to a direct product decomposition $R = \prod_{i,j} R_{ij}$ for $R_{ij} := c_id_jR$ as well as $D_R = \prod_{i,j} D_{ij}$ for $D_{ij} := D_{R_{ij}}$. The product of $(c_0, c_1)$, $(d_0, d_1)$ in $\mathrm{Aut}(D_R)$ is an automorphism of $D_R$ that is the identity on $D_{00} \times D_{11}$ and conjugation on $D_{01} \times D_{10}$. That is, the product in $\mathrm{Aut}(D_R)$ corresponds to the complete orthogonal system of idempotents $(c_0d_0 + c_1d_1, c_0d_1 + c_1d_0)$.

We describe the product in $(\mathbb{Z}/2)(R)$, which is a $k$-algebra homomorphism $k \times k \to R$, by evaluating it on an element $(x_0, x_1) \in k \times k$. Put $\Delta$ for the co-multiplication homomorphism defined in 24.20, $\phi_i$ for the map $k \times k \to k$ that is projection on factor $i = 0, 1$, and $1_i$ for the identity element of the $i$-th factor of

$k \times k$. Then the product of $(c_0, c_1)$, $(d_0, d_1)$ computing in $(\mathbb{Z}/2)(R)$ maps $(x_0, x_1)$ to

$$\begin{aligned}((c_0\phi_0 + c_1\phi_1) \otimes (d_0\phi_0 + d_1\phi_1))\,\Delta(x_0, x_1)\\ = (\sum_{i,j} c_i d_j \phi_i \otimes \phi_j)(x_0(1_0 \otimes 1_0 + 1_1 \otimes 1_1) + x_1(1_0 \otimes 1_1 + 1_1 \otimes 1_0))\\ = x_0(c_0d_0 + c_1d_1) + x_1(c_0d_1 + c_1d_0),\end{aligned}$$

confirming that the two products agree.

**24.30** For each $i$ and $\chi \in M_i^*$, there is a polynomial function $f_{i,\chi}$ on $\mathbf{GL}(M)$ defined by

$$f_{i,\chi}(g) = \chi(\rho_i(g)m_i - m_i).$$

Since $M_i$ is finitely generated projective, $f_{i,\chi}(g) = 0$ for all $\chi$ if and only if $\rho_i(g)m_i - m_i = 0$. That is, for $\mathcal{F} := \cup_{i\in I} \cup_{\chi_i \in M_i^*} f_{i,\chi}$, we have

$$\mathbf{H}(R) = \{g \in \mathbf{GL}(M)(R) \mid f(g) = 0 \text{ for all } f \in \mathcal{F}\}.$$

## Solutions for Section 25

**25.30** (a) Let $R'$ be a finitely presented $R$-algebra. Then there are presentations

$$0 \longrightarrow I \longrightarrow k[\mathbf{S}] \xrightarrow[\pi]{} R \longrightarrow 0\,, \tag{s1}$$

$$0 \longrightarrow J \longrightarrow R[\mathbf{T}] \xrightarrow[\rho]{} R' \longrightarrow 0 \tag{s2}$$

of $R$ over $k$, $R'$ over $R$, respectively, with chains $\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_m)$, $\mathbf{T} = (\mathbf{t}_1, \ldots, \mathbf{t}_n)$ of independent variables and finitely generated ideals $I \subseteq k[\mathbf{S}]$, $J \subseteq k[\mathbf{T}]$. Extending (s1) from $k$ to $k[\mathbf{T}]$, we conclude that the sequence

$$0 \longrightarrow I \otimes k[\mathbf{T}] \longrightarrow k[\mathbf{S}, \mathbf{T}] = k[\mathbf{S}] \otimes k[\mathbf{T}] \xrightarrow[\pi_{k[\mathbf{T}]}]{} R \otimes k[\mathbf{T}] = R[\mathbf{T}] \longrightarrow 0 \tag{s3}$$

is exact, whence

$$\varphi := \rho \circ \pi_{k[\mathbf{T}]} \colon k[\mathbf{S}, \mathbf{T}] \longrightarrow R' \tag{s4}$$

is a surjective morphism in $k$-**alg** which by (s2) satisfies

$$\operatorname{Ker}(\varphi) = \pi_{k[\mathbf{T}]}^{-1}(\operatorname{Ker}(\rho)) = \pi_{k[\mathbf{T}]}^{-1}(J). \tag{s5}$$

Now pick $g_1, \dots, g_r \in R[\mathbf{T}]$ such that $J = \sum_{j=1}^{r} R[\mathbf{T}]g_j$ and use (s3) to find a lift $h_j$ of $g_j$ in $k[\mathbf{S}, \mathbf{T}]$ under $\pi_{k[\mathbf{T}]}$: $\pi_{k[\mathbf{T}]}(h_j) = g_j$ for $1 \le j \le r$. By (s3)–(s5), this is easily seen to imply

$$\mathrm{Ker}(\varphi) = I \otimes k[\mathbf{T}] + \sum_{j=1}^{r} k[\mathbf{S}, \mathbf{T}]h_j.$$

But $I \otimes k[\mathbf{T}]$ is a finite $k[\mathbf{T}]$-module, forcing $\mathrm{Ker}(\varphi) \subseteq k[\mathbf{S}, \mathbf{T}]$ to be a finitely generated ideal. Hence $R'$ is finitely presented as a $k$-algebra.

(b) By (a), we may assume $R = k$. Since the $k$-algebra $E := k[\mathbf{t}]/(f\mathbf{t} - 1)$ is clearly finitely presented, it suffices to show that $k_f$ and $E$ are canonically isomorphic. Note first that the natural projection $\pi\colon k[\mathbf{t}] \to E$ makes $f$ invertible: $\pi(f) \in E^\times$ with inverse $\pi(\mathbf{t})$. Hence the unit homomorphism $k \to E$ extends to a homomorphism $\varphi\colon k_f \to E$ such that $\varphi(1/f) = \pi(\mathbf{t})$. On the other hand, the $k$-homomorphism $k[\mathbf{t}] \to k_f$ sending $\mathbf{t}$ to $1/f$ kills $f\mathbf{t} - 1$ and hence induces a $k$-homomorphism $\psi\colon E \to k_f$. One checks that $\varphi$ and $\psi$ are inverse to one another, and the assertion follows.

**25.31** (a) Let $\pi\colon k[\mathbf{T}] \to R$ be a surjective morphism in $k$-**alg**, giving rise to a presentation

$$0 \longrightarrow I \longrightarrow k[\mathbf{T}] \xrightarrow[\varphi\circ\pi]{} R' \longrightarrow 0$$

of $R'$ as a $k$-algebra. By Prop. 25.16, therefore, $I \subseteq k[\mathbf{T}]$ is a finitely generated ideal. But $I = \pi^{-1}(\mathrm{Ker}(\varphi))$, and we conclude that $\mathrm{Ker}(\varphi) = \pi(I) \subseteq R$ is a finitely generated ideal.

(b) Let

$$0 \longrightarrow I \longrightarrow k[\mathbf{T}] \xrightarrow[\pi]{} R \longrightarrow 0 \tag{s1}$$

be a finite presentation of $R$. Setting $J := \mathrm{Ker}(\varphi)$, this induces a presentation

$$0 \longrightarrow \pi^{-1}(J) \longrightarrow k[\mathbf{T}] \xrightarrow[\varphi\circ\pi]{} R' \longrightarrow 0 \tag{s2}$$

of $R'$. Apply (s1) and let $\pi(f_i)$, $f_i \in k[\mathbf{T}]$, $1 \le i \le m$, be finitely many generators of $J$ as an ideal in $R$. Then one checks that

$$\pi^{-1}(J) = I + \sum_{i=1}^{m} k[\mathbf{T}]f_i,$$

so (s2) makes $R'$ a finitely presented $k$-algebra.

**25.32** By 24.21, $k[M_{\mathbf{a}}] \cong S(M^*)$ is the symmetric algebra of $M^*$, the dual of $M$. Since $M^*$ is a finitely generated projective $k$-module as well, it suffices to show: if $M$ is a finitely generated projective $k$-module, then $S(M)$ is a finitely presented $k$-algebra.

Applying Exc. 9.31, we find a complete orthogonal system $(\varepsilon_i)_{i\in\mathbb{N}}$ of idempotents in $k$ such that $M_i = M \otimes k_i$ for each $i \in \mathbb{N}$ is a finitely generated projective module of rank $i$ over $k_i := k\varepsilon_i$. Note that $\varepsilon_i = 0$, hence $k_i = \{0\}$ and $M_i = \{0\}$, for almost all $i \in \mathbb{N}$. Since passing to the symmetric algebra of a module is compatible with base change [8, III.6, Prop. 7], we conclude

$$S(M) = \prod_{i\in\mathbb{N}} S(M_i)$$

as $k$-algebras. We are thus reduced to the case that $M$ is finitely generated projective of rank $r \in \mathbb{N}$ over $k$. But then 25.5 (ii) produces a faithfully flat $k$-algebra $k'$ making $M_{k'}$ a free $k'$-module of rank $r$. Since $S(M)_{k'} = S(M_{k'})$, therefore being a polynomial ring in $r$ variables [8, III.6], hence finitely presented over $k'$, so is $S(M)$ over $k$, by Cor. 25.17.

**25.33** It is straightforward to verify that $\tilde{w}$ is a subfunctor of $M_{\mathbf{a}}$. In order to derive the second part of the exercise, let us assume that $M$ is finitely generated projective. For $u^* \in M^*$, the set maps

$$f_{u^*}(R)\colon M_R \longrightarrow R, \quad x \longmapsto \langle u^*_R, x - w_R\rangle,$$

vary functorially with $R \in k$-**alg** and hence define an element $f_{u^*} \in k[M_{\mathbf{a}}]$. Since $M^*$ is finitely generated projective as well, and the canonical pairing $M^* \times M \to k$ is regular, we conclude that $x \in M_R$ agrees with $w_R$ if and only if $f_{u^*}(R)(x) = 0$ for all $u^* \in M^*$. By Exercises 25.31, 25.32 (b), therefore, $\tilde{w} \subseteq M_{\mathbf{a}}$ is a finitely presented closed affine subscheme.

**25.34** By definition of non-singularity (11.11), we have to prove that the quadratic form $q_K : M_K \to K$ over $K$ is non-degenerate, for any field $K \in k$-**alg**. By Exc. 9.26 there is a field $L \in R$-**alg** containing $K$ such that the maps $k \to K \to L$ and $k \to R \to L$ agree. Since $q_R$ is non-singular, the quadratic form $(q_K)_L \cong q_L \cong (q_R)_L$ over $L$ is non-degenerate. Hence so is $q_K$ over $K$.

**25.35** (a) For $i = 0, 1$, $T \in S$-**alg** and all $k$-modules $P$, we have the natural identifications

$$(P_S)_T = P_T = P_{T_i} = (P_R)_{T_i}$$

via (9.4.1), so $g_{iT}$ is a set map from $(M_S)_T$ to $(N_S)_T$, as claimed. It remains to show that these set maps vary functorially with $T$. In order to see this, we regard the identity map of $T$ as an isomorphism $T \to T_i$, $t \mapsto t_i$, of $k$-algebras. Given a morphism $\varphi\colon T \to T'$ in $S$-**alg**, we therefore obtain a morphism $\varphi_i\colon T_i \to T'_i$ in $R$-**alg** by defining $\varphi_i(t_i) := \varphi(t)_i$ for all $t \in T$. One checks

that $\mathbf{1}_{M_R} \otimes_R \varphi_i = \mathbf{1}_{M_S} \otimes_S \varphi$, and it follows that the diagram

$$\begin{array}{ccc} (M_S)_T & \xrightarrow[g_{iT}]{} & (N_S)_T \\ {\scriptstyle \mathbf{1}_{M_S}\otimes_S\varphi}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_{N_S}\otimes_S\varphi} \\ (M_S)_{T'} & \xrightarrow[g_{iT'}]{} & (N_S)_{T'} \end{array}$$

commutes. Hence $g_i \colon M_S \to N_S$ is a polynomial law over $S$.

(b) If $f \colon M \to N$ is a polynomial law over $k$ such that $f \otimes R = g$, then for all $T \in S$-**alg** we deduce that $g_{iT} = g_{T_i} = (f \otimes R)_{T_i} = f_{T_i} = f_T$ is independent of $i = 0, 1$. Thus $g_0 = g_2$. Conversely, assume $g_0 = g_1 =: h$. We first prove uniqueness of $f$ and let $k' \in k$-**alg**. One checks that the outer squares in (3) commute. Hence so does the inner one since $g_{R_{k'}} = f_{R_{k'}}$ by hypothesis. Moreover, the vertical arrows in (3) are injective by Prop. 25.4, proving uniqueness of the set maps $f_{k'}$, hence of $f$ as a polynomial law over $k$.

In order to prove existence, let $k' \in k$-**alg**. To simplify notation, we indicate the base change from $k$ to $k'$ simply by a dash, for example $M' = M_{k'}$, $R' = R \otimes k'$, $S' = S \otimes k' = R' \otimes_{k'} R'$. Furthermore, the notational conventions fixed in (a) on the level of $R$ and $S$ will now be employed for $R'$ and $S'$. In particular, the very definition of the $R'$-algebras $S'_i$ $(i = 0, 1)$ yield morphisms

$$\sigma_i^{R'} : R' \longrightarrow S'_i, \quad r' \longmapsto \sigma_i^{R'}(r') := d^i_{R'}(r')_i$$

in $R'$-**alg** $\subseteq R$-**alg**. Now we consider the following diagram.

$$\begin{array}{ccccccc} 0 & & & & & & 0 \\ \downarrow & & & & & & \downarrow \\ M' & & \xrightarrow{\exists! f_{k'}} & & & & N' \\ {\scriptstyle \mathrm{can}_{M',R'}}\downarrow & & & & & & \downarrow{\scriptstyle \mathrm{can}_{N',R'}} \\ M'_{R'} & \xrightarrow[\mathbf{1}]{} & (M_R)_{R'} & \xrightarrow[g_{R'}]{} & (N_R)_{R'} & \xrightarrow[\mathbf{1}]{} & N'_{R'} \\ {\scriptstyle \rho_i^{R',M'}}\downarrow & & \downarrow{\scriptstyle \mathbf{1}_{M_R}\otimes_R\sigma_i^{R'}} & & \downarrow{\scriptstyle \mathbf{1}_{N_R}\otimes_R\sigma_i^{R'}} & & \downarrow{\scriptstyle \rho_i^{R',N'}} \\ M'_{S'} & \xrightarrow[\mathbf{1}]{} & (M_R)_{S'_i} & \xrightarrow[h_{S'}=g_{S'_i}]{} & (N_R)_{S'_i} & \xrightarrow[\mathbf{1}]{} & N'_{S'}, \end{array} \tag{s1}$$

whose inner lower square commutes by the definition of polynomial laws, while the outer lower ones do thanks, e.g., to the following computation, for

all $x \in M$, $r \in R$, $\alpha', \beta' \in k'$:

$$\begin{aligned}
\rho_1^{R',M'}((x \otimes \alpha') \otimes_{k'} (r \otimes \beta')) &= (x \otimes \alpha') \otimes_{k'} ((r \otimes \beta') \otimes_{k'} (1_R \otimes 1_{k'})) \\
&= (x \otimes \alpha') \otimes_{k'} ((r \otimes 1_R) \otimes \beta') \\
&= x \otimes ((r \otimes 1_R) \otimes \alpha'\beta') \\
&= x \otimes ((r \otimes 1_R) \otimes \alpha'\beta')_1 \\
&= (x \otimes 1_R) \otimes_R ((r \otimes 1_R) \otimes \alpha'\beta')_1 \\
&= (x \otimes 1_R) \otimes_R ((r \otimes \alpha'\beta') \otimes_{k'} (1_R \otimes 1_{k'}))_1 \\
&= (x \otimes 1_R) \otimes_R \sigma_1^{R'}(r \otimes \alpha'\beta') \\
&= (\mathbf{1}_{M_R} \otimes_R \sigma_1^{R'})((x \otimes 1_R) \otimes_R (r \otimes \alpha'\beta')) \\
&= (\mathbf{1}_{M_R} \otimes_R \sigma_1^{R'})\Big(x \otimes (\alpha'(r \otimes \beta'))\Big) \\
&= (\mathbf{1}_{M_R} \otimes_R \sigma_1^{R'})((x \otimes \alpha') \otimes_{k'} (r \otimes \beta')).
\end{aligned}$$

The universal property (25.6) of the equalizer $\mathrm{can}_{N',R'}$ of $\rho_1^{R',N'}$, $\rho_0^{R',N'}$ (Prop. 25.7), applied to the map $u := g_{R'} \circ \mathrm{can}_{M',R'} \colon M' \to N'_{R'}$, by (s1) implies that there exists a unique set map $f_{k'} \colon M' \to N'$ making (s1) totally commutative. In other words, we have a commutative diagram

$$\begin{array}{ccc}
M' & \xrightarrow[f_{k'}]{} & N' \\
{\scriptstyle \mathrm{can}_{M',R'}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}_{N',R'}} \\
M'_{R'} = (M_R)_{R'} & \xrightarrow[g_{R'}]{} & (N_R)_{R'} = N'_{R'}.
\end{array} \tag{s2}$$

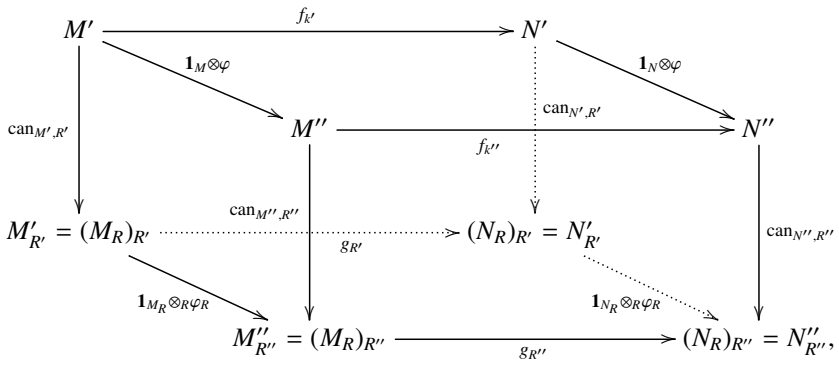
Next we show that $f_{k'}$ depends functorially on $k'$, so let $\varphi \colon k' \to k''$ be a morphism in $k$-**alg**. Indicating the base change from $k$ to $k''$ by a double dash, we see that

$$\varphi_R := \mathbf{1}_R \otimes \varphi \colon R' \longrightarrow R'' \tag{s3}$$

is a morphism in $R$-**alg**, and one checks that the diagram

$$\begin{array}{ccc}
M' & \xrightarrow[\mathbf{1}_M \otimes \varphi]{} & M'' \\
{\scriptstyle \mathrm{can}_{M',R'}}\downarrow & & \downarrow{\scriptstyle \mathrm{can}_{M'',R''}} \\
M'_{R'} = (M_R)_{R'} & \xrightarrow[\mathbf{1}_{M_R} \otimes_R \varphi_R]{} & (M_R)_{R''} = M''_{R''}
\end{array} \tag{s4}$$

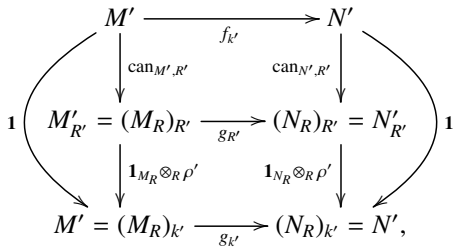
commutes. Now consider the cube




where by (s2)–(s4) all rectangles commute, with the possible exception of the top one. By diagram chasing, therefore, so does the top one after being composed with $\mathrm{can}_{N'',R''}$. But $R''$ is faithfully flat over $k''$, forcing $\mathrm{can}_{N'',R''}$ by Prop. 25.4 to be injective, and we have proved that the top rectangle commutes as well. Summing up, $f\colon M \to N$ is a polynomial law over $k$. Hence the solution of the problem will be complete once we have shown $f \otimes R = g$. In order to see this, let $k' \in R$-**alg** and $\rho\colon R \to k'$ the corresponding unit morphism in $k$-**alg**. With the notational simplifications introduced before, we obtain an induced morphism $\rho'\colon R' \to k'$ given by

$$\rho'(r \otimes \alpha') = \rho(r)\alpha' = r\alpha'$$

for $r \in R$, $\alpha' \in k'$. In particular, $\rho'$ is a morphism in $R$-**alg**, and we obtain a diagram




where the outer triangles are easily seen to be commutative. Hence $f_{k'} = g_{k'}$, as desired.

**25.36** In the special case where $M$ and $N$ are free, this holds by Cor. 12.12.

If $M$ and $N$ have constant rank, then there is a faithfully flat $R \in k$-**alg** such

that $M_R$ and $N_R$ are free $R$-modules. Then we have a commutative diagram

$$\begin{array}{ccc} S^d(M^*) \otimes N \otimes R & \longrightarrow & \mathrm{Pol}^d(M,N) \otimes R \\ \downarrow & & \downarrow \\ S^d(M_R^*) \otimes N_R & \longrightarrow & \mathrm{Pol}^d(M_R, N_R) \end{array}$$

where the left arrow is trivially an isomorphism, the bottom arrow is an isomorphism by the free case, and the right arrow is an isomorphism by 25.5 (iii), so the top arrow is also an isomorphism. Since $\Phi$ becomes an isomorphism after tensoring with the faithfully flat $R$, it is itself an isomorphism.

If $M$ and $N$ do not have constant rank, then there is an $n$ such that $k = \prod_{i=1}^n k_i$, $M = \prod_{i=1}^n M_i$, and $N = \prod_{i=1}^n N_i$ such that each $M_i$ and $N_i$ is a finitely generated projective $k_i$-module of constant rank. Then $S^d(M^*) \otimes N$ is naturally isomorphic to $\prod_{i=1}^n (S^d(M_i^*) \otimes N_i)$ and similarly for $\mathrm{Pol}^d(M,N)$, and the conclusion follows from the previous case.

**25.37** We systematically adhere to the notation and terminology of Exc. 25.35.

(a) Let $e$ be the unit element of $C_R$ and write $g := \tilde{e}\colon C_R \to C_R$ for the constant polynomial law over $R$ determined by $e$, as defined in Exc. 12.32. For $T \in S\text{-}\mathbf{alg}$ and $i = 1, 2$, $e_{T_i} \in (C_R)_{T_i} = (C_S)_T$ is the unit element of $(C_S)_T$, and we conclude $e_{T_1} = e_{T_2}$. Thus $g_1 = g_2$ as polynomial laws $C_S \to C_S$ over $S$. Applying Exc. 25.35, we find a unique polynomial law $f\colon C \to C$ over $k$ such that $f \otimes R = g$. Put $e_0 := f_k(0) \in C$. Since the vertical arrows in (3) are injective, we conclude not only $e_{0R} = e$ but also that $C$ is unital with $1_C = e_0$.

(b) Let $n\colon C_R \to R$ be a quadratic form over $R$ making $C_R$ a conic $R$-algebra. For $T \in S\text{-}\mathbf{alg}$ and $i = 1, 2$, there are two quadratic forms over $T$ making $(C_S)_T = (C_R)_{T_i}$ a conic $T$-algebra, namely, $n_{T_i}$. Hence Prop. 16.16 implies $n_{T_1} = n_{T_2}$. Viewing $n$ as a homogeneous polynomial law $g\colon C_R \to R$ of degree 2 over $R$, we have $g_1 = n_{T_1} = n_{T_2} = g_2$. Thus Exc. 25.35 yields a unique polynomial law $f\colon C \to k$ over $k$ such that $f \otimes R = g$. Hence the set map $n_0 := f_k\colon C \to k$ is a quadratic form over $k$, and from (3) we deduce as before that $C$ is a conic $k$-algebra with norm $n_0$ whose base change to $R$ is $C_R$ as a conic $R$-algebra with norm $n$.

**25.38** (a): If $M$ is a finitely generated free module, say of rank $d$, then the characteristic polynomial as in 12.3 does not depend on the choice of isomorphism $M \xrightarrow{\sim} k^d$, equivalently $\mathrm{End}_k(M) \xrightarrow{\sim} \mathrm{Mat}_d(k)$, and so defines a polynomial law on $\mathrm{End}_k(M)$ in that case determined by $d$. If $M$ is merely assumed to have constant rank $d$, then there is a faithfully flat $R \in k\text{-}\mathbf{alg}$ so that $M \otimes R$ is free of rank $d$, and we apply faithfully flat descent as in Exercises 25.35 and 25.37 to obtain a characteristic polynomial over $k$. Finally, if $M$ does not have constant

rank, we may write $k = \prod_{i=1}^{d} k_i$ where $M_i := M \otimes k_i$ is projective of constant rank for each $i$, and we define the characteristic polynomial of $x \in \mathrm{End}_k(M)$ in $k[\mathbf{t}]$ to be $(f_1, \ldots, f_d)$, where $f_i \in k_i[\mathbf{t}]$ is the characteristic polynomial of $x \otimes k_i$.

(b): For (i), note that $(x, y) \mapsto \det(xy) - (\det x)(\det y)$ is a polynomial law $\mathrm{End}_k(M) \times \mathrm{End}_k(M) \to k$ that is zero if $M$ is free. Note that this implies that $x$ invertible implies $\det x$ invertible in $k$.

For (ii), evaluating the characteristic polynomial of $x$ at $x$ defines a polynomial law $\mathrm{End}_k(M) \to \mathrm{End}_k(M)$ that is zero whenever $M$ is free.

For (iii), we reduce to the case where $M$ has constant rank $d$. The characteristic polynomial of $x$ is $\mathbf{t}^d - \alpha_1 \mathbf{t}^{d-1} + \cdots + (-1)^d \alpha_d$, with $\alpha_d := \det x$. Define $x^\sharp := (-1)^{d+1}(x^{d-1} - \alpha_1 x^{d-2} + \cdots + (-1)^{d-1}\alpha_{d-1})$. (The element $x^\sharp$ is known as the *classical adjoint* of $x$.) Then $xx^\sharp = (-1)^{d+1}(x^d - \alpha_1 x^{d-1} + \cdots (-1)^{d-1}\alpha_{d-1}x)$, which is almost the characteristic polynomial of $x$ evaluated at $x$. Applying (ii), we find:

$$xx^\sharp = (-1)^{d+1}(0 - (-1)^d \alpha_d) = \alpha_d 1_{\mathrm{End}_k(M)}.$$

Therefore, if $\alpha_d$ is invertible, we have $x^{-1} = x^\sharp \alpha_d^{-1}$, proving (iii).

**25.39** First of all, assume $\mathbf{X}_1, \mathbf{X}_2$ are both smooth over $k$. Then $k[\mathbf{X}_1]$ is finitely presented over $k$. But the property of a $k$-algebra in $k$-**alg** to be finitely presented is stable under base change (25.14), forcing $k[\mathbf{X}_1 \times \mathbf{X}_2] \cong k[\mathbf{X}_1] \otimes k[\mathbf{X}_2]$ (24.13) to be finitely presented over $k[\mathbf{X_2}]$. On the other hand, $k[\mathbf{X}_2]$ is finitely presented over $k$ as well, and we deduce from Exc. 25.30 (a) that $k[\mathbf{X}_1 \times \mathbf{X_2}]$ is finitely presented over $k$. Now let $R \in k$-**alg** and suppose $I \subseteq R$ is an ideal that squares to zero. Since the set maps $\mathbf{X}_i(R) \to \mathbf{X}_i(R/I)$ are surjective for $i = 1, 2$ by definition, so is their product

$$(\mathbf{X}_1 \times \mathbf{X}_2)(R) = \mathbf{X}_1(R) \times \mathbf{X}_2(R) \longrightarrow \mathbf{X}_1(R/I) \times \mathbf{X}_2(R/I) = (\mathbf{X}_1 \times \mathbf{X}_2)(R/I). \tag{s1}$$

Thus $\mathbf{X}_1 \times \mathbf{X}_2$ is smooth. Conversely, let this be so and assume that $\mathbf{X}_1$ is finitely presented over $k$ as well as $\mathbf{X}_2(k) \neq \emptyset$. Pick $x_2 \in \mathbf{X}_2(k)$ and write $x_2'$ for its canonical image in $\mathbf{X}_2(R/I)$. Given any $x_1' \in \mathbf{X}_1(R/I)$, the surjectivity of (s1) yields a pre-image $(x_1, x_2) \in (\mathbf{X}_1 \times \mathbf{X}_2)(R)$ of $(x_1', x_2') \in (\mathbf{X}_1 \times \mathbf{X}_2)(R/I)$, forcing $x_1$ to be a pre-image of $x_1'$ in $\mathbf{X}_1(R)$. Thus the natural map $\mathbf{X}_1(R) \to \mathbf{X}_1(R/I)$ is surjective, and $\mathbf{X}_1$ is smooth.

**25.40** $R$ is evidently finitely presented. Since it is free with basis $1_k, \mathbf{t}, \ldots, \mathbf{t}^{d-1}$, it is flat.

In case $k$ is a field, $R$ is étale if and only if the polynomial $\mathbf{t}^d - x$ has $d$ distinct roots in an algebraic closure $\bar{k}$ of $k$. The roots of this polynomial are in any case $d$-th roots of $x$. The derivative of this polynomial is $dx^{d-1}$. If $d$ and $x$

are both nonzero in $k$, then the derivative only has zero as a root, which is not a root of the polynomial, so it is separable. Conversely, if $d$ is divisible by the characteristic $p$ of $k$, then $\mathbf{t}^d - x = (\mathbf{t}^{d/p} - y)^p$ for a $p$-th root $y$ of $x$ in $\bar{k}$. And if $x = 0$ in $k$, then $\mathbf{t}^d - x = \mathbf{t}^d$. In either case, $R$ is not a direct product of finite separable extensions of $k$.

For general $k$, $d$ and $x$ are invertible in $k$ if and only if they are not contained in any maximal ideal $\mathfrak{m}$ of $k$, if and only if they have non-zero image in $k(\mathfrak{m})$. This holds if and only if — by the case for fields from the preceding paragraph — $R \otimes k(\mathfrak{m})$ is an étale $k(\mathfrak{m})$-algebra.

**25.41** (a) By 24.15, $\boldsymbol{\mu}_n$ is a closed subscheme of $\mathbb{A}^1_k$, with co-ordinate algebra $k[\mathbf{t}]/k[\mathbf{t}](\mathbf{t}^n - 1)$. But in actual fact, $\boldsymbol{\mu}_n$ is also a closed subgroup functor, and hence a closed $k$-group subscheme, of $\mathbf{G_m}$, with co-ordinate algebra $k[\mathbf{t}, \mathbf{t}^{-1}]/k[\mathbf{t}, \mathbf{t}^{-1}](\mathbf{t}^n - 1)$. This proves the isomorphism in the second displayed equation (which can also be derived quite easily directly) and completes the proof of part (a).

(b) There are $i, j \in \mathbb{Z}$ such that $il + jm = 1$. For $R \in k$-**alg**, the assignments

$$x \longmapsto (x^{jm}, x^{il}), \quad (\text{resp.}(x, y) \longmapsto xy)$$

define group homomorphisms $\boldsymbol{\mu}_n(R) \to \boldsymbol{\mu}_l(R) \times \boldsymbol{\mu}_m(R)$ (resp. $\boldsymbol{\mu}_l(R) \times \boldsymbol{\mu}_m(R) \to \boldsymbol{\mu}_n(R)$) that are inverse to one another and compatible with base change. Hence they yield an isomorphism $\boldsymbol{\mu}_n \cong \boldsymbol{\mu}_l \times \boldsymbol{\mu}_m$.

(c) (i) and (iii) are equivalent by part (a) and Exc. 25.40. (i) implies (ii) by 25.21(d). (ii) implies (i) as recalled in 25.19(viii).

**25.42** (a): The function

$$e \mapsto 1_E \wedge e \wedge e^2 \wedge \cdots \wedge e^{d-1} \in \wedge^d E \cong k$$

is a polynomial function $E \to k$. It is non-zero for some $e$ if and only if $k[e] = E$ [8, III.7, Thm. 2], proving that the set is Zariski-open. The fact that it is not empty when $k$ is infinite is standard, see for example [9, V.7, Prop. 7].

(b): Write an element $e$ as $(e_1, \ldots, e_d)$ for $e_i \in k$. Then $k[e] = E$ if and only if $1, e, \ldots, e^{d-1}$ are linearly independent, i.e., if and only if the matrix

$$\begin{pmatrix} 1 & e_1 & e_1^2 & \cdots & e_1^{d-1} \\ 1 & e_2 & e_2^2 & \cdots & e_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e_d & e_d^2 & \cdots & e_d^{d-1} \end{pmatrix}$$

is invertible. The determinant of this matrix is the Vandermonde determinant,

$\prod_{i<j}(e_i - e_j)$, and therefore $k[e] = E$ if and only if the $e_i$ are all distinct. Such an $e$ exists if and only if $|k| \geq d$.

**25.43** For elements $a, a' \in A \otimes R$, we write $a$ as a finite sum $a = \sum_i a_i \otimes r_i$ with $a_i \in A$, $r_i \in R$ and similarly for $a'$. Then

$$aa' = \sum_i \sum_j a_i a_j \otimes r_i r_j,$$

because $R \subseteq \mathrm{Cent}(A \otimes R)$. In particular, since there exist $a, a' \in A \otimes R$ with $aa' \neq 0$, there are $a_i, a'_j \in A$ for some $i$, $j$ such that $a_i a'_j \neq 0$ in $A$.

Next suppose that $I$ is an ideal in $A$. The displayed equation in the preceding paragraph shows that $I \otimes R$ is an ideal in $A \otimes R$, and therefore $I \otimes R = \{0\}$ or $A \otimes R$. Faithful flatness of $R$ implies that $I = \{0\}$ or $A$, as claimed.

**25.44** See [26, p. 33, Prop. 2.5].

**25.45** For each $R \in k$-**alg**, define a map $g \mapsto \gamma_g$ from $\mathbf{G}(R)$ to the group of automorphisms of $\mathbf{G}_R$ viewed as a $\mathbf{G}_R$ torsor via $\gamma_g(h) = gh$ for $h \in \mathbf{G}(R)$. (Note that $\gamma_g$ is indeed an automorphism of $\mathbf{G}_R$ because it acts on the left, whereas $\mathbf{G}_R$ acts on itself on the right.) The map is a homomorphism because

$$\gamma_{gg'}(h) = gg'h = \gamma_g \gamma_{g'}(h)$$

for all $g, g' \in \mathbf{G}(R)$. It is injective because $\gamma_g = \gamma_{g'}$ implies that $g = \gamma_g(1_G) = \gamma_{g'}(1_G) = g'$.

To see that it is surjective, let $\eta$ be an automorphism of $\mathbf{G}_R$ as a $\mathbf{G}_R$-torsor. Then for $h \in \mathbf{G}(R)$, we have

$$\eta(h) = \eta(1_G h) = \eta(1_G)h = \gamma_{\eta(1_G)}(h),$$

i.e., $\eta = \gamma_{\eta(1_G)}$.

**25.46** (i): Certainly, permuting the coordinates of elements of $E_\Gamma$ according to a permutation of $\Gamma$ does provide a $k$-algebra automorphism of $\Gamma$, so the group of permutations is a subgroup of $\mathrm{Aut}_{k\text{-}\mathbf{alg}}(E_\Gamma)$.

Conversely, since $k$ is connected, every idempotent in $E_\Gamma$ has a 0 or 1 in each coordinate. It follows that the collection of elements $\{1_\gamma \mid \gamma \in \Gamma\}$ from Example 24.20 is the unique maximal complete system of orthogonal idempotents. That is, every $k$-algebra automorphism of $E_\Gamma$ permutes this set. Given a $k$-algebra automorphism $f$ of $E_\Gamma$, we may modify it by a permutation of $\Gamma$ as in the preceding paragraph and so assume that $f$ fixes each $1_\gamma$. As $f$ is $k$-linear, it follows that $f$ is the identity on each copy of $k$ in the product for $E_\Gamma$, verifying the claim.

(ii): We abbreviate $E_\Gamma$ to $E$. Note that $\mathbf{Aut}(E)$ is a $k$-group scheme by Example 24.25. Put $\mathbf{G}$ for the constant group scheme corresponding to the permutation group on the set $\Gamma$. There is a morphism $\mathbf{G} \to \mathbf{Aut}(E)$ such that $\mathbf{G}(R) \to \mathbf{Aut}(E)(R)$ is injective for every $R \in k$-**alg**, constructed in the same way as the injection in the case $|\Gamma| = 2$ in Exc. 24.29. Our aim is to show that this injection is an isomorphism of group schemes, which we do following Exc. 19.33.

Identify $\Gamma$ with $\{1, \dots, n\}$ and write $e_i$ for the $i$-th standard basis vector of $k^n$. An element $A \in \mathrm{Aut}(E) = \mathbf{Aut}(E)(k)$ is an element of $\mathrm{GL}_n(k)$ that preserves the coordinate-wise multiplication on $k^n$, which we denote by $*$. For each $i$, we have $(Ae_i) * (Ae_i) = A(e_i * e_i) = Ae_i$, i.e., every entry of $A$ is an idempotent in $k$. For $i \neq j$, we have $0 = e_i * e_j = (Ae_i) * (Ae_j)$, so $A_{ri}A_{rj} = 0$ for all $r$. That is, for each row of $A$, the entries form a complete orthogonal system of idempotents in $k$.

Given any two complete orthogonal systems of idempotents, the collection of products (one from each set) forms a new complete orthogonal system of idempotents. Therefore, the collection of elements $\{A_{1i_1}A_{2i_2}\cdots A_{ni_n} \mid i_1, \dots, i_n \in \{1, \dots n\}\}$ is a complete orthogonal system of idempotents. Let $f_1, \dots, f_N$ be the nonzero elements. Then $k \cong \prod_{i=1}^N kf_i$ and we can view $A$ as an $N$-tuple of matrices with entries in $kf_1, \dots, kf_N$.

Focus on one of these $N$ matrices. Its entries are 0 or 1. Since each row is a complete orthogonal system of idempotents, it has at most one 1. Since $A$ is invertible, each row has at least one 1. In summary, each row has exactly one 1 and since $A$ is invertible it must be a monomial matrix.

In this way, we have recovered the $n$ arbitrary version of the $n = 2$ result contained in Exc. 19.33(b), which shows that surjectivity of $\mathbf{G}(R) \to \mathbf{Aut}(E)(R)$ as desired.

**25.47** (i): Since $E$ is finitely presented and flat over $k$, so is $E_R$ over $R$. For each $\mathfrak{q} \in \mathrm{Spec}(R)$, put $\mathfrak{p} := \mathfrak{q} \cap k$, so $R(\mathfrak{q})$ is a field containing $k(\mathfrak{p})$. Now

$$E_R \otimes_R R(\mathfrak{q}) \cong E \otimes_k R(\mathfrak{q}) \cong (E \otimes k(\mathfrak{p})) \otimes_{k(\mathfrak{p})} R(\mathfrak{q}),$$

where $E \otimes k(\mathfrak{p})$ is an étale algebra over the field $k(\mathfrak{p})$. The property of being an étale algebra over a field is stable under enlarging the field [9, V.6, Cor. 2], i.e., the tensor product on the right is an étale $R(\mathfrak{q})$-algebra, completing the proof of the claim.

(ii): The "only if" direction is trivial by taking $R = k$, so we prove "if". Suppose $R \in k$-**alg** is faithfully flat and $E_R$ is étale. Because $E_R$ is finitely presented and projective over $R$, the same is true for $E$ over $k$ by Cor. 25.17 and 25.5.

For each $\mathfrak{p} \in \operatorname{Spec}(k)$, Exc. 9.26 provides a field $L \in R\text{-}\mathbf{alg}$ containing $k(\mathfrak{p})$. By hypothesis, $(E_{k(\mathfrak{p})})_L = E_L$ is a finite direct product of separable field extensions of $L$, so it is a separable algebra. It follows by [9, V.15, Prop. 3d] that $E_{k(\mathfrak{p})}$ is a separable $k(\mathfrak{p})$-algebra of finite rank, and so is a finite product of finite separable extensions of $k(\mathfrak{p})$ by ibid., V.6, Thm. 4, proving that $E$ is étale.

## Solutions for Section 26

**26.12** By Exc. 25.32, the $k$-functor $M^{2n}_{\mathbf{a}} = (M^{2n})_{\mathbf{a}}$ of Example 24.21 is a finitely presented $k$-scheme. Hence so is $\mathbf{X} := \mathbf{Hyp}(Q)$, defined as a closed subfunctor of $M^{2n}_{\mathbf{a}}$ by finitely many equations (cf. (1) and Exc. 25.31 (b)). After an appropriate base change, it therefore remains to show that the natural set map $\mathbf{X}(k) \to \mathbf{X}(\bar{k})$ is surjective, where $\bar{k} := k/I$ and $I \subseteq k$ is an ideal satisfying $I^2 = \{0\}$. Note that 9.3 and Cor. 11.5 imply $\bar{M} := M_{\bar{k}} = M/IM$, and the quadratic form $\bar{q} := q_{\bar{k}} \colon \bar{M} \to \bar{k}$ over $\bar{k}$ is given by $\bar{q}(\bar{x}) = \overline{q(x)}$ for all $x \in M$, where $\alpha \mapsto \bar{\alpha}$ (resp. $x \mapsto \bar{x}$) stand for the natural maps $k \to \bar{k}$ (resp. $M \to \bar{M}$). We first note that a hyperbolic basis is indeed a basis of the underlying module and must show that any hyperbolic basis of $\bar{Q} := (\bar{M}, \bar{q})$ can be lifted to one of $Q$, so let $(w'_i)_{1\le i\le 2n}$ be a hyperbolic basis of $\bar{Q}$. We argue by induction on $n$. While the case $n = 0$ is trivial, the case $n = 1$ amounts to showing that a hyperbolic pair $(u', v')$ of $\bar{Q}$ in the sense of 11.17 can be lifted to a hyperbolic pair of $Q$. To this end, we pick any elements $a, b \in M$ such that $\bar{a} = u'$, $\bar{b} = v'$. Then $q(a), q(b) \in I$, $q(a, b) \in 1 + I \subseteq k^\times$, and since $I$ squares to zero, one checks that

$$u := a - q(a,b)^{-1}q(a)b, \qquad v := -q(a,b)^{-2}q(b)a + q(a,b)^{-1}b$$

form a hyperbolic pair of $Q$ lifting $(u', v')$. Now assume $n > 1$. By what we have just seen, the hyperbolic pair $(w'_n, w'_{2n})$ of $\bar{Q}$ can be lifted to a hyperbolic pair $(w_n, w_{2n})$ of $Q$. Put $V := kw_n \oplus kw_{2n}$ and $M_0 := V^\perp$ (relative to $Dq$). Then Lemma 11.10 implies $M = M_0 \perp V$, and $Q_0 := (M_0, q|_{M_0})$ is a quadratic space of rank $2(n-1)$ over $k$. Moreover, $\bar{Q}_0 = (\bar{M}_0, \bar{q}|_{\bar{M}_0})$ contains $(w'_i)_{1\le i\le 2(n-1)}$ as a hyperbolic basis, which, by the induction hypothesis, can be lifted to a hyperbolic basis $(w_i)_{1\le i\le 2(n-1)}$ of $Q_0$. Hence $(w_i)_{1\le i\le 2n}$ is the desired lift of $(w'_i)_{1\le i\le 2n}$.

(b) We proceed in several steps.

1°. For the time being, we dispense ourselves from the quadratic space $Q$ of (a) and consider instead arbitrary quadratic modules $Q = (M, q)$, $Q' = (M', q')$ over $k$. By an *isometry* from $Q$ to $Q'$ we mean a $k$-linear bijection $\eta \colon M \to M'$

satisfying $q' \circ \eta = q$. We define the set

$$\mathrm{Isom}(Q, Q') := \{\eta \mid \eta\colon Q \to Q' \text{ is an isometry}\},$$

which in general will be empty but gives rise to a $k$-functor

$$\mathbf{Isom}_k(Q, Q') := \mathbf{Isom}(Q, Q')\colon k\text{-}\mathbf{alg} \to \mathbf{set}$$

by defining

$$\mathbf{Isom}(Q, Q')(R) := \mathrm{Isom}_R(Q_R, Q'_R) \tag{s1}$$

for all $R \in k$-**alg** and by

$$\begin{aligned}\mathbf{Isom}(Q, Q')(\varphi)\colon \mathbf{Isom}(Q, Q')(R) &\longrightarrow \mathbf{Isom}(Q, Q')(S), \\ \mathrm{Isom}_R(Q_R, Q'_R) \ni \eta &\longmapsto \eta_S \in \mathrm{Isom}_S(Q_S, Q'_S)\end{aligned} \tag{s2}$$

for all morphisms $\varphi\colon R \to S$ in $k$-**alg**. The $k$-group functor $\mathbf{O}(Q)$ of Example 24.26 acts canonically in a simply transitive manner on $\mathbf{Isom}(Q, Q')$ from the right via

$$\mathrm{Isom}_R(Q_R, Q'_R) \times \mathrm{O}(Q_R) \longrightarrow \mathrm{Isom}_R(Q_R, Q'_R), \quad (\eta, \zeta) \longmapsto \eta \circ \zeta$$

for all $R \in k$-**alg**.

2°. After this digression, we return to our quadratic space $Q = (M, q)$ of rank $2n$ over $k$ as considered in (a).We denote by $\mathbf{h}_k^{2n}$ the split hyperbolic quadratic space of rank $2n$ over $k$ defined on $k^{2n} = \binom{k^n}{k^n}$ by the quadratic form

$$\langle S \rangle_{\mathrm{quad}}, \quad S := \begin{pmatrix} 0 & \mathbf{1}_n \\ 0 & 0 \end{pmatrix} \tag{s3}$$

in the sense of (11.7.2). The canonical basis of $k^{2n}$ is a hyperbolic basis for $\mathbf{h}_k^{2n}$ and obviously compatible with base change. It follows immediately from the definitions that the assignment

$$\eta \longmapsto (\eta(e_i))_{1 \le i \le 2n} \tag{s4}$$

defines a bijection

$$\Phi = \Phi(k)\colon \mathrm{Isom}(\mathbf{h}_k^{2n}, Q) \xrightarrow{\sim} \mathrm{Hyp}(Q). \tag{s5}$$

3°. Putting $\mathbf{X} := \mathbf{Isom}(\mathbf{h}_k^{2n}, Q)$, the set maps

$$\Phi(R)\colon \mathbf{X}(R) \longrightarrow \mathbf{Hyp}(Q)(R)$$

given by (s4), (s5) for all $R \in k$-**alg** are bijective and obviously compatible with base change, hence give rise to an isomorphism

$$\Phi\colon \mathbf{X} \xrightarrow{\sim} \mathbf{Hyp}(Q)$$

of $k$-functors. By (a), therefore, $\mathbf{X}$ is a smooth affine $k$-scheme. Moreover, $\mathbf{X}$ is faithful in the sense of 25.12 since regular even-dimensional quadratic forms over an algebraically closed field are (split) hyperbolic [14, Exc. 7.34]. Summing up, 25.25 (ii) implies that there exists a faithfully flat étale $k$-algebra $R$ satisfying $\mathbf{X}(R) \neq \emptyset$. But this means that $Q_R$ is split hyperbolic. Furthermore, $\mathbf{X}$ is a torsor with structure group $\mathbf{O}(\mathbf{h}_k^{2n})$ in the étale topology, forcing

$$\mathbf{O}(Q)_R \cong \mathbf{O}(Q_R) \cong \mathbf{O}(\mathbf{h}_k^{2n}) \cong \mathbf{X}_R$$

to be smooth over $R$. By 25.25 (iii), therefore $\mathbf{O}(Q)$ is smooth over $k$.

# Solutions for Chapter V

## Solutions for Section 27

**27.13** (a): $A^+$ is associative if and only if the following is zero for all $x, y, z \in A$:

$$\begin{aligned} 4(x \bullet (y \bullet z) - (x \bullet y) \bullet z) &= xzy + yzx - yxz - zxy = [x,z]y - y[x,z] \\ &= [[x,z],y]. \end{aligned}$$

Since $A$ is associative, $[x,z]$ is central if and only if $[[x,z],y] = 0$ for all $y \in A$, proving the claim.

(b): Consider first the case $n = 2$ and take

$$x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \quad \text{and} \quad y = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right).$$

Then

$$[x,y] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$$

and $[[x,y],x] = 2x \neq 0$, so $[x,y]$ is not central. In view of part (a), we conclude that $\mathrm{Mat}_2(k)^+$ is not associative.

For $n > 2$, we can perform the same argument, where the role of $x$ is played by a matrix with the 2-by-2 $x$ in the upper left corner and zeros elsewhere, and similarly for $y$. The same calculations show that $[x,y]$ is not central and therefore that $\mathrm{Mat}_n(k)^+$ is not associative.

## Solutions for Section 28

**28.20** (a) By induction on $m$. For $m = 0, 1$ there is nothing to prove. Now let $m > 1$ and suppose the assertion has been established for all natural numbers $< m$. By the induction hypothesis we have $x^m = U_x x^{m-2} \in \mathrm{Mon}_m(\{x\})$.

Conversely, let $x \in \mathrm{Mon}_m(\{x\})$. Then $x = U_y z$, $y \in \mathrm{Mon}_n(\{x\})$, $z \in \mathrm{Mon}_p(\{x\})$, $n, p \in \mathbb{N}$, $n > 0$, $2n + p = m$. By the induction hypothesis, $y = x^n$, $z = x^p$, and power associativity yields $x = U_{x^n} x^p = x^{2n+p} = x^m$, as claimed.

(b) For any subset $X \subseteq J$ and any homomorphism $\varphi\colon J \to J'$ of para-quadratic $k$-algebras, one makes the following observations by straightforward induction:

(i) $\varphi(\mathrm{Mon}_m(X)) = \mathrm{Mon}_m(\varphi(X))$ for all $m \in \mathbb{N}$.
(ii) $\mathrm{Mon}_m(Y) \subseteq \mathrm{Mon}_{mn}(X)$ for all $Y \subseteq \mathrm{Mon}_n(X)$ and all $m, n \in \mathbb{N}$.

If $x \in J$ is nilpotent, then (i) implies that $\varphi(x) \in J'$ is nilpotent. Hence if $I$ is a nil ideal in $J$, then $I'$ and $I/I'$ are nil ideals in $J$ and $J/I'$, respectively. Conversely, let this be so. Writing $\pi\colon J \to J/I'$ for the canonical epimorphism, any $x \in I$ makes $\pi(x) \in I/I'$ nilpotent, so by (i), $\mathrm{Mon}_n(\{x\})$ meets $I'$ for some $n \in \mathbb{N}$. But since $I'$ is nil, we conclude that some $y \in \mathrm{Mon}_n(\{x\})$ is nilpotent, leading to a positive integer $m$ such that $0 \in \mathrm{Mon}_{mn}(\{x\})$ by (ii). Thus $x$ is nilpotent, forcing $I$ to be a nil ideal. Now write $\mathfrak{n} := \mathrm{Nil}(J)$ for the sum of all nil ideals in $J$. Given $x \in \mathfrak{n}$, there are finitely many nil ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_r \subseteq J$ such that $x \in \mathfrak{n}_1 + \cdots + \mathfrak{n}_r$. Thus we only have to show that the sum of finitely many nil ideals in $J$ is nil. Arguing by induction, we are actually reduced to the case $r = 2$. But then the isomorphism $(\mathfrak{n}_1 + \mathfrak{n}_2)/\mathfrak{n}_1 \cong \mathfrak{n}_2/(\mathfrak{n}_1 \cap \mathfrak{n}_2)$ combines with what we have proved earlier to yield the assertion.

(c) It suffices to prove that $\mathrm{Nil}(k)J \subseteq J$ is a nil ideal. The ideal property being obvious, we are reduced to showing that $\mathrm{Nil}(k)J$ consists entirely of nilpotent elements. An arbitrary element $x \in \mathrm{Nil}(k)J$ actually belongs to $IJ$, where $I \subseteq \mathrm{Nil}(k)$ is some finitely generated ideal in $k$. A straightforward induction now shows $x^n \in I^n J$ for all $n \in \mathbb{N}$, and the assertion follows from the lemma in solution to Exc. 7.13.

**28.21** (a) For the first assertion, since $\varepsilon(1) = 1_J$, we need only show $(f^2 g)(x) = U_{f(x)} g(x)$ for all $f, g \in k[\mathbf{t}]$. By linearity, we may assume $g = \mathbf{t}^n$ for some $n \in \mathbb{N}$ and, writing $f = \sum \alpha_i \mathbf{t}^i$ with coefficients $\alpha_i \in k$, we obtain

$$f^2 g = (\sum \alpha_i^2 \mathbf{t}^{2i} + 2 \sum_{i<j} \alpha_i \alpha_j \mathbf{t}^{i+j}) \mathbf{t}^n = \sum \alpha_i^2 \mathbf{t}^{2i+n} + 2 \sum_{i<j} \alpha_i \alpha_j \mathbf{t}^{i+j+n},$$

hence, as $J$ is power-associative,

$$\begin{aligned}(f^2 g)(x) &= \sum \alpha_i^2 x^{2i+n} + \sum_{i<j} \alpha_i \alpha_j 2 x^{i+j+n} = \sum \alpha_i^2 U_{x^i} x^n + \sum_{i<j} \alpha_i \alpha_j \{x^i x^n x^j\} \\ &= (\sum \alpha_i^2 U_{x^i} + \sum_{i<j} \alpha_i \alpha_j U_{x^i, x^j}) x^n = U_{\sum \alpha_i x^i} x^n = U_{f(x)} g(x).\end{aligned}$$

Thus $\varepsilon_x$ is a homomorphism of para-quadratic algebras, and we conclude that

$I \subseteq k[\mathbf{t}]^{(+)}$ is an ideal. Our next aim will be to show that $I^0$ is an ideal in $k[\mathbf{t}]$. By linearity, it suffices to show for $f \in I^0$ that $\mathbf{t}^n f$ belongs to $I^0$ for all $n \in \mathbb{N}$. We do so by induction on $n$. For $n = 0$ there is nothing to prove. Now assume $n > 0$ and that the assertion holds for $n - 1$. Since $\varepsilon_x$ is a homomorphism of para-quadratic algebras, the induction hypothesis yields not only $(\mathbf{t}^n f)(x) = 0$, but also $(\mathbf{t}^{n+1} f)(x) = (\mathbf{t}^2 \mathbf{t}^{n-1} f)(x) = U_x(\mathbf{t}^{n-1} f)(x) = 0$, and we have shown $\mathbf{t}^n f \in I^0$. Next let $I^{0\prime}$ be any ideal of $k[\mathbf{t}]$ contained in $I$. Given $f \in I^{0\prime} \subseteq I$, we also have $\mathbf{t}f \in I^{0\prime} \subseteq I$, hence $f(x) = (\mathbf{t}f)(x) = 0$, which show $I^{0\prime} \subseteq I^0$, so $I^0$ is indeed the largest ideal of $k[\mathbf{t}]$ contained in $I$. Finally, let $f \in I$. Then $f^2(x) = U_{f(x)} 1_J = 0$ and $(\mathbf{t}f^2)(x) = U_{f(x)} x = 0$, hence $f^2 \in I^0$. Similarly, not only $2f \in I$ but also $(2\mathbf{t}f)(x) = (\mathbf{t} \circ f)(x) = x \circ f(x) = 0$, hence $2f \in I^0$. The assertions about $R$ and $\pi$ making a commutative diagram as shown in the exercise are now obvious, as is the statement that $k[x] \subseteq J$ is a para-quadratic subalgebra. The assertion about $\mathrm{Ker}(\pi) = I/I^{(0)}$ follows immediately from the fact that $f^2$ and $2f$ belong to $I^{(0)}$ for all $f \in I$. This completes the solution to (a).

(b) Write $f = \alpha_n \mathbf{t}^n + h \in I_n$ with $\alpha_n \in k$ and $h \in \mathbf{t}^{n+2} k[\mathbf{t}]$. Since $2 = 0$ in $k$ and $n \geq 2$, we have $f^2 = \alpha_n^2 \mathbf{t}^{2n} + h^2 \in \mathbf{t}^{n+2} k[\mathbf{t}]$, which is an ideal in $k[\mathbf{t}]$. Thus $U_f g = f^2 g \in \mathbf{t}^{n+2} k[\mathbf{t}] \subseteq I_n$ for all $g \in k[\mathbf{t}]$. Conversely, let $g = \sum \beta_i \mathbf{t}^i \in k[\mathbf{t}]$ with coefficients $\beta_j \in k$ for $j \in \mathbb{N}$. Then $U_g f = g^2 f \equiv \alpha_n \beta_0^2 \mathbf{t}^n \bmod \mathbf{t}^{n+2} k[\mathbf{t}]$ and hence $U_g f \in I_n$. Since $\{g_1 g_2 f\} = 2 f g_1 g_2 = 0 \in I_n$, it follows that $I_n$ is an ideal in $k[\mathbf{t}]^{(+)}$. But it is not an ideal in $k[\mathbf{t}]$ since $\mathbf{t}^n$ belongs to $I_n$ but $\mathbf{t}\mathbf{t}^n = \mathbf{t}^{n+1}$ does not. And finally, if $J_n \cong A^{(+)}$ for some unital flexible $k$-algebra $A$, then $x^n = 0$ would imply the contradiction $x^{n+1} = 0$ since powers in $A$ and $A^{(+)}$ coincide.

**28.22** (a) In the para-quadratic $k$-algebra $k[\mathbf{t}]^{(+)}$ we have $U_{fg} h = (fg)^2 h = f^2 g^2 h = U_f U_g h$ for all $f, g, h \in k[\mathbf{t}]$, hence

$$U_{fg} = U_f U_g \qquad (f, g \in k[\mathbf{t}]). \tag{s1}$$

Since $J$ is power-associative, the evaluation at $x$ (Exc. 28.21) is a homomorphism $k[\mathbf{t}]^{(+)} \to J$ of para-quadratic algebras with image $k[x]$. Applying this homomorphism to (s1) therefore gives (1) of the exercise, hence not only the first equation of (2) of the exercise but also

$$U'_{U'_{f(x)} g(x)} = U'_{(f^2 g)(x)} = U'_{f^2(x)} U'_{g(x)} = U'^2_{f(x)} U'_{g(x)},$$
$$U'_{x^n} = U'_{\mathbf{t}^n(x)} = U'^n_{\mathbf{t}(x)} = U'^n_x,$$

and the proof of (a) is complete.

(b) The polynomial

$$f := \alpha_d \mathbf{t}^d + \cdots + \alpha_{n-1} \mathbf{t}^{n-1} + \mathbf{t}^n \in k[\mathbf{t}]$$

kills $x$ and hence belongs to $I := \mathrm{Ker}(\varepsilon_x)$. From Exc. 28.21 (a) we therefore conclude that

$$f^2 = \alpha_d^2 \mathbf{t}^{2d} + \cdots + \mathbf{t}^{2n} \in k[\mathbf{t}]$$

belongs to $I^0$, so by Exc. 28.21 (a) we have $(\mathbf{t}^i f^2)(x) = 0$, i.e.,

$$\alpha_d^2 x^{2d+i} + \cdots + x^{2n+i} = 0 \qquad (i \in \mathbb{N}). \tag{s2}$$

Now, setting $k_r[x] := \sum_{s \geq r} k x^s$ for $r \in \mathbb{N}$, we find in $(k_r[x])_{r \in \mathbb{N}}$ a descending chain of submodules of $k[x]$. Invoking (s2), we therefore conclude that $k_{2d}[x] = k_{2d+1}[x] = k_{2(d+1)}[x]$ is a finitely generated $k$-module. Thus the linear map $U'_x \colon k_{2d}[x] \to k_{2d}[x]$, being surjective, is in fact bijective (7.11). This property carries over to $(U'_x)^d = U'_{x^d} \colon k_{2d}[x] \to k_{2d}[x]$, whence there exists a unique element $v \in k_{2d}[x]$ such that $U'_{x^d} v = x^{2d}$. Here (a) implies $U'_{x^{2d}} U'_v = U'_{x^{2d}}$, and we conclude that $U_v$ is the identity on $k_{2d}[x]$. With $c := v^2$, this means $U_c = (U_v)^2 = \mathbf{1}$ on $k_{2d}[x]$ and $c^2 = v^4 = U_v v^2 = c$, $c^3 = U_c c = c$, so $c \in k_{2d}[x]$ is an idempotent of the desired kind.

(c) Let $x \in J$ be a pre-image of $c'$ under $\varphi$. Then $x^2 - x$ is nilpotent, so some integer $d > 0$ has $0 = (x^2 - x)^d = x^{2d} - \cdots + (-1)^d x^d$. Pick $v \in k_{2d}[x]$ as in (b) and put $c := v^2$. Writing $\bar{u} := \varphi(u)$ for $u \in J$, we conclude $U_{c'} \bar{v} = U_{\bar{x}} \bar{v} = U_{\bar{x}^d} \bar{v} = \bar{x}^{2d} = c'$. On the other hand, $v = \sum_{i \geq 2d} \alpha_i x^i$ for some scalars $\alpha_i \in k$, $i \geq 2d$, so with $\alpha := \sum_{i \geq 2d} \alpha_i$ we obtain $\bar{v} = \bar{\alpha} c'$, hence $c' = U_{c'} \bar{v} = \bar{\alpha} U_{c'} c' = \bar{\alpha} c' = \bar{v}$. But this implies $\bar{c} = \bar{v}^2 = c'^2 = c'$, and the problem is solved.

**28.23** (i) $\Rightarrow$ (ii). We may assume $J \neq \{0\}$. Since $x$ is nilpotent and $J$ is power-associative at $x$, some positive integer $m$ has $0 \in \mathrm{Mon}_m(\{x\}) = \{x^m\}$ (by Exc. 28.20 (a)). Hence $x^m = 0$.

(ii) $\Rightarrow$ (iii). Let $n \in \mathbb{Z}$, $n \geq 2m$. Then $x^n = U_{x^m} x^{n-2m} = 0$.

(iii) $\Rightarrow$ (i). $0 = x^m \in \mathrm{Mon}_m(\{x\}) \subseteq \mathrm{Mon}(\{x\})$. Hence $x$ is nilpotent.

It remains to show that

$$I := \{x \in k[x] \mid x \text{ is nilpotent}\}$$

is an ideal in $k[x]$. To this end, let $v, w \in k[x]$. We claim

$$(U_v w)^n = U_{v^n} w^n \tag{s1}$$

for all $n \in \mathbb{N}$. This is clear for $n = 0, 1$. Assuming $n \geq 2$ and arguing inductively, we use notation and results of Exc. 28.22 to obtain

$$(U_v w)^n = (U'_v w)^n = U'_{U'_v w} (U_v w)^{n-2} = U'^2_v U'_w U'^{n-2}_v w^{n-2} = U'_{v^n} w^n = U_{v^n} w^n,$$

and the proof of (s1) is complete. From (s1) we conclude that $U_v w$ belongs to $I$ provided $v$ or $w$ do. Next we show that that $I$ is additively closed, so let $v, w \in I$

be written as $v = f(x)$, $w = g(x)$ for some $f, g \in k[\mathbf{t}]$. Applying (ii) above, we find a positive $n$ such that $v^n = w^n = 0$. Then

$$(v+w)^{4n} = (f+g)^{4n}(x) = \Big(\sum_{i=0}^{4n} \binom{4n}{i} f^i g^{4n-i}\Big)(x).$$

For $0 \le i \le 2n$, we obtain

$$(f^i g^{4n-i})(x) = (g^{2n} f^i g^{2n-i})(x) = U_{g^n(x)}((f^i g^{2n-i})(x)) = U_{w^n}((f^i g^{2n-i})(x)) = 0$$

and similarly, for $2n < i \le 4n$,

$$(f^i g^{4n-i})(x) = (f^{2n} f^{i-2n} g^{4n-i})(x) = U_{f^n(x)}((f^{i-2n} g^{4n-i})(x)) = U_{v^n}((f^{i-2n} g^{4n-i}(x)) = 0.$$

Summing up, $v + w \in I$, as desired. Finally we have to show $\{vwz\} \in I$ for $v, w \in k[x]$ and $z \in I$. With $v = f(x)$, $w = g(x)$ as before and $z = h(x)$, $h \in k[\mathbf{t}]$, we obtain $\{vwz\} = 2(fgh)(x)$, hence

$$\{vwz\}^n = (2fgh)^n(x) = 2^n(f^n g^n h^n)(x) = 2^{n-1}\{v^n w^n z^n\}$$

for all integers $n > 0$, from which the assertion follows.

**28.24** We closely follow the arguments used in the proofs of 9.20–9.23.

(a) Since $J$ is outer simple, $\mathrm{Mult}(J)$ acts irreducibly on $J$. Thus the assertion follows from Schur's lemma [23, p. 118].

(b) Since $\mathrm{Mult}(J)$ acts faithfully and irreducibly on $J$, it is a primitive Artinian $k$-algebra [23, Def. 4.1]. Moreover, by definition, its centralizer in $\mathrm{End}_k(J)$ is $\mathrm{Cent}_0(J)$. Thus the assertion follows from the double centralizer theorem [23, Thm. 4.10].

(c) If $J$ is outer central and outer simple, the assertion follows from (b). Conversely, suppose $J \neq \{0\}$ and $\mathrm{Mult}(J) = \mathrm{End}_k(J)$. Then $J$ is outer simple, and (b) implies that $\mathrm{Cent}_0(J)$ belongs to the centre of $\mathrm{End}_k(J)$. Hence $J$ is outer central.

(d) (i) $\Rightarrow$ (ii). Let $k'$ be an extension field of $k$ and put $J' = J \otimes k'$ as a paraquadratic $k'$-algebra. After identifying $\mathrm{End}_{k'}(J') = \mathrm{End}_k(J) \otimes k'$ canonically, a moment's reflection shows $\mathrm{Mult}(J') = \mathrm{Mult}(J) \otimes k'$. Hence the assertion follows from (c).

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (i). If $I \subseteq J$ is a non-trivial outer ideal, then so is $I \otimes \bar{k} \subseteq J \otimes \bar{k}$, a contradiction. Hence $J$ is outer simple. Since the multiplication algebra of $J$ behaves nicely under base field extensions, so does its centralizer. Therefore $\mathrm{Cent}_0(J) \otimes \bar{k}$ agrees with the outer centroid of $J \otimes \bar{k}$ and hence is a finite algebraic field extension of $\bar{k}$. As such, it has degree 1, forcing $\mathrm{Cent}_0(J) = k1_J$, and $J$ is outer central.

**28.25** (a) Setting $c := \sum_{i=1}^r c_i$, we have

$$c^2 = \sum_{i=1}^r c_i^2 + \sum_{i<j} c_i \circ c_j = \sum_{i=1}^r c_i = c,$$

$$c^3 = U_c c = \sum_{i,j=1}^r U_{c_i} c_j + \sum_{i<l} \sum_{j=1}^r \{c_i c_j c_l\} = \sum_{i=1}^r c_i^3 = \sum_{i=1}^r c_i = c,$$

and we have shown that $c$ is an idempotent in $J$. Hence so is $c_{r+1} := 1_J - c$ (28.9) and it remains to show that $(c_1, \dots, c_r, c_{r+1})$ is an orthogonal system of idempotents, completeness being obvious. For $1 \le i, l \le r$ distinct, we compute

$$U_{c_i} c_{r+1} = U_{c_i} 1_J - \sum_{j=1}^r U_{c_i} c_j = c_i^2 - U_{c_i} c_i = c_i - c_i^3 = c_i - c_i = 0,$$

$$U_{c_{r+1}} c_i = U_{1_J - c} c_i = c_i - c \circ c_i + U_c c_i = c_i - \sum_{m=1}^r c_m \circ c_i + \sum_{m=1}^r U_{c_m} c_i + \sum_{m<n} \{c_m c_i c_n\}$$

$$= c_i - 2c_i + c_i = 0,$$

$$\{c_i c_i c_{r+1}\} = c_i \circ c_i - \sum_{m=1}^r \{c_i c_i c_m\} = 2c_i^2 - 2U_{c_i} c_i = 2c_i^2 - 2c_i^3 = 0,$$

$$\{c_{r+1} c_{r+1} c_i\} = \{(1_J - c)(1_J - c) c_i\} = 2c_i - c \circ c_i - c \circ c_i + \{c c c_i\}$$

$$= 2c_i - 2c_i - 2c_i + \sum_{m,n=1}^r \{c_m c_n c_i\} = -2c_i + 2c_i = 0,$$

$$c_i \circ c_{r+1} = c_i \circ 1_J - c_i \circ c = 2c_i - 2c_i = 0,$$

$$\{c_i c_l c_{r+1}\} = c_i \circ c_l - \sum_{m=1}^r \{c_i c_l c_m\} = 0.$$

Hence $(c_1, \dots, c_r, c_{r+1})$ is a complete orthogonal system of idempotents in $J$.

(b) If $(c_1, \dots, c_r)$ is a (complete) orthogonal system of idempotents in $A$, then it is clearly one in $J$. Conversely, suppose it is a (complete) orthogonal system of idempotents in $J$. Comparing (1) with (28.9.1), we see that the idempotents $c_i, c_j$, $1 \le i < j \le r$, are orthogonal in $J$, hence, as we have seen in 28.9, in $A$. But this means that $(c_1, \dots, c_r)$ is a (complete) orthogonal system of idempotents in $A$.

## Solutions for Section 29

**29.17** (i) $\Rightarrow$ (iii). Obvious.

(iii) ⇒ (i). Since (1), (2) hold in all scalar extensions of $J$, by Cor. 12.11, $J$ is a Jordan algebra.

(i) ⇒ (ii). This follows from 29.2 since the identities (3)–(6) are respectively the same as (resp. part of) (29a.6)–(29a.9).

(ii) ⇒ (i). We will show successively that (4)–(6), (3), (2), (1) hold in $J_R$, for all $R \in k$-**alg**. In the sense of Exc. 11.35, the left (resp. right) of (4) defines a $k$-3-quadratic map $F$ (resp. $G$) from $J^3$ to $\mathrm{End}_k(J)$, and we have $F = G$ by hypothesis. Thus $F_R = G_R$ by Exc. 11.35, which by 28.13implies that (4) holds in $J_R$. For analogous reasons, (5), (6) holds in $J_R$ as well.

*Proof of* (3). By linearity in $z$, we may assume $z = w_R$, $w \in J$. Assume first $x = u_R$, $u \in J$. Since both sides of (3) are quadratic in $y$ and agree for $y = v_R$, $v \in J$, by hypothesis, it follows that (3) holds for all $y \in J_R$. Now fix $y \in J_R$ and put

$$M := \{x \in J_R \mid U_x U_y U_{x,z} + U_{x,z} U_y U_x = U_{U_{xy}, U_{x,z}y}\},$$

which is obiously closed under multiplication by scalars in $R$ and, as we have just seen, contains all elements $u_R$, $u \in J$. Hence (3) will follow once we have shown that $M$ is closed under addition. But this is implied by (5) and a straightforward computation.

*Proof of* (2). By linearity in $y$, we may assume $y = v_R$, $v \in J$. Arguing as before, it suffices to show that

$$M := \{x \in J_R \mid U_x V_{y,x} = V_{x,y} U_x\}$$

is closed under addition. But this is immediate, by (6) and a straightforward computation.

*Proof of* (1). Since (1) is quadratic in $y$, it suffices to prove it for $y = v_R$, $v \in J$. Again we will be through once we have shown that

$$M := \{x \in J_R \mid U_{U_{xy}} = U_x U_y U_x\}$$

is additively closed. This follows from (3), (4) by a lengthy, but still straightforward, computation.

Since a Jordan algebra satisfies (1)–(6), so do all its subalgebras and homomorphic images. By what we ahve just shown, therefore, they are all Jordan algebras.

**29.18** (a) By definition it suffices to show that $I$ is an outer ideal if $U_J I \subseteq I$. Indeed, if this inclusion holds, then, for all $x, y \in J$, we have $U_{x,y} I \subseteq I$ and given $z \in I$, equations (29a.14), (29a.5) imply

$$\{xyz\} = V_{x,y} z = V_x V_y z - U_{x,y} z = U_{x,1_J} U_{y,1_J} z - U_{x,y} z \in I,$$

which shows $\{JJI\} \subseteq I$ and completes the proof.

(b) If $c^2 = c$, then , then $U_c^2 = U_{c^2} = U_c$ by (29.15.1), hence $c^3 = U_c c = U_c c^2 = U_c U_c 1_J = U_c^2 1_J = U_c 1_J = c^2 = c$. Thus $c$ is an idempotent.

(c) Let $x, y \in J$ and $z \in \mathrm{Rex}(J)$. Then (29a.14) implies $V_{x,z} = V_x V_z - U_{x,z} = V_x U_{z,1_J} - U_{z,x} = 0$ and, similarly, $V_{z,x} = 0$. From the fundamental formula (29a.2) we deduce $U_{U_x z} = 0 = U_{U_z x}$. And, finally, applying (29a.9), we obtain

$$U_{U_x z, y} = U_{y, U_x z} = U_{x,y} V_{z,x} + U_x V_{z,y} - U_{x, U_{x,y} z} = -U_{x, V_{x,z} y} = 0,$$
$$U_{U_z x, y} = U_{y, U_z x} = U_{z,y} V_{x,z} + U_z V_{x,y} - U_{z, U_{z,y} x} = 0.$$

Hence $U_J \mathrm{Rex}(J) + U_{\mathrm{Rex}(J)} J \subseteq \mathrm{Rex}(J)$, and we have shown by (a) that $\mathrm{Rex}(J) \subseteq J$ is an ideal. Now suppose that $J$ is simple. Then $J \neq \{0\}$ by definition, hence $U_{1_J} = \mathbf{1}_J \neq 0$, which implies $\mathrm{Rex}(J) = \{0\}$ by simplicity. The final statement now follow from Thm. 28.18

**29.19** Let $a \in \mathrm{Cent}(J)$. Then $L_a L_x = L_x L_a = L_{ax}$ for all $x \in J$. Since, therefore, $L_a$ and $L_x$ commute, so do $L_a$ and $U_x = 2L_x^2 - L_{x^2}$, for all $x \in J$. Moreover, this and $a^2 \in \mathrm{Cent}(J)$ imply

$$U_{L_a x} = 2L_{ax}^2 - L_{(ax)^2} = 2L_a^2 L_x^2 - L_{a^2 x^2} = 2L_a^2 L_x^2 - L_{a^2} L_{x^2} = L_a^2 U_x,$$
$$U_{L_a x, y} = 2(L_{ax} L_y + L_y L_{ax} - L_{(ax)y}) = 2L_a(L_x L_y + L_y L_x - L_{xy}) = L_a U_{x,y}$$

for all $x, y \in J$, whence (28.14.1) yields $L_a \in \mathrm{Cent}(J^{\mathrm{quad}})$. Conversely, let $\varphi \in \mathrm{Cent}(J^{\mathrm{quad}})$. By (28.14.2) we have $\varphi V_x = V_x \varphi$ for $x \in J$, and from 29.3 we deduce $\varphi L_x = L_x \varphi$, hence $\varphi(xy) = x\varphi(y)$ for all $x, y \in J$. Setting $y = 1_J$, we obtain $\varphi = L_a$ with $a = \varphi(1_J)$. In particular, $L_a$ commutes with $L_x$ for all $x \in J$, whence $a$ belongs to the centre of $J$. Summing up we have shown that the injective algebra homomorphism $L\colon \mathrm{Cent}(J) \to \mathrm{End}_k(J)$ has image $\mathrm{Cent}(J^{\mathrm{quad}})$, and the assertion follows.

**29.20** If $J = J(M, q, e)$, then (1) holds strictly by (29b.6), (29b.7). Conversely, suppose (1) holds strictly. Then the second equation of (1) may be written as $U_x x = t(x)x^2 - q(x)x$, and linearizing we may apply (29a.13) to conclude

$$x^2 \circ y + U_x y = U_{x,y} x + U_x y = t(x)x \circ y + t(y)x^2 - q(x,y)x - q(x)y. \qquad \text{(s1)}$$

Applying the trace (resp. $q(-, y)$) to the first equation of (1), we obtain

$$t(x^2) = t(x)^2 - 2q(x), \quad q(x^2, y) = t(x)q(x,y) - q(x)t(y),$$

while linearizing it yields

$$x \circ y = t(x)y + t(y)x - q(x,y)e.$$

Hence on the one hand

$$\begin{aligned} x^2 \circ y + U_x y &= U_x y + t(x^2)y + t(y)x^2 - q(x^2, y)e \\ &= U_x y + (t(x)^2 - 2q(x))y + t(x)t(y)x - q(x)t(y)e - t(x)q(x, y)e + q(x)t(y)e \\ &= U_x y + (t(x)^2 - 2q(x))y + t(x)t(y)x - t(x)q(x, y)e, \end{aligned}$$

while on the other

$$\begin{aligned} t(x)x \circ y + t(y)x^2 - q(x, y)x - q(x)y = {} & t(x)^2 y + t(x)t(y)x - t(x)q(x, y)e \\ & + t(x)t(y)x - q(x)t(y)e - q(x, y)x - q(x)y \end{aligned}$$

Comparing by means of (s1) and writing $x \mapsto \bar{x}$ for the conjugation of $(M, q, e)$, we obtain

$$U_x y = q(x)y + t(x)t(y)x - q(x)t(y)e - q(x, y)x = q(x, \bar{y})x - q(x)\bar{y}.$$

Thus $J$ and $J(M, q, e)$ not only have the same unit element but also the same $U$-operator, which implies $J = J(M, q, e)$.

**29.21** Concerning the first part, assume that $x \in J$ is nilpotent. Then (29b.12) shows that $q(x)$ is nilpotent, while Exc. 28.23 yields a positive integer $m$ satisfying $x^n = 0$ for all integers $n \geq m$. We must show that $t(x)$ is nilpotent, and we will do so by induction on $m$. For $m = 1$, there is nothing to prove. For $m = 2$, we have $x^2 = 0$ and conclude from (29b.13) that $t(x)^2 = 2q(x)$ is nilpotent. Hence so is $t(x)$. We may therefore assume $m \geq 3$. Since $\lfloor \frac{m}{2} \rfloor \leq \frac{m}{2} < \lfloor \frac{m}{2} \rfloor + 1$ and $m > 2$, we deduce

$$\lfloor \frac{m}{2} \rfloor + 1 \leq \frac{m}{2} + 1 = m + 1 - \frac{m}{2} < m + 1 - 1 = m,$$

and if $n \geq \lfloor \frac{m}{2} \rfloor + 1$, then $2n \geq 2(\lfloor \frac{m}{2} \rfloor + 1) > 2\frac{m}{2} = m$. On the other hand, (28.8.5) yields $(x^2)^n = x^{2n} = 0$, and the induction hypothesis implies that $t(x^2)$ is nilpotent. But then so is $t(x)^2 = t(x^2) + 2q(x)$ by (29b.13), which shows that $t(x)$ is nilpotent and completes the induction. Summing up we have shown that if $x$ is nilpotent, then so are $t(x)$ and $q(x)$. Conversely, assume that $t(x)$ and $q(x)$ are nilpotent. Then so are $t(x)x$ and $q(x)1_J$, which both belong to $k[x]$. Since $J$ is power-associative by Prop. 29.16, Exc. 28.23 now implies that $x^2 = t(x)x - q(x)1_J$ is nilpotent. Hence so is $x$, and the first part of the problem is solved.

To establish the second part, put

$$N := \{x \in M \mid q(x), q(x, y) \in \mathrm{Nil}(k) \text{ for all } y \in M\}$$

and let $x \in N$, $y, z \in M$. Then (29b.12) yields $q(U_x z) = q(x)^2 q(z) \in \mathrm{Nil}(k)$

and, similarly, $q(U_z x) \in \mathrm{Nil}(k)$. Moreover, since the conjugation of $J$ leaves $q$ invariant, the definition of the $U$-operator implies

$$\begin{aligned} q(U_x z + U_z x, y) &= q(x, \bar{z})q(x, y) + q(z, \bar{x})q(z, y) - q(x)q(\bar{z}, y) - q(z)q(\bar{x}, y) \\ &= q(x, \bar{z})q(x + z, y) - q(x)q(y, \bar{z}) - q(x, \bar{y})q(z) \in \mathrm{Nil}(k). \end{aligned}$$

Thus $U_N J + U_J N \subseteq N$, and we have shown in view of Exc. 29.18 (a) that $N \subseteq J$ is an ideal which, by the first part of this problem, is nil. This proves $N \subseteq \mathrm{Nil}(J)$. Conversely, let $x \in \mathrm{Nil}(J)$. Then $q(x)$ and $t(x)$ are nilpotent and $\mathrm{Nil}(J)$ contains $x \circ y = t(x)y + t(y)x - q(x, y)1_J$. Hence $t(x)y - q(x, y)1_J \in \mathrm{Nil}(J)$, forcing

$$q(t(x)y - q(x, y1_J) = t(x)^2 q(y) - t(x)q(x, y)t(y) + q(x, y)^2$$

to be nilpotent. Since, therefore, $q(x, y)^2$ is nilpotent, so is $q(x, y)$ and we have shown $x \in N$. This shows $\mathrm{Nil}(J) \subseteq N$ and completes the proof.

**29.22** We begin with a simple lemma, which follows immediately from (29b.7).

**Lemma.** *Let $(M, q, e)$ be a pointed quadratic module over any commutative ring and $J := J(M, q, e)$. If $x \in J$ satisfies $x^2 = 0$, then $x^3 = -q(x)x$.* □

(a) We have $I_2 = k\mathbf{t}^2 \oplus k\mathbf{t}^4 \oplus k\mathbf{t}^5 \oplus \cdots$. Hence, writing $x$ for the imagae of $\mathbf{t}$ under the canonical map $k[\mathbf{t}]^{(+)} \to J_2$, we conclude that $J_2$ is free as a $k$-module, with basis $1_{J_2}, x, x^3$. In particular, $x$ and $x^3$ are linearly independent. Since $x^2 = 0$, and by the preceding lemma, therefore, $J_2$ cannot be isomorphic to the Jordan algebra of a pointed quadratic form over $k$.

(b) Let $k_0$ be a commutative ring and assume $2 = 0$ in $k_0$. Furthermore, let $k = k_0[\varepsilon]$, $\varepsilon^2 = 0$, be the $k_0$-algebra of dual numbers. As in Exc. 17.8, we may view $k_0$ as a $k$-algebra by means of the homomorphism $k \to k_0$, $\alpha \mapsto \bar{\alpha}$, given by $\bar{\varepsilon} = 0$. Now let $n$ be a positive integer, write $(e_1, \ldots, e_n)$ for the canonical basis of $k^n$ over $k$, put $M := k_0 \times k^n$ as a $k$-module, define $q\colon M \to k$ by

$$q((\bar{\alpha}, \sum_{i=1}^{n} \alpha_i e_i) := \alpha^2 + \varepsilon\alpha_1^2 + \sum_{i=2}^{n} \alpha_i^2 \qquad (\alpha, \alpha_1, \ldots, \alpha_n \in k),$$

and put $e := (1_{k_0}, 0)$. We claim that *the map $q$ is well-defined.* Indeed, if $\alpha, \beta \in k$ satisfy $\bar{\alpha} = \bar{\beta}$, then $\alpha = \beta + \varepsilon\gamma$, for some $\gamma \in k$, hence $\alpha^2 = \beta^2 + \varepsilon^2\gamma^2 = \beta^2$, as desired. It now follows trivially that $(M, q, e)$ is a pointed quadratic module over $k$ whose trace is identically zero. In particular, putting $J := J(M, q, e)$ and $x := e_1$, we have $t(x) = 0$ and $q(x) = \varepsilon$, hence $q(x)1_J = \varepsilon(1_{k_0}, 0) = (\bar{\varepsilon}, 0) = 0 = t(x)x$, so (29b.6) implies $x^2 = 0$. Now the preceding lemma yields $x^3 = -q(x)x = -\varepsilon e_1 \neq 0$, and we have obtained an example of the desired kind.

**29.23** For an appropriate commutative ring $k$, we must find examples of $R, S \in k$-**alg** and a homomorphism $R^{(+)} \to S^{(+)}$ of Jordan algebras that is not a morphism in $k$-**alg**. To this end, let $F$ be a field of characteristic two, $V$ a vector space over $F$, $a \in V$ a non-zero element, and $\sigma\colon V \times V \to F$ a non-zero alternating bilinear form having $\sigma(a, V) = \{0\}$. Since $\sigma$ is alternating, hence symmetric ($F$ having characteristic two), the multiplication $uv := \sigma(u, v)a$ for $u, v \in V$ makes $V$ a commutative $F$-algebra. Since $a$ belongs to radical of $\sigma$, we also have $(uv)w = 0 = u(vw)$ for all $u, v, w \in V$. Hence in actual fact $V$ is a commutative associative algebra over $F$, as therefore is $R$, the algebra arising from $V$ by adjoining an identity element. Also, $v^2 = \sigma(v, v)a = 0$ for all $v \in V$, from which we easily deduce that any $\varphi \in \mathrm{GL}(R)$ fixing $1_R$ and stabilizing $V$ is an automorphism of $R^{(+)}$. On the other hand, $\varphi$ will never be an automorphism of $R$ unles $a$ and $\varphi(a)$ are linearly dependent.

**29.24** Given a positive integer $n$ and writing $E := k^n$, the direct product of $n$ copies of $k$ as a $k$-algebra, we will show that every $k$-automorphism of the Jordan algebra $E^{(+)}$ is a $k$-automorphism of the commutative associative $k$-algebra $E$.

We first note that orthogonal idempotents $c, d$ in $E^{(+)}$ are orthogonal idempotents in $E$. Indeed, they are clearly idempotents in $E$, while orthogonality in $E$ follows from $cd = c^2d = cdc = U_c d = 0$. Thus, complete orthogonal systems of idempotents in $E$ and in $E^{(+)}$ are the same thing.

Now let $f$ be an automorphism of $E^{(+)}$ and write $(e_1, \dots, e_n)$ for the complete orthogonal system of idempotents in $E$ given by the unit vectors of $k^n$. By the above, $(f(e_1), \dots, f(e_n))$ is a complete orthogonal system of idempotents in $E$ such that $E = \sum kf(e_i)$. Extending the relations $f(e_ie_j) = \delta_{ij}f(e_i) = f(e_i)f(e_j)$ for all $i, j = 1, \dots, n$ bilinearly to all of $E$ now shows that $f$ is an automorphism of $E$.

**29.25** If $C$ is alternative, then (17.4.2) shows $C^{(+)} = J(C, n_C, 1_C)$. Conversely, let this be so. For $x, y \in C$ we apply (16.5.5), (16.5.10), (16.5.4) and obtain

$$\begin{aligned} n_C(x, \bar{y})x - n_C(x)\bar{y} = xyx &= (x \circ y)x - (yx)x = t_C(x)yx + t_C(y)x^2 - n_C(x, y)x - (yx)x \\ &= t_C(x)yx + \big(t_C(x)t_C(y) - n_C(x, y)\big)x - t_C(y)n_C(x)1_C - (yx)x \\ &= n_C(x, \bar{y})x - n_C(x)\bar{y} - n_C(x)y + (y\bar{x})x. \end{aligned}$$

Comparing, we arrive at one of Kirmse's identities (17.4.1), i.e., at $(y\bar{x})x = n_C(x)y$. But this means that $C$ is right alternative. Since it is also flexible by hypothesis, it is, in fact, alternative.

**29.26** Homomorphism of pointed quadratic modules are clearly homomorphisms of the corresponding Jordan algebras. Hence the assignment in ques-

tion defines a functor from $k$-$\mathbf{poqua}_{\mathrm{inj}}$ to $k$-$\mathbf{jord}_{\mathrm{inj}}$, which by its very definition is faithful Before we can show that it is full, we need the following lemma.

**Lemma.** *Let $(M, q, e)$ and $(M, q_1, e)$ be pointed quadratic modules over $k$, with the same underlying $k$-module $M$ and the same base point $e$. If $M$ is projective and $J(M, q, e) = J(M, q_1, e)$, then $q = q_1$.*

*Proof* Since $e \in M$ is unimodular by Lemma 11.15, the proof of Prop. 16.16 can be extended verbatim to this slightly different setting. □

Now let $(M, q, e)$ and $(M', q', e')$ be pointed quadratic modules over $k$ such that $M$ and $M'$ are both projective and let $\varphi\colon J(M, q, e) \to J(M', q', e')$ be an injective homomorphism of Jordan algebras over $k$. Setting $q_1 := q' \circ \varphi$, we conclude that $(M, q_1, e)$ is a pointed quadratic module over $k$ (since $\varphi$ preserves identity elements) and $\varphi\colon (M, q_1, e) \to (M', q', e')$ is a homomorphism of pointed quadratic modules. Hence $\varphi\colon J(M, q_1, e) \to J(M', q', e')$ is a homomorphism of Jordan algebras. But $\varphi$ was assumed to be injective. Hence $J(M, q, e) = J(M, q_1, e)$, which by the preceding lemma implies $q_1 = q$. Hence $\varphi\colon (M, q, e) \to (M', q', e')$ is a homomorphism of pointed quadratic modules. Thus the functor in question is full.

**29.27** We put $J := J(V, q, e)$. Since $F$ has characteristic not 2, we may extend $e = 1_J$ to an orthogonal basis of $V$ relative to $q$, allowing us to identify $q = \langle 1, \delta, \delta\varepsilon\rangle_{\mathrm{quad}}$ for some $\delta, \varepsilon \in F^\times$. Now put

$$K := \mathrm{Cay}(F, -\varepsilon) = F \oplus F j_1, \quad B := \mathrm{Cay}(K, -\delta) = K \oplus K j_2.$$

as in 18.3. Then $B$ is a quaternion algebra over $F$, while $K \subseteq B$ is a quadratic étale subalgebra. Let $\tau$ be the involution of $B$ corresponding to $K$ by Exc. 19.39 (b). Then $\tau(a \oplus b j_2) = \bar{a} \oplus b j_2$ for all $a, b \in K$, which implies $H(B, \tau) = W := F 1_B \oplus K j_2 = F 1_B \oplus F j_2 \oplus F j_1 j_2$. By Exc. 29.25 we have $B^{(+)} = J(B, n_B, 1_B)$ and therefore $H(B, \tau) = J(W, n_B|_W, 1_B)$. By standard properties of the Cayley-Dickson construction, the vectors $1_B, j_2, j_1 j_2$ are orthogonal relative to $n_B$ and satisfy $n_B(1_B) = 1$, $n_B(j_2) = \delta$, $n_B(j_1 j_2) = n_B(j_1) n_B(j_2) = \delta\varepsilon$. Hence the pointed quadratic modules $(V, q, e)$ and $(W, N_B|_W, 1_B)$ are isometric, forcing $J$ and $H(B, \tau)$ as the corresponding Jordan algebras by Exc. 29.26 to be isomorphic.

It remains to prove that $(B, \tau)$ as a quaternion algebra with involution is unique up to isomorphism. To this end, we require a lemma.

**Lemma.** *Let $B$, $B'$ be quaternion algebras over $F$ and suppose $W \subseteq (B, n_B)$, $W' \subseteq (B', n_{B'})$ are regular subspaces of co-dimension 1. If $W$ and $W'$ are isometric, then $B$ and $B'$ are isomorphic.*

*Proof* By Lemma 11.10 we have $B = W \perp Fu$, $B' = W' \perp Fu'$ for some non-zero $u \in B$, $u' \in B'$. Recall that the determinant of a quadratic space like $(B, n_B)$ (resp. $(B', n_{B'})$) is unique up to non-zero square factors in $F$. As a matter of fact, we deduce from (19.20.1) that this determinant is a square. On the other hand, it agrees with $\det(W)n_B(u)$ (resp. $\det(W')n_{B'}(u')$). But $W$ and $W'$ being isometric, their determinants differ by a square factor in $F$. Hence so do $n_B(u)$ and $n_{B'}(u')$. But this means that $B$ and $B'$ are norm-equivalent. By the norm equivalence theorem 23.5, therefore, they are isomorphic. □

Now let $(B', \tau')$ be another quaternion algebra with involution over $F$ having $W' := H(B', \tau') \cong J(V, q, e)$. By Exc. 29.26, the quadratic subspaces $W \subseteq (B, n_B)$ and $W' \subseteq (B', n_{B'})$ are not only regular but also isometric. Our preceding lemma therefore implies that $B$ and $B'$ are isomorphic. We may thus assume $B = B'$. Let $(1_B, j_2', j_3')$ be an orthogonal basis of $W'$ such that $n_B(j_2') = \delta$, $n_B(j_3') = \delta\varepsilon$, with $\delta, \varepsilon$ as above. Since $(B, n_B)$ has trivial determinant, we conclude $W'^{\perp} = Fj_1'$, $n_B(j_1') = \varepsilon$. Then $F[j_1'] \cong \mathrm{Cay}(F, -\varepsilon) = K$. Now (16.5.5) implies for $i = 2, 3$:

$$\begin{aligned} 0 &= \tau'(t_B(j_1')j_i' + t_B(j_i')j_1' - n_B(j_1', j_i')1_B) = \tau'(j_1' \circ j_i') = \tau'(j_1') \circ j_i' \\ &= t_B(j_1')j_i' + t_B(j_i')\tau'(j_1') - n_B(\tau'(j_1'), j_i')1_B = -n_B(\tau'(j_1'), j_i')1_B. \end{aligned}$$

Thus $n_B(\tau'(j_1'), j_i') = 0$, and since we trivially have $n_B(\tau'(j_1'), 1_B) = 0$, we deduce $\tau'(j_1') \in W'^{\perp} = Fj_1'$, Hence $\tau'(j_1') = \pm j_1'$. Here $\tau'(j_1') = j_1'$ would imply $\tau' = \mathbf{1}_B$, a contradiction. Hence $\tau'(j_1') = -j_1'$. Thus Thus $\tau'$ is the involution of $B$ corresponding to $F[j_1'] \cong K$, which implies $(B, \tau') \cong (B, \tau)$ by Exc. 19.39 (b).

## Solutions for Section 30

**30.12** (a) $x \in \mathrm{Rad}(q)$ implies $U_x y = q(x, \bar{y})x - q(x)\bar{y} = 0$ for all $y \in J$, hence $U_x = 0$, and $x$ is an absolute zero divisor of $J$. Conversely, let this be so. Then (29b.10) yields $q(x)^2 e = U_x \bar{x}^2 = 0$, and applying $q$ we conclude $q(x)^4 = 0$, hence $q(x) = 0$ since $k$ is reduced. For any $y \in J$, we therefore obtain $0 = U_x \bar{y} = q(x, y)x$ and then $q(x, y)^2 = q(q(x, y)x, y) = 0$. Thus $q(x, y) = 0$, and we have proved $x \in \mathrm{Rad}(q)$.

(b) Here $k$ is arbitrary. Then $\bar{k} := k/\mathrm{Nil}(k) \in k$-**alg** is reduced, and we have a canonical identification $J_{\bar{k}} = \bar{J} := J/\mathrm{Nil}(k)J$ via 9.3, matching $z_{\bar{k}}$ for $z \in J$ with $\bar{z}$, the image of $z$ under the natural map $J \to \bar{J}$. Since $x$ is an absolute zero divisor in $J$, $\bar{x}$ is one in $\bar{J}$, so by the special case just treated we have $\bar{q}(\bar{x}) = \bar{q}(\bar{x}, \bar{y}) = 0$ for all $y \in J$, where $\bar{q} = q_{\bar{k}}$ is the $\bar{k}$-quadratic extension of $q$.

But this means that $q(x)$ and $q(x,y)$ are nilpotent elements of $k$, for all $y \in J$, which implies $x \in \mathrm{Nil}(J)$ by Exc. 29.21. The rest is clear, by Thm. 30.11.

**30.13** If $J = J(M,q,e)$ for some pointed quadratic module $(M,q,e)$ over $F$, then the Dickson condition clearly holds. Conversely, suppose $J$ satisfies the Dickson condition. Then we are forced to put $M := J$ as a vector space over $F$ and $e := 1_J$. The problem is to construct the quadratic form $q\colon M \to F$. We do so by considering the following cases.

*Case 1:* $\mathrm{char}(F) \neq 2$. Then $J$ becomes a linear Jordan algebra under the product $x \cdot y := \frac{1}{2} x \circ y$, and by hypothesis, the quantities $1_J, x, x^2$ are linearly dependent over $F$. Hence Exc. 16.21 implies that $J$ is a commutative conic algebra over $F$, with norm $q$ and trace $t$, say. Linearizing the relation $x^2 = t(x)x - q(x)e$ and invoking (27.9.1), we conclude $J = J(M,q,e)$ as linear Jordan algebras, hence also as quadratic ones.

*Case 2:* $\mathrm{char}(F) = 2$. We may clearly assume that $J$ has dimension at least 2.

*Case 2.1:* $\dim_F(J) = 2$. Let $e = 1_J, u$ be a basis of $J$ over $F$. Then

$$u^2 = \gamma u + \delta e \tag{s1}$$

for some $\gamma, \delta \in F$, and we define a quadratic form

$$q(\xi_0 e + \xi_1 u) := \xi_0^2 + \gamma \xi_0 \xi_1 + \delta \xi_1^2 \tag{s2}$$

for $\xi_0, \xi_1 \in F$. One checks that $(M,q,e)$ is a pointed quadratic module over $F$, with bilinearized norm, trace and conjugation respectively given by

$$q(\xi_0 e + \xi_1 u, \eta_0 e + \eta_1 u) = \gamma(\xi_0 \eta_1 + \xi_1 \eta_0), \tag{s3}$$

$$t(\xi_0 e + \xi_1 u) = \gamma \xi_1, \tag{s4}$$

$$\overline{\xi_0 e + \xi_1 u} = (\xi_0 + \gamma \xi_1) e + \xi_1 u \tag{s5}$$

for $\xi_i, \eta_i \in F$, $i = 0, 1$. Moreover, since $J$ is locally linear, we have $u^3 = uu^2 = \gamma u^2 + \delta u$, hence

$$u^3 = \gamma\delta e + (\gamma^2 + \delta) u. \tag{s6}$$

Using (s1)–(s6), it is now straightforward to check that the $U$-operators of $J$ and $J(M,q,e)$ are the same. Hence $J = J(M,q,e)$.

*Case 2.2:* $\dim_F(J) \geq 3$. Choose a subspace $V \subseteq M$ that is complementary to $Fe$:

$$M = Fe \oplus V. \tag{s7}$$

Since $J$ satisfies the Dickson condition, we obtain

$$v^2 = q(v)e + s(v), \quad q(v) \in F, \quad s(v) \in V \tag{s8}$$

strictly for all $v \in V$ such that there eists a map $t\colon V \to F$ satisfying $t(0) = 0$ and

$$s(v) = t(v)v, \tag{s9}$$

again strictly for all $v \in V$ . Here $q\colon V \to F$ is a quadratic form, $s\colon V \to V$ is a quadratic map, and $t\colon V \to F$ is rational as well as homogeneous of degree 1. We wish to show that $t$ is linear. To this end, we may assume that $F$ is infinite, replace $v$ by $v + w$ in (s8), (s9) and collect mixed terms to obtain

$$v \circ w = \big(t(v + w) - t(v)\big)v + \big(t(v + w) - t(w)\big)w - q(v, w)e. \tag{s10}$$

Since $F$ has characteristic 2, this implies

$$v \circ (v \circ w) = \big(t(v + w) - t(w)\big)v \circ w, \tag{s11}$$

$$v^2 \circ w = t(v)v \circ w. \tag{s12}$$

By the same token and (29a.10), we have $v \circ (v \circ w) = v^2 \circ w$, hence

$$\big(t(v + w) - t(v) - t(w)\big)v \circ w = 0. \tag{s13}$$

Now, if $v \circ w = 0$ for all $v, w \in V$, then (s10) implies $t(v + w) = t(v) = t(w)$ provided $v, w$ are linearly independent. By Zariski density, therefore, $t$ is constant, hence zero, hence linear. On the other hand, if $v \circ w \neq 0$ for some $v, w \in V$, Zariski density again and (s13) imply that $t$ is linear. Thus $t$ is linear under all circumstances, and we have

$$v^2 = t(v)v - q(v)e$$

for all $v \in V$. Extending $q, t$ to all of $M$ via

$$q(\xi e + v) = \xi^2 + \xi t(v) + q(v), \quad t(\xi e + v) = t(v)$$

for $\xi \in k$, $v \in V$, one checks that $x^2 - t(x)x + q(x)e = 0$ for all $x \in M$. But $J$ is strictly locally linear, forcing $x^3 - t(x)x^2 + q(x)x = 0$ strictly for all $x \in M$. Now $J = J(M, q, e)$ follows from Exc. 29.20.

## Solutions for Section 31

**31.29** (i) $\Rightarrow$ (ii). This implication follows from the fact that $J$ contains invertible elements (e.g., the identity).

(ii) $\Rightarrow$ (iii) Let $x \in J$ be unimodular. For $\mathfrak{p} \in \operatorname{Spec}(k)$, Lemma 9.17 implies $x(\mathfrak{p}) \neq 0$, hence $J(\mathfrak{p}) \neq \{0\}$, and we conclude $\operatorname{rk}_{\mathfrak{p}}(J) = \dim_{k(\mathfrak{p})}(J(\mathfrak{p})) > 0$.

(iii) $\Rightarrow$ (i). For $x \in J^{\times}$, the linear map $U_x \colon J \to J$ is bijective (Prop. 31.2), and hence so is $U_{x(\mathfrak{p})} = U_x(\mathfrak{p})$. But from (iii) we deduce $J(\mathfrak{p}) \neq \{0\}$, which implies $x(\mathfrak{p}) \neq 0$, and Lemma 9.17 show that $x$ is unimodular.

**31.30** (a) By the results of §§29,30, equations (2)–(8) hold for all $i, j, m, n, p \in \mathbb{N}$. For $n \in \mathbb{Z}$, $n > 0$, we combine (1) with (31.3.1) and obtain $U_{x^{-n}} = U_{(x^{-1})^n} = U^n_{x^{-1}} = (U_x^{-1})^n = U_x^{-n}$. Hence (2) holds for all $n \in \mathbb{Z}$.

By (2), the set of all integers $m$ such that (3) holds for all integers $n$ is a subgroup of $\mathbb{Z}$. Hence, in order to prove (3), we may assume $m = 1$. Then we must show $U_x x^{-n} = x^{2-n}$ for all $n \in \mathbb{N}$ and we do so by induction on $n$. For $n = 0, 1$, there is nothing to prove. For $n \geq 2$, assuming the validity of the assertion for $n-2$ yields $U_x x^{-n} = U_x(x^{-1})^n = U_x U_{x^{-1}}(x^{-1})^{n-2} = x^{2-n}$, as claimed. Thus (3) holds.

Turning to (4), we first assume $n \in \mathbb{N}$ and then argue by induction. For $n = 0, 1$ there is nothing to prove. Now let $n \geq 2$ and assume the assertion is valid for $n-2$. Then $(x^m)^n = U_{x^m}(x^m)^{n-2} = U_{x^m} x^{mn-2m} = x^{2m+mn-2m} = x^{mn}$. as claimed. Next assume $n < 0$. The case just treated and (2), (3) yield $U_{(x^m)^{-n}}(x^m)^n = (x^m)^{-n} = x^{-mn} = U_{x^{-mn}} x^{mn} = U_{(x^m)^{-n}} x^{mn}$, and since $U_{(x^m)^{-n}}$ is bijective, the proof of (4) is complete.

Next we establish (7), where we may clearly assume $i = 1$. For $l \in \mathbb{N}$ such that $2l + m, 2l + n \in \mathbb{N}$, we obtain, using (2), (29a.3), (3), (30.4.5),

$$\begin{aligned} U_x U_{x^m, x^n} &= U_{x^{-l}} U_x U_{x^l} U_{x^m, x^n} U_{x^l} U_{x^{-l}} = U_{x^{-l}} U_x U_{U_{x^l} x^m, U_{x^l} x^n} U_{x^{-l}} = U_{x^{-l}} U_x U_{x^{2l+m}, x^{2l+n}} U_{x^{-l}} \\ &= U_{x^{-l}} U_{x^{2l+m+1}, x^{2l+n+1}} U_{x^{-l}} = U_{U_{x^{-l}} x^{2l+m+1}, U_{x^{-l}} x^{2l+n+1}} = U_{x^{m+1}, x^{n+1}} \end{aligned}$$

and, similarly, $U_{x^m, x^n} U_x = U_{x^{m+1}, x^{n+1}}$.Thus (7) holds.

Now we can prove (5) by letting $l \in \mathbb{N}$ satisfy $2l+m, 2l+n, 2l+p \in \mathbb{N}$. Then (7) yields

$$\begin{aligned} U_{x^{3l}}\{x^m x^n x^p\} &= U_{x^{3l}} U_{x^m, x^p} x^n = U_{x^l} U_{x^m, x^p} U_{x^l} U_{x^l} x^n = U_{U_{x^l} x^m, U_{x^l} x^p} U_{x^l} x^n = \{x^{2l+m} x^{2l+n} x^{2l+p}\} \\ &= 2x^{6l+m+n+p} = U_{x^{3l}}(2x^{m+n+p}). \end{aligned}$$

Thus (5) holds.

Turning to (6), we use (2), (29a.4), (3), (7) and obtain

$$\begin{aligned} V_{x^m, x^n} U_{x^{m+n}} &= V_{x^m, x^n} U_{x^m} U_{x^n} = U_{x^m, U_{x^m} x^n} U_{x^n} = U_{x^m, x^{2m+n}} U_{x^n} = U_{x^{m+n}, x^{2(m+n)}} \\ &= U_{x^{m+n}, U_{x^{m+n}} 1_J} = V_{x^{m+n}, 1_J} U_{x^{m+n}} = V_{x^{m+n}} U_{x^{m+n}}. \end{aligned}$$

Hence (6) follows.

Finally,in order to establish (8), we let $l \in \mathbb{N}$ satisfy $l+i, l+j, l+m, l+n \in \mathbb{N}$.

Then, by (2), (7), (30.4.6), 29a.3),

$$\begin{aligned} U_{x^i,x^j}U_{x^m,x^n} &= U_{x^{-l}}U_{x^l}U_{x^i,x^j}U_{x^l}U_{x^m,x^n}U_{x^{-l}} = U_{x^{-l}}U_{x^{l+i},x^{l+j}}U_{x^{l+m},x^{l+n}}U_{x^{-l}} \\ &= U_{x^{-l}}\Big(U_{x^{2l+i+m},x^{2l+j+n}} + U_{x^{2l+i+n},x^{2l+j+m}}\Big)U_{x^{-l}} \\ &= U_{x^{i+m},x^{j+n}} + U_{x^{i+n},x^{j+m}}, \end{aligned}$$

as claimed.

(b) Arguing as in the solution to Exc. 28.20 (a), it follows that $\varepsilon_x^\times\colon k[\mathbf{t},\mathbf{t}^{-1}]^{(+)} \to J$ is a homomorphism of Jordan algebras forcing $k[x,x^{-1}] \subseteq J$ to be a subalgebra containing $\varepsilon_x^\times(\mathbf{t}^{\pm 1}) = x^{\pm 1}$. Writing $J'$ for the subalgebra of $J$ generated by $x$ and $x^{-1}$, we therefore have $J' \subseteq k[x,x^{-1}]$. On the other hand, it follows immediately from the definitions that $J'$ contains all powers of $x$ with integer exponents. Since, therefore, $k[x,x^{-1}] \subseteq J'$, we have equality: $J' = k[x,x^{-1}]$.

(c) Arguing as in 30.3, replacing $\mathbb{N}$ by $\mathbb{Z}$ everywhere and using (7), (8), we deduce (9). The final assertion may be proved in exactly the same manner as Thm. 30.11.

**31.31** Put $x := 1_J - u$ and $y := \sum_{n\geq 0} u^n$. Then, since $J$ is power-associative,

$$\begin{aligned} U_x y &= y - u\circ y + U_u y = \sum_{n\geq 0} u^n - 2\sum_{n\geq 0} u^{n+1} + \sum_{n\geq 0} u^{n+2} \\ &= \sum_{n\geq 0} u^n - 2\sum_{n\geq 1} u^n + \sum_{n\geq 2} u^n = 1_J - u = x, \end{aligned}$$

while Thm. 30.1 yields

$$U_x y^2 = U_{1_J-u}U_{\sum_{n\geq 0}u^n}1_J = U_{\sum_{n\geq 0}u^n - \sum_{n\geq 1}u^n}1_J = U_{1_J}1_J = 1_J,$$

solving the first part of the problem. As to the second, if $x$ is invertible in $J$, then by Prop. 31.5 so is $\bar{x}$ in $\bar{J}$. Conversely, let this be so. Then Prop. 31.2 implies that some $y \in J$ satisfies $U_x y = 1_J - u$, where $u$ belongs to $I$ and hence is nilpotent. By the first part, therefore, $U_x y$ is invertible in $J$ and thus so is $x$, by Prop. 31.3.

**31.32** (a) By (27.4.2) we have

$$[L_{x^2}, L_y] = 0 \quad\Longleftrightarrow\quad [L_x, L_{xy}] = 0.$$

(b) (i) $\Rightarrow$ (ii). Let $y := x^{-1}$. Then $2xy = x\circ y = \{x1_J x^{-1}\} = 2\cdot 1_J$ by Exc. 31.30, (5). Hence $xy = 1_J$. Moreover, Exc. 31.30, (8) shows $4[L_x, L_y] = [U_{x,1_J}, U_{1_J,y}] = 0$, so $x$ and $y$ operator commute.

(ii) $\Rightarrow$ (iii). We have $xy = 1_J$, and since $x$ and $y$ operator commute, we also obtain $x^2y = y(xx) = x(yx) = x(xy) = x$,

(iii) ⇒ (i). Since $x$ and $xy = 1_J$ operator commute, so do $x^2$ and $y$, by (a). For the same reason $y^2$ and $x$ operator commute. Hence

$$U_x y^2 = 2x(y^2x) - x^2y^2 = x^2(yy) = y(x^2y) = yx = 1_J,$$

and $x$ is invertible in $J$ by Prop. 31.2.

Next suppose $y \in J$ satisfies (ii). Then $x$ is invertible and $U_x y = 2x(xy) - y(xx) = 2x - x(yx) = x$, hence $y = U_x^{-1}x = x^{-1}$. Similarly, if $y$ satisfies (iii), then $U_x y = 2x(xy) - x^2y = x$ and again $y = x^{-1}$.

**31.33** If $x$ is invertible in $J$, then $1 = q(1_J) = q(U_x x^{-2}) = q(x)^2 q(x^{-2})$ by (29b.12), so $q(x)$ is invertible in $k$. Conversely, let this be so and put $y := q(x)^{-1}\bar{x}$. Then (29b.10) yields $U_x y = q(x)^{-1}U_x\bar{x} = x$. On the other hand, writing $t$ for the trace of $(M, q, e)$, we apply (29b.11), (29b.6) and obtain not only $q(y) = q(x)^{-1}$ but also

$$U_x y^2 = t(y)U_x y - q(y)U_x 1_J = q(x)^{-1}t(x)x - q(x)^{-1}x^2 = 1_J.$$

Hence (31.1.1) shows that $x$ is invertible in $J$ with inverse $y$. The rest is clear.

**31.34** (a) $q^{(f)}\colon M \to k$ is a quadratic form and $e^{(f)} \in M$ satisfies $q^{(f)}(e^{(f)}) = q(f)q(f^{-1}) = 1$ by Exc. 31.33, (1). Hence $(M, q, e)^{(f)}$ is a pointed quadratic module over $k$. For $x \in M$, the definitions imply

$$\begin{aligned} t^{(f)}(x) &= q^{(f)}(e^{(f)}, x) = q(f)q(q(f)^{-1}\bar{f}, x) = q(\bar{f}, x), \\ \bar{x}^{(f)} &= t^{(f)}(x)e^{(f)} - x = q(f)^{-1}q(\bar{f}, x)\bar{f} - x, \end{aligned}$$

hence (2) and (3). In (4), both sides live on the same $k$-module and have the same identity element. Hence it suffices to show that they have the same $U$-operator. Let $x, y \in M$ and write $U_x$ (resp. $U'_x$) for the $U$-operator of $J(M, q, e)$ (resp. $J((M, q, e)^{(f)})$. We first note

$$\overline{U_f y} = U_{\bar{f}}\bar{y} = q(\bar{f}, y)\bar{f} - q(f)y \tag{s1}$$

by (29b.3), (29b.5) and (29b.11). Hence (2) and (3) imply

$$\begin{aligned} U'_x y &= q^{(f)}(x, \bar{y}^{(f)})x - q^{(f)}(x)\bar{y}^{(f)} \\ &= q(f)q(x, q(f)^{-1}q(\bar{f}, y)\bar{f} - y)x - q(f)q(x)(q(f)^{-1}q(\bar{f}, y)\bar{f} - y) \\ &= (q(\bar{f}, x)q(\bar{f}, y) - q(f)q(x, y))x - q(x)(q(\bar{f}, y)\bar{f} - q(f)y) \\ &= q(x, q(\bar{f}, y)\bar{f} - q(f)y)x - q(x)(q(\bar{f}, y)\bar{f} - q(f)y) \\ &= q(x, \overline{U_f y})x - q(x)\overline{U_f y} = U_x U_f y = U_x^{(f)} y, \end{aligned}$$

hence (4).

(b) From (a) we conclude that $g \in M$ is invertible in $(M, q, e)^{(f)}$ iff $k^\times \ni q^{(f)}(g) = q(f)q(g)$ iff $q(g) \in k^\times$ iff $g$ is invertible in $(M, q, e)$. In this case,

$((e^{(f)})^{(g)} = g^{(-1,f)}$ (by (a)) $= U_{f^{-1}}g^{-1}$ (by Thm. 31.10 (a)) $= (U_f g)^{-1}$ (by (31.3.2)) $= e^{(U_f g)}$ and $(q^{(f)})^{(g)}(x) = q^{(f)}(g)q^{(f)}(x) = q(f)^2q(g)q(x) = q(U_f g)q(x)$ (by (29b.12)) $= q^{(U_f g)}(x)$ for all $x \in M$. This proves (b).

(c) $\eta \in \mathrm{Str}(J)$ is an isomorphism $\eta\colon J \xrightarrow{\sim} J^{(p)}$, $J^{(p)} = J(M, e^{(p)}, q^{(p)})$ by (a), $p := \eta(1_J) \in J^\times$ (by (31.17.1)). By Exc. 29.26, therefore, $\eta\colon (M,q) \xrightarrow{\sim} (M, q^{(p)})$ is an isometry of quadratic modules, which implies $q \circ \eta = \alpha q$, $\alpha := q(p)^{-1}$. Conversely, let $\eta\colon M \to M$ be a linear bijection such that $q \circ \eta = \alpha q$, for some $\alpha \in k^\times$. Then $\alpha = q(\eta(e))$, so $\eta(e)$ is invertible in $(M,q,e)$ and $q^{(p)} \circ \eta = q$, $p := \eta(e)^{-1}$. Thus $\eta\colon (M,q,e) \to (M,q,e)^{(p)}$ is an isomorphism of pointed quadratic modules and hence, again by Exc. 29.26, and isomorphism $\eta\colon J \to J^{(p)}$ of Jordan algebras. Summing up, $\eta \in \mathrm{Str}(J)$ and we are done.

(d) With $p := e_3$ we have $q(p) = -1$ and hence $q^{(p)} = -q$. The signature of $q$ is $-1$, while the signature of $q^{(p)}$ is 1. Since, therefore, $q$ and $q^{(p)}$ are not isometric, $J$ and $J^{(p)}$ again by (a) and Exc. 29.26 are not isomorphic.

(e) The linear trace, $t^{(f)}$, of $J^{(f)} = J((M,q,e)^{(f)})$ by (a) satisfies $t^{(f)}(x) = q(f, \bar{x})$, hence is different from zero. It follows that $(M,q,e)$ and $(M,q,e)^{(f)}$ are not isomorphic. By Exc. 29.26, therefore, neither are $J$ and $J^{(f)}$. As an example put $M := F^3$ with the canonical basis $e_1, e_2, e_3$, $e := e_1$ and $q := \langle S \rangle_{\mathrm{quad}}$, where

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then $(M,q,e)$ is a pointed quadratic module over $F$ and $Dq = \langle S + S^\mathsf{T} \rangle$, where

$$S + S^\mathsf{T} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Thus $t = q(e,-) = 0$ and $f := e_2$ satisfies $q(f) = q(f, e_3) = 1$. Hence all hypotheses of (e) are fulfilled, irrespective of whether $F$ is or is not algebraically closed.

**31.35** Setting $1^{(y)} := 1_{J^{(y)}}$ as in (31.8.1), we apply (31.8.2) and obtain $U_{x^{-1}+y^{-1}}U_y = U^{(y)}_{1^{(y)}+z}$, $z := x^{-1}$. Here Thm. 31.10 (a) yields $z^{(-1,y)} = U_y^{-1}(x^{-1})^{-1} == U_y^{-1}x$, hence $U_y z^{(-1,y)} = x$. Using Exc. 31.30, (9), we therefore conclude

$$\begin{aligned} U_x U_{x^{-1}+y^{-1}} U_y &= U_{U_y z^{(-1,y)}} U^{(y)}_{1^{(y)}+z} = U_y U^{(y)}_{z^{(-1,y)}} U^{(y)}_{1^{(y)}+z} = U_y U^{(y)}_{z^{(-1,y)}+1^{(y)}} = U_y U_{z^{(-1,y)}+y^{-1}} U_y \\ &= U_{U_y z^{(-1,y)} + U_y y^{-1}} = U_{x+y}. \end{aligned}$$

**31.36** We have $xx^{-1} = L_x L_x^{-1} 1_J = 1_J$, and the Jordan identity (27.1.2) yields $x(x^2x^{-1}) = x^2(xx^{-1}) = x^2$, hence $x^2x^{-1} = x$ since $L_x$ is bijective. We therefore conclude from Exc. 31.32 that $x$ is invertible in $J$ with inverse $x^{-1}$. Now

(31.3.1) and (27.10.6) imply that $L_{x^{-1}} = \frac{1}{2}V_{x^{-1}} = \frac{1}{2}U_x^{-1}V_x = U_x^{-1}L_x$ is bijective, forcing $x^{-1}$ to be linearly invertible with linear (= ordinary) inverse $(x^{-1})^{-1} = x$.

Now let $F$ be a field of characteristic not 2 and $(M, q, e)$ a pointed quadratic module over $F$. If $q$ is anisotropic and $J := J(M, q, e)$ has dimension at most 2, then Exc. 19.27 shows that $J$ is a field and, in particular, a linear division algebra. Conversely, let $J$ be a linear division algebra. By what we have just seen, $J$ is a Jordan division algebra, forcing $q$ to be anisotropic by Exc. 31.33. Assume $J$ has dimension $n \geq 3$ and extend $1_J$ to an orthogonal basis $(e_1 = 1_J, e_2, e_3, \ldots, e_n)$ of $J$ relative to $Dq$. Applying (29b.9), we obtain

$$e_2e_3 = \frac{1}{2}(q(e_1, e_2)e_3 + q(e_1, e_3)e_2 - q(e_2, e_3)e_1) = 0.$$

Hence $e_2$, though invertible, is not linearly invertible, and $J$ cannot be a linear division algebra. This contradiction shows $n \leq 2$ and completes the proof.

**31.37** (a) Let $\eta\colon J \to J'$ be a strong homotopy, so some $p \in J^\times$ makes $\eta\colon J^{(p)} \to J'$ a homomorphism. Hence $\eta\colon J \to J'$ is a homotopy by Prop. 31.18 (b). Conversely, let $\eta\colon J \to J'$ be a homotopy such that $\eta(J^\times) = J'^\times$. Then there exists a $p' \in J'^\times$ such that $\eta\colon J \to J'^{(p')}$ is a homomorphism. By hypothesis, we find an element $p \in J^\times$ satisfying $\eta(p) = p'^{-2}$, Then 31.8 (ii) and Cor. 31.11 show that

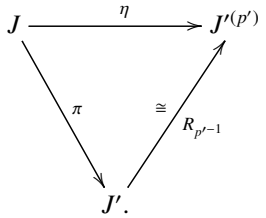
$$\eta\colon J^{(p)} \longrightarrow J'^{(p')(\eta(p))} = J'^{(p')(p'^{-2})} = J'$$

is a homomorphism, forcing $\eta\colon J \to J'$ to be a strong homotopy.

(b) Let $F$ be a field and $\mu \in F[\mathbf{t}]$ be an irreducible polynomial of degree at least 2, making $K := F[\mathbf{t}]/(\mu)$ a finite algebraic extension field of $F$. We denote by $\pi\colon F[\mathbf{t}] \to K$ the canonical projection and put $J := F[\mathbf{t}]^{(+)}$, $J' := K^{(+)}$. Pick an element $p' \in K \setminus F1_K$. Then $p' \in J'^\times$ and the linear map

$$\eta\colon J \longrightarrow J', \quad f \longmapsto \eta(f) := \pi(f)p'^{-1} \tag{s1}$$

fits into the commutative diagram




where, by (31.13.1), the horizontal arrow is a homomorphism. Thus $\eta\colon J \to J'$ is a homotopy. Assume that this homotopy is strong. Then there exists a $p \in J^\times$

such that $\eta\colon J^{(p)} \to J'$ is a homomorphism. But Ex. 31.6 shows $J^\times = F[\mathbf{t}]^\times = F^\times$, hence $p \in F^\times$. By (s1), therefore,

$$1_K = 1_{J'} = \eta(1_{J^{(p)}}) = \eta(p^{-1}) = p^{-1}\eta(1_J) = p^{-1}p'^{-1},$$

and we arrive at the contradiction $p' = p^{-1}1_K \in F1_K$. Thus $\eta$ is not a strong homotopy.

**31.38** (a) We argue by induction if $n \geq 0$. For $n = 0$, we have to show $\lambda(1_J) = 0$, which follows from (2) by setting $x = y = 1_J$: $\lambda(1_J) = \lambda(U_{1_J}1_J) = 3\lambda(1_J)$, and the assertion follows. For $n = 1$, there is nothing to prove, and if the formula is valid for all natural numbers $< n$ where $n \geq 2$, then (2) implies $\lambda(x^n) = \lambda(U_x x^{n-2}) = 2\lambda(x) + \lambda(x^{n-2}) = 2\lambda(x) + (n-2)\lambda(x) = n\lambda(x)$. If $n = -1$, we obtain $\lambda(x) = \lambda(U_x x^{-1}) = 2\lambda(x) + \lambda(x^{-1})$, hence $\lambda(x^{-1}) = -\lambda(x)$. And finally, for any integer $n > 0$, the definition (cf. Exc. 31.30 (1)) implies $\lambda(x^{-n}) = \lambda((x^{-1})^n) = n\lambda(x^{-1}) = -n\lambda(x)$. This completes the proof.

(b) We have $(vw)^2 = v^2w^2 = U_v w^2$. Hence (a) implies $2\lambda(vw) = \lambda((vw)^2) = \lambda(U_v w^2) = 2\lambda(v) + \lambda(w^2) = 2(\lambda(v) + \lambda(w))$, and the first part of (b) follows. The rest is clear.

(c) is straightforward.

(d) The statement is obvious if $\lambda$ is trivial, i.e., if $\lambda(x) = 0$ for all $x \in J^\times$. Otherwise, (a) yields a least positive integer $m \in \Gamma := \lambda(J^\times)$, and we have $\mathbb{Z}m \subseteq \Gamma$. Conversely, let $x \in J^\times$. Then $\lambda(x) \in \mathbb{Z}$ can be written as $\lambda(x) = (2i + j)m + l$, with $i, j, l \in \mathbb{Z}$, $j = 0, 1$, $0 \leq l < m$. This implies $jm + l = -(2im - \lambda(x)) \in \Gamma$ since $\Gamma$ by (2) and (a) is closed under the operation $(\alpha, \beta) \mapsto 2\alpha - \beta$. If $j = 0$, we conclude $l \in \Gamma$, hence $l = 0$ by the minimality of $m$. On the other hand, if $j = 1$, we conclude $m - l = (2m - (m + l)) \in \Gamma$, forcing again $l = 0$ by the minimality of $m$. In any event, $\lambda(x) = (2i + j)m \in \mathbb{Z}m$, which completes the proof.

(e) We have to verify (1)–(3) and do so by a straightforward computation: For $x, y \in J$ we obtain

$$\begin{aligned}
\lambda^{(p)}(x) = \infty &\iff \lambda(p) + \lambda(x) = \infty \iff \lambda(x) = \infty \iff x = 0,\\
\lambda^{(p)}(U_x^{(p)}y) &= \lambda(p) + \lambda(U_x U_p y) = \lambda(p) + 2\lambda(x) + 2\lambda(p) + \lambda(y)\\
&= 2(\lambda(p) + \lambda(x)) + (\lambda(p) + \lambda(y)) = 2\lambda^{(p)}(x) + \lambda^{(p)}(y),\\
\lambda^{(p)}(x + y) &= \lambda(p) + \lambda(x + y) \geq \lambda(p) + \min\{\lambda(x), \lambda(y)\}\\
&= \min\{\lambda(p) + \lambda(x), \lambda(p) + \lambda(y)\} = \min\{\lambda^{(p)}(x), \lambda^{(p)}(y)\},
\end{aligned}$$

and finally,

$$\begin{aligned}
(\lambda^{(p)})^{(q)}(x) &= \lambda^{(p)}(q) + \lambda^{(p)}(x) = \lambda(p) + \lambda(q) + \lambda(p) + \lambda(x) = 2\lambda(p) + \lambda(q) + \lambda(x)\\
&= \lambda(U_p q) + \lambda(x) = \lambda^{(U_p q)}(x).
\end{aligned}$$

(f) There is clearly no harm in assuming $x, y, z \in J^\times$. Suppose first that the assertion holds for $y = 1_J$, so we have

$$\lambda(x \circ z) \geq \lambda(x) + \lambda(z) \qquad (x, z \in J), \tag{s1}$$

and let $y \in J^\times$ be arbitrary. Then we pass to the $y$-isotopes $J^{(y)}$ and $\lambda^{(y)}$ and combine (31.8.5) with (s1) to conclude

$$\lambda(y) + \lambda(\{xyz\}) = \lambda^{(y)}(x \circ^{(y)} z) \geq \lambda^{(y)}(x) + \lambda^{(y)}(z) = 2\lambda(y) + \lambda(x) + \lambda(z).$$

Hence (4) follows. We are thus reduced to the case $y = 1_J$ and have to prove (s1). Fixing $x \in J^\times$ and letting $z \in J^\times$ be arbitrary, the estimate

$$\begin{aligned}
\lambda(x \circ z) = \lambda(U_{x,1_J} z) &= \lambda(U_{x+1_J} z - U_x z - z) \\
&\geq \min\{2\lambda(x + 1_J) + \lambda(z), 2\lambda(x) + \lambda(z), \lambda(z)\} \\
&\geq \min\{2\lambda(x), 0\} + \lambda(z) = \min\{\lambda(x), -\lambda(x)\} + \lambda(x) + \lambda(z) \\
&= \lambda(x) + \lambda(z) - \max\{\lambda(x), -\lambda(x)\} = \lambda(x) + \lambda(z) - |\lambda(x)|
\end{aligned}$$

shows that there exists a constant $\kappa \geq 0$, depending on $x$, such that

$$\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \kappa \qquad (z \in J^\times). \tag{s2}$$

We now consider (29a.15) for $z$ in place of $y$ and apply the result to $1_J$. Then

$$(x \circ z)^2 + z \circ U_x z = U_x z^2 + U_z x^2 + 2x \circ U_z x,$$

which in turn may be combined with (29a.17) to yield

$$(x \circ z)^2 = U_x z^2 + U_z x^2 + x \circ U_z x.$$

This and (s2) imply

$$\begin{aligned}
2\lambda(x \circ z) = \lambda((x \circ z)^2) &= \lambda(U_x z^2 + U_z x^2 + x \circ U_z x) \\
&\geq \min\{2(\lambda(x) + \lambda(z)), 2(\lambda(z) + \lambda(x)), \lambda(x \circ U_z x)\} \\
&\geq \min\{2(\lambda(x) + \lambda(z)), 2(\lambda(x) + \lambda(z)) - \kappa\} \\
&= 2(\lambda(x) + \lambda(z)) - \kappa.
\end{aligned}$$

Thus

$$\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \frac{\kappa}{2} \qquad (z \in J^\times),$$

and iterating this procedure, we end up with

$$\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \frac{\kappa}{2^n} \qquad (z \in J^\times, n \in \mathbb{N}).$$

Hence, as $n \to \infty$, we arrive at (s1).

**31.39** (a) Since $J$ by Thm. 30.11 is locally linear, $F[x] \subseteq J$ is a commutatuve

associative $F$-algebra. Every $y \neq 0$ in $F[x]$ is invertible in $J$ and hence $U_y\colon J \to J$ is bijective (Prop. 31.2). Thus $U_y$ via restriction induces a linear injection $F[x] \to F[x]$, and a dimension argument shows that $U_y\colon F[x] \to F[x]$ is, in fact, bijective. Since, therefore, $y \in F[x]^\times$, it follows that $F[x]/F$ is indeed a finite algebraic field extension.

(b) For $x \in J$, the finite algebraic field extension $F[x]/F$ has degree 1 since $F$ is algebraically closed. Hence $J = F \cdot 1_J$.

(c) For $x \in J$, the finite algebraic field extension $\mathbb{R}[x]/\mathbb{R}$ has degree at most 2. Thus $1_J, x, x^2$ are linearly independent, and invoking Exc. 16.21, we conclude that $J$ (viewed as a linear Jordan algebra with bilinear product $xy$) is conic. Writing $q$ for its norm and $M$ for its underlying real vector space, $(M, q, e)$, $e := 1_J$, is a pointed quadratic module over $\mathbb{R}$. Now (29b.9) and (27.9.1) imply $J = J(M, q, e)$. Since by Exc. 31.33, therefore, $q$ is anisotropic, it is either positive or negative definite. The latter alternative being excluded since $q(e) = 1 > 0$, the problem is solved.

## Solutions for Section 32

**32.18** Let $f = \sum_{i\geq 0} \alpha_i \mathbf{t}^i \in k[\mathbf{t}]$ and suppose $f(c) = 0$. By Prop. 30.6, we must show $(\mathbf{t}f)(c) = 0$. With $d := 1_J - c$ and $\alpha := \sum_{i\geq 1} \alpha_i \in k$ we have $0 = f(c) = \alpha_0 1_J + \alpha c = (\alpha_0 + \alpha)c + \alpha_0 d$, and since $c, d$ are orthogonal idempotents, we conclude $(\alpha_0 + \alpha)c = \alpha_0 d = 0$, hence $(\mathbf{t}f)(c) = (\sum_{i\geq 0} \alpha_i)c = (\alpha_0 + \alpha)c = 0$, as desired.

**32.19** Write $J_i := J_i(c)$ for $i = 0, 1, 2$ and put $d := 1_J - c$. Applying (32.2.8), we see that $U_v$ maps $J_2$ to $J_0$, hence via restriction induces a linear map $\varphi\colon J_2 \to J_0$. Write $w := v^{-1}$ as $w = w_2 + w_1 + w_0$, $w_i \in J_i$ for $i = 0, 1, 2$. Then (31.2.1) and (32.2.8) again yield

$$v = U_v w = U_v w_2 + U_v w_1 + U_v w_0, \quad U_v w_i \in J_{2-i} \qquad (i = 0, 1, 2).$$

Comparing Peirce components and using bijectivity of $U_v$ (Prop. 31.2), we conclude $w_2 = w_0 = 0$. Thus $w \in J_1$, and by (32.2.8) combined with Cor. 32.3 (b) we have

$$w^2 = p + q, \quad p := U_w d \in J_2^\times, \quad q := U_w c \in J_0^\times, \tag{s1}$$

which implies

$$U_v p = d, \quad U_v q = c. \tag{s2}$$

Next,writing $p^{-1}$ (resp. $q^{-1}$) for the inverse of $p$ (resp. $q$) in $J_2$ (resp. $J_0$), we claim

$$U_v d = p^{-1}, \quad U_v c = q^{-1}. \tag{s3}$$

Indeed, from (s1), (s2), Cor. 32.3 (b) and Exc. 31.30 we deduce $U_q U_v c = U_q U_{v^2} q = U_q U_{(w^2)^{-1}} q = U_q U_{p^{-1}+q^{-1}} q = U_q U_{q^{-1}} q = U_q q^{-1}$, and since $U_q \colon J_0 \to J_0$ is bijective, the second equation of (s3) is proved. The first one follows analogously. In particular, $\varphi$, viewed as a linear map $J_2 \to J_0^{(q)}$ preserves units. But it also preserves $U$-operators since for $x, y \in J_2$ we may apply (s2) to obtain

$$U^{(q)}_{\varphi(x)}\varphi(y) = U_{U_v x} U_q U_v y = U_v U_x U_v U_q U_v y = U_v U_x U_{U_v q} y = \varphi(U_x U_c y) = \varphi(U_x y),$$

as claimed. Thus $\varphi \colon J_2 \to J_0^{(q)}$ is a homomorphism. Interchanging the role of $c$ and $d$, we also obtain a homotopy $\psi \colon J_0 \to J_2$ induced by $U_w = U_v^{-1}$. Hence $\varphi$ is bijective with inverse $\psi$, and we have established the first part of the exercise.

As to the second, $v^2 = 1_J$ implies $w = v$, and (s1) yields $p = c$, $q = d$. Hence $\varphi \colon J_2 \to J_0$ is an isomorphism. Conversely, let this be so. By what we have just shown, $1_{J_0} = \varphi(1_{J_2}) = q^{-1}$, forcing $q = d$. On the other hand, $\varphi^{-1} \colon J_0 \to J_2$ is an isomorphism induced by $U_{v^{-1}}$, and from (s1) we conclude $p = U_{v^{-1}} d = \varphi^{-1}(d) = c$. Now (s1) again implies first $w^2 = 1_J$ and then $v^2 = (w^2)^{-1} = 1_J$ as well.

**32.20** From (32.3.1) we deduce for $x \in J_2$ that $V_x$ stabilizes $J_1$, so the map $\varphi$ is well dfined and linear. Moreover, $\varphi(1_{J_2}) = \varphi(c) = \mathbf{1}_{J_1}$ by (32.2.7). Now let $x, y \in J_2$, $z \in J_1$. Then (29a.14) yields

$$U_{\varphi(x)}\varphi(y)z = V_x V_y V_x z = U_{x,y} V_x z + V_{x,y} V_x z,$$

where $U_{x,y} V_x z \in \{J_2 J_1 J_2\} = \{0\}$ by (32.2.9).Applying (29a.19), we therefore conclude

$$U_{\varphi(x)}\varphi(y)z = V_{x,y} V_x z = V_{U_x y} z + U_x V_y z = V_{U_x y} z$$

since $U_x V_y z \in U_{J_2} J_1 = \{0\}$ by (32.2.8). Thus $\varphi$ is a homomorphism of Jordan algebras, and the first part of the problem is solved. Moreover, if $J_2$ is simple and $J_1 \neq \{0\}$, then $\mathrm{Ker}(\varphi) \subseteq J$ is an ideal $\neq J_2$ since $\varphi(c) = \mathbf{1}_{J_1} \neq 0$. Thus $\mathrm{Ker}(\varphi) = \{0\}$ and $\varphi$ is injective.

**32.21** (ii) $\Rightarrow$ (i). Clear.

(i) $\Rightarrow$ (ii). We may assume

$$\{i, j\} \cap \{l, m\} \neq \emptyset \tag{s1}$$

and then consider the following cases.

*Case 1:* $\{i, j\} \cap \{l, m\} \cap \{n, p\} = \emptyset$. We may assume $l = j$ by (s1), and since

$T$ is not connected, we have $m \neq n, p$ but also $j \neq n, p$ since we are in Case 1. Thus $T = (np, jm, ij)$ with $\{n, p\} \cap \{j, m\} = \emptyset$, as in the first alternative of (ii).

*Case 2:* $\{i, j\} \cap \{l, m\} \cap \{n, p\} \neq \emptyset$. Then we may assume $n = l = j$, and since $T = (ij, jm, jp)$ is not connected, we necessarily have $m \neq i, j, p$. The first part of the problem is thereby solved.

Now let $T = (ij, jl, ij)$ be as in the second part of the problem. If $i \neq l \neq j$, the first part of the problem shows that $T$ is not connected. Conversely, if $l = i$ or $l = j$, then $T$ is clearly connected and there is a unique positive integer $m$ having $ij = \{i, j\} = \{l, m\} = lm$.

**32.22** Let $R := k[\mathbf{t}_1^{\pm 1}, \ldots, \mathbf{t}_r^{\pm 1}]$ be the ring of Laurent polynomials in the variable $\mathbf{t}_1, \ldots, \mathbf{t}_r$. As in the proof of Thm. 32.15 (c), we have

$$A \subseteq A_R = \bigoplus_{i_1,\ldots,i_r \in \mathbb{Z}} (\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} A),$$

$$\mathrm{End}_k(A) \subseteq \mathrm{End}_k(A_R) = \bigoplus_{i_1,\ldots,i_r \in \mathbb{Z}} (\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} \mathrm{End}_k(A)) \subseteq \mathrm{End}_R(A_R).$$

(a) First of all, we have

$$\mathbf{1}_A = L_{1_A} R_{1_A} = L_{\sum c_i} R_{\sum c_j} = \sum_{i,j=1}^{r} L_{c_i} R_{c_j} = \sum_{i,j=1}^{r} E_{ij}.$$

It remains to show that the $E_{ij}$ are orthogonal projections. Since every base change of $A$ is flexible, we conclude

$$\sum_{i,j=1}^{r} \mathbf{t}_i \mathbf{t}_j L_{c_i} R_{c_j} = L_{\sum \mathbf{t}_i c_i} R_{\sum \mathbf{t}_j c_j} = R_{\sum \mathbf{t}_j c_j} L_{\sum \mathbf{t}_i c_i} = \sum_{i,j=1}^{r} \mathbf{t}_i \mathbf{t}_j R_{c_j} L_{c_i},$$

and comparing coefficients yields

$$E_{ij} = L_{c_i} R_{c_j} = R_{c_j} L_{c_i} \qquad (1 \leq i, j \leq r). \tag{s1}$$

Similarly,

$$\sum_{i=1}^{r} \mathbf{t}_i^2 L_{c_i} = L_{\sum \mathbf{t}_i^2 c_i} = L_{(\sum \mathbf{t}_i c_i)^2} = L^2_{\sum \mathbf{t}_i c_i} = (\sum_{i=1}^{r} \mathbf{t}_i L_{c_i})^2 = \sum_{i,j=1}^{r} \mathbf{t}_i \mathbf{t}_j L_{c_i} L_{c_j}$$

and the analogous relation for the right multiplication imply

$$L_{c_i} L_{c_j} = \delta_{ij} L_{c_i}, \quad R_{c_i} R_{c_j} = \delta_{ij} R_{c_i} \qquad (1 \leq i, j \leq r). \tag{s2}$$

Given $i, j, l, m = 1, \ldots, r$, we now apply (s1), (s2) and obtain

$$E_{ij} E_{lm} = L_{c_i} R_{c_j} R_{c_m} L_{c_l} = \delta_{jm} L_{c_i} R_{c_j} L_{c_l} = \delta_{jm} L_{c_i} L_{c_l} R_{c_j} = \delta_{il} \delta_{jm} L_{c_i} R_{c_j} = \delta_{il} \delta_{jm} E_{ij}.$$

Hence the $E_{ij}$ are orthogonal projections of $A$, as claimed.

(b) Let $1 \le i, j \le r$ and $x \in A_{ij}$. For $1 \le l \le r$, we apply (s2) to obtain

$$c_l x = L_{c_l} E_{ij} x = L_{c_l} L_{c_i} R_{c_j} x = \delta_{il} E_{ij} x = \delta_{il} x$$

and, similarly, $xc_l = \delta_{jl} x$. Thus the left-hand side of (3) is contained in the right. Conversely, let $x \in A$ and assume $c_l x = \delta_{il} x$, $xc_l = \delta_{jl} x$ for $l = 1, \dots, r$. Then this holds, in particular, for $l = i$ and $l = j$, which implies $E_{ij} x = c_i(xc_j) = x$, hence $x \in A_{ij}$. This completes the proof of (b).

(c) Since $\mathbf{t}_\lambda \in R^\times$ for $1 \le \lambda \le r$, we have

$$w := \sum_{\lambda=1}^{r} \mathbf{t}_\lambda c_\lambda \in J_R^\times, \quad w^{-1} = \sum_{\lambda=1}^{r} \mathbf{t}_\lambda^{-1} c_\lambda. \tag{s3}$$

For $1 \le i, j \le r$, we now claim

$$A_{ij} = \{x \in A \mid L_w x = \mathbf{t}_i x, \;\; R_w x = \mathbf{t}_j x\} = \{x \in A \mid L_{w^{-1}} x = \mathbf{t}_i^{-1} x, \;\; R_{w^{-1}} x = \mathbf{t}_j^{-1} x\}, \tag{s4}$$

where the second equation follows from the first since $L_{w^{-1}} = L_w^{-1}$, $R_{w^{-1}} = R_w^{-1}$ by (13.6.2). In order to prove the first, we decompose $x$ as $x = \sum x_{lm}$, $x_{lm} \in A_{lm}$ and apply (3) to obtain

$$L_w x = \sum_{\lambda,l,m} \mathbf{t}_\lambda c_\lambda x_{lm} = \sum_{l,m} \mathbf{t}_l x_{lm}, \quad R_w x = \sum_{\lambda,l,m} \mathbf{t}_\lambda x_{lm} c_\lambda = \sum_{l,m} \mathbf{t}_m x_{lm}. \tag{s5}$$

Thus $L_w x = \mathbf{t}_i x$ and $R_w x = \mathbf{t}_j x$ if and only if $x = x_{ij}$, which completes the proof (s4). In analogy to the proof of Thm. 32.15, we now put

$$T := \{\mathbf{t}_1^{i_1} \cdots \mathbf{t}_r^{i_r} \mid i_1, \dots, i_r \in \mathbb{Z}\}, \quad T_1 := \{\mathbf{t}_1, \dots, \mathbf{t}_r\}$$

and claim:

(∗) If $s, t \in T$ admit an element $x \ne 0$ in $A$ such that $L_w x = sx$ and $R_w x = tx$, then $s, t \in T_1$.

In order to see this, write $x = \sum x_{lm}$, $x_{lm} \in A_{lm}$. Then (s5) implies

$$\sum_{l,m} s x_{lm} = sx = L_w x = \sum_{l,m} \mathbf{t}_l x_{lm}, \quad \sum_{l,m} t x_{lm} = tx = R_w x = \sum_{l,m} \mathbf{t}_m x_{lm},$$

and comparing components yields unique indices $i, j = 1, \dots, r$ satisfying $s = \mathbf{t}_i$, $t = \mathbf{t}_j$ and $x = x_{ij}$.

For $1 \le i, j, l, m \le r$, $x_{ij} \in A_{ij}$, $y_{lm} \in A_{lm}$, we now obtain

$$L_w(x_{ij} y_{lm}) = \mathbf{t}_i \mathbf{t}_j \mathbf{t}_l^{-1} x_{ij} y_{lm}, \quad R_w(x_{ij} y_{lm}) = \mathbf{t}_j^{-1} \mathbf{t}_l \mathbf{t}_m x_{ij} y_{lm} \tag{s6}$$

since the left and right Moufang identities (13.3.1) and (13.3.2) combined with (13.6.2) and (s4) imply

$$L_w(x_{ij}y_{lm}) = w\Big(x_{ij}(w(w^{-1}y_{lm}))\Big) = (wx_{ij}w)(w^{-1}y_{lm}) = \mathbf{t}_i\mathbf{t}_j\mathbf{t}_l^{-1}x_{ij}y_{lm},$$
$$R_w(x_{ij}y_{lm}) = \Big(((x_{ij}w^{-1})w)y_{lm}\Big)w = (x_{ij}w^{-1})(wy_{lm}w) = \mathbf{t}_j^{-1}\mathbf{t}_l\mathbf{t}_m x_{ij}y_{lm},$$

as claimed. Specializing $l \mapsto j$, $m \mapsto l$ in (s6) yields $L_w(x_{ij}y_{jl}) = \mathbf{t}_i x_{ij}y_{jl}$, $R_w(x_{ij}y_{jl}) = \mathbf{t}_l x_{ij}y_{lj}$, hence (4). Similarly, (s6) for $l = i$, $m = j$ yields (5), while (6) follows from (∗) and (s6) since $j \neq l$ and $(i, j) \neq (l, m)$ imply that $\mathbf{t}_i\mathbf{t}_j\mathbf{t}_l^{-1}$ or $\mathbf{t}_j^{-1}\mathbf{t}_l\mathbf{t}_m$ does not belong to $T_1$. Finally, for $1 \leq i, j \leq r$, $i \neq j$, and $x \in A_{ij}$, we apply (5) to obtain $x^2 \in A_{ji}$. But then (s1), (3) and right alternativity yield $x^2 = E_{ji}x^2 = R_{c_i}L_{c_j}x^2 = ((c_jx)x)c_i = 0$, as claimed.

(d) Write $E_{ij}^{(+)}$, $1 \leq i \leq j \leq r$, for the Peirce projections of $\Omega$, viewed as a complete orthogonal system of idempotents in $A^{(+)}$. Comparing (32.12.1) with (s1), we let $1 \leq i \leq j \leq r$ and conclude

$$E_{ii}^{(+)} = U_{c_i} = L_{c_i}R_{c_i} = E_{ii}, \quad E_{ij}^{(+)} = U_{c_i,c_j} = L_{c_i}R_{c_j} + L_{c_j}R_{c_i} = E_{ij} + E_{ji}.$$

The assertion follows.

**32.23** Since the Peirce triples $(ij, ii, ij)$ and $(ij, jj, ij)$ are connected, (32.15.6) implies $U_{v_{ij}}J_{ii} \subseteq J_{jj}$ and $U_{v_{ij}}J_{jj} \subseteq J_{ii}$.

(a) (i) ⇒ (ii). Applying Exc. 32.19 to $J' := J_2(c_i + c_j)$, we conclude that $U_{v_{ij}}\colon J_{ii} \to J_{jj}$ is an isotopy. The first inclusion of (ii) now follows from Prop. 31.5 combined with Thm. 31.10 (a). The second one follows by symmetry.

(a) (ii) ⇒ (iii). Clear since $c_i \in J_{ii}^\times$ and $c_j \in J_{jj}^\times$.

(a) (iii) ⇒ (iv). Since the Peirce triples $(ij, ll, ij)$ are not connected for $l = 1, \ldots, r$, $i \neq l \neq j$, we have $v_{ij}^2 = \sum_{l=1}^r U_{v_{ij}}c_l = U_{v_{ij}}c_i + U_{v_{ij}}c_j \in (J_{ii} \oplus J_{jj})^\times$ (by (iii)) $\subseteq J'^\times$, and this is (a) (iv). Basically the same argument also yields (b) (i) ⇒ (b) (ii), while (b)(ii) ⇒ (b) (i) is obvious.

(a) (iv) ⇒ (i). By definition (31.1), invertibility in a Jordan subalgebra implies invertibility in the ambient Jordan algebra, while by Prop. 31.3 (b), invertibility of $x^2 = U_x1_J$ implies invertibility of $x$.

(c) (29a.7) for $x = v_{ij}$, $y = v_{jl}$, $z = 1_J$ yields

$$U_{v_{ij}\circ v_{jl}}c_i = U_{v_{ij}}U_{v_{jl}}c_i + U_{v_{jl}}U_{v_{ij}}c_i + V_{v_{ij}}U_{v_{jl}}V_{v_{ij}}c_i - U_{U_{v_{ij}}v_{jl},v_{jl}}c_i. \tag{s1}$$

Since $i, j, l$ are mutually distinct, the Peirce triples $(jl, ii, jl)$, $(jl, ij, jl)$ and $(ij, jl, ij)$ are not connected. Moreover, $V_{v_{ij}}c_i = c_i \circ v_{ij} = v_{ij}$ by (32.15.3) and (32.2.6). Summing up, therefore, (s1) collapses to $U_{v_{ij}\circ v_{jl}}c_i = U_{v_{jl}}U_{v_{ij}}c_i$ and, similarly, $U_{v_{ij}\circ v_{jl}}c_l = U_{v_{ij}}U_{v_{jl}}c_l$. Combining this with the characterization of (strong) connectedness in (a) (resp. (b)), the assertion follows.

**32.24** (a) Free use will be made of the Peirce multiplication rules assembled in the present section. Let $1 \le i, j \le r$. Setting $d_\lambda := c_\lambda^{(p)}$ for $\lambda = 1, \dots, r$, we apply (31.8.8) and deduce $d_i^{(2,p)} = U_{p_i^{-1}} \sum_{\lambda=1}^r p_\lambda = p_i^{-1} = d_i$, so $d_i$ is an idempotents in $J^{(p)}$. Now assume $i \neq j$ Since (1) is a direct sum of ideals, we obtain $U_{d_i}^{(p)} d_j = U_{d_i} U_{\sum p_\lambda} p_j^{-1} = U_{d_i} p_j = 0$, while (31.8.5) yields $d_i \circ^{(p)} d_j = \{d_i p d_j\} = 0$. Thus the idempotents $d_i, d_j$ are orthogonal in $J^{(p)}$ ((32.2.5) and Prop. 32.9). The equation $\sum_{\lambda=1}^r d_\lambda = p^{-1} = 1_{J^{(p)}}$ shows, therefore, that $\Omega^{(p)}$ is a complete orthogonal system of idempotents in $J^{(p)}$. Write $E_{lm}$ (resp. $E_{lm}^{(p)}$) for the Peirce projections of $\Omega$ in $J$ (resp. $\Omega^{(p)}$ in $J^{(p)}$). Then $E_{lm}^{(p)} = E_{lm} U_p$ by (32.12.1), hence $J_{ij}^{(p)} = E_{ij} U_p J = E_{ij} J = J_{ij}$, and the proof of (a) is complete.

(b) For $1 \le i \le r$ we have $(c_i^{(p)})^{(q)} = q_i^{(-1,p_i)} = U_{p_i^{-1}} q_i^{-1} = (U_{p_i} q_i)^{-1}$, and the assertion follows.

(c) Suppose $v_{1i} \in J_{1i}$ connects $c_1$ and $c_i$ for $2 \le i \le r$. By Exc. 32.23 (a) we have $p_i := U_{v_{1i}} c_1 \in J_{ii}^\times$. Put $p_1 := c_1 \in J_{11}^\times$ and $p := \sum_{\lambda=1}^r p_\lambda \in \mathrm{Diag}_\Omega(J)^\times$. By the solution to Exc. 32.19, $w_{1i} := v_{1i}^{-1}$ (the inverse of $v_{1i}$ in $J_2(c_1 + c_i)$), belongs to $J_{1i} = J_{1i}^{(p)}$ and satisfies $U_{w_{1i}} p_i = c_1$. Note that $v_{1i}^2 = q_{i1} + p_i$, for some $q_{i1} \in J_{11}^\times$ and hence $w_{1i}^2 = q_{i1}^{-1} + p_i^{-1}$. Hence (31.8.8) implies

$$\begin{aligned} w_{1i}^{(2,p)} &= U_{w_{1i}} p = U_{w_{1i}}(p_1 + p_i) = U_{w_{1i}} p_i + U_{w_{1i}} c_1 = c_1 + U_{w_{1i}^2} p_i = c_1 + U_{p_i^{-1}} p_i \\ &= c_1 + p_i^{-1} = c_1^{(p)} + c_i^{(p)}. \end{aligned}$$

Thus $c_1^{(p)}$ and $c_i^{(p)}$ are strongly connected by $w_{1i} \in J_{1i}^{(p)}$.

**32.25** We argue by induction on $r$. For $r = 1$, the assertion agrees with Exc. 28.22 (c). Now let $r > 1$ and assume the statement holds for $r - 1$ in place of $r$. Put $c' := c'_r$ and use Exc. 28.22 (c) again to find an idempotent $c = c_r \in J$ satisfying $\varphi(c) = c'$. Write $E_i$ (resp. $J_i$) for the Peirce projections (resp. components) of $J$ relative to $c$ and $E'_i$ (resp. $J'_i$) for the Peirce projections (resp. components) of $J'$ relative to $c'$, where $i = 0, 1, 2$. We have $\varphi \circ E_i = E'_i \circ \varphi$ and hence $\varphi(J_i) = (\varphi \circ E_i)(J) = E'_i \circ \varphi(J) = E'_i(J') = J'_i$. In particular, $\varphi_0 := \varphi|_{J_0} \colon J_0 \to J'_0$ is a surjective homomorphism of Jordan algebras whose kernel, $\mathrm{Ker}(\varphi_0) = J_0 \cap \mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\varphi)$ is a nil ideal in $J_0$. Moreover, $J'_0$ contains $(c'_1, \dots, c'_{r-1})$ as a complete orthogonal system of idempotents. Hence the induction hypothesis yields a complete orthogonal system $(c_1, \dots, c_{r-1})$ of idempotents in $J_0$ such that $\varphi(c_i) = c'_i$ for $1 \le i < r$. By Prop. 32.9 and Cor. 32.10, therefore, $(c_1, \dots, c_{r-1}, c_r)$ is a complete orthogonal system of idempotents in $J$ with the desired properties.

**32.26** Write $t$ for the trace and $x \mapsto \bar{x}$ for the conjugation of $(M, q, e)$. Let $I \subset J := J(M, q, e)$ be an ideal that remains stable under conjugation. We claim $I = \{0\}$. In order to see this, let $x \in I$. Then $I$ contains $U_x \bar{x}^2 = q(x)^2 1_J$

(by (29b.10)), and from $I \neq J$ we deduce $q(x) = 0$. Linearizing this, we obtai $q(x,y) = 0$ for all $y \in I$. Now let $y \in J \setminus I$. Since $\bar{x} \in I$ and $I \subset J$ is an ideal, $U_y\bar{x} = q(x,y)y - q(y)x$ belongs to $I$. But so does the second summand on the right of this expression, and we conclude $q(x,y)y \in I$, hence $q(x,y) = 0$. Summing up, we have shown $x \in \mathrm{Rad}(q) = \{0\}$, and our intermediate claim $I = \{0\}$ is proved.

Now assume that $J$ is not simple and let $I$ be any proper ideal of $J$. Then so is $\bar{I}$, and the ideals $I \cap \bar{I}$, $I + \bar{I}$ are stable under conjugation. This and our intermediate assertion imply $J = I \oplus \bar{I}$ as a direct sum of ideals. As observed in 28.7, $I$ and $\bar{I}$ are Jordan algebras in their own right such that the conjugation induces an isomorphism from $I$ onto $\bar{I}$. Put $c := 1_I$. Then $\bar{c} = 1_{\bar{I}}$ and $1_J = c + \bar{c}$. Moreover, $c$ and $\bar{c}$ are idempotents in $J$, and the assumption $q(c) = 1$ would imply $c \in J^\times$ (Exc. 31.33), hence $c = 1_J$, $\bar{c} = 0$, a contradiction. Hence $q(c) = 0$ (since $q(c) \in F$ by (29b.12) is an idempotent), and (29b.6) reduces to $0 \neq c = c^2 = t(c)c$. Taking traces, we conclude $0 \neq t(c) = t(c)^2$, hence $t(c) = 1$. Summing, we have shown that $c$ and $\bar{c}$ are elementary idempotents of $J$, whence the corresponding Peirce decomposition by Prop. 32.8 implies $I = J_2(c) = Fc$, $\bar{I} = J_0(c) = F\bar{c}$. Thus the assignment $(\alpha,\beta) \mapsto \alpha c + \beta\bar{c}$ defines an isomorphism from $(F \times F)^{(+)}$ onto $J$.

# Solutions for Chapter VI

## Solutions for Section 33

**33.13** (a) For $x \in X$, the assignment $y \mapsto N(x,y)$ defines linear form on $X$. By regularity, therefore, we find a unique element $x^\sharp \in X$ such that $T(x^\sharp, y) = N(x,y)$ for all $y \in X$. On the other hand, given $y \in X$, the assignment $x \mapsto N(x, y_R)$ for $R \in k$-**alg**, $x \in X_R$ defines a polynomial law $N(-,y)\colon X \to k$ which is homogeneous of degree 2, hence a quadratic form (Exc. 12.33 (b)). But then $x \mapsto x^\sharp$ must be a quadratic map since $T$ is regular, and the gradient identity holds in all scalar extensions. Next we prove that $X$ together with $1, \sharp, N$ is a cubic array. By Euler's differential equation and Exc. 12.40, (3), we have $T(1,y) = N(1,1)N(1,y) - N(1,1,y) = 3N(1,y) - 2N(1,y) = N(1,y)$, which implies $1^\sharp = 1$, as claimed. To finish the proof of (a), it remains to establish the unit identity. Linearizing the gradient identity, we conclude $T(x \times y, z) = N(x,y,z)$ is totally symmetric in $x,y,z \in X$, where as usual $x \times y$ is the bilinearization of the adjoint. Hence

$$\begin{aligned} T(x, 1 \times y) = T(x \times y, 1) = N(1,x,y) = N(1,x)N(1,y) - T(x,y) = T(x)T(y) - T(x,y) \\ = T(x, T(y)1 - y), \end{aligned}$$

and the unit identity follows again from regularity of $T$.

(b) Let $1'$, $N'$, $T'$ be the base point, norm, bilinear trace, respectively, of $X'$. We first show that $X'$ is regular. Since $\varphi$ is linear, the chain rule in the form (12.17.5) implies $N'(\varphi(x), \varphi(y)) = N(x,y)$ and then $N'(\varphi(x), \varphi(y), \varphi(z)) = N(x,y,z)$ in all scalar extensions of $X$. Since $\varphi$ also preserves base points, it therefore preserves bilinear traces as well: $T'(\varphi(x), \varphi(y)) = T(x,y)$. Now let $x' \in \mathrm{Rad}(T')$ and write $x' = \varphi(x)$ for some $x \in X$. Then $T(x,y) = T'(\varphi(x), \varphi(y)) = 0$ for all $y \in X$, hence $x = 0$ since $T$ is regular. On the other hand, let $\lambda'\colon X' \to k$ be a linear form. Then so is $\lambda := \lambda' \circ \varphi\colon X \to k$,

and regularity of $T$ yields an element $x \in X$ such that $\lambda = T(x, -)$. Since $\varphi$ is surjective, this implies $\lambda' = T'(\varphi(x), -)$, and we have shown that $X'$ is indeed regular.

For $x \in \mathrm{Ker}(\varphi)$, $y \in X$ we have $T(x, y) = T'(\varphi(x), \varphi(y)) = 0$, hence $x = 0$ since $T$ is regular. Thus, $\varphi$ is injective and, altogether, bijective. On the other hand, the gradient identity gives

$$T'(\varphi(x^\sharp), \varphi(y)) = T(x^\sharp, y) = N(x, y) = N'(\varphi(x), \varphi(y)) = T'(\varphi(x)^{\sharp'}, \varphi(y)),$$

and regularity of $T'$ combines with the surjectivity of $\varphi$ to yield $\varphi(x^\sharp) = \varphi(x)^{\sharp'}$, as claimed.

**33.14** If $X$ is a cubic norm structure over $k$, then (1)–(3) hold by definition, while (4), (5) have been recorded in (33a.10), (33a.8), respectively. Conversely, suppose (1)–(5) hold for all $x, y, z \in X$ and let $R \in k$-**alg**. Since (1), (2), (4) are homogeneous of degree at most 2 in each variable, they continue to hold in $X_R$, so it remains to verify (3), (5) over $R$. We first linearize (2) to conclude that $T(x \times y, z) = N(x, y, z)$ is totally symmetric in $x, y, z \in X$. Hence linearizing (4) with respect to $y$ implies

$$x^\sharp \times (y \times z) + (x \times y) \times (x \times z) = T(x^\sharp, y)z + T(x^\sharp, z)y + T(x \times y, z)x \qquad \text{(s1)}$$

for all $x, y, z \in X$. Turning now to the proof of (5), linearity allows us to assume $y = v_R$ for some $v \in X$; we then put

$$M := \{x \in X_R \mid x^\sharp \times (x \times y) = T(x^\sharp, y)x + N(x)y\}.$$

By homogeneity, we have $rx \in M$ for all $x \in M$, $r \in R$. Moreover, for $u \in X$, the validity of (5) over $X$ yields

$$\begin{aligned}(u_R)^\sharp \times (u_R \times v_R) &= (u^\sharp)_R \times (u_R \times v_R) = \big(u^\sharp \times (u \times v)\big)_R \\ &= \big(T(u^\sharp, v)u + N(u)v\big)_R = T((u_R)^\sharp, v_R)u_R + N_R(u_R)v_R,\end{aligned}$$

hence $u_R \in M$. But the elements $u_R$, with $u \in X$, span $X_R$ as an $R$-module. Therefore (5) will hold in all of $X_R$ once we have shown that $M$ is closed under addition. In order to do so, let $x, z \in M$. Then the definition of $M$ and (s1) yield

$$\begin{aligned}(x + z)^\sharp \times ((x + z) \times y) &= (x^\sharp + x \times z + z^\sharp) \times (x \times y + z \times y) \\ &= x^\sharp \times (x \times y) + x^\sharp \times (z \times y) + (x \times z) \times (x \times y) + \\ &\quad (x \times z) \times (z \times y) + z^\sharp \times (x \times y) + z^\sharp \times (z \times y) \\ &= T(x^\sharp, y)x + N(x)y + T(x^\sharp, y)z + \\ &\quad T(x^\sharp, z)y + T(x \times y, z)x + T(z^\sharp, y)x + T(z^\sharp, x)y + \\ &\quad T(x \times y, z)z + T(z^\sharp, y)z + N(z)y\end{aligned}$$

$$\begin{aligned}
&= T(x^\sharp + x \times z + z^\sharp, y)x + T(x^\sharp + x \times z + z^\sharp, y)z + \\
&\quad (N(x) + T(x^\sharp, z) + T(x, z^\sharp) + N(z))y \\
&= T((x+z)^\sharp, y)(x+z) + N(x+z)y,
\end{aligned}$$

forcing $x + z \in M$, and the proof of (5) is complete. Now (3) will be treated in a similar manner by putting

$$M' := \{x \in X_R \mid x^{\sharp\sharp} = N(x)x\} \subseteq X_R.$$

Since both sides of (3) are homogeneous of the same degree, $N$ is stable under scalar multiplication: $x \in M'$ and $r \in R$ implies $rx \in M'$. Moreover, for $x \in X$ we conclude, using the fact that $N$ is a polynomial law,

$$(x_R)^{\sharp\sharp} = (x^{\sharp\sharp})_R = (N(x)x)_R = (N(x)1_R)x_R = N(x_R)x_R,$$

hence $x_R \in M'$. But the elements $x_R$, $x \in X$, span $X_R$ as an $R$-module. Therefore (3) will hold in all of $X_R$ once we have shown that $M'$ is closed under addition. In order to do so, let $x, y \in M'$. Then (2), (4), (5) and the definition of $M'$ imply

$$\begin{aligned}
(x+y)^{\sharp\sharp} &= (x^\sharp + x \times y + y^\sharp)^\sharp \\
&= x^{\sharp\sharp} + x^\sharp \times (x \times y) + x^\sharp \times y^\sharp + (x \times y)^\sharp + (x \times y) \times y^\sharp + y^{\sharp\sharp} \\
&= N(x)x + T(x^\sharp, y)x + N(x)y + T(x^\sharp, y)y + \\
&\quad T(x, y^\sharp)x + T(x, y^\sharp)y + N(y)x + N(y)y \\
&= (N(x) + T(x^\sharp, y) + T(x, y^\sharp) + N(y))(x+y) = N(x+y)(x+y),
\end{aligned}$$

forcing $x + y \in M'$, as desired.

**33.15** We first linearize (33a.28) and obtain

$$\begin{aligned}
&u \times (v \times w) + v \times (w \times u) + w \times (u \times v) \qquad \text{(s1)} \\
&\quad = (T(u)S(v,w) + T(v)S(w,u) + T(w)S(u,v) - T(u \times v, w))1 - \\
&\quad\quad (S(u,v)w + S(v,w)u + S(w,u)v) - \\
&\quad\quad (T(u)v \times w + T(v)w \times u + T(w)u \times v)
\end{aligned}$$

for all $u, v, w \in X$. We must show that the submodule $M \subseteq X$ spanned by the elements assembled in (1) is stable under the adjoint map. First of all, we have $1^\sharp = 1 \in M$ by the base point identities (33a.1) and $1 \times M \subseteq M$ by the unit identity (33a.3). Moreover, $M$ is spanned by the elements $1$, $s$, $t$, $s \times t$, $s \in \{x, x^\sharp\}$, $t \in \{y, y^\sharp\}$. Hence it will be enough to show that, for all $s, s' \in \{x, x^\sharp\}$,

$t, t' \in \{y, y^\sharp\}$,

$$s^\sharp, t^\sharp, (s \times t)^\sharp \in M, \tag{s2}$$

$$s \times s', s \times (s' \times t) \in M, \tag{s3}$$

$$t \times t', t \times (s \times t') \in M, \tag{s4}$$

$$(s \times t) \times (s' \times t') \in M. \tag{s5}$$

The adjoint identity (33a.5) implies $s^\sharp \in \{N(x)x, x^\sharp\}$, $t^\sharp \in \{N(y)y, y^\sharp\}$, hence not only the first two inclusions of (s2) but also $s^\sharp \times t^\sharp \in M$, while the third one now follows from (33a.10). In the first inclusion of (s3) we may assume $s = x$, $s' = x^\sharp$, whence the assertion follows from (14). The second relation of (s3) follows from (33a.28) for $s = s'$ and from (33a.19)), (33a.8) for $s \neq s'$. Next, (s4) is (s3) with $x$ and $y$ interchanged, so we are left with (s5). We first note that $1 \times M \subseteq M$ and (s3), (s4) imply

$$s \times M + t \times M \subseteq M. \tag{s6}$$

Then we combine (s1) with (s2)–(s4) to conclude

$$(s \times t) \times (s' \times t') \equiv -s' \times (t' \times (s \times t)) - t' \times ((s \times t) \times s') \bmod M,$$

and (s6) implies (s5).

## Solutions for Section 34

**34.18** (a) Since cubic Jordan algebras and cubic norm structures are identified via Cor. 34.6, $\varphi$ will be a homomorphism of cubic Jordan algebras once we have shown $N_{J'} \circ \varphi = N_J$ as polynomial laws over $k$. Moreover, since the entire set-up is stable under base change, applying Prop. 12.24 to the polynomial law $g := N_{J'} \circ \varphi \colon J \to k$, we see that it suffices to prove $N_{J'}(\varphi(x)) = N_J(x)$ for all $x \in J$ having $\varphi(x) \in J'^\times$. But then the adjoint identity combined with the fact that $\varphi$ preserves adjoints implies $N_J(x)\varphi(x) = \varphi(x^{\sharp\sharp}) = \varphi(x)^{\sharp\sharp} = N_{J'}(\varphi(x))\varphi(x)$, hence the assertion since $\varphi(x)$ by Thm. 34.3 (b) is unimodular.

(b) Since $\varphi$ preserves unit elements and norms, it is a surjective homomorphism of pointed cubic forms in the sense of Exc. 33.13. By part (b) of that exercise, therefore, $\varphi$ is an isomorphism of cubic arrays, hence of cubic Jordan algebras.

**34.19** Write $N = N_J$, $T = T_J$, $S = S_J$, $1 = 1_J$. By (33a.2), we have $3 = T(1) = 0$ in $k$, hence $2 = -1 \in k^\times$. Thus $J$ may be viewed as a linear Jordan algebra. Since not only the linear trace but also the quadratic one (by (33a.12)) and the

bilinear one (by (33a.13)) are identically zero, the bilinear multiplication of $J$ by 29.3 and (34.1.8) is given by

$$xy = \frac{1}{2}x \circ y = -x \circ y = -x \times y.$$

We conclude $x^2 = x^\sharp$ (which follows also from (34.1.7)), while (27.10.1) and (33.6.1) imply

$$2x(xy) - x^2y = U_x y = T(x,y)x - x^\sharp \times y = -x^\sharp \times y = x^2y,$$

hence the left alternative law $x(xy) = x^2y$. Being also commutative, $J$ is in fact alternative. Since the entire set-up is stable under base change, it remains to show $N(xy) = N(x)N(y)$ for all $x, y \in J$. By Artin's theorem (Cor. 14.5), the unital subalgebra of $J$ generated by $x, y$ is (commutative) associative. Hence (34.11.4) implies $N(xy)1 = (xy)^3 = x^3y^3 = N(x)N(y)1$, and since $1 \in J$ is unimodular, the assertion follows.

**34.20** Let $X$ be a rational cubic norm structure over $k$, with base point 1, adjoint $x \mapsto x^\sharp$, bilinearized adjoint $(x,y) \mapsto x \times y$, bilinear trace $T$ and norm $N$. Combining (1) and (3) with the bilinearity of $\times$, we conclude that $\sharp\colon X \to X$ is indeed a quadratic map with bilinearization $\times$. Beside the map $N\colon X \to k$, we now consider the map $g\colon X \times X \to k$ defined by $g(x,y) := T(x^\sharp, y)$ for $x, y \in X$. Since the adjoint is a quadratic map with bilinearization $\times$, we deduce from (2), (4), (5) that conditions (i)–(iv) of Exc. 12.43 hold for $(N, g)$, so $(N, g)\colon X \to k$ is a cubic map. By parts (d), (e) of that exercise, therefore, we find a unique cubic form $\tilde{N} := N * g\colon X \to k$ such that $\tilde{N}(x) = N(x)$ and $\tilde{N}(x,y) = T(x^\sharp, y)$ for all $x, y \in X$. Here (6) and (9) imply $1 = 1^{\sharp\sharp} = N(1)1$, hence $N(1) = 1$ since 1 is unimodular. Thus $X$ together with the base point 1, the adjoint $\sharp$ and the norm $\tilde{N}$ is a cubic array over $k$, denoted by $\tilde{X}$. Write $\tilde{T}$ (resp. $\tilde{S}$) for the (bi-)linear (resp. the quadratic) trace of $X$. In view of (9), we have $\tilde{T}(x) := \tilde{N}(1,x) = T(1,x)$ and $\tilde{S}(x) = \tilde{N}(x,1) = T(x^\sharp, 1)$ for $x \in X$, while Exc. 12.43 (b) implies $T(x \times y, z) = g(x,y,z) = T(x, y \times z)$ for all $x, y, z \in X$. Putting $x = 1$ and combining (33.2.10) with (10), we conclude $\tilde{T}(y,z) = \tilde{T}(y)\tilde{T}(z) - \tilde{S}(y,z) = T(1,y)T(1,z) - T(1, y \times z) = T(y,z)$. Thus $T$ is the bilinear trace of $\tilde{X}$. Hence equation (2) of Exc. 33.14 holds over $k$ But so do (1), (3)–(5) of that exercise, by (10), (6)–(8), respectively. Thus all equations of Exc. 33.14 hold over $k$, forcing the cubic array $\tilde{X}$ to be, in fact, a cubic norm structure.

If $\varphi\colon X \to Y$ is a homomorphism of rational cubic norm structures, then $\varphi : \tilde{X} \to \tilde{Y}$ is a linear map preserving base points and adjoints. By Exc. 34.18 (a), therefore, it is a homomorphism of cubic norm structures. Summing up, we have constructed a functor from $k$-**racuno** to $k$-**cuno**. Conversely, let $X$ be a cubic norm structure over $k$, with base point 1, adjoint $x \mapsto x^\sharp$, bilinear

trace $T$ and norm $N$. We claim that 1, $x \mapsto x^\sharp$, $(x,y) \mapsto x \times y$, $T$ and the set map $N_k\colon X \to k$ make $X$ a rational cubic norm structure over $k$, denoted by $\mathrm{Rat}(X)$, i.e., equations (1)–(10) hold. Indeed, (1)–(3) are obvious, while (4)–(10) have been established in this order in (33a.6), (33a.11), (33a.5), (33a.10), (33a.8), (33a.1), (33a.3), respectively. If $\varphi\colon X \to Y$ is a homomorphism of cubic norm structures, then $\varphi\colon \mathrm{Rat}(X) \to \mathrm{Rat}(Y)$ is trivially one of rational cubic norm structures. Thus we obtain a functor from $k$-**cuno** to $k$-**racuno** which by Exc. 12.43 (c) is easily seen to be inverse to the functor $k$-**racuno** $\to$ $k$-**cuno** constructed before. This completes the proof.

**34.21** (a) Let $x \in I$ and $y \in J$. If $(\mathfrak{a}, I)$ is a cubic ideal in $J$, then $I$ is an ordinary one, and (33a.22), (33a.23) and (33a.13) imply

$$x^\sharp = x^2 - T_J(x, 1_J)x + T_J(x^\sharp, 1_J)1_J, \quad x \times y = x \circ y - T_J(x)y - T_J(y)x + (T_J(x)T_J(y) - T_J(x,y))1_J,$$

which both belong to $I$ by (i), (ii). Hence (iv) holds. Conversely, if this is so, then (i), (ii), (iv) imply

$$U_x y = T_J(x,y)x - x^\sharp \times y \in I, \quad U_y x = T_J(y,x)y - y^\sharp \times x \in I,$$

so $I \subseteq J$ is an ordinary ideal and, therefore, $(\mathfrak{a}, I)$ is a cubic one.

(b) The first part follows immediately from 34.10. As to the second, let us assume that $\sigma$ is surjective. Since $1_{J_1'} \in J_1'$ is unimodular, there exists a linear form $\lambda'$ on $J_1'$ over $K'$ such that $\lambda'(1_{J_1'}) = 1_{K'}$. Put $\mathfrak{a} := \mathrm{Ker}(\sigma)$, $I := \mathrm{Ker}(\varphi)$, write $\bar\sigma\colon K/\mathfrak{a} \xrightarrow{\sim} K'$ for the isomorphism in $k$-**alg** induced by $\sigma$ and $\lambda\colon J_1 \to K/\mathfrak{a}$ for the $k$-linear map rendering the diagram

$$\begin{array}{ccc} J_1 & \xrightarrow[\varphi]{} & J_1' \\ {\scriptstyle\lambda}\,\vdots & & \downarrow{\scriptstyle\lambda'} \\ K/\mathfrak{a} & \xrightarrow[\bar\sigma]{\cong} & K' \end{array}$$

commutative. Then one checks that $\lambda$ is, in fact, $K$-linear, $\lambda(1_{J_1}) = 1_{K/\mathfrak{a}}$ and $\lambda(I) = \{0\}$. Hence the cubic ideal $(\mathfrak{a}, I)$ in $J_1$ is separated.

(c) For the rest of this exercise, we systematically abbreviate $1 = 1_J$, $T = T_J$, $S = S_J$, $\sharp = \sharp_J$, $N = N_J$. By (i), there is a unique way of viewing $J_0$ as a Jordan algebra over $k_0$ such that $\pi$ becomes a $\sigma$-semi-linear homomorphism of (abstract) Jordan algebras. The crux is to show that the Jordan algebra $J_0$ is derived from an appropriate cubic norm structure over $k_0$ making $\pi$ a $\sigma$-semi-linear homomorphism of *cubic* Jordan algebras. For this purpose, we consult

(iv) to obtain a unique map $\sharp_0 \colon X_0 \to X_0$ producing in

$$\begin{array}{ccc} J & \xrightarrow[\pi]{} & J_0 \\ {\scriptstyle\sharp}\downarrow & & \vdots\,{\scriptstyle\exists!\,\sharp_0} \\ J & \xrightarrow[\pi]{} & J_0 \end{array} \tag{s1}$$

a commutative diagram of set maps. Since $\sigma$ and $\pi$ are surjective, one checks that $\sharp_0$ is, in fact, a quadratic map over $k_0$, so (s1) by Cor. 11.5 commutes as a $\sigma$-semi-linear polynomial square. Next we we consult (ii) again to find a unique symmetric bilinear form $T_0 \colon X_0 \times X_0 \to k_0$ such that the diagram

$$\begin{array}{ccc} X \times X & \xrightarrow[\pi\times\pi]{} & X_0 \times X_0 \\ {\scriptstyle T}\downarrow & & \vdots\,{\scriptstyle\exists!\,T_0} \\ k & \xrightarrow[\sigma]{} & k_0 \end{array} \tag{s2}$$

commutes. Defining set maps

$$f := N_k \colon J \to k, \quad g := (DN)_k \colon J \times J \to k,$$

Exc. 12.43 (d) implies $f * g = N$ as cubic forms acting on $J$. Moreover, the adjoint identity yields $g(x, y) = T(x^\sharp, y)$ for all $x, y \in X$. Now define $g_0 \colon J_0 \times J_0 \to k_0$ by $g_0(x_0, y_0) := T_0(x_0^{\sharp_0}, y_0)$ for $x_0, y_0 \in J_0$. By (s1), (s2), the diagram

$$\begin{array}{ccc} J \times J & \xrightarrow[\pi\times\pi]{} & J_0 \times J_0 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g_0} \\ k & \xrightarrow[\sigma]{} & k_0 \end{array} \tag{s3}$$

commutes, and using condition (iii) one checks that there is a unique set map $f_0 \colon J_0 \to k_0$ rendering the diagram

$$\begin{array}{ccc} J & \xrightarrow[\pi]{} & J_0 \\ {\scriptstyle f}\downarrow & & \vdots\,{\scriptstyle\exists!\,f_0} \\ k & \xrightarrow[\sigma]{} & k_0 \end{array} \tag{s4}$$

commutative. By (s3), (s4), we obtain a cubic map $(f_0, g_0) \colon J_0 \to k_0$, giving rise, by Exc. 12.43 to a cubic form $N_0 := f_0 * g_0 \colon J_0 \to k_0$. Here Exc. 12.48

combined with (s3), (s4) shows that the $\sigma$-semi-linear polynomial square

$$\begin{array}{ccc} X & \xrightarrow[\pi]{} & X_0 \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle N_0} \\ k & \xrightarrow[\sigma]{} & k_0 \end{array} \tag{s5}$$

commutes. We claim that the $k_0$-module $J_0$ together with $1_0 := \pi(1) = 1_{J_0}$, $\sharp_0$, $N_0$ is a cubic norm structure $X_0$ over $k_0$. Since $\sigma, \pi$ are surjective and equations (1)–(5) of Exc. 33.14 hold in $J$, they hold mutatis mutandis in $X_0$. Hence we need only show that $1_0 \in X_0$ is unimodular. Applying (1), we see that $\lambda$ factors uniquely through $\pi$ to a linear form $\lambda_0 \colon X_0 \to k_0$ satisfying $\lambda_0(1_0) = 1_{k_0}$. This proves the assertion. Combining (s1), (s5) with 34.10 (a), it follows that $\pi \colon X \to X_0$, with $X := X(J)$, is a $\sigma$-semi-linear homomorphism of cubic norm structures. By 34.10 (c), therefore, $\pi \colon J = J(X) \to J(X_0)$ is a $\sigma$-semi-linear homomorphism of cubic Jordan algebras, which forces $J_0 = J(X_0)$ as abstract Jordan algebras, and the solution of (b) is complete.

(d) If the linear trace $T$ of $J$ is surjective, some $u \in J$ has $T(u) = 1$. Now let $(\mathfrak{a}, I)$ be a cubic ideal in $J$ and write $\sigma \colon k \to k/\mathfrak{a}$ for the canonical projection. Then

$$\lambda \colon J \longrightarrow k/\mathfrak{a}, \quad x \longmapsto \lambda(x) := \sigma(T(u, x)),$$

is a $k$-linear map satisfying (1) since $T(u, x) \in \mathfrak{a}$ for all $x \in I$ by (ii). Hence $(\mathfrak{a}, I)$ is separated.

(e) Setting $I := \mathfrak{a}J$, condition (i) trivially holds, and one checks that so does (ii). Hence $(\mathfrak{a}, I)$ is a cubic ideal in $J$. Let $\lambda'$ be a linear form on $J$ satisfying $\lambda'(1) = 1_k$ and write $\sigma \colon k \to k/\mathfrak{a}$ for the canonical projection. Then the $k$-linear map $\lambda := \sigma \circ \lambda' \colon J \to k/\mathfrak{a}$ satisfies (1), forcing $(\mathfrak{a}, I)$ to be separated. From (9.3.1) we conclude that $\mathrm{can}_{J,k/\mathfrak{a}} \colon J \to J_{k/\mathfrak{a}} = J/\mathfrak{a}J$ is the canonical projection, which by 34.10 (c), (d) is a $\sigma$-semi-linear homomorphism of cubic Jordan algebras. In the sense of (b), therefore, $J/\mathfrak{a}J = J_0$ as cubic Jordan algebras over $k_0 = k/\mathfrak{a}$. The answer to the final question of (e) is no. In order to see this, assume $k \neq \{0\}$, consider the multiplicative cubic alternative algebra $(k \times k)_{\mathrm{cub}}$ of 34.15 and pass to the associated cubic Jordan algebra $J = (k \times k)^{(+)}_{\mathrm{cub}}$. Then $I := \{0\} \times k$ is an ideal in $J$ satisfying $\{0\} \neq I^\sharp \subseteq k \times \{0\}$ by (34.15.3), hence violating (iv). In particular, $I$ cannot be extended to a cubic ideal in $J$.

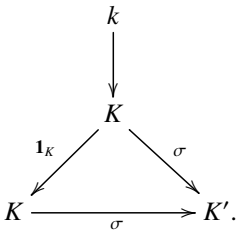
(f) We begin by establishing (ii), so let $x \in I$, $y \in J$ and write $\sigma \colon k \to k/\mathfrak{a}$ for the canonical projection. Then $I$ by (iv) contains $1 \times x = T(x)1 - x$, and applying the map $\lambda$ of (iii), we deduce $\sigma(T(x)) = T(x)1_{k/\mathfrak{a}} = \lambda(1 \times x) = 0$, hence $T(x) \in \mathfrak{a}$. Since $x \times y \in I$, again by (iv), we now conclude $T(x, y) = T(x)T(y) - T(x \times y) \in \mathfrak{a}$. Thus the first inclusion of (ii) holds, while the remaining ones by

(iv), (v) are now obvious. By (a), therefore, $(\mathfrak{a}, I)$ is a separated cubic ideal in $J$.

**34.22** (a) By 9.2, the assignment in question gives an additive bijection from the $K'$-linear maps $X_{K'} \to X'$ to the $\sigma$-semi-linear maps $X \to X'$ (i.e., the $K$-linear maps $X \to {}_K X'$). For a $K'$-linear map $\varphi' : X_{K'} \to X'$ and $\varphi := \varphi' \circ \mathrm{can}_{X,K'}$, it therefore remains to show that $\varphi'$ is a homomorphism of cubic arrays over $K'$ if and only if $\varphi$ is a $\sigma$-semi-linear homomorphism of cubic arrays.

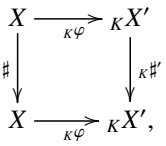
Let us first assume that $\varphi'$ is a homomorphism of cubic arrays over $K'$. It is a general fact following trivially from the definitions that if $\tau : L \to L'$, $\tau' : L' \to L''$ are morphisms in $k$-**alg**, $Y$ (resp. $Y'$, $Y''$) is a cubic array over $L$ (resp. $L'$, $L''$) and $\psi : Y \to Y'$ (resp. $\psi' : Y' \to Y''$) is a $\tau$- (resp. $\tau'$-)semi-linear homomorphism of cubic arrays, then $\psi' \circ \psi : Y \to Y''$ is a $(\tau' \circ \tau)$-semi-linear homomorphism of cubic arrays. Thus, since $\varphi' : X_{K'} \to X'$ is a homomorphism of cubic arrays and $\mathrm{can}_{X,K'} : X \to X_{K'}$ by 34.7 (d) is a $\sigma$-semi-linear one, so is $\varphi = \varphi' \circ \mathrm{can}_{X,K'}$.

Conversely, assume $\varphi : X \to X'$ is a $\sigma$-semi-linear homomorphism of cubic arrays. We abbreviate $\sharp = \sharp_X$, $\sharp' = \sharp_{X'}$, $N = N_X$, $N' = N_{X'}$, specialize (12.28.8) to



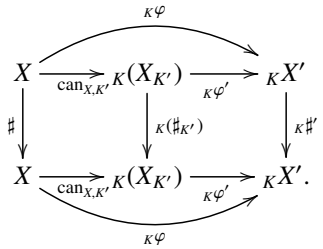

(s1)

Since the $\sigma$-semi-linear polynomial square (34.10.1) commutes, so does



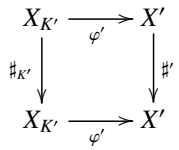

(s2)

by (s1) and (12.28.9). Now consider the diagram



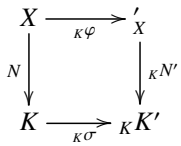
(s3)

Diagram chasing, (12.28.9) and (s2) imply that ${}_K(\varphi' \circ \sharp_{K'})$ and ${}_K(\sharp' \circ \varphi')$, being equalized by $\mathrm{can}_{X,K'}$, are the same, so the diagram



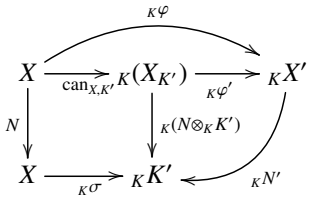
(s4)

of polynomial laws over $K'$ commutes by Exc. 12.45. Similarly, since (34.10.2) commutes, so does



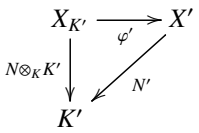
(s5)

by (s1) and (12.28.8). Using (s5), (12.28.9) and diagram chasing in



(s6)

conclude that ${}_K(N \otimes_K K')$ and ${}_K(N' \circ \varphi')$ are equalized by $\mathrm{can}_{X;K'}$, hence are the same, and the diagram



(s7)

of polynomial laws over $K'$ commutes. Summing up, therefore, the $K'$-linear map $\varphi' : X_{K'} \to X'$ is, in fact, a homomorphism of cubic arrays over $K'$.

(b) Let $\varphi\colon X \to X'$ be a $\sigma$-semi-linear map preserving base points and making (1) a commutative diagram of set maps. Then it is a commutative $\sigma$-semi-linear polynomial square. Let $\varphi'\colon X_{K'} \to X'$ be the $K'$-liner map such that $\varphi' \circ \mathrm{can}_{X,K'} = \varphi$. Arguing as in (a), we conclude that $\varphi'$ preserves adjoints. By Exc. 34.18 (a) and Cor. 34.6, therefore, $\varphi'$ is a homomorphism of cubic norm structures over $K'$. But then, by (a), $\varphi = \varphi' \circ \mathrm{can}_{X,K'}$ is a $\sigma$-semi-linear homomorphism of cubic norm structures.

**34.23** For the first part of the problem, if $T(x), S(x), N(x) \in k$ are nilpotent, then so are $T(x)x^2, S(x)x, N(x)1 \in J$. By (33.9.2) and Exc. 28.23, therefore, $x^3$ is nilpotent, whence $x$ is nilpotent. Conversely, assume that $x$ is nilpotent. Since $N$ permits Jordan composition, it commutes with taking powers, and we conclude $N(x) \in \mathrm{Nil}(k)$. Moreover, applying Exc. 28.23 again, there exists a positive integer $m$ such that $x^n = 0$ for all integers $n \geq m$. We now show $T(x), S(x) \in \mathrm{Nil}(k)$ by induction on $m$. For $m = 1$ there is nothing to prove. Next assume $m > 1$ and that the assertion holds for all positive integers $< m$. Since $(x^2)^n = x^{2n} = 0$ for all integers $n \geq m - 1$, the induction hypothesis implies that $T(x^2)$ and $S(x^2)$ are nilpotent. On the other hand, from (33a.22) and the adjoint identity (33a.5) we deduce

$$T(x)^2 = 2S(x) + T(x^2), \quad S(x)^2 = 2T(x)N(x) + S(x^2).$$

Since $N(x)$ is nilpotent, the induction hypothesis and the second equation imply that $S(x)$ is nilpotent, which combines with the first equation to show that $T(x)$ is nilpotent as well. This completes the proof of the first part.

In order to establish the second part, we put

$$I := \{x \in J \mid \forall y \in J : \ T(x,y), T(x^\sharp, y), N(x) \in \mathrm{Nil}(k)\} \tag{s1}$$

and have to show $I = \mathrm{Nil}(J)$. For $x, y \in I$ and $z \in J$, we apply (33a.6), (33a.7) and obtain

$$\begin{aligned} N(x+y) &= N(x) + T(x^\sharp, y) + T(x, y^\sharp) + N(y) \in \mathrm{Nil}(k), \\ T(x+y, z) &= T(x,z) + T(y,z) \in \mathrm{Nil}(k), \\ T((x+y)^\sharp, z) &= T(x^\sharp, z) + T(x, y \times z) + T(y^\sharp, z) \in \mathrm{Nil}(k), \end{aligned}$$

hence $x + y \in I$. Thus $I \subseteq J$ is a $k$-submodule. Next we claim

$$I^\sharp + I \times J \subseteq I. \tag{s2}$$

The inclusion $I^\sharp \subseteq I$ follows immediately from (s1), the adjoint identity (33a.5) and (33a.18). It remains to show $x \times y \in I$ for all $x \in I$, $y \in J$. Given $z \in J$, we

apply (33a.29), (33a.10), (33a.7)

$$\begin{aligned} N(x\times y) &= T(x^\sharp, y)T(x, y^\sharp) - N(x)N(y) \in \mathrm{Nil}(k),\\ T(x\times y, z) &= T(x, y\times z) \in \mathrm{Nil}(k),\\ T((x\times y)^\sharp, z) &= T(x^\sharp, y)T(y, z) + T(x, y^\sharp)T(x, z) - T(x^\sharp, y^\sharp\times z) \in \mathrm{Nil}(k). \end{aligned}$$

Hence $x\times y \in I$ and (s2) holds. Now let $x\in I$ and $y\in J$. Then $U_x y = T(x,y)x - x^\sharp\times y \in I$ by (s2), so $I\subseteq J$ is an inner ideal. But since

$$\begin{aligned} T(U_y x, z) &= T(x, U_y z) \in \mathrm{Nil}(k),\\ T((U_y x)^\sharp, z) &= T(U_{y^\sharp}x^\sharp, z) = T(x^\sharp, U_{y^\sharp}z) \in \mathrm{Nil}(k),\\ N(U_y x) &= N(y)^2 N(x) \in \mathrm{Nil}(k) \end{aligned}$$

for all $z\in J$ by (33a.21), (33a.31), (33a.20) and (s2), we also have $U_y x\in I$ by (s1), so $I\subseteq J$ is an outer ideal and altogether, therefore, an ideal in $J$ which by the first part of the problem consists entirely of nilpotent elements. This proves $I\subseteq \mathrm{Nil}(J)$.

Conversely, let $x\in\mathrm{Nil}(J)$. Then $T(x), S(x), N(x)\in\mathrm{Nil}(k)$ by the first part of the problem, and we have $\mathrm{Nil}(k)J\subseteq\mathrm{Nil}(J)$ by Exc. 28.20 (c). Furthermore, for all $y\in J$, $\mathrm{Nil}(J)\ni U_x y = T(x,y)x - x^\sharp\times y$, hence $x^\sharp\times y\in\mathrm{Nil}(J)$, which by (33a.12), (33a.13) implies $S(x)T(y) - T(x^\sharp, y) = T(x^\sharp\times y)\in\mathrm{Nil}(k)$. Thus $T(x^\sharp, y)\in\mathrm{Nil}(k)$. Since $z := U_y x = T(y,x)y^\sharp - y^\sharp\times x$ belongs to the ideal $\mathrm{Nil}(J)$, so does $x+z$, which by (33a.7), (33a.13), implies

$$\begin{aligned} T(x,y)^2 - 2T(x^\sharp, y^\sharp) &= T(x,y)^2 - T(x\times x, y^\sharp) = T(x,y)^2 - T(x, y^\sharp\times x) = T(x, U_y x)\\ &= T(x,z) = T(x)T(z) - S(x,z)\\ &= T(x)T(z) + S(x) + S(z) - S(x+z) \in \mathrm{Nil}(k). \end{aligned}$$

Thus $T(x,y)\in\mathrm{Nil}(k)$ and summing up we have shown $x\in I$. This completes the proof of (1).

Finally, let $x,y\in J$. If $\frac{1}{2}\in k$, then $T(x^\sharp, y) = \frac{1}{2}T(x\times x, y) = \frac{1}{2}T(x, x\times y)$ by (33a.7), so (1) implies (2). Similarly, if $\frac{1}{3}\in k$, then $N(x) = \frac{1}{3}T(x, x^\sharp)$ by (33a.11), so (1) implies (3). Finally, (4) follows by combining (2) and (3).

**34.24** (a) $N$ as defined by (1) is clearly a cubic form such that

$$N((r,u),(s,v)) = sq(u) + rq(u,v)$$

for $R\in k$-**alg**, $r,s\in R$, $u,v\in J_R$. Defining $T$ (resp. $S$) as a linear (resp. quadratic) form on $J$ by $T(x) := N(1_J, x)$ (resp. $S(x) := N(x, 1_J)$) for $x\in\hat{J}$, we therefore conclude that (3), (4) hold. For $x = (r,u)\in\hat{J}_R$, this and (29b.6),

(29b.7) imply

$$\begin{aligned} x^3 - T(x)x^2 + S(x)x - N(x)1_{\hat{J}} &= \big(r^3 - (r+t(u))r^2 + (rt(u)+q(u))r - rq(u), \\ &\qquad u^3 - (r+t(u))u^2 + (rt(u)+q(u))u - rq(u)e\big) \\ &= \big(0, u^3 - t(u)u^2 + q(u)u - r(u^2 - t(u)u + q(u)e)\big) \\ &= 0, \\ x^4 - T(x)x^3 + S(x)x^2 - N(x)x &= \big(r^4 - (r+t(u))r^3 + (rt(u+q(u))r^2 - rq(u)r, \\ &\qquad u^4 - (r+t(u))u^3 + (rt(u)+q(u))u^2 - rq(u)u\big) \\ &= \big(0, U_u(u^2 - t(u)u + q(u)e) - r(u^3 - t(u)u^2 + q(u)u)\big) \\ &= 0. \end{aligned}$$

Since $q$ permits Jordan composition by (29b.12), so does $N$ by (1), and we have shown that $\hat{J}$ is a cubic Jordan algebra with norm $N$ over $k$ such that (1), (3), (4) hold. Linearizing (4) and applying (33.2.10), we also obtain (2). Finally, (33a.22) implies, for $x = (\alpha, u)$, $\alpha \in k$, $u \in J$,

$$\begin{aligned} x^\sharp = x^2 - T(x)x + S(x)1_{\hat{J}} &= \big(\alpha^2 - (\alpha + t(u))\alpha + (\alpha t(u) + q(u)), \\ &\qquad u^2 - (\alpha + t(u))u + (\alpha t(u) + q(u))e\big) \\ &= \big(q(u), \alpha(t(u)e - u)\big) \\ &= (q(u), \alpha\bar{u}). \end{aligned}$$

This proves (5), and (a) is solved.

(b) Applying Exc. 29.25, we see that $C^{(+)}$ agrees with the Jordan algebra, $J := J(C, n_C, 1_C)$, of the pointed quadratic module $(C, n_C, 1_C)$. Thus

$$\hat{C}^{(+)} = k^{(+)} \times C^{(+)} = k^{(+)} \times J = \hat{J}$$

is a cubic Jordan algebra over $k$ with norm $N\colon \hat{C} \to k$ given by

$$N((r,u)) = rn_C(u) \qquad (R \in k\text{-}\mathbf{alg},\ \ r \in R\ \ u \in C_R). \tag{s1}$$

Hence $\hat{C}$ is a cubic alternative $k$-algebra with norm $N$ if and only if $C$ is multiplicative. Finally, Example 34.15 fits into this picture by setting $C := k$.

**34.25** (a): We write $\theta$ for the canonical image of $\mathbf{t}$ in $K$ and use the formula (34.24.4) for $S_J$, which says that for $u = c\theta + d$, $c, d \in F$, we have

$$S_J((\alpha, u)) = \alpha t_K(c\theta + d) + \beta c^2 + cd + d^2.$$

Now the trace on $K$ is given by

$$t_K(c\theta + d) = ct_K(\theta) + dt_K(1_K) = c + 2d = c,$$

so

$$S_J((\alpha,u)) = \alpha c + \beta c^2 + cd + d^2. \tag{s1}$$

That is the equation with respect to the basis $(1,0)$, $(0,\theta)$, $(0,1)$ of $J$. Using instead the basis $(1,1)$, $(0,\theta+1)$, $(0,1)$, we have for $r,s,d \in F$:

$$S_J((r(1,1)+s(0,\theta+1)+(0,d)) = S_J((r,s\theta+r+s+d)) = \beta s^2 + sd + d^2 + r^2,$$

a quadratic form of the claimed isomorphism class.

(b): By formula (34.24.3), the kernel of $T_J$ consists of elements $(\alpha,u)$ with $u = \alpha\theta+d$. For such an element, (s1) gives that $S_J((\alpha,u)) = (1+\beta)\alpha^2+\alpha d+d^2$, which is the claim.

**34.26** (a): Again, we write $\theta$ for the canonical image of $\mathbf{t}$ in $K$. Since $\theta \in K$ has trace zero, we conclude

$$t_K(c\theta+d) = 2d,$$

and use the formula (34.24.4) for $S_J$, which says that for $u = c\theta+d$ we have

$$S_J((\alpha,u)) = 2\alpha d + d^2 - \beta c^2. \tag{s1}$$

Re-writing this as $2(\alpha d + d^2/2) - \beta c^2$, we see that it has the same isomorphism class as $\langle 2\rangle \otimes [0,\frac{1}{2}] \perp \langle -\beta\rangle_{\text{quad}}$. Since $[0,\frac{1}{2}]$ has an isotropic vector (namely, $(1,0)$), it follows that it is isomorphic to $\mathbf{h}$, proving the claim.

(b): By the preceding formula for the trace on $K$ and (34.24.3), the kernel of $T_J$ consists of elements $(-2d, c\theta+d)$. For such an element, (s1) gives that $S_J((-2d,c\theta+d)) = -3d^2 - \beta c^2$, which is the claim.

(c): While it is possible to approach this by building on (b), it is perhaps simpler to argue directly, regardless of $\operatorname{char}(F)$, as follows. For $J := (F\times F\times F)^{(+)}$, $J^0$ consists of triples $(x,y,-x-y) \in F^3$ and $S_J^0$ sends such an element to $y(-x-y)+x(-x-y)+xy = -(x^2+xy+y^2)$.

**34.27** (i) $\Rightarrow$ (ii) Let $X$ be a cubic norm structure over $k$ as in (i). Then $X = (M,e,\sharp,N)$ for some quadratic map $\sharp\colon M \to M$, $x \mapsto x^\sharp$, and some cubic form $N\colon M \to k$. Write $T$ (resp. $S$) for the (bi-)linear (resp. quadratic) trace of $X$ and put $J := J(X) = J(M,q,e)$. For $x \in J^\times$, we combine (1) of Exc. 31.33 with (33.10.1) to conclude $q(x), N(x) \in k^\times$ and $q(x)^{-1}\bar{x} = x^{-1} = N(x)^{-1}x^\sharp$. Hence Prop. 12.24 implies that the identity

$$N(x)\bar{x} = q(x)x^\sharp \tag{s1}$$

holds strictly. We now put

$$\lambda := T - t\colon M \longrightarrow k \tag{s2}$$

as a linear form on $M$ and have $\lambda(e) = 1$ by (29b.2), (33a.2). Eventually, we will show that $\lambda$ satisfies (ii). Noting

$$M = ke \oplus L, \quad L := \mathrm{Ker}(\lambda), \tag{s3}$$

we begin by using (29b.3), (29b.6), (33a.22) to expand (s1): we obtain $N(x)\bar{x} = t(x)N(x)e - N(x)x$ and

$$\begin{aligned} q(x)x^\sharp &= q(x)x^2 - q(x)T(x)x + q(x)S(x)e \\ &= q(x)t(x)x - q(x)^2e - q(x)T(x)x + q(x)S(x)e \\ &= q(x)(S(x) - q(x))e - \lambda(x)q(x)x \qquad \text{(by(s2))}. \end{aligned}$$

Thus

$$\Big(N(x) - \lambda(x)q(x)\Big)x = \Big(t(x)N(x) - q(x)(S(x) - q(x))\Big)e.$$

Differentiating at $x$ in the direction $y$ yields

$$\begin{aligned} &(N(x,y) - \lambda(x)q(x,y) - \lambda(y)q(x))x + (N(x) - \lambda(x)q(x))y \\ &\quad = \Big(t(x)N(x,y) + t(y)N(x) - q(x)(S(x,y) - q(x,y)) - q(x,y)(S(x) - q(x))\Big)e. \end{aligned}$$

Setting $y = e$ and consulting (33a.2), we conclude

$$\begin{aligned} &(S(x) - \lambda(x)t(x) - q(x))x + (N(x) - \lambda(x)q(x))e \\ &\quad = \Big(t(x)S(x) + 2N(x) - q(x)(2T(x) - t(x)) - t(x)(S(x) - q(x))\Big)e, \end{aligned}$$

which after a short computation simplifies to

$$(N(x) - \lambda(x)q(x))e = (S(x) - q(x) - \lambda(x)t(x))x.$$

We claim that the identity

$$N(x) = \lambda(x)q(x) \tag{s4}$$

holds strictly, equivalently, that the cubic form

$$F\colon M \longrightarrow k, \quad x \longmapsto F(x) := N(x) - \lambda(x)q(x), \tag{s5}$$

is zero. By what we have just proved we know

$$F(x)e = (S(x) - q(x) - \lambda(x)t(x))x. \tag{s6}$$

Since $F(e) = 0$, the expansion formula (2) of Exc. 12.40 combined with (s3) implies that it suffices to show

$$F(u) = F(e,u) = F(u,e) = 0 \tag{s7}$$

strictly for all $u \in L$. Specializing $x$ to $u$ in (s6) and applying $\lambda$, we obtain

$F(u) = 0$. Moreover, $F(e,u) = N(e,u) - \lambda(e)q(e,u) - \lambda(u)q(e) = T(u) - t(u) = \lambda(u)$ (by (s2)) $= 0$, so it remains to show $F(u,e) = 0$. But

$$F(u,e) = N(u,e) - \lambda(u)q(u,e) - \lambda(e)q(u) = S(u) - q(u),$$

so we must show $S = q$ on $L$. Since $F(u) = 0$ for $u \in L$, applying (s6) to $x = u$ yields

$$(S(u) - q(u))u = 0, \tag{s8}$$

hence after linearizing

$$(S(u) - q(u))v + (S(u,v) - q(u,v))u = 0. \tag{s9}$$

Note by (s3) that $L$ is a projective $k$-module, so localizing if necessary, we may assume that $L$ is free. Pick a basis $(u_i)_{i\in I}$ of $L$. Then (s8), (s9) imply $S(u_i) = q(u_i)$ $(i \in I)$, $S(u_i,u_j) = q(u_i,u_j)$ $(i,j \in I,\ i \neq j)$. This shows $S = q$ on $L$ and completes the proof of (s7). Thus (s4) holds strictly. Returning to (s1), we therefore obtain $\lambda(x)q(x)\bar{x} = N(x)\bar{x} = q(x)x^\sharp$, and Prop. 12.24 implies (3). Now the adjoint identity yields $N(x)x = x^{\sharp\sharp} = \lambda(x)^2\bar{x}^\sharp = \lambda(x)^2\lambda(\bar{x})x$. Since invertible elements are unimodular by Thm. 34.3 (b), we end up with (4), which linearizes to

$$N(x,y) = 2\lambda(x)\lambda(\bar{x})\lambda(y) + \lambda(x)^2\lambda(\bar{y});$$

putting $x = e$ gives (5), while for $y = e$ we obtain (6). This in turn linearizes to $S(x,y) = 2(\lambda(x)\lambda(y) + \lambda(x)\lambda(\bar{y}) + \lambda(\bar{x})\lambda(y))$, and a short computation involving (5) and (33a.13) yields (7).

(ii) $\Rightarrow$ (i). If (1) holds, so obviously does (2). Define $X := (M, e, \sharp, N)$, where $\sharp$, $N$ are given by (3), (4), respectively. From (3), (4) we conclude that $X$ is a cubic array, and the preceding computations can be repeated verbatim to show that the (bi-)linear and quadratic traces of $X$satisfy (5)–(7). Now we show that $X$ is a cubic norm structure. Linearizing (3) yields

$$x \times y = \lambda(x)\bar{y} + \lambda(y)\bar{x}, \tag{s10}$$

hence $e \times x = \lambda(x)e + \bar{x} = (\lambda(x) + t(x))e - x = T(x)e - x$ by (2), (5). Thus the unit identity holds. From $x^{\sharp\sharp} = \lambda(x)^2\bar{x}^\sharp = \lambda(x)^2\lambda(\bar{x})x$ and (4) we read off the adjoint identity, while comparing $N(x,y) = 2\lambda(x)\lambda(\bar{x})\lambda(y) + \lambda(x)^2\lambda(\bar{y})$ with

$$T(x^\sharp, y) = 2\lambda(x^\sharp)\lambda(y) + \lambda(\overline{x^\sharp})\lambda(\bar{y}) = 2\lambda(x)\lambda(\bar{x})\lambda(y) + \lambda(x)^2\lambda(\bar{y})$$

proves also the gradient identity. Summing up, therefore, $X$ is a cubic norm structure. It remains to show $J(X) = J(M,q,e)$, i.e.,

$$q(x,\bar{y})x - q(x)\bar{y} = T(x,y)x - x^\sharp \times y. \tag{s11}$$

From (5), (s10), (3) we deduce

$$\begin{aligned} T(x,y)x - x^\sharp \times y &= (2\lambda(x)\lambda(y) + \lambda(\bar{x})\lambda(\bar{y}))x - \lambda(x^\sharp)\bar{y} - \lambda(y)\overline{x^\sharp} \\ &= (2\lambda(x)\lambda(y) + \lambda(\bar{x})\lambda(\bar{y}))x - \lambda(x)\lambda(\bar{x})\bar{y} - \lambda(x)\lambda(y)x \\ &= (\lambda(x)\lambda(y) + \lambda(\bar{x})\lambda(\bar{y}))x - \lambda(x)\lambda(\bar{x})\bar{y}, \end{aligned}$$

and by (1) (possibly linearized), this is the left-hand side of (s11). Thus (i) holds.

In order to prove (8), we put

$$I_1 := \{x \in J \mid x \text{ is nilpotent}\}, \quad I_2 := \{x \in J \mid \lambda(x), \lambda(\bar{x}) \in k \text{ are nilpotent}\}.$$

It suffices to show $\mathrm{Nil}(J) \subseteq I_1 \subseteq I_2 \subseteq \mathrm{Nil}(J)$. The first inclusion is obvious. For $x \in I_1$, we apply Exc. 29.21 to conclude that $q(x) = \lambda(x)\lambda(\bar{x})$ and $t(x) = \lambda(x) + \lambda(\bar{x})$ are nilpotent. Hence so is $\lambda(x)t(x) = \lambda(x)^2 + q(x)$, which implies $x \in I_2$. This proves the second inclusion. For $x \in I_2$, we conclude that $q(x) = \lambda(x)\lambda(\bar{x})$ is nilpotent, as is $q(x,y) = \lambda(x)\lambda(\bar{y}) + \lambda(y)\lambda(\bar{x})$ for all $y \in J$. Thus $x \in \mathrm{Nil}(J)$, again by Exc. 29.21, and we have established the third inclusion.

For the remainder of this exercise, we may assume that $(M, q)$ is a quadratic space of rank $r > 1$. Since (iii) implies (i) by 34.15, we need only show

(ii) $\Rightarrow$ (iii). By (s3), the $k$-module $L$ is projective of rank $r - 1$. Let us first assume that $L$ is free, and let $(u_i)_{1 \le i < r}$ be a $k$-basis of $L$. With $u_0 := e$, therefore, $(u_i)_{0 \le i < r}$ is a $k$-basis of $M$, and by (1), the matrix of $q$ relative to this basis is

$$S := \begin{pmatrix} 1 & t(u_1) & \cdots & t(u_{r-1}) \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

whence the matrix of $Dq$ is

$$S' = S + S^\mathsf{T} = \begin{pmatrix} 2 & t(u_1) & \cdots & t(u_{r-1}) \\ t(u_1) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t(u_{r-1}) & 0 & \cdots & 0 \end{pmatrix}.$$

Since $Dq$ is regular by hypothesis, the determinant of $S'$ is invertible in $k$. On the other hand, expanding with respect to the last row yields

$$\det(S') = (-1)^{r+1} t(u_{r-1}) \det \begin{pmatrix} t(u_1) & \cdots & t(u_{r-1}) \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix},$$

which would be zero for $r > 2$. Hence $r = 2$ and $k^\times \ni \det(S') = -t(u_1)^2$, forcing $t\colon L \to k$ to be surjective.

Now let $L$ be arbitrary. Localizing if necessary, the preceding considerations show that we still have $r = 2$ and $t\colon L \to k$ surjective. In particular, some $c \in L$ satisfies $t(c) = 1$. Moreover $q(c) = 0$ by the definitions of $q$ and $L$, so $c$ is an elementary idempotent in $J = J(M, q, e)$, and with $d := e - c$ we conclude $J = kc \oplus kd$ as a direct sum of ideals such that $\lambda(c) = 0$ and $\lambda(d) = 1$. By (4), therefore, the relation

$$N(\xi_1 c + \xi_2 d) = \lambda(\xi_1 c + \xi_2 d)^2 \lambda(\overline{\xi_1 c + \xi_2 d}) = \xi_1 \xi_2^2$$

holds strictly for all $\xi_1, \xi_2 \in k$, whence the assignment $\xi_1 c + \xi_2 d \mapsto (\xi_1, \xi_2)$ gives an isomorphism $J \xrightarrow{\sim} (k \times k)^{(+)}_{\mathrm{cub}}$ of cubic Jordan algebras.

In view of (iii), the final assertion about quadratic étale algebras is obvious.

**34.28** (a) The arguments solving Exc. 34.20 (a) go through for rational cubic norm pseudo-structures without change and prove (a).

(b) (i) $\Rightarrow$ (ii). Let $1 \le i \le n$. Then (i) and Euler's differential equation imply $\sigma(e_i^\sharp, e_i) = \mu(e_i, e_i) = 3\mu(e_i) = 3w_i$. Moreover, linearizing the relation $\mu(v, v') = \sigma(v^\sharp, v')$, we conclude $\sigma(v_1 \times v_2, v_3) = \mu(v_1, v_2, v_3)$, and this is totally symmetric in $v_1, v_2, v_3 \in V$.

(ii) $\Rightarrow$ (i). For $R \in k$-**alg**, we define a map $\mu_R\colon V_R \to W_R$ by setting

$$\mu_R\Big(\sum_{i=1}^n r_i e_{iR}\Big) := \sum_{i=1}^n r_i^3 w_{iR} + \sum_{1 \le i,j \le n, i \ne j} r_i^2 r_j \sigma(e_i^\sharp, e_j)_R + \sum_{1 \le i < j < l \le n} r_i r_j r_l \sigma(e_i \times e_j, e_l)_R \tag{s1}$$

for $r_1, \dots, r_n \in R$. Then $\mu := (\mu_R)_{R \in k\text{-}\mathbf{alg}}\colon V \to W$ is obviously a homogeneous polynomial law of degree 3 satisfying $\mu(e_i) = w_i$ for $1 \le i \le n$. Now let $v = \sum_{i=1}^n r_i e_{iR}, v' = \sum_{i=1}^n r_i' e_{iR} \in V_R$ with $r_i, r_i' \in R$ for $i = 1, \dots, n$. Then (s1) implies

$$\begin{aligned}\mu(v, v') = &\sum_i 3 r_i^2 r_i' w_{iR} + \sum_{i \ne j} (2 r_i r_i' r_j + r_i^2 r_j') \sigma(e_i^\sharp, e_j)_R \\ &+ \sum_{i<j<l} (r_i' r_j r_l + r_i r_j' r_l + r_i r_j r_l') \sigma(e_i \times e_j, e_l)_R.\end{aligned}$$

On the other hand

$$v^\sharp = \sum_i r_i^2 e_{iR}^\sharp + \sum_{i<j} r_i r_j e_{iR} \times e_{jR},$$

and hence (ii) gives

$$\begin{aligned}
\sigma(v^\sharp, v') &= \sum_{i,l} r_i^2 r_l' \sigma(e_i^\sharp, e_l)_R + \sum_{i,j,l, i<j} r_i r_j r_l' \sigma(e_i \times e_j, e_l)_R \\
&= \sum_i r_i^2 r_i' \sigma(e_i^\sharp, e_i)_R + \sum_{i\neq j} r_i^2 r_j' \sigma(e_i^\sharp, e_j)_R + \sum_{i<j} r_i r_i' r_j \sigma(e_i \times e_j, e_i)_R \\
&\quad + \sum_{i<j} r_i r_j r_j' \sigma(e_i \times e_j, e_j)_R + \Big( \sum_{l<i<j} + \sum_{i<l<j} + \sum_{i<j<l} \Big) r_i r_j r_l' \sigma(e_i \times e_j, e_l)_R \\
&= \sum_i 3 r_i^2 r_i' w_{iR} + \sum_{i\neq j} (r_i^2 r_j' + 2 r_i r_i' r_j) \sigma(e_i^\sharp, e_j)_R \\
&\quad + \sum_{i<j<l} (r_i' r_j r_l + r_i r_j' r_l + r_i r_j r_l') \sigma(e_i \times e_j, e_l)_R \\
&= \mu(v, v'),
\end{aligned}$$

and (i) holds. Finally, uniqueness of $\mu$ follows immediately from (5) of Exc. 12.40.

(c) Since a pseudo cubic norm pseudo-structure $X$ over $k$ is automatically a cubic norm structure if $\frac{1}{3} \in k$ ($\lambda := \frac{1}{3}T$ has $\lambda(1) = 1$), any example of the kind demanded in (c) must display pathologies of characteristic 3. With this in mind, we let $K/F$ be a purely inseparable field extension of characteristic 3 and exponent 1 and fix an element $a \in K \setminus F$. Then $F$ is infinite and $J_0 := K^{(+)}$ is a cubic Jordan algebra over $F$, with norm $N_0 \colon K \to F$ (by Cor. 12.13 an honest-to-goodness polynomial function) given by $N_0(v)1 = v^3$ for all $v \in J_0$. For $R \in F$-**alg** and $v, v' \in J_{0R}$, we conclude $N_0(v, v')1 = 3v^2 v' = 0$, so the (bi-)linear and quadratic traces of $J_0$ are both zero, and $v^\sharp = v^2$ by (33a.22) as well as $v \times v' = 2vv' = -vv'$ for all $v, v' \in J_0$. Now let $W$ be a vector space over $F$ of finite dimension at least 2, pick linearly independent vectors $w_1, w_2 \in W$ and let $\lambda \colon J_0 \to W$ be a non-zero linear map satisfying $\lambda(1) = 0$. Define a symmetric bilinear map $\sigma \colon J_0 \times J_0 \to W$ by $\sigma(v, v') := \lambda(vv')$ for $v, v' \in J_0$. Then $\sigma(v^\sharp, v) = \lambda(v^2 v) = \lambda(v^3) = N_0(v)\lambda(1) = 0$ for all $v \in J_0$, and $\sigma(v_1 \times v_2, v_3) = -\lambda(v_1 v_2 v_3)$ is totally symmetric in $v_1, v_2, v_3 \in J_0$. Thus (b) yields a homogeneous polynomial law $\mu \colon J_0 \to W$ of degree 3 such that $\mu(1) = 0$, $\mu(a) = w_1$, $\mu(a^\sharp) = \mu(a^2) = w_2$.

Now let $k := F \times W \in F$-**alg** be the "split-null extension" of $F$ by $W$, so $W \subseteq k$ is an ideal that squares to zero and $F$ acts canonically on $W$. In other words, the multiplication of $k$ obeys the rule

$$(\alpha, w)(\alpha', w') := (\alpha\alpha', \alpha w' + \alpha' w)$$

for $\alpha, \alpha' \in F$, $w, w' \in W$. By letting $W$ act trivially on $J_0$, we may and always will view $J_0$ as a Jordan algebra $J$ over $k$.

Next define a symmetric $F$-bilinear map $T\colon J \times J \to k$

$$T(v, v') := (0, \sigma(v, v')) = (0, \lambda(vv'))$$

for $v, v' \in J$, which is in fact a $k$-bilinear form since

$$T((\alpha, w)v, v') = T(\alpha v, v') = \alpha T(v, v') = (\alpha, w)(0, \lambda(vv')) = (\alpha, w)T(v, v')$$

for all $\alpha \in F$, $w \in W$, $v, v' \in J$. Similarly, we obtain a map

$$N := N_0 \times \mu\colon J \longrightarrow k, \quad v \longmapsto N(v) := (N_0(v), \mu(v))$$

and claim that *the identity element of $J$ as base point, the (bilinearized) adjoint of $J$ as (bilinearized) adjoint, the symmetric bilinear form $T$, and the map $N$ satisfy equations* (1)–(10) *of Exc.* 34.20. To show this, let $\alpha \in F$, $w \in W$ and $v, v' \in J$. Then

$$((\alpha, w)v)^\sharp = (\alpha v)^\sharp = \alpha^2 v^\sharp = (\alpha, 2\alpha w)v^\sharp = (\alpha, w)^2 v^\sharp \tag{s2}$$

proves (1) and

$$N((\alpha, w)v) = N(\alpha v) = \alpha^3(N_0(v), \mu(v)) = (\alpha, w)^3(N_0(v), \mu(v)) = (\alpha, w)^3 N(v)$$

proves (2). The equations (s2) and

$$((\alpha, w)v) \times v' = (\alpha v) \times v' = \alpha(v \times v') = (\alpha, w)(v \times v')$$

show that the adjoint $v \mapsto v^\sharp$ is not only $F$-quadratic but, in fact, $k$-quadratic. Moreover, the bilinearized adjoint is the $k$-bilinearization of the adjoint, and we have (3). Next we compute

$$\begin{aligned} N(v + v') &= (N_0(v + v'), \mu(v + v')) = (N_0(v) + N_0(v'), \mu(v) + \mu(v, v') + \mu(v', v) + \mu(v')) \\ &= (N_0(v), \mu(v)) + (0, \sigma(v^\sharp, v')) + (0, \sigma(v'^\sharp, v)) + (N_0(v'), \mu(v')) \\ &= N(v) + T(v^\sharp, v') + T(v'^\sharp, v) + N(v'), \end{aligned}$$

and (4) holds. Since $3 = 0$ in $k$, we have $T(v^\sharp, v) = (0, \sigma(v^\sharp, v)) = 0 = 3N(v)$, hence (5). Since the adjoint identity holds in $J_0$, we obtain

$$v^{\sharp\sharp} = N_0(v)v = (N_0(v), \mu(v))v = N(v)v,$$

hence (6). Similarly,

$$\begin{aligned} v^\sharp \times v'^\sharp + (v \times v')^\sharp = & -v^2 v'^2 + (vv')^2 = 0 = (0, \lambda(v^\sharp v'))v' + (0, \lambda(vv'^\sharp))v \\ &= T(v^\sharp, v')v' + T(v, v'^\sharp)v \end{aligned}$$

gives (7) and

$$v^\sharp \times (v \times v') = v^\sharp(vv') = (v^\sharp v)v' = (0 \oplus \lambda(v^\sharp v'))v + N_0(v)v' = (N_0(v), \mu(v))v'$$
$$= T(v^\sharp, v')v + N(v)v'$$

gives (8). While (9) is obvious, the unit identity for $J_0$ implies $1 \times v = -v = (0, \lambda(v))1 - v = T(1, v)1 - v$, hence (10).

By Exc. 34.20, therefore, we find a cubic form $\tilde{N}\colon X \to k$ making $X$ a cubic norm pseudo-structure over $k$. Now consider the element $a \in J$. By construction we have

$$N(a^\sharp) = (N_0(a^2), \mu(a^2)) = (N_0(a)^2, w_2),$$
$$N(a)^2 = (N_0(a), \mu(a))^2 = (N_0(a)^2, 2N_0(a)\mu(a)) = (N_0(a)^2, -N_0(a)w_1),$$

hence $N(a^\sharp) \neq N(a)^2$ since $w_1, w_2$ are linearly independent over $F$.

## Solutions for Section 35

**35.12** (i) $k$ is a cubic norm structure with base point 1, adjoint $\alpha \mapsto \alpha^2$, norm $r \mapsto r^3$, and bilinear (resp. quadratic) trace respectively given by $(\alpha, \beta) \mapsto 3\alpha\beta$ (resp. $\alpha \mapsto 3\alpha^2$). Scalar multiplication gives a bilinear action $k \times V \to V$, while the eikonal triple structure provides us with quadratic maps $Q\colon V \to k$, $H\colon V \to V$. Moreover, setting $v = u$ in (1), Euler's differential equation implies

$$Q(u, H(u)) = N(u) \qquad (R \in k\text{-}\mathbf{alg},\ u \in V_R). \tag{s1}$$

By 35.8, therefore, formulas (3)–(5) define a cubic array $X$ over $k$ whose bilinear trace by (35.8.5) is regular. Thus the solution to (i) will be complete once we have shown that $X$ is, in fact, a cubic norm structure. In order to do so, it suffices to show, by Prop. 35.9, that the identities (35c.1)–(35c.10) hold strictly in $X$. Here (35c.5) is just the eikonal equation, while (35c.7) has been established in (s1) with $\hat{N} = N$. Since (35c.1)–(35c.4), (35c.9) are obvious in the special case at hand, we are left with (35c.6), (35c.8), (35c.10), i.e., with

$$H(H(u)) = N(u)u - Q(u)H(u), \tag{s2}$$
$$Q(u, H(u, v)) = 2Q(H(u), v), \tag{s3}$$
$$H(u, H(u)) = 2Q(u)u. \tag{s4}$$

We begin with (s4) by linearizing (1) to conclude that

$$Q(H(u, v), w) = \frac{1}{3}N(u, v, w) \tag{s5}$$

is totally symmetric in $u, v, w \in V$. Combining this with the linearization of (2), i.e., with

$$Q(H(u), H(u,v)) = 2Q(u)Q(u,v), \tag{s6}$$

we conclude $Q(H(u, H(u)), v) = Q(H(u,v), H(u)) = 2Q(u)Q(u,v) = Q(2Q(u)u, v)$, and (s4) drops out since $Q$ is regular. Setting $w = u$ and using symmetry of (s5) again, we obtain $Q(H(u,v), u) = Q(H(u,u), v) = 2Q(H(u), v)$, hence (s3). And finally, linearizing (s4), we deduce

$$H(v, H(u)) + H\big(u, H(u,v)\big) = 2Q(u,v)u + 2Q(u)v.$$

Here we put $v = H(u)$ apply (s4), (s1) and obtain

$$\begin{aligned} 2H(H(u)) + 4Q(u)H(u) &= H(H(u), H(u)) + 2H(u, Q(u)u) \\ &= H(H(u), H(u)) + H\Big(u, H\big(u, H(u)\big)\Big) = 2Q(u, H(u))u + 2Q(u)H(u) \\ &= 2N(u)u + 2Q(u)H(u), \end{aligned}$$

hence (s2).

(ii) The cubic norm substructure $X_0 \subseteq X$ is regular since $\frac{1}{3} \in k$. Hence $(X_0, V)$ is a complemented cubic norm substructure of $X$. Defining a quadratic map $H\colon V \to V$ by $H(u) := Q(u) + u^\sharp$ for $u \in V$, we are in the situation 35.6 and conclude that the identities (35.6.1)–(35.6.6), (35b.1)–(35b.18) hold strictly in $X$. In particular, by (35.6.4) we have $3Q(u,v) = T(u,v)$, whence $(V, Q)$ is a quadratic space over $k$. Moreover, for $u, v \in V$ the gradient identity implies $3Q(H(u), v) = T(H(u), v) = T(u^\sharp, v) = N(u,v)$, so the quadratic map $H$ is connected with the cubic form $N$ on $V$ by (1). Finally, (35b.9) shows that the eikonal equation (2) holds strictly in $V$. Summing up we have proved that $(V, Q, N|_V)$ is an eikonal triple over $k$.

(iii) follows by a straightforward verification.

(iv) The gradient of $N$ at $u \in \mathbb{R}^n$ is defined by

$$(\operatorname{grad}(N))(u) = \begin{pmatrix} \frac{\partial N}{\partial x_1}(u) \\ \vdots \\ \frac{\partial N}{\partial x_n}(u) \end{pmatrix} \in \mathbb{R}^n$$

and can be characterized by

$$(\operatorname{grad}(N))(u)^{\mathsf{T}} v = N(u,v) \qquad\qquad (v \in \mathbb{R}^n).$$

This and (1) imply

$$H(u)^{\mathsf{T}} Q v = Q(H(u), v) = \frac{1}{3}(\operatorname{grad}(N))(u)^{\mathsf{T}} v,$$

and we conclude $H(u)^{\mathsf{T}}Q = \frac{1}{3}(\operatorname{grad}(N))(u)^{\mathsf{T}}$, hence

$$H(u)^{\mathsf{T}} = \frac{1}{3}(\operatorname{grad}(N))(u)^{\mathsf{T}}Q^{-1}, \quad H(u) = \frac{1}{3}Q^{-1}(\operatorname{grad}(N))(u).$$

Now the left-hand side of (2) becomes

$$H(u)^{\mathsf{T}}QH(u) = \frac{1}{9}(\operatorname{grad}(N))(u)^{\mathsf{T}}Q^{-1}QQ^{-1}(\operatorname{grad}(N))(u) = \sum_{i,j=1}^{n} q^{ij}\frac{\partial N}{\partial x_i}(u)\frac{\partial N}{\partial x_j}(u),$$

while the right-hand side of (1) is

$$\Big(\sum_{i,j=1}^{n} q_{ij}u_iu_j\Big)^2.$$

Hence (2) follows.

## Solutions for Section 36

**36.10** Write $\Gamma = \operatorname{diag}(\gamma_1, \gamma_2)$, $\gamma_1, \gamma_2 \in k^\times$, and put

$$u[12] := \gamma_2 u e_{12} + \gamma_1 \bar{u} e_{21} \qquad (u \in C) \tag{s1}$$

in terms of the usual matrix units in $\operatorname{Mat}_2(k)$. One checks that

$$M := \operatorname{Her}_2(C, \Gamma) = ke_{11} \oplus ke_{22} \oplus C[12], \quad C[12] := \{u[12] \mid u \in C\}. \tag{s2}$$

We define a quadratic form $q\colon M \to k$ by

$$q(\xi_1 e_{11} + \xi_2 e_{22} + u[12]) := \xi_1\xi_2 - \gamma_1\gamma_2 n_C(u)$$

for $\xi_1, \xi_2 \in k$, $u \in C$, which bilinearizes to

$$q(\xi_1 e_{11} + \xi_2 e_{22} + u[12], \eta_1 e_{11} + \eta_2 e_{22} + v[12]) = \xi_1\eta_2 + \xi_2\eta_1 - \gamma_1\gamma_2 n_C(u, v) \tag{s3}$$

for $\xi_i, \eta_i \in k$, $i = 1, 2$, $u, v \in C$. Then $(M, q, e)$, $e := \mathbf{1}_2 = e_{11} + e_{22}$, is a pointed quadratic module over $k$ whose linear trace by (s3) is given by

$$t\colon M \longrightarrow k, \quad t(\xi_1 e_{11} + \xi_2 e_{22} + u[12]) = \xi_1 + \xi_2$$

for $\xi_1, \xi_2 \in k$, $u \in C$. It follows that $J := J(M, q, e)$ is a Jordan algebra of Clifford type over $k$ and, writing $x^n$, $n \in \mathbb{N}$, for the $n$-th power of $x \in J$, a straightforward verification shows

$$xx = x^2 = t(x)x - q(x)e, \tag{s4}$$

where the expression on the very left is the matrix product of $x$ with itself. Linearizing shows that the circle peoduct of $x, y \in J$ is $x \circ y = xy + yx$. We now claim

$$(xx)x = x^3 = x(xx). \tag{s5}$$

Indeed, (s4) implies $(xx)x = t(x)xx - q(x)ex = t(x)x^2 - q(x)x = x^3$ (by (29b.7)), hence the first equation of (s5); the second one follows analogously. Actually, (s5) holds strictly, so we are allowed to differentiate at $x$ in the direction $y$. Doing so with $x^3 = U_x x$ gives $U_x y + U_{x,y} x = U_x y + x^2 \circ y$ (by (29a.13)), while the same procedure for $(xx)x$ and (s4) give

$$(yx)x + (xy)x + (xx)y = (xy)x + x^2 \circ y + [y, x, x],$$

hence the first equation of (1). The same argument applied to $x(xx)$ yields the second equation of (1).

Finally, assume $C$ is projective as a $k$-module and let $(M', q', e')$ be any pointed quadratic module over $k$ satisfying the conditions of the exercise. Then $M' = \mathrm{Her}_2(C, \Gamma) = M$ and $e' = \mathbf{1}_2 = e$. Moreover, (1) shows that $J = J(M, q, e)$ and $J' = J(M', q', e')$ have the same $U$-operator, i.e., $\mathbf{1}_M \colon J \to J$ is an isomorphism of Jordan algebras. Hence $q' = q' \circ \mathbf{1}_M = q$ by Exc. 29.26, as desired.

**36.11** We begin by showing (1). To this end, we put

$$x^2 = \sum (\eta_i e_{ii} + v_i[jl]) \qquad (\eta_i \in k,\ v_i \in C,\ 1 \le i \le 3), \tag{s1}$$

$$xx = (v_{ij}) \qquad (v_{ij} \in C,\ 1 \le i, j \le 3). \tag{s2}$$

From (33a.22) we deduce $x^2 = x^\sharp + T(x)x - S(x)\mathbf{1}_3$, which combines with (36.4.4), (36.4.8), (36.4.9) to yield

$$\begin{aligned}\eta_i = {} & \xi_j\xi_l - \gamma_j\gamma_l n_C(u_i) + (\xi_i + \xi_j + \xi_l)\xi_i - (\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i)) \\ & - (\xi_l\xi_i - \gamma_l\gamma_i n_C(u_j)) - (\xi_i\xi_j - \gamma_i\gamma_j n_C(u_l))\end{aligned}$$

and then simplifies to

$$\eta_i = \xi_i^2 + \gamma_l\gamma_i n_C(u_j) + \gamma_i\gamma_j n_C(u_l). \tag{s3}$$

Even simpler,

$$v_i = -\xi_i u_i + \gamma_i \overline{u_j u_l} + (\xi_i + \xi_j + \xi_l)u_i,$$

hence

$$v_i = (\xi_j + \xi_l)u_i + \gamma_i \overline{u_j u_l}. \tag{s4}$$

On the other hand, inspecting (36.6.1)and consulting (s3), we obtain

$$v_{11} = \xi_1^2 + \gamma_1\gamma_2 n_C(u_3) + \gamma_3\gamma_1 n_C(u_2) = \eta_1$$

and similarly $v_{ii} = \eta_i$ for $i = 1, 2, 3$. Moreover, by (s4),

$$v_{12} = \gamma_2\xi_1u_3 + \gamma_2\xi_2u_3 + \gamma_2\gamma_3\bar{u}_2\bar{u}_1 = \gamma_2\big((\xi_1 + \xi_2)u_3 + \gamma_3\overline{u_1u_2}\big) = \gamma_2v_3,$$
$$v_{21} = \gamma_1\xi_1\bar{u}_3 + \gamma_1\xi_2\bar{u}_3 + \gamma_3\gamma_1u_1u_2 = \gamma_1\big((\xi_1 + \xi_2)\bar{u}_3 + \gamma_3u_1u_2\big) = \gamma_1\bar{v}_3$$

and, similarly, $v_{jl} = \gamma_lv_i$, $v_{lj} = \gamma_j\bar{v}_i$. This completes the proof of (1).

Next we deal with the first equation of (2) by setting

$$x^3 = \sum(\zeta_ie_{ii} + w_i[jl]) \qquad (\zeta_i \in k,\ w_i \in C,\ 1 \le i \le 3), \tag{s5}$$
$$xx^2 = (w_{ij}) \qquad (w_{ij} \in C,\ 1 \le i, j \le 3). \tag{s6}$$

From (33.9.2) we deduce $x^3 = T(x)x^2 - S(x)x + N(x)\mathbf{1}_3$, and (s3) implies

$$\begin{aligned}\zeta_i = {} & (\xi_i + \xi_j + \xi_l)(\xi_i^2 + \gamma_l\gamma_in_C(u_j) + \gamma_i\gamma_jn_C(u_l))\\ & - \Big((\xi_j\xi_l - \gamma_j\gamma_ln_C(u_i)) + (\xi_l\xi_i - \gamma_l\gamma_in_C(u_j)) + (\xi_i\xi_j - \gamma_i\gamma_jn_C(u_l))\Big)\xi_i\\ & + \xi_i\xi_j\xi_l - \gamma_j\gamma_l\xi_in_C(u_i) - \gamma_l\gamma_i\xi_jn_C(u_j) - \gamma_i\gamma_j\xi_ln_C(u_l) + \gamma_1\gamma_2\gamma_3t_C(u_1u_2u_3).\end{aligned}$$

Expanding and collecting terms gives

$$\zeta_i = \xi_i^3 + \gamma_l\gamma_i(\xi_l + 2\xi_i)n_C(u_j) + \gamma_i\gamma_j(2\xi_i + \xi_j)n_C(u_l) + \gamma_1\gamma_2\gamma_3t_C(u_1u_2u_3). \tag{s7}$$

Much simpler,

$$\begin{aligned}w_i = {} & (\xi_i + \xi_j + \xi_l)((\xi_j + \xi_l)u_i + \gamma_i\overline{u_ju_l})\\ & - (\xi_j\xi_l - \gamma_j\gamma_ln_C(u_i) + \xi_l\xi_i - \gamma_l\gamma_in_C(u_j) + \xi_i\xi_j - \gamma_i\gamma_jn_C(u_l))u_i,\end{aligned}$$

which after a short computation reduces to

$$\begin{aligned}w_i = {} & (\xi_j^2 + \xi_j\xi_l + \xi_l^2 + \gamma_j\gamma_ln_C(u_i)\\ & + \gamma_l\gamma_in_C(u_j) + \gamma_i\gamma_jn_C(u_l))u_i + \gamma_i(\xi_1 + \xi_2 + \xi_3)\overline{u_ju_l}.\end{aligned} \tag{s8}$$

Again inspecting (36.6.1) and using (s3), (s4), we now compute

$$\begin{aligned}w_{11} = {} & \xi_1(\xi_1^2 + \gamma_3\gamma_1n_C(u_2) + \gamma_1\gamma_2n_C(u_3)) + \gamma_1\gamma_2u_3((\xi_1 + \xi_2)\bar{u}_3 + \gamma_3u_1u_2)\\ & + \gamma_3\gamma_1\bar{u}_2((\xi_3 + \xi_1)u_2 + \gamma_2\overline{u_3u_1}),\end{aligned}$$

which by (s7) simplifies to

$$\begin{aligned}w_{11} &= \zeta_1 + \gamma_1\gamma_2\gamma_3(u_3(u_1u_2) + \overline{(u_3u_1)u_2} - (u_3u_1)u_2 - \overline{(u_3u_1)u_2})\\ &= \zeta_1 - \gamma_1\gamma_2\gamma_3[u_1, u_2, u_3]\end{aligned}$$

and, similarly, $w_{ii} = \zeta_i - \gamma_1\gamma_2\gamma_3[u_1, u_2, u_3]$ for $i = 1, 2, 3$. On the other hand,

$$\begin{aligned}w_{23} = {} & \gamma_3\gamma_1\bar{u}_3((\xi_3 + \xi_1)\bar{u}_2 + \gamma_2u_3u_1) + \gamma_3\xi_2((\xi_2 + \xi_3)u_1 + \gamma_1\overline{u_2u_3})\\ & + \gamma_3(\xi_3^2 + \gamma_2\gamma_3n_C(u_1) + \gamma_3\gamma_1n_C(u_2))u_1,\end{aligned}$$

which by (s8) simplifies to $w_{23} = \gamma_3 w_1$. Similarly,

$$w_{32} = \gamma_1\gamma_2 u_2((\xi_1+\xi_2)u_3 + \gamma_3\overline{u_1u_2}) + \gamma_2(\xi_2^2 + \gamma_3\gamma_1 n_C(u_2) + \gamma_1\gamma_2 n_C(u_3))\bar{u}_1$$
$$+ \gamma_2\xi_3((\xi_2+\xi_3)\bar{u}_1 + \gamma_1 u_2u_3) = \gamma_2\bar{w}_1.$$

The same computation yields, more generally, $w_{jl} = \gamma_l w_i$, $w_{lj} = \gamma_j\bar{w}_i$ which completes the proof of the first part of (2).

Equation (1) amounts to saying that the squaring of $\mathrm{Mat}_3(C)$ restricts to the squaring of $J$. After linearizing, therefore, the symmetric matrix product $xy+yx$ of $\mathrm{Mat}_3(C)$ restricts to the circle product $x\circ y$ of $J$. Hence (29.16.2), (1) and the first equation of (2) imply

$$2x^3 = x\circ x^2 = x(xx) + (xx)x = x^3 - \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3] + (xx)x,$$

which yields the second equation of (2). In order to derive (3), we note that (2) holds strictly, so we are allowed to differentiate it at $x$ in the direction $y$. Doing so for the left-hand side,i.e., for $x^3 = U_x x$, we apply (29a.13) and obtain $U_xy + U_{x,y}x = U_xy + x^2\circ y = U_xy + (xx)y + yx^2$. Since the associator of $C$ is alternating, the same procedure applied to the middle term of (2) yields the expression

$$yx^2 + x(yx) + x(xy) + \gamma_1\gamma_2\gamma_3([u_1,u_2,v_3] + [u_2,u_3,v_1] + [u_3,u_1,v_2])\mathbf{1}_3,$$

and comparing, we end up with the first formula of (3). The second one follows by the same argument, using the second formula of (2) instead of the first. Alternatively, we may invoke (29a.10) to conclude

$$2U_xy = x\circ(x\circ y) - x^2\circ y = x(xy+yx) + (xy+yx)x - (xx)y - y(xx)$$
$$= x(yx) + (xy)x - [x,x,y] + [y,x,x],$$

so the second formula of (3) follows from this and the first. Subtracting the middle term of (2) from the right one, we obtain (4). Invoking (33a.22), (33.9.2) and (1), (2), we deduce

$$x^\sharp x = (xx)x - T(x)xx + S(x)x = x^3 - T(x)x^2 + S(x)x + \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3]\mathbf{1}_3$$
$$= (N(x)1_C + \gamma_1\gamma_2\gamma_3[u_1,u_2,u_3]1_C)\mathbf{1}_3,$$

hence (5), while (6) follows from (5) and $xx^\sharp + x^\sharp x = x\circ x^\sharp = 2N(x)\mathbf{1}_3$. Finally, turning to (7), we replace $x$ by $x^\sharp$ in (6) and apply (33a.18) to conclude

$$x^\sharp x^{\sharp\sharp} = (N(x)^2 1_C - \gamma_1\gamma_2\gamma_3[u_1^\sharp,u_2^\sharp,u_3^\sharp])\mathbf{1}_3.$$

On the other hand, the adjoint identity and (5) yield

$$x^\sharp x^{\sharp\sharp} = N(x)x^\sharp x = (N(x)^2 1_C + \gamma_1\gamma_2\gamma_3 N(x)[u_1,u_2,u_3])\mathbf{1}_3,$$

hence (7).

## Solutions for Section 37

**37.19** (a) We provide the solution to Exc. 16.26 with the following supplement. Let $f\colon M \to N$ be a polynomial law over $k$, $\varepsilon \in k$ an idempotent and $x \in M$. Then the identifications

$$M_R = \varepsilon M, \quad x_R = x \otimes \varepsilon = \varepsilon x \qquad (R = \varepsilon k \in k\text{-}\mathbf{alg}, \quad x \in M),$$

ditto for $N$, of 9.7 imply $f_R(\varepsilon x) = f_R(x_R) = f_k(x)_R = \varepsilon f_k(x)$, hence

$$f_R(\varepsilon x) = \varepsilon f_k(x) \qquad (x \in M). \tag{s1}$$

(b) Before dealing with the problem itself, we characterize the various types of idempotents $e \in J$ in the following way.

$$\begin{aligned}
e = 0 \quad &\Longleftrightarrow \quad T(e) = S(e) = N(e) = 0, && \text{(s2)}\\
e \text{ is elementary} \quad &\Longleftrightarrow \quad T(e) = 1, \ \ S(e) = N(e) = 0 && \text{(s3)}\\
&\Longleftrightarrow \quad T(e) = 1, \ \ S(e) = 0,\\
e \text{ is co-elementary} \quad &\Longleftrightarrow \quad T(e) = 2, \ \ S(e) = 1, \ \ N(e) = 0 && \text{(s4)}\\
&\Longleftrightarrow \quad T(e) = 2, \ \ S(e) = 1,\\
e = 1 \quad &\Longleftrightarrow \quad T(e) = S(e) = 3, \ \ N(e) = 1 \quad \Longleftrightarrow \quad N(e) = 1. && \text{(s5)}
\end{aligned}$$

In (s2), the implication from left to right is obvious. Conversely, assume $T(e) = S(e) = N(e) = 0$. Then (33.9.2) implies $e = e^3 = 0$. If $e$ is elementary, then $T(e) = 1$, $e^\sharp = 0$, hence $S(e) = T(e^\sharp) = 0$, while $N(e) = 0$ has been noted in 37.1. Conversely, assume $T(e) = 1$, $S(e) = 0$. Then (33a.22) yields $e^\sharp = e^2 - e = 0$, and $e$ is elementary, proving (s3). In (s4), we have

$$\begin{aligned}
e \text{ is co-elementary} \quad &\Longleftrightarrow \quad 1 - e \text{ is elementary}\\
&\Longleftrightarrow \quad T(1-e) = 1, \ \ S(1-e) = N(1-e) = 0.
\end{aligned}$$

But $T(1-e) = 3 - T(e)$ and $S(1-e) = S(1) - S(1,e) + S(e) = 3 - 2T(e) + S(e)$ by (33a.2), while $N(1-e) = 1 - T(e) + S(e) - N(e)$ by (33a.6), (33a.1). This proves (s4). Finally, if $e = 1$ in (s5), then $T(e) = S(e) = 3$ and $N(e) = 1$ by (33a.1), (33a.2). Conversely, if $N(e) = 1$, then $e \in J^\times$ by Cor. 33.10. Hence $U_e$ is a bijective projection by Prop. 31.2 and Thm. 32.2, which implies $U_e = \mathbf{1}_J$, hence $e = e^2 = U_e 1 = 1$.

(c) Turning, finally, to the solution of the problem, we begin by showing uniqueness, so let $(\varepsilon^{(i)})_{0 \le i \le 3}$ be a complete orthogonal system of idempotents in $k$ with the desired properties. For the sake of clarity, we write $T^{(i)}, S^{(i)}, N^{(i)}$

for the trace, quadratic trace, norm, respectively, of $J^{(i)}$ over $k^{(i)}$. Invoking (s1)–(s5), we obtain

$$\begin{aligned} T(e) &= (\varepsilon^{(i)}T(e))_{0\le i\le 3} = (T^{(i)}(\varepsilon^{(i)}e))_{0\le i\le 3} = (T^{(i)}(e^{(i)}))_{0\le i\le 3} \\ &= (0, \varepsilon^{(1)}, 2\varepsilon^{(2)}, 3\varepsilon^{(3)}) \end{aligned}$$

and, similarly,

$$S(e) = (S^{(i)}(e^{(i)}))_{0\le i\le 3} = (0, 0, \varepsilon^{(2)}, 3\varepsilon^{(3)}), \quad N(e) = (N^{(i)}(e^{(i)}))_{0\le i\le 3} = (0, 0, 0, \varepsilon^{(3)}).$$

Solving this system of linear equations in the unknowns $\varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)}$, we obtain (2)–(4). Now (1) follows from the completeness of the orthogonal system $(\varepsilon^{(i)})$.

(d) In order to prove existence, we define the $\varepsilon^{(i)}$, $0 \le i \le 3$ by (1)–(4) and must show that they have the desired properties. First of all, they clearly add up to 1. Next we have to show that they are orthogonal idempotents, equivalently, that $\varepsilon^{(i)}\varepsilon^{(j)} = 0$ for $0 \le i, j \le 3$, $i \ne j$. To begin with, since $N$ preserves powers by (33a.21), and $e, 1-e$ are idempotents, so are $\varepsilon^{(0)}, \varepsilon^{(3)}$. Moreover, $\varepsilon^{(0)}\varepsilon^{(3)} = N(e)^2N(1-e) = N(U_e(1-e)) = 0$. Summing up, we have proved

$$\varepsilon^{(0)2} = \varepsilon^{(0)}, \quad \varepsilon^{(3)2} = \varepsilon^{(3)}, \quad \varepsilon^{(0)}\varepsilon^{(3)} = 0. \tag{s6}$$

Next we apply (33.9.3) and obtain $e = e^4 = (T(e) - S(e) + N(e))e$, hence $N(1-e)e = 0$. Since $N(1-e) = \varepsilon^{(3)}$ by (s6) is an idempotent, applying $T$ and $S$ to the preceding equation, we end up with

$$N(1-e)e = 0, \quad T(e)N(1-e) = S(e)N(1-e) = 0. \tag{s7}$$

Combining with (2), (3), (s6), we conclude

$$\varepsilon^{(0)}\varepsilon^{(1)} = \varepsilon^{(0)}\varepsilon^{(2)} = 0. \tag{s8}$$

On the other hand, replacing $e$ by $1-e$ in (s7) yields $0 = T(1-e)N(e) = 3N(e) - T(e)N(e)$ and $0 = S(1-e)N(e) = (3 - 2T(e) + S(e))N(e) = 3N(e) - 6N(e) + S(e)N(e)$, hence

$$T(e)N(e) = S(e)N(e) = 3N(e). \tag{s9}$$

This implies $\varepsilon^{(1)}\varepsilon^{(3)} = 3N(e) - 6N(e) + 3N(e) = 0$, $\varepsilon^{(2)}\varepsilon^{(3)} = 3N(e) - 3N(e) = 0$, and we have

$$\varepsilon^{(1)}\varepsilon^{(3)} = \varepsilon^{(2)}\varepsilon^{(3)} = 0. \tag{s10}$$

In view of (s6), (s8), (s10), the $\varepsilon^{(i)}$ will form a complete orthogonal system of idempotents in $k$ once we have shown $\varepsilon^{(1)}\varepsilon^{(2)} = 0$. To this end, we first note

$T(e) = T(e,e) + T(1-e, U_e e) = T(e,e) + T(U_e(1-e), e) = T(e,e)$ by (33a.31) and then apply (33a.13) to conclude $2S(e) = S(e,e) = T(e)^2 - T(e,e)$, hence

$$2S(e) = T(e)^2 - T(e). \tag{s11}$$

Now we expand the last two equations of (s7) by using (s9) and (s11). We obtain $0 = T(e) - T(e)^2 + T(e)S(e) - 3N(e)$, hence

$$T(e)S(e) = 2S(e) + 3N(e), \tag{s12}$$

and $0 = S(e) - 2S(e) - 3N(e) + S(e)^2 - 3N(e)$, hence

$$S(e)^2 = S(e) + 6N(e). \tag{s13}$$

Using (s9), (s12), (s13), we can now compute

$$\begin{aligned}\varepsilon^{(1)}\varepsilon^{(2)} &= T(e)S(e) - 3T(e)N(e) - 2S(e)^2 + 6S(e)N(e) + 3S(e)N(e) - 9N(e)\\ &= 2S(e) + 3N(e) - 9N(e) - 2S(e) - 12N(e) + 27N(e) - 9N(e)\\ &= 0.\end{aligned}$$

Thus $(\varepsilon^{(i)})_{0\le i\le 3}$ is a complete orthogonal system of idempotents in $k$. In particular, we have $e = (e^{(i)})_{0\le i\le 3}$, $e^{(i)} = \varepsilon^{(i)}e \in J^{(i)}$ for $0 \le i \le 3$. From (s7) we deduce $e^{(0)} = N(1-e)e = 0$, while (s1) implies $N^{(3)}(e^{(3)}) = N^{(3)}(\varepsilon^{(3)}e) = \varepsilon^{(3)}N(e) = \varepsilon^{(3)}$, hence $e^{(3)} = 1_{J^{(3)}}$ by (s5). It remains to show that $e^{(1)} \in J^{(1)}$ is elementary and $e^{(2)} \in J^{(2)}$ is co-elementary, which follows from

$$\begin{aligned}T^{(1)}(e^{(1)}) &= T^{(1)}(\varepsilon^{(1)}e) = \varepsilon^{(1)}T(e) = T(e)^2 - 2T(e)S(e) + 3T(e)N(e)\\ &= T(e)^2 - 4S(e) - 6N(e) + 9N(e) = T(e) - 2S(e) + 3N(e) = \varepsilon^{(1)} = 1_{k^{(1)}},\\ S^{(1)}(e^{(1)}) &= S^{(1)}(\varepsilon^{(1)}e) = \varepsilon^{(1)}S(e) = T(e)S(e) - 2S(e)^2 + 3S(e)N(e)\\ &= 2S(e) + 3N(e) - 2S(e) - 12N(e) + 9N(e) = 0\end{aligned}$$

and (s3) in the first case, and from

$$\begin{aligned}T^{(2)}(e^{(2)}) &= T^{(2)}(\varepsilon^{(2)}e) = \varepsilon^{(2)}T(e) = T(e)S(e) - 3T(e)N(e)\\ &= 2S(e) + 3N(e) - 9N(e) = 2(S(e) - 3N(e)) = 2\varepsilon^{(2)} = 2\cdot 1_{k^{(2)}},\\ S^{(2)}(e^{(2)}) &= S^{(2)}(\varepsilon^{(2)}e) = \varepsilon^{(2)}S(e) = S(e)^2 - 3S(e)N(e) = S(e) + 6N(e) - 9N(e)\\ &= S(e) - 3N(e) = \varepsilon^{(2)} = 1_{k^{(2)}}\end{aligned}$$

and (s4) in the second.

**37.20** Applying equation (5) of Exc. 12.40 and the (bilinearized) gradient identity, we expand $N(q) = N(\sum u_i) = \sum N(u_i) + \sum_{i\ne j} T(u_i^\sharp, u_j) + T(u_1\times u_2, u_3) = \sum N(u_i) + T(u_1\times u_2, u_3)$, where (33a.18) implies $N(u_i)^2 = N(u_i^\sharp) = 0$. Since, therefore, the scalars $N(q)$ and $T(u_1\times u_2, u_3)$ differ by a nilpotent element in

$k$, one of them is invertible if and only if so is the other. This proves the first assertion. Now assume $q \in J^\times$ and $T(u_1 \times u_2, u_3) \in k^\times$. From (33a.7) we deduce $T(u_i \times u_j, u_l) = T(u_1 \times u_2, u_3)$. Hence the linear form $x \mapsto T(u_i \times u_j, x)$ from $J$ to $k$ takes $u_l$ to an invertible element in $k$, forcing $u_l \in J$ to be unimodular. The adjoint identity (33a.5) in the special form $N(u_l)u_l = u_l^{\sharp\sharp} = 0$ therefore yields $N(u_l) = 0$. so we have

$$N(q) = T(u_1 \times u_2, u_3); \tag{s1}$$

in particular,

$$p = q^{-1} = N(q)^{-1}q^\sharp = T(u_1 \times u_2, u_3)^{-1} \sum (u_j \times u_l) \tag{s2}$$

since the $u_i$, $1 \le i \le 3$, have $u_i^\sharp = 0$. From (33a.7) we deduce $T(u_j \times u_l, u_j) = 2T(u_j^\sharp, u_l) = 0$ and, similarly, $T(u_j \times u_l, u_l) = 0$. Applying (33.11.2), (33.11.5) and (s2), we not only conclude $u_i^{(\sharp,p)} = N(p)U_q u_i^\sharp = 0$ but also $T^{(p)}(u_i) = T(p, u_i) = N(q)^{-1}T(\sum u_m \times u_n, u_i) = N(q)^{-1}T(u_j \times u_l, u_i) = 1$ by (s1). Thus $u_1, u_2, u_3$ are elementary idempotents in $J^{(p)}$. That they do, in fact, form an elementary frame in that algebra will follow from Prop. 37.4 once we have shown $u_1 \times^{(p)} u_2 = 1^{(p)} - u_1 - u_2 = p^{-1} - u_1 - u_2 = q - u_1 - u_2$. In order to do so, we first linearize (33.11.2) and apply (s1), (s2) to obtain

$$\begin{aligned} u_1 \times^{(p)} u_2 &= N(q)^{-1}U_q(u_1 \times u_2) \\ &= N(q)^{-1}T(q, u_1 \times u_2)q - N(q)^{-1}q^\sharp \times (u_1 \times u_2) \\ &= q - T(u_1 \times u_2, u_3)^{-1} \sum (u_j \times u_l) \times (u_1 \times u_2) \end{aligned} \tag{s3}$$

The term for $i = 3$ in the sum on the very right of (s3) by (33a.10) gives $(u_1 \times u_2) \times (u_1 \times u_2) = 2(u_1 \times u_2)^\sharp = 2(T(u_1^\sharp, u_2)u_2 + T(u_1, u_2^\sharp)u_1 - u_1^\sharp \times u_2^\sharp) = 0$. On the other hand, invoking (33a.9) for $x = u_i$, $y = u_j$, $z = u_l$, we deduce

$$\begin{aligned} (u_i \times u_j) \times (u_i \times u_l) &= T(u_i^\sharp, u_j)u_l + T(u_i^\sharp, u_l)u_j + T(u_i \times u_j, u_l)u_i - u_i^\sharp \times (u_j \times u_l) \\ &= T(u_1 \times u_2, u_3)u_i \end{aligned}$$

Plugging all this this into (s3) we end up with $u_1 \times^{(p)} u_2 = q - u_2 - u_1$, as claimed.

Finally, in order to derive the very last statement of the problem, it suffices to note $\sum e_i = 1$ and apply the previous parts of the problem.

**37.21** (a) follows immediately from Exc. 28.20 (c), Exc. 34.23 and the definition of cubic ideals.

(b) Let $e \in \pi^{-1}(e_0)$ be an idempotent. Then $\pi(e) = e_0$, and with the usual notational conventions, (34.10.6) implies $\pi(e^\sharp) = e_0^\sharp = 0$, so $e^\sharp \in I$ is nilpotent. But it is also an idempotent since (33a.20) implies $e^{\sharp 2} = e^{2\sharp} = e^\sharp$. Summing

up, therefore, $e^\sharp = 0$. It remains to show $T(e) = 1$. From (34.10.5) we deduce $\sigma(T(e)) = T_0(e_0) = 1_{k_0}$, hence $T(e) \in 1_k + \mathfrak{a} \subseteq k^\times$. Thus $e \in J$ is unimodular. On the other hand, (33a.12) and (33a.22) yield $(1 - T(e))e = 0$, hence $T(e) = 1$, as claimed.

**37.22** (a) (i) $\Leftrightarrow$ (ii). Condition (i) implies $\Gamma'\Delta^2\Gamma^\sharp = \Gamma'\Gamma'^\sharp = N(\Gamma')\mathbf{1}_3 = N(\Delta)N(\Gamma)\mathbf{1}_3 = \Delta\Delta^\sharp\Gamma\Gamma^\sharp$. Canceling yields $\Gamma'\Delta = \Delta^\sharp\Gamma$, hence (ii). Thus (i) implies (ii). Conversely, suppose (ii) holds. Then $\Gamma'\Delta = \Delta^\sharp\Gamma$, and taking norms we conclude $N(\Gamma')N(\Delta) = N(\Delta)^2N(\Gamma)$, hence the second relation of (i). Moreover, $\Gamma'^\sharp\Delta^\sharp = (\Gamma'\Delta)^\sharp = (\Delta^\sharp\Gamma)^\sharp = \Delta^{\sharp\sharp}\Gamma^\sharp = N(\Delta)\Delta\Gamma^\sharp = \Delta^2\Delta^\sharp\Gamma^\sharp$, which implies $\Gamma'^\sharp = \Delta^2\Gamma^\sharp$, hence the first relation of (i). Thus (i) holds.

(ii) $\Rightarrow$ (iii). Suppose (ii) holds. Hence so does (i). Since $\varphi := \varphi_{C,\Delta}$ preserves base points, it suffices to show that it preserves adjoints as well (Exc. 34.18). Accordingly, let

$$x = \sum(\xi_i e_{ii} + u_i[jl]) \in \mathrm{Her}_3(C,\Gamma) \qquad (\xi_i \in k,\ u_i \in C,\ i = 1,2,3).$$

Then (36.4.4), (1) imply

$$\varphi(x^\sharp) = \sum(\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i))e_{ii} + \sum(-\delta_i^{-1}\xi_i u_i + \delta_i^{-1}\gamma_i\overline{u_j u_l})[jl]. \qquad \text{(s1)}$$

On the other hand, (1), (36.4.4) and (i), (ii) yield

$$\begin{aligned}\varphi(x)^\sharp &= \sum(\xi_j\xi_l - \gamma'_j\gamma'_l n_C(\delta_i^{-1}u_i))e_{ii} + \sum(-\xi_i\delta_i^{-1}u_i + \gamma'_i\overline{(\delta_j^{-1}u_j)(\delta_l^{-1}u_l)})[jl]\\ &= \sum(\xi_j\xi_l - \delta_i^{-2}\gamma'_j\gamma'_l n_C(u_i))e_{ii} + \sum(-\delta_i^{-1}\xi_i u_i + \delta_j^{-1}\delta_l^{-1}\gamma'_i\overline{u_j u_l})[jl]\\ &= \sum(\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i))e_{ii} + \sum(-\delta_i^{-1}\xi_i u_i + \delta_i^{-1}\gamma_i\overline{u_j u_l})[jl],\end{aligned}$$

and a comparison with (s1) gives the assertion.

Finally, let us assume that (iii) holds and $1_C \in C$ is unimodular. We wish to establish (ii), apply (37.7.4) to compute $\varphi(1_C[li] \times 1_C[ij]) = \varphi(1_C[li]) \times \varphi(1_C[ij])$ and obtain $\delta_i^{-1}\gamma_i 1_C[jl] = \delta_j^{-1}\delta_l^{-1}\gamma'_i 1_C[jl]$. Hence $\gamma'_i 1_C = \delta_j\delta_l\delta_i^{-1}\gamma_i 1_C$, and (ii) follows.

(b) Let $\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3 \in k^\times$. For (i), it suffices to put $\delta_1 = \delta_2 = \delta_3 = \varepsilon$ in (a), while (ii) follows by setting $\delta_i = \varepsilon_j\varepsilon_l$ in (a) since this implies $\delta_j\delta_l\delta_i^{-1} = \varepsilon_l\varepsilon_i\varepsilon_i\varepsilon_j\varepsilon_j^{-1}\varepsilon_l^{-1} = \varepsilon_i^2$. Finally, in (iii), we put $\delta_i = \gamma_i^{-1}$ and have $\gamma'_i = \gamma_j^{-1}\gamma_l^{-1}\gamma_i^2$.

**37.23** $\varphi$ is a linear bijection which obviously preserves units. By Exc. 34.18 (a), therefore, it suffices to show that $\varphi$ preserves adjoints. For

$$x = \sum(\xi_i e_{ii} + u_i[jl]) \in J := \mathrm{Her}_3(C,\Gamma),$$

we note $p^{-1} = \sum\gamma_i^{-1}e_{ii}$ and apply (33.11.2), (36.4.4), Prop. 32.12, (37.8.1) to

conclude

$$\begin{aligned} x^{(\sharp,p)} &= N(p)U_{p^{-1}}x^\sharp = \gamma_1\gamma_2\gamma_3 U_{\sum\gamma_i^{-1}e_{ii}}x^\sharp = \gamma_1\gamma_2\gamma_3\sum(\gamma_i^{-2}U_{e_{ii}}x^\sharp + \gamma_j^{-1}\gamma_l^{-1}U_{e_{jj},e_{ll}}x^\sharp) \\ &= \gamma_1\gamma_2\gamma_3\sum\Big(\gamma_i^{-2}(\xi_j\xi_l - \gamma_j\gamma_l n_C(u_i))e_{ii} + (\gamma_j^{-1}\gamma_l^{-1}(-\xi_i u_i + \gamma_i\overline{u_j u_l}))[jl]\Big) \\ &= \sum\Big(\gamma_i^{-1}(\gamma_j\gamma_l\xi_j\xi_l - \gamma_j^2\gamma_l^2 n_C(u_i))e_{ii} + \gamma_i(-\xi_i u_i + \gamma_i\overline{u_j u_l})[jl]\Big), \end{aligned}$$

hence

$$\begin{aligned} \varphi(x^{(\sharp,p)}) &= \sum\Big(((\gamma_j\xi_j)(\gamma_l\xi_l) - n_C(\gamma_j\gamma_l u_i))e_{ii} + (-(\gamma_i\xi_i)(\gamma_j\gamma_l u_i) + \overline{(\gamma_l\gamma_i u_j)(\gamma_i\gamma_j u_l)})[jl]\Big) \\ &= \Big(\sum((\gamma_i\xi_i)e_{ii} + (\gamma_j\gamma_l u_i)[jl])\Big)^\sharp = \varphi(x)^\sharp, \end{aligned}$$

as claimed.

**37.24** Put

$$(D,\Delta) := (C,\Gamma)^{(p,q)}, \quad \Delta = \operatorname{diag}(\delta_1,\delta_2,\delta_3), \quad \delta_i = \gamma_i^{(p,q)}$$

for $i = 1,2,3$. Then $C = D$ as $k$-modules, and we have

$$\delta_1 = n_C(q)\gamma_1, \quad \delta_2 = n_C(p)\gamma_2, \quad \delta_3 = n_C(pq)^{-1}\gamma_3. \tag{s1}$$

Moreover, from Exc. 17.12 we recall

$$n_D(u) = n_C(pq)n_C(u), \quad \bar{u}^{(p,q)} = n_C(pq)^{-1}\overline{pq}\,\bar{u}\,\overline{pq} = n_C(pq)^{-1}\overline{(pq)u(pq)} \quad (u \in C). \tag{s2}$$

Now let

$$x = \sum(\xi_i e_{ii} + u_i[jl]) \in \mathrm{Her}_3(D,\Delta) \qquad (\xi_i \in k, \;\; u_i \in D, \;\; i = 1,2,3) \tag{s3}$$

and write $\sharp_{p,q}$ for the adjoint of the cubic Jordan matrix algebra $\mathrm{Her}_3(D,\Delta)$. Furthermore, denote by $\eta_i, \zeta_i \in k$, $v_i, w_i \in C$ the quantities satisfying

$$\begin{aligned} x^{\sharp_{p,q}} &= \sum(\eta_i e_{ii} + v_i[jl]) \in \mathrm{Her}_3(D,\Delta), \\ \varphi(x)^\sharp &= \sum(\zeta_i e_{ii} + w_i[jl]) \in \mathrm{Her}_3(C,\Gamma). \end{aligned} \tag{s4}$$

Since

$$\begin{aligned} \varphi(x) &= \sum(\xi_i e_{ii} + u_i'[jl]) \in \mathrm{Her}_3(C,\Gamma), \\ \varphi(x^{\sharp_{p,q}}) &= \sum(\eta_i e_{ii} + v_i'[jl]) \in \mathrm{Her}_3(C,\Gamma), \end{aligned} \tag{s5}$$

where the $u_i', v_i'$ are to be determined by $u_i, v_i$, respectively, via (2), we have to show

$$\eta_i = \zeta_i, \quad v_i' = w_i \qquad (i = 1,2,3). \tag{s6}$$

Reading (36.4.4) in $\mathrm{Her}_3(D,\Delta)$ and invoking (s1), (s2), we compute

$$\begin{aligned}
\eta_1 &= \xi_2\xi_3 - \delta_2\delta_3 n_C(pq)n_C(u_1) = \xi_2\xi_3 - \gamma_2\gamma_3 n_C(p)n_C(u_1)\\
&= \xi_2\xi_3 - \gamma_2\gamma_3 n_C(u_1') = \zeta_1,\\
\eta_2 &= \xi_3\xi_1 - \delta_3\delta_1 n_C(pq)n_C(u_2) = \xi_3\xi_1 - \gamma_3\gamma_1 n_C(q)n_C(u_2)\\
&= \xi_3\xi_1 - \gamma_3\gamma_1 n_C(u_2') = \zeta_2,\\
\eta_3 &= \xi_1\xi_2 - \delta_1\delta_2 n_C(pq)n_C(u_3) = \xi_1\xi_2 - \gamma_1\gamma_2 n_C(pq)^2 n_C(u_3)\\
&= \xi_1\xi_2 - \gamma_1\gamma_2 n_C(u_3') = \zeta_3.
\end{aligned}$$

This proves the first set of equations in (s6). In the second one, we have to show $v_i' = w_i$ for $i = 1,2,3$. The case $i = 3$ is comparatively harmless since

$$\begin{aligned}
v_3' &= (pq)v_3(pq) = (pq)(-\xi_3u_3 + \delta_3\overline{(u_1p)(qu_2)}^{(p,q)})(pq)\\
&= -\xi_3(pq)u_3(pq) + \gamma_3 n_C(pq)^{-1}n_C(pq)^{-1}(pq)(\overline{pq}\,\overline{(u_1p)(qu_2)}\,\overline{pq})(pq)\\
&= -\xi_3u_3' + \gamma_3\overline{u_1'u_2'} = w_3,
\end{aligned}$$

as desired. But the remaining cases $i = 1,2$ are considerably more involved. At a crucial stage, they require an application of (13.5.4) combined with the Moufang identities:

$$\begin{aligned}
v_1' = v_1p &= (-\xi_1u_1 + \delta_1\overline{(u_2p)(qu_3)}^{(p,q)})p =\\
&= -\xi_1u_1p + \gamma_1 n_C(q)n_C(pq)^{-1}\overline{(pq)((u_2p)(qu_3))(pq)}p,
\end{aligned}$$

where

$$\begin{aligned}
(pq)((u_2p)(qu_3))(pq) &= ((pq)(u_2p))((qu_3)(pq)) = (p(qu_2)p)(q(u_3p)q)\\
&= p\big[(qu_2)\big(p(q(u_3p)q)\big)\big] = p\big((qu_2)((pq)u_3(pq))\big)\\
&= p(u_2'u_3').
\end{aligned}$$

Hence Kirmse's identities (17.4.1) yield

$$\begin{aligned}
v_1' &= -\xi_1u_1' + \gamma_1 n_C(p)^{-1}\overline{p(u_2'u_3')}p = -\xi_1u_1' + \gamma_1 n_C(p)^{-1}(\overline{u_2'u_3'}\bar{p})p\\
&= -\xi_1u_1' + \gamma_1\overline{u_2'u_3'} = w_1.
\end{aligned}$$

Similarly,

$$\begin{aligned}
v_2' = qv_2 &= q(-\xi_2u_2 + \delta_2\overline{(u_3p)(qu_1)}^{(p,q)})\\
&= -\xi_2qu_2 + \gamma_2 n_C(p)n_C(pq)^{-1}q\overline{(pq)((u_3p)(qu_1))(pq)},
\end{aligned}$$

where

$$\begin{aligned}(pq)((u_3p)(qu_1))(pq) &= ((pq)(u_3p))((qu_1)(pq)) = (p(qu_3)p)(q(u_1q)q)\\ &= \Big[\Big((p(qu_3)p)q\Big)(u_1p)\Big]q = \Big(((pq)u_3(pq))(u_1p)\Big)q\\ &= (u_3'u_1')q.\end{aligned}$$

Thus

$$\begin{aligned}v_2' &= -\xi_2u_2' + \gamma_2 n_C(q)^{-1}q\overline{(u_3'u_1')q} = -\xi_2u_2' + \gamma_2 n_C(q)^{-1}q(\bar{q}\overline{u_3'u_1'})\\ &= -\xi_2u_2' + \gamma_2\overline{u_3'u_1'} = w_2.\end{aligned}$$

Now (3) follows since multiplying each entry of $\Gamma^{(p,q)}$ by $n_C(pq)$ and clearing squares converts $\Gamma^{(p,q)}$ into $\Gamma'$, so Exc. 37.22 (b) applies.

**37.25** Let $\alpha \in \mathrm{Cent}_{\mathrm{out}}(J)$. We have $[\alpha, U_x] = [\alpha, V_{x,y}] = 0$ for all $x, y \in J$ and must show $\alpha = \xi\mathbf{1}_J$ for some $\xi \in k$. Since $\alpha$ commutes with the Peirce projections relative to the diagonal frame of $J$, it stabilizes the corresponding Peirce components, so there are $\xi_i \in k$ and $k$-linear maps $\varphi_i : C \to C$ such that

$$\alpha e_{ii} = \xi_i e_{ii}, \quad \alpha u_i[jl] = \varphi_i(u_i)[jl] \qquad (\xi_i \in k, \ \ u_i \in C, \ \ i = 1,2,3). \tag{s1}$$

Applying (37.7.6) and (s1), we obtain $\gamma_j\gamma_l\xi_j e_{ll} = U_{1_C[jl]}\xi_j e_{jj} = U_{1_C[jl]}\alpha e_{jj} = \alpha U_{1_C[jl]}e_{jj} = \gamma_j\gamma_l\alpha e_{ll} = \gamma_j\gamma_l\xi_l e_{ll}$, hence

$$\xi_1 = \xi_2 = \xi_3 =: \xi. \tag{s2}$$

Similarly, since $u_i[jl] \circ 1_C[li] = \gamma_l\bar{u}_i[ij]$ by (37.7.4), applying (s1) again gives $\gamma_l\varphi_l(\bar{u}_i)[ij] = \alpha\gamma_l\bar{u}_i[ij] = \alpha V_{1_C[li]}u_i[jl] = V_{1_C[li]}\alpha u_i[jl] = \varphi_i(u_i)[jl] \circ 1_C[li] = \gamma_l\overline{\varphi_i(u_i)}[ij]$, hence

$$\overline{\varphi_i(u_i)} = \varphi_l(\bar{u}_i) \qquad (u_i \in C, \ \ i = 1,2,3) \tag{s3}$$

On the other hand, (s1) and (37.7.5) imply $\gamma_j\gamma_l\overline{\varphi_i(v_i)}[jl] = U_{1_C[jl]}\varphi_i(v_i)[jl] = U_{1_C[jl]}\alpha v_i[jl] = \alpha U_{1_C[jl]}v_i[jl] = \gamma_j\gamma_l\alpha\bar{v}_i[jl] = \gamma_j\gamma_l\varphi_i(\bar{v}_i)[jl]$, hence

$$\overline{\varphi_i(v_i)} = \varphi_i(\bar{v}_i) \qquad (v_i \in C, \ \ i = 1,2,3). \tag{s4}$$

Combining (s3), (s4), we have

$$\varphi_1 = \varphi_2 = \varphi_3 =: \varphi. \tag{s5}$$

By (s2) and (s5), therefore, $\varphi(u_1)[23] = \alpha u_1[23] = \alpha V_{u_1[23]}e_{22} = V_{u_1[23]}\alpha e_{22} = \xi u_1[23] \circ e_{22} = \xi u_1[23]$. Thus $\varphi = \xi\mathbf{1}_C$, and we have shown $\alpha = \xi\mathbf{1}_J$, as claimed.

**37.26** (a) We consider arbitrary elements

$$x = \sum(\xi_i e_{ii} + u_i[jl]), \quad y = \sum(\eta_i e_{ii} + v_i[jl])$$

in $J$, with $\xi_i, \eta_i \in k$, $u_i, v_i \in C$ for $i = 1,2,3$. If $I$ is an ideal in $(C, \iota_C)$ and $I_0 \subseteq I \cap k$ is a weakly $I$-ample ideal in $k$, we must show that $H := H_3(I_0, I, \Gamma)$ is an outer ideal in $J$. For $u \in I$ and $v \in C$ we first note $n_C(u,v) = t_C(u\bar{v}) \in I_0$ since $I \subseteq C$ is an ideal and $I_0$ is weakly $I$-ample. Now assume $y \in H$, i.e., $\eta_i \in I_0$ and $v_i \in I$ for $i = 1,2,3$. Inspecting (36.4.7) and applying the preceding observation, we conclude $T(x,y) \in I_0$, hence $T(x,y)\xi_i \in I_0$ and $T(x,y)u_i \in I_0 C \subseteq IC \subseteq I$. Thus $T(x,y)x \in H$. Moreover, since $I$ is stabilized by $\iota_C$, and by (36.4.6), we have $x \times y \in H$, which after replacing $x$ by $x^\sharp$ implies $U_x y \in H$. Thus $H$ is an outer ideal in $J$. Conversely, let this be so. Then the Peirce projections relative to the diagonal frame of $J$, i.e., $U_{e_{ii}}$ and $U_{e_{jj},e_{ll}}$ for $i = 1,2,3$ stabilize $H$ and Prop. 37.8 yields

$$H = \sum ((H \cap ke_{ii}) + (H \cap C[jl])). \tag{s1}$$

We now put

$$I := \{u \in C \mid u[23] \in H\}, \quad I_0 := \{\xi \in k \mid \xi e_{11} \in H\}, \tag{s2}$$

which are $k$-submodules of $C, k$, respectively. For $u \in I$, we apply (37.7.5) and obtain $\gamma_2\gamma_3\bar{u}[23] = U_{1_C[23]}u[23] \in H$, hence $\bar{u} \in I$. Thus $\bar{I} = I$. From (37.7.4) we conclude that $u[jl] \times v[li] = u[jl] \circ v[li]$ belongs to $H$ if one of the "factors" does. We now claim

$$H \cap C[jl] = I[jl]. \tag{s3}$$

for $i = 1,2,3$. This follows from (s2) for $i = 1$. Arguing by "cyclic induction mod 3", suppose (s3) holds for some $i \in \{1,2,3\}$ and let $u \in C$. If $u \in I$, then $\bar{u} \in I$, and (37.7.4) yields $\gamma_j u[li] = 1_C[ij] \times \bar{u}[jl] \in H$, hence $u[li] \in H$. Conversely, if $u[li] \in H$, the $H$ contains $u[li] \times 1_C[ij] = \gamma_i\bar{u}[jl]$, which implies $\bar{u} \in I$, hence $u \in I$. Thus (s3) holds for $j$ instead of $i$, which completes its proof. Next we claim

$$H \cap ke_{ii} = I_0 e_{ii} \tag{s4}$$

for $i = 1,2,3$. Thanks to (s2), the case $i = 1$ is again obvious. Next suppose (s4) holds for some $i \in \{1,2,3\}$; we must prove it for $j$. Let $\xi \in k$. For $\xi \in I_0$ we obtain $\xi e_{ii} \in H$, so $H$ by (37.7.6) contains $U_{1_C[ij]}\xi e_{ii} = \gamma_j\gamma_i\xi e_{jj}$, hence $\xi e_{jj}$. Conversely, if $\xi e_{jj} \in H$, then $H$ contains $U_{1_C[ij]}\xi e_{jj} = \gamma_i\gamma_j\xi e_{ii}$, and we conclude $\xi \in I_0$. This completes the proof of (s4). Combining (s1) with (s3), (s4), we obtain

$$H = \sum (I_0 e_{ii} + I[jl]), \tag{s5}$$

and it remains to show that (i) $I$ is an ideal in $(C, \iota_C)$, (ii) $I_0 \subseteq I \cap k$, and (iii) $I_0$ is weakly $I$-ample. For $u \in I$, $v \in J$, we combine (37.7.4) with (s3)

to obtain $\gamma_1 uv[23] = \bar{v}[31] \circ \bar{u}[12] \in H$, hence $uv \in I$. Thus $I$, being stable under conjugation, is an ideal in $(C, \iota_C)$, and (i) is proved. Turning to (ii), let $\xi \in I_0$. Then (37.8.1), (32.15.3) imply $C[23] = J_{23} \subseteq J_1(e_{22})$, and (32.2.7) yields $\xi[23] = (\xi 1_C)[23] = e_{22} \circ (\xi 1_C)[23] = (\xi e_{22}) \circ 1_C[23] \in H$, hence $\xi \in I$. This proves (ii). Finally, turning to weak $I$-ampleness, let $u \in I$. Then $H$ contains $\{u[23]e_{22}1_C[23]\} = \gamma_2\gamma_3 t_C(u)e_{33}$ (by (37.7.6) linearized), which implies $t_C(u) \in I_0$ by (s4) and completes the proof (iii).

(b) Let $I$ be an ideal in $(C, \iota_C)$ and $I_0$ an ideal in $k$ that is weakly $I$-ample and contained in $I \cap k$. By (a) it will be enough to show that $H := H(I_0, I, \Gamma)$ is an inner ideal of $J$ if and only if $I_0$ is $I$-ample. Suppose first that $H \subseteq J$ is an inner ideal and let $u \in I$. Then $H$ contains $U_{u[23]}e_{22}$, which by (37.7.6) agrees with $\gamma_2\gamma_3 n_C(u)e_{33}$, and we conclude $n_C(u) \in I_0$. Thus $I_0$ is $I$-ample. Conversely, let this be so. For $x \in H$, i.e., $\xi_i \in I_0$ and $u_i \in I$, $i = 1, 2, 3$, we obtain $T(x, y)\xi_i \in I_0$, $T(x, y)u_i \in I$, hence $T(x, y)x \in H$. Moreover, $x^\sharp \in H$ by (36.4.4) since $I_0$ is $I$-ample. But then $x^\sharp \times y \in H$ after inspecting (36.4.6), and we conclude $U_x y \in H$. Summing up, we have shown that $H \subseteq J$ is an inner ideal.

(c) For $\xi \in I \cap k$ we obtain $2\xi = t_C(\xi 1_C) \in I_0$. Thus $2(I \cap k) \subseteq I_0$. The rest is clear.

(d) Let $H$ be an outer ideal in $J$. The (a) implies $H = H(I_0, I, \Gamma)$ for some ideal $I \subseteq (C, \iota_C)$ and some weakly $I$-ample ideal $I_0$ of $k$ contained in $I \cap k$. By Exc. 19.34, there exists an ideal $\mathfrak{a} \subseteq k$ such that $I = \mathfrak{a}C$ and $I_0 \subseteq I \cap k = \mathfrak{a}$. Since $C$ is regular, its trace form is surjective (Lemma 19.15), so some $u \in C$ has $t_C(u) = 1$. For $\xi \in \mathfrak{a}$, we obtain $\xi u \in I$ and therefore $\xi = t_C(\xi u) \in t_C(I) \subseteq I_0$ by weak $I$-ampleness. This proves $I_0 = \mathfrak{a}$, hence $H = \mathfrak{a}J$ by (1).

Finally, we must show that the homomorphism $\phi$ is injective. By what we have just seen, $\mathrm{Ker}(\phi) = \mathfrak{a}J$ for some ideal $\mathfrak{a} \subseteq k$, so it will be enough to prove $\mathfrak{a} = \{0\}$. But this is clear since $\alpha \in \mathfrak{a}$ implies $\alpha 1_J \in \mathrm{Ker}(\phi)$, hence $\alpha 1_A = \phi(\alpha 1_J) = 0$. But $1_A \in A$ is unimodular, which implies $\alpha = 0$, as claimed.

(e) By Kaplansky's theorem (Prop. 19.9), $C$ is either a regular composition algebra or a purely inseparable field extension $K/F$ of characteristic 2 and exponent at most 1. In the former case, the assertion follows immediately from (d). In the latter case, we first note that the bilinearized norm of $C = K$ is zero and hence $\mathrm{Rad}(T) = H(\{0\}, K, \Gamma)$ is an outer ideal in $J$. Conversely, suppose $H \subseteq J$ is a non-zero outer ideal and write $H = H(I_0, I, \Gamma)$ with $I_0, I$ as in (a). Then $H \neq \{0\}$ implies $I \neq \{0\}$, hence $I = K$, while $I_0 \subseteq I \cap F = F$ is an ideal in $F$, weak $I$-ampleness being automatic. If $I_0 = \{0\}$, then $H = \mathrm{Rad}(T)$, and if $I_0 = F$, then $H = J$. Thus $J$ is simple but nor outer simple.

**37.27** (a) We have $U_x = 0$ and must show $U_{x^\sharp} = 0$, i.e., $U_{x^\sharp}y = 0$ for all $y \in J$. Since cubic Jordan algebras are invariant under base change, viewing $U_{x^\sharp}$ as a polynomial law over $k$ and applying Prop. 12.24 allow us to assume $y \in J^\times$. Then (33.10.1) for $x = y^{-1}$ and (33a.20) imply $U_{x^\sharp}y = N(y)U_{x^\sharp}y^{-1\sharp} = N(y)(U_xy^{-1})^\sharp = 0$.

(b) (i) $\Rightarrow$ (ii). By (i) we have $x^2 = U_x1 = 0$, and since $k$ is reduced, Exc. 34.23 shows $T(x) = S(x) = N(x) = 0$. By (33a.22), therefore, $x^\sharp = x^2 - T(x)x + S(x)1 = 0$. Thus $T(x,y)x = U_xy = 0$, which implies $T(x,y)^2 = T(T(x,y)x,y)) = 0$, hence $T(x,y) = 0$ by our hypothesis on $k$. Summing up, (ii) holds.

(ii) $\Rightarrow$ (i). Obvious, by the formula for the $U$-operator.

(ii) $\Rightarrow$ (iii). The adjoint identity yields $N(x)x = x^{\sharp\sharp} = 0$, and applying the norm we obtain $N(x)^4 = 0$, hence $N(x) = 0$.

(c) Let $x \in J$ be an absolute zero divisor and assume first that $k$ is reduced. Then (b) implies $T(x,y) = T(x^\sharp,y) = N(x) = 0$ for all $y \in J$, and Exc. 34.23 shows $x \in \mathrm{Nil}(J)$.

Next assume that $k$ is arbitrary. Then $\bar{k} := k/\mathrm{Nil}(k) \in k$-**alg** is reduced, and we have a canonical identification $J_{\bar{k}} = \bar{J} := J/\mathrm{Nil}(k)J$ via 9.3, matching $z_{\bar{k}}$ for $z \in J$ with $\bar{z}$, the image of $z$ under the natural map $J \to \bar{J}$. Since $x$ is an absolute zero divisor in $J$, $\bar{x}$ is one in $\bar{J}$, so by the special case just treated we have $\bar{T}(\bar{x},\bar{y}) = \bar{T}(\bar{x}^\sharp,\bar{y}) = \bar{N}(\bar{x}) = 0$ for all $y \in J$, where $\bar{T} = T_{\bar{k}}$ (resp. $\bar{N} = N \otimes \bar{k}$) is the bilinear trace (resp, norm) of $\bar{J}$ over $\bar{k}$. But this means that $T(x,y)$, $T(x^\sharp,y)$, $N(x)$ are nilpotent elements of $k$, for all $y \in J$, which means $x \in \mathrm{Nil}(J)$.

(d) Let $F$ be a field of characteristic 2, $K/F$ a purely inseparable field extension of exponent at most 1, $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{GL}_3(F)$ and $J = \mathrm{Her}_3(K,\Gamma)$. By Exc. 37.26, $J$ is a simple Jordan algebra over $F$. If $u_1,u_2,u_3 \in K$ are not all zero, neither is $x := \sum u_i[jl] \in J$. Moreover, since the bilinearized norm of $K/F$ is zero, (36.4.5) and (36.4.7) show $N(x) = 0$ and $T(x,y) = 0$ for all $y \in J$, so $x$ satisfies condition (iii) of (b). On the other hand,

$$x^\sharp = \sum(\gamma_j\gamma_l n_K(u_i)e_{ii} + \gamma_i u_j u_l[jl]) \neq 0,$$

whence (b) shows that $x$ is *not* an absolute zero divisor of $J$.

(e) First assume $\mathrm{Nil}(J) = \{0\}$. We have seen in Exc. 28.20 (c) that $\mathrm{Nil}(k)J$ is a nil ideal in $J$. This proves $\mathrm{Nil}(k)J = \{0\}$, and in particular $\mathrm{Nil}(k)1 = \{0\}$. But $1 \in J$ is unimodular, and we conclude that $k$ is reduced. Now let $x \in J$ be an absolute zero divisor. Then (b) implies $N(x) = T(x,y) = T(x^\sharp,y) = 0$ for all $y \in J$. From Exc. 34.23 we therefore deduce $x \in \mathrm{Nil}(J)$, hence $x = 0$, and $J$ has no absolute zero divisors. Conversely, let $k$ be reduced and suppose $J$ has no absolute zero divisors. For $x \in \mathrm{Nil}(J)$ and $y \in J$, we have $T(x,y) = T(x^\sharp,y) =$

$N(x) = 0$. This implies $x^{\sharp\sharp} = N(x)x = 0$, so $x^\sharp$ is an absolute zero divisor by (b), forcing $x^\sharp = 0$ by hypothesis. But then, again by (b), $x$ is an absolute zero divisor, and we conclude $x = 0$, as desired.

**37.29** Let $i = 0, 2$. Then $J_i(e) \cap \mathrm{Nil}(J)$ is a nil ideal in $J_i(e)$ and hence contained in $\mathrm{Nil}(J_i(e))$. It therefore remains to prove the converse, i.e.,

$$\mathrm{Nil}\,(J_i(e)) \subseteq \mathrm{Nil}(J) \qquad (i = 0, 2). \tag{s1}$$

In order to do so, we first reduce to the case that $e$ is elementary. Indeed, assume that this case has been settled and let $e$ be arbitrary. Clearly, (s1) holds for $e$ if and only if it holds for the complementary idempotent $1_J - e$. By assumption, therefore, it holds for $e = 0, 1_J$, $e$ elementary and $e$ co-elementary. Applying now Exc. 37.19 and setting $e^{(0)} = 0$, $e^{(1)} = 1_{J^{(3)}}$, we observe that taking nil radicals commutes with direct products of ideals. Hence $J_i(e) = \prod_{l=0}^3 J_i^{(l)}(e^{(l)})$ implies

$$\mathrm{Nil}\,(J_i(e)) = \prod_{l=0}^{3} \mathrm{Nil}\,(J_i^{(l)}(e^{(l)})) \subseteq \prod_{l=0}^{3} \mathrm{Nil}(J_i^{(l)}) = \mathrm{Nil}(J)$$

and completes the reduction. We may thus assume that $e$ is elementary. Let us first consider the case $i = 2$. Since $\mathrm{Nil}(k) = \mathrm{Nil}(k^{(+)})$ and the map $\alpha \mapsto \alpha e$ is an isomorphism from $k^{(+)}$ to $J_2(e) = ke$, Exc. 28.20 (c) implies $\mathrm{Nil}(J_2(e)) = \mathrm{Nil}(k)e \subseteq \mathrm{Nil}(k)J \subseteq \mathrm{Nil}(J)$, as claimed. We are left with the case $i = 0$. Let $x \in \mathrm{Nil}(J_0(e))$ and put $f := 1 - e$. Combining Cor. 37.3 with Exc. 29.21, we conclude $S(x), S(x, y) \in \mathrm{Nil}(k)$ for all $y \in J_0(e)$, hence in particular $T(x) = S(x, f) \in \mathrm{Nil}(k)$. Thus (33a.13) implies $T(x, y) = T(x)T(y) - S(x, y) \in \mathrm{Nil}(k)$ for all $y \in J_0(e)$, and since the Peirce components of $J$ relative to $e$ are orthogonal with respect to the bilinear trace, by Prop. 37.2 (b), this amounts to $T(x, J) \subseteq \mathrm{Nil}(k)$. On the other hand, from Prop. 37.2 (c) we deduce $x^\sharp = S(x)e$, hence in particular, $T(x^\sharp, J) = S(x)T(e, J) \subseteq \mathrm{Nil}(k)$. And finally, $N(f) = N(1 - e) = 1 - T(e) + T(e^\sharp) - N(e) = 0$ and (33a.21) yield $N(x) = N(U_f x) = N(f)^2 N(x) = 0$. Summing up, Exc. 34.23 now shows $x \in \mathrm{Nil}(J)$, and the proof is complete.

**37.30** We put $I_0 := \mathrm{Nil}(k)$, $I := \mathrm{Nil}(C)$. In (1), the inclusion follows from Exc. 16.18 (c). As to the rest, we clearly have $I \cap k \subseteq I_0$, while Exc. 7.13 implies $I_0 \subseteq I_0 C \subseteq I$. By Exc. 37.26 (b), therefore,

$$H_3(I_0, I, \Gamma) = \sum (I_0 e_{ii} + I[jl])$$

is an ideal in $J := \mathrm{Her}_3(C, \Gamma)$. Now let $\xi_i \in I_0$, $u_i \in I$, $\eta_i \in k$, $v_i \in C$ for $i = 1, 2, 3$ and put

$$x := \sum (\xi_i e_{ii} + u_i[jl]) \in H_3(I_0, I, \Gamma), \quad y := \sum (\eta_i e_{ii} + v_i[jl]) \in J.$$

Using Exc. 16.18 (c), (36.4.5), (36.4.7), (36.4.10) and the relation $n_C(u_i, v_i) = t_C(u_i\bar{v}_i)$, one checks that $T(x, y)$, $T(x^\sharp, y)$, $N(x)$ all belong to $I_0$. Hence Exc. 34.23 implies $H_3(I_0, I, \Gamma) \subseteq \mathrm{Nil}(J)$. Conversely, let $x \in \mathrm{Nil}(J)$ and $i = 1, 2, 3$. Then Exc. 37.29 and the Peirce rules show $\xi_i e_{ii} = U_{e_{ii}} x \in J_2(e_{ii}) \cap \mathrm{Nil}(J) = \mathrm{Nil}(J_2(e_{ii})) = I_0 e_{ii}$, and we conclude $\xi_i \in I_0$. On the other hand,

$$u_i[jl] = U_{e_{jj}, e_{ll}} x \in \mathrm{Nil}(J) \cap J_0(e_{ii}) = \mathrm{Nil}\,(J_0(e_{ii})),$$

again by Exc. 37.29. But, by Cor. 37.3, $J_0(e_{ii})$ is the Jordan algebra of the pointed quadratic module $(M_0, S_0, f)$, where $M_0 = J_0(e_{ii})$ as $k$-modules, $S_0 = S|_{M_0}$ and $f = 1_J - e_{ii} = e_{jj} + e_{ll}$. Here Exc. 29.21 and (36.4.9), (36.4.11) imply that $S(u_i[jl]) = -\gamma_j\gamma_l n_C(u_i)$ and $S(u_i[jl], v_i[jl]) = -\gamma_j\gamma_l n_C(u_i, v_i)$ belong to $I_0$ for all $v_i \in C$. From Exc. 17.9 we therefore conclude $u_i \in I$, hence $x \in H_3(I_0, I, \Gamma)$, and (2) follows.

Since $(I_0, I)$ is a conic ideal in $C$ by Exc. 16.25 (b), we deduce from Exc. 16.24 (c) that there exists a unique way of viewing $C_0$ as a conic $k_0$-algebra making $\pi$ a $\sigma$-semi-linear homomorphism of conic algebras, and since $C$ is multiplicative alternative, so is $C_0$. Now put $J_0' := \mathrm{Her}_3(C_0, \Gamma_0)$ as a cubic Jordan matrix algebra over $k_0$ and consider the map $\Phi\colon J \to J_0'$ defined by

$$\Phi\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum(\sigma(\xi_i)e_{ii} + \pi(u_i)[jl]) \tag{s1}$$

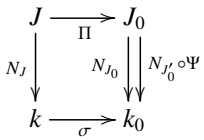
for $\xi_i \in k$, $u_i \in C$, $i = 1, 2, 3$. Obviously, $\Phi$ is $\sigma$-semi-linear preserving base points and, using (16.17.2), one checks that it makes a commutative diagram

$$\begin{array}{ccc} J & \xrightarrow[\Phi]{} & J_0' \\ {\scriptstyle \sharp_J}\downarrow & & \downarrow{\scriptstyle \sharp_{J_0'}} \\ J & \xrightarrow[\Phi]{} & J_0' \end{array}$$

of set maps. Hence, by Exc. 34.22 (b) and (2), $\Phi$ is a surjective $\sigma$-semi-linear homomorphism of cubic Jordan algebras with kernel $\mathrm{Nil}(J)$. By Exec. 37.21, on the other hand, $J_0 := J/\mathrm{Nil}(J)$ carries the unique structure of a cubic Jordan algebra over $k_0$ making the canonical projection $\Pi\colon J \to J_0$ a $\sigma$-semi-linear homomorphism of cubic Jordan algebras. Since $\Phi$ and $\Pi$ are $\sigma$-semi-linear surjective with the same kernel, there is a unique isomorphism $\Psi\colon J_0 \xrightarrow{\sim} J_0'$ of Jordan algebras over $k_0$ such that the diagram

$$\begin{array}{ccc} & J & \\ {\scriptstyle \Pi}\swarrow & & \searrow{\scriptstyle \Phi} \\ J_0 & \overset{\cong}{\underset{\exists!\Psi}{\dashrightarrow}} & J_0' \end{array}$$

commutes. It follows that




with *both* vertical arrows on the right is a commutative $\sigma$-semi-linear polynomial square. Since $\Pi$ is surjective, we conclude $N_{J_0'} \circ \Psi = N_{J_0}$ as cubic forms over $k_0$, whence $\Psi$ may be used to identify $J_0 = J_0'$ as cubic Jordan algebras over $k_0$. this completes the proof.

**37.31** We put

$$M := \{\sum \xi_i e_i \mid \xi_i \in k, \;\; \xi_i J_{ij} = \{0\} \;\text{ for }\; i = 1,2,3\},$$
$$N := \{\sum \xi_i e_i \mid \xi_i^2 = 2\xi_i = 0 \;\text{ for }\; i = 1,2,3\}.$$

By Exc. 29.18 (c), $\mathrm{Rex}(J) \subseteq J$ is an ideal. Thus, given $x = \sum(\xi_i e_i + v_{jl}) \in \mathrm{Rex}(J)$, $\xi_i \in k$, $v_{jl} \in J_{jl}$, its Peirce components relative to $(e_1, e_2, e_3)$ by Prop. 32.12 belong to $\mathrm{Rex}(J)$ as well, so we have $\xi_i e_i, v_{jl} \in \mathrm{Rex}(J)$ for $1 \leq i \leq 3$. Here (32.2.7) and (32.15.2) imply $v_{jl} = e_j \circ v_{jl} = U_{v_{jl},1} e_j = 0$, hence $x = \sum \xi_i e_i$. Similarly, $\xi_i J_{ij} = \xi_i e_i \circ J_{ij} = U_{\xi_i e_i,1} J_{ij} = \{0\}$, and we have shown $\mathrm{Rex}(J) \subseteq M$. Now suppose $x = \sum \xi_i e_i$, $\xi_i \in k$, satisfies $x \in M$, i. e., $\xi_i J_{ij} = \{0\}$ for $1 \leq i \leq 3$. Setting $u_{12} := u_{23} \times u_{31}$, we have $u_{jl} \in J_{jl}$ by Prop. 37.13 and $S(u_{jl}) \in k^\times$ by Lemma 37.14 for $i = 1,2,3$. In particular, $\xi_i^2 S(u_{ij}) = S(\xi_i u_{ij}) = 0$ and $2\xi_i S(u_{ij}) = S(\xi_i u_{ij}, u_{ij}) = 0$ imply $M \subseteq N$, and we have $U_{\xi_i e_i} = 0$. Moreover, the assignment $x \mapsto x \times u_{jl}$ by Lemma 37.14 gives a linear bijection from $J_{ij}$ to $J_{li}$. Hence $\xi_i J_{li} = \xi_i J_{ij} \times u_{jl} = \{0\}$ and then $\xi_i J_{jl} = \xi_i J_{li} \times u_{ij} = \{0\}$. Summing up, we have shown

$$\xi_i J = \sum_m (k\xi_i) e_m,$$

and from the Peirce rules we conclude

$$\{(\xi_i e_i) J J\} = \{e_i (\xi_i J) J\} = \sum_m \{e_i (k\xi_i) e_m J\} = \{e_i e_i (\xi_i J)\} = \sum_m \{e_i e_i (k\xi_i) e_m\}$$
$$= k\xi_i \{e_i e_i e_i\} = 2k\xi_i e_i = \{0\}.$$

But this means $U_{\xi_i e_i, J} = \{0\}$, and we have shown $x = \sum \xi_i e_i \in \mathrm{Rex}(J)$. This completes the proof of (1). Now let $(C, \Gamma)$ be a co-ordinate pair over $k$ and put $(J, \mathfrak{S}) := \mathbf{Her}_3(C, \Gamma)$ as a co-ordinated cubic Jordan algebra over $k$. By (1), and with the notation used before, the elements of $\mathrm{Rex}(J)$ have the form $\sum \xi_i e_{ii}$, $\xi_i \in k$, $\xi_i J_{ij} = 0$ for $1 \leq i \leq 3$. But $J_{ij} = C[ij]$ by Prop. 37.8, and we conclude

$\xi_i C = \{0\}$. In particular, $\xi_i 1_C = 0$, and if $1_C \in C$ is unimodular, we deduce $\xi_i = 0$. Thus the extreme radical of $J$ is zero.

Finally, let $k_0$ be any commutative ring in which $2 = 0$ and let $k := k_0[\varepsilon]$ be the $k_0$-algebra of dual numbers. Then $k_0$ may be viewed as an algebra $C \in k$-**alg** under the homomorphism $k \to k_0$ satisfying $\varepsilon \mapsto 0$. The squaring $\alpha_0 \mapsto \alpha_0^2$ may be regarded as a $k_0$-quadratic map $n_C\colon C \to k$ with zero bilinearization, which is in fact $k$-quadratic since

$$n_C((\beta_0 + \gamma_0\varepsilon)\alpha_0) = n_C(\beta_0\alpha_0) = \beta_0^2 n_C(\alpha_0) = (\beta_0 + \gamma_0\varepsilon)^2 n_C(\alpha_0)$$

for all $\alpha_0, \beta_0, \gamma_0 \in C$. Thus $C$ together with $n_C$ is a multiplicative conic commutative associative $k$-algebra such that $\varepsilon C = \{0\}$, and the extreme radical of $J$ is different from zero.

**37.32** (a) If

$$(C,\Gamma) \xrightarrow[(\eta,\Delta)]{} (C',\Gamma') \xrightarrow[(\eta',\Delta')]{} (C'',\Gamma'')$$

are morphisms of co-ordinate pairs, so obviously is

$$(\eta',\Delta') \circ (\eta,\Delta) := (\eta' \circ \eta, \Delta'\Delta)\colon (C,\Gamma) \longrightarrow (C'',\Gamma''). \tag{s1}$$

It is straightforward to check that we obtain a category in this way, denoted by $k$-**copa**. For example, the identity morphism of $(C,\Gamma)$ is $\mathbf{1}_{(C,\Gamma)} := (\mathbf{1}_C, \mathbf{1}_3)$.

(b) If

$$(J,\mathfrak{S}) \xrightarrow[(\varphi;\delta_1,\delta_2)]{} (J',\mathfrak{S}') \xrightarrow[(\varphi';\delta_1',\delta_2')]{} (J'',\mathfrak{S}'')$$

with $\mathfrak{S}'' = (e_1'', e_2'', e_3'', u_{23}'', u_{31}'')$ are morphisms of co-ordinated cubic Jordan algebras, so is

$$(\varphi';\delta_1',\delta_2') \circ (\varphi;\delta_1,\delta_2) := (\varphi' \circ \varphi; \delta_1'\delta_1, \delta_2'\delta_2)\colon (J,\mathfrak{S}) \longrightarrow (J'',\mathfrak{S}''). \tag{s2}$$

since $(\varphi' \circ \varphi)(e_i) = \varphi'(e_i') = e_i''$ for $i = 1,2,3$ by (iii) and $(\varphi' \circ \varphi)(u_{jl}) = \varphi'(\delta_i^{-1}u_{jl}') = \delta_i'^{-1}\delta_i^{-1}u_{jl}''$ for $i = 1,2$ by (iv).

It is straightforward to check that we obtain a category in this way, denoted by $k$-**cocujo**. For example, the identity morphism of $(J,\mathfrak{S})$ is $\mathbf{1}_{(J,\mathfrak{S})} := (\mathbf{1}_J; 1, 1)$.

(c) Let $\eta\colon C \to C'$ be a homomorphism of multiplicative conic alternative $k$-algebras. We define

$$\mathrm{Her}_3(\eta)\colon\ \mathrm{Her}_3(C,\Gamma) \longrightarrow \mathrm{Her}_3(C',\Gamma)$$

component-wise by

$$\mathrm{Her}_3(\eta)\Big(\sum(\xi_i e_{ii} + u_i[jl])\Big) := \sum(\xi_i e_{ii} + \eta(u_i)[jl]) \tag{s3}$$

for $\xi_i \in k$, $u_i \in C$, $i = 1,2,3$. Strictly speaking, $\mathrm{Her}_3(\eta)$ depends not only on $\eta$

(and thus on $C$ and $C'$) but also on $\Gamma$. However, it will always be clear from the context which $\Gamma$ we have in mind. Since $\eta$ by definition preserves units, norms, traces and conjugations, we easily deduce from (36.4.3)–(36.4.5) that $\mathrm{Her}_3(\eta)$ is a homomorphism of cubic Jordan algebras. Given homomorphisms

$$C \xrightarrow[\eta]{} C' \xrightarrow[\eta']{} C''$$

of multiplicative conic alternative algebras, (s3) easily implies $\mathrm{Her}_3(\eta' \circ \eta) = \mathrm{Her}_3(\eta') \circ \mathrm{Her}_3(\eta)$.

Now 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. We claim that

$$\mathbf{Her}_3(\eta, \Delta) := (\,\mathrm{Her}_3(\eta, \Delta); \delta_1, \delta_2)\colon \mathbf{Her}_3(C, \Gamma) \longrightarrow \mathbf{Her}_3(C', \Gamma') \tag{s4}$$

is a homomorphism of co-ordinated cubic Jordan algebras. Indeed, since $\Gamma' = \Delta^\sharp \Delta^{-1} \Gamma$ by (ii), Exc. 37.22 shows that $\mathrm{Her}_3(\eta, \Delta) = \mathrm{Her}_3(\eta) \circ \varphi_{C,\Delta} = \varphi_{C',\Delta} \circ \mathrm{Her}_3(\eta)$ is a homomorphism of the underlying cubic Jordan algebras and by (1) satisfies $\mathrm{Her}_3(\eta, \Delta)(e_{ii}) = e_{ii}$ for $i = 1, 2, 3$ and $\mathrm{Her}_3(\eta, \Delta)(1_C[jl]) = (\delta_i^{-1} 1_{C'})[jl]$ for $i = 1, 2$.

It is straightforward to check using (1) that in this way we obtain a functor

$$\mathbf{Her}_3\colon k\text{-}\mathbf{copa} \longrightarrow k\text{-}\mathbf{cocujo}. \tag{s5}$$

(d) Writing $T', S'$ for the trace, quadratic trace of $J'$, we put

$$\begin{aligned}
\mathfrak{S} &= (e_1, e_2, e_3, u_{23}, u_{31}), \quad \omega := \omega_{J,\mathfrak{S}}, \\
(C, \Gamma) &:= \mathrm{Cop}(J, \mathfrak{S}) = (C_{J,\mathfrak{S}}, \Gamma_{J,\mathfrak{S}}), \quad \Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3), \\
\mathfrak{S}' &= (e_1', e_2', e_3', u_{23}', u_{31}'), \quad \omega' := \omega_{J',\mathfrak{S}'}, \\
(C', \Gamma') &:= \mathrm{Cop}(J', \mathfrak{S}') = (C_{J',\mathfrak{S}'}, \Gamma_{J',\mathfrak{S}'}), \quad \Gamma' = \mathrm{diag}(\gamma_1', \gamma_2', \gamma_3').
\end{aligned}$$

to deduce from (37.15.1) and (iv)

$$\begin{aligned}
\omega' &= S'(u_{23}')^{-1} S'(u_{31}')^{-1} = S'(\delta_1 \varphi(u_{23}))^{-1} S'(\delta_2 \varphi(u_{31}))^{-1} \\
&= \delta_1^{-2} \delta_2^{-2} S(u_{23})^{-1} S(u_{31})^{-1},
\end{aligned}$$

which amounts to

$$\omega' = \delta_1^{-2} \delta_2^{-2} \omega. \tag{s6}$$

Now let $v, w \in C = J_{12}$. Then (s6) combines with (37.15.3) to imply

$$\begin{aligned}
\varphi_{12}(v)\varphi_{12}(w) &= \omega'(\varphi(v) \times u_{23}') \times (u_{31}' \times \varphi(w)) \\
&= \delta_1^{-2} \delta_2^{-2} \delta_1 \delta_2 \omega(\varphi(v) \times \varphi(u_{23})) \times (\varphi(u_{31}) \times \varphi(w)) \\
&= \delta_1^{-1} \delta_2^{-1} \omega \varphi((v \times u_{23}) \times (u_{31} \times w)) = \delta_1^{-1} \delta_2^{-1} \varphi_{12}(vw),
\end{aligned}$$

and we conclude

$$\varphi_{12}(vw) = \delta_1\delta_2\varphi_{12}(v)\varphi_{12}(w) \qquad (v, w \in C = J_{12}). \tag{s7}$$

In accordance with (2), we now define $\eta := \delta_1\delta_2\varphi_{12} \colon C \to C'$. Given $v, w \in C$ and applying (s7), we deduce $\eta(vw) = \delta_1\delta_2\varphi_{12}(vw) = \delta_1\delta_2\varphi_{12}(v)\delta_1\delta_2\varphi_{12}(w) = \eta(v)\eta(w)$, so $\eta$ is an algebra homomorphism which by (37.15.6), (37.15.4), (s6) satisfies $\eta(1_C) = \delta_1\delta_2\varphi(u_{23} \times u_{31}) = \delta_1\delta_2\varphi(u_{23}) \times \varphi(u_{31}) = u'_{23} \times u'_{31} = 1_{C'}$, $n_{C'}(\eta(v)) = -\omega' S'(\delta_1\delta_2\varphi(v)) = -\delta_1^2\delta_2^2\omega' S'(\varphi(v)) = -\omega S(v) = n_C(v)$. Summing up we have thus shown that $\eta \colon C \to C'$ is a homomorphism of conic algebras, so condition (i) holds for $(\eta, \Delta)$. We now verify condition (ii). An application of (37.15.10) yields $\gamma'_1 = -S'(u'_{31}) = -\delta_2^2 S'(\varphi(u_{31})) = -\delta_2^2 S(u_{31})$, $\gamma'_2 = -S'(u'_{23}) = -\delta_1^2 S'(\varphi(u_{23})) = -\delta_1^2 S(u_{23})$, and we conclude

$$\gamma'_1 = \delta_2^2\gamma_1, \quad \gamma'_2 = \delta_1^2\gamma_2, \quad \gamma'_3 = \gamma_3 = 1. \tag{s8}$$

In view of (2), (s8), we therefore have $\delta_2\delta_3\delta_1^{-1}\gamma_1 = \delta_2\delta_1\delta_2\delta_1^{-1}\gamma_1 = \delta_2^2\gamma_1 = \gamma'_1$, $\delta_3\delta_1\delta_2^{-1}\gamma_2 = \delta_1\delta_2\delta_1\delta_2^{-1}\gamma_2 = \delta_1^2\gamma_2 = \gamma'_2$, $\delta_1\delta_2\delta_3^{-1}\gamma_3 = \gamma_3 = \gamma'_3$, which comes down to $\delta_j\delta_l\delta_i^{-1}\gamma_i = \gamma'_i$ for $i = 1, 2, 3$, hence to $\Gamma' = \Delta^\sharp\Delta^{-1}\Gamma$, and we have shown that condition (ii) holds as well. Thus $\mathrm{Cop}(\varphi; \delta_1, \delta_2)$ is indeed a morphism of co-ordinate pairs. It remains to show compatibility with compositions, so let

$$(J, \mathfrak{S}) \xrightarrow[(\varphi;\delta_1,\delta_2)]{} (J', \mathfrak{S}') \xrightarrow[(\varphi';\delta'_1,\delta'_2)]{} (J'', \mathfrak{S}''),$$

be morphisms of co-ordinated cubic Jordan algebras. Setting $\Delta' := \mathrm{diag}(\delta'_1, \delta'_2, \delta'_3)$, $\delta'_3 := \delta'_1\delta'_2$, gives

$$\Delta'\Delta = \mathrm{diag}\,(\delta'_1\delta_1, \delta'_2\delta_2, (\delta'_1\delta_1)(\delta'_2\delta_2))$$

Applying (2), we therefore conclude

$$\begin{aligned}
\mathrm{Cop}(\varphi'_1; \delta'_1, \delta'_2) \circ \mathrm{Cop}(\varphi; \delta_1, \delta_2) &= (\delta'_1\delta'_2\varphi'_{12}, \Delta') \circ (\delta_1\delta_2\varphi_{12}, \Delta) \\
&= (\delta'_1\delta'_2\delta_1\delta_2\varphi'_{12} \circ \varphi_{12}, \Delta'\Delta) \\
&= \Big((\delta'_1\delta_1)(\delta'_2\delta_2)(\varphi' \circ \varphi)_{12}, \mathrm{diag}\,(\delta'_1\delta_1, \delta'_2\delta_2, (\delta'_1\delta_1)(\delta'_2\delta_2))\Big) \\
&= \mathrm{Cop}(\varphi' \circ \varphi; \delta'_1\delta_1, \delta'_2\delta_2) = \mathrm{Cop}\,((\varphi'; \delta'_1, \delta'_2) \circ (\varphi; \delta_1, \delta_2)),
\end{aligned}$$

and the assertion follows. Thus we have indeed a functor

$$\mathrm{Cop} \colon k\text{-}\mathbf{cocujo} \longrightarrow k\text{-}\mathbf{copa}.$$

(e) We employ the standard notation of 37.10 for the co-ordinated cubic Jordan algebra $(J, \mathfrak{S}) := \mathbf{Her}_3(C, \Gamma)$ and then combine (37.15.2) with Prop. 37.8 to

conclude $C' = J_{12} = C[12]$ as $k$-modules, giving the first assertion. Applying (37.11.1), (37.11.2), (37.15.1), (36.4.9), we obtain

$$\omega = S(1_C[23])^{-1}S(1_C[31])^{-1} = (-\gamma_2\gamma_3 n(1_C))^{-1}(-\gamma_3\gamma_1 n(1_C))^{-1},$$

hence

$$\omega = \gamma_1^{-1}\gamma_2^{-1}\gamma_3^{-2}. \tag{s9}$$

Now, for $v, w \in C$, the multiplication in $C'$ by (37.15.3), (s9), (37.7.4) may be expressed as

$$\begin{aligned} v[12]w[12] &= \omega(v[12] \times 1_C[23]) \times (1_C[31] \times w[12]) = \gamma_1^{-1}\gamma_2^{-1}\gamma_3^{-2}\gamma_2\gamma_1\bar{v}[31] \times \bar{w}[23] \\ &= \gamma_3^{-2}\gamma_3\overline{\bar{w}\bar{v}}[12] = \gamma_3^{-1}(vw)[12], \end{aligned}$$

which amounts to

$$(vw)[12] = \gamma_3 v[12]w[12] \qquad (v, w \in C). \tag{s10}$$

Similarly, combining (37.15.6) and (37.11.1) with (37.7.4) yields $1_{C'} = 1_C[23] \times 1_C[31] = \gamma_3\bar{1}_C[12]$, hence

$$1_{C'} = \gamma_3 1_C[12]. \tag{s11}$$

Also, using (37.15.4), (36.4.9), we obtain

$$n_{C'}(v[12]) = -\omega S(v[12]) = -\gamma_1^{-1}\gamma_2^{-1}\gamma_3^{-2}(-\gamma_1\gamma_2 n_C(v)),$$

which may be summarized to

$$n_{C'}(v[12]) = \gamma_3^{-2} n_C(v) \qquad (v \in C). \tag{s12}$$

Invoking (s10)–(s12), the map $\psi := \psi_{C,\Gamma}$ satisfies

$$\begin{aligned} \psi(vw) &= \gamma_3(vw)[12] = \gamma_3 v[12]\gamma_3 w[12] = \psi(v)\psi(w), \\ \psi(1_C) &= \gamma_3 1_C[12] = 1_{C'}, \\ n_{C'}(\psi(v)) &= n_{C'}(\gamma_3 v[12]) = \gamma_3^2\gamma_3^{-2} n_C(v) = n_C(v) \end{aligned}$$

for all $v, w \in C$. Hence $\psi\colon C \to C'$ is an isomorphism of conic algebras. Finally, setting $\Gamma' = \operatorname{diag}(\gamma_1', \gamma_2', \gamma_3')$ and observing (37.15.10), (37.11.1), we deduce $\gamma_1' = -S(1_C[31]) = \gamma_3\gamma_1 n_C(1_C)$, $\gamma_2' = -S(1_C[23]) = \gamma_2\gamma_3 n_C(1_C)$, which yields

$$\gamma_1' = \gamma_3\gamma_1, \quad \gamma_2' = \gamma_2\gamma_3, \quad \gamma_3' = 1. \tag{s13}$$

Combining (s13) with (5), we obtain $\lambda_2\lambda_3\lambda_1^{-1}\gamma_1 = \gamma_3\gamma_1 = \gamma_1'$, $\lambda_3\lambda_1\lambda_2^{-1}\gamma_2 = \gamma_3\gamma_2 = \gamma_2'$, $\lambda_1\lambda_2\lambda_3^{-1}\gamma_3 = \gamma_3^{-1}\gamma_3 = 1 = \gamma_3'$, which may be unified to $\lambda_j\lambda_l\lambda_i^{-1}\gamma_i =$

$\gamma_i'$. Thus, setting $\Lambda := \Lambda_{C,\Gamma}$, we see $\Gamma' = \Lambda^\sharp \Lambda^{-1}\Gamma$. Hence $\Psi_{C,\Gamma}$ is an isomorphism of co-ordinate pairs, as claimed.

(f) This is clear since $\Phi = \Phi_{J,\mathfrak{S}}$ as defined in Thm. 37.17 matches *exactly* the diagonal co-ordinate system of $\mathrm{Her}_3(C,\Gamma)$ with the co-ordinate system $\mathfrak{S}$ of $J$.

(g) It suffices to show

(v) that the $\Phi_{J;\mathfrak{S}}$ for all co-ordinated cubic Jordan algebras $(J,\mathfrak{S})$ over $k$ determine an isomorphism

$$\mathbf{Her}_3 \circ \mathrm{Cop} \xrightarrow{\sim} \mathrm{Id}_{k\text{-}\mathbf{cocujo}}$$

of functors from $k$-**cocujo** to itself and, similarly,

(vi) that the $\Psi_{C,\Gamma}$ for all co-ordinate pairs $(C,\Gamma)$ over $k$ determine an isomorphism

$$\mathrm{Id}_{k\text{-}\mathbf{copa}} \xrightarrow{\sim} \mathrm{Cop} \circ \mathbf{Her}_3$$

of functors from $k$-**copa** to itself.

We begin with (v). Given a co-ordinated cubic norm structure $(J,\mathfrak{S})$ over $k$, Thm. 37.17 shows that

$$\Phi_{J,\mathfrak{S}} \colon (\mathbf{Her}_3 \circ \mathrm{Cop})(J,\mathfrak{S}) \xrightarrow{\sim} (J,\mathfrak{S})$$

is an isomorphism in $k$-**cocujo**. Thus, by [23, Def. 1.3, p. 23], the proof will be complete once we have shown that any homomorphism $(\varphi;\delta_1,\delta_2)\colon (J,\mathfrak{S}) \to (J',\mathfrak{S}')$ of co-ordinated cubic Jordan algebras gives rise to a commutative diagram

$$\begin{array}{ccc} (\mathbf{Her}_3 \circ \mathrm{Cop})(J,\mathfrak{S}) & \xrightarrow[\Phi_{J,\mathfrak{S}}]{\cong} & (J,\mathfrak{S}) \\ \downarrow{\scriptstyle (\mathbf{Her}_3\circ\mathrm{Cop})(\varphi;\delta_1,\delta_2)} & & \downarrow{\scriptstyle (\varphi;\delta_1,\delta_2)} \\ (\mathbf{Her}_3 \circ \mathrm{Cop})(J',\mathfrak{S}') & \xrightarrow[\Phi_{J',\mathfrak{S}'}]{\cong} & (J',\mathfrak{S}'). \end{array} \tag{s14}$$

In order to establish the commutativity of (s14), we write $S$ (resp. $S'$) for the quadratic trace of $J$ (resp. $J'$); moreover, we put $\mathfrak{S} = (e_1,e_2,e_3,u_{23},u_{31})$, $\mathfrak{S}' = (e_1',e_2',e_3',u_{23}',u_{31}')$.

Applying (7), we first obtain $(\varphi;\delta_1,\delta_2)\circ\Phi_{J,\mathfrak{S}} = (\varphi;\delta_1,\delta_2)\circ(\phi_{J,\mathfrak{S}};1,1)$, hence

$$(\varphi;\delta_1,\delta_2) \circ \Phi_{J,\mathfrak{S}} = (\varphi \circ \phi_{J,\mathfrak{S}};\delta_1,\delta_2). \tag{s15}$$

On the other hand, setting

$$\eta := \delta_1\delta_2\varphi_{12}, \quad \Delta := \mathrm{diag}(\delta_1, \delta_2, \delta_1\delta_2) \in \mathrm{Diag}_3(k)^\times, \tag{s16}$$

we deduce from (s4)), (s16) that

$$\begin{aligned}\Phi_{J',\mathfrak{S}'} \circ \mathbf{Her}_3(\,\mathrm{Cop}(\varphi;\delta_1,\delta_2)) &= (\phi_{J',\mathfrak{S}'};1,1) \circ \mathbf{Her}_3(\eta,\Delta)\\ &= (\phi_{J',\mathfrak{S}'};1,1) \circ (\,\mathrm{Her}_3(\eta,\Delta);\delta_1,\delta_2)\\ &= (\phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta);\delta_1,\delta_2),\end{aligned}$$

so in view of (s15), it suffices to show

$$\varphi \circ \phi_{J,\mathfrak{S}} = \phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta). \tag{s17}$$

In order to do so, we write $(C,\Gamma) := \mathrm{Cop}(J,\mathfrak{S})$ (resp. $(C',\Gamma') = \mathrm{Cop}(J',\mathfrak{S}')$). Combining (37.17.1) with condition (a), (i) of Exc. 37.22, we obtain $\varphi\circ\phi_{J,\mathfrak{S}}(e_{ii}) = \varphi(e_i) = e'_i = \phi_{J',\mathfrak{S}'}(e_{ii}) = \phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta)(e_{ii})$ for $i = 1,2,3$, so it remains to show that both sides of (s17) agree on $v_i[jl]$, for all $v_i \in C = J_{12}$, $i = 1,2,3$. Since $\eta$ as defined in (s16), being an isomorphism of conic algebras, preserves conjugations, so does every scalar multiple of it, in particular $\varphi_{12}$. With this in mind, we apply (37.17.3), (s16) and obtain

$$\begin{aligned}\varphi \circ \phi_{J,\mathfrak{S}}(v_1[23]) &= -S(u_{31})^{-1}\varphi(u_{31} \times \bar{v}_1) = -S'(\varphi(u_{31}))^{-1}\varphi(u_{31}) \times \varphi(\bar{v}_1)\\ &= -S'(\delta_2^{-1}u'_{31})^{-1}\delta_2^{-1}u'_{31} \times \varphi_{12}(\bar{v}_1) = -\delta_2^2\delta_2^{-1}S'(u'_{31})^{-1}u'_{31} \times \overline{\varphi_{12}(v_1)}\\ &= -\delta_2 S'(u'_{31})^{-1}u'_{31} \times \overline{\varphi_{12}(v_1)} = \delta_2\phi_{J',\mathfrak{S}'}(\varphi_{12}(v_1)[23])\\ &= \phi_{J',\mathfrak{S}'}(\delta_1^{-1}(\delta_1\delta_2\varphi_{12})(v_1)[23]) = \phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta)(v_1[23]).\end{aligned}$$

Similarly,

$$\begin{aligned}\varphi \circ \phi_{J,\mathfrak{S}}(v_2[31]) &= -S(u_{23})^{-1}\varphi(u_{23} \times \bar{v}_2) = -S'(\varphi(u_{23}))^{-1}\varphi(u_{23}) \times \varphi(\bar{v}_2)\\ &= -S'(\delta_1^{-1}u'_{23})^{-1}\delta_1^{-1}u'_{23} \times \varphi_{12}(\bar{v}_2) = -\delta_1^2\delta_1^{-1}S'(u'_{23})^{-1}u'_{23} \times \overline{\varphi_{12}(v_2)}\\ &= -\delta_1 S'(u'_{23})^{-1}u'_{23} \times \overline{\varphi_{12}(v_2)} = \delta_1\phi_{J',\mathfrak{S}'}(\varphi_{12}(v_2[31]))\\ &= \phi_{J',\mathfrak{S}'}(\delta_2^{-1}(\delta_1\delta_2\varphi_{12})(v_2[31])) = \phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta)(v_2[31]).\end{aligned}$$

And, finally,

$$\begin{aligned}\varphi \circ \phi_{J,\mathfrak{S}}(v_3[12]) &= \varphi(v_3) = \varphi_{12}(v_3) = \phi_{J',\mathfrak{S}'}(\varphi_{12}(v_3)[12])\\ &= \phi_{J',\mathfrak{S}'}((\delta_1\delta_2)^{-1}(\delta_1\delta_2\varphi_{12})(v_3)[12]) = \phi_{J',\mathfrak{S}'} \circ \mathrm{Her}_3(\eta,\Delta)(v_3[12]).\end{aligned}$$

Summing up, this completes the proof of (s17), and we have shown that the diagram (s14) commutes. Thus (v) holds.

It remains to establish (vi). To this end, we let $(\eta,\Delta)\colon (C,\Gamma)\to(C',\Gamma'))$ be a morphism of co-ordinate triples and must show that the diagram

$$\begin{array}{ccc}(C,\Gamma) & \xrightarrow[\Psi_{C,\Gamma}]{\cong} & (\mathrm{Cop}\circ\mathbf{Her}_3)(C,\Gamma)\\ \Big\downarrow{\scriptstyle(\eta,\Delta)} & & \Big\downarrow{\scriptstyle(\mathrm{Cop}\circ\mathbf{Her}_3)(\eta,\Delta)}\\ (C',\Gamma') & \xrightarrow[\Psi_{C',\Gamma'}]{\cong} & (\mathrm{Cop}\circ\mathbf{Her}_3)(C',\Gamma').\end{array} \tag{s18}$$

commutes. We begin by making the specifications

$$\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3),\quad \Gamma' = \mathrm{diag}(\gamma_1',\gamma_2',\gamma_3'), \tag{s19}$$

$$(\hat{C},\hat{\Gamma}) := \mathrm{Cop}\,(\mathbf{Her}_3(C,\Gamma)),\quad \hat{\Gamma} = \mathrm{diag}(\hat{\gamma}_1,\hat{\gamma}_2,\hat{\gamma}_3), \tag{s20}$$

$$(\hat{C}',\hat{\Gamma}') := \mathrm{Cop}\,(\mathbf{Her}_3(C',\Gamma')),\quad \hat{\Gamma}' = \mathrm{diag}(\hat{\gamma}_1',\hat{\gamma}_2',\hat{\gamma}_3'). \tag{s21}$$

We abbreviate $\Psi_{C,\Gamma}=(\psi,\Lambda)$, $\Psi_{C',\Gamma'}=(\psi',\Lambda')$ and deduce from (5)) that

$$\Lambda = \mathrm{diag}(\lambda_1,\lambda_2,\lambda_3),\quad \lambda_1=\lambda_2=1,\quad \lambda_3=\gamma_3, \tag{s22}$$

$$\Lambda' = \mathrm{diag}(\lambda_1',\lambda_2',\lambda_3'),\quad \lambda_1'=\lambda_2'=1,\quad \lambda_3'=\gamma_3'. \tag{s23}$$

Hence $\Psi_{C',\Gamma'}\circ(\eta,\Delta)=(\psi',\Lambda')\circ(\eta,\Delta)$, and (s1)) implies

$$\Psi_{C',\Gamma'}\circ(\eta,\Delta)=(\psi'\circ\eta,\Lambda'\Delta), \tag{s24}$$

where (4) yields

$$(\psi'\circ\eta)(v)=\gamma_3'\eta(v)[12] \qquad (v\in C). \tag{s25}$$

On the other hand, writing $\Delta=\mathrm{diag}(\delta_1,\delta_2,\delta_3)$ and invoking (s23), we obtain

$$\Lambda'\Delta=\mathrm{diag}(\delta_1,\delta_2,\gamma_3'\delta_3). \tag{s26}$$

Next we use (s4) to compute

$$\mathrm{Cop}\,(\mathbf{Her}_3(\eta,\Delta)) = \mathrm{Cop}\Big(\big(\mathrm{Her}_3(\eta,\Delta);\delta_1,\delta_2\big)\Big),$$

where

$$\mathrm{Cop}\,(\mathbf{Her}_3(\eta,\Delta))=(\hat{\eta},\hat{\Delta}),\quad \hat{\eta}:=\delta_1\delta_2\,\mathrm{Her}_3(\eta,\Delta)_{12},\quad \hat{\Delta}:=\mathrm{diag}(\delta_1,\delta_2,\delta_1\delta_2). \tag{s27}$$

From $(\hat{\eta},\hat{\Delta})\circ\Psi_{C,\Gamma}=(\hat{\eta},\hat{\Delta})\circ(\psi,\Lambda)$ we therefore deduce

$$(\mathrm{Cop}\circ\mathbf{Her}_3)(\eta,\Delta)\circ\Psi_{C,\Gamma}=(\hat{\eta}\circ\psi,\hat{\Delta}\Lambda). \tag{s28}$$

Given $v \in C$, we observe $\Gamma' = \Delta^\sharp \Delta^{-1}\Gamma$ (since $(\eta, \Delta)$ is a morphism in $k$-**copa**), which yields

$$\begin{aligned}(\hat\eta \circ \psi)(v) &= \hat\eta(\psi_{C,\Gamma}(v)) = \gamma_3 \hat\eta(v[12]) = \delta_1\delta_2\gamma_3 \operatorname{Her}_3(\eta, \Delta)_{12}(v[12]) \\ &= \delta_1\delta_2\delta_3^{-1}\gamma_3\eta(v)[12] = \gamma_3'\eta(v)[12] = (\psi' \circ \eta)(v).\end{aligned}$$

Thus $\hat\eta \circ \psi = \psi' \circ \eta$. Moreover, by (s27), (s22), (s23),

$$\begin{aligned}\hat\Delta\Lambda &= \operatorname{diag}(\delta_1, \delta_2, \delta_1\delta_2)\operatorname{diag}(1, 1, \gamma_3) = \operatorname{diag}(\delta_1, \delta_2, \delta_1\delta_2\gamma_3) \\ &= \operatorname{diag}(\delta_1, \delta_2, \delta_3\gamma_3') = \operatorname{diag}(1, 1, \gamma_3')\operatorname{diag}(\delta_1, \delta_2, \delta_3) = \Lambda'\Delta.\end{aligned}$$

Comparing now (s24) with (s28), we see that the diagram (s18) commutes, which completes the proof of (vi).

## Solutions for Section 38

**38.19** (a) Define polynomial laws $f\colon M \to k$ and $g\colon M \to M$ by $f(u) := q(u)^2$, $g(u) := q(u)u$ for all $u \in M_R$, $R \in k$-**alg**. Note that $f$ is a bi-quadratic form, while $g$ is homogeneous of degree 3. Combining the first and second order product rules (12.17.7), (12.17.8) with (12.17.2), (12.17.3), we conclude that

$$\begin{aligned}(Df)(u, v) &= 2q(u)q(u, v) \\ (D^2 f)(u, v) &= q(u, v)^2 + 2q(u)q(v), \\ (Dg)(u, v) &= q(u, v)u + q(u)v\end{aligned}$$

hold strictly for $u, v \in M$. Fixing $v \in M$, the cubic form $h_v\colon M \to k$ defined by $h_v(u) := 2q(u)q(u, v)$ for $u \in M_R$, $R \in k$-**alg** satisfies

$$(Dh_v)(u, w) = 2\big(q(u, v)q(u, w) + q(u)q(v, w)\big)$$

strictly for $u, w \in M$. It now follows from a repeated application of Exc. 12.36 (b) that (1) holds strictly if and only if (1)–(5) hold over $k$.

Non-trivial weird quadratic modules exist, as the following simple example shows. Let $k_0$ be a commutative ring, $I$ a $k_0$-module and $k := k_0 \oplus I$ the split-null extension of $k_0$ by $I$. Regard any $k_0$-module $M_0$ as a $k$-module $M$ by letting $I$ act trivially on $M_0$. We claim that *any quadratic form $q\colon M \to k$ taking values in $I$ makes $(M, q)$ a weird quadratic module over $k$.* Indeed, since $I$ kills $M$ and $I^2 = \{0\}$ in $k$, not only (1) but also (2)–(5) hold over $k$, which proves the assertion.

(b) Localizing if necessary and invoking Exc. 12.36 (a), we may assume that $M$ is free of rank at least 2. Let $(e_i)_{i\in I}$ be a basis of $M$ over $k$. Given $i, j \in I$

distinct, (5) implies $q(e_i, e_j)e_i + q(e_i)e_j = 0$, hence $q(e_i) = q(e_i, e_j) = 0$. Thus $q = 0$.

(c) Put $\mathbf{M}_0 := (M_0, q_0, e_0)$ with $M_0 := ke_0$ and $q_0 \colon M_0 \to k$ being the quadratic form given by $q_0(\xi_0 e_0) := \xi_0^2$ for $\xi_0 \in k$. Then $\mathbf{M}_0$ is a pointed quadratic $k$-module whose (bi-)linear trace and conjugation have the form $t_0(\xi_0 e_0) = 2\xi_0$, $t_0(\xi_0 e_0, \eta_0 e_0) = 2\xi_0\eta_0$ and $\overline{\xi_0 e_0} = \xi_0 e_0$ for $\xi_0, \eta_0 \in k$. Let $M_0$ act bilinearly on $M_1 := M$ by $e_0 \,.\, u := u$ for all $u \in M$ and define a quadratic map $Q \colon M_1 \to M_0$ by $Q(u) := q(u)e_0$ for all $u \in M$. Then $\mathbf{M}_1 := (M_1, \,.\,, Q)$ is a Peirce-one extension of $\mathbf{M}_0$, and comparing (38.9.1)–(38.9.4) with (6)–(9) we see that $X = X(\mathbf{M}_0, \mathbf{M}_1)$ is indeed a cubic array such that (10)–(14) hold. By Prop. 38.10, therefore, $X$ is a cubic norm structure if and only if (38.10.1)–(38.10.6) are strictly fulfilled. After the specifications described above (38.10.1)–(38.10.3), (38.10.5) are trivial, while (38.10.4), (38.10.6) amount to the strict validity of (1). Thus $X$ is a cubic norm structure if and only if $(M, q)$ is weird. The remaining assertions in (c) now follow from the final statement of Prop. 38.10.

(d) Basically, the arguments in the solution to (c) will be read backwards. Write $X$ for the cubic norm structure underlying $J$. By definition, $e := 1 - c$ is an elementary idempotent in $J$ having $e_0 := 1 - e = c$. With $M := J_1(e)$, the Peirce decomposition of $J$ relative to $e$ therefore attains the form

$$X = ke \oplus M \oplus ke_0, \tag{s1}$$

where $ke$, $ke_0$ are free $k$-modules of rank 1. We put $M_0 := ke_0$ and define $q_0 \colon M_0 \to k$ by $q(\xi_0 e_0) := \xi_0^2$ for $\xi_0 \in k$ to obtain a pointed quadratic module $\mathbf{M}_0 = (M_0, q_0, e_0)$ whose (bi-)linear trace and conjugation are respectively given by $t_0(\xi_0 e_0) = 2\xi_0$, $t_0(\xi_0 e_0, \eta_0 e_0) = 2\xi_0\eta_0$ and $\overline{\xi_0 e_0} = \xi_0 e_0$ for $\xi_0, \eta_0 \in k$. Applying the formalism of 38.7, there exists a quadratic form $q \colon M \to k$ such that the quadratic map $Q$ of (38.7.10) may be written as $Q(u) = q(u)e_0$ for all $u \in M$. With these specifications, and in view of (32.2.7), formulas (38.7.11), (38.7.12) are converted to (8), (9), which therefore hold strictly in $X$. But $X$ is a cubic norm structure . Hence (c) implies that $(M, q)$ is a weird quadratic module. By its very definition, the cubic norm structure underlying $J' := J_{\mathrm{cub}}(M, q)$ identifies canonically with $X$. Thus $J \cong J'$ under an isomorphism matching $e_0 = c \in J$ with $e_0 \in J'$.

**38.20** Let $X, X'$ be two cubic norm structures over $k$ such that $J(X) = J = J(X')$ as abstract Jordan algebras. We must show $X = X'$ and clearly have $X = J = X'$ as $k$-modules as well as $1_X = 1_J = 1_{X'}$. Put $N := N_X - N_{X'}$, $T := T_X - T_{X'}$, $S := S_X - S_{X'}$. Then (33.9.2) implies that

$$T(x)x^2 - S(x)x + N(x)1_J = 0 \tag{s1}$$

holds strictly for all $x \in J$. Let $\mathfrak{p} \in \operatorname{Spec}(k)$ and $K$ an algebraic closure of $k(\mathfrak{p})$. Then the composite map

$$\vartheta : k \longrightarrow k/\mathfrak{p} \longrightarrow k(\mathfrak{p}) \longrightarrow K$$

has kernel $\mathfrak{p}$ and makes $K$ a $k$-algebra. Let $\varphi \in \{T, S, N\}$ and $x \in J_K$. If $\Xi_K^J(x) \neq 0$, then (s1) shows $\varphi_K(x) = 0$. Thus $((\varphi \otimes K)(\Xi^J \otimes K))_K = 0$, and Exc. 12.35 (b) implies $\varphi \otimes K = 0$, in particular $\varphi_K = 0$ as a set map $J_K \to K$. Given $x \in J$, we therefore conclude $0 = \varphi_K(x_K) = \varphi(x)_K = \vartheta(\varphi(x))$, hence $\varphi(x) \in \mathfrak{p}$. This is true for all $\mathfrak{p} \in \operatorname{Spec}(k)$, i.e.,

$$\varphi(x) \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}(k)} \mathfrak{p} = \operatorname{Nil}(k) = \{0\},$$

and we have shown

$$T_X(x) = T_{X'}(x), \quad S_X(x) = S_{X'}(x), \quad N_X(x) = N_{X'}(x) \qquad (x \in J), \tag{s2}$$

which by (33a.22) implies

$$x^{\sharp_X} = x^{\sharp_{X'}} \qquad (x \in J) \tag{s3}$$

Writing $\times_X, \times_{X'}$ for the bilinearizations of $\sharp_X, \sharp_{X'}$, respectively, we deduce from (s2), (s3) that

$$(X, 1_X, \sharp_X, \times_X, T_X, N_X) = (X', 1_{X'}, \sharp_{X'}, \times_{X'}, T_{X'}, N_{X'})$$

as rational cubic norm structures in the sense of Exc. 34.20. This exercise therefore implies $X = X'$ as ordinary cubic norm structures.

**38.21** (a) Put $\mathfrak{a} := \operatorname{Nil}(k)$, $I := \operatorname{Nil}(J)$. If $x \in I$, then $T(x, J) + T(x^\sharp, J) \subseteq \mathfrak{a}$ by Exc. 34.23. In particular, $\xi = T(x, e) \in \mathfrak{a}$ by (38.9.10). Moreover, $x_0 = U_{e_0} x \in J_0(e) \cap I = \operatorname{Nil}(J_0(e))$ by Exc. 37.29, and Exc. 29.21 implies $q_0(x_0), q_0(x_0, y_0) \in \mathfrak{a}$ for all $y_0 \in M_0$. Next, by (38.9.10) we have $t_0(Q(x_1, y_1)) = T(x, y_1) \in \mathfrak{a}$ for all $y_1 \in M_1$ and, finally,

$$q_0(Q(x_1), y_0) = t_0(Q(x_1), \bar{y}_0) = -T(x^\sharp, \bar{y}_0) + \xi q_0(x_0, \bar{y}_0) \in \mathfrak{a}$$

for all $y_0 \in M_0$ by (38.9.3), (38.9.10) and by what we have seen before. Hence all the quantities of (2) belong to $\mathfrak{a}$. Conversely, let this be so. Then $t_0(x_0, y_0) = q_0(x_0, \bar{y}_0) \in \mathfrak{a}$ for all $y_0 \in M_0$ by (29b.4) and $T(x, J) \subseteq \mathfrak{a}$ by (38.9.10). For $y = (\eta e, y_1, y_0)$, $\eta \in k$, $y_i \in M_i$, $i = 0, 1$, we apply (38.9.3), (38.9.10) to conclude

$$T(x^\sharp, y) = q_0(x_0)\eta + \xi q_0(x_0, y_0) - q_0(Q(x_1), \bar{y}_0) + t_0(Q(x_0 \,.\, x_1, y_1)).$$

By hypothesis, all summands on the right with the possible exception of the last belong to $\mathfrak{a}$. But since (38.10.5) implies that

$$t_0(Q(x_0 \,.\, x_1, y_1)) = t_0(x_0, Q(x_1, y_1)) = q_0(x_0, \overline{Q(x_1, y_1)})$$

belongs to $\mathfrak{a}$ as well, so does $T(x^\sharp, y)$. Finally, (38.9.4) combined with (2) yields $N(x) \in \mathfrak{a}$, and summing up, we have shown $x \in I$.

(b) (i) $\Rightarrow$ (ii). By Exc. 37.29, the nil radical of $J_2(e) \cong k^{(+)}$ is zero. Hence $k$ is reduced and, by (a), $q_0$ is non-degenerate.

(ii) $\Rightarrow$ (iii). By (a), (38.10.4) and (ii), an element $x$ as in (1) belongs to $\mathrm{Nil}(J)$ if and only if $\xi = 0$, $x_0 = Q(x_1) = 0$, and $t_0(Q(x_1, y_1)) = 0$ for all $y_1 \in M_1$. Hence (iii) holds.

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

**38.22** From condition (iii) of (b) in Exc. 38.21 we conclude $Q(x_1) \neq 0$. We clearly have $T(e') = 1$, while (38.9.3) implies

$$e'^\sharp = \Big(q_0(Q(x_1)), -Q(x_1) \,.\, x_1, -\overline{Q(x_1)} - Q(x_1)\Big),$$

where $q_0(Q(x_1)) = 0$ by (38.10.4) and $Q(x_1) \,.\, x_1 = t_0(Q(x_1))x_1$ (by (38.10.6)) $= 0$. Hence $e'^\sharp = 0$, i.e., $e'$ is an elementary idempotent. Put $e'_0 := 1_J - e' = (0, -x_1, e_0 + Q(x_1))$. For $y = (\eta e, y_1, y_0)$, $\eta \in k$, $y_i \in M_i$, $i = 0, 1$, we apply (38.9.10) and obtain

$$\begin{aligned} T(e'_0, y) &= T\Big((0, -x_1, e_0 + Q(x_1)), (\eta e, y_1, y_0)\Big) \\ &= t_0(Q(x_1), y_0) = q_0(Q(x_1), \bar{y}_0). \end{aligned}$$

Since $Q(x_1) \neq 0$, $q_0(Q(x_1)) = 0$ and $q_0$ is non-degenerate by Exc. 38.21 (b), some $y_0 \in M_0$ has $T(e'_0, y) = q_0(Q(x_1), \bar{y}_0) \neq 0$. Now write $y = \eta' e' + y'_1 + y'_0$, $\eta' \in k$, $y'_i \in J_i(e')$, $i = 0, 1$. Since the Peirce components of $J$ relative to $e'$ are orthogonal with respect to the bilinear trace of $J$, we may apply Cor. 37.3 to $e'$ to obtain $0 \neq T(e'_0, y) = T(e'_0, y'_0) = t'_0(y'_0)$, and the problem is solved.

**38.23** For $r > 2$, we are in case (i), by Thm. 38.17. For $r = 1$, we are in case (iii), so we may assume $r = 2$. Thanks to Exc. 34.27 it suffices to show that *there exists a pointed quadratic space* $(M, q, e)$ *over* $k$ *satisfying* $J = J(M, q, e)$ *as abstract Jordan algebras.* By faithfully flat descent, combining Thm. 38.6 with Exercises. 25.35 and 29.26, there is no harm in assuming that $J$ contains an elementary idempotent $c$. Put $d := 1_J - c$. For all $\mathfrak{p} \in \mathrm{Spec}(k)$, the idempotent $c(\mathfrak{p}) \in J(\mathfrak{p})$ continues to be elementary, forcing $d(\mathfrak{p}) \neq 0$ by 37.1. By Lemma 9.17, therefore, $d \in J$ is unimodular. Thus, by the Peirce rules, $kc \times kd$ is not only free of rank 2 but also a direct summand of $J$ as a $k$-module. This implies $J = kc \times kd$ as a direct product of ideals, and one checks that the hyperbolic quadratic form $q\colon J \to k, \xi c + \eta d \mapsto \xi\eta$, gives rise to a pointed quadratic

space $(M, q, e)$, $M := J$, $e := 1_J$, satisfying $J = J(M, q, e)$ as abstract Jordan algebras.

## Solutions for Section 39

**39.37** If $\varphi_K\colon M_K \to N_K$ is bijective for all fields $K \in k$-**alg**, then in particular so is $\varphi(\mathfrak{p})\colon M(\mathfrak{p}) \to N(\mathfrak{p})$, for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Then a standard consequence of Nakayama's lemma (as in the solution to 9.32) implies that $\varphi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is bijective for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Thus $\varphi\colon M \to N$ is bijective. The converse is obvious.

Now suppose $J$ is a cubic Jordan algebra over $k$ that is finitely generated projective as a $k$-module and makes $T_K\colon M_K \times M_K \to K$ a non-degenerate symmeetric bilinear form over $K$, for all fields $K \in k$-**alg**. Since $J_K$ has finite dimension over $K$, the natural map $J \to J^*$ (the dual module of $J$) induced by $T$ becomes an isomorphism when extending scalars from $k$ to $K$. By the first part of the exercise, therefore, the natural map in question must be an isomorphism to begin with, i.e., $J$ is regular.

**39.38** Since passing from $(C, \Gamma)$ to $J$ is compatible with base change, the specific nature of the conditions imposed on $J$ (resp. $C$) allows us to assume that $k = K$ is a field, in which case we have to show that $J$ is semi-simple, i.e., $\operatorname{Nil}(J) = \{0\}$, if and only if the quadratic form $n_C$ is non-degenerate. But this follows immediately from Exercises 37.30 and 17.9 combined:

$$\operatorname{Nil}(J) = \{0\} \;\Leftrightarrow\; \operatorname{Nil}(C) = \{0\} \;\Leftrightarrow\; n_C \text{ is non-degenerate.}$$

**39.39** (i) $\Rightarrow$ (ii). By (36.4.4), condition (i) is equivalent to

$$\alpha_j\alpha_l = \gamma_j\gamma_l n_C(v_i), \quad \alpha_i v_i = \gamma_i \overline{v_j v_l} \qquad (i = 1, 2, 3), \tag{s1}$$

which in turn implies

$$\gamma_1\gamma_2\gamma_3 v_1(v_2v_3) = (\gamma_2\gamma_3 v_1)(\gamma_1 v_2 v_3) = \gamma_2\gamma_3\alpha_1 v_1\bar{v}_1 = \alpha_1\gamma_2\gamma_3 n_C(v_1)1_C = \alpha_1\alpha_2\alpha_3 1_C,$$

and (ii) holds.

(ii) $\Rightarrow$ (iii). Assume that (ii) holds. We first claim

$$\gamma_1\gamma_2\gamma_3(v_1v_2)v_3 = \alpha_1\alpha_2\alpha_3 1_C. \tag{s2}$$

If $v_1 = 0$, then $\alpha_2\alpha_3 = \gamma_2\gamma_3 n_C(v_1) = 0$, forcing $\alpha_1\alpha_2\alpha_3 = 0$, and (s2) holds. Similarly, if $v_2 = 0$, then $\alpha_3\alpha_1 = \gamma_3\gamma_1 n_C(v_2) = 0$, and we have again $\alpha_1\alpha_2\alpha_3 = 0$, hence (s2). Thus we may assume $v_1 \neq 0 \neq v_2$. Multiplying

the second equation of (ii) from the left first by $\bar{v}_1$, then by $\bar{v}_2$ and invoking Krimse's identities as well as the fact that $C$ is multiplicative (Prop. 17.6) and its conjugation is an involution (Prop. 17.2 (a)), we obtain

$$\gamma_1\gamma_2\gamma_3 n_C(v_1)v_2v_3 = \alpha_1\alpha_2\alpha_3\bar{v}_1,$$
$$\gamma_1\gamma_2\gamma_3 n_C(v_1v_2)v_3 = \gamma_1\gamma_2\gamma_3 n_C(v_1)n_C(v_2)v_3 = \alpha_1\alpha_2\alpha_3\bar{v}_2\bar{v}_1 = \alpha_1\alpha_2\alpha_3\overline{v_1v_2}.$$

On the other hand, multiplying the left-hand side of (s2) by $\overline{v_1v_2}$ from the left gives

$$\gamma_1\gamma_2\gamma_3 n_C(v_1v_2)v_3 = \gamma_1\gamma_2\gamma_3\overline{v_1v_2}\big((v_1v_2)v_3\big).$$

In the expressions on the very right of the last two displayed equations, we may cancel the factor $\overline{v_1v_2}$ since $C$ has no zero divisors and arrive at (s2). Applying (s2), we now obtain

$$\gamma_1\gamma_2\gamma_3\bar{v}_3\big(v_3(v_1v_2)\big) = \gamma_1\gamma_2\gamma_3 n_C(v_3)v_1v_2 = \gamma_1\gamma_2\gamma_3\big((v_1v_2)v_3\big)\bar{v}_3 = \alpha_1\alpha_2\alpha_3\bar{v}_3.$$

Hence

$$\gamma_1\gamma_2\gamma_3 v_3(v_1v_2) = \alpha_1\alpha_2\alpha_3 1_C \tag{s3}$$

provided $v_3 \neq 0$. But if $v_3 = 0$, then the first equation of (ii) yields $\alpha_1\alpha_2 = \gamma_1\gamma_2 n_C(v_3) = 0$, hence $\alpha_1\alpha_2\alpha_3 = 0$, and (s3) holds in full generality. We have thus arrived at both displayed equations of (iii) for $(ijl) = (123)$ and at the second one for $(ijl) = (312)$, i.e., for the right shift of (123). Repeating the preceding arguments if necessary, we may therefore conclude that (iii) holds.

Finally, suppose $k$ is an integral domain and $\gamma_i \neq 0$ for $i = 1, 2, 3$. Then we must show (iii) $\Rightarrow$ (i), so assuming (iii), we must establish (s1). For $i = 1, 2, 3$ we obtain

$$\begin{aligned}\gamma_j\gamma_l v_i(\gamma_i v_j v_l) &= \gamma_1\gamma_2\gamma_3 v_i(v_jv_l) = \alpha_1\alpha_2\alpha_3 1_C\\ &= \alpha_i\alpha_j\alpha_l 1_C = \alpha_i\gamma_j\gamma_l n_C(v_i)1_C = \gamma_j\gamma_l v_i(\alpha_i\bar{v}_i).\end{aligned}$$

This proves $\alpha_i\bar{v}_i = \gamma_i v_j v_l$, hence the second equation of (s1), if $v_i \neq 0$. But of $v_i = 0$, then $\alpha_j\alpha_l = \gamma_j\gamma_l n_C(v_i) = 0$, forcing $\alpha_j = 0$ or $\alpha_l = 0$ since $k$ is an integral domain, which in turn gives $0 = \alpha_i\alpha_j = \gamma_i\gamma_j n_C(v_l)$ in the former case and $0 = \alpha_l\alpha_i = \gamma_l\gamma_i n_C(v_j)$ in the latter. Since $C$ has no zero divisors, its norm represents zero only trivially (Exc. 18.20). Therefore $v_j = 0$ or $v_l = 0$, and the proof of (s1) is complete.

**39.40** The first (resp. second) part of (a) follows by applying 25.3 to $f|_N : N \to M'$ (resp. to $\pi \circ f : M \to M'/N'$, $\pi : M' \to M'/N'$ being the canonical projection). In (b) we apply (a) with $N' = P$ to the natural embedding $i : N \to M$. For (c), we consider the canonical map $\bigoplus_{\alpha\in I} N_\alpha \to M$ determined

by the inclusions $N_\alpha \to M$ and apply 25.3. Finally, in (d), we let $M^0$ be a free $k$-module with basis $(e_\alpha)_{\alpha\in I}$ and apply 25.3 to the $k$-linear map $M^0 \to M$, $e_\alpha \mapsto x_\alpha$, $\alpha \in I$.

**39.41** (a) Let $R \in k$-**alg** be a flat $k$-algebra. As usual, for a submodule $M \subseteq J$, we identify $M_R \subseteq J_R$ canonically. Any $x \in \mathrm{Sq}(J)$ may be written as $x = \sum \alpha_j x_j^2$, $\alpha_j \in k$, $x_j \in J$, and we conclude $x_R = \sum \alpha_{jR}(x_{jR})^2 \in \mathrm{Sq}(J_R)$. This show $\mathrm{Sq}(J)_R \subseteq \mathrm{Sq}(J_R)$. Conversely, let $x \in \mathrm{Sq}(J_R)$. Then $x = \sum r_j x_j^2$, $r_j \in R$, $x_j \in J_R$, and writing $x_j = \sum_m x_{mj} \otimes r_{mj}$, $x_{mj} \in J$, $r_{mj} \in R$, we obtain

$$x = \sum_{j,m} x_{mj}^2 \otimes r_j r_{mj}^2 + \sum_{j,m<n} (x_{mj} \circ x_{nj}) \otimes (r_j r_{mj} r_{nj}) \in \mathrm{Sq}(J)_R.$$

Summing up, we have shown $\mathrm{Sq}(J)_R = \mathrm{Sq}(J_R)$.

Next assume that $J$ is split. The assertion $\mathrm{Sq}(J) = J$ is trivial for $n = 1$ and obvious for $n = 3$ since $\mathrm{Sq}(J)$ contains all idempotents. Let us therefore assume $n \geq 6$. By definition (39.20), we may assume $J = \mathrm{Her}_3(C)$, where $C$ is a split composition algebra of rank $\frac{n-3}{3}$ over $k$. The diagonal of $\mathrm{Her}_3(C)$ clearly belongs to $\mathrm{Sq}(J)$. Furthermore, for $i = 1, 2, 3$ and $u_i \in C$, we note $u_i[jl] \in J_1(e_{jj})$ by Prop. 37.8 and (32.15.3). Hence (32.2.7), (33a.22), (36.4.8), (36.4.9) imply

$$\begin{aligned}(e_{jj} + u_i[jl])^2 &= e_{jj}^2 + e_{jj} \circ u_i[jl] + u_i[jl]^2 \\ &= e_{jj} + u_i[jl] + u_i[jl]^\sharp + T(u_i[jl])u_i[jl] - S(u_i[jl])1_J \\ &= e_{jj} + u_i[jl] - n_C(u_i)e_{ii} + n_C(u_i)1_J,\end{aligned}$$

which in turn shows $C[jl] \subseteq \mathrm{Sq}(J)$. Thus $\mathrm{Sq}(J) = J$ if $J$ is split.

Finally, let $J$ be arbitrary. Cor. 39.32 yields a faithfully flat $k$-algebra $R \in k$-**alg** making $J_R$ a split Freudenthal algebra of rank $n$ over $R$. By what we have just seen, $\mathrm{Sq}(J)_R = \mathrm{Sq}(J_R) = J_R$. Hence the inclusion $\mathrm{Sq}(J) \to J$ becomes an isomorphism after changing scalars from $k$ to $R$ and thus, by faithful flatness, must have been one all along. In other words, $\mathrm{Sq}(J) = J$.

(b) It suffices to prove the following implications.

1°. *If $\mathfrak{a} \subseteq k$ is an ideal, then so is $\mathfrak{a}J \subseteq J$.* Obvious.

2°. *If $I \subseteq J$ is an outer ideal, then $I \cap k \subseteq k$ is an ideal.* This is clear since outer ideals of $J$ are, in particular, $k$-submodules.

3°. *If $\mathfrak{a} \subseteq k$ is an ideal, then $\mathfrak{a} = (\mathfrak{a}J) \cap k$.* For $\alpha \in \mathfrak{a}$ we have $\alpha = \alpha 1_J \subseteq (\mathfrak{a}J) \cap k$, so the left-hand side is contained in the right. Conversely, let $\alpha \in (\mathfrak{a}J) \cap k$. Then $\alpha \in k$ satisfies $\alpha 1_J = \sum \alpha_i x_i$, $\alpha_i \in \mathfrak{a}$, $x_i \in J$. Since $1_J \in J$ is unimodular, some linear form $\lambda\colon J \to k$ has $\lambda(1_J) = 1$, hence $\alpha = \sum \alpha_i \lambda(x_i) \in \mathfrak{a}$.

4°. *If $I \subseteq J$ is an outer ideal, then* $(I \cap k)J = I$. Let $\alpha \in I \cap k$ and $x \in J$. Then $\alpha \in k$ and $\alpha 1_J \in I$. Since $I \subseteq J$ is an outer ideal, we conclude $\alpha x^2 = U_x(\alpha 1_J) \in I$, and (a) implies $\alpha J = \alpha \operatorname{Sq}(J) \subseteq I$. Hence $(I \cap k)J \subseteq I$.

In order to prove equality, we first assume that $J = \operatorname{Her}_3(C)$ is split, $C$ a split composition algebra of rank $\frac{n-3}{3}$ over $k$. Since regularity of $J$ is inherited by $C$, Exc. 37.26 yields an ideal $\mathfrak{b} \subseteq k$ such that

$$I = \mathfrak{b} \operatorname{Her}_3(C) = H_3(\mathfrak{b}, \mathfrak{b}C, \mathbf{1}_3) = \sum (\mathfrak{b}e_{ii} + (\mathfrak{b}C)[jl]),$$

hence $I \cap k = \mathfrak{b}$ and $(I \cap k)J = \mathfrak{b}J = I$.

Finally, let $J$ be arbitrary and apply Cor. 39.32 to find a faithfully flat $k$-algebra $R \in k$-**alg** making $J_R$ split of rank $n$ over $R$. Let $y \in I$ and write $x \in J_R$ as $x = \sum x_i \otimes r_i$, $x_i \in J$, $r_i \in R$. Then

$$U_x y = \sum (U_{x_i} y) \otimes r_i^2 + \sum_{i<j} \{x_i y x_j\} \otimes (r_i r_j) \in I_R$$

since $I \subseteq J$ is an outer ideal. Thus $U_x I_R = R(U_x I) \subseteq R I_R = I_R$, and we have shown that $I_R \subseteq J_R$ is an outer ideal. Now we combine Exc. 39.40 (c),(d) to compute

$$((I \cap k)J)_R = (I \cap k)_R J_R = (I_R \cap k_R)J_R = (I_R \cap R)J_R = I_R.$$

But this means that the inclusion $(I \cap k)J \to I$ becomes an isomorphism when extending scalars from $k$ to $R$, which by arguing as before completes the proof of 4°.

**39.42** (a) The second statement follows immediately from the first combined with 25.25 (ii). Since elementary frames are invariant under base change, the defining equation for $\mathbf{Elfr}(J)$ does indeed define a subfunctor of $J^3_{\mathbf{a}}$. Let $u_1^*, \dots, u_m^*$ be a finite set of generators of $J^*$, the dual of the $k$-module $J$. Then

$$\begin{aligned}\mathbf{Elfr}(J)(R) = \{(e_1, e_2, e_3) \in J_R \mid\ & T_J(e_j) = 1, \\ & \langle u_{iR}^*, e_j^\sharp \rangle = \langle u_{jR}, e_1 \times e_2 - e_3 \rangle = 0 \ \ (0 \le i \le m,\ j = 1, 2)\}\end{aligned}$$

for all $R \in k$-**alg**, and we conclude from 24.15, 25.11, Exercises 25.32 and 25.31 (b) that $\mathbf{X} := \mathbf{Elfr}(J)$ is a finitely presented closed subscheme of $J^3_{\mathbf{a}}$; 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 frame of $J_{R/\mathfrak{a}} = J_R/\mathfrak{a}J_R$ can be lifted to an elementary frame of $J_R$. But this follows from Exercises 32.25, 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 $I := \mathrm{Nil}(J_K)$. Then $\bar{J} := J_K/\mathrm{Nil}(J_K)$ is semi-simple cubic Jordan $K$-algebra of dimension at least 3, and by Exercises 32.25 and 37.21 (b) again, we will be through once we have shown that $\bar{J}$ contains two orthogonal elementary idempotents. Thanks to Thm. 39.6, we may assume $J = F^{(+)} \times J(M,q,e)$, where $(M,q,e)$ is a non-degenerate pointed quadratic module of dimension at leas 2 over $K$. We must show that $J(M,q,e)$ contains an elementary idempotent, i.e., by 29.13, an element $c$ having $q(c) = 0$ and $q(c,e) = 1$. If not, then $q(x) = 0$ implies $q(x,e) = 0$, for all $x \in M$, and from the Hilbert Nullstellensatz we deduce $q(x) = q(x,e)^2$ for all $x \in M$. But this contradicts non-degeneracy of $q$, so $\mathbf{X}(K) \neq \emptyset$, and the solution of (a) is complete.

(b) Since $J$ is regular, it will be enough to show that there is a *unique* bilinear multiplication $J \times J \to J$, $(x,y) \mapsto xy$, making $J$ a cubic commutative associative $k$-algebra $E$ such that $E^{(+)} = J$ as cubic Jordan algebras. Since $J$ is regular, it is separable (Exc. 34.23), so by (a) and faithfully flat descent, we may assume that $J$ contains an elementary frame $\Omega = (e_1, e_2, e_3)$. Since the corresponding Peirce components of $J$ are orthogonal relative to the bilinear trace (Prop. 37.4 (c)), $J_0 := \sum ke_i \subseteq J$ is a regular cubic Jordan subalgebra, which implies $J = J_0 \oplus J_0^{\perp}$, and comparing ranks, we conclude that $J$ is free of rank 3 as a $k$-module, with basis $(e_1, e_2, e_3)$. Introducing the multiplication rules $e_i e_j = \delta_{ij} e_i$ on the basis vectors and extending it bilinearly to all of $J$, we obtain the structure of a split cubic étale $k$-algebra $E$ on the $k$-module $J$. From (37.13.2) and (34.17.1) we deduce $N_J(\sum \xi_i e_I) = \xi_1\xi_2\xi_3 = N_E(\sum \xi_i e_i)$ in all scalar extensions, and combining with Prop. 34.12, we conclude $J = E^{(+)}$ as cubic Jordan algebras. It remains to prove uniqueness, so let $E'$ be any cubic commutative associative $k$-algebra having $E'^{(+)} = J$ as cubic Jordan algebras. For $i, j = 1, 2, 3$ distinct, $e_i e_j = e_i^2 e_j = U_{e_i} e_j = 0$, so $E' = E$ as cubic commutative associative $k$-algebras.

**39.43** (a) Expanding the $U$-operator, we obtain

$$U_x e = U_{\xi e + x_1 + x_0} e = \xi^2 U_e e + \xi\{e e x_1\} + \xi\{e e x_0\} + U_{x_1} e + \{x_1 e x_0\} + U_{x_0} e,$$

where the Peirce rules of Thm. 32.2 imply $\{x_1 e x_0\} = U_{x_0} e = 0$, $U_{x_1} e \in J_0(e)$, $\{e e x_i\} = e \circ x_i - \{e(1_J - e)x_i\} = i x_i$ for $i = 0, 1$, $U_e e = e$, and (a) is proved.

(b) Assume first that $J$ is split, so there is an identification $J = \mathrm{Her}_3(C)$, for some composition $k$-algebra $C$. We write

$$x = \sum (\xi_i e_{ii} + u_i[jl]) \qquad (\xi_i \in k,\ u_i \in C,\ i = 1, 2, 3),$$

let $(mnp)$ be a cyclic permutation of (123) and apply (a) to $e := e_{mm}$. Since $U_x e = e$, we conclude $\xi_m^2 = 1$, hence $\xi_m \in k^\times$ and $x_1 = 0$. Thus

$$x = \sum \xi_i e_{ii} + x_0, \quad x_0 \in J_0(e_{mm}) = C[mn] \oplus C[pm].$$

Since this is true for all $m = 1, 2, 3$, we actually have $x = \sum \xi_i e_{ii}$. Now the hypothesis and (37.7.6), (37.7.7) imply $1_C[np] = U_x 1_C[np] = \xi_n \xi_p 1_C[np]$, hence $\xi_n \xi_p = 1$ and then $\xi_p = \xi_n \xi_p^2 = \xi_n$: the assertion is proved.

If $J$ is arbitrary, we apply Cor. 39.32 to find a faithfully flat algebra $R \in k$-**alg** making $J_R$ a split Freudenthal algebra over $R$. The special case just treated implies $x_R \in R 1_{JR}$. On the other hand, since $1_J \in J$ is unimodular, we have $J = k1_J \oplus M$, for some submodule $M \subseteq J$. In particular, $x = \xi 1_J + m$, for some $m \in M$. Changing scalars from $k$ to $R$, we conclude $m_R = 0$, hence $m = 0$ since $R$ is faithfully flat. Thus $x = \xi 1_J$, and $U_x = \mathbf{1}_J$ implies $\xi^2 = 1$.

## Solutions for Section 40

**40.14** (a) Write $W$ for the subspace of $J^0$ spanned by the invertible trace-zero elements of $J$. For $v_i, v_l \in C^\times$, the quantities

$$\begin{aligned} x_1 &:= e_{ii} - e_{jj} + v_i[jl], \\ x_2 &:= e_{ll} - e_{ii} + v_l[ij], \\ x_3 &:= e_{jj} - e_{ll} - v_l[ij] \end{aligned}$$

are invertible of trace zero and thus all belong to $W$. Hence so does $x_1 + x_2 + x_3 = v_i[jl]$. This not only implies $e_{ii} - e_{jj} = x_1 - v_i[jl] \in W$ but also $C[ij] \subseteq W$ by the hypothesis on $C$. Summing up we conclude $J^0 = W$.

(b) Assume that $J$ is simple. By Thm. 39.6, $J$ is either a division algebra, in which case the assertion is obvious, or it has the form $J \cong \mathrm{Her}_3(C, \Gamma)$, where $\Gamma \in \mathrm{GL}_3(F)$ is a diagonal matrix and $C$ is a pre-composition algebra over $F$. We check when the hypotheses of (a) are fulfilled.

**Lemma.** *A pre-composition algebra $C$ over $F$ either is spanned as a vector space over $F$ by $C^\times$, or $F = \mathbb{F}_2$ and $C \cong F \times F$ is split quadratic étale.*

*Proof* If $F = \mathbb{F}_2$ and $C \cong F \times F$, then $C^\times = \{1_C\}$ cannot possibly span $C$ as an $F$-vector space. Conversely, assume $F \ncong \mathbb{F}_2$ or $C$ is not split quadratic étale. We must show $C = FC^\times$ and may assume that $C$ is not a division algebra, so we are reduced to the case that $C$ is a split composition algebra of dimension $> 1$. If $C = F \times F$ is split quadratic étale, then $F$ contains an element $\alpha \neq 0, 1$, and since $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = (1-\alpha)^{-1}((\begin{smallmatrix} 1 \\ \alpha \end{smallmatrix}) - (\begin{smallmatrix} \alpha \\ \alpha \end{smallmatrix}))$, $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = (1-\alpha)^{-1}((\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}) - (\begin{smallmatrix} \alpha \\ \alpha \end{smallmatrix}))$, the assertion follows. If $C = \mathrm{Mat}_2(F)$ is the split quaternions, the automorphism group of $C$ acts transitively on its elementary idempotents, but also on its non-

zero nilpotent elements, so the equations

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}-\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}-\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

give what we want. Finally, the case that $C = \mathrm{Zor}(F)$ is the split octonions is reduced to the quaternionic case since every element of $C$ is contained in a quaternion subalgebra (Exc. 19.38). □

In view of the lemma, the first part of (b) follows from (a) unless $F = \mathbb{F}_2$ and $J \cong \mathrm{Her}_3(F \times F, \Gamma) \cong \mathrm{Her}_3(F \times F)$ (by Prop. 40.6) $\cong A^{(+)}$, $A := \mathrm{Mat}_3(F)$ (by Prop. 36.9). The subspace $W$ of $J$ spanned by $J^0 \cap J^\times$ is stable under the action of $\mathrm{GL}_3(F)$ on $A$ by conjugation. Since

$$e_{12}=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}=\begin{pmatrix}1&1&0\\0&1&1\\0&1&0\end{pmatrix}+\begin{pmatrix}1&0&0\\0&1&1\\0&1&0\end{pmatrix}\in W,$$

we therefore conclude $e_{ij} \in W$ $(1 \le i, j \le 3,\ i \ne j)$. On the other hand,

$$e_{11}+e_{22}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}=\begin{pmatrix}1&1&0\\1&1&0\\0&0&0\end{pmatrix}+e_{12}+e_{21},$$

where the first summand on the very right is nilpotent of index 2, hence conjugate to $e_{12}$ and thus belongs to $W$. This implies $e_{11} + e_{22} \in W$ and, similarly, $e_{11} + e_{33} \in W$. Summing up, therefore, we have $W = J^0$.

In order to prove the second part of (b), it suffices to note that $\mathrm{diag}(1, -1, 1) \in J$ is invertible of trace 1, hence together with $J^0$ spans all of $J$ as a vector space over $F$.

**40.15** (a) (33.11.2), the adjoint identity (33a.5) and (33.11.3).

(b) If $u$ is an elementary idempotent in some isotope of $J$, then $u$ has rank 1 by (a). Conversely, assume $u$ has rank 1. By hypothesis, $\mathrm{Nil}(J) = \{0\}$ and hence $J$ has no absolute zero divisors (Exc. 37.27 (e)), while part (b) of that exercise implies $T(q, u) \ne 0$ for some $q \in J$. By Exc. 40.14 (b) we may assume $q \in J^\times$, whence (33.11.5) implies $T^{(p)}(u) = 1$ for $p := T(q, u)^{-1}q \in J^\times$. Thus $u$ is an elementary idempotent in $J^{(p)}$.

Next assume $u$ is a co-elementary idempotent in some isotope $J'$ of $J$. By (a), we may assume $J' = J$. Then $u = 1_J - e$, for some elementary idempotent $e \in J$. Then $u^\sharp = e$ (by Prop. 37.2 (a)) has rank 1, so $u$ has rank 2. Conversely, if $u$ has rank 2, arguing as before with $u^\sharp$ in place of $u$, we find an invertible element $p \in J$ having $T(u^\sharp, p^{-1}) \ne 0$, hence $T(p^\sharp, u^\sharp) = N(p)T(u^\sharp, p^{-1}) \ne 0$. Passing to the isotope $J^{(p)}$ if necessary, we may therefore assume $T(u^\sharp) = S(u) \ne 0$.

But this means that the element $e := T(u^\sharp)^{-1}u^\sharp \in J$ is an element of rank 1 and trace 1, hence an elementary idempotent. Now (33a.14) yields

$$\begin{aligned} e \times u &= T(u^\sharp)^{-1}u^\sharp \times u = T(u^\sharp)^{-1}\Big((T(u)T(u^\sharp) - N(u))1 - T(u^\sharp)u - T(u)u^\sharp\Big) \\ &= T(u)1 - u - T(u)e = T(u)(1-e) - u. \end{aligned}$$

This implies $u \in J_0(e)$ by Prop. 37.2 (b), while Cor. 37.3 shows that $u$ is invertible in $J_0(e)$. Write $v \in J_0(e)$ for the corresponding inverse and pass to the isotope $J' := J^{(p)}$, $p := e + v \in J^\times$. Since $e$ continues to have rank 1 in $J'$ and satisfies $T^{(p)}(e) = T(e,p) = T(e,e) = T(e) = 1$ by Prop. 37.2 (b), it is, in fact, an elementary idempotent in $J'$. Moreover, $1_{J'} = p^{-1} = e + u$, forcing $u = 1_{J'} - e$, and (ii) holds.

(c) $e$ can be extended to an elementary frame of $J$ if and only if $J_0(e) = J(M_0, q_0, e_0)$ as in Cor. 37.3 contains an elementary idempotent (Prop. 37.4). Since semi-simplicity of $J$ is inherited by $J_0(e)$ (Exc. 37.29), the quadratic form $q_0$ is non-degenerate (Exc. 29.21). Moreover, by (38.10.4) and Exc. 38.21 (b), it is also isotropic. By Prop. 39.5, therefore, $J_0(e)$ contains an elementary idempotent if and only if the linear trace of $J_0(e)$, which by Cor. 37.3 agrees with $T$ on $J_0(e)$, is different from zero.

(d) Since

$$e = \sum (e_{ii} + 1_K[jl])$$

and $2 = 0$ in $k$, we have $T(e) = 3 = 1$. On the other hand, since the the conjugation of $K$ is the identity, (36.4.4) shows $e^\sharp = 0$. Thus $e$ is an elementary idempotent in $J$ and we have $e_0 := 1_J - e = \sum 1_K[jl]$. Now let $x = \sum(\xi_i e_{ii} + u_i[jl]) \in J_0(e)$. Then (37.2.3) implies $x = T(x)e_0 - e\times x = T(x)\sum 1_K[jl] - e\times x$. But (36.4.6) gives

$$\begin{aligned} e \times x &= \sum \big((\xi_j + \xi_l)e_{ii} + (-u_i - \xi_i 1_K + u_l + u_j)[jl]\big) \\ &= \sum \big((\xi_j + \xi_l)e_{ii} + (\xi_i 1_K + u_1 + u_2 + u_3)[jl]\big), \end{aligned}$$

and a comparison shows $\xi_1 = \xi_2 + \xi_3$, hence $T(x) = \sum \xi_i = 0$. By (c), therefore, $e$ cannot be extended to an elementary frame in $J$.

As to the second part of (d), we argue indirectly and assume $u = u_1 + u_2$ for some rank-one elements $u_1, u_2 \in J$. In particular, $u_j$ for $j = 1, 2$ is a symmetric 3-by-3 matrix of rank 1 with entries in $K$, and hence there are $a_j \in K^\times$, $0 \neq x_j \in K^3$ such that $u_j = a_j x_j x_j^\mathsf{T}$. Since

$$u = a_1 x_1 x_1^\mathsf{T} + a_2 x_2 x_2^\mathsf{T}$$

has rank 2, the quantities $x_1, x_2$ are linearly independent over $K$, and $a_1, a_2$ are both different from zero. Moreover, they are contained in $\mathrm{Im}(u) = Ke_1 + Ke_2$,

where $(e_1, e_2, e_3)$ stands for the canonical basis of $K^3$ over $K$. Thus $x_j = b_{1j}e_1 + b_{2j}e_2$ for $j = 1, 2$ and some matrix $(b_{ij}) \in \mathrm{GL}_2(K)$. Writing $e_{ij}$ for the ordinary matrix units in $\mathrm{Mat}_3(K)$, we now obtain

$$\begin{aligned} e_{12} + e_{21} = u &= a_1(b_{11}e_1 + b_{21}e_2)(b_{11}e_1^{\mathsf{T}} + b_{21}e_2^{\mathsf{T}}) + a_2(b_{12}e_1 + b_{22}e_2)(b_{12}e_1^{\mathsf{T}} + b_{22}e_2^{\mathsf{T}}) \\ &= a_1(b_{11}^2e_{11} + b_{11}b_{21}e_{12} + b_{21}b_{11}e_{21} + b_{21}^2e_{22}) \\ &\quad + a_2(b_{12}^2e_{11} + b_{12}b_{22}e_{12} + b_{22}b_{12}e_{21} + b_{22}^2e_{22}). \end{aligned}$$

Since the characteristic is 2, this implies $a_1b_{11}^2 = a_2b_{12}^2$, $a_1b_{21}^2 = a_2b_{22}^2$, hence

$$a_1a_2 \det(b_{ij})^2 = a_1b_{11}^2a_2b_{22}^2 - a_2b_{12}^2a_1b_{21}^2 = 0,$$

a contradiction. This completes the solution of (d).

(e) Since two vectors in $F^3$ are linearly independent if and only if they are distinct, one checks that that $J := \mathrm{Her}_3(F)$ contains precisely seven elements of rank 1, namely,

$$e_{11}, e_{22}, e_{33}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

and precisely four elementary idempotents, namely,

$$e_{11}, e_{22}, e_{33}, e := \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

It follows (again) that $e$, which agrees with the idempotent of (d), cannot be completed to an elementary frame in $J$.

(f) (i) $\Rightarrow$ (ii). Let $e_0$ be a co-elementary idempotent in some isotope $J'$ of $J$. Replacing $J$ by $J'$ if necessary, we may assume $J' = J$. Then $e := 1_J - e_0$ is an elementary idempotent in $J$, which by hypothesis can be extended to an elementary frame $(e = e_1, e_2, e_3)$ of $J$. Hence $e_0 = e_2 + e_3$, as claimed.

(ii) $\Rightarrow$ (iii). (b) and (ii).

(iii) $\Rightarrow$ (iv). If $J$ were not regular, then, by Thm. 39.6 and up to isotopy, it would be as in (d), hence would contain an element of rank 2 that violates the condition described in (iii).

(iv) $\Rightarrow$ (i). By hypothesis, the bilinear trace $T$ of $J$ is regular, and the Peirce components of $J$ relative to an elementary idempotent $e \in J$ are orthogonal with respect to $T$. Hence $T$ stays regular on $J_0(e)$ and since $T(x_0) = T(1_J, x_0) = T(1_J - e, x_0)$ for all $x_0 \in J_0(e)$, the linear trace of $J$ cannot be zero on $J_0(e)$. The assertion now follows from (c).

**40.16** Given $x \in J^\times$ such that $N_J(x) = 1$, we wish to find $g \in \mathrm{Inv}(J)$ such that

$gx = 1_J$. By Lemma 40.11, we may assume that $x$ is diagonal, i.e., $x = \sum x_i e_{ii}$ for some $x_i \in k^\times$ such that $\prod x_i = 1$. Pick $y_i \in k^\times$ such that $y_i^2 = x_i$ and define $g := U_y$ for $y = \sum y_i e_{ii}$, so $gx = 1_J$ as desired. Furthermore, for $z \in J$, we have

$$N(gz) = N(U_y z) = N(y)^2 N(z) = N(y^2)N(z) = N(x)N(z) = N(z),$$

so $U_y \in \mathrm{Inv}(J)$.

**40.17** (a): Let $J$ be a Freudenthal algebra of rank $n > 6$ over $F$. The norm of $J$ is a cubic form in more than 3 variables and is therefore isotropic by the Chevalley-Warning Theorem. Then by Prop. 39.17, $J \cong \mathrm{Her}_3(C, \Gamma)$ for a composition algebra $C$ over $F$ of rank $> 1$. If the rank is $> 2$, then, again since $F$ is finite, $C$ is split, and therefore $J$ is itself split (Prop. 40.6). If the rank is 2, then $C$ is either split quadratic étale or isomorphic to $K$. In the former case, $J$ is split while in the latter case, the norm of $C \cong K$ is surjective (since, again by Chevalley-Warning, any quadratic form in more than three variables over $F$ is isotropic), and (37.24.3) combined with Exc. 23.33 implies $J \cong \mathrm{Her}_3(K)$.

(b): Let $k$ be a finite commutative ring, let $C$ be a composition algebra of rank $r > 2$ and $J$ a Freudenthal algebra of rank $n > 9$ over $k$. We first assume that $k$ is reduced. Since $k$, being finite, is artinian, we conclude from [22, p. 203] that $k = k_1 \times \cdots \times k_m$ is a finite direct product of finite fields. This implies $C = C_{k_1} \times \cdots \times C_{k_m}$, where each $C_{k_i}$, for $1 \le i \le m$, is composition algebra of rank $r$ over the finite field $k_i$, hence split, by 23.14. Thus $C$ is split over $k$. Similarly, $J = J_{k_1} \times \cdots \times J_{k_m}$, where each $J_i := J_{k_i}$ is a simple Freudenthal algebra of rank $n$ over the finite field $k_i$, and therefore is split by part (a).

If $k$ is arbitrary, we only consider the case of a Freudenthal algebra, the composition algebra case being completely analogous. We put $\mathfrak{a} := \mathrm{Nil}(k)$, $\bar{k} := k/\mathfrak{a}$ and $\bar{J} := J/\mathfrak{a}J = J_{\bar{k}}$. Since $\bar{k}$ is (finite and) reduced, the special case just treated implies that $\bar{J}$ is split over $\bar{k}$. Since $k$ is artinian, the ideal $\mathfrak{a} \subseteq k$ is nilpotent, forcing $\mathfrak{a}^m = \{0\}$ for some positive integer $m$. We show by induction on $i = 1, \ldots, m$ that $J_{k/\mathfrak{a}^i}$ is split over $k/\mathfrak{a}^i$. By the special case treated at the beginning, this is true for $i = 1$. Now let $i > 1$ and suppose the assertion holds for $i-1$. We have $k/\mathfrak{a}^{i-1} = (k/\mathfrak{a}^i)/(\mathfrak{a}^{i-1}/\mathfrak{a}^i)$ and $(\mathfrak{a}^{i-1}/\mathfrak{a}^i)^2 = \{0\}$. By Prop. 39.26, the affine scheme $\mathbf{Splid}(J)$ is smooth, so the natural map

$$\mathbf{Splid}(J)(k/\mathfrak{a}^i) \longrightarrow \mathbf{Splid}(J)(k/\mathfrak{a}^{i-1}) \tag{s1}$$

is surjective. By the induction hypothesis, $J_{k/\mathfrak{a}^{i-1}}$ is split and hence there exists a splitting datum for $J_{k/\mathfrak{a}^{i-1}}$ (Prop. 39.30). We therefore conclude from the surjectivity of the map in (s1) that there exists a splitting datum for $J_{k/\mathfrak{a}^i}$, which is therefore split over $k/\mathfrak{a}^i$. This completes the induction, and for $i = m$ we conclude that $J = J_{k/\mathfrak{a}^m}$ is split over $k/\mathfrak{a}^m = k$.

**40.18** (a): We use the group homomorphism $\mu : \mathrm{Str}(J) \to k^\times$ from Lemma 40.4 and note that

$$\mu(\phi\eta\phi^{-1}) = \mu(\eta) \quad \text{and} \quad \mu(\eta^{\sharp-1}) = \mu(\eta)^{-1}.$$

Therefore, it suffices to find an $\eta$ with $\mu(\eta)^2 \neq 1$.

Taking now $\eta$ to be multiplication by $c$, which is a similarity of the norm form, so belongs to $\mathrm{Str}(J)$. Since $\mu(\eta)^2 = c^6 \neq 1$, this provides the desired example.

(b): $\eta = \eta^{\sharp-1}$ if and only if $\eta^{-1} = \eta^\sharp = \eta^{-1}U_{\eta(1_J)}$, i.e., $U_{\eta(1_J)} = \mathbf{1}_J$. Exercise 39.43 shows that this is equivalent to $\eta(1_J) = \zeta 1_J$ for some $\zeta \in \boldsymbol{\mu}_2(k)$.

Given $\eta$ fixed by the automorphism, then, $\eta = \zeta\phi$ for some $\zeta \in \boldsymbol{\mu}_2(k)$ and $\phi \in \mathrm{Str}(J)$ such that $\phi(1_J) = 1_J$, i.e., $\phi \in \mathrm{Aut}(J)$ by Thm. 31.22 (c). Conversely, given $\zeta \in \boldsymbol{\mu}_2(k)$ and $\phi \in \mathrm{Aut}(J)$, $\eta := \zeta\phi$ is in $\mathrm{Str}(J)$ and satisfies $\eta(1_J) = \zeta 1_J$, so it is fixed by the automorphism, proving (1).

For part (2), we aim to show that $\mathrm{Inv}(J) \cap \boldsymbol{\mu}_2(k)\,\mathrm{Aut}(J) = \mathrm{Aut}(J)$. For $\zeta \in \boldsymbol{\mu}_2(k)$, $\phi \in \mathrm{Aut}(J)$, we have $N(\zeta\phi(1_J)) = \zeta^3 = \zeta$. Consequently. $\zeta\phi$ belongs to $\mathrm{Inv}(J)$ if and only if $\zeta = 1_k$.

## Solutions for Section 41

**41.30** As in the solution of Exc. 40.17, every Freudenthal algebra over a finite field $F$ is of the form $J = \mathrm{Her}_3(F, \Gamma)$ for some $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, 1) \in \mathrm{GL}_3(F)$. If $F$ has characteristic 2, then everything is a square, and $J$ is split (Exc. 37.22 (b)). If $F$ has characteristic different from 2, then $J$ is regular, and $Q_J = \langle \gamma_2, \gamma_1, \gamma_2\gamma_1 \rangle_{\mathrm{quad}}$ is a classifying invariant (Thm. 41.21). Note that over $F$ we may identify quadratic forms and symmetric bilinear forms, allowing us to use notation and terminology of O'Meara [32]. Since the determinant of $Q_J$ is a square, [32, 62:1a, p. 157] implies $Q_J \cong \langle 1, 1, 1 \rangle$, and $J$ is split.

**41.31** Let $\Omega = (e_1, e_2, e_3)$, $\Omega' = (e'_1, e'_2, e'_3)$ be two elementary frames in $J$. Writing $C$ for the co-ordinate algebra of $J$, let

$$\Phi\colon J \xrightarrow{\sim} \mathrm{Her}_3(C, \Gamma), \quad \Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3) \in \mathrm{GL}_3(F)$$

be any $\Omega$-co-ordinatization of $J$. If $\eta$ is an automorphism of $J$ sending $e'_i$ to $e_i$ for $1 \leq i \leq 3$, then $\Phi' := \Phi \circ \eta$ is an $\Omega'$-co-ordinatization of $J$, and (41.13.1) combined with (1) shows $\kappa(\Omega') = \kappa(\Omega)$. Conversely, let this be so and suppose

$$\Phi'\colon J \xrightarrow{\sim} \mathrm{Her}_3(C, \Gamma'), \quad \Gamma' = \mathrm{diag}(\gamma'_1, \gamma'_2, \gamma'_3) \in \mathrm{GL}_3(F)$$

is any $\Omega'$-co-ordinatization of $J$. By Exc. 37.22 (b), we may assume $\gamma_3 = \gamma_3' = 1$. Then (41.13.1) and (1) show $\mathrm{cl}(-\gamma_i) = \mathrm{cl}(-\gamma_i')$ for $i = 1, 2$, so there are $p, q \in C^\times$ having $\gamma_1 = n_C(p)\gamma_1'$, $\gamma_2 = n_C(q)\gamma_2'$. and we deduce $C^{(p,q)} \cong C$ from Exc. 19.31. By Exc. 37.24, therefore, we find a diagonal isomorphism $\eta\colon \mathrm{Her}_3(C, \Gamma') \xrightarrow{\sim} \mathrm{Her}_3(C, \Gamma)$, whence $\eta \circ \Phi'\colon J \to \mathrm{Her}_3(C, \Gamma)$ is an $\Omega'$-co-ordinatization of $J$. In particular $\Phi^{-1} \circ \eta \circ \Phi' \in \mathrm{Aut}(J)$ sends $e_i'$ to $e_i$ for $1 \le i \le 3$. The final statement of the exercise follows from the fact that the class group of $J$ is trivial under the hypotheses stated.

**41.32** Recall from (34.9.1) that $(x \times y)^\sharp = T(x, y^\sharp)x$ for all $y \in J$. So it suffices to find a $y \in J$ with $T(x, y^\sharp) \neq 0$. And, since $J$ is regular, it suffices to argue that the elements $y^\sharp$ span $J$. If $J$ has rank 1 this is obvious and if $J$ has rank $\ge 6$ it follows from Prop. 39.17, Exc. 40.14 (b) and $Fy^\sharp = Fy^{-1}$ for all $y \in J^\times$.

It remains to consider the case where $J$ has rank 3. If $J$ is a division algebra, the claim is obvious so suppose $J = (F \times K)^{(+)}$ for $K$ a quadratic étale $F$-algebra. Applying (34.24.5), one checks

$$(\alpha, u) = (\alpha - n_K(u))(0, 1_K)^\sharp + (1, \bar{u})^\sharp$$

for $\alpha \in F$, $u \in K$, and the assertion follows.

**41.33** (i): Suppose first that $y = e_{11}$. For sake of contradiction, suppose $x \times y = 0$, so $x = \xi_1 e_{11} + u_2[31] + u_3[12]$ for some $\xi_1 \in F$ and $u_2, u_3 \in C$. Put $x_0 = u_2[31] + u_3[12]$. Then $x_0^\sharp = (x - \xi_1 e_{11})^\sharp = x^\sharp + \xi_1^2 e_{11}^\sharp = 0$, and $x_0 \times y = (x - \xi_1 e_{11}) \times y = 0$. However,

$$x_0^\sharp = -\gamma_3\gamma_1 n_C(u_2)e_{22} - \gamma_1\gamma_2 n_C(u_3)e_{33} + \gamma_1\overline{u_2u_3}[23].$$

Since $n_C$ does not represent 0, $x_0 = 0$. Thus $x = \xi_1 e_{11} \in Fy$, a contradiction, verifying that $x \times y \neq 0$.

In the general case, since $C$ is regular, Thm. 41.29 provides a $g \in \mathrm{Inv}(J)$ such that $gy \in F^\times e_{11}$. Then

$$0 \neq gx \times gy = g^{\sharp -1}(x \times y)$$

by Lemma 40.4 (iii), so $x \times y \neq 0$.

The fact that $(x \times y)^\sharp = 0$ follows immediately from (33a.10).

(ii): The easy direction is when $x = y \times z$ for some $z \in J$. Then by (29b.7) we have

$$T(x, y) = T(y \times z, y) = T(z, y \times y) = 0.$$

So suppose $T(x, y) = 0$.

In the case when $y = e_{11}$, the fact that $T(x, y) = 0$ implies that $x = \xi_2 e_{22} +$

$\xi_3 e_{33} + \sum_i u_i[jl]$. The diagonal entries of $x^\sharp$ are in particular zero, so for each $i$ we have

$$0 = \xi_j \xi_l - \gamma_j \gamma_l n_C(u_i).$$

For $i = 2, 3$, $j$ or $l$ is 1, so the $\xi_j \xi_l$ term vanishes and we find that $n_C(u_i) = 0$. Since $C$ is division, $u_i = 0$. Thus $x = \xi_2 e_{22} + \xi_3 e_{33} + u_1[23]$, i.e., $x$ is in $y \times J$, compare Example 36.8.

In general, Thm. 41.29 provides a $g \in \mathrm{Inv}(J)$ such that $gy \in F^\times e_{11}$. Then

$$0 = T(x, y) = T(g^{\sharp -1} x, gy)$$

by Lemma 40.4 (iv), so $g^{\sharp -1} x = gy \times gz$ for some $z \in J$ and we conclude that $x = y \times z$.

(iii): By (i), $x \times y$ has rank 1, so $(x \times y) \times J$ is a line. It contains $Fx$ because $T(x, x \times y) = T(x \times x, y) = 0$ and similarly for $Fy$.

So suppose $z \times J$ is a line containing $Fx$ and $Fy$. If $z = e_{11}$, then by hypothesis $x$ and $y$ have zeros in their top row and left column. It immediately follows that $x \times y$ is in $Fe_{11}$. Moreover, $x \times y \neq 0$, so $x \times y \in F^\times e_{11}$. For general $z$, Thm. 41.29 provides a $g \in \mathrm{Inv}(J)$ such that $gz \in F^\times e_{11}$. Then $g^{\sharp -1} x$ and $g^{\sharp -1} y$ are rank 1 elements contained in $gz \times J$, so $g^{\sharp -1} x \times g^{\sharp -1} y \in F^\times gz$, i.e., $x \times y$ is contained in $F^\times z$. That is, $Fz = F(x \times y)$, proving uniqueness.

(iv): Among the three axioms, the first was verified in (iii). Two lines $x \times J$, $y \times J$ pass through a point $Fz$ if and only if $Fz \subseteq (x \times J) \cap (y \times J)$ if and only if $T(z, x) = T(z, y) = 0$ if and only if $Fx, Fy \subseteq z \times J$. It follows now from (iii) that $Fz = F(x \times y)$, proving the second axiom.

Finally, consider the four points $Fe_{11}$, $Fe_{22}$, $Fe_{33}$, and $Fx$ for

$$x = \sum_i \gamma_i e_{ii} + 1[jl].$$

(One checks that $x^\sharp = 0$.) It remains to verify that no three of them are collinear. Any subset of three of these points contains, say, $e_{jj}$ and $e_{ll}$, so the line they lie on is $(e_{jj} \times e_{ll}) \times J = e_{ii} \times J$, which contains neither $e_{ii}$ nor $x$.

**41.34** Let $\varphi\colon J_1 \to J_1'$ be any isomorphism. By definition (41.1), the algebra $J_1$ contains an elementary frame $\Omega$, which by Prop. 39.2 can be extended to a co-ordinate system

$$\mathfrak{S} = (\Omega, u_{23}, u_{31}) \text{ of } J_1, \quad \Omega = (e_1, e_2, e_3).$$

Applying $\varphi$, we obtain a co-ordinate system

$$\mathfrak{S}' = (\Omega', u_{23}', u_{31}') \text{ of } J_1', \quad \Omega' = (e_1', e_2', e_3'),$$

where $e_i' = \varphi(e_i)$ for $i = 1, 2, 3$ and $u_{jl}' = \varphi(u_{jl})$ for $i = 1, 2$. Note that $\mathfrak{S}$ and

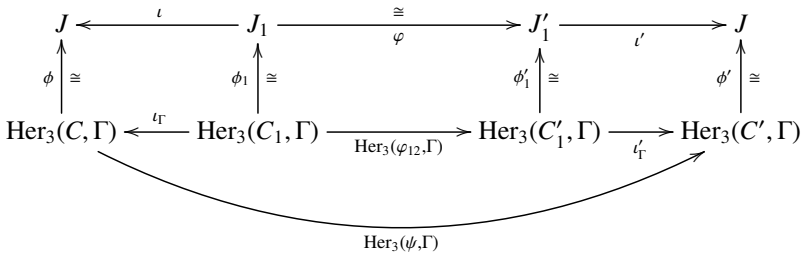
$\mathfrak{E}'$ are both co-ordinate systems of $J$. Since $\varphi$ preserves cubic norm structures, Prop. 37.15 implies

$$\omega := \omega_{J_1,\mathfrak{E}} = \omega_{J,\mathfrak{E}} = \omega_{J_1',\mathfrak{E}'} = \omega_{J,\mathfrak{E}'},$$
$$C_1 := C_{J_1',\mathfrak{E}} \subseteq C_{J,\mathfrak{E}} =: C, \quad C_1' := C_{J_1',\mathfrak{E}'} \subseteq C_{J,\mathfrak{E}'} =: C'$$

as composition subalgebras and

$$\Gamma := \Gamma_{J_1',\mathfrak{E}} = \Gamma_{J,\mathfrak{E}} = \Gamma_{J_1',\mathfrak{E}'} = \Gamma_{J,\mathfrak{E}'}.$$

Moreover, $\varphi$ restricts to a linear bijection from $(J_1)_{12}(\Omega)$ to $(J_1')_{12}(\Omega')$, which actually is an isomorphism $\varphi_{12}\colon C_1 \to C_1'$. Now the Jacobson co-ordinatization theorem 37.17 produces isomorphisms $\phi_1, \phi_1', \phi, \phi'$ making the two top rows of the diagram




commutative. By the Jacobson-Faulkner theorem 41.8, $C$ and $C'$ are isomorphic. Hence the Skolem-Noether theorem for composition algebras (Exc. 23.28) implies that there exists an isomorphism $\psi\colon C \to C'$ extending $\varphi_{12}$. Setting

$$\Psi := \phi' \circ \mathrm{Her}_3(\psi, \Gamma) \circ \phi^{-1} \in \mathrm{Aut}(J),$$

diagram chasing shows $\Psi \circ \iota = \iota' \circ \varphi$, which solves the problem.

**41.35** Regularity of Freudenthal $F$-algebras in dimension 6 implies that $F$ has characteristic not 2, so there is a natural identification of quadratic forms over $F$ with symmetric bilinear ones. We may write $J = \mathrm{Her}_3(F, \Gamma)$, $J' = \mathrm{Her}_3(F, \Gamma')$ for some invertible matrices $\Gamma = \mathrm{diag}(\gamma_1, \gamma_2, \gamma_3)$, $\Gamma' = \mathrm{diag}(\gamma_1', \gamma_2', \gamma_3')$ over $F$. By Lemma 41.7, the quadratic forms $Q_J$ and $Q_{J'}$ are isometric, and from (41.5.1) we deduce

$$\langle \gamma_2\gamma_3, \gamma_3\gamma_1, \gamma_1\gamma_2 \rangle \cong \langle \gamma_2'\gamma_3', \gamma_3'\gamma_1', \gamma_1'\gamma_2' \rangle.$$

Maltiplying the left-hand side with $\gamma_1\gamma_2\gamma_3$ and the right-hand side with $\gamma_1'\gamma_2'\gamma_3'$, we see that $\langle \Gamma \rangle \cong \alpha \langle \Gamma' \rangle$ for some $\alpha \in F^\times$. But $J'$ does not change when multiplying $\Gamma'$ by an invertible scalar. Hence we may assume $\alpha = 1$ and thus find a $P \in \mathrm{GL}_3(F)$ such that $\Gamma' = P^\mathsf{T}\Gamma P$. Now one checks that the assignment $x \mapsto P^{-1}xP$ is an isomorphism from $J$ onto $J'$.

# Solutions for Chapter VII

## Solutions for Section 42

**42.19** Put $N := N_A$. Then $N' := N(pq)N$ is a cubic form on $A' := A^{(p,q)}$. From (31.14.1) we deduce $A'^{(+)} = A^{(+)(pq)}$. By Prop. 33.12 and Cor. 34.6, therefore, $A'^{(+)}$ is a cubic Jordan algebra over $k$ with norm $N'$. Since $N'$ permits composition relative to the multiplication of $A'$, it follows that $A'$ is, in fact, a cubic alternative algebra with norm $N'$ over $k$. Now let $x \in A'$. Then Prop. 34.12, (33.11.6) and Prop. 42.1 imply

$$S_{A'}(x) = S_{A'^{(+)}}(x) = S_{A^{(+)(pq)}}(x) = T_{A^{(+)}}((pq)^\sharp, x^\sharp) = T_A(q^\sharp p^\sharp x^\sharp),$$

hence the second equation of (1). Similarly,

$$T_{A'}(x) = T_{A'^{(+)}}(x) = T_{A^{(+)(pq)}}(x) = T_{A^{(+)}}(pq, x) = T_A(pqx).$$

In particular, $A$ and $A^p$ have the same linear and quadratic trace. Thanks to Prop. 42.1, the bilinear trace of $A^p$ satisfies $T_{A^p}(x,y) = T_{A^p}((xp^{-1})(py)) = T_A((xp^{-1})(py))) = T_A(([xp^{-1}]p)y) = T_A(x,y)$ and thus agrees with the bilinear trace of $A$.

**42.20** (a) Since $(\mathfrak{a}, I)$ is a cubic ideal in $A^{(+)}$, we have $\mathfrak{a}A \subseteq I$ and $T_A(x,y), T_A(x^\sharp, y), N_A(x) \in \mathfrak{a}$ for all $x \in I$, $y \in A$. Now let $x_i \in I$, $y_i \in A$, $i = 0,1,2$, and $x := x_0 + x_1 j_1 + x_2 j_2 \in J(I,\mu)$, $y := y_0 + y_1 j_1 + y_2 j_2 \in J$. Then

$$T_J(x,y) = T_A(x_0,y_0) + \mu T_A(x_1,y_2) + \mu T_A(x_2,y_1) \tag{s1}$$

$$\begin{aligned} T_J(x^\sharp, y) &= T_A(x_0 - \mu x_1 x_2, y_0) + \mu T_A(\mu x_2^\sharp - x_0 x_1, y_2) + \mu T_A(x_1^\sharp - x_2 x_0, y_1) \\ &= T_A(x_0^\sharp, y_0 - \mu T_A(x_1, x_2 y_0) + \mu^2 T_A(x_2^\sharp, y_2) \\ &\quad - \mu T_A(x_0, x_1 y_2) + \mu T_A(x_1^\sharp, y_1) - \mu T_A(x_2, x_0 y_1), \end{aligned} \tag{s2}$$

$$N_J(x) = N_A(x_0) + \mu N_A(x_1) + \mu^2 N_A(x_2) - \mu T_A(x_0, x_1 x_2) \tag{s3}$$

all belong to $\mathfrak{a}$. Moreover, $I^\sharp + I \times A \subseteq I$ by Exc. 34.21 (a), which by (42.11.3), (42.11.5) implies $J(I,\mu)^\sharp + J(I,\mu) \times J \subseteq J(I,\mu)$. Hence $(\mathfrak{a}, J(I,\mu))$ is a cubic ideal in $J$ (loc. cit.). Next suppose $(\mathfrak{a}, I)$ is a cubic nil ideal in $A$, i.e., $\mathfrak{a}$ and $I$ are both nil (Exc. 37.21). Then (s1)-(s3) combined with Exc. 34.23 show that the ideal $J(I,\mu) \subseteq J$ is nil. Thus $(\mathfrak{a}, J(I,\mu))$ is a cubic nil ideal in $J$. On the other hand, assume $(\mathfrak{a}, I)$ is separated, so some $k$-linear map $\lambda\colon A \to k/\mathfrak{a}$ has $\lambda(1_A) = 1_{k/\mathfrak{a}}$ and $\lambda(I) = \{0\}$. Let $\lambda'\colon J \to k/\mathfrak{a}$ be the projection from $J$ onto the initial summand followed by $\lambda$. Then $\lambda'$ is $k$-linear, sends $1_J$ to $1_{k/\mathfrak{a}}$ and kills $J(I,\mu)$. Hence $(\mathfrak{a}, J(I,\mu))$ is separated. Moreover, $A/I$ is an alternative algebra over $k/\mathfrak{a}$, whence Exc. 34.21 (b) implies that $A^{(+)}/I = (A/I)^{(+)}$ carries a unique cubic Jordan algebra structure over $k/\mathfrak{a}$ making the canonical projection $\pi\colon A^{(+)} \to (A/I)^{(+)}$ a $\sigma$-semi-linear homomorphism of cubic Jordan algebras. Hence $A/I$ carries a unique structure of a cubic alternative algebra over $k/\mathfrak{a}$ making $\pi$ a $\sigma$-semi-linear homomorphism of cubic alternative algebras. The final assertion of (a) is obvious.

(b) The first statement is clear while (4) follows from the fact that $J(\mathrm{Nil}(A),\mu)$ by (a) is a nil ideal in $J$. Now suppose $k \neq \{0\}$ and $\mu$ is nilpotent. Setting $I_1 := \mathrm{Nil}(A) \oplus A j_1 \oplus A j_2$ and combining (42.11.3), (42.11.5) with Exc. 28.20 (c), we conclude $I_1^\sharp + I_1 \times J \subseteq I_1$. By Exc. 34.21 (a) and (s1)-(s3), therefore, $I_1$ is a nil ideal in $J$ properly containing $J(\mathrm{Nil}(A),\mu)$. Hence we can't have equality in (4). Next let $F$ be a field of characteristic 3 and $J = J(F,1)$. Then $\mathrm{Nil}(F) = \{0\} \neq \mathrm{Nil}(J)$ since, for example, $(j_1 - 1_J)^3 = j_1^3 - 1_J = 0$.

(c) By (4), the right-hand side of (5) is contained in the left. Conversely, put $\mathfrak{a} := \mathrm{Nil}(k)$, $I := \mathrm{Nil}(A)$. By (3),

$$J(A,\mu)/J(I,\mu) \cong J(A/I, \sigma(\mu)),$$

where the right-hand side is regular by Cor. 42.14. But the nil radical of $J(A/I,\sigma(\mu))$ is zero by regularity and since $k_0$ is reduced. Hence $\mathrm{Nil}(J(A,\mu)) \subseteq J(I,\mu)$, and (5) is proved.

**42.21** (a) Let $A$ be a semi-simple cubic alternative $F$-algebra. Then $J := A^{(+)}$ by Cor. 42.2 is a semi-simple cubic Jordan algebra over $F$, hence falls into precisely one of the categories listed in Thm. 39.6. We now proceed in several steps.

1°. Suppose first $J$ is as in (ii) of 39.6, so up to isomorphism we have

$$J = F^{(+)} \times J(M,q,e) \tag{s1}$$

as a direct product of ideals, $(M,q,e)$ being a non-degnenerate pointed quadratic module over $F$. Then $c := (1,0) \in J$ by (5), (3) of Exc. 34.24 is an elementary idempotent satisfying $J_2(c) = F^{(+)}$, $J_1(c) = \{0\}$, $J_0(c) = J(M,q,e)$.

Hence Example 32.7 implies $A_{11}(c) = F$, $A_{12}(c) = A_{21}(c) = \{0\}$, $A_{22}(c)^{(+)} = J(M,q,e)$, and the Peirce rules for alternative algebras (Exc. 14.12) show that (s1) is in fact a decomposition into a direct product of ideals in $A$:

$$A = F \times C, \tag{s2}$$

where $C := A_{22}(c)$ is a conic alternative $F$-algebra with identity element $1_C = e$ and norm $n_C = q$. By (1) of Exc. 34.24 we have $N_A((1,u)) = n_C(u)$ for all $u \in C$, and since $N_A$ permits composition, so does $n_C$. Summing up, we have shown that $C$ is a pre-composition algebra over $F$, forcing $A = \hat{C}$ to be as in (iv) or (v) depending on whether $C$ is split quadratic étale or not.

2°. Next suppose $J$ is as in (iii) of 39.6, so $J = \mathrm{Her}_3(C,\Gamma)$ for some pre-composition algebra $C$ over $F$ and some $\Gamma = \mathrm{diag}(\gamma_1,\gamma_2,\gamma_3) \in \mathrm{GL}_3(F)$; in particular, $\dim_F(C) = 2^n$, $n \in \mathbb{N}$. Arguing as in 1°,

$$J' := Fe_{11} \oplus J_0(e_{11}) = Fe_{11} \oplus (Fe_{22} \oplus C[23] \oplus Fe_{33}) \cong F^{(+)} \times J(M,q,e),$$

where $M = Fe_{22} \oplus C[23] \oplus Fe_{33}$ as a $k$-module, $e = e_{22} + e_{33}$ and $q\colon M \to F$ is defined by

$$q(\alpha_2 e_{22} + u_1[23] + \alpha_3 e_{33}) := \alpha_2\alpha_3 - \gamma_2\gamma_3 n_C(u_1) \tag{s3}$$

for $\alpha_2, \alpha_3 \in F$, $u_1 \in C$, carries the structure of a cubic alternative $F$-algebra $A'$ having $A'^{(+)} = J'$ as cubic Jordan algebras. By 1°, therefore, $M$ becomes a pre-composition algebra $C'$ over $F$ such that $n_{C'} = q$ and $A' = \hat{C}'$; in particular, $2^n + 2 = \dim_F(C') = 2^m$ for some $m \in \mathbb{N}$, which is impossible unless $n = 1$. But the norm of a pre-composition algebra over a field is either anisotropic or hyperbolic. Hence (s3) implies that $C$ is split quadratic étale, and we deduce from Prop. 40.6 that

$$A^{(+)} \cong \mathrm{Her}_3(F \times F, \Gamma) \cong \mathrm{Her}_3(F \times F) \cong \mathrm{Mat}_3(F)^{(+)}.$$

This isomorphism extends to one over the algebraic closure $\bar{F}$ of $F$, and since $A_{\bar{F}}^{(+)} \cong \mathrm{Mat}_3(\bar{F})^{(+)}$ is simple, so is $A_{\bar{F}}$. From Cor. 9.23 we therefore conclude that $A$ is central simple, and Thm. 13.10 implies $A \cong \mathrm{Mat}_3(F)$, first as abstract alternative algebras and then as cubic ones, thanks to Cor. 42.4. Thus we are in case (vi).

3°. Finally, we are able to deal with case (i) of 39.6, so $J$ is a cubic Jordan division algebra, forcing $A$ to be an alternative division algebra. Since the radical of the bilinear trace of $A$ by Prop. 42.1 (a) is a two-sided ideal in $A$, we either have $T_A = 0$ or $A$ is regular.

Assume first $T_A = 0$. Then $F$ has characteristic 3 and (33a.6) implies that $N_A\colon A \to F$ is a homomorphism of algebras over $\mathbb{Z}$. Moreover, $A$ being a

division algebra, this homomorphism is injective, forcing $A/F$ to be a purely inseparable field extension of exponent at most 1. Thus we are either in case (i) or in case (ii).

We are left with the case that $A$ is regular. The $A' := A_{\bar{F}}$ is a semi-simple cubic alternative algebra over $\bar{F}$, so $J' := A'^{(+)}$ falls into one of the categories (i), (ii), (iii) of 39.6. If $J'$ satisfies (i), then $A' \cong \bar{F}$ by Exc. 8.16, hence $A \cong F$, and we are in case (i). If $J'$ satisfies (ii) of 39.6, so $J' = \bar{F}^{(+)} \times J(M', q', e')$ is a direct product of ideals, where $(M', q', e')$ is a non-degenerate pointed quadratic module over $\bar{F}$, then we may assume $\dim_{\bar{F}}(M') \geq 3$ and $c := (1_{\bar{F}}, 0)$ by Prop. 32.8 is the only elementary idempotent of $J'$ having $J_1'(c) = \{0\}$. Thus, by descent, $c$ belongs to $J$, and $J$ satisfies condition (ii) of 39.6. Now 2° implies $A = \hat{C}$ for some pre-composition algebra $C$ over $F$, which is actually a composition algebra since $A$ is regular. Finally, if $J'$satisfies (iii) of 39.6, then $A'$ is simple of dimension 9 over $\bar{F}$ by 2°, forcing $A$ to be central simple of dimension 9 over $F$. By Thm. 13.10, therefore, we are in case (vi) or (vii) of our Exc.

(b) (i) $\Rightarrow$ (ii). Regular cubic alternative algebras are separable by Exc. 34.23 and Cor. 42.2. Moreover, $k$ (resp. $(k \times k)_{\mathrm{cub}}$) are both separable but not regular unless $\frac{1}{3}$ (resp. $\frac{1}{2}$) belong to $k$.

(ii) $\Rightarrow$ (i). In view of (a), (b) of (ii) combined with Exc. 34.27, we may assume $n \geq 3$. Note that $A$ is regular (resp. separable) if and only if so is $A_F$, for any algebraically closed field $F \in k$-**alg** (for the regular case, see Exc. 39.37). Hence we may assume that $F$ is an algebraically closed field, so $A$ satisfies one of the conditions (i)-(vii) of (a). Since $F$ is algebraically closed, only cases (iv)-(vi) are possible, where $C$ in (v) has dimension at least 2 and hence is regular. But then so is $A$ and we are done.

**42.22** We will repeatedly make use of the fact that a linear map between cubic Jordan algebras is a homomorphism if and only if it preserves unit elements and adjoints (Exc. 34.18 (a)).

(a) $\varphi := \varphi_{A,\mu,p}$ is the identity on $A^{(+)}$ and, in particular, preserves units. Furthermore, since $A$ is associative,

$$\begin{aligned}\varphi(x)^\sharp &= (x_0 + (x_1 p)j_1 + (p^\sharp x_2)j_2)^\sharp \\ &= (x_0^\sharp - N_A(p)\mu x_1 x_2) + (N_A(p)\mu x_2^\sharp p - (x_0 x_1)p)j_1 + (p^\sharp x_1^\sharp - p^\sharp x_2 x_0)j_2 \\ &= \varphi(x^\sharp),\end{aligned}$$

so $\varphi\colon J(A, N_A(p)\mu) \to J(A, \mu)$ is a homomorphism of cubic Jordan algebras. The final assertion is clear.

(b) In order to show for $x \in A$ that $x[A, A] = \{0\}$ implies $x = 0$, we

may assume that $k$ is a local ring with maximal ideal $\mathfrak{m}$. Since $[A,A](\mathfrak{m}) = [A(\mathfrak{m}),A(\mathfrak{m})]$ is the kernel of the reduced trace of the central simple associative algebra $A(\mathfrak{m})$ of degree 3 over the field $k(\mathfrak{m})$, it contains invertible elements. Hence so does $[A,A]$ over $k$, and we conclude $x = 0$, as desired.

(ii) $\Rightarrow$ (i). Follows immediately from (a).

(i) $\Rightarrow$ (ii). Observe $A^{(+)\perp} = Aj_1 + Aj_2$ in $J(A,\nu)$ and $J(A,\mu)$, respectively, by (42.11.6) since $\mu,\nu \in k$ are invertible. Moreover, given $x,y,z_1,z_2 \in A$ and setting $z := z_1j_1 + z_2j_2$, we may apply (42.12.1) to obtain

$$x\,.\,(y\,.\,z) = x\,.\,((yz_1)j_1 + (z_2y)j_2) = (xyz_1)j_1 + (z_2yx)j_2 = (xy)\,.\,z - (z_2[x,y])j_2.$$

By what we have just shown, therefore, $x\,.\,(y\,.\,z) = (xy)\,.\,z$ for all $x,y \in A$ if and only if $z_2 = 0$, and we conclude

$$Aj_1 = \{z \in A^{(+)\perp} \mid x\,.\,(y\,.\,z) = (xy)\,.\,z \text{ for all } x,y \in A\}. \tag{s1}$$

Since $\varphi$ preserves traces, it maps $A^{(+)\perp} \subseteq J(A,\nu)$ to $A^{(+)\perp} \subseteq J(A,\mu)$, and since $\varphi$ preserves bilinearized adjoints, we have $\varphi(x\,.\,z) = x\,.\,\varphi(z)$ for all $x \in A^{(+)}$, $z \in A^{(+)\perp}$. Hence (s1) implies that $\varphi$ sends $Aj_1 \subseteq J(A,\nu)$ to $Aj_1 \subseteq J(A,\mu)$. In particular, $\varphi(j_1) = pj_1$ for some $p \in A$, which implies

$$N_A(p)\mu = N_{J(A,\mu)}(pj_1) = N_{J(A,\mu)}(\varphi(j_1)) = N_{J(A,\nu)}(j_1) = \nu,$$

proving the first part of (b). But we also have $\varphi(j_2) = \varphi(j_1^\sharp) = \varphi(j_1)^\sharp = (pj_1)^\sharp = p^\sharp j_2$, and for $z_1,z_2 \in A$, we conclude

$$\varphi(z_1j_1 + z_2j_2) = z_1\,.\,(p\,.\,j_1 + z_2\,.\,(p^\sharp\,.\,j_2)) = (z_1p)j_1 + (p^\sharp z_2)j_2.$$

Hence $\varphi = \varphi_{A,\mu,p}$, which is an isomorphism by (a) since $p \in A^\times$.

(c) Put $\psi := \psi_{A,\mu,p}$. Then

$$\begin{aligned}
\psi(x^\sharp) &= \psi\Big((x_0^\sharp - \mu(x_1p^{-1})(px_2)) + (\mu x_2^\sharp - (x_0p^{-1})(px_1))j_1 \\
&\qquad + (x_1^\sharp - (x_2p^{-1})(px_0))j_2\Big) \\
&= (x_0^\sharp - \mu(x_1p^{-1})(px_2)) + (\mu x_2^\sharp p^{-1} - [(x_0p^{-1})(px_1)]p^{-1})j_1 \\
&\qquad + (N_A(p)^{-1}px_1^\sharp - N_A(p)^{-1}p[(x_2p^{-1})(px_0)])j_2 \\
&= \Big(x_0^\sharp - N_A(p)\mu(x_1p^{-1})(N_A(p)^{-1}px_2)\Big) \\
&\qquad + \Big(N_A(p)\mu(N_A(p)^{-1}px_2)^\sharp - x_0(x_1p^{-1})\Big)j_1 \\
&\qquad + \Big((x_1p^{-1})^\sharp - (N_A(p)^{-1}px_2)x_0\Big)j_2 \\
&= \Big(x_0 + (x_1p^{-1})j_1 + (N_A(p)^{-1}px_2)j_2\Big)^\sharp = \psi(x)^\sharp.
\end{aligned}$$

Thus $\psi$ is an isomorphism of cubic Jordan algebras. It remains to show that the diagram (3) commutes:

$$\begin{aligned}\psi_{A,N_A(q)\mu,p}\circ\ &\psi_{A^p,\mu,q}(x)\\ &= \psi_{A,N_A(q)\mu,p}(x_0 + [(x_1p^{-1})(pq^{-1})]j_1 + N_A(q)^{-1}[(qp^{-1})(px_2)]j_2)\\ &= x_0 + ([(x_1p^{-1})(pq^{-1})]p^{-1})j_1 + N_A(p)^{-1}N_A(q)^{-1}(p[(qp^{-1})(px_2)])j_2\\ &= x_0 + (x_1(pq)^{-1})j_1 + N_A(pq)^{-1}((pq)x_2)j_2 = \psi_{A^{pq},\mu,pq}(x),\end{aligned}$$

as desired.

(d) We apply Cor. 42.13 to $J := J(A^{\mathrm{op}},\mu^{-1})$, $J_0 := A^{\mathrm{op}(+)} \subseteq J$, $V := A^{\mathrm{op}}j_1 \oplus A^{\mathrm{op}}j_2 \subseteq J$ and $l := \mu j_2 = \mu j_1^\sharp \in J$. Then $l$ is a Kummer element of $J$ relative to $(J_0, V)$ satisfying $l^\sharp = \mu^2 j_2^\sharp = \mu^2\mu^{-1}j_1 = \mu j_1$, and Thm. 42.10 (b) combined with (42.12.2) implies

$$A^{\mathrm{op}} = A_{j_1}(J, J_0, V) = A_{l^\sharp}(J, J_0, V) = A_l(J, J_0, V)^{\mathrm{op}},$$

hence $A = A_l(J, J_0, V)$. We also have $N_J(l) = \mu^3 N_J(j_2) = \mu^3\mu^{-2} = \mu$, and Cor. 42.13 yields a unique homomorphism

$$\varphi\colon J(A,\mu) \longrightarrow J = J(A^{\mathrm{op}},\mu^{-1})$$

of cubic Jordan algebras inducing the identity on $A^{(+)} = A^{\mathrm{op}(+)} = J_0$ and satisfying

$$\varphi(x_0 + x_1j_1 + x_2j_2) = x_0 + x_1 \,.\, l + x_2 \,.\, l^\sharp = x_0 + \mu x_2 j_1 + \mu x_1 j_2$$

for $x_0, x_1, x_2 \in A$. Clearly, $\varphi$ is an isomorphism.

**42.23** We begin with recalling some standard notation from linear algebra. Let $n$ be a positive integer. We denote by $k^n$ rank-$n$ column space over $k$ and by $(e_i)_{1\le i\le n}$ its canonical basis. Analogously, we denote by $k_n$ rank-$n$ row space over $k$ and have $(e_i^{\mathsf{T}})_{1\le i\le n}$ as its canonical basis. Matrices $x, y \in \mathrm{Mat}_n(k)$ can be written as columns of their row vectors, i.e.,

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad x_i = e_i^{\mathsf{T}}x \in k_n, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \quad y_i = e_i^{\mathsf{T}}y \in k_n \quad (1 \le i \le n), \qquad \text{(s1)}$$

ditto for $xy \in \mathrm{Mat}_n(k)$. If $x = (\xi_{ij})_{1\le i,j\le n}$, then (s1) implies

$$(xy)_i = e_i^{\mathsf{T}}xy = x_iy = \sum_{j=1}^n \xi_{ij}e_j^{\mathsf{T}}y = \sum_{j=1}^n \xi_{ij}y_j \qquad (1 \le i \le n). \qquad \text{(s2)}$$

Let us now get back to to the exercise proper. Note first that the off-diagonal components in

$$C = \mathrm{Zor}(k) = \begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix}$$

are rank-3 *column* vectors. Given $y \in \mathrm{Mat}_3(k)$ as in (s1) for $n = 3$, we put

$$l_y = \sum \begin{pmatrix} 0 & 0 \\ y_i^{\mathsf{T}} & 0 \end{pmatrix} [jl] \in \mathrm{Her}_3(C) = J. \tag{s3}$$

We now identify $\mathrm{Mat}_3(k)^{(+)} = \mathrm{Her}_3(k \times k)$ via Prop. 36.9 and the split quadratic étale $k \times k$ with the diagonal of $C = \mathrm{Zor}(k)$. Then another matrix $x = (\xi_{ij})_{1 \le i,j \le 3} \in \mathrm{Mat}_3(k)$ may be viewed canonically as an element of $J$, and we claim

$$x \times l_y = -l_{xy}. \tag{s4}$$

To see this, we combine (36.4.6) with (s2) and obtain

$$\begin{aligned} -x \times l_y &= -\sum \left(\xi_i e_{ii} + \begin{pmatrix} \xi_{jl} & 0 \\ 0 & \xi_{lj} \end{pmatrix} [jl]\right) \times \sum \begin{pmatrix} 0 & 0 \\ y_i^{\mathsf{T}} & 0 \end{pmatrix} [jl] \\ &= \sum \Big(\xi_{ii} \begin{pmatrix} 0 & 0 \\ y_i^{\mathsf{T}} & 0 \end{pmatrix} - \overline{\begin{pmatrix} \xi_{li} & 0 \\ 0 & \xi_{il} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ y_l^{\mathsf{T}} & 0 \end{pmatrix}} - \overline{\begin{pmatrix} 0 & 0 \\ y_j^{\mathsf{T}} & 0 \end{pmatrix} \begin{pmatrix} \xi_{ij} & 0 \\ 0 & \xi_{ji} \end{pmatrix}}\Big)[jl] \\ &= \sum \begin{pmatrix} 0 & 0 \\ \xi_{ii} y_i^{\mathsf{T}} + \xi_{il} y_l^{\mathsf{T}} + \xi_{ij} y_j^{\mathsf{T}} & 0 \end{pmatrix} [jl] \\ &= \sum \begin{pmatrix} 0 & 0 \\ (\sum_{\nu=1}^{3} \xi_{i\nu} y_\nu)^{\mathsf{T}} & 0 \end{pmatrix} [jl] = \sum \begin{pmatrix} 0 & 0 \\ (xy)_i^{\mathsf{T}} & 0 \end{pmatrix} [jl] = l_{xy}, \end{aligned}$$

as claimed.

We now put

$$u_i := \begin{pmatrix} 0 & 0 \\ e_i & 0 \end{pmatrix} \in C^0 \ni \begin{pmatrix} 0 & e_i \\ 0 & 0 \end{pmatrix} =: v_i \qquad (1 \le i \le 3),$$

where $C^0$ stands for the $k$-module of trace-zero-elements in $C$. Adopting the ternary cyclicity convention 36.1 and applying (21.18.4), we conclude

$$u_i u_j = v_l, \quad v_i v_j = u_l \qquad (1 \le i \le 3). \tag{s5}$$

Now put

$$l := l_{\mathbf{1}} = \sum u_i [jl] \tag{s6}$$

where $n_C(u_i) = 0$ and (s5) combined with (36.4.4) imply

$$l^\sharp = \sum \bar{v}_i [jl] = -\sum v_i [jl]. \tag{s7}$$

Moreover, by (36.4.5), (s5), (21.18.4),

$$N_J(l) = t_C(u_1u_2u_3) = t_C(u_1v_1) = t_C(\begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix}) = -1, \tag{s8}$$

so $l$ is invertible in $J$.

(a) We put $J_0 := \mathrm{Mat}_3(k)^{(+)} = \mathrm{Her}_3(k \times k) \subseteq J$ as a regular cubic Jordan subalgebra and have

$$J_0^{\perp} = \sum \begin{pmatrix}0 & k^3\\ k^3 & 0\end{pmatrix}[jl],$$

whence (s6), (s7) imply that $l$ is strongly orthogonal to $J_0$. It is also invertible in $J$ and from (s4) we deduce $x \,.\, (y \,.\, l) = x \,.\, (y \,.\, l_{\mathbf{1}}) = x \,.\, l_y = l_{xy} = (xy) \,.\, l$ for all $x, y \in \mathrm{Mat}_3(k)$, i.e., the stability condition for $l$. In other words, $l$ is a Kummer element of $J$ relative to $J_0$ and $A_l(J, J_0) = \mathrm{Mat}_3(k)$. Since the norm of $\mathrm{Mat}_3(k)$ is surjective, (a) follows from Cor. 42.13 combined with Exc. 42.22 (a).

(b) The regularity of $J_0 := \mathrm{Sym}_3(k) \subseteq J$ is clear, and since $l$ is an ivertible element of $J$ strongly orthogonal to $\mathrm{Mat}_3(k)^{(+)}$, it is so to $J_0$. But if $l$ were a Kummer element relative to $J_0$, then what we have seen in (a) would imply that $\mathrm{Sym}_3(k) \subseteq \mathrm{Mat}_3(k)$ were an *associative* subalgebra, a contradiction.

**42.24** By Lemma 38.4, there exists an elementary idempotent $e \in J$ such that $u \in J_0(e)$. Since $J$ is split, so the class group of $J$ is trivial (Lemma 41.15), the automorphism group of $J$ acts transitively on the elementary idempotents (Cor. 41.19). Hence we may assume $J = \mathrm{Her}_3(C)$, $C := \mathrm{Zor}(F)$, $e = e_{11}$. Consulting the Peirce rules (32.15.1) and (37.8.1) combined with the fact that $u$ has trace zero (Exc. 34.23), we deduce from (36.4.8) that $u = \xi(e_{22} - e_{33}) + v[23]$, for some $\xi \in F$ and some $v \in C$.

($*$) We claim that *there exists a $w \in C^\times$ such that $w^{-1}v$ is contained in a (split) quadratic étale subalgebra of $C$.*

If $v$ is invertible, then $w := v$ does the job. If not, then Zariski density yields a $w \in C^\times$ having $t_C(w^{-1}v) = 1$. Since $n_C(w^{-1}v) = n_C(w)^{-1}n_C(v) = 0$, we conclude that $w^{-1}v$ is an elementary idempotent in $C$, and ($*$) follows.

Replacing $w$ by $\sqrt{w}^{-1}w$ if necessary, we may assume $n_C(w) = 1$. Consulting (36.4.5), we see that the assignment

$$\sum(\xi_i e_{ii} + v_i[jl]) \longmapsto \sum \xi_i e_{ii} + (w^{-1}v_1)[23] + (v_2w^{-1}[31] + (wv_3w)[12]$$

gives a linear bijection $J \to J$ that preserves unit element and norm, hence is an automorphism of $J$ (Exc. 34.18). By ($*$), we may therefore assume that $v$ itself belongs to a split quadratic étale subalgebra of $J$. But this means that $u = \xi(e_{22} - e_{33}) + v[23]$ belongs to a subalgebra of $J$ isomorphic to $\mathrm{Her}_3(F \times$

$F) \cong \mathrm{Mat}_3(F)^{(+)}$. By Exercises 42.23 and 41.34, therefore, we may assume $J = J(\mathrm{Mat}_3(F), 1)$ as a first Tits construction such that $u \in \mathrm{Mat}_3(F)^{(+)}$. Since nilpotent elements of $A := \mathrm{Mat}_3(F)$ having index 2 (i.e., rank 1) are conjugate under (inner) automorphisms of $A$, and every automorphism $\varphi$ of $A$ extends to the automorphism $J(\varphi, 1)$ of $J$, the problem is solved.

**42.25** We put $J := J(A, \mu)$. Then Thm. 42.11 yields

$$U_p x = T_J(p, x)p - p^\sharp \times x = T_A(p, x_0)p - p^\sharp \times x_0 + (p^\sharp x_1)j_1 + (x_2 p^\sharp)j_2,$$

and (1) follows from Prop. 34.12. Combining (33.11.2) with (1), we conclude

$$\begin{aligned} x^{(\sharp,p)} &= N_A(p)U_{p^{-1}}x^\sharp \\ &= N_A(p)\Big(p^{-1}(x_0^\sharp - \mu x_1 x_2)p^{-1} + (p^{-1\sharp}(\mu x_2^\sharp - x_0 x_1))j_1 \\ &\quad + ((x_1^\sharp - x_2 x_0)p^{-1\sharp})j_2\Big), \end{aligned}$$

and (2) has been proved. That $\tilde{L}_p$, $\tilde{R}_p$ are isomorphisms of cubic Jordan algebras as indicated could now be proved by using (2) and showing that they preserve adjoints. Leaving this to the reader, we prefer to adopt a different approach and begin by deriving (5). The first two equations follow immediately from the left (resp. right) Moufang identity. For the third, we apply (13.5.4) and obtain

$$\begin{aligned} \tilde{L}_p U_q \tilde{R}_p(x) &= \tilde{L}_p U_q(x_0 p + (p^{-1}x_1 p^\sharp)j_1 + (px_2)j_2) \\ &= \tilde{L}_p\Big(q(x_0 p)q + (q^\sharp(p^{-1}x_1 p^\sharp))j_1 + ((px_2)q^\sharp)j_2\Big) \\ &= p(q(x_0 p)q) + \Big((q^\sharp(p^{-1}x_1 p^\sharp))p\Big)j_1 + \Big(p^\sharp((px_2)q^\sharp)p^{-1}\Big)j_2 \\ &= (pq)x_0(pq) + ((pq)^\sharp x_1)j_1 + (x_2(pq)^\sharp)j_2 = U_{pq}(x) \end{aligned}$$

and, similarly,

$$\begin{aligned} \tilde{R}_q U_p \tilde{L}_q(x) &= \tilde{R}_q U_p(qx_0 + (x_1 q)j_1 + (q^\sharp x_2 q^{-1})j_2) \\ &= \tilde{R}_q\Big(p(qx_0)p + (p^\sharp(x_1 q))j_1 + ((q^\sharp x_2 q^{-1})p^\sharp)j_2\Big) \\ &= (p(qx_0)p)q + \Big(q^{-1}(p^\sharp(x_1 q))q^\sharp\Big)j_1 + \Big(q((q^\sharp x_2 q^{-1})p^\sharp)\Big)j_2 \\ &= (pq)x_0(pq) + ((pq)^\sharp x_1)j_1 + (x_2(pq)^\sharp)j_2 = U_{pq}(x). \end{aligned}$$

Thus (5) holds. Its last equation combined with Prop. 12.24 and 31.20 implies $\tilde{L}_p, \tilde{R}_p \in \mathrm{Str}(J)$ with $\tilde{L}_p^\sharp = \tilde{R}_p$, $\tilde{R}_p^\sharp = \tilde{L}_p$. Since $\tilde{L}_p^\sharp(1_J) = p = \tilde{R}_p^\sharp(1_J)$, therefore, we deduce from Thm. 31.22 (d) that $\tilde{L}_p$, $\tilde{R}_p$ are indeed isomorphisms of abstract Jordan algebras from $J^{(p)}$ to $J$. It remains to prove that they are, in fact, homomorphisms of cubic ones, i.e., that they preserve norms. Putting

$J := J(A,\mu)$, we compute

$$\begin{aligned} N_J \circ \tilde{L}_p(x) &= N_J(px_0 + (x_1p)j_1 + (p^\sharp x_2 p^{-1})j_2) \\ &= N_A(p)N_A(x_0) + \mu N_A(p)N_A(x_1) + \mu^2 N_A(p)N_A(x_2) \\ &\quad - \mu T_A((px_0)(x_1p)(p^\sharp x_2 p^{-1}), \end{aligned}$$

where the last summand, up to the factor $-\mu$, agrees with

$$\begin{aligned} N_A(p)T_A\Big((p(x_0x_1)p)(p^{-1}x_2p^{-1})\Big) &= N_A(p)T_A\Big(p((x_0x_1)(x_2p^{-1}))\Big) \\ &= N_A(p)T_A((x_0x_1)(x_2p^{-1})p) \\ &= N_A(p)T_A(x_0x_1x_2). \end{aligned}$$

Hence the relation $N_J \circ \tilde{L}_p = N_{J^{(p)}}$ holds strictly, so $\tilde{L}_p\colon J^{(p)} \to J$ is indeed a homomorphism of cubic Jordan algebras. The map $\tilde{R}_p$ can be treated similarly. The rest is clear.

**42.26** (a) We begin by showing that (1) makes $E^\perp$ a left $E$-module. Since $1\,.\,u = u$, we must show

$$x \times (y \times u) = -(xy) \times u \tag{s1}$$

for all $x, y \in E$, $u \in E^\perp$. After a faithfully flat base change that splits $E$ (Cor. 39.32), and consulting Prop. 25.4, we may assume that $E$ itself is split, so there is an elementary frame $\Omega = (e_1, e_2, e_3)$ in $J$ satisfying $E = \sum ke_i$. Let $J = \sum(ke_i + J_{jl})$ be the Peirce decomposition of $J$ relative to $\Omega$. Then $E^\perp = \sum J_{jl}$ by (37.13.5), and we have $x = \sum \xi_i e_i$, $y = \sum \eta_i e_i$, $u = \sum u_{jl}$, for some $\xi_i, \eta_i \in k$, $u_{jl} \in J_{jl}$, $1 \le i \le 3$. Now (37.13.4) implies

$$x \times (y \times u) = -x \times \sum \eta_i u_{jl} = \sum \xi_i \eta_i u_{jl} = (xy) \times u_{jl},$$

and this is (s1).

(b) The property of $q_E$ to be a quadratic form over $E$ can be proved in a similar manner as in (a), but we prefer an approach that is "rational" by avoiding scalar extensions once (a) is taken for granted. Note first that (2) is a viable definition of $q_E$ as a map since $T_E$ is a regular symmetric bilinear form on $E$. Actually, $q_E$ is nothing else than the $k$-quadratic map belonging to the complemented cubic Jordan subalgebra $(E, E^\perp)$ of $J$ via (35.6.1) and denoted there by $Q$. In particular, by (35b.1), $q_E$ is homogeneous of degree 2 over $E$: $q_E(x\,.\,u) = x^2 q_E(u)$ for all $x \in E$, $u \in E^\perp$. Now let $x \in E$, $u, v \in E^\perp$ and $z \in E$.

Then the equations

$$\begin{aligned} T_E(z, q_E(x\,.\,u, v)) &= T_J(z, (x \times u) \times v) = T_J(x \times (z \times v), u) \\ &= -T_J((xz) \times v, u) = -T_J(xz, u \times v) = T_E(xz, q_E(u, v)) \\ &= T_E\big(z, xq_E(u, v)\big) \end{aligned}$$

show that the $k$-bilinearization of $q_E$ is, in fact, $E$-bilinear, as desired.

(c) The first part follows from the decomposition $J = E \oplus E^\perp$. In (3) we first note that $q_{E_R}$ is nothing else than the $R$-quadratic extension of $q_E$ viewed as a quadratic map over $k$, so adopting the notational conventions of 12.27, the top row of (3) becomes

$$({}_k(q_E))_R \colon ({}_k(E^\perp))_R \longrightarrow ({}_kE)_R = E \otimes R,$$

and it makes sense to regard the vertical arrow on the left of (3) as the identification (12.27.1). On the other hand, the bottom row of (3) should be written, more accurately, as

$$(q_E)_{R_E} \colon (E^\perp)_{R_E} \longrightarrow E_{R_E} = E \otimes_E R_E = R \otimes E. \tag{s2}$$

But $({}_kE)_R = E_{R_E}$, again under the identification (12.27.1), and combining (s2) with (12.27.2), we obtain $r \otimes x = 1_E \otimes_E (r \otimes x) = x \otimes r$ for $x \in E$, $r \in R$. Thus the commutativity of (3) is equivalent to $({}_k(q_E))_R = (q_E)_{R_E}$, which follows from (12.27.5).

(d) If $R \in k$-**alg** and $S \in R$-**alg** are both faithfully flat, then so is $S \in k$-**alg** (25.3 (i)). The same conclusion holds for the property of being finitely presented in place of being faithfully flat (Exc. 25.30 (a)). By Cor. 39.32, therefore, we may assume that $E$ is split. Accordingly, let $\Omega = (e_1, e_2, e_3)$ be an elementary frame in $J$, with Peirce decomposition $J = \sum(ke_i + J_{jl})$, such that $E = \sum ke_i$. By Prop. 39.28, we may assume that $J$ is regular of rank $n \geq 9$. Changing scalars to any algebraically close field $K \in k$-**alg** makes $J_K$ split of dimension 9, 15, or 27, and Cor. 39.3 shows that the off-diagonal Peirce spces of $J_K$ relative to $\Omega_K$ all have the same dimension 2, 4, or 8, respectively. From (37.13.8) combined with Prop. 37.4 (c) we therefore deduce that the restriction of $S_J$ to $J_{jl}$ is a regular quadratic form of even rank. After an appropriate étale cover of $k$, Exc. 26.12 (b) allows us to assume that this restriction is split hyperbolic. In particular $S(u_{jl}) = -1$ for some $u_{jl} \in J_{jl}$, and we have found a strong co-ordinate system in $J$ extending $\Omega$. Combining the Jacobson co-ordinatization theorem 37.17 with Exc. 39.38, we therefore obtain an identification $J = \mathrm{Her}_3(C)$, for some composition algebra $C$ over $k$, such that $E = \sum ke_{ii}$ is the diagonal of $J$. After yet another fppf base change, we may assume that $C = C_{0r}$ is split of rank $r = \frac{1}{3}(n - 3)$, proving the first part of

(d). Note that $E_R = R_E$ (by (b)) is faithfully flat over $E$ since faithful flatness is stable under base change (25.2). Combining (3) with (36.4.7), (36.4.6), we therefore conclude that

$$(E^\perp)_{R_E} = E_R^\perp = \sum C[jl]$$

is a free $E_R$-module of rank $r$. Hence $E^\perp$ by [26, I, Lemme 3.6 (c)] is a finitely generated projective $E$-module of rank $r$. It remains to show that $q_E$ is non-singular, and even regular unless $n = 6$ and $2 \notin k^\times$. Since a quadratic form on a projective module that becomes regular (resp. non-singular) after a faithfully flat base change must have been so all along (which follows immediately from the definitions in the regular case and from Exc. 25.34 in the non-singular one), it suffices to prove the assertion for $q_{E_R}$ rather than $q_E$. But (36.4.4) shows $q_{E_R} \cong (n_C)_{E_R}$, and $n_C$ by Cor. 19.11 is regular unless $r = 1$ and $\frac{1}{2} \notin k$, in which case it is at least non-singular. The assertion follows.

(e) Since $E^\perp$ is an $E$-module under the action (1), the stability condition (iii) of 42.8 holds automatically for any $l \in E^\perp$. Thus $l$ is a Kummer element relative to $E$ if and only if $l$ is invertible in $J$ and both $l$ and $l^\sharp$ belong to $E^\perp$; the latter condition, in turn, is equivalent to $q_E(l) = 0$, proving the first part of (e). In this case, we clearly have $A_l(J, E) = E$, and Cor. 42.13 yields the indicated embedding from $J(E, \lambda)$ to $J$. The final assertion will follow once we have shown that $l$ is unimodular as an element of $E^\perp$ *as an $E$-module*. But this is clear since $q_E(l, l^\sharp) = N_J(l)1_E$ by (35b.11).

**42.27** (a) We begin with the reduction to the case $\mu = 1$, $p = 1_C$. For any $\alpha \in k^\times$, $p \in C^\times$, we have $\hat{p} := (\alpha, p) \in A^\times$ and

$$A^{\hat{p}} = k \times C^p, \quad N_A(\hat{p}) = \alpha n_C(p). \tag{s1}$$

Now let $\alpha := \mu$ and $p := 1_C$. Then (s1) implies $A^{\hat{p}} = A$, $N_A(\hat{p}) = \mu$ and applying Exc. 42.22 yields $J(A, \mu) \cong J(A, 1)$. Next assume $\alpha = 1$ in (s1). Assuming the case $\mu = 1$, $p = 1_C$ has been settled, we conclude

$$\mathrm{Her}_3(C^p, \Gamma_0) \cong J(A^{\hat{p}}, 1) \cong J(A, N_A(\hat{p})) \cong J(A, 1) \cong \mathrm{Her}_3(C, \Gamma_0).$$

From now on, we may therefore assume $\mu = 1$ and $p = 1_C$.

(i) We abbreviate $t := t_C$, $n := n_C$, $T := T_J$, $S := S_J$, $N := N_J$ and write $C^0$ for the module of trace-zero elements in $C$. Moreover, we put $e_1 := (1, 0) \in A$, have $A = ke_1 \oplus C$ as a direct sum of submodules, and recall from Exc. 34.24 (b)

the relations

$$1 := 1_A = e_1 + 1_C, \tag{s2}$$
$$N(\alpha e_1 + u) = \alpha n(u), \tag{s3}$$
$$(\alpha e_1 + u)^\sharp = n(u)e_1 + \alpha\bar{u}, \tag{s4}$$
$$(\alpha e_1 + u) \times (\beta e_1 + v) = n(u,v)e_1 + \alpha\bar{v} + \beta\bar{u}, \tag{s5}$$
$$T(\alpha e_1 + u, \beta e_1 + v) = \alpha\beta + t(uv), \tag{s6}$$
$$T(\alpha e_1 + u) = \alpha + t(u), \tag{s7}$$
$$S(\alpha e_1 + u) = \alpha t(u) + n(u), \tag{s8}$$
$$S(\alpha e_1 + u, \beta e_1 + v) = \alpha t(v) + \beta t(u) + n(u,v) \tag{s9}$$

for all $\alpha, \beta \in$, $u, v \in C$. From (s4) and (s7) we conclude that $e_1$ is an elementary idempotent in $J$. It remains to establish the corresponding Peirce rules. While (3) follows immediately from (37.2.1), the remaining assertions require a proof. Let

$$x = x_0 + x_1 j_1 + x_2 j_2, \quad x_i = \alpha_i e_1 + v_i \in A, \quad \alpha_i \in k, \quad v_i \in C, \quad 0 \le i \le 2. \tag{s10}$$

Then (42.11.7) and (s7) imply

$$T(x) = T(x_0) = \alpha_0 + t(v_0). \tag{s11}$$

On the other hand, (42.11.5) yields $e_1 \times x = e_1 \times x_0 - (e_1 x_1) j_1 - (x_2 e_1) j_2$, and applying (s5) we conclude

$$e_1 \times x = \bar{v}_0 - (\alpha_1 e_1) j_1 - (\alpha_2 e_1) j_2. \tag{s12}$$

Now (4) follows by combining (37.2.2) with (s11) and (s12). Observing

$$e_0 := 1 - e_1 = 1_C, \tag{s13}$$

we obtain $T(x)e_0 - x = (\alpha_0 + t(v_0))1_C - x_0 - x_1 j_1 - x_2 j_2 = \alpha_0(1_C - e_1) + \bar{v}_0 - x_1 j_1 - x_2 j_2$, and comparing this with (s12), we deduce (5) from (37.2.3).

(ii) We clearly have $\sum e_i = 1$. Suppose we know that $e_2$ is an elementary idempotent of $J$. Then (5) shows that it is orthogonal to $e_1$, and the assertion follows from Prop. 37.4. Thus we only need to show that $e_2$ is an elementary idempotent. From (s7), (42.11.7) and (s4) we deduce $T(e_2) = t(u_0) = 1$, while (42.11.5) and (s5) yield $e_2^\sharp = (u_0^\sharp - n(u_0)e_1) + (n(u_0)^2 e_1^\sharp - n(u_0)u_0 e_1) j_1 + (e_1^\sharp - n(u_0)e_1 u_0) j_2 = n(u_0)e_1 - n(u_0)e_1 = 0$, so $e_2$ is indeed an elementary idempotent.

(iii) Decomposing an arbitrary element $x \in J$ as in (s10)), we claim ,

$$e_2 \times x = \big((n(u_0, v_0) - n(u_0)\alpha_1 - \alpha_2)e_1 + \alpha_0\bar{u}_0\big) + \big(-\alpha_0 e_1 + (n(u_0)\bar{v}_2 - u_0 v_1)\big)j_1 + \big(-n(u_0)\alpha_0 e_1 + (\bar{v}_1 - v_2 u_0)\big)j_2, \tag{s14}$$

$$e_3 \times x = \big((n(\bar{u}_0, v_0) + n(u_0)\alpha_1 + \alpha_2)e_1 + \alpha_0 u_0\big) + \big(\alpha_0 e_1 - (n(u_0)\bar{v}_2 + \bar{u}_0 v_1)\big)j_1 + \big(n(u_0)\alpha_0 e_1 - (\bar{v}_1 + v_2\bar{u}_0)\big)j_2. \tag{s15}$$

To establish (s14), we expand the left-hand side by (42.11.5) and apply (s5) to conclude

$$\begin{aligned} e_2 \times x &= \big(u_0 + e_1 j_1 + (n(u_0)e_1)j_2\big) \times \big(x_0 + x_1 j_1 + x_2 j_2\big) \\ &= (u_0 \times x_0 - e_1 x_2 - n(u_0)x_1 e_1) + (n(u_0)e_1 \times x_2 - u_0 x_1 - x_0 e_1)j_1 + \\ &\quad (e_1 \times x_1 - n(u_0)e_1 x_0 - x_2 u_0)j_2 \\ &= (n(u_0, v_0)e_1 + \alpha_0\bar{u}_0 - \alpha_2 e_1 - n(u_0)\alpha_1 e_1) + \\ &\quad (n(u_0)\bar{v}_2 - u_0 v_1 - \alpha_0 e_1)j_1 + (\bar{v}_1 - n(u_0)\alpha_0 e_1 - v_2 u_0)j_2. \end{aligned}$$

Hence (s14) follows. Similarly,

$$\begin{aligned} e_3 \times x &= \big(\bar{u}_0 - e_1 j_1 - (n(u_0)e_1)j_2\big) \times \big(x_0 + x_1 j_1 + x_2 j_2\big) \\ &= (\bar{u}_0 \times x_0 + e_1 x_2 + n(u_0)x_1 e_1) + (-n(u_0)e_1 \times x_2 - \bar{u}_0 x_1 + x_0 e_1)j_1 + \\ &\quad (-e_1 \times x_1 + n(u_0)e_1 x_0 - x_2\bar{u}_0)j_2 \\ &= (n(\bar{u}_0, v_0)e_1 + \alpha_0 u_0 + \alpha_2 e_1 + n(u_0)\alpha_1 e_1) + \\ &\quad (-n(u_0)\bar{v}_2 - \bar{u}_0 v_1 + \alpha_0 e_1)j_1 + (-\bar{v}_1 + n(u_0)\alpha_0 e_1 - v_2\bar{u}_0)j_2 \end{aligned}$$

gives (s15).

We now prove (6) by applying (37.5.2), (s14), (s15) and (s11) to obtain the following chain of equivalent statements.

$$\begin{aligned} x \in J_{23} &\iff T(x) = 0, \quad e_2 \times x = e_3 \times x = 0 \\ &\iff \alpha_0 + t(v_0) = 0, \quad n(u_0, v_0) = n(u_0)\alpha_1 + \alpha_2, \quad \alpha_0 = 0, \\ &\qquad n(u_0)\bar{v}_2 = u_0 v_1, \quad \bar{v}_1 = v_2 u_0, \\ &\qquad n(\bar{u}_0, v_0) + n(u_0)\alpha_1 + \alpha_2 = 0, \quad n(u_0)\bar{v}_2 + \bar{u}_0 v_1 = 0 = \bar{v}_1 + v_2\bar{u}_0; \end{aligned}$$

if this holds, then $0 = \bar{v}_1 - \bar{v}_1 = v_2 u_0 + v_2\bar{u}_0 = v_2$, hence $v_1 = 0$ as well, and (6)

is proved. Similarly, also using (s12),

$$\begin{aligned} x \in J_{31} &\iff T(x) = 0, \quad e_1 \times x = 0 = e_3 \times x \\ &\iff \alpha_0 + t(v_0) = 0, \quad v_0 = 0, \quad \alpha_1 = \alpha_2 = 0, \\ &\quad\ \alpha_0 = 0, \quad n(u_0)\bar{v}_2 + \bar{u}_0 v_1 = 0 = \bar{v}_1 + v_2 \bar{u}_0 \\ &\iff \alpha_0 = \alpha_1 = \alpha_2 = 0, \quad v_0 = 0, \quad v_1 = -u_0 \bar{v}_2, \end{aligned}$$

and this amounts to (7). Finally,

$$\begin{aligned} x \in J_{12} &\iff T(x) = 0, \quad e_1 \times x = 0 = e_2 \times x \\ &\iff v_0 = 0, \quad \alpha_1 = \alpha_2 = 0, \\ &\quad\ \alpha_0 = 0, \quad n(u_0)\bar{v}_2 - u_0 v_1 = 0 = \bar{v}_1 - v_2 u_0 \\ &\iff v_0 = 0, \quad \alpha_0 = \alpha_1 = \alpha_2 = 0, \quad v_1 = \bar{u}_0 \bar{v}_2, \end{aligned}$$

which proves (8).

(iv) From (8) we deduce that $u_{31}$ belongs to $J_{31}$. Since $2u_0 - 1_C$ has trace zero and

$$u_{23} = (2u_0 - 1_C) + 2e_1 j_1 + (n_C(u_0, 2u_0 - 1_C) - 2n_C(u_0))e_1 j_2,$$

$u_{23}$ by (6) belongs to $J_{23}$. It remains to compute $S(u_{jl})$ for $i = 1, 2$. We do so by applying (42.11.8), (s8) and (s6) to conclude

$$\begin{aligned} S(u_{23}) &= S(2u_0 - 1_C) - T\big(2e_1, (2n_C(u_0) - 1)e_1\big) = n(2u_0 - 1_C) - 2(2n(u_0) - 1) \\ &= 4n(u_0) - 2 + 1 - 4n(u_0) + 2 = 1, \\ S(u_{31}) &= T(u_0) = t(u_0) = 1, \end{aligned}$$

and the proof of (iv) is complete.

(v) In the terminology of Prop. 37.15 we have

$$\omega = 1, \quad \gamma_1 = \gamma_2 = -1, \quad \gamma_3 = 1. \tag{s16}$$

We begin by verifying (11). By Prop. 12.24, we may assume that $u$ is invertible. Then the left Moufang identity yields

$$\begin{aligned} u((uv - \bar{u}\bar{v})(uw)) &= (u(uv - \bar{u}\bar{v})u)w = (u(uvu))w - n(u)(\bar{v}u)w \\ &= n(u, \bar{v})u^2 w - n(u)(u\bar{v} + \bar{v}u)w \\ &= n(u, \bar{v})u^2 w - n(u)(t(u)\bar{v} + t(v)u - n(u, \bar{v})1_C)w \\ &= u\big(n(u, \bar{v})uw - t(u)\bar{u}(\bar{v}w) - n(u)t(v)w + n(u, \bar{v})\bar{u}w\big) \\ &= u\Big(\big(t(u)n(u, \bar{v}) - n(u)t(v)\big)w - t(u)\bar{u}(\bar{v}w)\Big). \end{aligned}$$

Cancelling $u$, the assertion follows.

Now let

$$x = (\bar{u}_0\bar{v})j_1 + vj_2, \quad y = (\bar{u}_0\bar{w})j_1 + wj_2, \qquad (v, w \in C) \tag{s17}$$

be arbitrary elements of $J_{12} = C_{J,\ominus}$. Then (42.11.5) yields

$$\begin{aligned} x \times u_{23} &= ((\bar{u}_0\bar{v})j_1 + vj_2) \times \big((2u_0 - 1_C) + 2e_1j_1 + (2n(u_0) - 1)e_1j_2\big) \\ &= \big( - (2n(u_0) - 1)(\bar{u}_0\bar{v})e_1 - 2e_1v\big) + \big((2n(u_0) - 1)v \times e_1 - (2u_0 - 1_C)\bar{u}_0\bar{v}\big)j_1 \\ &\quad + (2(\bar{u}_0\bar{v}) \times e_1 - v(2u_0 - 1_C))j_2 \\ &= \big((2n(u_0) - 1)\bar{v} - 2n(u_0)\bar{v} + \bar{u}_0\bar{v}\big)j_1 + (2vu_0 - 2vu_0 + v)j_2 \\ &= (-\bar{v} + \bar{u}_0\bar{v})j_1 + vj_2 = (-u_0\bar{v})j_1 + vj_2, \end{aligned}$$

hence

$$x \times u_{23} = -(u_0\bar{v})j_1 + vj_2. \tag{s18}$$

Similarly,

$$\begin{aligned} u_{31} \times y &= ( - u_0j_1 + 1_Cj_2) \times ((\bar{u}_0\bar{w})j_1 + wj_2) \\ &= (u_0w - \bar{u}_0\bar{w}) + (1_C \times w)j_1 - (u_0 \times (\bar{u}_0\bar{w}))j_2, \end{aligned}$$

hence

$$u_{31} \times y = (u_0w - \bar{u}_0\bar{w}) + (t(w)e_1)j_1 - (n(u_0, \bar{u}_0\bar{w})e_1)j_2. \tag{s19}$$

As a side remark we note $u_0w - \bar{u}_0\bar{w} \in C^0$ and $n(u_0, u_0w - \bar{u}_o\bar{w}) - n(u_0)t(w) = n(\bar{u}_0u_0, w) - n(u_0, \bar{u}_0\bar{w}) - n(u_0)t(w) = -n(u_0, \bar{u}_0\bar{w})$, so

$$u_{31} \times y = (u_0w - \bar{u}_0\bar{w}) + (t(w)e_1)j_1 + ([n(u_0, u_0w - \bar{u}_0\bar{w}) - n(u_0)t(w)]e_1)j_2$$

by (6) does indeed belong to $J_{23}$, as it should. Using (s18), (s19) and (42.11.5), (s5), we can now compute

$$\begin{aligned} (x \times u_{23}) \times (u_{31} \times y) &= \big( - (u_0\bar{v})j_1 + vj_2\big) \times \\ &\qquad \big((u_0w - \bar{u}_0\bar{w}) + (t(w)e_1)j_1 - (n(u_0, \bar{u}_0\bar{w})e_1)j_2\big) \\ &= ( - n(u_0, \bar{u}_0\bar{w})(u_0\bar{v})e_1 - t(w)e_1v) + \\ &\qquad ( - n(u_0, \bar{u}_0\bar{w})v \times e_1 + (u_0w - \bar{u}_0\bar{w})(u_0\bar{v}))j_1 + \\ &\qquad ( - t(w)(u_0\bar{v}) \times e_1 - v(u_0w - \bar{u}_0\bar{w}))j_2 \\ &= ((u_0w - \bar{u}_0\bar{w})(u_0\bar{v}) - n(u_0, \bar{u}_0\bar{w})\bar{v})j_1 + \\ &\qquad ( - t(w)v\bar{u}_0 - v(u_0w) + v(\bar{u}_0\bar{w}))j_2. \end{aligned}$$

Here we note

$$-t(w)v\bar{u}_0 - v(u_0w) + v(\bar{u}_0\bar{w}) = -v(\bar{u}_0w) - v(\bar{u}_0\bar{w}) - v(u_0w) + v(\bar{u}_0\bar{w}) = -vw$$

since $u_0$ has trace 1 and apply (11) to conclude

$$\begin{aligned}(u_0w - \bar{u}_0\bar{w})(u_0\bar{v}) - n(u_0, \bar{u}_0\bar{w})\bar{v} &= \big(n(u_0, \bar{w}) - n(u_0)t(w)\big)\bar{v} - \bar{u}_0(\bar{w}\bar{v}) - n(u_0^2, \bar{w})\bar{v}\\ &= -\bar{u}_0\overline{vw} + \big(n(u_0, \bar{w}) - n(u_0)t(w)\\ &\quad - n(u_0, \bar{w}) + n(u_0)t(w)\big)\bar{v}\\ &= -\bar{u}_0\overline{vw}.\end{aligned}$$

Hence

$$(x \times u_{23}) \times (u_{31} \times y) = (-\bar{u}_0\overline{vw})j_1 + (-vw)j_2. \tag{s20}$$

We put $C' := C_{J,\varepsilon}$ and $n' := n_{C_{J,\varepsilon}}$. Since $\omega = 1$ by (s16), we combine (s20) with (37.15.3) to conclude that

$$\varphi\colon C \longrightarrow C', \quad v \longmapsto (-\bar{u}_0\bar{v})j_1 - vj_2$$

is an isomorphism of $k$-algebras; in particular, it is unital. Moreover, by (37.15.4), $(n' \circ \varphi)(v) = -S(-(\bar{u}_0\bar{v})j_1 - vj_2) = n(v)$, so $\varphi\colon (C, n) \to (C', n')$ is actually an isomorphism of *conic* $k$-algebras.

(b) $C$ is free of rank 8 as a $k$-module. By Exc. 37.22, we may assume $\Gamma = \operatorname{diag}(\gamma_1, \gamma_2, \gamma_3)$, $\prod \gamma_i = 1$. Since $n_C$ is universal, we find $p, q \in C^\times$ satisfying $n_C(p) = -\gamma_2^{-1}$, $n_C(q) = -\gamma_1^{-1}$, hence $n_C(pq) = \gamma_3$. By Exc. 37.24, therefore, we may assume $\Gamma = \Gamma_0$. On the other hand, the Alsaody-Gille theorem 23.10 yields some $p \in C^\times$ making $C^p$ split. By (a), therefore, $\mathrm{Her}_3(C, \Gamma) \cong \mathrm{Her}_3(C^p, \Gamma_0)$ is split by Prop. 40.6.

## Solutions for Section 43

**43.11** In order to get the terminology straight, let us denote by $\mathbf{paltinv}_k$ the category of pointed alternative $k$-algebras with involution as defined in Exc. 43.11. By contrast, let us denote by $\mathbf{altist}_k$ the category of alternative $k$-algebras with isotopy involution as defined in 43.4.

We begin by defining a functor $\Phi\colon \mathbf{paltinv}_k \to \mathbf{altist}_k$. Let $((B, \tau), q)$ be an object of $\mathbf{paltinv}_k$. Then Cor. 43.8 shows that

$$\Phi\Big(((B, \tau), q)\Big) := (B^q, \tau^q, q)$$

is an object of $\mathbf{altist}_k$. If $\varphi\colon ((B, \tau), q) \to ((B', \tau'), q')$ is a morphism in $\mathbf{paltinv}_k$, then it is straightforward to check that

$$\varphi\colon (B^q, \tau^q, q) \longrightarrow (B'^{q'}, \tau'^{q'}, q')$$

is a morphism in $\mathbf{altist}_k$. Hence we obtain a functor $\Phi$ of the desired kind.

Next we define a functor $\Psi\colon$ **altist**$_k \to$ **paltinv**$_k$ in the opposite direction. Let $(B, \tau, q)$ be an object of **altist**$_k$, i.e., an alternative $k$-algebra with isotopy involution. Then Prop. 43.7 and Lemma 43.1 show with $p := q^{-1}$ that

$$\Psi((B, \tau, q)) := ((B^p, \tau^p), q)$$

is an object of **paltinv**$_k$. If $\psi\colon (B, \tau, q) \to (B', \tau', q')$ is a morphism in **altist**$_k$ and $p := q^{-1}$, $p' := q'^{-1}$, then $\psi(p) = p'$, and it is straightforward to check that

$$\psi\colon ((B^p, \tau^p), p) \longrightarrow ((B'^{p'}, \tau'^{p'}), q')$$

is a morphism in **paltinv**$_k$. Hence we obtain a functor $\Psi$ of the desired kind.

Now we simply apply (43.7.5) to conclude that $\Psi \circ \Phi$ is the identity on **paltinv**$_k$ and $\Phi \circ \Psi$ is the identity on **altist**$_k$. Summing up

$$\Phi\colon \textbf{paltinv}_k \xrightarrow{\sim} \textbf{altist}_k$$

is an isomorphism of categories with inverse $\Psi$.

**43.12** The map $\epsilon_A$ has clearly period two and fixes $p$. For the first part of the problem, it therefore suffices to show (43.2.1) for $\epsilon_A$ in place of $\tau$. To this end, let $x, x', y, y' \in A$. Then

$$\begin{aligned}
\Big(\epsilon_A((y,y'))p^{-1}\Big)\Big(p\epsilon_A((x,x'))\Big) &= ((y',y)(q,q))((q^{-1},q^{-1})(x',x)) \\
&= ((y'q^{-1})(qq), qy)((q^{-1}q^{-1})(qx'), xq^{-1}) \\
&= (y'q, qy)(q^{-1}x', xq^{-1}) \\
&= \Big(((y'q)q^{-1})(q(q^{-1}x')), (xq^{-1})(qy)\Big) = (y'x', (xq^{-1})(qy)) \\
&= \epsilon_A\Big(((xq^{-1})(qy)), y'x'\Big) = \epsilon_A((x,x')(y,y')),
\end{aligned}$$

as desired. Turning to the second part of the problem, we first note

$$H(A^q \times A^{\mathrm{op}}, \epsilon_A) = \{(x,x) \mid x \in A\}.$$

On the other hand, given $x, x' \in A$, we have

$$\begin{aligned}
\Big(\epsilon_A((x,x'))p\Big)(x,x') &= ((x',x)(q^{-1},q^{-1}))(x,x') \\
&= ((x'q^{-1})(qq^{-1}), q^{-1}x)(x,x')) \\
&= (x'q^{-1}, q^{-1}x)(x,x') = \Big(((x'q^{-1})q^{-1})(qx), x'(q^{-1}x)\Big) \\
&= ((x'q^{-2})(qx), x'(q^{-1}x)).
\end{aligned}$$

Combining, and using (15.9.3), we obtain the following chain of equivalent

conditions:

$$\begin{aligned}\forall x, x' \in A:\ \big(\epsilon_A((x,x'))p\big)(x,x') \in H(A^q \times A^{\mathrm{op}}, \epsilon_A)\\ &\iff \forall x, x' \in A:\ (x'q^{-2})(qx) = x'(q^{-1}x)\\ &\iff \forall x, x' \in A:\ (x'q^{-2})(q^2x) = x'x\\ &\iff A = A^{q^2}\\ &\iff q^2 \in \mathrm{Nuc}(A).\end{aligned}$$

This solves the problem.

## Solutions for Section 44

**44.29** (a) $M_0$ is clearly a $k$-submodule of $M$ and (9.2.5) implies $\Phi(x_0 \otimes a) = ax_0$ for all $x_0 \in M_0$ and $a \in K$. In particular, (1) commutes. It remains to show that $\Phi$ is bijective. To this end, we note for any prime ideal $\mathfrak{p} \subseteq k$ that $k_\mathfrak{p}$ is a flat $k$-algebra (Bourbaki [7, II, §2, Thm. 1]), which implies $H(M_\mathfrak{p}, \tau_\mathfrak{p}) = H(M,\tau)_\mathfrak{p}$ by Exc. 39.40. Hence we may assume that $k$ is a local ring and apply Prop. 19.8 to pick $\theta \in K$ as in the hint. The $k$-linear map $M_0^2 \to M_0 \otimes K$, $(x_0, y_0) \mapsto x_0 \otimes 1_K + y_0 \otimes \theta$ is bijective and $\Phi(x_0 \otimes 1_K + y_0 \otimes \theta) = x_0 + \theta y_0$ for all $x_0, y_0 \in M_0$. Given $z \in M$, $x_0, y_0 \in M_0$, it therefore suffices to show

$$z = x_0 + \theta y_0 \iff \begin{cases} x_0 = (1 - 4n_K(\theta))^{-1}((1-2\theta)\bar\theta z + (1-2\bar\theta)\theta\tau(z)),\\ y_0 = (1 - 4n_K(\theta))^{-1}((1-2\bar\theta)z + (1-2\theta)\tau(z)).\end{cases} \tag{s1}$$

If $x_0, y_0$ have the form indicated in (s1), then it is straightforward to check that they remain fixed under $\tau$, hence belong to $M_0$, and $t_K(\theta) = 1$ implies

$$\begin{aligned}x_0 + \theta y_0 &= (1 - 4n_K(\theta))^{-1}\Big(((1-2\theta)\bar\theta + (1-2\bar\theta)\theta)z + ((1-2\bar\theta)\theta + (1-2\theta)\theta)\tau(z)\Big)\\ &= (1 - 4n_K(\theta))^{-1}\Big((1 - 4n_K(\theta))z - 2(\theta^2 - \theta + n_K(\theta)1_K)\tau(z)\Big) = z.\end{aligned}$$

Conversely, suppose $z \in M$ has $z = x_0 + \theta y_0$, $x_0, y_0 \in M_0$. Then $\tau(z) = x_0 + \bar\theta y_0 = (x_0 + y_0) - \theta y_0$, forcing

$$2x_0 + y_0 = z + \tau(z). \tag{s2}$$

Applying (s2) to $\bar\theta z = \bar\theta x_0 + n_K(\theta)y_0 = (x_0 + n_K(\theta)y_0) - \theta x_0$ in place of $z$, we conclude

$$x_0 + 2n_K(\theta)y_0 = 2(x_0 + n_K(\theta)y_0) - x_0 = \bar\theta z + \tau(\bar\theta z). \tag{s3}$$

Multiplying (s3) by 2 and subtracting the result from (s2), we obtain $(1 - 4n_K(\theta))y_0 = (1 - 2\bar\theta)z + \tau((1 - 2\bar\theta)z)$. Similarly, multiplying (s2) by $2n_K(\theta)$

and subtracting the result from (s3), we obtain$(1 - 4n_K(\theta))x_0 = (1 - 2\theta)\bar{\theta}z + \tau((1 - 2\theta)\bar{\theta}z)$, so $x_0, y_0$ have the form indicated in (s1). This shows that $\Phi$ is bijective.

(b) We begin with the hint. Since $K$ is faithfully flat as a $k$-module, Prop. 25.4 shows that the natural map $M_0 \to M_{0K}$ is injective, hence gives an isomorphism $M_0 \xrightarrow{\sim} M_0 \otimes 1_K$. In order to prove $M_0 \otimes 1_K = H(M_{0K}, \mathbf{1}_{M_0} \otimes \iota)$, we may again assume that $k$ is a local ring and pick $\theta$ as in (a). Again the map $M_0^2 \to M_0 \otimes K$, $(x_0, y_0) \mapsto x_0 \otimes 1_K + y_0 \otimes \theta$, is a $k$-isomorphism and $(\mathbf{1}_{M_0} \otimes \iota)(x_0 \otimes 1_K + y_0 \otimes \theta) = x_0 \otimes 1_K + y_0 \otimes \bar{\theta} = (x_0 + y_0) \otimes 1_K - y_0 \otimes \theta$ for all $x_0, y_0 \in M_0$. For $x_0 \otimes 1_K + y_0 \otimes \theta$ to remain fixed under $\mathbf{1}_{M_0} \otimes \iota$ it is therefore necessary and sufficient that $x_0 + y_0 = x_0$ and $y_0 = -y_0$, so the assertion follows. In (b), everything is clear except for the final statement. Changing scalars from $k$ to $R$ in (1), we obtaina commutative diagram

$$\begin{array}{ccc} M_{0R} \otimes_R K_R & \xrightarrow{\mathbf{1}_{M_{0R}} \otimes_R \iota_{K_R}} & M_{0R} \otimes_R K_R \\ {\scriptstyle \Phi_R}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \Phi_R} \\ M_R & \xrightarrow[\tau_R]{} & M_R \end{array}$$

of $R$-modules. Combined with the hint on the level of $R$ rather than $k$, this yields a chain of isomorphisms

$$M_{0R} \xrightarrow[-\otimes_R 1_{K_R}]{\cong} M_{0R} \otimes_R 1_{K_R} = H(M_{0R} \otimes_R K_R, \mathbf{1}_{M_{0R}} \otimes_R \iota_{K_R}) \xrightarrow[\Phi_R]{\cong} H(M_R, \tau_R) = M_{R0}$$

sending $x_0 \otimes r \in M_{0R}$ ($x_0 \in M_0$, $r \in R$) after natural identifications[8] to

$$\begin{aligned} \Phi_R((x_0 \otimes r) \otimes_R 1_{K_R}) &= \Phi_R((x_0 \otimes r) \otimes_R (1_K \otimes 1_R)) = \Phi_R((x_0 \otimes 1_K) \otimes r) \\ &= \Phi(x_0 \otimes 1_K) \otimes r = x_0 \otimes r \in M_{R0} \end{aligned}$$

and showing that $\Phi_R \circ (- - \otimes 1_{K_R})$ is indeed an isomorphism from $M_{0R}$ to $M_{R0}$.

**44.30** $\varrho\colon K \to {}^{\varrho}K$ is $K$-linear and, after identifying $B = B \otimes_K K$ canonically, $\mathrm{can} := \mathrm{can}_{\mathcal{B}} = \mathbf{1}_B \otimes_K \varrho$ is $\varrho$-semi-linear bijective. Thus ${}^{\varrho}\tau\colon {}^{\varrho}B \to {}^{\varrho}B$ exists as a ${}^{\varrho}\iota$-semi-linear map, where ${}^{\varrho}\iota = \iota_{\varrho K}$ is the conjugation of ${}^{\varrho}K$. Write ${}^{\varrho}\sharp$ for the adjoint of ${}^{\varrho}B$, which agrees with the ${}^{\varrho}K$-quadratic extensions of the adjoint of $B$. This implies ${}^{\varrho}\tau \circ {}^{\varrho}\sharp = {}^{\varrho}\sharp \circ {}^{\varrho}\tau$, and we deduce from 44.2 (b) that ${}^{\varrho}\tau\colon {}^{\varrho}B^{(+)} \to {}^{\varrho}B^{(+)}$ is a ${}^{\varrho}\iota$-semi-linear automorphism of cubic Jordan algebras. Thus ${}^{\varrho}\mathcal{B}$ is an involutorial $k$-system, and arguing as before, it follows that $(\varrho, \mathrm{can})\colon \mathcal{B} \xrightarrow{\sim} {}^{\varrho}\mathcal{B}$ is an isomorphism.

[8] Given $k$-modules $M, N$ and $R \in k$-**alg**, we identify $(M \otimes N)_R = M_R \otimes_R N_R$ via $(x \otimes y) \otimes r = (x \otimes r) \otimes_R (y \otimes 1_R) = (x \otimes 1_R) \otimes_R (y \otimes r)$ and $(x \otimes r_1) \otimes_R (y \otimes r_2) = (x \otimes y) \otimes (r_1 r_2)$ for $x \in M$, $y \in N$, $r, r_1, r_2 \in R$.

**44.31** (a) For the first part, it suffices to show that $\mathcal{B}(A,q)$ is an involutorial system, core splitness being obvious. Since $\varepsilon_A$ is a $K/k$-involution of $B$ *as a module* fixing $p$, it remains to show

$$\varepsilon_A((u_1,u_1')(u_2,u_2')) = \Big(\varepsilon_A((u_2,u_2'))p^{-1}\Big)\Big(p\varepsilon_A((u_1,u_1'))\Big) \tag{s1}$$

for all $u_i, u_i' \in B$, $i = 1,2$. Noting that the Jordan structures of $B$ and $B^{q\,\mathrm{op}}$ are the same by 44.1, we manipulate the right-hand side of (s1) to obtain

$$\begin{aligned}
\Big(\varepsilon_A((u_2,u_2'))p^{-1}\Big)\Big(p\varepsilon_A((u_1,u_1'))\Big) &= ((u_2',u_2)(q^{-1},q^{-1}))((q,q)(u_1',u_1)) \\
&= \Big((u_2'q^{-1},(q^{-1}q^{-1})(qu_2))\Big)\Big(qu_1',(u_1q^{-1})(qq))\Big) \\
&= (u_2'q^{-1},q^{-1}u_2)(qu_1',u_1q) \\
&= \Big((u_2'q^{-1})(qu_1'),((u_1q)q^{-1})(q(q^{-1}u_2))\Big) \\
&= (u_2'q^{-1})(qu_1'),u_1u_2) \\
&= \varepsilon_A\Big((u_1u_2,(u_2'q^{-1})(qu_1'))\Big) \\
&= \varepsilon_A((u_1,u_1')(u_2,u_2')),
\end{aligned}$$

as claimed. The second part of (a) follows by a straightforward computation.

(b) Since $(B,p)$ is a pointed cubic alternative algebra over $K$, its base change $({}^{\varrho}B_+, {}^{\varrho}p_+)$ is one over $k$, proving the first part of (b). As to the second, we have ${}^{\varrho}k_+ = {}^{\varrho'}k_+ = k$ as commutative rings, and since $\varrho' \circ \sigma = \varrho$ by definition, we conclude $a\alpha = \sigma(a)\alpha$ for all $a \in K$, $\alpha \in k$, i.e., $\mathbf{1}_k \colon {}^{\varrho}k_+ \to {}^{\varrho'}k_+$ is $\sigma$-semi-linear. In the sense of 12.26, therefore, $\varphi \otimes_\sigma \mathbf{1}_k \colon {}^{\varrho}B_+ \to {}^{\varrho'}B'_+$ exists as a $\sigma$-semi-linear map, which is obviously a unital homomorphism of alternative $k$-algebras and is easily checked to send ${}^{\varrho}p_+$ to ${}^{\varrho'}p'_+$ and to make the diagram

$$\begin{array}{ccc}
{}^{\varrho}B_+ & \xrightarrow[\varphi\otimes_\sigma \mathbf{1}_k]{} & {}^{\varrho'}B'_+ \\
{\scriptstyle {}^{\varrho}\sharp}\downarrow & & \downarrow{\scriptstyle {}^{\varrho'}\sharp} \\
{}^{\varrho}B_+ & \xrightarrow[\varphi\otimes_\sigma \mathbf{1}_k]{} & {}^{\varrho'}B'_+
\end{array}$$

of set maps commutative. Hence, by Exc. 34.22, it is a homomorphism of cubic alternative algebras.

(c) We must show that the composites

$$\mathrm{Pocu} \circ \mathrm{Cosp} \colon k\text{-}\mathbf{pocu} \to k\text{-}\mathbf{pocu} \quad \text{and} \quad \mathrm{Cosp} \circ \mathrm{Pocu} \colon k\text{-}\mathbf{cosp} \to k\text{-}\mathbf{cosp}$$

are (naturally) isomorphic to the respective identity functors. As to the first case, let $(A,q)$ be a pointed cubic alternative $k$-algebra. Then $\mathrm{Cosp}(A,q) = (\mathcal{B}(A,q),\varrho)$, where $\mathcal{B}(A,q) = (k \times k, B, \tau, p)$, $B = A \times A^{q\,\mathrm{op}}$, $\tau = \varepsilon_B$, $p =$

$(q,q)$ and $\varrho = \mathbf{1}_{k\times k}$. Writing $\pi_+\colon K \to k$ and $\Pi_+\colon B \to A$ for the respective projections onto the first factor, we obtain

$$\Pi_+((\alpha_+,\alpha_-)(u_+,u_-)) = \Pi_+((\alpha_+u_+,\alpha_-u_-)) = \alpha_+u_+ = \pi_+((\alpha_+,\alpha_-))\Pi_+(((u_+,u_-))$$

for $\alpha_\pm \in k$, $u_\pm \in A$. Moreover $\Pi_+$ commutes with the respective adjoints:

$$\begin{array}{ccc} B & \xrightarrow[\Pi_+]{} & A \\ {\scriptstyle \sharp_B=\sharp_A\times\sharp_A}\downarrow & & \downarrow{\scriptstyle \sharp_A} \\ B & \xrightarrow[\Pi_+]{} & A. \end{array}$$

By Exc. 34.22, therefore, $\Pi_+$ is a $\pi_+$-semi-linear homomorphism of cubic alternative algebras, and part (a) of the same exercise yields a unique homomorphism $\Pi_{A,q}\colon {}^{\varrho}B_+ = B \otimes_K {}^{\varrho}k_+ \to A$ of cubic alternative ${}^{\varrho}k_+$- algebras satisfying $\Pi_{A,q} \circ \mathrm{can}_{B,{}^{\varrho}k_+} = \Pi_+$, hence

$$\Pi_{A,q}((u_+,u_-)\otimes_K \alpha_+) = \alpha_+(\Pi_{A,q}\circ \mathrm{can}_{B,{}^{\varrho}k_+})((u_+,u_-)) = \alpha_+\Pi_+((u_+,u_-)) = \alpha_+u_+$$

for $u_\pm \in A$, $\alpha_+ \in {}^{\varrho}k_+$. On the other hand, we have a natural map $\varphi\colon A \to {}^{\varrho}B_+$ given by $u_+ \mapsto ((u_+,0)\otimes_K 1_{{}^{\varrho}k_+})$, and one checks that $\Pi_{A,q}$ and $\varphi$ are inverse to one another. In particular, $\Pi_{A,q}$ is a bijection sending ${}^{\varrho}p_+ = (q,q)\otimes_K 1_{{}^{\varrho}k_+}$ to $q$. Summing up, therefore, we have found an isomorphism

$$\Pi_{A,q}\colon\ \mathrm{Pocu}(\mathrm{Cosp}(A,q)) \xrightarrow{\sim} (A,q)$$

of pointed cubic alternative $k$-algebras such that

$$\Pi_{A,q}((u_+,u_-)\otimes_K \alpha_+) = \alpha_+u_+ \tag{s2}$$

for $u_\pm \in A$, $\alpha_+ \in {}^{\varrho}k_+$. Now let $\varphi\colon (A,q) \to (A',q')$ be a homomorphism of pointed cubic alternative $k$-algebras. Then we have $\mathrm{Cosp}(\varphi) = (\mathbf{1}_K, \varphi\times\varphi)$ and $\mathrm{Pocu}(\mathrm{Cosp}(\varphi)) = (\varphi\times\varphi)\otimes_{\mathbf{1}_K}\mathbf{1}_k = (\varphi\times\varphi)\otimes_K \mathbf{1}_k$. We therefore have to show that the diagram

$$\begin{array}{ccc} (\mathrm{Pocu}\circ\mathrm{Cosp})(A,q) & \xrightarrow[\Pi_{A,q}]{} & (A,q) \\ {\scriptstyle (\varphi\times\varphi)\otimes_K\mathbf{1}_k}\downarrow & & \downarrow{\scriptstyle \varphi} \\ (\mathrm{Pocu}\circ\mathrm{Cosp})(A',q') & \xrightarrow[\Pi_{A',q'}]{} & (A',q') \end{array}$$

commutes, which follows immediately from (s2).

Turning to the second case, let $(\mathcal{B},\varrho)$ with $\mathcal{B} = (K,B,\tau,p)$ be a core-split involutorial system over $k$. We first treat the special case $K = k\times k$ and $\varrho = \mathbf{1}_{k\times k}$. As before, let $\pi_\pm\colon K \to k$ be the two canonical projections making $k$ a $K$-algebra $k_\pm$. Then $B_\pm := B_{k_\pm}$ are cubic alternative $k$-algebras with norms $N_\pm =$

$N_B \otimes_K k_\pm$, giving rise to natural identifications $B = B_+ \times B_-$ as a cubic alternative $K$-algebra with norm $N = N_+ \times N_-$. Put $\varepsilon_+ := (1,0) \in K$, $\varepsilon_- := (0,1) = \bar{\varepsilon}_+ \in K$. Since $\tau$ is semi-linear with respect to the conjugation of $K$, there are $k$-linear maps $\sigma_\pm \colon B_\pm \to B_\mp$ such that $\tau((u_+,u_-)) = (\sigma_-(u_-), \sigma_+(u_+))$ for all $u_\pm \in B_\pm$, and since $\tau^2 = \mathbf{1}_B$, the map $\sigma_+$ is bijective with inverse $\sigma_-$. Thus

$$\tau((u_+,u_-)) = (\sigma_+^{-1}(u_-), \sigma_+(u_+)) \qquad (u_\pm \in B_\pm). \tag{s3}$$

By (44.2.1), the relation $N_B(\tau(u)) = \overline{N_B(u)}$ holds strictly for all $u \in B$, which by (s3) implies

$$N_- \circ \sigma_+ = N_+ \tag{s4}$$

as polynomial laws over $k$. Since $p = (p_+, p_-)$ remains fixed under $\tau$, we conclude

$$p_- = \sigma_+(p_+). \tag{s5}$$

$\tau$ being an $\iota$-semi-linear isotopy involution of $B$, hence a $k$-isomorphism $B \to B^{p\,\mathrm{op}}$, it may equally well be viewed as a $k$-isomorphism $B^{p\,\mathrm{op}} \to B$, which amounts to $\tau((vp^{-1})(pu)) = \tau(u)\tau(v)$ for all $u, v \in B$. Expanding with the aid of (s3), (s5), and applying (s4), we conclude that

$$\sigma_+ \colon B_+^{p_+\,\mathrm{op}} \xrightarrow{\sim} B_-$$

is an isomorphism of cubic alternative $k$-algebras. It follows that

$$\chi := \chi_{(\mathcal{B},\mathbf{1}_{k\times k})} := \mathbf{1}_{B_+} \times \sigma_+ \colon B_+ \times B_+^{p_+\,\mathrm{op}} \xrightarrow{\sim} B \tag{s6}$$

is an isomorphism of cubic alternative $K$-algebras. We now claim that

$$(\mathbf{1}_K, \chi) : \mathrm{Cosp}\,(\,\mathrm{Pocu}(\mathcal{B}, \mathbf{1}_{k\times k})) \xrightarrow{\sim} (\mathcal{B}, \mathbf{1}_{k\times k}) \tag{s7}$$

is an isomorphism in $k$-**cosp**. From (s5), (s6) we deduce $\chi((p_+,p_+)) = p$, so we only have to show that $\chi$ respects isotopy involutions: $\chi \circ \varepsilon_{B_+} = \tau \circ \chi$, which follows from (s3) and a straightforward computation. Next we show that any morphism in $k$-**cosp** having the form $(\mathbf{1}_{k\times k}, \varphi) \colon (\mathcal{B}, \mathbf{1}_{k\times k}) \to (\mathcal{B}', \mathbf{1}_{k\times k})$ gives rise to a commutative diagram

$$\begin{array}{ccc}
\mathrm{Cosp}\,(\,\mathrm{Pocu}(\mathcal{B}, \mathbf{1}_{k\times k})) & \xrightarrow[\mathrm{Cosp}(\mathrm{Pocu}(\mathbf{1}_{k\times k},\varphi))]{} & \mathrm{Cosp}\,(\,\mathrm{Pocu}(\mathcal{B}', \mathbf{1}_{k\times k})) \\
{\scriptstyle (\mathbf{1}_{k\times k}, \chi_{(\mathcal{B},\mathbf{1}_{k\times k})})}\downarrow \cong & & \cong \downarrow {\scriptstyle (\mathbf{1}_{k\times k}, \chi_{(\mathcal{B}',\mathbf{1}_{k\times k})})} \\
(\mathcal{B}, \mathbf{1}_{k\times k}) & \xrightarrow[(\mathbf{1}_{k\times k},\varphi)]{} & (\mathcal{B}', \mathbf{1}_{k\times k}).
\end{array} \tag{s8}$$

Indeed, (5) implies $\mathrm{Pocu}(\mathbf{1}_{k\times k}, \varphi) = \varphi \otimes_{k\times k} \mathbf{1}_k = \varphi_+$, hence $\mathrm{Cosp}(\mathrm{Pocu}(\mathbf{1}_{k\times k}, \varphi)) =$

$(\mathbf{1}_{k\times k}, \varphi_+ \times \varphi_+)$ by (3). Combining with (s3) and the relation $\tau' \circ \varphi = \varphi \circ \tau$, the assertion follows.

Finally, we turn to the general case. By Exc. 44.30, $(\varrho, \mathrm{can}_{\mathcal{B}})\colon (\mathcal{B}, \varrho) \to ({}^{\varrho}\mathcal{B}, \mathbf{1}_{k\times k})$ is an isomorphism of core-split involutorial systems over $k$. Write ${}^{\varrho}K$ for $k \times k$ viewed as a $K$-algebra via $\varrho$ and let $(\sigma, \varphi)\colon (\mathcal{B}, \varrho) \to (\mathcal{B}', \varrho')$ be a morphism in $k$-**cosp**. Then $\varphi$ and $\mathbf{1}_{k\times k}\colon {}^{\varrho}K \to {}^{\varrho'}K'$ are both $\sigma$-semi-linear. By 12.26, therefore, $\varphi \otimes_\sigma \mathbf{1}_{k\times k}$ exists as a $\sigma$-semi-linear map ${}^{\varrho}B \to {}^{\varrho'}B'$, and one checks that it is compatible with adjoints, hence a $\sigma$-semi-linear isomorphism of cubic alternative algebras (Exc. 34.22 (b)). Moreover,

$$(\mathbf{1}_{k\times k}, \varphi \otimes_\sigma \mathbf{1}_{k\times k})\colon ({}^{\varrho}\mathcal{B}, \mathbf{1}_{k\times k}) \longrightarrow ({}^{\varrho'}\mathcal{B}', \mathbf{1}_{k\times k})$$

is a homomorphism of core-split involutorial systems over $k$ which is easily seen to make the diagram

$$\begin{array}{ccc} (\mathcal{B}, \varrho) & \xrightarrow[(\sigma,\varphi)]{} & (\mathcal{B}', \varrho') \\ {\scriptstyle (\varrho,\mathrm{can}_{\mathcal{B}})}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle (\varrho',\mathrm{can}_{\mathcal{B}'})} \\ ({}^{\varrho}\mathcal{B}, \mathbf{1}_{k\times k}) & \xrightarrow[(\mathbf{1}_{k\times k}, \varphi\otimes_\sigma \mathbf{1}_{k\times k})]{} & ({}^{\varrho'}\mathcal{B}', \mathbf{1}_{k\times k}) \end{array} \tag{s9}$$

commutative. Combining (s8), (s9) and applying the functor $\mathrm{Cosp} \circ \mathrm{Pocu}$ to the latter, we obtain the commutative diagram

$$\begin{array}{ccc} \mathrm{Cosp}\,(\,\mathrm{Pocu}(\mathcal{B}, \varrho)) & \xrightarrow[\mathrm{Cosp}(\mathrm{Pocu}(\sigma,\varphi))]{} & \mathrm{Cosp}\,(\,\mathrm{Pocu}(\mathcal{B}', \varrho')) \\ {\scriptstyle \mathrm{Cosp}(\mathrm{Pocu}(\varrho,\mathrm{can}_{\mathcal{B}}))}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \mathrm{Cosp}(\mathrm{Pocu}(\varrho',\mathrm{can}_{\mathcal{B}'}))} \\ \mathrm{Cosp}\,(\,\mathrm{Pocu}({}^{\varrho}\mathcal{B}, \mathbf{1}_{k\times k})) & \xrightarrow[\mathrm{Cosp}(\mathrm{Pocu}(\mathbf{1}_{k\times k}, \varphi\otimes_\sigma \mathbf{1}_{k\times k}))]{} & \mathrm{Cosp}\,(\,\mathrm{Pocu}({}^{\varrho'}\mathcal{B}', \mathbf{1}_{k\times k}) \\ {\scriptstyle (\mathbf{1}_{k\times k}, \chi(\mathcal{B}, \mathbf{1}_{k\times k}))}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle (\mathbf{1}_{k\times k}, \chi(\mathcal{B}', \mathbf{1}_{k\times k}))} \\ ({}^{\varrho}\mathcal{B}, \mathbf{1}_{k\times k}) & \xrightarrow[(\mathbf{1}_{k\times k}, \varphi\otimes_\sigma \mathbf{1}_{k\times k})]{} & ({}^{\varrho'}\mathcal{B}', \mathbf{1}_{k\times k}) \\ {\scriptstyle (\varrho,\mathrm{can}_{\mathcal{B}})^{-1}}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle (\varrho',\mathrm{can}_{\mathcal{B}'})^{-1}} \\ (\mathcal{B}, \varrho) & \xrightarrow[(\sigma,\varphi)]{} & (\mathcal{B}', \varrho'), \end{array}$$

from which an isomorphism from $\mathrm{Cosp} \circ \mathrm{Pocu}$ to the identity functor of $k$-**cosp** can be immediately read off.

**44.32** (a) (44.15.6) implies $w \in J_0^{\perp}$, while (44.15.3) yields $Q(w) = u(p\tau(u))$. In conjunction with Prop. 44.13 we conclude

$$\begin{aligned} N_{J_0}(Q(w)) &= N_B(u(p\tau(u))) = N_B(p)N_B(u)\overline{N_B(u)} \\ &= \mu\bar{\mu}N_B(u)\overline{N_B(u)} = n_K(\mu N_B(u)). \end{aligned}$$

Moreover, $N_J(w) = t_K(\mu N_B(u))$ by (44.15.4). Hence (i) and (ii) are equivalent. (ii) combined with Prop. 19.8 shows that $k[\mu N_B(u)] \subseteq K$ is a quadratic étale subalgebra. Since $K$ has rank 2 as a finitely generated projective $k$-module, we have equality and (iii) holds. Finally, if (iii) holds, the preceding formulas imply the final assertion of (a), whence $w$ must be an étale element relative to $J_0$.

(b) Write $J'$ for the Jordan subalgebra of $J$ generated by $J_0$ and $j$. Then $J'$ is stable under the (bilinearized) adjoint, and we deduce from (44.16.2) that $J_0 j = J_0 \,.\, j = J_0 \times j$ is contained in $J'$. On the other hand, (44.15.3) implies that $(p^\sharp j)^\sharp = -N_J(p)p + N_J(p)\bar{\mu} j$ belongs to $J'$. Hence so does the second summand, and since $\bar{\mu}$ by (a) generates $K$ as a $k$-algebra, we conclude $Kj \subseteq J'$. Summing up, therefore, $Bj = (KJ_0)j \subseteq J'$, and we have shown $J' = J$, i.e., $J_0$ and $j$ generate $J$ as a Jordan $k$-algebra.

**44.33** (a) By (43.5.2) and (1), the quantity $p \,.\, w$ remains fixed under $\tau$. Hence $\mathcal{B} \,.\, w$ will be an involutorial system over $k$ once we have shown that $\tau$ is a $k$-homomorphism from $B^w$ to $(B^w)^{(p \,.\, w)\,\mathrm{op}}$. It is certainly one from $B$ to $B^{p\,\mathrm{op}}$. Using (15.9.3) both for $B$ and $B^w$ in place of $A$, it follows that $\tau$ is also a $k$-homomorphism from$B^w$ to

$$\begin{aligned}((B^p)^{\mathrm{op}})^{\tau(w)} &= ((B^p)^{\tau(w^{-1})})^{\mathrm{op}} = (B^{p\tau(w^{-1})})^{\mathrm{op}} = \Big(((B^w)^{w^{-1}})^{p\tau(w^{-1})}\Big)^{\mathrm{op}} \\ &= ((B^w)^{(w^{-1}w^{-1})(w[p\tau(w^{-1})])})^{\mathrm{op}} = ((B^w)^{w^{-1}(p\tau(w^{-1}))})^{\mathrm{op}} = (B^w)^{(p \,.\, w)\,\mathrm{op}},\end{aligned}$$

as desired. The assertion about $\mu$ being obvious, we proceed to show that $\Phi := \Phi_{\mathcal{B},w}$ is an isomorphism of cubic Jordan algebras. By Exc. 34.18 (a), it suffices to show that $\Phi$ preserves adjoints. Let $x_0 \in H(\mathcal{B})$, $u \in B$ and put $x := x_0 + uj \in J(\mathcal{B}, N_B(w)\mu)$. Then (44.15.3) implies

$$x^\sharp = \Big(x_0^\sharp - u(p\tau(u))\Big) + \Big(\overline{N_B(w)}\bar{\mu}\tau(u^\sharp)p^{-1} - x_0 u\Big)j,$$

hence

$$\Phi(x^\sharp) = \Big(x_0^\sharp - u(p\tau(u))\Big) + \Big(\overline{N_B(w)}\bar{\mu}[\tau(u^\sharp)p^{-1}]w - (x_0 u)w\Big)j. \tag{s1}$$

On the other hand, $\Phi(x) = x_0 + (uw)j \in J(\mathcal{B} \,.\, w, \mu)$, hence

$$\begin{aligned}\Phi(x)^\sharp = \Big(x_0^\sharp - [(uw)w^{-1}][w\{((p \,.\, w)w^{-1})(w\tau(uw))\}]\Big) \\ + \Big(\bar{\mu}[\tau((uw)^\sharp)w^{-1}][w(p \,.\, w)^{-1}] - (x_0 w^{-1})(wuw)\Big)j.\end{aligned} \tag{s2}$$

By the Moufang identities, the very last summands on the right of (s1) and (s2) are the same. It therefore suffices to show that the second (resp. third) summand on the right of (s1) agrees with the second (resp. third) summand on

the right of (s2). Indeed, making free use of the Moufang identities combined with (43.5.3), (1), the second summand on the right of (s2) is the negative of

$$u\Big((w(p\,.\,w))\tau(uw)\Big) = u\Big((p\tau(w^{-1}))\tau(uw)\Big) = u\Big(p\tau((uw)w^{-1})\Big) = u(p\tau(u)),$$

which is also the negative on the right of the second summand of (s1). Similarly, the equations

$$\begin{aligned}\bar\mu\Big(\tau((uw)^\sharp)w^{-1}\Big)(w(p\,.\,w)^{-1}) &= \bar\mu\Big(\tau((uw)^\sharp)w^{-1}\Big)\Big(w(\tau(w)p^{-1})w\Big)\\ &= \bar\mu\Big(\tau(w^\sharp u^\sharp)(\tau(w)p^{-1})\Big)w = \bar\mu\Big(\tau(w(w^\sharp u^\sharp))p^{-1}\Big)w\\ &= \overline{N_B(w)}\bar\mu(\tau(u^\sharp)p^{-1})w\end{aligned}$$

show that the third summands on the right of (s1) and (s2) are the same. Summing up we have proved that $\Phi$ is an isomorphism of cubic Jordan algebras.

(b) For the first part, we must show $(p\,.\,v)\,.\,w = p\,.\,(vw)$, where we have to keep in mind that the second dot on the left refers to the algebra $B^v$ rather than $B$. Hence (43.5.3) implies

$$\begin{aligned}(p\,.\,v)\,.\,w &= (w^{-1}v^{-1})\Big(v[((p\,.\,v)v^{-1})(v\tau(w^{-1}))]\Big)\\ &= (vw)^{-1}\Big((v(p\,.\,v))\tau(w^{-1})\Big) = (vw)^{-1}\Big((p\tau(v^{-1}))\tau(w^{-1})\Big)\\ &= (vw)^{-1}\Big(p\tau((vw)^{-1})\Big) = p\,.\,(vw).\end{aligned}$$

The assertion about $\mu$ (resp. $N_B(w)\mu$ or $N_B(vw)\mu$) being an admissible scalar for $\mathcal{B}\,.\,(vw)$ (resp. $\mathcal{B}\,.\,v$ or $\mathcal{B}$) being obvious, we show that the diagram (3) is commutative. For $u \in B$ we compute

$$\begin{aligned}\Phi_{\mathcal{B}\,.\,v,w}\circ\Phi_{\mathcal{B},v}(uj) = \Phi_{\mathcal{B}\,.\,v,w}((uv)j) &= \Big(((uv)v^{-1})(vw)\Big)j\\ &= (u(vw))j = \Phi_{\mathcal{B},vw}(uj),\end{aligned}$$

and the assertion follows.

(c) For any $w \in B^\times$, we conclude from (a), (b) that $\mu' := N_B(w)^{-1}\mu$ is an admissible scalar for $\mathcal{B}\,.\,w$ and

$$\Phi_{\mathcal{B}\,.\,w,w^{-1}}\colon J(\mathcal{B}\,.\,w,\mu') \xrightarrow{\sim} J(\mathcal{B},\mu)$$

is an isomorphism. In the special case $w := \mu p^{-1}$ we conclude $\mu' = \mu^{-3}\mu\bar\mu\mu = \bar\mu\mu^{-1}$, hence $N_{B^w}(p\,.\,w) = n_K(\mu') = 1$.

**44.34** For sake of contradiction, suppose such a $z$ exists and write it as $z = x + iy$, $x, y \in \mathbb{Z}$. Cross-multiplying the equation $i = \bar z z^{-1}$, we obtain

$$x - iy = \bar z = iz = -y + ix.$$

Thus $y = -x$ and $z = x(1-i)$. Hence $x \neq 0$ and taking norms, we obtain $n_C(z) = 2|x| > 1$ so $z$ is not invertible in $C$ (Prop. 17.5), a contradiction.

**44.35** Since $K$ is split, it contains a complete orthogonal system $(\varepsilon_+, \varepsilon_-)$ of elementary idempotents. Hence $K = k_+ \times k_-$, $k \cong k_\pm := k\varepsilon_\pm \in K$-**alg**, which implies $A = A_+ \times A_-$, $A_\pm = A_{k_\pm}$; in particular, $A_\pm$ are Azumaya algebras of degree $n$ over $k$. Since $\tau$ is unitary, there are $k$-linear maps $\tau_\pm\colon A_\pm \to A_\mp$ such that $\tau((x_+, x_-)) = (\tau_-(x_-), \tau_+(x_+))$ for all $x_\pm \in A_\pm$, and since $\tau$ has order 2, the map $\tau_+$ must be bijective with inverse $\tau_-$: $\tau((x_+, x_-)) = (\tau_+^{-1}(x_-), \tau_+(x_+))$. Finally, since $\tau$ is an anti-isomorphism, so is $\tau_+$, i.e., $\tau_+\colon A_+^{\mathrm{op}} \to A_-$ is an isomorphism. Now one checks that

$$\varphi\colon (A_+ \times A_+^{\mathrm{op}}, \varepsilon_{A_+}) \xrightarrow{\sim} (A, \tau), \quad (x_+, y_+) \longmapsto (x_+, \tau_+(y_+))$$

is an isomorphism of algebras with involution. This proves the first part with $B = A_{k_+}$.

If $K$ is arbitrary, then $K_K \cong K \times K$ by Exc. 19.36, and (12.27.1) yields $A_K = ({}_kA)_K = A_{K_k} \cong A_{K\times K} = A \times A$ as $K \times K$-algebras. Now the first part proves the second.

**44.36** Put $J_0 := H(\mathcal{B})$ and write $T_0$ (resp. $T$) for the bilinear trace of $J_0$ (resp. $B$). By (44.15.6), we obtain

$$T_J(x, y) = T_0(x_0, y_0) + 2T\Big((p\tau(u))v\Big) \tag{s1}$$

for $x = x_0 + uj$, $y = y_0 + vj$, $x_0, y_0 \in J_0$, $u, v \in B$. In standard notation we have $J^* = J_0^* \oplus B^* j$, and writing $T_J^*\colon J \to J^*$ for the linear map induced by the symmetric bilinear form $T_J$ (ditto for $T_0^*$, $T^*$), equation (s1) implies

$$T_J^* = T_0^* \oplus (2\varphi)j, \quad \varphi := T^* \circ L_p \circ \tau\colon B \longrightarrow B^*. \tag{s2}$$

Assume first that $B$ is regular and $2 \in k^\times$. Then $B = J_0 \oplus B_-$, $B_- = \{u \in B \mid \tau(u) = -u\}$, and since $B$ is finitely generated projective as a $k$-module, so are $J_0, B_-$ and $J$. Moreover, $B^* = J_0^* \oplus B_-^*$, and $T(J_0, B_-) = \{0\}$ implies $T^* = T_0^* \oplus T_-^*$, $T_-$ being the restriction of $T$ to $B_- \times B_-$. From this we deduce that $T_0^*$ is bijective and hence, by (s2), so is $T_J^*$. Thus $J$ is regular. Conversely, assume that $J$ is regular. Then $J_0$ and $B$ are finitely generated projective as $k$-modules and we conclude from (s2) that multiplication by 2 is a bijection $B \to B$; in particular, some $u \in B$ has $2u = 1_B$. But $1_B \in B$ is unimodular, so there exists a $k$-linear form $\lambda\colon B \to k$ satisfying $\lambda(1_B) = 1$. Thus $2\lambda(u) = 1$ makes 2 invertible in $k$, as claimed.

**44.37** By Exc. 44.33 (c), up to isomorphism of $J$, we may assume $N_B(p) = 1_K$, $n_K(\mu) = 1$. Passing to the $p$-isotope of $J$ and invoking Thm. 44.26, we may

indeed assume $p = 1_B$ up to isotopy of $J$. Now assume that the norm of $B$ is surjective as a set map from $B$ to $K$. Then Exc. 44.33 (a) shows that, up to isomorphism of $J$, we may assume $\mu = 1_K$, which in particular implies $N_B(p) = 1_K$. Arguing as before, we may therefore assume $p = 1_B$, $\mu = 1_K$ up to isotopy of $J$.

**44.38** (a) It suffices to verify that $\tau_B$ is an involution of $C$. Localizing if necessary we may assume $C = \mathrm{Cay}(B,\mu) = B \oplus Bj_0$ for some $\mu \in k^\times$. Then $\varphi := \tau \circ \iota_C \colon C \to C$ satisfies $\varphi(v + wj_0) = \tau(\bar{v} - wj_0) = v - wj_0$ for $v, w \in B$, hence is an isomorphism (Exc. 18.19), forcing $\tau = \varphi \circ \iota_C$ to be an involution.

(b) is clear.

(c) Arbitrary elements of $J$ have the form

$$x = x_0 + uj, \quad x_0 = (\alpha_0, \beta_0 1_C + w_0), \quad u = (\alpha, v + w) \tag{s1}$$

with $\alpha_0, \beta_0, \alpha \in k$, $v \in B$, $w_0, w \in B^\perp$. Writing $T_0, S_0, N_0$ (resp. $T, S, N$) for the trace, quadratic trace, norm of $J_0$ (resp, $J$), we begin by using Prop. 37.2 to determine the Peirce components of $J$ relative to $e_1$:

$$J_2(e_1) = ke_1, \tag{s2}$$

$$J_1(e_1) = (\{0\} \times C)j, \tag{s3}$$

$$J_0(e_1) = (\{0\} \times H(C,\tau_B)) \oplus (ke_1)j. \tag{s4}$$

here (s2) is clear, while for the rest (44.15.7), (44.15.5) and Exc. 34.24 imply

$$T(x) = \alpha_0 + 2\beta_0, \tag{s5}$$

$$e_1 \times x = (0, \beta_0 1_C - w_0) - (\alpha, 0)j, \tag{s6}$$

which immediately yields (s3) but also (s4) since $e_0 := 1_J - e_1 = (0, 1_C)$ and

$$\begin{aligned} T(x)e_0 - x &= (\alpha_0 + 2\beta_0)(0, 1_C) - (\alpha_0, \beta_0 1_C + w_0) - (\alpha, v + w)j \\ &= (-\alpha_0, (\alpha_0 + \beta_0)1_C - w_0) - (\alpha, v + w)j. \end{aligned}$$

Now assume $x \in (J_0)_0(e_1)$, i.e., $\alpha_0 = \alpha = 0$, $v = w = 0$. Then (44.15.3) yields

$$x^\sharp = (\beta_0^2 + n_C(w_0))e_1. \tag{s7}$$

Hence an elementary frame of the desired kind exists if and only if some $e_2 = (0, \beta_0 1_C + w_0)$, $\beta_0 \in k$, $w_0 \in B^\perp$ has $2\beta_0 = T(e_2) = 1$ and $e_2^\sharp = 0$, i.e., $\beta_0 = \frac{1}{2}$ and $n_C(w_0) = -\frac{1}{4}$ by (s7). Combining Prop. 18.7 with regularity, we find an identification of $C$ as in (4) matching $j_0$ with $2w_0$. Thus $e_2$ satisfies the first equation of (5), forcing $e_3 := 1_J - e_1 - e_2$ to do the same with the second. Conversely, if (4) and (5) hold, then $\Omega$ is an elementary frame of the desired kind.

For the rest of the solution, we assume this to be the case. We proceed to determine the Peirce-one-spaces of

$$e_\pm := (0, \frac{1}{2}(1_C \pm j_0)), \text{ i.e., of } e_+ = e_2, e_- = e_3. \tag{s8}$$

Adjusting the notation of (s1) to the identification (4) by writing

$$x = x_0 + uj, \quad x_0 = (\alpha_0, \beta_0 1_C + w_0 j_0), \quad u = (\alpha, v + w j_0) \tag{s9}$$

for $\alpha_0, \beta_0, \alpha \in k$, $w_0, v, w \in B$, we obtain

$$\begin{aligned} e_\pm \times x &= (0, \frac{1}{2}(1_C \pm j_0)) \times (\alpha_0, \beta_0 1_C + w_0 j_0) + (0, \frac{1}{2}(1_C \pm j_0)) \times ((\alpha, v + w j_0) j) \\ &= (\frac{1}{2} n_C(1_C \pm j_0, \beta_0 1_C + w_0 j_0), \alpha_0 \frac{1}{2}(1_C \mp j_0)) - \Big((0, \frac{1}{2}(1_C \pm j_0))(\alpha, v + w j_0)\Big) j \\ &= (\beta_0 \mp \frac{1}{2} t_B(w_0), \frac{\alpha_0}{2} 1_C \mp \frac{\alpha_0}{2} j_0) - (0, \frac{1}{2}(v \pm \bar{w}) + \frac{1}{2}(w \pm \bar{v}) j_0) j. \end{aligned}$$

For $x$ as in (s9) to belong to $J_1(e_\pm)$ it is necessary and sufficient that $T(x) = 0$ and $e_\pm \times x = 0$. Hence

$$J_1(e_2) = \{(0, w_0 j_0) + (\alpha, v - \bar{v} j_0) j \mid \alpha \in k\ w_0 \in B^0,\ v \in B\}, \tag{s10}$$

$$J_1(e_3) = \{(0, w_0 j_0) + (\alpha, v + \bar{v} j_0) j \mid \alpha \in k,\ w_0 \in B^0,\ v \in B\}. \tag{s11}$$

Combining with (s3), the off-diagonal Peirce components of $J$ relative to $\Omega$ attain the form

$$J_{12} = \{(0, v - \bar{v} j_0) j \mid v \in B\}, \tag{s12}$$

$$J_{23} = \{(0, w_0 j_0) + (\alpha, 0) j \mid w_0 \in B^0,\ \alpha \in k\}, \tag{s13}$$

$$J_{31} = \{(0, v + \bar{v} j_0) j \mid v \in B\}. \tag{s14}$$

Now put

$$u_{23} = (1, 0) j \in J_{23}, \quad u_{31} = (0, \frac{1}{2}(1_B + j_0)) j \in J_{31}. \tag{s15}$$

Using (44.15.8) one checks $S(u_{23}) = S(u_{31}) = -1$, so $\mathfrak{S} := (\Omega, u_{23}, u_{31})$ is a strong co-ordinate system of $J$ in the sense of 39.21.

Next we consider the multiplicative conic alternative algebra $B' := C_{J,\mathfrak{S}}$ of 37.15 living uon the $k$-module $J_{12}$ under the multiplication (37.15.3) with $\omega = 1$. In order to describe this multiplication explicitly, we let $v, w \in B$, put $x := (0, v - \bar{v} j_0) j$, $y := (0, w - \bar{w} j_0) j$, write $x \bullet y$ for their product in $B'$ and

obtain

$$\begin{aligned}
x \times u_{23} &= (0, v - \bar{v}j_0)j \times (1,0)j = \hat{\tau}_B((0, v - \bar{v}j_0) \times (1,0))j \\
&= \hat{\tau}_B((0, \bar{v} + \bar{v}j_0))j = (0, v + \bar{v}j_0)j, \\
u_{31} \times y &= (0, \frac{1}{2}(1_B + j_0))j \times (0, w - \bar{w}j_0)j \\
&= -\frac{1}{2}((0, 1_B + j_0)(0, \bar{w} - \bar{w}j_0) + (0, w - \bar{w}j_0)(0, 1_B + j_0)) \\
&\quad + \hat{\tau}_B\Big((0, \frac{1}{2}(1_B + j_0)) \times (0, w - \bar{w}j_0)\Big)j \\
&= -\frac{1}{2}(0, \bar{w} - \bar{w}j_0 + wj_0 - w + w + wj_0 - \bar{w}j_0 - \bar{w}) \\
&\quad + \hat{\tau}_B\Big((\frac{1}{2}n_C(1_B + j_0, w - \bar{w}j_0), 0)\Big)j \\
&= (0, (\bar{w} - w)j_0) + (t_B(w), 0)j,
\end{aligned}$$

hence

$$\begin{aligned}
x \bullet y &= (x \times u_{23}) \times (u_{31} \times y) \\
&= (0, v + \bar{v}j_0)j \times (0, (\bar{w} - w)j_0) + (0, v + \bar{v}j_0)j \times (t_B(w), 0)j \\
&= \Big((0, (w - \bar{w})j_0)(0, v + \bar{v}j_0)\Big)j - (0, v + \bar{v}j_0)(t_B(w), 0) \\
&\quad - (t_B(w), 0)(0, \bar{v} + \bar{v}j_0) + \hat{\tau}_B\Big((0, v + \bar{v}j_0) \times (t_B(w), 0)\Big)j \\
&= \Big(0, ((w - \bar{w})\bar{v})j_0 + v(w - \bar{w})\Big)j + \hat{\tau}_B\Big((0, t_B(w)(\bar{v} - \bar{v}j_0)\Big)j \\
&= \Big(0, v(w - \bar{w}) + ((w - \bar{w})\bar{v})j_0 + v(w + \bar{w}) - ((w + \bar{w})\bar{v})j_0\Big)j \\
&= (0, 2vw - (2\overline{vw})j_0)j.
\end{aligned}$$

Thus the assignment $v \mapsto \frac{1}{2}(v - \bar{v}j_0)j$ yields an isomorphism $B \xrightarrow{\sim} B'$ of composition algebras, and the Jacobson co-ordinatization theorem 37.17 yields (6). For the final assertion, we put $\Gamma = \operatorname{diag}(\gamma_1, \gamma_2, \gamma_3)$ and, by Exc. 37.22, may assume $\det(\Gamma) = 1$. Then

$$p := \sum \gamma_i e_{ii} \in \operatorname{Her}_3(B) \text{ and } q := \sum \gamma_i^{-1} e_i \in J_0$$

have norm 1, and the isomorphism (6) matches $p^{-1}$ with $q$. By Exc.e 37.23, the assignment

$$\sum(\xi_i e_{ii} + u_i[jl]) \longmapsto \sum(\gamma_i \xi_i e_{ii} + \gamma_j \gamma_l u_i[jl])$$

defines an isomorphism $\varphi\colon \operatorname{Her}_3(B, \Gamma)^{(p)} \to \operatorname{Her}_3(B)$, and since $\varphi(p^{-2}) = p^{-1}$, Thm. 44.26 implies

$$\operatorname{Her}_3(B, \Gamma) \cong \operatorname{Her}_3(B)^{(p^{-1})} \cong J^{(q)} \cong J({}^q\mathcal{B}, 1),$$

as claimed.

**44.39** (a) We have $J_0 = k \times k1_C$, so the elements of $J$ have the form

$$x = (\alpha_0, \beta_0 1_C) + (\alpha, v)j \qquad (\alpha_0, \beta_0, \alpha \in k,\ v \in C), \tag{s1}$$

and, writing $T$ for the linear trace of $J$, we conclude

$$T(x) = \alpha_0 + 2\beta_0. \tag{s2}$$

While $e_1$ is clearly an elementary idempotent, $e_2$ has trace 1 and satisfies

$$\begin{aligned} e_2^\sharp &= \frac{1}{4}((0, 1_C) + (1, 0)j)^\sharp \\ &= \frac{1}{4}((1,0) - (1,0)(1,0)) + \frac{1}{4}\big(\hat{\imath}_C((1,0)^\sharp) - (0,1_C)(1,0)\big) = 0, \end{aligned}$$

hence is an elementary idempotent as well. Furthermore,

$$\begin{aligned} e_1 \times e_2 &= \frac{1}{2}(1,0) \times (0,1_C) + \frac{1}{2}(1,0) \times (1,0)j = \frac{1}{2}(0,1_C) - \frac{1}{2}(1,0)j \\ &= \frac{1}{2}(e_0 - e_1 j) = e_3. \end{aligned}$$

By Prop. 37.4, therefore, $\Omega$ is an elementary frame of $J$. Now assume $x \in J_1(e_3)$. Then $T(x) = 0$, i.e., $\alpha_0 + 2\beta_0 = 0$ by (s2), and $e_3 \times x = 0$. But, quite generally,

$$\begin{aligned} e_3 \times x &= \frac{1}{2}((0,1_C) - (1,0)j) \times ((\alpha_0, \beta_0 1_C) + (\alpha, v)j) \\ &= \frac{1}{2}((2\beta_0, \alpha_0 1_C) - (0,v)j + (\alpha_0, 0)j + (\alpha, 0) + (\alpha, 0) - (0,v)j) \\ &= (\beta_0 + \alpha, \frac{1}{2}\alpha_0 1_C) + (\frac{1}{2}\alpha_0, -v)j. \end{aligned}$$

This proves $J_1(e_3) = \{0\}$. Moreover, $x \in J_0(e_3)$ means $e_3 \times x = T(x)(1_J - e_3) - x$, i.e.,

$$\begin{aligned} (\beta_0 + \alpha, \frac{1}{2}\alpha_0 1_C) + (\frac{1}{2}\alpha_0, -v)j &= (\alpha_0 + 2\beta_0)((1, \frac{1}{2}1_C) + (\frac{1}{2}, 0)j) - (\alpha_0, \beta_0 1_C) - (\alpha, v)j \\ &= (2\beta_0, \frac{1}{2}\alpha_0 1_C) + (\frac{1}{2}\alpha_0 + \beta_0 - \alpha, -v)j, \end{aligned}$$

and we conclude

$$J_0(e_3) = \{(\alpha_0, \alpha 1_C) + (\alpha, v)j \mid \alpha_0, \alpha \in k, v \in C\},$$

i.e.,

$$J_0(e_3) = M_0 := ke_1 + ke_2 + (\{0\} \times C)j. \tag{s3}$$

By Faulkner's lemma 37.3, it remains to determine $q_0 := S|_{M_0}$. For $\alpha_1, \alpha_2 \in k$, $v \in C$ we compute

$$\begin{aligned} q_0(\alpha_1 e_1 + \alpha_2 e_2 + (0,v)j) &= S((\alpha_1, \frac{1}{2}\alpha_2 1_C) + (\frac{1}{2}\alpha_2, v)j) \\ &= T((\frac{1}{4}\alpha_2^2, \frac{1}{2}\alpha_1\alpha_2 1_C)) - T((\frac{1}{2}\alpha_2, v)(\frac{1}{2}\alpha_2, \bar{v})) \\ &= \frac{1}{4}\alpha_2^2 + \alpha_1\alpha_2 - \frac{1}{4}\alpha_2^2 - 2n_C(v) = \alpha_1\alpha_2 - 2n_C(v), \end{aligned}$$

and the final assertion follows.

(b) Since $2 = 0$ in $k$, we have

$$H(\hat{\mathcal{C}}) = k \times C^0, \quad C^0 = \mathrm{Ker}(t_C). \tag{s4}$$

Note that $C$ is regular since $r > 1$, so by Lemma 19.15, some $w \in C$ has $t_C(w) = 1$. Thus $C = kw \oplus C^0$, and $C^0$ is finitely generated projective of rank $r-1$, proving the rank formula for $J$. Moreover, the second Tits construction using $\hat{\mathcal{C}}$ is stable not just under flat but actually under arbitrary base change.

(i) Arbitrary elements of $J$ have the form

$$x = x_0 + uj, \quad x_0 = (\alpha_0, v_0), \quad u = (\alpha, v) \quad (\alpha_0, \alpha \in k,\ v_0 \in C^0,\ v \in C). \tag{s5}$$

Hence

$$T(x) = \alpha_0 \tag{s6}$$

and

$$\begin{aligned} x^\sharp &= \Big((\alpha_0, v_0)^\sharp - (\alpha, v)\hat{\imath}_C((\alpha, v))\Big) + \Big(\hat{\imath}_C((\alpha, v)^\sharp) - (\alpha_0, v_0)(\alpha, v)\Big)j \\ &= \Big((n_C(v_0), \alpha_0 v_0) - (\alpha^2, n_C(v)1_C)\Big) + \Big((n_C(v), \alpha v) - (\alpha_0\alpha, v_0 v)\Big)j \\ &= (n_C(v_0) - \alpha^2, \alpha_0 v_0 - n_C(v)1_C) + (n_C(v) - \alpha_0\alpha, \alpha v - v_0 v)j. \end{aligned} \tag{s7}$$

Thus $x$ is an elementary idempotent if and only if $\alpha_0 = 1$, $v_0 = n_C(v)1_C$, $\alpha = n_C(v)$, and we have shown that the elementary idempotents of $J$ are precisely of the form $e_v$, $v \in C$. Since the assignment $v \mapsto e_v$ is compatible with base change, it yields an isomorphism from $C_{\mathbf{a}}$ to $\mathbf{Elid}(J)$. Conversely, the projection onto the last factor produces a morphism from $\mathbf{Elid}(J)$ to $C_{\mathbf{a}}$, and by what we have just seen, the two morphisms are inverse to one another.

(ii) For $v, w \in C$, we obtain

$$\begin{aligned} T(e_v, e_w) &= T_0\Big((1, n_C(v)1_C), (1, n_C(w)1_C)\Big) + T\Big((n_C(v), v)(n_C(w), \bar{w})\Big) \\ &\quad + T\Big((n_C(w), w)(n_C(v), \bar{v})\Big) \\ &= 1 + n_C(vw) - t_C(v\bar{w}) - n_C(vw) - t_C(w\bar{v}) = 1, \end{aligned}$$

whence $e_v, e_w$ can never be orthogonal.

(iii) Since $2 = 0$ in $k$ and $k$ is reduced, Exc. 34.23 yields

$$\mathrm{Nil}(J) = \{x \in J \mid T(x, J) = T(x^\sharp, J) = \{0\}\}. \tag{s8}$$

For $\beta_0, \beta \in k$, $w_0 \in C^0$, $w \in C$, we obtain

$$\begin{aligned} T(x, (\beta_0, w_0)) &= \alpha_0\beta_0 + t_C(v_0, w_0), \\ T(x, (\beta, w)) &= T((\alpha, v)(\beta, \bar{w})) + T((\beta, w)(\alpha, \bar{v})) = 0, \end{aligned}$$

so $T(x, J) = \{0\}$ is equivalent to $\alpha_0 = 0$ and $v_0 \in k1_C$. By (s7), (s8), therefore, $x \in \mathrm{Nil}(J)$ if and only if $\alpha_0 = 0$, $v_0 = \gamma 1_C$ for some $\gamma \in k$ and $\gamma^2 = n_C(v_0) = \alpha^2$. But since $2 = 0$ in $k$ and $k$ is reduced, this implies $\gamma = \alpha$, and (iii) is proved.

**44.40** (a) By (16.17.2) we have $t_C(\tau(x)) = \iota_K(t_C(x))$ for all $x \in C$, which implies that the $k$-linear maps $\iota_C$ and $\tau$ commute. Thus $\tau_0 := \tau \circ \iota_C : C \to C$ is an $\iota_K$-semi-linear automorphism of order 2. By Exc. 44.29, therefore,

$$C_0 := H(C, \tau_0) = \{x \in C \mid \tau(x) = \bar{x}\} \subseteq C$$

is a unital $k$-subalgebra, and the inclusion $C_0 \hookrightarrow C$ induces a $K$-linear bijection $\Phi : C_0 \otimes K \to C$ making the diagram

$$\begin{array}{ccc} C_0 \otimes K & \xrightarrow[\mathbf{1}_{C_0} \otimes \iota_K]{} & C_0 \otimes K \\ \Phi \downarrow \cong & & \cong \downarrow \Phi \\ C & \xrightarrow[\tau_0]{} & C \end{array}$$

commutative. Now one checks that $\Phi : (C_0 \otimes K, \iota_{C_0} \otimes \iota_K) \to (C, \tau)$ is an isomorphism of $k$-algebras with involution.

(b) One checks that $\mathcal{B}$ is a unitary involutorial system over $k$. Setting $J := J(\mathcal{B}, \mu)$, Cor. 44.20 and Exc. 42.27 (a) imply that $J_K \cong J(\hat{C}, \mu) \cong \mathrm{Her}_3(C, \Gamma_0)$, $\Gamma_0 := \mathrm{diag}(-1, -1, 1)$, is a Freudenthal algebra of rank $3(r+1)$ over $K$. Since $K$, being quadratic étale, is faithfully flat over $k$, the assertion now follows from Cor. 39.32.

**44.41** Since $\tau : B \to B^{p\,\mathrm{op}}$ is an $\iota_K$-semi-linear isomorphism of cubic alternative $K$-algebras, it is also one from $B^{\mathrm{op}}$ to $B^p = (B^{\mathrm{op}})^{\mathrm{op}p} = (B^{\mathrm{op}})^{p^{-1}\mathrm{op}}$. Hence $\mathcal{B}^{\mathrm{op}}$ is an involutorial system over $k$. Let $\mu \in K$ be an admissible scalar for $\mathcal{B}$. The $\mu^{-1}$ is clearly one for $\mathcal{B}^{\mathrm{op}}$, and we only have to show that $\Phi$ is an isomorphism. As usual, it suffices to show that $\Phi$ preserves adjoints, so let $x_0 \in H(\mathcal{B})$ and $u \in B$. Writing $u \,.\, v$ for the product in $B^{\mathrm{op}}$, we apply Lemma 43.5 and

obtain

$$\begin{aligned}\Phi((x_0+uj)^\sharp) &= \Phi\Big([x_0^\sharp - u(p\tau(u))] + [\bar\mu\tau(u^\sharp)p^{-1} - x_0u]j\Big)\\ &= [x_0^\sharp - u(p\tau(u))] + \tau\Big([\bar\mu\tau(u^\sharp)p^{-1} - x_0u]p\Big)j\\ &= \Big(x_0^\sharp - \tau(up)\,.\,(p^{-1}\,.\,(up))\Big) + \Big(\mu u^\sharp - (p\tau(u))x_0\Big)j.\end{aligned}$$

But $\mu u^\sharp = \bar\mu^{-1}N_B(p)u^\sharp = \bar\mu^{-1}p(up)^\sharp = \bar\mu^{-1}\tau(\tau(up)^\sharp)\,.\,(p^{-1})^{-1}$ and $(p\tau(u))x_0 = x_0\,.\,\tau(up)$. Hence

$$\begin{aligned}\Phi((x_0+uj)^\sharp) &= \Big(x_0^\sharp - \tau(up)\,.\,(p^{-1}\,.\,(up))\Big) + \Big(\bar\mu^{-1}\tau(\tau(up)^\sharp)\,.\,(p^{-1})^{-1}\\ &\qquad - x_0\,.\,\tau(up)\Big)j\\ &= (x_0+\tau(up)j)^\sharp = \Phi(x_0+uj)^\sharp,\end{aligned}$$

as claimed.

## Solutions for Section 45

**45.15** (a), (b) The assertion of (a) is clear if $E$ is a field. Next assume $E = F\times K$, where $K/F$ is a separable quadratic field extension. Letting $u$ be a generator of $K/F$ and setting $a := (1,u) \in E$, one checks that $1_E = (1,1_K), a, a^2$ are linearly independent over $F$. Hence $a$ generates $E$ as a unital $F$-algebra. Finally let us assume that $E = F\times F\times F$ is split. If $F$ contains more than two elements, some quantity $\alpha \in F^\times$ is different from 1. Since the components of the vector $a := (\alpha,1,0) \in E$ are mutually distinct, a Vandermonde argument shows that $a$ generates $E$ as a unital $F$-algebra. This completes the proof of (a). On the other hand, if $F = \mathbb{F}_2$ is the field with two elements, then the elements of $E$ have the form $a = (\alpha,\beta,\gamma)$ where at least two of the quantities $\alpha,\beta,\gamma \in F$ are the same. Hence $a$ does not generate $E$ as a unital $F$-algebra. This completes the proof of (b).

(c) Obvious.

(d)(i) Suppose first that $a \in J$ is étale relative to $J_0$. Then (c) implies $T_J(a) = 0$, while we deduce from Exc. 44.32 (b) that $a$ generates $E$ as a unital $F$-algebra. Finally $a^\sharp = \frac{1}{3}S_J(a)\cdot 1_E + (a^\sharp - \frac{1}{3}S_J(a)\cdot 1_E)$, where the second summand belongs to $J_0^\perp$. In the terminology of 44.8 , therefore, $Q(a) = -\frac{1}{3}S_J(a)$, which must be different from zero by the definition of an étale element.

Conversely, suppose $a \in J_0^\perp$ generates $E$ as a unital $F$-algebra and has $S_J(a) \neq 0$. We claim that the discriminant

$$D := -4S_J(a)^3 - 27N_J(a)^2 \in F^\times. \tag{s1}$$

This is well known, see for example [4, §3.1]. Here is a sketch of a proof.

There is clearly no harm in assuming that $F$ is algebraically closed. Then $E = F \times F \times F$ is split and for some $\alpha_1, \alpha_2, \alpha_3 \in F$ we have $a = (\alpha_1, \alpha_2, \alpha_3)$ as well as $\sum \alpha_i = 0$. Short computations give

$$S_J(a) = -(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2), \quad N_J(a) = -(\alpha_1^2\alpha_2 + \alpha_1\alpha_2^2)$$

and then

$$D = 4\alpha_1^6 + 12\alpha_1^5\alpha_2 - 3\alpha_1^4\alpha_2^2 - 26\alpha_1^3\alpha_2^3 - 3\alpha_1^2\alpha_2^4 + 12\alpha_1\alpha_2^5 + 4\alpha_2^6. \tag{s2}$$

On the other hand, let $\varrho\colon E \to E$ be the *shift operator* sending $(\alpha_1, \alpha_2, \alpha_3)$ to $(\alpha_3, \alpha_1, \alpha_2)$. Then $\varrho \in \mathrm{Aut}(E)$ has order 3 and fixed algebra $F \cdot 1_E$. We have

$$a - \varrho(a) = (2\alpha_1 + \alpha_2, \alpha_2 - \alpha_1, -\alpha_1 - 2\alpha_2), \tag{s3}$$

which implies

$$N_J(a - \varrho(a)) = (2\alpha_1 + \alpha_2)(\alpha_1 - \alpha_2)(\alpha_1 + 2\alpha_2) = 2\alpha_1^3 + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 - 2\alpha_2^3$$

Now a straightforward computation combined with (s2) yields

$$N_J(a - \varrho(a))^2 = D \tag{s4}$$

Since $a$ generates $E$ as a unital $F$-algebra, the quantities $\alpha_1, \alpha_2, -(\alpha_1 + \alpha_2)$ are mutually distinct, and we conclude from (s3) that $a - \varrho(a)$ is invertible in $E$. This in conjunction with (s4) proves $D \in F^\times$, as claimed.

As before we have $Q(a) = -\frac{1}{3}S_J(a) \cdot 1_J$. By hypothesis, this belongs to $J_0^\times$, and since $E/F$ by what we have just shown has discriminant

$$0 \neq D = -4S_J(a)^3 - 27N_J(a)^2 = -27\Big(N_J(a)^2 - 4N_{J_0}(Q(a))\Big),$$

$a$ is an étale element of $J$ relative to $J_0$.

(d)(ii) We must show that $E$ is split cubic étale and $J = J(F, 1)$ over $F = \mathbb{F}_4$ if and only if $(J, J_0)$ does not admit étale elements.

Suppose first $E = F \times F \times F$ is split cubic étale and $J = J(F, 1)$ over $F = \mathbb{F}_4$. Note that $\mathrm{char}(F) = 2$ and $F^\times = \{1, \zeta, \zeta^2\}$, with $\zeta \in F$ a primitive cube root of 1. Assuming $a = (\alpha, \beta, \gamma) \in J$ with $\alpha, \beta, \gamma \in F$ is étale relative to $J_0$, then (i) implies $0 = T_J(a) = \alpha + \beta + \gamma$ and that $a$ generates $E$ as a unital $F$-algebra, equivalently, that $\alpha, \beta, \gamma$ are mutually distinct. If $\gamma = 0$, then $\beta = \alpha$, hence $a = \alpha(1, 1, 0)$ and $a^\sharp = \alpha^2(0, 0, 1)$, so we have the relation $\alpha a + a^\sharp = \alpha^2 \cdot 1_J$, whence $a$ cannot generate $E$ as a unital $F$-algebra, a contradiction.By symmetry, therefore, we may assume $\alpha, \beta, \gamma \in F^\times$, so up to applications of the shift operator we have $a = (1, \zeta, \zeta^2) \in J_0^\perp$, hence $a^\sharp = (1, \zeta^2, \zeta) \in J_0^\perp$. In particular, $a$ cannot be étale relative to $J_0$.

Conversely, suppose $(J, J_0)$ does not admit étale elements and apply (a) to

pick $a \in J$ that generates $E$ as a unital $F$-algebra. Replacing $a$ by $a - \frac{1}{3}T_J(a)\cdot 1_J$ if necessary, we may assume $T_J(a) = 0$. Then (i) implies $S_J(a) = 0$ since $a$ is not étale relative to $J_0$. Hence $a = N_J(a)\cdot 1_J$, and since $E$ is reduced as a commutative ring, we conclude $N_J(a) \neq 0$. Also, $b := a + a^\sharp \in J_0^\perp$, and (33a.14) implies $b^\sharp = a^\sharp + a \times a^\sharp + a^{\sharp\sharp} = -N_J(a)\cdot 1_J + N_J(a)a + a^\sharp$. Thus $S_J(b) = -3N_J(a) \neq 0$. But $b$ is not étale relative to $J_0$, so we deduce from (i) that $1_J, b, b^\sharp$ are linearly dependent, yielding $\alpha, \beta \in F$ which satisfy $b^\sharp = \alpha 1_J + \beta b = \alpha 1_J + \beta a + \beta a^\sharp$. Comparing coefficients gives $N_J(a) = \beta = 1$. Summing up, therefore,

$$E = F[\mathbf{t}]/(\mathbf{t}^3 - 1) = F \times K, \quad K := F[\mathbf{t}]/(\mathbf{t}^2 + \mathbf{t} + 1). \tag{s5}$$

Since $a \in J$ is a Kummer element of norm 1 relative to $J_0$ (Thm. 42.16), Cor. 42.13 yields a natural identification $(J, J_0) = (J(F, 1), F\cdot 1_J)$. Combining Prop. 45.2 with the fact that this Freudenthal pair does not admit étale elements implies $\alpha^3 = 1$ for all $\alpha \in F^\times$. But this amounts to $F = \mathbb{F}_4$ and that $K$ as defined in (s5) is split. Hence so is $E$, and the proof of (ii) is complete.

**45.16** [40, pp. 96-98].

**45.17** (a) The first statement is clear while the second one follows immediately from (36.4.7).

(b) We apply (36.4.5) to obtain $N_J(w) = \gamma_1\gamma_2\gamma_3 t_C(w_1w_2w_3)$, so we only have to worry about the last factor in this product, where we note that Thm. 21.12 implies $w_3 \in M = D^\perp$, hence $\bar{w}_3 = -w_3$, and then

$$\begin{aligned} t_C(w_1w_2w_3) &= t_C((w_1w_2)w_3) = n_C(w_1w_2, \bar{w}_3) = -n_C(w_1w_2, w_3) \\ &= -n_C(-h(w_1, w_2) + w_1 \times_{h,\Delta} w_2, w_3) = -t_D(h(w_1 \times_{h,\Delta} w_2, w_3)). \end{aligned}$$

Now the definition of the hermitian vector product (21.9) yields (1). The verification of (2) is a bit more involved. From (36.4.4) and Thm. 21.12 we deduce

$$Q(w) = \sum (\gamma_j\gamma_l h(w_i, w_i)e_{ii} + \gamma_i\overline{h(w_j, w_l)}[jl]),$$

and taking norms via (36.4.5) yields

$$\begin{aligned} N_{J_0}(Q(w)) &= (\gamma_1\gamma_2\gamma_3)^2\Big(h(w,w_1)h(w_2, w_2)h(w_3, w_3) - \sum h(w_i, w_i)n_D(h(w_j, w_l)) \\ &\quad + t_D(h(w_3, w_2)h(w_1, w_3)h(w_2, w_1))\Big) \\ &= (\gamma_1\gamma_2\gamma_3)^2(h(w_1, w_1)h(w_2, w_2)h(w_3, w_3) \\ &\quad - h(w_1, w_1)h(w_2, w_3)h(w_3, w_2) - h(w_2, w_2)h(w_3, w_1)h(w_1, w_3) \\ &\quad - h(w_3, w_3)h(w_1, w_2)h(w_2, w_1) + h(w_3, w_2)h(w_1, w_3)h(w_2, w_1) \\ &\quad + h(w_1, w_2)h(w_3, w_1)h(w_2, w_3)) \end{aligned}$$

$$= (\gamma_1\gamma_2\gamma_3)^2 \det\big((h(w_i, w_j))_{1\le i,j\le 3}\big)$$
$$= (\gamma_1\gamma_2\gamma_3)^2(\bigwedge^3 h)(w_1 \wedge w_2, \wedge w_3, w_1 \wedge w_2, \wedge w_3)$$

But since $\Delta\colon \bigwedge^3(M,h) \xrightarrow{\sim} (D, \langle \det_\Delta(h)\rangle_{\mathrm{sesq}})$ is an isometry by 21.8 and $\det_\Delta(h) = 1$ by hypothesis, the last expression equals $(\gamma_1\gamma_2\gamma_3)^2 n_D(\Delta(w_1 \wedge w_2 \wedge w_3))$, and (2) is proved.

(c) Applying (1), (2), we see that (i) holds if and only if $\delta(w) \in D^\times$ and $t_D(\delta(w))^2 - 4n_D(\delta(w)) \in D^\times$. By Prop. 19.8, the latter condition is equivalent to $D = k[\delta(w)]$. Hence (i) and (ii) are equivalent.

(d) We begin with a simple lemma.

**Lemma.** *Let $M$ be a finitely generated projective $k$-module of rank $n \in \mathbb{N}$. For elements $v_1, \dots, v_n \in M$ to form a basis of $M$ it is necessary and sufficient that $v_1 \wedge \cdots \wedge v_n$ form a basis of* $\det(M) = \bigwedge^n(M)$.

*Proof* The condition is clearly necessary. Conversely, suppose $v_1 \wedge \cdots \wedge v_n$ is a basis of $\det(M)$. Localizing if necessary, we may assume that $M$ is free. Let $e_1, \dots, e_n$ be a basis of $M$ and write $v_j = \sum_{i=1}^n \alpha_{ij} e_i$, for some $\alpha_{ij} \in k$, $1 \le i, j \le n$. Then $v_1 \wedge \cdots \wedge v_n = \det((\alpha_{ij}))e_1 \wedge \cdots \wedge e_n$, so $\det(\alpha_{ij}) \in k^\times$, and the assertion follows. □

If $w \in J$ is an étale element relative to $J_0$, it may be written as $w = \sum w_i[jl]$, $w_i \in M$, $1 \le i \le 3$, and (c) combined with the lemma implies that $w_1, w_2, w_3$ is a $D$-basis of $M$, and $D = k[a]$, $a = \delta(w) \in D^\times$. Conversely, let $v_1, v_2, v_3$ be a $D$-basis of $M$ and $a \in D^\times$ such that $D = k[a]$. Again by the lemma, $b := \Delta(v_1 \wedge v_2 \wedge v_3) \in D^\times$, and setting $w_1 := v_1 b^{-1} a$, $w_i := v_i$ for $i = 2, 3$, we put $w := \sum w_i[jl]$ and conclude $\delta(w) = a$, forcing $w$ by (c) to be an étale element of $J$ relative to $J_0$.

**45.18** By definition, $J_0$ contains an elementary frame, which by Prop. 39.2 can be extended to a co-ordinate system $\mathfrak{S} = (e_1, e_2, e_3, u[23], u[31])$ of $J_0$. Note that $\mathfrak{S}$ is clearly a co-ordinate system of $J$, and consulting Prop. 37.15, we see that $C_{J_0,\mathfrak{S}} \subseteq C_{J,\mathfrak{S}}$ is a composition subalgebra. Moreover, $\Gamma := \Gamma_{J_0,\mathfrak{S}} = \Gamma_{J;\mathfrak{S}}$, and the Jacobson co-ordinatization theorem 37.17 yields isomorphisms $C_0 \cong C_{J_0,\mathfrak{S}}$, $C \cong C_{J,\mathfrak{S}}$ as well as (1). That the existence of the latter isomorphism is, in fact, independent of the preceding ones follows from the Skolem-Noether theorem for composition algebras (Exc. 23.28).

**45.19** We consider the cubic form $g := N_J|_{J_0^\perp}\colon J_0^\perp \to F$ and assume that the set map $g_F\colon J_0^\perp \to F$ is (identically) zero. The polynomial law $g$ is certainly different from zero since passing to the algebraic closure $\bar{F}$ of $F$ allows us to identify $J_{\bar{F}} = \mathrm{Her}_3(C)$, $C = \bar{F} \times \bar{F}$ and $J_{0\bar{F}} = \sum \bar{F} e_{ii}$, hence $J_{0\bar{F}}^\perp = \sum C[jl]$,

whence $u := \sum c[jl] \in J_{0\bar{F}}^{\perp}$, $c := (1,0) \in C$ by (36.4.5) satisfies $g_{\bar{F}}(u) = N_J(u) = t_C(c) = 1$. From Exc. 12.40 combined with (33a.4) linearized we therefore conclude

$$T_J(u \times v, w) = N_J(u, v, w) = g_F(u, v, w) = 0$$

for all $u, v, w \in J_0^{\perp}$. Since the bilinear trace of $J$ is regular on $J_0^{\perp}$, this implies $u \times v \in J_0$ for all $u, v \in J_0^{\perp}$. Thanks to bilinearity, this condition is stable under base change, hence continues to hold over $\bar{F}$. On the other hand, applying (37.7.4), we obtain $1_C[23] \times 1_C[31] = 1_C[12] \notin J_{0\bar{F}}$,a contradiction. Thus $N_J(u) \neq 0$ for some $u \in J_0^{\perp}$.

**45.20** As in the proof of Thm. 45.11, we define polynomial laws $e_i \colon J \times J \to J$ for $1 \leq i \leq 9$ by

$$e_1(x,y) := 1_{J_R}, \quad e_2(x,y) := x, \quad e_3(x,y) := x^\sharp, \quad e_4(x,y) := y, \quad e_5(x,y) := y^\sharp,$$
$$e_6(x,y) := x \times y, \quad e_7(x,y) := x^\sharp \times y, \quad e_8(x,y) := x \times y^\sharp, \quad e_9(x,y) := x^\sharp \times y^\sharp$$

for all $x, y \in J_R$, $R \in k$-**alg**. We claim that *it suffices to show*

$$\det\Big((T_J(e_i(x,y), e_j(x,y))_{1 \leq i,j \leq 9}\Big) \in k^\times \tag{s1}$$

*for some* $x, y \in J$. Indeed, once such elemnts have been exhibited, the quantities $e_i(x,y)$, $1 \leq i \leq 9$, generate a free submodule $M \subseteq J$ of rank 9 on which the bilinear trace of $J$ is regular. By Lemma 11.10, this implies $J = M \oplus M^\perp$, and by comparing ranks, we conclude $J = M$. On the other hand, $M$ is the subalgebra of $J$ generated by $x, y$ (Exc. 33.15), and we are done.

Thus we need only show that elements $x, y \in J$ exist satisfying (1). 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 invertible element of $k$ if and only if it represents an invertible element of $k/\mathfrak{m}$, for each maximal ideal $\mathfrak{m} \subseteq k$. We may therefore assume that $k = F$ is a field.

If $F$ contains more than four elements, we let $E \subseteq J$ be any cubic étale subalgebra. Then $(J, E)$ is a Freudenthal pair over $F$, hence by Thm. 45.10 admits étale elements. By Cor. 44.18, therefore, $J = J(\mathcal{B}, \mu) = H(\mathcal{B}) \oplus Bj$ is a second Tits construction, for some involutorial system $\mathcal{B} = (K, B, \tau, p)$ of the second kind over $k$ and some admissible scalar $\mu$ for $\mathcal{B}$. such that $E = H(\mathcal{B})$ and $j \in J$ is étale relative to $E$. Now Exc. 44.32 (b) shows that $J$ is generated by $E$ and $j$ as a Jordan $F$-algebra. Since $E$ has a single generator by Exc. 45.15 (a), the assertion follows.

We are left with the case that $F = \mathbb{F}_2$ and consider the following subcases. (i) $J = \mathrm{Mat}_3(F^{(+)}$. Let $E/F$ be the unique (cyclic) cubic field extension of $F$,

$\varrho$ a generator of its Galois group and write $A$ for the cyclic algebra $(E/F, \varrho, 1)$ over $F$ [23, 8.5, p. 484]. By [23, Thm. 8.7, p. 477], $A$ is central simple of degree 3 over $F$, hence isomorphic to $\mathrm{Mat}_3(F)$. It therefore suffices to show that the Jordan algebra $A^{(+)}$ is generated by two elements. Recall that $A$ as a three-dimensional left vector space over $E$ has a basis $1_A, y, y^2$ for some $y \in A$ having $y^3 = 1_A$, subject to the relations $ya = \varrho(a)y$ for all $a \in A$. This implies $(ay)^3 = (ay^2)^3 = N_E(a)1_A$, hence $T_A(ay) = T_A(ay^2) = 0$. Thus $y$ and $y^\sharp = y^2$ (by (33a.22)) both belong to $E^\perp$, and we conclude that $y$ is a Kummer element of $A^{(+)}$ relative to $E$. By 42.12 (a), therefore, $A^{(+)}$ is generated by $E$ and $y$, and since $E$ is generated by a single element, we are done. (ii) $J = \mathrm{Her}_3(K)$, where $K/F$ is the unique quadratic field extension. Consulting Exc. 42.27, we see that $J$ is isomorphic to the first Tits construction $J(F \times K, 1)$. Since $F \times K$ is generated by one element (Exc. 45.15 (a),(b)), $A^{(+)}$ is generated by two elements.

**45.21** Arguing as in the proof of Thm. 45.11, we define polynomial laws $e_i \colon J \to J$, $1 \le i \le 3$, by $e_1(x) := 1_J$, $e_2(x) := x$, $e_3(x) := x^\sharp$ for all $x \in J_R$, $R \in k$-**alg**. We claim that it suffices to show

$$\det\Big((T_J(e_i(x), e_j(x)))_{1\le i\le 3}\Big) \in k^\times$$

for some $x \in J$. Indeed, if such an element has been exhibited, it generates a subalgebra $E \subseteq J$ which, as a submodule, is spanned by $1, x, x^\sharp$ ((33a.14) and Exc. 33.15) and hence is cubic étale, making $(J, E^{(+)})$ a Freudenthal pair over $k$. To find an element making the above determinant invertible, we are reduced in the usual way to the case that $F := k$ is a field. If $F$ is algebraically closed, then $J = \mathrm{Her}_3(F \times F)$ is split and $x := \sum \xi_i e_{ii} \in J$, $\xi_i \in F$ mutually distinct, satisfies the desired condition. By Zariski density, this also settles the problem if $F$ is infinite. On the other hand, if $F$ is finite, it suffices to find a cubic étale $E \subseteq J$ generated by a single element. If $J = \mathrm{Mat}_3(F)^{(+)}$ is split, any cubic subfield of $J$ will do. If $J = \mathrm{Her}_3(K)$, $K$ the unique quadratic field extension of $F$, the norm of $K$ is a universal quadratic form, and setting $\Gamma_0 := \mathrm{diag}(-1, -1, 1)$, (37.24.3) and Exc. 42.27 yield

$$J = \mathrm{Her}_3(K) \cong \mathrm{Her}_3(K, \Gamma_0) \cong J(F \times K, 1),$$

whence $F \times K$ is a cubic étale subalgebra of $J$ generated by a single element (Exc. 45.15 (a),(b)).

**45.22** If $A$ has rank $n$, then $J(A, \mu)$ is finitely generated projective of rank $3n$ as a $k$-module and regular as a cubic Jordan algebra, so $(J(A, \mu), A^{(+)})$ is a balanced pair of cubic Jordan algebras in the sense of 44.6. It remains to show that $J(A, \mu)$ is a Freudenthal algebra. By 39.8, this will follow once we have shown

for all fields $K \in k$-**alg** that $J(A,\mu)_K \cong J(A_K,\mu_K)$ is simple or cubic étale. We are thus reduced to the case that $k = F$ is a field, which we may assume as well from the outset to be algebraically closed. The latter hypothesis makes the norm of $A$ surjective as a set map from $A$ to $F$, and by Exercise 42.22 (c), we may assume $\mu = 1$. According to Exercise 42.21, this up to isomorphism leaves the following options for $A$.

(a) $A = F$, $\mathrm{char}(F) \neq 3$: By 42.12 (b), $J = J(F,1)$ has degree 3, so some $x \in J$ makes $1, x, x^2$ an $F$-basis of $J$, and we conclude that $J = F[x]$ is a 3-dimensional regular cubic Jordan $F$-algebra. As such, it has no absolute zero divisors (Exercise 37.27 (e)) and hence is locally linear (Theorem 30.11). Summing up, therefore, $J$ is split cubic étale.

(b) $A = F \times C$, $C$ a regular (split) composition $F$-algebra: Since $F$ is algebraically closed, Exercises 42.27 (a) and 37.22 (b) imply $J \cong \mathrm{Her}_3(C)$, which is simple by Exercise 37.26 (e).

(c) $A = \mathrm{Mat}_3(F)$: By Exercise 42.23 (a) combined with Corollary 42.15, $J = J(\mathrm{Mat}_3(F),1)$ is a split Albert algebra over $F$, hence simple (Exercise 37.26 (e)).

## Solutions for Section 46

**46.22** Suppose first that $A$ is a division algebra and note that the algebra $A$ has dimension $d^2$ for some $d$. For $c \in F$, consider the polynomial law $A \times F \to F$ defined by $(a,x) \mapsto \mathrm{Nrd}_A(a) - cx^d$. It is a homogenous form of degree $d$ in $d^2+1$ variables so it is isotropic. That is, there is some $(a,x)$ such that $\mathrm{Nrd}_A(a) = cx^d$. Since $A$ is division, $cx^d = \mathrm{Nrd}_A(a) \neq 0$, whence $x \neq 0$ and we find $\mathrm{Nrd}_A(a/x) = \mathrm{Nrd}_A(a)/x^d = c$.

In the general case, by the Wedderburn-Artin Theorem, $A \cong M_n(D)$ for some $n \geq 1$ and some division algebra $D$, both of which are determined by $A$. By the preceding paragraph, we may assume that $n > 1$ and the claim holds for $D$, i.e., there is an element $d \in D$ such that $\mathrm{Nrd}_D(d) = c$. Define $a := \mathrm{diag}(d,1,1,\ldots,1) \in M_n(D)$. It suffices to show

$$\mathrm{Nrd}_{\mathrm{Mat}_n(D)}(a) = \mathrm{Nrd}_D(d).$$

In order to see this, we extend scalars to the algebraic closure $K$ of $F$ and write $r$ for the degree of $D$. Then the left-hand side of the displayed equation is the determinant of the block diagonal matrix $\mathrm{diag}(d_K, \mathbf{1}_r, \ldots, \mathbf{1}_r)$, which obviously is the same as the determinant of $d_K$, hence to its right-hand side.

**46.23** (a) From Cor. 44.24 and Thm. 46.10 we deduce that $J$ is a reduced Albert algebra over $F$.

(b) Following Cor. 45.12, we may realize $J$ by means of the second Tits construction: $J = J(B, \tau, p, \mu)$ as in part (b) of the problem. We define $f_3(J)$ as the 3-Pfister form of the left $p$-twist of $\tau$. In order to show that $f_3(J)$ thus defined satisfies the characterizing conditions of (b), we may assume that $J$ itself is reduced, so by Thm. 46.10 some $q \in B^\times$ has $N_B(q) = \mu$. Now apply Exc. 44.33 to $\mathcal{B} := (K, B, \tau, p)$ and $w := q^{-1}$. Since $B$ is associative, we have $\mathcal{B}.w = (K, B, \tau, p.w)$, where $p.w = qp\tau(q)$, and one checks that the assignment $u \mapsto quq^{-1}$ gives an isomorphism $(B,^p\tau) \to (B,^{pw}\tau)$ of algebras with involution. Hence passing from $\mathcal{B}$ to $\mathcal{B}.w$ doesn't change the isometry class of $f_3(J)$, and Exc. 44.33 (a) allows us to assume $\mu = 1_K$. This implies $N_B(p) = 1$, hence $J^{(p)} \cong J(B,^p\tau, 1_B, 1_K)$ by Thm. 44.26, and since, by the Jacobson-Faulkner theorem 41.8, the coefficient algebra of $J$ does not change when passing to an isotope, we conclude that $f_3(J)$ is indeed the coordinate norm of $J$. This proves existence. For uniqueness, it suffices to combine Springer's theorem with Cor. 46.7 and Prop. 46.6 (b) (5).

**46.24** *Reduction to the finite-dimensional case*. Assume the finite-dimensional case has been settled and let $0 \neq x \in J$. We must show that the linear map $V_x\colon J \to J$, $y \mapsto x \circ y$, is bijective. Gven $y \in J$, the cubic Jordan subalgebra, $J'$, of $J$ generated by $x, y$ is finite-dimensional (Exc. 33.15), so by assumption $V_x z = y$ for some $z \in J'$, and $x \circ y = 0$ implies $y = 0$. Thus $V_x$ is indeed bijective. For the rest of the proof, we may assume that $J$ is finite-dimensional, whence it suffices to establish (1). Suppose on the contrary that some non-zero elements $x, y \in J$ have $x \circ y = 0$. Since $1_J \circ y = 2y \neq 0$, and by symmetry, we obtain $x, y \notin F1_J$. Hence $E := F[x]$ and $E' := F[y]$ are cubic subfields of $J$ (Prop. 46.6 (b) (1)). By (33a.24), we also have $T_J(x, y) = \frac{1}{2}T_J(x \circ y) = 0$. We now consider the following cases.

1°. *$E$ is separable over $F$.* Then $J = E \oplus E^\perp$ as a direct sum of subspaces and the action

$$E \times E^\perp \longrightarrow E^\perp, \quad (z, w) \longmapsto z.w := -z \times w, \tag{s1}$$

makes $E^\perp$ a left vector space over $E$ (Exc. 42.26 (a)). Here (33a.33) implies $E \circ E^\perp \subseteq E^\perp$. Writing $y = u + v$, $u \in E$, $v \in E^\perp$, we obtain $0 = x \circ y = x \circ u + x \circ v$, where $x \circ u \in E$, $x \circ v \in E^\perp$, hence $x \circ u = x \circ v = 0$. But $x \circ u = 2xu$ in terms of the product in $E$, so we have $u = 0$. Thus, $y = v \in E^\perp$. Now (33a.23) and (s1) show $x.y = -x \times y = T_J(x)y$, hence $(x - T_J(x)1_E).y = 0$. Thus $x = T_J(x)1_J$, and taking traces we obtain $2T_J(x) = 0$, hence $x = 0$, a contradiction.

2°. *$E$ is purely inseparable over $F$.* By symmetry, we may also assume that

$E'$ is purely inseparable over $F$. Then (33a.23) gives $x \times y = x \circ y = 0$, and from (33a.8) we deduce $0 = x^\sharp \times (x \times y) = N_J(x)y + T_J(x^\sharp, y)x$. Since $N_J(x) \neq 0$ (Cor. 33.10), this forces $y = \alpha x$, for some $\alpha \in F^\times$, and we arrive at the contradiction $0 = x \circ y = 2\alpha x^2$.

**46.25** It suffices to show that $S_J^0$, the restriction of the quadratic trace to the elements of trace zero in $J$, is isotropic because any isotropic vector in $J^0$ relative to $S_J^0$ generates a cubic subfield of $J$ (Prop. 46.6 (b) (1)) that, by the preceding hint to this exercise, must be cyclic. Let $E/F$ be any cubic subfield of $J$ (Cor. 46.7). Then the base change $J_E$ by Prop. 46.6 (b) (5) is a reduced regular Freudenthal algebra of dimension $\geq 9$ over $E$, hence identifies with $J_E = \mathrm{Her}_3(C, \Gamma)$, for some (regular) composition algebra $C$ over $E$ and some diagonal matrix $\Gamma \in \mathrm{GL}_3(E)$ (Prop. 39.17). By Springer's theorem, it suffuces to show that the binary quadratic form $q$ derived from restricting the quadratic trace of $J_E$ to the *diagonal* elements of trace zero is isotropic. Since the diagonal of $J_E$ is split cubic étale, we can apply Exc. 34.26 (b) with $\beta = 1$ to conclude $q \cong \langle -3, -1 \rangle_{\mathrm{quad}}$. But $-3$ is a square in $F$ since $F$ contains the cube roots of 1, so $q \cong \langle 1, -1 \rangle_{\mathrm{quad}}$ is hyperbolic ([14, Cor. 13.3]).

# Solutions for Chapter VIII

## Solutions for Section 47

**47.16** The solution is modeled after pages 6–9 of [31].

(a): The displayed identity holds if and only if the following expression is identically zero:

$$J(x,y,[xz]) - [J(x,y,z),x] = [[xy][xz]] + [[y[xz]]x] + [[[[xz]x]y] \\ - [[[xy]z]x] - [[[yz]x]x] - [[[zx]y]x].$$

On the right side, the second and last terms cancel, leaving an expression which vanishes if and only if the Malcev identity holds.

(b): The very definition of $S$ shows that it is unchanged by a cyclic permutation of its arguments. On the other hand, linearizing the flexible law, replacing $x$ with $x+z$, gives the identity $[x,y,z] = -[z,y,x]$. We find

$$S(z,y,x) = [z,y,x]+[y,x,z]+[x,z,y] = -[x,y,z]-[z,x,y]-[y,z,x] = -S(x,y,z).$$

That is, for a cyclic permutation and for the transposition interchanging 1 and 3, the claim about how $S$ changes under permuting its arguments holds. Because these permutations generate the group of all permutations, this verifies the claim in full generality.

(c): We expand $[[x,y,z],x] = [x,y,xz] - [x,y,zx]$. Using that the Kleinfeld function is alternating, we have

$$0 = f(x,z,y,x) = [xz,y,x] - z[x,y,x] - [z,y,x]x$$

and we find $[x,y,z]x = [x,y,xz]$. Similarly, $f(z,x,y,x) = 0$ implies that $[x,y,zx] = x[x,y,z]$. Putting these together, we obtain

$$[[x,y,z],x] = [x,y,[x,z]] \quad \forall x,y,z \in A.$$

Now $J(x,y,z) = 2S(x,y,z) = 6[x,y,z]$ for all $x,y,z \in A$, so $A^-$ is Malcev by (a).

For the second claim, $A^-$ is Lie if and only if $J(x,y,z) = 0$ for all $x,y,z$, if and only if $[x,y,z] = 0$ for all $x,y,z$.

**47.17** Suppose first that $k$ has characteristic 2. Then the kernel $I$ of the trace map $C \to k$ is a codimension 1 subspace of $C$ containing $k$. For $x \in I$ and $c \in C$, we have

$$t_C([x,c]) = t_C(xc) - t_C(cx) = 0.$$

That is, the image of $I$ in $C^-/k$ is a codimension 1 ideal which is not zero, so $C^-/k$ is not simple.

It remains to consider the case where $k$ has characteristic different from 2. By Exercise 25.43, we may assume that $k$ is algebraically closed and in particular that $C$ is split. Let $I$ be a subspace of $C$ properly containing $k$ such that the image of $I$ in $C^-/k$ is an ideal; we aim to show that $I = C$. Note that $I$ is an ideal in $C^-$.

We treat the case $C = \mathrm{Mat}_2(k)$. Suppose first that $I$ contains $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$. Since

$$\left[\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)\right] = \left(\begin{smallmatrix}-a & b\\ -c & d\end{smallmatrix}\right) - \left(\begin{smallmatrix}-a & -b\\ c & d\end{smallmatrix}\right) = \left(\begin{smallmatrix}0 & 2b\\ -2c & 0\end{smallmatrix}\right),$$

we deduce that $I = C$. If $I$ contains a trace zero element $x$ that is not nilpotent, then the Jordan form of $x$ is $\left(\begin{smallmatrix}a & 0\\ 0 & -a\end{smallmatrix}\right)$ for some nonzero $a$, and the previous calculation shows that $I = C$.

If $I$ contains a trace zero element $x$ that is nilpotent, then up to conjugacy $x$ is $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$. Since

$$\left[\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)\right] = \left(\begin{smallmatrix}-c & a-d\\ 0 & c\end{smallmatrix}\right),$$

we deduce that $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ is in $I$, whence $I = C$, completing the argument for the rank 4 case.

Now assume $C$ is an octonion algebra. There is a nonzero element of $I \setminus k$, which by Exercise 19.38 is contained in a quaternion subalgebra $B$ of $C$. Because $I$ is an ideal in $C^-$, $I \cap B \supseteq [B, I \cap B]$, which is $B$ by the rank 4 case.

From the 4-dimensional subspace of $C$ perpendicular to $B$, pick a $j$ with $n_C(j) \neq 0$. Then $C$ is obtained by the internal Tits construction $C = \mathrm{Cay}(B, n_C(j))$ as in Prop. 18.1. For each $b$ in the space $B_0$ of trace zero elements of $B$, set $u = \frac{1}{2}b$, so $u - \bar{u} = b$. In the notation of the external Tits construction 18.3, the calculations in 18.13 give that $I$ contains $[u, j] = bj$ and therefore $I$ contains $B_0 j$. For $x, y \in B_0$, we have $[\frac{1}{2}x, yj] = (yx)j$, hence $(B_0 B_0)j \subseteq I$. Since $B_0^2 = B$, we conclude that $I = C$ as desired.

(For the rank 8 case, one might compare p. 435 in [43], which starts with an explicit multiplication table for a basis for $C$.)

**47.18** See for example [19].

**47.19** (a): It is straightforward to check that $q([A,B]x,x) = 0$ for all $A, B \in \mathfrak{sp}_{2n}(F)$ and $x \in k^{2n}$, verifying $\subseteq$. For the opposite containment, let us simplify notation by writing $L := [\mathfrak{sp}_{2n}(F), \mathfrak{sp}_{2n}(F)]$. For any $B \in \mathrm{Alt}_n(F)$, pick $A \in \mathrm{Mat}_n(F)$ such that $B = A - A^{\mathsf{T}}$ and note that

$$\left[\begin{pmatrix} 0 & \mathbf{1}_n \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} A & 0 \\ 0 & -A^{\mathsf{T}} \end{pmatrix}\right] = \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \quad \in L.$$

An analogous computation shows that $\left(\begin{smallmatrix} 0 & 0 \\ B & 0 \end{smallmatrix}\right) \in L$. For $A, A' \in \mathfrak{sl}_n(F)$, we have

$$\left[\begin{pmatrix} A & 0 \\ 0 & -A^{\mathsf{T}} \end{pmatrix}, \begin{pmatrix} A' & 0 \\ 0 & -(A')^{\mathsf{T}} \end{pmatrix}\right] = \begin{pmatrix} [A,A'] & 0 \\ 0 & -[A,A']^{\mathsf{T}} \end{pmatrix}.$$

By Exc. 47.18(c) we conclude that

$$\begin{pmatrix} A & 0 \\ 0 & -A^{\mathsf{T}} \end{pmatrix} \in L \tag{s1}$$

for all $A \in \mathfrak{sl}_n(F)$. Take now $B \in \mathrm{Sym}_n(F)$ to have a 1 in the $(1,1)$-entry and zeros elsewhere. Then

$$\left[\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ B & 0 \end{pmatrix}\right] = \begin{pmatrix} B & 0 \\ 0 & -B^{\mathsf{T}} \end{pmatrix} \in L.$$

In particular, matrices of the form (s1) include those with $A$ of trace zero and at least one of trace 1, ergo include all $A \in \mathrm{Mat}_n(F)$.

(b): Put $L' := [L, L]$. The same computations as in part (a) show that $L'$ contains the claimed subalgebra, i.e., those $\left(\begin{smallmatrix} A & B \\ C & -A^{\mathsf{T}} \end{smallmatrix}\right)$ with $A \in \mathfrak{sl}_n(F)$ and $B, C \in \mathrm{Alt}_n(F)$. Conversely, if we take generic elements $\left(\begin{smallmatrix} A & B \\ C & -A^{\mathsf{T}} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} A' & B' \\ C' & -(A')^{\mathsf{T}} \end{smallmatrix}\right)$ of $L$, then the upper left corner of the commutator is $[A,A'] + BC' - B'C$. Therefore, we are done once we verify the following: *If* $B, C \in \mathrm{Alt}_n(F)$, *then* $\mathrm{tr}(BC) = 0$.

To verify that, note that $B = B_0 - B_0^{\mathsf{T}}$ and $C = C_0 - C_0^{\mathsf{T}}$ for some matrices $B_0, C_0$. Plugging this in, we find

$$\begin{aligned} \mathrm{tr}(BC) &= \mathrm{tr}((B_0 - B_0^{\mathsf{T}})(C_0 - C_0^{\mathsf{T}})) \\ &= \mathrm{tr}(B_0C_0 + B_0^{\mathsf{T}}C_0^{\mathsf{T}}) - \mathrm{tr}(B_0^{\mathsf{T}}C_0 + B_0C_0^{\mathsf{T}}). \end{aligned}$$

Since $\mathrm{tr}(XY) = \mathrm{tr}(X^{\mathsf{T}}Y^{\mathsf{T}})$ for all $X, Y \in \mathrm{Mat}_n(F)$ and $\mathrm{char}(F) = 2$, we conclude that $\mathrm{tr}(BC) = 0$.

**47.20** The action of $\phi \in \mathfrak{sl}_{2n}(k)$ on $\wedge^d k^{2n}$ for any $d$ is given by

$$\begin{aligned} \phi(x_1 \wedge \cdots \wedge x_d) = (\phi x_1) \wedge x_2 \wedge \cdots \wedge x_d + x_1 \wedge (\phi x_2) \wedge x_3 \wedge \cdots \wedge x_d \\ + \cdots + x_1 \wedge \cdots \wedge x_{d-1} \wedge (\phi x_d). \end{aligned}$$

Writing out the coordinates, we find that for a basis $e_1, \dots, e_{2n}$ of $k^{2n}$, we find that the action of $\phi$ on $\wedge^{2n}k^{2n}$ is given by

$$\phi(e_1 \wedge \cdots \wedge e_{2n}) = \operatorname{tr}(\phi)\,(e_1 \wedge \cdots \wedge e_{2n}).$$

Therefore, for $x, y \in \wedge^n k^{2n}$, we have

$$\begin{aligned} b(\rho(\phi)x, y) + b(x, \rho(\phi)y) &= \Delta(\rho(\phi)x \wedge y + x \wedge \rho(\phi)y) \\ &= \Delta(\phi(x \wedge y)) = \operatorname{tr}(\phi)\Delta(x \wedge y) = 0, \end{aligned}$$

so the image of $\phi$ is contained in $\mathfrak{g}$, as required. We omit the verification that $\rho$ is compatible with the Lie bracket. Let $\phi \in \mathfrak{sl}_{2n}(k)$ be such that $\phi(e_1) = e_{n+1}$ and $\phi(e_i) = 0$ for $i \neq 1$. Then

$$\rho(\phi)(e_1 \wedge \cdots \wedge e_n) = e_{n+1} \wedge e_2 \wedge e_3 \wedge \cdots \wedge e_n \neq 0,$$

i.e., $\rho(\phi) \neq 0$, completing the verification of (a).

Note that $\rho(\mathbf{1}_{2n})$ is multiplication by $n$. Therefore, if $n = 0$ in $k$, we have $\mathbf{1}_{2n} \subseteq \operatorname{Ker}\rho$.

(b): Suppose now that $k$ is a field of characteristic not dividing $2n$. Then $\mathfrak{sl}_{2n}(k)$ is simple (Exc. 47.18), so $\operatorname{Ker}\rho$ must be the zero ideal, i.e., $\rho$ is injective. In the case $n = 2$, we note that $\mathfrak{sl}_4(k)$ and $\mathfrak{o}_6(k)$ both have dimension 15, so $\rho$ is an isomorphism.

(c): Finally assume $k$ is a field of characteristic 2. Since $\rho$ is not the zero map and its kernel contains $\mathbf{1}_{2n}$, Exc. 47.18 gives that $\operatorname{Ker}(\rho) = k\mathbf{1}$. Since $\mathbf{1}$ is the center of $\mathfrak{sl}_4(k)$, $\rho$ induces an inclusion

$$[\mathfrak{sl}_4(k), \mathfrak{sl}_4(k)]/k\mathbf{1} \hookrightarrow [\mathfrak{g}, \mathfrak{g}].$$

But $[\mathfrak{sl}_4(k), \mathfrak{sl}_4(k)] = \mathfrak{sl}_4(k)]$ by Exc. 47.18(c), so the domain is $\mathfrak{sl}_4(k)/k\mathbf{1}$ of dimension 14. The codomain has $\dim[\mathfrak{g}, \mathfrak{g}] = \dim \mathfrak{g} - 1$ by Exc. 47.19, which is $\binom{6}{2} - 1 = 14$.

## Solutions for Section 48

**48.25** The linear maps $\Delta_A$ and $s_A$ commute with base change. Recall the descriptions of $\operatorname{LMDer}(A)$, $\operatorname{InDer}(A)$ and $\operatorname{ComDer}(A)$ in (48.10.1), (48.11.1) and (48.11),

$$\begin{aligned} \operatorname{LMDer}(A) &= \{\Delta_x \mid x \in W(A), s(x) \in \operatorname{Nuc}(A)\} = \Delta_A({s_A}^{-1}(\operatorname{Nuc}(A))), \\ \operatorname{InDer}(A) &= \{\Delta_x \mid x \in W(A), s(x) = 0\} = \Delta_A(\operatorname{Ker}(s_A)), \\ \operatorname{ComDer}(A) &= \{\Delta_a \mid a \in A, s(a) = 0\} = \Delta_A(\operatorname{Ker}(s_A)) \cap A). \end{aligned}$$

Using (25.3.2), (25.3.3), we obtain (a), (b) and (c). Finally $(D_{a,b})_R = D_{a_R,b_R}$ yields (d).

## Solutions for Section 49

**49.10** If $C$ is a norm associative conic algebra then $t_C(cd) = t_C(dc)$ (16.13.1) and $[C,C] \subseteq C^0$.

For the opposite inclusion, we are reduced by the usual argument to considering the case $C = \mathrm{Zor}(k)$. Let $c = \begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix}$, $d = \begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix} \in C$. Using (21.18.4),

$$[c,d] = \begin{pmatrix} v_2^{\mathsf{T}}u_1 - u_2^{\mathsf{T}}v_1 & (\alpha_1-\alpha_2)v_2 + (\beta_2-\beta_1)u_2 + 2u_1\times v_1 \\ (\beta_1-\beta_2)u_1 + (\alpha_2-\alpha_2)v_1 + 2u_2\times v_2 & v_1^{\mathsf{T}}u_2 - u_1^{\mathsf{T}}v_2 \end{pmatrix}$$

One sees easily that $[C,C] \supseteq C^0$.

**49.11** We use the notation and results of 49.2. 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

$$\phi(g)\begin{pmatrix} \alpha_1 & v^* \\ v & \alpha_2 \end{pmatrix} := \begin{pmatrix} 0 & -g^*v^* \\ gv & 0 \end{pmatrix}.$$

That the two representations of $\mathfrak{sl}_3(k)$ above are faithful and irreducible is clear. Since $k$ is a field, $M$ and $M^*$ are vector spaces of dimension 3 and we may write $M$ for both. Also $\langle x^*, y\rangle = x^{*\mathsf{T}}y$ and if $g \in \mathrm{End}(M)$ then $g^* = g^{\mathsf{T}}$. Assume there exists an isomorphism of $\psi : M \to M$ of $\mathfrak{sl}$-modules, i.e., $\psi(gv) = -g^{\mathsf{T}}\psi(v)$. So we have $c^{-1}gc = -g^{\mathsf{T}}$ for some invertible $c \in \mathrm{Mat}_3(K)$ and all $g \in \mathfrak{sl}(M)$. Equivalently $gc = -cg^{\mathsf{T}}$ for all $g \in \mathfrak{sl}(M)$. Write $c = \sum_{i,j}\gamma_{ij}e_{ij}$ with $\gamma_{ij} \in k$ and $e_{ij}$ the usual matrix units in $\mathrm{Mat}_3(k)$. For distinct $p,q \in \{1,2,3\}$, we put $g := e_{pq} \in \mathfrak{sl}_3(k)$ and obtain $g^{\mathsf{T}} = e_{qp}$, hence

$$gc = \sum_j \gamma_{qj}e_{pj}, \quad -cg^{\mathsf{T}} = -\sum_i \gamma_{iq}e_{ip}.$$

Comparing gives $\gamma_{qj} = \gamma_{iq} = 0$ for $j \neq p \neq i$, hence $c = 0$, a contradiction.

## Solutions for Section 50

This section contains no exercises.

## Solutions for Section 51

**51.32** If $x = \alpha 1_J$, $\alpha \in k$ then $V_x y = 2\alpha y = 0$ and $V_x = 0$. Let $x = \sum(\alpha_i e_i + a_l[ij]) \in J$ and assume $V_x = 0$. Then $V_x e_i = 2\alpha_i e_i + a_l[ij] + a_j[li] = 0$ and $a_l[ij] = 0 = a_j[li]$. Similarly $a_l[ij] = 0$ and $x = \sum \alpha_i e_i$. In that case $V_x 1_C[ij] = (\alpha_i + \alpha_j)1_C[ij] = 0$. Hence $\alpha_i = \alpha_j$. Similarly $\alpha_i = \alpha_l$ and $x = \alpha_i 1_J$.

**51.33** We need only verify non-zero products. Assume $\{i, j, l\} = \{1, 2, 3\}$. We have $J_0 \circ J_i \subseteq J_i$ by Th.32.2 (note conflicting notation) and $J_i \circ J_j \subseteq J_l$. Consider the triple products. We use 37.7. If at least 2 of the entries are from $J_0$ the result of the product is in the submodule corresponding to the third entry. If exactly one of the entries is from $J_0$, the result of the product is in $J_0$ if the other two entries are from the same submodule, while if they are from two distinct submodules then the result belongs to the third. If two of the entries are from the same off-diagonal submodule then the result belongs to the submodule of the third entry. Finally if each of the entries are from distinct off-diagonal submodules the result lands in $J_0$. So the triple products respect the grading.

# Solutions for Chapter IX

## Solutions for Section 52

**52.10** The split hyperbolic plane $\mathbf{h}$ contains a hyperbolic pair $(u, v)$ as defined in 11.17. For every $R \in k$-**alg** and $t \in R^\times$, we have a linear transformation $g_t$ of the module underlying $\mathbf{h} \perp Q$ defined by setting $g_t(u) = tu$, $g_t(v) = t^{-1}v$, and $g_t$ to be the identity on the module underlying $Q$.

## Solutions for Section 53

This section contains no exercises.

## Solutions for Section 54

**54.22** The crux is to prove (i) implies (iii). For sake of contradiction, suppose that the collection $C$ is a set and $k$ is not the zero ring. Then there is a field $K \in k$-**alg** and we define

$$\mathcal{D} := \{\dim(M \otimes K) \mid M \in C\}$$

where dim is the cardinality of a basis of the vector space $M \otimes K$. (It is the same for all bases of $M \otimes K$ by [8, II.7.2, Th. 3].) Note that it is a set because $C$ is a set.

Consider the case of $k$-modules. For any cardinal $n$, we take $M$ to be the module $k^n$. Since $M \otimes K \cong K^n$, $\mathcal{D}$ contains every cardinal, contradicting that $\mathcal{D}$ is a set by [11, III.3.6, Cor.].

Consider the case of $k$-algebras. For each $n$, we consider the module $k^n$ as

a nonassociative $k$-algebra with a multiplication that is identically zero and set $M \in k$-**alg** to be the "unital hull" of $k^n$. As a $k$-module, $M = k1_M \oplus k^n$, where $1_M$ is the identity of the multiplication on $M$. Constructing the set $\mathcal{D}$ by the same recipe, we find that it in this case $\mathcal{D}$ contains $\dim(M \otimes K) = n+1$. Again we find a contradiction, so $C$ is not a set.

For the rest of the implications, note that the only module under the zero ring is the module 0.

**54.23** Because $\sigma_i(M)$, $\tau_i(M)$ are finitely generated projective, by (54.7.1) we may view each $\alpha_i$ as an element of $\sigma_i(M)^* \otimes \tau_i(M)$. Therefore, for every $R \in k$-**alg**, $\mathrm{Aut}(A_R)$ is the subgroup of $\mathrm{GL}(M_R)$ consisting of those $g$ stabilizing $\alpha_i$ for all $i$, and the claim follows from Exercise 24.30.

**54.24** Write $i$ for the inclusion of $\mathbf{G_m}$ in $\mathbf{Aut}(f)$. Trivially, in the weight space decomposition (52.2.1) of $V$ relative to $i(\mathbf{G_m})$, $V_\chi \neq 0$ for some nonzero $\chi$. The composition $\chi \circ i$ is raising to a power $e \in \mathbb{Z}$ where $e \neq 0$ because $\chi \neq 0$. The statement about the weight space means that there is a nonzero $v \in V$ such that for every $F \in k$-**alg** and $t \in F^\times$, we have:

$$f_F(v) = f_F(i(t)v) = f_F(t^e v) = t^{de} f_F(v).$$

In particular, taking $F = k(\mathbf{t})$ and $t = \mathbf{t}$, we find $(\mathbf{t}^{de} - 1) f_{k(\mathbf{t})}(v \otimes 1) = 0$, ergo the second term in the product must be zero and $f_k(v) = 0$.

**54.25** Since $F$ is perfect, we may apply Prop. 54.20, reducing us to showing that the Galois cohomology set $H^1(K/F, \mathbf{G})$ is zero for every finite extension $K \supseteq F$.

For such a $K$, the group $\mathrm{Aut}_{F\text{-}\mathbf{alg}}(K)$ is cyclic of order $[K : F]$, generated by $\sigma$. Following the notation in 54.4, a 1-cocycle is a map $g\colon \mathrm{Aut}_{F\text{-}\mathbf{alg}}(K) \to \mathbf{G}(K)$ satisfying (54.4.1). By Lang, there is an $h \in \mathbf{G}(K)$ such that $g(\sigma) = h^{-1}\sigma(h)$. By induction, we have

$$g(\sigma^{i+1}) = g(\sigma) \cdot \sigma g(\sigma^i) = h^{-1}\sigma(h)\sigma(h^{-1})\sigma^{i+1}(h) = h^{-1}\sigma^{i+1}(h),$$

so the cocycle $g$ is equivalent to the trivial cocycle that maps all of $\mathrm{Aut}_{F\text{-}\mathbf{alg}}(K)$ to $1 \in \mathbf{G}(K)$. Since this holds for any 1-cocycle, we have shown that $H^1(K/F, \mathbf{G}) = 0$.

**54.26** Suppose $\mathbf{X}$ is a $\mathbf{G}$-torsor in the flat topology, i.e., a representative of a class in $H^1(k, \mathbf{G})$. Our aim is to show that $\mathbf{X}$ is the trivial torsor, i.e., $\mathbf{X}(k)$ is nonempty. There is some fppf $R \in k$-**alg** such that $\mathbf{X}(R)$ is nonempty.

If $k$ is reduced, then since it is artinian it is a finite product $k_1 \times \cdots \times k_m$ of finite fields $k_i$. Write $R = \prod R_i$ where each $R_i$ is a $k_i$-algebra which is necessarily

faithfully flat over $k_i$. Then $H^1(R/k, \mathbf{G}) = \prod_i H^1(R_i/k_i, \mathbf{G}_{k_i})$, where each term in the product is zero by Lang's Theorem (Exc. 54.25).

Drop the hypothesis that $k$ is reduced and put $\mathfrak{a} := \mathrm{Nil}(k)$. Because $k$ is finite, there is some minimal $m \geq 1$ such that $\mathfrak{a}^m = 0$. We proceed by induction on $m$, with the case $m = 1$ being settled by the previous paragraph, so suppose $m \geq 2$. Put $I := \mathfrak{a}^{m-1}$. The ring $k/I$ has $\mathrm{Nil}(k/I)^{m-1} = (\mathrm{Nil}(k)/I)^{m-1} = 0$, so by induction $X(k/I)$ is nonempty. On the other hand, $I^2 = \mathfrak{a}^{2m-2} = \mathfrak{a}^m \cdot \mathfrak{a}^{m-2} = 0$ and $\mathbf{X}$ is smooth, so the natural map $\mathbf{X}(k) \to \mathbf{X}(k/I)$ is surjective.

**54.27** The first key point is an expression of elements of $\mathbf{X}_\Gamma(K)$ in terms of constant classes. (This description has already appeared in the solutions to Exercises 19.33 and 25.46 in the case where $\Gamma$ is a symmetric group.) An element $\phi \in \mathbf{X}_\Gamma(K)$ is a homomorphism of rings $\mathbb{Z}^\Gamma \to K$. Under this homomorphism, the elements $\{\phi(1_\gamma) \in K \mid \gamma \in \Gamma\}$ is a complete orthogonal system of idempotents in $K$. This corresponds to an isomorphism $K \cong \prod_{\gamma\in\Gamma} K_\gamma$ for $K_\gamma \in k$-**alg**, some of which may be the zero ring. The image of $\phi$ under the natural projection $\mathbf{X}_\Gamma(K) \to \mathbf{X}_\Gamma(K_\gamma)$ equals the image of

$$\gamma \in \Gamma = \mathbf{X}_\Gamma(\mathbb{Z}) \to \mathbf{X}_\Gamma(K_\gamma).$$

The second key point is that the description of a tensor system consists of terms that are $k$-linear, so that the isomorphism $K \cong \prod K_\gamma$ determined by $\phi$ induces isomorphisms $\mathbf{Aut}(A_K) \cong \prod_{\gamma\in\Gamma} \mathbf{Aut}(A_{K_\gamma})$. The diagram

$$\begin{array}{ccc} \mathbf{Aut}(A_K) & \xrightarrow{f(K)} & \mathbf{X}_\Gamma(K) \\ \cong\downarrow & & \downarrow\cong \\ \prod \mathbf{Aut}(A_{K_\gamma}) & \xrightarrow{\prod f(K_\gamma)} & \prod \mathbf{X}_\Gamma(K_\gamma) \end{array}$$

commutes because of functoriality of $f$. The image of $\phi$ under the composition $\mathbf{X}_\Gamma(K) \to \mathbf{X}_\Gamma(K_\gamma)$ is the constant class that is the image of $\gamma$, so by hypothesis it is in the image of $f(K_\gamma)$. That is, the element $\phi \in \mathbf{X}_\Gamma(K)$ maps down to something in the image of the bottom arrow. Commutativity of the diagram proves the claim.

## Solutions for Section 55

**55.11** By Corollary 55.2, $J = E^{(+)}$ for some cubic étale $k$-algebra $E$. Therefore, the claim is equivalent to the same statement for $E$, which is Exercise 25.42.

**55.12** The proof proceeds in the same manner as the proofs of Propositions

55.4 and 55.6. Note that for each central simple associative $F$-algebra $B$, we get an algebra with unitary involution $A = B \times B^{\mathrm{op}}$, $K = F \times F$, and $\tau$ the map that swaps the two factors, and in this case we abuse notation and write simply $B$ for the involutorial system. The automorphism group of the algebra $\mathrm{Mat}_3(F)$ is the same as the automorphism group of the corresponding algebra with unitary involution, which is $\mathbf{PGL}_3 \rtimes \mathbb{Z}/2$ as in [25, pp. 346, 400]. The automorphism group of $\mathrm{Sym}(\mathrm{Mat}_3(F))$ is the same by Proposition 53.6.(ii), and the automorphism group of the split adjoint semisimple group of type $\mathsf{A}_2$, $\mathbf{PGL}_3$, is the same as described in 52.7.

The $F$-algebras with involution that are twisted forms of the algebra with unitary involution corresponding to $\mathrm{Mat}_3(F)$ are exactly the ones described in (i) by [25, §29.D]. The rank 9 Freudenthal $F$-algebras are the $F$-forms of $\mathrm{Mat}_3(F)^{(+)}$ by Corollary 39.32. The adjoint semisimple groups of type $\mathsf{A}_2$ are by definition the $F$-forms of $\mathbf{PGL}_3$.

**55.13** The solution is similar to that of Exc. 55.12.

The automorphism group of $(\mathrm{Mat}_6(F), \tau_{\mathrm{spl}})$ is $\mathbf{PGSp}_6$ by [25, pp. 347, 359]. We already asserted that the split Freudenthal algebra of rank 15 had automorphism group $\mathbf{PGSp}_6$, see Theorem 53.4. Finally, the automorphism group of $\mathbf{PGSp}_6$ is itself $\mathbf{PGSp}_6$ by Lemma 52.6.

The $F$-algebras with involution $(A, \sigma)$ in (i) are twisted forms of $(\mathrm{Mat}_6(F), \tau_{\mathrm{spl}})$, because $A \otimes \bar{F} \cong \mathrm{Mat}_6(\bar{F})$ and all non-degenerate skew-symmetric bilinear forms on $\bar{F}^6$ are equivalent, so all symplectic involutions on $\mathrm{Mat}_6(\bar{F})$ are conjugate to $\tau_{\mathrm{spl}}$. Conversely, if $(A, \sigma)$ is a twisted form of $(\mathrm{Mat}_6(F), \tau_{\mathrm{spl}})$, then $A$ is a central simple $F$-algebra (Corollary 9.23) and the involution $\sigma$ is evidently also symplectic.

## Solutions for Section 56

**56.7** (a) Being euclidean, $J$ does not contain nilpotent elements other than zero. By Exc. 8.13 (c), therefore, the unital commutative associative subalgebra $\mathbb{R}[x] \subseteq J$, which has dimension at most 3 by Thm. 33.9, is a direct product of finitely many finite algebraic field extensions of $\mathbb{R}$, i.e., of copies of $\mathbb{R}$ and $\mathbb{C}$. Copies of $\mathbb{C}$ cannot occur since $1^2 + i^2 = 0$ and hence $\mathbb{C}^{(+)}$ is not a *euclidean* Jordan algebra. Thus, for some $n = 1, 2, 3$, there is a complete orthogonal system $(d_1, \ldots, d_n)$ of non-zero idempotents in $J$ such that $\mathbb{R}[x] = \mathbb{R}d_1 \oplus \cdots \oplus \mathbb{R}d_n$ as a direct sum of ideals. By Exc. 37.19, each $d_i$, $1 \le i \le n$, is either elementary or co-elementary or equal to $1_J$ and hence, by Exc. 40.15 (f), splits into the

orthogonal sum of elementary idempotents. By 37.5, therefore, an elementary frame $(c_1, c_2, c_3)$ of $J$ and scalars $\alpha_1, \alpha_2, \alpha_3$ exist such that (1) holds.

(b) For $x \in J$ as given in (a), we recall from (34.17.1)–(34.17.3) that

$$N(x) = \alpha_1\alpha_2\alpha_3, \quad T(x) = \alpha_1 + \alpha_2 + \alpha_3, \quad S(x) = \alpha_2\alpha_3 + \alpha_3\alpha_1 + \alpha_1\alpha_2. \tag{s1}$$

(i) $\Rightarrow$ (ii). Pick an elementary frame $(c_1, c_2, c_3)$ in $J$ and positive real numbers $\alpha_1, \alpha_2, \alpha_3$ such that (1) holds. Then $y := \sum \sqrt{\alpha_i} c_i \in J$ satisfies $N(y) = \sqrt{\alpha_1\alpha_2\alpha_3} \in \mathbb{R}^\times$ by (s1), hence $y \in J^\times$, and $y^2 = x$.

(ii) $\Rightarrow$ (iii). Choose $y$ as in (ii). By (a) and (s1), there exist an elementary frame $(c_1, c_2, c_3)$ of $J$ and $\beta_1, \beta_2, \beta_3 \in \mathbb{R}^\times$ such that $y = \sum \beta_i c_i$, hence $x = \sum \alpha_i c_i$, $\alpha_i = \beta_i^2 > 0$ for $i = 1, 2, 3$. Since $T$ is an associative bilinear form, $L_x$ is self-adjoint relative to $T$, and it suffices to prove (2). Before doing so, we show

$$T(c, d) \geq 0 \tag{s2}$$

for all idempotents $c, d \in J$. By Exc. 37.19, there are four cases: $c = 0$ (trivial), $c$ elementary, $c$ co-elementary, and $c = 1_J$. The same distinction can be made about $d$; hence $T(d) \in \{0, 1, 2, 3\}$, and the case $c = 1_J$ is obvious. Now let $c$ be elementary. Then the Peirce decomposition of $d$ with respect to $c$ attains the form $d = T(c, d)c + d_1 + d_0$, $d_i \in J_i(c)$, $i = 0, 1$. The Peirce-2-component of $d^2$ with respect to $c$ may therefore be written as $\alpha c$,

$$\begin{aligned} \alpha = T(c, d^2) &= T(c, d)^2 T(c, c) + T(c, d_1^2) = T(c, d)^2 + T(c \bullet d_1, d_1) \\ &= T(c, d)^2 + \frac{1}{2} T(d_1, d_1) \geq T(c, d)^2 \end{aligned}$$

since $T$ is positive definite. But $d^2 = d$ and we conclude $T(c, d) \geq T(c, d)^2$, i.e.,

$$0 \leq T(c, d) \leq 1 \tag{s3}$$

if $c$ is elementary. Finally, let $c$ be co-elementary. Then $c' := 1_J - c$ is elementary, and since (s2) is trivial for $d = 0$, we may assume $d \neq 0$, in which case (s3) yields $T(c, d) = T(d) - T(c', d) \geq T(d) - 1 \geq 0$. This completes the proof of (s2). Returning to (2), we now write $0 \neq z \in J$ as $z = \sum \gamma_i d_i$ for some elementary frame $(d_1, d_2, d_3)$ in $J$ and $\gamma_i \in \mathbb{R}$, $1 \leq i \leq 3$, not all zero. From (s2) we deduce $T(c_i, z^2) = \sum_m \gamma_m^2 T(c_i, d_m) \geq 0$ for $1 \leq i \leq 3$, and setting $\alpha := \min_{1 \leq i \leq 3} \alpha_i > 0$, we obtain

$$T(x \bullet z, z) = T(x, z^2) = \sum \alpha_i T(c_i, z^2) \geq \alpha \sum T(c_i, z^2) = \alpha T(z^2) = \alpha T(z, z) > 0,$$

as claimed.

(iii) $\Rightarrow$ (i). Writing $x$ as in (a), we obtain $\alpha_i = T(x \bullet c_i, c_i) > 0$ for $1 \leq i \leq 3$, hence (i).

(iii) ⇒ (iv). Being positive definite, the linear operator $L_x$ is bijective, and we see that $x$ is linearly invertible in the sense of Exc. 31.36, hence invertible. Thus

$$X := \{x' \in J \mid L_{x'} \text{ is positive definite relative to } T\} \subseteq J^\times. \tag{s4}$$

Clearly, $X$ is convex, hence connected with $1_J \in X$, and we have shown

$$X \subseteq \mathrm{Pos}(J). \tag{s5}$$

In particular, (iv) holds.

Before tackling to the final implication (iv) ⇒ (iii) of (b), we prove:

(c) (i) ⇒ (ii) ⇒ (iii) ⇒ (i). This follows from the corresponding implications in (b) by noting that (c) (i) (resp. (c) (ii), (c) (iii)) holds for $x$ if and only if (b) (i) (resp. (b) (ii), (b) (iii)) holds for for $x+\varepsilon 1_J$ and all $\varepsilon > 0$. By the same token, the solution to the entire exercise will be complete once we have established the implication

(b) (iv) ⇒ (iii). By homogeneity, (2) holds if and only if

$$T(x \bullet z, z) > 0 \qquad\qquad (z \in S), \tag{s6}$$

where $S$ stands for the "sphere"

$$S := \{z \in J \mid T(z, z) = 1\}.$$

Since $S$ is compact, (s6) and a standard continuity argument show that $X$ as defined in (s4) is open in $\mathrm{Pos}(J)$. On the other hand, $\mathrm{Pos}(J)$ is connected, so if $X$ were not all of $\mathrm{Pos}(J)$, it could not be closed in $\mathrm{Pos}(J)$, i.e., we would have $X \subset \bar{X} \cap \mathrm{Pos}(J)$. Write $x' \in (\bar{X} \cap \mathrm{Pos}(J)) \setminus X$ as in (a). The set

$$Y := \{y \in J \mid L_y \text{ is positive semi-definite relative to } T\}$$

is closed in $J$ and contains $X$, hence $\bar{X}$, hence $x'$. The implication (iii) ⇒ (i) in (c) therefore implies $\alpha_i \geq 0$ for $1 \leq i \leq 3$, but also $\alpha_i = 0$ for some $i = 1, 2, 3$ since, otherwise, $x'$ would belong to $X$. But then, by (s1), $x'$ cannot be invertible, hence does not belong to $\mathrm{Pos}(J)$, a contradiction. Thus $X = \mathrm{Pos}(J)$, implying (iii), and the solution is complete.

**56.8** In each of the four cases, it suffices for obvious reasons to establish only the first of the two claimed relations.

(a) We put $Y := \mathrm{Pos}(J)$. Since $U_p \colon J^\times \to J^\times$ is a topological map, it permutes the connected components of $J^\times$. In particular, $U_p Y \subseteq J^\times$ is a connected component containing $U_p 1_J = p^2$. But by Exc. 56.7 (b), this element is also contained in $Y$, which implies $U_p Y = Y$.

(b) By Exc. 56.7 (b) we have $p = y^2 = U_y 1_J$ for some $y \in J^\times$, hence $J^{(p)} \cong J$

by Cor. 31.23. From (a) we deduce $U_p^{-1}Y = U_{p^{-1}}Y = Y$, whence $p^{-1} = U_p^{-1}p \in Y$. By definition, $\mathrm{Pos}(J^{(p)})$ is the connected component of $J^{(p)\times} = J^\times$ containing $1_{J^{(p)}} = p^{-1} \in Y$. Thus $\mathrm{Pos}(J^{(p)}) = Y$.

(c) Assume first $\eta \in \mathrm{Aut}(J)$. Again, $\eta\colon J^\times \to J^\times$ is a topological map, forcing $\eta(Y) \subseteq J^\times$ to be a connected component containg $\eta(1_J) = 1_J$. Thus $\eta(Y) = Y$. Since $\mathrm{Str}^0(J)$ acts canonically on $J^\times$, the orbit $\mathrm{Str}^0(J)p \in J^\times$ of $p \in Y$ is a connected subset containing $p$ and hence belonging to $Y$. Thus $\eta(Y) \subseteq Y$ for $\eta \in \mathrm{Str}^0(J)$, and applying this also to $\eta^{-1}$ in place of $\eta$ gives the assertion.

(d) $\mathrm{Pos}(J') \subseteq J'^\times \subseteq J^\times$ is a connected subset containing $1_{J'} = 1_J$. Hence $\mathrm{Pos}(J') \subseteq \mathrm{Pos}(J) \cap J'^\times \subseteq \mathrm{Pos}(J) \cap J'$. Conversely, suppose $y \in \mathrm{Pos}(J) \cap J'$. Then $y \in J'$, being invertible in $J$, is so in $J'$ since we are dealing with *finite-dimensional* Jordan algebras. Thus $y \in \mathrm{Pos}(J) \cap J'^\times$. Now Exc. 56.7, (2) shows $T(y \bullet z, z) > 0$ for all non-zero elements $z \in J$. Since the bilinear trace of $J$ restricts to the bilinear trace of $J'$, we conclude from $T(y \bullet z, z) > 0$ for all non-zero elements $z \in J'$ that $y \in \mathrm{Pos}(J')$. This proves the first two equations of (d). As to the last, $\overline{\mathrm{Pos}}(J) \cap J'$ is a closed subset of $J'$ containing $\mathrm{Pos}(J) \cap J' = \mathrm{Pos}(J')$. Thus $\overline{\mathrm{Pos}}(J') \subseteq \overline{\mathrm{Pos}}(J) \cap J'$. Conversely, let $y \in \overline{\mathrm{Pos}}(J) \cap J'$. Then Exc. 56.7, (3)) shows $T(y \bullet z, z) \geq 0$ for all $z \in J$, hence, in particular, for all $z \in J'$. Thus $y \in \overline{\mathrm{Pos}}(J')$.

**56.9** (a) Let $y \in \mathrm{GL}_n(\mathbb{D})$ and $\eta := \Phi_y$. For $x, z \in J$, we obtain

$$U_{\eta(x)}z = U_{\bar{y}^\mathsf{T}xy}z = \bar{y}^\mathsf{T}xyz\bar{y}^\mathsf{T}xy = \eta U_x\eta^\sharp z,$$

with $\eta^\sharp := \Phi_{\bar{y}^\mathsf{T}}$. Hence (a) follows from (31.20.1).

(b) We have $\Phi_{y_1y_2} = \Phi_{y_2} \circ \Phi_{y_1}$ for all $y_1, y_2 \in \mathrm{GL}_n(\mathbb{D})$, so (b) will follow once we have shown $\Phi_y \in \mathrm{Str}^0(J)$ for all $y \in \mathrm{Tri}_n(\mathbb{D})$. But $\mathrm{Tri}_n(\mathbb{D})$, being homeomorphic to $\mathbb{D}^{\frac{n(n-1)}{2}}$ as a topological space, is connected, and the assertion follows from the fact that $\Phi$ is continuous.

(c) (i) $\Rightarrow$ (ii). The case $n = 1$ being trivial, let us assume $n > 1$ and that the implication holds for $n - 1$ in place of $n$. Write

$$x = \begin{pmatrix} x_1 & u \\ \bar{u}^\mathsf{T} & \xi \end{pmatrix}, \quad x_1 \in J_1 := \mathrm{Her}_{n-1}(\mathbb{D}),\ u \in \mathrm{Mat}_{n-1,1}(\mathbb{D}),\ \xi \in \mathbb{R}. \tag{s1}$$

Since $x_1$ along with $x$ is positive definite, hence invertible, (1) yields $y \in \mathrm{Tri}_n(\mathbb{D})$ such that

$$x' := \bar{y}^\mathsf{T}xy = \begin{pmatrix} x_1 & 0 \\ 0 & \xi_n \end{pmatrix} \in J.$$

Since $x'$ is positive definite as well, we obtain $\xi_n > 0$, and the induction hypothesis leads to an element $y_1 \in \mathrm{Tri}_{n-1}(\mathbb{D})$ making $\bar{y}_1^\mathsf{T}x_1y_1$ a diagonal matrix with

positive diagonal entries. This property carries over to $\overline{yy'}^{\mathsf{T}} xyy' = \overline{y'}^{\mathsf{T}} \bar{y}^{\mathsf{T}} xyy'$ with $y' = \left(\begin{smallmatrix} y_1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and the induction is complete.

(ii) $\Rightarrow$ (i). By (ii) we find a matrix $z \in J^\times$ satisfying $x' := \bar{y}^{\mathsf{T}} xy = z^2 = \bar{z}^{\mathsf{T}} z$. Hence $x'$ is positive definite and thus so is $x$.

Now let $n = 3$. (ii) $\Rightarrow$ (iii). Again some $z \in J^\times$ has $x' := \bar{y}^{\mathsf{T}} xy = z^2$, which by Exc. 56.7 (b) belongs to $\mathrm{Pos}(J)$. Hence so does $x = \Phi_{y^{-1}} x'$ by (b) and Exc. 56.8 (c).

(iii) $\Rightarrow$ (i). $x \in \mathrm{Pos}(J)$ leads to an element $z \in J^\times$ such that $x = z^2 = \bar{z}^{\mathsf{T}} z$. Hence $x$ is positive definite.

**56.10** (a) (i) $\Rightarrow$ (ii). From Exc. 56.7 (b) we deduce $T(x, e_{ii}) = T(x, e_{ii}^2) = T(x \bullet e_{ii}, e_{ii}) > 0$ for $1 \le i \le 3$. The same exercise implies $x = y^2$ for some $y \in J^\times$, hence $x^\sharp = y^{2\sharp} = y^{\sharp 2} \in \mathrm{Pos}(J)$, and we also have $T(x^\sharp, e_{ii}) > 0$. Finally, $N(x) = N(y)^2 > 0$.

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (i). Note first that the unital subalgebras of $\mathbb{O}$ up to conjugation under $\mathrm{Aut}(\mathbb{O})$ are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ itself (Exc. 23.28).

Next we claim that *there is no harm in assuming* $u_1 = 0$ *or* $u_1 = 1_\mathbb{O}$. Indeed, if $u_1 \neq 0$, we replace $x$ by $\alpha^{-1} x$, $\alpha := \sqrt{n_\mathbb{O}(u_1)}$, if necessary to ensure $n_\mathbb{O}(u_1) = 1$. By Exc. 5.18, the assignment

$$\sum (\eta_i e_{ii} + v_i[jl]) \longmapsto \sum \eta_i e_{ii} + (u_1^{-1} v_1)[23] + (v_2 u_1^{-1})[31] + (u_1 v_3 u_1)[12]$$

defines an automorphism $\varphi$ of $J$ that leaves all minors of $x$ as well as $\mathrm{Pos}(J)$ (Exc. 56.8 (c)) invariant and sends $x$ to

$$\sum \xi_i e_{ii} + 1_\mathbb{O}[23] + (u_2 u_1^{-1})[31] + (u_1 u_3 u_1)[12],$$

proving our claim.

From now on we therefore assume $u_1 \in \{0, 1_\mathbb{O}\}$. Then Exc. 17.10 combined with our initial observation implies that there is no harm in assuming $x \in J' := \mathrm{Her}_3(\mathbb{H})$. Write

$$x = \begin{pmatrix} x_1 & u \\ \bar{u}^{\mathsf{T}} & \xi_3 \end{pmatrix}, \quad x_1 \in \mathrm{Her}_2(\mathbb{H}), \quad u \in \mathrm{Mat}_{2,1}(\mathbb{H}), \quad \xi_3 \in \mathbb{R}.$$

More precisely, we have $x_1 \in J'' := \mathrm{Her}_2(\mathbb{R}[u_3])$, and $\mathbb{R}[u_3]$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, hence commtative associative. Since the principal minors of $x_1$ are positive by (iii), we deduce from Bourbaki [6, IX.7, Prop. 3] that $x_1$ is positive definite, hence invertible. Invoking (1) of Exc. 56.9, we therefore find an element $y \in \mathrm{Tri}_3(\mathbb{H})$ such that

$$x' := \bar{y}^{\mathsf{T}} xy = \begin{pmatrix} x_1 & 0 \\ 0 & \xi_3' \end{pmatrix} \in J'' \tag{s1}$$

for some $\xi_3' \in \mathbb{R}$. Since $\Phi_y$ by Exc. 56.9 (a) belongs to the structure group of $J'$, and $J'$ has degree 3, it reproduces the norm up to the factor $N(\bar{y}^{\mathsf{T}} y)$, which must be positive since $\mathrm{Tri}_3(\mathbb{H})$ is connected and $y \mapsto N(\bar{y}^{\mathsf{T}} y)$ is continuous. This proves $N(x') > 0$, and we have shown that all principal minors of $x'$ are positive, forcing $x'$ itself to be positive definite (Bourbaki, loc. cit.). From Exercises 56.9 (b) and 56.8 (d), we therefore deduce $x' \in \mathrm{Pos}(J'') \subseteq \mathrm{Pos}(J')$, hence $x \in \mathrm{Pos}(J') \subseteq \mathrm{Pos}(J)$.

(b) Apply (a) to $x + \varepsilon \mathbf{1}_3$, $\varepsilon > 0$, and let $\varepsilon \to 0$.

## Solutions for Section 58

This section contains no exercises.

# References


[1] Abramowitz, M., Stegun, I.: Handbook of mathematical functions with formulas, graphs, and mathematical tables, *National Bureau of Standards Applied Mathematics Series*, vol. 55. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. (1972) 77

[2] Albert, A.: On a certain algebra of quantum mechanics. Ann. of Math. (2) **35**(1), 65–73 (1934). DOI 10.2307/1968118. URL http://dx.doi.org/10.2307/1968118 6

[3] Albert, A., Paige, L.: On a homomorphism property of certain Jordan algebras. Trans. Amer. Math. Soc. **93**(1), 20–29 (1959). DOI 10.2307/1993420 6

[4] Bhargava, M.: On the classification of rings of "small" rank (2009). URL https://swc-math.github.io/aws/2009/09BhargavaNotes.pdf 299

[5] Van der Blij, F., Springer, T.: The arithmetics of octaves and of the group $G_2$. Nederl. Akad. Wetensch. Proc. Ser. A 62 = Indag. Math. **21**, 406–418 (1959) 14

[6] Bourbaki, N.: Algèbre. Chapitre 9: Formes sesquilinéaires et formes quadratiques. Actualités Sci. Ind. no. 1272. Hermann, Paris (1959) 320

[7] Bourbaki, N.: Commutative algebra: Chapters 1–7. Elements of mathematics. Hermann, Paris (1972). Translated from the French 3, 61, 62, 63, 64, 72, 81, 115, 144, 283

[8] Bourbaki, N.: Algebra, Part I: Chapters 1–3. Hermann, Paris (1974). Translated from the French 138, 144, 159, 165, 313

[9] Bourbaki, N.: Algèbre. Chapitres 4 à 7. [Algebra. Chapters 4–7]. Masson, Paris (1981) 10, 73, 165, 167, 168

[10] Bourbaki, N.: Lie groups and Lie algebras: Chapters 4–6. Springer-Verlag, Berlin (2002) 4

[11] Bourbaki, N.: Theory of sets. Elements of Mathematics (Berlin). Springer-Verlag, Berlin (2004). DOI 10.1007/978-3-642-59309-3. Reprint of the 1968 English translation [Hermann, Paris] 313

[12] Braun, H., Koecher, M.: Jordan-Algebren. Springer-Verlag, Berlin (1966) 64

[13] Dieudonné, J.: Sur les groupes classiques. Actualités Sci. Ind., no. 1040 = Publ. Inst. Math. Univ. Strasbourg (N.S.) no. 1 (1945). Hermann et Cie., Paris (1948) 153

[14] Elman, R., Karpenko, N., Merkurjev, A.: The algebraic and geometric theory of

quadratic forms, *Coll. Publ.*, vol. 56. Amer. Math. Soc., Providence, RI (2008) 17, 71, 156, 170, 306

[15] Garibaldi, S., Merkurjev, A., Serre, J.P.: Cohomological invariants in Galois cohomology, *University Lecture Series*, vol. 28. Amer. Math. Soc. (2003) 16

[16] Garibaldi, S., Petersson, H., Racine, M.: Albert algebras over $\mathbb{Z}$ and other rings. Forum of Mathematics: Sigma **11**, e18 (2023). DOI 10.1017/fms.2023.7 5, 95

[17] Garibaldi, S., Petersson, H., Racine, M.: Albert algebras over commutative rings, *New Mathematical Monographs*, vol. 48. Cambridge University Press (2024). DOI 10.1017/9781009426862 1

[18] Glennie, C.: Some identities valid in special Jordan algebras but not valid in all Jordan algebras. Pacific J. Math. **16**(1), 47–59 (1966) 8

[19] Hogeweij, G.: Almost-classical Lie algebras. I, II. Nederl. Akad. Wetensch. Indag. Math. **44**(4), 441–460 (1982) 309

[20] Jacobson, N.: Structure and representations of Jordan algebras. American Mathematical Society Colloquium Publications, Vol. XXXIX. American Mathematical Society, Providence, R.I. (1968) 7, 17

[21] Jacobson, N.: Structure theory of Jordan algebras, *University of Arkansas Lecture Notes in Mathematics*, vol. 5. University of Arkansas, Fayetteville, Ark. (1981) 6

[22] Jacobson, N.: Basic algebra. I, second edn. W. H. Freeman and Company, New York (1985) 260

[23] Jacobson, N.: Basic algebra. II, second edn. W. H. Freeman and Company, New York (1989) 20, 58, 64, 175, 244, 303

[24] Jacobson, N., Rickart, C.: Jordan homomorphisms of rings. Trans. Amer. Math. Soc. **69**, 479–502 (1950) 18, 20

[25] Knus, M.A., Merkurjev, A., Rost, M., Tignol, J.P.: The book of involutions, *Amer. Math. Soc. Coll. Publ.*, vol. 44. American Mathematical Society, Providence, RI (1998) 16, 316

[26] Knus, M.A., Ojanguren, M.: Théorie de la descente et algèbres d'Azumaya. Lecture Notes in Mathematics, Vol. 389. Springer-Verlag, Berlin-New York (1974) 166, 276

[27] Lang, S.: Algebra, *Graduate Texts in Mathematics*, vol. 211, third edn. Springer-Verlag, New York (2002) 64

[28] McCrimmon, K.: The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras. Trans. Amer. Math. Soc. **139**, 495–510 (1969) 17

[29] McCrimmon, K.: The Freudenthal-Springer-Tits constructions revisited. Trans. Amer. Math. Soc. **148**, 293–314 (1970) 17

[30] McCrimmon, K., Zel′manov, E.: The structure of strongly prime quadratic Jordan algebras. Adv. in Math. **69**(2), 133–222 (1988). DOI 10.1016/0001-8708(88)90001-1. URL http://dx.doi.org/10.1016/0001-8708(88)90001-1 7

[31] Myung, H.: Malcev-admissable algebras. No. 64 in Progress in Mathematics. Springer (1986) 307

[32] O'Meara, O.: Introduction to quadratic forms. Die Grundlehren der mathematischen Wissenschaften, Bd. 117. Springer-Verlag, New York (1963) 261

[33] Parimala, R., Sridharan, R., Thakur, M.: A classification theorem for Albert algebras. Trans. Amer. Math. Soc. **350**(3), 1277–1284 (1998). DOI 10.1090/S0002-9947-98-02102-3. URL https://doi.org/10.1090/S0002-9947-98-02102-3 20

[34] Petersson, H.: The structure group of an alternative algebra. Abh. Math. Sem. Univ. Hamburg **72**, 165–186 (2002) 98, 99

[35] Petersson, H.: Structure theorems for Jordan algebras of degree three over fields of arbitrary characteristic. Comm. Algebra **32**(3), 1019–1049 (2004). DOI 10.1081/AGB-120027965. URL https://doi.org/10.1081/AGB-120027965 20

[36] Petersson, H.: Norm equivalences and ideals of composition algebras. Münster J. of Math. **14**, 283–293 (2021) 124

[37] Petersson, H., Racine, M.: On the invariants mod 2 of Albert algebras. J. Algebra **174**(3), 1049–1072 (1995). DOI 10.1006/jabr.1995.1166. URL https://doi.org/10.1006/jabr.1995.1166 16

[38] Petersson, H., Racine, M.: An elementary approach to the Serre-Rost invariant of Albert algebras. Indag. Math. (N.S.) **7**(3), 343–365 (1996) 16

[39] Petersson, H., Racine, M.: The Serre-Rost invariant of Albert algebras in characteristic three. Indag. Math. (N.S.) **8**(4), 543–548 (1997) 16

[40] Petersson, H., Thakur, M.: The étale Tits process of Jordan algebras revisited. J. Algebra **273**(1), 88–107 (2004). DOI 10.1016/j.jalgebra.2002.10.002 300

[41] Racine, M.: The arithmetics of quadratic Jordan algebras. Mem. Amer. Math. Soc. **136**, vi+125 (1973) 14

[42] Rice, A., Brown, E.: Why Hamilton couldn't multiply triples. The College Mathematics Journal **52**(3), 185–192 (2021). DOI 10.1080/07468342.2021.1897418 23

[43] Sagle, A.A.: Malcev algebras. Trans. Amer. Math. Soc. **101**(3), 426–458 (1961) 309

[44] Stacks Project Authors, T.: Stacks project. https://stacks.math.columbia.edu (2018) 4, 11, 13, 64

[45] Tits, J.: Sur les degrés des extensions de corps déployant les groupes algébriques simples. C. R. Acad. Sci. Paris Sér. I Math. **315**(11), 1131–1138 (1992) 16

# Subject index


adjoint
  action, 570
  group scheme, 572
  of a cubic euclidean Jordan matrix algebra, 31
admissible scalar for $(A, \tau)$, 487
affine scheme, 206
  closed subfunctor, 215
  co-morphism, 215
  direct product, 215
  étale, 235
  faithfully flat, 230
  flat, 230
  open subfunctor, 216
  smooth, 236
affine space, 207
Albert algebra, 404
  3-Pfister form, 441
  3-invariant mod 2, 441
  5-Pfister form, 441
  5-invariant mod 2, 441
  euclidean, 30
  local-global principle, 604
  over $\mathbb{Z}$, 614
  purity, 604
Albert isotopy, 121
algebra
  antomorphism, 64
  associative, 45
  associator, 44
  central simple, 61
  commutative, 45
  commutator, 44
  étale, 234
  faithfully flat, 225
  finite presentation, 231
  finitely presented, 231
  flat, 225
  flexible, 127
  homomorphism, 43
  identity element, 47
  non-associative, 43
  opposite, 65
  power-associative, 15, 45
  powers, 45
  presentation, 231
  residually simple, 63
  simple, 48
  structure constants, 46
  unit element, 47
  unital, 47
    algebraic, 50
    central, 48
    central idempotent, 50
    centralization, 48
    split algebraic, 50
  unital homomorphism, 47
algebra with involution, 65
  base change or scalar extension, 65
  centre, 65
  homomorphism, 65
  ideal, 65
  simple, 66
algebraic element, 49
algebraic geography, 8
algebraically closed field
  associative algebras over, 51
alternating matrix, 67
alternative algebra, 109
  Artin's theorem, 115
  invertible element, 111
  of degree 3, 447

one-sided inverse, 116
separable, 178
strongly associative subset, 114
weakly two-pointed, 118
with isotopy involution, 465
base change, 465
homomorphism, 465
anisotropic, 83
group scheme, 575
anti-Dickson condition, 385
anti-homomorphism, 65
anti-regular, 84
automorphism group scheme, 220
Azumaya algebra, 156, 449
of degree 1, 449
of degree 2, 449
of degree 3, 449
of degree $n$, 449
reduced norm, 449
with involution of the second kind, 486
with unitary involution, 486

balanced pair, 471
base change or scalar extension
of a module, 51
of a linear map, 52
of an algebra, 60
basis
associated with a lattice, 16
$\theta$-balanced, 183
bilinear form
associative, 45
Brown's theorem, 159

canonical pairing of a right module, 163
canonical scalar product, 11
Cayley-Dickson construction
external, 138
internal, 137
universal property, 140
Cayley-Dickson process, 140
Cayley-Hamilton Theorem, 240
central element, 48
centre, 48
of a unital algebra, 48
Chevalley-Warning theorem, 195, 504, 515
Chinese Remainder Theorem, 35
co-ordinate algebra, 358
octonionic, 358
co-ordinate pair, 358
octonionic, 358
complete orthogonal system of idempotents, 47
composition algebra, 148
over a finite ring, 428
over an LG ring, 162, 188, 192, 193, 202, 203
reduced, 179
regular, 148
Skolem-Noether theorem, 202
split, 175
of rank 1, 175
of rank 2, 175
of rank 4, 175
of rank 8, 175
splitting, 247
splitting datum, 242
splitting field, 200
standard split, 176
ternary hermitian construction, 171
conic algebra, 123
bilinear trace, 124
co-ordinates, 130
conic ideal, 132
conic nil ideal, 132
conjugation, 124
Dickson condition, 131
homomorphism, 124
multiplicative, 133
norm, 123
norm equivalence, 191
norm isometry, 191
norm similarity, 191
norm-associative, 128
semi-linear homomorphism, 130
trace, 124
unital norm equivalence, 191
cross product identity, 9
cubic étale algebra, 340
split, 340
cubic alternative algebra, 337
bilinear trace, 338, 448
cubic ideal, 459
cubic nil ideal, 459
homomorphism, 337
semi-linear, 448
linear trace, 337
norm, 337
pointed, 491
base change, 491
homomrphism, 491
quadratic trace, 337
separated cubic ideal, 459
cubic array, 318

adjoint, 318
associated para-quadratic algebra, 321
base change or scalar extension, 318
base point, 318
base point identities, 318
bilinear trace, 319
cubic subarray, 320
homomorphism, 318
linear trace, 319
norm, 318
quadratic trace, 319
semi-linear homomorphism, 335
cubic associative algebra, 337
cubic euclidean Jordan matrix algebra, 34
non-negative cone, 606
positive cone, 605
minor, 612
principal minor, 612
cubic form, 89
cubic ideal, 342
cubic Jordan algebra, 329
absolute zero divisor, 381
adjoint, 330
as an abstract Jordan algebra, 384
balanced pair, 471
homomorphism, 471
bilinear trace, 330
co-ordinate system, 368
co-ordinated, 368
homomorphism, 329
linear trace, 329
nil radical, 343
norm, 329
quadratic trace, 330
semi-linear homomorphism, 336
strong co-ordinate system, 406
cubic Jordan matrix algebra, 361
diagonal co-ordinate system, 369
diagonal isomorphism, 380
diagonally isomorphic, 380
cubic map, 105
cubic nil ideal, 379
cubic norm pseudo-structure, 345
cubic norm structure, 320
adjoint identity, 320
associated Jordan algebra, 326
cubic norm substructure, 321
complemented, 347
complemented under isotopy, 355
generated by a subset, 321
orthogonal complement, 347
strong orthogonality, 348
gradient identity, 320
hermitian, 358
homomorphism, 320
isotope, 326
supported by a pointed quadratic module, 345
unit identity, 320
cyclic permutation of (123), 2

Dedekind domain, 190
derivation, 531
derivations of alternative algebras, 536
associator derivations, 537
commutator derivations, 537
inner derivation, 536
determinant
of an integral quadratic lattice, 18
diagonal frame, 368
Dickson condition, 131, 287, 395
discriminant
of a finite rank free quadratic module, 77
of an integral quadratic lattice, 18
division algebra, 48
Jordan, 289
para-quadratic, 261
dual module, 57
duality functor, 57

$E_8$-lattice, 25
eikonal equation, 356
elementary frame, 366
associated with a co-ordinate system, 368
elementary idempotent
Clifford case, 277
conic case, 131
cubic Jordan case, 364
norm class, 434
equalizer, 228
étale Jordan algebra, 599
étale cohomology, 596
étale cover, 235, 238
étale element, 472
Euler's differential equation, 94

faithfully flat descent, 240
Fano plane, 11
Faulkner's lemma, 365
Ferrar's lemma, 379
finite étale algebra, 155
first Tits construction, 455
classical, 456
external, 453

formal, 455
internal, 451
flat cohomology, 596
flexible, 529
flexible algebra, 127, 259
flexible law, 109, 127
form, 89
isotropic, 103
represents zero, 103
fppf, 237
fppf cohomology, 596
Freudenthal algebra, 401
over a finite ring, 428
reduced, 429
regular reduced simple
Ω-co-ordinatization, 434
class group, 434
co-ordinate (coefficient) algebra, 433
co-ordinatization, 433
Pfister forms, 433
re-co-ordinatized, 433
splitting, 411
splitting datum, 407
standard split, 405
standard splitting datum, 409
Freudenthal algebras
over $\mathbb{Z}$, 614
Freudenthal pair, 495
Frobenius's theorem, 159
full support, 80

Gaussian integers, 19
Gaussian integers of $\mathbb{H}$, 19
Gaussian integers of $\mathbb{O}$, 19
gradings of algebras, 540
*e*-grading, 540
Grassmann identity, 2

hermitian form, 165
hermitian Grassmann identity, 170
hermitian inner product, 1
hermitian matrix, 357
twisted, 357
hermitian module, 165
hermitian space, 167
determinant relative to an orientation, 169
ternary, 169
hermitian space of rank $n$, 167
hermitian vector product, 169
Hoffmann's $\mathcal{S}_4$ example, 200
Hoffmann's Klein-four example, 205
homotope
of an alternative algebra, 117
of an associative algebra, 117
hyperbolic pair, 77
hyperbolic plane, 78
split, 78
hyperbolic space, 78
split, 78
hyperline, 444

idempotent, 45
absolutely primitive, 177
co-elementary, 378
elementary
conic algebra, 131
cubic Jordan algebra, 364
in a para-quadratic algebra, 261
primitive, 50, 177
idempotents
complete orthogonal system of, 47, 50
orthogonal, 45
orthogonal system of, 45
incidence geometry, 11
inflation, 595
integral, 79
integral element, 15
involution, 9, 29, 65
conjugate transpose, 29, 67
exchange involution, 66
split orthogonal, 67
split symplectic, 68
twisted conjugate transpose, 357
involutorial system, 468
admissible scalar, 470
associative, 471
admissible scalar, 471
base change, 470
base point, 492
core, 469
core split, 470
base change, 470
homomorphism, 470
homomorphism, 469
left isotope, 487
of the $r$-th kind, 469
opposite, 495
right isotope, 487
scalar extension, 470
unitary, 469
isotope
of a Jordan algebra, 290
of an alternative algebra, 119
isotopy involution, 464
isotropic

group scheme, 575
J-structure, 577
Jacobi identity, 2, 521
Jacobson
co-ordinatization theorem, 375
categorical set-up, 382
radical, 79
Jordan algebra, 268
absolute zero divisor, 287
autotopy, 293
complete orthogonal system of idempotents
connected, 315
strongly connected, 315
cubic étale, 340
derivation algebra, 549
exceptional, 275
fundamental formula, 269
generically algebraic, 394
having no absolute zero divisors, 287
homotopy, 293
Hua identity, 297
inner structure group, 295
inverse of an invertible element, 288
invertible element, 288
isotope, 290
isotopy, 293
isotopy over LG rings, 424
Jordan circle product, 269
Jordan triple product, 269
linear at an element, 286
locally linear, 286
of a pointed quadratic module, 276
of Clifford type, 277
elementary idempotent, 277
of degree 3, 384
semi-simple, 398
separable, 394
special, 275
strong homotopy, 300
structure group, 295
structure Lie algebra, 549
Jordan division algebra, 289
$k$-functor, 205
base change or scalar extension, 221
direct product, 206
projection morphism, 206
of isomorphisms, 246
regular function, 209
structure morphism, 212
subfunctor, 206
$k$-group functor, 216
morphism, 216
subgroup functor, 216
$k$-group scheme, 217
additive group of $k$, 217
multiplicative group of $k$, 217
of a finitely generated projective module, 218
Kirmse's identities, 134
Klein-four group, 560
Kleinfeld function, 115
Kleinfeld's theorem, 113
Kummer element
in the sense of Thakur, 451
invertibility condition, 450
relative to a complemented cubic Jordan subalgebra, 450
relative to a cubic étale subalgebra, 462
relative to a regular cubic Jordan subalgebra, 451
stability condition, 450
strong orthogonality condition, 450
Lagrange identity, 134
Lang's Theorem, 599
lattice, 16
integral quadratic, 16
unimodular, 18
Kirmse, 27
unital, 16
left alternative law, 109
left multiplication
extended, 122
left multiplication operator, 44
LG ring, 79–81, 84, 159
composition algebras over, 154, 162, 188, 192, 193, 202, 203
isotopy for Jordan algebras over, 424
quadratic spaces over, 80–81
Lie algebra, 521
abelian, 522
adjoint representation, 522
Cartan subalgebra, 525
inner derivation algebra, 551
Inner structure Lie algebra, 551
semisimple element, 525
Lie multiplication algebra, 534
Lie multiplication derivation algebra
derivation algebra, 535
line bundle, 57
linear form
associative, 45
linear invertibility, 300

linear Jordan algebra, 252
  exceptional, 253
  fully linearized Jordan identity, 254
  invertible element, 298
  Jordan identity, 252
  Jordan triple product, 256
  of a pointed quadratic module, 255
  special, 253
  $U$-operator, 255
linearization, 5
Lipschitz quaternions, *see* Hurwitz quaternions
local linearity, 286

matrix
  of a bilinear form, 74
  of a quadratic form, 74
matrix unit, 48
minimum polynomial, 15, 49
module
  faithfully flat, 224
  flat, 224
  projective, 56
    of constant rank, 56
    of finite constant rank, 56
    of locally even rank, 75
    of rank $r$, 56
monogenic $k$-algebra, 241
monomials over a subset, 44
Moufang identities, 110
  left Moufang identity, 110
  middle Moufang identity, 110
  right Moufang identity, 110
multi-indices, 87
multi-quadratic map, 82
multiplication algebra, 47

natural representation
  derivation, 531
nil radical, 46
nilpotent element, 46
  in a para-quadratic algebra, 265
  of index 2, 461
norm
  of a cubic euclidean Jordan matrix algebra, 31
norm class of an elementary idempotent, 434
norm equivalence theorem, 192
norm isometry, 420
norm similarity, 420
norm variety, 458
nucleus
  of a unital algebra, 48
Nullstellensatz, 230
  separable, 237

octonion algebra, 157
  of $(M, \theta)$-twisted Zorn vector matrices, 183
  of Zorn vector matrices, 175
octonions
  Dickson-Coxeter, 23
  Graves-Cayley, 3
    associator, 5, 9
    automorphism group, 12
    Cartan-Schouten basis, 10
    conjugation, 4
    inversion formula, 6
    Moufang identities, 9
    norm, 4
    trace, 4
  over algebraic number fields, 198
  over Dedekind domains, 190
  over finite algebraic extensions of $\mathbb{Q}_p$, 196
  over finite fields, 195
  over $\mathbb{R}$, 195
  over $\mathbb{Z}$, 204, 614
one-generated $k$-algebra, 241
opposite
  algebra, 65
  group, 593
orientation, 169
orthogonal complement, 74
orthogonal group scheme, 221

para-quadratic algebra, 258
  base change or scalar extension, 262
  base point, 258
  central, 264
  centroid, 262
  circle product, 258
  evaluation, 266
  extreme radical, 264
  homomorphism, 258
  ideal, 259
  idempotent, 261
  inner ideal, 260
  multiplication algebra, 261
  nil radical, 265
  orthogonal idempotents, 261
  orthogonal system of idempotents, 267
  outer centroid, 267
  outer ideal, 260
  power-associative, 261
  power-associative at an element, 261
  powers, 260
  subalgebra, 259

triple product, 258
$U$-operator, 258
unital, 259
$V$-operator, 258
weak identity element, 258
Peirce component, 303
Peirce decomposition, 571
elementary
conic case, 160
multiple
alternative case, 314
elementary cubic Jordan case, 367
Jordan case, 310
singular
alternative case, 116
elementary cubic Jordan case, 364
Jordan case, 303
Peirce projection, 303
Peirce triple, 310
period, 4
permutation matrix, 70
Pfister (quadratic) form, 429
Pfister bilinear form, 429
Picard group, 58
pointed quadratic module, 76
bilinear trace, 76
conjugation, 76
homomorphism, 76
invertible element, 299
isotope, 299
norm, 76
Peirce-one extension, 389
admissible, 391
trace, 76
pointed quadratic space, 76
polynomial function, 85
polynomial law, 86
base change or scalar extension, 86
binary linearization, 93
constant, 102
differential calculus, 94
directional derivative, 95
faithfully flat descent, 239
homogeneous, 88
linearization or polarization, 91
locally finite family, 89
multi-homogeneous, 88
restriction of scalars, 99
Taylor expansion, 94
total derivatives, 93
total linearization, 91
polynomial map, 85
powers of an element
in a unital algebra, 47
pre-co-ordinate pair, 358
isotope, 380
octonionic, 358
pre-composition algebra, 146
primitive hermitian matrices, 29
primitive twisted hermitian matrices, 357
principal open set, 53
projective plane, 11, 444

$\mathbb{Q}$-algebra, 15
quadratic algebra, 125, 159
quadratic étale algebra, 155
over $\mathbb{Z}$, 204
quadratic form, 70
non-degenerate, 75
non-singular, 75
real, 3
regular, 75
splitting field, 430
weakly regular, 75
quadratic map, 70
base change or scalar extension, 72
bilinearization, 70
polar map, 70
quadratic module, 75
homomorphism, 75
hyperbolic pair, 77
isometry, 76
isotropic, 78
isotropic element, 77
totally isotropic submodule, 78
weird, 396
quadratic space, 76
quadratic-linear map, 82
quaternion algebra, 156
of $L$-twisted 2-by-2 matrices, 181
over $\mathbb{Z}$, 615
quaternions
Hamiltonian, 6
conjugation, 7
norm, 7
trace, 7
Hurwitz, 20

radical, 571
of a (skew-)symmetric bilinear map, 71
of a quadratic map, 71
rank
of a torus, 570
of elements in cubic Jordan algebras, 427

rank decomposition, 63
real algebra, 2
  alternative, 5
  homomorphism, 2
  squaring, 3
  structure constants, 2
  unital, 2
real division algebra, 2
real Jordan algebra, 30
  euclidean, 30
  exceptional, 31
  fully linearized Jordan identity, 35
  Jordan identity, 30
  Jordan triple product, 38
  special, 31
  $U$-operator, 38
real quadratic form
  negative definite, 3
  permitting composition, 5
  positive definite, 3
real quadratic map, 3
  bilinearization, 3
  polar map, 3
real sedenions, 159, 203
reflection, 525
regular
  bilinear form, 74
  cubic alternative algebra, 448
  cubic array, 320
  involutorial system of the second kind, 486
residually big, 499
restriction of scalars, 15
right alternative law, 109
right multiplication
  extended, 122
right multiplication operator, 44
root datum, 572
root system, 525
  basis, 526
  irreducible, 526
  isomorphism, 526
root system $\mathsf{D}_4$, 26
root system $\mathsf{E}_8$, 25
Rost invariant, 604
round form, 419

scalar polynomial law
  form, 89
Schafer's isotopy theorem, 121
second Tits construction, 482
  external, 479
  formal, 482
  internal, 475
sedenions, 157, 159, 203
semi-linear polynomial square, 99
  commutative, 100
semi-local ring, 79
semisimple
  group scheme, 571, 572
separable Nullstellensatz, 237
sesquilinear form, 163
  base change or scalar extension, 164
  exterior power, 168
  regular, 167
sesquilinear module, 164
  homomorphism, 164
  isometry, 164
sesquilinear space, 167
sextonions, 158
simple
  para-quadratic algebra, 261
simply connected, 572
skew-symmetric bilinear form
  regular, 74
smooth, 236
special orthogonal group, 575
split
  Freudenthal algebra, 406
split algebraic element, 49
splitting field, 200
Springer form, 461
strictly valid identity, 320
structure group
  of a Jordan algebra, 295
  of an alternative algebra, 121
subalgebra, 2, 43
  generated by a subset, 44
  nuclear, 48
  unital, 2, 47
    generated by a subset, 47
subfunctor, 97
submodule
  pure, 490
switch, 66
symmetric matrix product, 29
symmetric or skew-symmetric bilinear form
  regular, 74
symmetric product, 253
symplectic Lie algebra, 529

ternary cyclicity convention, 357
torsor, 237
trace
  of a conic algebra, 124

of a cubic euclidean Jordan matrix algebra, 31
transitive action, 186, 296, 399, 428, 443, 461
twist of an involution, 67
twisted dual of a right module, 163

unimodular element, 58, 126
unital isotope, 120
unital structure group of an alternative algebra, 122

versor, 7

weight space decomposition, 571
Witt cancellation, 81

Yoneda Lemma, 208

$\mathbb{Z}$-algebra, 15
$\mathbb{Z}$-structure, 16
  linear, 36
  quadratic, 38, 277
Zariski-closed set, 53
Zariski-open set, 53
zero divisor, 48, 140