Holger P. Petersson and Michel L. Racine

Octonions and Albert algebras over commutative rings

Preliminary version

October 23, 2019

Springer
## Contents

1. **Prologue: the ancient protagonists** .................................................. 1
   1. The Graves-Cayley octonions .................................................. 1
   2. Cartan-Schouten bases .................................................. 7
   3. Unital subalgebras of $\mathcal{O}$ and their $\mathbb{Z}$-structures .......... 11
   4. Maximal quaternionic and octonionic $\mathbb{Z}$-structures ................. 16
   5. The euclidean Albert algebra ........................................... 24
   6. $\mathbb{Z}$-structures of unital real Jordan algebras ....................... 31
   7. The Leech lattice .................................................. 37

2. **Foundations** ............................................................................... 39
   8. The language of non-associative algebras ................................... 39
   9. Unital algebras .......................................................... 42
   10. Scalar extensions ......................................................... 46
   11. Involutions .............................................................. 56
   12. Quadratic maps .......................................................... 60
   13. Polynomial laws .......................................................... 68

3. **Alternative algebras** .................................................................. 85
   14. Basic identities and invertibility ......................................... 85
   15. Strongly associative subsets ............................................... 89
   16. Homotopes ................................................................. 91
   17. Isotopy involutions ....................................................... 96
   18. Finite-dimensional alternative algebras over fields ...................... 101

4. **Composition algebras** ................................................................ 103
   19. Conic algebras ........................................................... 103
   20. Conic alternative algebras .................................................. 110
   21. The Cayley-Dickson construction ........................................ 113
   22. Basic properties of composition algebras ............................... 120
   23. Hermitian forms .......................................................... 133
   24. Ternary hermitian spaces .................................................. 136
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 Reduced composition algebras</td>
<td>146</td>
</tr>
<tr>
<td>26 Norm equivalences and isomorphisms</td>
<td>157</td>
</tr>
<tr>
<td>27 Affine schemes</td>
<td>167</td>
</tr>
<tr>
<td>28 Faithfully flat étale splittings of composition algebras</td>
<td>184</td>
</tr>
<tr>
<td>5 Jordan algebras</td>
<td>205</td>
</tr>
<tr>
<td>29 Linear Jordan algebras</td>
<td>205</td>
</tr>
<tr>
<td>30 Para-quadratic algebras</td>
<td>209</td>
</tr>
<tr>
<td>31 Jordan algebras and basic identities</td>
<td>218</td>
</tr>
<tr>
<td>32 Power identities</td>
<td>231</td>
</tr>
<tr>
<td>33 Inverses, isotopes and the structure group</td>
<td>237</td>
</tr>
<tr>
<td>34 The Peirce decomposition</td>
<td>249</td>
</tr>
<tr>
<td>6 Cubic Jordan algebras</td>
<td>263</td>
</tr>
<tr>
<td>35 From cubic norm structures to cubic Jordan algebras</td>
<td>263</td>
</tr>
<tr>
<td>36 Building up cubic norm structures</td>
<td>285</td>
</tr>
<tr>
<td>37 Elementary idempotents and cubic Jordan matrix algebras</td>
<td>295</td>
</tr>
<tr>
<td>References</td>
<td>459</td>
</tr>
</tbody>
</table>
Chapter 1
Prologue: the ancient protagonists

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

1. The Graves-Cayley octonions

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

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

$$\mathbb{C}^3 \times \mathbb{C}^3 \rightarrow \mathbb{C}, \quad (u,v) \mapsto \bar{u}^t v,$$

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

$$(u \times v)^t w = \det(u,v,w) \quad (u,v,w \in \mathbb{C}^3).$$

The cross product is complex linear in each variable and alternating; more precisely, $u \times v = 0$ if and only if $u$ and $v$ are linearly dependent; in particular $u \times u = 0$. Moreover, (1) implies that the expression $(u \times v)^t w$ remains invariant under cyclic permutations of its arguments. The cross product of the unit vectors is determined by the formula

$$e_i \times e_j = e_l \quad \text{for} \quad (ijl) \in \{(123),(231),(312)\}.$$
The specification of the indices \(i, j, l\) in this formula will henceforth be expressed by saying that it holds for all cyclic permutations \((ijl)\) of \((123)\). Finally, the cross product satisfies the Grassmann identity
\[
(u \times v) \times w = vw' u - uv' v = w \times (v \times u)
\] 
for all \(u, v, w \in \mathbb{C}^3\), which immediately implies the Jacobi identity
\[
(u \times v) \times w + (v \times w) \times u + (w \times u) \times v = 0.
\]

1.2. Real algebras. A detailed dictionary of non-associative algebras will be presented in 8.1 below. For the time being, it suffices to define a real algebra as a vector space \(A\) over the field \(\mathbb{R}\) of real numbers together with an \(\mathbb{R}\)-bilinear product \((x, y) \mapsto xy\) from \(A \times A\) to \(A\) that need neither be associative nor commutative. Nor will \(A\) in general admit an identity element, but if it does, it is said to be unital. A sub-vector space of \(A\) stable under multiplication is called a subalgebra; it is a real algebra in its own right. We speak of a unital subalgebra \(B\) of \(A\) if \(B\) is a subalgebra containing the identity element of \(A\). For \(X, Y \subseteq A\), we denote by \(XY\) the additive subgroup of \(A\) generated by all products \(xy, x \in X, y \in Y\); we always write \(X^2 := XX\) and \(XY := X\{y\}, xY := \{x\}Y\) for all \(x \in X, y \in Y\). If \(A\) and \(B\) are real algebras, we define a homomorphism from \(A\) to \(B\) as a linear map \(h: A \rightarrow B\) preserving products:
\[
h(xy) = h(x)h(y)
\]
for all \(x, y \in A\). A real algebra \(A\) is said to be a division algebra if \(A \neq \{0\}\) and for all \(u, v \in A\), \(u \neq 0\), the equations \(ux = v\) and \(yu = v\) can be solved uniquely in \(A\); if \(A\) has finite dimension (as a vector space over \(\mathbb{R}\)), this is equivalent to the absence of zero divisors: for all \(a, b \in A\), the equation \(ab = 0\) implies \(a = 0\) or \(b = 0\).

Now suppose \(A\) is a finite-dimensional real algebra and let \((e_i)_{1 \leq i \leq n}\) be a basis of \(A\) over \(\mathbb{R}\). Then there is a unique family \((\gamma_{ij})_{1 \leq i, j \leq n}\) of real numbers such that
\[
e_i e_l = \sum_{j=1}^{n} \gamma_{ij} e_i \quad (1 \leq j, l \leq n).
\]
The \(\gamma_{ij}\) are called the structure constants of \(A\) relative to the basis chosen; they determine the multiplication of \(A\) uniquely. But note that different bases of the same algebra may have vastly different structure constants. Given a finite-dimensional real algebra, the objective must be to find a basis with a particularly simple set of structure constants. If \(A\) and \(B\) are two real algebras of the same finite dimension, with bases \((e_i)_{1 \leq i \leq n}\) and \((d_i)_{1 \leq i \leq n}\), respectively, then the linear bijection \(h: A \rightarrow B\) sending \(e_i\) to \(d_i\) for \(1 \leq i \leq n\) is easily seen to be an isomorphism of real algebras if and only if the family of structure constants of \(A\) relative to \((e_i)\) is the same as the family of structure constants of \(B\) relative to \((d_i)\).

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

**DQ**: \( V \times V \rightarrow W, \quad (v_1, v_2) \mapsto Q(v_1 + v_2) - Q(v_1) - Q(v_2). \) (1)

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

For example, given a finite-dimensional real algebra \( A \), the squaring \( \text{sq}: A \rightarrow A, \quad x \mapsto x^2 \) (2) is a quadratic map with bilinearization given by

\[
\text{sq}(x, y) = D\text{sq}(x, y) = xy + yx
\]

for all \( x, y \in A \).

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

**1.4. Defining the Graves-Cayley octonions.** By restricting scalars from \( \mathbb{C} \) to \( \mathbb{R} \), \( \mathbb{O} := \mathbb{C} \oplus \mathbb{C}^3 \)

may be viewed as a real vector space (of dimension 8 whose elements will be written as \( a \oplus u, \ a, u \in \mathbb{C}^3 \). Following Zorn [129, p. 401], we make \( \mathbb{O} \) into a real algebra by the multiplication

\[
(a \oplus u)(b \oplus v) := (ab - \bar{u} \bar{v}) \oplus (\bar{v}a + ub + \bar{u} \times \bar{v}) \quad (a, b \in \mathbb{C}, \ u, v \in \mathbb{C}^3). \quad (1)
\]

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

\[
1_{\mathbb{O}} := 1 \oplus 0 \quad (2)
\]

but is neither commutative nor associative. For example, an easy computation shows

\[
((0 \oplus e_1)(0 \oplus e_2))(0 \oplus e_3i) = (-i) \oplus 0 = -(0 \oplus e_1)((0 \oplus e_2)(0 \oplus e_3i)).
\]

**1.5. Norm, trace and conjugation.** The map \( n_\mathbb{O}: \mathbb{O} \rightarrow \mathbb{R} \) defined by

\[
n_\mathbb{O}(a \oplus u) := \bar{a}a + \bar{u}u = |a|^2 + \bar{u}u \quad (a \in \mathbb{C}, \ u \in \mathbb{C}^3) \quad (1)
\]

is called the norm of \( \mathbb{O} \). It is a positive definite quadratic form whose bilinearization may be written as

\[
n_\mathbb{O}(x, y) = \bar{a}b + \bar{b}a + \bar{u}v + \bar{v}u = 2 \text{Re}(\bar{a}b + \bar{u}v)
\]

for \( x = a \oplus u, \ y = b \oplus v, \ a, b \in \mathbb{C}, \ u, v \in \mathbb{C}^3 \) and hence gives rise to a euclidean scalar product on \( \mathbb{O} \) defined by
\[ (x, y) := \frac{1}{2} n_\mathcal{O}(x, y) = \Re(\bar{a}b + \bar{u}v), \] (3)

making \( \mathcal{O} \) into a real euclidean vector space with corresponding euclidean norm

\[ ||x|| := \langle x, x \rangle = \sqrt{n_\mathcal{O}(x)} = \sqrt{|a|^2 + ||u||^2}. \] (4)

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

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

\[ t_\mathcal{O}(x) := n_\mathcal{O}(1_\mathcal{O}, x) = 2 \Re(a) = a + \bar{a}, \] (5)

and the conjugation of \( \mathcal{O} \), i.e., the linear map \( \iota_\mathcal{O}: \mathcal{O} \to \mathcal{O}, \ x \mapsto \bar{x} := t_\mathcal{O}(x)1_\mathcal{O} - x, \) (6)

which obviously satisfies

\[ \bar{a} \oplus \bar{u} = \bar{a} \oplus (-u) \quad (a \in \mathbb{C}, \ u \in \mathbb{C}^3), \] (7)

leaves the norm invariant:

\[ n_\mathcal{O}(\bar{x}) = n_\mathcal{O}(x) \quad (x \in \mathcal{O}), \] (8)

and has period 2: \( \bar{x} = x \) for all \( x \in \mathcal{O} \). We view

\[ \mathcal{O}^0 := \text{Ker}(t_\mathcal{O}) = \{ x \in \mathcal{O} \mid \bar{x} = -x \} = (i\mathbb{R}) \oplus \mathbb{C}^3. \] (9)

as a euclidean subspace of \( \mathcal{O} \). For \( a \in \mathbb{C}, \ u \in \mathbb{C}^3 \), we use (1.4.1) to compute

\[ (a \oplus u)^2 = (a^2 - \bar{a}u) \oplus (2\Re(a)u) = 2 \Re(a)(a \oplus u) - (|a|^2 + ||u||^2)(1 \oplus 0), \]

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

\[ x^2 - t_\mathcal{O}(x)x + n_\mathcal{O}(x)1_\mathcal{O} = 0. \] (10)

Combining this with (6), we conclude

\[ xx = n_\mathcal{O}(x)1_\mathcal{O} = \bar{x}x, \quad x + \bar{x} = t_\mathcal{O}(x)1_\mathcal{O}. \] (11)

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

\[ x \circ y := xy + yx = t_\mathcal{O}(x)y + t_\mathcal{O}(y)x - n_\mathcal{O}(x, y)1_\mathcal{O}. \] (12)
The process of passing from (10) to (12) will be encountered quite frequently in the present work and is called linearization. We also note

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

(13) for $x = a \oplus u$, $y = b \oplus v$, $a, b \in \mathbb{C}$, $u, v \in \mathbb{O}$ since (1.4.1), (5), (2) yield

$$t_\mathbb{O}(xy) = 2\Re(\bar{a}b - \bar{a}v) = n_\mathbb{O}(\bar{a} \oplus (-u), b \oplus v) = n_\mathbb{O}((x,y)),$$

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

### 1.6. Alternativity.

As we have seen in (1.4) the algebra of Graves-Cayley octonions is not associative. On the other hand, it follows from Exc. 1 below that it is alternative: the associator $[x,y,z] := (xy)z - x(yz)$ is an alternating (trilinear) function of its arguments $x,y,z \in \mathbb{O}$. In particular, the identities

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

hold in all of $\mathbb{O}$. Alternative algebras are an important generalization of associative algebras and will be studied more systematically, under a much broader perspective, in later portions of the book, see particularly Chap. 3 below.

### 1.7. Theorem.

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

**Proof.** As we have seen, the real algebra $\mathbb{O}$ is alternative (1.6) but not associative (1.4). It remains to show that the positive definite quadratic form $n_\mathbb{O}$ permits composition since this immediately implies that $\mathbb{O}$ has no zero divisors, hence is a division algebra (1.2). Accordingly, let $x = a \oplus u$, $y = b \oplus v$, $a, b \in \mathbb{C}$, $u, v \in \mathbb{C}^3$. Then (1.4.1), (1.5.1) yield

$$n_\mathbb{O}(xy) = n_\mathbb{O}((ab - \bar{a}v) \oplus (v\bar{a} + ub + \bar{u} \times \bar{v}))$$

$$= (\bar{a}\bar{b} - \bar{v}u)(ab - \bar{a}v) + (\bar{v}a + \bar{u}b + (u \times v)^t)(v\bar{a} + ub + \bar{u} \times \bar{v})$$

$$= a\bar{a}\bar{b}b - \bar{a}\bar{b}v - \bar{v}u\bar{a}b + \bar{v}u\bar{v}a + \bar{v}v\bar{a}u + \bar{v}v\bar{v}a + \bar{v}(u \times \bar{v}) + \bar{u}va\bar{b}$$

$$+ \bar{u}ub\bar{b} + \bar{u}^t(u \times \bar{v}) + (u \times v)^t\bar{v}a + (u \times v)^tub + (u \times v)^t(u \times \bar{v})$$

Observing (1.1), we obtain

$$\bar{v}(\bar{u} \times \bar{v}) = \bar{u}(\bar{u} \times \bar{v}) = (u \times v)^t\bar{v} = (u \times v)^t\bar{u} + 0,$$

while (1.1) combined with the Grassmann identity (1.13) implies

$$(u \times v)^t(\bar{u} \times \bar{v}) = \bar{v}((u \times v) \times \bar{u}) = \bar{v}uv\bar{u} - \bar{v}uv\bar{v}.$$

Hence the preceding displayed formula reduces to

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

as claimed.
1.8. Remark. The composition formula \( n_\mathcal{O}(xy) = n_\mathcal{O}(x)n_\mathcal{O}(y) \) is bi-quadratic in \( x, y \in \mathcal{O} \) and by (repeated) linearization yields
\[
\begin{align*}
n_\mathcal{O}(x_1y_1,x_2y_2) &= n_\mathcal{O}(x_1,x_2)n_\mathcal{O}(y_1,y_2), \\
n_\mathcal{O}(xy_1,xy_2) &= n_\mathcal{O}(x)n_\mathcal{O}(y_1,y_2), \\
n_\mathcal{O}(x_1y_1,x_2y_2) + n_\mathcal{O}(x_1y_2,x_2y_1) &= n_\mathcal{O}(x_1,x_2)n_\mathcal{O}(y_1,y_2)
\end{align*}
\]
for all \( x, y, x_1, x_2, y_1, y_2 \in \mathcal{O} \).

1.9. A formula for the inverse. Given \( x \neq 0 \) in \( \mathcal{O} \), Thm. 1.7 yields unique elements \( y, z \in \mathcal{O} \) such that \( xy = zx = 1_\mathcal{O} \). In fact, by (1.5.11), we necessarily have
\[
y = z = x^{-1} := \frac{1}{n_\mathcal{O}(x)} \bar{x}.
\]
We call \( x^{-1} \) the inverse of \( x \) in \( \mathcal{O} \).

1.10. The Hamiltonian quaternions. The subspace \( \mathbb{H} := \mathbb{R} \oplus \mathbb{R}^3 \) of \( \mathcal{O} \) is actually a subalgebra since
\[
(\alpha \oplus u)(\beta \oplus v) = (\alpha\beta - u'v) \oplus (\alpha v + \beta u + u \times v). \quad (\alpha, \beta \in \mathbb{R}, u, v \in \mathbb{R}^3)
\]
This algebra is called the algebra of Hamiltonian quaternions. It contains an identity element since \( 1_{\mathbb{H}} := 1_\mathcal{O} \in \mathbb{H} \). Note that the Hamiltonian quaternions can be defined directly, without recourse to the Graves-Cayley octonions, by the product (1) on the real vector space \( \mathbb{R} \oplus \mathbb{R}^3 \). Moreover, the vectors
\[
l_{\mathbb{H}} := 1_\mathcal{O}, \quad i := 0 \oplus e_1, \quad j := 0 \oplus e_2, \quad k := 0 \oplus e_3
\]
form a basis of \( \mathbb{H} \) over \( \mathbb{R} \) in which \( l_{\mathbb{H}} \) acts as a two-sided identity element and, by (1) combined with (1.1.2),
\[
i^2 = j^2 = k^2 = -l_{\mathbb{H}}, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.
\]
Thus we have obtained a basis of the Hamiltonian quaternions with a particularly simple family of structure constants (cf. 1.2).

Restricting the norm, trace, conjugation of \( \mathcal{O} \) to \( \mathbb{H} \), we obtain what we call the norm, trace, conjugation of \( \mathbb{H} \), denoted by \( n_{\mathbb{H}}, t_{\mathbb{H}}, \iota_{\mathbb{H}} \), respectively, which enjoy the same algebraic properties we have derived for the Graves-Cayley octonions in 1.5. By the same token, \( \mathbb{H} \) may also be viewed canonically as a real euclidean vector space. Consulting Thm. 1.7 we now obtain the following result.

1.11. Corollary. The Hamiltonian quaternions \( \mathbb{H} \) form an associative but not commutative real division algebra of dimension four, and the norm of \( \mathbb{H} \) permits composition: \( n_{\mathbb{H}}(xy) = n_{\mathbb{H}}(x)n_{\mathbb{H}}(y) \) for all \( x, y \in \mathbb{H} \).
Proof. The only statement demanding a proof is the assertion that \( \mathbb{H} \) is associative. But this can either be verified directly, or follows immediately from Exc. 1[30] combined with the Jacobi identity (1.1.4). \( \Box \)

Exercises.

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

\[
[x_1,x_2,x_3] = (\det(u_1,u_2,u_3) - \det(u_1,u_2,u_3)) \oplus \left( \sum ((u_1 \times u_2) \times u_3 + (u_1 \times u_3) (u_2 - u_3)) \right),
\]

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

2. **Prove directly, i.e., without recourse to properties of the norm, that \( O \) is a division algebra.**

3. **Norm, trace and conjugation under the product of \( O \).**
   (a) Prove that the conjugation of \( O \) is an algebra involution, so not only \( \bar{x} = x \) but also \( \bar{xy} = \bar{y} \bar{x} \) for all \( x,y \in O \).
   (b) Show that trace and norm of \( O \) satisfy

\[
t_0(xy) = t_0(yx), \quad t_0((xy)z) = t_0(x(yz)), \quad n_0(x,y,z) = n_0(y,x,z)
\]

for all \( x,y,z \in O \).
   (c) Prove \( x(yz) = n_0(x)(y) = (xy)z \) and \( xy := (xy)x = x(yx) = n_0(x,y)x - n_0(x)(y) \) for all \( x,y \in O \).

4. **The Moufang identities.** We will see later (cf. 14.3) that the Moufang identities

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

(cf. Exc. 5[30](c) for a parantheses-saving notation) hold in arbitrary alternative algebras. Give a direct proof for the alternative algebra \( O \) by reducing to the case \( y,z \in \{0\} \oplus \mathbb{C}^3 \) and using as well as proving the cross product identity

\[
(u \times v)u' + (v \times w)v' + (w \times u)w' = \det(u,v,w)1_3
\]

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

2. **Cartan-Schouten bases**

In 1.10 we have exhibited a basis for the Hamiltonian quaternions with a particularly simple family of structure constants. In this section, we will pursue the same objective for the Graves-Cayley octonions. Due to their higher dimension and the lack of associativity, however, matters will be not quite as simple as in the quaternionic case.
2.1. Defining Cartan-Schouten bases (Cartan-Schouten [18]). We define a Cartan-Schouten basis of $\mathcal{O}$ as a basis consisting of the identity element $1_\mathcal{O}$ and additional vectors $u_1, \ldots, u_7 \in \mathcal{O}$ such that the following two conditions are fulfilled, for all $r = 1, \ldots, 7$:

\begin{align*}
u_r^2 &= -1_\mathcal{O}, \quad (1) \\
u_{r+i} + u_{r+3i} &= u_r = -u_{r+3i}u_{r+i} \quad (i = 1, 2, 4), \quad (2)
\end{align*}

where the indices in (2) are to be reduced mod 7. We then put $u_0 := 1_\mathcal{O}$, allowing us to write Cartan-Schouten bases as $(u_r)_{0 \leq r \leq 7}$. By (1) and (1.5.10), we have $t_\mathcal{O}(u_r) = 0$, hence $u_r \in \mathcal{O}^0$ for $1 \leq r \leq 7$. The conscientious reader may wonder whether equations (1), (2) really define a multiplication table for the basis chosen, i.e., whether all possible products between the basis vectors are well defined and uniquely determined by the preceding conditions. That this is indeed the case will be settled affirmatively in Exc. 5 below. We also note by Exc. 6 that Cartan-Schouten bases are orthonormal.

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

Proof. Let $(u_1, u_2)$ be a pair of orthonormal vectors in the seven-dimensional euclidean vector space $\mathcal{O}^0$. Then (1.5.13) yields

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

hence $u_1 u_2 \in \mathcal{O}^0$. Now let $u_3 \in \mathcal{O}^0$ be an orthonormal vector that is perpendicular to $u_1$, $u_2$, and $u_1 u_2$. Then Exc. 8 shows that $u_0 = 1_\mathcal{O}, u_1, u_2, u_3, u_r := u_{r-3} u_{r-2} (4 \leq r \leq 7)$ make up a Cartan-Schouten basis of $\mathcal{O}$. \(\square\)

There is a remarkable interplay between Cartan-Schouten bases and projective planes that provides a first glimpse at the profound connection between non-associative algebras and geometry; for more on this fascinating topic, we refer the reader to Faulkner [30]. Here we only sketch some details.

2.3. Incidence geometries. An incidence geometry $\mathcal{G}$ consists of

(i) two disjoint sets $\mathcal{P} = \mathcal{P}(\mathcal{G})$, whose elements are called points, and $\mathcal{L} = \mathcal{L}(\mathcal{G})$, whose elements are called lines,

(ii) a relation between points and lines, i.e., a subset $I \subseteq \mathcal{P} \times \mathcal{L}$.

If $P \in \mathcal{P}$, $\ell \in \mathcal{L}$ satisfy $(P, \ell) \in I$, we write $P | \ell$ or $\ell \not| P$ and say $P$ is incident to $\ell$ (or $P$ lies on $\ell$, or $\ell$ passes through $P$). If several points all lie on a single line, they are said to be collinear.

2.4. Projective planes. An incidence geometry $\mathcal{G}$ as in 2.3 is called a projective plane if

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

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

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

In the standard visualization of the Fano plane (see Fig. 1 below), its seven lines are represented by (i) the three sides, (ii) the three medians, and (iii) the inner circle of an isosceles triangle, while its seven points are located and numbered as shown. The entire picture fits into a directed graph whose nodes agree with the points of the Fano plane and give rise to subdivisions of the seven lines, yielding fifteen edges directed in the way indicated. The key feature of this construction is that it allows to recover the Graves-Cayley octonions on the free real vector space generated by the nodes \( u_r \), \( 1 \leq r \leq 7 \), and an additional element \( u_0 \). In order to accomplish this, it suffices to define a multiplication on the basis vectors that enjoys the characteristic properties \( \{ 2.1.1 \}, \{ 2.1.2 \} \) of Cartan-Schouten bases. We do so by setting \( u_0 u_r := u_r =: u_r u_0 \) for \( 0 \leq r \leq 7 \), \( u_0^2 = -u_0 \) for \( 1 \leq r \leq 7 \), and by defining \( u_r u_s \) for \( 1 \leq
\[ r,s \leq 7, \ r \neq s, \] in the following way: let \( u_t, \ 1 \leq t \leq 7, \) be the third point on the line containing \( u_r \) and \( u_s. \) If, after an appropriate cyclic permutation of the indices \( r,s,t, \) the orientation of the edge joining \( u_r \) and \( u_s \) leads from \( u_r \) to \( u_s \) (resp. from \( u_s \) to \( u_r \)), we put \( u_r u_s := u_t \) (resp. \( u_r u_s := -u_t \)). Then (2.1.1) holds by definition, while (2.1.2) can be verified in a straightforward manner.

**2.6. Symmetries of the Graves-Cayley octonions.** One of the most important features of the Graves-Cayley octonions is the fact that, in spite of their non-associative character, they have lots of symmetries. More specifically, we consider their automorphism group, denoted by \( \text{Aut}(\mathcal{O}) \) and defined as the set of bijective linear maps \( \varphi : \mathcal{O} \to \mathcal{O} \) satisfying \( \varphi(xy) = \varphi(x)\varphi(y) \) for all \( x,y \in \mathcal{O}; \) it is obviously a subgroup of \( \text{GL}(\mathcal{O}) \), the full linear group of the real vector space \( \mathcal{O}. \) We know from Exc. 7 below that \( \text{Aut}(\mathcal{O}) \) canonically embeds as a closed subgroup into the orthogonal group \( O(\mathcal{O}) \cong O_7(\mathbb{R}) \) of the euclidean vector space \( \mathcal{O}^0, \) a compact real Lie group of dimension 21, and hence is a compact real Lie group in its own right \[19, \text{Cor. of Prop. IV.XIV.2}. \] Our claim that \( \mathcal{O} \) has lots of symmetries will now be corroborated by the formula

\[ \dim (\text{Aut}(\mathcal{O})) = 14. \] \hfill (1)

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

First of all, the automorphism group of \( \mathcal{O} \) acts simply transitively on the set of Cartan-Schouten bases of \( \mathcal{O}. \) Each Cartan-Schouten basis, in turn, by Exc. 6 below, is completely determined by an element of

\[ X^0 := \{(u_1,u_2,u_3) \in X \mid \langle u_1 u_2, u_3 \rangle = 0 \}, \] \hfill (2)

where \( X \) stands for the set of orthonormal systems of length 3 in the euclidean vector space \( \mathcal{O}^0 \cong \mathbb{R}^7. \) Thus we have \( \dim (\text{Aut}(\mathcal{O})) = \dim (X^0). \) On the other hand, the orthogonal group \( O_7(\mathbb{R}) \) acts transitively on \( X, \) and for the first three unit vectors \( e_1,e_2,e_3 \in \mathbb{R}^7, \) the isotropy group of \( (e_1,e_2,e_3) \in X \) identifies canonically with \( O_4(\mathbb{R}). \) Hence

\[ \dim (X) = \dim (O_7(\mathbb{R})) - \dim (O_4(\mathbb{R})) = \frac{7 \cdot 6}{2} - \frac{4 \cdot 3}{2} = 21 - 6 = 15. \]

But \[2\] shows that \( X^0 \) is a “hyper-surface” in \( X, \) which gives

\[ \dim (\text{Aut}(\mathcal{O})) = \dim (X^0) = \dim (X) - 1 = 14, \]

as claimed in (1).

**Exercises.**
6. Characterization of Cartan-Schouten bases. Prove for a family \((u_r)_{0 \leq r \leq 7}\) of elements in \(\mathcal{O}\) that the following conditions are equivalent.

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

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

\[
u_r^2 = -1_{\mathcal{O}} = (u_r u_{r+1}) u_{r+3} = u_r (u_{r+1} u_{r+3}) \quad (1 \leq r \leq 7, \text{indices mod 7}).\]  

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

\[
u_r (u_{r+1}) = u_r, \quad (1 \leq r \leq 7, i = 1, 2, 4, \text{indices mod 7}).\]  

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

\[
u_3 (u_1 u_2) = 0, \quad u_r = u_{r-3} u_{r-2} \quad (4 \leq r \leq 7).\]  

In this case, \((u_r)_{1 \leq r \leq 7}\) is an orthonormal basis of \(\mathcal{O}^0\).

7. The algebra \(\mathcal{O}^+\). The real vector space \(\mathcal{O}\) becomes a commutative real algebra \(\mathcal{O}^+\) under the multiplication

\[x \cdot y := \frac{1}{2} x o y + \frac{1}{2} \nu_0 (x) y - \frac{1}{2} \nu_0 (y) x - \frac{1}{2} \nu_0 (x, y) 1_{\mathcal{O}} \quad (x, y \in \mathcal{O})\]

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

3. Unital subalgebras of \(\mathcal{O}\) and their \(\mathbb{Z}\)-structures

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

3.1. The general set-up. (a) Throughout this section, we fix a real vector space \(V\) of finite dimension \(n\) and assume most of the time, but not always, that \(V\) is equipped with a positive definite quadratic form \(q: V \to \mathbb{R}\). Speaking of \((V, q)\) as a positive definite real quadratic space under these circumstances, we may and always will regard \(V\) as a euclidean vector space with the scalar product \(\langle x, y \rangle := \frac{1}{2} q(x, y)\) and denote the associated euclidean norm by \(\|x\| = \sqrt{\langle x, x \rangle} = \sqrt{q(x)}\), for all \(x, y \in V\).
(b) We also denote by \( \mathbb{D} \) one of the unital subalgebra \( \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O} \) of \( \mathbb{O} \). Via restriction, \( \mathbb{D} \) inherits from \( \mathbb{O} \) the data norm, trace, bilinearized norm and conjugation, denoted by \( n_{\mathbb{D}}, t_{\mathbb{D}}, Dn_{\mathbb{D}}, t_{\mathbb{D}} \), respectively, that mutatis mutandis enjoy the various properties assembled in \([1.5]\) for the Graves-Cayley octonions. These properties will be freely used here without further ado. In particular, \((\mathbb{D}, n_{\mathbb{D}})\) is a positive definite real quadratic space as in (a), allowing us to regard \( \mathbb{D} \) as a euclidean subspace of \( \mathbb{O} \) in a natural way.

3.2. Algebras over \( \mathbb{Z} \) and \( \mathbb{Q} \). There is nothing special about the base field \( \mathbb{R} \) in the definition of an algebra. It may be replaced by any commutative associative ring of scalars, a point of view adopted systematically in the remainder of the book. For example, we may pass to the field \( \mathbb{Q} \) of rational numbers or the ring \( \mathbb{Z} \) of rational integers: by a \( \mathbb{Q} \)-algebra (resp. a \( \mathbb{Z} \)-algebra) we mean \( \mathbb{Q} \) vector space (resp. an additive abelian group) \( A \) together with a \( \mathbb{Q} \)-bilinear (resp. a bi-additive) map from \( A \times A \) to \( A \). The conventions of \([1.2]\) carry over to this modified setting virtually without change. Any real algebra may be viewed as a \( \mathbb{Q} \)-algebra (resp. a \( \mathbb{Z} \)-algebra) by restriction of scalars.

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

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

is a unital commutative associative subalgebra, for all \( x \in A \). Hence it makes sense to talk about the minimum polynomial of \( x \) (over \( K \)) in its capacity as an element of \( K[t] \). It will be denoted by \( \mu_x \), or \( \mu^K_x \) to indicate dependence on \( K \), and is the unique monic polynomial in \( K[t] \) that generates the ideal of all polynomials in \( K[t] \) killing \( x \).

The preceding considerations apply in particular to \( K = \mathbb{R} \) and the real algebra \( \mathbb{D} \); indeed, \( \mathbb{D} \) is power-associative since, for \( x \in \mathbb{D} \), we may invoke \([1.5.10]\) to conclude that \( \mathbb{R}[x] = \mathbb{R}1_D + \mathbb{R}x \subseteq \mathbb{D} \) is a unital commutative associative subalgebra of dimension at most 2. Moreover, again by \([1.5.10]\),

\[
\mu_x = t^2 - t_D(x)t + n_D(x) \iff x \notin \mathbb{R}1_D,
\]

while, of course, \( \mu_{\alpha 1_D} = t - \alpha \) for \( \alpha \in \mathbb{R} \).

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

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


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

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

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

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

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

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

(c) Let $A$ be a finite-dimensional unital $\mathbb{R}$-algebra. A lattice $L$ in $A$ is said to be unital if $1_A \in L$. Note in particular that a unital integral quadratic lattice $L \subseteq \mathbb{D}$ satisfies $q_\mathbb{D}(L) \subseteq \mathbb{Z}$ and is stable under conjugation; in particular, the minimum polynomial of $x \in L$ by $3.5$ has integer coefficients, so $L$ consists entirely of integral elements.

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

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

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

3.8. Proposition. Let $A$ be a finite-dimensional unital power-associative real algebra, $M$ a $\mathbb{Z}$-structure of $A$ and $x \in \mathbb{Q}M \subseteq A$. Then $\mu_x^\mathbb{R} = \mu_x^\mathbb{Q}$, so the minimum polynomial of $x$ over $\mathbb{R}$ agrees with the minimum polynomial of $x$ over $\mathbb{Q}$. In particular, it belongs to $\mathbb{Q}[t]$. 

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

Proof. Unitality being obvious, it remains to show $n_{\mathcal{D}}(x) \in \mathbb{Z}$ for all $x \in M$. First of all, $\mathbb{Q}M$ is a finite-dimensional unital power-associative $\mathbb{Q}$-algebra containing $x$, and $\mu_x$ as given in 3.3 by Prop. 3.8 is the minimum polynomial of $x$ over $\mathbb{Q}$. On the other hand, let $\mathbb{Z}[x] = \sum_{n \geq 0} \mathbb{Z}x^n$ be the unital subalgebra of $M$ generated by $x$. Since $M$ is finitely generated as a $\mathbb{Z}$-module, so is $\mathbb{Z}[x] \subseteq M$. Thus $x$ is integral over $\mathbb{Z}$ (Prop. 33.2). By Prop. 33.2 again and (3.3.2), this implies $n_{\mathcal{D}}(x) \in \mathbb{Z}$, as claimed. \qed

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

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

\[ Dq(E) := (q(e_i,e_j))_{1 \leq i,j \leq n} \in \text{Mat}_n(\mathbb{R}) \]  \hspace{1cm} (1)

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

\[ Dq(E^S) = S Dq(E) S. \]  \hspace{1cm} (2)

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

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

\[ \det(L) := \det \left( Dq(E) \right) \]

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

Proof. Since $Dq(E)$ belongs to $\text{Mat}_n(\mathbb{Z})$, its determinant is an integer, which must be positive since $Dq(E)$ is positive definite. The transition matrix from $E$ to another basis $E'$ of $V$ associated with $L$ not only has integral coefficients but is also unimodular, i.e., has determinant $\pm 1$. Now 3.10(2) shows $\det(Dq(E')) = \det(Dq(E))$. \qed

3.12. The discriminant. Let $L$ be an integral quadratic lattice of $V$. The quantity $\det(L)$ exhibited in Prop. 3.11 is called the discriminant of $L$; it is a positive integer.
By contrast, the non-zero (possibly negative) integer
\[ \text{disc}(L) := (-1)^{\frac{1}{2}} \det(L) \]
is called the discriminant of \( L \). By a unimodular integral quadratic lattice of \( V \) we mean an integral quadratic lattice of discriminant \( \pm 1 \).

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

**Proof.** Let \( E \) (resp. \( E' \)) be an \( \mathbb{R} \)-basis of \( V \) associated with \( L \) (resp. \( L' \)) and \( S \) the transition matrix from \( E \) to \( E' \). Then \( S \in \text{Mat}_n(\mathbb{Z}) \cap \text{GL}_n(\mathbb{R}) \), and the Elementary Divisor Theorem [46, Thm. 3.8] implies that there exist \( P, Q \in \text{GL}_n(\mathbb{Z}) \) and a chain of successive non-zero integral divisors \( d_1 \mid \cdots \mid d_n \) satisfying
\[ S = P \text{diag}(d_1, \ldots, d_n) Q. \]
Replacing \( E' \) by \( E' T := Q^{-1} \), and \( E \) by \( E P \), we may assume \( S = \text{diag}(d_1, \ldots, d_n) \).

With \( E = (e_1, \ldots, e_n) \) this implies \( E' = E S = (d_1 e_1, \ldots, d_n e_n) \), and \( L/L' \cong (\mathbb{Z}/d_1 \mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n \mathbb{Z}) \) is finite of order \( \prod_{i=1}^n |d_i| \). On the other hand, applying Prop. 3.11 and (3.10.2), we conclude
\[ \text{disc}(L') = (-1)^{\frac{1}{2}} \det(Dq(E')) = (-1)^{\frac{1}{2}} \left( \prod_{i=1}^n d_i \right)^2 \det(Dq(E)) = \left[ \frac{L}{L'} \right]^2 \text{disc}(L), \]
as claimed. \( \square \)

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

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

**3.16. Examples.** Let \( M \) be a \( \mathbb{Z} \)-structure and \( E \) an orthonormal basis of \( A \) (as a euclidean real vector space). If \( E \) is associated with \( M \), then (3.10.1) shows \( Dn_A(E) = 2 \cdot 1_r, r := \dim_{\mathbb{R}}(A) \), and we conclude
\[ \text{disc}(M) = (-1)^{\frac{1}{2}} 2^r. \] (1) \( \square \)

We now consider a number of specific cases.

(a) By Exc. 10 below, \( M := \mathbb{Z} \) is the unique \( \mathbb{Z} \)-structure of \( A := \mathbb{R} \), and we have \( \text{disc}(\mathbb{Z}) = 2 \).

(b) The Gaussian integers \( \text{Ga}(\mathbb{C}) := \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i \) are a \( \mathbb{Z} \)-structure of \( A := \mathbb{C} \), and
we have \( \text{disc}(\text{Ga}(\mathbb{C})) = -2^2 = -4 \). The Gaussian integers are the integral closure of \( \mathbb{Z} \) in \( \mathbb{C} \) (Neukirch [89, Thm. 1.5]), hence by Cor. 3.9 are a maximal \( \mathbb{Z} \)-structure.

(c) In (1.10.1) we have exhibited an orthonormal basis \( (1_{\mathbb{H}}, i, j, k) \) of \( A := \mathbb{H} \), with structure constants by (1.10.3) equal to \( \pm 1 \). Thus

\[
\text{Ga}(\mathbb{H}) := \mathbb{Z}1_{\mathbb{H}} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k
\]

(2) \( \text{GARA} \)

is a \( \mathbb{Z} \)-structure of \( \mathbb{H} \) having discriminant \( \text{disc}(\text{Ga}(\mathbb{H})) = -2^4 = -16 \), called the Gaussian integers of \( \mathbb{H} \).

(d) Let \( E = (u_r)_{0 \leq r \leq 7} \) be a Cartan-Schouten basis of \( A := \mathbb{O} \). From Exc. 6 we deduce that \( E \) is an orthonormal basis of \( \mathbb{O} \), while (2.1.1), (2.1.2) show that the corresponding structure constants are \( \pm 1 \). Hence

\[
\text{Ga}(\mathbb{O}) := \text{Ga}_E(\mathbb{O}) := \bigoplus_{r=0}^{7} \mathbb{Z}u_r
\]

(3) \( \text{GAGC} \)

is a \( \mathbb{Z} \)-structure of \( \mathbb{O} \) having discriminant \( \text{disc}(\text{Ga}(\mathbb{O})) = 2^8 = 256 \), called the Gaussian integers of \( \mathbb{O} \) relative to \( E \).

Exercises.

8. Prove for an additive subgroup \( L \subseteq V \) that the following conditions are equivalent.
   (i) \( L \) is a lattice.
   (ii) \( L \) spans \( V \) as a real vector space and is a free abelian group of rank at most \( \text{dim}_\mathbb{R}(V) \).
   (iii) There are lattices \( L_0, L_1 \subseteq V \) such that \( L_0 \subseteq L \subseteq L_1 \).

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

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

4. Maximal quaternionic and octonionic \( \mathbb{Z} \)-structures

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

4.1. Towards the Hurwitz \( \mathbb{Z} \)-structure of \( \mathbb{H} \). Starting out from the orthonormal basis \( (1_{\mathbb{H}}, i, j, k) \) of \( \mathbb{H} \) exhibited in (1.10.2), we put

\[
h := \frac{1}{2} (1_{\mathbb{H}} + i + j + k) \in \mathbb{H}
\]

(1) \( \text{HIJK} \)

and note
4 Maximal quaternionic and octonionic \( Z \)-structures

\[
n_{\mathbb{H}}(h) = t_{\mathbb{H}}(h) = n_{\mathbb{H}}(i, h) = n_{\mathbb{H}}(j, h) = n_{\mathbb{H}}(k, h) = 1.
\]

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

\[
\mathbb{C} := \mathbb{R}[i] = \mathbb{R}1_{\mathbb{H}} \oplus \mathbb{R}i
\]

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

\[
\mathbb{H} = \mathbb{C} \oplus \mathbb{C}h
\]

as a direct sum of subspaces. To see this, it suffices to show that the sum on the right of (4.1) is direct, so let \( u, v \in \mathbb{C} \) and suppose \( u = vh \). If \( v \neq 0 \), then \( h = v^{-1}u \in \mathbb{C} \), a contradiction. Thus \( u = v = 0 \), as desired. Note that

\[
\text{Ga}(\mathbb{C}) = \mathbb{Z}[i] = \mathbb{Z}1_{\mathbb{H}} \oplus \mathbb{Z}i
\]

after the identification carried out in (3).

4.2. Theorem (Hurwitz [40]). With the notation and assumptions of 4.1

\[
\text{Hur}(\mathbb{H}) := \text{Ga}(\mathbb{C}) \oplus \text{Ga}(\mathbb{C})h
\]

is a \( Z \)-structure and a maximal integral quadratic lattice of \( \mathbb{H} \), called its \( Z \)-structure

of (or simply the) Hurwitz quaternions. \( \text{Hur}(\mathbb{H}) \) contains the Gaussian integers of \( \mathbb{H} \) as a sub-
\( Z \)-structure and has discriminant 4:

\[
\text{Ga}(\mathbb{H}) \subseteq \text{Hur}(\mathbb{H}), \quad \text{disc } (\text{Hur}(\mathbb{H})) = 4.
\]

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

Proof. Since \( \mathbb{H} \) is a division algebra by Cor. 1.11, the map \( \mathbb{H} \to \mathbb{H}, x \mapsto xh \), is bijective. Combining (4.1.4), (4.1.5) with (1), we therefore conclude that \( M := \text{Hur}(\mathbb{H}) \subseteq \mathbb{H} \) is a unital lattice and that \((1_{\mathbb{H}}, i, h, ih)\) is an \( \mathbb{R} \)-basis of \( \mathbb{H} \) associated with \( M \).

Next we prove that \( M \) is closed under multiplication. Let \( u \in \text{Ga}(\mathbb{C}) \). Then (1.5.12) implies \( uh + hu = t_{\mathbb{H}}(u|h) + t_{\mathbb{H}}(h|u) - n_{\mathbb{H}}(u, h)1_{\mathbb{H}} \), where the coefficients of the linear combination on the right by (4.1.2) are all integers. Hence \( M = \text{Ga}(\mathbb{C}) \oplus h\text{Ga}(\mathbb{C}) \). Combining this with (1.5.10), (4.1.2), we obtain

\[
\text{Ga}(\mathbb{C})h\text{Ga}(\mathbb{C})h \subseteq \text{Ga}(\mathbb{C})\text{Ga}(\mathbb{C}) + \text{Ga}(\mathbb{C})\text{Ga}(\mathbb{C})h^2
\]

\[
= \text{Ga}(\mathbb{C}) + \text{Ga}(\mathbb{C})(h - 1_{\mathbb{H}}) \subseteq \text{Ga}(\mathbb{C}) \oplus \text{Ga}(\mathbb{C})h = M.
\]

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

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

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

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

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

It remains to show that $M$ is a maximal integral quadratic lattice of $\mathbb{H}$, which we leave as an exercise (Exc. 12).

**4.3. Remark.** The Hurwitz quaternions are endowed with a rich arithmetic structure that has been investigated extensively in the literature. For example, it is possible to derive Jacobi’s famous formula [21] for the number of ways a positive integer can be expressed as a sum of four (integral) squares in a purely arithmetic fashion by appealing to properties of the Hurwitz quaternions [20, p. 335]. The reader may consult Brandt [14] or Conway-Smith [20, Ch. 5] for further details on the subject. There are also profound connections with the theory of automorphic forms, cf. Krieg [64] for a systematic and essentially self-contained study of this topic.

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

**4.4. Towards the Coxeter octonions.** In 1.10 we have defined the Hamiltonian quaternions $\mathbb{H}$ explicitly as a unital subalgebra of $\mathbb{O}$. For our subsequent considerations, it will be important to select a different realization of this kind, depending on the choice of a Cartan-Schouten basis $E = (u_r)_{0 \leq r \leq 7}$ of $\mathbb{O}$ that will remain fixed throughout the rest of this section. Recall from Exc. 6 (c) that $E$ is an orthonormal basis of $\mathbb{O}$ obeying the multiplication rules (2.1.2) which may be conveniently read off from Fig. 1 in 2.5 above.

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

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

as a unital subalgebra of $\mathbb{O}$ under the matching $1_\mathbb{H} = 1_\mathbb{O}, i = u_1, j = u_2, k = u_4$. This obviously implies
4 Maximal quaternionic and octonionic $\mathbb{Z}$-structures

$\text{Ga}(\mathbb{H}) = \mathbb{Z}_{12} \oplus \mathbb{Z}_{u_{1}} \oplus \mathbb{Z}_{u_{2}} \oplus \mathbb{Z}_{u_{4}}$ (2) \text{GACS}

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

$p := \frac{1}{2}(1_{O} + u_{1} + u_{2} + u_{3}) \in O$ (3) \text{BFEL}

and note

$u_{1}p = \frac{1}{2}(-1_{O} + u_{1} + u_{4} + u_{7})$, (4) \text{ONEL}

$u_{2}p = \frac{1}{2}(-1_{O} + u_{2} - u_{4} + u_{5})$, (5) \text{TWOL}

$u_{3}p = \frac{1}{2}(-1_{O} + u_{3} - u_{5} - u_{7})$, (6) \text{THRL}

$u_{4}p = \frac{1}{2}(-u_{1} + u_{2} + u_{4} - u_{6})$ (7) \text{FOUL}

as well as

$n_{O}(p) = n_{O}(u_{1}, p) = n_{O}(u_{2}, p) = n_{O}(u_{3}, p) = 1, \quad n_{O}(u_{4}, p) = 0$. (8) \text{ENTO}

We also claim

$\mathcal{O} = \mathbb{H} \oplus \mathbb{H}p$, (9) \text{DECO}

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

4.5. Theorem (Coxeter [21]). With the notation and assumptions of 4.4

$\text{Cox}(\mathcal{O}) := \text{Cox}_{E}(\mathcal{O}) := \text{Ga}(\mathbb{H}) \oplus \text{Ga}(\mathbb{H})p$ (1) \text{COXGC}

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

$E' := (1_{O}, u_{1}, u_{2}, u_{4}, p, u_{1}p, u_{2}p, u_{4}p)$ (2) \text{BECO}

is a an $\mathbb{R}$-basis of $\mathcal{O}$ associated with $\text{Cox}(\mathcal{O})$.

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

Now we show that the lattice $M$ is integral quadratic. Indeed, from (4.4.8) we obtain $n_{O}(\text{Ga}(\mathbb{H}), p) \subseteq \mathbb{Z}$. But then, given $u, v \in \text{Ga}(\mathbb{H})$, we may apply Exc. 3(c) as well as Thm. 1.7 and (4.4.3) to conclude

$n_{O}(u + vp) = n_{O}(u) + n_{O}(u, vp) + n_{O}(vp) = n_{O}(u) + n_{O}(\bar{v}u, p) + n_{O}(v) \in \mathbb{Z}$,
as claimed. Moreover, consulting \([4.4.3]−[4.4.7]\), we see that \(Ga(\mathcal{O}) \subseteq M\), so \(M\) contains the Gaussian integers of \(\mathcal{O}\).

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

\[
\begin{align*}
Ga(\mathbb{H}) (Ga(\mathbb{H})\mathfrak{p}) & \subseteq M, \\
(Ga(\mathbb{H})\mathfrak{p}) Ga(\mathbb{H}) & \subseteq M, \\
(Ga(\mathbb{H})^2) & \subseteq M.
\end{align*}
\]

(3) \text{GAGAL} \hspace{1cm} (4) \text{GALGA} \hspace{1cm} (5) \text{GALGAL}

Noting that \(M\) is a unital integral quadratic lattice, we first let \(u \in Ga(\mathbb{H})\) and apply \((1.5.12)\) to obtain

\[
\begin{align*}
u \mathfrak{p} + u \mathfrak{p} & = t_\mathcal{O}(u)\mathfrak{p} + t_\mathcal{O}(u)\mathfrak{p}u - n_\mathcal{O}(u,\mathfrak{p})1_\mathcal{O} = (u - n_\mathcal{O}(u,\mathfrak{p})1_\mathcal{O}) + t_\mathcal{O}(u)\mathfrak{p},
\end{align*}
\]

which in view of \((1.5.6)\) implies

\[
\begin{align*}
u \mathfrak{p} + u \mathfrak{p} & = t_\mathcal{O}(u)\mathfrak{p} \mod Ga(\mathbb{H}), \\
u \mathfrak{p} & = \bar{u} \mathfrak{p} \mod Ga(\mathbb{H}).
\end{align*}
\]

(6) \text{USYL} \hspace{1cm} (7) \text{LUBAR}

Now let \(u, v \in \mathbb{H}\). Linearizing the first alternative law in \((1.6)\) and using \((6), (7)\) as well as Exc. 3 (a), we obtain

\[
u (p v) \equiv (\nu + u) v - p (\bar{u} v) \equiv t_\mathcal{O}(u) p v - p (\bar{u} v)
\]

\[
\equiv p (\bar{u} v) \equiv (\bar{u} v) p \mod Ga(\mathbb{H}),
\]

hence \(u(pv) \in M\). But then \((3)\) follows since \(u(pv) \equiv u(pv) \mod Ga(\mathbb{H})\) by \((7)\). On the other hand,

\[
(\nu p) u = \nu(p) u + (v p) u - u(v p)
\]

\[
= t_\mathcal{O}(u) p + t_\mathcal{O}(v) u - n_\mathcal{O}(u, v, p) 1_\mathcal{O} - u(v p),
\]

which by \((3)\) proves \((4)\). And finally, by \((7), (5),\) Exc. \((4)\) and Exc. \((3)\) (c),

\[
(\nu p) (p v) \equiv (\bar{u} v) (p v) \equiv p (\bar{u} v) p \equiv n_\mathcal{O}(p, \bar{u} v) p - n_\mathcal{O}(p) \bar{u} v \equiv 0 \mod M,
\]

which proves \((5)\).

It remains to show that \(M\) is unimodular as an integral quadratic lattice. To this end, we compute the matrix \(D_{n_\mathcal{O}(E')}(E')\). Applying \((1.8)\) we obtain \(n_\mathcal{O}(u, \mathfrak{p}, u, \mathfrak{p}) = n_\mathcal{O}(u_r, u_s) = 2 \cdot \delta_{rs}\), so \(D_{n_\mathcal{O}(E')}(E')\) is the block matrix

\[
\begin{pmatrix}
2 \cdot 1_4 & T \\
T^t & 2 \cdot 1_4
\end{pmatrix},
\]

where \(T := (n_\mathcal{O}(u_r, u_s))_{r,s \in \{0,1,2,4\}}\) by \((4.4.3)−(4.4.7)\) has the form
4 Maximal quaternionic and octonionic $\mathbb{Z}$-structures

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

One checks immediately that the columns of $T$ all have euclidean length $\sqrt{3}$ and are mutually orthogonal. Hence Exc. 13 below implies $\det(D_{nO}(E')) = (2^2 - 3)^4 = 1$, and the proof of the theorem is complete.

4.6. Vista: even positive definite inner product spaces. One of the key notions dominating the arithmetic theory of quadratic forms is that of a unimodular integral quadratic lattice as defined in 3.6 (b), which is studied, e.g., in Milnor-Husemoller [86] (see also Serre [117] or Kneser [57]), under the name “even positive definite inner product space over $\mathbb{Z}$”. A prominent and particularly important example is furnished by the integral quadratic lattice underlying the Coxeter octonions. In order to appreciate the significance of this example, we record the following facts.

(a) Every even positive definite inner product space over $\mathbb{Z}$ splits uniquely into the orthogonal sum of indecomposable subspaces [86, (6.4)].
(b) The rank of an even positive definite inner product space over $\mathbb{Z}$ is divisible by 8 [86 (5.1)].
(c) There exists an even positive definite inner product space of rank 8 over $\mathbb{Z}$ [86 (6.1)] which is unique up to isomorphism [???].

The integral quadratic lattice in (c), discovered independently by Smith [???] and Korkine-Zolotarev [63], is closely connected with the root system $E_8$ and is therefore called the $E_8$-lattice. We will come back to this connection in ??? below. By (a), (b) above, the $E_8$-lattice is indecomposable, while uniqueness in (c) shows that it is isomorphic to the integral quadratic lattice underlying the Coxeter octonions.

4.7. Remarks. (a) Since the automorphism group of $\mathbb{O}$ acts simply transitively on the set of Cartan-Schouten bases of $\mathbb{O}$, the Coxeter octonions up to isomorphism do not depend on the Cartan-Schouten basis chosen.
(b) The similarity of our approach to the Hurwitz quaternions on the one hand and to the Coxeter octonions on the other is not accidental: in Chap. ??? below, we will develop a purely algebraic formalism that contains both of these constructions as special cases.
(c) The reader is referred to Van der Blij-Springer [123] and Conway-Smith [20 Chap. 9–11] for a detailed study of arithmetic properties of the Coxeter octonions. Concerning a purely arithmetic approach to a Jacobi-type formula for the number of ways a positive integer may be expressed as a sum of eight squares using the Coxeter octonions, the reader may consult Rehm [111].

Exercises.

11. Characterization of the Hurwitz quaternions by congruence conditions. Prove
Complete the proof of Thm. 4.2 by showing that the Hurwitz quaternions form a maximal integral quadratic lattice in $\mathbb{H}$: if $L \subseteq \mathbb{H}$ is an integral quadratic lattice containing $\text{Hur}(\mathbb{H})$, then $\text{Hur}(\mathbb{H}) = L$.

**A determinant formula.** Let $p, q$ be positive integers and $r, s$ be positive real numbers. Prove for matrices $T_1 \in \text{Mat}_{p,q}(\mathbb{R}), T_2 \in \text{Mat}_{q,p}(\mathbb{R})$ that the matrix

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

has determinant $\det(S) = r^{p-q} \det(T_1 T_2)$, where “char” stands for the characteristic polynomial of a square matrix. Conclude in the special case $T_1 = T, T_2 = T'$, where all the columns of $T \in \text{Mat}_{p,q}(\mathbb{R})$ are assumed to have euclidean length $\sqrt{a}$ for some $a > 0$ and to be mutually orthogonal, that $\det(S) = r^{p-q} (rs - a)^q$ and that $S$ is positive definite if $a < rs$. What happens if we drop the assumption of the columns of $T$ all having the same euclidean length but retain the one that they are mutually orthogonal?

**Units.** An element $u$ of an integral quadratic lattice $L$ in a positive definite real quadratic space $(V, q)$ is called a **unit** if $q(u) = 1$. The set of units in $L$ (possibly empty) will be denoted by $L^*$. 

(a) Let $M$ be a $\mathbb{Z}$-structure of $\mathbb{D}$. Show $1_D \in M^*$ and that $M^*$ is closed under multiplication. Show further for $u \in M$ that the following conditions are equivalent.

(i) $u \in M^*$.
(ii) $uv = 1_D$ for some $v \in M$.
(iii) $vu = 1_D$ for some $v \in \mathbb{D}$.

In this case, $v$ in (ii) (resp. (iii)) is unique and $v = \bar{u}$.

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

**Alternate description of the Hurwitz quaternions.** Show with

$$e_1 := \frac{1}{2}(j - k), \quad e_2 := -\frac{1}{2}(j + k), \quad e_3 := \frac{1}{2}(1_H + i), \quad e_4 := -\frac{1}{2}(1_H - i)$$

that $(e_i)_{1 \leq i \leq 4}$ is an orthonormal basis of $\mathbb{H}$ relative to the euclidean scalar product $(x, y)$ and that

$$\text{Hur}(\mathbb{H}) = \mathbb{Z}(e_1 - e_2) \oplus \mathbb{Z}(e_2 - e_1) \oplus \mathbb{Z}(e_3 - e_4) \oplus \mathbb{Z}(e_3 + e_4).$$

Conclude

$$\text{Hur}(\mathbb{H}) = \{ \sum_{i=1}^{4} \xi_i e_i : e_i \in \mathbb{Z}, \ 1 \leq i \leq 4, \ \sum_{i=1}^{4} \xi_i \in 2\mathbb{Z} \}$$

and

$$\text{Hur}(\mathbb{H})^* = \{ \pm e_i \pm e_j : 1 \leq i < j \leq 4 \}.$$

**Remark.** The last two equations show that $\text{Hur}(\mathbb{H})$ is the root lattice of the root system $D_4$, while $\text{Hur}(\mathbb{H})^*$ consists precisely of the roots of that system. See ??? for more details.

**Alternate description of the Coxeter octonions and their units.** Let $E = (u_i)_{0 \leq i \leq 7}$ be a Cartan-Schouten basis of $\mathbb{O}$.

(a) Show with

$$e_1 := \frac{1}{2}(-u_0 + u_2), \quad e_2 := \frac{1}{2}(u_0 + u_2), \quad e_3 := -\frac{1}{2}(u_1 + u_3), \quad e_4 := \frac{1}{2}(u_1 - u_3),$$

$$e_5 := \frac{1}{2}(-u_4 + u_5), \quad e_6 := \frac{1}{2}(u_4 + u_5), \quad e_7 := \frac{1}{2}(u_6 - u_7), \quad e_8 := \frac{1}{2}(u_6 + u_7)$$
that \((e_i)_{1 \leq i \leq 8}\) is an orthonormal basis of \(O\) relative to the euclidean scalar product \((x, y)\).

(b) Conclude that \(\text{Cox}(O)\) is the additive subgroup of \(O\) generated by the expressions

\[
\pm e_i \pm e_j, \quad \frac{1}{2} \sum_{i=1}^{8} s_i e_i, \quad (1)
\]

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

(c) Show further that

\[
\text{Cox}(O) = \{ \sum_{i=1}^{8} \xi_i e_i \mid \xi_i \in \mathbb{R}, 2 \xi_i, \xi_i - \xi_j \in \mathbb{Z} (1 \leq i, j \leq 8), \sum_{i=1}^{8} \xi_i \in 2\mathbb{Z} \}. \quad (2)
\]

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

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

Remark. The elements of [1] are precisely the roots of the root system \(E_8\) and, therefore, \(\text{Cox}(O)\) is the corresponding root lattice. See ??? for more details.

17. The Kirmse lattice. (Kirmse [55]) Let \(E := (u_i)_{0 \leq i \leq 7}\) be a Cartan-Schouten basis of \(O\). Show that

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

with

\[
v_1 := \frac{1}{2} (1_O + u_1 + u_2 + u_4), \quad v_2 := \frac{1}{2} (u_3 + u_5 - u_6 - u_7), \quad v_3 := \frac{1}{2} (1_O + u_1 + u_4 - u_7), \quad v_4 := \frac{1}{2} (1_O + u_2 + u_3 + u_4)
\]

is a unital unimodular integral quadratic lattice in \(O\) which, however, contrary to what has been claimed in [55] p. 70, is not a \(\mathbb{Z}\)-structure of \(O\). (Hint. Consider the product \(v_1 v_3\).)

Remark. It follows from [47] that \(\text{Kir}(O)\) is isomorphic to the Coxeter octonions as an integral quadratic lattice, hence, by what has been shown in Exc. 16 (d), must have exactly 240 units, in agreement with [55] p. 76.

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

18. An alternate model of the Coxeter octonions. Let \((u_i)_{0 \leq i \leq 7}\) be a Cartan-Shouten basis of \(O\) and put

\[
v_1 := \frac{1}{2} (1_O + u_1 + u_2 + u_4), \quad v_2 := \frac{1}{2} (1_O + u_1 + u_5 + u_6), \quad v_3 := \frac{1}{2} (1_O + u_1 + u_3 + u_7), \quad v_4 := \frac{1}{2} (u_1 + u_2 + u_3 + u_5)
\]

Then show that

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

is a \(\mathbb{Z}\)-structure isomorphic to the Coxeter octonions.
19. Show that there is an embedding of the Hurwitz quaternions into the Coxeter octonions as \( \mathbb{Z} \)-algebras.

5. The euclidean Albert algebra

The euclidean Albert algebra made its first appearance in the work of Jordan-von Neumann-Wigner [51], who suspected it to be what would later be called an exceptional simple formally real Jordan algebra. But while the authors were able to show that it is simple and formally real, the remaining two properties eluded them. This gap was subsequently closed by Albert [2] in an immediate follow-up to [51].

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

5.1. The standard subalgebras of \( \mathbb{O} \). Throughout this section, we fix a positive integer \( n \) and, as in 3.1, we write \( \mathbb{D} \) for one of the four unital subalgebras \( \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O} \) of \( \mathbb{O} \). We also put \( d := \dim_{\mathbb{R}}(\mathbb{D}) \). As explained more fully in 3.1, the algebra \( \mathbb{D} \) inherits its unit element, norm, trace, conjugation from \( \mathbb{O} \) via restriction. We identify the base field \( \mathbb{R} \) canonically inside \( \mathbb{D} \) via \( \mathbb{R} = \mathbb{R}1_{\mathbb{D}} = \mathbb{R}1_{\mathbb{O}} \). Note by (1.5.7) that only the elements of \( \mathbb{R} \) remain fixed under the conjugation of \( \mathbb{D} \).

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

\[
\text{Mat}_n(\mathbb{D}) \rightarrow \text{Mat}_n(\mathbb{D}), \quad x \mapsto \bar{x}',
\]

is an involution, i.e., it is \( \mathbb{R} \)-linear of period 2 and satisfies the relation

\[
\bar{xy}' = y'ar{x}' \quad (x, y \in \text{Mat}_n(\mathbb{D})).
\]

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

\[
\text{Her}_n(\mathbb{D}) := \{ x \in \text{Mat}_n(\mathbb{D}) \mid x = \bar{x}' \}
\]

the set of elements in \( \text{Mat}_n(\mathbb{D}) \) that are hermitian in the sense that they remain fixed under the conjugate transpose involution. Note by the conventions of 5.1 that the diagonal entries of \( x \in \text{Her}_n(\mathbb{D}) \) are all scalars, and so \( \text{Her}_n(\mathbb{D}) \subseteq \text{Mat}_n(\mathbb{D}) \) is a real subspace of dimension
The ordinary matrix units $e_{ij}$, $1 \leq i, j \leq n$, of $\text{Mat}_n(\mathbb{D})$ canonically induce hermitian matrix units in $\text{Her}_n(\mathbb{D})$ according to the rules
\[ v[ij] := ve_{ij} + \overline{ve}_{ji} \quad (v \in \mathbb{D}, 1 \leq i, j \leq n, i \neq j). \tag{5} \]

The conjugate transpose involution by (5.2.2) does not preserve multiplication and hence the subspace $\text{Her}_n(\mathbb{D}) \subseteq \text{Mat}_n(\mathbb{D})$ is not a subalgebra. In order to remedy this deficiency, we pass from ordinary matrix multiplication to the symmetric matrix product
\[ x \cdot y := \frac{1}{2} (xy + yx) \quad (x, y \in \text{Mat}_n(\mathbb{D})). \tag{1} \]

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

On the positive side, the conjugate transpose involution, again by (5.2.2), does preserve multiplication of $\text{Mat}_n(\mathbb{D})^+$, allowing us to conclude that $\text{Her}_n(\mathbb{D})$ becomes a unital commutative real algebra under the symmetric matrix product and is, in fact, a unital subalgebra of $\text{Mat}_n(\mathbb{D})^+$. Note that, thanks to the factor $\frac{1}{2}$ on the right-hand side of (1), squares of elements in $\text{Her}_n(\mathbb{D})$, computed in $\text{Mat}_n(\mathbb{D})$ and in $\text{Her}_n(\mathbb{D})$, respectively, coincide, though cubes in general do not.

5.4. The case $n = 3$. The formalism described in 5.2, 5.3 will become particularly important for $n = 3$. The unital subalgebra $\text{Her}_3(\mathbb{D}) \subseteq \text{Mat}_3(\mathbb{D})^+$ by (5.2.4) has dimension
\[ \dim_\mathbb{R} \left( \text{Her}_3(\mathbb{D}) \right) = 3(d + 1) \tag{1} \]
and consists of the elements
\[ x = \begin{pmatrix} \alpha_1 & u_3 & \bar{u}_2 \\ \bar{u}_3 & \alpha_2 & u_1 \\ u_2 & \bar{u}_1 & \alpha_3 \end{pmatrix} = \sum (\alpha_i e_{ii} + u_i [ij]) \quad (\alpha_i \in \mathbb{R}, u_i \in \mathbb{O}, 1 \leq i \leq 3), \tag{2} \]
where the sum on the very right is extended over all cyclic permutations $(ijl)$ of $(123)$. As will be seen in due course, the structure of this algebra becomes exceedingly delicate for $\mathbb{D} = \mathbb{O}$.

5.5. Enter the euclidean Albert algebra. The real algebra
\[ \text{Her}_3(\mathbb{O}) \]
of $3 \times 3$ hermitian matrices with entries in the Graves-Cayley octonions under the symmetric matrix product is called the euclidean Albert algebra\footnote{The prefix “euclidean” will be explained in 5.6 below.}. It is commutative, contains an identity element and by (5.4.1) has dimension 27.

The euclidean Albert algebra derives its importance from profound connections with various branches of mathematics and physics. Suffice it to mention at this stage connections with

- Exceptional Lie groups of type $E_6, F_4, D_4$, see ??? for more details,
- Self-dual homogeneous convex cones (Koecher [62]),
- Bounded symmetric domains (Loos [68]),
- Theta functions (Dorfmeister-Walcher [25]),
- Elementary particles (Dray-Manogue [26]).

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

### 5.6. Real Jordan algebras and euclidicity.

By a real Jordan algebra we mean a real algebra $J$ (the term “real” being understood if there is no danger of confusion) satisfying the following identities, for all $x, y \in J$.

1. $xy = yx$ \quad (commutative law),
2. $x(x^2y) = x^2(xy)$ \quad (Jordan identity).

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

$$\forall x_1, \ldots, x_m \in J : \left( \sum_{r=1}^{m} x_r^2 = 0 \implies x_1 = \cdots = x_m = 0 \right)$$

### 5.7. Special and exceptional real Jordan algebras.

(a) Standard examples of real Jordan algebras are easy to construct: let $A$ be an associative algebra with multiplication $(x, y) \mapsto xy$. Then it is readily checked that, in analogy to (5.3.1), the symmetric product

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

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

(b) The real algebras $\mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ are all associative. Hence so is $\text{Mat}_n(\mathbb{D})$, and we deduce from (5.3) that $\text{Her}_n(\mathbb{D})$ is a special Jordan algebra. By contrast, the preceding argument breaks down for $\mathbb{D} = \mathbb{O}$ since $\mathbb{O}$ is not associative. In fact, while $\text{Her}_3(\mathbb{O})$, ...
as a delicate argument in Thm. 5.10 below will show, continues to be a Jordan algebra, it will be an exceptional one. Moreover, \( \text{Her}_n(\mathbb{D}) \) for \( n > 3 \) is not even a Jordan algebra anymore (Exc. 21).

(c) Our principal aim in the present section will be to show in a unified fashion that \( \text{Her}_3(\mathbb{D}) \), for any \( \mathbb{D} \), including \( \mathbb{D} = \mathbb{O} \), is a euclidean Jordan algebra, thereby justifying the terminology of 5.5. We do so not by following Albert’s original approach \cite{Albert1963} but by adopting an idea of Springer’s [???], according to which some fundamental properties of ordinary \( 3 \times 3 \)-matrices over a field survive in the algebra \( \text{Her}_3(\mathbb{D}) \).

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

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

where \( \alpha_i, \beta_i \in \mathbb{R}, u_i, v_i \in \mathbb{D} \) for \( 1 \leq i \leq 3 \), and unadorned summations will always be taken over the cyclic permutations \((i j l)\) of (123). Then we define the norm \( N := N_j: J \to \mathbb{R} \), the trace \( T := T_j: J \to \mathbb{R} \) and the adjoint \( \dagger: J \to J, x \mapsto x^\dagger \), by the formulas

\[
N(x) := \alpha_1 \alpha_2 \alpha_3 - \sum \alpha_i (\alpha_i - n(\alpha_i)),
\]

\[
T(x) := \sum \alpha_i,
\]

\[
x^\dagger := \sum (\alpha_i \alpha_j - n(\alpha_j)) e_{ii} + (- \alpha_i u_i + \overline{u}_j [jl]).
\]

By Exc. 1(b), the final term on the right of (2) is unambiguous. Moreover, the norm \( N \) is a cubic form, i.e., after choosing a basis of \( \text{Her}_3(\mathbb{D}) \) as a real vector space, \( N \) is represented by a homogeneous polynomial of degree 3 in \( d \) variables. Similarly, the trace \( T \) is a linear form, while the adjoint is a real quadratic map in the sense of 1.3. In particular, the expression \( x \cdot y := (x + y)^2 - x^2 - y^2 \) is (symmetric) bilinear in \( x, y \).

More precisely,

\[
x \cdot y = \sum \left( (\alpha_i \beta_j + \beta_j \alpha_i - n(\alpha_i)) e_{i j} + (- \alpha_i v_i - \beta_j u_i + \overline{u}_j v_i + \overline{v}_j [jl]) \right)
\]

Finally, we put

\[
S(x) := T(x^\dagger) = \sum (\alpha_i \alpha_j - n(\alpha_j)),
\]

and note that \( S := S_j: J \to \mathbb{R} \) is a quadratic form with bilinearization given by

\[
S(x, y) := DS(x, y) = T(x \cdot y) = \sum (\alpha_i \beta_j + \beta_j \alpha_i - n(\alpha_j, v_j)).
\]

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

(b) For arbitrary elements

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

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

$$x^3 := x \cdot x^2 = \frac{1}{2}(x^2 \cdot x + x^3)$$

the cube of $x$ in $J$ (which in general is not the same as its cube in $\text{Mat}_3(\mathbb{D})$) and claim that the following relations hold.

$$x^2 = \sum \left( \left( \alpha_i^2 + n_\mathbb{D}(u_i) + n_\mathbb{D}(u_i) \right)e_{ii} + \left((\alpha_j + \alpha_i)u_i + u_ju_i] [jl] \right) \right),$$

$$x \cdot y = \sum \left( \left( \alpha_i \beta_i + \frac{1}{2}n_\mathbb{D}(u_i, v_i) + \frac{1}{2}n_\mathbb{D}(u_i, v_i) \right)e_{ii} + \frac{1}{2}((\alpha_j + \alpha_i)v_i + (\beta_j + \beta_i)u_i + u_jv_i + v_ju_i) [jl] \right),$$

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

$$S(x, y) = T(x) T(y) - T(x \cdot y),$$

$$x^2 = x^2 - T(x) x + S(x) 1_3,$$

$$DN(x)(y) = T(x \cdot y) = T(x^2 \cdot y) - T(x) T(x \cdot y) + S(x) T(y),$$

$$x^3 = T(x)x^2 - S(x)x + N(x)1_3,$$

$$x^2 \cdot y = 2T(x)x \cdot y + T(y)x^2 - 2x \cdot (x \cdot y) - S(x)y - (T(x)T(y) - T(x \cdot y))x$$

$$- S(x, y)x + DN(x)(y)1_3 - 2x \cdot (x \cdot y).$$

The verification of these identities is either straightforward or part of Exc. 20 below.

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

**Proof.** We know from 5.3 that the algebra $J := \text{Her}_3(\mathbb{D})$ is unital and commutative, so our first aim must be to establish the Jordan identity (5.6.2). To this end, we combine (5.9.11) with (5.9.7), (5.9.9) and obtain

$$x^2 \cdot y = 2T(x)x \cdot y + T(y)x^2 - 2x \cdot (x \cdot y) - S(x)y - (T(x)T(y) - T(x \cdot y))x$$

$$+ (T(x^2 \cdot y) - T(x)T(x \cdot y) + S(x)T(y))1_3.$$ 

Multiplying this equation by $x$, we conclude
The euclidean Albert algebra

\[ x \cdot (x^2 \cdot y) = 2T(x)x \cdot (x \cdot y) + T(y)x^3 - 2x \cdot (x \cdot (x \cdot y)) \]

with clividicity is now anti-climactic: let \( J \) be a real Jordan algebra. To establish its euclidicity, we have

\[ T(x)x \cdot (x \cdot y) = 2T(x)x \cdot (x \cdot y) + T(y)x^3 - 2x \cdot (x \cdot (x \cdot y)) \]

On the other hand, replacing \( y \) by \( x \cdot y \) in (1) and applying (5.9.10), we deduce

\[ x^2 \cdot (x \cdot y) = 2T(x)x \cdot (x \cdot y) + T(x \cdot y)x^2 - 2x \cdot (x \cdot (x \cdot y)) \]

Subtracting this from (2) and applying (5.9.10) twice now yields

\[ x \cdot (x^2 \cdot y) - x^2 \cdot (x \cdot y) = T(y)x^3 - T(x)T(y)x^2 + S(x)T(y)x \]

and the Jordan identity holds. Thus \( J \) is a real Jordan algebra. To establish its euclidicity, we have

\[ T(x)x \cdot (x \cdot y) = 2T(x)x \cdot (x \cdot y) + T(y)x^3 - 2x \cdot (x \cdot (x \cdot y)) \]

5.11. Cubic euclidean Jordan matrix algebras. The algebras \( \text{Her}_3(\mathbb{D}) \) are called cubic euclidean Jordan matrix algebras. This terminology is justified by Thm. 5.10 combined with (5.9.10).

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

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

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

Proof. Since \( x \cdot x^2 = x^3 \) by (5.9.2), we have \( x \cdot \mathbb{R}[x] \subseteq \mathbb{R}[x] \). Moreover, the Jordan identity and (5.9.10) yield

\[ (x^3)^2 = x^2 \cdot (x \cdot x) = x \cdot (x^2 \cdot x) = x \cdot x^3 \in x \cdot \mathbb{R}[x] \subseteq \mathbb{R}[x]. \]
Thus \( \mathbb{R}[x] \subseteq J := \text{Her}_3(\mathbb{D}) \) is a unital subalgebra. While commutativity is inherited from \( J \), associativity may be checked on the spanning set \( 1_3, x, x^2 \), where it is either obvious or a consequence of (1). The final assertion follows immediately from the definition (3.3) \( \square \)

5.13. The minimum polynomial. (a) As in (3.3) we denote by \( \mu_x \in \mathbb{R}[t] \) the minimum polynomial of \( x \) in the finite-dimensional unital power-associative real algebra \( J := \text{Her}_3(\mathbb{D}) \). From (5.9.10) we deduce

\[
\mu_x = t^3 - T(x)t^2 + S(x)t - N(x) \iff 1_3 \wedge x \wedge x^2 \neq 0 \text{ in } \mathbb{R}[3](J). \tag{1} \]

Note that, since powers of \( x \) in \( J \) are well behaved, \( J \) by euclidicity (cf. Thm. 5.10) contains no nilpotent elements other than zero.

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

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

and there exists a basis \( (c_r)_{1 \leq r \leq m} \) of \( \mathbb{R}[x] \) as a real vector space that up to order is uniquely determined by the conditions

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

Proof. Write \( \mu \) for the product of the distinct irreducible factors of \( \mu_x \). Then \( \mu_x \) divides \( \mu^n \) for some positive integer \( n \), which implies \( \mu(x)^n = 0 \). But \( J := \text{Her}_3(\mathbb{D}) \) does not contain non-zero nilpotent elements (5.13). Hence \( \mu(x) = 0 \), and we conclude that \( \mu_x = \mu \) has only simple irreducible factors over \( \mathbb{R} \). Suppose one of these has degree 2. Then \( \mathbb{C} \), by the Chinese Remainder Theorem [65, II, Cor. 2.2], becomes a (possibly non-unital) subalgebra of \( \mathbb{R}[x] \). As such it inherits euclidicity from \( J \), contradicting the equation \( i^2 + j^2 = 0 \) in \( \mathbb{C} \). Thus \( \mu_x \) splits into distinct linear factors, and applying the Chinese Remainder Theorem again yields quantities \( c_r \), \( 1 \leq r \leq m \), with the desired properties. It remains to prove uniqueness up to order. Let \( (d_r) \) be another basis of \( \mathbb{R}[x] \) satisfying (1) after the obvious notational adjustments. Then, with indices always varying over \( \{1, 2, 3\} \), we have \( d_r = \sum c_r \alpha_x \) for some \( u := (\alpha_x) \in \text{GL}_3(\mathbb{R}) \), and \( d^2 = d_1 \) yields \( \alpha_x \in \{0, 1\} \). On the other hand, \( \sum d_r = 1_3 \) amounts to \( \sum c_r \alpha_x = 1 \). Hence, given \( x \), there is a unique index \( \pi(s) \) such that \( \alpha_x = \delta_{\pi(s)} \). Assuming \( \pi(s) = \pi(s') \) for some \( s \neq s' \) would therefore imply the contradiction that two distinct columns of \( u \in \text{GL}_3(\mathbb{R}) \) are presented by the same vector in \( \mathbb{R}^3 \). Thus \( \pi \in S_3 \) and \( c_r = d_{\pi(r)} \) for all \( r \). \( \square \)

Exercises.

20. Verify the identities (5.9.3) – (5.9.11).
21. Show for a positive integer $n$ that Her$_n(\mathbb{D})$ under the symmetric matrix product is a Jordan algebra if and only if $n \leq 3$. (Hint. Prove by repeated linearization, equivalently, by repeatedly taking directional derivatives, that a real Jordan algebra $J$ satisfies the fully linearized Jordan identity $u((vw)x) + v((uw)x) + w((uv)x) = (uv)(wx) + (vw)(ux) + (wu)(vx)$ for all $u, v, w, x \in J$.)

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

(a) If $I_3 \wedge x \wedge x^2 \neq 0$ in $\wedge^3(J)$, then

$$
\mu_x = \det (I_3 \otimes x - L^0_3), \quad N(x) = \det(L^0_3), \quad T(x) = \text{tr}(L^0_3).
$$

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

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

$$
x^{-1} = N(x)^{-1} x^2.
$$

(d) $x^N = N(x)x$ (adjoint identity) and $N(x^2) = N(x)^2$.

(Hint. For (b) and (d), use Zariski density arguments [??].)

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

$$
\varphi \left( \sum \alpha_i e_i + u_3[j]l \right) := \sum \alpha_i e_i + (u^{-1}u_3)[23] + (u^2u^{-1})[31] + (uu_3u)[12]
$$

for $\alpha \in \mathbb{R}$, $u_3 \in \mathbb{O}$, $1 \leq i \leq 3$, is an automorphism of $J$ if and only if $n_3(u) = 1$.

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

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

In order to overcome this difficulty, we take up an idea of Knebusch [56] by defining what we call quadratic $\mathbb{Z}$-structures of finite-dimensional unital real Jordan algebras. In contradistinction to their linear counterpart, quadratic $\mathbb{Z}$-structures are based not on the bilinear product $xy$ but on the cubic operation $U_{xy}$ provided by the $U$-operator (see 6.4 below) of the ambient Jordan algebra. This not only yields an abundant variety of natural examples but also a first glimpse at how Jordan algebras should be treated over commutative rings in which $\frac{1}{2}$ is not available: through McCrimmon’s theory [75] of quadratic Jordan algebras.

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

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

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

6.2. **Examples: the Jordan algebras \( \mathbb{D}^+ \).** Either by definition (5.7) or by Exc. 25 \( J := \mathbb{D}^+ \) is a special unital real Jordan algebra, and it would be perfectly natural to expect any \( \mathbb{Z} \)-structure of \( \mathbb{D} \) to be a linear one of \( J \). But this, though valid in some isolated cases (see Exc. 26 below) is **not true in general.** In fact, it fails to be valid in the following important examples.

(a) (Knebusch \[56\] p. 175) Let \( \mathbb{D} := \mathbb{H} \) and \( M := \text{Hur}(\mathbb{H}) \subseteq \mathbb{H} \) be the \( \mathbb{Z} \)-structure of Hurwitz quaternions. Then \( i,h \in M \) by Thm. 4.2 while (1.5.12) and (4.1.2) yield

\[
i \cdot h = \frac{1}{2}(ih + hi) = \frac{1}{2}(t_H(i)h + t_H(h)i - n_H(i, h)1_H) = \frac{1}{2}(-1_H + i),
\]

which by Exc. 11 does not belong to \( M \). Thus \( \text{Hur}(\mathbb{H}) \subseteq \mathbb{H}^+ \) is not a linear \( \mathbb{Z} \)-structure.

(b) Similarly, let \( \mathbb{D} := \mathbb{O} \) and \( M := \text{Cox}_E(\mathbb{O}) \subseteq \mathbb{O} \) be the \( \mathbb{Z} \)-structure of Coxeter octonions relative to a Cartan-Shouten basis \( E = (u_i)_{0 \leq i \leq 7} \) of \( \mathbb{O} \). Then \( u_1, p \in M \) by Thm. 4.5 while (1.5.12) and (4.1.8) yield

\[
u_1 \cdot p = \frac{1}{2}(u_1p + pu_1) = \frac{1}{2}(t_O(u_1)p + t_O(p)u_1 - n_O(u_1, p)1_O) = \frac{1}{2}(-1_O + u_1) \in \mathbb{H}.
\]

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

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

\[
\Lambda := \text{Her}_3(M) := \{ x \in \text{Mat}_3(M) \mid x = \bar{x} \}
\]

makes sense and is a unital lattice in \( J \). However, \( \Lambda \) fails to be closed under multiplication since, e.g., \( 1[23] \) and \( 1[31] \) both belong to \( \Lambda \) while \( 1[23] \cdot 1[31] = \frac{1}{2}[21] = \frac{1}{2}[12] \) obviously does not.
In view of the deficiencies highlighted in the preceding examples, we will abandon linear \(\mathbb{Z}\)-structures of real Jordan algebras and replace them by quadratic ones, which are based on the following concept.

### 6.4. The \(U\)-operator

For \(x \in J\), the linear map

\[
U_x : J \rightarrow J, \quad y \mapsto U_x y := 2x(xy) - x^2 y, \tag{1}
\]

is called the \(U\)-operator of \(x\). The map

\[
U : J \rightarrow J, \quad x \mapsto U_x \tag{2}
\]

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

\[
\{xyz\} := U_{x+z}y - U_x - U_z y = 2(xy)(zy) - (xz)y \quad (x, y, z \in J). \tag{3}
\]

The \(U\)-operator is of the utmost importance for a deeper understanding of Jordan algebras. Its fundamental algebraic properties will be addressed in ??? below. For the time being, it will be enough to observe a few elementary facts assembled in Exercises 24, 25.

### 6.5. Quadratic \(\mathbb{Z}\)-structures

(Cf. Knebusch [56, p. 175].) By a quadratic \(\mathbb{Z}\)-structure of \(J\) we mean a unital lattice \(\Lambda \subseteq J\) such that \(U_{x+y} \in \Lambda\) for all \(x, y \in \Lambda\). This implies that \(\Lambda\) is closed under the Jordan triple product \((6.4.3)\) and, in particular, \(2xy = \{xy1_J\} \in \Lambda\) for all \(x, y \in \Lambda\). However, while an inspection of \((6.4.1)\) shows that linear \(\mathbb{Z}\)-structures are always quadratic ones, the converse does not hold, as may be seen from the following examples.

### 6.6. Examples

Let \(M\) be a \(\mathbb{Z}\)-structure of \(D\). Then \(1_{D^+} = 1_D \in M\), and Exc. 25 yields \(U_{1_D} = 1_D \in M\) for all \(x, y \in M\). Thus \(M\) is a quadratic \(\mathbb{Z}\)-structure of \(D^+\); as such it will be denoted by \(M^+\). Now it follows from \(6.2\) that both Hur(\(\mathbb{H}\))^+ and Cox(E(\(\mathbb{O}\))^+) are quadratic \(\mathbb{Z}\)-structures of \(\mathbb{H}^+\) and \(\mathbb{O}^+\), respectively, but not linear ones.

We have observed in \(6.3\) that

\[
\Lambda := \text{Her}_3(M) = \{x \in \text{Mat}_3(M) \mid x = x^2\}
\]

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

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

we have \(\alpha_i, \beta_i \in M \cap \mathbb{R} = \mathbb{Z}\) by Exc. 10, \(u_i, v_i \in M\) for \(1 \leq i \leq 3\), and \(5.9.5, 5.8.4\) yield \(T(x \bullet y) \in \mathbb{Z}, x^2 \in \Lambda\). Linearizing ad applying Exc. 24(b), we therefore obtain \(U_{x+y} = T(x \bullet y)x - x^2 \times y \in \Lambda\), and the proof is complete.
Our next aim will be to show that, in analogy to Cor. 5.9 the linear form $T$, the quadratic form $S$, and the cubic form $N$ of $J := \text{Her}_3(\mathbb{D})$ all take on integral values on any quadratic $\mathbb{Z}$-structure of $J$. Actually, we will be able to establish this result under slightly less restrictive conditions. The following lemma paves the way.

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

**Proof.** From Prop. 3.8 we deduce $\mu_x := \mu_x^R = \mu_x^Q \in \mathbb{Q}[t]$, so $m := \deg(\mu_x)$ is at most 3. If $m = 3$, then (5.13) implies the assertion. At the other extreme, if $m = 1$, then $x = \alpha 1_J$ for some $\alpha \in \mathbb{Q}$, which again implies the assertion. We are left with the case $m = 2$, so $\mu_x = t^2 - \alpha_1 t + \alpha_2$ for some $\alpha_1, \alpha_2 \in \mathbb{Q}$, and a short computation gives

$$x^3 = (\alpha_1^2 - \alpha_2)x - \alpha_1 \alpha_2 1_J.$$

Similarly, invoking (5.9), we obtain

$$x^3 = (\alpha_1 T(x) - S(x)) x - (\alpha_2 T(x) - N(x)) 1_J,$$

and comparing coefficients, we conclude

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

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

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

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

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

**6.9. Proposition.** Let $\Lambda \subseteq J := \text{Her}_3(\mathbb{D})$ be a lattice that is stable under taking powers with arbitrary integer exponents $\geq 0$. Then every $x \in \Lambda$ is integral and $T(x), S(x), N(x) \in \mathbb{Z}$.

**Proof.** For $x \in \Lambda$ we have $1_J = x^0 \in \Lambda$ (so $\Lambda$ is unital) and $x^2 \in \Lambda$. This property carries over to $\mathbb{Q} \Lambda$ which, by Remark 6.8 is a unital subalgebra of $J$. Given $x \in \Lambda$, Lemma 6.7 therefore implies $T(x), S(x), N(x) \in \mathbb{Q}$. Moreover, $\Lambda$ being stable under powers, $\mathbb{Z}[x] \subseteq \Lambda$ is an additive subgroup which, along with $\Lambda$, is finitely generated. Thus Propositions 5.2 and 3.8 show that $x$ is integral and $\mu_x := \mu_x^R = \mu_x^Q \in \mathbb{Z}[t]$. Since the remaining assertions of the proposition will follow, either for obvious reasons or from Exc. 10 and 5.13 if $m := \deg(\mu_x) \in \{1, 3\}$, we may assume $m = 2$. Then Cor. 5.14 yields non-zero elements $c_1, c_2 \in \mathbb{R}[x]$ and scalars $\alpha_1, \alpha_2 \in \mathbb{R}$ such that
Let $X \subseteq \mathbb{Q}$ be closed under squaring ($\xi \in X \Rightarrow \xi^2 \in X$) and suppose the additive subgroup of $\mathbb{Q}$ generated by $X$ is finitely generated. Then $X \subseteq \mathbb{Z}$.

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

6.11. Theorem (cf. Racine [109, Prop. IV.1]). For a unital lattice $\Lambda \subseteq J := \text{Her}_3(\mathbb{D})$ the following conditions are equivalent.

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

Proof. (i) $\Rightarrow$ (ii). Let $x \in \Lambda$. Then [6.4] shows $x^2 = U_x \mathbf{1}_3 \in \Lambda$.

Before we can deal with the remaining implications, it will be important to note that
In order to see this, let \( (e_1, \ldots, e_n) \) be an \( \mathbb{R} \)-basis of \( J \) associated with \( \Lambda \). Since \( N(\Lambda) \) by Exc. 23 is contained in the additive subgroup of \( \mathbb{R} \) generated by the quantities \( N(e_i) \) \( (1 \leq i \leq n) \), \( T(e_i, e_j) \) \( (1 \leq i, j \leq n, i \neq j) \), \( T(e_i \times e_j, e_l) \) \( (1 \leq i < j < l \leq n) \), it generates a finitely generated additive subgroup of \( \mathbb{R} \) on its own, as claimed. We also note

\[
N(1_3 + x) = 1 \pm T(x) + S(x) = N(1_3 + x) + N(1_3 - x) - 2 \in \mathbb{Z}.
\]

But from (2) we also deduce \( 2T(x) = N(1_3 + x) - N(1_3 - x) - 2N(x) \in \mathbb{Z} \), which combined with (3) shows that \( 2T(x) = S(x, x) = 2S(x) = N(1_3 + x) + N(1_3 - x) - 2 \in \mathbb{Z} \). Hence \( N(\Lambda) \subseteq \mathbb{Z} \). Combining (5.9.7) with (3) for \( x \in \Lambda \), we therefore conclude

\[
T(x)^2 - T(x^2) = S(x, x) = 2S(x) = N(1_3 + x) + N(1_3 - x) - 2 \in \mathbb{Z}.
\]

Exercise.

24. Properties of the \( U \)-operator. Let \( J \) be a real Jordan algebra. Prove:

(a) If \( J \) is a subalgebra of \( A' \) for some associative real algebra \( A \), then \( U_{J,y} = xyx \) for all \( x, y \in J \)

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

\[
U_{J,y} = T(x \bullet y)x - x^2 \times y
\]

for all \( x, y \in J \).

25. Show that a linear map between commutative real algebras is a homomorphism if and only if it preserves squares. Conclude that the algebra \( \mathbb{O}^+ \) of Exc. 7 is a unital special real Jordan algebra algebra such that \( U_{J,y} = xyx \) for all \( x, y \in \mathbb{O} \). Is \( \mathbb{O}^+ \) euclidean?

26. Let \( (e_i)_{i \in \mathbb{N}_0} \) be an orthonormal basis of \( \mathbb{D} \) as a euclidean real vector space such that \( e_0 = 1_D \). Prove that
The Leech lattice.

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

is a linear \( \mathbb{Z} \)-structure of the special real Jordan algebra \( \mathbb{D}^+ \) (cf. Exc. 25). Conclude that the Gaussian integers \( \mathbb{G}(\mathbb{D}) \) form linear \( \mathbb{Z} \)-structure of \( \mathbb{D} \), denoted by \( \mathbb{G}(\mathbb{D})^+ \).

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

28. Prove

\[ N(x+y) = N(x) + T(x^2, y) + T(x, y^2) + N(y) \]

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

7. **The Leech lattice.**
Chapter 2
Foundations

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

The possibility of \( k = \{0\} \) being the zero ring is expressly allowed. The only module over \( k = \{0\} \) is the zero module \( M = \{0\} \). It is free of rank one with basis \( 0 \).

8. The language of non-associative algebras

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

8.1. The concept of a non-associative algebra. A non-associative algebra or just an algebra over \( k \) (or a \( k \)-algebra for short) is a \( k \)-module \( A \) together with a bilinear map \( A \times A \to A \), called the multiplication (or product) of \( A \) and usually indicated by juxtaposition: \( (x, y) \mapsto xy \). Thus \( k \)-algebras satisfy both distributive laws and are compatible with scalar multiplication but may fail to be associative or commutative or to contain a unit element. Nevertheless, the standard vocabulary of ring theory (ideals, homomorphisms, quotients, direct sums, direct products, ...) easily extends to this more general setting and will be used here mostly without further comment.

To mention just two examples, a subalgebra of \( A \) is a submodule closed under multiplication, and a homomorphism \( h : A \to B \) of \( k \)-algebras is a linear map preserving the product: \( h(xy) = h(x)h(y) \) for all \( x, y \in A \). Examples of \( k \)-algebras for \( k = \mathbb{R} \) or \( k = \mathbb{Z} \) have been discussed in the preceding chapter.

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

8.2. Left and right multiplication. For \( x \in A \), the linear map

\[ L_x : A \to A, \quad y \mapsto L_x y := xy, \]

is called the left multiplication by \( x \) in \( A \). Similarly, the right multiplication by \( x \) in \( A \) will be denoted by

\[ R_x : A \to A, \quad y \mapsto R_x y := yx. \]
The linear map

\[ L : A \rightarrow \text{End}_k(A), x \mapsto L_x, \quad (\text{resp. } R : A \rightarrow \text{End}_k(A), x \mapsto R_x), \]

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

**8.3. Generators.** For arbitrary subsets \( X, Y \subseteq A \), we write \( XY \) as in [26.11] for the additive subgroup of \( A \) spanned by all products \( xy, x \in X, y \in Y \). Similar conventions apply to other multi-linear mappings in place of the product of \( A \). We abbreviate \( X^2 := XX \). A submodule \( B \subseteq A \) is a subalgebra if and only if \( B^2 \subseteq B \).

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

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

\[ \text{Mon}(X) := \bigcup_{m \in \mathbb{Z}, m > 0} \text{Mon}_m(X) \]

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

**8.5. Associators and commutators.** The trilinear map

\[ A \times A \times A \rightarrow A, \quad (x, y, z) \mapsto [x, y, z] := (xy)z - x(yz), \]

is called the associator of \( A \), which we have described in Exc. [1] for the real algebra of Graves-Cayley octonions. Similarly, the bilinear map

\[ A \times A \rightarrow A, \quad (x, y) \mapsto [x, y] := xy - yx, \]

is called the commutator of \( A \). It is straightforward to check that they satisfy the relations

\[ [xy, z] - x[y, z] - [x, z]y = [x, y, z] - [x, z, y] + [z, x, y], \quad (1) \]
\[ [xy, z, w] - [x, y, z, w] + [x, y, z, w] = x[y, z, w] + [x, y, z]w \]

for all \( x, y, z, w \in A \). Observe that the commutator is alternating, so \( [x, x] = 0 \) for all \( x \in A \), while the associator in general is not. This gives rise to the important concept of an alternative algebra that we encountered already in the study of Graves-Cayley octonions [1.6] and that will be discussed more systematically in the next chapter.
8.6. Commutative and associative algebras. The $k$-algebra $A$ is commutative if it satisfies the commutative law $xy = yx$, equivalently, if its commutator is the zero map. Similarly, $A$ is associative if it satisfies the associative law $(xy)z = x(yz)$, equivalently, if its associator is the zero map. Note that $A$ is commutative if and only if its left and right multiplications are the same, and that the following conditions are equivalent.

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

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

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

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

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

8.9. Associative bilinear and linear forms. A bilinear form $\sigma: A \times A \to k$ is said to be associative if it is symmetric and satisfies the relation $\sigma(xy,z) = \sigma(x,yz)$ for all $x,y,z \in A$. If in this case $I \subseteq A$ is an ideal, then so is $I^\perp = \{ x \in A \mid \sigma(x,I) = \{0\} \}$, its orthogonal complement relative to $\sigma$. To every linear form $t: A \to k$ corresponds canonically a bilinear form $\sigma_t: A \times A \to k$ via $\sigma_t(x,y) := t(xy)$ for all $x,y \in A$. We say that $t$ is associative if $\sigma_t$ is, equivalently, if $t$ vanishes on all commutators and associators of $A$. For example, it follows immediately from (1.4.1) and (1.5.5) combined with Exc. 3(a) that the trace form of the Graves-Cayley octonions is associative, even though the Graves-Cayley octonions themselves are not.

8.10. Structure constants. Generalizing the set-up described in 1.2, suppose $A$ is free as a $k$-module, with basis $(e_i)_{i \in I}$. Then there exists a unique family $(\gamma_{ij})_{i,j \in I}$ of scalars in $k$ such that, for all $j,l \in I$,
\[ \gamma_{ij,l} = 0 \quad \text{for almost all } i \in I, \]  
\[ e_j e_l = \sum_{i \in I} \gamma_{ij,l} e_i. \]  
\[ \text{(1) \quad \text{FIGU}} \]
\[ \text{pr.HOSI} \]
\[ \text{ss.UNELT} \]
\[ \text{pr.HOSI} \]
\[ \text{ss.UNELT} \]

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

Exercises.

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

30. The nil radical. (Behrens [9]) Let \( A \) be a \( k \)-algebra. An element \( x \in A \) is said to be nilpotent if \( 0 \in \text{Mon}(\{x\}) \) is a monomial over \( x \). This concept of nilpotency is the usual one for associative or, more generally, for power-associative algebras. \( A \) is said to be a nil algebra if it consists entirely of nilpotent elements, ditto for a nil ideal. Prove for any ideal \( I \subseteq A \) that \( A \) is a nil algebra if and only if \( I \) is a nil ideal and \( A/I \) is a nil algebra. Conclude that the sum of all nil ideals in \( A \) is a nil ideal, called the nil radical of \( A \) and denoted by \( \text{Nil}(A) \).

31. Lifting Idempotents. Let \( A \) be a power-associative \( k \)-algebra.

(a) Suppose \( x \in A \) satisfies a monic polynomial with invertible least coefficient, i.e., there exist integers \( n > d > 0 \), and scalars \( \alpha_0, \ldots, \alpha_{n-1} \in k \) with \( \alpha_d x^d + \cdots + \alpha_0 = 0 \). Given \( r \in \mathbb{Z} \), \( r > 0 \), write \( k[x] \) for the \( k \)-submodule of \( A \) spanned by the powers \( x^n, n \in \mathbb{Z}_{\geq r} \). Then show that there is a unique element \( c \in k[x] \) satisfying \( cx^d = x^d \). Conclude that \( c \in A \) is an idempotent. (Hint. Use the fact that a surjective linear map from a finitely generated \( k \)-module to itself is bijective.)

(b) Let \( \phi : A \rightarrow A' \) be a surjective homomorphism of unital power-associative algebras over \( k \) and suppose \( \text{Ker}(\phi) \subseteq A \) is a nil ideal (Exc. 50). Conclude from (a) that every idempotent \( c' \in A' \) can be lifted to \( A \), i.e., there exists an idempotent \( c \in A \) satisfying \( \phi(c) = c' \).

\[ \text{pr.NILRAD} \]
\[ \text{ss.UNELT} \]
\[ \text{pr.HOSI} \]
\[ \text{ss.UNELT} \]

9. Unital algebras

Let \( A \) be a \( k \)-algebra.

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

9.2. The unital hull. Every \( k \)-algebra \( A \) may be embedded into its unital hull, given on the \( k \)-module \( \hat{A} = k \oplus A \) by the multiplication
An orthogonal system of commutative associative subalgebras and, in fact, agrees with the unital subalgebra over $\text{Cent}$ multiplication on $A$. So we have $k[i] = k_i 1_A + k_i [x]$. If $A$ is power-associative, then $k[x] \subseteq A$ is a unital commutative associative subalgebra and, in fact, agrees with the unital subalgebra of $A$ generated by $x$.

(b) An orthogonal system $\mathcal{F} = (c_i)_{i \in I}$ of idempotents in $A$ is said to be complete if $c_i = 0$ for almost all $i \in I$ and $\sum_{i \in I} c_i = 1_A$. Any orthogonal system $\mathcal{F} = (c_i)_{i \in I}$ of idempotents in $A$ having $c_i = 0$ for almost all $i \in I$ can be enlarged to a complete one: with an additional index $i_0 \notin I$ and $I_0 := \{i_0\} \cup I$ put $\mathcal{F}' := (c_i)_{i \in I_0}$ where $c_{i_0} := 1_A - \sum_{i \in I} c_i$.

9.3. Powers and idempotents revisited. Suppose $A$ is unital.

(a) For $x \in A$, we define $x^0 := 1_A$ and, combining with (8.7), obtain powers $x^n$ for all $n \in \mathbb{N}$. The submodule of $A$ spanned by these powers will be denoted by $k[x]$, so we have $k[x] = k1_A + k_1 [x]$. If $A$ is power-associative, then $k[x] \subseteq A$ is a unital commutative associative subalgebra and, in fact, agrees with the unital subalgebra of $A$ generated by $x$.

(b) An orthogonal system $\mathcal{F} = (c_i)_{i \in I}$ of idempotents in $A$ is said to be complete if $c_i = 0$ for almost all $i \in I$ and $\sum_{i \in I} c_i = 1_A$. Any orthogonal system $\mathcal{F} = (c_i)_{i \in I}$ of idempotents in $A$ having $c_i = 0$ for almost all $i \in I$ can be enlarged to a complete one: with an additional index $i_0 \notin I$ and $I_0 := \{i_0\} \cup I$ put $\mathcal{F}' := (c_i)_{i \in I_0}$ where $c_{i_0} := 1_A - \sum_{i \in I} c_i$.

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

9.5. The centre. Let $A$ be unital. An element $a \in A$ is said to be central if $[a, x] = [x, a, y] = [x, a, y] = [x, y, a] = 0$ for all $x, y \in A$. The totality of central elements in $A$, written as $\text{Cent}(A)$, is called the centre of $A$. By (8.5.1), (8.5.3), $\text{Cent}(A)$ is a unital commutative associative subalgebra of $A$. The assignment $\alpha \mapsto \alpha 1_A$ gives a unital homomorphism from $k$ to $\text{Cent}(A)$. If this homomorphism is an isomorphism, $A$ is said to be central. By restricting the product of $A$ to $\text{Cent}(A) \times A$, we obtain a scalar multiplication on $A$ by elements of the centre, that converts $A$ into a central algebra over $\text{Cent}(A)$, denoted by $A_{\text{cent}}$ and called the centralization of $A$.

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

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

Following (8.5.2), the nucleus is a unital associative subalgebra of $A$, but will fail in general to be commutative. A subalgebra $B \subseteq A$ is said to be nuclear if it is unital (as a subalgebra) and is contained in the nucleus of $A$.

9.7. Simplicity and division algebras. $A$ is said to be simple if it has non-trivial multiplication, so $A^2 \neq \{0\}$, and $\{0\}$ and $A$ are the only (two-sided) ideals of $A$. 

$$(\alpha \oplus x)(\beta \oplus y) := \alpha \beta \oplus (\alpha y + \beta x + xy) \quad (\alpha, \beta \in k, x, y \in A).$$

Indeed, $\hat{A}$ is unital with unit element $1_{\hat{A}} = 1 \oplus 0$, and $A$ embeds into $\hat{A}$ through the second summand via $x \mapsto 0 \oplus x$. Identifying $A \subseteq \hat{A}$ accordingly, we obtain $\hat{A} = k1_{\hat{A}} + A$ as a direct sum of submodules, and $A \subseteq \hat{A}$ is an ideal. The unital hull may be characterized by the universal property that every homomorphism from $A$ to a unital $k$-algebra $B$ extends uniquely to a unital homomorphism from $\hat{A}$ to $B$. 

9 Unital algebras
Examples are fields or, more generally, division algebras, where $A$ is called a division algebra if it is non-zero and, for all $u, v \in A$, $u \neq 0$, the equations $ux = v$, $yu = v$ can be solved uniquely in $A$. Division algebras have no zero divisors: if $A$ is a division algebra and $x, y \in A$ satisfy $xy = 0$, then $x = 0$ or $y = 0$. Examples of division algebras are provided by arbitrary field extensions but also, for $k = \mathbb{R}$, by the Graves-Cayley octonions (1.7) and the Hamiltonian quaternions (1.11). Note that an algebra $A$ over $k$ with non-trivial multiplication is simple if and only if it is an irreducible $\text{Mult}(A)$-module.

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

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

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

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

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

**Proof.** It suffices to show that any ideal in $\text{Mat}_n(A)$ has the form $\text{Mat}_n(\alpha)$ for some ideal $\alpha$ in $A$, so let $I \subseteq \text{Mat}_n(A)$ be an ideal and put $\alpha := \{a \in A \mid ae_{11} \in I\}$. From (9.8) we deduce

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

for $a, b \in A, 1 \leq i, j \leq n$, which implies that $\alpha \subseteq A$ is an ideal satisfying $\text{Mat}_n(\alpha) \subseteq I$. Conversely, let $x = \sum e_{ij}a_{ij}e_{ij} \in I$, $a_{ij} \in A$. For $1 \leq l, m \leq n$, the matrix $a_{im}e_{1l} = \sum e_{ij}(a_{ij}e_{ij})e_{m1} = (e_{11}a_{im})e_{m1}$ is contained in $I$, forcing $a_{im} \in \alpha$, hence $x \in \text{Mat}_n(\alpha)$, and the proposition is proved. \hfill $\Box$

**9.10. Corollary.** If $A$ is a simple unital $k$-algebra, then so is $\text{Mat}_n(A)$, for any integer $n > 0$. \hfill $\Box$

**Exercises.**

**32. Ideals of direct sums.** Let $(A_j)_{1 \leq j \leq n}$ be a finite family of unital $k$-algebras. Show that the ideals of the direct sum $A = A_1 \oplus \cdots \oplus A_n$ (under the componentwise multiplication) are precisely of the form $I_1 \oplus \cdots \oplus I_n$ where $I_j$ are ideals of $A_j$ for $1 \leq j \leq n$. Does this conclusion also hold if the
33. **Algebraic elements in power-associative algebras.** Let $A$ be a unital power-associative algebra over a field $F$. An element $x \in A$ is said to be algebraic (over $F$) if the subalgebra $F[x] \subseteq A$ is finite-dimensional. In this case, the unique monic polynomial of least degree in $F[t]$ killing $x$ is called the minimum polynomial of $x$ (over $F$) and is denoted by $\mu_x$; note that $\mu_x$ generates the ideal of all polynomials in $F[t]$ killing $x$. We say that $x$ is split algebraic (over $F$) if it is algebraic and its minimum polynomial decomposes into linear factors over $F$. The algebra $A$ is called algebraic (resp. split algebraic) if every element of $A$ has this property.

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

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

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

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

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

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

(c) The following conditions are equivalent.

(i) $\text{Nil}(F[x]) = \{0\}$.

(ii) $n_1 = \cdots = n_r = 1$.

(iii) $x = \sum_{i=1}^{r} \alpha_i c_i$.

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

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

(e) Assume $\text{char}(F) \neq 2$ and $\alpha_i \in F^{n \times n}$ for $1 \leq i \leq r$. Then there exists a $y \in F[x]$ such that $y^2 = x$.

(Hint. Reduce to the case $\alpha_1 = \cdots = \alpha_r = 1$.)

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

$$(e_1)_{1 \leq j \leq n} \mapsto (Ae_1)_{1 \leq j \leq n}$$

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

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

$\text{Nuc} \left( \text{Mat}_n(A) \right) = \text{Mat}_n \left( \text{Nuc}(A) \right), \quad \text{Cent} \left( \text{Mat}_n(A) \right) = \text{Cent}(A)I_k.$

36. **Associative linear forms and unitality.** Let $A$ be a $k$-algebra. Show that $A$ is unital provided it admits an associative linear form whose corresponding (symmetric) bilinear form is non-singular.

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

---

**Note:** The text seems to be cut off and contains multiple references to other documents or sections, which are not fully visible. The above content is a natural reformulation of the visible text from the document.
10. Scalar extensions

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

10.1. Scalar extensions of modules. We denote by $k\text{-alg}$ the category of unital commutative associative $k$-algebras. The objects of this category are commutative associative $k$-algebras containing an identity element, while its morphism are $k$-algebra homomorphisms taking 1 into 1. Similarly, we write $k\text{-mod}$ for the category of $k$-modules, its objects being (left) $k$-modules and its morphisms being $k$-linear maps.

Now let $M \in k\text{-mod}$ and $R \in k\text{-alg}$. Then the $k$-module $M \otimes R$ may be converted into an $R$-module by the scalar multiplication

$$s(x \otimes r) = x \otimes (rs) \quad (x \in M, r, s \in R).$$

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

$$f_R := f \otimes 1_R : M_R \rightarrow N_R, \quad x \otimes r \mapsto f(x) \otimes r$$

is an $R$-linear map between $R$-modules. Summing up, we thus obtain a functor from $k\text{-mod}$ to $R\text{-mod}$. We also have a natural map

$$\text{can} := \text{can}_M := \text{can}_{M,R} : M \rightarrow M_R, \quad x \mapsto x_R := x \otimes 1_R,$$

which is $k$-linear but in general neither injective nor surjective. Moreover, given an $R$-module $M'$ and a $k$-linear map $g : M \rightarrow M'$, there is a unique $R$-linear map $g' : M_R \rightarrow M'$ such that $g' \circ i = g$, namely the one given by

$$g'(x \otimes r) = rg(x) \quad (x \in M, r \in R).$$

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

$$(\bar{\alpha}, \bar{x}) \mapsto \bar{\alpha} \bar{x} \quad (\alpha \in k, x \in M)$$

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

$$x \otimes \bar{\alpha} = \bar{\alpha} \bar{x}$$

(1)
for \( x \in M \) and \( \alpha \in k \).

### 10.3. Iterated scalar extensions

Iterated scalar extensions collapse to simple ones: for \( R \in k\text{-alg} \), we have \( R\text{-alg} \subseteq k\text{-alg} \) canonically, and, given a \( k \)-module \( M \), any \( S \in R\text{-alg} \) yields a natural identification \( (M_R)_S = M_S \) as \( S \)-modules via

\[
(x \otimes r) \otimes_R S = x \otimes (rs), \quad x \otimes S = (x \otimes 1_R) \otimes_R S = x_R \otimes_R S
\]

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

\[
(1_M \otimes \vartheta)(x) = x_S
\]

for all \( x \in M_R \).

### 10.4. Localizations

Particularly important instances of scalar extensions are provided by localizations at prime ideals. Here are some of the relevant facts. Unless explicitly saying otherwise, we refer the reader to Bourbaki [11, II] for details and further reading.

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

\[
D(f) := \{ p \in \text{Spec}(k) \mid f \notin p \} \subseteq \text{Spec}(k) \quad (f \in k).
\]

We also put

\[
V(Z) := \{ p \in \text{Spec}(k) \mid Z \subseteq p \} \quad (Z \subseteq k),
\]

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

Let \( \vartheta: k \to k' \) be a homomorphism of commutative rings, i.e., a morphism in \( Z\text{-alg} \). Then

\[
\text{Spec}(\vartheta): \text{Spec}(k') \to \text{Spec}(k), \quad p' \mapsto \text{Spec}(\vartheta)(p') := \vartheta^{-1}(p'),
\]

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

The localization of \( k \) at a prime ideal \( p \subseteq k \) will be denoted by \( k_p \); it is a local ring whose residue field, written as \( k(p) \), agrees with the quotient field of \( k/p \). Now let \( M \) be a \( k \)-module. We write \( M_p := M \otimes k_p \) (resp. \( M(p) := M \otimes k(p) = M_p \otimes_{k_p} k(p) \)) for the base change of \( M \) from \( k \) to \( k_p \) (resp. to \( k(p) \)), and obtain natural maps
can_p := can_{M,k_p}: M \rightarrow M_p, \quad x \mapsto x_p := x_{k_p}, \quad (4)  
\text{can}(p) := can_{M,k(p)}: M \rightarrow M(p), \quad x \mapsto x(p) := x_{k(p)}. \quad (5)

Moreover, for any k-linear map \( \varphi: M \rightarrow N \) of k-modules \( M, N \), we put \( \varphi_p := \varphi_{k_p}: M_p \rightarrow N_p \) and \( \varphi(p) := \varphi_{k(p)}: M(p) \rightarrow N(p) \).

Given a ring homomorphism \( \vartheta: k \rightarrow k' \) as above, let \( p' \in \text{Spec}(k') \) and put \( p := \text{Spec}(\vartheta)(p') = \vartheta^{-1}(p') \). Then we obtain a commutative diagram

\[
\begin{array}{ccc}
k & \xrightarrow{\vartheta} & k' \\
\text{can}_p & \downarrow & \text{can}_{p'} \\
k_p & \xrightarrow{\vartheta'} & k'_p \\
\text{can}_p(p) & \downarrow & \text{can}_{p'}(p') \\
k(p) & \xrightarrow{\vartheta} & k'(p'),
\end{array}
\]

\( \text{where } \vartheta': k_p \rightarrow k'_p \) is the local homomorphism canonically induced by \( \vartheta \) and in turn determines the field homomorphism \( \tilde{\vartheta}: \kappa(p) \rightarrow \kappa(p') \), making \( \kappa(p') \) a field extension of \( \kappa(p) \). Now let \( M \) be a k-module, regard \( k' \) (resp. \( k'_p \)) as an element of \( k\text{-alg} \) (resp. \( k_p\text{-alg} \)) by means of \( \vartheta \) (resp. \( \vartheta' \)) and put \( M' := M_{k'} \) as \( k' \)-modules. Then \( 10.3 \text{[1]} \) and \( 10.2 \text{[1]} \) yield natural identifications

\[
M'_p = M_p \otimes_{k_p} k'_p, \quad (7) \text{ } \text{MPRLO}
\]
as \( k'_p \)-modules that are functorial in \( M \). Similarly,

\[
M'(p') = M(p) \otimes_{k(p)} \kappa(p') \quad \text{as vector spaces over } \kappa(p'). \quad (8) \text{ } \text{MPRFI}
\]

10.5. Principal open sets as spectra. For \( f \in k \), we denote by

\[
k_f := \{ \alpha/f^n | \alpha \in k, \ n \in \mathbb{N} \} \quad (1) \text{ } \text{KAF}
\]
the ring of fractions associated with the multiplicative subset \( \{ f^n | n \in \mathbb{N} \} \subseteq k \) and by

\[
\text{can}_f: k \rightarrow k_f, \quad \alpha \mapsto \alpha/1, \quad (2) \text{ } \text{CANF}
\]
the canonical homomorphism, making \( k_f \) a \( k \)-algebra. The continuous map

\[
\text{Spec}(\text{can}_f): \text{Spec}(k_f) \rightarrow \text{Spec}(k)
\]
induces canonically a homeomorphism
\[ \Phi_f : \text{Spec}(k_f) \xrightarrow{\sim} D(f) \subseteq \text{Spec}(k) \]

such that

\[ \Phi_f(q) = \{ \alpha \in k \mid \alpha/1 \in q \} \quad (q \in \text{Spec}(k_f)), \quad (3) \]
\[ \Phi_f^{-1}(p) = p_f := \{ \alpha/f^n \mid \alpha \in k, \ n \in \mathbb{N} \} \quad (p \in D(f)). \quad (4) \]

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

\[ \Phi_f(D(g/f^n)) = D(f) \cap D(g) = D(fg). \quad (5) \]

Finally, for a \( k \)-linear map \( \varphi : M \to N \) of \( k \)-modules \( M, N \), we denote

\[ \text{ny}_{\varphi} : M \to N \]

its \( k \)-linear extension.

**10.6. Principal open sets of idempotents.** Let \( \varepsilon \in k \) be an idempotent and \( M \) a \( k \)-module. We put

\( \varepsilon_+ := \varepsilon, \varepsilon_- := 1 - \varepsilon, k_\pm := \varepsilon_\pm k, M_\pm := \varepsilon_\pm M = k_\pm M \) and have

\( k = k_+ \oplus k_- \) as a direct sum of ideals, \( M = M_+ \oplus M_- \) as a direct sum of submodules. The projections

\[ \pi_\pm : k \to k_\pm, \quad \alpha \mapsto \varepsilon_\pm \alpha, \quad (1) \]

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

\[ M_{k_\pm} = M \otimes k_\pm = M_\pm \quad (2) \]

as \( k_\pm \)-modules such that

\[ x \otimes \alpha_\pm = \alpha_\pm x = \alpha_\pm x_\pm \quad (\alpha_\pm \in k_\pm, \ x \in M). \quad (3) \]

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

Specializing \( f \) to \( \varepsilon \) in [10.5] we obtain

\[ k_\varepsilon = \{ \alpha/\varepsilon \mid \alpha \in k_+ \} = \{ \alpha/1 \mid \alpha \in k_+ \} = \{ \alpha/1 \mid \alpha \in k \}. \quad (4) \]

There is a unique morphism \( \pi_+: k_\varepsilon \to k_+ \) in \( k\text{-alg} \) that makes the diagram

\[ \begin{array}{ccc}
k & \xrightarrow{\pi_+} & k_+ \\
\downarrow \text{can} & & \downarrow \text{can} \\
k_\varepsilon, & \xrightarrow{\pi_\varepsilon} & k_+ \\
\end{array} \quad (5) \]

commutative and is actually an isomorphism. By [10.5] therefore,

\[ \text{Spec}(\pi_+) : \text{Spec}(k_+) \to \text{Spec}(k) \]
induces canonically a homeomorphism $\text{Spec}(k_+) \sim D(\mathfrak{p}) \subseteq \text{Spec}(k)$. Note that
\begin{equation}
\text{Spec}(\pi_+(\mathfrak{p}_+)) = \mathfrak{p}_+ \oplus k_- \in D(\mathfrak{p})
\end{equation}
for all $\mathfrak{p}_+ \in \text{Spec}(k_+)$. 

\textbf{10.7. Projective modules.} Recall that a $k$-module $M$ is projective if it is a direct summand of a free $k$-module. This property is stable under base change, i.e., if $M$ is projective over $k$, then so is $M_R = M \otimes R$ over $R$, for all $R \in k\text{-alg}$. Given a projective $k$-module $M$, a theorem of Kaplansky \cite{Kap} (see also Scheja-Storch \cite{SchSt} § 88, Aufg. 45) shows that $M_p$ is a free $k_p$-module, possibly of infinite rank, for all prime ideals $p \subseteq k$. Hence to every projective $k$-module $M$ we can associate its \textit{rank function}
\begin{equation}
\text{Spec}(k) \longrightarrow \mathbb{N} \cup \{\infty\}, \quad \mathfrak{p} \longmapsto \text{rk}_p(M) := \text{rk}_{k_p}(M_p) = \dim_{k(\mathfrak{p})} (M(\mathfrak{p})).
\end{equation}
By \cite{SchSt} II. Theorem 1] a $k$-module $M$ is finitely generated projective if and only if, for all $\mathfrak{p} \in \text{Spec}(k)$, the $k_p$-module $M_p$ is free of finite rank and the rank function of $M$ is locally constant relative to the Zariski topology of $\text{Spec}(k)$. For a projective $k$-module $M$ and $r \in \mathbb{N}$, we say $M$ has \textit{rank} $r$ if $\text{rk}_p(M) = r$ for all $\mathfrak{p} \in \text{Spec}(k)$. This condition forces $M$ to be finitely generated and determines $r$ uniquely, unless $k = \{0\}$, in which case $M = \{0\}$ has rank $r$ for any $r \in \mathbb{N}$. If $M$ is projective but not necessarily finitely generated, the preceding terminology makes sense and will be used also for $r = \infty$.

Finally, we deviate slightly from the terminology of Knus \cite{Knus} I §9, p. 52] by calling a $k$-module \textit{faithfully projective} if it is projective and faithful.

\textbf{10.8. Line bundles.} As usual, a \textit{line bundle} over $k$ is defined as a finitely generated projective $k$-module of rank 1. This means that the following two equivalent conditions are fulfilled.

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

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

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

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

(b) $\text{Pic}(k) := \{[L] | L$ is a line bundle over $k\}$, where $[L]$ stands for the isomorphism class of $L$, is an abelian group under the operation $[L][L'] := [L \otimes L']$, with unit element and inverse of $[L]$ given by $[k]$ and $[L^*]$, respectively. $\text{Pic}(k)$ is called the \textit{Picard group} of $k$.

(c) For $R \in k\text{-alg}$, $L_R = L \otimes R$ is a line bundle over $R$ and $L \mapsto L_R$ gives a group homomorphism $\text{Pic}(k) \rightarrow \text{Pic}(R)$. Thus we obtain a (covariant) functor $\text{Pic}$ from $k$-algebras to abelian groups.
10.9. **Faithful and unimodular elements.** Fixing a $k$-module $M$, we write $M^* = \text{Hom}_k(M, k)$ for the dual module of $M$ and $(x^*, x) \mapsto \langle x^*, x \rangle$ for the canonical pairing $M^* \times M \to k$. Given $x \in M$,

\[
\text{Ann}(x) := \{ \alpha \in k \mid \alpha x = 0 \}, \quad \langle M^*, x \rangle := \{ \langle x^*, x \rangle \mid x^* \in M^* \}
\]

are ideals in $k$, the former being called the **annihilator** of $x$, and we have

\[
\text{Ann}(x)(M^*, x) = \{ 0 \}.
\]

We say $x$ is **faithful** if $\text{Ann}(x) = \{ 0 \}$, equivalently, if the map $k \to M, \alpha \mapsto \alpha x$, is injective. A much stronger condition is provided by the notion of unimodularity: $x$ is said to be **unimodular** if $kx \subseteq M$ is a free submodule (of rank 1) and a direct summand of $M$ at the same time. This obviously happens if and only if $(x^*, x) = 1$ for some $x^* \in M^*$, i.e., $(M^*, x) = k$; in this case, the $k$-module $kx$ has $\{ x \}$ as a basis. Note that for an element of a projective (hence free) module $M$ over a **local** ring $k$ to be unimodular it is necessary and sufficient that it can be extended to a basis of $M$.

Unimodular elements are faithful but not conversely since unimodularity is stable under base change while faithfulness is not. Therefore we call $x \in M$ **strictly faithful** if $x_R \in M_R$ is faithful for all $R \in k\text{-alg}$. Given a unital $k$-algebra $A$, the identity element $1_A \in A$ is faithful if and only if $A$ is faithful as a $k$-module: $\alpha A = \{ 0 \}$ implies $\alpha = 0$, for all $\alpha \in k$.

10.10. **A notational ambiguity.** Let $M$ be a $k$-module, $x^* \in M^*$ and $R \in k\text{-alg}$. Then the symbol $x_R^* := (x^*)_R$ can be interpreted in two ways: on the one hand, as $x_R^* = x^* \otimes 1_R$ via (10.11), which belongs to $(M^*)_R$, on the other as $x_R^* = x^* \otimes 1_R: M_R \to k_R = R$ via (10.10), which belongs to $(M_R)^*$. In general, these interpretations lead to completely different objects, but, as the following result shows, in an important special case they may be identified under a canonical isomorphism. In fact, this isomorphism survives as a homomorphism in full generality as follows:

For a $k$-module $M$ and any $R \in k\text{-alg}$ as above, the assignment $x^* \mapsto x^* \otimes 1_R$ determines a $k$-linear map $M^* \to (M_R)^*$, which by (10.11) gives rise to an $R$-linear map $\varphi: (M^*)_R \to (M_R)^*$ satisfying $\varphi(x^* \otimes r) = r(x^* \otimes 1_R)$ for all $x^* \in M^$, $r \in R$.

10.11. **Lemma.** Let $M$ be a finitely generated projective $k$-module and $R \in k\text{-alg}$. Then the natural map

\[
\varphi: (M^*)_R \longrightarrow (M_R)^*, \quad x^* \otimes r \longmapsto r(x^* \otimes 1_R)
\]

is an isomorphism of $R$-modules. Identifying $(M^*)_R = (M_R)^*$ via $M_R^1$ by means of this isomorphism, we have $\langle x^*, x \rangle_R = \langle x_R^*, x_R \rangle$ for all $x \in M, x^* \in M^*$, in other words, the
Lemma 10.11, we therefore obtain
\[ (v) \Rightarrow (i) \Rightarrow (iii). \]

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

1.10.12. Lemma. (Loos [71]) Assume \( M \) is a finitely generated projective \( k \)-module and let \( x \in M \). If \( p \subseteq k \) is a prime ideal, then \( x(p) = 0 \) if and only if \( \langle M^\ast, x \rangle \subseteq p \).

Proof. \( M(p) \) being a vector space over \( \kappa(p) \), we have \( x(p) = 0 \) if and only if \( \langle y^\ast, x(p) \rangle = 0 \) for all \( y^\ast \in M(p)^\ast \). Identifying \( M(p)^\ast = M(p)^\ast(p) \) by means of Lemma [10.11] we therefore obtain
\[
\begin{align*}
x(p) = 0 & \iff \langle x^\ast(p), x(p) \rangle = 0 \quad \text{for all } x^\ast \in M^\ast \\
& \iff \langle x^\ast, x \rangle(p) = 0 \quad \text{for all } x^\ast \in M^\ast \\
& \iff \langle x^\ast, x \rangle \in p \quad \text{for all } x^\ast \in M^\ast \\
& \iff \langle M^\ast, x \rangle \subseteq p.
\end{align*}
\]
□

1.10.13. Lemma. Consider the following conditions, for a \( k \)-module \( M \) and \( x \in M \).

(i) \( x \) is unimodular.
(ii) \( x \) is strictly faithful.
(iii) \( x_R \neq 0 \) for all \( R \in k\text{-}\text{alg} \) with \( R \neq \{0\} \).
(iv) \( x_K \neq 0 \) for all fields \( K \in k\text{-}\text{alg} \).
(v) \( x(p) \neq 0 \) for all \( p \in \text{Spec}(k) \).

Then the implications
\[
(i) \implies (ii) \implies (iii) \iff (iv) \iff (v)
\]
hold, and if \( M \) is finitely generated projective, then all five conditions are equivalent.

Proof. Since the implications (i) \( \Rightarrow \) (ii) \( \Rightarrow \) (iii) \( \Rightarrow \) (iv) \( \Rightarrow \) (v) are obvious, while (v) \( \Rightarrow \) (i) follows immediately from Lemma [10.12], if \( M \) is finitely generated projective, it remains to prove (v) \( \Rightarrow \) (iv) \( \Rightarrow \) (iii).

(v) \( \Rightarrow \) (iv). If \( K \in k\text{-}\text{alg} \) is a field, the kernel of the natural map \( k \to K \) is a prime ideal \( p \subseteq k \), making \( K/\kappa(p) \) a field extension, and \( x_K = x(p)_K \neq 0 \) by (v).

(iv) \( \Rightarrow \) (iii). Let \( \{0\} \neq R \in k\text{-}\text{alg} \) and \( m \subseteq R \) be a maximal ideal. Then \( K := R/m \in k\text{-}\text{alg} \) is a field and \( (x_K)_K = x_K \neq 0 \) by (iv), forcing \( x_R \neq 0 \). □
10.14. Tensor products of algebras. Given $k$-algebras $A, B$, the $k$-module $A \otimes B$ is again a $k$-algebra under the multiplication

$$(x_1 \otimes y_1)(x_2 \otimes y_2) = (x_1, x_2)(y_1, y_2) \quad (x_i, y_i \in A, B, i = 1, 2). \quad (1)$$

Moreover, if $A$ and $B$ are both unital, so is $A \otimes B$, with unit element $1_{A \otimes B} = 1_A \otimes 1_B$.

For example, given any unital $k$-algebra $A$ and a positive integer $n$, we have a natural identification $\text{Mat}_n(k) \otimes A = \text{Mat}_n(A)$ such that $x \otimes a = xa = (\xi_{ij} a)$ for $x = (\xi_{ij}) \in \text{Mat}_n(k), a \in A$.

Now let $A$ be a $k$-algebra and $R \in k\text{-alg}$. Then the $R$-module structure of $A_R$\[10.1\] is compatible with the $k$-algebra structure of $A \otimes R$ as defined in (1). In other words, $A_R$ is canonically an $R$-algebra, and the observations made in [10.1]–[10.9] carry over mutatis mutandis from modules to algebras. In particular, the assignment $A \mapsto A_R$ gives a functor from $k$-algebras to $R$-algebras.

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

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

$$R : \text{Cent}(A) \xrightarrow{\sim} \text{End}_{\text{Mult}(A)}(A)$$

of $k$-algebras.

Proof. For $a \in \text{Cent}(A)$, $R_a$ clearly belongs to $\text{End}_{\text{Mult}(A)}(A)$, so we obtain a unital homomorphism $R : \text{Cent}(A) \to \text{End}_{\text{Mult}(A)}(A)$, which is obviously injective. To show that it is also surjective, let $d \in \text{End}_{\text{Mult}(A)}(A)$ act on $A$ from the right by juxtaposition. Then $(xy)d = x(yd) = (xd)y$ for all $x, y \in A$. Putting $y = 1_A$, we conclude $d = R_a$, where $a := 1_A d$. Hence the preceding relation is equivalent to $(xy)a = x(ya) = (xa)y$, which in turn is easily seen to imply that $a$ belongs to the centre of $A$. \hfill \Box

10.16. Corollary. The centre of a unital simple algebra is a field.

Proof. Since $\text{Mult}(A)$ acts irreducibly on $A$, it suffices to combine Prop. [10.15] with Schur’s lemma [47, p. 118]. \hfill \Box

For the remainder of this section, we use Prop. [10.15] to identify $\text{Cent}(A) = \text{End}_{\text{Mult}(A)}(A)$ for any unital $k$-algebra $A$.

10.17. Corollary. Let $A$ be a unital finite-dimensional algebra over a field $k$ and suppose $A$ is simple. Then $\text{End}_{\text{Cent}(A)}(A) = \text{Mult}(A)$.

Proof. Since $\text{Mult}(A)$ acts faithfully and irreducibly on $A$, it is a primitive Artinian $k$-algebra [47, Def. 4.1]. Moreover, by Prop. [10.15] its centralizer in $\text{End}_k(A)$ is $\text{Cent}(A)$. Thus the assertion follows from the double centralizer theorem [47, Thm. 4.10]. \hfill \Box
Algebras that are both central and simple are called central simple.

10.18. Corollary. A unital finite-dimensional algebra $A$ over a field $k$ is central simple if and only if it is non-zero and $\text{Mult}(A) = \text{End}_k(A)$.

Proof. If $A$ is central simple, the assertion follows from Cor. [10.17] Conversely, suppose $A \neq \{0\}$ and $\text{Mult}(A) = \text{End}_k(A)$. Then $A$ is simple, and Cor. [10.17] implies that $\text{Cent}(A)$ belongs to the centre of $\text{End}_k(A)$. Hence $A$ is central. □

10.19. Corollary. For a unital finite-dimensional algebra $A$ over a field $k$, the following conditions are equivalent.

(i) $A$ is central simple.
(ii) Every base field extension of $A$ is central simple.
(iii) $A \otimes \bar{k}$ is simple, where $\bar{k}$ denotes the algebraic closure of $k$.

Proof. (i) $\Rightarrow$ (ii). Let $k'$ be an extension field of $k$ and put $A' = A \otimes k'$ as a $k'$-algebra. After identifying $\text{End}_{k'}(A') = \text{End}_k(A) \otimes k'$ canonically, a moment’s reflection shows $\text{Mult}(A') = \text{Mult}(A) \otimes k'$. Hence the assertion follows from Cor. [10.18] (ii) $\Rightarrow$ (iii). Obvious.
(iii) $\Rightarrow$ (i). If $I \subseteq A$ is a non-trivial ideal, then so is $I \otimes \bar{k} \subseteq A \otimes \bar{k}$, a contradiction. Hence $A$ is simple. By Exc. [44] (a), $\text{Cent}(A) \otimes \bar{k}$ agrees with the centre of $A \otimes \bar{k}$ and therefore is a finite algebraic field extension of $k$. As such, it has degree 1, forcing $\text{Cent}(A) = k1_A$, and $A$ is central. □

Exercises.

38. Centre and nucleus under base change. Show that the centre (resp. the nucleus) of a unital $k$-algebra $A$ in general does not commute with base change, even if one assumes that the centre (resp. the nucleus) be free of finite rank and a direct summand of $A$ as a $k$-module. (Hint. Let $A$ be the unital $\mathbb{Z}$-algebra given on a free $\mathbb{Z}$-module of rank 3 with basis $1_A, x, y$ by the multiplication table $x^2 = 2 \cdot 1_A, xy = yx = y^2 = 0$ and consider its base change to $R := \mathbb{Z}/2\mathbb{Z} \in k$-alg.)

39. Fibers of prime spectra. Let $\varphi: k \rightarrow k'$ be a homomorphism of commutative rings, let $p \in \text{Spec}(k)$ and view $k'$ as a $k$-algebra by means of $\varphi$. Consider the ring homomorphism

$$\psi: k' \rightarrow k' \otimes \kappa(p), \quad \alpha' \mapsto \psi(\alpha') := \alpha' \otimes 1_{\kappa(p)}$$

and show that the continuous map

$$\text{Spec}(\psi): \text{Spec}(k') \rightarrow \text{Spec}(k)$$

induces canonically a homeomorphism

$$\text{Spec}(k' \otimes \kappa(p)) \rightarrow \text{Spec}(\varphi^{-1}(p)),$$

where the right-hand side carries the topology induced from the Zariski topology of $\text{Spec}(k')$.

40. Put $X := \text{Spec}(k)$.

(a) Let $\psi, \chi: M \rightarrow N$ be $k$-linear maps of $k$-modules and suppose $M$ is finitely generated. Show that

$$U := \{p \in X \mid \psi_p = \chi_p\}$$

is a Zariski-open subset of $X$. 

(b) Let $\varphi : A \to B$ be a $k$-linear map of $k$-algebras and suppose $A$ is finitely generated as a $k$-module. Prove that

$$V := \{ p \in X \mid \varphi_p : A_p \to B_p \text{ is an algebra homomorphism}\}$$

is a Zariski-open subset of $X$.

41. Idempotents and partitions. Consider $X = \text{Spec}(k)$ under the Zariski topology as in \[10.4\]

(a) Let $\epsilon \in k$ be an idempotent. Prove

$$D(\epsilon) = \{ p \in X \mid \epsilon_p = 1_p \} = \{ p \in X \mid \epsilon_p \neq 0 \} = V(1 - \epsilon).$$

Conclude for an orthogonal system $(\epsilon_i)_{i \in I}$ of idempotents in $k$ that $\bigcup D(\epsilon_i) = D(\sum \epsilon_i)$ and the union on the left is disjoint.

(b) Prove that the assignment $(\epsilon_i)_{i \in I} \mapsto (D(\epsilon_i))_{i \in I}$ yields a bijection from the set of complete orthogonal systems of idempotents in $k$ in the sense of \[9.3\] (b) onto the set of decompositions of $X$ into the disjoint union of open subsets almost all of which are empty. (Hint. To prove surjectivity, you may either argue with the structure sheaf of the geometric (= locally ringed) space attached to $k$ (Grothendieck \[56\] Chap. 1, § 1), Demazure-Gabriel \[22\] I, § 1, no. 1.2, particularly Prop. 2.6], Hartshorne \[39\] II, § 2) or imitate the proof of Bourbaki \[11\] II, § 4, Prop. 15], but watch out in the latter case for a sticky point on lines 2, 3, p. 104.)

42. Rank decomposition. Let $M$ be a finitely generated projective $k$-module. Prove:

(a) The set

$$\text{Rk}(M) := \{ \text{rk}_p(M) \mid p \in \text{Spec}(k) \}$$

is finite.

(b) There exists a unique complete orthogonal system $(\epsilon_i)_{i \in \mathbb{N}}$ of idempotents in $k$ such that, with the induced decompositions

$$k = \bigoplus_{i \in \mathbb{N}} k_i, \quad k_i = k \epsilon_i \quad (i \in \mathbb{N}), \quad (1)\,$$

$$M = \bigoplus_{i \in \mathbb{N}} M_i, \quad M_i = M \otimes k_i \quad (i \in \mathbb{N}), \quad (2)\,$$

as direct sums of ideals (resp. of additive subgroups), the $k_i$-modules $M_i$ are finitely generated projective of rank $i$, for all $i \in \mathbb{N}$. Show further that $\epsilon_i = 0$ for all $i \in \mathbb{N} \setminus \text{Rk}(M)$.

Remark. Equation \[2\] is called the rank decomposition of $M$. It remains virtually unchanged by ignoring the components belonging to some or all indices $i \in \mathbb{N} \setminus \text{Rk}(M)$. Note also that, if $M$ carries an algebra structure, \[3\] is a direct sum of ideals.

43. Residually simple algebras. (Cf. Knus \[58\] III, (5.1.8)) Let $A$, $A'$ be unital $k$-algebras that are finitely generated projective of the same rank $r \in \mathbb{N}$ as $k$-modules. Suppose $A$ is residually simple, so $A(p)$ is a simple algebra over the field $k(p)$, for all $p \in \text{Spec}(k)$. Prove that every unital algebra homomorphism from $A$ to $A'$ is an isomorphism.

44. Groups of automorphisms.\[1\] By an algebra with a group of automorphisms over $k$ we mean a pair $(A, G)$ consisting of a $k$-algebra $A$ and a group $G$ of automorphisms or anti-automorphisms of $A$. An ideal of $(A, G)$ is an ideal of $A$ which is stabilized by every element of $G$. We say that $(A, G)$ is simple if $A^2 \neq \{0\}$ and there are no ideals of $(A, G)$ other than $\{0\}$ and $A$. If $A$ contains an identity element, in which case we also say that $(A, G)$ is unital, we define the center of $(A, G)$ as the set of elements in the center of $A$ that remain fixed under $G$:

\[1\] This is not a misprint.
Cent(A, G) = \{a \in \text{Cent}(A) \mid g(a) = a \text{ for all } g \in G\}.

If the natural map from \(k\) to \(\text{Cent}(A, G)\) is an isomorphism of \(k\)-algebras, then \((A, G)\) is said to be central. Unital algebras with a group of automorphisms which are both central and simple are called central simple. By the multiplication algebra of \((A, G)\), written as \(\text{Mult}(A, G)\), we mean the unital subalgebra of \(\text{End}_k(A)\) generated by \(G\) and all left and right multiplications affected by arbitrary elements of \(A\). Base change of algebras with a group of automorphisms is defined canonically. Note that ordinary \(k\)-algebras are algebras with a group of automorphisms in a natural way, as are algebras with involution.

Now let \(k\) be a field and \((A, G)\) a \(k\)-algebra with a group of automorphisms. Then prove:

(a) \(\text{Cent}(\mathcal{A}) \otimes R) = \mathcal{A}(\mathcal{A}) \otimes R\) as \(R\)-algebras, for any \(R \in k\text{-alg}\).

(b) The right multiplication of \(A\) induces an isomorphism

\[
R : \text{Cent}(A, G) \xrightarrow{\sim} \text{End}_{\text{Mult}(A, G)}(A)
\]

of \(k\)-algebras.

(c) The centre of a unital simple algebra with a group of automorphisms is a field.

(d) If \((A, G)\) is finite-dimensional, then \(\text{End}_{\text{Cent}(A, G)}(A) = \text{Mult}(A, G)\), and for \((A, G)\) to be central simple it is necessary and sufficient that \(A \neq \{0\}\) and \(\text{Mult}(A, G) = \text{End}_k(A)\).

### 45. Central simplicity of algebras with groups of automorphisms

Let \((A, G)\) be a finite-dimensional unital algebra with a group of automorphisms over a field \(k\). Then show that the following conditions are equivalent.

(i) \((A, G)\) is central simple.

(ii) Every base field extension of \((A, G)\) is central simple.

(iii) \((A, G) \otimes \bar{k}\) is simple, where \(\bar{k}\) denotes the algebraic closure of \(k\).

### 46. Tensor products of algebras with groups of automorphisms

Let \((A, G), (A', G')\) be unital \(k\)-algebras with a group of automorphisms and suppose (i) \(A\) is commutative or \(G' \subseteq \text{Aut}(A')\), and (ii) \(A'\) is commutative or \(G \subseteq \text{Aut}(A)\). Define \((A, G) \otimes (A', G') = (A \otimes A', G \otimes G')\), where \(G \otimes G'\) is supposed to consist of all \(g \otimes g', g \in G, g' \in G'\) having the same parity in the sense that they are both either automorphisms or anti-automorphisms of \(A, A'\), respectively. Show that if \((A, G)\) is central simple and \((A', G')\) is simple, then \((A, G) \otimes (A', G')\) is simple.

### 11. Involutions

Involutions of associative algebras are a profound concept with important connections to other branches of algebra and arithmetic. An in-depth account of this concept over fields may be found in Knus-Merkurjev-Rost-Tignol [59]. Over arbitrary commutative rings, the reader may consult Knus [58 III, § 8] for less complete but still useful results on the subject. In the present section, elementary properties of involutions will be studied for unital non-associative algebras.

#### 11.1. Algebras with involution

An involution of a unital \(k\)-algebra \(B\) is a \(k\)-linear map \(\tau : B \rightarrow B\) satisfying the following conditions.

(i) \(\tau\) is involutorial, i.e., \(\tau^2 = 1_B\).

(ii) \(\tau\) is an anti-homomorphism, i.e., \(\tau(xy) = \tau(y)\tau(x)\) for all \(x, y \in B\).
In particular, \( \tau \) is bijective, hence by (ii) may be viewed as an isomorphism \( \tau : B \to B^{\text{op}} \) of \( k \)-algebras, where the opposite algebra \( B^{\text{op}} \) lives on the same \( k \)-module as \( B \) under the new multiplication \( x \cdot y := yx \) for \( x, y \in B \). Examples of involutions are provided by the conjugation of the Graves-Cayley octonions or the Hamiltonian quaternions (Exc. 11.3.1(a)).

### 11.2. Homomorphisms, base change and ideals of algebras with involution.

By a **k-algebra with involution** we mean a pair \( (B, \tau) \) consisting of a unital \( k \)-algebra \( B \) and an involution \( \tau \) of \( B \). A homomorphism \( h : (B, \tau) \to (B', \tau') \) of \( k \)-algebras with involution is a unital homomorphism \( h : B \to B' \) of \( k \)-algebras that respects the involutions, i.e., \( \tau' \circ h = h \circ \tau \). In this way, we obtain the category of \( k \)-algebras with involution. If \( (B, \tau) \) is a \( k \)-algebra with involution, then \( (B, \tau)_R := (B_R, \tau_R) \) for \( R \in k \text{-alg} \) is an \( R \)-algebra with involution, called the **scalar extension** or base change of \( (B, \tau) \) from \( k \) to \( R \). By an ideal of \( (B, \tau) \) we mean an ideal \( I \subseteq B \) that is stabilized by \( \tau \): \( \tau(I) = I \). In this case, \( (B, \tau)/I := (\bar{B}, \bar{\tau}) \), with \( \bar{B} := B/I \) and \( \bar{\tau} : \bar{B} \to \bar{B} \) being the \( k \)-linear map canonically induced by \( \tau \), is a \( k \)-algebra with involution making the canonical projection \( B \to \bar{B} \) a homomorphism \( (B, \tau) \to (\bar{B}, \bar{\tau}) \) of \( k \)-algebras with involution.

### 11.3. The centre of an algebra with involution.

If \( (B, \tau) \) is a \( k \)-algebra with involution, then \( \tau \) stabilizes the centre of \( B \), and via restriction we obtain an involution of \( \text{Cent}(B) \), i.e., an automorphism of period 2. We call

\[
\text{Cent}(B, \tau) := \{ a \in \text{Cent}(B) \mid \tau(a) = a \}
\]

the centre of \( (B, \tau) \). It is a unital (commutative associative) subalgebra of \( \text{Cent}(B) \).

### 11.4. Simplicity and the exchange involution

Let \( (B, \tau) \) be a \( k \)-algebra with involution. We say that \( (B, \tau) \) is **simple** (as an algebra with involution) if \( B \) has non-trivial multiplication and there are no ideals of \( (B, \tau) \) other than \( \{0\} \) and \( B \). If \( B \) is simple, so obviously is \( (B, \tau) \). The converse, however, does not hold. To see this, we consider the following class of examples.

Let \( A \) be a unital \( k \)-algebra. Then a straightforward verification shows that the map

\[
\varepsilon_A : A^{\text{op}} \oplus A \to A^{\text{op}} \oplus A, \quad x \oplus y \mapsto \varepsilon_A(x \oplus y) := y \oplus x,
\]

is an involution, called the **exchange involution** (or switch) of \( A^{\text{op}} \oplus A \).

### 11.5. Proposition

Let \( (B, \tau) \) be a \( k \)-algebra with involution. For \( (B, \tau) \) to be simple as an algebra with involution it is necessary and sufficient that \( B \) be simple or there exist a simple unital \( k \)-algebra \( A \) such that \( (B, \tau) \cong (A^{\text{op}} \oplus A, \varepsilon_A) \).

**Proof.** By Exc. 32 the condition is clearly sufficient. Conversely, suppose \( (B, \tau) \) is simple but \( B \) is not. Let \( \{0\} \neq I \subseteq B \) be any proper ideal of \( B \). Then \( \tau(I) + I, \tau(I) \cap I \) are both ideals of \( (B, \tau) \), the former being different from \( \{0\} \), the latter being different from \( B \). Since \( (B, \tau) \) is simple, we conclude \( B = \tau(I) \oplus I \) as a direct sum.
of ideals. Regarding \( A = I \) as a unital \( k \)-algebra in its own right, any non-zero ideal \( J \) of \( A \) is a proper ideal of \( B \), so by what we have just shown, \( B = \tau(J) \oplus J \), which implies \( J = A \), and \( A \) is simple. One now checks easily that the map
\[
(A^{\text{op}} \oplus A, e_A) \xrightarrow{\sim} (B, \tau), \quad x \oplus y \mapsto \tau(x) + y,
\]
is an isomorphism of algebras with involution. \( \square \)

11.6. Symmetric and skew elements. Let \((B, \tau)\) be a \( k \)-algebra with involution. Following the notational conventions of \([59, \S 2]\), we put
\[
H(B, \tau) := \text{Sym}(B, \tau) := \{ x \in B \mid \tau(x) = x \},
\]
\[
\text{Symd}(B, \tau) := \{ y + \tau(y) \mid y \in B \},
\]
\[
\text{Skew}(B, \tau) := \{ x \in B \mid \tau(x) = -x \},
\]
\[
\text{Alt}(B, \tau) := \{ y - \tau(y) \mid y \in B \},
\]
which are all submodules of \( B \), the first one among these containing the identity of \( B \). The elements of \( \text{Sym}(B, \tau) \) (resp. \( \text{Skew}(B, \tau) \)) are called \textit{\( \tau \)-symmetric} (resp. \( \tau \)-skew). If \( k \) contains \( \frac{1}{2} \), then \( \text{Sym}(B, \tau) = \text{Symd}(B, \tau) \), \( \text{Skew}(B, \tau) = \text{Alt}(B, \tau) \), and \( B = \text{Sym}(B, \tau) \oplus \text{Skew}(B, \tau) \) as a direct sum of submodules. At the other extreme, if \( 2 = 0 \) in \( k \), then
\[
\text{Symd}(B, \tau) = \text{Alt}(B, \tau) \subseteq \text{Sym}(B, \tau) = \text{Skew}(B, \tau),
\]
and in general this containment is proper.

11.7. Ample submodules. Let \((B, \tau)\) be an associative \( k \)-algebra with involution. Then \( \text{Symd}(B, \tau) \) is a \( \tau \)-ample submodule of \( B \) in the sense that \( x \text{Symd}(B, \tau) \tau(x) \subseteq \text{Symd}(B, \tau) \) for all \( x \in B \). This follows from \((11.6.2)\) and \( x(z + \tau(z)) \tau(x) = xz \tau(x) + \tau(xz \tau(x)) \) for all \( z \in B \).

11.8. The conjugate transpose involution. Let \( B \) be a unital \( k \)-algebra and \( \tau : B \to B, x \mapsto \bar{x} \), an involution of \( B \). Given \( n \in \mathbb{Z}, n > 0 \), it is readily checked that the map
\[
\text{Mat}_n(\tau) : \text{Mat}_n(B) \longrightarrow \text{Mat}_n(B), \quad x \mapsto \bar{x}',
\]
which sends an \( n \times n \) matrix over \( B \) into its conjugate transpose, is an involution of \( \text{Mat}_n(B) \), called the \textit{conjugate transpose involution} induced by \( \tau \). We put
\[
\text{Mat}_n(B, \tau) := \left( \text{Mat}_n(B), \text{Mat}_n(\tau) \right), \quad \text{Sym}_n(B, \tau) := \text{Sym} \left( \text{Mat}_n(B), \text{Mat}_n(\tau) \right).
\]
In the special case \( B = k, \tau = 1_k \), we obtain
\[
\tau_{\text{ort}} : \text{Mat}_n(k) \longrightarrow \text{Mat}_n(k), \quad S \mapsto \tau(S) := S',
\]
called the \textit{split orthogonal involution of degree} \( n \) \textit{over} \( k \). We put
11.11. The split symplectic involution of degree $n$. Let $n$ be a positive integer. We view the elements of $\text{Mat}_{2n}(k)$ as $2 \times 2$-blocks of $n \times n$-matrices over $k$. With this in mind, we put

$$I := I_n := \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \in \text{GL}_{2n}(k)$$

and have

$$I^2 = -I_{2n}, \quad I^{-1} = I' = -I.$$  

Hence we may form the $I$-twist \[11.9\] of the split orthogonal involution of degree $2n$ over $k$ \[11.8\], which we call the split symplectic involution of degree $n$ over $k$, denoted by

$$\tau_{spl} : \text{Mat}_{2n}(k) \rightarrow \text{Mat}_{2n}(k), \quad S \mapsto \tau_{spl}(S) := ISI^{-1} = IS'I' = I^{-1}SI.$$  

A verification shows

$$\tau_{spl}(S) = \begin{pmatrix} d' & -b' \\ -c' & d' \end{pmatrix} \quad (\text{for } S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_{2n}(k)), \quad (4)$$

and we conclude

$$\text{Sym} \left( \text{Mat}_{2n}(k), \tau_{spl} \right) = \left\{ \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \mid a \in \text{Mat}_n(k), b, c \in \text{Skew}_n(k) \right\}.$$  

In particular, $\text{Sym}_{n}(k)$ is a free $k$-module of rank $\frac{1}{2}n(n+1)$. 

11.9. Twisting involutions. Let $(B, \tau)$ be a $k$-algebra with involution and $q \in \text{Nuc}(B)^{\times}$ an invertible element of the unital associative subalgebra $\text{Nuc}(B) \subseteq B$ \[9.6\]. Then the map $B \rightarrow B, x \mapsto q^{-1}xq$ is an unambiguously defined automorphism, forcing

$$\tau^q : B \rightarrow B, \quad x \mapsto \tau^q(x) := q^{-1}\tau(x)q$$

to be an anti-automorphism of $B$. Moreover $\tau^q$ is an involution provided $\tau(q) = \pm q$, in which case we sometimes call $\tau^q$ the $q$-twist of $\tau$. 

11.10. Alternating matrices. For $n \in \mathbb{Z}$, $n > 0$, a matrix $S \in \text{Mat}_{n}(k)$ is said to be alternating if it satisfies one (hence all) of the following equivalent conditions.

(i) $S$ is skew-symmetric and its diagonal entries are zero.
(ii) $S = T - T'$ for some $T \in \text{Mat}_{n}(k)$.
(iii) $x'Tx = 0$ for all $x \in k^n$.

The submodule of $\text{Mat}_{n}(k)$ consisting of all alternating $n \times n$-matrices over $k$ will be denoted by $\text{Alt}_{n}(k)$. By \[11.8\] and \[11.6.4\], we obviously have $\text{Alt}_{n}(k) = \text{Alt}(\text{Mat}_{n}(k), \tau_{ort})$, which is a free $k$-module of rank $\frac{n(n-1)}{2}$. 

11 Involution
On the other hand, combining \(11.10\) (ii) with \(11.6.4\) and \(4\), we deduce that

\[
\text{Symd} \left( \text{Mat}_{2n}(k), \tau_{\text{sym}} \right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \in \text{Mat}_n(k), b, c \in \text{Alt}_n(k) \right\}
\]

is a free \(k\)-module of rank \(2n^2 - n\).

### 12. Quadratic maps

#### 12.1. The concept of a quadratic map.

Let \(M, N\) be \(k\)-modules. A map \(Q: M \to N\) is said to be quadratic if it satisfies the following two conditions.

1. \(Q\) is homogeneous of degree 2: \(Q(\alpha x) = \alpha^2 Q(x)\) for all \(\alpha \in k\) and all \(x \in M\).
2. The map \(DQ: M \times M \to N\), \((x, y) \mapsto (DQ)(x, y) := Q(x + y) - Q(x) - Q(y)\) is (symmetric) bilinear.

We sometimes call \(DQ\) the bilinearization or polar map belonging to \(Q\). Conditions (i), (ii) imply \((DQ)(x, x) = 2Q(x)\) for all \(x \in M\), so the quadratic map \(Q\) may be recovered from its polar map \(DQ\) if \(\frac{1}{2} \in k\) but not in general. At the other extreme, if \(2 = 0\) in \(k\), then \(DQ\) is alternating. In the general set-up, we often relax the notation and simply write \(Q(x, y)\) instead of \((DQ)(x, y)\) for \(x, y \in M\) if there is no danger of confusion. Quadratic forms are quadratic maps taking values in the base ring, hence arise in the special case \(N = k\). The polar map of a quadratic form is of course called its polar form. Examples are provided by the positive definite real quadratic forms of \(3.1\) and, more specifically, by the norm of the Graves-Cayley octonions \([1.3]\).

Elementary manipulations of quadratic maps, like scalar multiples, composition with linear maps and direct sums, are defined in the obvious manner; we omit the details. Less obvious are scalar extensions, which we address here in a slightly more general set-up. We begin with two preparations.

#### 12.2. Tensor products of bilinear maps.

If \(b: M \times M \to N\) and \(b': M' \times M' \to N'\) are bilinear maps between \(k\)-modules, then so is

\[
b \otimes b': (M \otimes M') \times (M \otimes M') \to N \otimes N', \quad (x \otimes x', y \otimes y') \mapsto b(x, y) \otimes b'(x', y').
\]

The same simple-minded approach does not work for quadratic maps, see Milnor-Husemoller [86, p. 111] for comments.

#### 12.3. Radicals of bilinear and quadratic maps.

Let \(M, N\) be \(k\)-modules and \(b: M \times M \to N\) a symmetric or skew-symmetric bilinear map. Then the submodu...
Rad(b) := \{x \in M \mid b(x,y) = 0 \text{ for all } y \in M\} \subseteq M \tag{1}

is called the \textit{radical} of \(b\). Now suppose we are given a \(k\)-module \(M_1\) and a surjective linear map \(\pi: M \rightarrow M_1\) such that \(\text{Ker}(\pi) \subseteq \text{Rad}(b)\). Then \(b\) factors uniquely through \(\pi \times \pi\) to a symmetric or skew-symmetric bilinear map \(b_1: M_1 \times M_1 \rightarrow N\) satisfying \(\text{Rad}(b_1) = \text{Rad}(b)/\text{Ker}(\pi)\).

Along similar lines, let \(Q: M \rightarrow N\) be a quadratic map. Then

\[
\text{Rad}(Q) := \{x \in \text{Rad}(DQ) \mid Q(x) = 0\} = \{x \in M \mid Q(x) = (DQ)(x,y) = 0 \text{ for all } y \in M\}
\]

is a submodule of \(M\), called the \textit{radical} of \(Q\). If, for \(M_1, \pi\) as above, we assume \(\text{Ker}(\pi) \subseteq \text{Rad}(Q)\), then \(Q\) factors uniquely through \(\pi\) to a quadratic map \(Q_1: M_1 \rightarrow N\) (well) defined by \(Q_1(x) := Q(x)\) for \(x \in M\). Moreover, \(\text{Rad}(Q_1) = \text{Rad}(Q)/\text{Ker}(\pi)\) and \(D(Q_1) = (DQ)_1\).

12.4. Proposition. Let \(M, N, V, W\) be \(k\)-modules, \(Q: M \rightarrow N\) a quadratic map and \(b: V \times V \rightarrow W\) a symmetric bilinear map. Then there exists a unique quadratic map

\[Q \otimes b: M \otimes V \rightarrow N \otimes W\]

such that

\[
(Q \otimes b)(x \otimes v) = Q(x) \otimes b(v, v) \quad (x \in M, v \in V), \tag{1}
\]

\[
D(Q \otimes b) = (DQ) \otimes b. \tag{2}
\]

\textit{Proof.} Uniqueness is clear, so we only have to show existence. We first consider the case that the \(k\)-module \(M\) is free, with basis \((e_i)_{i \in I}\) where we may assume the index set \(I\) to be totally ordered. Then every element \(z \in M \otimes V\) can be written uniquely as \(z = \sum_i e_i \otimes v_i, v_i \in V\), and setting

\[(Q \otimes b)(z) := \sum_i Q(e_i) \otimes b(v_i, v_i) + \sum_{i < j} Q(e_i, e_j) \otimes b(v_i, v_j),\]

we obtain a quadratic map which, since \(b\) is symmetric, has the desired properties. Now let \(M\) be arbitrary. Then there exists a short exact sequence

\[
0 \longrightarrow L \overset{i}{\longrightarrow} F \overset{\pi}{\longrightarrow} M \longrightarrow 0
\]

of \(k\)-modules, where \(F\) is free. Since the functor \(- \otimes V\) is right exact \([12, \text{II, § 3, Prop. 5}]\), we obtain an induced exact sequence

\[
L' \overset{\ell}{\longrightarrow} F' \overset{\pi'}{\longrightarrow} M' \longrightarrow 0,
\]

and the special case just treated yields a quadratic map \(\hat{Q} := (Q \circ \pi) \otimes b: F' \rightarrow N \otimes W\) satisfying \((1), (2)\). Let \(z = \sum u_j \otimes v_j \in L', u_j \in L, v_j \in V,\) and \(x \in F, v \in V\).
12.5. Corollary. Let $Q : M \to N$ be a $k$-quadratic map of $k$-modules and $R \in k$-alg.
Then there exists a unique $R$-quadratic map $Q_R : M_R \to N_R$ of $R$-modules making a
commutative diagram
\[
\begin{array}{ccc}
M & \xrightarrow{Q} & N \\
\downarrow & & \downarrow \\
M_R & \xrightarrow{Q_R} & N_R.
\end{array}
\]
In particular, $D(Q_R) = (DQ)_R$ is the $R$-bilinear extension of $DQ$. We call $Q_R$ the scalar extension or base change of $Q$ from $k$ to $R$.

Proof. Applying Prop. [12.4] to $Q$ and the symmetric bilinear map $b : R \times R \to R$
given by the multiplication of $R$, we obtain a $k$-quadratic map $Q_R : M_R \to N_R$, which
is in fact a quadratic map over $R$ satisfying the condition of the corollary. \hfill $\square$

We now proceed to list a few elementary properties of bilinear and quadratic forms.

12.6. Notation. Let $M$ be a $k$-module. Then we write $\text{Bil}(M)$ for the $k$-module
of bilinear forms on $M$. The submodules of $\text{Bil}(M)$ consisting of all symmetric, skew-symmetric, alternating bilinear forms on $M$ will be denoted respectively by $\text{Sbil}(M)$, $\text{Skil}(M)$, $\text{Abil}(M)$. Recall that a bilinear form $\sigma : M \times M \to k$ is alternating if $\sigma(x, x) = 0$ for all $x \in M$. We then have $\text{Abil}(M) \subseteq \text{Skil}(M)$ with equality if $\frac{1}{2} \in k$.

Finally, we write $\text{Quad}(M) := \text{Quad}(M)$ for the $k$-module of quadratic forms on $M$.
The assignment $q \mapsto D_q$ defines a linear map from $\text{Quad}(M)$ to $\text{Sbil}(M)$.

12.7. Connecting matrices with bilinear and quadratic forms. Let $n$ be a positive integer. For $S \in \text{Mat}_n(k)$, the map
\[
\langle S \rangle : k^n \times k^n \to k, \quad (x, y) \mapsto \langle S \rangle(x, y) := x^tSy
\]  
(1) is a bilinear form on $k^n$, and the assignment $S \mapsto \langle S \rangle$ gives a linear bijection from $\text{Mat}_n(k)$ onto $\text{Bil}(k^n)$ matching $\text{Sym}_n(k)$, $\text{Skew}_n(k)$, $\text{Alt}_n(k)$ respectively with $\text{Sbil}(k^n)$, $\text{Skil}(k^n)$, $\text{Abil}(k^n)$. If $S = \text{diag}(\alpha_1, \ldots, \alpha_n) \in \text{Mat}_n(k)$ is a diagonal matrix,
we put $\langle \alpha_1, \ldots, \alpha_n \rangle := \langle S \rangle$ as a symmetric bilinear form on $k^n$; it sends
\[
\begin{pmatrix}
\xi_1 \\
\vdots \\
\xi_n
\end{pmatrix}, \begin{pmatrix}
\eta_1 \\
\vdots \\
\eta_n
\end{pmatrix} \in k^n \times k^n \quad \text{to} \quad \sum_{i=1}^n \alpha_i \xi_i \eta_i.
\]

On the other hand, the map
\[
\langle S \rangle_{\text{quad}} : k^n \longrightarrow k, \quad x \mapsto \langle S \rangle_{\text{quad}}(x) := x^t S x
\]
is a quadratic form on $k^n$ such that $D\langle S \rangle_{\text{quad}} = \langle S + S^t \rangle$, and the assignment $S \mapsto \langle S \rangle_{\text{quad}}$ gives rise to a short exact sequence
\[
0 \longrightarrow \text{Alt}_n(k) \longrightarrow \text{Mat}_n(k) \longrightarrow \text{Quad}(k^n) \longrightarrow 0
\]
of $k$-modules. Thus, roughly speaking, quadratic forms on $k^n$ are basically the same as arbitrary $n \times n$-matrices modulo alternating $n \times n$-matrices over $k$. Again, if $S = \text{diag}(\alpha_1, \ldots, \alpha_n) \in \text{Mat}_n(k)$ is a diagonal matrix, we put $\langle \alpha_1, \ldots, \alpha_n \rangle_{\text{quad}} := \langle S \rangle_{\text{quad}}$ as a quadratic form form on $k^n$; it sends
\[
\begin{pmatrix}
\xi_1 \\
\vdots \\
\xi_n
\end{pmatrix} \in k^n \quad \text{to} \quad \sum_{i=1}^n \alpha_i \xi_i^2.
\]

12.8. Bilinear and quadratic forms on free modules. Let $M$ be a free $k$-module of finite rank $n > 0$ and $(e_i)_{1 \leq i \leq n}$ a basis of $M$ over $k$. Given a bilinear form $\sigma : M \times M \to k$, we call $S := (\sigma(e_i, e_j))_{1 \leq i, j \leq n} \in \text{Mat}_n(k)$ the matrix of $\sigma$ with respect to the basis $(e_i)$, and identifying $M = k^n$ by means of this basis matches $\sigma$ with the bilinear form $\langle S \rangle$ on $k^n$ [12.7]. On the other hand, given a quadratic form $q : M \to k$, we find a matrix $S = (s_{ij}) \in \text{Mat}_n(k)$ by
\[
s_{ij} := \begin{cases} 
q(e_i, e_j) & (1 \leq i < j \leq n), \\
q(e_i) & (1 \leq i = j \leq n), \\
0 & (1 \leq j < i \leq n).
\end{cases}
\]
We call $S$ the matrix of $q$ with respect to the basis $(e_i)$ and, again, identifying $M = k^n$ by means of this basis matches $q$ with the quadratic form $\langle S \rangle_{\text{quad}}$ on $k^n$.

12.9. Regularity conditions on bilinear forms. Let $\sigma : M \times M \to k$ be a symmetric or skew-symmetric bilinear form on a $k$-module $M$. For a submodule $N \subseteq M$, the submodule
\[
N^\perp := N^{\perp \sigma} := \{ x \in M \mid \sigma(x, y) = 0 \text{ for all } y \in N \} \subseteq M
\]
We call $S$ the matrix of $q$ with respect to the basis $(e_i)$ and, again, identifying $M = k^n$ by means of this basis matches $q$ with the quadratic form $\langle S \rangle_{\text{quad}}$ on $k^n$. 

12.9. Regularity conditions on bilinear forms. Let $\sigma : M \times M \to k$ be a symmetric or skew-symmetric bilinear form on a $k$-module $M$. For a submodule $N \subseteq M$, the submodule
\[
N^\perp := N^{\perp \sigma} := \{ x \in M \mid \sigma(x, y) = 0 \text{ for all } y \in N \} \subseteq M
\]
is called the orthogonal complement of $N$ in $M$. In particular, $M^\perp = \text{Rad}(\sigma)$ is the kernel of the natural map

$$\sigma : M \longrightarrow M^*, \quad x \longmapsto \sigma(x,-).$$

(2) $\sigma$ is said to be non-singular if

(i) $M$ is finitely generated projective as a $k$-module,

(ii) $\sigma : M \overset{\sim}{\longrightarrow} M^*$ is an isomorphism.

This implies $\text{Rad}(\sigma) = \{0\}$ but not conversely. Since passing to the dual of a finitely generated projective module is compatible with base change (Lemma 10.11), so is the property of a (skew-)symmetric bilinear form to be non-singular. If $M = k^n$ is free of finite rank $n$ and $S \in \text{Mat}_n(k)$ is (skew-)symmetric, then the (skew-)symmetric bilinear form $(S) : k^n \times k^n \rightarrow k$ is non-singular if and only if $S \in \text{GL}_n(k)$.

12.10. Lemma. Let $\sigma : M \times M \rightarrow k$ be a symmetric or skew-symmetric bilinear form over $k$ and suppose $N \subseteq M$ is a submodule on which $\sigma$ is non-singular. Then $M = N \oplus N^\perp$.

Proof. We write $\sigma'$ for the restriction of $\sigma$ to $N \times N$. Since $N \cap N^\perp = \text{Rad}(\sigma') = \{0\}$, it remains to show $M = N + N^\perp$, so let $x \in M$. Then $\sigma(x,-)$ restricts to a linear form on $N$, which by non-singularity of $\sigma'$ has the form $\sigma'(u,-)$ for some $u \in N$. Thus $\sigma(x,y) = \sigma(u,y)$ for all $y \in N$, and we conclude $x = u + v$, $v := x - u \in N^\perp$. $\square$

12.11. Regularity conditions on quadratic forms. A quadratic form $q : M \rightarrow k$ is said to be non-degenerate if $\text{Rad}(q) = \{0\}$. Unfortunately, this property is not invariant under base change, even if we allow $M$ to be finitely generated projective. Following Loos [70, 3.2] in a slightly more general vein, we therefore call $q$ separable if $M$ is projective, possibly of infinite rank, and the scalar extension $q_K$ is non-degenerate for all fields $K \in k$-alg. Indeed, the property of a quadratic form to be separable is clearly stable under base change. As a simple example, we note that the one-dimensional quadratic form $\langle \alpha \rangle_{\text{quad}}, \alpha \in k^o$, is always separable but becomes degenerate if $2 = 0$ in $k$ and $k$ is not reduced, i.e., contains non-zero nilpotent elements.

A regularity condition even stronger than separability is provided by the concept of non-singularity: $q$ is said to be non-singular if its induced symmetric bilinear form $Dq$ has this property. In this case, $M$ is finitely generated projective by [12.9](ii), and if $2 = 0$ in $k$, then $Dq$ is an alternating non-singular bilinear form, forcing $\text{rk}_p(M)$ to be even for all $p \in \text{Spec}(k)$. For a finitely generated free module $M = k^n$ over any commutative ring $k$ and $S \in \text{Mat}_n(k)$, the quadratic form $\langle S \rangle_{\text{quad}} : k^n \rightarrow k$ is non-singular if and only if $S + S' \in \text{GL}_n(k)$.

Finally, $q$ is said to be weakly non-singular if for all $u \in M$, the relation $q(u,v) = 0$ for all $v \in M$ implies $u = 0$. This is equivalent to $Dq : M \rightarrow M^*$ being injective. Note that weak non-singularity is not stable under base change, making this notion distinctly less interesting than the previous one.
12.12. Quadratic modules and spaces. It is sometimes linguistically convenient to think of a quadratic form $q: M \to k$ as a quadratic module $(M, q)$. Given quadratic modules $(M, q)$ and $(M', q')$ over $k$, a homomorphism $h: (M, q) \to (M', q')$ is a $k$-linear map $h: M \to M'$ satisfying $q' \circ h = q$. In this way one obtains the category of quadratic modules over $k$. Isomorphisms between quadratic modules over $k$ are called isometries. A quadratic module $(M, q)$ over $k$ is said to be a quadratic space if $q$ is non-singular. We write $(M, q) \perp (M', q')$ for the orthogonal sum of the quadratic modules $(M, q)$, $(M', q')$ defined on the direct sum $M \oplus M'$ by the quadratic form

$$q \perp q': M \oplus M' \to k, \quad x \oplus x' \mapsto q(x) + q'(x').$$

We sometimes use the alternate notation $(M, q) \oplus (M', q') := (M, q) \perp (M', q')$.

12.13. Pointed quadratic modules. By a pointed quadratic module over $k$ we mean a triple $(M, q, e)$ consisting of a quadratic module $(M, q)$ and a distinguished element $e \in M$, called the base point, such that $q(e) = 1$. Homomorphisms of pointed quadratic modules are defined as homomorphism of the underlying quadratic modules preserving base points in the obvious sense. We speak of $(M, q, e)$ as a pointed quadratic space if $(M, q)$ is a quadratic space.

Let $(M, q, e)$ be a pointed quadratic module over $k$. We call $q$ its norm, the linear form $t := (Dq)(e, -)$ on $M$ its trace and the linear map

$$t: M \to M, \quad x \mapsto \bar{x} := t(x)e - x, \quad (1)$$

its conjugation. Obviously, the trace satisfies $t(e) = 2$, while the conjugation has period 2 and preserves base point, norm and trace.

The following lemma, which is obvious but quite useful, has been communicated to me by O. Loos and E. Neher.

12.14. Lemma. Let $(M, q, e)$ be a pointed quadratic module over $k$ and suppose there exists a bilinear form $\beta: M \times M \to k$, possibly not symmetric, such that $q(x) = \beta(x, x)$ for all $x \in M$ (which holds automatically if $M$ is projective as a $k$-module (Exc. [50]), then the base point $e \in M$ is unimodular.

Proof. The linear form $\lambda := \beta(e, -)$ on $M$ has $\lambda(e) = \beta(e, e) = q(e) = 1$. \hfill \square

12.15. The naive discriminant. The multiplicative group $k^\times$ acts on the additive group $k$ by multiplication form the right, allowing us to form the quotient $k/k^\times$. Now suppose we are given a quadratic module $(M, q)$ over $k$ such that the underlying $k$-module $M$ is free of finite rank. In analogy to [3.10] [3.12] we let $E = (e_1, \ldots, e_n)$ be any $k$-basis of $M$, put

$$Dq(E) := \{q(e_i, e_j)\}_{1 \leq i, j \leq n} \in \text{Mat}_n(k) \quad (1)$$

and have
Let $(M, q)$ be a quadratic space over $k$. An element $u \in M$ is said to be isotropic (relative to $q$ or in $(M, q)$) if $u$ is unimodular and satisfies the relation $q(u) = 0$. As in the case of quadratic forms over fields, isotropic vectors may always be completed to hyperbolic pairs: given $u \in M$ isotropic, there exists $v \in M$ such that $(u, v)$ is a hyperbolic pair, i.e., $q(u) = q(v) = 0$, $q(u, v) = 1$. Indeed, since $q$ is non-singular, unimodularity of $u$ yields an element $w \in M$ satisfying $q(u, w) = 1$, and one checks that $(u, v), v := -q(w)u + w$, is a hyperbolic pair.

The quadratic space $(M, q)$ (or $q$) will be called isotropic if $M$ contains an isotropic vector relative to $q$. A submodule $N \subseteq M$ is said to be totally isotropic (relative to $q$) if it is a direct summand of $M$ and satisfies $q(N) = \{0\}$.

### 12.17. Hyperbolic spaces.

Let $M$ be a finitely generated projective $k$-module. Then

\[
\mathfrak{h}_M : \text{M}^* \oplus M \longrightarrow k, \quad v^* + v \longmapsto \mathfrak{h}_M(v^* + v) := \langle v^*, v \rangle,
\]

is a non-singular quadratic form since $M^{**}$ identifies canonically with $M$ and $(\mathfrak{Dh}_M)^* : \text{M}^* \oplus M \rightarrow M \oplus \text{M}^*$ (cf. [12.9]) is the switch $v^* \oplus v \mapsto v \oplus v^*$. We also write

\[
\mathfrak{h}_M := (\text{M}^* \oplus M, \mathfrak{h}_M)
\]

as a quadratic space and call this the hyperbolic space associated with $M$ or simply a hyperbolic space. Observe that both $\text{M}^*$ and $M$ may be viewed canonically as totally isotropic submodules of $\text{M}^* \oplus M$ relative to $\mathfrak{h}_M$. The functor assigning to $M$ its associated hyperbolic space is additive, so for another finitely generated projective $k$-module $N$ we obtain a natural isomorphism

\[
\mathfrak{h}_{M \oplus N} \cong \mathfrak{h}_M \oplus \mathfrak{h}_N.
\]

If $M \cong k^n$ is free of rank $n \in \mathbb{N}$, we speak of the split hyperbolic space of rank $n$. For $L$ a line bundle in the sense of [10.8], $\mathfrak{h}_L$ will be referred to as a hyperbolic plane, which is said to be split if $L$ is free of rank 1.

A quadratic space is said to be hyperbolic (resp. a (split) hyperbolic plane) if it is isometric to some hyperbolic space (resp. (the split) hyperbolic plane).
Exercises.

47. A splitness criterion for hyperbolic planes. Let \( L \) be a line bundle over \( k \). Show that the following conditions are equivalent.

(i) The hyperbolic plane \( \mathbf{h}_L \) is split.
(ii) \( L \oplus L \) contains a hyperbolic pair relative to \( \mathbf{h}_L \).
(iii) \( L \cong k \) is free.

(Hint: To prove (ii) \( \Rightarrow \) (iii), find a unimodular vector in \( L \).)

48. Let \( \mathbf{h} \) be the split hyperbolic plane over \( k \) and \((e_1, e_2)\) a hyperbolic pair in \( \mathbf{h} \). Show for \( u_1, u_2 \in \mathbf{h} \) that the following conditions are equivalent.

(i) \((u_1, u_2)\) is a hyperbolic pair in \( \mathbf{h} \).
(ii) There exists a decomposition \( k = k_1 \oplus k_- \) of \( k \) as a direct sum of ideals such that in the induced decompositions
\[
\mathbf{h} = \mathbf{h}_1 \oplus \mathbf{h}_- \quad \text{ and } \quad u_j = u_{j1} \oplus u_{j-} \quad (j = 1, 2),
\]
where \( \mathbf{h}_1 = \mathbf{h}_1 \) is the split hyperbolic plane over \( k_1 \) with the corresponding hyperbolic pair \((e_{1\pm}, e_{2\pm})\) = \((e_1, e_2)\), the quantities \( u_{j1} = (u_j)_{k_1} \in \mathbf{h}_1 \) (\( j = 1, 2 \)) satisfy the relations
\[
\begin{align*}
u_{1+} &= \gamma_{i1} e_{1+}, \quad &u_{2+} &= \gamma_{i-1} e_{2+}, \\
u_{1-} &= \gamma_{i1} e_{2-}, \quad &u_{2-} &= \gamma_{i-1} e_{1-}
\end{align*}
\]
for some \( \gamma_{i1} \in k_1^\times \).

49. Multi-quadratic maps. For a positive integer \( n \) and \( k \)-modules \( M_1, \ldots, M_n, M \), a map
\[
F : M_1 \times \cdots \times M_n \rightarrow M
\]
is called \( k \)-multi-quadratic or \( k-n \)-quadratic if for all \( i = 1, \ldots, n \) and for all \( u_j \in M_j \), 1 \( \leq j \leq n \), \( j \neq i \),
\[
M_i \rightarrow M, \quad u_i \mapsto F(u_1, \ldots, u_i, \ldots, u_n)
\]
is a quadratic map over \( k \). Show for \( R \in k-\text{alg} \) and a \( k-n \)-quadratic map \( F : M_1 \times \cdots \times M_n \rightarrow M \) that there exists a unique \( R-n \)-quadratic map \( F_R : M_{1R} \times \cdots \times M_{nR} \rightarrow M_R \) rendering the diagram
\[
\begin{array}{ccc}
M_1 \times \cdots \times M_n & \rightarrow & M \\
\downarrow \text{can} & & \downarrow \text{can} \\
M_{1R} \times \cdots \times M_{nR} & \rightarrow & M_R
\end{array}
\]
commutative, where can : \( M_1 \times \cdots \times M_n \rightarrow M_{1R} \times \cdots \times M_{nR} \) is defined by
\[
\text{can}(u_1, \ldots, u_n) := (u_{1R}, \ldots, u_{nR})
\]
for all \( u_i \in M_i \), 1 \( \leq i \leq n \). Writing \( \text{Quad}(M_1, \ldots, M_n; M) \) for the \( k \)-module of \( k-n \)-quadratic maps from \( M_1 \times \cdots \times M_n \) to \( M \), show further that the assignment \( F \mapsto F_R \) defines a \( k \)-linear map from \( \text{Quad}(M_1, \ldots, M_n; M) \) to \( \text{Quad}(M_{1R}, \ldots, M_{nR}; M_R) \). We call \( F_R \) the \( R-n \)-quadratic extension of \( F \).

50. Let \((M, q)\) be a quadratic module over \( k \) and suppose \( M \) is projective. Show that there exists a bilinear form \( \beta : M \times M \rightarrow k \), possibly not symmetric, such that \( q(x) = \beta(x, x) \) for all \( x \in M \).

51. Separable quadratic forms over fields. Let \( q : V \rightarrow F \) be a quadratic form over a field \( F \) and \( K/F \) an algebraically closed extension field. Show that the following conditions are equivalent.
52. Let \( (V, q) \) be a quadratic space of dimension \( n \) over the field \( F \).

(a) If \( n \geq 3 \), show that every element in \( V \) can be decomposed into the sum of at most two anisotropic elements in \( V \).

(b) Assume that \( (V, q) \) has Witt index at least 3. Show for anisotropic vectors \( x_1, x_2 \in V \) that \( q(x_1, x_2) \neq 0 \) or there exists an anisotropic vector \( y \in V \) satisfying \( q(x_1, y) \neq 0 \neq q(y, x_2) \).

Can the extra conditions on \( (V, q) \) in (a), (b) be avoided?

13. Polynomial laws

The differential calculus for polynomial (or rational) maps between finite-dimensional vector spaces, as explained in Braun-Koecher [15] or Jacobson [43], for example, belongs to the most useful techniques from the toolbox of elementary non-associative algebra. It elevates the linearization procedures that we have encountered so far, and that will become much more involved in subsequent portions of the book (see, e.g., the identities in 31.3 below), to a new level of systematic conciseness. While it works most smoothly over infinite base fields, it can be slightly adjusted to work over finite ones as well. There is also a variant due to McCrimmon [76] that allows infinite-dimensional vector spaces.

Extending this formalism to arbitrary modules over arbitrary commutative rings, however, requires a radically new approach. The one adopted in the present volume, due to Roby [112], is based on the concept of a polynomial law. In the present section, we explore this concept in detail and show, in particular, how the differential calculus for polynomial maps over infinite fields can be naturally extended to this more general setting. For a different approach, see Faulkner [29].

Throughout, we let \( k \) be an arbitrary commutative ring and \( M, N, M_1, \ldots, M_n (n \in \mathbb{Z}, n > 0) \) be arbitrary \( k \)-modules.

13.1. Reminder: polynomial maps. For the time being, let \( V, W \) be finite-dimensional vector spaces over an infinite field \( F \) and \( (v_i)_{1 \leq i \leq m}, (w_j)_{1 \leq j \leq n} \) be bases of \( V, W \), respectively, over \( F \). By a polynomial map from \( V \) to \( W \) we mean a set map \( f: V \to W \) such that there exist polynomials \( p_1, \ldots, p_n \in F[t_1, \ldots, t_m] \) satisfying the equations

\[
f(\sum_{i=1}^m \alpha_i v_i) = \sum_{j=1}^n p_j(\alpha_1, \ldots, \alpha_m) w_j \quad (\alpha_1, \ldots, \alpha_m \in F).
\]  

Since \( F \) is infinite, \( 1 \) determines the polynomials \( p_j, 1 \leq j \leq n \), uniquely. Moreover, the concept of a polynomial map is obviously independent of the bases chosen.

In the special case \( W = F \), we speak of a polynomial function on \( V \). The totality of all polynomial functions on \( V \) forms a unital commutative associative \( F \)-algebra,
denoted by $F[V]$ and canonically isomorphic to the polynomial ring $F[t_1, \ldots, t_n]$ over $F$.

Returning to our polynomial map $f: V \to W$ as above, we generalize (1) by defining a family of set maps $f_R: V_R \to W_R$, one for each $R \in F$-alg, given by

$$f_R(\sum_{i=1}^m r_i v_{iR}) := \sum_{j=1}^n p_j(r_1, \ldots, r_m) w_{jR} \quad (r_1, \ldots, r_m \in R).$$

(2)

The key property of this family may be expressed by a coherence condition, saying that its constituents $f_R$ vary functorially with $R \in k$-alg: every morphism $\phi: R \to S$ in $k$-alg yields a commutative diagram

$$\begin{array}{ccc}
V_R & \xrightarrow{f_R} & W_R \\
\downarrow{1_V \otimes \phi} & & \downarrow{1_W \otimes \phi} \\
V_S & \xrightarrow{f_S} & W_S,
\end{array}$$

(3)

as shown. This coherence condition will now be isolated in the formal definition of a polynomial law.

13.2. The concept of a polynomial law. With the $k$-module $M$ we associate a (covariant) functor $M_a: k$-alg $\to$ set (where set stands for the category of sets) by setting $M_a(R) = M_R$ as sets for $R \in k$-alg and $M_a(\phi) = 1_M \otimes \phi: M_R \to M_S$ as set maps for morphisms $\phi: R \to S$ in $k$-alg. Analogously, we obtain the functor $N_a: k$-alg $\to$ set associated with the $k$-module $N$. We then define a polynomial law $f$ from $M$ to $N$ (over $k$) as a natural transformation $f: M_a \to N_a$. In explicit terms, this means that, for all $R \in k$-alg, we are given set maps $f_R: M_R \to N_R$ varying functorially with $R$, so whenever $\phi: R \to S$ is a unital homomorphism of $k$-algebras, the diagram

$$\begin{array}{ccc}
M_R & \xrightarrow{f_R} & N_R \\
\downarrow{1_M \otimes \phi} & & \downarrow{1_N \otimes \phi} \\
M_S & \xrightarrow{f_S} & N_S,
\end{array}$$

(1)

commutes. A polynomial law from $M$ to $N$ will be symbolized by $f: M \to N$, in spite of the fact that it is not a map from $M$ to $N$ in the usual sense. But it induces one, namely $f_k: M \to N$, which, however, does not determine $f$ uniquely. If $\phi: R \to S$ is a morphism in $k$-alg, then $S$ belongs to $R$-alg via $\phi$, and identifying $(M_R)_S = M_S$, $(N_R)_S = N_S$ canonically by means of (10.3.1), we conclude from (10.3.2) that (1) is equivalent to

$$f_R(x)_S = f_S(x_S) \quad (x \in M_R).$$

(2)
The totality of polynomial laws from $M$ to $N$ will be denoted by $\text{Pol}(M,N)$, or by $\text{Pol}_k(M,N)$ to indicate dependence on $k$. It is a $k$-module in a natural way, the sum of $f,g \in \text{Pol}(M,N)$ being given by $(f+g)_R = f_R + g_R$ for all $R \in k\text{-alg}$, ditto for scalar multiplication. The multiplication of polynomial laws $M \to N$ by scalar polynomial laws $M \to k$ is defined analogously. In particular, $\text{Pol}(M,k)$ is a unital commutative associative $k$-algebra. If $f : M \to N$ and $g : N \to P$ are polynomial laws over $k$, so obviously is $g \circ f : M \to P$, given by $(g \circ f)_R = g_R \circ f_R, R \in k\text{-alg}$. Every polynomial law $f : M \to N$ over $k$ gives rise to its scalar identification or base change $f \otimes R : M_R \to N_R$, a polynomial law over $R$ determined by the condition $(f \otimes R)_S := f_S$ for all $S \in R\text{-alg} \subseteq k\text{-alg}$, where $(M_R)_S = M_S, N_R \cdot S = N_S$ are canonically identified as before. We mostly write $f_R$, or simply $f$, for $f \otimes R$ if there is no danger of confusion.

13.3. Convention: multi-indices. For $R \in k\text{-alg}$ it is often convenient to use the multi-index notation $\nu^\alpha := r_1^{\alpha_1} \cdots r_n^{\alpha_n}$, where $\nu = (r_1, \ldots, r_n) \in \mathbb{R}^n$ and $\nu = (v_1, \ldots, v_n) \in \mathbb{N}^n$ are sequences of length $n \geq 1$ in $R, \mathbb{N}$, respectively. Also, we put $|\nu| := \sum_{i=1}^n v_i$.

For example, given a finite chain $T = (t_1, \ldots, t_r)$ of indeterminates, the elements of the polynomial algebra $k[T] = k[t_1, \ldots, t_r]$ may be written as $\sum_{\nu \in \mathbb{N}^r} \alpha_\nu T^\nu$, where $(\alpha_\nu)_{\nu \in \mathbb{N}^r}$ is a family of finite support in $k$. Moreover, observing the identifications of \([3.2]\) we obtain

$$M_{k[T]} = \bigoplus_{\nu \in \mathbb{N}^r} (T^\nu M)$$

as a direct sum of $k$-modules. For a polynomial law $f : M \to N$ over $k$, these identifications (replacing $k$ by $R$ and $f$ by $f \otimes R$) yield

$$f_{R[T]}(x) = f_R(x) \quad (R \in k\text{-alg}, x \in M_R)$$

since $f_{R[T]}(x) = (f \otimes R)_{R[T]}(x_{R[T]}) = (f \otimes R)_R(x)_{R[T]} = f_R(x)$ by \([3.2]\), particularly by \([13.2]3\). Similarly, given a positive integer $q$ and writing $k[\varepsilon]$ for the free $k$-algebra on a single generator $\varepsilon$, subject to the relation $\varepsilon^q = 0$ (so $k[\varepsilon] = k[t_1]/(t_1^q)$), $\varepsilon = t_1 + (t_1^q)$, we have

$$M_{k[\varepsilon]} = \bigoplus_{j=0}^{q-1} (\varepsilon^j M_i)$$

as $R$-modules such that

13.4. A standard identification. For all $R \in k\text{-alg}$, we will systematically adopt the canonical identification

$$(M_1 \times \cdots \times M_n)_R = M_{1R} \times \cdots \times M_{nR}$$

as $R$-modules such that
(v_1 \oplus \cdots \oplus v_n) \otimes r = (v_1 \otimes r) \oplus \cdots \oplus (v_n \otimes r), \quad (1)

(v_1 \otimes r_1) \oplus \cdots \oplus (v_n \otimes r_n) = \sum_{i=1}^n (0 \oplus \cdots \oplus 0 \oplus v_i \oplus 0 \oplus \cdots \oplus 0) \otimes r_i

for all \(v_i \in M, r_i \in R, 1 \leq i \leq n\). Given a morphism \(\varphi : R \to S\) in \(k\text{-alg}\), this identification implies

\[(1_{M_1} \otimes \varphi) \times \cdots \times (1_{M_n} \otimes \varphi) = 1_{M_1 \times \cdots \times M_n} \otimes \varphi. \quad (2)\]

### 13.5. Homogeneous polynomial laws.

A polynomial law \(f : M \to N\) is said to be homogeneous of degree \(d \in \mathbb{N}\) if \(f_R(rx) = r^df_R(x)\) for all \(R \in k\text{-alg}, r \in R, x \in M_R\). More generally, a polynomial law \(f : M_1 \times \cdots \times M_n \to N\) is said to be multi-homogeneous of multi-degree \(d = (d_1, \ldots, d_n) \in \mathbb{N}^n\) if

\[f_R(r_1x_1, \ldots, r_nx_n) = r_1^{d_1} \cdots r_n^{d_n} f_R(x_1, \ldots, x_n)\]

for all \(R \in k\text{-alg}, r_i \in R, x_i \in M_{R,i}, i = 1, \ldots, n\). Here and in the sequel, we always identify \((M_1 \times \cdots \times M_n)_R = M_{1R} \times \cdots \times M_{nR}\) canonically by means of \([13.4.1]\).

Thanks to Exc. [56], multi-homogeneous (resp. homogeneous) polynomial laws of multi-degree \(\mathbf{1} = (1, \ldots, 1)\) (resp. of degree 2) identify canonically with multi-linear (resp. quadratic) maps in the usual sense (resp. in the sense of \([12.1]\)). Notice also that a multi-homogeneous polynomial law of multi-degree \(d \in \mathbb{N}^n\) is homogeneous of degree \(|d|\). Scalar homogeneous polynomial laws are called forms. We speak of linear, quadratic, cubic, quartic, ... forms instead of forms of degree \(d = 1, 2, 3, 4, \ldots\).

### 13.6. Local finiteness.

A family \((f_i)_{i \in I}\) of polynomial laws \(f_i : M \to N\) \((i \in I)\) is said to be locally finite if, for all \(R \in k\text{-alg}\) and all \(x \in M_R\), the family \((f_{IR}(x))_{i \in I}\) of elements in \(N_R\) has finite support. In this case, we obtain a well defined polynomial law

\[\sum_{i \in I} f_i : M \longrightarrow N\]

over \(k\) by setting

\[(\sum_{i \in I} f_i)_R(x) := \sum_{i \in I} f_{iR}(x) \quad (R \in k\text{-alg}, x \in M_R).\]

Note that this definition mutatis mutandis makes sense also if each \(f_i, i \in I\), is merely assumed to be a family of set maps \(f_{IR} : M_R \to N_R, R \in k\text{-alg}\), which may or may not vary functorially with \(R\).

### 13.7. Theorem.

Let \(f : M \to N\) be a polynomial law over \(k\) and \(n\) a positive integer. Then there exists a unique locally finite family of polynomial laws

\[\Pi^v f : M^n \longrightarrow N \quad (v \in \mathbb{N}^n)\]

such that
Thus the family \( (2) \) holds. We have thus obtained a locally finite family of set maps \( k \) and \( \phi \), the identification (10.3.1) implies

\[
1, \quad \sum_{v \in \mathbb{N}^n} T^v (\Pi^v f)_R(x),
\]

(2) yields \( (\Pi^v f)_{R} \) uniquely. In particular,

\[
\sum_{i=1}^n r_i x_i = \sum_{v \in \mathbb{N}^n} r^v (\Pi^v f)_R(x)
\]

for all \( R \in k\text{-alg}, r = (r_1, \ldots, r_n) \in R^n, x = (x_1, \ldots, x_n) \in (M_R)^n \). In particular,

\[
f_R \left( \sum_{i=1}^n t_i x_i \right) = \sum_{v \in \mathbb{N}^n} T^v (\Pi^v f)_R(x).
\]

This completes the proof of (1). It remains to show that the \( (\Pi^v f)_R \), \( v \in \mathbb{N}^n \) vary functorially with \( R \in k\text{-alg} \) and \( \phi : R[T] \to S[T] \) an arbitrary morphism in \( k\text{-alg} \). Let \( \psi \) be any natural extension fixing \( t_i \) for \( 1 \leq i \leq n \). One checks \( (1_M \otimes \phi)(T^y) = T^v (1_M \otimes \phi)(y) \) for \( v \in \mathbb{N}^n, y \in M_R \). Ditto for \( N \) in place of \( M \), and (13.4.2) yields \( (1_M \otimes \phi)^n = 1_{M^n} \otimes \phi \). Hence
\[
\sum_{\nu \in \mathbb{N}^n} T^\nu(1_N \otimes \varphi) \circ (\Pi^\nu f)_R(x) = (1_N \otimes \psi)(\sum_{\nu \in \mathbb{N}^n} T^\nu(\Pi^\nu f)_R(x)) = (1_N \otimes \psi) \circ f_{R[T]}(\sum_{i=1}^n t_i x_i) = f_{R[T]}(\sum_{i=1}^n t_i (1_M \otimes \varphi)(x_i)) = \sum_{\nu \in \mathbb{N}^n} T^\nu(\Pi^\nu f)_R((1_M \otimes \varphi)(x_1), \ldots, (1_M \otimes \varphi)(x_n)) = \sum_{\nu \in \mathbb{N}^n} T^\nu((\Pi^\nu f)_R \circ (1_M \otimes \varphi))(x),
\]
and comparing coefficients, the assertion follows. □

13.8. Linearizations. The polynomial laws \(\Pi^\nu f\) for \(\nu \in \mathbb{N}^n, n \in \mathbb{Z}, n > 0\) as constructed in Thm. \(13.7\) are called the linearizations or polarizations of the polynomial law \(f : M \to N\) over \(k\). We list a few elementary properties.

(a) For \(\nu \in \mathbb{N}^n\), the polynomial law \(\Pi^\nu f : M^n \to N\) is multi-homogeneous of multi-degree \(\nu\). Indeed, replacing \(x_i\) by \(r x_i\) \((r_i \in R, 1 \leq i \leq n)\) on the left-hand side of \(13.7(2)\) amounts to the same as carrying out the substitution \(t_i \mapsto r t_i (1 \leq i \leq n)\). Hence the assertion follows from \(13.7(1)\), \(13.3(2)\).

(b) Writing \(\pi_\nu := (\nu_{\pi^{-1}(1)}, \ldots, \nu_{\pi^{-1}(n)})\) for \(\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n\) and \(\pi \in S_n\), we have

\[
(\Pi^\nu f)_R(x_{\pi(1)}, \ldots, x_{\pi(n)}) = (\Pi^{\pi_\nu} f)_R(x_1, \ldots, x_n) \tag{1}
\]

for all \(R \in k\)-alg, \(x_1, \ldots, x_n \in M_R\), which follows immediately from the fact that the left-hand side of \(13.7(2)\) remains unaffected by any permutation of the summands.

(c) If \(f\) is homogeneous of degree \(d \in \mathbb{N}\), then \(\Pi^\nu f = 0\) for all \(\nu \in \mathbb{N}^n, n \in \mathbb{Z}, n > 0\), unless \(|\nu| = d\). In order to see this, let \(s\) be a new variable, replace \(t_i\) by \(s t_i\) for \(1 \leq i \leq n\) in \(13.7(2)\) and compare coefficients of \(s^{|\nu|}\).

In particular, assume \(d > 0\), let \(n = d\) and \(\nu := 1 := (1, \ldots, 1) \in \mathbb{N}^d\). Then (a) shows that \(\Pi^1 f : M^d \to N\) is multi-homogeneous of multi-degree 1, i.e., it is a multilinear map (Exc. 56(a)), while we conclude from (b) that it is totally symmetric. Putting \(x_1 = \cdots = x_d := y \in M_R\) in \(13.7(2)\) and comparing coefficients of \(t_1 \cdots t_d\) in

\[
( \sum_{i_1, \ldots, i_d=1}^d t_{i_1} \cdots t_{i_d}) f_R(y) = ( \sum_{i=1}^d t_i)^d f_R(y) = \sum_{\nu \in \mathbb{N}^d} T^\nu(\Pi^\nu f)_R(y, \ldots, y),
\]
we conclude

\[
(\Pi^1 f)_R(y, \ldots, y) = d! f_R(y) \tag{2}
\]

TOTLIN
for all $R \in k\text{-alg}$, $y \in M_R$. We call $\Pi^1 f$ the total linearization of $f$.

**13.9. Corollary.** A polynomial law over $k$ is zero if and only if all its linearizations vanish identically over $k$: for all polynomial laws $f : M \to N$ over $k$, we have

$$f = 0 \iff \forall n \in \mathbb{Z}, \ n > 0, \ \forall v \in \mathbb{N}^n : (\Pi^1 f)_k = 0.$$ 

**Proof.** The implication from left to right is obvious. Conversely, suppose $(\Pi^1 f)_k = 0$ for all $n \in \mathbb{Z}$, $n > 0$, $v \in \mathbb{N}^n$. We must show $f_R = 0$ for all $R \in k\text{-alg}$. Every $x \in M_R$ can be written as $x = \sum_{i=1}^{n} r_i v_i R$ for some $n \in \mathbb{Z}$, $n > 0$, $r = (r_1, \ldots, r_n) \in R^n$, $v = (v_1, \ldots, v_n) \in M^n$. From (13.7.1) and (13.2.3) we therefore deduce

$$f_R(x) = \sum_{v \in \mathbb{N}^n} r^\nu (\Pi^1 f)_R(v_R) = \sum_{v \in \mathbb{N}^n} r^\nu (\Pi^1 f)_k(v)_R = 0,$$

as desired. □

**13.10. Corollary.** Assume the $k$-modules $M$ and $N$ are free of finite rank, with bases $(v_1, \ldots, v_m)$ and $(w_1, \ldots, w_n)$, respectively. A family of set maps $f_R : M_R \to N_R$, $R \in k\text{-alg}$, is a polynomial law over $k$ if and only if there exist polynomials $p_1, \ldots, p_n \in k[t_1, \ldots, t_m]$ such that

$$f_R(\sum_{i=1}^{m} r_i v_i R) = \sum_{j=1}^{n} p_j (r_1, \ldots, r_m) w_j R \quad (1)$$

for all $R \in k\text{-alg}$, $r_1, \ldots, r_m \in R$.

**Proof.** If such polynomials exist, it is readily checked that the $f_R$ vary functorially with $R \in k\text{-alg}$, hence give rise to a polynomial law $f : M \to N$. Conversely, let $f : M \to N$ be a polynomial law over $k$. For $R \in k\text{-alg}$ and $r = (r_1, \ldots, r_m) \in R^n$, we put $v := (v_1, \ldots, v_m)$ and apply (13.7.1) to conclude

$$f_R(\sum_{i=1}^{m} r_i v_i R) = \sum_{v \in \mathbb{N}^m} r^\nu (\Pi^1 f)_R(v_R) = \sum_{v \in \mathbb{N}^m} r^\nu (\Pi^1 f)_k(v)_R.$$ 

Here $(\Pi^1 f)_k(v) \in N$, $v \in \mathbb{N}^m$, may be written as

$$(\Pi^1 f)_k(v) = \sum_{j=1}^{n} \beta_{jv} w_j$$

with unique coefficients $\beta_{jv} \in k$, $1 \leq j \leq n$. Since the family $(\Pi^1 f)_v \in \mathbb{N}^m$ is locally finite, we can form the polynomials

$$p_j := \sum_{v \in \mathbb{N}^m} \beta_{jv} T^v \in k[T]$$

$(T := (t_1, \ldots, t_m), \ 1 \leq j \leq n)$

which obviously satisfy (1). □
13.11. Corollary. Let $V, W$ be finite-dimensional vector spaces over an infinite field $F$. Then the assignment $f \mapsto f_R$ defines a linear bijection from $\text{Pol}_F(V, W)$ onto the vector space of polynomial maps from $V$ to $W$. For bases $(v_1, \ldots, v_m), (w_1, \ldots, w_n)$ of $V, W$, respectively, over $F$, the inverse of this bijection assigns to every polynomial map $f : V \to W$ the polynomial law given by the family of set maps $f_R : V_R \to W_R, R \in k\text{-alg}$, as defined in (13.1.2).

Proof. This follows from Cor. 13.10 combined with 13.1. □

13.12. Binary linearizations. It is sometimes useful to rewrite the formalism of Thm. 13.7 for $n = 2$, so let $f : M \to N$ be any polynomial law over $k$. With independent variables $s, t$, we then apply (13.7.2) and obtain

$$f_R(s, t)(sx + ty) = \sum_{m \geq 0, n \geq 0} s^m t^n (\Pi^{(m,n)} f)_R(x, y)$$

(1) for all $R \in k\text{-alg}, x, y \in M_R$, and (13.8) yields

$$(\Pi^{(m,n)} f)_R(x, y) = (\Pi^{(n,m)} f)_R(y, x).$$

(2) If $f$ is homogeneous of degree $d \in \mathbb{N}$, we obtain $\Pi^{(m,n)} f = 0$ for $m, n \geq 0$ unless $m + n = d$ (13.8 (c)), so (1) collapses to

$$f_R(s, t)(sx + ty) = \sum_{n=0}^{d} s^{d-n} t^n (\Pi^{(d-n,n)} f)_R(x, y)$$

for all $R \in k\text{-alg}, x, y \in M_R$.

13.13. Total derivatives. Let $f : M \to N$ be any polynomial law over $k$. By Thm. 13.7 the family $(\Pi^{(m,n)} f)_{m,n \geq 0}$ of polynomial laws $M \times M \to N$ is locally finite, allowing us to define, for all $n \in \mathbb{N}$, a polynomial law

$$D^n f := \sum_{m \geq 0} \Pi^{(m,n)} f : M \times M \to N,$$

(1) called the $n$-th (total) derivative of $f$. By 13.8 (a), it is homogeneous of degree $n$ in the second variable, i.e.,

$$(D^0 f)_R(x, ry) = r^n (D^n f)_R(x, y). \quad (R \in k\text{-alg}, r \in R, x, y \in M_R)$$

In particular, Exc. 53 and (13.7) imply

$$(D^0 f)_R(x, y) = \sum_{m \geq 0} (\Pi^{(m,0)} f)_R(x, y) = \sum_{m \geq 0} (\Pi^{m} f)_R(x) = f_R(x),$$

(2) hence $D^0 f = f$ as polynomial laws over $k$. Moreover, abbreviating $D f := D^1 f$. 

\[(Df)_R(x) : M_R \rightarrow N_R, y \mapsto (Df)_R(x)(y) := (Df)_R(x,y),\]
by Ex. 56 is an \(R\)-linear map for all \(x \in M_R, R \in k\text{-}\mathbf{alg}.\) Similarly,
\[
(D^2f)_R(x) : M_R \rightarrow N_R, \ y \mapsto (D^2f)_R(x,y),
\]
is an \(R\)-quadratic map in the usual sense. Specializing \(s \mapsto 1\) in (13.12.1), we obtain
the relation
\[
f_R[t](x+ty) = \sum_{n \geq 0} t^n (D^n f)_R(x,y),
\]
called the Taylor expansion of \(f\) at \(x\). For \(q \in \mathbb{Z}, \ q > 0\), it is sometimes convenient

to replace \(R[t]\) by the algebra \(R[\varepsilon], \varepsilon^{q+1} = 0\), and to apply (13.7.1). The ensuing
relation
\[
f_R[\varepsilon](x+\varepsilon y) = \sum_{n = 0}^{q} \varepsilon^n (D^n f)_R(x,y)
\]
determines the first \(q\) derivatives of \(f\) uniquely. In particular, for \(q = 1, \ R[\varepsilon]\) is the
algebra of dual numbers and
\[
f_R[\varepsilon](x+\varepsilon y) = f_R(x) + \varepsilon (Df)_R(x,y).
\]

**13.14. Total derivatives of homogeneous polynomial laws** Let \(f : M \rightarrow N\) be a
homogeneous polynomial law of degree \(d \geq 0\) over \(k\). By 13.8 (c), the terms \(\Pi^{(m,n)} f\)
in the sum on the right of (13.13.1) vanish unless \(m+n = d\). Thus \(D^n f = 0\) for \(n > d\) and
\[
D^n f = \Pi^{(d-n,n)} f \quad (0 \leq n \leq d).
\]
Comparing this with (13.12.2), we conclude
\[
(D^n f)_R(x,y) = (D^{d-n} f)_R(y,x) \quad (R \in k\text{-}\mathbf{alg}, \ 0 \leq n \leq d, \ x,y \in M_R).
\]
We also obtain Euler’s differential equation
\[
(Df)_R(x,x) = d f_R(x)
\]
by setting \(y = x\) in (13.13.5), which gives \(f_R(x) + \varepsilon (Df)(x,x) = (1 + \varepsilon)^d f_R(x) = f_R(x) + \varepsilon d f_R(x),\) as claimed.

**13.15. Differential calculus** The standard rules of differentiation are valid for arbitrary
polynomial laws and will henceforth be used without further comment. For convenience, we mention just a few examples.

Let \(f : M \rightarrow N, \ g : N \rightarrow P, \ f_i : M \rightarrow N_i (i = 1, 2)\) be polynomial laws over \(k\) and suppose \(N_1 \times N_2 \rightarrow N\) is a \(k\)-bilinear map written multiplicatively. Furthermore, let
\( \lambda : M \to N \) (resp. \( Q : M \to N \)) be a linear (resp. quadratic) map. Then, dropping the subscript “\( R \)” for simplicity (e.g., by writing \( f(x) \) instead of \( f_R(x) \)), we have

\[
\begin{align*}
(D\lambda)(x,y) &= \lambda(y), \\
(DQ)(x,y) &= Q(x,y), \\
(D^2Q)(x,y) &= Q(y), \\
(D(g \circ f))(x,y) &= (Dg)(f(x),(Df)(x,y)), \\
(D(g \circ \lambda))(x,y) &= (Dg)(\lambda(x),\lambda(y)), \\
(D^2(g \circ f))(x,y) &= (Dg)(f(x),(D^2f)(x,y)) \\
& \quad + (D^2g)(f(x),(Df)(x,y)) \\
(D(f_1f_2))(x,y) &= (Df_1)(x,y)f_2(x) + f_1(x)(Df_2)(x,y), \\
(D^2(f_1f_2))(x,y) &= (D^2f_1)(x,y)f_2(x) + (Df_1)(x,y)(Df_2)(x,y) \\
& \quad + f_1(x)(D^2f_2)(x,y)
\end{align*}
\]

for all \( R \in k\text{-alg} \) and all \( x,y \in M_R \). Note that (4) (resp. (6)) is the first (resp. second) order chain rule, while (7) (resp. (8)) is the first (resp. second) order product rule of the differential calculus. Moreover, (5) by (1) is a special case of (4).

13.16. **Directional derivatives** Let \( y \in M \). For any polynomial law \( f : M \to N \) over \( k \), the rule

\[
(\partial_y f)(x) := (Df)_R(x,y_R) \in N_R \quad (R \in k\text{-alg}, x \in M_R)
\]

defines a new polynomial law \( \partial_y f : M \to N \), called the *derivative of \( f \) in the direction \( y \)*, and the map

\[
\partial_y : \text{Pol}_k(M,N) \to \text{Pol}_k(M,N)
\]
is obviously \( k \)-linear.

Our next aim will be to show that the operators \( \partial_y, y \in M \), commute and that their iterations relate to the total linearization of a homogeneous polynomial law. To accomplish this, we need some preparation.

13.17. **Lemma.** Let \( f : M \to N \) be a polynomial law over \( k \). Then

\[
(D^p f)_{R[T]}(\sum_{i=1}^{n+1} t_i x_i, x_{n+1}) = \sum_{v \in \mathbb{N}^p} T^v \Pi^{(v,p)} f_R(x_1, \ldots, x_n, x_{n+1})
\]

for all \( R \in k\text{-alg} \), \( p, n \in \mathbb{N}, n > 0, x_1, \ldots, x_n, x_{n+1} \in M_R \).

**Proof.** With an additional indeterminate \( t_{n+1} \), we apply (13.7) and obtain

\[
f_{R[T\{ t_{n+1} \}]}(\sum_{i=1}^{n+1} t_i x_i) = \sum_{v \in \mathbb{N}^p, p \geq 0} T^v t_{n+1}^p \Pi^{(v,p)} f_R(x_1, \ldots, x_n, x_{n+1}).
\]
Invoking the Taylor expansion (13.13.3) and comparing coefficients of $t_{n+1}^p$, the lemma follows.

13.18. Lemma. Let $f : M \to N$ be a polynomial law over $k$ and $y \in M$. Then

$$(\Pi^v \partial_y f)_R(x_1, \ldots, x_n) = (\Pi^{(v, 1)} f)_R(x_1, \ldots, x_n, y_R)$$

for all $R \in k\text{-alg}$, $n \in \mathbb{Z}$, $n > 0$, $v \in \mathbb{N}_0^n, x_1, \ldots, x_n \in M_R$.

Proof. Applying (13.7.2) to $\partial_y f$, we obtain

$$(\partial_y f)_R[T](\sum_{i=1}^n t_i x_i) = \sum_{v \in \mathbb{N}^n} T^v(\Pi^v \partial_y f)_R(x_1, \ldots, x_n).$$

On the other hand, treating the left-hand side to the definition of $\partial_y$ (13.16) and applying Lemma 13.17 for $p = 1$, we conclude

$$(\partial_y f)_R[T](\sum_{i=1}^n t_i x_i) = \sum_{v \in \mathbb{N}^n} T^v(\Pi^{(v, 1)} f)_R(x_1, \ldots, x_n, y_R),$$

as desired. □

13.19. Proposition. Let $f : M \to N$ be a polynomial law over $k$, $p \in \mathbb{N}$, and $y_1, \ldots, y_p \in M$. Then

$$(\partial_{y_1} \cdots \partial_{y_p} f)_R(x) = \sum_{i \geq 0} (\Pi^{(i, 1, \ldots, 1)} f)_R(x, y_1 R, \ldots, y_p R)$$

(1)

for all $R \in k\text{-alg}$, $x \in M_R$. In particular, the operators $\partial_y, y \in M$, commute.

Proof. To establish the first part, we argue by induction on $p$. For $p = 0$, the assertion is just (13.7.1), while the induction step follows immediately from Lemma 13.18. The second part now derives from the first for $p = 2$ and (13.8.1). □

13.20. Corollary. Let $f : M \to N$ be a homogeneous polynomial law of degree $d > 0$. Then the total linearization of $f$ relates to its directional derivatives by the formula

$$(\Pi^1 f)_k(y_1, \ldots, y_{d-1}, y_d) = (\partial_{y_1} \cdots \partial_{y_{d-1}} f)_k(y_d)$$

(1)

for all $y_1, \ldots, y_{d-1}, y_d \in M$. In particular, the right-hand side is totally symmetric in $y_1, \ldots, y_d$.

Proof. Since $f$ is homogeneous of degree $d$, the expression on the right of (13.19.1) by (13.8) (c) collapses to the single term $(\Pi^{d, 1, \ldots, 1} f)_R(x, y_1 R, \ldots, y_p R)$, and (1) follows for $p = d - 1$. The rest is clear. □

Our next aim in this section will be to show that a particularly simple and useful Zariski density argument easily extends from the setting of finite-dimensional vector
spaces over infinite fields to arbitrary modules over commutative rings. The key to this extension is the following concept, which is modeled after standard notions in algebraic geometry (cf. Demazure-Gabriel [22, §1, 1.2] or Jantzen [50, 1.5], see also [27,15] below).

13.21. Subfunctors Let \( A \) be a unital associative \( k \)-algebra, possibly not commutative, and \( g : M \rightarrow A \) a polynomial law over \( k \). For \( R \in \kalg \), we put

\[
\mathcal{D}(g)(R) := \{ x \in M_R \mid g_R(x) \in A_R^R \},
\]

where \( A_R^R \) on the right as usual stands for the group of invertible elements in \( A_R \).

Clearly, \( \mathcal{D}(g) \) is a subfunctor of \( \mathcal{M}_A \), i.e., \( \mathcal{D}(g)(R) \subseteq \mathcal{M}_A(R) = M_R \) is a subset for all \( R \in \kalg \) and \( (1_M \otimes \varphi)(\mathcal{D}(g)(R)) \subseteq \mathcal{D}(g)(S) \) for all morphisms \( \varphi : R \rightarrow S \) in \( \kalg \).

13.22. Proposition. Let \( A \) be a unital associative \( k \)-algebra and \( g : M \rightarrow A \) a polynomial law over \( k \) such that \( \mathcal{D}(g)(k) \neq \emptyset \). If \( f : M \rightarrow N \) is a homogeneous polynomial law over \( k \) that vanishes on \( \mathcal{D}(g) \), i.e., \( f_R|_{\mathcal{D}(g)(R)} = 0 \) for all \( R \in \kalg \), then \( f = 0 \).

For most applications, this proposition is totally adequate. But sometimes the following more detailed, but also more technical, version will be needed.

13.23. Lemma. With \( A \) and \( g \) as in Prop. 13.22 let \( f : M \rightarrow N \) be a homogeneous polynomial law over \( k \) and \( R \in \kalg \) such that \( f_S|_{\mathcal{D}(g)(S)} = 0 \) for all \( S \in \Ralg \subseteq \kalg \) which are free of positive rank as \( R \)-modules. Then \( f_R = 0 \).

Proof. After replacing \( g \) by \( g \otimes R \) and \( f \) by \( f \otimes R \) if necessary, we may assume \( R = k \).

Pick \( e \in \mathcal{D}(g)(k) \), so \( e \in M \) satisfies \( u := g_k(e) \in A^k \). Substituting \( L_{n-1} \circ g \) for \( g \), we may assume \( g_k(e) = 1_A \). Now write \( d \) for the degree of \( f \) and consider the \( k \)-algebra \( S := k[e] \), \( e^{d+1} = 0 \), which is free as a \( k \)-module of rank \( d + 1 \). Picking any \( x \in M \) and using the identifications of \( (13.3) \), the Taylor expansion \( (13.13) \) implies that

\[
g_S(e + \varepsilon x) = 1_A + \sum_{n=1}^{d} \varepsilon^n(D^n g)_k(e,x)
\]

is invertible in \( A_S \). Hence \( e_S + \varepsilon x \in \mathcal{D}(g)(S) \) and, by hypothesis,

\[
0 = f_S(e + \varepsilon x) = \sum_{n=0}^{d} \varepsilon^n(D^n f)_k(e,x).
\]

Comparing coefficients of \( \varepsilon^d \), we conclude from \( (13.13) \), \( (13.14) \) that

\[
f_k(x) = (D^0 f)_k(x,e) = (D^d f)_k(e,x) = 0.
\]

\[\square\]

For our subsequent applications, it will sometimes be necessary to consider a slight twist of polynomial laws that relates to ordinary polynomial laws as semi-linear
maps relate to linear ones. The general set-up of this twist may be described as follows.

### 13.24. Twisting modules and linear maps

Let \( \sigma : K' \to K \) be a morphism in \( \text{k-alg} \), i.e., a homomorphism of \( k \)-algebras taking 1 into 1. For a \( K \)-module \( M \), we denote by \( M^\sigma \) the \( K' \)-module which has the same additive group structure as \( M \) (in particular, \( M^\sigma = M \) as sets), and whose scalar multiplication is the one of \( M \) twisted by \( \sigma \):

\[
  a'x := a'.\sigma x := \sigma(a')x \quad (a' \in K', x \in M). \tag{1}
\]

Note that the identity map of \( M \) may be viewed as a \( \sigma \)-semi-linear bijection

\[
  \sigma_M : M^\sigma \to M. \tag{2}
\]

For \( x \in M \), we put \( x^\sigma := (\sigma_M)^{-1}(x) \in M^\sigma \) and have

\[
  \sigma_M(x^\sigma) = x, \quad a'x^\sigma = (\sigma(a')x)^\sigma = (a' \in K', x \in M). \tag{3}
\]

Given another morphism \( \tau : K'' \to K' \) in \( \text{k-alg} \), and abbreviating \( \sigma \tau := \sigma \circ \tau \), we clearly have \((M^\sigma)^\tau = M^{\sigma\tau}\) and \((\sigma\tau)_M = \sigma_M \circ \tau_M\), hence \((x^\sigma)^\tau = x^{\sigma\tau}\) for all \( x \in M \). If \( \varphi : M \to N \) is a \( K \)-linear map of \( K \)-modules, then \( \varphi^\sigma : M^\sigma \to N^\sigma \) defined by \( \sigma_N \circ \varphi^\sigma = \varphi \circ \sigma_M \), equivalently,

\[
  \varphi^\sigma(x^\sigma) = \varphi(x)^\sigma \quad (x \in M), \quad \tag{4}
\]

is a \( K' \)-linear map of \( K' \)-modules. Note that \( \varphi^\sigma = \varphi \) as set maps and \((\varphi^\sigma)^\tau = \varphi^{\sigma\tau}\).

In this way we obtain a functor from \( \text{K-mod} \) to \( \text{K'-mod} \) that restricts canonically to a functor from \( \text{k-alg} \) to \( \text{k'-alg} \).

### 13.25. The concept of a semi-polynomial law

Let \( \sigma : K' \to K \) be a morphism in \( \text{k-alg} \), \( M \) a \( K \)-module and \( M' \) a \( K' \)-module. Then [13.24] yields a functor \( M_\sigma : \text{k-alg} \to \text{set} \). Similarly, utilizing the formalism of [13.24] we obtain a functor \( \sigma_\sigma M'_\sigma : \text{k-alg} \to \text{set} \) by setting \((\sigma_\sigma M'_\sigma)(R) := M' \otimes_{K'} R^\sigma\) as sets and

\[
  (\sigma_\sigma M'_\sigma)(\varphi) := 1_{M'} \otimes_{K'} \varphi^\sigma : M' \otimes_{K'} R^\sigma \to M' \otimes_{K'} S^\sigma
\]

as set maps for morphisms \( \varphi : R \to S \) in \( \text{k-alg} \). A \( \sigma \)-semi-polynomial law from \( M' \) to \( M \) over \( k \) is now defined as a natural transformation \( f : \sigma_\sigma M'_\sigma \to \sigma_\sigma M_\sigma \). This means that we are given a family of set maps

\[
  f_R : M'_\rho \to M' \otimes_{K'} R^\sigma \to M \otimes_K R = M_R,
\]

one for each \( R \in \text{k-alg} \), which varies functorially with \( R \), so for every morphism \( \varphi : R \to S \) in \( \text{k-alg} \), the diagram
commutes.

**Exercises.**

**pr.ZERLIN** 53. Let \( f : M \rightarrow N \) be a polynomial law over \( k, R \in k \cdot \text{alg} \), \( n, p \) be positive integers and \( x \in M^n_R \), \( y \in M^p_R \). Prove for \( v \in \mathbb{N}^0 \) that

\[
(\prod_{i=0}^{v} f(x, y)) \circ \theta(x, y) = (\prod_{i=0}^{v} f(x, y)) \circ \theta(x, y).
\]

**pr.HOCO** 54. (Roby [112]) Let \( f : M \rightarrow N \) be a polynomial law over \( k \). Show that there is a unique family \((f_d)_{d \geq 0}\) of polynomial laws \( M \rightarrow N \) over \( k \) such that the following conditions hold: (i) the family \((f_d)_{d \geq 0}\) is locally finite, (ii) \( f = \sum f_d \), (iii) \( f_d \) is homogeneous of degree \( d \) for all \( d \geq 0 \). Give an example where \( f_d \neq 0 \) for all \( d \geq 0 \).

**pr.COPOLA** 55. Constant polynomial laws (Roby [112]). Show that the homogeneous polynomial laws \( M \rightarrow N \) of degree 0 are precisely of the form \( \hat{w} \circ \theta \) where \( \hat{w} : M_R \rightarrow N_R \) for \( R \in k \cdot \text{alg} \) is given by \( \hat{w}_R(x) := w_R \cdot x \in M_R \).

**pr.MULTI** 56. (Roby [112]) (a) Let \( \mu : M_1 \times \cdots \times M_n \rightarrow N \) be a multi-linear map. Show that \( \hat{\mu} : M_1 \times \cdots \times M_n \rightarrow N \) given by \( \hat{\mu}_R := \mu \otimes R \) (the \( R \)-multi-linear extension of \( \mu \)) for \( R \in k \cdot \text{alg} \) is a multi-homogeneous polynomial law of multi-degree \( \vec{1} = (1, \ldots, 1) \). Show that, conversely, every multi-homogeneous polynomial law \( M_1 \times \cdots \times M_n \rightarrow N \) of multi-degree \( \vec{1} \) uniquely arises in this way.

(b) If \( Q : M \rightarrow N \) is a quadratic map, show that \( \hat{Q} : M \rightarrow N \) given by \( \hat{Q}_R := Q \otimes R \) (the base change of \( Q \) from \( k \) to \( R \)) in the sense of [12.5] for \( R \in k \cdot \text{alg} \) is a homogeneous polynomial law of degree 2 over \( k \). Show that, conversely, every homogeneous polynomial law \( M \rightarrow N \) of degree 2 uniquely arises in this way. Identifying quadratic maps and homogeneous polynomial laws of degree 2 accordingly, prove that the total first derivative \( DQ : M \times M \rightarrow N \) of \( Q \) as a polynomial law is the same as the bilinearization of \( Q \) as quadratic map.

**pr.HIDIDE** 57. (Roby [112]) Let \( f : M \rightarrow N \) be a polynomial law over \( k \) and \( p \in \mathbb{N} \).

(a) Show for \( n \in \mathbb{Z}, n > p, v_1, \ldots, v_n \in \mathbb{N}, x_1, \ldots, x_p \in M_{k, R} \) that

\[
(\prod_{i=1}^{v} f(x_1, \ldots, x_p, \ldots, x)) \circ \theta(x_1, \ldots, x_p, \ldots, x) = \frac{(v_1 + \cdots + v_n)!}{v_1! \cdots v_n!} (\prod_{i=1}^{v} f(x_1, \ldots, x_p, \ldots, x)) \circ \theta(x_1, \ldots, x_p, \ldots, x).
\]

(b) Show for \( y \in M \) that \( \partial y \circ f : M \rightarrow N \) given by \( (\partial y \circ f)(x) = (D^p f)(x, y_R) (R \in k \cdot \text{alg}, x \in M_R) \) is a polynomial law over \( k \). Moreover, the map \( \partial y : \text{Pol}_k(M, N) \rightarrow \text{Pol}_k(M, N) \) satisfies \( (\partial y)^p = p! \partial y^p \).

(c) Show that \( \partial y \circ z = \partial y \circ z + \partial z \circ y + \partial z \circ z \) for \( y, z \in M \).

**pr.EXOCUB** 58. Exotic cubic forms. Even when working over a field, homogeneous polynomial laws of degree \( \geq 3 \) are no longer determined by the set maps they induce over the base ring. Examples for this phenomenon will be discussed in the present exercise.

(a) Let \( f : M \rightarrow N \) be a homogeneous polynomial law of degree 3 over \( k \). Simplify notation by writing \( f(x) = f_k(x) \) for \( R \in k \cdot \text{alg}, x \in M_R \) (ditto for other polynomial laws), and put
for $x, y, z \in M_R$. Then prove

$$f(x + ty) = f(x) + tf(x,y) + t^2f(y,x) + t^3f(y),$$

$$f(x + y, z) = f(x,z) + f(x,y) + f(y,z),$$

$$f(x, y, z) = f(x + y + z) - f(x + y) - f(y + z) - f(z + x) + f(x) + f(y) + f(z),$$

$$f(\sum_{i=1}^{n} r_i x_i) = \sum_{i=1}^{n} r_i^2 f(x_i) + \sum_{1 \leq i < j \leq n} r_i r_j f(x_i, x_j) + \sum_{1 \leq i < j < k \leq n} r_i r_j r_k f(x_i, x_j, x_k)$$

for all $R \in k\text{-alg}, n \in \mathbb{Z}, n > 0$, a variable $t$ and elements $x, y, z, x_1, \ldots, x_n \in M_R, r_1, \ldots, r_n \in R$.

(b) Let $F$ be a field, $n \in \mathbb{Z}, n > 0$, $F^n$ $n$-dimensional column space over $F$ with the canonical basis $\{e_i\}_{1 \leq i \leq n}$ and $g: F^n \rightarrow F$ a cubic form. View $F^n$ as a unital commutative associative $F$-algebra under the component-wise multiplication and prove that the following conditions are equivalent.

(i) The set map $g_F: F^n \rightarrow F$ is zero but $g$ itself is not.
(ii) $F \cong \mathbb{F}_2$ consists of two elements,

$$g_F(e_i) = g_F(x, x) = g_F(x, y, z) = 0 \quad (1 \leq i \leq n, x, y, z \in F^n),$$

and there are $x_0, y_0 \in F^n$ such that $g_F(x_0, y_0) \neq 0$.
(iii) $F \cong \mathbb{F}_2$ consists of two elements and there exists a non-zero alternating matrix $S \in \text{Mat}_n(F)$ such that

$$g_R(x) = x^t S x^2$$

for all $R \in F\text{-alg}$ and all $x \in (F^n)_R = R^n$.

### 59. Cubic maps

In this exercise, we compare Faulkner’s approach [29] to homogeneous polynomial maps, for simplicity restricted here to the special case of degree 3, with the formalism of polynomial laws.

(a) Show that the totality of polynomial laws over $k$ can be canonically converted into a category, denoted by $k\text{-polaw}$, and regard the homogeneous polynomial laws of degree 3 as a full subcategory, denoted by $k3\text{-holaw}$, of $k\text{-polaw}$.

(b) Let $M$ and $N$ be $k$-modules. Following Faulkner [29], define a cubic map from $M$ to $N$ as a pair $(f, g)$ of set maps $f: M \rightarrow M$ and $g: M \times M \rightarrow N$ satisfying the following conditions.

(i) $f$ is homogeneous of degree 3: $f(\alpha x) = \alpha^3 f(x)$ for all $\alpha \in k$ and all $x \in M$.

(ii) $g$ is quadratic-linear: For all $x \in M$,

$$g(x, -): M \rightarrow N, \quad y \mapsto g(x, y),$$

is a linear map, and for all $y \in M$,

$$g(-, y): M \rightarrow N, \quad x \mapsto g(x, y),$$

is a quadratic map.

(iii) $(f, g)$ satisfies the expansion

$$f(x + y) = f(x) + g(x, y) + g(y, x) + f(y)$$

for all $x, y \in M$. 

### 59. Cubic maps

In this exercise, we compare Faulkner’s approach [29] to homogeneous polynomial maps, for simplicity restricted here to the special case of degree 3, with the formalism of polynomial laws.

(a) Show that the totality of polynomial laws over $k$ can be canonically converted into a category, denoted by $k\text{-polaw}$, and regard the homogeneous polynomial laws of degree 3 as a full subcategory, denoted by $k3\text{-holaw}$, of $k\text{-polaw}$.

(b) Let $M$ and $N$ be $k$-modules. Following Faulkner [29], define a cubic map from $M$ to $N$ as a pair $(f, g)$ of set maps $f: M \rightarrow M$ and $g: M \times M \rightarrow N$ satisfying the following conditions.

(i) $f$ is homogeneous of degree 3: $f(\alpha x) = \alpha^3 f(x)$ for all $\alpha \in k$ and all $x \in M$.

(ii) $g$ is quadratic-linear: For all $x \in M$,

$$g(x, -): M \rightarrow N, \quad y \mapsto g(x, y),$$

is a linear map, and for all $y \in M$,

$$g(-, y): M \rightarrow N, \quad x \mapsto g(x, y),$$

is a quadratic map.

(iii) $(f, g)$ satisfies the expansion

$$f(x + y) = f(x) + g(x, y) + g(y, x) + f(y)$$

for all $x, y \in M$. 

### 59. Cubic maps

In this exercise, we compare Faulkner’s approach [29] to homogeneous polynomial maps, for simplicity restricted here to the special case of degree 3, with the formalism of polynomial laws.

(a) Show that the totality of polynomial laws over $k$ can be canonically converted into a category, denoted by $k\text{-polaw}$, and regard the homogeneous polynomial laws of degree 3 as a full subcategory, denoted by $k3\text{-holaw}$, of $k\text{-polaw}$.

(b) Let $M$ and $N$ be $k$-modules. Following Faulkner [29], define a cubic map from $M$ to $N$ as a pair $(f, g)$ of set maps $f: M \rightarrow M$ and $g: M \times M \rightarrow N$ satisfying the following conditions.

(i) $f$ is homogeneous of degree 3: $f(\alpha x) = \alpha^3 f(x)$ for all $\alpha \in k$ and all $x \in M$.

(ii) $g$ is quadratic-linear: For all $x \in M$,

$$g(x, -): M \rightarrow N, \quad y \mapsto g(x, y),$$

is a linear map, and for all $y \in M$,

$$g(-, y): M \rightarrow N, \quad x \mapsto g(x, y),$$

is a quadratic map.

(iii) $(f, g)$ satisfies the expansion

$$f(x + y) = f(x) + g(x, y) + g(y, x) + f(y)$$

for all $x, y \in M$. 

Euler’s differential equation holds:

\[ g(x, x) = 3f(x) \]

for all \( x \in M \).

Cubic maps from \( M \) to \( N \) as above, symbolized by \( (f, g): M \to N \), form a \( k \)-module in the obvious way. Now prove:

(c) If \( (f, g): M \to N \) is a cubic map, then the assignment

\[ (x, y, z) \mapsto g(x, y, z) := g(x + y, z) - g(x, z) - g(y, z) \]

defines a trilinear map \( M \times M \times M \to N \) which is totally symmetric. Moreover,

\[ \text{Rad}(f, g) := \{ x \in M \mid \forall y \in M : f(x) = g(x, y) = g(y, x) = 0 \} \]

called the radical of \( (f, g) \), is a submodule of \( M \) such that

\[ g(\text{Rad}(f, g), M, M) = \{ 0 \} \]

and for any linear surjection \( \pi: M \to M_1 \) of \( k \)-modules having \( \text{Ker}(\pi) \subseteq \text{Rad}(f, g) \), there is a unique cubic map \( (f_1, g_1): M_1 \to N \) such that \( f_1 \circ \pi = f \) and \( g_1 \circ (\pi \times \pi) = g \).

(d) The totality of cubic maps between \( k \)-modules can be canonically converted into a category, denoted by \( k\text{-cump} \). Furthermore, the assignment \( f \mapsto (f_1, (Df)_k) \) on objects and the identity on morphisms yields a well defined isomorphism of categories from \( k\text{-holaw} \) onto \( k\text{-cump} \), the inverse of that isomorphism on objects being denoted by \( (f, g) \mapsto f \circ g \).

**60. Matching non-scalar polynomial laws with scalar ones.** (Loos [67], 18.5) Prove for \( k \)-modules \( M, N \) that there exists a unique \( k \)-linear map

\[ \Psi: N \otimes \text{Pol}(M, k) \to \text{Pol}(M, N) \]

satisfying

\[ \Psi(v \otimes f)(x) = v \otimes f_R(x) \]

for all \( v \in N, f \in \text{Pol}(M, k), R \in k\text{-alg}, x \in M_k \). Moreover, \( \Psi \) is an isomorphism if \( N \) is finitely generated projective.

**61.** Let \( \sigma: K' \to K \), \( \tau: K'' \to K' \) be morphisms in \( k\text{-alg} \). \( M \) a \( K \)-module, \( M' \) a \( K' \)-module and \( M'' \) a \( K'' \)-module

(a) Let \( \varphi: M' \to M \) be a \( \sigma \)-semi-linear map. Show for \( R \in k\text{-alg} \) that there is a unique \( \sigma \)-semi-linear map \( \varphi_R: M'_{\text{gen}} \to M_R \) satisfying

\[ \varphi_R(x' \otimes_K r^R) = \varphi(x') \otimes_K r \]

for all \( x' \in M', \: r \in R \). Moreover, \( \varphi_R \) is \( \sigma_R \)-semi-linear, and the family of set maps \( \varphi_R: M'_{\text{gen}} \to M_R, R \in k\text{-alg} \), is a \( \sigma \)-semi-polynomial law \( \varphi: M' \to M \) over \( k \).

(b) Let \( f: M' \to M \) (resp. \( g: M'' \to M' \)) be a \( \sigma \)- (resp. \( \tau \)-) semi-polynomial law over \( k \). Show that the family of set maps

\[ (f \circ g)_R := f_R \circ g_{\text{gen}} : M'_{\text{gen}} = M'_{\text{gen}} \to M_R \]

defines a \( \sigma \tau \)-semi-polynomial law \( f \circ g: M'' \to M \) over \( k \), called the composition of \( f \) and \( g \). Conclude that the composition \( (f, g) \to f \circ g \) is associative in the obvious sense.
(c) Let $\varphi : M' \to M$ (resp. $\psi : M'' \to M'$) be $\sigma$- (resp. $\tau$-) semi-linear maps. Prove $(\varphi \circ \psi)^\sim = \varphi \circ \psi$ as an equality of semi-polynomial laws.

(d) Assume $\sigma : K' \tilde{\to} K$ is an isomorphism in $k$-$\textbf{alg}$. Prove that $f : M' \to M$ is a $\sigma$-semi-polynomial law over $k$ if and only if there exists an ordinary polynomial law $g : M' \to M^\sigma$ over $K'$ satisfying $f = (\sigma_M)^\sim \circ g$, and that, in this case, $g$ is unique.

**Pr. POSEPO 62.** Extend all concepts and results of the present section from ordinary polynomial laws to semi-polynomial laws.
Chapter 3
Alternative algebras

Alternative algebras belong to the most important building blocks of Albert algebras. They will be presented here with this connection always in mind. We begin by deriving a number of important identities, proceed to establish a fairly general version of Artin’s associativity theorem and investigate homotopes of alternative algebras, which in turn give rise to the study of isotopy involutions in the final section of this chapter.

14. Basic identities and invertibility

Having gained some proficiency in the language of arbitrary non-associative algebras, we are now adequately prepared to deal with the more specific class of alternative algebras. After giving the formal definition, we derive the Moufang identities and introduce the notion of invertibility. Throughout, we let \( k \) be an arbitrary commutative ring.

14.1. The concept of an alternative algebra. A \( k \)-algebra \( A \) is said to be alternative if its associator (cf. 8.5), i.e., the trilinear map \( (x,y,z) \mapsto [x,y,z] = (xy)z - x(yz) \) from \( A \times A \times A \) to \( A \), is alternating. This means that the following identities hold in \( A \):

\[
\begin{align*}
    x(xy) &= x^2y, \quad \text{(left alternative law)} \\
    (yx)x &= yx^2, \quad \text{(right alternative law)} \\
    (xy)x &= x(yx). \quad \text{(flexible law)}
\end{align*}
\]

In fact, since the symmetric group on three letters is generated by any two of the transpositions \( (1,2), (2,3), (3,1) \), any two of the above equations imply the third, hence force \( A \) to be alternative. An alternative algebra and its opposite have the same associator, so \( A^{\text{op}} \) is alternative if and only if \( A \) is. It is sometimes convenient to express the alternative laws in operator form, i.e., in terms of left and right multiplications as follows:

\[
\begin{align*}
    L_x^2 &= L_{x^2} \quad \text{(4) \quad LALT} \\
    R_x^2 &= R_{x^2} \quad \text{(5) \quad RALT} \\
    L_xR_x &= R_xL_x. \quad \text{(6) \quad FLEX}
\end{align*}
\]
14.2. Linearizations. For the rest of this section, we fix an alternative algebra \( A \) over \( k \). Then, thanks to flexibility, the expression \( xyx \) is unambiguous in \( A \). Also, since (14.1.1) \(-\) (14.1.3) are quadratic in \( x \), they may be linearized to yield new identities valid in \( A \). For example, replacing \( x \) by \( x + z \) in (14.1.1), collecting mixed terms and interchanging \( y \) with \( z \), we obtain

\[
x(yz) + y(xz) = (xy + yx)z.
\]

Similarly,

\[
(xy)z + (xz)y = x(yz + zy),
\]

\[
(xy)z + (zy)x = x(yz) + z(xy).
\]

Again these relations can be expressed in terms of left and right multiplications; details are left to the reader. Also, it is now straightforward to check that the property of an algebra to be alternative remains stable under base change: \( A_R \) is alternative, for any \( R \in k\text{-alg} \).

14.3. The Moufang identities. Less obvious is the fact that the Moufang identities

\[
(xy)x = (yx)x, \quad (yz)x = y(xz), \quad (xy)(zx) = x(zy)x,
\]

hold in any alternative algebra. Since the associator is alternating, (1) follows from (14.1.1), (14.2.2) and

\[
(xy)x - x(y(xz)) = [xy, x, z] + [x, y, xz] = -[x, xy, z] - [x, xz, y]
\]

\[
= -((x^2)y)z - (x^2)z)y + x((xy)z + (xz)y)
\]

\[
= -x^2(yz + zy) + x(yz + zy) = 0.
\]

Reading the left Moufang identity in the opposite algebra \( A^\text{op} \) gives the right Moufang identity. Finally, again using the fact that the associator is alternating, but also (1), we obtain

\[
(xy)(zx) - x(yz)x = [x, y, zx] - x[y, z, x] = -[x, zx, y] - x[z, x, y]
\]

\[
= -((zx)y) + x((zx)y) - x((zx)y) + x(z(xy)) = 0,
\]

and the middle Moufang identity is proved.

Viewing (1), (2) as linear maps in \( z \) and (3) as a bilinear one in \( y, z \), the Moufang identities may also be expressed as.
14.4. Inverses. There is no useful concept of invertibility in arbitrary non-associative algebras. Fortunately, however, the standard notion for associative algebras carries over to the alternative case without change. If \( A \) is unital (with identity element \( 1_A \)), an element \( x \in A \) is said to be invertible if there exists an element \( y \in A \), called an inverse of \( x \) in \( A \), that satisfies the relations \( xy = 1_A = yx \). Indeed, the concept of invertibility enjoys the usual properties. Before proving this, we need a preparation.

### 14.5. The \( U \)-operator

The \( U \)-operator of \( A \) (no longer assumed to be unital) is defined as the quadratic map

\[
U : A \rightarrow \text{End}_k(A), \quad x \mapsto U_x := L_x R_x = R_x L_x,
\]

which acts on individual elements as

\[
U_x y = xyx.
\]

Note that the \( U \)-operator does not change when passing to the opposite algebra. Moreover, it may be used to rewrite the middle Moufang identity in the form

\[
U_x (yz) = (L_x y)(R_x z).
\]

Finally, the \( U \)-operator satisfies the following important relations:

\[
U_{xy} = L_x U_y R_x = R_x U_y L_x
\]

for all \( x, y \in A \). Indeed, using \( [14.3][7], [14.3][5], [14.3][2], [14.1][1] \), we obtain

\[
U_{xy} z = (xy)z)(xy) = x((yz)(xy) + [(xy)z]y) - ([x(xy)]z)y = x(yz + x(yz)) - x^2(yz) = x(yz)y
\]

for all \( z \in A \), giving the first part of \( [4] \). The second one follows by passing to \( A^{op} \).

### 14.6. Proposition

Let \( A \) be unital and \( x \in A \). Then the following conditions are equivalent.

(i) \( x \) is invertible.
(ii) \( L_x \) is bijective.

(iii) \( R_x \) is bijective.

(iv) \( U_x \) is bijective.

(v) \( L_x \) and \( R_x \) are surjective.

(vi) \( U_x \) is surjective.

(vii) \( 1_A \in \text{Im}(L_x) \cap \text{Im}(R_x) \).

(viii) \( 1_A \in \text{Im}(U_x) \).

**In this case, \( x \) has a unique inverse in \( A \), denoted by \( x^{-1} \), and**

\[
\begin{align*}
x^{-1} &= L_x^{-1}1_A = R_x^{-1}1_A = U_x^{-1}x, \\
L_{x^{-1}} &= L_x^{-1}, \quad R_{x^{-1}} = R_x^{-1}, \quad U_{x^{-1}} = U_x^{-1}.
\end{align*}
\]

**Proof.** (i) \( \iff \) (ii). If \( x \) is invertible with inverse \( y \), we obtain \( xy^2x = 1_A \) by \((14.3.3)\), hence \( L_xL_xL_x = 1_A \) by \((14.3.4)\), and (ii) follows. Conversely, suppose \( L_x \) is bijective. Then there is a unique \( y \in A \) satisfying \( xy = 1_A \), and the relation \( x(yx) = (xy)x = 1_Ax = x1_A \) combined with (ii) shows \( yx = 1_A \), hence (i).

(i) \( \iff \) (iii). This is just (i) \( \iff \) (ii) in \( C^{op} \).

(iii) \( \implies \) (iv). Obvious since (iii) implies (ii).

(iv) \( \implies \) (v). Obvious since \( L_x \) and \( R_x \) commute by flexibility \((14.1.6)\).

(v) \( \implies \) (vi) \( \implies \) (vii). Obvious, again by flexibility.

(vii) \( \implies \) (viii). We find elements \( y,z \in A \) satisfying \( xy = zx = 1_A \), and \((14.3.3)\) gives \( x(yz)x = 1_A \).

(viii) \( \implies \) (ii). We find an element \( w \in A \) satisfying \( xwx = 1_A \), and \((14.3.1)\) implies \( L_xL_xL_x = 1_A \), forcing \( L_x \) to be bijective.

Uniqueness of the inverse and \((1)\) now follow from (ii), (iii), (iv). Furthermore, \( xx^{-1}x = x \) and the \((14.3.4)\) implies \( L_xL_{x^{-1}}L_x = L_x \), so (ii) gives \( L_{x^{-1}} = L_x^{-1} \). Reading this in \( A^{op} \) yields \( R_{x^{-1}} = R_x^{-1} \), hence \( U_{x^{-1}} = U_x^{-1} \), and the proof of \((2)\) is complete. \( \square \)

**14.7. The set of invertible elements.** If \( A \) is unital, then the set of its invertible elements will be denoted by \( A^\times \). Clearly, \( 1_A \in A^\times \), and \( x \in A^\times \) implies \( x^{-1} \in A^\times \) with \((x^{-1})^{-1} = x \). Moreover, \( A^\times \) is closed under multiplication. More precisely, if \( x,y \in A \) are invertible, so is \( xy \) and

\[
(xy)^{-1} = y^{-1}x^{-1}.
\]

Indeed, setting \( z = y^{-1}x^{-1} \), the Moufang identities and \((14.6.2)\) imply \((xy)z) = x(y(y^{-1}x^{-1})y) = x(x^{-1}y) = y \), hence \((xy)z = 1_A \) by Prop. \((14.6)(ii)\). Replacing \( x \) by \( y^{-1} \) and \( y \) by \( x^{-1} \) yields \( z(xy) = 1_A \), and \((1)\) follows.

**14.8. Remark.** Prop. \((14.6)\) shows that a unital alternative algebra is a division algebra in the sense of \((9.7)\), if and only if \( 1_A \neq 0 \) and every non-zero element is invertible.
15. Strongly associative subsets

Our aim in this section will be to prove Artin’s associativity theorem, which says that every alternative algebra on two generators is associative. Actually, we will derive a somewhat more general result by adopting the approach of Bourbaki \cite{12} III, Appendix, \S 1\) (see also Braun-Koecher \cite{15} VII, \S 1). Throughout we let \( k \) be a commutative ring and \( A \) an alternative \( k \)-algebra.

15.1. The concept of a strongly associative subset. A subset \( X \subseteq A \) is said to be strongly associative if \([x,y,z] = 0\) provided at least two of the elements \( x, y, z \in A \) belong to \( X \). Since the associator is alternating, this is equivalent to the condition \([X,X,A] = \{0\}\). Hence, if \( X \subseteq A \) is strongly associative, so is the submodule spanned by \( X \), and \( X \cup \{1_A\} \) provided \( A \) is unital. Examples of strongly associative subsets are \( X = \{x\} \), for any \( x \in A \) (by \((14.1.1)\)) , and \( X = \{x,x^{-1}\} \), for \( A \) unital and any \( x \in A^\times \) (by \((14.1.1)\), \((14.6.2)\)).

15.2. Lemma. Let \( X \subseteq A \) be a set of generators for \( A \) as a \( k \)-algebra. Suppose \( M \subseteq A \) is a \( k \)-submodule that contains \( X \) and satisfies \( XM + MX \subseteq M \). Then \( M = A \).

Proof. We begin by showing that \( A' \), the set of elements \( x \in A \) satisfying \( xm + Mx \subseteq M \), is closed under multiplication, so let \( x, y \in A' \). Then, for all \( z \in M \), \((xy)z = [x,y,z] + x(zy) = x(zy) - [x,z,y] = x(yz) - (xz)y + x(zy) \in M \) and, similarly, \( z(xy) \in M \), forcing \( xy \in A' \), as claimed. It follows that \( A' \), being a subalgebra of \( A \) containing \( X \), agrees with \( A \), which implies \( AM \subseteq M \). But then \( M \) must be a subalgebra of \( A \) containing \( X \), and we conclude \( M = A \). \( \square \)

15.3. Proposition. If \( X \) is a strongly associative subset of \( A \), then so is the subalgebra of \( A \) generated by \( X \).

Proof. By \((8.4)\) it suffices to show that \( \text{Mon}(X) = \bigcup_{m \geq 0} \text{Mon}_m(X) \), the set of monomials over \( X \), is a strongly associative subset of \( A \). To this end, we only need to prove

\[
[\text{Mon}_m(X),\text{Mon}_n(X),A] = \{0\} \quad (m,n \in \mathbb{Z}, m,n > 0), \tag{1} \]

and we do so by induction on \( p = m + n \geq 2 \). The case \( p = 2 \) being obvious by hypothesis, let us assume \( p > 2 \). Since \((1)\) is symmetric in \( m,n \) by alternativity, we may even assume \( m > 1 \). Hence, given \( u \in \text{Mon}_m(X), v \in \text{Mon}_n(X), a \in A \), we obtain \( u = u_1u_2, u_i \in \text{Mon}_{m_i}(X), m_i \in \mathbb{Z}, m_i > 0, i = 1,2, m_1 + m_2 = m \), and \((8.5.2)\) yields

\[
-[u,v,a] = [u_1u_2,v,a] = -u_1[u_2,v,a] + [u_1,u_2,a]v - [u_1,v,u_2,a] - [u_1,u_2,av],
\]

where all terms on the right vanish by the induction hypothesis. Hence \([u,v,a] = 0\), which completes the induction. \( \square \)

15.4. Proposition. Let \( X,Y \) be strongly associative subsets of \( A \). Then the subalgebra of \( A \) generated by \( X \) and \( Y \) is associative.
Proof. We may not only assume that \( A \) itself is generated by \( X \) and \( Y \) but also, by Prop. \([15.3]\), that \( X,Y \subseteq A \) are subalgebras. Then the set \( B \) of elements \( z \in A \) such that \([X,Y,z] = \{0\}\) is a submodule of \( A \) containing \( X \) and \( Y \) since they are both strongly associative. The proof will be complete once we have shown \( B = A \) since this implies \([X \cup Y,X \cup Y,A] = \{0\}\), forcing \( X \cup Y \) to be a strongly associative subset of \( A \); this property is inherited by the subalgebra generated by \( X \) and \( Y \), which shows that \( A \) is associative, as desired. In order to prove \( B = A \), we apply Lemma \([15.2]\) and hence must show

\[
XB + BX + YB + BY \subseteq B. \tag{1}
\]

Accordingly, let \( x,x' \in X, y \in Y, z \in B \). Then \([8.5][2]\) yields

\[
[x'x,z,y] - [x',xz,y] + [x',x,y]z = 0
\]

since \( z \in B \) and \( X \) is strongly associative, which implies \([x',x,y] = 0\) as well. But \( X \) is also a subalgebra of \( B \), whence \([x'x,z,y] = 0\). Altogether, we conclude \([X,Xz,Y] = \{0\}\), forcing \( Xz \subseteq B \). Interchanging the roles of \( X \) and \( Y \) and passing to the opposite algebra, we obtain \([1]\), and the proof is complete. \( \square \)

15.5. Corollary. (Artin’s theorem) Let \( x,y \in A \). Then the subalgebra of \( A \) generated by \( x \) and \( y \) is associative. If \( A \) is unital, the same conclusion holds for the unital subalgebra of \( A \) generated by \( x, y \) and (if they exist) their inverses.

Proof. In the non-unital case, put \( X = \{x\}, Y = \{y\} \). In the unital case, put \( X = \{x, 1_A\} \) if \( x \) is not invertible, \( X = \{x, 1_A, x^{-1}\} \) otherwise, ditto for \( Y \). \( \square \)

15.6. Corollary. Alternative algebras are power-associative. Moreover, if \( A \) is unital, then \( x^{m+n} = x^m x^n \) and \( (x^n)^m = x^{mn} \) for all \( x \in A^\times \), \( m, n \in \mathbb{Z} \). \( \square \)

Exercises.


64. A characterization of unital alternative algebras (McCrimmon \([29]\)). Let \( A \) be an alternative \( k \)-algebra. Show that the following conditions are equivalent.

(i) \( A \) is unital.
(ii) For some \( x \in A \), both \( L_x \) and \( R_x \) are bijective.
(iii) For some \( x \in A \), both \( L_x \) and \( R_x \) are surjective.
(iv) For some \( x \in A \), \( U_x \) is surjective.
(v) For some \( x, y \in A \), both \( L_x \) and \( R_x \) are bijective.

65. One-sided inverses (McCrimmon \([29]\)). Let \( A \) be a unital alternative \( k \)-algebra and \( x, y \in A \). Show that the following conditions are equivalent.

(i) \( xy = 1_A \).
(ii) \( L_x L_y = 1_A \).
(iii) \( R_x R_y = 1_A \).
16 Homotopes

(Hint. For the implication (i) ⇒ (ii) prove that \( E = L_s, L_t, F = R_s R_t \) are projections of the \( k \)-module \( A \) satisfying \( EF = 1_A \).)

If these conditions are fulfilled, \( x \) (resp. \( y \)) is said to be right-invertible (resp. left-invertible) with right (resp. left) inverse \( y \) (resp. \( x \)) (in general not unique).

pr.INVPRODALT

66. (McCrimmon [79]) Let \( A \) be a unital alternative algebra over \( k \) and \( x, y \in A \) such that \( xy \) is invertible. Show in the language of Exc. 65 that \( x \) is right-invertible with \( y(xy)^{-1} \) as a right inverse and \( y \) is left-invertible with \( (xy)^{-1} x \) as a left inverse. (Hint. For the first assertion, use (14.5.4) to show that \( L_y \) is injective.)

pr.PEIRCEALT

67. The singular Peirce decomposition of alternative algebras (cf. Schafer [114]). Let \( A \) be a unital alternative algebra over \( k \) and \( c \in A \) an arbitrary idempotent. Put \( c_1 = c, c_2 = 1_A - c \) to prove that the maps \( L_c, R_c : A \to A \) (i, \( j = 1, 2 \)) form a complete orthogonal system of projections satisfying \((c_1 x)c_j = c_i(xc_j) = 0 \) for all \( x \in A \). (Hint. Expand \( U_{c_1 + c_2} \).) Conclude

\[
A = A_{11} \oplus A_{12} \oplus A_{21} \oplus A_{22}
\]

(1) as a direct sum of submodules

\[
A_{ij} := A_{ij}(c) := \{ x \in A \mid c_ixc_j = x \} = \{ x \in A \mid c_i(x = x = xc_j) \}
\]

(2) that satisfy the multiplication rules

\[
A_{ij} A_{ji} \subseteq A_{ii}, \quad A_{ij} A_{il} = A_{ij} A_{il} = \{0\}, \quad (i \neq j) \quad (3) \quad \text{PALTC}
\]

\[
A_{ij}^2 \subseteq A_{ii}, \quad (i \neq j) \quad (4) \quad \text{PALTU}
\]

for all \( i, j, l = 1, 2 \). Prove \( x^2 = 0 \) for all \( x \in A_{ij}, i \neq j \), and that (5) can be sharpened to \( A_{ij}^2 = \{0\} \) (for \( i \neq j \)) if \( A \) is associative.

16. Homotopes

Homotopes have been established a long time ago as an extremely versatile tool in the theory of Jordan algebras and can look back to a long, respectable history. Though they entered the scene of alternative algebras only much later, without ever receiving the amount of attention they were accustomed to from the Jordan setting, it will be shown in the present book that, also in these new surroundings, they provide a useful and convenient formalism for many problems related to Albert algebras.

In the present section, the conceptual foundations for homotopes and isotopes of alternative algebras will be laid down following McCrimmon [79]. Throughout, we let \( k \) be an arbitrary commutative ring and \( A \) an alternative algebra over \( k \). We begin with an easy special case of the general concept.

ss.HOMOTASS

16.1. Digression: associative algebras For the time being, let \( B \) be an associative \( k \)-algebra and \( p \in B \). Define a new \( k \)-algebra \( B^{(p)} \) on the \( k \)-module \( B \) by the multiplication

\[
B^{(p)} = B 
\]
We call $B^{(p)}$ the \textit{$p$-homotope} of $B$, which is obviously associative; moreover, the maps $L_p, R_p: B^{(p)} \to B$ is an algebra homomorphism. In particular, if $B$ is unital and $p$ is invertible, $B^{(p)} \cong B$ under $L_p$ or $R_p$. This explains why homotopes do not play a significant role in (associative) ring theory.

16.2. The concept of a homotope Returning to our original alternative algebra $A$, let $p, q \in A$. On the $k$-module $A$ we define a new $k$-algebra $A^{(p,q)}$ by the multiplication

\[ x \cdot p \cdot y := (xp)(qy) \quad (x, y \in A). \tag{1} \]

We call $A^{(p,q)}$ the \textit{$p,q$-homotope} (or just a homotope) of $A$. We obviously have

\[ (A^{(p,q)})^{op} = (A^{op})^{(p,q)}, \quad A^{(\alpha p, \alpha^{-1}q)} = A^{(p,q)} \quad (\alpha \in k^\times). \tag{2} \]

A $k$-algebra is said to be \textit{homotopic} to $A$ if it is isomorphic to some of its homotopes. If $A$ is associative, \textit{(1)} collapses to $x \cdot p \cdot q = xpq$, so $A^{(p,q)} = A^{(pq)}$ as in \textit{16.1}.

Our next aim will be to show that homotopes of alternative algebras are alternative, and that homotopes of homotopes are homotopes. More precisely, we obtain the following proposition.

16.3. Proposition. Let $p, q, p', q' \in A$. Then $A^{(p,q)}$ is an alternative $k$-algebra and

\[ (A^{(p,q)})^{(p',q')} = A^{(p''q)} \quad p'' := p(qp')p, \quad q'' := q(q'p)q. \tag{1} \]

\textit{Proof.} For the first part, it suffices to verify the left alternative law \textit{(14.1)} since by passing to the opposite algebra and invoking \textit{(16.2)}, we will obtain the right alternative law as well. So let $x, y \in A$. Then \textit{(14.3)} and the Moufang identities \textit{(14.3.1)}, \textit{(14.3.2)} imply

\[ x \cdot p \cdot (x \cdot p \cdot q) = (xp)(q[xp](qy))] = (Uxpq)(qy) = (LqURxq)(qy) = (xp)(pqx)p(y) = (xp)(qy) = (x \cdot p \cdot q) \cdot p \cdot q, \]

hence \textit{(14.1)} for $A^{(p,q)}$. The verification of the second part is straightforward and left to the reader. \hfill \square

16.4. Functoriality. We denote by $k$-$\text{alt}$ the category of (possibly non-unital) alternative $k$-algebras, morphisms being ordinary $k$-algebra homomorphisms \textit{(8.1)}. By contrast, the category of \textit{weakly 2-pointed alternative $k$-algebras} will be denoted by $k$-$\text{alt}$. Its objects are triples $(A, p, q)$ consisting of an alternative $k$-algebra $A$ and a pair of elements $p, q \in A$, while its morphisms have the form $h: (A, p, q) \to (A', p', q')$ with weakly two-pointed alternative $k$-algebras $(A, p, q), (A', p', q')$ and
an algebra homomorphism \( h : A \to A' \) satisfying \( h(p) = \alpha p' \), \( h(q) = \alpha^{-1} q' \) for some \( \alpha \in k^{\times} \). It is then clear that the assignment \( (A, p, q) \mapsto A^{(p,q)} \) gives rise to a (covariant) functor from \( k\text{-twalt} \) to \( k\text{-alt} \) which is the identity on morphisms.

16.5. The connection with unital algebras \( \) We are particularly interested in homotopes containing an identity element. In order to find necessary and sufficient conditions for this to happen, we consider the \( U \)-operator \( U^{(p,q)} \) of \( A^{(p,q)} \) \( (p, q \in A) \), so \( U^{(p,q)} \) \( = L^{(p,q)} A^{(p,q)} \) by \( \{14.5.1\} \), where \( L^{(p,q)} \), \( R^{(p,q)} \) stand for the left, right multiplication of \( A^{(p,q)} \). We claim

\[
U^{(p,q)}_x = U_x U_{pq} \quad (x \in A).
\]

To prove this, we let \( x, y \in A \) and compute, using flexibility in \( A^{(p,q)} \), the Moufang identities and \( \{14.5.2\}, \{14.5.4\} \)

\[
U^{(p,q)}_x y = \left( (xp)(qy)p \right)(qx) = (x[pqy])q(xq) = x(R_q U_p L_q y)x = U_x U_{pq} y,
\]

as desired.

16.6. Proposition. \( \) For \( p, q \in A \), the \( p, q \)-homotope \( A^{(p,q)} \) has a unit element if and only if \( A \) has a unit element and \( pq \) is invertible in \( A \). In this case, \( 1^{(p,q)}_A := (pq)^{-1} \) is the unit element of \( A^{(p,q)} \).

Proof. If \( e \in A \) is a unit element for \( A^{(p,q)} \), then \( \{16.5.1\} \) implies \( 1_A = U^{(p,q)} e = U_x U_{pq} \), so \( U_{pq} \) is surjective. But then \( A \) is unital (Exc. \( \{64\} \), and \( e \) must be invertible in \( A \) (Prop. \( \{14.6\} \)). Hence so is \( pq \) with \( U_{pq}^{-1} = U_e \) and \( (pq)^{-1} = U_{pq}^{-1} U_p U_q = (ep)(q) = e.p.q e = e \) since \( e \) is a unit element for \( A^{(p,q)} \). Conversely, let \( A \) be unital and suppose \( pq \in A \) is invertible with inverse \( e := (pq)^{-1} \). Then Exc. \( \{66\} \) implies \( (ep)q = 1_A \), forcing \( L_q L_p = 1_A \) by Exc. \( \{65\} \) and we conclude \( e.p.q x = (ep)(qx) = x \) for all \( x \in A \), so \( e \) is a left unit element for \( A^{(p,q)} \). Passing to the opposite algebra of \( A \) will show that \( e \) is also a right unit for \( A^{(p,q)} \), forcing \( A^{(p,q)} \) to be unital with identity element \( e \).

\( \square \)

16.7. Isotopes \( \) If \( A \) is unital and \( p, q \in A \) are both invertible (which is stronger than just requiring \( pq \) to be invertible), then \( A^{(p,q)} \) is called the \( p, q \)-isotope (or simply an isotope) of \( A \). By Props. \( \{16.3\}, \{16.6\} \) \( A^{(p,q)} \) is a unital alternative algebra in this case, with unit element

\[
1^{(p,q)}_A = (pq)^{-1} = q^{-1} p^{-1}, \quad \text{(1)}
\]

and \( \{16.3.1\} \) gives

\[
(A^{(p,q)})^{(p', q')} = A \quad \text{for} \quad (p' := q^{-1} p^{-1}, q' := q^{-2} p^{-1}). \quad \text{(2)}
\]
In particular, calling a $k$-algebra isotopic to $A$ if it is isomorphic to some of its isotopes, isotopy is an equivalence relation on unital alternative algebras.

By (1), the algebra $A^\langle p,q \rangle$, for $A$ unital and $p,q \in A^\times$, determines the product $pq$ uniquely. But it is important to note that the factors of this product are not uniquely determined by $A^\langle p,q \rangle$. Indeed, bringing in the nucleus of $A$ (cf. [9.6]), we have

16.8. Proposition. Let $A$ be unital and $p,q,p',q' \in A^\times$. Then $A^\langle p,q \rangle = A^\langle p',q' \rangle$ if and only if $p' = pu, q' = u^{-1}q$ for some $u \in \text{Nuc}(A)^\times$.

Proof. $p' = pu, q' = u^{-1}q$ for some $u \in \text{Nuc}(C)^\times$ clearly implies $A^\langle p,q \rangle = A^\langle p',q' \rangle$. Conversely, assume $A^\langle p,q \rangle = A^\langle p',q' \rangle$. Then

$$(xp)(qy) = (xp')(q'y) \quad (x,y \in A). \quad (1)$$

Setting $u := p^{-1}p'$, we obtain $p' = pu$, and (1) for $x = p'^{-1}, y = 1_A$ yields $q' = u^{-1}q$, hence $u = qq^{-1}$. It remains to prove $u \in \text{Nuc}(A)$ and, since $A$ is alternative, it suffices to show $[A,u,A] = \{0\}$. To this end, we put $y = q'^{-1}$ (resp. $x = p'^{-1}$) in (1) to obtain $(xp)u = xp'$ (resp. $u^{-1}(qy) = q'y$). Hence (1) reads $(xp)(qy) = ((xp)u)(u^{-1}(qy))$, and since $p,q$ are invertible, this amounts to $xy = (xu)(u^{-1}y)$ for all $x,y \in A$. Replacing $y$ by $uy$ and invoking (14.6.2), we conclude $[A,u,A] = \{0\}$, as desired. □

16.9. Unital isotopes. If $A$ is unital, an isotope of $A$ is said to be unital if it has the same identity element as $A$. By (16.7.1), unital isotopes have the form

$$A^p := A^\langle p^{-1}, p \rangle \quad (p \in A^\times). \quad (1)$$

By Exc. 68 invertibility and inverses in $A$ and $A^p$ ($p \in A^\times$) are the same, while from (16.2.1), (16.3.1) we conclude

$$(A^p)^p = (A^p)^{p^{-1}}, \quad (A^p)^q = A^{pq}, \quad A^{\alpha p} = A^p \quad (p,q \in A^\times, \alpha \in k^\times). \quad (2)$$

Moreover, Prop. [16.8] implies

$$A^p = A^q \iff p = uq \text{ for some } u \in \text{Nuc}(A)^\times \quad (p,q \in A^\times). \quad (3)$$

In particular, $A^p = A$ for all $p \in A^\times$ if $A$ is associative.

Unital isotopes are important for various reasons: for example, they play a useful role in the two Tits constructions of cubic norm structures. Moreover, arbitrary isotopes are always isomorphic to appropriate unital ones (cf. Exc. 73 below). And finally, working in unital isotopes turns out to be computationally smooth, as may be seen from the following lemma.

16.10. Lemma. Let $A$ be unital and $p \in A^\times$. Then $A$ and $A^p$ have the same $U$-operators as well as the same powers $x^m$ for $x \in A, m \in \mathbb{N}$ (resp. for $x \in A^\times, m \in \mathbb{Z}$).
Proof. The equality of $U$-operators follows from (16.5). Since $U_{m,n}x^n = (U_n)^m x^n = x^{2m+n}$ for $x \in A, m, n \in \mathbb{N}$ (resp. $x \in A^\times$, $m, n \in \mathbb{Z}$), the remaining assertions can now be derived by induction. 

16.11. Functoriality. Adjusting the terminology of [16.4] to the unital case, we denote by $k$-alt$_1$ the category of unital alternative $k$-algebras, morphisms being unital $k$-algebra homomorphisms (9.1). By contrast, the category of pointed alternative $k$-algebras will be denoted by $k$-palt. Its objects are pairs $(A, p)$ consisting of a unital alternative $k$-algebra $A$ and an invertible element $p \in A$, while its morphisms have the form $h: (A, p) \to (A', p')$ with pointed alternative $k$-algebras $(A, p)$, $(A', p')$ and a unital algebra homomorphism $h: A \to A'$ satisfying $h(p) = \alpha p'$ for some $\alpha \in k^\times$. Again, it is then clear that the assignment $(A, p) \mapsto A^p$ gives rise to a (covariant) functor from $k$-palt to $k$-alt$_1$ which is the identity on morphisms.

16.12. Isotopy versus isomorphism. Recall that unital alternative $k$-algebras $A, B$ are isotopic if $A \cong B^{(p,q)}$ for some invertible elements $p, q \in B$, equivalently by Exc. [73] (a), if $A \cong B^p$ for some invertible element $p \in B$. It is then a natural question to ask whether isotopic unital alternative algebra are always isomorphic. This question has a trivial affirmative answer in the associative case (cf. 16.1), but a less trivial negative one in general, cf. McCrimmon [79] p. 259 for a counter example. It is not known, however, whether isotopic unital alternative $k$-algebras exist that are finitely generated projective as $k$-modules (or even finite-dimensional over a field) but not isomorphic.

Exercises.

68. Inverses in isotopes. Let $A$ be a unital alternative $k$-algebra and $p, q \in A^\times$. Show that the invertible elements of $A$ and $A^{(p,q)}$ are the same and that, for $x \in A^\times = A^{(p,q)}$,

$$x^{(−1,p,q)} := U_{pq} x^{−1}$$

is the inverse of $x$ in $A^{(p,q)}$.

69. Albert isotopies (Albert [3]). Given non-associative $k$-algebras $A, B$, an Albert isotopy from $A$ to $B$ is a triple $(f, g, h)$ of $k$-linear bijections $f, g, h: A \to B$ such that $f(xy) = g(x)h(y)$ for all $x, y \in A$. Albert isotopies from $A$ to itself are called Albert autotopies of $A$. They form a subgroup of $\text{GL}(A) \times \text{GL}(A) \times \text{GL}(A)$, denoted by $\text{Atp}(A)$. Now prove Schafer’s isotopy theorem (Schafer [113], McCrimmon [79]). If $A, B$ are $k$-algebras, with $A$ alternative and $B$ unital, and if $(f, g, h)$ is an Albert isotopy from $A$ to $B$, then $A, B$ are both unital alternative, $g^{-1}(1_B)h^{-1}(1_A)$ are invertible in $A$, and $f: A^{(p,q)} \to B$, $p := h^{-1}(1_A)^{-1}$, $q := g^{-1}(1_A)^{-1}$, is an isomorphism.

70. The structure group of an alternative algebra (Petersson [59]). Let $A$ be a unital alternative $k$-algebra and $\text{Str}(A)$ the set of all triples $(p, q, g)$ composed of elements $p, q \in A^\times$ and an isomorphism $g: A \cong A^{(p,q)}$. Show that $\text{Str}(A)$ is a group under the multiplication

$$(p, q, g)(p', q', g') := (p|q|g(p')|p|q|g(q')|p|q|g(g'))$$

for $(p, q, g), (p', q', g') \in \text{Str}(A)$ by performing the following steps.

(a) $\text{Str}(A)$ is closed under the operation $[1]$.

(b) For $p, q \in A^\times$, $g \in \text{GL}(A)$, the following conditions are equivalent.
(i) \((p,q,g) \in \text{Str}(A)\).
(ii) \(g(xy)p = g(x)[(pq)(g(y)p)]\) for all \(x,y \in A\).
(iii) \(qg(xy) = [(gq(x))(pq)]g(y)\) for all \(x,y \in A\).

(c) The assignment \((f,g,h) \mapsto (h(1_A)^{-1}g(1_A)^{-1},f)\) determines a well defined bijection from \(\text{Aut}_p(A)\), the group of Albert autotopies of \(A\) (Exc. [99]), onto \(\text{Str}(A)\) that is compatible with multiplications and whose inverse is given by \((p,q,g) \mapsto (g,R_g,L_g)\).

What is the unit element of \(\text{Str}(A)\)? What is the inverse of \((p,q,g) \in \text{Str}(A)\)?

**71. Extended left and right multiplications** (Petersson [99]). Let \(A\) be a unital alternative algebra and \(u \in A^\times\). Prove that

\[
L_u := (u,u^{-2},L_u), \quad R_u := (u^{-2},u,R_u)
\]

belong to the structure group of \(A\) (Exc. [70]). Show further for \(u,v \in A^\times\) that the following identities hold in \(\text{Str}(A)\):

\[
\begin{align*}
L_{uv} &= L_u L_v L_u, & (L_u)^{-1} &= L_{u^{-1}}, \\
R_{uv} &= R_u R_v R_u, & (R_u)^{-1} &= R_{u^{-1}}, \\
L_u R_v &= (v^{-2} u, u^{-1} vu^{-1}, L_u R_v), \\
R_u L_v &= (v^{-1} u, u^{-1} vu^{-1}, R_u L_v), \\
L_u &= R_u L_u.
\end{align*}
\]

**72. The unital structure group** (Petersson [99]). Let \(A\) be a unital alternative \(k\)-algebra. Show that the set \(\text{Str}_1(A)\) of all elements \((p,q,g) \in \text{Str}(A)\) such that \(g(1_A) = 1_A\) (equivalently, \(p = q^{-1}\)) is a subgroup of \(\text{Str}(A)\), called the **unital structure group** of \(A\). More precisely, show:

(a) Abbreviating the elements of \(\text{Str}_1(A)\) as \((p,g) := (p^{-1},p,g)\) (so for \((p,g), p \in A^\times, g \in \text{GL}(A)\), to belong to the unital structure group of \(A\) it is necessary and sufficient that \(g\colon A \to A^p\) be an isomorphism), its group structure is determined by \(1_{\text{Str}_1(A)} = (1_A,1_A,1_A)\)

\[\begin{align*}
(p,g)(p',g') &= (pq,g'g'^{-1})
\end{align*}\]

for \((p,g),(p',g') \in \text{Str}_1(A)\).

(b) \(\text{Int}(p) := (p^{-1},L_p R_p^{-1})\) belongs to the unital structure group of \(A\). Why can \(\text{Int}(p)\) be viewed as the alternative version of the inner automorphism affected by an invertible element of a unital associative algebra?

**73.** Let \(A\) be a unital alternative algebra over \(k\).

(a) Show that arbitrary isotopes of \(A\) are canonically isomorphic to unital ones. (Hint. For \(p,q \in A^\times\), consider the extended right multiplication by \(pq\) (Exc. [71]).)

(b) Computing the iterated unital isotope \((A^p)^{q r} p\) for \(p,q,r \in A^\times\) in two different ways seems to imply \((pq)r = up(qr)\) for some invertible element \(u \in \text{Nuc}(A)\). What’s wrong with this argument and with this conclusion?

**74. Nucleus and centre of an isotope** (Petersson [95]). Let \(A\) be a unital alternative \(k\)-algebra and \(p,q \in A^\times\). Prove \(\text{Nuc}(A^{p q}) = \text{Nuc}(A) (pq)^{-1}\) and \(\text{Cent}(A^{p q}) = \text{Cent}(A) (pq)^{-1}\). (Hint. Reduce to the case of unital isotopes.)

**17. Isotropy involutions**

We have learned in [11.9] how to twist involutions of unital non-associative algebras by symmetric or skew-symmetric invertible elements in the nucleus. This procedure
is useful when the nucleus is big, e.g., for associative algebras, but distinctly less so when it is small, e.g., when it agrees with the scalar multiples of the identity element, as happens, for example, in the case of octonions (Exc. ??? below), arguably the most important class of properly alternative algebras. In the present section, we describe a way out of this impasse by introducing the notion of isotopy involution for alternative algebras that allows twisting by arbitrary symmetric or skew-symmetric invertible elements.

Throughout, we let $k$ be an arbitrary commutative ring. We begin with a simple but useful preparation.

1.7. Lemma. Let $B$ be a unital alternative $k$-algebra, $p \in B^\times$ and $\tau: B \to B^p$ a unital homomorphism or anti-homomorphism. Then $\tau$ preserves $U$-operators and arbitrary powers: $\tau \circ U_x = U_{\tau(x)} \circ \tau$ for all $x \in B$ and $\tau(x^n) = \tau(x)^n$ for all $x \in B$, $n \in \mathbb{N}$ (resp. $x \in B^\times$, $n \in \mathbb{Z}$).

Proof. By Lemma 16.10, $U$-operators and powers do not change when passing to the opposite or a unital isotope of $B$. $\square$

17.2. The concept of an isotopy involution. Let $B$ be a unital alternative algebra over $k$ and $\varepsilon = \pm$. By an isotopy involution of type $\varepsilon$ of $B$ we mean a pair $(\tau, p)$ satisfying the following conditions.

(i) $p \in B^\times$ and $\tau(p) = \varepsilon p$.
(ii) $\tau: B \to B^p$ is an anti-isomorphism.
(iii) $\tau^2 = 1_B$.

We often speak of isotopy involutions if the type is clear from the context. In explicit terms, condition (ii) is equivalent to $\tau$ being a linear bijection satisfying

$$\tau(xy) = (\tau(y)p^{-1})(p\tau(x))$$

$(x, y \in B).$ \hspace{1cm} (1)

Note that the preceding conditions are compatible in the following sense: suppose the pair $(\tau, p)$ satisfies (i), (ii). Then Lemma 17.1 implies $\tau(p^{-1}) = \varepsilon p^{-1}$, we obtain isomorphisms $\tau: B \to (B^p)^{\text{op}}$, $\tau^*: B^p \to B^p$, and functoriality 16.11 applied to the latter yields the second arrow in

$$B \xrightarrow{\tau} (B^p)^{\text{op}} = (B^{\text{op}})^{p^{-1}} \xrightarrow{\tau^*} (B^p)^{\tau(p^{-1})} = (B^p)^{p^{-1}} = B.$$  

Thus, regardless of (iii), it follows from (i), (ii) alone that $\tau^2: B \to B$ is an isomorphism, so in the presence of (i), (ii), condition (iii) makes sense.

Trivial examples of isotopy involutions are provided by the observation that the isotopy involutions of an associative algebra $B$ have the form $(\tau, p)$, where $\tau: B \to B$ is an ordinary involution and $p \in B^\times$ is symmetric or skew-symmetric relative to $\tau$. Less trivial examples may be found by consulting the following lemma, which gives a first indication of twisting in the setting of alternative algebras.
17.3. Lemma. Let \((B, \tau)\) be an alternative \(k\)-algebra with involution and suppose \(q \in B^\times\) satisfies \(\tau(q) = \varepsilon q\) for some \(\varepsilon = \pm\). Then \((\tau^q, q^3)\) with

\[
\tau^q : B \to B^3, \quad x \mapsto \tau^q(x) := q^{-1} \tau(x) q
\]

is an isotopy involution of type \(\varepsilon\) of \(B\).

Proof. By Cor. \([15,5]\) the definition of \(\tau^q\) is unambiguous, and we have \((\tau^q)^2 = 1_B\), \(\tau^q(q^3) = \varepsilon q^3\). From Exc. \([?2]\) we deduce that \(\text{Int}(q^{-1}) = L_{q^{-1}} R_q : B \to B^3\) is an isomorphism, forcing \(\tau^q := \text{Int}(q^{-1}) \circ \tau : B \to B^3\) to be an anti-isomorphism.

17.4. Homomorphisms and base change. Fix \(\varepsilon = \pm\). By an alternative \(k\)-algebra with isotopy involution of type \(\varepsilon\) we mean a triple \((B, \tau, p)\) consisting of a unital alternative \(k\)-algebra \(B\) and an isotopy involution \((\tau, p)\) of type \(\varepsilon\) of \(B\). We also speak of an alternative algebra with isotopy involution of positive (resp. negative) type if \(\varepsilon = +\) (resp. \(\varepsilon = -\)). A homomorphism \(h : (B, \tau, p) \to (B', \tau', p')\) of alternative \(k\)-algebras with isotopy involution of type \(\varepsilon\) is a unital homomorphism \(h : B \to B'\) of \(k\)-algebras that respects the isotopy involutions: \(\tau' \circ h = h \circ \tau\) and satisfies \(h(p) = \alpha p'\) for some \(\alpha \in k^\times\). In this way, we obtain the category of alternative \(k\)-algebras with isotopy involution of type \(\varepsilon\). If \((B, \tau, p)\) is an alternative \(k\)-algebra with isotopy involution of type \(\varepsilon\) over \(k\), then \((B, \tau, p)_R := (B_R, \tau_R, p_R)\) is one over \(R\), for any \(R \in k\text{-alg}\), called the scalar extension or base change of \((B, \tau, p)\) from \(k\) to \(R\). Note that \((B, \tau, 1_B)\) is an alternative algebra with isotopy involution if and only if \((B, \tau)\) is an alternative algebra with involution.

We now proceed to assemble a few elementary properties of isotopy involutions. For the time being, we fix an alternative algebra \((B, \tau, p)\) with isotopy involution of type \(\varepsilon = \pm\) over \(k\).

17.5. Lemma. The following identities hold for all \(x, y \in B\) and all \(n \in \mathbb{Z}\).

\[
\begin{align*}
\tau(x p^n) &= \varepsilon^n p^n \tau(x), \quad \tau(p^n x) = \varepsilon^n \tau(x) p^n, & (1) \quad \text{POPM} \\
\tau(\tau(x) p y) &= \varepsilon \tau(y) (p x), \quad \tau(\tau(x) p^{-1} y) = \varepsilon (\tau(y) p^{-1}) x, & (2) \quad \text{TAUTAU} \\
\tau((x y) p) &= \varepsilon p \tau(x y) = \varepsilon (p \tau(y)) \tau(x), & (3) \quad \text{TAUP} \\
\tau(p^{-1}(x y)) &= \varepsilon \tau(y) x p^{-1} = \varepsilon \tau(y) (\tau(x) p^{-1}). & (4) \quad \text{TAUPI}
\end{align*}
\]

Proof. Since \(\tau\) preserves powers by Lemma \([17,1]\) applying \([17,2]\) to \(y = p^n\) (resp. \(x = p^n\)) yields \([1]\). Using this for \(n = 1\) and \([17,2]\) again, we deduce \(\tau(\tau(x) (p y)) = (\tau(p y) \tau^{-1})(p x) = \varepsilon ((\tau(y) p) \tau^{-1})(p x) = \varepsilon \tau(y)(p x)\), hence the first relation of \([2]\); the second one follows analogously. To derive the first relation in \([3]\), one applies \([1]\) for \(n = 1\), while the second one is a consequence of the Moufang identities \([14,3]\) \([1]\) \([14,5]\) : \(p \tau(xy) = p((\tau(y) p^{-1})(p \tau(x))) = [p(\tau(y) p^{-1}) p] \tau(x) = (p \tau(y)) \tau(x)\). Relation \([4]\) follows in a similar way.

\[\text{ss.SYSP}\]
17. Symmetric elements. For $\varepsilon' = \pm$, we put
\[ \text{Sym}_{\varepsilon'}(B, \tau, p) := \{ x \in B \mid \tau(x) = \varepsilon' x \}, \] (1)
and more specifically, as in \[11.6\]
\[ \text{Sym}(B, \tau, p) := \text{Sym}_+(B, \tau, p) = \{ x \in B \mid \tau(x) = x \}, \] (2)
\[ \text{Skew}(B, \tau, p) := \text{Sym}_-(B, \tau, p) = \{ x \in B \mid \tau(x) = -x \}. \] (3)

They are both submodules of $B$, and by \[17.2\] we have $p \in \text{Sym}_{\varepsilon}(B, \tau, p)$. Applying \[17.5\] for $y = x$ yields
\[ \tau(x)(px), (\tau(x)p^{-1})x \in \text{Sym}_{\varepsilon}(B, \tau, p) \] (4)
\[ (x \in B). \]

By contrast, $\tau(x)p$ or $\tau(x)(p^{-1}x)$ will in general not belong to $\text{Sym}_{\varepsilon}(B, \tau, p)$ (see Exc. \[76\] below).

The twisting of isotopy involutions, which we now proceed to discuss, takes on a slightly different form from what we have seen in the case of ordinary involutions (Lemma \[17.3\]).

17.7. Proposition. Let $\varepsilon' = \pm$ and $q \in \text{Sym}_{\varepsilon'}(B, \tau, p)$ be invertible in $B$. Then
\[ (B, \tau, p)^q := (B^{q'}, \tau^q, p^{q'}) \] (1)
with
\[ \tau^q(x) := \varepsilon' q^{-1} \tau(qx), \quad p^q = pq \] (2)
\[ (x \in B) \]
is an alternative $k$-algebra with isotopy involution of type $\varepsilon \varepsilon'$, called the $q$-isotope of $(B, \tau, p)$, such that
\[ \tau^q(xq) = \varepsilon' \tau(x)q, \] (3)
\[ \text{Sym}_{\varepsilon'}(B^{q'}, \tau^q, p^{q'}) = q^{-1} \text{Sym}_{\varepsilon' \varepsilon'}(B, \tau, q) = \text{Sym}_{\varepsilon' \varepsilon'}(B, \tau, p)q, \] (4)
\[ ((B, \tau, p)^q)^{q'} = (B, \tau, p)^{q'} \] (5)
for all $x \in B$, $\varepsilon'' = \pm$ and all $q' \in \text{Sym}_{\varepsilon'}(B^{q'}, \tau^q, p^{q'})$ that are invertible in $B$.

Proof. Starting with \[3\], we apply Lemma \[17.1\] to obtain $\tau^q(xq) = \varepsilon' q^{-1} \tau(qx) = \varepsilon' q^{-1} \tau(U_{q}x) = \varepsilon' q^{-1} U_{\tau(q)} \tau(x) = \varepsilon' q^{-1} [q \tau(x)q]$, and \[3\] follows. Setting $x = p$, this implies $\tau^q(p^q) = \varepsilon' \tau(p)q = \varepsilon \varepsilon' p^q$, while applying $\tau^q$ to \[3\] yields $\tau^q((xq)q) = \varepsilon' \tau^q(\tau(x)q) = \tau^2(x)q = xq$, hence $\tau^2 = 1_{B^q}$. In order to establish \[1\] as an alternative $k$-algebra with isotopy involution of type $\varepsilon \varepsilon'$, it therefore suffices to show that $\tau: B^q \to (B^q)^{p^q} = B^{pq}$ is an anti-isomorphism, equivalently, that
\[ (\tau^q(y)(pq)^{-1})(pq)^{-1}) = \tau^q((xq)^{-1})(qy) \] (6)
\[ (x, y \in B). \]
In order to do so, we replace $y$ by $yq$ and apply (2), (3), (17.3), the Moufang identities and (17.2) to compute
\[
(\tau^q(y)(pq)^{-1}((pq)^q\tau^q(x))) = \left[\left((\tau(y)q)q^{-1}\right)p^{-1}\right]q^{-1} \cdot q\left[p\left(q(q^{-1}\tau(qx))\right)\right]
\]
\[
= (\tau(y)p^{-1})q^{-1} \cdot q(p\tau(qx))
\]
\[
= (\tau(y)p^{-1})q^{-1} \cdot q(p\tau(x))q
\]
\[
= (\tau(y)p^{-1})(p\tau(x))\]q
\[
= \epsilon'(\tau(y)p^{-1})(p\tau(x))\]q
\[
= \epsilon'(\tau(xy))q = \tau^q((xy)q)
\]
\[
= \tau^q((xq^{-1})(q(yq)))
\]
and (6) holds. It remains to establish (4), (5). While (4) follows immediately from (2), (3), we note in (2) that $(B'^q)^q = B''$. Also, with $p' := p^q$ it must be borne in mind that the expression $(p')^q$ has to be computed not in $B$ but in $B''$, so $(p')^q = ((pq)^{-1})(pqq) = pqq = pqq$. Moreover, by (4), $(qqq') = \epsilon'\epsilon''qq'$, so the right-hand side of (5) makes sense. And finally, (3) gives
\[
(\tau^q((xqqq'))) = (\tau^q)((xqq^{-1}(q)) = \epsilon''(\tau^q((xq)q^{-1})(q))
\]
\[
= (\epsilon'\epsilon''\tau(x)(qq')) = \tau^q((xqq'))
\]
for all $x \in B$, and the proof of (5) is complete.
\[\square\]

**Corollary.** Up to isomorphism, the alternative $k$-algebras with isotopy involution of type $\epsilon = \pm$ are precisely of the form
\[
(B, \tau, 1_B)^q = (B'', \tau^q, q),
\]
where $(B, \tau)$ is an alternative $k$-algebra with involution and $q \in B$ is invertible satisfying $\tau(q) = \epsilon q$. Moreover,
\[
\tau^q(x) = q^{-1}\tau(x)q \quad (x \in B). \tag{1}
\]

**Proof.** Let $(B', \tau', p')$ be an alternative $k$-algebra with isotopy involution and put $q := p'$. Then Prop. [17.7] implies $(B', \tau', p') = (B, \tau, 1_B)^q$, with $B := (B')^q = (B')^q$, $\tau := (\tau')^q$. In particular, $(B, \tau)$ is an alternative $k$-algebra with involution, which combines with (17.7) to yield $\tau'(x) = \tau^q(x) = \epsilon q^{-1}\tau(qx) = \epsilon q^{-1}\tau(x)\tau(q) = q^{-1}\tau(x)q$, hence (1).

**Remark.** Equation (17.8) shows that the notational conventions of Prop. [17.7] and Cor. [17.8] are compatible with the ones of Lemma [17.3].

**Exercises.**
18. Finite-dimensional alternative algebras over fields.

Our sole purpose in this short section will be to recall the basic results of the structure theory for finite-dimensional alternative algebras over an arbitrary field. Since this theory, mostly due to Zorn [128]-[130] is well documented in book form (see, e.g., Schafer [114, Chap. III]), proofs in the present account will be mostly omitted.

Throughout we let \( k \) be a commutative ring and \( F \) a field of arbitrary characteristic.

18.1. Nilpotent algebras. Let \( A \) be a non-associative algebra over \( k \). For a positive integer \( n \), we write

\[
A^n := \mathbb{Z} \text{Mon}_n(A)
\]

(1)

for the additive subgroup of \( A \) generated by all products, in some association, of \( n \) factors in \( A \). By induction on \( n \), one sees easily that

\[
A = A^1 \supseteq A^2 \supseteq \cdots \supseteq A^n \supseteq A^{n+1} \supseteq \cdots
\]

(2)

forms a descending chain of ideals in \( A \). The algebra \( A \) is said to be nilpotent if \( A^n = \{0\} \) for some integer \( n \geq 1 \), equivalently, if some positive integer \( n \) has the property that all products of \( n \) factors in \( A \), no matter how associated, are equal to zero.

18.2. The nil radical. Let \( A \) be an alternative algebra over \( k \). Since \( A \) is power-associative (Cor. 15.6), an element \( x \in A \) is nilpotent in the sense of Exc. 30 if and only if \( x^n = 0 \) for some integer \( n \geq 0 \). Recall from loc. cit. that the nil radical of \( A \), denoted by \( \text{Nil}(A) \) and defined as the sum of all nil ideals in \( A \), is a nil ideal itself, hence the biggest nil ideal in \( A \). Moreover, the nil radical of \( A/\text{Nil}(A) \) is zero.

18.3. Semi-simplicity. Let \( A \) be a finite-dimensional alternative algebra over the field \( F \). We say that \( A \) is semi-simple if \( \text{Nil}(A) = \{0\} \).
18.4. **Theorem** (Schafer [114, Thm. 3.2]). The nil radical of a finite-dimensional alternative algebra over $F$ is nilpotent.

18.5. **Theorem** (Schafer [114, Thm. 3.10]). A finite-dimensional semi-simple alternative $F$-algebra contains an identity element.

18.6. **Theorem** (Schafer [114, Thm. 3.12]). A finite-dimensional alternative algebra $A$ over $F$ is semi-simple if and only if there is a decomposition

$$A = A_1 \oplus \cdots \oplus A_r$$

of $A$ as a finite direct sum of simple ideals. In this case, the decomposition is unique up to isomorphism and up to the order of the summands.

18.7. **Theorem** (Schafer [114, Thm. 3.17]). A finite-dimensional alternative algebra over $F$ is central simple if and only if it is either isomorphic to $\text{Mat}_n(D)$ for some positive integer $n$ and some finite-dimensional central associative division algebra $D$ over $F$, or it is an octonion algebra over $F$ as defined in 22.20 below. In the former case, $n$ is unique and $D$ is unique up to isomorphism.

**18.8. Properly nilpotent elements.** Along the way towards proving the preceding structure theorems, it turns out to be convenient to take advantage of properly nilpotent elements: given an alternative algebra $A$ over $k$, an element $x \in A$ is said to be *properly nilpotent* if $xu \in A$ is nilpotent for all $u \in A$. This is equivalent to $ux \in A$ being nilpotent for all $u \in A$ since $(ux)^{n+1} = u(xu)^nx$ for all positive integers $n$, which follows from Artin’s theorem (Cor. 15.5). The most important technical results pertaining to the notion of properly nilpotent elements are as follows.

18.9. **Lemma.** Let $A$ be a unital alternative algebra of finite dimension over $F$ and suppose there are no idempotents in $A$ other than $0$ and $1_A$. Then every element of $A$ is either invertible or nilpotent. Moreover, the set of nilpotent elements in $A$ is an ideal.

**Proof.** The first assertion holds by [114, Lemma 3.5], which also shows that the set of properly nilpotent elements in $A$ is an ideal. Hence it suffices to show that every nilpotent element is properly nilpotent. Otherwise, there exist $x, y \in A$ such that $x$ is nilpotent and $xy$ is invertible. Let $n$ be the least positive integer satisfying $x^n = 0$. Then $x^{n-1}(xy) = x^ny = 0$ implies $x^{n-1} = 0$, a contradiction.

18.10. **Theorem** (Schafer [114, Thm. 3.7]). The nil radical of a finite-dimensional alternative algebra over a field agrees with the set of its properly nilpotent elements.

18.11. **Corollary** (Schafer [114, Cor. 3.8]). Let $A$ be a finite-dimensional alternative algebra over $F$ and $c \in A$ an idempotent. Then $\text{Nil}(A_n(c)) = (\text{Nil}(A)) \cap A_n(c)$ for $i = 1, 2$. 


Chapter 4
Composition algebras

We have seen in Thm. 1.7 that the algebra of Graves-Cayley octonions as defined in 1.4 carries a positive definite real quadratic form that permits composition. In the present chapter we will study a class of non-associative algebras over an arbitrary commutative ring for which such a property is characteristic. Many results we derived for the Graves-Cayley octonions in the first chapter will resurface here under far more general circumstances, and with much more natural proofs attached.

19. Conic algebras

By (1.5.10), every element \( x \) in the algebra of Graves-Cayley octonions satisfies a quadratic equation which is universal in the sense that its coefficients depend “algebraically” on \( x \). This innocuous but useful property gives rise to the notion of a conic algebra that will be studied in the present section.

The term “conic algebra” made its first appearance in a paper by Loos [72] and derives its justification from the fact that conic algebras, just like ordinary conics as curves in the (affine or projective) plane, are intimately tied up with quadratic equations; for a more sophisticated motivation of this term, see 19.3 below. In deriving the main properties of conic algebras, we adhere rather closely to the treatment of McCrimmon [82], who calls them degree 2 algebras, while other authors speak of quadratic algebras in this context. By contrast, the term “quadratic algebra” will be used here in a much more restrictive sense, as in Knus [58, I, (1.3.6)].

Throughout we let \( k \) be an arbitrary commutative ring.

19.1. The concept of a conic algebra. By a conic algebra over \( k \) we mean a unital \( k \)-algebra \( C \) together with a quadratic form \( n_C: C \to k \) such that

\[
    n_C(1_C) = 1, \quad x^2 - n_C(1_C, x) x + n_C(x) 1_C = 0 \quad (x \in C). \tag{1}
\]

We call \( n_C \) the norm of \( C \). Most of the time, we will just speak of a conic algebra \( C \) over \( k \), its norm \( n_C \) being understood.

Let \( C \) be a conic algebra over \( k \). Viewing \( C \) merely as a \( k \)-module, \((C, n_C, 1_C)\) is a pointed quadratic module over \( k \) with norm \( n_C \), base point \( 1_C \) and trace \( t_C \) given by \( t_C(x) = n_C(1_C, x) \) for all \( x \in C \), in the present context called the trace of \( C \).

\footnote{It follows from Exc. 86 below that the algebra \( C \) and condition (1) do not determine the quadratic form \( n_C \) uniquely. In spite of this, we feel justified in phrasing our definition, as well as similar ones later on, in this slightly informal manner because it is convenient and there is no danger of confusion.}
The linear map $t_C : C \to k$ defined by $t_C(x) = n_C(1_C, x)$ for $x \in C$ is called the (linear) trace of $C$, while we refer to $t_C : C \to C$, $x \mapsto \bar{x} := t_C(x)1_C - x$ (which is linear as well and of period two) as the conjugation of $C$. We also denote by $t_C$ the bilinear trace of $C$, i.e., the bilinear form $C \times C \to k$, $(x,y) \mapsto t_C(xy)$, which in general is not symmetric. Given a submodule $M \subseteq C$, we always write $M^\perp = \{x \in C \mid n_C(x,M) = \{0\}\}$ for the orthogonal complement of $M$ in $C$ relative to the polarized norm.

Let $C'$ be another conic algebra over $k$. By a homomorphism $h : C \to C'$ of conic algebras we mean a unital $k$-algebra homomorphism which preserves norms in the sense that $n_C \circ h = n_{C'}$. It is clear that homomorphisms of conic algebras also preserve (linear as well as bilinear) traces and conjugations. If $B \subseteq C$ is a unital subalgebra, it may and always will be regarded as a conic algebra in its own right by defining its norm $n_B := n_C|_B$ as the restriction of the norm of $C$ to $B$; in this way, the inclusion $B \hookrightarrow C$ becomes a homomorphism of conic algebras.

Conic algebras are clearly invariant under base change. If $C$ is a conic algebra over $k$, then so is $C^\text{op}$, with the same norm, linear trace and conjugation as $C$, while the bilinear trace changes in the obvious way to $t_{C^\text{op}}(x,y) := t_C(y,x)$.

19.2. Examples of conic algebras.
Examples of conic algebras exist in abundance. Aside from the Graves-Cayley octonions, the Hamiltonian quaternions and, more generally, any unital subalgebra of $\mathcal{O}$, the following examples seem to be particularly noteworthy.

(a) The base ring $k$ itself, with norm $n_k : k \to k$ given by the squaring: $n_k(\alpha) = \alpha^2$ for $\alpha \in k$. We have $t_k(\alpha) = 2\alpha$, and the conjugation of $k$ is the identity.

(b) $R = k \oplus k$ (as a direct sum of ideals), with norm $n_R : R \to k$ given by $n_R(\alpha \oplus \beta) = \alpha\beta$ for $\alpha, \beta \in k$. We have $t_R(\alpha \oplus \beta) = \alpha + \beta$, and the conjugation of $R$ is the “switch”: $\alpha \oplus \beta = \beta \oplus \alpha$. In particular, the quadratic module $(R, n_R)$ is the split hyperbolic plane $\mathcal{D}(12.17)$.

(c) $R = k[\epsilon], \epsilon^2 = 0$, the $k$-algebra of dual numbers, with norm, trace, conjugation respectively given by $n_R(\alpha 1_R + \beta \epsilon) = \alpha^2$, $t_R(\alpha 1_R + \beta \epsilon) = 2\alpha$, $\alpha 1_R + \beta \epsilon = \alpha 1_R - \beta \epsilon$ for $\alpha, \beta \in k$.

(d) $R = K$, where $k$ is a field and $K/k$ is a quadratic field extension. Then $R$ is a conic $k$-algebra, with $n_R = N_{K/k}$ (resp. $t_R = T_{K/k}$) the field norm (resp. the field trace) of $K/k$. Moreover, $t_R$ is the non-trivial Galois automorphism of $K/k$ if $K/k$ is separable, and the identity otherwise.

19.3. Motivation.
Let $k$ be a field and $X \subseteq \mathbb{P}^3_k$ a smooth conic in the plane, given by a separable quadratic form in three variables. Then one checks easily that the scheme-theoretic intersection (cf. [36] I, 4.4) of $X$ with appropriate lines in $\mathbb{P}^3_k$ has the form $\text{Spec}(R)$ (viewed as an affine scheme), where $R$ is one of the algebras listed in 19.2(b),(c),(d) above. This gives another motivation of the term “conic algebra”.
19.4. Quadratic algebras

In analogy to Knus [58 I, (1.3.6)], an algebra $R$ over $k$ is said to be quadratic if it contains an identity element and is projective of rank 2 as a $k$-module. In this case, we claim that $1_R \in R$ is unimodular, $R$ is commutative associative and its conjugation is an involution, i.e., a $k$-automorphism of period two. As to the first part, we note that $R(p)$, for any $p \in \text{Spec}(k)$, is a unital two-dimensional $k(p)$-algebra, forcing $1_R(p) \neq 0$. Hence $1_R$ is unimodular by Lemma [10.13] Since the remaining assertions are local on $k$, we may assume that $k$ is a local ring, making $R$ a free $k$-module of rank 2. Extending $1_R$ to a basis of $R$, which we are allowed to do by unimodularity, the commutative and the associative law for the multiplication of $R$ trivially hold, as does the property of the conjugation to be a $k$-automorphism of period two. Thus our assertion is proved.

It now follows from the Hamilton-Cayley theorem that a quadratic $k$-algebra $R$ is conic, with norm and trace given by

$$n_R(x) = \det(L_x), \quad t_R(x) = \text{tr}(L_x) \quad (x \in R). \tag{1}$$

19.5. Basic identities. Let $C$ be a conic algebra over $k$. The following identities either hold by definition or are straightforward to check.

$$x^2 = t_C(x)x - n_C(x)1_C, \tag{1}$$
$$t_C(x) = n_C(1_C, x), \tag{2}$$
$$n_C(1_C) = 1, \quad t_C(1_C) = 2, \tag{3}$$
$$\bar{x} = t_C(x)1_C - x, \quad \bar{1}_C = 1_C, \quad \bar{x} = x, \tag{4}$$
$$x \circ y = xy + yx = t_C(x)y + t_C(y)x - n_C(x, y)1_C, \tag{5}$$
$$x\bar{x} = n_C(x)1_C = \bar{x}x, \quad x + \bar{x} = t_C(x)1_C, \tag{6}$$
$$n_C(\bar{x}) = n_C(x), \quad t_C(\bar{x}) = t_C(x), \tag{7}$$
$$t_C(x^2) = t_C(x)^2 - 2n_C(x), \tag{8}$$
$$t_C(x \circ y) = t_C(x, y) + t_C(y, x) = 2[t_C(x)t_C(y) - n_C(x, y)], \tag{9}$$
$$n_C(x, y) = t_C(x)t_C(y) - n_C(x, y), \tag{10}$$
$$\bar{xy} - y\bar{x} = (t_C(x, y) - n_C(x, y))1_C. \tag{11}$$

By (1) and [8.7] $k[x]$ agrees with the submodule of $C$ spanned by $1_C$ and $x$; it is a commutative associative subalgebra. In particular, conic algebras are power-associative.

Before we can proceed, we require two short digressions.

19.6. Unimodular elements revisited. For several of our subsequent results it will be important to know that $1_C \in C$ is unimodular. While this is not always true, it does hold automatically if the linear trace of $C$ is surjective, since this is equivalent to $t_C(x) = 1$ for some $x \in C$ and so the linear form $\lambda : C \to k, y \mapsto t_C(xy)$, satisfies $\lambda(1_C) = 1$.

---

2 I am indebted to Erhard Neher, who discovered a faulty argument in the original presentation of this subsection.
For example, if $\frac{1}{2} \in k$, then $t_C(x) = 1$ for $x = \frac{1}{2} \cdot 1_C$ and $1_C$ is unimodular. Moreover, we have

$$C = k1_C \oplus C^0$$

as a direct sum of submodules, where

$$C^0 = \text{Ker}(t_C) = \{x \in C \mid \bar{x} = -x\},$$

and

$$H(C, t_C) = k1_C.$$

Another important condition that ensures unimodularity of $1_C$ will be stated separately.

**19.7. Proposition.** Let $C$ be a conic algebra over $k$ which is projective as a $k$-module. Then $1_C \in C$ is unimodular and $C_p \neq \{0\}$ for all prime ideals $p \subseteq k$.

**Proof.** The first part follows immediately from Lemma 12.14 (applied to the pointed quadratic module $(C, n_C, 1_C)$), which in turn implies the second, by Lemma 10.13.

**19.8. Trivial conjugation.** A conic algebra $C$ over $k$ is said to have trivial conjugation if $\iota_C = 1_C$. Having trivial conjugation is a rather exotic phenomenon. For example, if $\frac{1}{2} \in k$, then (19.6.109), (19.6.2) show that $C$ does not have trivial conjugation unless $C \cong k$. More generally, the same conclusion holds if $t_C$ is surjective (Exc. 85). On the other hand, if $2 = 0$ in $k$ and $t_C = 0$ (e.g., if $k$ is a field and $C$ an inseparable quadratic field extension of $k$), then $C$ does have trivial conjugation.

In subsequent applications, conic algebras which are flexible (i.e., satisfy the identity $(xy)x = x(yx)$) or whose conjugation is an (algebra) involution play an important role. These two properties will now be related to one another in various ways.

**19.9. Proposition.** Let $C$ be a conic algebra over $k$.

(a) The conjugation of $C$ is an involution if and only if

$$t_C(x, y) - n_C(x, \bar{y}) \in \text{Ann}(C)$$

for all $x, y \in C$.

(b) $C$ is flexible if and only if

$$(t_C(x, y) - n_C(x, \bar{y}))x = (n_C(x, xy) - t_C(y)n_C(x))1_C$$

for all $x, y \in C$.

**Proof.** (a) follows immediately from (19.5.11). In (b) one simply notes $(xy)x - x(yx) = (xy) \circ x - x(x \circ y)$ and expands the right-hand side using (19.5.5), (19.5.1).
19.10. Corollary. Let \( C \) be a conic \( k \)-algebra whose conjugation is an involution. Then \( C \) is flexible if and only if \( n_C(x, xy) - t_C(y)n_C(x) \in \text{Ann}(C) \) for all \( x, y \in C \).

19.11. Proposition. The following (collections of) identities are equivalent in any conic algebra \( C \) over \( k \):

\[
\begin{align*}
n_C(x, yx) &= t_C(y)n_C(x), \quad (1) \\
n_C(x, xy) &= t_C(y)n_C(x), \quad (2) \\
n_C(xy, z) &= n_C(x, z\bar{y}), \quad (3) \\
n_C(xy, z) &= n_C(y, x\bar{z}), \quad (4) \\
t_C(x, y) &= n_C(x, \bar{y}), \quad t_C(xy, z) = t_C(x, yz). \quad (5)
\end{align*}
\]

Proof. Since (2) (resp. (4)) is (1) (resp. (3)) in \( C^\text{op} \), the equivalence of (1)–(5) will follow once we have established the following implications.

1. \( \iff \) 2. Combine (19.5.2) with (19.5.5) to conclude \( n_C(x, x \circ y) = 2t_C(y)n_C(x) \).
2. \( \Rightarrow \) 3. Linearize (2) and apply (19.5.4).
3. \( \Rightarrow \) 4. Put \( z = x \) in (4) and apply (19.5.6).
4. \( \Rightarrow \) 5. Put \( z = 1_C \) in (5) and apply (19.5.2) to deduce the first two equations of (5). But then, by Prop. 19.9 (a), \( t_C \) is an involution of \( C \), yielding the final statement of the proposition, while the last equation of (5) follows by a straightforward computation.

5. \( \Rightarrow \) 1. By Prop. 19.9 (a) and the first equation of (5), \( t_C \) is an involution of \( C \), which implies \( n_C(x, yx) = t_C(x, \bar{x}y) = t_C(x\bar{x}, \bar{y}) \) by (5), and (1) follows from (19.5.6) (19.5.7).

19.12. Norm-associative conic algebras. A conic algebra satisfying one (hence all) of the identities (19.11.1) – (19.11.5) is said to be norm-associative. If \( C \) is a norm-associative conic algebra, then (19.11.5) combined with (19.5.10) shows that the bilinear trace of \( C \) is an associative bilinear form, so

\[
t_C(xy) = t_C(yx), \quad t_C((xy)z) = t_C(x(yz)) = t_C(xyz).
\]

Norm-associativity is clearly invariant under scalar extensions. Also, if \( C \) is a norm-associative conic algebra, then so is \( C^\text{op} \).

19.13. Proposition. Let \( C \) be a norm-associative conic algebra over \( k \). Then \( C \) is flexible and its conjugation is an involution, called the canonical involution of \( C \). Conversely, suppose \( C \) is a flexible conic algebra and projective as a \( k \)-module. Then \( C \) is norm-associative.

Proof. If \( C \) is a norm-associative conic \( k \)-algebra, then by (19.11.5) and (19.11.2) combined with Prop. 19.9 (a), \( C \) is flexible and its conjugation is an involution. Conversely, suppose \( C \) is flexible and projective as a \( k \)-module. Given \( y \in C \), it
suffices to show

\[ t_C(x, y) = n_C(x, \bar{y}) \quad (x \in C) \]  

(1)

since \[ 19.9.1 \] and unimodularity of \( 1_C \) (Prop. \[ 19.7 \]) then imply \( 19.11.2 \). To establish \( 1 \), we may assume that \( k \) is a local ring and extend \( e_0 := 1_C \) to a basis \( (e_i) \) of the \( k \)-module \( C \). Then \( 1 \) holds for \( x = e_0 \) by \[ 19.5.7 \] and for \( x = e_i, i \neq 0 \), by \[ 19.9.1 \], hence on all of \( C \) by linearity.

19.14. Corollary. For a faithful conic algebra over \( k \) to be norm-associative it is necessary and sufficient that it be flexible and its conjugation be an involution.

Proof. By Prop. \[ 19.13 \] the condition is clearly necessary. Conversely, suppose \( C \) is a flexible faithful conic \( k \)-algebra whose conjugation is an involution. Combining Prop \[ 19.9 \] with faithfulness, we see that \( 19.11.2 \) holds, so \( C \) is norm-associative.

19.15. Proposition. Let \( C \) be a conic algebra over \( k \). If \( C \) is projective as a \( k \)-module, then the norm of \( C \) is uniquely determined by the algebra structure of \( C \).

Proof. Let \( n : C \to k \) be any quadratic form making \( C \) a conic algebra and write \( t \) for the corresponding linear trace. Then \( \lambda := t_C - t \) (resp. \( q := n_C - n \)) is a linear (resp. a quadratic) form on \( C \), and \( 19.5.1 \) yields

\[ \lambda(x) = q(x)1_C, \]

for all \( x \in C \). We have to prove \( \lambda = q = 0 \). Since \( 1_C \in C \) is unimodular by Prop. \[ 19.7 \] it suffices to show \( \lambda = 0 \). This can be checked locally, so we may assume that \( k \) is a local ring, allowing us to extend \( e_0 := 1_C \) to a basis \( (e_i) \) of \( C \) as a \( k \)-module. But \( \lambda(e_0) = 0 \) by \[ 19.5.1 \]. Hence it remains to show \( \lambda(e_i) = 0 \) for all \( i \neq 0 \), which follows immediately from \( 1 \).

Exercises.

77. Let \( C \) be a conic algebra over \( k \). Prove

(a) \( n_C(zy) = n_C(y)n_C(z) \) for all \( y, z \in k[x] \).
(b) \( x \) is invertible in (the commutative associative \( k \)-algebra) \( k[x] \) if and only if \( n_C(x) \) is a unit in \( k \), in which case

\[ x^{-1} = n(x)^{-1}x. \]

(c) \( x \) is a nilpotent element of \( C \) (Exc. \[ 30 \]) if and only if \( t_C(x) \) and \( n_C(x) \) are nilpotent elements of \( k \).

78. Let \( C, C' \) be conic \( k \)-algebras and suppose \( C \) is projective as \( k \)-modules. Prove that every injective homomorphism \( \varphi : C \to C' \) of unital \( k \)-algebras is, in fact, one of conic algebras, i.e., it preserves norms (hence traces and conjugations as well). Does this conclusion continue to hold without the hypothesis of \( \varphi \) being injective?

79. Co-ordinates for conic algebras (Loos \[ 72 \]). Let \( k \) be a commutative ring, \( X \) a \( k \)-module, \( e \in X \) a unimodular element and \( \lambda : X \to k \) a linear form such that \( \lambda(e) = 1 \). Putting \( M_k := \text{Ker}(\lambda) \), we then have \( X = ke \oplus M_k \) as a direct sum of submodules.
Let \((T, B, K)\) be a conic co-ordinates system relative to \((X, e, \lambda)\) in the sense that \(T: M_k \to k\) is a linear form, \(B: M_2 \times M_2 \to k\) is a (possibly non-symmetric) bilinear form and \(K: M_2 \times M_2 \to M_2, \quad (x, y) \mapsto x \times y,\)
is an alternating bilinear map. Define a \(k\)-algebra structure \(C := \text{Con}(T, B, K) = C_{X, e, \lambda}(T, B, K)\) on \(X\) by the multiplication
\[(\alpha e + x)(\beta e + y) := (\alpha \beta - B(x, y))e + ((\alpha + T(x))y + \beta x - x \times y)\]
for \(\alpha, \beta \in k, x, y \in M_2\). Show that \(C\) is a conic \(k\)-algebra with identity element \(e\) and norm \(n_C: C \to k\) given by
\[n_C(\alpha e + x) := \alpha^2 + \alpha T(x) + B(x, x)\]
for \(\alpha \in k\) and \(x \in M_2\).

Conversely, suppose \(C\) is a conic \(k\)-algebra with underlying \(k\)-module \(X\) and identity element \(1_C = e\). Show that \((T_C, B_C, K_C)\), where \(T = T_C: M_k \to k, B = B_C: M_2 \times M_2 \to k\) and \(K = K_C: M_2 \times M_2 \to M_2, (x, y) \mapsto x \times y\) are defined by
\[T(x) := t_C(x), \quad B(x, y) := -\lambda(x), \quad x \times y := t_C(x)y - xy + \lambda(y) \quad (x, y \in M_2),\]
is a conic co-ordinate system for \((X, e, \lambda)\). Show further that the assignments \((T, B, K) \mapsto \text{Con}(T, B, K)\) and \(C \mapsto (T_C, B_C, K_C)\) define inverse bijections between the set of conic co-ordinate systems for \((X, e, \lambda)\) and the set of conic \(k\)-algebras with underlying \(k\)-module \(X\) and identity element \(e\).

**Remarks.** (a) It is sometimes convenient to define conic co-ordinate systems on a \(k\)-module that is independent of the choice of \(\lambda\), namely, on \(X/k e\). This point of view, systematically adopted by Loos [22], turns out to be particularly useful when analyzing the question of how conic co-ordinate systems change with \(\lambda\).

(b) Let \(C\) be a conic \(k\)-algebra, \(X = C\) as a \(k\)-module and \(e := 1_C\). If \(2 \in k\) is a unit, then conic co-ordinate systems may be taken relative to \((X, e, \lambda)\) with \(\lambda := 1/4,\) in which case the conic co-ordinate system corresponding to \(C\) is already in Osborn [21] Thm. 1.

**pr.CONFIELD**

80. (Dickson [23]) Let \(k\) be a field of characteristic not 2 and \(C\) a unital algebra over \(k\). Show that \(C\) is conic if and only if \(1_C, x, x^2\) are linearly dependent over \(k\) for all \(x \in C\). (Hint: If this condition is fulfilled, linearize the expression \(1_C \times x \times x^2 \in M^3\) to show that 0 and the elements \(u \in C - k1_C\) satisfying \(u^2 = k1_C\) form a vector subspace of \(C\).)

**pr.DICON**

81. The Dickson condition Generalize Exc. 80 in the following way: let \(C\) be a unital algebra over \(k\) which is either free or finitely generated projective as a \(k\)-module and whose identity element is unimodular. Show that there exists a quadratic form \(n_C: C \to k\) making \(C\) a conic \(k\)-algebra if and only if \(C\) satisfies the Dickson condition: For all \(R \in k\text{-alg}\) and all \(x \in C_R\), the element \(x^2 \in C_R\) is an \(R\)-linear combination of \(x\) and \(1_C\).

**pr.IDEMP**

82. Elementary idempotents. (a) Let \(C\) be a conic \(k\)-algebra. Show that, if \(k \neq \{0\}\) is connected (so 0, 1 are the only idempotents of \(k\), equivalently by Exc. 41 the topological space \(\text{Spec}(k)\) is connected), an element \(e \in C\) is an idempotent \(\neq 0, 1_C\) if and only if \(n_C(e) = 0\) and \(t_C(e) = 1\). Conclude that, for any commutative ring \(k\) and any element \(e \in C\), the following conditions are equivalent.

(i) \(e\) is an idempotent satisfying \(e^2 = 1_C\) for all \(R \in k\text{-alg}, R \neq \{0\}\).

(ii) \(e\) is an idempotent satisfying \(e^2 = 0, 1_C\) for all prime ideals \(p \subseteq k\).

(iii) \(n_C(e) = 0, \quad t_C(e) = 1\).

(iv) \(e\) is an idempotent and the elements \(e, 1_C - e\) are unimodular.
If these conditions are fulfilled, we call $c$ an *elementary* idempotent of $C$.

**pr.LILID**  
Let $C$ be a conic $k$-algebra and suppose $I \subseteq k$ is a nil ideal. Write $\alpha \mapsto \bar{\alpha}$, $x \mapsto \bar{x}$ for the canonical projection $k \to \bar{k} := k/I$, 

$$C \to \bar{C} := C \otimes \bar{k} = C/I,$$

respectively, and show that any elementary idempotent $c' \in \bar{C}$ can be lifted to an elementary idempotent $c \in C$ satisfying $\bar{c} = c'$.

**pr.DECID**  
Let $C$ be a conic algebra over $k$. Prove for $c \in C$ that the following conditions are equivalent.

(i) $c$ is an idempotent in $C$.
(ii) There exists a complete orthogonal system $(\epsilon^{(0)}, \epsilon^{(1)}, \epsilon^{(2)})$ of idempotents in $k$, giving rise to decompositions 

$$k = k^{(0)} \oplus k^{(1)} \oplus k^{(2)}, \quad C = C^{(0)} \oplus C^{(1)} \oplus C^{(2)}$$

as direct sums of ideals, where $k^{(i)} = ke^{(i)}$ and $C^{(i)} = e^{(i)}C = Cl_i$ as a conic algebra over $k^{(i)}$ for $i = 0, 1, 2$, such that 

$$c = 0 \oplus c^{(1)} \oplus 1c^{(2)},$$

where $c^{(1)}$ is an elementary idempotent of $C^{(1)}$.

In this case, the idempotents $\epsilon^{(i)}$, $i = 0, 1, 2$, in (ii) are unique and given by 

$$\epsilon^{(0)} := (1 - nc(c))(1 - tc(c)), \quad \epsilon^{(1)} := (1 - nc(c))tc(c), \quad \epsilon^{(2)} := nc(c).$$

**pr.TRICO**  
Let $C$ be a conic $k$-algebra that is faithful as a $k$-module and whose linear trace is surjective. Show that $C$ has trivial conjugation if and only if $C \cong k$.

### 20. Conic alternative algebras

In §23 we have defined the euclidean Albert algebra as a commutative non-associative real algebra that lives on the $3 \times 3$ hermitian matrices with entries in the Graves-Cayley octonions. As we will show in due course, this important construction can be generalized to arbitrary conic alternative algebras over commutative rings once a peculiar additional hypothesis has been inserted. The elementary properties of conic alternative algebras needed to carry out this generalization will be assembled in the present section. Throughout we let $k$ be an arbitrary commutative ring.

We begin by identifying the “peculiar additional hypothesis” alluded to above as follows.

#### 20.1. Multiplicative conic algebras

A conic algebra $C$ over $k$ is said to be *multiplicative* if its norm permits composition:

$$nc(xy) = nc(x)nc(y) \quad (x, y \in C)$$

Linearizing this identity repeatedly, we conclude that multiplicative conic algebras also satisfy the relations
for all \(x, x_1, x_2, y, y_1, y_2 \in C\). We conclude from this that multiplicative conic algebras are stable under base change and that, if \(C\) is a multiplicative conic algebra, then so is \(C^{op}\).

Putting \(y_1 := 1_C\), \(y_2 := y\) in (3), we see that multiplicative conic algebras satisfy the identity (19.11.3). Therefore Prop. [19.13] immediately implies the first part of the following observation, while the second part is a consequence of (19.4.1).

### 20.2. Proposition

(a) Multiplicative conic algebras are norm-associative. In particular, they are flexible, and their conjugation is an involution.

(b) Quadratic algebras are multiplicative.

### 20.3. Identities in conic alternative algebras

Let \(C\) be a conic alternative algebra over \(k\). Combining the left and right alternative laws, \(x(xy) = x^2y\) and \((yx)x = xy^2\), with (19.5.1), (19.5.2), we deduce Kirmse’s identities [55, p. 67]

\[
x(\bar{y}x) = n_C(x)y = (yx)x.
\]

We can also derive a formula for the \(U\)-operator,

\[
U_{xy} = xyyx = n_C(x, y)x - n_C(x)y,
\]

which follows by using (19.5.1), (19.5.5), (19.5.4) to manipulate the expression

\[
xyx = (x \circ y)x - yx^2,
\]

see Exc. 3(c) in the special case \(k = \mathbb{R}, C = \mathbb{R}\). Applying the norm to the right-hand side of (2) and expanding, we conclude

\[
n_C(U_{xy}) = n_C(xyyx) = n_C(x)^2n_C(y).
\]

In view of this, one might be tempted to conjecture that conic alternative algebras are multiplicative. But, according to Exc. 86 below, this is not so. Fortunately, however, (3) is strong enough to characterize invertibility in conic alternative algebras.

### 20.4. Proposition

Let \(C\) be a conic alternative algebra over \(k\). An element \(x \in C\) is invertible in \(C\) if and only if \(n_C(x) \in k\) is invertible in \(k\). In this case, \(x^{-1} = n_C(x)^{-1}\bar{x}\) and \(n_C(x^{-1}) = n_C(x)^{-1}\).

**Proof.** If \(n_C(x) \in k^\times\), then Kirmse’s identities (20.3.1) show that \(y := n_C(x)^{-1}\bar{x}\) satisfies \(xy = 1_C = yx\), forcing \(x \in C^\times\) and \(y = x^{-1}\) by Prop. [14.6]. Conversely, suppose \(x\) is invertible in \(C\). Then \(U_xx^{-2} = 1_C\), and (20.3.2) yields \(1 = n_C(x^2)n_C(x^{-2})\), hence \(n_C(x) \in k^\times\). The final formula follows from the fact that the conjugation of \(C\) leaves its norm invariant.
While it is not true general that conic alternative algebras are multiplicative, this implication does hold under natural conditions on the module structure.

20.5. Proposition. Let $C$ be a conic alternative algebra over $k$ which is projective as a $k$-module. Then $C$ is multiplicative.

Proof. As an alternative algebra, $C$ is flexible, whence Prop. [19.13] implies that $C$ is norm-associative. In particular, the conjugation of $C$ is an involution. Let $x,y \in C$. By Artin’s Theorem (Cor. [15.5]), the unital subalgebra of $C$ generated by $x,y$ is associative. Moreover, by [19.5.4], it contains $\bar{x}$ and $\bar{y}$. Hence [19.5.6] yields
\[
n_C(xy)I_C = xy\bar{x}y = n_C(y)x\bar{x} = n_C(x)y\bar{C}(y)1_C,
\]
and since $1_C$ is unimodular, $C$ is indeed multiplicative. \qed

Exercises.

86. (McCrimmon [82]) The following exercise will produce an example of an algebra that supports many different conic algebra structures, some of which are multiplicative (resp. norm-associative), while others are not.

Let $k = k_0[\epsilon]$, $\epsilon^2 = 0$, be the algebra of dual numbers over a commutative ring $k_0$, and view $k_0$ as a $k$-algebra via the natural map $k \to k_0$, $\epsilon \mapsto 0$, the corresponding module action $k \times k_0 \to k_0$ being indicated by $(\alpha, \alpha_0) \mapsto \alpha \cdot \alpha_0$. In particular, (column) 3-space $k_0^3$ becomes a $k$-module in this way. In fact, it becomes a $k$-algebra under the multiplication
\[
\begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\alpha_3
\end{pmatrix}
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\beta_3
\end{pmatrix}
:=
\begin{pmatrix}
0 \\
0 \\
0
\end{pmatrix}
+ \left(\begin{array}{c}
\alpha_1 \beta_3 \\
\alpha_2 \beta_3 \\
\alpha_3 \beta_3
\end{array}\right)
\tag{1}
\]

Furthermore, let
\[
z = \begin{pmatrix}
\delta_1 \\
\delta_2 \\
\delta_3
\end{pmatrix}
\in k_0^3
\]
be arbitrary. Now consider the $k$-algebra $C$ defined on the $k$-module $k \oplus k_0^3$ by the multiplication
\[
(\alpha \oplus u_1)(\alpha_2 \oplus u_2) := \alpha_1 \alpha_2 + (\alpha_1 \cdot u_2 + \alpha_2 \cdot u_1 + [u_1, u_2])
\]
for $\alpha, \alpha_2 \in k, u_1, u_2 \in k_0^3$, $i = 1, 2$, where $[u_1, u_2]$ is the commutator belonging to the $k$-algebra structure of $k_0^3$, just defined, and let $n_C : C \to k$ be given by
\[
n_C(\alpha \oplus u) := \alpha^2 + (\alpha, (\epsilon \cdot u)) \epsilon
\]
for $\alpha \in k, u \in k_0^3$. Then show that $C$ is an associative conic $k$-algebra with norm $n_C := n_C$, and that the following conditions are equivalent.

(i) $C$ is multiplicative.
(ii) $C$ is norm-associative.
(iii) The conjugation of $C$ is an involution.
(iv) $\delta_3 = 0$.

87. Let $C$ be a multiplicative conic algebra over $k$. Show that its nil radical has the form
\[
\text{Nil}(C) = \{ x \in C | n_C(x), n_C(x, y) \in \text{Nil}(k) \text{ for all } y \in C \}.
\]
88. Artin’s theorem for conic alternative algebras. Let $C$ be a conic alternative $k$-algebra that is unitally generated by two elements $x, y \in C$. Show that $C$ is spanned by $1_C, x, y, xy$ as a $k$-module. Conclude without recourse to Artin’s theorem (Cor. 15.5) that $C$ is associative.

89. Norms of associators. (Garibaldi-Petersson [33]) Let $C$ be a multiplicative conic alternative algebra over $k$. Prove

\[
 n_C([x_1, x_2, x_3]) = 4n_C(x_1)n_C(x_2)n_C(x_3) - \sum t_C(x_j)^2 n_C(x_j)
 + \sum t_C(x_j, x_i) n_C(x_j) n_C(x_i) - t_C(x_1 x_2) t_C(x_2 x_3) t_C(x_3 x_1)
 + t_C(x_1 x_2 x_3) t_C(x_2 x_3 x_1)
\]

for all $x_1, x_2, x_3 \in C$, where both summations on the right are to be taken over the cyclic permutations $(ijl)$ of $(123)$.

90. Isotopes of conic alternative algebras. Let $C$ be a conic alternative $k$-algebra. Prove for $p, q \in C^k$ that $C(p, q)$ is again a conic alternative $k$-algebra with norm $n_{C(p, q)} = n_C(pq)n_C$. Moreover, trace and conjugation of $C(p, q)$ are given by

\[
 t_{C(p, q)}(x) = n_C(pq, x), \quad \tau_{C(p, q)}(x) = \tau(pq)^{-1}pq \tau pq \quad (x \in C).
\]

Show further that, if in addition, $C$ is multiplicative, then so is $C(p, q)$.

91. Let $C$ be a multiplicative conic alternative algebra over $k$ and suppose $q \in C^k$ has trace zero. Show that $(C, \tau, q)$ with $\tau: C \to C$ defined by $\tau(x) := q^{-1}xq$ for $x \in C$ is an alternative algebra with isotropy involution of negative type over $k$ and describe the pointed alternative $k$-algebra with involution corresponding to $(C, \tau, q)$ via Exc. 75

### 21. The Cayley-Dickson construction

The only example we have encountered so far of an alternative algebra which is not associative is the real algebra of Graves Cayley octonions. The Cayley Dickson construction will provide us with a tool to accomplish the same over any commutative ring. Moreover, it will play a crucial role in the structure theory of composition algebras over fields later on.

Throughout this section, we fix an arbitrary commutative ring $k$. Our first aim will be to present what might be called an internal version of the Cayley-Dickson construction.

21.1. Proposition. (Internal Cayley-Dickson construction) Let $C$ be a multiplicative conic alternative algebra over $k$ and $B \subseteq C$ a unital subalgebra. If $l \in C$ is perpendicular to $B$ relative to $Dn_C$, then $B + Bl \subseteq C$ is the subalgebra of $C$ generated by $B$ and $l$. Moreover, setting $\mu := -n_C(l)$, the identities
\[ u(vl) = (vu)l, \quad (vl)u = (v\bar{u})l, \quad (ul)(vl) = \mu \bar{v}u, \]

\[ n_C(u + vl) = n_C(u) - \mu n_C(v), \]

\[ t_C(u + vl) = t_C(u), \quad \bar{u} + vl = \bar{u} - vl \]

hold for all \( u, v \in B \), and

\[ Bl = lB \subseteq B^\perp. \]

**Proof.** The first assertion follows from (1)–(3), so it will be enough to establish (1)–(7). Since \( l \) is orthogonal to \( B \) and, in particular, has trace zero, (19.5.5) implies

\[ u \circ l = t_C(u)l, \]

hence \( lu = t_C(ul)l - ul \), and we have (2) in the special case \( v := 1_C \). Combining this with the linearized left alternative law (14.2.1) and (8), we conclude \( u(vl) = u(lv) = (u \circ l)v - l(u\bar{v}) = t_C(u)l\bar{v} - l(u\bar{v}) = l(\bar{u}v) = (vu)l \), since \( t_C \) is an involution by Prop. 20.2(a). Thus (1) holds. Reading (1) in \( C^{op} \) and invoking (5) once more gives (2) in full generality. In order to establish (3), we combine the middle Moufang identity (14.3.3) with (20.3.2) to conclude \( (ul)(vl) = (lul)(vl) = l(\bar{u}v)l = n_C(l, \bar{v}u)l - n_C(l)v\bar{u} = \mu \bar{v}u \), as claimed. Turning to (4), we use (19.11.4) to expand the left-hand side and obtain \( n_C(u + vl) = n_C(u) + n_C(u,vl) + n_C(v)n_C(l) = n_C(u + n_C(\bar{v}u,l) - \mu n_C(v) = n_C(u) - \mu n_C(v) \), and the proof of (3) is complete. It is now straightforward to verify (4) and (5). Finally, turning to (6), we have \( Bl = lB \) by (2) for \( v = 1_B \) and note that \( C \) is norm-associative by Prop. 20.2(a). Hence (19.11.4) yields \( n_C(u,vl) = n_C(\bar{v}u,l) = 0 \) for all \( u,v \in B \), which implies \( Bl \subseteq B^\perp \) and (6) holds. \[ \square \]

**Remark.** The above sum \( B + Bl \) of \( k \)-submodules of \( C \) need not be direct. For example, it could happen that \( 0 \neq l \in \text{Rad}(Dn_B) \subseteq B \).

**21.2. The external Cayley-Dickson construction.** We will now recast the preceding considerations on a more abstract, but also more general, level. Let \( B \) be any conic algebra over \( k \) and \( \mu \in k \) an arbitrary scalar (playing the role of \(-n_C(l)\) in Prop. 21.1). We define a \( k \)-algebra \( C \) on the direct sum \( B \oplus Bj \) of two copies of \( B \) as a \( k \)-module by the multiplication

\[ (u_1 + v_1)j(u_2 + v_2j) := (u_1u_2 + \mu \bar{v}_2v_1) + (v_2u_1 + v_1\bar{u}_2)j, \]

for \( u_i,v_i \in B \), \( i = 1,2 \), and a quadratic form \( n_C: C \rightarrow k \) by

\[ n_C(u + vj) := n_B(u) - \mu n_B(v) \quad (u,v \in B). \]
$C$ together with $n_C$ is said to arise from $B, \mu$ by means of the Cayley-Dickson construction, and is written as $\text{Cay}(B, \mu)$ in order to indicate dependence on the parameters involved. Note that $\iota_C = \iota_B + 0 \cdot j$ is an identity element for $C$ and that the assignment $u \mapsto u + 0 \cdot j$ gives an embedding, i.e., an injective homomorphism, $B \hookrightarrow C$ of unital $k$-algebras, allowing us to identify $B \subseteq C$ as a unital subalgebra.

**21.3. Proposition.** Let $B$ be a conic $k$-algebra and $\mu \in k$ an arbitrary scalar. Then $C = \text{Cay}(B, \mu)$ as defined in 21.2 is a conic $k$-algebra whose algebra structure, unit element, norm, polarized norm, trace, conjugation relate to the corresponding objects belonging to $B$ by the formulas

\[
(u_1 + v_1 j)(u_2 + v_2 j) = (u_1 u_2 + \mu \overline{v_1} v_1) + (v_2 u_1 + v_1 \overline{u_2} j), \quad (1)\]

\[
\iota_C = \iota_B, \quad (2)\]

\[
n_C(u + v j) = n_B(u) - \mu n_B(v), \quad (3)\]

\[
n_C(u_1 + v_1 j, u_2 + v_2 j) = n_B(u_1, u_2) - \mu n_B(v_1, v_2), \quad (4)\]

\[
n_C(u_1 + v_1 j, u_2 + v_2 j) = n_B(u_1, u_2) - \mu n_B(v_1, v_2), \quad (5)\]

\[
\iota_C(u + v j) = u + v j = \bar{u} - v j \quad (6)\]

for all $u, u_i, v, v_i \in B$, $i = 1, 2$. In particular,

\[
B j = jB \subseteq B^\perp. \quad (7)\]

**Proof.** (1)–(5) are simply repetitions of things stated in 21.2 and immediately imply (4). Hence $n_C(1_C, x) = \iota_B(u)$ for $x = u + v j, u, v \in B$, and from (1), (19.5.4), (19.5.1) we conclude

\[
x^2 = (u^2 + \mu n_B(v) \iota_B) + \iota_B(u) v j = \iota_B(u) (u + v j) - (n_B(u) - \mu n_B(v)) j = n_C(1_C, x) x - n_C(x) 1_C.
\]

Thus $C$ is a conic $k$-algebra. (1)–(6) are now clear, while (7) follows directly from (1) and (4).

**21.4. Remark.** In the situation of Prop. 21.3 the norm of the Cayley-Dickson construction $\text{Cay}(B, \mu)$ may be written more concisely as

\[
n_{\text{Cay}(B, \mu)} = n_B \oplus (-\mu) n_B = (1, -\mu) \otimes n_B.
\]

**21.5. The Cayley Dickson process.** Since the Cayley-Dickson construction stabilizes the category of conic algebras, it can be iterated: given a conic algebra $B$ over $k$ and scalars $\mu_1, \ldots, \mu_n \in k$, we say that

\[
\text{Cay}(B; \mu_1, \mu_2, \ldots, \mu_n) := \text{Cay}\left( \ldots \left( \text{Cay}(\text{Cay}(B, \mu_1), \mu_2) \right) \ldots \right).
\]

arises from $B$ and $\mu_1, \ldots, \mu_n$ by means of the Cayley-Dickson process.
Before we can proceed, we will have to insert an easy technicality.

21.6. Proposition. (Universal property of the Cayley-Dickson construction) Let \( g: B \to C \) be a homomorphism of conic \( k \)-algebras and suppose in addition that \( C \) is multiplicative alternative. Given \( l \in g(B)^\perp \subseteq C \) and setting \( \mu := -n_C(l) \), there exists a unique extension of \( g \) to a homomorphism \( h: \text{Cay}(B, \mu) \to \text{Cay}(C) \) of conic algebras over \( k \) sending \( j \) to \( h(j) = l \). The image of \( h \) is the subalgebra of \( C \) generated by \( g(B) \) and \( l \), while its kernel has the form

\[ \ker(h) = \{ u + vl \mid u, v \in B, g(u) = -g(v)l \} . \]

Proof. Any such \( h \) has the form \( h(u + vl) = g(u) + g(v)l \) for \( u, v \in B \). Conversely, defining \( h \) in this manner, we obtain \( h(j) = l \) and deduce from (21.1.1)–(21.1.4) combined with (21.3.1) that \( h \) is a homomorphism of conic algebras. The remaining assertions are clear. \( \square \)

Before we can proceed, we will have to insert an easy technicality.

21.7. Zero divisors of modules. Let \( M \) be a \( k \)-module. In accordance with Bourbaki [11 1, 8.1], an element \( \mu \in k \) is called a zero divisor of \( M \) if the homothety \( x \mapsto \mu x \) from \( M \) to \( M \) is not injective. We claim that, if \( M \) is projective and contains unimodular elements, the zero divisors of \( M \) are precisely the zero divisors of \( k \). Indeed, since the injectivity of linear maps can be tested locally, we may assume that \( k \) is a local ring, in which case \( M \neq \{0\} \) is free as a \( k \)-module, and the assertion follows.

21.8. Corollary. Under the hypotheses of Prop. 21.6 assume that \( g \) is injective, \( B \) is projective as a \( k \)-module, \( n_B \) is weakly non-singular and \( \mu \) is not a zero divisor of \( k \). Then \( h \) is an isomorphism from \( \text{Cay}(B, \mu) \) onto the subalgebra of \( C \) generated by \( B \) and \( l \).

Proof. We need only show that \( h \) is injective, so let \( u, v \in B \) satisfy \( u + vl \in \ker(h) \). By Prop. 21.6 and (21.1.7), we have \( g(u) = -g(v)l \in g(B) \cap g(B)^\perp \), forcing \( g(u) = g(v)l = 0 \) by weak non-singularity of \( n_B \), and (21.1.3) yields \( g(\mu v) = \mu g(v) = (g(v)/l)l = 0 \), hence \( \mu v = 0 \). But \( \mu \), not being a zero divisor of \( k \), neither is one of \( B \) by (21.7). Thus \( v = 0 \), as claimed. \( \square \)

21.9. Examples. Considering the conic algebras of Chap. 11 over the field \( k = \mathbb{R} \) of real numbers, we note that \( i \in \mathbb{C} \) belongs to \( (\mathbb{R}1_\mathbb{C})^\perp \) and has norm 1. Hence Cor. 21.8 yields a canonical identification \( \mathbb{C} = \text{Cay}(\mathbb{R}, -1) \). Similarly, identifying \( \mathbb{C} = \mathbb{R}1_{\mathbb{C}} \) as a subalgebra of \( \mathbb{H} \), the Hamiltonian quaternions, \( j \in \mathbb{H} \) belongs to \( \mathbb{C}^\perp \) and again has norm 1, which implies \( \mathbb{H} = \text{Cay}(\mathbb{C}, -1) = \text{Cay}(\mathbb{R}; -1, -1) \). And finally, viewing \( \mathbb{H} \) via (1.10) as a subalgebra of \( \mathbb{O} \), the Graves-Cayley octonions, and consulting (1.5.1), (1.5.2), we conclude that \( j := 0 \oplus (ie_1) \in \mathbb{H}^\perp \subseteq \mathbb{O} \) has norm 1. Therefore \( \mathbb{O} = \text{Cay}(\mathbb{H}, -1) = \text{Cay}(\mathbb{C}; -1, -1) = \text{Cay}(\mathbb{R}; -1, -1, -1) \).
Useful properties of conic algebras preserved by the Cayley-Dickson construction are in short supply. For instance, the property to be projective as a $k$-module trivially carries over from a conic algebra $B$ to any Cayley-Dickson construction $\text{Cay}(B, \mu)$, $\mu \in k$. Other examples are provided by the following result.

21.10. Proposition. Let $B$ be a conic algebra over $k$ and $\mu \in k$. If the conjugation of $B$ is an involution, then so is the conjugation of $C := \text{Cay}(B, \mu)$. If $B$ is norm-associative, then so is $C$.

Proof. The first part follows by a straightforward computation. As to the second, it suffices to verify (19.12.2), so we must show

$$n_C(u_1 + v_1 j, (u_1 + v_1 j)(u_2 + v_2 j)) = \pi_C(u_2 + v_2 j)n_C(u_1 + v_1 j)$$

for $u_i, v_i \in B$, $i = 1, 2$. To this end, one expands the left-hand side using (21.3.1), (21.3.4) and observes that (19.12.4) holds for $B$. Details are left to the reader. □

On the other hand, preserving flexibility under the Cayley-Dickson construction is only possible with a caveat.

21.11. Proposition. For a conic $k$-algebra $B$ and $\mu \in k$, the Cayley-Dickson construction $C := \text{Cay}(B, \mu)$ is flexible if and only if $B$ is flexible and the conjugation of $B$ is an involution.

Proof. Suppose first that $C$ is flexible. Then $B$ is flexible and (19.9.1) holds for all $x, y \in C$. In particular, for $u_1, u_2, v_1 \in B$, we set $x := u_1 + v_1 j, y := u_2$ and conclude that

$$\left(tr_C(x, y) - n_C(x, \bar{y})\right)x = \left(tr_C((u_1 + v_1 j)u_2) - n_C(u_1 + v_1 j, \bar{u}_2)\right)(u_1 + v_1 j)$$

$$= \left(tr_B(u_1 u_2 + (v_1 \bar{u}_2) j) - n_B(u_1, \bar{u}_2)\right)(u_1 + v_1 j)$$

$$= \left(tr_B(u_1, u_2) - n_B(u_1, \bar{u}_2)\right)(u_1 + v_1 j),$$

belongs to $k_1B \subseteq B$. Comparing $B$-components, we obtain $tr_B(u_1, u_2) - n_B(u_1, \bar{u}_2) \in \text{Ann}(B)$, whence the conjugation of $B$ is an involution (Prop. 19.9 (a)).

Conversely, suppose $B$ is flexible and its conjugation is an involution. Then, by Prop. 21.10, the conjugation of $C$ is an involution, and we deduce from Cor. 19.10 that it suffices to show

$$n_C(x, xy) - t_C(y)n_C(x) \in \text{Ann}(C)$$

for all $x, y \in C$. By linearity (in $y$), assuming $x = u_1 + v_1 j$ with $u_1, u_2 \in B$, we are left with the following cases.

Case 1. $y = u_2 \in B$. Then
\[ n_C(x,xy) - t_C(y)n_C(x) = n_C(u_1 + v_1 j, u_1 u_2 + (v_1 \bar{u}_2) j) - t_B(u_2) n_C(u_1 + v_1 j) \]
\[ = n_B(u_1, u_1 u_2) - \mu n_B(v_1, v_1 \bar{u}_2) \]
\[ - t_B(u_2) n_B(u_1) + \mu t_B(u_2) n_B(v_1) \]
\[ = (n_B(u_1, u_1 u_2) - t_B(u_2) n_B(u_1)) \]
\[ - \mu (n_B(v_1, v_1 \bar{u}_2) - t_B(\bar{u}_2) n_B(v_1)), \]

where both summands on the right by the hypotheses on \( B \) and Cor. [19.10] belong to \( \text{Ann}(B) = \text{Ann}(C) \). Hence so does \( n_C(x,xy) - t_C(y)n_C(x) \).

**Case 2.** \( y = v_2 j, v_2 \in B \). Then

\[ n_C(x,xy) - t_C(y)n_C(x) = n_C(u_1 + v_1 j, \mu \bar{v}_2 v_1 + (v_2 u_1) j) \]
\[ = \mu (n_B(\bar{v}_2 v_1, u_1) - n_B(v_1, v_2 u_1)). \]

It therefore remains to show \( n_B(u, vw) - n_B(\bar{v} u, w) \in \text{Ann}(B) \) for all \( u, v, w \in B \). Since \( B^{\text{op}} \) is a flexible conic algebra whose conjugation is an involution, Cor. [19.10] implies \( n_B(u, vu) - t_B(v)n_B(u) \in \text{Ann}(B) \), so after linearization, \( \text{Ann}(B) \) contains \( n_B(u, vw) + n_B(w, vu) - t_B(v)n_B(u, w) = n_B(u, vw) - n_B(\bar{v} u, w) \), as desired. \( \square \)

**21.12. Commutators and associators.** Let \( B \) be a conic algebra over \( k \). For \( \mu \in k \), we wish to find conditions that are necessary and sufficient for the the Cayley-Dickson construction \( C = \text{Cay}(B, \mu) \) to be commutative, associative, alternative, respectively. To this end, we will describe the commutator and the associator of \( C \) in terms of \( B \) and \( \mu \) under the assumption that, in case of the associator, the conjugation of \( B \) be an involution. Then, letting \( u_i, v_i \in B, i = 1, 2, 3 \) and keeping the notation of [21.2] a lengthy but straightforward computation yields

\[ [u_1 + v_1 j, u_2 + v_2 j] = u + v j, \]
\[ [u_1 + v_1 j, u_2 + v_2 j, u_3 + v_3 j] = \bar{u} + \bar{v} j, \]

where

\[ u = [u_1, u_2] + \mu (\bar{v}_3 v_1 - v_1 \bar{v}_3), \]  
(1) \hspace{1cm} \text{CDCOMONE}

\[ v = v_2 (u_1 - \bar{u}_1) - v_1 (u_2 - \bar{u}_2), \]  
(2) \hspace{1cm} \text{CDCOMTWO}

\[ \bar{u} = [u_1, u_2, u_3] + \mu (v_1 \bar{v}_3 u_3 - (v_3 \bar{v}_3) v_1 + \]  
\[ v_3 (v_2 u_1) + \bar{v}_3 (v_1 \bar{u}_2) - u_1 (\bar{v}_3 v_2) - (\bar{v}_2 \bar{v}_3) v_1) \],  
(3) \hspace{1cm} \text{CDASSONE}

\[ \bar{v} = v_3 (u_1 u_2) - (v_3 u_2) u_1 + (v_2 u_1) \bar{u}_3 + (v_1 \bar{u}_3) \bar{u}_3 \]
\[ - (v_2 \bar{u}_3) u_1 - v_1 (\bar{u}_3 \bar{u}_3) + \mu (v_3 (\bar{v}_2 v_1) - v_1 (\bar{v}_2 \bar{v}_3)). \]  
(4) \hspace{1cm} \text{CDASSTWO}

With the aid of these identities, we can now prove the following important result.

**21.13. Theorem.** For a conic \( k \)-algebra \( B \), an arbitrary scalar \( \mu \in k \) and the corresponding Cayley-Dickson construction \( C := \text{Cay}(B, \mu) \), the following statements hold.
21 The Cayley-Dickson construction

(a) $C$ is commutative if and only if $B$ is commutative and has trivial conjugation.
(b) $C$ is associative if and only if $B$ is commutative associative and its conjugation
is an involution.
(c) $C$ is alternative if and only if $B$ is associative and its conjugation is an involution.

Proof. (a) If $C$ is commutative, then so is $B$ and $(21.12.2)$ for $v_2 = 1_B, v_1 = 0$ implies $t_B = 1_B$. Conversely, let $B$ be commutative and suppose $t_B = 1_B$. Then an inspection of $(21.12.1), (21.12.2)$ shows that $C$ is commutative as well.

(b) If $C$ is associative, then so is $B$, its conjugation is an involution by Prop. 21.11, and $(21.12.4)$ for $u_3 = v_1 = v_2 = 0, v_3 = 1_C$ shows that $B$ is commutative as well. Conversely, if $B$ is commutative associative and its conjugation is an involution, an inspection of $(21.12.3), (21.12.4)$ shows that $C$ is associative.

(c) If $C$ is alternative, then the conjugation of $B$ by Prop. 21.11 is an involution. Moreover, $\tilde{a} = 0$ for $u_1 = u_2, v_1 = v_2, v_3 = 0$ and $(21.12.4)$ combined with $(19.5.4)$ yield

$$0 = (v_1 u_1)\overline{u_3} + (v_1 u_1)\overline{u_3} - (v_1 u_3)u_1 - v_1(\overline{u_3} u_1)$$
$$= t_B(u_1)\overline{v_3} - (v_1\overline{u_3})u_1 - t_B(u_1)v_1\overline{u_3} + v_1(\overline{u_3} u_1)$$
$$= -[v_1, \overline{u_3}, u_1].$$

Hence $B$ is associative. Conversely, let this be so and suppose $t_B$ is an involution. Setting $u_1 = u_2, v_1 = v_2$ in $(21.12.3), (21.12.4)$, Kirmse’s identities $(20.3.1)$ and $(19.5.4)$ imply

$$\tilde{a} = \mu(n_B(v_1)u_3 - n_B(v_1)u_3 + t_B(u_1)\overline{v_3}v_1 - t_B(u_1)\overline{v_3}v_1) = 0,$$
$$\tilde{v} = t_B(u_1)v_1\overline{u_3} - t_B(u_1)v_1\overline{u_3} + \mu(n_B(v_1)v_3 - n_B(v_1)v_3) = 0,$$

forcing $C$ to be alternative. □

21.14. Corollary. In addition to the above, assume that $B$ is projective as a $k$-module. Then

(a) $C$ is associative if and only if $B$ is commutative associative.
(b) $C$ is alternative if and only if $B$ is associative.

Proof. All the algebras of Thm. 21.13 are flexible. Hence in each case Prop. 19.13
shows the hypothesis of the conjugation of $B$ being an involution is automatic. □

21.15. Examples. (a) Let $R$ be a quadratic $k$-algebra whose conjugation is non-
trivial. For any $\mu_1 \in k$, Cor. 21.14 (a) combined with Thm. 21.13 (a) shows that
the conic algebra $B := \text{Cay}(R, \mu_1)$ is associative but not commutative. Applying
Cor. 21.14 again, we therefore conclude for any $\mu_2 \in k$ that the conic algebra
$C := \text{Cay}(B, \mu_2) = \text{Cay}(R, \mu_1, \mu_2)$ is alternative but not associative. In view of Ex. 21.9
these results generalize what we have found in Exc. 1 and Cor. 1.11.
(b) At the other extreme, assume \( 2 = 0 \) in \( k \). If \( B \) is a commutative associative conic \( k \)-algebra with trivial conjugation (e.g., \( B = k \)), then by Thm. \( [21.13] \) and \( [21.36] \) so is the Cayley-Dickson process \( C := \text{Cay}(B; \mu_1, \ldots, \mu_n) \), for any positive integer \( n \) and any \( \mu_1, \ldots, \mu_n \in k \).

**Exercises.**

**pr.CDMUL** 92. Let \( B \) be a multiplicative conic algebra over \( k \) and \( \mu \in k \). Show that the Cayley-Dickson construction \( \text{Cay}(B, \mu) \) is multiplicative if and only if \( [B, B, B] \subseteq \text{Rad}(B) \).

**pr.CDSCAPAR** 93. Let \( B \) be a multiplicative conic \( k \)-algebra, and let \( \mu \in k, a \in \text{Nuc}(B) \). Show that the map
\[
\varphi : \text{Cay}(B, n_B(a)\mu) \rightarrow \text{Cay}(B, \mu)
\]
developed by \( \varphi(u + vj) := u + (av)j \) for \( u, v \in B \) is a homomorphism of conic algebras. Moreover, it is an isomorphism if and only if \( a \) is invertible in \( \text{Nuc}(B) \).

**pr.ZERDIV** 94. Zero divisors of algebras. Let \( A \) be a \( k \)-algebra. An element \( x \in A \) is called a right (resp. left) zero divisor of \( A \) if the left (resp. right) multiplication \( L_x : A \rightarrow A \) (resp. \( R_x : A \rightarrow A \)) of \( x \) in \( A \) is not injective. We say \( A \) has left (resp. right) zero divisors if it contains left (resp. right) zero divisors other than zero.

Now let \( C \) be a conic alternative \( k \)-algebra which is projective as a \( k \)-module. Prove for \( x \in C \) that the following conditions are equivalent.

(i) \( x \) is a right zero divisor of \( C \).
(ii) \( x \) is a left zero divisor of \( C \).
(iii) \( n_C(x) \) is a zero divisor of \( k \).

(Hint. For the implication (i) \( \Rightarrow \) (iii), argue indirectly and pass to the base change \( C_f = C \otimes k_f, f = n_C(x) \).

**pr.VARCD** 95. A variant of the Cayley-Dickson construction. Let \( B \) be a conic \( k \)-algebra and \( \mu \in k \). On the direct sum \( B \oplus jB \) of two copies of \( B \) as a \( k \)-module we define a \( k \)-algebra structure \( \text{Cay}'(B, \mu) \) by the formula
\[
(u_1 + jv_1)(u_2 + jv_2) := (u_1u_2 + \mu v_2v_1) + j(\bar{u}_1v_2 + u_2v_1)
\]
for \( u_1, u_2, v_1, v_2 \in B \). Show that there is a natural isomorphism
\[
\text{Cay}(B^\text{op}, \mu) \cong \text{Cay}'(B, \mu)^\text{op}
\]
and conclude that \( \text{Cay}'(B, \mu) \) is a conic \( k \)-algebra with norm, trace and conjugation canonically isomorphic to the corresponding objects attached to \( \text{Cay}(B, \mu) \). Show further that, if the conjugation of \( B \) is an involution, then
\[
\text{Cay}(B, \mu) \overset{\cong}{\longrightarrow} \text{Cay}'(B, \mu), \quad u + vj \longmapsto u + j\bar{v},
\]
is an isomorphism of conic algebras.

**22. Basic properties of composition algebras.**

Before being able to deal with the main topic of this section, it will be necessary to introduce an auxiliary notion that can hardly stand on its own but turns out to be technically useful. Throughout, we let \( k \) be an arbitrary commutative ring.
22.1. Pre-composition algebras. By a pre-composition algebra over $k$ we mean a $k$-algebra $C$ satisfying the following conditions.

(i) $C$ is unital.
(ii) $C$ is projective as a $k$-module.
(iii) There exists a non-degenerate quadratic form $n : C \rightarrow k$ that permits composition:

$$n(1_C) = 1,$$

$$n(xy) = n(x)n(y) \quad (x, y \in C).$$  \hspace{1cm} (1) \hspace{1cm} (2)

In this case, (2) may be linearized (repeatedly) and yields the relations

$$n(xy, xz) = n(x)n(y, z),$$

$$n(xy, yz) = n(x, z)n(y),$$

$$n(xy, wz) + n(wy, xz) = n(x, w)n(y, z)$$  \hspace{1cm} (3) \hspace{1cm} (4) \hspace{1cm} (5)

for all $x, y, z, w \in C$.

In view of Prop. 20.5, conic alternative algebras which are projective as $k$-modules are pre-composition algebras provided their norm is a non-degenerate quadratic form. Remarkably, the converse of this is also true.

22.2. Proposition. Let $C$ be a pre-composition algebra over $k$ and $n : C \rightarrow k$ any non-degenerate quadratic form that permits composition. Then $C$ is a conic alternative $k$-algebra with unique norm $n_C = n$. Moreover,

$$C^\perp := \text{Rad}(Dn_C) = \{x \in C \mid n_C(x, y) = 0 \text{ for all } y \in C\} \subseteq \text{Cent}(C)$$

is a central ideal of $C$ satisfying

$$2C^\perp = n_C(x, y)C^\perp = \{0\}$$

for all $x, y \in C$.

Proof. For the first part, it suffices to show that $C$ is a conic alternative algebra with norm $n_C := n$ since uniqueness follow from Prop. 19.15. By (22.1.1), we have $n(1_C) = 1$. Now we put $z = 1_C$ in (22.1.3). Then

$$n(xy, z) = n(x)n(y, z),$$

where $t(y) := n(1_C, y)$. Setting $y = x, w = z = 1_C$ in (22.1.5), we obtain $t(x^2) + n(x, x) = t(x)^2$, hence

$$t(x^2) = t(x)^2 - 2n(x).$$  \hspace{1cm} (2)

Furthermore, setting $z = x, w = 1_C$ in (22.1.5), we also obtain $n(xy, x) + n(x^2, y) = t(x)n(x, y)$, so by (1),
Similarly, one can show \( n(x^2 - t(x)x + n(x)1_C, y) = 0 \) by expanding the left-hand side and using (1) (for \( y = x \)) as well as (2). Since \( n \) is non-degenerate, \( C \) is therefore a conic \( k \)-algebra with norm \( n_C = n \). Moreover, (1) shows that \( C \) is norm-associative, hence flexible by Prop. 19.13. Thus alternativity will follow once we have established the left alternative law, equivalently, the first of Kirmse’s identities (20.311). To this end, we combine (19.11.4) with (22.1.3) and the multiplicativity of \( n \) to obtain \( n(x(\overline{xy}), z) = n(\overline{xy}, \overline{xz}) = n(n(x)y, z) \). A similar computation yields \( n(x(\overline{xy}) - n(x)y) = 0 \), and non-degeneracy of \( n \) implies the first Kirmse identity \( x(\overline{xy}) = n(x)y \), as claimed.

We now turn to \( C^\perp \). By non-degeneracy of \( n \), \( n : C^\perp \to k \) is an embedding of additive groups. In particular, \( n(2x) = 2n(x, x) = 0 \) for \( x \in C^\perp \) implies \( 2C^\perp = \{0\} \). Moreover, (19.11.3) and (19.11.4) show that \( C^\perp \subseteq C \) is an ideal. We claim that this ideal belongs to the centre of \( C \). Indeed, for \( x, y, z \in C, z \in C^\perp \), evaluating \( n \) at \( (xy)z, x(yz) \in C^\perp \) yields the same value \( n(x)n(y)n(z) \), which implies \( [x, y, z] = 0 \). Similarly, \( [y, z] = 0 \), and the assertion follows. It remains to prove \( n(x, y)z = 0 \). Since the conjugation of \( C \) is the identity on \( C^\perp \), this follows from (19.11.5) and \( n(x, y)z = t(\overline{xy})z = (\overline{xy})z + (yz)z = (zx)y + yzx = n(x, y)1_C = 0 \).

\[ \square \]

Pre-composition algebras suffer the serious disadvantage of not being stable under base change. This may be seen from the following example.

### 22.3. Example.

Let \( K/k \) be a purely inseparable field extension of characteristic 2 and exponent at most 1, so \( K^2 \subseteq k \) (we allow the degree of \( K/k \) to be infinite). Then \( K \) is a pre-composition algebra over \( k \) whose norm, given by the squaring \( K \to k, x \mapsto x^2 \), is an anisotropic quadratic form with zero bilinearization. In particular, for \( [K : k] > 1 \), \( n_K \) becomes isotropic, hence degenerate, when extending scalars to the algebraic closure, so the corresponding scalar extension of the \( k \)-algebra \( K \) is not a pre-composition algebra anymore.

Our next objective in this section will be to define the concept of a composition algebra in such a way that it remains stable under base change and always, even when 2 is not a unit, includes the base ring as an, albeit trivial, example. This is ensured by insisting on suitable separability conditions on the constituents entering into the definition of a composition algebra. We then proceed to derive a number of important properties that are all related in one way or another to the Cayley-Dickson construction. We show in particular that composition algebras over semi-local rings always contain quadratic étale subalgebras, which in turn may be used to recover the ambient composition algebra by means of the Cayley-Dickson process. It follows that, over any commutative ring, composition algebras (if they have a rank at all) exist only in ranks 1, 2, 4, 8. The section concludes with a brief discussion of quaternion and octonion algebras.
22.4. The concept of a composition algebra. Basically following a suggestion of O. Loos, we define a composition algebra over \( k \) as a \( k \)-algebra \( C \) satisfying the following conditions.

(i) \( C \) is unital.
(ii) \( C \) is projective as a \( k \)-module.
(iii) The rank function \( p \mapsto \text{rk}_p(C) \) from \( \text{Spec}(k) \) to \( \mathbb{N} \cup \{\infty\} \) is locally constant with respect to the Zariski topology of \( \text{Spec}(k) \).
(iv) There exists a separable quadratic form \( n: C \to k \) that permits composition:

\[
\begin{align*}
  n(1_C) &= 1, \\
  n(xy) &= n(x)n(y) \\
  (x, y &\in C).
\end{align*}
\]

If even a non-singular quadratic form (rather than just a separable one) exists on \( C \) permitting composition, we speak of a non-singular composition algebra. Note that condition (iii) above holds automatically if \( C \) is not only projective but also finitely generated as a \( k \)-module (Bourbaki [11, II, Thm. 1]).

Comparing conditions (i)–(v) above with the corresponding ones of 22.1, we see that the main difference between pre-composition algebras and (non-singular) composition algebras lies in the respective regularity condition imposed on the quadratic form permitting composition. In view of this difference, non-singular composition algebras are always pre-composition algebras. On the other hand, ordinary composition algebras are pre-composition algebras if the base ring \( k \) is a field, but not in general. For example, \( k \) is always a composition algebra over itself, while it is a pre-composition algebra if and only if, for all \( \alpha \in k \), the relations \( \alpha^2 = 2\alpha = 0 \) imply \( \alpha = 0 \), which fails to be the case if, e.g., \( k \) contains non-zero nilpotent elements and \( 2 = 0 \) in \( k \). At the other extreme, if \( \frac{1}{2} \in k \), then \( k \) will always be a non-singular composition algebra.

The most important feature of composition algebras (as opposed to pre-composition algebras, cf. Ex. 22.3 above) is that they are stable under base change. This constitutes the main reason why the former are to be preferred to the latter. Our next aim will be to examine the relationship between (non-singular) composition algebras and pre-composition algebras more closely. We first note that if \( C \) is a (non-singular, resp. pre-) composition algebra over \( k \), so is \( C^{op} \). We also need to characterize a class of composition algebras sitting inside conic algebras as “small” unital subalgebras.

22.5. Proposition. Let \( C \) be a conic algebra over \( k \) and \( u \in C \). Then \( D := k[u] \subseteq C \) is a unital commutative associative subalgebra and the following conditions are equivalent.

(i) \( D \) is a non-singular composition algebra of rank 2.
(ii) \( D \) is free of rank 2 as a \( k \)-module with basis \((1_C, u)\), and the quadratic form \( n_C \) is non-singular on \( D \).
(iii) \( t_C(u)^2 - 4n_C(u) \in k^\times \).

In this case,
\[
\text{disc} \left( (D,n_D) \right) = \left( t_C(u)^2 - 4n_C(u) \right) \mod k^{\times 2}
\] (1)

is the discriminant of the quadratic space \((D,n_D)\).

**Proof.** Since conic algebras are power-associative by \([19.5]\), the first part is clear.

(i) \(\Leftrightarrow\) (ii). Suppose (i) holds. Since \(D\) is a finitely generated projective \(k\)-module of rank 2, the natural surjection \(k^2 \to D\) determined by the elements \(1_C, u\) must be a bijection, giving the first part of (ii). As to the second, \(D\) is a pre-composition algebra, hence a conic one, so \(n_C\) by Prop. \([22.2]\) restricts to the unique non-degenerate (actually, non-singular) quadratic form on \(D\) permitting composition. Conversely, (i) is a consequence of (ii) by Exc. \([77]\)(a).

(ii) \(\Leftrightarrow\) (iii). Since \(D\) is flexible, (ii) combined with Prop. \([19.13]\) implies that it is norm-associative, so by \([19.11.5]\) the bilinear trace \(t_D = t_C|_{D \times D}\) is non-singular along with \(n_D = n_C|_{D \times D}\). Computing the determinant of \(Dn_D\) relative to the basis \((1_D, u)\) of \(D\), we obtain

\[
det \begin{pmatrix}
   n_C(1_C, 1_C) & n_C(1_C, u) \\
   n_C(u, 1_C) & n_C(u, u)
\end{pmatrix}
= \det \begin{pmatrix}
   2 & t_C(u) \\
   t_C(u) & 2n_C(u)
\end{pmatrix}
= 4n_C(u) - t_C(u)^2,
\]

hence (iii), and the formula for the discriminant. Conversely, if (iii) holds, it suffices to show that \(1_C, u\) are linearly independent over \(k\), so suppose \(\alpha, \beta \in k\) satisfy the relation \(\alpha 1_C + \beta u = 0\). Then \(\alpha u + \beta u^2 = 0\), and taking traces we conclude

\[
\begin{pmatrix}
   2 & t_C(u) \\
   t_C(u) & 2n_C(u)
\end{pmatrix}
\begin{pmatrix}
   \alpha \\
   \beta
\end{pmatrix}
= \begin{pmatrix}
   t_C(1_C) & t_C(u) \\
   t_C(u) & t_C(u^2)
\end{pmatrix}
\begin{pmatrix}
   \alpha \\
   \beta
\end{pmatrix}
= 0.
\]

But by (iii) the matrix on the very left is invertible, forcing \(\alpha = \beta = 0\), as desired.

\[\square\]

**22.6. Proposition** (Kaplansky [52]). *If \(k\) is a field, a \(k\)-algebra \(C\) is a pre-composition algebra if and only if it is either a (finite-dimensional) non-singular composition algebra or a purely inseparable field extension of characteristic 2 and exponent at most 1.*

**Proof.** In view of the Ex. \([22.3]\) we only have to prove that a pre-composition algebra \(C\) over \(k\) has the form indicated in the proposition. Adopting the notation of Prop. \([22.2]\) we first assume \(C^\perp \neq \{0\}\). Since \(2C^\perp = \{0\}\) and \(C^\perp\) is a central ideal of \(C\) whose non-zero elements, by non-degeneracy, are anisotropic relative to \(n_C\), hence invertible in \(C\) (Prop. \([20.4]\)), we conclude that \(k\) has characteristic 2 and \(K := C = C^\perp = \text{Cent}(C)\) is an extension field of \(k\) whose trace (in its capacity as a conic algebra) vanishes identically. Thus \(K/k\) is purely inseparable of exponent \(\leq 1\). We are left with the case \(C^\perp = \{0\}\), so \(n_C\) is weakly non-singular. It suffices to show that \(C\) is finite-dimensional. Our first aim will be to exhibit a unital subalgebra \(D \subseteq C\) of dimension at most 2 on which \(n_C\) is non-singular. For \(\text{char}(k) \neq 2\), \(D := k1_C\) will do, so suppose \(\text{char}(k) = 2\). Then weak non-singularity of \(n_C\) produces an element \(u \in C\) of trace 1, and Prop. \([22.5]\) shows that \(D := k[u] \subseteq C\) is a
subalgebra of the desired kind. Now let $B \subset C$ be any proper unital subalgebra of finite dimension on which $n_C$ is non-singular. Then $C = B \oplus B^\perp$ by Lemma 12.10, and since $n_C$ is weakly non-singular on $C$, we find an anisotropic vector $l \in B^\perp$. But $C$ is a conic alternative $k$-algebra, so Cor. 21.8 leads to an embedding Cay($B, \mu$) $\hookrightarrow C$, $\mu = -n_C(l) \in k^\times$, whose image continues to be a unital subalgebra of $C$ on which $n_C$ is non-degenerate. Assuming $C$ were infinite-dimensional and starting from $D$, we could repeat this procedure indefinitely but, by Cor. 21.14 after at most four steps, would arrive at a subalgebra of $C$ that is no longer alternative. This contradiction to Prop. 22.2 shows that $C$ is indeed finite-dimensional. □

Remark. The preceding proof actually yields more than is claimed in the proposition. But since the situation described here will soon be re-examined in the more general set-up of semi-local rings, we see no point at this stage to state this additional piece of information explicitly.

22.7. Corollary. Let $C$ be a composition algebra over $k$. Then $C$ is finitely generated projective as a $k$-module, and if it has rank $r$, then $C$ is either non-singular, or $r = 1$ (i.e., $C \cong k$) and $\frac{1}{2} \notin k$.

Proof. In view of 22.4 (iii), the assertion is local on $k$, so we may assume that $k$ is a local ring with maximal ideal $m$. The $C(m)$ is a composition algebra, hence also a pre-composition algebra, over the field $k(m)$ and thus, by Prop. 22.6 combined with Ex. 22.3 is either finite-dimensional non-singular or one-dimensional of characteristic 2. □

22.8. Theorem. A $k$-algebra $C$ is a composition algebra (resp. a non-singular composition algebra) if and only if it is a conic alternative algebra which is finitely generated projective as a $k$-module and has a separable (resp. non-singular) norm. In this case, the norm $n_C$ (cf. Prop. 19.15) is the only separable quadratic form on $C$ permitting composition.

Proof. A conic alternative algebra which is finitely generated projective as a $k$-module and has a separable (resp. non-singular) norm is a composition algebra (resp. a non-singular composition algebra) by Prop. 20.5. Conversely, let $C$ be a composition algebra and $n : C \rightarrow k$ a separable quadratic form permitting composition. By Cor. 22.7, we need only show that $C$ is conic alternative with norm $n_C = n$. By Prop. 22.2 we are done if $C$ is a pre-composition algebra. Otherwise, $C$ is a singular composition algebra, and Cor. 22.7 implies $C = k$ and $n = \varepsilon \langle 1 \rangle_q$ for some idempotent $\varepsilon \in k$ such that $\varepsilon(p) = 1$ in $k(p)$ for all $p \in \text{Spec}(k)$ since $n$ is separable. Hence $\varepsilon = 1$. □

22.9. Examples. (a) We know from 19.2 that $D = k \oplus k$ is a quadratic commutative associative $k$-algebra whose norm is the hyperbolic plane on $D$ given by $n_D(\alpha \oplus \beta) = \alpha \beta$ for $\alpha, \beta \in k$. Hence $D$ is a non-singular composition algebra, called (for reasons that will become apparent later) the split composition algebra of rank 2.

(b) The algebra $\text{Mat}_2(k)$ of 2-by-2 matrices over $k$ is a non-singular associative composition algebra whose norm is the determinant det: $\text{Mat}_2(k) \rightarrow k$. Indeed, det
is a quadratic form that permits composition and is isometric to $2h$, the direct sum of two copies of the hyperbolic plane, hence non-singular.

In order to gain a more detailed understanding of composition algebras, they will now be exposed to the Cayley-Dickson construction.

**22.10. Theorem.** Let $B$ be a conic $k$-algebra and $\mu \in k$ an arbitrary scalar. Then $C = \text{Cay}(B, \mu)$ is a composition algebra if and only if $B$ is a non-singular associative composition algebra and $\mu$ is invertible in $k$. In this case, $C$ is a non-singular composition algebra as well.

**Proof.** Assume first that $B$ is a non-singular associative composition algebra and $\mu \in k$ is a unit. Then $B$ is conic associative by Thm. 22.8, forcing $C$ to be conic alternative by Cor. 21.14 and $n_C \cong n_B \oplus (-\mu)n_B$ (by (21.3.3)) to be a non-singular quadratic form. By Cor. 22.7 and Thm. 22.8 therefore, $C$ is a non-singular composition algebra. Conversely, assume that $C$ is a composition algebra. Since $C$ is conic alternative by Thm. 22.8, $B$ is conic associative by Cor. 21.14. Furthermore, for every field $K \in k$-alg, the decomposition $(n_C)_K \cong (n_B)_K \oplus (-\mu_K)(n_B)_K$ combines with the non-degeneracy of $(n_C)_K$ to show that $(n_B)_K$ is non-degenerate as well and $\mu_K \neq 0$. Hence $B$ is a composition algebra, and specializing $K = \kappa(p)$ for all $p \in \text{Spec} \ k$ implies $\mu \in k^\times$. It remains to prove that $B$ is non-singular. Otherwise, $B_p$ would be a singular composition algebra over $k_p$, for some $p \in \text{Spec} \ k$, forcing $C_p$ to be a singular composition algebra as well. But then Cor. 22.7 implies that $C_p$ has rank 1, a contradiction. □

Before exploiting the Cayley-Dickson construction still further, it is advisable to insert a technicality.

**22.11. Lemma.** The linear trace of a non-singular composition algebra is surjective. Up to isomorphism, the only composition algebra over $k$ having trivial conjugation is $k$ itself.

**Proof.** For the first part, we combine the non-singularity of the bilinear trace with the unimodularity of the identity to find an element in $C$ having trace 1. For the second part, we let $C$ be a composition algebra over $k$ with trivial conjugation. Localizing if necessary, we may assume by Cor. 22.7 that $C$ is non-singular. Then the assertion follows from the first part and Exc. 85. □

Our next aim will be to show that, under suitable conditions on $k$, all composition algebras arise from composition algebras of rank 2 by means of the Cayley-Dickson process. Within the framework of the present section, it would be enough to do so for $k$ being a local ring. But with an eye on subsequent applications, it will be important to relax this condition in a way that is tied up with the following concept.

**ss.SEMLOC**

**22.12. Semi-local rings.** Our base ring $k$ is said to be semi-local if it satisfies the following two equivalent conditions (Bourbaki [11, II, §3, Prop. 16]):

(i) The set of maximal ideals in $k$ is finite.
22 Basic properties of composition algebras.

(ii) The quotient $k/Jac(k)$ is a finite direct product of fields.

Here $Jac(k)$ denotes the Jacobson radical of $k$ (Bourbaki [13, VII, §6, Def. 3]. While every local ring is semi-local, the zero ring $k = \{0\}$ is semi-local without being local. Less trivial examples arise as follows (Bourbaki [11, IV, §2, Cor. 3 of Prop. 9]): Suppose $k_0$ is a (commutative) Noetherian semi-local ring and $k \in k_0$ is finitely generated as a $k_0$-module. Then $k$ is Noetherian and semi-local as well. But note that $k$ need not be local even if $k_0$ is.

We proceed by collecting a few useful properties of semi-local rings, addressed to projective modules and quadratic forms.

### 22.13. Proposition (Bourbaki [11, II, §5, Prop. 5]).

Let $k$ be a semi-local ring. Then every finitely generated projective $k$-module of rank $r \geq 0$ is free.

**Remark.** Since semi-local rings need not be connected, the condition on the rank function cannot be avoided.


Let $k$ be a semi-local ring. Then every quadratic space $(M, q)$ over $k$ satisfying $\text{Supp}(M) = \text{Spec}(k)$ represents some unit in $k$.

**Proof.** The assertion clearly holds over a finite direct product of fields since it is valid over each individual factor. Now let $k$ be arbitrary and write $\pi$ for the canonical map from $k$ to $R := k/Jac(k)$. By the special case just treated, applied to $(M, q) \otimes R$, some $x \in M$ satisfies $\pi(q(x)) \in R^\times$, hence $q(x) \in k^\times$.

Returning after this brief detour to the setting of compositions algebras, we can now establish the following basic result.

### 22.15. Theorem.

Let $k$ be a semi-local ring and $C$ a composition algebra of rank $r$ over $k$.

(a) If $B \subseteq C$ is a non-singular composition subalgebra of rank $s < r$, there exists a unit $\mu \in k^\times$ such that the inclusion $B \hookrightarrow C$ extends to an embedding $\text{Cay}(B, \mu) \rightarrow C$.

(b) If $r > 1$, then $C$ contains a composition subalgebra of rank 2 having the form $D = k[u]$ for some $u \in C$ of trace 1.

**Proof.** (a) Since $n_C$ is non-singular on $B$, Lemma [22.10] yields an orthogonal splitting $C = B \oplus B^\perp$, and the assumption $s < r$ implies that $(B^\perp, n_C|_{B^\perp})$ is a quadratic space over $k$ with $\text{Supp}(B^\perp) = \text{Spec}(k)$. Thus, by Lemma [22.14] there exists an element $l \in B^\perp$ satisfying $\mu := -n_C(l) \in k^\times$. Now Cor. [21.8] implies (a).

(b) We consider three cases.

- **Case 1.** $k$ is a field. Suppose first $\text{char}(k) \neq 2$. Then (a) yields a unital embedding of $D := \text{Cay}(k, \mu) = k \oplus kj$ into $C$ for some $\mu \in k^\times$, and $D$ is a composition algebra of rank 2 (Prop. [22.5]). Moreover, $D = k[u]$ with $u = \frac{1}{2} + j \in D$ having trace 1. We are left with the case $\text{char}(k) = 2$. Since $C$ is non-singular, we find an element $u \in C$ with $t_C(u) = 1$. Then $t_C(u)^2 - 4n_C(u) \in k^\times$, so $D := k[u] \subseteq C$ is a composition subalgebra of rank 2 by Prop. [22.5].
Case 2. $k$ is a finite product of fields. Then $k = k_1 \oplus \cdots \oplus k_m$ as a direct sum of ideals, with $m \in \mathbb{N}$ and fields $k_i$, $1 \leq i \leq m$. This implies $C = C_1 \oplus \cdots \oplus C_m$, where $C_i = C \otimes k_i$ ($1 \leq i \leq m$) is a composition algebra of dimension $> 1$ over $k_i$. Thus Case 1 yields a composition $k_i$-subalgebra $D_i \subseteq C_i$ of rank 2 generated by an element of trace 1, forcing $D := D_1 \oplus \cdots \oplus D_m \subseteq C$ to have the same properties over $k$.

Case 3. The general case. Then Case 2 applies to the base change $C' := C \otimes R$ over $R := k / \text{Jac}(k)$, and we find an element $v \in C$ such that $v' := v \otimes 1 \in C'$ has trace 1 and generates a rank 2 composition subalgebra of $C'$. Invoking Prop. 22.5, we conclude that $v$ generates a rank 2 composition subalgebra of $C$ and $t_C(v) \in 1 + \text{Jac}(k) \subseteq k^\times$, so $u := t_C(v)^{-1}v \in C$ is an element of the kind we are looking for. □

22.16. Corollary. Every composition algebra of rank $> 1$ over a semi-local ring arises from a composition algebra of rank 2, and even from the base ring itself if 2 is a unit, by an application of the Cayley-Dickson process. □

The preceding theorem has important consequences also in the case when the base ring is arbitrary.

22.17. Corollary (cf. Legrand [66]). Let $C$ be a composition algebra of rank $r$ over $k$ and assume $k \neq \{0\}$. Then $r = 1, 2, 4$ or 8 and the following statements hold.

(a) $C$ is non-singular unless $r = 1$ and $\frac{1}{2} \notin k$.
(b) If $r = 2$, then $C$ is commutative associative and has non-trivial conjugation.
(c) If $r = 4$, then $C$ is associative but not commutative.
(d) If $r = 8$, then $C$ is alternative but not associative.

Proof. We conclude from Cor. 22.16 that $r = 2^s$ is a power of 2. Localizing whenever necessary, (a)−(d) now follow by a straightforward combined application of Cor. 22.7, Lemma 22.11 and Thms. 22.10, 22.15, 21.13. Finally, Thm. 22.8 and Cor. 21.14 show that $s > 3$ is impossible. □

We conclude this section by taking a closer look at the remaining cases.

22.18. Quadratic étale algebras. Let $D$ be a unital commutative associative $k$-algebra that is finitely generated projective as a $k$-module. Then the following conditions are easily seen (and well known) to be equivalent.

(i) For all maximal ideals $m \subseteq k$, the algebra $D(m)$ over the field $\kappa(m) = k/m$ may be written as a (finite) direct product of (finite) separable field extensions.

(ii) For all prime ideals $p \subseteq k$, the $\kappa(p)$-algebra $D(p)$ may be written as a (finite) direct product of (finite) separable field extensions.

(iii) The bilinear trace $D \times D \rightarrow k, (x,y) \mapsto \text{tr}(L_{xy})$, $L$ being the left multiplication of $D$, is a non-singular symmetric bilinear form.

If these conditions are fulfilled, $D$ is said to be â©taté (or separable) over $k$. If, in addition, $D$ has rank 2 as a finitely generated projective $k$-module, we speak of a
quadratic étale $k$-algebra. Comparing (iii) with \([19.11],[19.4]\) and Cor. \([22.17]\), we see that being a quadratic étale $k$-algebra and a composition algebra over $k$ of rank 2 are equivalent notions; therefore these terms will henceforth be used interchangeably.

Typical examples of quadratic étale $k$-algebras arise as follows.

(iv) Let $\lambda \in k$ and $D := k[t]/(t^2 - t + \lambda) = k[u]$, where $u$, the canonical image of $t$ in $D$, has trace 1 and norm $\lambda$. Then $D$ is free of rank 2 as a $k$-module, with basis $1_D, u$, hence a quadratic $k$-algebra whose norm satisfies $n_D(\alpha 1_D + \beta u) = \alpha^2 + \alpha \beta + \lambda \beta^2$ for all $\alpha, \beta \in k$. By Prop. \([22.5]\), the algebra $D$ is quadratic étale if and only if $1 - 4\lambda \in k^\times$.

(v) If $k$ contains $\frac{1}{2}$, the Cayley-Dickson construction $D := \text{Cay}(k, \mu)$ yields a quadratic algebra over $k$ with norm $n_D \cong \langle 1, -\mu \rangle$ in the sense of \([12.7]\). Moreover, $D$ is étale if and only if $\mu \in k^\times$.

\[ss.QUATALG\]

22.19. Quaternion algebras. Quaternion algebras over $k$ are defined as composition algebras of rank 4. By Cor. \([22.17]\), they are associative but not commutative. Typical examples arise from the Cayley-Dickson construction as follows:

(i) $B = \text{Cay}(D, \mu)$, $D$ a quadratic étale $k$-algebra and $\mu \in k^\times$, by Thm. \([22.10]\) is a quaternion algebra over $k$ with norm

$$n_B = n_D \oplus (-\mu)n_D = \langle 1, -\mu \rangle \otimes n_D.$$  \[QUATNOR\]

(ii) More specifically, if $\frac{1}{2} \in k$, then $B = \text{Cay}(k; \mu_1, \mu_2)$, $\mu_1, \mu_2 \in k^\times$, is a quaternion algebra over $k$ with norm

$$n_B = \langle 1, -\mu_1, -\mu_2, \mu_1 \mu_2 \rangle_{\text{quad}} \quad (1) \quad \text{QUATNOR}$$

The most prominent examples of quaternion algebras are provided by

(iv) the algebra $\text{Mat}_2(k)$ of 2-by-2 matrices over $k$, cf. Example \([22.9]\) (c), and

(v) the Hamiltonian quaternions over the field $\mathbb{R}$ of real numbers as defined in \([1.10]\).

But note that the Hurwitz quaternions of Thm. \([4.2]\), though conic associative and free of rank 4 as a $\mathbb{Z}$-module, are not a quaternion algebra over the ring of rational integers since they have discriminant 4. Instead, they belong to a wider class investigated by Loos \([72]\) under the term quaternionic algebras: associative conic algebras over a commutative ring that are finitely generated projective of rank 4 as modules.

\[ss.OCTALG\]

22.20. Octonion algebras. Octonion algebras over $k$ are defined as composition algebras of rank 8. By Cor. \([22.17]\), they are alternative but not associative. Typical examples arise again from the Cayley-Dickson construction:

(i) $C = \text{Cay}(B, \mu)$, $B$ a quaternion algebra over $k$, $\mu \in k^\times$, by Thm. \([22.10]\) is an octonion algebra over $k$ with norm

$$n_C \cong n_B \oplus (-\mu)n_B \cong \langle 1, -\mu \rangle \otimes n_B.$$  \[QUATNOR\]
(ii) \( C = \text{Cay}(D; \mu_1, \mu_2), \) \( D \) a quadratic étale \( k \)-algebra and \( \mu_1, \mu_2 \in k^\times \), is an octonion algebra with norm
\[
\eta_C = \eta_D \oplus (-\mu_1)\eta_D \oplus (-\mu_2)\eta_D \oplus (\mu_1\mu_2)\eta_D = \langle (1, -\mu_1, -\mu_2, \mu_1\mu_2) \rangle \otimes n_D.
\]

(iii) If \( \frac{1}{2} \in k \), then \( C = \text{Cay}(k; \mu_1, \mu_2, \mu_3) \), with \( \mu_1, \mu_2, \mu_3 \in k^\times \), is an octonion algebra over \( k \), whose norm is given by norm
\[
\eta_C = \langle (1, -\mu_1, -\mu_2, \mu_3, \mu_1\mu_3, \mu_2\mu_3, -\mu_1\mu_2\mu_3) \rangle_{\text{quad}} \quad (1)
\]

The most prominent example of an octonion algebra is provided by
(iv) the *Graves-Cayley octonions* \( O \) over the field \( \mathbb{R} \) of real numbers as defined in 1.4.

In a more arithmetic vein,
(v) the Coxeter octonions of Thm. 4.5 form an octonion algebra over the ring of rational integers. Since they are indecomposable as an integral quadratic lattice (cf. 4.6), they provide an example of an octonion algebra that cannot be obtained from the Cayley-Dickson construction. For other examples of this remarkable phenomenon, see Knus-Parimala-Sridharan [61] or Thakur [122].

We are not ready yet to define the notion of a split octonion algebra; this task has to be postponed to the next section.

**Exercises.**

**pr.COMPUN** 96. Let \( C \) be a unital \( k \)-algebra and \( \eta : C \to k \) a quadratic form such that all the conditions of 22.1 hold, with the possible exception of 22.1.1. Show that the following conditions are equivalent.

(i) \( C \) is a pre-composition algebra.
(ii) \( 1_C \in C \) is unimodular in the sense of 10.9
(iii) \( 1_C \in C \) is faithful in the sense of 10.9

**pr.CONIL** 97. Let \( F \) be a field. Show that a two-dimensional unital \( F \)-algebra is precisely one of the following.

(i) a separable quadratic extension field of \( F \),
(ii) split quadratic étale,
(iii) an inseparable quadratic extension field of \( F \),
(iv) isomorphic to the \( F \)-algebra of dual numbers.

Conclude that, if \( F \) is perfect of characteristic 2 and \( C \) is a conic \( F \)-algebra without nilpotent elements other than 0, then \( C \) has dimension at most 2.

**pr.COSIM** 98. Let \( F \) be a field and \( C \) a conic \( F \)-algebra whose conjugation is an involution and whose norm is a non-degenerate quadratic form. Prove that \((C, i_C)\) is simple as an algebra with involution and conclude that \( C \) is either simple or split quadratic étale.

**pr.CDDIVALG** 99. For a conic algebra over a field to be a division algebra it is necessary that its norm be anisotropic. Show that the converse of this statement does not hold, even in the finite-dimensional case, by proving *Brown’s theorem* (Brown [16, Thm. 3]): given an octonion algebra \( B \) over a field of characteristic not 2 and a non-zero scalar \( \mu \), the Cayley-Dickson construction \( C = \text{Cay}(B, \mu) \) is a division algebra if and only if \( \mu \) is not the norm of an element in \( B \) and \( -\mu \) is not the norm of a trace zero element in \( B \). In order to do so, let \( F \) be a field of arbitrary characteristic and with \( B, \mu \) as above perform the following steps.
22 Basic properties of composition algebras.

(a) Suppose $\mu \notin n_B(B^+)$. Show for $0 \neq x_i = u_i + v_j \in C$, $u_i, v_j \in B$, $i = 1, 2$ that $x_1 x_2 = 0$ if and only if $u_i \neq 0 \neq v_j$ for $i = 1, 2$ and the following relations hold.

(i) $n_B(u_1) = -\mu n_B(v_1)$,
(ii) $(u_1u_2)v_1 = -u_1(u_2v_1)$,
(iii) $v_2 = -(v_1u_2)u_1^{-1}$.

(b) Conclude from (a) that if $F$ has characteristic 2, then $C$ is a division algebra if and only if its norm is anisotropic.

(c) Suppose $\text{char}(F) \neq 2$ and $B$ is a division algebra. Then non-zero elements $x, y, z \in B$ satisfy the relation $(xy)z = -x(yz)$ if and only if there is a quaternion subalgebra $A \subseteq B$ with $x, y \in A$, $x \circ y = 0$, $z \in A^-$.

(d) Now prove Brown's theorem.

(e) Conclude from (d) that the norm of the real sedenions

$S := \text{Cay}(O; -1)$

is anisotropic but the algebra itself fails to be a division algebra.

Remark. The final statement of (e) follows also from the Bott-Milnor-Kervaire theorem $[10, 54]$ according to which finite-dimensional real division algebras exist only in dimensions $1, 2, 4, 8$. For a more precise statement about the zero divisors of $S$, see Exc. $[132]$ below.

100. Frobenius' theorem for alternative real division algebras. Prove that a finite-dimensional alternative real division algebra is isomorphic to $\mathbb{R}, \mathbb{C}, \mathbb{H}$, or $\mathbb{O}$. (Hint. Exc. $[64]$, Exc. $[80]$)

101. Isotopes and the Cayley-Dickson construction. Let $B$ be a multiplicative conic associative algebra over $k$, $\mu \in k$ and $p \in B^*$. Prove that the assignment $u + v j \mapsto p^{-1} u p + v j$ determines an isomorphism from $\text{Cay}(B, \mu)$ onto the unital isotope $\text{Cay}(B, \mu)^p$. Conclude for an octonion algebra $C$ over $k$ and $p, q \in C^*$ that the algebras $C$ and $C^{[p,q]}$ are isomorphic provided the element $pq^2$ belongs to a quaternion subalgebra of $C$.

102. Centre and nucleus of quaternion and octonion algebras.

(a) Show for a quadratic $k$-algebra $R$ and $a \in R$ that $a - \bar{a}$ is invertible if and only if $R$ is étale and generated by $a$. Show further that a quadratic étale $k$-algebra $D$ contains an element $u$ with $u - \bar{u} \in D^*$ provided $k$ is a semi-local ring. Conclude for $k$ arbitrary that $H(D, D) = k1_D$.

(b) Conclude from (a) and Cor. $[22, 16]$ that a quaternion algebra over any commutative ring $k$ is central, hence an Azumaya algebra (cf. Knus-Ojanguren $[60]$, III, §5). Prove similarly that an octonion algebra $C$ over $k$ satisfies

$$\text{Nuc}(C) = \{x \in C \mid xy = yx \text{ for all } y \in C\} = k1_C.$$

103. Automorphisms of quadratic étale algebras. Let $D$ be a quadratic étale $k$-algebra. Prove: a $k$-linear map $\varphi$: $D \to D$ is an automorphism of $D$ if and only if there exists a decomposition $k = k_+ \oplus k_-$ of $k$ as a direct sum of ideals such that the induced decompositions

$$D = D_+ \oplus D_-, \quad D_\pm := D_{k_\pm}, \quad \varphi = \varphi_+ \oplus \varphi_-, \quad \varphi_\pm := \varphi_{k_\pm}$$

satisfy $\varphi_+ = 1_{D_+}, \varphi_- = 1_{D_-}$.

104. Ideals in composition algebras (Petersson $[93]$). Let $C$ be a composition algebra over $k$ and view $k \subseteq C$ as a subalgebra in the natural way. Show that the assignments

$$a \mapsto aC, \quad I \mapsto k \cap I$$

give inclusion preserving inverse bijections between the ideals of $k$ and the ideals of $(C, \text{inv})$ as an algebra with involution. Show further that, if $C$ has rank $r \neq 2$ as a projective $k$-module, the
Peirce decomposition relative to elementary idempotents. Let $C$ be a multiplicative conic alternative algebra over $k$. If $c \in C$ is an elementary idempotent (cf. Exc. 82), put $c_1 := c, c_2 := 1_C - c, C_{ij} := C_{ij}(c)$ for $i, j = 1, 2$ and show

$$C_{ii} = kc_i$$

(i = 1, 2).  \(\text{(2)}\)

Show further for elements

$$x = \alpha_1 c_1 + x_{12} + x_{21} + \alpha_2 c_2, \quad y = \beta_1 c_1 + y_{12} + y_{21} + \beta_2 c_2,$$

in $C$, where $\alpha_i, \beta_i \in k, x_{ij}, y_{ij} \in C_{ij}$ for $i, j = 1, 2, i \neq j$ (Excs. 67-82), that

$$n_C(x) = n_C(x_1 c_1)$$

$$n_C(x, y) = \alpha_1 \beta_2 + \alpha_2 \beta_1 + n_C(x_{12}, y_{21}) + n(x_{21}, y_{12}),$$

$$l_C(x) = \alpha_1 + \alpha_2,$$

$$x = \alpha_2 c_1 - x_{12} - x_{21} + \alpha_1 c_2.$$  \(\text{(4)-(7)}\)

Moreover, if $C$ is a composition algebra, then the $k$-modules $C_{12}, C_{21}$ are in duality to each other under $Dn_C$. Finally, for $i, j = 1, 2$, the trilinear form

$$C_{ij} \rightarrow k, \quad (x, y, z) \mapsto l_C(xyz),$$

(cf. \(\text{[19,12]1}\)) is alternating.

Minimal splitting of quadratic étale algebras. Let $D$ be a quadratic étale $k$-algebra.

(a) Prove that the map $\varphi \colon D \otimes D \rightarrow D \otimes D$ defined by

$$\varphi(x \otimes d) := (xd) \oplus (\bar{xd})$$

for $x, d \in D$ is an isomorphism of $D$-algebras. (Hint. For $u \in D$ compute $\varphi(u \otimes 1_D - 1_D \otimes \bar{u})$ and $\varphi(1_D \otimes u - u \otimes 1_D)$.)

(b) Conclude from (a) that

$$\sigma := 1_D \otimes t_D : D \otimes D \rightarrow D \otimes D,$$

$$\sigma' := \varphi \circ \sigma \circ \varphi^{-1} : D \otimes D \rightarrow D \otimes D$$

are $t_D$-semi-linear involutions of $D \otimes D, D \otimes D$, respectively, with

$$\sigma'(a \otimes b) = \bar{b} \otimes \bar{a}$$

for all $a, b \in D$.

Quadratic forms permitting composition on quadratic algebras. Let $R$ be a quadratic algebra over $k$.

(a) Prove for an idempotent $e \in R$ with $n_R(e) = 0$ that

$$t_b \circ L_e : R \rightarrow k, \quad x \mapsto t_b(ex)$$

is a (possibly non-unital) algebra homomorphism.
(b) Conclude from (a) that for idempotents $e, f \in k$, $e \in R$ with $ef = 0$, $n_R(e) = 0$, the quadratic form

$$q: R \to k, \quad x \mapsto \tau_R(ex^2) + ef$$

permits composition.

(c) Let $D = k \oplus k$ be the split quadratic étale $k$-algebra. Show that a quadratic form $q: D \to k$ permits composition if and only if there exists an orthogonal system $(e_1, e_2, e_3)$ of idempotents in $k$ (possibly incomplete) such that

$$q(\alpha \oplus \beta) = e_1\alpha^2 + e_2\alpha\beta + e_3\beta^2$$

for all $\alpha, \beta, \gamma \in k$.

(d) Finally, show that if $D$ is étale, all quadratic forms on $D$ permitting composition have the form described in (b). (Hint. Reduce to the split case $D = k \oplus k$ by using (c) and Exc. 106.)

**108. Quadratic forms on composition algebras permitting composition.** Given any quadratic space $(M, Q)$ over $k$ and writing $\text{Alt}(M, Q)$ for the $k$-module of elements $f \in \text{End}_k(M)$ satisfying $Q(f(x), x) = 0$ for all $x \in M$, make use of the short exact sequence

$$0 \to \text{Alt}(M, Q) \to \text{End}_k(M) \to \text{Quad}(M) \to 0$$

to show that a quadratic form $q$ on a composition algebra $C$ of rank $r \neq 2$ over $k$ permits composition if and only if $q = \epsilon n_C$ for some idempotent $\epsilon \in k$.

**109. Embeddings into quaternion subalgebras.** Let $C$ be an octonion algebra over a semi-local ring $k$ and $R \subset C$ a quadratic subalgebra that is a direct summand of $C$ as a $k$-module. Show that there exists a quaternion subalgebra of $C$ containing $R$. (Hint. Show more precisely that there exists an element $b \in C$ making the subalgebra of $C$ generated by $R$ and $b$ a quaternion algebra and reduce this assertion to the case that $k$ is a field by arguing as in the proof of Thm. 22.15(b).)

**Remark.** Over fields, the preceding result amounts to [121] Prop. 1.6.4: every element of an octonion algebra over field can be embedded into a quaternion subalgebra.

**110. Reflections and involutions of composition algebra.** (cf. Jacobson [41] and Racine-Zel’manov [110]) Let $k$ be a commutative ring containing $\frac{1}{2}$ and $C$ a composition algebra of rank $r > 1$ over $k$.

(a) Let $\sigma$ be a reflection of $C$, i.e., an automorphism of order 2. Show that its fixed algebra $\text{Fix}(\sigma) := \{ x \in C \mid \sigma(x) = x \} \subset C$ is a composition subalgebra of rank $\frac{1}{2}$ and that the assignment $\sigma \mapsto \text{Fix}(\sigma)$ determines a bijection from the set of reflections of $C$ onto the set of composition subalgebras of $C$ having rank $\frac{1}{2}$. Show further that two reflections of $C$ are conjugate under $\text{Aut}(C)$ if and only if their fixed algebras are.

(b) Show that an involution of $C$ commutes with its conjugation. Use this and (a) to set up a bijective correspondence between the set of involutions of $C$ that are distinct from its conjugation (resp. the set of their isomorphism classes) and the set of composition subalgebras of $C$ having rank $\frac{1}{2}$ (resp. the set of their conjugacy classes under $\text{Aut}(C)$). Finally, show for an involution $\tau \neq 1_C$ of $C$ that $H(C, \tau) \subset C$ is a finitely generated projective submodule of rank $\frac{1}{2} + 1$.

23. Hermitian forms

Before being able to proceed with the study of composition algebras, it will be necessary to insert a few basic facts about hermitian forms over commutative rings that will be useful not only in the present context but also for cubic Jordan algebras.
later on. A systematic account of the subject may be found in Knus [58] or Hahn-O’Meary [38].

Throughout we let \( k \) be an arbitrary commutative ring and \((B, \tau)\) an associative algebra with involution over \( k \) in the sense of §11. In particular, \( B \) contains an identity element. We also write \( \bar{x} := \tau(x) \) for \( x \in B \).

### 23.1. Passing from left to right modules and conversely.

Any left \( B \)-module \( M \) may be converted into a right \( B \)-module by defining \( xa := \bar{a}x \) for \( x \in M \) and \( a \in B \). We denote this right module by \( M^\tau \). A \( B \)-linear map \( f : M \to N \), \( x \mapsto (x)f \), of left \( B \)-modules may be viewed as a \( B \)-linear map \( f^\tau : M^\tau \to N^\tau \) of right \( B \)-modules, so we have \( f^\tau(x) = (x)f \) for all \( x \in M^\tau \). The preceding conventions make equally good sense with left and right modules interchanged. We then have \( M^{\tau\tau} = M \) for any left (right) module \( M \) over \( B \) and \( f^{\tau\tau} = f \) for any \( B \)-linear map \( f : M \to N \) of left (right) \( B \)-modules.

Writing \( _BB \) (resp. \( B_\)B) for \( B \) viewed as a left (resp. right) \( B \)-module, \( \tau : (_BB)^\tau \to B_\)B is a linear bijection of right \( B \)-modules. Hence, if a left \( B \)-module is (finitely generated) projective (resp. free), then so is \( M^\tau \) as a right \( B \)-module, and conversely.

### 23.2. The twisted dual of a module.

Let \( M \) be a right \( B \)-module. Then the additive group \( M^* := \text{Hom}_B(M, B) \) canonically becomes a left \( B \)-module if one defines \( ax^* : M \to B \) by \( (ax^*)(y) := ax^*(y) \) for \( a \in B, x^* \in M^* \) and \( y \in M \). Using the formalism of 23.1, we may then convert the left \( B \)-module \( M^* \) into the right \( B \)-module \( M^{\tau*} \), which we call the \( \tau \)-twisted dual, or simply the twisted dual, of \( M \). Note that for \( B \) commutative and \( \tau = 1_B \), the terms “right \( B \)-module” and “left \( B \)-module” may be used interchangeably, and the twisted dual of \( M \) agrees with the ordinary dual as defined in 10.9. On the other hand, if \( (B \) still being commutative \( ) \) is not the identity, the twisted dual and the ordinary dual are different notions. However, it will always be clear from the context which one of the two we have in mind.

For any right \( B \)-module \( M \), we have its canonical pairing

\[
\text{cap}_M : M^* \times M \to B, \quad (x^*, y) \mapsto \langle x^*, y \rangle := x^*(y),
\]

which is anti-linear in the first variable and linear in the second:

\[
\langle x^*a, yb \rangle = \bar{a}\langle x^*, y \rangle b \quad (a, b \in B, x^* \in M^*, y \in M).
\]

If \( f : M \to N \) is a linear map of right \( B \)-modules, then the assignment \( y^* \mapsto y^* \circ f \) defines a linear map \( f^* : N^* \to M^* \), called the adjoint of \( f \) because it is characterized by the relation

\[
\langle f^*(y^*), x \rangle = \langle y^*, f(x) \rangle \quad (y^* \in N^*, x \in M).
\]

In this way, we obtain a contravariant additive functor from the category of right \( B \)-modules to itself.
23.3. Sesquilinear forms. By a sesquilinear form over $B$ we mean a bi-additive map $h: M \times N \to B$, where $M, N$ are right $B$-modules such that $h(xa, yb) = \overline{ah(x,y)b}$ for all $a, b \in B$ and all $x \in M, y \in N$. In this case, we define the adjoint map or simply the adjoint of $h$ as the $B$-linear map

$$\varphi_h: M \to N^*, \quad x \mapsto \varphi_h(x) := h(x, -).$$

Conversely, given a $B$-linear map $\varphi: M \to N^*$, we obtain a sesquilinear form $h_\varphi: M \times N \to B$ via $h_\varphi(x, y) := \langle \varphi(x), y \rangle$ for $x \in M, y \in N$, and the two constructions are inverse to each other.

As an example, let $M$ be any right $B$-module. Then the canonical pairing of $(23.2)[1]$ by $(23.2)[2]$ is a sesquilinear form over $B$ whose adjoint map $M^* \to M^*$ is the identity on $M^*$.

23.4. Base change. For $R \in k$-alg, we can form the base change $(B, \tau) = (B_R, \tau_R)$, which is an associative algebra with involution over $R$, and for a right $B$-module $M$, the $R$-module $M_R = M \otimes B_R$ becomes a right $B_R$-module in a natural way. If $f: M \to N$ is a homomorphism of right $B$-modules, then its $R$-linear extension $f_R: M_R \to N_R$ is in fact one of right $B_R$-modules.

For $x^* \in M^*$, we clearly have $x^* \otimes 1_R \in (M_R)^*$, and the assignment $x^* \mapsto x^* \otimes 1_R$ gives a $k$-linear map $M^* \rightarrow (M_R)^*$, which in turn induces an $R$-linear map

$$\phi: (M^*)_R \rightarrow (M_R)^*, \quad x^* \otimes r \mapsto r(x^* \otimes 1_R).$$

This map is, in fact, a homomorphism of right $B_R$-modules and will henceforth be referred to as the canonical homomorphism from $(M^*)_R$ to $(M_R)^*$.

Any sesquilinear form $h: M \times N \to B$ over $B$ yields canonically an extended sesquilinear form $h_R: M_R \times M_R \to B_R$ over $B_R$, called the base change or scalar extension of $h$ from $k$ to $R$, such that the diagram

\[
\begin{array}{ccc}
M_R & \xrightarrow{(\varphi_h)_R} & (N^*)_R \\
\downarrow \varphi(\varphi) & & \downarrow \\
(N_R)^* & \text{(ADBA)} & \\
\end{array}
\]

commutes, where the vertical arrow refers to the canonical homomorphism from $(N^*)_R$ to $(N_R)^*$.

23.5. Sesquilinear modules. By a sesquilinear module over $B$, we mean a pair $(M, h)$ consisting of a right $B$-module $M$ and a sesquilinear form $h: M \times M \to B$. Given two sesquilinear modules $(M, h)$ and $(M', h')$ over $B$, a homomorphism from $(M, h)$ to $(M', h')$ (or from $h$ to $h'$) is a $B$-linear map $f: M \to M'$ preserving sesquilinear forms in the sense that $h' \circ f \times f = h$. In this way one obtains the category of sesquilinear modules over $D$. Isomorphisms in this category are called isometries.
23.6. Sesquilinear forms and matrices. Let \( p, q \) be positive integers. Viewing \( M := B^p \), \( N := B^q \) as free right \( B \)-modules in the natural way, every matrix \( T \in \text{Mat}_{p,q}(B) \) determines a sesquilinear form
\[
\langle T \rangle_{\text{sesq}} : B^p \times B^q \rightarrow B, \quad (x,y) \mapsto \bar{x}^tTy,
\]
and every sesquilinear form on \( B^p \times B^q \) can be written uniquely in this way. Identifying a vector \( x \in B^q \) with the linear form \( B^q \rightarrow B \), \( y \mapsto \bar{x}^t y \), we obtain an identification \( B^q = B^q \ast \). The adjoint of \( \langle T \rangle_{\text{sesq}} \) then agrees with the linear map \( \bar{T}^t : B^p \rightarrow B^q \).

23.7. The double dual. Given a right \( B \)-module \( M \), we obtain a natural \( B \)-linear map \( \text{can}_M : M \rightarrow M^{**} \) determined by the condition
\[
\text{can}_M(x)(y^\ast) := \langle y^\ast, x \rangle \quad (x \in M, y^\ast \in M^\ast).
\]
In important cases, \( \text{can}_M \) is an isomorphism. For example, if \( M = B^n \), then \( B^{n**} = B^n \) and \( \text{can}_M = 1_{B^n} \) under the identifications of 23.6. Now let \( h : M \times M \rightarrow B \) be a sesquilinear form. Then so is \( h^\ast : M \times M \rightarrow B \) defined by \( h^\ast(x,y) := \bar{h}(y,x) \) for \( x,y \in M \), and the adjoints of \( h, h^\ast \) are related to one another by the commutative diagram
\[
\begin{array}{ccc}
M & \xrightarrow{\text{can}_M} & M^\ast \\
\downarrow{\text{can}_M^\ast} & & \downarrow{(h^\ast)^\ast} \\
M^{**} & & 
\end{array}
\]
Hence if \( \text{can}_M \) is bijective, allowing us to identify \( M = M^{**} \) accordingly, the adjoint of \( h^\ast \) agrees with the adjoint of the adjoint of \( h \).

23.8. Hermitian forms. By a hermitian form on a right \( B \)-module \( M \) we mean a sesquilinear form \( h : M \times M \rightarrow B \) satisfying \( h(y,x) = \bar{h}(x,y) \) for all \( x,y \in M \); this is equivalent to \( h = h^\ast \). For \( T \in \text{Mat}_{p,q}(B) \), we obtain \( (\langle T \rangle_{\text{sesq}})^\ast = (\bar{T}^t)_{\text{sesq}} \), so \( \langle T \rangle_{\text{sesq}} \) is a hermitian form if and only if \( T = T^\dagger \) is a hermitian matrix. By a hermitian module we mean a pair \( (M, h) \) consisting of a right \( B \)-module \( M \) and a hermitian form \( h : M \times M \rightarrow B \). We view hermitian modules as a full subcategory of sesquilinear modules.

24. Ternary hermitian spaces

The Cayley-Dickson construction discussed in some of the preceding sections is not an appropriate tool when dealing with octonion algebras that fail to contain any quaternion subalgebras. In the sequel, we therefore propose a different method of constructing composition algebras which is due to Thakur [122] over rings containing \( \frac{1}{2} \) and has been sketched by the author [100] over fields of arbitrary character-
The main constituents of this construction are quadratic étale algebras and ternary hermitian spaces. They always lead to octonion algebras and, conversely, every octonion algebra containing a quadratic étale subalgebra arises in this manner; in particular, this holds true for the Graves-Cayley octonions over the reals as defined in [14] and for arbitrary octonion algebras over any commutative ring that contains 2 in its Jacobson radical (cf. Prop. 24.16 below). A slight generalization of our method leads to a similar construction of quaternion algebras due to to Pumplün [107] provided \( \frac{1}{2} \) belongs to the base ring. Both constructions, the octonionic as well as the quaternionic one, will be treated here in a unified fashion.

In this section, we fix a composition algebra \( D \) of rank at most 2 over an arbitrary commutative ring \( k \). By Cor. 22.17 \( D \) is commutative associative and is endowed with its canonical involution, which we abbreviate as \( t := t_D, a \mapsto \bar{a} \). The set-up of the preceding section may thus be specialized to \( (B, t) := (D, t) \). By Exc. 102 we can identify \( k = H(D, t) \) as a unital subalgebra of \( D \), and this identification is compatible with base change.

### 24.1. Some useful identifications

Fix \( R \in k\text{-alg} \) and let \( M \) be a right \( D \)-module. Then we obtain a natural identification

\[
M_R = M \otimes R = M \otimes_D (D \otimes R) = M_{DR}
\]

as right \( D_R \)-modules such that

\[
x \otimes r = x \otimes_D (1_D \otimes r), \quad x \otimes_D (a \otimes r) = (xa) \otimes r \quad (x \in M, \; r \in R, \; a \in D),
\]

ditto for left \( D \)-modules. It follows that, if \( M \) is finitely generated projective over \( D \), then so is \( M_R \) over \( D_R \).

Now suppose that \( M \) is a left \( D \)-module. Since \( M^t = M \) as \( k \)-modules, we obtain a canonical identification \( (M^t)_R = (M_R)^t \), and (1) yields an identification \( (M^t)_R = (M_{DR})^{\text{op}} \) as right \( D_R \)-modules matching \( x \otimes_D (a \otimes r) \) in \( (M^t)_R \) with \( x \otimes_D (a \otimes r) \) in \( (M_{DR})^{\text{op}} \), for \( x \in M, \; a \in D, \; r \in R \).

Combining the previous identifications with 23.4 and Lemma 10.11 we obtain

### 24.2. Lemma

Let \( M \) be a finitely generated projective right \( D \)-module and \( R \in k\text{-alg} \). Then the canonical homomorphism

\[
(M^*)_R \longrightarrow (M_R)^*, \quad x^* \otimes r \longmapsto r(x^* \otimes 1_R),
\]

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

---

\(^3\) If I remember correctly, Harald Holmann from the University of Fribourg (Switzerland), in his Fernstudienkurs “Aufbau des Zahlsystems” written in the early 1980ies for the Department of Mathematics of Fernuniversität, used this method to construct the Graves-Cayley octonions over the reals. This should be checked, and the appropriate historical context should be investigated.
24.3. **Non-singular sesquilinear forms.** A sesquilinear form \( h: M \times N \to D \) over \( D \) with right \( D \)-modules \( M, N \) is said to be **non-singular** if \( M \) and \( N \) are both finitely generated projective and the adjoint \( \varphi_h: M \to N^* \) is an isomorphism. Note that for \( h \) to be non-singular it is necessary that \( M \) and \( N \) be finitely generated projective right \( D \)-modules having the same rank function. Combining (23.4.1) with Lemma 24.2, we see that the property of a sesquilinear form to be non-singular is stable under base change. By a **sesquilinear** (resp. **hermitian**) space over \( D \) we mean a sesquilinear (resp. hermitian) module \((M, h)\) such that the sesquilinear (resp. hermitian) form \( h: M \times M \to D \) is non-singular. Given a positive integer \( n \), we speak of a **hermitian space of rank** \( n \) if the underlying module has rank \( n \) as a finitely generated right \( D \)-module.

24.4. **Exterior powers.** Let \( M, N \) be right \( D \)-modules and \( h: M \times N \to D \) a sesquilinear form. Given a positive integer \( n \), we may pass to the \( n \)-th exterior power

\[
\bigwedge^n h: \bigwedge^n M \times \bigwedge^n N \to D
\]

(well) defined by

\[
(\bigwedge^n h)(x_1 \wedge \cdots \wedge x_n, y_1 \wedge \cdots \wedge y_n) = \det \left( h(x_i, y_j) \right)_{1 \leq i, j \leq n}
\]

for \( x_i \in M, y_j \in N, 1 \leq i, j \leq n \). We call \( \bigwedge^n h \), which is again a sesquilinear form over \( D \), the **\( n \)-th exterior power** of \( h \). Passing to the adjoint maps, we conclude that the diagram

\[
\begin{array}{ccc}
\bigwedge^n M & \xrightarrow{\bigwedge^n \varphi_h} & \bigwedge^n (N^*) \\
\downarrow{\varphi_{\bigwedge^n h}} & & \downarrow{\Phi_{\bigwedge^n (N^*)}} \\
(\bigwedge^n N)^* & & \\
\end{array}
\]

commutes. Since exterior powers of right \( D \)-modules commute with base change (Bourbaki [12, III, § 7, Prop. 8]), so do exterior powers of sesquilinear forms.

24.5. **Lemma.** If \( h: M \times N \to D \) is a non-singular sesquilinear form over \( D \), then so is its \( n \)-th exterior power, for any positive integer \( n \).

**Proof.** it suffices to show that the vertical arrow in (24.4.2) is an isomorphism. Since \( N \) is finitely generated projective over \( D \), we may assume that it is free of finite rank \( p \geq n \). Let \( (e_i)_{1 \leq i \leq p} \) be a \( k \)-basis of \( N \) and \( (e_i')_{1 \leq i \leq p} \) the corresponding dual basis of \( N^* \). Then

\[
(e_{j_1} \wedge \cdots \wedge e_{j_n})_{1 \leq j_1 < \cdots < j_n \leq p}
\]

is a \( k \)-basis of \( \bigwedge^n N \), while
is a spanning family of $\bigwedge^n(N^*)$ as a right $D$-module such that
\[
(\varphi_{\bigwedge^n N}(e_{i_1} \wedge \cdots \wedge e_{i_n}))(e_{j_1} \wedge \cdots \wedge e_{j_n}) = \det((\langle e_{i_k}^*, e_{j_\mu} \rangle)_{1 \leq k, \mu \leq n}),
\]
which is 1 for $(i_1, \ldots, i_n) = (j_1, \ldots, j_n)$ and 0 otherwise. Thus $\varphi_{\bigwedge^n N}$ maps the spanning family (2) of $\bigwedge^n(N^*)$ onto the dual of the basis (1) of $\bigwedge^n N$, hence must be an isomorphism. □

24.6. Remark. Let $M$ be a finitely generated projective right $D$-module and $n$ a positive integer. Then the preceding result (or its proof) yields an identification $\bigwedge^n(M^*) = (\bigwedge^n M)^*$ such that the canonical pairing
\[
\bigwedge^n(M^*) \times \bigwedge^n M = (\bigwedge^n M)^* \times \bigwedge^n M \rightarrow D
\]
is given by
\[
\langle x_1^* \wedge \cdots \wedge x_n^*, y_1 \wedge \cdots \wedge y_n \rangle = \det((\langle x_i^*, y_j \rangle)_{1 \leq i, j \leq n})
\]
for $x_1^*, \ldots, x_n^* \in M^*$, $y_1, \ldots, y_n \in M$.

24.7. Determinants. Let $(M, h)$ be a hermitian space of rank $n$ over $D$. An isomorphism $\Delta : \bigwedge^n V \rightarrow D$ may not exist but if it does, we follow Loos-Petersson-Racine [73, 4.3] and call it an orientation of $M$; it is unique up to an invertible factor in $D$. Given an orientation $\Delta : \bigwedge^n V \rightarrow D$, there exists a unique element $\det_{\Delta}(h) \in k^\times$, called the $\Delta$-determinant of $h$, such that $\Delta : \bigwedge^n(M, h) \rightarrow (D, \langle \det_{\Delta}(h) \rangle_{\text{sesq}})$ is an isometry. The $\Delta$-determinant changes with $\Delta$ according to the rule
\[
\det_{\omega\Delta}(h) = n_D(a)^{-1} \det_{\Delta}(h) \quad (a \in D^\times). \tag{1}
\]
If $M$ is free of rank $n$ as a right $D$-module with basis $(e_i)$ and $T = (h(e_i, e_j)) \in \text{GL}_n(D)$ stands for the corresponding hermitian matrix, then $\det_{\Delta}(h) = \det(T)$, where $\Delta : \bigwedge^n M \rightarrow D$ is the orientation normalized by $\Delta(e_1 \wedge \cdots \wedge e_n) = 1$.

24.8. Ternary hermitian spaces and the hermitian vector product. Let $(M, h)$ be a hermitian space over $D$ which is ternary in the sense that it has rank $n = 3$ and suppose $\Delta : \bigwedge^3 M \rightarrow D$ is an orientation of $M$. By non-singularity of $h$, there exists a unique map $M \times M \rightarrow M, (x, y) \mapsto x \times_{h, \Delta} y$, such that
\[
h(x \times_{h, \Delta} y, z) = \Delta(x \wedge y \wedge z). \quad (x, y, z \in M)
\]
We call $\times_{h, \Delta}$ the hermitian vector product induced by $h$ and $\Delta$. It is obviously bi-additive, alternating and anti-linear in both arguments. Moreover, the expression $h(x \times_{h, \Delta} y, z)$ remains unaffected by a cyclic change of variables and vanishes if two of them coincide.
24.9. Example. In keeping with the previous conventions, we regard $D^3$ as a free right $D$-module of rank 3 that is equipped with the canonical basis $(e_1, e_2, e_3)$ of ordinary unit vectors, and denote by $x \times y$ the usual vector product of $x, y \in D^3$, as defined [1.1] for the special case $k = \mathbb{R}, D = \mathbb{C}$. It satisfies the Grassmann identity (1.1.3), i.e.,

\[(x \times y) \times z = y(z \times x) - x(z \times y),\]

(1) \[\text{GRARE}\]

but also

\[(Sx) \times (Sy) = (S^T)^\dagger (x \times y)\]

(2) \[\text{MAVE}\]

for all $x, y, z \in D^3$ and all $S \in \text{Mat}_3(D)$, where $S^T \in \text{Mat}_3(D)$ stands for the usual adjoint of $S$ in the sense of linear algebra.

Now suppose $T \in \text{GL}_3(D)$ is a hermitian matrix and consider the ternary hermitian space $(D^3, \langle T \rangle_{\text{sesq}})$. Writing $\Delta_0 : \wedge^3 D^3 \to D$ for the ordinary determinant, i.e., for the orientation normalized by $\Delta_0(e_1 \wedge e_2 \wedge e_3) = 1$, any other volume element on $D^3$ has the form $\Delta = a\Delta_0$ for some $a \in D^\times$, and it is easily checked that the hermitian vector product induced by $\langle T \rangle_{\text{sesq}}$ and $\Delta$ relates to the ordinary one according to the formula

\[x \times \langle T \rangle_{\text{sesq}} \Delta y = T^{-1}(\bar{x} \times \bar{y})\bar{a} = (\bar{T}x \times \bar{T}y)\det(T)^{-1}\bar{a}.\]

(3) \[\text{HEROR}\]

**24.10. Proposition.** Let $(M, h)$ be a ternary hermitian space over $D$ and suppose $\Delta : \wedge^3 M \to D$ is a volume element of $M$. Then the hermitian vector product induced by $h$ and $\Delta$ satisfies the hermitian Grassmann identity

\[(x \times_{h, \Delta} y) \times_{h, \Delta} z = (yh(z, x) - xh(z, y))\det_\Delta(h)^{-1} (x, y, z \in M).\]

(1) \[\text{HERGRAS}\]

**Proof.** The question is local on $D$, so we may assume $M = D^3, h = \langle T \rangle_{\text{sesq}}, \Delta = a\Delta_0$ as in Example [24.9]. Then the assertion follows from [24.7][1], [24.9][1], [24.9][3] by a straightforward computation. \[\square\]

We will now be able to derive the first main result of this section. It turns out to be a direct generalization of the construction leading to the Graves-Cayley octonions (1.4) and to Thm. 1.7.

**24.11. Theorem** (Thakur [122]). Let $D$ be a non-singular composition algebra of rank $r \leq 2$ over $k$, $(M, h)$ a ternary hermitian space over $D$ and suppose $\Delta : \wedge^3 M \to D$ is an orientation of $M$ satisfying $\det_\Delta(h) = 1$. Then the $k$-module $D \otimes M$ becomes a composition algebra over $k$ under the multiplication

\[(a \oplus x)(b \oplus y) := (ab - h(x, y)) \oplus (yx + xb + x \times_{h, \Delta} y)\]

(1) \[\text{TEMU}\]

for $a, b \in D, x, y \in M$. Identifying $k \subseteq D$ canonically, this composition algebra, written as...
has unit element, norm, linearized norm, trace, conjugation given by

\[ 1_C = 1_D \oplus 0, \]
\[ n_C(a \oplus x) = n_D(a) + h(x,x), \]
\[ n_C(a \oplus x, b \oplus y) = n_D(a,b) + t_D(h(x,y)), \]
\[ t_C(a \oplus x) = t_D(a), \]
\[ a \oplus x = \bar{a} \oplus (-x) \]

for all \( a, b \in D, x, y \in M. \)

**Proof.** \( C \) is clearly a \( k \)-algebra with unit element given by \((\text{I})\), and it follows from Exc.\((\text{II})\) below that the quadratic form \( n_C : C \to k \) as defined in \((\text{II})\), which trivially satisfies \((\text{III})\), is non-singular. Therefore the theorem will follow once we have shown that \( n_C \) permits composition relative to the multiplication \((\text{IV})\). Accordingly, using standard properties of the hermitian vector product \((24.8)\), we expand

\[ n_C((a \oplus x)(b \oplus y)) = n_C((ab - h(x,y)) \oplus (y\bar{a} + xb + x \times h_{\Delta} y)) \]
\[ = n_D(ab) - n_D(ab, h(x,y)) + n_D(h(x,y)) \]
\[ + h(y\bar{a} + xb + x \times h_{\Delta} y, y\bar{a} + xb + x \times h_{\Delta} y) \]
\[ = n_D(a)n_D(b) - n_D(ab, h(x,y)) + n_D(h(x,y)) \]
\[ + n_D(a)h(y,y) + abh(y,x) + \bar{a}bh(x,y) \]
\[ + n_D(b)h(x,x) + h(x \times h_{\Delta} y, x \times h_{\Delta} y). \]

Here \( abh(y,x) + \bar{a}bh(x,y) = n_D(ab, h(x,y)) \) by \((19.5)\), \((19.11)\), and the hermitian Grassmann identity \((24.10)\) yields

\[ h(x \times h_{\Delta} y, x \times h_{\Delta} y) = h(y, x \times h_{\Delta} y) \]
\[ = h(y, yh(x,x) - xh(x,y)) \]
\[ = h(x,x)h(y,y) - n_D(h(x,y)). \]

Hence \( n_C \) does indeed permit composition relative to \((\text{I})\) and the proof is complete. \( \square \)

**24.12. The ternary hermitian construction.** The composition algebra

\[ C = \text{Ter}(D; M, h, \Delta) \]

obtained in Thm.\((24.1)\) is said to arise from the parameters involved by means of the ternary hermitian construction. Note that \( C \) has rank \( 4r \). After the canonical identification \( a = a \oplus 0 \) for \( a \in D \), the composition algebra \( C \) contains \( D \) as a composition subalgebra. The entire construction will now be reversed by showing that any com-
position algebra containing $D$ as a composition subalgebra arises from $D$ by means of the ternary hermitian construction.

24.13. Theorem (Thakur [122]). Let $C$ be a composition algebra of rank $4r$ over $k$ containing $D$ as a non-singular composition subalgebra of rank $r \leq 2$. Then there exist a ternary hermitian space $(M, h)$ over $D$ and an orientation $\Delta : \wedge^3 M \to D$ satisfying $\det_\Delta(h) = 1$ such that the inclusion $D \hookrightarrow C$ extends to an isomorphism from $\text{Ter}(D; M, h, \Delta)$ onto $C$.

Proof. Identifying $k = k_1 \subseteq C$ throughout, we proceed in several steps.

1. Since $n_C$ is non-singular on $D$, Lemma 12.10 yields a decomposition

$$C = D \oplus M, \quad M = D^\perp$$

(1)

as a direct sum of $k$-submodules. Associativity of the norm ((19.11.3), (19.11.4)) implies $MD \subseteq M$ and we claim that $M$ becomes a right $D$-module in this way.

Localizing if necessary we may assume that $D$ is generated by a single element (Thm. 22.15 (b)), in which case the assertion follows immediately from the alternative law. We also observe $M \subseteq \text{Ker}(\iota_C)$ and

$$ax = x\bar{a} \quad (x \in M, a \in D)$$

(2)

since $ax + xa = t_D(a)x$ by (19.5.5) and (1).

2. Next we define $k$-bilinear maps $h : V \times V \to D, \times_D : M \times M \to M$ by

$$xy = -h(x, y) + x \times_D y, \quad h(x, y) \in D, \quad x \times_D y \in M,$$

(3)

for all $x, y \in M$. From $x^2 = -n_C(x)$ we conclude

$$n_C(x) = h(x, x)$$

(4)

and that the map $\times_D$ is alternating. Moreover, $\overline{xy} = y\overline{x} = (-y)(-x) = yx$ yields

$$\overline{h(x, y)} = h(y, x),$$

(5)

hence

$$n_C(x, y) = t_D(h(x, y)).$$

(6)

In particular, $h(x, y) = 0$ for all $y \in M$ implies $x = 0$.

3. We claim that $(M, h)$ is a hermitian module over $D$. By (5), it suffices to show that $h$ is linear in the second variable. Using (19.11.3), (19.11.4) repeatedly and observing that $M$ is a right $D$-module by 1, we obtain $n_C(x(yb), a) = n_C((xy)b, a)$ for all $x, y \in M, a, b \in D$, and 3 in conjunction with non-singularity of $n_D$ gives the assertion.

4. Consider the $k$-trilinear map $\delta : M^3 \to D$ defined by $\delta(x, y, z) = h(x \times_D y, z)$, which by 3 is $D$-linear in $z$. We clearly have $\delta(x, x, z) = 0$, but also $\delta(x, y, y) = 0$.
since \( \mathbf{2}, \mathbf{3} \) imply \((x \times_D y) y = h(x, y) y + xy^2 = yh(x, y) - n_C(y) x \in M\). Hence \( \delta \) is alternating, forcing it to be in fact \( D\)-trilinear, and we obtain a unique \( D\)-linear map \( \Delta : \Lambda^3 \ M \rightarrow D \) satisfying
\[
\Delta(x \wedge y \wedge z) = h(x \times_D y, z).
\]
\[(x, y, z \in M) \tag{7} \]

5\. We now show that \((M, h)\) is a ternary hermitian space over \(D\), \( \Delta : \Lambda^3 \ M \rightarrow D \) is an orientation of \(M\) satisfying \(\det_3(h) = 1\) and \(\times_D\) is the hermitian vector product induced by \(h\) and \(\Delta\). The final statement follows immediately from \(\mathbf{7}\) as soon as the preceding ones have been established. To do so, we may assume that \(k\) is a local ring, forcing \(C\) to arise from \(D\) by a twofold application of the Cayley-Dickson construction (Cor. \[\mathbf{22.16}\]): there are units \(\mu_1, \mu_2 \in k\) satisfying
\[
C = \text{Cay}(D; \mu_1, \mu_2) = D \oplus D j_1 \oplus D j_2 \oplus D j_3,
\]
where \(j_1 \in D^\perp = M\) satisfies \(n_C(j_1) = -\mu_1\), \(j_2 \in (D \oplus D j_1)^\perp\) satisfies \(n_C(j_2) = -\mu_2\), and \(j_3 = j_1 j_2\). Hence, by \(\mathbf{2}\),
\[
M = j_1 D \oplus j_2 D \oplus j_3 D.
\]

More precisely, \(\mathbf{3}, \mathbf{4}\) and the relations \(j_1 j_2 = j_3 \in M\), \(j_1 j_3 = \mu_1 j_2 \in M\), \(j_2 j_3 = \mu_2 j_1 \in M\) show that \((j_1, j_2, j_3)\) is a basis of \(M\) over \(D\) with respect to which the matrix of \(h\) has the form \(\text{diag}(-\mu_1, -\mu_2, \mu_1 \mu_2) \in \text{GL}_3(D)\). Hence \((M, h)\) is a ternary hermitian space over \(D\); moreover, \(j_1 \times_D j_2 = j_3\) by \(\mathbf{5}\). Thus \(\mathbf{7}\) gives \(\Delta(j_1 \wedge j_2 \wedge j_3) = h(j_3, j_3) = \mu_1 \mu_2 \in k^\times\), so \(\Delta\) is indeed an orientation of \(M\). The remaining assertion \(\det_3(h) = 1\) is now straightforward to check.

6\. In view of \(5\) we can form the composition algebra \(C' := \text{Ter}(D; V, h, \Delta)\) and our construction yields a natural identification \(C = C'\) matching \(D\) with the first summand of \(C'\). \[\square\]

24.14. Corollary (Pumplün \[\mathbf{107}\]). For \(\frac{1}{2} \in k\), every quaternion algebra over \(k\) has the form \(\text{Ter}(k; M, \beta, \Delta)\), where \((M, \beta)\) is a ternary symmetric bilinear space over \(k\) and \(\Delta\) is a volume element of \(M\) satisfying \(\det_3(\beta) = 1\). Conversely, every such algebra is a quaternion algebra. \[\square\]

24.15. Example. Working over the field \(k = \mathbb{R}\) of real numbers, we have
\[
\mathcal{O} = \text{Ter}(\mathbb{C}; \mathbb{C}^3, \{1_3\}_{\text{sesq}}, \Delta_0), \quad \mathbb{H} = \text{Ter}(\mathbb{R}; \mathbb{R}^3, \{1_3\}, \Delta_0),
\]
where \(\Delta_0\) is the normalized orientation of \(\mathbf{24.9}\).

The Coxeter octonions and the examples of Knus-Parimala-Sridharan \[\mathbf{61}\] (see also Thakur \[\mathbf{122}\]) show that there are octonion algebras to which the ternary hermitian construction does not apply since they do not contain any quadratic étale subalgebras. On the other hand, if \(2 \in k\) is sufficiently far removed from being a unit, then quadratic étale subalgebras always exist.
24.16. Proposition. Let \( C \) be a composition algebra of rank \( r > 1 \) over \( k \) and assume \( 2 \in k \) is contained in the Jacobson radical of \( k \) (e.g., \( 2 = 0 \) in \( k \)). Then \( C \) contains quadratic étale subalgebras.

Proof. By Lemma 22.11, \( C \) contains an element \( u \) of trace 1. Then \( t_C(u)^2 - 4n_C(u) = 1 - 4n_C(u) \in k^\times \) by hypothesis, so \( k[u] \subseteq C \) is a quadratic étale subalgebra by Prop. 22.5.

24.17. Zorn vector matrices. Let \( D := k \oplus k \) be the split quadratic étale \( k \)-algebra. Then \( \iota = \iota_D \) is the exchange involution, and the free right \( D \)-module \( D_3 = k^3 \oplus k^3 \) is endowed with the normalized orientation \( \Delta : \wedge^3 D_3 \to D \) as in 24.7 and with the unit hermitian form \( h := \langle 1_3 \rangle_{\text{sesq}} \) which satisfies \( \det \Delta(h) = 1 \). Hence we may form the octonion algebra

\[
C := \text{Ter}(D; D_3, h, \Delta)
\]

over \( k \), which may now be described more explicitly as follows.

Writing elements \( a, b \in D, x, y \in D_3 \) as

\[
a = \alpha_1 \oplus \alpha_2, \quad b = \beta_1 \oplus \beta_2, \quad x = u_1 \oplus u_2, \quad y = v_1 \oplus v_2 \tag{1}
\]

with \( \alpha_i, \beta_i \in k, u_i, v_i \in k^3, i = 1, 2, \) we have

\[
h(x, y) = u_1^t u_2^t (v_1 \oplus v_2) = (u_2 \oplus u_1)^t (v_1 \oplus v_2),
\]

hence

\[
h(x, y) = (u_2^t v_1) \oplus (u_1^t v_2), \tag{2}
\]

and applying (24.9.3), we obtain

\[
x \times_h \Delta y = \bar{x} \times \bar{y} = (u_2 \times v_2) \oplus (u_1 \times v_1). \tag{3}
\]

Visualizing the elements of \( C = D \oplus D_3 \) in matrix form as

\[
a \oplus x = \begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix}, \quad b \oplus y = \begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix},
\]

we deduce from (24.11.1), (3), (5) that

\[
\begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \beta_1 - u_2^t v_1 & \alpha_4 v_2 + \beta_2 u_2 + u_1 \times v_1 \\ \alpha_2 v_1 + \beta_2 u_2 + u_1 \times v_1 & \alpha_2 \beta_2 - u_2^t v_1 \end{pmatrix}. \tag{4}
\]

Consulting Thm. 24.11 we therefore conclude that the multiplication rule (4) converts the \( k \)-module

\[
\text{Zor}(k) := \begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix}
\]

(5)
into an octonion algebra, called the octonion algebra of Zorn vector matrices over $k$. Norm, trace and conjugation of this octonion algebra are given by

$$n_{\text{Zor}} \left( \begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix} \right) = \alpha_1 \alpha_2 + u_1' u_2$$

(6) \hspace{1cm} \text{ZONO}

$$t_{\text{Zor}} \left( \begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix} \right) = \alpha_1 + \alpha_2$$

(7) \hspace{1cm} \text{ZOTR}

$$\begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_2 & -u_2 \\ -u_1 & \alpha_1 \end{pmatrix}$$

(8) \hspace{1cm} \text{ZOCONJ}

24.18. Split composition algebras. Let $C$ be a composition algebra over $k$. We say that $C$ is

(a) split of rank 1 if $C \cong k$,

(b) split of rank 2 or split quadratic étale if $C \cong k \oplus k$ (as a direct sum of ideals).

(c) split of rank 4 or a split quaternion algebra if $C \cong \text{Mat}_2(k)$,

(d) split of rank 8 or a split octonion algebra if $C \cong \text{Zor}(k)$.

If $C$ is an arbitrary composition algebra over $k$, we consider its rank decomposition \[^{[10]}\text{Exercise 42}\] , which in the special case at hand, thanks to Corollary 22.17, attains the form

$$k = k_0 \oplus k_1 \oplus k_2 \oplus k_3, \quad k_i := k \varepsilon_i \quad (0 \leq i \leq 3)$$

(1) \hspace{1cm} \text{KKEIF}

$$C = C_0 \oplus C_1 \oplus C_2 \oplus C_3, \quad C_i := C \otimes k_i \quad (0 \leq i \leq 3)$$

(2) \hspace{1cm} \text{CKKEIF}

as direct sums of ideals induced by a complete orthogonal system $(\varepsilon_i)_{0 \leq i \leq 3}$ of idempotents in $k$ uniquely determined by the condition that $C_i$ is a composition algebra of rank $2^i$ over $k_i$ for $0 \leq i \leq 3$. Then $C$ is said to be split if $C_i$ is split of rank $2^i$ for all $i = 0, 1, 2, 3$. Note that the property of a composition algebra to be split (resp. split of rank $r \in \{1, 2, 4, 8\}$) is stable under base change.

For the split composition algebras of rank $r = 1, 2, 4, 8$ over $k$ exhibited in (a)–(d) above, it is sometimes helpful to introduce a unified notation. We put

$$C_{0r}(k) := \begin{cases} k & \text{for } r = 1, \\
 k \oplus k & \text{for } r = 2, \\
 \text{Mat}_2(k) & \text{for } r = 4, \\
 \text{Zor}(k) & \text{for } r = 8 \end{cases}$$

(3) \hspace{1cm} \text{NOTASP}

and have

$$C_{0r}(k)_R = C_{0r}(R)$$

for all $R \in k\text{-alg}$. We call $C_{0r}(k)$ the standard split composition algebra of rank $r$ over $k$.

Exercises.
114. Let $D$ be a quadratic étale $k$-algebra, use Exc. 102 to identify $k = H(D, t_D) \subseteq D$ canonically, and let $(M, h)$ be a hermitian space of rank $n$ over $D$.

(a) If $k$ is a local ring, show that $h$ can be diagonalized: there exist a basis $(e_i)_{1 \leq i \leq n}$ of $M$ as a right $D$-module and scalars $\alpha_1, \ldots, \alpha_n \in k^\times$ such that $h(e_i, e_j) = \delta_{i,j} \alpha_i$ for $1 \leq i, j \leq n$.

(b) Deduce from (a) that $(M, q)$, where $M$ is viewed canonically as a $k$-module and $q : M \to k$ is defined by $q(x) := h(x, x)$ for $x \in M$, is a quadratic space of rank $2n$ over $k$.

112. Isotopes of the ternary hermitian construction. Let $D$ be a quadratic étale $k$-algebra, $(M, h)$ a ternary hermitian space over $D$ and $\Delta : \wedge^3 M \to D$ an orientation of $M$ satisfying $\det(h) = 1$. Put $C = \text{Ter}(D; M, h, \Delta)$. For $p \in D^\times \subseteq C^\times$, we refer to the concept of unital $p$-isotopes as defined in Thm. 24.13 and have $D = D^p \subseteq C^p$, so Thm. 24.13 yields a ternary hermitian space $(M, h)^p = (M^p, h^p)$ over $D$ and an orientation $\Delta^p$ of $M^p$ such that $C^p = \text{Ter}(D; M^p, h^p, \Delta^p)$. Describe $M^p, h^p, \Delta^p$ explicitly. What does this description mean for the octonion algebras of Zorn vector matrices?

113. (Thakur [123]) For $i = 1, 2$, let $(M_i, h_i)$ be ternary hermitian spaces over a quadratic étale $k$-algebra $D$ and $\Delta_i : \wedge^3 M_i \to D$ an orientation of $M_i$ satisfying $\det(h_i) = 1$. Put

$$C_i := \text{Ter}(D; M_i, h_i, \Delta_i) = D \oplus M_i \quad (i = 1, 2)$$

and prove for any map $\chi : M_1 \to M_2$ that the following conditions are equivalent.

(i) $\chi : (M_1, h_1, \Delta_1) \to (M_2, h_2, \Delta_2)$ is an isomorphism, i.e., $\chi : (M_1, h_1) \sim (M_2, h_2)$ is an isometry satisfying $\Delta_2 \circ (\wedge^3 \chi) = \Delta_1$.

(ii) $\chi : (M_1, h_1) \sim (M_2, h_2)$ is an isometry satisfying

$$\chi(x \times_{h_1} y) = \chi(x) \times_{h_2} \chi(y).$$

$x, y \in M_1$.

(iii) $1_D \oplus \chi : C_1 \sim C_2$ is an isomorphism.

114. A presentation of the split octonions. Show that $C := \text{Zor}(k)$ is the free unital alternative $k$-algebra on three generators $E, X_1, X_2$ satisfying the relations

$$E^2 = E, \quad X_1^2 = X_2 = 1_C, \quad X_1 X_2 X_1 = -X_2,$$  

$$X_1 E X_1 = X_2 E X_2 = -(X_1 X_2) E (X_1 X_2) = E = 1_C - E.$$  

(4)  

i.e., that $C$ has three generators $E, X_1, X_2$ satisfying (4) and, conversely, given any unital alternative $k$-algebra $A$ and three element $e, x_1, x_2 \in A$ such that (4) holds (after the obvious notational adjustments), there exists a unique homomorphism $C \to A$ of unital $k$-algebras sending $E, X_1, X_2$ respectively to $e, x_1, x_2$. Conclude that, for some ideal $\alpha \subseteq k$, the subalgebra of $A$ generated by $e, x_1, x_2$ is isomorphic to $\text{Zor}(k/\alpha)$ as a $k$-algebra.

25. Reduced composition algebras

s.REDCO

In the classical theory of finite-dimensional linear non-associative algebras over fields, the standard way to define the notion of a reduced algebra consists in requiring the existence of a complete orthogonal system of absolutely primitive idempotents. This approach will be adapted here to the setting of composition algebras over arbitrary commutative rings. We then proceed to explore more accurately the structure of reduced composition algebras and compare it with the more restrictive notion of splitness as defined in 24.18.

Throughout we let $k$ be an arbitrary commutative ring.
25.1. Primitive and absolutely primitive idempotents. Recall from, e.g., Braun-Koecher [15, p. 52] or Schafer [114, pp. 39, 56] that an idempotent of an algebra over a field is said to be primitive if it is non-zero and it cannot be decomposed into the sum of two non-zero orthogonal idempotents; we speak of an absolutely primitive idempotent if it remains primitive in every base field extension. These definitions have natural extensions to algebras over arbitrary commutative rings as follows.

Let \( A \) be a \( k \)-algebra. An idempotent \( c \in A \) is called primitive if \( c \neq 0 \) and for all orthogonal idempotents \( c_1, c_2 \in A \) satisfying \( c = c_1 + c_2 \), there exists a complete orthogonal system \( (\varepsilon_1, \varepsilon_2) \) of idempotents in \( k \) such that \( c_i = \varepsilon_i c \) for \( i = 1, 2 \); this notion obviously reduces to the previous one if \( k \) is a field (or, more generally, a connected commutative ring).

Note that for an alternative algebra \( A \) over a field, an idempotent \( c \in A \) is primitive if and only if the subalgebra \( A_{11}(c) \subseteq A \) contains no idempotents other than 0 and \( c \).

25.2. Proposition. Let \( A \) be an algebra over \( k \) and suppose \( A \) is finitely generated projective as a \( k \)-module. Then every absolutely primitive idempotent of \( A \) is a unimodular element.

Proof. Let \( c \in A \) be an absolutely primitive idempotent. Then, for all \( p \in \text{Spec}(k) \), the idempotent \( c(p) \in A(p) \) is primitive, hence non-zero. The assertion follows from Lemma 10.13. □

25.3. Separable alternative algebras over rings. Recall from Schafer [114, p. 58] that a finite-dimensional alternative algebra \( A \) over a field \( F \) is said to be separable if, for every field extension \( K/F \), the extended alternative algebra \( A_K \) over \( K \) is semi-simple in the sense of 18.3. Using the theory of Azumaya algebras (Knus-Ojanguren [60, III, Thm. 5.1]) or that of separable Jordan pairs (Loos [69]) as a guide, this notion will now be extended to algebras over commutative rings as follows.

A unital alternative algebra \( C \) over \( k \) is said to be separable if

(i) \( C \) is finitely generated projective as a \( k \)-module.

(ii) \( C(p) \) is a (finite-dimensional) separable (alternative) algebra over the field \( \kappa(p) \), for all \( p \in \text{Spec}(k) \).

We claim that composition algebras are separable alternative. Indeed, alternativity and condition (i) follow from Thm. 22.8 while, in order to establish condition (ii), it suffices to show that a composition algebra \( C \) over a field \( F \) is semi-simple. Assuming (as we may) \( \dim_F(C) > 1 \), the norm of \( C \) is a non-singular quadratic form (Cor. 22.17), forcing \( \text{Nil}(C) = \{0\} \) by Exc. 77.

For arbitrary separable alternative algebras, the property of an idempotent to be absolutely primitive can be characterized by means of its Peirce decomposition (Exc. 67).
25.4. Proposition. Let $A$ be a separable alternative algebra over $k$. For an idempotent $c \in A$ to be absolutely primitive it is necessary and sufficient that $A_{11}(c)$ be free of rank 1 as a $k$-module. In this case, $c$ is a basis of $A_{11}(c)$.

Proof. Note first that by Exc. 67 the Peirce components of $A$ relative to $c$ are compatible with base change, i.e., $A_{ij}(c)_R \cong (A_R)_{ij}(c_R)$ canonically, for all $i, j = 1, 2$, $R \in k$-$\text{alg}$. In order to prove sufficiency, suppose $A_{11}(c)$ is free of rank 1 as a $k$-module. Then $c$ is a basis of $A_{11}(c)$ and obviously a primitive idempotent, hence an absolutely primitive one since the property of $A_{11}(c)$ to be free of rank 1 remains stable under base change. Conversely, in order to prove necessity, suppose $c$ is absolutely primitive. The Peirce decomposition shows that $A_{11}(c)$ is finitely generated projective as a $k$-module. For any prime ideal $p \subseteq k$, let $K \in k$-$\text{alg}$ be the algebraic closure of the residue field $k(p)$. Then $c_K \in C_K$ is a primitive idempotent and, combining Lemma 18.9 with Cor. 18.11, we see that $A_{11}(c)_K \cong (A_K)_{11}(c_K)$ is a finite-dimensional alternative division algebra over the algebraically closed field $K$. By Exc. 37 this implies $\text{rk}_p(A_{11}(c)) = \dim_K((A_K)_{11}(c_K)) = 1$, so $A_{11}(c)$ is a line bundle. But $c \in A_{11}(c)$ is a unimodular vector by Prop. 25.2, forcing $A_{11}(c)$ to be free of rank 1 with basis $c$. \qed

25.5. Reduced composition algebras. A composition algebra over $k$ is said to be reduced if it contains an absolutely primitive idempotent. The base ring $k$ itself is clearly a reduced composition algebra of rank 1. In order to describe the reduced composition algebras of rank $> 1$, we require a few preparations. The first one of these connects absolutely primitive idempotents with elementary ones as defined in Exc. 82.

25.6. Proposition. Elementary idempotents in conic algebras are absolutely primitive. Conversely, let $C$ be a composition algebra of rank $r > 1$ over $k$. The every absolutely primitive idempotent in $C$ is elementary.

Proof. Let $C$ be a conic $k$-algebra and suppose $c \in C$ is an elementary idempotent. Since the property of an idempotent to be elementary is stable under base change, it suffices to show for the first part of the proposition that $c$ is primitive. Accordingly, assume $c = c_1 + c_2$ with orthogonal idempotents $c_i \in C_i, i = 1, 2$. Then $2c_i = c \circ c_i = tc(c_i)c_i + tc(c_i)c_i - nc(c_i)c_i 1_C$ and we conclude $c_i = tc(c_i)c_i - nc(c_i)c_i 1_C$. Multiplying this by $c$, we obtain $c_i = e_i c$ for some $e_i \in k$, and since $c$ is unimodular, $(e_1, e_2)$ is a complete orthogonal system of idempotents in $k$. Thus $c$ is primitive, as claimed.

For the second part of the proposition, assume $C$ is a composition algebra of rank $r > 1$ and let $c \in C$ be an absolutely primitive idempotent. Then so is $c_R$, for any $R \in k$-$\text{alg}, R \neq \{0\}$. This gives $c_R \neq 0$ by definition, but also $c_R \neq 1_{C_R}$ since $r > 1$ and $C_{11}(c)$ is free of rank 1 as a $k$-module by Prop. 25.4. Hence $c$ is elementary. \qed

Remark. The proof of the first part of the preceding proposition shows, more generally,

$$kc = \{x \in C \mid cx = xc\}$$

for any elementary idempotent in a conic algebra $C$ over $k$. 
25.7. **Proposition.** Let $C$ be a composition algebra of rank $r > 1$ over $k$. Then the following conditions are equivalent.

(i) $C$ is reduced.

(ii) $C$ contains a split quadratic étale subalgebra.

(iii) The norm of $C$ is isotropic.

(iv) The norm of $C$ is hyperbolic.

If these conditions are fulfilled and $c \in C$ is an absolutely primitive idempotent, then

$$n_C \cong h_{kC_{12}(c)}. \quad (1)$$

**Proof.** (i) $\Rightarrow$ (ii). By definition and Prop. 25.6, $C$ contains an elementary idempotent $c$, whence Exc. 82 shows that $kc \oplus k\bar{c} \subseteq C$ is a split quadratic étale subalgebra.

(ii) $\Rightarrow$ (iii). Let $D \subseteq C$ be a split quadratic étale subalgebra. Since $n_D = n_C|_D$ is isotropic (Ex 22.9 (a)), so is $n_C$.

(iii) $\Rightarrow$ (i). Choose an isotropic vector $u \in C$ relative to $n_C$. Since $u$ is unimodular and $n_C$ is non-singular, some $v \in C$ satisfies $t_C(uv) = n_C(u, \bar{v}) = 1$. But $n_C(uv) = n_C(u)n_C(v) = 0$, so (by Exc. 82) $c = uv \in C$ is an elementary, hence absolutely primitive, idempotent.

(i) $\Rightarrow$ (iv). Let $c \in C$ be an elementary idempotent with Peirce components $C_{ij} = C_{ij}(c), i, j = 1, 2$. By [4], [5] of Exc. 105, the norm $n_C$ determines a duality between the $k$-modules $kc \oplus C_{12}$ and $k\bar{c} \oplus C_{21}$, on which it is identically zero. Hence (i) and (iv) follow.

(iv) $\Rightarrow$ (iii). If (iv) holds, $C = M_1 \oplus M_2$ may be written as the direct sum of two totally isotropic submodules $M_i \subseteq C$ relative to $n_C$, $i = 1, 2$. In particular, $1_C = e_1 + e_2$, $e_i \in M_i, i = 1, 2$, which implies $n_C(e_i) = 0, 1 = n_C(1_C) = n_C(e_1, e_2)$. Thus $(e_1, e_2)$ is a hyperbolic pair in $(C, n_C)$.

25.8. **Corollary.** The reduced composition algebras of rank 2 are precisely the split quadratic étale $k$-algebras.

25.9. **Twisted $2 \times 2$-matrices.** Let $L$ be a line bundle over $k$. Then there is a natural identification

$$\text{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}$$

as $k$-algebras, where multiplication on the right is the usual matrix product, taking advantage of the canonical pairing $L^* \times L \to k$ at the appropriate place. We claim that $C := \text{End}_k(k \oplus L)$ is a quaternion algebra over $k$, with norm, trace, conjugation respectively given by
for \( \alpha_1, \alpha_2 \in k, \; u^* \in L^* \) and \( v \in L \). Since passing to the dual of a finitely generated projective module by Lemma \[10.11\] commutes with base change, so does the construction of \( C \). Hence our claim may be checked locally, in which case \( L \) is a free \( k \)-module of rank 1 and \( C \) becomes isomorphic to the split quaternion algebra of \( 2 \times 2 \)-matrices, with (1)–(3) converted into the formulas for the ordinary determinant, trace, conjugation, respectively, of \( 2 \times 2 \)-matrices. We call \( C = \text{End}_k(k \oplus L) \) the quaternion algebra of \( L \)-twisted \( 2 \times 2 \)-matrices over \( k \). Note that

\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
\]

form a complete orthogonal system of elementary idempotents in \( C \) with off-diagonal Peirce components

\[
C_{12}(e) = \begin{pmatrix} 0 & L^* \\ 0 & 0 \end{pmatrix}, \quad C_{21}(e) = \begin{pmatrix} 0 & 0 \\ L & 0 \end{pmatrix}.
\]

We can now characterize reduced quaternion algebras in the following way.

**25.10. Proposition.** Up to isomorphism, the reduced quaternion algebras over \( k \) are precisely the quaternion algebras of \( L \)-twisted \( 2 \times 2 \)-matrices, for some line bundle \( L \) over \( k \). More precisely, let \( C \) be a quaternion algebra over \( k \) and \( c \in C \) an absolutely primitive idempotent. Then there exist a line bundle \( L \) over \( k \) and an isomorphism \( \phi : C \xrightarrow{\sim} \text{End}_k(k \oplus L) \) such that

\[
\phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.
\]

**Proof.** Let \( L \) be a line bundle over \( k \). By \[25.9\], the norm of \( C := \text{End}_k(k \oplus L) \) is hyperbolic, and Prop. \[25.7\] shows that \( C \) is reduced. Conversely, suppose \( C \) is a reduced quaternion algebra over \( k \) and \( c_1 := c \in C \) is an absolutely primitive idempotent. Then \( c \) is an elementary idempotent by Proposition \[25.6\] so the corresponding Peirce decomposition of \( C \) takes on the form \( C = kc_1 \oplus C_{12} \oplus C_{21} \oplus kc_2 \), with \( c_2 := 1_C - c_1 \) and finitely generated projective \( k \)-modules \( C_{12}, \; C_{21} \) which, by \[22\] Exercise \[105\] are in duality under the bilinearized norm. Counting ranks, we conclude that \( L := C_{21} \) is a line bundle over \( k \) and \( C_{12} = L^* \) under the natural
identification induced by the bilinearized norm. Since $C$ is associative, Exercise 15 shows $C^2_{ij} = \{0\}$. By the same token, given $x_{21} \in C_{21}$, $y^*_{21} \in C_{12}$, we obtain $y^*_{21}x_{21} = \alpha c_1$ for some $\alpha \in k$, and taking traces in conjunction with (7) of Exercise 105 yields

$$\alpha = tc(y^*_{21}, x_{21}) = n_C(y^*_{21}, x_{21}) = -n_C(y^*_{21}, x_{21}) = -\langle y^*_{21}, x_{21} \rangle.$$

Thus $y^*_{21}x_{21} = -\langle y^*_{21}, x_{21} \rangle c_1$. But then

$$x_{21}y^*_{21} = (-\bar{x}_{21})(-\bar{y}^*_{21}) = \bar{x}_{21}\bar{y}^*_{21} = y^*_{21}x_{21} = -\langle y^*_{21}, x_{21} \rangle c_2.$$

Now one checks easily that

$$\phi: C \xrightarrow{\sim} \text{End}(k \oplus L), \quad \alpha_1 c_1 \oplus x^*_{21} \oplus x_{21} + \alpha_2 c_2 \mapsto \left( \begin{array}{l} \alpha_1 -x^*_{21} \alpha_2 \\ x_{21} \end{array} \right)$$

is an isomorphism of quaternion algebras having the desired property. \hfill \Box

### 25.11. Twisted Zorn vector matrices. Let $M$ be a finitely generated projective $k$-module of rank 3 and $\theta$ an orientation of $M$, i.e., a $k$-linear bijection $\theta: \wedge^3 M \xrightarrow{\sim} k$. Dualizing by means of the identification $24.6$, we obtain a $k$-linear bijection $\theta^*: k = k^* \xrightarrow{\sim} (\wedge^3 M)^* = \wedge^3 (M^*)$, hence an induced orientation $\theta^{-1}$ on $M^*$ uniquely determined by the condition

$$\theta(v_1 \wedge v_2 \wedge v_3) \theta^{-1}(v_i^* \wedge v_j^* \wedge v_k^*) = \det ((\langle v_i^*, v_j \rangle))_{1 \leq i, j \leq 3}$$

for $v_j \in M, v_i^* \in M^*, 1 \leq i, j \leq 3$. These two orientations in turn give rise to alternating bilinear maps

$$M \times M \longrightarrow M^*, \quad (v, w) \longmapsto v \wedge w,$$

$$M^* \times M^* \longrightarrow M, \quad (v^*, w^*) \longmapsto v^* \wedge w^*,$$

called the associated vector products, according to the rules

$$\theta(u \wedge v \wedge w) = \langle u \wedge v, w \rangle, \quad \theta^{-1}(u^* \wedge v^* \wedge w^*) = \langle w^*, u^* \wedge v^* \rangle$$

for $u, v, w \in M, u^*, v^*, w^* \in M^*$. Now the $k$-module

$$Zor(M, \theta) = \left( \begin{array}{c} k \\ M^* \\ M \\ k \end{array} \right)$$

becomes a unital $k$-algebra under the multiplication

$$(\alpha_1 v^*, v, \alpha_2) (\beta_1 w^*, w, \beta_2) = \left( \begin{array}{c} \alpha_1 \beta_1 - \langle v^*, w \rangle \\ \beta_1 v + \alpha_2 w + v^* \wedge w^* \\ \alpha_1 w^* + \beta_2 v^* + v \wedge w^* \\ -\langle w^*, v \rangle + \alpha_2 \beta_2 \end{array} \right)$$

for $\alpha_i, \beta_i \in k, v, w \in M, v^*, w^* \in M^*, i = 1, 2$, whose unit element is the identity matrix $I_2$. We call $Zor(M, \theta)$ the algebra of $(M, \theta)$-twisted Zorn vector matrices over $k$. 
We claim that $C := \text{Zor}(M, \theta)$ is an octonion algebra over $k$, with norm, trace, conjugation given by

\[ n_C \left( \begin{array}{c} \alpha_1 u^* \\ v \\ \alpha_2 \end{array} \right) = \alpha_1 \alpha_2 - \langle u^*, v \rangle, \]  

(4) \hspace{1cm} \text{NOTWI} \hspace{1cm}

\[ t_C \left( \begin{array}{c} \alpha_1 u^* \\ v \\ \alpha_2 \end{array} \right) = \alpha_1 + \alpha_2, \]  

(5) \hspace{1cm} \text{TRTWI} \hspace{1cm}

\[ \left( \begin{array}{c} \alpha_1 u^* \\ v \\ \alpha_2 \end{array} \right) = \left( \begin{array}{c} \alpha_2 - u^* \\ -v \\ \alpha_1 \end{array} \right). \]  

(6) \hspace{1cm} \text{CONJTWI} \hspace{1cm}

for $\alpha_1, \alpha_2 \in k$, $u^* \in M^*$, $v \in M$. Since the construction of $C$, as in the quaternionic case, commutes with base change, this may be checked locally, so we may assume that $M$ is a free $k$-module of rank 3. Hence there exist elements $u_1, u_2, u_3 \in M$ satisfying the following equivalent conditions.

(i) $\mathcal{B} := (u_1, u_2, u_3)$ is a basis of $M$.

(ii) $u_1 \wedge u_2 \wedge u_3 \in \wedge^3(M)$ is unimodular.

(iii) $\theta(u_1 \wedge u_2 \wedge u_3) \in k^\times$.

Replacing, e.g., $u_3$ by an appropriate scalar multiple, we may therefore assume $\mathcal{B}$ to be $\theta$-balanced in the sense that $\theta(u_1 \wedge u_2 \wedge u_3) = 1$. Hence we find a natural identification $M = k^3$ such that $\mathcal{B} = (e_1, e_2, e_3)$ is the basis of ordinary unit vectors and $\theta = \det: \wedge^3(k^3) \to k$ is given by the ordinary determinant. This in turn yields a natural identification $M^* = k^3$ such that the canonical pairing $M^* \times M \to k$ agrees with the map $k^3 \times k^3 \to k$, $(u, v) \mapsto u \cdot v$. Thus the basis $(e_i)_{1 \leq i \leq 3}$ is selfdual, and applying (1) we conclude $\theta^{-1} = \det$ as well. Hence both vector products $\times_{\text{det}}$ agree with the ordinary vector product $\times$ on $k^3$ and $\text{Zor}(k^3, \det) = \text{Zor}(k)$ is the same as the algebra of ordinary Zorn vector matrices over $k$. The assertion follows. As in the case of reduced quaternion algebras,

\[ e := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e' := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \]  

(7) \hspace{1cm} \text{DIACONO} \hspace{1cm}

form a complete orthogonal system of elementarly idempotents in $C$ with off diagonal Peirce components

\[ C_{12}(e) = \begin{pmatrix} 0 & M^* \\ 0 & 0 \end{pmatrix}, \quad C_{21}(e) = \begin{pmatrix} 0 & 0 \\ M & 0 \end{pmatrix} \]  

(8) \hspace{1cm} \text{OFFPEO} \hspace{1cm}

Remark. In [98], the algebras of $(M, \theta)$-twisted Zorn vector matrices have been called split octonion algebras. K. McCrimmon (oral communication) has rightly objected that splitness for composition algebras should be defined in such a way as to allow, up to isomorphism, precisely one example in each rank 1, 2, 4, 8. We have adopted his point of view in the definition 24.18 above.
25.12. Theorem (Pettersson [98]). Up to isomorphism, the reduced octonion algebras over \( k \) are precisely the algebras of \((M, \theta)\)-twisted Zorn vector matrices, for some finitely generated projective \( k \)-module \( M \) of rank 3 and some orientation \( \theta \) of \( M \). More precisely, given an octonion algebra \( C \) over \( k \) and an absolutely primitive idempotent \( c \in C \), there exist \( M, \theta \) as above and an isomorphism \( \phi : C \to \text{Zor}(M, \theta) \) such that

\[
\phi(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.
\]  

Proof. Let \( M \) be a finitely generated projective \( k \)-module of rank 3 and \( \theta \) an orientation of \( M \). Then \( 25.11.4 \) shows that the norm of the octonion algebra \( \text{Zor}(M, \theta) \) is hyperbolic, forcing the algebra itself to be reduced (Prop. 25.7). Conversely, suppose \( C \) is a reduced octonion algebra over \( k \) and \( c_1 := c \in C \) is an absolutely primitive idempotent. Then \( c \) is an elementary one by Proposition 25.6, so the corresponding Peirce decomposition takes on the form \( C = kC_1 \oplus C_2 \oplus kC_2 \), with \( C_2 := kC_1 - c_1 \) and finitely generated projective \( k \)-modules \( C_1 \), \( C_2 \) in duality under the bilinearized norm (\( 22 \), Exercise 105). Counting ranks, we conclude that \( M := C_1 \) is a finitely generated projective \( k \)-module of rank 3 and \( C_1 \) under the natural identification induced by the bilinearized norm. Given \( v \in M = C_2, u \in M^* = C_1 \), we claim

\[
u^*v = -\langle u^*, v \rangle c_1, \quad vu^* = -\langle u^*, v \rangle c_2.
\]

Indeed, the Peirce rule \( 3 \) of \( 15 \), Exercise 67, yield \( u^*v = \alpha c_1 \) for some \( \alpha \in k \), and taking traces in conjunction with \( 7 \) of \( 22 \), Exercise 105, we conclude

\[
\alpha = \iota_C(u^*v) = n_C(u^*, \bar{v}) = -n_C(u^*, v) = -\langle u^*, v \rangle.
\]

Hence the first equation of \( 2 \) holds; the second one follows analogously. Now combine \( 19.11.5 \) with \( 22 \), Exercise 105, and observe that the expression \( \iota_C(uvw) = n_C(\langle u^*, v \rangle, w) = n_C(u^*v, w) \) is alternating trilinear in \( u^*v, w \in M \). Since \( M^2 \subseteq M^* \) by the Peirce rules \( 15 \), Exercise 67, we therefore obtain a unique linear map \( \theta : \wedge^3(M) \to k \) such that

\[
\theta(u \wedge v \wedge w) = -\iota_C(\langle u^*, v \rangle, w) = n_C(\langle u^*, v \rangle, w) = \langle uvw, w \rangle \quad (u, v, w \in M).
\]  

We claim that \( \theta \) is an isomorphism. In order to see this, we may assume that \( k \) is a local ring and first treat the case that \( k \) is a field. Then we must show \( \theta \neq 0 \). Otherwise, \( \langle uvw, w \rangle = n_C(u^*v, w) = 0 \) for all \( u, v, w \in M \), hence \( M^2 = \{0\} \). But then, given \( u, v \in M \), \( w^* \in M^* \), linearized right alternativity yields \( (uv)w^* + (uv^*)v = u(vw^*) + u(w^*v) \), which combines with \( 2 \) to imply \( \langle w^*, u \rangle c_2 v = \langle w^*, v \rangle (uc_2 + uc_1) \), hence the contradiction \( \langle w^*, u \rangle v = \langle w^*, v \rangle u \). We are left with the case that \( k \) is a local ring. Given any basis \( \{u_1, u_2, u_3\} \) of \( M \), the case just treated implies that \( \theta(u_1 \wedge u_2 \wedge u_3) \) does not vanish after passing to the residue field of \( k \). Hence \( \theta(u_1 \wedge u_2 \wedge u_3) \) is a unit in \( k \), and we conclude that \( \theta \) is indeed an isomorphism. Moreover,
With (25.11) we obtain \( u \times_\theta v = uv \) for the associated vector product of \( u, v \in M \). Our next aim is to prove

\[
\theta^{-1}(u^* \wedge v^* \wedge w^*) = n_C(u^*v^*, w^*) = (w^*, u^*v^*) \quad (u^*, v^*, w^* \in M^*). \tag{4}
\]

Localizing if necessary, we may assume that \( M \) is a free \( k \)-module, with basis \((e_i)_{1 \leq i \leq 3}\) chosen in such a way that \( \theta(e_1 \wedge e_2 \wedge e_3) = 1 \). If we write \((e_i^*)_{1 \leq i \leq 3}\) for the corresponding dual basis of \( M^* \), then (25.11) shows \( \theta^{-1}(e_1^* \wedge e_2^* \wedge e_3^*) = 1 \), and since both sides of (4) are alternating trilinear in \( u^*, v^*, w^* \), the proof will be complete once we have shown \( e_1^*e_2^* = e_3 \). Consulting (3), and making use of its alternating character, we obtain \( c_1c_2 = e_3 \), whence a cyclic change of variables also yields \( c_2c_3 = e_1, c_3c_1 = e_2 \). Since \( \overline{e_i} = -e_i, \overline{e_i^*} = -e_i^* \) for \( i = 1, 2, 3 \) by (7) of [22], Exercise [105] the middle Moufang identity (14.3.3) combined with (20.3.2) yields

\[
e_1^*e_2^* = \overline{e_1^*e_2^*} = (e_3e_2)(e_1e_3) = e_3(e_2e_1)e_3 = -e_3(e_1e_2)e_3 = -e_3e_2^*e_3
\]

and (4) is proved. Consequently, \( u^* \times_\theta v^* = uv^* \in M \) is the corresponding vector product of \( u^*, v^* \in M^* \). Now one checks easily that \( \phi : C \to \text{Zor}(M, \theta) \) defined by

\[
\phi(\alpha_1c_1 \oplus v^* \oplus u \oplus \alpha_2c_2) := \left( \begin{array}{c} \alpha_1 v^* \\ u \\ \alpha_2 \end{array} \right)
\]

for \( \alpha_1, \alpha_2 \in k, v^* \in M^* = C_{12}, u \in M = C_{21} \) is an isomorphism of octonion algebras satisfying (1).

\[ \square \]

**25.13. Corollary.** Split composition algebras over any commutative ring are reduced. Conversely, if \( k \) is a local ring, then every reduced composition algebra over \( k \) is split.

**Proof.** The first part follows by comparing the list [24.18] with Prop. 25.7. Conversely, let \( k \) be a local ring and \( C \) a reduced composition algebra of rank \( r = 1, 2, 4, 8 \) over \( k \). While the case \( r = 1 \) is trivial, and the case \( r = 2 \) follows immediately from Prop. 25.7, the remaining cases \( r = 4, 8 \) are a consequence of Prop. 25.10 and Thm. 25.12, since finitely generated projectives over \( k \) are free.

\[ \square \]

**25.14. Corollary.** For a composition algebra \( C \) of dimension \( > 1 \) over a field \( F \), the following conditions are equivalent.

(i) \( C \) is split.

(ii) The norm of \( C \) is isotropic.

(iii) The norm of \( C \) is hyperbolic.

(iv) \( C \) is not a division algebra.

**Proof.** By Cor. 25.13 \( C \) is split if and only if it is reduced. Thus (i)–(iii) are equivalent (Prop. 25.7). Moreover, the implication (i)⇒(iv) is obvious, while (iv)⇒(ii) follows from Prop. 20.4.
25.15. Proposition. Let $C$ be a composition algebra over $k$ and $D \subseteq C$ a quadratic étale subalgebra. Then $C_D$, the base change of $C$ from $k$ to $D$, is reduced.

Proof. By Lemma 12.10, we have $C = D \oplus D^\perp$ as a direct sum of $k$-modules, which implies $C_D = D_D \oplus (D^\perp)_D$ as a direct sum of $D$-modules. But $D_D$ is split quadratic étale (Exc. 106 (a)), forcing $C$ to be reduced by Prop. 25.7. □

25.16. Corollary. Let $C$ be a composition algebra of rank $r > 1$ over the local ring $k$. Then every quadratic étale subalgebra of $C$ splits $C$.

Proof. This follows immediately by combining Prop. 25.15 with Cor. 25.13. □

Remark. Quadratic étale subalgebras of $C$ as in Cor. 25.16 exist by Thm. 22.15 (b).

Exercises.

115. Let $C$ be a composition algebra over $k$ and $c$ an idempotent in $C$. Use Exc. 84 to show that $c$ is absolutely primitive if and only if there exist a decomposition

\[ k = k^{(1)} \oplus k^{(2)} \]

as a direct sum of ideals, a composition algebra $C^{(1)}$ over $k^{(1)}$ and an elementary idempotent $c^{(1)} \in C^{(1)}$ such that

\[ C = C^{(1)} \oplus k^{(2)} \]

as composition algebras over $k$ and

\[ c = c^{(1)} \oplus 1_{k^{(2)}}. \]

Conclude that $C$ is reduced if and only if it allows decompositions as in (1), (2) such that $C^{(1)}$ is a composition algebra over $k^{(1)}$ whose rank (as a function Spec$(k) \to \mathbb{Z}$) is nowhere equal to 1.

116. Elementary idempotents in reduced quaternion algebras. Let $L_0$ be a line bundle over $k$ and write

\[ B = \text{End}_k(k \oplus L_0) = \begin{pmatrix} k & L_0^* \\ L_0 & k \end{pmatrix} \]

for the corresponding reduced quaternion algebra over $k$. Prove:

(a) For $c \in B$, the following conditions are equivalent.

(i) $c$ is an elementary idempotent.

(ii) Viewing $c$ as a linear map $k \oplus L_0 \to k \oplus L_0$,

\[ L_c := \text{Im}(c) \subseteq k \oplus L_0 \]

is a line bundle over $k$.

(iii) There exist a line bundle $L$ over $k$ and an isomorphism

\[ \Phi : B \iso \text{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix} \]

such that

\[ \Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \]
In this case $\mathfrak{e} \in B$ is an elementary idempotent as well and
\[ k \oplus L_0 = L_\mathfrak{e} \oplus L_\mathfrak{e}, \quad L_0 \cong L_\mathfrak{e} \oplus L_\mathfrak{e}. \] (3) ELCE

Moreover, $L$ in (iii) is unique up to isomorphism and
\[ L \cong B_{21}(c) \cong L_0 \oplus L_0^{\oplus 2}, \quad B_{12}(c) \cong L_0 \oplus L_0^{\oplus 2}. \] (4) BETCE

(b) Two elementary idempotents $c, d \in B$ are conjugate under inner automorphisms of $B$ if and only if $L_\mathfrak{e} \cong L_\mathfrak{d}$. They are conjugate under arbitrary automorphisms of $B$ if and only if $L_\mathfrak{e}^{\oplus 2} \cong L_\mathfrak{d}^{\oplus 2}$.

(c) If $L$ is any line bundle over $k$, then $L \cong L_\mathfrak{e}$ for some elementary idempotent $\mathfrak{e} \in B$ if and only if $L$ is (isomorphic to) a direct summand of $k \oplus L_0$.

117. Line bundles on two generators. Let $L$ be a line bundle over $k$.

(a) Let $n$ be a positive integer and suppose there are elements $f_1, \ldots, f_n \in k$ such that $k = \sum k_f$ and $L_f$ is free (of rank one) over $k_f$ for $1 \leq i \leq n$. Show that $L$ is generated by $n$ elements.

(b) Show that the following conditions are equivalent.

(i) $L$ is generated by two elements.

(ii) $L \oplus L^*$ is a free $k$-module of rank two.

(iii) There exists an elementary idempotent $\mathfrak{e} \in B := \text{Mat}_2(k)$ such that $L \cong L_{\mathfrak{e}}$.

(iv) There exist elements $f_1, f_2 \in k$ such that $kf_1 + kf_2 = k$ and $L_{\mathfrak{e}}$ is free (of rank one) over $k_{\mathfrak{e}}$ for $1 \leq i \leq 2$.

Conclude that if $L$ satisfies one (hence all) conditions (i)--(iv) above, then so does $L^{\otimes n}$, for all $n \in \mathbb{Z}$. In particular, there exists an elementary idempotent $\mathfrak{e}^{(n)} \in \text{Mat}_2(k)$, unique up to conjugation by inner automorphisms of $B$, satisfying $L^{\otimes n} \cong L_{\mathfrak{e}^{(n)}}$. Describe such an idempotent as explicitly as possible.

Remark. Let $k$ be a Dedekind domain. Then there is a canonical identification of the class group of $k$ with its Picard group, and every fractional ideal of $k$ is generated by two elements (O'Meara [99 22.5b]). Hence the preceding two exercises yield a bijective correspondence between the set of conjugacy classes of elementary idempotents in $\text{Mat}_2(k)$ under inner automorphisms and the class group of $k$. In particular, for $k$ the ring of integers of an algebraic number field $K := \text{Quot}(k)$, the number of these conjugacy classes agrees with the class number of $K$.

118. Isomorphisms of reduced quaternion algebras. Let $L_0, L'_0$ be line bundles over $k$ and $B = \text{End}_d(k \oplus L_0), B' = \text{End}_d(k \oplus L'_0)$ the corresponding reduced quaternion algebras. Use Exc. [116] to show that the following conditions are equivalent.

(i) $B \cong B'$.

(ii) Every line bundle $L$ over $k$ that is a direct summand of $k \oplus L_0$ admits a line bundle $L'$ over $k$ that is a direct summand of $k \oplus L'_0$ and satisfies
\[ L_0 \otimes L^{\otimes 2} \cong L'_0 \otimes L'^{\otimes 2}. \] (5) ISOCOND

(iii) There exist line bundles $L, L'$ over $k$ that are direct summands of $k \oplus L_0, k \oplus L'_0$, respectively, and satisfy (5).

119. Let $L$ be a line bundle over $k$. Prove that the reduced quaternion algebra $\text{End}_d(k \oplus L)$ is split if and only if $L \cong L^{\otimes 2}$ for some line bundle $L'$ on two generators over $k$. Use this to construct examples of reduced quaternion algebras over $k$ that are free as $k$-modules but not split.

120. Failure of Witt cancellation. Let $L$ be a line bundle on two generators over $k$ that is not of period 2 in $\text{Pic}(k)$. Put $L' := L^{\otimes 2}$ and show $h \perp h \cong h \perp h'$ even though $h_{L'}$ is not split. (Hint. Use Exc. [119] to prove that the reduced quaternion algebra $\text{End}_d(k \oplus L')$ is split.)
26. Norm equivalences and isomorphisms

One of the most important results in the classical theory of composition algebras is the norm equivalence theorem. It says that composition algebras over fields are classified by their norms, in other words, two composition algebras over a field are isomorphic if and only if their norms are equivalent, i.e., isometric. Our first aim in this section will be to establish this result in the more general setting of semi-local rings. As in the case of fields, the key ingredient of the proof is Witt cancellation of non-singular quadratic forms, which fails over arbitrary commutative rings (see Exc. 120 below) but is valid over semi-local ones. As an application, we classify composition algebras over special fields, like the reals and the complexes, finite fields, the p-adics and algebraic number fields. The section also contains a few general comments on norm equivalence over arbitrary commutative rings.

Let k be a commutative ring. We begin by introducing the concept of norm equivalence and some useful modifications.

26.1. Norm similarities. Let C, C' be conic algebras over k. A norm similarity from C to C' is a bijective k-linear map f: C → C' such that there exists a scalar μ ∈ k× satisfying \( n_{C'} \circ f = \mu n_C \); in this case, \( \mu = n_C(f(1_C)) \) is unique and called the multiplier of f. Norm similarities with multiplier 1 are called norm isometries or norm equivalences. We say that C and C' are norm similar (resp. norm equivalent) if there exists a norm similarity (resp. a norm equivalence) from C to C'. Norm similarities f: C → C' preserving units (so f(1_C) = 1_{C'}) automatically have multiplier 1; we speak of unit norm equivalences in this context.
It is clear that the preceding notions are stable under base change. Generally speaking, the principal objective of the present section is to understand the connection between unital norm equivalences and isomorphisms (resp. anti-isomorphisms) of composition algebras.

26.2. Proposition. Let \( C, C' \) be conic alternative \( k \)-algebras.

(a) If \( C \) is multiplicative, then for any \( a \in C^\times \), the maps \( L_a, R_a : C \to C \) are norm similarities, with multipliers \( \mu_{L_a} = \mu_{R_a} = n_C(a) \).

(b) Let \( f : C \to C' \) be a norm similarity. Then \( f(C^\times) = C'^\times \). Moreover, if \( f \) is even a unital norm equivalence, then \( f \) preserves norms, traces, conjugations and inverses.

Proof. (a) follows from the property of \( n_C \) permitting composition combined with Prop. 14.6. In order to establish (b), it suffices to combine Prop. 20.4 with (19.5.2), (19.5.4).

□

26.3. Corollary. Multiplicative conic alternative algebras \( C, C' \) over \( k \) are norm similar if and only if there exists a unital norm equivalence from \( C \) to \( C' \).

Proof. Let \( f : C \to C' \) be a norm similarity. By Prop. 26.2 (b), the element \( a' := f(1_C) \) is invertible in \( C'^\times \), and \( L_{a'}^{-1} \circ f : C \to C' \) is a unital norm equivalence.

□

26.4. Proposition. (a) Let \( C, C' \) be conic algebras over \( k \) that are projective as \( k \)-modules. Then every isomorphism or anti-isomorphism from \( C \) to \( C' \) is a unital norm equivalence.

(b) A unital norm equivalence from one quadratic \( k \)-algebra onto another is an isomorphism.

Proof. (a) follows immediately from Exc. [14.6] below.

(b) Let \( R, R' \) be quadratic \( k \)-algebras and \( f : R \to R' \) a unital norm equivalence. In order to show that \( f \) is an isomorphism, we may assume that \( k \) is a local ring, which implies \( R = k[u] \) for some \( u \in R \) such that \( 1_R, u \) is a basis of \( R \) over \( k \). Then \( R' = k[u'] \), \( u' := f(u) \), and since \( f \) preserves units, norms and traces by Prop. 26.2 (b), we have \( f(u^2) = u'^2 = f(u)^2 \) and \( f \) is an isomorphism.

□

We proceed by briefly recalling Witt extension and Witt cancellation of quadratic forms over semi-local rings.

26.5. Theorem (Baeza [8, III, 4.1]). (Witt extension theorem) Let \( (M, Q) \) be a quadratic space over the semi-local ring \( k \) and suppose the submodule \( N \subseteq M \) is a direct summand such that the set \( Q(N^\perp) := \{ Q(x) \mid x \in N^\perp \} \) generates the ring \( k \).

Then every monomorphism from \( (N, Q|_N) \) to \( (M, Q) \) whose image is a direct summand of \( M \) can be extended to an isometry from \( (M, Q) \) onto itself.

□

26.6. Corollary. (Witt cancellation theorem) Let \( (M_1, q_1), (M_2, q_2), (M'_2, q'_2) \) be quadratic spaces over the semi-local ring \( k \) and suppose
\[(M_1, q_1) \perp (M_2, q_2) \cong (M_1, q_1) \perp (M_2', q_2').\]

Then \((M_2, q_2) \cong (M_2', q_2').\)

**Proof.** We may assume that \(M_2\) and \(M_2'\) both have rank \(r > 0\). By Lemma 22.14 this implies
\[q_2(M_2) \cap k^\times \neq \emptyset \neq q_2'(M_2') \cap k^\times.\] 

Now put
\[(M, Q) := (M_1, q_1) \perp (M_2, q_2), \quad (M', Q') := (M_1, q_1) \perp (M_2', q_2')\]

and let \(i_1: (M_1, q_1) \rightarrow (M, Q), \ i_1': (M_1, q_1) \rightarrow (M', Q')\) be the natural embeddings.

Then \(N := i_1(M_1) \subseteq M, \ N' := i_1'(M_1) \subseteq M'\) are submodules giving rise to non-singular subspaces \((N, Q|_N) \subseteq (M, Q), \ (N', Q'|_{N'}) \subseteq (M', Q')\) such that
\[\langle N^\perp, Q|_{N^\perp} \rangle \cong (M_2, q_2), \quad \langle N'^\perp, Q'|_{N'^\perp} \rangle \cong (M_2', q_2'),\]

and given any isometry
\[\Psi: (M', Q') \rightsquigarrow (M, Q),\]

we obtain a monomorphism \(\alpha: (N, Q|_N) \rightarrow (M, Q)\) determined by
\[\alpha(i_1(x_1)) = \Psi(i_1'(x_1)) \quad (x_1 \in M_1).\]

The image of \(\alpha\) is \(\Psi(N')\), hence a direct summand of \(M\) by Lemma 12.10. By (1) and Thm. 26.5, therefore, \(\alpha\) can be extended to an isometry \(\Lambda\) from \((M, Q)\) onto itself. Then
\[\Phi := \Psi^{-1} \circ \Lambda: (M, Q) \rightsquigarrow (M', Q')\]

is an isometry that maps \(N\) onto \(N'\), hence \(N^\perp\) onto \(N'^\perp\). By (2), this means \((M_2, q_2) \cong (M_2', q_2').\) \(\square\)

**26.7. Norm Equivalence Theorem** (cf. Jacobson [31], Van der Blij-Springer [125]).

Let \(k\) be a semi-local ring and \(C, C'\) be composition algebras over \(k\). Then the following conditions are equivalent.

(i) \(C\) and \(C'\) are isomorphic.

(ii) \(C\) and \(C'\) are norm equivalent.

(iii) \(C\) and \(C'\) are norm similar.

**Proof.** (i) \(\Rightarrow\) (ii). Prop. 26.4 (a).

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

(iii) \(\Rightarrow\) (i). We may assume that \(C, C'\) both have rank \(r > 0\). There is nothing to prove for \(r = 1\), so let us assume \(r \geq 2\). By Cor. 26.3 there exists a unital norm equivalence \(f: C \rightarrow C'\), and Thm. 22.15 (a) yields a quadratic étale subalgebra \(D = k[u] \subseteq C\), for some \(u \in C\) having trace 1. Since \(f\) preserves units, norms and traces by Prop. 26.2 (b), we conclude that \(D' := f(D) = k[u'], u' := f(u)\), is a quadratic étale
subalgebra of \( C' \) (Prop. 22.5) and \( f : D \to D' \) is an isomorphism (Prop. 26.4 (b)).
Now suppose \( B \subseteq C, B' \subseteq C' \) are any non-singular composition subalgebras of rank \( s < r \) that are isomorphic. Then \( B, B' \) are associative (Cor. 22.17), and combining Lemma 22.14 with the Witt cancellation theorem (Cor. 26.6), we find invertible elements \( l \in B^\perp \subseteq C, l' \in B'^\perp \subseteq C' \) such that \( n_C(l) = n_{C'}(l') \in k^\times \). Therefore \( B, l \) (resp. \( B', l' \)) generate non-singular composition subalgebras \( B_1 \subseteq C \) (resp. \( B'_1 \subseteq C' \)) of rank \( 2s \) that are isomorphic (Cor. 21.8). Continuing in this manner, we eventually obtain an isomorphism from \( C \) to \( C' \) (actually, we do so after at most two steps). \( \square \)

26.8. Corollary. Let \( B \) be a non-singular associative composition algebra over the semi-local ring \( k \) and \( \mu, \mu' \in k^\times \). Then

\[
\text{Cay}(B, \mu) \cong \text{Cay}(B, \mu') \iff \mu \equiv \mu' \mod n_B(B^\times). 
\]

Proof. Put \( C := \text{Cay}(B, \mu), C' := \text{Cay}(B, \mu') \). By Thm. 26.7 \( C \cong C' \) implies \( n_C \cong n_{C'} \), and Remark 21.4 combines with Witt cancellation (Cor. 26.6) to yield an isometry \( \phi : \mu n_B \to \mu' n_B \). But then \( \mu = \mu' n_B(u), u = \phi(1_B) \in B^\times \). Conversely, if \( \mu = \mu' n_B(u) \) for some \( u \in B^\times \), then \( L_u : \mu n_B \to \mu' n_B \) is an isometry, so \( n_C, n_{C'} \) by Remark 21.4 are isometric, forcing \( C \) and \( C' \) to be isomorphic by the norm equivalence theorem 26.7. \( \square \)

Remark. Cor. 26.8 fails if \( B \) is singular. For example, let \( k \) be a field of characteristic 2 and \( \mu, \mu' \in k \). Then one checks easily that \( \text{Cay}(k, \mu) \) and \( \text{Cay}(k, \mu') \) are isomorphic if and only if \( \mu' = \mu + \alpha^2 \) for some \( \alpha \in k \).

26.9. Comments. Apart from its potential for a great many important applications, some of which will be dealt with in the remainder of this section, the norm equivalence theorem enjoys a few remarkable properties of a different kind. Here are some examples.

(a) The norm equivalence theorem does not claim that every unital norm equivalence between composition algebras over a field (or a semi-local ring) is an isomorphism or an anti-isomorphism. While this is certainly true for quadratic étale algebras over any ring (Prop. 26.4 (b)) and, as will be seen later in ???? below (see also Knus [55, V, (4.3.2)] or Gille [35, Thm. 2.4]), is basically true for quaternion algebras, again over any ring, it fails miserably in the octonionic case. The reader may either consult Exc. 130 below to see this or turn to the octonion algebra \( \mathbb{O} \) over \( k = \mathbb{R} \): in the latter case, the automorphisms or anti-automorphisms of \( \mathbb{O} \) form a closed subset of \( \text{GL}(\mathbb{O}) \) that may be written as the union of two 14-dimensional pieces [2.6], while the unital norm equivalences of \( \mathbb{O} \) identify canonically with the Lie group \( O_7 \), which has dimension 21.

(b) It is a natural question to ask whether the norm equivalence theorem holds over an arbitrary commutative ring. By (a), the answer is yes for composition algebras of rank 2 or 4. On the other hand, it has recently been shown by Gille [35, Thm. 3.3] that the answer is no in rank 8, so there exist commutative rings \( k \) and non-isomorphic octonion algebras over \( k \) whose norms are isometric. More surpris-
ingly still, there are non-split octonion algebras over an appropriate commutative ring whose norms are split hyperbolic [35, p. 308].

(c) The norm equivalence theorem was anticipated already by Zorn [129, p. 399], where one finds the following remarkable statement:

Das System wurde allein aus der quadratischen Form \( \varpi \varpi \) gewonnen, die Äquivalenz der Formen ist also mit der Äquivalenz der Systeme gleichbedeutend.\(^4\)

By “das System” (resp. the expression “\( \varpi \varpi \)”), Zorn is referring to an octonion algebra (resp. to its norm). However, the reason given by him for the validity of the norm equivalence theorem is not convincing since, e.g., it would imply that the theorem would hold over any commutative ring, contrary to Gille’s result mentioned in (b), and that any unital norm equivalence would be an isomorphism.

One reason for the importance of the norm equivalence theorem is that we know a lot about quadratic forms over special fields, and this knowledge may be used to classify composition algebras over these fields. Recall from Cor. 25.14 that composition algebras over any field are either split or division algebras.

26.10. Algebraically closed fields. Quadratic spaces over an algebraically closed field \( k \) are classified by their dimension. Hence the norm equivalence theorem implies that, up to isomorphism, in each dimension 1, 2, 4, 8 there is exactly one composition algebra over \( k \), namely, the split one.

26.11. The reals. Thanks to Sylvester’s inertia theorem, quadratic spaces over \( \mathbb{R} \) (or, more generally, over any real closed field) are classified by their dimension and their signature. In particular, in each dimension there are precisely two isometry classes of anisotropic quadratic forms, a positive definite and a negative definite one. Hence each dimension \( r = 1, 2, 4, 8 \) allows exactly one isomorphism class of composition division algebras over \( \mathbb{R} \): uniqueness follows from the norm equivalence theorem [26.7], while existence is provided by the classical examples \( \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O} \) of \( \S 1 \).

26.12. Finite fields. The key fact to be used here is Chevalley’s theorem (Lang [65 IV, Ex. 7 (a))): every form (= homogeneous polynomial) of degree \( d \) in \( n > d \) indeterminates over a finite field \( k = \mathbb{F}_q \), \( q \) a prime power, has a non-trivial zero in \( \mathbb{F}_q^n \). It follows that every quadratic form in at least three variables over \( \mathbb{F}_q \) is isotropic. In particular, quaternion and octonion algebras over \( \mathbb{F}_q \) are all split (Cor. [25.14]), while the only non-split composition algebra of dimension 2 over \( \mathbb{F}_q \) up to isomorphism is the unique quadratic field extension \( \mathbb{F}_{q^2}/\mathbb{F}_q \).

26.13. \( p \)-adics and their finite extensions. Let \( p \) be a prime. The completion of \( \mathbb{Q} \) relative to its \( p \)-adic valuation is \( \mathbb{Q}_p \), the field of \( p \)-adic numbers. Given a finite algebraic extension \( K \) of \( \mathbb{Q}_p \), the following classical results on quadratic forms over

\(^4\) Emphasis in the original.
Composition algebras

162 4 Composition algebras

K are due to Hasse (see Scharlau [115, Chap. 5, Thm. 6.3] in the case $K = \mathbb{Q}_p$ and O’Meara [90, 63:11b, 63:17, 63:19] in general for details).

(i) Up to isometry, there is a unique anisotropic quadratic form of dimension 4 over $K$, and this form is universal in the sense that it represents every element of $K$.

(ii) Every quadratic form in at least five variables over $K$ is isotropic.

(iii) Up to isomorphism, there is a unique quaternion division algebra over $K$.

By (ii), all octonion algebras over $K$ are split. To complete the picture, it remains to classify composition algebras of dimension 2 over $K$, which are parametrized by $K^\times/K^\times 2$. Describing this group is pretty straightforward if $p$ is odd, but requires some care for $p = 2$; again we refer to Scharlau [115, Chap. 5, § 6] and O’Meara [90, § 63 A, particularly 63:9] for details.

26.14. Algebraic number fields. In this subsection, we assume some familiarity with the foundations of algebraic number theory. Let $K$ be an algebraic number field, i.e., a finite algebraic extension of the field $\mathbb{Q}$ of rational numbers. We denote by $\Omega$ the set of places of $K$, including the infinite ones, and by $K_v$ the completion of $K$ at the place $v \in \Omega$; the natural embedding $\lambda_v: K \to K_v$ makes the image $\lambda_v(K)$ a dense subfield of $K_v$ relative to the $v$-adic topology. The set of real places of $K$ will be denoted by $S$, so we have a natural identification $K_v = \mathbb{R}$ for $v \in S$; in fact, the assignment $v \mapsto \lambda_v$ determines a bijective correspondence between $S$ and the set of embeddings $K \to \mathbb{R}$. Given an algebra $A$ (resp. a quadratic form $Q$) over $K$, we abbreviate $A_v = A \otimes_K K_v$ (resp. $Q_v = Q \otimes_K K_v$) for $v \in \Omega$.

The key to understand composition algebras over $K$ is provided by the Hasse-Minkowski theory of quadratic forms. Referring to O’Meara [90, 66:1, 66:4], Scharlau [115, Chap. 5, 7.2, 7.3] for details, one of its most fundamental results reads as follows.

26.15. Theorem (Hasse-Minkowski). With the notation of 26.14 the following statements hold.

(a) A quadratic form $Q$ over $K$ is isotropic if and only if $Q_v$ is isotropic over $K_v$ for all $v \in \Omega$.

(b) Non-singular quadratic forms $Q, Q'$ over $K$ are isometric if and only if $Q_v, Q'_v$ are isometric over $K_v$ for all $v \in \Omega$.

Since a non-singular quadratic form $Q$ over a field represents a scalar $\alpha$ if and only if the form $(\alpha)_{\text{quad}} \perp Q$ is isotropic, the first part of the Hasse-Minkowski theorem immediately implies:

26.16. Corollary. A non-singular quadratic form $Q$ over $K$ represents an element $\alpha \in K$ if and only if $Q_v$ represents $\lambda_v(\alpha) \in K_v$ for all $v \in \Omega$.

Combining the second part of Thm. 26.15 with the norm equivalence theorem 26.7 it follows that composition algebras over number fields are completely determined by their local behavior:
26.17. Corollary. Composition algebras $C$ and $C'$ over $K$ are isomorphic if and only if $C_v$ and $C'_v$ are isomorphic over $K_v$ for all $v \in \Omega$. □

Cor. 26.17 may be regarded as the first step towards the classification of composition algebras over number fields. In order to complete this classification, it seems natural to invoke another fundamental fact from Hasse-Minkowski theory: every “local family” of non-singular quadratic forms $Q(v)$ over $K_v$, $v \in \Omega$, has a “global realization” by a non-singular quadratic form $Q$ over $K$ satisfying $Q_v \cong Q^{(v)}$ for all $v \in \Omega$ if and only if a certain obstruction, based on Hilbert’s reciprocity law and involving Hasse symbols, vanishes. But since there is no a priori guarantee that the property of being the norm of a composition algebra descends from the totality of forms $Q_v$, $v \in \Omega$, to the form $Q$, one has to argue in a different manner.

For simplicity, we confine ourselves to quaternion and octonion algebras. The classification of the former is accomplished by the following result from class field theory, which we record (again) without proof.

26.18. Theorem (O’Meara [90, 7:19]). With the notation of 26.14, let $T \subseteq \Omega$ be a finite set consisting of an even number of real or finite places of $K$. Then there exists a quaternion algebra $B$ over $K$, unique up to isomorphism, such that $B_v$ is split for all $v \in \Omega \setminus T$ and a division algebra for all $v \in T$. □

Remark. Recall from 26.11 and 26.13 (iii) that $K_v$, for $v \in T$, admits precisely one quaternion division algebra, so uniqueness of $B$ follows from Cor. 26.17.

Surprisingly, the classification of octonion algebras over $K$ turns out to be much simpler. In fact, it can be deduced quite easily from the results assembled so far.

26.19. Theorem (Albert-Jacobson [7]). With the notation of 26.14 write $B := \text{Cay}(K; -1, -1)$ as a quaternion algebra over $K$. Then every octonion algebra over $K$ is isomorphic to $\text{Cay}(B, \mu)$ for some $\mu \in K^\times$. Moreover, given $\mu, \mu' \in K^\times$, the following conditions are equivalent.

(i) $\text{Cay}(B, \mu) \cong \text{Cay}(B, \mu')$.
(ii) $\lambda_v(\mu \mu') > 0$ for all $v \in S$.

Proof. For the first part, it will be enough to prove that every octonion algebra $C$ over $K$ contains a unital subalgebra isomorphic to $B$. To this end, we claim that every non-singular sub-form of $n_C$ having dimension at least 5 represents the element $1 \in K$.

Indeed, let $Q$ be such a sub-form. By Cor. 26.16 it suffices to show for all $v \in \Omega$ that $Q_v$ represents the element $1 \in K_v$. If $C_v$ is split, $n_{C_v}$ has maximal Witt index, and a dimension argument shows that every maximal totally isotropic subspace of $C_v$ relative to $n_{C_v}$ intersects $Q_v$ non-trivially. Thus $Q_v$ is isotropic, hence universal and so represents 1. On the other hand, if $C_v$ is a division algebra, $v \in S$ must be real [26.10] [26.13], forcing $n_{C_v}$ to be positive definite. But then so is $Q_v$, which therefore again represents 1. This proves our claim. We first apply the claim to $n_C^0$, the restriction of $n_C$ to the pure octonions $C^0 = \text{Ker}(c)$, and find an element $j_1 \in C$ satisfying $tc(j_1) = 0$, $nc(j_1) = 1$. By Cor. 21.8 and Prop. 22.5 $D := K[j_1] \cong$
Cay\((K, -1)\) is a quadratic étale subalgebra of \(C\). Applying our claim once more, this time to the restriction of \(n_C\) to \(D^1\), yields an element \(j_D \in D^1\) satisfying \(n_C(j_D) = 1\), and invoking Cor. 26.18 again, we see that the subalgebra of \(C\) generated by \(D\) and \(j_D\) is isomorphic to \(B\), giving the first part of the theorem. As to the second, we conclude \(C_v \cong \text{Cay}(\mathbb{H}, \lambda_v(\mu))\), \(C'_v \cong \text{Cay}(\mathbb{H}, \lambda_v(\mu'))\) for all \(v \in S\), and since \(C_v, C'_v\) are both split for \(v \in \Omega \setminus S\) \((26.10, 26.13)\), we can apply Corollaries 26.17, 26.8 to obtain the following chain of equivalent conditions.

\[
C \cong C' \iff \forall v \in S : C_v \cong C'_v \\
\iff \forall v \in S : \text{Cay}(\mathbb{H}, \lambda_v(\mu)) \cong \text{Cay}(\mathbb{H}, \lambda_v(\mu')) \\
\iff \forall v \in S : \lambda_v(\mu \mu') \in n_{\mathbb{H}^+}(\mathbb{H}^+) = \mathbb{R}_+^*.
\]

\[\square\]

26.20. Corollary (Zorn \[129\]). With the notation of 26.14, there are precisely \(2^{|S|}\) isomorphism classes of octonion algebras over \(K\).

**Proof.** Adopting the notation of Thm. 26.19 let \(T \subseteq S\). We apply the weak approximation theorem (O’Meara \[90, 11:8\]) and find an element \(\mu_T \in K\) satisfying

\[
|\lambda_v(\mu_T) + 1| < 1 \ (v \in T), \quad |\lambda_v(\mu_T) - 1| < 1 \ (v \in S \setminus T).
\]

Up to isomorphism, the octonion algebra \(C_T := \text{Cay}(B, \mu_T)\) does not depend on the choice of \(\mu_T\) (Thm. 26.19), so the assignment \(T \mapsto C_T\) gives a well defined map from \(2^S\) to the set of isomorphism classes of octonion algebras over \(K\). Conversely, let \(C\) be an octonion algebra over \(K\). Then \(T_C := \{v \in S \mid C_v \cong \mathbb{O}\}\) is a subset of \(S\), and \(C \mapsto T_C\) gives a map in the opposite direction. Since the two maps thus defined are easily seen to be inverse to one another, the assertion follows.

**Remark.** Given a family of octonion algebras \(C(v)\) over \(K_v, v \in \Omega\), Cor. 26.20 shows that there always exists an octonion algebra \(C\) over \(K\), unique up to isomorphism, which satisfies \(C_v \cong C(v)\) for all \(v \in \Omega\), so the Hilbert reciprocity law yields no obstructions when dealing with octonion norms.

**Exercises.**

125. The Skolem-Noether theorem for composition algebras. Let \(k\) be a semi-local ring, \(C\) a composition algebra of rank \(r\) over \(k\) and \(B, B' \subseteq C\) two composition subalgebras of the same rank \(s \leq r\). Show that every isomorphism from \(B\) to \(B'\) can be extended to an automorphism of \(C\). Conclude that, up to conjugation by automorphisms of \(\mathbb{O}\) (the Graves-Cayley octonions), the only non-zero subalgebras of \(\mathbb{O}\) are \(\mathbb{R}, \mathbb{C}, \mathbb{H}\) and \(\mathbb{O}\).

126. (cf. Van der Blij-Springer \[125\] (3.3)) Let \(k\) be a principal ideal domain and \(C\) a composition algebra of rank \(> 1\) over \(k\) that has (left or right) zero divisors (cf. Ex. 94). Show that \(C\) is split.

127. Unital norm equivalences of conic alternative algebras. \((\text{à la Jacobson-Rickart} \[49\])\) Let \(C, C'\) be conic alternative \(k\)-algebras and suppose \(f: C \rightarrow C'\) is a unital norm equivalence.

\[\text{According to loc. cit., p. 400, there should be a reference to the work of H. Brandt.}\]
(a) Show

\[ f(U, y) = U_{f(x)}f(y), \quad (1) \]

\[ (f(xy) - f(x)f(y))(f(xy) - f(y)f(x)) = [f(x), f(xy), f(y)] \quad (2) \]

for all \( x, y \in C \). In particular, the left-hand side of (2) is symmetric in \( x, y \).

(b) Conclude from (1) and its linearizations that if \( c \in C \) is an elementary idempotent, so is

\[ c' := f(c) \in C' \]

and

\[ f(C_{12}(c) + C_{21}(c)) = C_{12}(c') + C_{21}(c'). \]

128. Unital norm equivalences of quaternion algebras (Petersson [22]). (a) Show for quaternion algebras \( B, B' \) over \( k \): if \( f : B \to B' \) is a unital norm equivalence, then there exists a decomposition \( k = k_+ \oplus k_- \) of \( k \) as a direct sum of ideals such that, with the corresponding decompositions

\[ B = B_+ \oplus B_-, \quad B_+ = B'_+ \oplus B'_1, \quad B'_- = B'_{-1}, \quad f = f_+ \oplus f_-, \quad f_k = f_{k_+} + f_{k_-}, \quad (3) \]

\[ f_+ : B_+ \to B'_+ \] is an isomorphism of quaternion algebras over \( k_+ \), and \( f_- : B_- \to B'_- \) is an anti-isomorphism of quaternion algebras over \( k_- \). (Hint. Reduce to the case that \( k \) is a local ring by applying 6.10 Exercise 11. Then imitate the beginning of the proof of the implication (iii) \( \Rightarrow \) (i) in the norm equivalence theorem.)

(b) Use (a) to prove a slightly weakened version of Knus’s theorem [58, V, (4.3.2)] (see also Gille 138 2.4): for quaternion algebras \( B, B' \) over \( k \), the following conditions are equivalent.

(i) \( B \) and \( B' \) are isomorphic.

(ii) \( B \) and \( B' \) are norm equivalent.

(iii) \( B \) and \( B' \) are norm similar.

129. Elementary idempotents and unital norm equivalences. Write \( e_{ij} (i, j = 1, 2) \) for the usual matrix units in the split quaternion algebra \( B = \text{Mat}_2(k) \) and prove for any element \( c \in B \) that there exists an automorphism of \( B \) sending \( e_{11} \) to \( c \) if and only if there exists a unital norm equivalence of \( B \) sending \( e_{11} \) to \( c \).

130. Octonionic norm equivalences. Let \( C \) be an octonion algebra over \( k \) and \( p \in C^\circ \). Show that \( L_p R_{p^{-1}} \) is

(a) always a unital norm equivalence of \( C \),

(b) an automorphism of \( C \) if and only if \( p^2 \in k1_C \),

(c) never an anti-automorphism of \( C \).

(Hint. Use Ex. 72(c))

131. Isotopes of composition algebras. Show that isotopes of a composition algebra \( C \) over \( k \) are composition algebras which are non-singular if \( C \) is, and which are isomorphic to \( C \) if \( k \) is a semi-local ring.

132. Zero divisor pairs of the real sedenions. Recall that the real sedenions \( S = \text{Cay}(\mathbb{O}, -1) = \mathbb{O} \oplus \mathbb{O} \) as defined in Ex. 99 form a conic real algebra with norm \( n_5 \) canonically isometric to \( n_0 \perp n_0 \). By a zero divisor pair of \( S \) we mean a pair \((x, y)\) of non-zero elements in \( S \) such that \( xy = 0 \). Note that if \((x, y)\) is a zero divisor pair of \( S \), then so is \((\alpha x, \beta y)\) for all \( \alpha, \beta \in \mathbb{R}^\times \). Thus the study of arbitrary zero-divisor pairs in \( S \) is equivalent to the one of zero divisor pairs with pre-assigned norm. With this in mind, we define

\[ \text{Zer}(S) := \{ (x, y) \in S \times S \mid xy = 0, \quad n_5(x) = n_5(y) = 2 \} \quad (4) \]

and let \( G := \text{Aut}(\mathbb{O}) \) act diagonally first on \( S \) and then on \( \text{Zer}(S) \) via

\[ G \times \text{Zer}(S) \to \text{Zer}(S), \quad (\sigma, (x, y)) \mapsto (\sigma(x), \sigma(y)). \]
Use Exc. 99 to show that \( \text{Zer}(\mathbb{S}) \) becomes a principal homogeneous \( G \)-space in this way, i.e., the action of \( G \) on \( \text{Zer}(\mathbb{S}) \) is simply transitive.

**Remark.** This result is a refined version of Moreno’s theorem [87 Cor. 2.14], which says that \( \text{Zer}(\mathbb{G}) \subseteq \mathbb{S} \times \mathbb{S} \) is a closed subset homeomorphic to \( \text{Aut}(\mathbb{G}) \).

The following sequence of exercises is designed to put the units of the Coxeter octonions (Exc. 16) in a broader perspective.

**Exercise 133.** Let \( q \) be a prime power and \( C := \text{Zor}(\mathbb{F}_q) \) the unique octonion algebra over the field with \( q \) elements. Show

\[ |C^\times| = q^2(q-1)(q^3-1), \quad |\{x \in C \mid n_C(x) = 1\}| = q^3(q^2-1), \]

**Exercise 134.** Positive definite integral quadratic modules and minimal vectors. By a positive definite integral quadratic module we mean a quadratic module \((M, Q)\) over \( \mathbb{Z} \) such that \( M \) is a finitely generated free abelian group and the quadratic form \( Q: M \to \mathbb{Z} \) is positive definite. Then \( M \) is an integral quadratic lattice in the positive definite real quadratic space \((M_{\mathbb{R}}, Q_{\mathbb{R}})\) in the sense of 3.12 and, conversely, every integral quadratic lattice in a positive definite real quadratic space becomes a positive definite integral quadratic module in a natural way. The discriminant of a positive definite integral quadratic module may be defined as in 3.12. A positive definite integral quadratic module is called indecomposable if it cannot be written as the sum of two orthogonal non-zero submodules.

Now let \((M, Q)\) be a positive definite finite integral quadratic module over \( \mathbb{Z} \). A vector \( x \in M \) is said to be minimal if it cannot be written as the sum of two vectors of strictly shorter length: \( x = y + z \) with \( y, z \in M \) and \( Q(y) < Q(x), Q(z) < Q(x) \) is impossible. The set of minimal vectors in \((M, Q)\) will be denoted by \( \text{Min}(M, Q) \). Two minimal vectors \( x, y \in M \) are said to be equivalent if there exists a finite sequence \( x = x_0, x_1, \ldots, x_{k-1}, x_k = y \) of minimal vectors in \( M \) such that \( Q(x_{i-1}, x_i) \neq 0 \) for \( 1 \leq i \leq k \).

(a) Show that \( \text{Min}(M, Q) \) generates the additive group \( M \).

(b) Show that equivalence of minimal vectors defines an equivalence relation on \( \text{Min}(M, Q) \).

(c) Denoting by \( [x] \) the equivalence class of \( x \in \text{Min}(M, Q) \) with respect to the equivalence relation defined in (b), and setting \( M_{[x]} := \sum_{y \in [x]} \mathbb{Z}y \), prove Eichler’s theorem: \((M, Q)\) splits into the orthogonal sum of indecomposable integral quadratic submodules \( M_{[x]} \), where \( [x] \) varies over the equivalence classes of \( \text{Min}(M, Q) \).

**Exercise 135.** Let \( C \) be a multiplicative conic alternative algebra over \( \mathbb{Z} \) such that the following conditions are fulfilled.

(a) \( C \) is free of rank 8 as a \( \mathbb{Z} \)-module.

(b) The norm of \( C \) is positive definite.

(c) The discriminant of the integral quadratic module \((C, n_C)\) is odd.

Prove that \( |C^\times| \leq 240 \), and that if \( |C^\times| = 240 \), then \((C, n_C)\) is an indecomposable positive definite integral quadratic module. (Hint. Reduce \( C \) mod 2 to obtain an octonion algebra \( C^\wedge \) over \( \mathbb{F}_2 \), and show that the fibers of the natural map \( C^\wedge \to C^\times \) consist of two elements. Then apply Excs. 133. 134.)

**Exercise 136.** Show that a quadratic étale algebra over the integers is split. Conclude that the algebra of Hurwitz quaternions cannot be obtained from the Cayley-Dickson construction: there are no quadratic \( \mathbb{Z} \)-algebra \( R \) and no scalar \( \mu \in \mathbb{Z} \) such that \( \text{Hur}(\mathbb{H}) \cong \text{Cay}(R, \mu) \).

**Remark.** It can also be shown that a quaternion algebra over the integers is split, but the proof requires more work.
137. Classification of octonion algebras over the integers (Van der Blij-Springer [125]). Show that an octonion algebra over \( \mathbb{Z} \) is either split or isomorphic to the Coxeter octonions. In order to do so, let \( C \) be a non-split octonion algebra over \( \mathbb{Z} \) with product \( x \cdot y \), write \( xy \) for the product in \( \text{Cox}(\mathbb{O}) \) and perform the following steps.

(a) Reduce to the case that \( C = \text{Cox}(\mathbb{O}) \) as additive groups, \( 1_C = 1_\mathbb{O} \) and \( n_C = n_{\text{Cox}(\mathbb{O})} \) (Hint. Use [4.6] and Exc. [126]).

(b) Show that there is an isomorphism \( \psi: C \otimes \mathbb{Z} \mathbb{F}_2 \sim \to \text{Cox}(\mathbb{O}) \otimes \mathbb{Z} \mathbb{F}_2 \) and use the fact that the orthogonal group of \( n_C \otimes \mathbb{Z} \mathbb{F}_2 \) is generated by orthogonal transvections (Dieudonné [24, Prop. 14]) to lift \( \psi \) to an orthogonal transformation \( \phi: C \to \text{Cox}(\mathbb{O}) \) such that \( \phi(x \cdot y) = \pm \phi(x)\phi(y) \) for all \( x, y \in C \times \). (Hint. Use the fact, known from the solution to Exc. [135], that the map \( C^\times \to (C \otimes \mathbb{Z} \mathbb{F}_2)^\times \) induced by the natural surjection \( C \to C \otimes \mathbb{Z} \mathbb{F}_2 \) is itself surjective and that each fiber consists of two elements.)

(c) Now prove that \( \phi \) or \( -\phi \) is an isomorphism.

138. Splitting fields of composition algebras. Let \( C \) be a composition algebra over a field \( F \). A field extension \( K/F \) is said to be a splitting field of \( C \) if the extended composition algebra \( C_K \) over \( K \) is split. Prove:

(a) (Ferrar [31, Lemma 5], Petersson-Racine [92, Proposition 4.3]). For a quadratic field extension \( K/F \) to be a splitting field of \( C \) it is necessary and sufficient that one of the following hold.

(i) \( C \cong F \).
(ii) \( C \) is split quadratic étale.
(iii) There exists an \( F \)-embedding \( K \hookrightarrow C \).

(b) The separable closure of \( F \) is a splitting field of \( C \).

27. Affine schemes

A treatment of octonions and Albert algebras over commutative rings would be incomplete without taking advantage of, and giving applications to, the theory of affine group schemes. Our aim in the present section will be to carry out a first thrust into this important topic. We do so by explaining the most elementary and basic notions from scheme theory and by illustrating them through a number of simple examples. We always focus attention on what is absolutely essential for the intended applications. Though a considerable amount of what we will be doing here retains its validity under much more general circumstances (e.g., in the setting of category theory), generalizations of this sort will be completely ignored.

Throughout we let \( k \) be an arbitrary commutative ring. In our treatment of affine \( k \)-schemes, we follow Demazure-Gabriel [22] by adopting the functorial point of view. However, in order to keep matters simple, the delicate formalism developed by loc. cit. in order to stay within a consistent framework of set theory will be avoided; instead, we favor a more stream-lined “naive” approach as given, e.g., by Jantzen [50]. Our notation will combine that of Jantzen [50] and Loos [71].

27.1. \( k \)-functors, subfunctors and direct products. By a \( k \)-functor we mean a functor \( X \) from the category of unital commutative associative \( k \)-algebras to the
category of sets:

\[ X : k\text{-}\mathbf{alg} \to \mathbf{set}. \]

Morphisms of \( k \)-functors are defined as natural transformations, so if \( X, X' \) are \( k \)-functors, a *morphism* \( f : X \to X' \) is a family of set maps \( f(R) : X(R) \to X'(R) \), one for each \( R \in k\text{-}\mathbf{alg} \), such that, for each morphism \( \rho : R \to R' \) in \( k\text{-}\mathbf{alg} \), the diagram

\[
\begin{array}{ccc}
X(R) & \xrightarrow{f(R)} & X'(R) \\
X(\rho) \downarrow & & \downarrow X'(\rho) \\
X(R') & \xrightarrow{f(R')} & X'(R')
\end{array}
\]

commutes. The category of \( k \)-functors will be denoted by \( k\text{-}\mathbf{fct} \). Given \( k \)-functors \( X, X' \), we will denote by \( \text{Mor}(X, X') \) the totality of morphisms from \( X \) to \( X' \). Note that a morphism \( f : X \to X' \) is an isomorphism if and only if the set maps \( f(R) : X(R) \to X'(R) \) are bijective for all \( R \in k\text{-}\mathbf{alg} \).

By a subfunctor of a \( k \)-functor \( X \) we mean a \( k \)-functor \( Y \) such that \( Y(R) \subseteq X(R) \) for all \( R \in k\text{-}\mathbf{alg} \) and the inclusion maps \( i(R) : Y(R) \to X(R) \) give rise to a morphism \( i : Y \to X \) of \( k \)-functors; in other words, for any morphism \( \rho : R \to R' \) in \( k\text{-}\mathbf{alg} \), we have \( X(\rho)(Y(R)) \subseteq Y(R') \), and the set map \( Y(\rho) : Y(R) \to Y(R') \) is induced by \( X(\rho) \) via restriction. We sometimes write \( Y \subseteq X \) for \( Y \) being a subfunctor of \( X \).

Let \( X_1, X_2 \) be \( k \)-functors. Then we define a \( k \)-functor \( X_1 \times X_2 \), called their *direct product*, by setting \( (X_1 \times X_2)(R) := X_1(R) \times X_2(R) \) for all \( R \in k\text{-}\mathbf{alg} \) and \( (X_1 \times X_2)(\rho) := X_1(\rho) \times X_2(\rho) \) for all morphisms \( \rho : R \to R' \) in \( k\text{-}\mathbf{alg} \). The direct product comes equipped with two *projection morphisms* \( p_i : X_1 \times X_2 \to X_i \) for \( i = 1, 2 \) such that \( p_i(R) \) is the projection from \( X_1(R) \times X_2(R) \) onto the \( i \)-th factor, for each \( R \in k\text{-}\mathbf{alg} \). It then follows that \( X_1 \times X_2 \) together with \( p_1, p_2 \) is an honest-to-goodness direct product in the category \( k\text{-}\mathbf{fct} \) by satisfying the corresponding universal property.

**27.2. The concept of an affine \( k \)-scheme.** Let \( R \in k\text{-}\mathbf{alg} \). We define

\[
\text{Spec}(R) := \text{Hom}_{k\text{-}\mathbf{alg}}(R, -) : k\text{-}\mathbf{alg} \to \mathbf{set},
\]

so \( \text{Spec}(R) \) is the \( k \)-functor given by

\[
\text{Spec}(R)(S) = \text{Hom}_{k\text{-}\mathbf{alg}}(R, S)
\]

for all \( S \in k\text{-}\mathbf{alg} \) and

\[
\text{Spec}(R)(\sigma) : \text{Hom}_{k\text{-}\mathbf{alg}}(R, S) \to \text{Hom}_{k\text{-}\mathbf{alg}}(R, S'),
\]

\[
\text{Hom}_{k\text{-}\mathbf{alg}}(R, S) \ni \varphi \mapsto \text{Spec}(R)(\sigma)(\varphi) := \sigma \circ \varphi \in \text{Hom}_{k\text{-}\mathbf{alg}}(R, S')
\]
for all morphisms $\sigma: S \to S'$ in $k\text{-alg}$. By an affine $k$-scheme or an affine scheme over $k$ we mean a $k$-functor that is isomorphic to $\text{Spec}(R)$, for some $R \in k\text{-alg}$. We view affine $k$-schemes as a full subcategory of $k\text{-fct}$, denoted by $k\text{-aff}$.

Let $\varphi: R' \to R$ be a morphism in $k\text{-alg}$. Then

$$\text{Spec}(\varphi) := \text{Hom}_{k\text{-alg}}(-, \varphi): \text{Spec}(R) \longrightarrow \text{Spec}(R')$$

is a morphism of $k$-functors, explicitly given by

$$\text{Spec}(\varphi)(S): \text{Spec}(R)(S) \longrightarrow \text{Spec}(R')(S),$$

$$\text{Hom}_{k\text{-alg}}(R,S) \ni \psi \longmapsto \text{Spec}(\varphi)(S)(\psi) := \psi \circ \varphi \in \text{Hom}_{k\text{-alg}}(R',S)$$

for all $S \in k\text{-alg}$. If $\varphi': R'' \to R'$ is another morphism in $k\text{-alg}$, we have

$$\text{Spec}(1_R) = 1_{\text{Spec}(R)}, \quad \text{Spec}(\varphi \circ \varphi') = \text{Spec}(\varphi') \circ \text{Spec}(\varphi).$$

Summing up we conclude that the data presented in (1), (4) define a contra-variant functor

$$\text{Spec}: k\text{-alg} \longrightarrow k\text{-fct},$$

which may also be regarded as a contra-variant functor

$$\text{Spec}: k\text{-alg} \longrightarrow k\text{-aff}.$$}

In the latter capacity, it will be seen in due course to induce an anti-equivalence of categories.

### 27.3. Affine $n$-space

Let $n$ be a positive integer. We define a $k$-functor $A^n_k$, called affine $n$-space, by setting $A^n_k(R) := R^n$ as a set and

$$A^n_k(\rho) := \rho^n: R^n \longrightarrow R^n, \quad R^n \ni (r_1, \ldots, r_n) \longmapsto (\rho(r_1), \ldots, \rho(r_n)) \in R^n$$

for a morphism $\rho: R \to R'$ in $k\text{-alg}$ as a set map. With independent indeterminates $t_1, \ldots, t_n$, we claim that

$$A^n_k \cong \text{Spec}(k[t_1, \ldots, t_n])$$

and, in particular, that $A^n_k$ is an affine scheme over $k$. Indeed, letting $R \in k\text{-alg}$ and $r_1, \ldots, r_n \in R$, write

$$\mathcal{E}^n(R)(r_1, \ldots, r_n): k[t_1, \ldots, t_n] \longrightarrow R$$

for the morphism in $k\text{-alg}$ given by

$$\mathcal{E}^n(R)(r_1, \ldots, r_n)(g) := g(r_1, \ldots, r_n) \quad (g \in k[t_1, \ldots, t_n]).$$
Note that $\varepsilon^n(R)(r_1, \ldots, r_n)$ is uniquely determined by the condition of sending $t_i$ to $r_i$ for $1 \leq i \leq n$. In this way we obtain a bijective set map

$$\varepsilon^n(R) : R^n \overset{\sim}{\rightarrow} \text{Hom}_{k-\text{alg}}(k[t_1, \ldots, t_n], R) = \text{Spec}(k[t_1, \ldots, t_n])(R)$$

varying functorially with $R$. Hence

$$\varepsilon^n : \mathbb{A}_k^n \overset{\sim}{\rightarrow} \text{Spec}(k[t_1, \ldots, t_n])$$

is an isomorphism of $k$-functors.

27.4. Proposition (Yoneda Lemma). Let $X$ be a $k$-functor and $R \in k$-alg. Then the assignment

$$\text{Mor}((\text{Spec}(R), X) \ni f \mapsto \Phi_{R,X}(f) := f(R)(1_R) \in X(R)$$

defines a bijection

$$\Phi_{R,X} : \text{Mor}((\text{Spec}(R), X) \overset{\sim}{\rightarrow} X(R),$$

and we have

$$\Phi_{R,X}^{-1}(x)(S)(\varphi) = X(\varphi)(x)$$

for all $x \in X(R), S \in k$-alg, $\varphi \in \text{Hom}_{k-\text{alg}}(R, S)$.

Proof. Given $x \in X(R), S \in k$-alg, we define a set map $\Theta(x)(S) : \text{Spec}(R)(S) \rightarrow X(S)$ by

$$\Theta(x)(S)(\varphi) := X(\varphi)(x) \quad (\varphi \in \text{Hom}_{k-\text{alg}}(R, S)).$$

For a morphism $\sigma : S \rightarrow S' \in k$-alg it follows easily from (27.3) that the diagram

$$\begin{array}{ccc}
\text{Spec}(R)(S) & \xrightarrow{\Theta(x)(S)} & X(S) \\
\text{Spec}(R)(\sigma) \downarrow & & \downarrow X(\sigma) \\
\text{Spec}(R)(S') & \xrightarrow{\Theta(\sigma)(S')} & X(S')
\end{array}$$

commutes. Thus $\Theta(x) \in \text{Mor}((\text{Spec}(R), X)$, and we have obtained a map $\Theta : X(R) \rightarrow \text{Mor}((\text{Spec}(R), X)$. It is now straightforward to verify that $\Theta \circ \Phi_{R,X}$ is the identity on $\text{Mor}((\text{Spec}(R), X)$ and $\Phi_{R,X} \circ \Theta$ is the identity on $X(R)$. Hence $\Phi_{R,X}$ is bijective with inverse $\Theta$. □

27.5. Corollary. Let $R, R' \in k$-alg.

(a) The map
is a bijection with inverse
\[ \text{Hom}_{k\text{-alg}}(R', R) \xrightarrow{\sim} \text{Mor}(\text{Spec}(R), \text{Spec}(R')), \quad \varphi \mapsto \text{Spec}(\varphi). \] (2)

(b) \( \varphi \in \text{Hom}_{k\text{-alg}}(R', R) \) is an isomorphism if and only if
\[ \text{Spec}(\varphi) \in \text{Mor}(\text{Spec}(R), \text{Spec}(R')) \]
is an isomorphism, and in this case \( \text{Spec}(\varphi)^{-1} = \text{Spec}(\varphi^{-1}) \).

**Proof.** Specializing Proposition 27.4 to \( X := \text{Spec}(R') \) and applying (27.2.3), we obtain (a). It remains to establish (b). If \( \varphi \) is an isomorphism, then so is \( \text{Spec}(\varphi) \), by 27.2.6, with \( \text{Spec}(\varphi)^{-1} = \text{Spec}(\varphi^{-1}) \). Conversely, suppose \( \text{Spec}(\varphi) \) is an isomorphism. Then there exists a morphism \( g: \text{Spec}(R') \to \text{Spec}(R) \) such that \( g \circ \text{Spec}(\varphi) = 1_{\text{Spec}(R')} \), \( \text{Spec}(\varphi) \circ g = 1_{\text{Spec}(R')} \). Here (a) implies \( g = \text{Spec}(\varphi') \) for some morphism \( \varphi': R \to R' \) in \( k\text{-alg} \). From (27.2.6) we therefore deduce \( \text{Spec}(\varphi \circ \varphi') = 1_{\text{Spec}(R')} \), \( \text{Spec}(\varphi' \circ \varphi) = 1_{\text{Spec}(R')} \), and (a) again shows that \( \varphi \) is an isomorphism with inverse \( \varphi' \). \( \square \)

**27.6. Regular functions.** With affine 1-space \( \mathbb{A}^1_k \), also called the *affine line*, we consider the contra-variant functor
\[ k[-] := \text{Mor}(-, \mathbb{A}^1_k): k\text{-fct} \to \text{set}, \] (1)
so we have
\[ k[X] := \text{Mor}(X, \mathbb{A}^1_k) \] (2)
for all \( k \)-functors \( X \) and
\[ k[f]: k[X] \to k[X], \quad \text{Mor}(X', \mathbb{A}^1_k) \ni f' \mapsto k[f](f') := f' \circ f \in \text{Mor}(X, \mathbb{A}^1_k) \] (3)
for all morphisms \( f: X \to X' \) of \( k \)-functors. Since \( \mathbb{A}^1_k(R) = R \) for all \( R \in k\text{-alg} \), the set \( k[X] \), for any \( k \)-functor \( X \), carries the structure of a unital commutative associative \( k \)-algebra by defining the scalar multiple \( \alpha f \in k[X] \), the sum \( f_1 + f_2 \in k[X] \) and the product \( f_1 f_2 \in k[X] \) according to the rules
\[ (\alpha f)(R)(x) := \alpha f(R)(x), \]
\[ (f_1 + f_2)(R)(x) := f_1(R)(x) + f_2(R)(x), \]
\[ (f_1 f_2)(R)(x) := f_1(R)(x) f_2(R)(x) \] (4)
for \( \alpha \in k, f, f_1, f_2 \in k[X], R \in k\text{-alg} \) and \( x \in X(R) \). Thus \( k[X] \in k\text{-alg} \), with
We call \( k[X] \) the \( k \)-algebra of regular functions on \( X \). Note for \( R \in k\text{-alg} \) that the bijection

\[
\Phi_{R,A^n_1} : k[\text{Spec}(R)] \sim R
\]

of Proposition 27.4 is an isomorphism of \( k \)-algebras.

If \( f : X \to X' \) is a morphism of \( k \)-functors, then one checks easily that

\[
k[f] : k[X'] \to k[X]
\]

is a morphism of unital commutative associative \( k \)-algebras. Thus the functor (1) may actually be viewed as a contra-variant functor

\[
k[-] = \text{Mor}(-, A^n_1) : k\text{-fct} \to k\text{-alg},
\]

from which we recover (1) by composing (7) with the forgetful functor \( k\text{-alg} \to \text{set} \).

On the other hand, restricting the functor (7) to the category of affine \( k \)-schemes, we obtain a contra-variant functor

\[
k[-] = \text{Mor}(-, A^n_1) : k\text{-aff} \to k\text{-alg}.
\]

The fact that all these functors are denoted by the same symbol will not cause any confusion.

27.7 Example. Let \( n \) be a positive integer. For \( g \in k[t_1, \ldots, t_n] \), the set maps

\[
\tilde{g}(R) : R^n \to R, \quad (r_1, \ldots, r_n) \mapsto \tilde{g}(R)(r_1, \ldots, r_n) := g(r_1, \ldots, r_n)
\]

vary functorially with \( R \in k\text{-alg} \), hence give rise to an element \( \tilde{g} \in \text{Mor}(A^n_1, A^n_1) = k[A^n_1] \). On the other hand, \( g \) determines a unique morphism \( g^* : k[t] \to k[t_1, \ldots, t_n] \) in \( k\text{-alg} \) given by

\[
g^*(h) := h(g) \quad (h \in k[t]),
\]

and one checks that the diagram

\[
\begin{array}{ccc}
R^n & \xrightarrow{\tilde{g}(R)} & R \\
\epsilon^n(R) \downarrow & & \downarrow \epsilon^1(R) \\
\text{Spec}(k[t_1, \ldots, t_n])(R) & \xrightarrow{\text{Spec}(g^*)(R)} & \text{Spec}(k[t])(R)
\end{array}
\]

commutes. Hence, by Corollary 27.5(a), since every morphism \( k[t] \to k[t_1, \ldots, t_n] \) in \( k\text{-alg} \) has form \( g^* \) for a unique \( g \in k[t_1, \ldots, t_n] \),
Affine schemes

\[ k[t_1, \ldots, t_n] \xrightarrow{\sim} k[A^n_k], \quad g \mapsto \tilde{g} \]  

is an isomorphism of \( k \)-algebras. We usually identify \( k[t_1, \ldots, t_n] = k[A^n_k] \)

\[ k[t_1, \ldots, t_n] \ni g = \tilde{g} \in k[A^n_k] \]  

accordingly.

27.8. Proposition. The contra-variant functors

\[ \text{Spec}: \text{k-alg} \to \text{k-fct}, \quad [\cdot]: \text{k-fct} \to \text{k-alg} \]

are adjoint to one another in the sense that, for all \( k \)-functors \( X \) and all \( R \in \text{k-alg} \), there exists a natural bijection

\[ \Psi_{X,R}: \text{Mor}(X, \text{Spec}(R)) \xrightarrow{\sim} \text{Hom}_{\text{k-alg}}(R, k[X]) \]

given by

\[ \Psi_{X,R}(f)(r)(S)(x) = f(S)(x)(r) \]  

for all \( f \in \text{Mor}(X, \text{Spec}(R)) \), \( r \in R \), \( S \in \text{k-alg} \), \( x \in X(S) \). Moreover,

\[ \Psi_{X,R}^{-1}(g)(S)(x)(r) = g(r)(S)(x) \]  

for all \( g \in \text{Hom}_{\text{k-alg}}(R, k[X]) \), \( S \in \text{k-alg} \), \( x \in X(S) \), \( r \in R \).

Proof. We define \( \Psi := \Psi_{X,R} \) by [1]. Since \( f(S)(x): R \to S \) is a morphism in \( k \)-alg, so will be \( (\Psi)(S): R \to k[X] \) once we have shown that the left-hand side of [1] varies functorially with \( S \). Thus, fixing \( r \in R \) and a morphism \( \sigma: S \to S' \) in \( k \)-alg, we must show with \( g := \Psi(f) \) that the diagram

\[ \begin{array}{ccc}
X(S) & \xrightarrow{g(r)(S)} & S \\
\downarrow{X(\sigma)} & & \downarrow{\sigma} \\
X(S') & \xrightarrow{g(r)(S')} & S'
\end{array} \]  

commutes, which follows by a straightforward computation from [1] and the commutativity of

\[ \begin{array}{ccc}
X(S) & \xrightarrow{f(S)} & \text{Spec}(R)(S) \\
\downarrow{X(\sigma)} & & \downarrow{\text{Spec}(R)(\sigma)} \\
X(S') & \xrightarrow{f(S')} & \text{Spec}(R)(S').
\end{array} \]

Conversely, define \( \Psi': \text{Hom}_{\text{k-alg}}(R, k[X]) \to \text{Mor}(X, \text{Spec}(R)) \) by
\[\Psi'(g)(S)(x)(r) := g(r)(S)(x)\]  

(4) \[\text{ADJPR}\]

for \(g \in \text{Hom}_{k\text{-alg}}(R, k[X]), S \in k\text{-alg}, x \in X(S), r \in R\). Again we must show that the set map \(\Psi'(g)(S) : X(S) \to \text{Spec}(R)(S)\) varies functorially with \(S\), i.e., that for a morphism \(\sigma : S \to S'\) in \(k\text{-alg}\) the diagram

\[
\begin{array}{ccc}
X(S) & \xrightarrow{\Psi'(g)(S)} & \text{Spec}(R)(S) \\
\downarrow & & \downarrow \\
X(S') & \xrightarrow{\Psi'(g)(S')} & \text{Spec}(R)(S')
\end{array}
\]

commutes, which follows from the commutativity of (3) for all \(r \in R\). Finally, the definitions (1), (4) show that the maps \(\Psi, \Psi'\) are inverse to one another. \(\square\)

27.9. Example. The affine \(k\)-scheme \(\text{Spec}(k)\) satisfies

\[\text{Spec}(k)(R) = \text{Hom}_{k\text{-alg}}(k, R) = \{\varnothing_R\}\]  

(1) \[\text{SPEK}\]

for all \(R \in k\text{-alg}\), where

\[\varnothing_R : k \to R, \quad \alpha \mapsto (\varnothing_R(\alpha)) := \alpha 1_R.\]  

(2) \[\text{BUR}\]

is the unit morphism in \(k\text{-alg}\) corresponding to \(R\). Hence

\[\text{Spec}(k)(\varnothing)(\varnothing_R) = \varnothing_S\]  

(3) \[\text{SPEPHI}\]

for all morphisms \(\varnothing : R \to S\) in \(k\text{-alg}\).

Now let \(X\) be any \(k\)-functor. By Proposition 27.8 there is a unique morphism \(\sigma_X : X \to \text{Spec}(k)\), called the structure morphism of \(X\), and (1), (3) imply for all \(R \in k\text{-alg}\) that

\[\sigma_X(R) : X(R) \longrightarrow \text{Spec}(k)(R) = \{\varnothing_R\}\]

is the constant map

\[X(R) \ni x \mapsto \varnothing_R \in \text{Spec}(k)(R).\]

Moreover, every morphism \(f : X \to X'\) of \(k\)-functors is one over \(\text{Spec}(k)\) in the sense that the triangle

\[
\begin{array}{ccc}
X & \xrightarrow{f} & X' \\
\downarrow & & \downarrow \\
\text{Spec}(k) & \xrightarrow{\sigma_X} & \text{Spec}(k)
\end{array}
\]

commutes. Finally, if \(X = \text{Spec}(R)\) is an affine \(k\)-scheme, then

\[\sigma_X = \text{Spec}(\varnothing_R).\]  

(4) \[\text{SIGMAX}\]
27.10. Proposition. (a) Let \( X \) be a \( k \)-functor. With the notation of Proposition 27.8,

\[
f_X := \Psi^{-1}_{X,k[X]}(1_{k[X]}): X \rightarrow \text{Spec}(k[X])
\]

is a morphism of \( k \)-functors such that

\[
f_X(R)(x)(g) = g(R)(x)
\]

for all \( R \in k\text{-alg} \), \( x \in X(R) \), \( g \in k[X] \), and if \( h: X \rightarrow X' \) is any morphism of \( k \)-functors, then the diagram

\[
\begin{array}{ccc}
X & \xrightarrow{f_X} & \text{Spec}(k[X]) \\
\downarrow h & & \downarrow \text{Spec}(k[h]) \\
X' & \xrightarrow{f_{X'}} & \text{Spec}(k[X'])
\end{array}
\]

commutes.

(b) With the notation of Proposition 27.4,

\[
f_{\text{Spec}(R)} = \text{Spec}(\Phi R, A^1_k)
\]

(c) A \( k \)-functor \( X \) is an affine \( k \)-scheme if and only if \( f_X \) is an isomorphism.

Proof. (a) That the \( k \)-functor \( f_X \) satisfies (2) follows immediately from (27.8.2). Using (2), it is now straightforward to verify the commutativity of (3).

(b) Put \( X := \text{Spec}(R) \). We have noted in (27.6.6) that \( \Phi R, A^1_k: k[X] \rightarrow R \) is an isomorphism of \( k \)-algebras. By Corollary 27.5, therefore,

\[
\text{Spec}(\Phi R, A^1_k): X \xrightarrow{\sim} \text{Spec}(k[X])
\]

is an isomorphism of \( k \)-functors. In order to establish (4), let \( S \in k\text{-alg} \), \( x \in X(S) \), \( g \in k[X] \). With \( \Phi := \Phi R, A^1_k \) we must show \( \text{Spec}(\Phi)(S)(x)(g) = f_X(S)(x)(g) \), which follows easily by direct computation since the diagram

\[
\begin{array}{ccc}
\text{Spec}(R)(R) & \xrightarrow{g(R)} & R \\
\downarrow \text{Spec}(R)(x) & & \downarrow x \\
\text{Spec}(R)(S) & \xrightarrow{g(S)} & S
\end{array}
\]

commutes.

(c) follows immediately from (3), (4) and (5). \( \square \)

27.11. Corollary. The contra-variant functors
4 Composition algebras

\[
\begin{array}{ccc}
\text{k-alg} & \xrightarrow{\text{Spec}} & \text{k-aff} \\
\downarrow \text{k}[-] & & \\
\end{array}
\]

define an anti-equivalence of categories.

Proof. Let \(X\) be an affine \(k\)-scheme. Then \(f_X : X \xrightarrow{\sim} \text{Spec}(k[X])\) is an isomorphism by Proposition 27.10 (c), and (27.10.3) shows that the family \(f_X, X \in \text{k-aff}\), determines an isomorphism of functors from \(1_{\text{k-aff}}\) to \(\text{Spec} \circ k[-]\). Conversely, let \(R \in \text{k-alg}\). Then the bijective map

\[
\Phi = \Phi_{R, A_1^1} : k[\text{Spec}(R)] \xrightarrow{\sim} R
\]

of Proposition 27.4 by (27.6.6) is an isomorphism of \(k\)-algebras. Now let \(\rho : R \to R'\) be a morphism of \(k\)-algebras. Since for all \(f \in k[\text{Spec}(R)]\) the diagram

\[
\begin{array}{ccc}
\text{Spec}(R)(R) & \xrightarrow{f(R)} & R \\
\downarrow \text{Spec}(R)(\rho) & & \downarrow \rho \\
\text{Spec}(R)(R') & \xrightarrow{f(R')} & R'
\end{array}
\]

commutes, one checks that so does

\[
\begin{array}{ccc}
k[\text{Spec}(R)] & \xrightarrow{\Phi_{R, A_1^1}} & R \\
\downarrow k[\text{Spec}(\rho)] & & \downarrow \rho \\
k[\text{Spec}(R')] & \xrightarrow{\Phi_{R', A_1^1}} & R'.
\end{array}
\]

Thus the family \(\Phi_{R, A_1^1}, R \in \text{k-alg}\), determines an isomorphism of functors from the composition \(k[-] \circ \text{Spec}\) to \(1_{\text{k-alg}}\). \(\square\)

27.12. Notational conventions. (a) Let \(f : X \to X'\) be a morphism of \(k\)-functors. If there is no danger of confusion, the set map \(f(R) : X(R) \to X'(R)\) for \(R \in \text{k-alg}\) will simply be written as \(f\):

\[
f : X(R) \longrightarrow X'(R) \quad (R \in \text{k-alg}). \quad (1)
\]

For a morphism \(\rho : R \to R'\) in \(\text{k-alg}\) and \(x \in X(R)\), we therefore have

\[
f(X(\rho)(x)) = X'(\rho)f(x). \quad (2)
\]

(b) Let \(X\) be an affine \(k\)-scheme. Then we identify
by means of the isomorphism \( f_X \) of Proposition 27.10. Given \( R \in \text{alg} \), \( x \in X(R) \) and \( f \in k[X] \), an application of (27.10.2) yields

\[
x(f) = f_x(R)(f) = f(R)(x),
\]

hence

\[
x(f) = f(x).
\]

(c) Let \( f : X \to X' \) be a morphism of affine \( k \)-schemes. By Corollary 27.11 there is a unique morphism \( f^* : k[X'] \to k[X] \) in \( k \text{-alg} \) having \( f = \text{Spec}(f^*) \). We call \( f^* \) the co-morphism of \( f \).

27.13. Direct products of affine schemes. Let \( X_i \), for \( i = 1, 2 \) be affine \( k \)-schemes. Then the \( k \)-functor \( X_1 \times X_2 \) of \( \text{Spec} \) is an affine \( k \)-scheme as well. More precisely, one checks easily that

\[
\Pi : X_1 \times X_2 \to \text{Spec}(k[X_1] \otimes k[X_2])
\]

is an isomorphism. Given

\[
\Pi(x_1, x_2)(f_1 \otimes f_2) := x_1(f_1) x_2(f_2) = f_1(x_1) f_2(x_2)
\]

for \( R \in \text{alg} \), \( x_i \in X_i(R) \), \( f_i \in k[X_i] \), \( i = 1, 2 \) is an isomorphism. Note that the projections \( p_i : X_1 \times X_2 \to X_i \) correspond to the co-morphisms \( p_i^* : k[X_i] \to k[X_1] \otimes k[X_2] \) given by \( p_i^*(f_i) = f_i \otimes 1_{k[X_2]} \) and \( p_2^*(f_2) = 1_{k[X_1]} \otimes f_2 \).

27.14. Closed subfunctors. Let \( X \) be an affine \( k \)-scheme. For any subset \( I \subseteq k[X] \), we use (27.12.4) to define a subfunctor \( V(I) \) of \( X \) by setting

\[
V(I)(R) := \{ x \in X(R) \mid x(I) = \{0\} \} = \{ x \in X(R) \mid \forall f \in I : f(x) = 0 \}
\]

for all \( R \in \text{alg} \). We call \( V(I) \) the closed subfunctor of \( X \) determined by \( I \). On the other hand, if \( I \subseteq k[X] \) is an ideal, with canonical projection \( \pi : k[X] \to k[X]/I \), then \( \text{Spec}(\pi) : \text{Spec}(k[X]/I) \to \text{Spec}(k[X]) \) may be regarded as an isomorphism

\[
\text{Spec}(\pi) : \text{Spec}(k[X]/I) \to V(I).
\]

In particular, closed subfunctors of \( X \) are affine \( k \)-schemes. If \( I' \) is another ideal in \( k[X] \), with canonical projection \( \pi' : k[X] \to k[X]/I' \), then we claim

\[
I \subseteq I' \iff V(I') \subseteq V(I).
\]

The implication from left to right being obvious, let us assume \( V(I') \subseteq V(I) \). Since these are both affine \( k \)-schemes, the inclusion \( V(I') \hookrightarrow V(I) \) of closed subfunctors of \( X \) has the form \( \text{Spec}(\rho) \) for some morphism \( \rho : R/I \to R/I' \) in \( \text{alg} \) satisfying \( \rho \circ \pi = \pi' \). Thus \( I \subseteq \text{Ker}(\rho \circ \pi) = \text{Ker}(\pi') = I' \).
27.15. Open subfunctors. Let $X$ be an affine $k$-scheme. For any subset $I \subseteq k[X]$, we define a subfunctor $D(I)$ of $X$ by setting

$$D(I)(R) := \{ x \in X(R) \mid Rx(I) = R \} = \{ x \in X(R) \mid \sum_{f \in I} Rf(x) = R \}$$

for all $R \in k\text{-alg}$. This is indeed a subfunctor of $X$ since, for all morphisms $\rho : R \to R'$ in $k\text{-alg}$ and all $x \in X(R)$, we find finitely many $r_i \in R, f_i \in I$ such that $\sum r_i f_i(x) = 1_R$, which by (27.12.2) implies $\sum \rho(r_i)f_i(X(\rho))(x) = \sum \rho(r_i)\rho(f_i(x)) = \rho(\sum r_i f_i(x)) = 1_{R'}$, and we conclude $X(\rho)(x) \in D(I)(R')$.

Subfunctors of $X$ having the form $D(I)$ for some $I \subseteq k[X]$ are said to be open. Of particular importance is the case of a principal open subfunctor, defined by the property that $I = \{ f \}, f \in k[X]$, is a singleton. We put $X_f := D(f) := D(\{ f \})$ and have

$$X_f(R) = \{ x \in X(R) \mid f(x) \in R^\times \} = \{ x \in X(R) \mid x(f) \in R^\times \}.$$

The elements $x \in X(R) = \text{Hom}_{k\text{-alg}}(k[X], R)$ having $x(f) \in R^\times$ can be characterized by the property that they factor through the localization $k[X]_f$, in which case they do so uniquely. Thus there is a natural identification

$$X_f = \text{Spec}(k[X]_f)$$

such that the co-morphism of the inclusion $X_f \hookrightarrow X$ is the canonical map $k[X] \to k[X]_f$. In particular, principal open subfunctors of affine $k$-schemes are affine. Note, however, that an arbitrary open subfunctor of an affine $k$-scheme will in general not be affine.

27.16. $k$-group schemes. By a $k$-group functor we mean a functor from the category $k\text{-alg}$ to the category of groups:

$$G : k\text{-alg} \longrightarrow \text{grp}.$$

By composing $G$ with the forgetful functor $\text{grp} \to \text{set}$, we obtain a $k$-functor, also denoted by $G$, to which the formalism of the preceding subsections applies. By a subgroup functor of $G$ we mean a subfunctor $H$ of $G$ (viewed as a $k$-functor) such that $H(R)$ is a subgroup of $G(R)$ for all $R \in k\text{-alg}$. Then $H$ may be regarded as a $k$-group functor in its own right. More generally, morphisms of $k$-group functors are defined as natural transformations. Thus, given $k$-group functors $G, G'$, a morphism $f : G \to G'$ is nothing else than a morphism of $k$-functors making $f(R) : G(R) \to G'(R)$ a group homomorphism for all $R \in k\text{-alg}$.

By an affine $k$-group scheme, we mean a $k$-group functor that, regarded as a $k$-functor, is isomorphic to an affine $k$-scheme, so we have $G \cong \text{Hom}_{k\text{-alg}}(R, -)$ as $k$-functors, for some $R \in k\text{-alg}$. From now on, we will drop the prefix “affine” and just talk about $k$-group schemes to mean affine $k$-group schemes.
27.17. Examples. (a) The additive group of $k$ is defined as the $k$-group functor $G_{\mathbb{A}}$ given by $G_{\mathbb{A}}(R) = R$ (viewed as an additive group) for all $R \in k\text{-}\text{alg}$ and $G_{\mathbb{A}}(\varphi) = \varphi$ for all morphisms $\varphi: R \to S$ in $k\text{-}\text{alg}$. Thus $G_{\mathbb{A}} = \mathbb{A}_k$ as $k$-functors and $k[G_{\mathbb{A}}] \cong k[t]$ canonically.

(b) The multiplicative group of $k$ is defined as the $k$-group functor $G_{\mathbb{G}}$ given by $G_{\mathbb{G}}(R) = R^\times$ (viewed as a multiplicative group) for all $R \in k\text{-}\text{alg}$ and $G_{\mathbb{G}}(\varphi): R^\times \to S^\times$ induced by a morphism $\varphi: R \to S$ in $k\text{-}\text{alg}$ via restriction. Thus $G_{\mathbb{G}} = (\mathbb{A}_k^1)_t$ as $k$-functors and $k[G_{\mathbb{G}}] \cong k[t, t^{-1}]$ canonically.

27.18. Example. Let $M$ be a $k$-module. Generalizing the additive group of $k$ as in Example 27.17(a), we obtain a $k$-group functor $M_{\mathbb{A}}$ by setting $M_{\mathbb{A}}(R) := M_R := M \otimes R$ (viewed as an additive group) for all $R \in k\text{-}\text{alg}$ and $M_{\mathbb{A}}(\varphi) := 1_M \otimes \varphi: M_{\mathbb{A}}(R) \to M_{\mathbb{A}}(S)$ (viewed as an additive group homomorphism) for all morphisms $\varphi: R \to S$ in $k\text{-}\text{alg}$. Regarded just as a $k$-functor, $M_{\mathbb{A}}$ has made its appearance before, in our treatment of polynomial laws (§13). Writing $S(M^\times)$ for the symmetric algebra of the dual of $M$ (Bourbaki [12, III, §6]), we claim that if $M$ is finitely generated projective, then $M_{\mathbb{A}}$ is a $k$-group scheme with $k[M_{\mathbb{A}}] \cong S(M^\times)$ canonically.

Indeed, for any $R \in k\text{-}\text{alg}$, the universal property of the symmetric algebra combined with [10.1] and Lemma [10.11] yield the following chain of canonical isomorphisms:

$$\text{Hom}_{k\text{-}\text{alg}}(S(M^\times), R) \cong \text{Hom}_k(M^\times, R) \cong \text{Hom}_R(M^\times \otimes R, R)$$

$$\cong (M^\times \otimes R)^\times \cong M^{**} \otimes R \cong M \otimes R = M_{\mathbb{A}}(R).$$

Keeping track of how these isomorphisms act on individual elements, we obtain an identification

$$M_{\mathbb{A}}(R) = \text{Hom}_{k\text{-}\text{alg}}(S(M^\times), R)$$

such that $u \otimes r$ for $u \in M, r \in R$ is the unique unital $k$-algebra homomorphism $S(M^\times) \to R$ satisfying

$$(u \otimes r)(v^\times) = \langle v^\times, u \rangle r$$

for all $v^\times \in M^\times$. It is now easily checked that, for any morphism $\varphi: R \to S$ in $k\text{-}\text{alg}$, this identification matches $M_{\mathbb{A}}(\varphi)$ with $\text{Hom}_{k\text{-}\text{alg}}(S(M^\times), \varphi)$, which completes the proof.

27.19. Scalar polynomial laws revisited. Since $\mathbb{A}_k^1$, the affine line, is nothing else than the forgetful functor $k\text{-}\text{alg} \to \text{set}$, it follows for any $k$-module $M$ that $k[M_{\mathbb{A}}] = \text{Mor}(M_{\mathbb{A}}, \mathbb{A}_k^1)$ agrees with the $k$-algebra of scalar polynomial laws on $M$ as defined in [13.2]. Thus Example 27.18 combined with Corollary 27.11 implies $\text{Pol}_k(M, k) \cong S(M^\times)$ as $k$-algebras provided $M$ is finitely generated projective.

27.20. Example. Let $A$ be a unital associative $k$-algebra which is finitely generated projective as a $k$-module. We claim that $\text{GL}_1(A)$ defined by $\text{GL}_1(A)(R) := A_R^\times$ (viewed as a multiplicative group) for all $R \in k\text{-}\text{alg}$ and $\text{GL}_1(A)(\varphi): A_R^\times \to A_S^\times$...
induced from a morphism \( \varphi : R \to S \) in \( k\text{-}\textup{alg} \) via restriction of \( 1_A \otimes \varphi : A_R \to A_S \) is a group scheme over \( k \). Indeed, we know from Example 27.18 that \( A_a \) is a group scheme over \( k \). Let \( f \in k[A_a] \) be any regular function on \( A_a \) such that \( x \in A_R, R \in k\text{-}\textup{alg} \), is invertible if and only if \( f(x) \) is a unit in \( R \) (for instance, one could choose \( f = \det \circ L \), where \( L : A \to \text{End}_k(A) \) is the left multiplication of \( A \) and \( \det : \text{End}_k(A) \to k \) is the determinant, which are both compatible with base change). Then \( GL_1(A) = (A_a)_f \) as \( k\text{-}-\textup{functors} \) and (27.15.3) shows that \( GL_1(A) \) is a \( k\text{-}\textup{group scheme satisfying} \)

\[
k[GL_1(A)] \cong k[A_a]_f. \tag{1} \]

The preceding construction specializes to \( G_m = GL_1(k) \) but also to \( GL_n : = GL_1(\text{Mat}_n(k)) \), \( (2) \)

where we have

\[
k[GL_n] \cong k[t_{ij} \mid 1 \leq i, j \leq n]_{\det}. \tag{3} \]

27.21. Some identifications. We fix two \( k\text{-}\textup{modules} M, N \) and let \( R \in k\text{-}\textup{alg} \). By \( 10.1 \) the \( k\text{-}\textup{linear map} \)

\[
\text{Hom}_k(M, N) \longrightarrow \text{Hom}_R(M_R, N_R), \quad \eta \longmapsto \eta_R
\]

extends uniquely to an \( R\text{-}\textup{linear map} \)

\[
\Phi_{R, R} : \text{Hom}_k(M, N)_R \longrightarrow \text{Hom}_R(M_R, N_R)
\]

such that

\[
\Phi_{R, R}(\eta \otimes r)(u \otimes r') = \eta(u) \otimes rr' \tag{1} \]

for \( \eta \in \text{Hom}_k(M, N), u \in M, r, r' \in R \). Now suppose \( \varphi : R \to S \) is a morphism in \( k\text{-}\textup{alg}, \) so we have \( S \in R\text{-}\textup{alg} \) via \( \varphi \), identify \( M_S = (M_R)_S, N_S = (N_R)_S \) by means of \( 10.5.1 \) and let

\[
\Psi : \text{Hom}_R(M_R, N_R) \longrightarrow \text{Hom}_S((M_R)_S, (N_R)_S) = \text{Hom}_S(M_S, N_S)
\]

be the \( R\text{-}\textup{linear map given by} \)

\[
\Psi(\zeta) := \zeta_S = \zeta \otimes_R 1_S \quad (\zeta \in \text{Hom}_R(M_R, N_R)). \tag{2} \]

Then it is straightforward to check that the diagram
Finally, let us assume that \( M, N \) are both finitely generated projective. Then \( \Phi_{k,R} \) is an isomorphism (Bourbaki [12, II, § 5, Prop. 7]), allowing us to identify

\[
\text{Hom}_k(M, N) \cong \text{Hom}_R(M, N)
\]

by means of \( \Phi_{k,R} \), ditto for \( S \) in place of \( R \), and since (3) commutes, we conclude

\[
\zeta_S = \text{Hom}_k(M, N)(\phi)(\zeta)
\]

for all \( \zeta \in \text{Hom}_k(M, N)_R \).

27.22. Example. Let \( M \) be a finitely generated projective \( k \)-module and \( R \in k\text{-alg} \). The identifications of 27.21 show \( \text{End}_k(M)_R = \text{End}_R(M) \) as \( R \)-algebras. Thus

\[
\text{GL}(M) := \text{GL}_1(\text{End}_k(M))
\]

is a \( k \)-group scheme having \( \text{GL}(M)(R) = \text{GL}(M) \) for all \( R \in k\text{-alg} \) and

\[
\text{GL}(M)(\phi) : \text{GL}(M)_R \rightarrow \text{GL}(M)_S, \quad \text{GL}(M)_R \ni \eta \mapsto \eta_S \in \text{GL}(M)_S
\]

for any morphism \( \phi : R \rightarrow S \) in \( k\text{-alg} \). Moreover, (27.20) implies

\[
k[\text{GL}(M)] = k[\text{End}_k(M)]_{\text{det}}.
\]

27.23. Example. Let \( A \) be a non-associative \( k \)-algebra. We define a \( k \)-group functor \( \text{Aut}(A) \) by setting \( \text{Aut}(A)(R) := \text{Aut}(A)_R \) for all \( R \in k\text{-alg} \) and

\[
\text{Aut}(A)(\phi) : \text{Aut}(A)_R \rightarrow \text{Aut}(A)_S, \quad \text{Aut}(A)_R \ni \eta \mapsto \eta_S \in \text{Aut}(A)_S
\]

for all morphisms \( \phi : R \rightarrow S \) in \( k\text{-alg} \), where we regard \( S \) as an \( R \)-algebra via \( \phi \) and use (10.3.1) to identify \( A_S = (A_R)_S \) as \( S \)-algebras. We claim:

(*) if \( A \) is finitely generated projective as a \( k \)-module, then \( \text{Aut}(A) \) is a closed subfunctor of \( \text{GL}(A) \) and hence, in particular, a \( k \)-group scheme, called the automorphism group scheme of \( A \).

In order to see this, let \( u, v \in A \) and \( w^* \in A^* \). For \( R \in k\text{-alg} \) we define a set map

\[
f_{u,v,w^*}(R) : \text{GL}(A)_R \rightarrow R
\]

by
for \( \eta \in \GL(A_R) \). It follows immediately from Lemma \([10.11]\) and \([27.22]\) that these set maps vary functorially with \( R \). Thus \( f_{u,v,w^*} \in k(\GL(A)) \). Moreover, since the canonical pairing \( A^* \times A \to k \) is non-singular, \( \eta \in \GL(A_R) \) belongs to \( \Aut(A_R) \) if and only if \( f_{u,v,w^*}(\eta) = 0 \) for all \( u,v \in A \) and all \( w^* \in A^* \). Hence we deduce from \([27.14]\) that \( \Aut(A) \) is the closed subfunctor of \( \GL(A) \) determined by the ideal \( I \subseteq k[\GL(A)] \) generated by the quantities \( f_{u,v,w^*} \), \( u,v \in A \), \( w^* \in A^* \). In particular, assertion (+) follows. Note that, since \( A \) and \( A^* \) are both finitely generated as \( k \)-modules, so is \( I \) as an ideal in \( k[\GL(A)] \).

**27.24. Example.** In a similar vein, let \( Q := (M,q) \) be a quadratic module over \( k \). Then

\[
O(Q) := O(M,q) := \{ \eta \in \GL(M) \mid q \circ \eta = q \}
\]  

(1)

is a subgroup of \( \GL(M) \), called the orthogonal group of \( Q \). Moreover, this group may be converted into a \( k \)-group functor by using Corollary \([12.5]\) to define \( O(Q)(R) := O(Q_R) \), \( Q_R := (M_R,q_R) \), for all \( R \in k\text{-}\text{alg} \), and

\[
O(Q)(\varphi) : O(Q)(R) \to O(Q)(S), \quad O(Q_R) \ni \eta \mapsto \eta_S \in O(Q_S)
\]

(2)

for all morphisms \( \varphi : R \to S \) in \( k\text{-}\text{alg} \), where we employ the same identifications as in \([27.23]\). If \( M \) is finitely generated projective, we let \( (w_i)_{1 \leq i \leq n} \) be a finite family of generators for \( M \) and define set maps

\[
f_i(R,f_{ij}(R) : \GL(M_R) \to R
\]

for \( 1 \leq i,j \leq n \) and all \( R \in k\text{-}\text{alg} \) by setting

\[
f_i(R)(\eta) := q_R(\eta(w_iR)) - q_R(w_iR),
\]

\[
f_{ij}(R)(\eta) := q_R(\eta(w_iR),\eta(w_jR)) - q_R(w_iR,w_jR)
\]

for \( \eta \in \GL(M_R) \). These set maps vary functorially with \( R \), hence define elements \( f_i,f_{ij} \in k[\GL(M)] \), and writing \( I \subseteq k[\GL(M)] \) for the ideal they generate, \( O(Q) \) is clearly the closed subfunctor of \( \GL(M) \) determined by \( I \). In particular, \( O(Q) \) is a \( k \)-group scheme, called the orthogonal group scheme of \( Q \).

**27.25. Base change.** Let \( k' \) be a fixed commutative associative \( k \)-algebra with 1. Under restriction of scalars, every \( k' \)-algebra becomes a \( k \)-algebra, and every homomorphism of \( k' \)-algebras becomes one of \( k \)-algebras. In particular, \( k'\text{-}\text{alg} \) may be viewed canonically as a subcategory, though not a full one, of \( k\text{-}\text{alg} \):

\[
k'\text{-}\text{alg} \subseteq k\text{-}\text{alg}.
\]

(1)

Restricting a \( k \)-functor \( X \) as defined in \([27.1]\) to \( k'\text{-}\text{alg} \), we obtain a \( k' \)-functor, denoted by \( X_{k'} \) and called the base change or scalar extension of \( X \) from \( k \) to \( k' \). Similarly,
restricting a morphism \( f : X \rightarrow Y \) of \( k \)-functors to \( k'\text{-alg} \), we obtain a \( k' \)-functor \( f_k : X_k \rightarrow Y_k \), called the base change or scalar extension of \( f \) from \( k \) to \( k' \).

Most of our preceding constructions commute with base change. For instance, we have

\[
\left( \mathbb{A}^n_k \right)_{k'} = \mathbb{A}^n_{k'} \tag{2} \]

for any positive integer \( n \). If \( M \) is a \( k \)-module, then

\[
\left( M_a \right)_{k'} = \left( M_{k'} \right) \tag{3} \]

under the identification \([10.3]\) since \( \left( M_a \right)_{k'} (R') = M \otimes R' = (M \otimes k') \otimes_{k'} R' = (M_{k'})_{k'} (R') \) for all \( R' \in k'\text{-alg} \), similarly for morphisms in \( k'\text{-alg} \).

Let \( R \in k\text{-alg} \). For \( R' \in k'\text{-alg} \), \([10.1]\) yields a bijection

\[
\text{can}_R (R') : \text{Hom}_{k\text{-alg}} (R, R') \sim \rightarrow \text{Hom}_{k' \text{-alg}} (R_{k'}, R') \tag{4} \]

given by

\[
\text{can}_R (R')(\rho)(r \otimes \alpha') = \alpha' \rho(r) \tag{5} \]

for all \( \rho \in \text{Hom}_{k\text{-alg}} (R, R') \), \( r \in R \), \( \alpha' \in k' \), and this bijection depends functorially on \( R' \). Thus we obtain an isomorphism

\[
\text{can}_R : \left( \text{Spec}(R) \right)_{k'} \sim \rightarrow \text{Spec}(R_{k'}) \tag{6} \]

Moreover, for a morphism \( \varphi : R \rightarrow S \) in \( k\text{-alg} \), one checks that the diagram

\[
\begin{array}{ccc}
\left( \text{Spec}(S) \right)_{k'} & \xrightarrow{\sim} & \text{Spec}(S_{k'}) \\
\downarrow \text{can}_S & & \downarrow \text{Spec}(\varphi_{k'}) \\
\left( \text{Spec}(R) \right)_{k'} & \xrightarrow{\sim} & \text{Spec}(R_{k'})
\end{array} \tag{7} \]

commutes.

27.26. Regular functions under base change. We continue the discussion begun in \([27.25]\). Let \( X \) be a \( k \)-functor. An element \( f \in k[X] \) by \([27.6.2]\) is a morphism \( f : X \rightarrow \mathbb{A}^1_k \) of \( k \)-functors, hence gives rise to a morphism \( f_k : X_k \rightarrow (\mathbb{A}^1_k)_{k'} = \mathbb{A}^1_{k'} \) of \( k' \)-functors, and we conclude \( f_k \in k'[X_{k'}] \). By \([27.6.4]\), the map

\[
k[X] \rightarrow k'[X_{k'}], \quad f \mapsto f_k \tag{1} \]

is a morphism in \( k\text{-alg} \) and thus gives rise to a morphism

\[
\text{can}_X : k[X]_{k'} \rightarrow k'[X_{k'}] \tag{2} \]
in \( k'\text{-alg} \) given by

\[
\text{can}_X(f \otimes \alpha') = \alpha' f_{k'}
\]

for \( f \in k[X] \) and \( \alpha' \in k'\text{-alg} \). Consulting the morphisms \( f_X \) (resp. \( f_{X_k} \)) described in (27.10.2) it is now easily checked, using (27.25.5), (27.25.6) and (3), that the diagram

\[
\begin{array}{ccc}
X_{k'} & \xrightarrow{f_{X_{k'}}} & \text{Spec}(k'[X_{k'}]) \\
\downarrow (f_X)_{k'} & & \downarrow \text{Spec}(\text{can}_X) \\
\text{Spec}(k[X])_{k'} & \xrightarrow{\text{can}_X} & \text{Spec}(k'[X_{k'}])
\end{array}
\]

commutes. Now suppose \( X \) is an affine \( k \)-scheme. Since \((f_X)_{k'} \) and \( f_{X_k} \) are both isomorphisms of \( k'\text{-functors, by Proposition 27.10(c), so is } \text{Spec}(\text{can}_X) \) by (4), and we conclude from Corollary 27.5(b) that

\[
\text{can}_X : k[X]_{k'} \xrightarrow{\sim} k'[X_{k'}]
\]

is an isomorphism of \( k'\text{-algebras.} \)

28. Faithfully flat étale splittings of composition algebras.

Given a commutative ring \( k \), remaining fixed throughout this section, and a prime ideal \( p \subseteq k \), it follows immediately from (26) Exercise 138(b), that a composition algebra over \( k \) becomes split after extending scalars to the separable closure of \( \kappa(p) \). Unfortunately, this observation is as obvious as it is useless. For example, the base change from \( k \) to any field in \( k\text{-alg} \) trivializes the linear algebra of \( k \) and thus destroys all the relevant information one could possibly have about this important ingredient.

In the present section, this deficiency will be overcome by dealing with scalar extensions relative to faithfully flat étale \( k \)-algebras. After having derived (resp. recalled) a number of basic properties pertaining to this important concept, we will indeed be able to show that every composition algebra \( C \) over \( k \) becomes split after a faithfully flat étale base change. The proof is not at all obvious and, following [73], will be based on a number of scheme-theoretic concepts and results due to Grothendieck [37] and Demazure-Gabriel [22] which will be quoted here in due course. As an important by-product of our approach we also show that \( \text{Aut}(C) \) as defined in Example 27.23 is a smooth group scheme in the sense of 28.16 below.

We begin our preparations for the main results of this section by recalling a few elementary facts from Bourbaki [12], Knus-Ojanguren [60] and Waterhouse [126], sometimes with proofs, sometimes without.
28. Flat and faithfully flat modules. Let $N$ be a $k$-module. By [12, II, §3, Corollary of Proposition 5], the functor $\_ \otimes N: \text{k-mod} \to \text{k-mod}$ is right exact, so whenever we are given an exact sequence

$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$,

of $k$-modules, the induced sequence

$M' \otimes N \xrightarrow{\varphi \otimes 1_N} M \otimes N \xrightarrow{\psi \otimes 1_N} M'' \otimes N \to 0$

is also exact. $N$ is said to be flat if the functor $\_ \otimes N$ is exact in the sense that it preserves exact sequences, equivalently, if for every injective $k$-linear map $\varphi: M' \to M$ of $k$-modules, the induced linear map $\varphi \otimes 1_N: M' \otimes N \to M \otimes N$ is also injective.

We say $N$ is faithfully flat provided a sequence of $k$-modules is exact if and only if it becomes so after tensoring with $N$. A free $k$-module is always flat, while it is faithfully flat if and only if it is non-zero.

28.2. (Faithful) flatness under base change. Let $k' \in \text{k-alg}$ and $N$ be a $k$-module.

(a) Generalizing iterated scalars extensions as in [10.3] we consider a $k'$-module $M'$ and let $k'$ act on $M' \otimes k = M' \otimes_k N$ through the first factor, making $M' \otimes N$ a module over $k'$. We then have a natural identification

$M' \otimes_k N = M' \otimes_{k'} N_{k'}$

of $k'$-modules such that

$x' \otimes_k y = x' \otimes_{k'} y_{k'}$, \quad $x' \otimes_{k'} (y \otimes \alpha') = (\alpha' x') \otimes_{k'} y$

for $x' \in M'$, $y \in N$, $\alpha' \in k'$. Moreover, for a $k'$-linear map $\varphi': M' \to M'_1$ of $k'$-modules and a $k$-linear map $\psi: N \to N_1$ of $k$-modules, we obtain

$\varphi' \otimes_k \psi = \varphi' \otimes_{k'} \psi_{k'}$

under this identification.

(b) Let

$M'_1 \xrightarrow{\varphi'_1} M'_2 \xrightarrow{\varphi'_2} M'_3$

be a sequence of $k'$-modules. Since $1_{N_{k'}} = (1_N)_{k'}$, we may apply (a) to obtain a commutative diagram
Now suppose $N$ is flat over $k$ and assume (4) is exact. Then so is the bottom row of (5), hence also its top row, and we conclude that $N_{k'}$ is flat over $k'$. Moreover, if $N$ is faithfully flat over $k$ and the top row of (5) is exact, so is its bottom row, hence also (4). Thus $N_{k'}$ is faithfully flat over $k'$.

In summary: (faithful) flatness is stable under base change.

28.3. Flat and faithfully flat algebras. By a (faithfully) flat $k$-algebra we mean a unital commutative associative algebra over $k$, i.e., an object of $k$-alg, that is (faithfully) flat as a $k$-module.

Let $R$ be a flat $k$-algebra. If $M$ is a $k$-module and $N \subseteq M$ is a $k$-submodule, then the inclusion $i: N \hookrightarrow M$ gives rise to an $R$-linear injection $i_R: N_R \rightarrow M_R$, which may and always will be used to identify $N_R \subseteq M_R$ as an $R$-submodule. Extending the short exact sequence $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ from $k$ to $R$, we obtain

$$ (M/N)_R = M_R/N_R. $$

Similarly, given any $k$-linear map $f: M \rightarrow M'$ of $k$-modules and doing the same with

$$ 0 \rightarrow \text{Ker}(f) \rightarrow M \xrightarrow{f} M' \rightarrow \text{Coker}(f) \rightarrow 0 $$

yields

$$ \text{Ker}(f_R) = \text{Ker}(f)_R, \quad \text{Coker}(f_R) = \text{Coker}(f)_R. $$

Finally, the factorization

$$ M \xrightarrow{f} M' \xrightarrow{g} \text{Im}(f) \xrightarrow{0}, $$

where $g: M \rightarrow \text{Im}(f)$ is the unique $k$-linear map induced by $f$, gives rise to the commutative diagram
28 Faithfully flat étale splittings of composition algebras.

\[
\begin{array}{ccc}
M_R & \xrightarrow{f_R} & M'_R \\
\downarrow{s_R} & & \downarrow{\psi_R} \\
\text{Im}(f)_R & \rightarrow & M''_R \\
\downarrow{\phi_R} & & \downarrow{\psi_R} \\
0 & & 0
\end{array}
\]

of \(R\)-modules, which shows

\[
\text{Im}(f_R) = \text{Im}(f)_R. \quad (3)
\]

**28.4. Proposition.** Let \(R\) be a flat \(k\)-algebra. Then the following conditions are equivalent.

(i) \(R\) is faithfully flat.

(ii) For all \(k\)-modules \(M\), the linear map \(\text{can}_M := \text{can}_{M,R} : M \rightarrow M_R, x \mapsto x_R\), is injective.

(iii) \(M_R = \{0\}\) implies \(M = \{0\}\), for all \(k\)-modules \(M\).

*Proof.* (i) \(\Rightarrow\) (ii). Put \(\phi := \text{can}_M\). By faithful flatness, it suffices to show that

\[
\phi_R : M \otimes R \rightarrow (M \otimes R) \otimes R
\]
is injective. But since it is easily checked that the \(k\)-linear map

\[
\psi : (M \otimes R) \otimes R \rightarrow M \otimes R, \quad (x \otimes r_1) \otimes r_2 \mapsto x \otimes (r_1 r_2),
\]
satisfies \(\psi \circ \phi_R = 1_{M \otimes R}\), the assertion follows.

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

(iii) \(\Rightarrow\) (i). Let

\[
\begin{array}{ccc}
M' & \xrightarrow{\phi} & M \\
\downarrow{\psi} & & \downarrow{\psi} \\
M'_R & \xrightarrow{\phi_R} & M'_R \\
\downarrow{\psi_R} & & \downarrow{\psi_R} \\
M''_R & \xrightarrow{\phi_R} & M''_R
\end{array}
\]

be a commutative diagram, with the top row being given as any sequence in \(k\text{-mod}\), and the bottom row assumed to be exact. We must show that the top row is exact as well. The \(k\)-linear map \(f := \psi \circ \phi : M' \rightarrow M''\) satisfies \(f_R = 0\), hence \(\text{Im}(f)_R = \text{Im}(f_R)\) (by \(28.3.3\)) = \(\{0\}\) and then \(f = 0\) by (iii). Thus \(\text{Im}(\phi) \subseteq \text{Ker}(\psi)\). On the other hand, \((28.3.2), (28.3.3)\) and exactness of the bottom row imply \(\text{Im}(\phi)_R = \text{Im}(\phi_R) = \text{Ker}(\psi_R) = \text{Ker}(\psi_R)\). From \((28.3.1)\) we therefore deduce \((\text{Ker}(\psi)/\text{Im}(\phi))_R = \{0\}\), and (iii) again shows \(\text{Im}(\phi) = \text{Ker}(\psi)\), as claimed. \(\Box\)
28.5. Equalizers. Let $\mathcal{C}$ be a category. By an equalizer of morphisms $f, g: X \rightarrow Y$ in $\mathcal{C}$ we mean a morphism $e: E \rightarrow X$ in $\mathcal{C}$ such that $f \circ e = g \circ e$ and, for any morphism $u: U \rightarrow X$ in $\mathcal{C}$ such that $f \circ u = g \circ u$, there is a unique morphism $h: U \rightarrow E$ in $\mathcal{C}$ such that the diagram

\[
\begin{array}{c}
E \\
\downarrow^e \\
X \downarrow^f \\
\downarrow^g \\
Y \\
\end{array}
\]

commutes. Clearly, if an equalizer exists, it is unique up to a unique isomorphism. For more details on this concept, see D. Pumplün [106, 4.2].

It is sometimes important to realize the linear map $\text{can}_M$ in condition (ii) of Proposition 28.4 as an equalizer. To this end, we consider an arbitrary $R \in k\text{-alg}$ and two morphisms

\[
\rho_i = \rho^{R_i}: R \rightarrow S := R \otimes R \quad (i = 1, 2)
\]

in $k\text{-alg}$ defined by

\[
\rho_1(r) := r \otimes 1_R, \quad \rho_2(r) := 1_R \otimes r \quad (r \in R).
\]

Given a $k$-module $M$, we also put

\[
\rho_i^M := \rho_i^{R,M} := 1_M \otimes \rho_i: M_R \rightarrow M_S.
\]

28.6. Proposition. Let $M$ be a $k$-module and suppose $R \in k\text{-alg}$ is faithfully flat. With the notation of 28.5, the sequence

\[
0 \rightarrow M \xrightarrow{\text{can}_M} M_R \xrightarrow{\rho_1^M} M_S \quad (1)
\]

is exact. In particular, the natural map $\text{can}_M: M \rightarrow M_R$ is an equalizer of $\rho_1^M, \rho_2^M$ in the category $k\text{-mod}$.

Proof. The final statement follows immediately from the exactness of (1). By faithful flatness of $R$, it therefore suffices to show that

\[
0 \rightarrow M \otimes R \xrightarrow{\text{can}_M \otimes 1_R} M_R \otimes R \xrightarrow{\rho \otimes 1_R} M_S \otimes R
\]

is exact, where $\rho := \rho_1^M - \rho_2^M$. Since $\text{can}_M$ is injective by Proposition 28.4, so is $\text{can}_M \otimes 1_R$ by flatness of $R$, and we have exactness of (2) at $M \otimes R$. Since, obviously, $\rho \circ \text{can}_M = 0$, we conclude $(\rho \otimes 1_R) \circ (\text{can}_M \otimes 1_R) = (\rho \circ \text{can}_M) \otimes 1_R = 0$, hence $\text{Im}(\text{can}_M \otimes 1_R) \subseteq \ker(\rho \otimes 1_R)$, and exactness of (2) at $M_R \otimes R$ will follow once we have shown the reverse inclusion. For this purpose, we define a $k$-linear
map \( \varphi : M_S \otimes R \to M_R \otimes R \) by

\[
\varphi \left( (x \otimes (r_1 \otimes r_2)) \otimes r_3 \right) := (x \otimes r_1) \otimes (r_2 r_3)
\]

for all \( x \in M \) and all \( r_1, r_2, r_3 \in R \). A straightforward verification shows

\[
\varphi \circ (\rho^M \otimes 1_R) = 1_{M_R \otimes R}, \quad \text{Im} \left( \varphi \circ (\rho^M \otimes 1_R) \right) \subseteq \text{Im}(\text{can}_M \otimes 1_R).
\]

For \( z \in \text{Ker}(\rho \otimes 1_R) \), we therefore conclude

\[
z = \varphi \left( (\rho^M \otimes 1_R)(z) \right) = \varphi \left( (\rho^M \otimes 1_R)(z) \right) \in \text{Im}(\text{can}_M \otimes 1_R),
\]

which completes the proof. \( \square \)

28.7. Proposition. Let \( R \in k\text{-alg} \) and \( p \in \text{Spec}(R) \). Writing \( \vartheta_R : k \to R \) for the unit homomorphism corresponding to \( R \) as in 27.9, \( \kappa(p) \) for the algebraic closure of the field \( k(p) \) and setting \( X := \text{Spec}(R) \) as an affine \( k \)-scheme, we consider the following conditions on \( R \) and \( p \).

(i) \( \text{Spec}(\vartheta_R)^{-1}(p) \neq \emptyset \).
(ii) \( R \otimes \kappa(p) \neq \{0\} \).
(iii) \( \text{X}(\kappa(p)) \neq \emptyset \).

Then the implications

\[
(i) \iff (ii) \iff (iii)
\]

hold. Moreover, if \( R \) is finitely generated as a \( k \)-algebra, then all three conditions are equivalent.

Proof. Put \( K := \kappa(p) \).

(i) \( \iff \) (ii). [10] Exercise [39]

(iii) \( \Rightarrow \) (ii). If \( \text{X}(K) \neq \emptyset \), then there exists a morphism \( R \to K \) in \( k\text{-alg} \), which in turn induces a unital homomorphism \( R \otimes \kappa(p) \to K \) of \( \kappa(p) \)-algebras. Hence (ii) holds.

We have thus shown \( \{1\} \). Assuming that \( R \) is finitely generated as a \( k \)-algebra, it remains to verify the implication (ii) \( \Rightarrow \) (iii). If (ii) holds, then \( R \otimes \kappa(p) \) is a non-zero finitely generated \( \kappa(p) \)-algebra. By [11] V, \( \S 3 \), Proposition 1, therefore, we find a morphism \( R \otimes \kappa(p) \to K \) in \( \kappa(p) \)-alg. Composing with the natural map \( R \to R \otimes \kappa(p) \) yields an element of \( \text{X}(K) \). Hence (iii) holds. \( \square \)

28.8. Proposition. For a flat \( k \)-algebra \( R \), the following conditions are equivalent.

(i) \( R \) is faithfully flat.
(ii) \( R \otimes \kappa(p) \neq \{0\} \) for all \( p \in \text{Spec}(k) \).
(iii) The natural map \( \text{Spec}(R) \to \text{Spec}(k) \) induced by the unit homomorphism \( k \to R \) is surjective.
(iv) \( mR \neq R \) for all maximal ideals \( m \subseteq k \).

Proof. (i) \( \Rightarrow \) (ii). Apply Proposition [28.4]

(ii) \( \Rightarrow \) (iii). Apply Proposition [28.7]
(iii) ⇒ (iv). By (ii), some prime ideal $q \subseteq R$ lies above $m$. Hence $mR \subseteq q \subset R$.

(iv) ⇒ (i). By Proposition 28.4 we have to show $M_R \neq \{0\}$ for all $k$-modules $M \neq \{0\}$. Let $0 \neq x \in M$ and $I := \text{Ann}(x) \subset k$. The $kx \cong k/I$ as $k$-modules, so we have an exact sequence $0 \to k/I \to M$. Since $R$ is flat, this implies that the sequence $0 \to (k/I) \otimes_R R/I \to M_R$ is also exact. Let $m \subseteq k$ be a maximal ideal in $k$ containing $I$. Then $IR \subseteq mR \subset R$ by (iv), which implies $R/I \neq \{0\}$ and then $M_R \neq \{0\}$.

The two preceding results are related to a concept that turns out to be useful later on.

**28.9. Faithful affine $k$-schemes.** An affine $k$-scheme $X$ is said to be faithful if $X(K) \neq \emptyset$ for all algebraically closed fields $K \in k$-alg. In this case, we also say that $X$ has non-empty geometric fibers.

**28.10. Convention.** It is sometimes convenient to use notions originally defined for unital commutative associative $k$-algebras also for affine $k$-schemes and vice versa. This convention is justified by the anti-equivalence of these categories established in Corollary 27.11. For example, an affine $k$-scheme $X$ is faithfully flat if and only if $k[X] \in k$-alg has this property.

**28.11. Corollary.** Consider the following conditions, for any affine $k$-scheme $X$.

(i) $X$ is faithful and flat.

(ii) $X$ is faithfully flat.

Then (i) implies (ii), and both conditions are equivalent if $k[X]$ is finitely generated as a $k$-algebra.

**Proof.** If condition (i) holds, so does condition (ii) of Proposition 28.7 for $R := k[X]$ and any $p \in \text{Spec}(k)$. Hence that proposition combined with Proposition 28.8 shows that $X$ is faithfully flat. Conversely, suppose $X$ is faithfully flat and $R$ is finitely generated as a $k$-algebra. If $K \in k$-alg is an algebraically closed field, the kernel of the unit homomorphism $\vartheta_K: k \to K$ is some prime ideal $p \in \text{Spec}(k)$, making $K$ a $\kappa(p)$-algebra in a natural way. Hence the unit homomorphism $\vartheta_K$ factors uniquely through the unit homomorphism $\vartheta_L: k \to L, \quad L := \kappa(p)$.

On the other hand, since $\text{Spec}(\vartheta_R): \text{Spec}(R) \to \text{Spec}(k)$ is surjective by Proposition 28.8, we have $X(L) \neq \emptyset$ by Proposition 28.7. Therefore $X(K) \neq \emptyset$, and $X$ is faithful. □

The property of an algebra to be finitely generated, which shows up as an important ingredient of Proposition 28.7, is sometimes not enough for the intended applications and has to be replaced by the following refinement.
28 Faithfully flat étale splittings of composition algebras.

28.12. Finitely presented \( k \)-algebras. By a presentation of a \( k \)-algebra \( R \in k \text{-alg} \), we mean a short exact sequence

\[
0 \longrightarrow I \longrightarrow k[T] \longrightarrow R \longrightarrow 0, \tag{1}
\]

where \( T = (t_1, \ldots, t_n) \) is a finite chain of independent indeterminates, \( \pi \) is a morphism in \( k \text{-alg} \) and \( I \subseteq k[T] \) is an ideal. For a presentation of \( R \) to exist it is necessary and sufficient that \( R \) be finitely generated as a \( k \)-algebra. The presentation (1) of \( R \) is said to be finite if the ideal \( I \subseteq k[T] \) is finitely generated. We say a \( k \)-algebra \( R \) (the condition \( R \in k \text{-alg} \) being understood) is finitely presented if a finite presentation of \( R \) exists.

Tensoring (1) with any \( k' \in k \text{-alg} \), we obtain a commutative diagram

\[
\begin{array}{ccc}
I' & \overset{i'}{\longrightarrow} & k'[T] \\
\downarrow j' & & \downarrow \pi' \\
0 & \overset{i'}{\longrightarrow} & R'
\end{array}
\]

where \( I' := i'(I) \subseteq k'[T] \) and \( j' \) is induced by \( i' \). Since this diagram is everywhere exact and \( I' \subseteq k'[T] \) is obviously a finitely generated ideal if \( I \subseteq k[T] \) is, it follows that the property of a \( k \)-algebra to be finitely presented is stable under base change. We wish to show, among other things, that this property is also stable under faithfully flat descent. We require a preparation.

28.13. Proposition. Every presentation of a finitely presented \( k \)-algebra is finite.

Proof. Let \( R \in k \text{-alg} \) be finitely presented and let

\[
0 \longrightarrow I \longrightarrow k[T] \longrightarrow R \longrightarrow 0 \tag{1}
\]

be any presentation of \( R \) as in (28.12.1). By hypothesis, there exists a finite presentation

\[
0 \longrightarrow J \longrightarrow k[S] \longrightarrow R \longrightarrow 0 \tag{2}
\]

of \( R \), so \( J \subseteq k[S] \) is a finitely generated ideal. We must show that \( I \subseteq k[T] \) is a finitely generated ideal as well. Writing \( S = (s_1, \ldots, s_m), \ T = (t_1, \ldots, t_n) \), the quantities \( \pi(t_j) \in R \) by (2) have a lift under \( \mu \) to polynomials \( g_j \in k[S] \). Thus

\[
\mu(g_j) = \pi(t_j) \quad (1 \leq j \leq n). \tag{3}
\]
The morphism

\[
\varphi: k[S, T] = k(S) \otimes k[T] \xrightarrow{\mu \otimes \pi} R \otimes R \xrightarrow{\text{mult}_R} R
\]  

is surjective satisfying, in obvious notation,

\[
\varphi(S) = \mu(S), \quad \varphi(T) = \pi(T).
\]

We now claim

\[
\text{Ker}(\varphi) = J + \sum_{j=1}^{n} k[S, T](t_j - g_j).
\]

Consulting (2), (5), we see that the right-hand side is contained in the left. Conversely, let \( f \in \text{Ker}(\varphi) \), write \( g := (g_1, \ldots, g_n) \in k[S]^n \) and regard \( f \) as a polynomial \( h(T) \in k[S][T] \). Then (5), (3), (2) imply

\[
h(g(S)) = f(S, g(S)) \in J,
\]

while the Taylor expansion (cf. (13.13.3) below) yields

\[
h(T) = h(g(S) + T - g(S)) = h(g(S)) + \sum_{r \geq 1} (D^r h)(g(S), T - g(S)),
\]

where the first summand on the right by (7) belongs to \( J \). On the other hand, \( (D^r h)(g(S), T) \) for \( r \geq 1 \) is homogeneous of degree \( r \) in \( T \) and thus belongs to the ideal in \( k[S, T] \) generated by \( t_1, \ldots, t_n \). We therefore conclude

\[
(D^r h)(g(S), T - g(S)) \in \sum_{j=1}^{n} k[S, T](t_j - g_j),
\]

which completes the proof of (6). Now let \( h_i \in k[T] \) for \( 1 \leq i \leq m \) be lifts of \( \mu(s_i) \) under \( \pi \), so

\[
\pi(h_i) = \mu(s_i) \quad (1 \leq i \leq m).
\]

Setting \( h := (h_1, \ldots, h_m) \in k[T]^m \), we consider the surjective homomorphism

\[
\psi: k[S, T] \to k[T]
\]

of unital \( k \)-algebras given by

\[
\psi(S) = h, \quad \psi(T) = T.
\]

Since \( \text{Ker}(\varphi) \subseteq k[S, T] \) is a finitely generated ideal by (6), the proof will be complete once we have shown
By (2), (3), (6), (8), (9), the left-hand side is clearly contained in the right. Conversely, let \( f(T) \in I \). Then (1), (3) show \( f(g(S)) \in J \), hence
\[
f(T) = f(g(S) + T - g(S)) = f(g(S)) + \sum_{r \geq 1} (D^r f)(g(S), T - g(S))
\]
\[\in J + \sum_{r \geq 1} k[S, T](t_j - g_j).
\]
Now (9) implies \( f(T) \in \ker(\phi) \cap k[T] \), and from (9) we deduce \( f(T) = \psi(f(T)) \in \psi(\ker(\phi)) \), which completes the proof of (10).

**28.14. Corollary.** Let \( R, k' \in k\text{-}alg \) and suppose \( k' \) is faithfully flat. If \( R_{k'} \) is finitely generated (resp. finitely presented) over \( k' \), then so is \( R \) over \( k \).

**Proof.** Assume first that \( R_{k'} \) is finitely generated over \( k' \). Then there exists an exact sequence
\[
k'[T'] \xrightarrow{\pi} R_{k'} \longrightarrow 0
\]
in \( k'\text{-}alg \) with \( T' = (t'_1, \ldots, t'_n) \), and the quantities \( \pi'(t'_j) \in R_{k'} \) for \( 1 \leq j \leq n \) may be written as
\[
\pi'(t'_j) = \sum_{i=1}^m r_{ij} \otimes \alpha_{ij}', \quad r_{ij} \in R, \quad \alpha_{ij}' \in k' \quad (1 \leq i \leq m, 1 \leq j \leq n).
\]

Let \( T = (t_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \) be a chain of independent variables and \( \pi : k[T] \rightarrow R \) be the morphism in \( k\text{-}alg \) given by \( \pi(t_{ij}) = r_{ij} \) for \( 1 \leq i \leq m, 1 \leq j \leq n \). Since the \( \pi'(t'_j) \), \( 1 \leq j \leq n \), generate \( R_{k'} \) as a \( k' \)-algebra, so do the \( (r_{ij})_{k'} \), \( 1 \leq i \leq m, 1 \leq j \leq n \), by (2). Thus the sequence
\[
k[T] \xrightarrow{\pi} R \longrightarrow 0
\]
in \( k\text{-}alg \) becomes exact after tensoring with \( k' \), hence must have been so all along since \( k' \) is faithfully flat over \( k \). Thus it follows from the exactness of (3) that \( R \) is a finitely generated \( k \)-algebra.

Now suppose \( R_{k'} \) is finitely presented over \( k' \). By what we have just seen, \( R \) is finitely generated over \( k \), so we have a presentation
\[
0 \longrightarrow I \longrightarrow k[T] \xrightarrow{\pi} R \longrightarrow 0
\]
of \( R \) as in (28.12). By faithful flatness of \( k' \), the extended sequence
\[
0 \longrightarrow I \otimes k' \longrightarrow k'[T] \xrightarrow{\pi_{k'}} R_{k'} \longrightarrow 0
\]
By Proposition \ref{prop:composition-algebras}, therefore, \( I \otimes k' \subseteq k'[T] \) is a finitely generated ideal. On the other hand, from \( \ref{prop:tensor-product} \) we deduce \( I \otimes k' = I \otimes_{k'[T]} k'[T] \) as \( k'[T] \)-modules. Applying Exercise \ref{ex:ideal-prop}, we conclude that \( I \subseteq k[T] \) is a finitely generated ideal. Hence \( R \) is finitely presented as a \( k \)-algebra.

\[ \Box \]

\subsection*{Étale \( k \)-algebras}

The notion of a finite étale algebra as defined in \ref{subsection:finite-etale} will now be generalized as follows. A \( k \)-algebra \( R \in k\text{-alg} \) is said to be \( \text{étale} \) if it is finitely presented and satisfies one of the following equivalent conditions (\cite{ exposé}, (17.1.1), (17.3.1), (17.6.2)), applied to the structure morphism \( \text{Spec}(R) \to \text{Spec}(k) \) of \ref{subsection:finiteness} and \$\S\$ \ref{subsection:smooth-affine}.

The notion of a finite étale algebra as defined in \ref{subsection:finite-etale} will now be generalized as follows. A \( k \)-algebra \( R \in k\text{-alg} \) is said to be \( \text{étale} \) if it is finitely presented and satisfies one of the following equivalent conditions (\cite{ exposé}, (17.1.1), (17.3.1), (17.6.2)), applied to the structure morphism \( \text{Spec}(R) \to \text{Spec}(k) \) of \ref{subsection:finiteness} and \$\S\$ \ref{subsection:smooth-affine}.

(i) For all \( k' \in k\text{-alg} \) and all ideals \( I' \subseteq k' \) satisfying \( I'^2 = \{0\} \), the set map

\[ \text{Hom}_{k\text{-alg}}(R, k') \to \text{Hom}_{k\text{-alg}}(R, k'/I') \]

induced by the projection \( \pi : k' \to k'/I' \) is bijective.

(ii) \( R \) is flat over \( k \), and for all \( p \in \text{Spec}(k) \), the extended algebra \( R(p) = R \otimes \kappa(p) \) over the field \( \kappa(p) \) is a possibly infinite direct sum of finite separable extension fields of \( \kappa(p) \).

\subsection*{Smooth affine \( k \)-schemes}

Since the original definition of smoothness as given in \cite{ exposé} I, \$\S$ 4, 4.1] is rather technical, although more akin to what one expects from the study of classical algebraic varieties or differentiable manifolds, we prefer to recall the one of \cite{ exposé} (17.1.1), (17.3.1) (see also the characterization in \cite{ exposé} I, \$\S$ 4, 4.6) because it is more easily accessible in the present context. Accordingly, an affine \( k \)-scheme \( X \) is said to be \textit{smooth} if \( X \) is finitely presented and, for all \( R \in k\text{-alg} \) and all ideals \( I \subseteq R \) having \( I^2 = \{0\} \), the set map \( X(R) \to X(R/I) \) induced by the projection from \( R \) to \( R/I \) is surjective.

Let \( X \) be an affine \( k \)-scheme.

(i) \( \text{[17.16.2], 28.11} \) If \( X \) is faithful, flat and finitely presented, abbreviated \( \text{fpff} \) ("fidelement plat et de presentation finis"), then there exists an \( \text{fpff} R \in k\text{-alg} \) such that \( X(R) \neq \emptyset \).

(ii) \( \text{[17.16.3], (ii), 28.8} \) If \( X \) is faithful and smooth, then there exists an étale \( \text{fpff} R \in k\text{-alg} \) such that \( X(R) \neq \emptyset \).

(iii) \( \text{[17.7.3], (ii), 27.26} \) If \( R \in k\text{-alg} \) is faithfully flat, then for \( X \) to be smooth over \( k \) it is necessary and sufficient that the base change

\[ X_R \cong \text{Spec}(k[X|R]) \in R\text{-aff} \]

be smooth over \( R \).

\subsection*{Torsors}

Let \( X \) be an affine \( k \)-scheme and \( G \) a \( k \)-group scheme acting on \( X \) from the right, so we have a morphism \( X \times G \to X \) of \( k \)-functors such that, for all \( R \in k\text{-alg} \).

\[ \Box \]
is a group action in the usual sense depending functorially on \( R \). Note that \( X(R) \) may well be empty! We say \( X \) is a \textit{torsor in the flat topology with structure group} \( G \) if

(i) the action of \( G \) on \( X \) is simply transitive, i.e., for all \( R \in k\text{-alg} \) and all \( x, y \in X(R) \), there is a unique \( g \in G(R) \) satisfying \( y = xg \).

(ii) There exists an fppf \( S \in k\text{-alg} \) such that \( X(S) \neq \emptyset \)

In this case, fixing as in (ii), we may apply (i) to obtain an isomorphism \( X_S \cong G_S \) of affine \( S \)-schemes, allowing us to conclude from \([28.17](iii)\) that, e.g., \( X \) is smooth if and only if so is \( G \).

Finally, if instead of(ii), we even have

(iii) there exists an \( \text{étale fppf} \ S \in k\text{-alg} \) having \( X(S) \neq \emptyset \),

then \( X \) is called a \textit{torsor (with structure group} \( G \) \text{)} in the \( \text{étale topology} \).

**28.19. The set-up.** After the preparations we have presented in the preceding parts of this section, we will finally be able to describe the set-up for the applications we have in mind.

Unless other arrangements have been made, we fix a composition algebra \( C \) of rank \( r > 1 \) over \( k \). By Corollaries \([22.17](2)\) and \([22.7](r)\) \( r \in \{2, 4, 8\} \) and \( C \) is non-singular. Moreover, given an elementary idempotent \( e \in C \), the Peirce components \( C_{12}(e) \) and \( C_{21}(e) \) by \([22](105)\) are in duality to each other under the bilinearized norm of \( C \). Hence they are finitely generated projective \( k \)-modules of rank \( m = \frac{r}{2} - 1 \).

**28.20. The concept of a splitting datum.** In order to define splitting data for \( C \), we discuss the cases \( r = 2, 4, 8 \) separately.

(a) For \( r = 2 \), a \textit{splitting datum} for \( C \) by definition has the form \( \Delta = (e) \in C^1 \), where \( e \in C \) is an elementary idempotent.

(b) For \( r = 4 \), a \textit{splitting datum} for \( C \) by definition has the form \( \Delta = (e, x, y) \in C^3 \), where \( e \in C \) is an elementary idempotent and \( x \in C_{21}(e) \), \( y \in C_{12}(e) \) satisfy the following conditions, with \( e' := 1_C - e \).

\[
xy = e', \quad t_C(xy) = 1, \quad yx = e. \tag{1} \]

Actually, one checks easily that these equations are mutually equivalent.

(c) For \( r = 8 \), a \textit{splitting datum} for \( C \) by definition has the form \( \Delta = (e, x_1, x_2, x_3) \in C^4 \), where \( e \in C \) is an elementary idempotent and \( x_1, x_2, x_3 \in C_{21}(e) \) satisfy the following conditions.

\[
(x_1 x_2) x_3 = -e, \quad t_C(x_1 x_2 x_3) = -1, \quad (x_i x_j) x_l = -e \tag{2} \]

for all cyclic permutations \((ijl)\) of \((123)\). Again one checks that these equations are mutually equivalent.

In summary, splitting data of \( C \) belong to \( C^n \), where \( n = 1, 2, 4 \) for \( r = 2, 4, 8 \), respectively. Moreover, they are preserved by isomorphisms: if \( \eta : C \to C' \) is an...
isomorphism of composition algebras of rank $r$ over $k$, and $\Delta$ is a splitting datum for $C$, then the linear bijection $\eta^n : C^n \to C''$ maps $\Delta \subseteq C^n$ to the splitting datum $\eta(\Delta) := \eta^n(\Delta) \subseteq C''$ of $C'$. Finally, splitting data are stable under base change, so if $\Delta \subseteq C^n$ is a splitting datum for $C$, then $\Delta_R \subseteq C''_R$ is one for $C_R$, for all $R \in k$-alg.

28.21. The affine scheme of splitting data. Again we treat the cases $r = 2, 4, 8$ separately and let $R \in k$-alg be arbitrary.

(a) Let $r = 2$. Then $(e) \in C^1_R$ by \[19\] Exercise 82\[19\] is a splitting datum for $C_R$ if and only if

$$
n_C(e) = 0, \quad t_C(e) = 1.
$$

(1) \tag{AFSPLIT}

(b) Let $r = 4$. Then $(e, x, y) \in C^3_R$ is a splitting datum for $C_R$ if and only if

$$
n_C(e) = 0, \quad t_C(e) = 1, \quad \langle u^*_R, ex \rangle = \langle u^*_R, xe - x \rangle = \langle u^*_R, ye - y \rangle = 0, \quad t_C(xy) = 1
$$

(2) \tag{AFSPLIF}

for all $u^* \in C^*$.

(c) Let $r = 8$. Then $(e, x_1, x_2, x_3) \in C^4_R$ is a splitting datum for $C_R$ if and only if

$$
n_C(e) = 0, \quad t_C(e) = 1, \quad \langle u^*_R, ex_i \rangle = \langle u^*_R, x_ie - x_i \rangle = 0, \quad t_C(x_1x_2x_3) = -1
$$

(3) \tag{AFSPLIE}

for all $u^* \in C^*$ and all $i = 1, 2, 3$.

Setting $n = 1, 3, 4$ for $r = 2, 4, 8$, respectively, we therefore conclude that equations (1), (2), (3), respectively, define a closed subscheme of $C^1_R := (C''^n)_R = (C^n)_R$ in the sense of \[27.14\] denoted by $\text{Splid}(C)$ and called the affine scheme of splitting data for $C$. By definition we have

$$
\text{Splid}(C)(R) := \text{Splid}(C_R) := \{ \Delta \mid \Delta \text{ is a splitting datum for } C_R \}
$$

(4) \tag{SPLIDO}

for all $R \in k$-alg and, in view of \[10.3.2\],

$$
\text{Splid}(C)(\varphi) : \text{Splid}(C)(R) \to \text{Splid}(C)(S),
$$

(5) \tag{SPLIDM}

for all morphisms $\varphi : R \to S$ in $k$-alg. Passing from $C$ to its affine scheme of splitting data is obviously compatible with base change.

As will be seen in due course, for a splitting datum to exist it is necessary and sufficient that the ambient composition algebra be split. In fact, a much more precise statement will be derived in Proposition \[28.25\] below. Before proceeding to this result, we discuss a few examples.
28.22. Standard examples of splitting data. Here we present examples of splitting data for the standard split composition algebras \(C_0 := C_{0r}(k)\) of rank \(r > 1\) over \(k\) as described in [24.18](b)–(d). Again we treat the cases \(r = 2, 4, 8\) separately.

(a) \(r = 2\). Then \(C = k \oplus k\) is the direct sum of two copies of \(k\) as ideals and

\[
\Delta_0 := \Delta_{02}(k) := (E), \quad E := 1 \oplus 0 \in C
\]

is a splitting datum for \(C\).

(b) \(r = 4\). Then \(C_0 = \text{Mat}_2(k)\) is the algebra of \(2 \times 2\)-matrices with entries in \(k\) and

\[
\Delta_0 := \Delta_{04}(k) := (E, X, Y), \quad E := E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X := E_{21} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad Y := E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}
\]

is a splitting datum for \(C_0\).

(c) \(r = 8\). The \(C_0 = \text{Zor}(k)\) is the algebra of Zorn vector matrices over \(k\) and, writing \((e_i)_{1 \leq i \leq 3}\) for the canonical basis of \(k^3\) over \(k\),

\[
\Delta_0 := \Delta_{08}(k) := (E, X_1, X_2, X_3), \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_i = \begin{pmatrix} 0 & 0 \\ e_i & 0 \end{pmatrix} \quad (1 \leq i \leq 3)
\]

is a splitting datum for \(C\) since (24.17.4) implies

\[
(X_1X_2)X_3 = \begin{pmatrix} 0 & e_1 \times e_2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ e_3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = -\det(e_1, e_2, e_3)E = -E.
\]

The splitting datum \(\Delta_{0r}(k)\) exhibited in [38], [42], [43] above will henceforth be referred to as the standard splitting datum for \(C_{0r}(k)\) \((r = 2, 4, 8)\). We clearly have \(\Delta_{0r}(k)_R = \Delta_{0r}(R)\) for all \(R \in k\)-alg.

28.23. Proposition. The affine \(k\)-scheme of splitting data for \(C\) is smooth.

Proof. Consulting [28.21][1]–[28.21][3] we see that \(X := \text{Splid}(C)\) is defined by finitely many equations as a closed subscheme of \(C^n\). By Exercise [141][b] and Exercise [142] therefore, \(X\) is finitely presented. Hence, by [28.16] it suffices to show that the set map \(X(R) \to X(R/I)\) induced by the projection \(R \to R/I\) is surjective, for all ideals \(I \subseteq R\) satisfying \(I^2 = \{0\}\). In order to do so, we may assume \(R = k\) and write \(\alpha \mapsto \bar{\alpha}, x \mapsto \bar{x}\) for the projection \(k \to \bar{k} := k/I, C \to \bar{C} := C \otimes \bar{k} = C/IC\), respectively. We must show that every splitting datum \(\Delta'\) of \(\bar{C}\) can be lifted to a splitting datum \(\Delta\) of \(C\) satisfying \(\Delta = \Delta'\). In order to do so, we treat the cases \(r = 2, 4, 8\) separately.
(a) $r = 2$. A splitting datum for $C$ has the form $\Delta' = (e')$ for some elementary idempotent $e' \in C$. By Exercise 28.24, $e'$ can be lifted to an elementary idempotent $e \in C$. Thus $\Delta := (e)$ is a splitting datum for $C$ such that $\Delta = \Delta'$.

(b) $r = 4$. A splitting datum for $C$ has the form $\Delta' = (e', x', y')$ for some elementary idempotent $e' \in C$, where $x' \in C_{21}(e')$, $y' \in C_{12}(e')$ satisfy $t_C(x'y') = 1_k$. As in (a), we find an elementary idempotent $e \in C$ satisfying $\bar{e} = e'$. The canonical projection $C \to C$ induces surjections $C_{ij}(e) \to C_{ij}(e')$ for $i, j \in \{1, 2\}$. Hence $x', y'$ can be lifted to elements $\bar{x}', \bar{y}' \in C_{21}(e), v \in C_{12}(e)$, respectively, satisfying $\bar{u} = x', \bar{v} = y'$. Hence

$$t_C(uv) = t_C(x'y') = 1_k,$$

and we conclude $t_C(uv) = 1 + \alpha$ for some $\alpha \in I$. This implies $1 + \alpha \in k^\times$ with inverse $1 - \alpha$ since $I^2 = \{0\}$. Setting $x := u \in C_{21}(e)$, $y := (1 - \alpha)v \in C_{12}(e)$, we therefore deduce not only $\bar{x} = x'$, $\bar{y} = y'$ but also $t_C(xy) = 1$, so $\Delta := (e, x, y)$ is a splitting datum for $C$ such that $\Delta = \Delta'$.

(c) $r = 8$. A splitting datum for $C$ has the form $\Delta' = (e', x_1', x'_2, x'_3)$ for some elementary idempotent $e' \in C$ and some $x_1', x'_2, x'_3 \in \bar{C}_{21}(e')$ satisfying $t_C(x'_1x'_2x'_3) = -1_k$. Again $e'$ can be lifted to an elementary idempotent $e \in C$ satisfying $\bar{e} = e'$, and again $x_i'$ can be lifted to an element $u_i \in C_{21}(e)$ satisfying $\bar{u}_i = x'_i$ for $1 \leq i \leq 3$. Hence

$$t_C(u_1u_2u_3) = t_C(x'_1x'_2x'_3) = -1_k,$$

and we conclude $t_C(u_1u_2u_3) = -1 + \alpha$ for some $\alpha \in I$. This implies $-1 + \alpha \in k^\times$ with inverse $-(1 - \alpha)$ since $I^2 = \{0\}$, and $x_i := u_i$ for $i = 1, 2$ and $x_3 := \alpha u_3$, we therefore deduce not only $\bar{x}_i \in C_{21}(e)$ and $\bar{x}_i = x'_i$ for $1 \leq i \leq 3$ but also $t_C(x_1x_2x_3) = -1$. Thus $\Delta := (e, x_1, x_2, x_3)$ is a splitting datum for $C$ such that $\Delta = \Delta'$.

28.24. The $k$-functor of isomorphisms. Let $A, B$ be non-associative $k$-algebras. (a) In partial generalization of 27.23, we consider the set of $(k$-algebra$)$ isomorphisms from $A$ to $B$:

$$\text{Isom}_k(A, B) := \{ \eta \mid \eta : A \to B \text{ is a } k\text{-isomorphism} \}.$$  

This set will in general be empty but it gives rise to a $k$-functor

$$\text{Isom}_k(A, B) : \text{Alg}_k \to \text{set}$$

by defining

$$\text{Isom}_k(A, B)(R) := \text{Isom}_k(A_R, B_R)$$

for all $R \in \text{Alg}_k$ and

$$\text{Isom}_k(A, B)(\phi) : \text{Isom}_k(A, B)(R) \to \text{Isom}_k(A, B)(S),$$

$$\text{Isom}(A_R, B_R) \ni \eta \mapsto \eta_S \in \text{Isom}_S(A_S, B_S).$$
for all morphisms $\varphi: R \to S$ in $k\text{-alg}$, where we view $S$ as an $R$-algebra via $\varphi$ and identify $A_S = (A_R)_S$, $B_S = (B_R)_S$ as $S$-algebras via (10.3.1).

(b) The $k$-group functor $\text{Aut}(A)$ of (27.23) acts canonically on $\text{Isom}(A,B)$ from the right via

$$\text{Isom}_R(A_R,B_R) \times \text{Aut}(A_R) \to \text{Isom}(A_R,B_R), \quad (\eta, \zeta) \mapsto \eta \circ \zeta,$$

and this action is simply transitive.

(c) Returning to our composition algebra $C$ of rank $r > 1$ over $k$, we define a splitting of $C$ as an isomorphism from $C_{0r}(k)$ onto $C$, where $C_{0r}(k)$ is the split composition algebra over $k$ described in (24.24.18). Thus $\text{Isom}(C_{0r}(k),C)$ is the set of splittings of $C$.

(d) The terminology introduced in (a)–(c) above applies equally well to other algebraic structures, like quadratic forms (Exercise 27.22), associative algebras with or without involution (Exercise 28.25) or para-quadratic algebras (34.22) below.

28.25. Proposition. Let $C$ be a composition algebra of rank $r > 1$ over $k$ and denote by $\Delta_{0r}(k)$ the standard splitting datum for $C_{0r}(k)$ as defined in (28.22). Then the assignment

$$\eta \mapsto \eta(\Delta_{0r}(k))$$

defines a bijection from the set of splittings of $C$ onto the set of splitting data of $C$:

$$\Phi := \Phi(k): \text{Isom} (C_{0r}(k),C) \cong \text{Splid}(C).$$

Proof. Since $\Delta_0 := \Delta_{0r}(k)$ is a splitting datum for $C_0 := C_{0r}(k)$, its image under an isomorphism $\eta: C_0 \cong C$ is a splitting datum for $C$. Thus the map $\Phi$ is well defined, and it remains to show that it is bijective.

We begin with injectivity, which will follow once we have shown that $\Delta_0$ generates $C_0$ as a unital $k$-algebra. By (28.22) this is trivial for $r = 2$ and obvious for $r = 4$, while for $r = 8$ it suffices to note $X_i X_j = (0,e_i)$ for all cyclic permutations $(ijl)$ of $(123)$, which follows immediately from (24.17) and (28.22).

In order to show that $\Phi$ is surjective, we pick any splitting datum $\Delta$ of $C$ and have to find an isomorphism $\eta: C_0 \to C$ sending $\Delta_0$ to $\Delta$. We do so again by treating the cases $r = 2, 4, 8$ separately.

$r = 2$. Then $\Delta = (e)$ for some elementary idempotent $e \in C$. From (19) Exercise 8, we deduce that $e, e$ are unimodular and $ke + k\bar{e}$ is a quadratic étale subalgebra of $C$. Hence $C = ke \oplus k\bar{e}$ since $C$ has rank 2 as a $k$-module, and

$$\eta: C_0 \to C, \quad \alpha \oplus \beta \mapsto \alpha e + \beta \bar{e}$$

is an isomorphism sending $\Delta_0$ to $\Delta$.

$r = 4$. Then $\Delta = (e,x,y)$, with $e \in C$ an elementary idempotent and $x,y \in C_{21}(e)$ satisfying (28.20). By Proposition 25.10 we may assume
for some line bundle \( L \) over \( k \), and \([25.9][3]\) yields elements \( u \in L, v^t \in L^* \) such that \( x = \begin{pmatrix} 0 & 0 \\ u & 0 \end{pmatrix} \), \( y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \). Now \([28.20][1]\) implies \( \langle v^t, u \rangle = 1 \), forcing \( L, L^* \) to be free \( k \)-modules of rank 1 with dual basis vectors \( u, v^t \), respectively. Hence the assignment

\[
\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta v^t \\ \gamma u & \delta \end{pmatrix}
\]

defines an isomorphism \( \eta : C_0 \sim C \) sending \( \Delta_0 \) to \( \Delta \).

\( r = 8 \). Then \( \Delta = (e, x_1, x_2, x_3) \), where \( e \in C \) is an elementary idempotent and \( x_1, x_2, x_3 \in C_{21}(e) \) satisfy \([28.20][2]\). By Theorem \([25.12]\) we may assume

\[
C = \text{Zor}(M, \theta) = \left( \begin{array}{cc} k & M^* \\ M & k \end{array} \right), \quad e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},
\]

for some finitely generated projective \( k \)-module \( M \) of rank 3 and some orientation \( \theta \) of \( M \), where \([25.11][8]\) yields elements \( u_1, u_2, u_3 \in M \) satisfying \( x_i = \begin{pmatrix} 0 & 0 \\ u_i & 0 \end{pmatrix} \) for \( i = 1, 2, 3 \). Combining \([28.20][2]\) with \([25.11][3]\), \([25.11][2]\), we conclude

\[
-e = (x_1 x_2) x_3 = \begin{pmatrix} 0 & u_1 \times u_2 \\ u_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & u_3 \end{pmatrix} = \begin{pmatrix} -\langle u_1, u_2, u_3 \rangle 0 \\ 0 & 0 \end{pmatrix}
\]

hence \( \theta(u_1 \land u_2 \land u_3) = 1 \). Thus \( (u_1, u_2, u_3) \) is a \( \theta \)-balanced basis of \( M \) in the sense of \([25.11]\) which also implies that there is an identification \( C = \text{Zor}(k) = C_{\theta 8}(k) = C_0 \) matching \( u_i \) with \( e_i \) for \( i = 1, 2, 3 \). But this means we have found an isomorphism from \( C_0 \) to \( C \) sending \( \Delta_0 \) to \( \Delta \).

**28.26. Theorem** (Loos-Petersson-Racine \([73][4.10]\)]. Let \( C \) be a composition algebra of rank \( r \in \{1, 2, 4, 8\} \) over \( k \). Then the \( k \)-functor

\[
\text{Isom}(C_{0r}(k), C)
\]

is an affine smooth torsor in the étale topology with structure group \( G = \text{Aut}(C_{0r}(k)) \).

**Proof.** The assertion is trivial for \( r = 1 \) since in this case, applying Exercise \([145]\) below, we obtain a natural identification of \( \text{Isom}(C_{01}(k), C) \) with the closed subscheme \( I_C \subseteq C_a \). Hence we may assume \( r > 1 \). Putting \( X := \text{Isom}(C_{0r}(k), C) \), the set maps

\[
\Phi(R) : X(R) \sim \text{Splid}(C)(R)
\]

given by Proposition \([28.25]\) for any \( R \in k\text{-alg} \) are bijective and one checks that they are compatible with base change, hence give rise to an isomorphism

\[
\Phi : X \sim \text{Splid}(C)
\]
of $k$-functors. By Proposition $28.23$ therefore, $X$ is a smooth affine $k$-scheme acted upon by $G$ from the right in a simply transitive manner $28.24$ (b)). In view of $28.9$ $28.17$ (ii), the proof of the theorem will be complete once we have shown $X(K) \neq \emptyset$ for all algebraically closed fields $K \in k_{\text{alg}}$. But this follows immediately from $26.10$. □

The preceding theorem has two corollaries which, up to a point, will be proved simultaneously.

28.27. Corollary (Loos-Petersson-Racine [73, 4.11]). For any $k$-algebra $C$, the following conditions are equivalent.

(i) $C$ is a composition algebra over $k$.

(ii) There exists a faithfully flat $k$-algebra $R \in k_{\text{alg}}$ making $C_R$ a composition algebra over $R$.

(iii) There exists a faithfully flat $k$-algebra $R \in k_{\text{alg}}$ making $C_R$ a composition algebra over $R$ that is split in the sense of $24.18$.

(iv) There exists a fppf étale $k$-algebra $R \in k_{\text{alg}}$ making $C_R$ a split composition algebra over $R$.

28.28. Corollary (Loos-Petersson-Racine [73, 4.12]). Let $C$ be a composition algebra over $k$. Then $\text{Aut}(C)$ is a smooth $k$-group scheme.

Proof of 28.27, 28.28. We first note that in 28.27, the implications (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) are obvious, while the implication (ii) $\Rightarrow$ (i) follows from the fact that $C$ is a conic algebra (by Exercise $146$) whose norm, $n_C$, is separable (by Exercise $144$, since $(n^C)_R = n^C_R$ is and $R$ is faithfully flat) and permits composition (since $(n^C)_R$ does and the natural map $C \to C_R$ by Proposition $28.4$ is injective). In 28.27 therefore, it remains to prove the implication (i) $\Rightarrow$ (iv).

Next we reduce both corollaries to the case that $C$ has rank $r \in \{1, 2, 4, 8\}$ as a $k$-module. (1) REDRAN This is accomplished by considering the rank decomposition of $C$, which, by $24.18$ attains the form

$$k = k_0 \oplus k_1 \oplus k_2 \oplus k_3, \quad C = C_0 \oplus C_1 \oplus C_2 \oplus C_3$$

(2) RADECO as direct sums of ideals, where $C_j := C_{k_j}$ is a composition algebra of rank $2^j$ over $k_j$ for $0 \leq j \leq 3$. Hence, assuming the implication (i) $\Rightarrow$ (ii) of 28.27 if (1) holds, we find fppf étale $k_j$-algebras $R_j$ for $0 \leq j \leq 3$ such that the composition algebra $C_{kR_j}$ over $R_j$ is split of rank $2^j$. It is now straightforward to check that $R := R_0 \oplus R_1 \oplus R_2 \oplus R_3$ is an fppf étale $k$-algebra making $C_R = C_{kR_0} \oplus C_{kR_1} \oplus C_{kR_2} \oplus C_{kR_3}$ a split composition algebra over $k$. This completes the reduction for 28.27.

Assuming 28.28 if (1) holds, let $R \in k_{\text{alg}}$ and $I \subseteq R$ be an ideal having $I^2 = \{0\}$. Using $[9]$ Exercise $32$ and arguing as before, we have
\[ R = R_0 \oplus R_1 \oplus R_2 \oplus R_3, \]
\[ I = I_0 \oplus I_1 \oplus I_2 \oplus I_3, \]  
(3) \[ C_R = C_{0R_0} \oplus C_{1R_1} \oplus C_{2R_2} \oplus C_{3R_3}, \]
\[ C_{R/I} = C_{0R_0/I_0} \oplus C_{1R_1/I_1} \oplus C_{2R_2/I_2} \oplus C_{3R_3/I_3}. \]

Since \( C_{j,R_j} = 1_j C_R \), we conclude that \( \text{Aut}(C_R) \) stabilizes \( C_{j,R_j} \) for \( 0 \leq j \leq 3 \). Thus
\[ \text{Aut}(C_R) = \text{Aut}(C_{0R_0}) \times \text{Aut}(C_{1R_1}) \times \text{Aut}(C_{2R_2}) \times \text{Aut}(C_{3R_3}), \]
and, similarly,
\[ \text{Aut}(C_{R/I}) = \text{Aut}(C_{0R_0/I_0}) \times \text{Aut}(C_{1R_1/I_1}) \times \text{Aut}(C_{2R_2/I_2}) \times \text{Aut}(C_{3R_3/I_3}). \]

Since \( C_{j,R_j} \) has rank \( 2^j \) over \( R_j \), the \( k_j \)-group scheme \( \text{Aut}(C_j) \) is smooth, forcing it to be finitely presented and the natural map \( \text{Aut}(C_{j,R_j}) \rightarrow \text{Aut}(C_{j,R_j/I_1}) \) to be surjective for \( 0 \leq j \leq 3 \). Hence so is the natural map \( \text{Aut}(C_R) \rightarrow \text{Aut}(C_{R/I}) \), which completes the reduction also for \( 28.28 \).

For the remainder of the proof, we may therefore assume that \( \mathcal{I} \) holds. Hence Theorem 28.26 implies that \( X := \text{Isom}(C_{0R_0}(k), C) \) is an affine smooth torsor in the \( \text{étale} \) topology, with structure group \( G = \text{Aut}(C_{0R_0}(k)) \). Thus condition (iii) of 28.18 implies \( X(R) \neq \emptyset \) for some \( \text{étale fppf} \) \( R \in \text{k-alg} \). Hence \( C_R \cong C_{0R_0}(R) \) is split of rank \( r \) over \( R \). This completes the proof of 28.27. Moreover, the chain of isomorphisms
\[ \text{Aut}(C)_R \cong \text{Aut}(C_R) \cong \text{Aut}(C_{0R_0}(R)) \cong G_R \cong X_R \]
shows that \( \text{Aut}(C)_R \) is smooth over \( R \). But then, by 28.17 (iii), \( \text{Aut}(C) \) must be smooth over \( k \).

28.29. Concluding remarks. The three fundamental facts from algebraic geometry assembled in 28.17 form an extremely versatile tool to derive non-trivial results about non-associative algebras over commutative rings, having first been applied by Loos [69] in the setting of Jordan pairs more than forty years ago. Further application in many different directions will be given in subsequent portions of this work.

Exercises.

139. Modules and faithful flatness. Let \( M \) be a \( k \)-module.

(a) If \( k' \in \text{k-alg} \) is faithfully flat and \( M_{k'} \) is finitely generated as a \( k' \)-module, show that so is \( M \) as a \( k \)-module.

(b) If \( M \) is projective of rank \( r \in \mathbb{N} \), show that there exists a faithfully flat \( k \)-algebra \( k' \) making \( M_{k'} \) a free \( k' \)-module of rank \( r \).

140. Let \( R \) be a finitely presented \( k \)-algebra.

(a) Prove that a finitely presented \( R \)-module is finitely presented over \( k \).

(b) Conclude from (a) that \( R_f \) is a finitely presented \( k \)-algebra, for any \( f \in R \).
141. Let $\varphi : R \to R'$ be a surjective morphism in $k\text{-alg}$. Prove:

(a) (cf. [22, § 3, 1.3 (b)]) If $R$ is finitely generated and $R'$ is finitely presented, then $\operatorname{Ker}(\varphi) \subseteq R$ is a finitely generated ideal.

(b) If $R$ is finitely presented and $\operatorname{Ker}(\varphi) \subseteq R$ is a finitely generated ideal, then $R'$ is finitely presented.

142. Let $M$ be a finitely generated projective $k$-module. Show that the affine $k$-scheme $M_a$ of $M$ is finitely presented.

143. Let $M$ be a $k$-module and $w \in M$. Show that $\tilde{w} : k\text{-alg} \to \text{set}$ defined by $\tilde{w}(R) = \{w_R\} \subseteq M_R$ for all $R \in k\text{-alg}$ is a subfunctor of $M_a$, and even a finitely presented closed affine subscheme if $M$ is finitely generated projective.

144. Let $M$ be a projective $k$-module, and $q : M \to k$ a quadratic form and $R$ a faithfully flat $k$-algebra. Show that if $q_R : M_R \to R$ is separable over $R$ in the sense of [12, 11] then so is $q$ over $k$.

145. Faithfully flat descent of polynomial laws. Let $R$ be a faithfully flat $k$-algebra. As in 28.5 consider the two morphisms

$$\rho_i : R \to S := R \otimes R$$

in $k\text{-alg}$ defined by

$$\rho_i(r) := r \otimes 1_R, \quad \rho_2(r) := 1_R \otimes r \quad (r \in R).$$

Pulling back scalar multiplication from $S$ to $R$ by means of $\rho_i$ converts any $T \in S\text{-alg}$ into some $T_i \in R\text{-alg}$ such that $T_1 = T_2 = T$ as $k$-algebras. Now let $M, N$ be $k$-modules and suppose $g : M_R \to N_R$ is a polynomial law over $R$. Then prove:

(a) For $i = 1, 2$, there are unique polynomial laws $g_i : M_S \to N_S$ over $S$ such that $g_{R_T} := (g_i)_R = g_T$ as set maps from $(M_S)_T = M_T = (M_R)_T$ to $(N_S)_T = N_T = (N_R)_T$ for all $T \in S\text{-alg}$.

(b) There exists a polynomial law $f : M \to N$ over $k$ satisfying $f \otimes R = g$ if and only if $g_1 = g_2$. In this case, $f$ is unique, and for all $k' \in k\text{-alg}$, the morphism

$$\psi : k' \to R_{k'}, \quad \alpha' \longmapsto 1_R \otimes \alpha',$$

in $k\text{-alg}$ makes the diagram

$$\begin{array}{cccccc}
M_{k'} & \xrightarrow{1_{k'} \otimes \psi} & M_{k'} & \xrightarrow{\text{can}_{\psi, k'}} & M_{k'} & \xrightarrow{1_{k'} \otimes \psi} & M_{k'} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
M_{R_{k'}} & \xrightarrow{1_{R_{k'}} \otimes \psi} & (M_{k'})_{R_{k'}} = (M_{R_{k'}})_{k'} & \xrightarrow{\text{can}_{\psi, R_{k'}}} & (N_{k'})_{R_{k'}} = (N_{R_{k'}})_{k'} & \xrightarrow{1_{R_{k'}} \otimes \psi} & N_{R_{k'}}
\end{array}$$

commutative.

146. Faithfully flat descent of conic algebras. Let $C$ be a non-associative $k$-algebra and suppose $R \in k\text{-alg}$ is faithfully flat. Prove:

(a) If $C_R$ is unital, then so is $C$.

(b) If $C$ is projective as a $k$-module and $C_R$ carries a quadratic form over $R$ making it a conic $R$-algebra, then $C$ carries a quadratic form over $k$ making it a conic $k$-algebra such that the base change from $k$ to $R$ of $C$ as a conic $k$-algebra is $C_R$ as a conic $R$-algebra.
Remark. This exercise is a routine application of the previous one. Applications of this kind will occur quite frequently in the present volume. Rather than always carrying out the details, we from now on refer to these applications by saying that the corresponding results are obtained by faithfully flat descent.

Let $Q := (M, q)$ be a quadratic space of rank $2n$, $n \in \mathbb{N}$, over $k$. By a hyperbolic basis of $Q$ we mean a family $(w_i)_{1 \leq i \leq 2n}$ of elements in $M$ such that

$$q(w_i) = q(w_{n+i}) = q(w_i, w_j) = q(w_{n+i}, w_{n+j}) = 0, \quad q(w_i, w_{n+j}) = \delta_{ij}$$

for $1 \leq i, j \leq n$. The set of hyperbolic bases of $Q$ will be denoted by $\text{Hyp}(Q) \subseteq M^{2n}$.

(a) Show that the $k$-functor $\text{Hyp}(Q) : k\text{-alg} \rightarrow \text{set}$ given by

$$\text{Hyp}(Q)(R) := \text{Hyp}(Q_R), \quad Q_R := (M_R, q_R),$$

for all $R \in k\text{-alg}$ and

$$\text{Hyp}(Q)(\varphi) : \text{Hyp}(Q)(R) \rightarrow \text{Hyp}(Q)(S),$$

$$\text{Hyp}(Q_R) \ni (w_i)_{1 \leq i \leq 2n} \mapsto (w_S)_{1 \leq i \leq 2n} \in \text{Hyp}(Q_S)$$

for all morphisms $\varphi : R \rightarrow S$ in $k\text{-alg}$ is a smooth closed $k$-subscheme of $M^{2n}$.

(b) Conclude from (a) that

(i) there exists a fpqc étale $k$-algebra $R$ making $Q_R$ a split hyperbolic quadratic space over $R$ in the sense of 12.17

(ii) $O(Q)$ is a smooth group scheme.

(Hint. Imitate the arguments of 28.24–28.28)
Chapter 5
Jordan algebras

In the preceding chapter, we investigated some fundamental properties of composition algebras, particularly of octonions, over arbitrary commutative rings. Our next main objective will be to accomplish the same for what we call cubic Jordan algebras, among which Albert algebras are arguably the most important. In order to achieve this objective, a few prerequisites from the general theory of Jordan algebras are indispensable. Rather than striving for maximum generality, we confine ourselves to what is absolutely necessary for the intended applications.

29. Linear Jordan algebras

Linear Jordan algebras have been introduced by Albert, who in three fundamental papers [4, 5, 6] developed a virtually complete structure theory of the finite-dimensional ones over arbitrary fields of characteristic not 2. While the main focus of the present volume is primarily on (quadratic) Jordan algebras, linear Jordan algebras are still of some interest since, e.g., they motivate the study of quadratic ones and provide useful illustrations of why certain weird phenomena can only occur in characteristic 2. In this section, the most elementary properties of linear Jordan algebras will be discussed. Since linear Jordan algebras have been extensively treated in book form (Braun-Koecher [15], Jacobson [43], Zhevlakov et al [127], and particularly McCrimmon [83]), proofs will often be omitted.

Throughout we let \( k \) be a commutative ring containing \( \frac{1}{2} \). We begin by repeating the definitions 5.6, 5.7.

29.1. The concept of a linear Jordan algebra. By a linear Jordan algebra over \( k \) we mean a (non-associative) \( k \)-algebra \( J \) satisfying the following identities, for all \( x, y \in J \).

\[
\begin{align*}
xy &= yx \quad \text{(commutative law),} \\
x(x^2y) &= x^2(xy) \quad \text{(Jordan identity).}
\end{align*}
\]

29.2. Special and exceptional linear Jordan algebras. (a) Let \( A \) be a \( k \)-algebra with multiplication \((x,y) \mapsto xy\). Then the symmetric product

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

converts \( A \) into a commutative algebra over \( k \), denoted by \( A^+ \). Moreover, one checks easily that, if \( A \) is associative, then \( A^+ \) is a linear Jordan algebra. Linear Jordan
algebras that are isomorphic to a subalgebra of $A^+$, for some associative algebra $A$, are said to be special. Non-special linear Jordan algebras are called exceptional.

(b) For example, let $B$ be a unital $k$-algebra and $\tau : B \to B$ an involution. Then $H(B, \tau) = \{ x \in B \mid \tau(x) = x \}$ is a unital subalgebra of $B^+$. In particular, if $B$ is associative, then $H(B, \tau)$ is a unital special Jordan algebra.

29.3. Elementary identities. The Jordan identity (29.1.2) can be expressed in terms of left multiplication operators as

$$[L_x, L_{x^2}] = 0,$$  \hspace{1cm} (1)

so a commutative algebra is linear Jordan if and only if (1) holds, i.e., if and only if the left multiplication operators $L_x$ and $L_{x^2}$ commute.

Now let $J$ be a linear Jordan algebra over $k$. Replacing $x$ by $\alpha x + y$ in (1) for $x, y \in J$, $\alpha \in k$, expanding and comparing mixed terms by using the fact that $J$ is commutative and $k$ contains $\frac{1}{2}$, we conclude

$$2[L_x, L_{xy}] + [L_y, L_{x^2}] = 0.$$  \hspace{1cm} (2)

Repeating this procedure and dividing by 2 yields

$$[L_x, L_{yz}] + [L_y, L_{zx}] + [L_z, L_{xy}] = 0,$$  \hspace{1cm} (3)

which, when applied to any $w \in J$, amounts to

$$x((yz)w) + y((zx)w) + z((xy)w) = (yz)(\alpha w) + (zx)(yw) + (xy)(zw).$$  \hspace{1cm} (4)

We call (3) or (4) the fully linearized Jordan identity. Viewing (4) as a linear operator in $x$, we deduce, after an obvious change of notation,

$$L_{(xy)z} = L_{xy}L_z + L_yL_{xz} + L_{yz}L_x - L_yL_xL_y - L_zL_xL_z.$$  \hspace{1cm} (5)

Here the sum of the first three terms on the right is symmetric in $x, y, z$, hence remains unaffected by interchanging $x$ and $z$. Since $[x, y, z] = (xy)z - (yz)x = z(xy) - x(zy)$, this implies

$$L_{[x, y, z]} = L_{[L_z, L_x]}y = [[L_z, L_x], L_y].$$  \hspace{1cm} (6)

For any integer $m > 1$, we may put $y := x^{m-1}$, $z := x$ in (5) and obtain the identity

$$L_{x^{m+1}} = 2L_{xm}L_x + L_xL_{x^{m-1}} - L_x^2L_{x^{m-1}} - L_{x^{m-1}}L_x^2,$$  \hspace{1cm} (7)

which for $m = 2$ reduces to

$$L_x^3 = 3L_xL_{x^2} - 2L_x^3.$$  \hspace{1cm} (8)
29.4. Proposition. If $J$ is a linear Jordan algebra over $k$, then $J_R$ is a linear Jordan algebra over $R$, for any $R \in k$-alg.

Proof. It suffices to check the Jordan identity (29.1.2) for $J_R$, which is straightforward, using the identities derived in 29.3. See [83, p. 149] for details. □

29.5. Proposition. Let $J$ be a linear Jordan algebra over $k$ and $x \in J$.

(a) For $u \in k[x]$ (resp. $u \in k[x]$ if $J$ is unital), $L_u$ is a polynomial in $L_x$ and $L_x^2$.

(b) For $u, v \in k[x]$ (resp. $u, v \in k[x]$ if $J$ is unital), $L_u$ and $L_v$ commute: $[L_u, L_v] = 0$.

Proof. (a) We may assume $u = x^m$ for some $m \in \mathbb{Z}$, $m > 0$ (resp. $m \in \mathbb{N}$). Then the assertion follows from (29.3.7) by induction on $m$.

(b) Since $L_x, L_x^2$ commute by (29.3.1), so do $L_u, L_v$ by (a). □

29.6. Corollary. Linear Jordan algebras over $k$ are power-associative.

Proof. This follows from a straightforward application of Prop. 29.5 (b). Details are left to the reader. □

29.7. Remark. In view of Prop. 29.5, equation (29.3.7) simplifies to

$$L_{x^{m+1}} = 2(L_{x^m} - L_{x^m - 1}L_x)L_x + L_{x^2}L_{x^m - 1}. \tag{1}$$

We have encountered examples of linear Jordan algebras in 29.2 (special Jordan algebras) and in Thm. 5.10 (cubic euclidean Jordan matrix algebras, in particular the euclidean Albert algebra). Other examples, seemingly of a completely different nature, will now be introduced.

29.8. The linear Jordan algebra of a pointed quadratic module. Let $(M, q, e)$ be a pointed quadratic module over $k$, with trace $t$ and conjugation $\iota$, cf. 12.13 for details. Then the $k$-module $M$ becomes a $k$-algebra $J = J(M, q, e)$ under the multiplication

$$xy = \frac{1}{2}(t(x)y + t(y)x - q(x, y)e) \quad (x, y \in M). \tag{1}$$

$J$ is obviously commutative and unital, with identity element $1_J = e$, and we have

$$x^2 - t(x)x + q(x, 1)1_J = 0 \quad (2)$$

for all $x \in J$. Thus $L_x^2$, being a linear combination of $L_x$ and $1_J$, commutes with $L_x$, and we conclude that $J$ is a unital linear Jordan algebra, called the linear Jordan algebra of the pointed quadratic module $(M, q, e)$. Extending the proof of [43, Thm. VII.1] from fields of characteristic not 2 to commutative rings containing $\frac{1}{2}$ in the obvious way, it follows that $J(M, q, e)$ is a special Jordan algebra.

Since $q(e) = 1$, we conclude from (2) that $J = J(M, q, e)$ is a commutative conic $k$-algebra in the sense of 19.1 whose norm, trace, conjugation agree with the corresponding data attached to $(M, q, e)$. Conversely, consider any conic algebra $C$ over $k$. 

As we have noted before, \((C, n_C, 1_C)\) is a pointed quadratic module, and comparing (1) with (19.5.5) divided by 2, we obtain

\[ J(C, n_C, 1_C) = C^+. \]  

We now extend the definition of the \(U\)-operator as given in 6.4 to the present more general context.

### 29.9. The \(U\)-operator of a linear Jordan algebra

Let \(J\) be a linear Jordan algebra over \(k\). For \(x \in J\), the linear map

\[ U_x : J \to J, \quad y \mapsto U_x y := 2x(xy) - x^2y, \]  

is called the \(U\)-operator of \(x\). The quadratic map

\[ U : J \to \text{End}_k(J), \quad x \mapsto U_x = 2L_x^2 - L_{x^2}, \]  

is called the \(U\)-operator of \(J\). Its bilinearization gives rise to the tri-linear Jordan triple product

\[ \{xyz\} := U_{x+z}y = (U_{x+z}y - U_x y - U_z z) = 2(x(zy) + z(xy) - (xz)y). \]  

Viewing this as a map acting on \(z\), we obtain the linear operators

\[ V_{x,y} := 2(L_{xy} + [L_x, L_y]), \]  

uniquely determined by the condition

\[ V_{x,y}z = \{xyz\}. \]  

In particular, we have

\[ V_x := V_{x,1} = V_{1,x} = 2L_x, \]  

so up to the factor 2, the operator \(V_x\) agrees with the left multiplication by \(x\) in \(J\).

### 29.10. Examples

In addition to the \(U\)-operator of cubic Jordan matrix algebras (Exc. 24 (b)), we now discuss the following cases.

(a) Let \(A\) be an associative algebra over \(k\). As in Exc. 24 (a), the \(U\)-operator of he linear Jordan algebra \(A^+\) is given by the formula

\[ U_{x,y} = xyx \quad (x, y \in A) \]  

in terms of the associative product in \(A\). In particular, any subalgebra of \(A^+\) is closed under the binary operation \((x, y) \mapsto xyx\).

(b) Let \((M, q, e)\) be a pointed quadratic module over \(k\), with trace \(t\) and conjugation \(i, x \mapsto \bar{x}\). Then the \(U\)-operator of the linear Jordan algebra \(J(M, q, e)\) is given by the
formula
\[ U_{xy} = q(x, \bar{y})x - q(x)\bar{y} \quad (x, y \in J) \] (2)  

since \([29.8.1], (29.8.2), (29.9.1)\) and \([12.13.1]\) yield
\[ U_{xy} = 2xy - x^2y = t(x)xy + t(y)x^2 - q(x,y)x - t(x)xy + q(x)y \]
\[ = q(x, e)t(y)x - q(x)t(y) e - q(x,y)x + q(x)y \]
\[ = q(x, t(y)e - y)x - q(x)(t(y)e - y) = q(x, \bar{y})x - q(x)\bar{y}, \]
as claimed.

The \(U\)-operator and its variants described in \(29.9\) are of the utmost importance for a proper understanding of (linear) Jordan algebras. This is primarily due to a number of fundamental identities satisfied by these operators.

29.11. Advanced identities. Let \(J\) be a linear Jordan algebra over \(k\). Then the following identities hold for all \(x, y, z, u, v \in J\), where for the validity of the first, \(J\) is required to be unital.

\[ U_{1J} = 1_J, \] (1)  
\[ L_xU_t + U_tL_y = U_{xy,t}, \] (2)  
\[ L_yU_{x,z} + U_{x,z}L_y = U_{xyz} + U_{zyx}, \] (3)  
\[ \{xyz\} = \{zyx\}, \] (4)  
\[ [V_{x,y}, V_{u,v}] = V_{\{xyu\},v} - V_{u,\{yxv\}}, \] (5)  
\[ V_{x,y}U_z = U_zV_{y,x} = U_{xyz}, \] (6)  
\[ V_{U_{x,y}} = V_{x,U_y}, \] (7)  
\[ U_{x,y} = U_xU_y. \] (8)  

A verification of these identities, which (with the exception of (1) and (4)) are highly non-trivial, will be omitted because they are logically not strictly necessary for the subsequent applications to cubic Jordan algebras. The interested reader is referred to McCrimmon [83, p. 202] or Meyberg [85].

30. Para-quadratic algebras.

Just as linear Jordan algebras fit naturally into the more general framework of arbitrary non-associative algebras, i.e., of modules (over a commutative ring) equipped with a binary operation that is linear in each variable, (quadratic) Jordan algebras to be investigated below fit naturally into the more general framework of what we call para-quadratic algebras—modules equipped with a binary operation that is quadratic in the first variable and linear in the second. It is the purpose of the present section
to extend the language of (linear) non-associative algebras as explained in §8 to this modified setting.

Throughout we let $k$ be an arbitrary commutative ring. With an eye on subsequent applications, we discuss the notion of a para-quadratic algebra only in the presence of a base point which serves as a “weak identity element”.

### 30.1. The concept of a para-quadratic algebra.

By a para-quadratic algebra over $k$ we mean a $k$-module $J$ together with a quadratic map

$$U: J \longrightarrow \text{End}_k(J), \quad x \longmapsto Ux,$$

the $U$-operator, and a distinguished element $1_J \in J$, the base point, such that

$$U1_J = 1_J.$$ (2)

We then write

$$\{xyz\} := U_{x+z}y - U_x - U_zy \quad (x,y,z \in J)$$ (3)

for the associated trilinear triple product, and

$$x \circ y := \{x1_Jy\} \quad (x,y \in J)$$ (4)

for the associated bilinear circle product. Note that the triple product (3) is symmetric in the outer variables, while the circle product (4) is commutative. Moreover, $\{xyx\} = 2Uxy$ for all $x, y \in J$. Viewing (3) (resp. (4)) as a linear operator in $z$, we obtain linear maps

$$V_{x,y}: J \longrightarrow J, \quad z \longmapsto \{xyz\},$$ (5)

$$V_x := V_{x,1_J}: J \rightarrow J, \quad y \longmapsto x \circ y = \{x1_Jy\}. \quad (6)$$

that depend bilinearly on $x, y$ (resp. linearly on $x$). Most of the time, we simply write $J$ for a para-quadratic algebra, its $U$-operator, base point, triple and circle product being understood. In keeping with our introductory promise, $1_J$ because of (2), (4) may be regarded as a weak identity element for $J$.

If $J$ and $J'$ are para-quadratic algebras over $k$, a homomorphism from $J$ to $J'$ is defined as a $k$-linear map $\varphi: J \rightarrow J'$ preserving $U$-operators and base points in the sense that

$$\varphi(U_{x,y}) = U_{\varphi(x),\varphi(y)}, \quad \varphi(1_J) = 1_{J'}$$ (7)

for all $x, y \in J$. In this case, $\varphi$ also preserves triple and circle products, so we have

$$\varphi(\{xyz\}) = \{\varphi(x)\varphi(y)\varphi(z)\}, \quad \varphi(x \circ y) = \varphi(x) \circ \varphi(y) \quad (x,y \in J).$$ (8)

Summing up we obtain the category $k\text{-paquad}$ of para-quadratic $k$-algebras.
30.2. **Unital para-quadratic algebras.** A para-quadratic algebra $J$ over $k$ is said to be **unital** if $x \circ y = \{1, xy\}$ for all $x, y \in J$. Since the triple product is symmetric in the outer variables, and because of (30.12.4), we then have

$$x \circ y = \{1, xy\} = \{xy, 1\} = \{xy, 1\}$$  

for all $x, y \in J$ and, in particular, $1_J \circ x = 2U_1, x = 2x$. If $J$ is unital, the weak identity element $1_J$ is called the **unit or identity element** of $J$.

For the rest of this section, we fix a para-quadratic algebra $J$ over $k$.

30.3. **Subalgebras.** For $X, Y, Z \subseteq J$ we denote by $U_X Y$ (resp. $\{X, Y, Z\}$) the additive subgroup of $J$ generated by the expressions $U_{xy}$ (resp. $\{xyz\}$) for $x \in X, y \in Y, z \in Z$. We say that $J'$ is a subalgebra of $J$ if $J' \subseteq J$ is a $k$-submodule satisfying $1_J \in J'$ and $U_{J'J'} + U_{J'J'} + \{J'J\} \subseteq I$. Then $\{J'J'J\} + J' \circ J' \subseteq J'$ and there is a unique way of viewing $J'$ as a para-quadratic $k$-algebra in its own right such that the inclusion $J' \to J$ is a homomorphism. This implies not only $1_{J'} = 1_J$ but also that the triple (resp. circle) product of $J'$ is obtained from the triple (resp. circle) product of $J$ via restriction.

30.4. **Example.** Let $A$ be a flexible unital $k$-algebra, so we have $(xy)x = x(yx)$ for all $x, y \in A$. Then the $U$-operator defined by

$$U_{xy} := xyz$$  

and the unit element of $A$ convert $A$ into a para-quadratic $k$-algebra denoted by $A^{(+)}$. Triple and circle product of $A^{(+)}$ are given by

$$\{xyz\} = (xy)z + (yz)x = x(yz) + z(yx), \quad x \circ y = xy + yx \quad (x, y, z \in A).$$  

In particular, the para-quadratic algebra $A^{(+)}$ is unital.

30.5. **Ideals.** We say $I$ is an **ideal** in $J$ if it is a $k$-submodule satisfying the inclusion relations

$$U_{IJ} + U_{J} + \{J\} \subseteq I.$$  

In this case, there is a unique way of making the $k$-module $J' := J/I$ into a para-quadratic $k$-algebra such that the canonical map from $J$ to $J'$ is a homomorphism. Conversely, the kernel of any homomorphism of para-quadratic algebras is an ideal. Moreover, if $I_1$ and $I_2$ are ideals in $J$, then so is $I_1 + I_2$, and the standard isomorphism theorems of abstract algebra continue to hold in this modified setting.

30.6. **Inner and outer ideals.** There is a vague analogy between one-sided ideals in ring theory and the following notions for para-quadratic algebras. A $k$-submodule $I \subseteq J$ is said to be an **inner (resp. an outer) ideal** if
Thus a submodule of $J$ is an ideal if and only if it is an inner and an outer ideal. But the analogy to one-sided ideals goes only so far: for example, let $I \subseteq J$ be an outer ideal and $x \in I$, $y \in J$. The $2U,I=\{xyx\}\subseteq I$, and we conclude that, if $\frac{1}{2} \in k$, then outer ideals of $J$ are ideals.

30.7. Direct sums of ideals. Let $J_1, \ldots, J_r$ be para-quadratic algebras over $k$. Then

$$J := J_1 \oplus \cdots \oplus J_r,$$

their direct sum as a $k$-module, becomes a para-quadratic $k$-algebra, with $U$-operator and base point respectively given by

$$U_{x_1 \oplus \cdots \oplus x_r} (y_1 \oplus \cdots \oplus y_r) = (U_{x_1} y_1) \oplus \cdots \oplus (U_{x_r} y_r), \quad 1_J = 1_{J_1} \oplus \cdots \oplus 1_{J_r}$$

for $x_i,y_i \in J_i$, $1 \leq i \leq r$. It follows immediately from the definition that also the triple and circle product of $J$ are carried out component-wise. In particular, $J$ is unital if and only if $J_i$ is unital, for each $i = 1, \ldots, r$. Identifying $J_i \subseteq J$ canonically for $1 \leq i \leq r$, we clearly have $U_{J_i} J_j = \{0\}$ for $1 \leq i, j \leq r$, $i \neq j$ and $\{J_i J_j\} = \{0\}$ for $1 \leq i, j, l \leq r$ unless $i = j = l$.

Conversely, let $J$ be a para-quadratic algebra over $k$ and suppose $I_1, \ldots, I_r \subseteq J$ are ideals such that $J = I_1 \oplus \cdots \oplus I_r$ as a direct sum of submodules (i.e., of ideals). For all $i, j, l \in 1, \ldots, r$, this implies $U_{I_i} I_j = \{0\}$ unless $i = j$ and $\{I_i I_j\} = \{0\}$ unless $i = j = l$. It follows that $I_1, \ldots, I_r$ are para-quadratic $k$-algebras in their own right, and $J$ identifies canonically with their direct sum as para-quadratic algebras.

30.8. Powers. Let $x \in J$. We define the powers $x^n \in J$ for $n \in \mathbb{N}$ inductively by

$$x^0 = 1_J, \quad x^1 = x, \quad x^n = U_{x^{n-2}} \quad (n \in \mathbb{N}, n \geq 2)$$

and write

$$k[x] := \sum_{n \in \mathbb{N}} kx^n$$

for the submodule of $J$ spanned by the powers of $x$. More generally, we define

$$k_r[x] := \sum_{n \geq r} kx^n$$

for $r \in \mathbb{N}$ as a submodule of $k[x]$. We say $J$ is power-associative at $x$ if

$$U_{x^m} x^n = x^{2m+n}, \quad \{x^m, x^n x^p\} = 2x^{m+n+p}$$

for all $m, n, p \in \mathbb{N}$. This is easily seen to imply

$$(x^m)^n = x^{mn}$$
30 Para-quadratic algebras.

For all \( m, n \in \mathbb{N} \), and that \( k[x] \subseteq J \) is a para-quadratic subalgebra.

For example, let \( A \) be a unital flexible \( k \)-algebra as in \([30.4]\). Then the powers of \( x \in A \) are the same in \( A \) and \( A^{(+)} \). In particular, if \( A \) is power-associative, then so is \( A^{(+)} \) and conversely.

30.9. Idempotents. An element \( c \in J \) is called an idempotent if \( c^2 = c \). This implies \( c^n = c \) for all positive integers \( n \), hence \( k[c] = k1_J + kc; \) in particular, \( J \) is power-associative at \( c \). There are always the trivial idempotents 0 and 1 but possibly no others. Two idempotents \( c, d \in J \) are said to be orthogonal, written as \( c \perp d \), if

\[
U_c d = U_d c = \{ c d \} = \{ d c \} = c \circ d = 0. \tag{1}
\]

Orthogonality of idempotents is obviously a symmetric relation. Moreover, \( c \perp d \) is easily seen to imply that \( c + d \in J \) is an idempotent. If \( c \in J \) is an idempotent, then so is \( 1_J - c \), and the idempotents \( c, 1_J - c \) are orthogonal.

Let \( A \) be a unital flexible \( k \)-algebra. Then the idempotents of \( A \) and \( A^{(+)} \) are the same. Moreover, for two idempotents \( c, d \in A \) to be orthogonal in \( A^{(+)} \) it is necessary and sufficient that they be orthogonal in \( A \), i.e., \( cd = dc = 0 \).

30.10. The multiplication algebra. The subalgebra of \( \text{End}_k(J) \) generated by the linear operators \( U_x, V_{x,y} \) for \( x, y \in J \) is called the multiplication algebra of \( J \), denoted my \( \text{Mult}(J) \). Note by \([30.11]\) that \( \text{Mult}(J) \) is a unital subalgebra of \( \text{End}_k(J) \), so \( 1_J \in \text{Mult}(J) \). We may view \( J \) canonically as a \( \text{Mult}(J) \)-left module. Then the \( \text{Mult}(J) \)-submodules of \( J \) are precisely the outer ideals of \( J \).

30.11. Simplicity and division algebras. \( J \) is said to be simple if it is non-zero and has only the trivial ideals \( \{0\} \) and \( J \). We say \( J \) is outer-simple if it is non-zero and the only outer ideals are \( \{0\} \) and \( J \). Note by \([30.6]\) that simplicity and outer simplicity are equivalent notions if \( \frac{1}{2} \in k \) but not in general, see ?? below for examples. Note further by \([30.10]\) that outer simplicity (and not simplicity) is equivalent to \( J \) being an irreducible \( \text{Mult}(J) \)-module.

And finally, \( J \) is said to be a division algebra if it is non-zero and \( U_x : J \to J \) is bijective for all nonzero elements \( x \in J \). For example, if \( A \) is a unital flexible division algebra, then \( A^{(+)} \) is a para-quadratic division algebra.

30.12. Scalar extensions. For an \( R \in k\text{-alg} \), the assignment \( \varphi \mapsto \varphi_R = \varphi \otimes 1_R \) determines a unital homomorphism \( \text{End}_k(J) \to \text{End}_R(J_R) \) of \( k \)-algebras, which in turn yields canonically a unital \( R \)-algebra homomorphism

\[
\omega : \big( \text{End}_k(J) \big)_R \longrightarrow \text{End}_R(J_R), \quad \varphi \otimes r \longmapsto r \varphi_R = \varphi \otimes (r 1_R). \tag{1}
\]

Composing this with the \( R \)-quadratic extension of the \( U \)-operators of \( J \) (Cor. \([12.5]\)), we obtain an \( R \)-quadratic map \( U : J_R \to \text{End}_R(J_R) \).
which, together with $1_{J_R} := (1_J)_R$, makes $J_R$ a para-quadratic algebra over $R$, called the scalar extension or base change of $J$ from $k$ to $R$. The para-quadratic algebra structure of $J_R$ is characterized by the conditions that

$$U_{x ⊗ r}(y ⊗ s) = (U_x y ⊗ r^2 s) \quad (x, y ∈ J, \ r, s ∈ R) \tag{3}$$

and that the triple (resp. circle) product of $J_R$ is the $R$-trilinear (resp. $R$-bilinear) extension of the triple (resp. circle) product of $J$. The standard properties enjoyed by the scalar extensions of $k$-modules or linear non-associative algebras over $k$ (cf. [10.1]) now carry over to this modified setting without change.

### 30.13. The centroid

Due to the non-linear character of para-quadratic algebras, it seems impossible to define a meaningful analogue of the centre inside the algebras themselves. Instead, just as in the case of linear non-associative algebras without a unit (e.g., of Lie algebras, cf. Jacobson [42, Chap. X, §1]), one has to work inside their endomorphism algebras.

Accordingly, we define the centroid of $J$, denoted by $\text{Cent}(J)$, as the set of all elements $a ∈ \text{End}_k(J)$ such that, writing $ax := a(x)$ ($a ∈ \text{End}_k(J)$, $x ∈ J$) for simplicity,

$$U_{ax} = a^2 U_x, \quad U_{ax,y} = aU_{x,y}, \quad aU_x = U_x a, \quad (x, y ∈ J). \tag{1}$$

The difficulty with this definition is that one of the conditions imposed on the elements of the centroid is no longer linear in $a$, and hence it is not at all clear whether $\text{Cent}(J) ⊆ \text{End}_k(J)$ is a submodule, let alone a commutative subalgebra. Before discussing this question any further, let us observe for $a ∈ \text{Cent}(J)$ that

$$aU_{x,y} = U_{ax,y} = U_{x,ay} = U_{x,ay} = V_{x,ay} = V_{x,ay} \quad (x, y ∈ J). \tag{2}$$

These relations either follow by linearizing (1) or by straightforward verification, e.g., $aV_{x,y} = aU_{x,y} = U_{ax,y} = V_{ax,y}$ for $z ∈ J$. Note that, in view of (1), (2), the elements of the centroid behave “just like scalars” not only with respect to the $U$-operator but also with respect to the triple and circle product:

$$a\{xyz\} = \{(ax)yz\} = \{x(ay)z\} = \{xy(az)\}, \tag{3}$$

$$a(x ∘ y) = (ax) ∘ y = x ∘ (ay) \tag{4}$$

for all $a ∈ \text{Cent}(J), x, y, z ∈ J.$
Our next aim will be to exhibit conditions under which the centroid becomes a commutative subalgebra (resp. a subfield) of the endomorphism algebra of $J$.

**30.14. Proposition** (cf. McCrimmon [78, Thm. 2]). The following conditions are equivalent.

(i) Cent$(J)$ is a commutative (unital) subalgebra of End$_k(J)$.
(ii) Cent$(J)$ is a (unital) subalgebra of End$_k(J)$.
(iii) Cent$(J)$ is an additive subgroup of End$_k(J)$.
(iv) The elements of Cent$(J)$ commute by pairs: $[a,b] = 0$ for all $a,b \in$ Cent$(J)$.

**Proof.** In (i), (ii), unitality is automatic since $1_J \in$ Cent$(J)$.

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

Before tackling the remaining implications (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i), we claim, for all $a, b \in$ Cent$(J)$,

$$a + b \in$ Cent$(J) \iff \forall x \in J : U_{(a+b)x} = (a + b)^2 U_x \iff [a, b] = 0.$$

Indeed, since the last two conditions of (30.13.1) are linear in $a$, the first equivalence in (1) is obvious. As to the second, we use (30.13.1), (30.13.2) and compute

$$U_{(a+b)x} - (a + b)^2 U_x = U_{ax} + U_{ax, bx} + U_{bx} - a^2 U_x - (ab + ba)U_x - b^2 U_x$$

$$= (2ab - ab - ba)U_x = [a, b]U_x,$$

which by (30.12) is zero for all $x \in J$ if and only if $[a, b] = 0$. This completes the proof of (1).

(iii) $\Rightarrow$ (iv). This follows immediately from (1).

(iv) $\Rightarrow$ (i). By (1) and (iv), we need only show that Cent$(J)$ is closed under multiplication, so let $a, b \in$ Cent$(J)$. Then

$$U_{(ab)x} = a^2 U_{bx} = a^2 b^2 U_x = (ab)^2 U_x$$

since $a$ and $b$ by (iv) commute. Thus $ab \in$ Cent$(J)$.

**30.15. Central para-quadratic algebras.** $J$ is said to be central if the linear map $k \rightarrow$ End$_k(J)$, $\alpha \rightarrow \alpha \cdot 1_J$, is injective with image Cent$(J)$. In this case, Cent$(J)$ $\subseteq$ End$_k(J)$ is a unital subalgebra isomorphic to $k$. Conversely, suppose Cent$(J)$ $\subseteq$ End$_k(J)$ is a subalgebra, automatically unital and commutative by Prop. 30.14. Then the natural action of Cent$(J)$ on $J$ converts $J$ into a central para-quadratic algebra over Cent$(J)$, denoted by $J_{\text{cent}}$ and called the centralization of $J$. See 9.5 for the analogous, but more elementary, concept in the context of linear non-associative algebras.

**30.16. The extreme radical.** We wish to show that, under some mild extra condition, the centroid of a simple para-quadratic algebra is a field. This extra condition is best understood in terms of the extreme radical of $J$, which is defined by
30.17. **Theorem** (Schur’s lemma) (cf. McCrimmon [78] Thm. 3). *The centroid of a simple para-quadratic algebra with zero extreme radical is a field.*

**Proof.** Let \( a, b \in \text{Cent}(J) \) and \( x, y \in J \). Then (30.13.1), (30.13.2) yield

\[
U_{[a,b]x} = U_{abx - bax} = U_{abx} - U_{bax} + U_{bax} = a^2 U_{bx} - a U_{b,ax} b + U_{ax} b^2 = 0,
\]

\[
U_{[a,b]x,y} = U_{abx - bax,y} = a U_{x,y} b - a U_{x,y} b = 0.
\]

Hence \([a,b]x \in J(J) = \{0\}\), and we deduce from Prop. [30.14] that \( \text{Cent}(J) \subseteq \text{End}_k(J) \) is a commutative unital subalgebra. It remains to show that its non-zero elements are invertible, so let \( a \in \text{Cent}(J) \) be non-zero. For \( x, y, z \in J \) we have

\[
U_{ax,y} = a^2 U_{x,y} \in \text{Im}(a), \quad U_{ax} = a U_{x} \in \text{Im}(a), \quad \{yz(ax)\} = a \{yzx\} \in \text{Im}(a),
\]

whence \( \text{Im}(a) \subseteq J \) is a non-zero ideal. Thus \( \text{Im}(a) = J \) by simplicity, and \( a \) is surjective. On the other hand, let \( z \in I := \text{Ker}(a) \). Then \( a \{xyz\} = \{xyz\} = 0 \) for all \( x, y \in J \), forcing \( \{JJI\} \subseteq I \). Similarly, \( UJ \subseteq I \). And finally, since \( a \) is surjective, \( x = aw \) for some \( w \in J \), which implies \( U_{ax} = a U_{aw} = a^2 U_{aw} = 0 \), hence \( U_{ax} \in I \). Thus \( I \subseteq J \) is an ideal, and we conclude \( I = \{0\} \). Summing up, we have shown that \( a: J \to J \) is bijective.

**Exercises.**

148. **Monomials and the nil radical in para-quadratic algebras.** Let \( J \) be a para-quadratic algebra over \( k \). For \( X \subseteq J \) and \( m \in \mathbb{N} \) we define subsets \( \text{Mon}_m(X) \subseteq J \) by setting \( \text{Mon}_0(X) := \{1_J\} \), \( \text{Mon}_1(X) := X \) and by requiring that \( \text{Mon}_m(X) \) for \( m > 1 \) consist of all elements \( U_{x,z} y \in \text{Mon}_m(X) \) for \( m, p \in \mathbb{N}, n > 0, m = 2n + p \). The elements of

\[
\text{Mon}(X) := \bigcup_{m \in \mathbb{N}} \text{Mon}_m(X)
\]

are called *monomials* (in \( J \)) over \( X \).

(a) Prove \( \text{Mon}_m(\{x\}) = \{x^m\} \) for all \( x \in J \) and all \( m \in \mathbb{N} \) if \( J \) is power-associative.

(b) An element \( x \in J \) is said to be *nilpotent* if \( 0 \in \text{Mon}(\{x\}) \) is a monomial over \( \{x\} \). We say \( I \subseteq J \) is a nil ideal if it is an ideal consisting entirely of nilpotent elements. Prove that the image of a nilpotent element under a homomorphism of para-quadratic algebras is nilpotent, and that for ideals \( I' \subseteq J \) in \( J \), the ideal \( I \) is nil if and only if \( I' \) is nil and \( I/I' \) is a nil ideal in \( J/I' \). Conclude that the sum of all nil ideals in \( J \) is a nil ideal, called the *nil radical of \( J \)*, denoted by \( \text{Nil}(J) \).

(c) Prove \( \text{Nil}(k)J \subseteq \text{Nil}(J) \).

149. **Para-quadratic evaluation.** Let \( J \) be a para-quadratic algebra over \( k \) and \( x \in J \) such that \( J \) is power-associative at \( x \). We define the *evaluation* at \( x \in J \) as the linear map \( \varepsilon_x: k[1] \to J \) determined by \( \varepsilon_x(1^n) = x^n \) for all \( n \in \mathbb{N} \) and put \( f(x) := \varepsilon_x(f) \) for all \( f \in k[1] \).
(a) Show that $\varepsilon_x^t : k[t]^{(+)} \to J$ is a homomorphism of para-quadratic $k$-algebras and conclude that

$$I := I_x := \ker(\varepsilon_x) := \{ f \in k[t] : f(x) = 0 \}$$

is an ideal in $k[t]^{(+)}$. Show further that

$$J^0 := J^0_x := \ker(\varepsilon_x) = \{ f \in k[t] : f(x) = (t^f)(x) = 0 \}$$

is the unique largest ideal in $k[t]$ contained in $I$. Moreover, both $f^2$ and $2f$ belong to $J^0$ for all $f \in I$. It follows that $R := k[t]/J^0$ is a unital commutative associative $k$-algebra, and with the canonical projection $\varepsilon_x^t : k[t] \to R$, there is a unique homomorphism $\pi : R^{(+)} \to J$ of para-quadratic algebras making the diagram

\begin{center}
\begin{tikzcd}
 k[t]^{(+)} \arrow[r, \varepsilon_x^t] \arrow[d, \pi] & k[t] \arrow[d, \varepsilon_x] \\
 R^{(+)} \arrow[r, \pi] & J
\end{tikzcd}
\end{center}

commutative. In particular, $k[x] = \text{Im}(\pi) \subseteq J$ is a para-quadratic subalgebra of $J$, and $a^2 = 2a = 0$ for all $a \in \ker(\pi)$.

(b) Suppose $2 = 0$ in $k$ and let $n \geq 2$ be an integer. Show that

$$I_n := k[t^n + t^{n+2}]$$

is an ideal in $k[t]^{(+)}$ but not in $k[t]$. Conclude from the relations

$$x^{n+1} \neq 0, x^n = x^{n+2} = x^{n+3} = \ldots$$

for the image of $t$ under the canonical projection $k[t]^{(+)} \to J_n := k[t]^{(+)}/I_n$ that $J_n$ has no linear structure, i.e., there is no unital flexible algebra $A$ over $k$ satisfying $J_n \cong A^{(+)}$.

\textbf{Pr.Paponi} 150. Let $J$ be a para-quadratic algebra over $k$ and $x \in J$. Show that, if $J$ is power-associative at $x$, the following conditions are equivalent.

(i) $x$ is nilpotent in the sense of Exc. [148](b).
(ii) $x^n$ for some positive integer $m$.
(iii) There exists a positive integer $m$ such that $x^n = 0$ for all integers $n \geq m$.

Show further for the para-quadratic subalgebra $k[x] \subseteq J$ (cf. Exc. [149](a)) that

$$\text{Nil}(k[x]) = \{ v \in k[x] : v \text{ is nilpotent} \}.$$ 

\textbf{Pr.Paralift} 151. Para-quadratic lifting of idempotents. Let $J$ be a para-quadratic algebra over $k$ and $x \in J$ such that $J$ is power-associative at $x$.

(a) For $v \in k[x]$, let $U^t_v : k[x] \to k[x]$ be the restriction of $U_v$ to $k[x]$. Prove

$$U^t_v(fg)(x) = U^t_v(f)(x)U^t_v(g)(x) \quad (1)$$

for all $f, g \in k[t]$ and conclude

$$[U^t_v, U^t_w] = 0, \quad U^t_{v+w} = U^t_v U^t_w, \quad U^t_n = U^t_0^n \quad (2)$$

for all $v, w \in k[x]$ and all $n \in \mathbb{N}$.

(b) Assume there are integers $n > d > 0$ and scalars $\alpha_d, \ldots, \alpha_{d-1} \in k$ such that $\alpha_d \in k^*$ and

$$\alpha_d x^d + \alpha_{d+1} x^{d+1} + \cdots + \alpha_{d-1} x^{d-1} + x^n = 0.$$
Show that there is a unique element \( v \in k[x] \) satisfying \( U_v v = x^2 \). Conclude \( U_v = 1 \) on \( k[x] \) and that \( c := v^2 \) is an idempotent in \( k[x] \) satisfying \( U_c = 1 \) on \( k[x] \). (Hint. Apply Exc. 81(a) and Exc. 149(a).)

(c) Let \( \varphi : J \to J' \) be a surjective homomorphism of power-associative para-quadratic algebras over \( k \) and suppose \( \text{Ker}(\varphi) \subseteq J \) is a nil ideal (Exc. 148). Conclude from (b) that every idempotent \( c' \in J' \) can be lifted to \( J \), i.e., there exists an idempotent \( c \in J \) satisfying \( \varphi(c) = c' \).

**152. The outer centroid.** Let \( J \) be a para-quadratic algebra over \( k \) and define the **outer centroid** of \( J \), denoted by \( \text{Cent}_{\text{out}}(J) \), as the centralizer of the multiplication algebra of \( J \). We say \( J \) is outer central if the natural map \( \alpha \to \alpha 1_J \) from \( k \) to the outer centroid of \( J \) is an isomorphism. Prove:

(a) If \( J \) is outer simple, then its outer centroid is an associative division ring.
(b) If \( k \) is a field and \( J \) is finite-dimensional and outer simple over \( k \), then \( \text{End}_{\text{Cent}_{\text{out}}(J)}(J) = \text{Mult}(J) \).
(c) Assume \( k \) is a field and \( J \) is finite-dimensional over \( k \). Then \( J \) is outer central and outer simple if and only if it is non-zero and \( \text{Mult}(J) = \text{End}_{k}(J) \).
(d) For a finite-dimensional para-quadratic algebra over a field, the following conditions are equivalent.

(i) \( J \) is outer central and outer simple.
(ii) Every base field extension of \( J \) is outer simple.
(iii) The scalar extension of \( J \) to the algebraic closure of the base field is outer simple.

**153. Orthogonal systems of idempotents.** Let \( J \) be a para-quadratic algebra over \( k \). A finite family \( (c_1, \ldots, c_r) \) of elements in \( J \) is called an **orthogonal system of idempotents** if each \( c_i, 1 \leq i \leq r \), is an idempotent, and the following relations hold, for all \( i, j, l = 1, \ldots, r \).

\[
U_{c_i}c_j = \{c_i c_j c_j\} = c_i \circ c_j = 0 \quad (i \neq j), \quad \{c_i c_j c_l\} = 0 \quad (i, j, l \text{ mutually distinct}). \tag{3}
\]

An orthogonal system \( (c_1, \ldots, c_r) \) of idempotents in \( J \) is said to be **complete** if \( \sum_{i=1}^r c_i = 1_J \). Prove:

(a) If \( (c_1, \ldots, c_r) \) is an orthogonal system of idempotents in \( J \), then \( \sum_{i=1}^r c_i \) is an idempotent, and

\[
(c_1, \ldots, c_r, 1_J - \sum_{i=1}^r c_i)
\]

is a complete orthogonal system of idempotents in \( J \).

(b) If \( J = A^{(a)} \) for some unital flexible \( k \)-algebra \( A \), then the (complete) orthogonal systems of idempotents in \( J \) and in \( A \) are the same.

### 31. Jordan algebras and basic identities.

As experimental studies carried out by Jacobson in the nineteen-fifties suggest, the most promising way of extending the theory of linear Jordan algebras to arbitrary commutative rings from those containing \( \frac{1}{2} \) consists in axiomatizing properties of the \( U \)-operator. The fruitfulness of this approach is underscored by the fact that the explicit formulas for the \( U \)-operator in our examples of linear Jordan algebras (Exc. 24 (b), 29.10.1 [29.10.2]), as opposed to the ones for the bilinear product (5.3.1), 29.2 [29.8], are defined over the integers and hence make sense over any commutative ring. Unfortunately, however, the question of which specific properties of the \( U \)-operator should be singled out as axioms remained a mystery for a long
time. But then, in 1966, McCrimmon [75] introduced the concept of what he called a \textit{quadratic Jordan algebra}. He showed that this concept is equivalent to the concept of a unital linear Jordan algebra over rings containing $\frac{1}{2}$ and that it gives rise to a far reaching structure theory, culminating eventually in the Zel’manov-McCrimmon enumeration [84] of non-degenerate prime quadratic Jordan algebras.

Our aim in the present section will be to define quadratic Jordan algebras (henceforth referred to simply as \textit{Jordan algebras}) and to show that in the presence of $\frac{1}{2}$ they are categorically isomorphic to unital linear Jordan algebras. Using some basic identities, we derive a few elementary properties of Jordan algebras and extend the standard examples previously obtained in the linear case to the more general quadratic setting.

Throughout we let $k$ be an arbitrary commutative ring. In deriving the elementary properties of Jordan algebras required in the present volume, we mostly follow Jacobson [45].

31.1. The concept of a Jordan algebra. By a \textit{Jordan algebra} over $k$ we mean a para-quadratic $k$-algebra $J$ with $U$-operator $U$ and base point $1_J$ satisfying the following identities in all scalar extensions.

\begin{align}
U_{Uxy} &= U_{Ux}U_y, \\
U_xV_{yx} &= V_{yx}U_x.
\end{align}

Equation (1) is called the \textit{fundamental formula}. We write $k\text{-jord}$ for the category of Jordan algebras over $k$, viewed as a full subcategory of $k\text{-paquad}$, the category of para-quadratic algebras over $k$. By definition, Jordan algebras remain stable under base change.

Let $J$ be a Jordan algebra over $k$. The triple (resp. circle) product associated with $J$ in its capacity as a para-quadratic algebra will be referred to as the \textit{Jordan triple product} (resp. the \textit{Jordan circle product}) of $J$. Setting $x = 1_J$ in (2) and observing (30.1.2), (30.1.6), we conclude $V_{1_J,x} = V_x$, hence $\{1_Jxy\} = \{x1_Jy\} = x \circ y$ for all $x, y \in J$. Thus \textit{Jordan algebras are unital para-quadratic algebras.}

Before we can proceed, we require a rather obvious but still useful observation.

31.2. Unimodular free base change. Let $R \in k\text{-alg}$ and assume that $1_R$ can be extended to basis $(t_i)_{i \in I}$ of $R$ as a $k$-module. Since tensor products commute with direct sums, the natural map $M \rightarrow M_R$, for any $k$-module $M$, is an embedding, and identifying $M \subseteq M_R$ canonically, we conclude

\begin{equation}
M_R = \bigoplus_{i \in I} (t_i M)
\end{equation}

as a direct sum of $k$-modules. Moreover, any linear map $f: M \rightarrow N$ between $k$-modules $M, N$ may be recovered from its $R$-linear extension $f_R: M_R \rightarrow N_R$ via restriction, and it follows that the assignment $f \mapsto f_R$ defines an injection from $\text{Hom}_k(M, N)$ to $\text{Hom}_R(M_R, N_R)$. We identify $\text{Hom}_k(M, N) \subseteq \text{Hom}_R(M_R, N_R)$ accord-
ingly and claim that the $R$-linear map
\[ \bigoplus_{i \in I} (t_i \text{Hom}_k(M, N)) = \text{Hom}_k(M, N)_R \rightarrow \text{Hom}_R(M_R, N_R) \]

extending the inclusion $\text{Hom}_k(M, N) \hookrightarrow \text{Hom}_R(M_R, N_R)$ is injective. Indeed, given a family $(f_i)$ of elements in $\text{Hom}_k(M, N)$ with finite support, the map in question, thanks to the preceding identifications, sends $\sum t_i f_i = \sum (f_i \otimes t_i)$ to $\sum t_i f_i R = \sum t_i f_i$, and if this is zero, then so is $\sum t_i f_i(x)$ for all $x \in M$, which by (1) implies $f_i = 0$ for all $i$ and proves the assertion. Summing up we have shown that after the appropriate identifications, the following inclusions hold:

\[ \text{Hom}_k(M, N) \subseteq \text{Hom}_k(M, N)_R = \bigoplus_{i \in I} (t_i \text{Hom}_k(M, N)) \subseteq \text{Hom}_R(M_R, N_R). \quad (2) \]

Moreover, the elements of $\text{Hom}_k(M, N)_R$ act on $M_R$ according to the rule
\[ (t_i f)(t_j x) = t_i t_j f(x) \quad \text{for all } f \in \text{Hom}_k(M, N), \; i, j \in I, \; x \in M \quad (3) \]

since $(t_i f)(t_j x) = (t_i f_R)(x \otimes t_j) = t_i f_R(x \otimes t_j) = t_i (f(x) \otimes t_j) = f(x) \otimes (t_i t_j) = t_i t_j f(x)$.

**31.3. Basic identities.** Let $J$ be a Jordan algebra over $k$. The following identities hold strictly in $J$, i.e., for all $x, y, z, w$ in every scalar extension.
identities for all
Since Jordan algebras are stable under base change, it suffices to verify these
31 Jordan algebras and basic identities. 221

\[ U_{1} = 1, \quad (1) \]
\[ U_{0} = U_{1} U_{1}, \quad (2) \]
\[ U_{1} U_{2} U_{3} = U_{1} U_{2} U_{1}, \quad (3) \]
\[ U_{2} U_{3} V_{4} = U_{2} U_{3} V_{4}, \quad (4) \]
\[ V_{2} = V_{2}, \quad (5) \]
\[ U_{2} U_{1} U_{3} = U_{2} U_{1} U_{3}, \quad (6) \]
\[ U_{2} U_{1} U_{2} U_{3} + U_{2} U_{1} U_{2} U_{1}, \quad (7) \]
\[ U_{2} U_{1} U_{3} + U_{1} U_{2} U_{3} U_{4} + U_{2} U_{1} U_{2} U_{1}, \quad (8) \]
\[ U_{2} U_{1} U_{2} U_{3} = U_{2} U_{1} U_{2} U_{1}, \quad (9) \]
\[ 2U_{1} = U_{2} - U_{2}, \quad (10) \]
\[ U_{1} V_{2} = V_{2} U_{1}, \quad (11) \]
\[ V_{1} V_{2} + V_{2} V_{1} = V_{2} V_{1} + V_{2} V_{1}, \quad (12) \]
\[ U_{1} x z = \{ x y \} = x^2 \circ y, \quad (13) \]
\[ U_{1} x = x, \quad (14) \]
\[ U_{1} x y + U_{1} y x = U_{1} x y + U_{1} y x + V_{1} x y V_{1} x, \quad (15) \]
\[ U_{1} x y + U_{1} y x = U_{1} x y + U_{1} y x + V_{1} x y V_{1} x, \quad (16) \]
\[ x y) \circ y = x \circ (U x y), \quad (17) \]
\[ V_{1} x y x y + U_{1} y = V_{1} x y x y + U_{1} y, \quad (18) \]
\[ V_{1} y x y = V_{1} x y x y + U_{1} y, \quad (19) \]
\[ V_{1} x y + U_{1} y x = V_{1} x y + U_{1} y x, \quad (20) \]
\[ V_{1} x y x + U_{1} y x = V_{1} x y x + U_{1} y x, \quad (21) \]
\[ U_{1} x y x + U_{1} y x = U_{1} x y x + U_{1} y x, \quad (22) \]
\[ x y) \circ y = x \circ (U x y), \quad (23) \]
\[ V_{1} x y + U_{1} y x = V_{1} x y + U_{1} y x, \quad (24) \]
\[ V_{1} x y x + U_{1} y x = V_{1} x y x + U_{1} y x, \quad (25) \]
\[ V_{1} x y x + U_{1} y x = V_{1} x y x + U_{1} y x, \quad (26) \]
\[ V_{1} x y + U_{1} y x = V_{1} x y + U_{1} y x, \quad (27) \]
\[ [V_{1} x y, V_{1} x] = V_{1} x y, \quad (28) \]
\[ V_{1} x y x = U_{1} y x, \quad (29) \]
\[ V_{1} x y x = U_{1} y x, \quad (30) \]
\[ U_{1} x y + U_{1} y x = U_{1} x y + U_{1} y x, \quad (31) \]
\[ U_{1} x y + U_{1} y x = U_{1} x y + U_{1} y x, \quad (32) \]

\textbf{Proof.} Since Jordan algebras are stable under base change, it suffices to verify these identities for all \(x, y, z, u, v, w \in J\). Here \((1), (5)\) hold since \(J\) is unital para-quadratic,
while (2) and the first equation in (4) are valid by the definition of a Jordan algebra. Applying this part of (4) to \( z \), viewing the result as a linear map acting on \( y \), using the fact that the Jordan triple product is symmetric in the outer variables and writing again \( y \) for \( z \), the second equation of (4) drops out. On the other hand, (3) follows immediately by linearizing (2) with respect to \( y \). Passing to the polynomial ring \( k[t] \), which is free as a \( k \)-module with basis \( \langle t^i \rangle_{i \in \mathbb{N}} \), we may apply [31,2] to obtain natural identifications

\[
J \subseteq J_{k[t]} = \bigoplus_{i \in \mathbb{N}} \langle t^i \rangle, \quad \text{End}_k(J) \subseteq \text{End}_k(J_{k[t]}) = \bigoplus_{i \in \mathbb{N}} \{ t_i \text{End}_k(J) \} \subseteq \text{End}_k(J_R)
\]

as direct sums of \( k \)-modules. Replacing \( x \) by \( x + tz \), \( x, z \in J \), in (2) and comparing coefficients of \( t, t^2 \), respectively, we conclude that (6), (7) hold. Similarly, replacing \( x \) by \( x + tw \), \( x, w \in J \), in (6) (resp. by \( x + tz \), \( x, z \in J \), in (4)) yields (8) (resp. (9)). Specializing \( y \) and \( z \) to \( 1_J \) in (7), we obtain \( V_2z = 4U_x = 2U_x + V_2^2 \), hence (10). On the other hand, since Jordan algebras are unital para-quadratic, setting \( y = 1_J \) in (4) yields (11). Next we put \( z = 1_J \) in (9) and observe (5). Writing \( x \) for \( z \), we end up with (12), which, when applied to \( z \), amounts to

\[
x \circ (y \circ z) + \{xyz\} = y \circ (x \circ z) + \{xyz\}.
\]

Putting \( z = x \) and applying (10), we conclude

\[
x \circ (x \circ y) + U_x x = 2x^2 \circ y + 2U_x y = 2x^2 \circ y + x \circ (x \circ y) - x^2 \circ y.
\]

Thus (13) holds, which linearizes to \( \{ xyz \} + \{ xyy \} = (x \circ z) \circ y \) and yields (14) after interchanging \( x \) and \( y \). Next we put \( z = 1_J \) in (7) to obtain (15), while linearizing (11) yields (16). Applying this to \( y \) and using (13), we conclude

\[
2U_x y^2 + \{ x(x \circ y) y \} = x \circ \{ xyy \} + y \circ (U_x y) = x \circ (x \circ y^2) + y \circ (U_x y) = V_2^2 y^2 + y \circ (U_x y).
\]

Now (10) yields with

\[
y \circ (U_x y) = \{ x(x \circ y) y \} + (2U_x - V_2^2) y^2 = \{ x(x \circ y) y \} - V_2^2 y = \{ x(x \circ y) y \} - x^2 \circ y^2
\]

an equation whose right-hand side is symmetric in \( x \) and \( y \). Hence so is the left, and we have proved (17). Linearizing gives

\[
y \circ (U_x z) + z \circ (U_x y) = x \circ (U_{y,x} x) = x \circ (U_{y,z}) = V_2(U_{y,z}),
\]

and viewing this as a linear map in \( z \), we arrive at

\[
V_{U_x y} = V_x V_{y,x} - V_x U_x.
\]
This proves (20), which linearizes to (21). Applying this to \( w \) hence (27). Linearizing (26) at \( z \) obtain \( w \) and (29) is proved. Applying the left-hand side of (29) to \( w \) when viewed as a linear map in \( z \) and, viewing \( z \) for \( w \), yields the first equation of (22), while the second now follows from (9). We now apply (9) to \( u \) and obtain

\[
\{ (U_{xy})zw \} + \{ (U_{xz})yw \} = \{ xyxz \} w,
\]

which in turn may be viewed as a linear map in \( z \) and, writing \( z \) for \( w \), yields the first equation of (22), while the second now follows from (9). We now apply (9) to \( u \) and obtain

\[
\{ x \{ yu \} u \} + U_{x} \{ yz \} u = \{ zy \{ u \} u \} + \{ x \{ xu \} u \} = \{ zy \{ u \} u \} + \{ x \{ xu \} u \}.
\]

Viewing this as a linear map in \( z \) and replacing \( u \) by \( z \), we arrive at (23). Next we apply (20) to \( z \) and linearize the resulting equation, \( \{ (U_{xy})yz \} = \{ x \{ U_{xy} \} z \} \), with respect to \( x \):

\[
\{ x \{ yw \} yz \} = \{ w \{ U_{xy} \} z \} + \{ x \{ U_{yz} \} w \}.
\]

Viewing (34) as a linear map in \( z \) and replacing \( w \) by \( z \) gives (24), while viewing it as a linear map in \( w \) and interchanging \( x \) with \( z \) gives (25). Applying first (22) and then (9), we obtain, after interchanging \( x \) with \( z \),

\[
V_{x,y}U_{z} + U_{z}V_{y,x} = U_{x}V_{y,z} - U_{x,y,z} + U_{z}V_{y,x} = U_{x,\{ yz \}},
\]

hence (26). Combining (23) with (21) yields

\[
V_{x,y}V_{z} + V_{U_{y},z} = V_{x,\{ yz \}} + U_{y}V_{z} = V_{U_{y,z}} + V_{U_{y},z} + U_{y}U_{y,z},
\]

hence (27). Linearizing (26) at \( z \) in the direction \( u \) and applying the result to \( v \), we obtain

\[
\{ xy \{ uv \} z \} + \{ u \{ xy \} v \} = \{ uv \{ xy \} z \} + \{ xy \{ uv \} v \},
\]

which, when viewed as a linear map in \( z \), amounts to (28). Letting the left-hand side of (29) act on \( w \) and observing (6), we conclude

\[
V_{U_{y},z}U_{y}w = U_{U_{y},z}U_{y}wz = U_{y}U_{y}U_{y}z = U_{y}V_{y,s}w,
\]

and (29) is proved. Applying the left-hand side of (29) to \( w \) and observing (6) implies

\[
V_{U_{y},z}V_{x,y}w = U_{U_{y},x}\{ yz \} z = U_{y}U_{y}U_{y}wz + U_{y}U_{y}U_{y}z = (U_{y}U_{y}V_{y,z} + V_{y,s}U_{y})w.
\]
hence (30). Consulting (22), (27) and (22) again, we now compute

\[ V_{x,y}U_{z,x} = U_{x,z}V_{x,y} - U_{U_{x,y},x} = U_{x,z}V_{U_{x,y},x} + U_{x,z}U_{y}U_{x,z} - U_{U_{x,y},x} \]

which by (20) implies

\[ V_{x,y}U_{z,x} = U_{x,z}U_{y} + U_{U_{x,y},z} - U_{U_{y},U_{x}}, \]

during which combines with (7) to yield

\[ U_{V_{x,y},z} + U_{U_{x,y},U_{z}} = U_{V_{x,y},z} + U_{U_{x,y},U_{z}} - U_{U_{x,y},U_{z}} = U_{U_{x,y},U_{z}} + U_{U_{x,y},U_{z}} + V_{x,y}U_{z}, \]

and this is (31). Finally, in order to derive (32), we linearize (6) with respect to \( y \) and obtain

\[ U_{U_{x,y},U_{z}} + U_{U_{x,y},U_{z}} = U_{x,y}U_{z} + U_{x,z}U_{y}U_{z}. \]

Here we replace \( u \) by \( U_{z} \). Then a computation involving (4), (20), (22) and (6) (with \( U_{y} \) in place of \( z \)) yields

\[ U_{U_{x,y},U_{z}} = U_{x,y}U_{z} + U_{x,z}U_{y}U_{z} - U_{U_{x,y},U_{z}} \]

which completes the proof of (32).

31.4. The connection with unital linear Jordan algebras. Assume that 2 is invertible in \( k \). Let \( J \) be a unital linear Jordan algebra over \( k \). Then its identity element and the \( U \)-operator (29.9) convert \( J \) into a para-quadratic algebra \( J^{\text{quad}} \), which by the advanced identities (29.11), (29.11), (29.11) combined with the usual scalar extension argument (cf. Prop. 29.4) is a Jordan algebra.

Conversely, let \( J \) be a Jordan algebra over \( k \) Then the bilinear multiplication

\[ xy := \frac{1}{2} U_{x,y}1_{J} = \frac{1}{2} \{ x1_{J}y \} = \frac{1}{2} V_{x,y} \]

gives \( J \) the structure of a non-associative \( k \)-algebra \( J^{\text{lin}} \) with left multiplication \( L_{x} = \frac{1}{2} V_{x} \) for \( x \in J \). By definition and (31.3), \( J^{\text{lin}} \) is commutative with identity element \( 1_{J} \), and its squaring agrees with the one of \( J \). By (31.3), the linear operators \( V_{x}, U_{x} \) commute, hence by (31.3) so do \( V_{x} \) and \( U_{x} \). This shows \( [L_{x}, L_{z}] = 0 \), and from (29.11) we conclude that \( J^{\text{lin}} \) is a unital linear Jordan algebra. One checks easily that the two constructions \( J \mapsto J^{\text{quad}} \) and \( J \mapsto J^{\text{lin}} \) are inverse
to each other, and that a linear map between unital linear Jordan algebras is a homomorphism of unital linear Jordan algebras if and only if it is one of Jordan algebras. Summing up, we have thus proved the following result.

**31.5. Theorem.** Assume that 2 is invertible in \( k \). Then the constructions presented in 31.4 yield inverse isomorphisms between the categories of unital linear Jordan algebras over \( k \) and Jordan algebras over \( k \). □

**31.6. Convention.** Assume that 2 is invertible in \( k \). If there is no danger of confusion, we will always use Thm. 31.5 to identify Jordan algebras over \( k \) in the sense of 31.1 with unital linear Jordan algebras over \( k \) in the sense of 29.1; accordingly, the terms “unital linear Jordan algebra over \( k \)” and “Jordan algebra over \( k \)” will be used interchangeably. Note that under the preceding identification, the advanced identities valid in linear Jordan algebras translate equivalently to appropriate identities in the long list of formulas derived in 31.3.

The reader may wonder why, in defining Jordan algebras over arbitrary base rings, we have insisted on an identity element. The reason is that, without this restriction, the algebraic structure which ensues becomes computationally much more difficult to deal with. We refer to McCrimmon [80] for details.

**31.7. Examples: associative algebras.** Let \( A \) be a unital associative \( k \)-algebra. We claim that the para-quadratic algebra \( A^{(+)} \) of 30.4 with base point \( 1_{A^{(+)}} = 1_A \) and \( U \)-operator

\[
U_{x,y} = x y x
\]

is in fact a Jordan algebra. Indeed, since associativity is preserved by scalar extensions, it suffices to verify (31.1.1) and (31.1.2) over the base ring, so let \( x, y, z \in A \). Then

\[
U_{U_x,y}z = (x y x)z(x y x) = x(\tau(x) y)z = U_x U_y U_z ,
\]

\[
U_x V_{x,z} = x(y z x + z y x) = x y (x z x) + (x z x) y = V_{x,y} U_z z ,
\]

as desired. Recall from (30.4.2) that the Jordan triple and circle products of \( A^{(+)} \) are respectively given by

\[
\{x y z\} = x y z + y z x, \quad x \circ y = x y + y x
\]

for all \( x, y \in A \). Recall further that, if 2 \( \in k \) is invertible, the identifications of 31.6 show \( A^{(+)} = A^+ \) as unital linear Jordan algebras over \( k \).

**31.8. Examples: associative algebras with involution.** Let \( (B, \tau) \) be an associative algebra with involution over \( k \). By definition, \( B \) is unital and

\[
H(B, \tau) = \{ x \in B \mid \tau(x) = x \}
\]
obviously is a subalgebra of $B^+$ and hence is a Jordan algebra (Exc. 154).

In particular, if $(B, \tau) = (A^\circ \oplus A, \epsilon_A)$ as in [11.4] with $\epsilon_A$ the exchange involution, then the diagonal embedding $A \to A \oplus A$ determines an isomorphism

$$A^+ \xrightarrow{\sim} H(A^\circ \oplus A, \epsilon_A), \quad x \mapsto x \oplus x,$$

of Jordan algebras.

31.9. Special and exceptional Jordan algebras. A Jordan algebra over $k$ is said to be special if it is isomorphic to a subalgebra of $A^{(+)}$, for some unital associative $k$-algebra $A$. Otherwise, it is said to be exceptional. If $2 \in k$ is invertible, one checks easily that these notions are equivalent to the ones defined in 29.2 (a).

31.10. Examples: alternative algebras. Let $A$ be a unital alternative $k$-algebra. Then the left Moufang identity (14.3.1) implies that the left multiplication of $A$,

$$L: A^{(+)} \to \text{End}_k(A^{(+)}), \quad x \mapsto L_x,$$

is a homomorphism of para-quadratic algebras and obviously injective. Hence $A^{(+)}$ is a special Jordan algebra. Recall that we have encountered the $U$-operator of $A^{(+)}$ already in 14.5, where it was referred to as the $U$-operator of $A$.

Now let $(B, \tau, p)$ be an alternative algebra with isotopy involution of type $\epsilon = \pm$ over $k$. Then Lemma [17.1] shows that

$$\text{Sym}(B, \tau, p) = \{ x \in B \mid \tau(x) = x \}$$

is a subalgebra of $B^{(+)}$, hence a special Jordan algebra.

31.11. Examples: pointed quadratic modules. Let $(M, q, e)$ be a pointed quadratic module over $k$ and write $x \mapsto \bar{x}$ for its conjugation. Then we claim that that the base point $e$ and the quadratic map $x \mapsto U_x$ from $M$ to $\text{End}_k(M)$ given by

$$U_{x,y} := q(x, \bar{y})x - q(x)\bar{y} \quad (x, y \in M)$$

(1)

give $M$ the structure of a Jordan algebra over $k$, denoted by $J := J(M, q, e)$ and called the Jordan algebra of $(M, q, e)$. Indeed, writing $t$ for the trace of $(M, q, e)$, we obtain $U_{x,y} = t(\bar{y})e - \bar{y} = t(y)e - t(y)e - y$ for all $y \in M$, hence $U_e = 1_M$. Thus $J$ is a para-quadratic $k$-algebra. In order to show that this para-quadratic algebra is, in fact, a Jordan algebra, we first note that the construction of $J$ out of $(M, q, e)$ is compatible with base change, so it suffices to verify (31.1.1) and (31.1.2) over $k$. First of all, (1) implies

$$V_{x,y,z} = \{xyz \} = q(x, \bar{y})z + q(z, \bar{y})x - q(x, z)\bar{y}$$

(2)

and a straightforward verification shows
Thus (31.1.1), (31.1.2) hold in \( J \) and the proof is complete.


Letting \((M, q, e)\) be a pointed quadratic module over \( k \), we write \( t \) for its trace, \( x \mapsto x^\ast \) for its conjugation and \( J := J(M, q, e) \) for the corresponding Jordan algebra. The following identities, valid for all \( x, y, z \in J \) and all \( n \in \mathbb{N} \), are either easily verified or have been checked before, and are collected here for convenience.
5 Jordan algebras

\[ t(x) = q(1_J, x), \quad q(1_J) = 1, \quad t(1_J) = 2, \]
\[ x = t(x)1_J - x, \quad \bar{1}_J = 1_J, \quad \bar{x} = x, \]
\[ U_x y = q(x, y)x - q(x)y, \]
\[ x^2 = t(x)x - q(x)1_J, \]
\[ x^3 = t(x)x^2 - q(x)x, \]
\[ V_{x, y} = \{xyz\} = q(x, y)z + q(y, z)x - q(z, x)y, \]
\[ x \circ y = t(x)y + t(y)x - q(x, y)1_J, \]
\[ U_x \bar{x} = q(x)x, \quad U_x \bar{x}^2 = q(x)^2 1_J, \quad x + \bar{x} = t(x)1_J, \]
\[ q(\bar{x}) = q(x), \quad t(\bar{x}) = t(x), \]
\[ q(U_x y) = q(x)^2 q(y), \quad q(x^n) = q(x)^n, \]
\[ t(x^2) = t(x)^2 - 2q(x), \]
\[ t(x \circ y) = 2(t(x)t(y) - q(x, y)), \]
\[ q(x, \bar{y}) = t(x)t(y) - q(x, y), \]
\[ U_x \bar{y} = U_{\bar{y}}. \]

Note the analogy of these formulas with the ones of \[19.5\].

The Jordan algebras of pointed quadratic modules are often referred to collectively as Jordan algebras of Clifford type.

31.13. Quadratic \( \mathbb{Z} \)-structures as Jordan algebras. Let \( \mathbb{D} \) be one of the subalgebras \( \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O} \) of the Graves-Cayley octonions. We have seen in Thm. 5.10 that \( J := \text{Her}_3(\mathbb{D}) \) is a unital linear Jordan algebra over \( \mathbb{R} \) and hence may be viewed canonically as a real Jordan algebra by means of the identification \[31.6\]. Now suppose \( \Lambda \subseteq J \) is a quadratic \( \mathbb{Z} \)-structure of \( J \). By its very definition (cf. 6.3), \( \Lambda \) is a \( \mathbb{Z} \)-subalgebra of \( J \) as a (quadratic) Jordan algebra. Hence \( \Lambda \) is a quadratic Jordan algebra over \( \mathbb{Z} \) in its own right but, in general, not a linear one. For example, if \( M \) is a \( \mathbb{Z} \)-structure of \( \mathbb{D} \) in the sense of \[3.6\](d), then \( \Lambda := \text{Her}_3(M) \) by \[6.3\] is not closed under the bilinear Jordan product of \( J \).

31.14. Towards power-associativity. We wish to show in analogy to Cor. 29.6 that Jordan algebras are power-associative. Combining the fundamental formula \[31.3\](2) and its linearization \[31.3\](3) with the recursive definition of powers in \[30.8\](1), we see by induction that any Jordan algebra \( J \) over \( k \) satisfies the identities

\[ U_x^n = U_x^n, \quad U_x U_x^{m,n} U_x = U_x^{m+2,n+2} \]

for all \( x \in J \) and all \( m, n \in \mathbb{N} \).

31.15. Proposition. Jordan algebras are power-associative: for all Jordan algebras \( J \) over \( k \), all \( x \in J \) and all \( m, n, p \in \mathbb{N} \) we have
\[ U_{nm} x^n = \chi^{m+n}, \]
\[ \{x^m x^n x^p\} = 2\chi^{m+n+p}. \]

**In particular, \( k[x] \subseteq J \) is a Jordan subalgebra.**

**Proof.** Equation (1) follows immediately from (31.14) by induction on \( m \). Equation (2) will now be proved by induction on \( l := m+n+p \). We first note that (2) follows from (1) for \( m = p \) and is symmetric in \( m, p \). Hence we may always assume if necessary that \( m < p \). Moreover, (2) is obvious if two of the exponents \( m, n, p \) are zero. Summing up, not only the induction beginning \( l = 0 \) is trivial, but also the cases \( l = 1, 2 \) are. Let us now assume \( l \geq 3 \) and that (2) holds for all exponents \( m', n', p' \in \mathbb{N} \) having \( m' + n' + p' < l \). We consider the following cases.

**Case 1.** \( m = 0 \). Then (2) amounts to \( x^n x^p = 2\chi^{n+p} \), hence is symmetric in \( n, p \) and obvious for \( n = 0 \) or \( n = p \). Thus we may assume \( 1 \leq n < p \). But the assertion can also be written in the form \( \{x^n x^p\} = 2\chi^{n+p} \), so we have reduced Case 1 to

**Case 2.** \( m \geq 1 \).

**Case 2.1.** \( m = 1 \). Then \( p \geq 2 \), and (30.8), (31.3) combine with the induction hypothesis to imply
\[ \{x^n x^p\} = V_{n+1,1} U_{n+1,2} x^{n+1} x^p = U_x V_{n,2} x^{n+1} = U_x \{x^{n+1} x^p\} = 2U_x x^n x^p, \]
as claimed.

**Case 2.2.** \( m \geq 2 \). Then \( p \geq m \geq 2 \) and the induction hypothesis combined with (31.14) yields
\[ \{x^m x^n x^p\} = U_x U_{m-2,1} U_{n,2} x^{m-1} x^n = U_x U_{m-2,1} U_{n,2} x^{m-2} x^n = U_x \{x^{m-1} x^n x^p\} = 2U_x x^{m+n+p-2} = 2\chi^{m+n+p}, \]
which completes the induction. \( \square \)

**Exercises.**

**154.** Show for a para-quadratic algebra \( J \) over \( k \) that the following conditions are equivalent.

(i) \( J \) is a Jordan algebra.
(ii) The identities
\[ U_{ij} = U_i U_j, \]
\[ U_{ij} V_{kl} = V_{kl} U_{ij}, \]
\[ U_{ij} U_{kl} = U_{ij} U_{kl} + U_{ij} U_{kl} + U_{ij} U_{kl}, \]
\[ U_{ij} U_{kl} + U_{ij} U_{kl} = U_{ij} U_{kl} + U_{ij} U_{kl} + U_{ij} U_{kl} + U_{ij} U_{kl} + U_{ij} U_{kl}, \]
hold in \( J \).
(iii) The identities (3), (4) hold in \( J_{k[\chi]} \).
Conclude that subalgebras and homomorphic images of Jordan algebras (in the category $k$-\textit{paquad}) are Jordan algebras.

**pr.OUTIJO** 155. Let $J$ be a Jordan algebra over $k$. Show that

(a) a $k$-submodule $I \subseteq J$ is an outer ideal (resp. an ideal) if and only if $U_I J \subseteq I$ (resp. $U_I J + U_J I \subseteq I$),

(b) an element $c \in J$ is an idempotent if and only if $c^2 = c$,

(c) the extreme radical of $J$ is an ideal. Conclude that the centroid of a simple Jordan algebra is a field.

**pr.CENCENT** 156. Assume $\frac{1}{2} \in k$ and let $J$ be a unital linear Jordan algebra over $k$. Show that the centroid of $J^{\text{quad}}$ is a unital commutative associative subalgebra of $\text{End}_k(J)$ and that the left multiplication of $J$ induces an isomorphism $\text{Cent}(J) \cong \text{Cent}(J^{\text{quad}})$.

**pr.CHAJOCLI** 157. Let $J$ be a Jordan algebra over $k$ and $q$: $J \to k$ a quadratic form with $q(1) = 1$, so that $(M, q, e)$ is a pointed quadratic module over $k$, where $M$ stands for the $k$-module underlying $J$ and $e = 1$.

Write $t$ for the trace of $(M, q, e)$ and prove that $J = J(M, q, e)$ if and only if the equations

$$x^2 - t(x)x + q(x)e = 0 = x^3 - t(x)x^2 + q(x)x$$

(9) hold strictly in $J$.

**pr.NIPOQUA** 158. Let $(M, q, e)$ be a pointed quadratic module over $k$ and $J = J(M, q, e)$ the corresponding Jordan algebra. Write $t$ for the trace of $(M, q, e)$ and show that an element $x \in J$ is nilpotent if and only if $t(x)$ and $q(x)$ are nilpotent elements of $k$. Conclude that $\text{Nil}(J) = \{x \in M \mid q(x), q(x,y) \in \text{Nil}(k) \text{ for all } y \in M\}$.

**pr.EVPOQUA** 159. (a) Suppose $2 = 0$ in $k$ and consider the situation of Exc. [149] (b) for $n = 2$. Decide whether there exists a pointed quadratic module $(M, q, e)$ over $k$ such that $J(M, q, e) \cong J_2 = k[t_1^{(1)}]/(I_2$).

(b) Show that, over an appropriate commutative ring, there exists a pointed quadratic module whose corresponding Jordan algebra contains an element $t$ satisfying $t^2 = 0 \neq x^3$.

**pr.IDPOQUA** 160. Let $(M, q, e)$ be a pointed quadratic module over $k$ and $J = J(M, q, e)$. Write $t$ for the trace of $(M, q, e)$ and show that, if $k \neq \{0\}$ is connected, then $c \in J$ is an idempotent $\neq 0$, $1$ in $J$ if and only if $t(c) = 1$ and $q(c) = 0$. Conclude that, for any commutative ring $k$ and any element $c \in J$, the following conditions are equivalent.

(i) $c$ is an idempotent satisfying $c_R \neq 0, 1_J$ for all $R \in k$-\textit{alg}, $R \neq \{0\}$.

(ii) $c$ is an idempotent satisfying $c_p \neq 0, 1_J$ for all prime ideals $p \subseteq k$.

(iii) $q(c) = 0$, $t(c) = 1$.

(iv) $c$ is an idempotent and the elements $c, 1_J - c$ are unimodular.

If these conditions are fulfilled, we call $c$ an \textit{elementary} idempotent of $J$.

**pr.DECPOQUA** 161. Let $(M, q, e)$ be a pointed quadratic module over $k$ and $J := J(M, q, e)$. Write $t$ for the trace of $(M, q, e)$ and prove for $c \in J$ that the following conditions are equivalent.

(i) $c$ is an idempotent in $J$.

(ii) There exists a complete orthogonal system $(e^{(0)}, e^{(1)}, e^{(2)})$ of idempotents in $k$, giving rise to decompositions

$$k = k^{(0)} \oplus k^{(1)} \oplus k^{(2)}$$

as direct sums of ideals, where $k^{(0)} = ke^{(0)}$ and $J^{(i)} = e^{(i)}J = Jk^{(i)}$ as the Jordan algebra corresponding to the pointed quadratic form $(M, q, e)_{(i)}$ for $t = 0, 1, 2$, such that

$$c = 0 \oplus e^{(1)} \oplus 1_{J^{(2)}}$$

where $e^{(1)}$ is an elementary idempotent of $J^{(1)}$. 
In this case, the idempotents $\varepsilon^{(i)}$, $i = 0, 1, 2$, in (ii) are unique and given by

$$
\varepsilon^{(0)} := (1 - q(c))(1 - t(c)), \quad \varepsilon^{(1)} := (1 - q(c))t(c), \quad \varepsilon^{(2)} := q(c). \quad (10)
$$

162. Let $C$ be a flexible conic algebra over $k$. Show that the para-quadratic algebra $C^{(+)}$ agrees with the Jordan algebra of the pointed quadratic module $(C, n_C, 1_C)$ if and only if $C$ is alternative.

163. Let $k$-poqa$_{\text{ inj}}$ be the category of pointed quadratic modules over $k$ whose underlying $k$-modules are projective, with injective homomorphisms of pointed quadratic modules as morphisms, and similarly, let $k$-jord$_{\text{ inj}}$ the category of Jordan algebras over $k$, with injective homomorphisms of para-quadratic algebras as morphisms. Prove that the assignment

$$(\phi : (M, q, e) \rightarrow (M', q', e')) \rightarrow (\phi : J(M, q, e) \rightarrow J(M', q', e'))$$

defines a faithful and full embedding from $k$-poqa$_{\text{ inj}}$ to $k$-jord$_{\text{ inj}}$.

164. Let $(V, q, e)$ be a non-degenerate pointed quadratic module of dimension 3 over a field $F$ of characteristic not 2. Show that there exist a quaternion algebra $B$ over $F$ and an involution $\tau$ of $B$ such that $J(V, q, e) \cong H(B, \tau)$. Show further that $(B, \tau)$ is uniquely determined by this condition. (Hint. Use Exc. 110.)

32. Power identities.

By showing in Cor. 29.6 that linear Jordan algebras over a commutative ring containing $\frac{1}{2}$ are power-associative, we derived what may be called a local property: every subalgebra on a single generator is associative. The proof of this result has been reduced to yet another property of linear Jordan algebras that, though no longer local, could at least be called semi-local: given any element $x$ in a linear Jordan algebra $J$, the left multiplication operators of arbitrary elements in $k[x] \subseteq J$ acting on all of $J$ commute by pairs.

The local property of a linear Jordan algebra to be power-associative has been extended to the setting of Jordan algebras in Prop. 31.15. It is the purpose of the present section to accomplish the same objective for the semi-local analogue of this property alluded to above. More specifically, fixing a Jordan algebra $J$ over an arbitrary commutative ring $k$ throughout this section, the main result we wish to establish reads as follows.

32.1. Theorem. Let $x \in J$. Then

$$U_{(fg)}(x) = U_f(x)U_g(x)$$

for all $f, g \in k[t]$.

32.2. Remark. The proof of this result given in Jacobson [45] Cor. 3.3.3] rests on a general principle [45 3.3.1] that may be regarded as a weak version of Macdonald’s theorem [45, Thm. 3.4.15]. The proof we are going to provide below will work instead with explicit and elementary manipulations of some of the basic identities in 31.3 valid in arbitrary Jordan algebras.
32.3. A first reduction. In order to derive Thm. [32.1] we write the polynomials $f, g \in k[t]$ in the form

$$f = \sum_{i \in \mathbb{N}} \alpha_i t^i, \quad g = \sum_{m \in \mathbb{N}} \beta_m t^m,$$

where the families $(\alpha_i)_{i \in \mathbb{N}}, (\beta_m)_{m \in \mathbb{N}} \in k^\mathbb{N}$ both have finite support. With $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$, this implies

$$fg = \sum_{(i, m) \in \mathbb{N}^2} \alpha_i \beta_m t^{i+m},$$

hence

$$(fg)(x) = \sum_{(i, m) \in \mathbb{N}^2} \alpha_i \beta_m x^{i+m},$$

and endowing $\mathbb{N}^2$ with the lexicographic ordering, we apply (31.14.1) to obtain the expansion

$$U(fg)(x) = \sum_{(i, m) \in \mathbb{N}^2} \alpha_i^2 \beta_m^2 U_{x^{i+m}} + \sum_{(i, m), (j, n) \in \mathbb{N}^2, (i, m) < (j, n)} \alpha_i \alpha_j \beta_m \beta_n U_{x^{i+m} x^{j+n}}$$

$$= \sum_{i, m \in \mathbb{N}} \alpha_i^2 \beta_m^2 U_{x^{i+m}} + \sum_{i, j, m, n \in \mathbb{N}, i < j} \alpha_i \alpha_j \beta_m \beta_n U_{x^{i+m} x^{j+n}}$$

$$+ \sum_{i, j, m, n \in \mathbb{N}, i < m < j} \alpha_i \alpha_j \beta_m \beta_n (U_{x^{i+m} x^{j+n}} + U_{x^{i+m} x^{j+n}}).$$

Thus we have

$$U(fg)(x) = \sum_{i, m \in \mathbb{N}} \alpha_i^2 \beta_m^2 U_{x^{i+m}} + \sum_{i, m, n \in \mathbb{N}, m < n} \alpha_i^2 \beta_m \beta_n U_{x^{i+m} x^{j+n}}$$

$$+ \sum_{i, j, m, n \in \mathbb{N}, i < j} \alpha_i \alpha_j \beta_m \beta_n U_{x^{i+m} x^{j+n}} + \sum_{i, j, m, n \in \mathbb{N}, i < m < j} \alpha_i \alpha_j \beta_m \beta_n (U_{x^{i+m} x^{j+n}} + U_{x^{i+m} x^{j+n}}).$$

On the other hand, from

$$f(x) = \sum_{i \in \mathbb{N}} \alpha_i x^i, \quad g(x) = \sum_{m \in \mathbb{N}} \beta_m x^m$$

we deduce
32 Power identities.

\[ U_f(x) U_g(x) = \left( \sum_{i \in \mathbb{N}} \alpha_i^2 U_i^t + \sum_{i,j \in \mathbb{N}, j < i} \alpha_i \alpha_j U_{i,j}^t \right) \left( \sum_{m \in \mathbb{N}} \beta_m^2 U_m^t + \sum_{m,n \in \mathbb{N}, m < n} \beta_m \beta_n U_{m,n}^t \right) \]

\[ = \sum_{i,j \in \mathbb{N}} \alpha_i^2 \beta_j^2 U_{i,j}^t + \sum_{i,j \in \mathbb{N}} \alpha_i \beta_j U_{i,j}^t + \sum_{i,j \in \mathbb{N}} \alpha_i \alpha_j \beta_m \beta_n U_{i,j}^t U_{m,n}^t. \]

Comparing this with (1), we see that Thm. 32.1 will be a consequence of the identities (32.4.5), (32.4.6) below.

32.4. Proposition. For all \( x \in J \) and all \( i, j, m, n \in \mathbb{N} \), the following identities hold.

\[ V_{x+2} = V_x^2 V_{x} - U_x V_{x} - V_x U_{x}, \quad (1) \]
\[ U_{x+2} = U_x (V_x V_{x} - U_x V_{x}), \quad (2) \]
\[ V_{x+1} = V_x V_{x} - U_x V_{x}, \quad (3) \]
\[ U_{x+2} = V_x U_{x+1}, \quad (4) \]
\[ U_{x+1} U_{x+1} = U_{x+1} + U_{x+2}, \quad (5) \]
\[ U_{x+1} U_{x+2} = U_{x+1} + U_{x+2}. \quad (6) \]

The proof of this result will be preceded by the following lemma.

32.5. Lemma. For \( x \in J \), the linear operators \( U_{x}, U_{x+2} \) commute by pairs, and we have

\[ V_{x+2} = V_x V_{x} - U_x V_{x} - V_x U_{x}, \quad (1) \]
\[ U_{x+2} = U_x (V_x V_{x} - U_x V_{x}) \quad (2) \]

for all \( n \in \mathbb{N} \).

Proof. We first apply (31.3.19) to obtain \( V_{x+2} = V_x V_{x} - U_x V_{x} - V_x U_{x} \). Similarly, since \( U_{x+2} = U_x U_{x+1} = U_x V_{x} \), by (31.3.14), another application of (31.3.14) gives (2). It remains to prove

\[ [U_{x}, U_{x+1}] = 0, \quad (3) \]
\[ [U_{x}, U_{x+2}] = 0 \quad (4) \]

for all \( i, j, m, n \in \mathbb{N} \).

We begin with (3), note by symmetry and (31.4.1) that we may assume \( i = 1, m < n \) and argue by induction on \( l := m + n \). For \( l = 0 \), there is nothing to prove. For \( l = 1 \), we have \( m = 0, n = 1 \), and the assertion comes down to \([U_{x}, V_{x}] = 0\), which holds by (31.3.11). Now suppose \( l \geq 2 \) and assume (3) holds for all natural numbers \( m', n' \) in place of \( m, n \) having \( m' + n' < l \). Then we consider the following cases.

(1) \( m = 0, n = l \). Then the assertion comes down to \([U_{x}, V_{x}] = 0\), which follows from (1) for \( n = l - 2 \) and the induction hypothesis since, in particular, \([U_{x}, U_{x,l-2}] = 0\).
20. 0 < m < n. Then l ≥ 3. Here m = 1 implies n = l − 1, and the assertion comes
down to [U_x, U_x, x^{l−1}] = 0, which follows from (2) for n = l − 3 since [U_x, V_{x,l−3}] = 0 = [U_x, U_x, x^{l−3}]
by the induction hypothesis. On the other hand, if n > m ≥ 2, then
(31.3) gives U_{x,x} = U_{x,x}^{m−2} U_{x,x}^{m−2} = U_x U_{x,x}^{m−2} U_{x,x}^{m−2} U_{x,x}, and the assertion follows
from the induction hypothesis. This completes the proof of (3).

Turning to (4), we note that the assertion is symmetric in (i, j) and (m, n) and that,
by (3), we may assume i < j, m < n. Now we argue by induction on l := i + j + m + n.
The cases l = 0, 1 are obvious by what we have just noted, while for l = 2 we may
assume i = m = 0, j = n = 1, in which case the assertion reduces to the triviality
[V_x, V_x] = 0. Now let l ≥ 3 and assume the assertion holds for all natural numbers
i, j, m, n having i + j + m + n < l. Then we consider the following cases.

1. i = m = 0. Then we have to show [V_x, V_x] = 0. For i = j, hence n = l − j ≥ 2,
the assertion follows from (1) for n − 2 in place of n since the induction hypothesis
implies [V_x, U_{x,x}^{n−2}] = 0. On the other hand, if j ≥ 2, the assertion follows again from
(1), this time for n = j − 2, and the induction hypothesis since [U_{x,x}^{j−2}, V_x] = 0.

2. i = m = 1. This implies j ≥ 2, and we have to show [U_{x,x}, U_{x,x}] = 0, which
follows from (2) for n = j − 2 since the induction hypothesis implies [V_{x,x}^{j−2}, U_{x,x}] = 0 = [U_{x,x}^{j−2}, U_{x,x}]. Now, by symmetry, the only remaining case is

3. j > i ≥ 2. Then equation (31.3) yields U_{x,x} = U_{x,x}^{l−2} U_{x,x}^{l−2} U_{x,x},
which commutes with U_{x,x} by (3) and the induction hypothesis. □

32.6. Proof of Proposition 32.4
Combining the first part of Lemma 32.5 with
(32.1), we obtain (32.4), while (32.4) agrees with (32.5).

Next we prove (32.4) for i = 1, m = 0, i.e.,

\[ U_x V_x = U_{x,x}^{m+1}, \tag{1} \]

and (32.4) simultaneously by induction on n. Both equations are obvious for n = 0.
Now suppose n > 0 and assume (32.4) and (1) both hold for all natural numbers
< n. Then (32.4) for n − 1 in place of n and the induction hypothesis for (32.4) imply

\[ U_{x,x}^{m+1} = U_x (V_x V_{x,x}^{n−1} − U_{x,x}^{n−1}) = U_x V_x, \]

hence (1). Combining both parts of the induction hypothesis with (32.4) for n − 1
in place of n, we now obtain

\[ V_x V_x − U_x V_x = V_x^2 V_{x,x}^{n−1} − V_x U_x V_{x,x}^{n−1} = V_{x,x}^{n+1}, \]

hence (32.4). This completes the proof of (32.4) and (1).

We are now in a position to prove (32.4), where (31.14) allows us to assume
i = 1, and first deduce from Lemma 32.5 that it suffices to establish the first one
of the two equations. By symmetry and (31.14) we may assume m < n and then
argue by induction on m. The case m = 0 has been settled in (1). For m > 0, we
apply (31.3) and the induction hypothesis to conclude.
\[ U_{x_{m+1}, x^{n+1}} = U_{U_{x_{m}, x^{n}} U_{x_{m-1}, x^{n-1}} U_{x} = U_{x_{m}, x^{n}} U_{x} = U_{x_{m}, x^{n}}, \]

as claimed.

Turning to (32.4.4), we first deduce from Lemma 32.5 that the linear operators \( V_{x, m}, V_{x, n} \) commute. Hence (31.3.12) implies \( V_{x, m} = V_{x, n} \), so our assertion is symmetric in \( m \) and \( n \). We now argue by induction on \( m \). For \( m = 0 \) there is nothing to prove. For \( m = 1 \), we apply (31.3.14) and (32.4.5) to obtain \( V_{x, 1} = U_{x} V_{x, 1} - U_{x, 1} = V_{x, 1} \), hence the assertion. Now suppose \( m \geq 2 \) and assume the assertion holds for all \( m' \in \mathbb{N} \) in place of \( m \) satisfying \( m' < m \). Combining (31.3.12) with Prop. 31.15 the case \( m = 1 \) and the induction hypothesis, we deduce

\[
V_{x, m} = V_{U_{x, m-2}, x^{n}} - V_{U_{x, m}, x^{m-1}} = 2V_{x, m-1} - V_{x, m+1} = V_{x, m},
\]

and the proof of (32.4.4) is complete.

Finally, turning to (32.4.6), we may assume \( i < j \) and \( m < n \) by symmetry, Lemma 32.5 and (32.4.4). Then we argue by induction on \( l := i + m \). For \( l = 0 \), i.e., \( i = m = 0 \), we have to prove \( V_{x, i} V_{x, j} = V_{x, i+j} + U_{x, i} V_{x, j} \). But \( V_{x, i} V_{x, j} = U_{x, i} V_{x, j} + V_{x, j} \) by (31.3.14), and the assertion follows from (32.4.4). Next suppose \( i + m > 0 \) and assume (32.4.6) for all natural numbers \( i', j', m', n' \) in place of \( i, j, m, n \) satisfying \( i' + m' < l \). Since \( U_{x, i+j} \) and \( U_{x, m} \) commute by Lemma 32.5, we may assume \( i > 0 \). Then (32.4.5) and the induction hypothesis yield

\[
U_{x, i} U_{x, m, n} = U_{x} U_{x_{i-1}, x^{j-1}} U_{x_{i}, x^{m}, n} = U_{x} U_{x_{i+1}, x^{j+1}, n} + U_{x} U_{x_{i+1}, x^{j+1}, n} = U_{x_{i+m}, x^{j+n}} + U_{x_{i+m}, x^{j+n}},
\]

which completes the induction and the proof of Prop. 32.4.

With the proof of Prop. 32.4, we have also established Thm. 32.1. The remainder of this section will be devoted to a useful application. We begin with an auxiliary result, where we use the notation already employed in Exc. 149.

32.7. Proposition. For \( x \in J \) and \( R \in k\text{-algebra} \) such that \( R = k[x] \) as \( k \)-modules, the following conditions are equivalent.

(i) \( R^{(1)} = k[x] \) as Jordan algebras.

(ii) The powers of \( x \) in \( R \) and in \( J \) coincide.

(iii) \( f(x) = 0 \) implies \( (tf)(x) = 0 \), for all \( f \in k[t] \).

(iv) \( I_{x} := \{ f \in k[t] \mid f(x) = 0 \} \subseteq k[t] \) is an ideal.

(v) \( I_{x} := I_{x}^{0} := \{ f \in k[t] \mid f(x) = (tf)(x) = 0 \} \).

If these conditions are fulfilled, \( R \) is unique. In fact, the evaluation map \( \varepsilon_{x} : k[t] \to J \) of Exc. 149 (a) induces canonically an isomorphism

\[
\tilde{\varepsilon}_{x} : k[t]/I_{x} \sim R, \quad f + I_{x} \mapsto f(x), \quad (1)
\]

of unital commutative associative \( k \)-algebras.
5 Jordan algebras

Proof. (i) ⇒ (ii). By [30.8] the powers of \( x \) in \( R \) and \( R^{+} \) coincide.

(ii) ⇒ (iii). Denote the multiplication of \( R \) by juxtaposition. Assume \( f = \sum \alpha_t t \in k[t] \) with \( \alpha_t \in k \) satisfies \( f(x) = 0 \). From (ii) we deduce \( (tf)(x) = \sum \alpha_t x^{t+1} = x\sum \alpha_t x^t = xf(x) = 0 \). Thus (iii) holds.

(iii) ⇒ (iv). By [149] (a), \( I = I^0 \) is an ideal in \( k[t] \). Thus (iv) holds.

(iv) ⇒ (i). The evaluation \( \epsilon_\times : k[t] \to k[x] \) (Exc. [149]) induces a \( k \)-linear bijection \( \hat{\epsilon}_\times : k[t]/I_x \to k[x] \). Let \( R \in k\text{-alg} \) be the unique \( k \)-algebra having \( R = k[x] \) as \( k \)-modules and making \( \hat{\epsilon}_\times : k[t]/I_x \to R \) an isomorphism in \( k\text{-alg} \). But then \( \hat{\epsilon}_\times \) is an isomorphism of Jordan algebras from \( (k[t]/I_x)^{(+)} = k[t]^{(+)}/I_x \) not only to \( R^{(+)} \) but also to \( k[x] \subseteq J \). Hence (i) holds.

Uniqueness of \( R \) follows from the fact that it is spanned by the powers of \( x \) in \( J \) as a \( k \)-module. The rest is clear \( \square \)

Remark. The preceding arguments show that the proposition holds, more generally, for para-quadratic algebras that are power-associative at \( x \).

32.8. Local linearity. Our Jordan algebra \( J \) is said to be linear at \( x \in J \) if there exists a unital commutative associative \( k \)-algebra \( R \), necessarily unique, such that \( R = k[x] \) as \( k \)-modules and the equivalent conditions (i)–(iv) of Prop. 32.7 hold. By abuse of language, we simply write \( R = k[x] \) for this \( k \)-algebra and have

\[
(fg)(x) = f(x)g(x) \quad \text{for } f, g \in k[t].
\]

Finally, we say \( J \) is locally linear if it is linear at \( x \), for every \( x \in J \).

32.9. Examples. (a) If \( \frac{1}{x} \in k \), then every Jordan algebra over \( k \) is locally linear. This follows from Exc. [149] (a) combined with Prop. 32.7

(b) Every special Jordan algebra is locally linear. Indeed, if \( A \) is a unital associative \( k \)-algebra and \( J \subseteq A^{(+)} \) is a subalgebra, then for any \( x \in J \) the meanings of \( k[x] \) in \( J \) and in \( A \) are the same.

(c) There are pointed quadratic modules \( (M, q, e) \) over appropriate base rings such that the associated Jordan algebra, \( J(M, q, e) \), is not locally linear (Exc. [159] (b)).

32.10. Absolute zero divisors. An element \( x \in J \) is called an absolute zero divisor in \( J \) if \( U_x = 0 \). By abuse of language we say that \( J \) has no absolute zero divisors if \( U_x = 0 \) implies \( x = 0 \), for all \( x \in J \), in other words, if \( 0 \) is the only absolute zero divisor of \( J \).

32.11. Theorem (McCrimmon [78 Prop. 1]). \( J \) is locally linear provided it has no absolute zero divisors.

Proof. Let \( x \in J \) and \( f \in I_x \) (cf. Prop. 32.7 (iii)). Then Thm. 32.1 implies \( U_{(fg)}(x) = U_{f(x)}U_{g(x)} = 0 \) for all \( g \in k[t] \), forcing \( (fg)(x) = 0 \) by hypothesis, hence \( fg \in I_x \).
Thus $I \subseteq k[x]$ is an ideal, whence $J$ is linear at $x$, by Prop. 32.7 (iii). Thus $J$ is locally linear.

Exercises.

165. Absolute zero divisors in Jordan algebras of Clifford type. Let $(M,q,e)$ be a pointed quadratic module over $k$ and $J := J(M,q,e)$ the corresponding Jordan algebra of Clifford type.

(a) Show that if $k$ is reduced, then $x \in J$ is an absolute zero divisor if and only if $x \in \text{Rad}(q)$, i.e., $q(x) = q(x,y) = 0$ for all $y \in J$.

(b) Deduce from (a) that the absolute zero divisors of $J$ are contained in the nil radical of $J$. Conclude that $J$ is locally linear if $\text{Nil}(J) = \{0\}$ but not in general.

33. Inverses, isotopes and the structure group.

The present section is devoted to three fundamental concepts that have dominated the theory of Jordan algebras since ancient times. To begin with, the notions of invertibility and inverses arise naturally out of the analogy connecting the $U$-operator of Jordan algebras with the left (or right) multiplication operator of associative algebras. Isotopes, on the other hand, have been discussed earlier for alternative algebras but unfold their full potential only in the setting of Jordan algebras. And, finally, the structure group derives its importance not only from the connection with isotopes but, more significantly, from the one with exceptional algebraic groups that will be discussed more fully in later portions of the book.

Throughout this section, we let $k$ be a commutative ring and $J, J', J''$ be Jordan algebras over $k$.

33.1. The concept of invertibility. The idea of defining invertibility of an element in a linear Jordan algebra by properties (e.g., as in the alternative or associative case, by the bijectiveness) of its left multiplication operator is not a particularly useful one, see Exc. [171] below for details. Instead, it turns out to be much more profitable to do so by properties of the $U$-operator, an approach that has the additional advantage of making sense also for arbitrary Jordan algebras.

Accordingly, an element $x \in J$ is said to be invertible (in $J$) if there exists an element $y \in J$, called an inverse of $x$ (in $J$), such that

$$U_x y = x, \quad U_x y^2 = 1_J. \quad (1)$$

We will see in a moment that an inverse of $x$ in $J$, if it exists, is unique. More precisely, we can derive the following characterization of invertibility.

33.2. Proposition. For $x \in J$, the following conditions are equivalent.

(i) $x$ is invertible.

(ii) $U_x$ is bijective.

(iii) $U_x$ is surjective.
In this case, \( x \) has a unique inverse, written as \( x^{-1} \) and given by

\[
x^{-1} = U_x^{-1} x.
\]  

**Proof.** (i) \( \Rightarrow \) (ii). Let \( y \in J \) be an inverse of \( x \). Then \((33.1.1)\) and the fundamental formula \((31.3.2)\) imply \( U_x U_x U_y = 1_J \). Hence, \( U_x \), having a left and a right inverse in \( \text{End}_c(J) \), is bijective.

(ii) \( \Rightarrow \) (iii) \( \Rightarrow \) (iv). Clear.

(iv) \( \Rightarrow \) (i). Put \( y := U_x^{-1} x \in J \). Then \( U_y x = x \), \( U_x U_x U_y = U_y \), and since \( U_x \) is bijective, we conclude \( U_x = U_y^{-1} \). Hence, \( U_y^2 = U_x U_x U_y U_y^{-1} 1_J = 1_J \). Thus \((33.1.1)\) holds, and \( x \) is invertible with inverse \( y \). Combining \((33.1.1)\) with condition (ii), we see that the remaining assertions of the proposition also hold.

**33.3. Proposition.** Let \( x, y \in J \).

(a) If \( x \) is invertible, then so is \( x^{-1} \) and

\[
(x^{-1})^{-1} = x, \quad U_{x^{-1}} = U_x^{-1}, \quad V_{x^{-1}} = U_x^{-1} V_x = V_x U_x^{-1}.
\]  

(b) \( x \) and \( y \) are both invertible if and only if \( U_{xy} \) is invertible. In this case,

\[
(U_{xy})^{-1} = U_{x^{-1} y^{-1}}.
\]  

**Proof.** (a) From the fundamental formula and \((33.1.1)\) we deduce \( U_x U_{x^{-1}} U_x = U_{U_x U_{x^{-1}}} = U_x \), which implies \( U_{x^{-1}} = U_x^{-1} \) since \( U_x \) is bijective by Prop. 33.2. Thus \( x^{-1} \) is invertible, and \((33.2.1)\) yields \((x^{-1})^{-1} = U_x^{-1} x^{-1} = U_x x^{-1} = x \). Finally, \((33.1.1)\) implies \( U_x V_{x^{-1} x} = V_{x^{-1} x} U_x = 2U_x \), hence \( V_{x^{-1} x} = 2 \cdot 1_J. \) Now \((31.3.19)\) yields \( V_x = V_{U_x U_y} = V_y V_{x^{-1} x} = V_y V_{x^{-1} U_x} = V_y V_{x^{-1}} U_x = V_y V_{x^{-1}} U_x \), hence \( V_x = V_{x^{-1}} U_x \), and similarly, \( V_x = V_{U_x} V_{x^{-1}} \). This completes the proof of (a).

(b) By Prop. 33.2, the element \( U_{xy} \in J \) is invertible if and only if the linear map \( U_{xy} \) is invertible, i.e. so are \( U_x \) and \( U_y \) if \( x \) and \( y \) are both invertible. In this case, \((33.2.1)\) gives \((U_{xy})^{-1} = U_{U_y U_x} = U_{x^{-1} y^{-1}} U_{xy} = U_{x^{-1} y^{-1}} U_{xy} = U_{x^{-1} y^{-1}} U_{xy} = U_{x^{-1} y^{-1}} U_{xy} = U_{x^{-1} y^{-1}} U_{xy} = U_{x^{-1} y^{-1}}, \) as claimed.

**33.4. The set of invertible elements.** We denote by \( J^{\times} \) the set of invertible elements in \( J \). By Prop. 33.3 (b), it contains the identity element and is closed under the para-quadratic operation \( (x, y) \mapsto U_{xy} \). Note for a subalgebra \( J' \subseteq J \) that if an element \( x \in J' \) is invertible in \( J' \), then it is so in \( J \) and the two inverses are the same.

We say that \( J \) is a Jordan division algebra if \( J \not= \{0\} \) and all its non-zero elements are invertible: \( J^{\times} = J \setminus \{0\} \). We will see in Exc. 171 combined with Exc. 168 below that, in the presence of \( \frac{1}{2} \), Jordan division algebras are not the same as linear Jordan algebras that are division algebras in the sense of 9.7.

The following result is an immediate consequence of the definitions.
33.5. Proposition. If \( \varphi: J \to J' \) is a homomorphism, then \( \varphi(J^\times) \subseteq J'^\times \) and \( \varphi(x^{-1}) = \varphi(x)^{-1} \) for all \( x \in J^\times \). \( \square \)

33.6. Examples: alternative algebras. Let \( A \) be a unital alternative algebra over \( k \). We claim that an element \( x \in A \) is invertible in the Jordan algebra \( A^{(+)} \) if and only if it is so in \( A \), in which case the two inverses coincide. This follows immediately from Propositions 14.6 and 33.2. In particular, \( A^{(+)} \) is a Jordan division algebra if and only if \( A \) is an alternative division algebra.

33.7. Examples: associative algebras with involution. Let \( (B, \tau) \) be an associative \( k \)-algebra with involution and \( J := H(B, \tau) \) the Jordan algebra of \( \tau \)-symmetric elements in \( B \). Then \( \tau(x^{-1}) = \tau(x)^{-1} \) for all \( x \in B^\times \), by Lemma 17.1 for \( p = 1 \). Hence \( x \in J \) is invertible in \( J \) if and only if \( x \) is so in \( B \), in which case its inverses in \( J \) and \( B \) coincide. In particular, if \( B \) is an associative division algebra, then \( J \) is a Jordan division algebra.

But the converse of this implication does not hold: Let \( A \) be an associative division algebra and \( \varepsilon \) the exchange involution on \( B := A^{op} \oplus A \). Then \( H(B, \varepsilon) \) is a Jordan division algebra by (31.8) and 33.6 but \( B \) is not an associative division algebra.

33.8. Isotopes. Let \( p \in J \) be invertible. On the \( k \)-module \( J \) we define a new para-quadratic algebra over \( k \), depending on \( p \) and written as \( J^{(p)} \), by the \( U \)-operator \( U^{(p)}: J \to \text{End}_k(J), x \mapsto U^{(p)}(x) := U_xU_p \) and the base point \( 1^{(p)} := 1^p := p^{-1} \), which by (33.3) does indeed satisfy the relation \( U^{(p)}(1^p) = 1^{(p)} \). For \( x, y, z \in J \), the triple and circle product associated with \( J^{(p)} \) are given by \( \{xyz\}^{(p)} = U_{x,y}^{(p)}z = U_xU_py = \{x(U_p)y\}z \) and \( x \circ^{(p)} y = \{x1^p(y)\}^{(p)} = \{x(U_p)p^{-1}y\} = \{xy\} \), respectively. Summing up, writing \( V^{(p)} \) for the \( V \)-operator of \( J^{(p)} \), we obtain the formulas

\[
\begin{align*}
1^{(p)} &= 1^p = p^{-1}, \quad (1) \\
U_x^{(p)} &= U_xU_p, \quad (2) \\
U_{x,y}^{(p)} &= U_{x,y}U_p, \quad (3) \\
\{xyz\}^{(p)} &= \{x(U_p)y\}z, \quad (4) \\
x \circ^{(p)} y &= \{xy\}, \quad (5) \\
V_{x,y}^{(p)} &= V_{x,y}U_p, \quad (6) \\
V_x^{(p)} &= V_xU_p, \quad (7)
\end{align*}
\]

for all \( x, y, z \in J \). The para-quadratic algebra \( J^{(p)} \) is called the \( p \)-isotope (or simply an isotope) of \( J \). Note that passing to isotopes is

(i) unital: \( J^{(1)} = J \).
Functorial: if \( \varphi: J \to J' \) is a homomorphism, then \( \varphi: J^{(p)} \to J'^{(\varphi(p))} \) is a homomorphism of para-quadratic algebras.

(iii) compatible with base change: \( (J^{(p)})_R = (J_R)^{(p)} \) for all \( R \in k\text{-alg} \).

For \( n \in \mathbb{N} \), the \( n \)-th power of \( x \in J \) performed in the \( p \)-isotope \( J^{(p)} \) will be denoted by \( x^{(n,p)} \). For example \( x^{(2,p)} = U_x^{(p)} U_x^{(p)} = U_x U_p U_p^{-1} \), hence
\[
x^{(2,p)} = U_x p. \tag{8} \]

The first fundamental fact to be derived in the present context is that isotopes of Jordan algebras are Jordan algebras.

**33.9. Theorem.** \( J^{(p)} \) is a Jordan algebra over \( k \), for all \( p \in J^x \).

**Proof.** Since passing to isotopes is compatible with base change (33.8 (iii)), it suffices to prove (31.1.1), (31.1.2) for \( J^{(p)} \). Let \( x, y \in J \). Then (33.1.1) for \( J \) and (33.8.2) imply
\[
U_x^{(p)} U_y^{(p)} U_p = U_x U_p U_y U_p = U_x^{(p)} U_y^{(p)} U_p,
\]
hence (31.1.1) for \( p \). In order to accomplish the same for the identity (31.1.2), we apply (31.1.2) and (33.8.2), (33.8.6) for \( J \) to conclude
\[
U_p U_x^{(p)} U_y^{(p)} = U_p U_x U_p V_x U_p = U_x U_p U_x U_p = V_x U_p U_x U_p = U_x U_p U_x U_p,
\]
and canceling \( U_p \) yields (31.1.2) for \( J^{(p)} \). \( \square \)

**33.10. Theorem.** Let \( p \in J \) be invertible.

(a) An element \( x \in J \) is invertible in \( J^{(p)} \) if and only if it is so in \( J \). In this case, its inverse in \( J^{(p)} \) is given by \( x^{(-1,p)} = U_p^{-1} x^{-1} \).

(b) Let \( q \in J^{(p)x} = J^x \). Then \( (J^{(p)})^{(q)} = J^{(U_p q)} \).

**Proof.** (a) The first part follows immediately from (33.8.2) combined with Prop. 33.2. Moreover, applying (33.2.1) to \( J^{(p)} \) and \( J \), we conclude
\[
x^{(-1,p)} = U_x^{(p)-1} x = U_p^{-1} U_x^{-1} x = U_p^{-1} x^{-1},
\]
as claimed.

(b) From (33.8.1) and (a) we deduce \( (1^{(p)})^{(q)} = q^{(-1,p)} = U_p^{-1} q^{-1} = (U_p q)^{-1} = 1^{(U_p q)} \). Moreover, for \( x \in J \) we apply (33.8.2) repeatedly and obtain
\[
(U_x^{(p)})^{(q)} = U_x^{(p)} U_q^{(p)} = U_x U_p U_q U_p = U_x U_p U_q = U_x^{(U_p q)}.
\]
Summing up, we have proved (b). \( \square \)
33.11. Corollary. Setting $p^{-2} := (p^{-1})^2$, we have $(J(p))^{(p^{-2})} = J$ for all $p \in J^\times$.

Proof. $(J(p))^{(p^{-2})} = J(U_p(p^{-1})^2) = J$ by (33.11).

33.12. Examples: alternative algebras. Let $A$ be a unital alternative algebra over $k$ and $p \in A^{(+)} = A^\times$ (33.6). Writing $R_p$ for the right multiplication operator of $p$ in $A$, we claim that

$$R_p : A^{(+)}(p) \to A^{(+)}$$

is an isomorphism of Jordan algebras. Indeed, $R_p1_{A^{(+)}(p)} = R_p^{-1} = 1_{A^{(+)}}$, so $R_p$ preserves identity elements. Moreover, letting $x, y \in A$ and applying (14.5.4), we obtain

$$R_pU_x^{(p)}y = R_pU_xU_py = R_pU_xL_pR_py = U_xpR_py = U_{R_p}pR_py,$$

hence the assertion.

In particular, we can now conclude that isotopes of special Jordan algebras are special. Indeed, if $J$ is special, then there exists a unital associative algebra $A$ over $k$ and an injective homomorphism $\varphi : J \to A^{(+)}$. Therefore we deduce for $p \in J^\times$ that $\varphi$ is also an injective homomorphism from $J(p)$ to $A^{(+)}(\varphi(p)) \cong A^{(+)}$. Thus $J(p)$ is special.

33.13. The connection with isotopes of alternative algebras. Let $A$ be a unital alternative algebra over $k$ and $p, q \in A^\times$. Consulting (16.5.1) and Prop. 16.6, we conclude

$$A^{(p,q)(+)} = A^{(+)(pq)},$$

(1) ISTALT

In particular, as is already implicit in Lemma 16.10 passing to unital isotopes of alternative algebras does not change the Jordan structure:

$$A^{p(+)} = A^{(+)} \quad (p \in A^\times).$$

(2) JUNIST

33.14. Examples: associative algebras with involution. Let $(B, \tau)$ be an associative $k$-algebra with involution and $p \in H(B, \tau)^\times = H(B, \tau) \cap B^\times$ (33.7). Then it is readily checked that

$$\tau^p : B \to B, \quad x \mapsto \tau^p(x) := p^{-1}\tau(x)p$$

(1) PETWIN

is an involution of $B$ satisfying

$$H(B, \tau^p) = H(B, \tau)p;$$

(2) PETSYM

this also follows from Prop. 17.7. In view of 33.12 we therefore conclude that

$$R_p : H(B, \tau)^{(p)} \to H(B, \tau^p)$$

(3) HABEP
is an isomorphism of Jordan algebras that fits into the commutative diagram

\[
\begin{array}{ccc}
B^{(+)(p)} & \cong & B^{(+)} \\
\eta & \mapsto & \eta \\
H(B, \tau)^{(p)} & \cong & H(B, \tau^p).
\end{array}
\]

**Remark.** The second fundamental fact to be observed in the present context is that isotopes of \( J \), though they are always Jordan algebras, will in general not be isomorphic to \( J \). For examples along these lines, see Exc. [169](d),(e) below.

**33.15. Homotopies.** Homotopies of Jordan algebras are homomorphisms into appropriate isotopes. More precisely, a homotopy from \( J \) to \( J' \) is a map \( \eta : J \rightarrow J' \) such that \( \eta : J \rightarrow J'^{(p)} \) is a homomorphism, for some \( p' \in J'^{\times} \). In this case, Prop. [33.5](d) and Thm. [33.10](a) imply \( \eta(J^{(p)}) \subseteq J'^{(p')\times} = J'^{\times} \), and \( p' \) is uniquely determined since \( \eta(1) = 1_{J'^{(p)}} = p'^{-1} \), hence

\[
p' = \eta(1)\big)^{-1}.
\]

We will see in Prop. [33.16](e) below that compositions of homotopies are homotopies. Hence Jordan \( k \)-algebras under homotopies form a category, denoted by \( k\text{-jord}_{\text{hmt}} \). The isomorphisms in this category are precisely the bijective homotopies and are called *isotopies*. The isotopies from \( J \) to itself are called *autotopies*.

**33.16. Proposition.** (a) \( \eta : J \rightarrow J' \) is a homomorphism if and only if \( \eta \) is a homotopy preserving units: \( \eta(1) = 1_J \).

(b) Let \( p \in J^{\times} \), \( p' \in J'^{\times} \). Then \( \eta : J \rightarrow J' \) is a homotopy if and only if so is \( \eta : J^{(p)} \rightarrow J'^{(p')} \).

(c) If \( \eta : J \rightarrow J' \) and \( \eta' : J' \rightarrow J'' \) are homotopies, then so is \( \eta' \circ \eta : J \rightarrow J'' \).

**Proof.** (a) A homomorphism is a homotopy preserving units. Conversely, let \( \eta : J \rightarrow J' \) be a homotopy preserving units. By [33.15](e), therefore, \( \eta : J \rightarrow J'^{(p)} \) is a homomorphism, with \( p' = \eta(1)\big)^{-1} = 1_J \).

(b) Assume first that \( \eta : J \rightarrow J' \) is a homotopy. Then some \( q' \in J'^{\times} \) makes \( \eta : J \rightarrow J'^{(q')} \) a homomorphism. Hence a repeated application of Thm. [33.10](b) implies that so is \( \eta : J^{(p)} \rightarrow J'^{(p')(q')} \), with \( q' = U_{p',q} \eta(p) \). Thus \( \eta : J^{(p)} \rightarrow J'^{(p')} \) is a homotopy. Conversely, if \( \eta : J^{(p)} \rightarrow J'^{(p')} \) is a homotopy, then what we have just shown implies that so is \( \eta : J = J^{(p'(p^{-2})} \rightarrow J^{(p')(p'^{-2})} = J' \).

(c) Some \( p'^{\prime} \in J'^{\times} \) makes \( \eta : J \rightarrow J'^{(p')} \) a homomorphism. But \( \eta' : J'^{(p')} \rightarrow J'' \) is a homotopy by (a), so some \( p'' \in J''^{\times} \) makes \( \eta' : J'^{(p')} \rightarrow J'^{(p'')} \) a homomorphism. Hence so is \( \eta' \circ \eta : J \rightarrow J'^{(p'')} \), implying (c).
33.17. Proposition. For all linear maps \( \eta : J \to J' \), the following conditions are equivalent.

(i) \( \eta \) is an isotopy from \( J \) to \( J' \).
(ii) \( \eta \) is bijective and there exists a bijective linear map \( \eta^\sharp : J' \to J \) such that

\[ U_{\eta(x)} = \eta U_{x} \eta^\sharp \]

for all \( x \in J \).

In this case, \( \eta^\sharp \) is uniquely determined and satisfies

\[ \eta^\sharp = \eta^{-1} U_{\eta(1_J)}. \]

Proof. The final assertion follows immediately from (1) for \( x = 1_J \).

(i) \( \Rightarrow \) (ii). Some \( p' \in J'^\times \) makes \( \eta : J \to J'(p') \) an isomorphism. For \( x, y \in J \) we therefore conclude \( \eta(U_{x}\eta) = U_{\eta(x)}\eta^{(p')}\eta(y) = U_{\eta(x)}\eta U_{p'}\eta(y) \), hence \( \eta U_{x} = U_{\eta(x)}\eta^{(p')}\eta \), and we obtain (1) by setting \( \eta^\sharp := \eta^{-1} U_{p'}^{-1} \).

(ii) \( \Rightarrow \) (i). Put \( p' := \eta(1_J)^{-1} \in J'^\times \). Then \( \eta(1_J) = p'^{-1} \) and (1) yields \( U_{p'} = U_{\eta(1_J)} = (\eta \eta^\sharp)^{-1} = \eta^\sharp^{-1} \eta^{-1} \). Applying (1) once more, we therefore deduce

\[ U_{\eta(x)}^{(p')}\eta(y) = U_{\eta(x)} U_{p'} \eta(y) = \eta U_{\eta^\sharp} \eta^{\sharp^{-1}} \eta^{-1} \eta(y) = \eta(U_{\eta(x)} \eta(y)) \]

for all \( x, y \in J \). Thus \( \eta : J \to J'(p') \) is an isomorphism, making \( \eta : J \to J' \) an isotopy.

33.18. The structure group. The group of autotopies of \( J \) is denoted by \( \text{Str}(J) \) and called the structure group of \( J \). By Prop. 33.17 for \( J' = J \), it consists of all \( \eta \in \text{GL}(J) \) such that there exists an \( \eta^\sharp \in \text{GL}(J) \) satisfying

\[ U_{\eta(x)} = \eta U_{x} \eta^\sharp \]

for all \( x \in J \). Combining this with the fundamental formula (31.1) and Prop. 33.2 we see that \( U_{x} \in \text{Str}(J) \) for all \( x \in J' \); in fact, we then have \( U_{x}' = U_{x} \). The subgroup of \( \text{Str}(J) \) generated by the linear operators \( U_{x}, x \in J' \), is called the inner structure group of \( J \), denoted by \( \text{Instr}(J) \). Combining (1) with (33.17.2), we obtain \( \eta U_{x} \eta^{-1} = U_{\eta(x)} U_{\eta(1_J)}^{-1} \) for all \( \eta \in \text{Str}(J) \) and all \( x \in J' \). Thus \( \text{Instr}(J) \subseteq \text{Str}(J) \) is actually a normal subgroup. It is also readily checked that the assignment \( \eta \mapsto \eta^\sharp \) determines an involution of \( \text{Str}(J) \), i.e., an anti-automorphism of period 2.

33.19. Theorem. (a) Both the structure group and the inner structure group remain unchanged when passing to isotopes:

\[ \text{Str}(J^{(p)}) = \text{Str}(J), \quad \text{Instr}(J^{(p)}) = \text{Instr}(J) \quad (p \in J'^\times). \]
(b) The structure group of $J$ acts canonically on $J^\times$, and we have

$$\eta(x)^{-1} = \eta^{x^{-1}}(x^{-1}) \quad (\eta \in \text{Str}(J), x \in J^\times).$$

(c) The stabilizer of $1_J$ in $\text{Str}(J)$ is $\text{Aut}(J)$, the automorphism group of $J$.

(d) For $p, q \in J^\times$ and $\eta \in \text{End}_k(J)$, the following conditions are equivalent.

(i) $\eta : J(p) \to J(q)$ is an isomorphism.

(ii) $\eta \in \text{Str}(J)$ and $\eta(p^{-1}) = q^{-1}$.

(iii) $\eta \in \text{Str}(J)$ and $\eta^{\sharp}(q) = p$.

Proof. (a) follows immediately from Prop. 33.16 (b) and (33.8.2).

(b) The first part follows immediately from (33.18.1) combined with Prop. 33.2.

Moreover, given $x \in J^\times$, an application of (33.18.1) and (33.2.1) yields $\eta(x)^{-1} = U_{\eta(x)}^{-1}\eta(x) = \eta^{x^{-1}}U_{\eta(x)}^{-1} \eta^{-1}(x)$, hence (2).

(c) follows immediately from Prop. 33.16 (a).

(d) (i) $\iff$ (ii). By Prop. 33.16, condition (i) holds if and only if $\eta \in \text{Str}(J)$ and $\eta(p^{-1}) = 1^1_{(p)} = q^{-1}$.

(ii) $\iff$ (iii). For $\eta \in \text{Str}(J)$, the condition $\eta(p^{-1}) = q^{-1}$ by (2) is equivalent to $q = \eta(p^{-1})^{-1} = \eta^{\sharp}(p)$, hence to $\eta^{\sharp}(q) = p$. \qed

33.20. Corollary. For $p, q \in J^\times$, the isotopes $J(p)$ and $J(q)$ are isomorphic if and only if $p$ and $q$ belong to the same orbit of $J^\times$ under the action of the structure group of $J$.

33.21. Corollary. Let $J$ be an algebraic Jordan algebra over an algebraically closed field $F$ of characteristic not 2. Then the inner structure group of $J$ acts transitively on $J^\times$, and any two isotopes of $J$ are isomorphic.

Proof. Let $p \in J^\times$. By Exc. 33, there exists a $q \in J^\times$ such that $p = q^2 = U_q 1_J$. Hence $p$ belongs to the orbit of $1_J$ under the inner structure group of $J$. This proves the first assertion, while the second one now follows immediately from Cor. 33.20. \qed

Remark. Cor. 33.21 does not hold in characteristic 2, see Exc. 169 (e) below.

33.22. On the methodological importance of isotopes. By deriving the results of the present section, we have brought to the fore the close analogy connecting the $U$-operator of Jordan algebras with the left (or right) multiplication operator of associative algebras. There are important differences, however. For example, the trivial observation that the group of left multiplications induced by invertible elements of a unital associative algebra $A$ is transitive on $A^\times$ has no analogue in the Jordan setting. In fact, combining Cor. 33.20 with Exc. 169 (d) below, it follows that there are Jordan algebras over fields where not even the full structure group, let alone the inner one, acts transitively on their invertible elements.

Isotopes may be regarded as a substitute for this deficiency. For example, one is often confronted with the task of proving an identity for Jordan algebras involving invertible elements $x, y, z, \ldots$. This task can sometimes be simplified by passing to
an appropriate isotope, which would then allow one to assume that, e.g., $x$ is the identity element. Here is a typical result where the procedure just described turns out to be successful.

**33.23. Theorem** (Jacobson [45, Prop. 1.7.10]). Let $x, y$ be elements of $J$ and assume that $y$ is invertible. If two of the elements $x, x + U_2 y, x + y^{-1}$ are invertible, then so is the third and

$$
(x + U_2 y)^{-1} + (x + y^{-1})^{-1} = x^{-1}.
$$

**Proof.** We first treat the case $y = 1_J$ by showing that if two of the elements $x, x + x^2, 1_J + x$ are invertible, then so is the third and

$$
(x + x^2)^{-1} + (1_J + x)^{-1} = x^{-1}.
$$

We begin by applying Thm. 32.1 to deduce

$$U_{x + x^2} = U_x U_{1_J + x}.
$$

Hence our first intermediate assertion holds. Moreover, combining (31.11) with (31.15.2), we obtain $U_{x + x^2} x^{-1} = V_x U_{x + x^2} x^{-1} = 2x^2$, which together with (3) implies

$$U_{x + x^2} ((x + x^2)^{-1} + (1_J + x)^{-1}) = x + x^2 + U_x (1_J + x) = x + 2x^2 + x^3 = U_{x + x^2} x^{-1} + U_{x + x^2} x^{-1} = U_{x + x^2} x^{-1},$$

hence (2).

Next let $y \in J^x$ be arbitrary. Passing to the $y$-isotope $J^{(y)}$, which satisfies $J^{(y)^x} = J^x$ by Thm. 33.10 (a), the relations

$$x + U_2 y = x + x^{(2,y)}, \quad x + y^{-1} = 1^{(y)} + x$$

and the special case treated before prove the first part of the theorem. Moreover, by Thm. 33.10 (a) again and (2) for $J^{(y)}$,

$$
(x + U_2 y)^{-1} + (x + y^{-1})^{-1} = U_y (x + x^{(2,y)})^{-1} + (1^{(y)} + x)^{-1} = U_y x^{-1} = x^{-1}.
$$

□

**33.24. Corollary.** (Hua’s identity). Let $x, y \in J$ be invertible such that $x - y^{-1}$ is invertible as well. Then so is $x^{-1} - (x - y^{-1})^{-1}$ and

$$U_2 y = x - (x^{-1} - (x - y^{-1})^{-1})^{-1}.$$

**Proof.** Thm. 33.23 for $-x$ in place of $x$ shows that $-x + U_2 y$ is invertible and
\[-x + U_n y \]^{-1} = -(x^{-1} - (x - y)^{-1}).

The assertion follows. \[\square\]

Exercises.

166. Evaluation at invertible elements. Let \( x \) be an invertible element of \( J \).

(a) Define

\[ x^{-n} := (x^{-1})^n \]  

for all positive integers \( n \) (see Cor. [33,11] for \( n = 2 \)) and prove

\[ U_e = U_1^n, \]  
\[ U_{e^n} x^n = x^{2m+n}, \]  
\[ (x^n)^n = x^{2m}, \]  
\[ \{ x^m x^n \}^p = 2x^{m+n+p}, \]  
\[ V_{e^n} v^n = V_{v^{m+n}}, \]  
\[ U_{e^n} U_{e^{m+n}} = U_{e^{m+n}} U_{e^n}, \]  
\[ U_{e^n} U_{e^{m+n}} + U_{e^{m+n}} U_{e^n} \]

for all \( i, j, m, n \in \mathbb{Z} \).

(b) Write \( k[t, t^{-1}] \) for the ring of Laurent polynomials in the variable \( t \) over \( k \) and

\[ \epsilon^n : k[t, t^{-1}) \rightarrow J \]

for the unique linear map sending \( t^n \) to \( x^n \) for all \( n \in \mathbb{Z} \). Show that \( \epsilon^n \) is a homomorphism of Jordan algebras and that \( k[x, x^{-1}) := \text{Im}(\epsilon^n) \) is the subalgebra of \( J \) generated by \( x \) and \( x^{-1} \).

(c) Write \( f(x) := \epsilon^n(f) \) for \( f \in k[t, t^{-1}] \) and show that

\[ U_{\epsilon^n(f)} = U_{f(x)} U_{\epsilon^n(f)} \]

for all \( f, g \in k[t, t^{-1}] \). Conclude that if \( J \) has no absolute zero divisors, then \( k[x, x^{-1}] \) carries the structure of a unique algebra \( R \in k\text{-alg} \) such that \( k[x, x^{-1}] = R^{(1)} \) as Jordan algebras.

167. Invertibility in linear Jordan algebras. Let \( J \) be a linear Jordan algebra over a commutative ring containing \( \frac{1}{2} \). Elements \( x, y \in J \) are said to operator commute if \( [L_x, L_y] = 0 \).

(a) Prove for \( x, y \in J \) that \( x^2 \) and \( y \) operator commute if and only if so do \( x \) and \( xy \).

(b) Prove for \( x \in J \) that the following conditions are equivalent.

(i) \( x \) is invertible.
(ii) There exists an element \( y \in J \) such that \( xy = 1_J \) and \( x, y \) operator commute.
(iii) There exists an element \( y \in J \) such that \( xy = 1_J \) and \( x^2 y = x \).

Show further that if these conditions are fulfilled, then \( y \) as in (ii) (resp. (iii)) is unique and equal to \( x^{-1} \).

Remark. The characterization of invertibility in (b) (ii) is due to Koecher (unpublished).

168. Invertibility in pointed quadratic modules. Let \( (M, q_1, e) \) be a pointed quadratic module with conjugation \( x \mapsto \overline{x} \) over \( k \). Prove that an element \( x \in M \) is invertible in the Jordan algebra \( J := J(M, q_1, e) \) if and only if \( q_1(x) \in k \) is invertible in \( k \). In this case,
Inverses, isorotaes and the structure group.

\[ x^{-1} = q(x)^{-1} x, \quad q(x)^{-1} = q(x)^{-1}. \]  

(10) \[ \text{INVPOI} \]

If \( x \) is invertible in \( J \), we also say \( x \) is invertible in \( (M, q, e) \) with inverse \( x^{-1} \). Thus the Jordan algebra of a pointed quadratic module \( (M, q, e) \) over a field is a Jordan division algebra if and only if the quadratic form \( q \) is anisotropic.

**pr.ISTPOI**

169. Isorotopes of pointed quadratic modules. Let \((M, q, e)\) be a pointed quadratic module over \( k \), with trace \( t \) and conjugation \( x \mapsto \bar{x} \).

(a) Let \( f \in M \) be invertible in \((M, q, e)\) (Exc. 166). Show that

\[ (M, q, e)^{(f)} := (M, q^{(f)}, e^{(f)}) \], \quad q^{(f)} := q(f)q, \quad e^{(f)} := f^{-1} \]

is a pointed quadratic module over \( k \) with trace

\[ t^{(f)} : M \to k, \quad x \mapsto t^{(f)}(x) := q(f, x), \]

and conjugation

\[ x \mapsto \bar{x}^{(f)} := q(f)^{-1} q(f, x) f - x. \]

Show further

\[ J((M, q, e)^{(f)}) = (J(M, q, e))^{(f)}. \]

We call \((M, q, e)^{(f)}\) the \( f \)-isorotope (or simply an isotope) of \((M, q, e)\).

(b) Let \( f \in M \) be invertible in \((M, q, e)\). Prove that the isorotopes of \((M, q, e)\) and \((M, q, e)^{(f)}\) are the same, and that

\[ (M, q, e)^{(f)}(g) = (M, q, e)^{(f/g)} \]

for all invertible elements \( g \) of \((M, q, e)\), where \( U \) stands for the \( U \)-operator of the Jordan algebra \( J(M, q, e) \).

(c) Prove that if \( M \) is projective as a \( k \)-module, then the structure group of \( J(M, q, e) \) agrees with the group of similarity transformations of the quadratic module \((M, q)\), consisting by definition of all bijective linear maps \( \eta : M \to M \) such that \( q \circ \eta = \alpha q \) for some \( \alpha \in k^\times \).

(d) Let \( k := \mathbb{R} \) and \( M := \mathbb{R}^3 \) with the canonical basis \((e_1, e_2, e_3)\). Put \( e := e_1 \) and \( q := \langle S \rangle_{\text{quad}} \) with

\[ S := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \]

Find an isotope of \( J := J(M, q, e) \) which is not isomorphic to \( J \).

(e) Let \( k := F \) be a field of characteristic 2 and assume \((M, q, e)\) is traceless in the sense that \( t = 0 \). Furthermore, let \( f \in M \) be anisotropic relative to \( q \) and assume \( f \notin \text{Rad}(Dq) \). Then put \( J := J(M, q, e) \) and prove that the isotope \( J^{(f)} \) is not isomorphic to \( J \). Finally, give an example where the preceding hypotheses are fulfilled even when \( F \) is algebraically closed.

**pr.FOUROP**

170. A useful formula for the \( U \)-operator: (cf. Braun-Koecher [15] IV, Satz 3.8) Let \( x, y \) be invertible elements of \( J \). Prove

\[ U_x U_{x^{-1} y} U_y = U_{x y}. \]

(Hint. Pass to the isotope \( J^{(i)} \) and apply Exc. 166[9].)

**pr.LININV**

171. Linear invertibility. Let \( J \) be a linear Jordan algebra over a commutative ring \( k \) containing \( \frac{1}{2} \). An element \( x \in J \) is said to be \textit{linearly invertible} if the left multiplication operator \( L_x : J \to J \) is bijective. In this case we call \( x^{-1} := L_x^{-1} \) the \textit{linear inverse} of \( x \) in \( J \). Prove that if \( x \) is
5 Jordan algebras

linearly invertible, then it is invertible, and its linear inverse and its ordinary inverse are the same. Finally, prove that invertible elements of $J$ need not be linearly invertible by showing for any pointed quadratic module $(M, q, e)$ over a field of characteristic not 2 that $J := J(M, q, e)$ is a linear division algebra in the sense of 9.7 if and only if $q$ is anisotropic and $\dim_F(J) \leq 2$.

For more on the connection between linear and ordinary Jordan division algebras, see Petersson [97].

172. **Strong homotopies.** A linear map $\eta: J \to J'$ is called a strong homotopy if some $p \in J^\times$ makes $\eta: J(p) \to J'$ a homomorphism.

(a) Prove that strong homotopies are homotopies. Conversely, if $\eta: J \to J'$ is a homotopy and $\eta(J^\times) = J'^\times$, show that $\eta$ is a strong homotopy.

(b) Give an example of a homotopy which is not a strong homotopy.

173. (Petersson [94, 96] **Discrete valuations of Jordan division rings**). Let $J$ be a Jordan division ring, i.e., a Jordan division algebra over $\mathbb{Z}$, and write $F$ for the centroid of $J$. Recall from Exc. [55] (c) that $F$ is a field and that $J$ may canonically be regarded as a Jordan algebra over $F$.

By a discrete valuation of $J$ we mean a map $\lambda: J \to \mathbb{Z}_\infty := \mathbb{Z} \cup \{\infty\}$ satisfying the following conditions, for all $x, y \in J$.

\begin{align*}
\lambda(x) = 0 & \iff x = 0, \quad \text{(15)} \\
\lambda(xy) = 2\lambda(x) + \lambda(y), & \quad \text{(16)} \\
\lambda(x + y) & \geq \min\{\lambda(x), \lambda(y)\}. \quad \text{(17)}
\end{align*}

For the rest of this exercise, fix a discrete valuation $\lambda$ of $J$ and observe by Thm. [32.11] that $J$ is locally linear. Then prove:

(a) For all $x \in J^\times$ and all $n \in \mathbb{Z}$, we have $\lambda(x^n) = n\lambda(x)$.

(b) For all $x \in J$ and all $v, w \in F[x]$, we have $\lambda(vw) = \lambda(v) + \lambda(w)$. Conclude that $\lambda_0: F \to \mathbb{Z}_\infty, \quad a \mapsto \lambda_0(a) := \lambda(a1)\text{,}$

is a discrete valuation of $F$, with valuation ring, valuation ideal, and residue field respectively given by

\[ o_0 := \{a \in F \mid \lambda_0(a) \geq 0\}, \]
\[ p_0 := \{a \in F \mid \lambda_0(a) > 0\}, \]
\[ F := o_0/p_0. \]

(c) The sets

\[ \mathcal{D} := \{x \in J \mid \lambda(x) \geq 0\} \subseteq J, \]
\[ \mathcal{Q} := \{x \in J \mid \lambda(x) > 0\} \subseteq \mathcal{D}, \]
\[ \mathcal{J} := \mathcal{D}/\mathcal{Q} \]

are respectively an $o_0$-subalgebra of $J$, an ideal in $\mathcal{D}$, a Jordan division algebra over $F$. But note that, even if $J$ is a linear Jordan algebra over $F$ (i.e., $F$ has characteristic not 2), $\mathcal{D}$ need not be one over $o_0$, and $J$ need not be one over $F$.

(d) $\lambda(J^\times)$ is a subgroup of $\mathbb{Z}$, called the value group of $\lambda$.

(e) For $p \in J^\times$, the map

\[ \lambda^{(p)}: J^{(p)} \to \mathbb{Z}_\infty, \quad x \mapsto \lambda^{(p)}(x) := \lambda(p) + \lambda(x), \]

In this exercise, the reader is assumed to be familiar with the rudiments of valuation theory.
is a discrete valuation of $J(p)$ having the same value group as $\lambda$. We call $\lambda(p)$ the $p$-isotope of $\lambda$. Given another element $q \in J^*$, show further $(\lambda(p))(q) = \lambda(U_p q)$.

(f) $\lambda$ satisfies the Jordan triple product inequality

$$\lambda(\{xyz\}) \geq \lambda(x) + \lambda(y) + \lambda(z)$$

(18) \text{LATRI}

for all $x, y, z \in J$. (Hint. Reduce to the case $y = 1_J$. Then derive and use the formula

$$(x \circ y)^2 = U_{x^2} + U_{y^2} + x \circ (U_{x^2}),$$

(19) \text{CIRSQU}

valid for all $x, y$ in arbitrary Jordan algebras.)

174. Let $J$ be an algebraic Jordan division algebra over a field $F$. Prove:

(a) For $x \in J$, the subalgebra $F[x] \subseteq J$ is a finite algebraic field extension of $F$.

(b) If $F$ is algebraically closed, then $J \cong F^{(+)}$.

(c) For $F = \mathbb{R}$, there exists a pointed quadratic module $(M, q, e)$ over $\mathbb{R}$ such that $J \cong J(M, q, e)$ and $q$ is positive definite.

34. The Peirce decomposition

The Peirce decomposition in its various guises belongs to the most powerful techniques in the structure theory of Jordan algebras. Initiated by Jordan-von Neumann-Wigner in their study of euclidean Jordan algebras, it dominated the scene way into the nineteen-sixties, losing a certain amount of its appeal only when research began to focus on Jordan algebras without finiteness conditions where idempotents (the principal ingredient of the Peirce decomposition) are in short supply.

The present section is devoted to those properties of the Peirce decomposition that are relevant for our subsequent applications to cubic Jordan algebras. Our treatment of the subject relies quite heavily on the approach of Loos [67, § 5] (after being specialized from Jordan pairs to algebras), which in turn owes much to the one of Springer [120, § 10].

Throughout we let $k$ be a commutative ring and $J$ a Jordan algebra over $k$. Recall from Exc. 155 (b) that an idempotent in $J$ is an element $c$ satisfying $c^2 = c$. The additional hypothesis $c^3 = c$ that has to be imposed in the setting of arbitrary para-quadratic algebras (cf. 30.9), implying $c^n = c$ for all positive integers $n$, holds automatically in the Jordan case.

34.1. Lemma. Let $c$ be an idempotent in $J$ and put $d := 1_J - c$. Writing $D := k \oplus k$ for the split quadratic étale $k$-algebra,

$$\Theta_c : D \longrightarrow \text{End}_k(J), \quad \gamma \oplus \delta \longmapsto \Theta_c(\gamma \oplus \delta) := U_{\gamma c + \delta d} \quad (\gamma, \delta \in k)$$

is a quadratic map that is unital and permits composition:

$$\Theta_c(1_D) = 1_J, \quad \Theta_c((\gamma_1 \oplus \delta_1)(\gamma_2 \oplus \delta_2)) = \Theta_c(\gamma_1 \oplus \delta_1)\Theta_c(\gamma_2 \oplus \delta_2)$$

(1) \text{THUNCO}

for all $\gamma, \delta_i \in k, i = 1, 2$. In particular,
Moreover, $\Theta_c$ is compatible with base change: $\Theta_cR = (\Theta_c)_R$ for all $R \in k$-alg.

Proof. The first equation of (3) is obvious. In order to prove the second, we let $i = 1, 2$ and note $\Theta_c(\gamma \oplus \delta)_i = U_{\delta_i1J + (\gamma - \delta)_i} = U_{f_i(c)}$, where $f_i := \delta_i + (\gamma - \delta)_i t \in k[t]$. Hence Thm. 32.1 implies $\Theta_c(\gamma \oplus \delta)_i \Theta_c(\gamma_2 \oplus \delta_2)_i = U_{(f_1f_2)(c)}$, where

\[ f_1f_2 = \delta_1 \delta_2 + ((\gamma_1 - \delta_1) \delta_2 + \delta_1 (\gamma_2 - \delta_2)) t + (\gamma_1 - \delta_1)(\gamma_2 - \delta_2) t^2. \]

Evaluating at $c$, we conclude

\[
(f_1f_2)(c) = \delta_1 \delta_2 1J + ((\gamma_1 - \delta_1) \delta_2 + \delta_1 (\gamma_2 - \delta_2)) c
= \delta_1 \delta_2 1J + ((\gamma_1 - \delta_1) \gamma_2 + \delta_1 (\gamma_2 - \delta_2)) c
= (\gamma_1 \gamma_2) c + (\delta_1 \delta_2) d,
\]

and the second equation of (3) is proved. The remaining assertions are now obvious. \hfill $\Box$

3.4.2. Theorem (Singular Peirce decomposition). Let $c$ be an idempotent in $J$ and put $d := 1 - c$. Then the following statements hold.

(a) The linear endomorphisms of $J$ defined by

\[ E_2 := E_2(c) := U_c, \quad E_1 := E_1(c) = U_{c,d} = V_c - 2U_c, \quad E_0 := E_0(c) := U_d \]

satisfy the relation

\[ U_{1R} + dR = E_{0R} + tE_{1R} + t^2 E_{2R} \]

for all $R \in k$-alg and all $t \in R$.

(b) The $E_i$, $i = 0, 1, 2$, are orthogonal projections of $J$, called its Peirce projections relative to $c$, and their sum is the identity. Hence they give rise to a decomposition

\[ J = J_2 \oplus J_1 \oplus J_0 \]

as a direct sum of submodules $J_i := J_i(c) := \text{Im}(E_i)$ for $i = 0, 1, 2$, called the Peirce components of $J$ relative to $c$.

(c) We have

\[ J_2 = \text{Im}(U_c), \quad J_1 \oplus J_0 = \text{Ker}(U_c), \quad (4) \]

\[ J_0 = \text{Ker}(U_c) \cap \text{Ker}(V_c), \quad (5) \]

\[ J_i \subseteq \{x \in J \mid c \circ x = ix\} \quad (i = 0, 1, 2), \quad (6) \]

\[ J_1 = \{x \in J \mid c \circ x = x\}. \quad (7) \]

\[ J_{\text{one}} \]

\[ J_{\text{two}} \]

\[ J_{\text{zero}} \]

\[ J_{\text{Peprsi}} \]

\[ J_{\text{UCDEXP}} \]

\[ J_{\text{PEDESI}} \]

\[ J_{\text{JTWO}} \]

\[ J_{\text{JZERO}} \]

\[ J_{\text{JONE}} \]
while (2) is equally obvious.

(a) Expanding Proof.

Setting $J_i$ yields as direct sums of $J_i$ and comparing coefficients of $x_i$ yields (6) implies $x_i = 0$. Then (5) follows. From (4) we also deduce $V_{i,j} = V_{0,j} = 0$, hence $x_i = 0$. Then (6) implies $x_i = 0$. Hence the identifications of 31.2 imply

$$J \subseteq J_R = \bigoplus_{i,j \geq 0} (s^i t^j)J, \quad \text{End}_k(J) \subseteq \text{End}_k(J)_R = \bigoplus_{i,j \geq 0} (s^i t^j \text{End}_k(J)) \subseteq \text{End}_k(J_R)$$

as direct sums of $k$-modules. With this in mind, Lemma 34.1 combined with 2 yields

$$\sum_{i,j=0}^2 s^i t^j E_i E_j = \sum_{i,j=0}^2 s^i E_i (\sum_{j=0}^2 t^j E_j) = \Theta_{R^2} (s \oplus 1_R) \Theta_{R}(t \oplus 1_R)$$

Comparing coefficients of $s^i t^j$, we obtain $E_i E_j = \delta_{ij} E_i$ for $i, j = 0, 1, 2$, and the first assertion of (b) follows. The remaining ones are obvious.

(c) Since $U_c = E_2$ by (1), equation (4) is obvious. Applying (1) once more, we conclude $J_0 = \text{Ker}(E_2) \cap \text{Ker}(E_1) = \text{Ker}(U_c) \cap \text{Ker}(V_c - 2U_c)$, and (5) follows. From (1) we also deduce $V_c = V_{1,2} = 2E_2 + E_1 = \sum_{j=0}^2 jE_j$, and applying this to $x_i \in J_i$, we obtain $c \circ x_i = V_c x_i = \sum_j E_j x_i = i x_i$, giving (6) and the inclusion from left to right in (7). Conversely, suppose $x \in J$ satisfies $c \circ x = x$ and write $x = x_2 + x_1 + x_0$, $x_i \in J_i$. Then (6) implies $x = 2x_2 + x_1$ and comparing $J_i$-components for $i = 0, 1, 2$, we conclude $x_2 = x_0 = 0$, hence $x = x_1 \in J_1$. This completes the proof of (7).

(d) Let $R = k[t, t^{-1}]$ be the $k$-algebra of Laurent polynomials in the variable $t$ over $k$, which is free as a $k$-module with basis $(t^i)_{i \in \mathbb{Z}}$. Hence 31.2 yields the identifications

$$J \subseteq J_R = \bigoplus_{i \in \mathbb{Z}} (t^i)J, \quad \text{End}_k(J) \subseteq \text{End}_k(J)_R = \bigoplus_{i \in \mathbb{Z}} (t^i \text{End}_k(J)) \subseteq \text{End}_k(J_R)$$

as direct sums of $k$-modules. Since $t \in R^\times$, we deduce from (2) and Lemma 34.1 that the map

$$U_{t^i + d} = \sum_{j=0}^2 t^j E_j : J_R \rightarrow J_R$$
is bijective with inverse $U_{1+c+d}$. Moreover, for $x = \sum_{i=0}^{2} y_i$, $x_i \in J$, $i = 0, 1, 2$, we compute

$$U_{1+c+d}x = \sum_{j=0}^{2} t^j E_j x_i = \sum_{i=0}^{2} t^i x_i,$$

which shows

$$J_i = \{x \in J \mid U_{1+c+d}x = t^i x \} = \{x \in J \mid U_{1+c+d}x = t^{-i} x \}. \quad (11)$$

Now let $i, j, l \in \{0, 1, 2\}$ and $x_i \in J_i$, $y_j \in J_j$, $z_l \in J_l$. Then the fundamental formula (1) imply

$$U_{1+c+d}u_i y_j = U_{1+c+d}u_i U_{1+c+d}u_i^{-1+c+d} y_j = U_{1+c+d}u_i U_{1+c+d}u_i^{-1+c+d} y_j$$

$$= U_{1+c+d}u_i t^{-i} y_j = t^{2i-j} U_{1+c+d}u_i y_j,$$

hence $U_{1+c+d}u_i y_j \in J_{2i-j}$. This proves (8). Similarly,

$$U_{1+c+d}\{x_i y_j z_l \} = U_{1+c+d}u_i u_j u_i t^{-i+c+d} y_j$$

$$= U_{1+c+d}u_i u_j u_i t^{-i+c+d} y_j = U_{1+c+d}u_i u_j t^{-i} y_j$$

$$= t^{i+j} \{x_i y_j z_l \},$$

which proves $\{x_i y_j z_l \} \in J_{i+j+l}$, hence (9). It remains to prove the first equation of (10) since the second one then follows after the substitution $c \rightarrow d$. For $x_i \in J_i$, $i = 0, 2$, we must show $V_{x_2, x_0} = 0$. Applying (3.13, 21), (3.13, 13) and (1), (4), (6), we first obtain $V_{c, x_0} = V_{c, x_0} = V_{c, x_0} - V_{U_{1+c+d}} = V_{c, x_0} = 0$ from (1), (6) and then $V_{x_2, x_0} = V_{x_2, x_0} = V_{x_2, x_0} - V_{U_{1+c+d}} = 0$ since $x_2 c x_0 \in J_0$ by (9). This completes the proof. \hfill \Box

### 34.3. Corollary.

Let $c$ be an idempotent in $J$ and put $d := 1_J - c$.

(a) For all $R \in k$-alg, there are natural identifications

$$< (J_R)_i (c_R) = J_i (c)_R \quad (i = 0, 1, 2).$$

(b) $d$ is an idempotent in $J$ satisfying $J_i (d) = J_{2-i} (c)$ for $i = 0, 1, 2$.

(c) The $k$-module $J_2 (c)$ (resp. $J_0 (c)$) is a Jordan algebra over $k$ with unit element $c$ (resp. $d$) whose $U$-operator is derived from the $U$-operator of $J$ by restriction. Moreover, $J_2 (c) \oplus J_0 (c)$ is a direct sum of ideals and a subalgebra of $J$.

(d) The Peirce components $J_i : = J_i (c)$ of $J$ ($i = 0, 1, 2$) satisfy the bilinear composition rules

$$J_i \circ J_i \subseteq J_i, \quad J_i \circ J_1 \subseteq J_1, \quad J_2 \circ J_0 = \{0\}, \quad J_1 \circ J_1 \subseteq J_2 \oplus J_0 \quad (1)$$

for $i = 0, 2$.

**Proof.** (a) This follows immediately from (34.2) and the fact that scalar extensions of $k$-modules commute with direct sums.
(b) This follows immediately from Thm. 34.2(a), (b).

c) We put \( c_2 := c, c_0 := d \) and let \( i = 0, 2 \). From (34.2.8) we deduce \( U_1 J_i \subseteq J_i \), so restricting the \( U \)-operator of \( J \) to \( J_i \) gives a quadratic map \( U : J_i \rightarrow \text{End}_k(J_i) \) which by Thm. 34.2 sends \( c_i \) to identity on \( J_i \). In this way, therefore, \( J_i \) becomes a para-quadratic algebra over \( k \), which is in fact a Jordan algebra since the defining identities (31.1.1), (31.1.12) hold not only on \( J_i \) but by (a) on all scalar extensions as well. By (34.2.8) we have \( U_1 J_0 + U_0 J_2 = \{0\} \), which together with (34.2.10) implies that \( J_2 \oplus J_0 \) is a direct sum of ideals. As such it is a Jordan algebra in its own right with identity element \( c_1 + c_0 = 1_J \), hence a subalgebra of \( J \).

d) For \( i = 0, 2, j = 0, 1, 2 \), we apply (34.2.9), (34.2.10) and obtain \( J_i \circ J_j \subseteq \{ J_i J_j J_j \} + \{ J_i J_2 J_j \} \subseteq J_j \) hence first two relations of (1), while the third one now follows by symmetry: \( J_2 \circ J_0 \subseteq J_0 \cap J_2 = \{0\} \). On the other hand, \( J_1 \circ J_1 \subseteq \{ J_1 J_2 J_1 \} + \{ J_1 J_0 J_1 \} \subseteq J_0 + J_2 \) by (34.2.9), giving also the fourth relation, and the proof of (1) is complete. \( \square \)

**Remark.** \( J_2(c) \), though a Jordan algebra, in general is not a subalgebra of \( J \); in fact, it is one if and only if \( c = 1_J \).

### 34.4. The Peirce decomposition in linear Jordan algebras.

Suppose \( k \) contains \( \frac{1}{2} \) and let \( c \) be an idempotent in \( J \). We claim

\[
J_i(c) = \{ x \in J \mid c \circ x = ix \} \quad (i = 0, 1, 2). \tag{1}
\]

By (34.2.9), (34.2.12), the left-hand side is contained in the right and we have equality for \( i = 1 \). Now assume \( i = 0, 2 \) and that \( x \in J \) satisfies \( c \circ x = ix \). Writing \( x = x_2 + x_0, x_j \in J_j(c) \) for \( j = 0, 1, 2 \), we conclude \( ix_2 + ix_1 + ix_0 = c \circ x = 2x_2 + x_1 \). For \( i = 0 \), this implies \( 2x_2 = x_1 = 0 \), hence \( x = x_0 \in J_0(c) \) since \( k \) contains \( \frac{1}{2} \). By the same token, \( i = 2 \) implies \( x_1 = 2x_0 = 0 \), hence \( x = x_2 \in J_2(c) \). This completes the proof.

Viewing \( J \) as a unital linear Jordan algebra over \( k \) via Thm. 31.3 with bilinear multiplication \( xy = \frac{1}{2}x \circ y = \frac{1}{2}V_x y \), the left multiplication operator of \( c \) in \( J \) is \( L_c = \frac{1}{2} V_c \), and (1) may be rewritten as

\[
J_i := J_i(c) = \{ x \in J \mid cx = \frac{i}{2}x \}, \quad (i = 0, 1, 2), \tag{2}
\]

so the Peirce components of \( c \) are basically the “eigenspaces” of \( L_c \) with respect to the “eigenvalues” \( 0, \frac{1}{2}, 1 \). For this reason, the \( i \)-th Peirce component of \( c, i = 0, 1, 2 \), in the classical literature is usually denoted by \( J_i(c) \). But we will never adhere to this convention. Instead we confine ourselves to rewriting the composition rules (34.3.1) in the language of linear Jordan algebras: for \( i = 0, 2 \) we have

\[
J_i^2 \subseteq J_i, \quad J_i J_1 \subseteq J_1, \quad J_2 J_0 = \{0\}, \quad J_1^2 \subseteq J_2 \oplus J_1.
\]

### 34.5. Proposition.

Let \( (M, q, e) \) be a pointed quadratic module over \( k \). An element \( c \in M \) is an elementary idempotent in \( J := J(M, q, e) \) (cf. Exc. 160) if and only if
(c, d) with \( d := e - c \) is a hyperbolic pair in the quadratic module \((M, q)\). In this case, \( d \) is an elementary idempotent of \( J \) as well and

\[
J_2(c) = kc, \quad J_1(c) = (kc \oplus kd)^\perp, \quad J_0(c) = kd,
\]

where “\( \perp \)” stands for orthogonal complementation relative to the bilinearization of \( q \), are the Peirce components of \( J \) relative to \( c \).

**Proof.** Write \( t \) for the trace and \( x \mapsto \bar{x} \) for the conjugation of \((M, q, e)\). If \((c, d)\) is a hyperbolic pair of \((M, q)\), then \( q(c) = 0 \) and \( t(c) = q(c, c + d) = 2q(c) + q(c, d) = 1 \). Thus \( c \in J \) is an elementary idempotent. Conversely, let this be so. Then \( q(d) = q(e - c) = 1 - t(c) + q(e) = 0 \) and \( q(c, d) = q(c, e - c) = t(c) - 2q(c) = 1 \). Thus \((c, d)\) is a hyperbolic pair of \((M, q)\). It remains to determine the Peirce components of \( J \) relative to \( c \). To begin with, let \( x \in J_2(c) \). Then \( 31.12.4 \) implies \( x = U x = q(c, \bar{x})c - q(c, x)e = x + t(x)c - q(c, x)e \), and \( 34.2.7 \) yields

\[
J_1(c) = \{ x \in M \mid t(x)c = q(c, x)e \}. \tag{2}
\]

Suppose first \( x \in J_1(c) \). Then \( 2 \) implies \( q(c, x) = t(c)q(c, x) = q(q(c, x)e) = q(t(x)c, c) = 2t(x)q(c) = 0 \), hence \( t(x)c = q(c, x)e = 0 \), forcing \( t(x) = 0 \) since \( c \) is unimodular, and then \( q(d, x) = t(x) - q(c, x) = 0 \). Thus \( x \in (kc \oplus kd)^\perp \). Conversely, let \( x \in (kc \oplus kd)^\perp \). Then \( q(c, x) = q(d, x) = 0 \) implies \( t(x) = q(c, x) + q(d, x) = 0 \), and \( 2 \) implies \( x \in J_1(c) \). \( \square \)

The Peirce decomposition of a Jordan algebra relative to a single idempotent is often not fine enough for the intended applications. We therefore wish to replace it by a Peirce decomposition relative to a complete orthogonal system of as many idempotents as possible. In order to accomplish this, we require a number of preparations that we are now going to address.

Orthogonality of a family of idempotents has been defined in \( 30.9 \) and Exc. \( 153 \) for arbitrary para-quadratic algebras. In the case of Jordan algebras, there is a simple characterization in terms of the Peirce decomposition.

**34.6. Proposition.** For idempotents \( c_1, c_2 \in J \), the following conditions are equivalent.

(i) \( c_1 \perp c_2 \).
(ii) \( c_2 \in J_0(c_1) \).
(iii) \( c_1 \in J_0(c_2) \).

**Proof.** Orthogonality being a symmetric relation on idempotents, it suffices to establish the equivalence of (i) and (ii). Combining \( 30.9.1 \) with \( 31.3.13 \), we see that (i) holds if and only if \( U_{c_1} c_2 = U_{c_2} c_1 = V_{c_1} c_2 = 0 \). In this case, \( 34.2.5 \) implies \( c_2 \in J_0(c_1) \). Conversely, suppose \( c_2 \in J_0(c_1) \). Then \( U_{c_1} c_2 = V_{c_1} c_2 = 0 \), but also \( U_{c_2} c_1 \in U_{J_0(c_1)} J_2(c_1) = \{ 0 \} \) by Cor. \( 34.3 \)(b). Thus (i) holds. \( \square \)
34.7. Corollary. A finite family \( (c_1, \ldots, c_r) \) \((r \in \mathbb{Z}, r > 0)\) of idempotents in \( J \) is an orthogonal system of idempotents if and only if \( c_i \perp c_j \) for \( 1 \leq i, j \leq r, \ i \neq j \).

**Proof.** Assume \( c_i \perp c_j \) for \( 1 \leq i, j \leq r, \ i \neq j \) and let \( i, j, l \in \{1, \ldots, r\} \). The first set of relations in Exc. 153 (3), holds by the definition of orthogonality (cf. (30.9.1)). For the second set, let \( i, j, l \) be mutually distinct. From Prop. 34.6 and (34.2.10) we deduce \( \{c_i c_j \} \in J_2(c_i)J_0(c_j)J \} = \{0\} \). Thus all of Exc. 153 (3) holds, so \( (c_1, \ldots, c_r) \) is an orthogonal system of idempotents. The converse is obvious., again by Exc. 153 (3).

34.8. Proposition. Let \( \Omega = (c_1, \ldots, c_r) \) be a complete orthogonal system of idempotents in \( J \) and define linear maps

\[
E_{ii} := E_{ii}(\Omega) := U_{c_i}, \quad E_{ij} := E_{ij}(\Omega) := U_{c_i c_j} \quad (1 \leq i, j \leq r, \ i \neq j).
\] (1)

Then \( E_{ij} = E_{ji} \) for \( 1 \leq i, j \leq r \), and the \( E_{ij}, \ 1 \leq i \leq j \leq r, \) are orthogonal projections of \( J \), called its Peirce projections relative to \( \Omega \), such that \( \sum_{1 \leq i \leq r} E_{ij} \) is the identity.

**Proof.** The first assertion is obvious, and we clearly have \( \sum_{i=1}^r E_{ij} = U_{\sum_i c_i} = U_{1_j} = 1_j \), so we need only show that the \( E_{ij}, \ 1 \leq i \leq j \leq r, \) are orthogonal projections. We do so in two steps.

1. Let \( 1 \leq i, j \leq r, \ i \neq j \). Exc. 153 (a) shows that \( c_i + c_j \in J \) is an idempotent, forcing \( J' := J_2(c_i + c_j) \) by Cor. 34.3 (b) to be a Jordan algebra with identity \( c_i + c_j \).

Applying Thm. 34.2 to \( J', c_i \) in place of \( J, c \), respectively, we see that \( E_{ii}, E_{ij}, E_{jj} \) are orthogonal projections on \( J' \) vanishing identically on \( J_1(c_i + c_j) \oplus J_0(c_i + c_j) \).

Hence they are orthogonal projections on all of \( J \) that map \( J \) to \( J' \).

2. The proof will be complete once we have shown

\[
E_{ij}E_{im} = 0 \quad (1 \leq i, j, l, m \leq r, \ \{i, j\} \neq \{l, m\}).
\] (2)

First suppose \( i = j \) in (2). By 1, we may assume \( l \neq m \) and \( i \notin \{l, m\} \). Then \( c_l \perp c_m \), which implies \( c_l + c_m \perp c_l \) by Prop. 34.6 and then

\[
E_{ii}E_{im} = E_{im}E_{ii} \subseteq U_{J_0(c_l + c_m)}J_0(c_l + c_m) + \{J_2(c_l + c_m)J_0(c_l + c_m)J \} = \{0\}.
\]

This shows (2) not only for \( i = j \) but also for \( l = m \). We are left with the case \( l \neq j, l \neq m \). By symmetry, we may assume \( i \notin \{l, m\} \), which implies

\[
E_{ij}E_{im} = \{c_iJ_2(c_l + c_m)e_j\} \subseteq \{J_0(c_l + c_m)J_2(c_l + c_m)J \} = \{0\}
\]

and completes the proof of (2).

34.9. Corollary. Let \( \Omega = (c_1, \ldots, c_r) \) be a complete orthogonal system of idempotents in \( J \) and put \( D := k \oplus \cdots \oplus k \in k-\text{alg} \) (r summands) as a direct sum of ideals. Then

\[
\Theta_\Omega : D \to \operatorname{End}_k(J), \quad x \mapsto U_{i=1}^r x c_i
\]
for \( x = \gamma_1 \oplus \cdots \oplus \gamma_r \in D, \, \gamma_i \in k, \, 1 \leq i \leq r \), is a quadratic map that is unital and permits composition:

\[
\Theta_\Omega(1_D) = 1_J, \quad \Theta_\Omega(xy) = \Theta_\Omega(x)\Theta_\Omega(y)
\]

for all \( x, y \in D \). In particular, \( \Theta_\Omega(x) \in \text{GL}(J) \) for all \( x \in D^\times \). Moreover, \( \Theta_\Omega \) is compatible with base change: \( \Theta_\Omega(x) \in \Omega_R \Omega_R := (c_{1R}, \ldots, c_{rR}), \) for all \( R \in k\text{-alg} \).

**Proof.** All assertions are obvious except, possibly, the property of \( \Theta_\Omega \) permitting composition. But this follows immediately from Prop. \ref{prop:composition} since \( \Theta_\Omega(x) = \sum_{i \leq j} \gamma_i \gamma_j E_{ij}(\Omega) \).

**34.10. Peirce triples.** By a *Peirce triple*, we mean a(n ordered) triple of unordered pairs of positive integers. Thus a Peirce triple has the form

\[
(ij, lm, np) := \{\{i, j\}, \{l, m\}, \{n, p\}\}
\]

for integers \( i, j, l, m, n, p > 0 \). A Peirce triple \( (ij, lm, np) \) will always be identified with the Peirce triple \( (np, lm, ij) \). It is said to be connected if (up to the identification just defined) it can be written in the form \( (ij, jm, np) \). For example, the Peirce triple \( (43, 23, 12) \) is connected but \( (54, 23, 12) \) is not.

**34.11. Theorem.** (Multiple Peirce decomposition). Let \( \Omega = (c_1, \ldots, c_r) \) be a complete orthogonal system of idempotents in \( J \).

(a) Setting \( J_{ij} := J_{ij}(\Omega) := \text{Im}(E_{ij}(\Omega)) \) in the notation of Prop. \ref{prop:composition} we have \( J_{ij} = J_{ji} \) for \( 1 \leq i, j \leq r \) and

\[
J = \bigoplus_{1 \leq i \leq j \leq r} J_{ij}
\]

as a direct sum of submodules, called the Peirce components of \( J \) relative to \( \Omega \). Furthermore, the following relations hold, for all \( i, j = 1, \ldots, r \):

\[
J_2(c_i) = J_{ii}, \quad J_1(c_i) = \sum_{j \neq i} J_{ij}, \quad J_0(c_i) = \sum_{l, m \neq i} J_{lm},
\]

\[
J_{ij} = J_1(c_i) \cap J_1(c_j) \quad (i \neq j).
\]

(b) More generally, if \( I \subseteq \{1, \ldots, r\} \), then \( c_I := \sum_{i \in I} c_i \) is an idempotent in \( J \) with the Peirce components

\[
J_2(c_I) = \sum_{i, j \in I} J_{ij}, \quad J_1(c_I) = \sum_{i \in I, j \notin I} J_{ij}, \quad J_0(c_I) = \sum_{i, j \notin I} J_{ij},
\]

(c) The composition rule

\[
\{J_{ij}J_{kl}I_{m}\} \subseteq J_{lm}
\]
holds for all \(i, j, l, m = 1, \ldots, r\). Moreover, if the Peirce triple \((ij, jl, ij)\) is connected, there exists a unique \(m = 1, \ldots, r\) such that \(ij = lm\), and we have
\[
U_{J_i}J_{jl} \subseteq J_{lm}. \tag{6}
\]

In particular,
\[
U_{J_i}J_{ij} \subseteq J_{ij}. \tag{7}
\]

Finally, if \((ij, lm, np)\) (resp. \((ij, lm, ij)\)) is not connected, then
\[
\{J_{ij}J_{lm}J_{np}\} = \{0\} \quad \text{(resp. } U_{J_i}J_{lm} = \{0\}). \tag{8}
\]

Proof. (a), (b). The first assertion of (a) and eqn. (1) follow immediately from Prop. 34.8, eqn. (3) is a consequence of (2), and (2) is a special case of (4). In order to complete the proof of (a) and (b), it therefore suffices to establish (4). To this end, we put \(d_i := 1_j - c_i = \sum_{d_j \in J_i} c_i\) and apply Thm. 34.2 to obtain
\[
J_2(c_l) = \text{Im}(U_{c_l}) = \text{Im}(\sum_{i, j \leq i} E_{ij}) = \sum_{i, j \leq i} J_{ij},
\]
\[
J_1(c_l) = \text{Im}(U_{c_l, d_l}) = \text{Im}(\sum_{i \in I, j \in I} E_{ij}) = \sum_{i \in I, j \in I} J_{ij},
\]
\[
J_0(c_l) = \text{Im}(U_{d_l}) = \sum_{i, j \in I} J_{ij}.
\]

(c) Let \(R := k[t_{1}^{\pm 1}, \ldots, t_{r}^{\pm 1}]\) the ring of Laurent polynomials over \(k\) in the variables \(t_1, \ldots, t_r\), which is free as a \(k\)-module with basis \((t_{1}^{0} \cdot \ldots \cdot t_{r}^{0})_{i_{1}, \ldots, i_{r} \in \mathbb{Z}}\). Thus the identifications of 31.2 imply
\[
J \subseteq J_R = \bigoplus_{i_{1}, \ldots, i_{r} \in \mathbb{Z}} (t_{1}^{i_{1}} \cdot \ldots \cdot t_{r}^{i_{r}} J),
\]
\[
\text{End}_k(J) \subseteq \text{End}_k(J_R) = \bigoplus_{i_{1}, \ldots, i_{r} \in \mathbb{Z}} (t_{1}^{i_{1}} \cdot \ldots \cdot t_{r}^{i_{r}} \text{End}_k(J)) \subseteq \text{End}_R(J_R)
\]
as direct sums of \(k\)-modules. We now claim
\[
w := \sum_{\lambda = 1}^{r} t_{\lambda} c_{\lambda} \in J_{R}^{\mathbb{N}} \quad \text{and} \quad w^{-1} = \sum_{\lambda = 1}^{r} t_{\lambda}^{-1} c_{\lambda}. \tag{9}
\]

Indeed, since \(t_{\lambda} \in R^{\mathbb{N}}\) for \(1 \leq \lambda \leq r\), Cor. 34.9 shows not only \(U_{w} \in \text{GL}(J_R)\) but also \(U_{w'} = U_{w}^{-1}\), where \(w' = \sum_{\lambda = 1}^{r} t_{\lambda}^{-1} c_{\lambda}\). Hence \(w \in J_{R}^{\mathbb{N}}\) by Prop. 33.2 and since \(c_{\lambda} \in J_{\lambda \lambda}\) by (2), we conclude
\[
U_{w}w' = \sum_{i \leq j} t_{i}t_{j}E_{ij} \sum_{\lambda} t_{\lambda}^{-1} c_{\lambda} = \sum_{i = 1}^{r} t_{i}^{-1} t_{i} c_{i} = \sum_{i = 1}^{r} t_{i} c_{i} = w,
\]
which in turn implies \( w' = U_w^{-1}w = w^{-1} \) by (33.2). Next we claim

\[
J_{ij} = \{ x \in J \mid U_w x = t_j x \} = \{ x \in J \mid U_{w^{-1}}x = t_i^{-1}t_j^{-1}x \}. 
\]  

(10)

Indeed, given \( x \in J \), the expansion \( U_w x = \sum_{i \leq j} t_i t_j E_{i,j} x \), where \( E_{i,j} x \in J_{i,j} \), combined with (1) yields the first equation of (10), while the second follows from the first. We now put

\[
T := \{ t_1^i \cdots t_r^i \mid i_1, \ldots, i_r \in \mathbb{Z} \}, \quad T_0 := \{ t_i t_j \mid 1 \leq i, j \leq r \}
\]

and claim

\( \ast \) Every \( t \in T \) such that \( U_w x = tx \) for some non-zero element \( x \in J \) belongs to \( T_0 \).

In order to see this, we write \( x = \sum_{i \leq j} x_{ij} \), \( x_{ij} \in J_{ij} \), and deduce

\[
\sum_{i \leq j} tx_{ij} = tx = U_w x = \sum_{i \leq j} t_i t_j x_{ij}
\]

from (10), and comparing Peirce components, the assertion follows. Now fix integers \( i, j, l, m, n, p = 1, \ldots, r \) and \( x \in J_{ij}, y \in J_{lm}, z \in J_{np} \). Then we claim

\[
U_w \{xyz\} = t_i t_j t_l^{-1}t_m^{-1} t_p \{xyz\}, \quad U_w U_{x,y} = t_i^2 t_j^2 t_l^{-1} t_m^{-1} U_{x,y}. 
\]

(11)  (12)

In order to prove (11), we apply (9), (10), (31.3.3) and obtain

\[
U_w \{xyz\} = U_w U_{x,z} U_w U_{w^{-1}y} = U_{w,x} U_{w,z} U_{w^{-1}y} = U_{t_i t_j t_l t_p} t_l^{-1} t_m^{-1} y,
\]

hence (11). Similarly,

\[
U_w U_{x,y} = U_w U_{x,z} U_w U_{w^{-1}y} = U_{t_i t_j t_l t_p} t_l^{-1} t_m^{-1} y,
\]

and this yields (12). Now (5) follows by specializing \( l = j, n = m = l, p = m \) in (11) and applying (10). Next suppose the Peirce triple \( (ij, j, i) \) is connected. By Exc. (178) below, there is a unique \( m = 1, \ldots, r \) such that \( ij = lm \), and specializing \( l = j, m = l \) in (12) gives \( t_i^2 t_j^2 t_l^{-1} t_m^{-1} = t_i t_j t_l t_p = t_i t_j^{-1} t_m \), hence (5), which for \( l = i \) specializes to (7). It remains to establish (8). To this end, assume first that \( (ij, lm, np) \) is not connected. If \( \{i,j\} \cap \{l,m\} = \emptyset = \{l,m\} \cap \{n,p\} \), then \( t_i t_j^{-1} t_m^{-1} t_p \not\in T_0 \), and (\( \ast \)) implies \( \{xyz\} = 0 \). Otherwise, since the \( k \)-module \( \{ J_{ij}, J_{lm}, J_{np} \} \) remains unaffected by the identification of Peirce triples described in 34.10, Exc. (178) below allows us to assume \( l = n = j, m = l, p = n \), with \( l \neq i, j, n \), which implies \( t_i t_j^{-1} t_m^{-1} t_p \not\in T_0 \), hence again \( \{xyz\} = 0 \). This proves the first part of (8). As to the second, assume that \( (ij, lm, ij) \) is not connected. If \( \{i,j\} \cap \{l,m\} = \emptyset \), the \( t_i^2 t_i^{-1} t_j t_m^{-1} \not\in T_0 \), and we conclude \( U_{x,y} = 0 \) from (\( \ast \)). Otherwise, we may assume \( l = j \), put \( m := l \) and have \( i \neq l \neq j \), hence \( t_i^2 t_j^{-1} t_m^{-1} = t_i^2 t_j^{-1} \not\in T_0 \). This again implies \( U_{x,y} = 0 \) and completes the proof of (8). □
34.12. **Corollary.** Let \( \Omega = (c_1, \ldots, c_r) \) be a complete orthogonal system of idempotents in \( J \).

(a) For \( R \in {\text{-alg}} \), \( \Omega_R := (c_1 R, \ldots, c_r R) \) is a complete orthogonal system of idempotents in \( J_R \) and there are canonical identifications
\[
(J_R)_{ij}(\Omega_R) = J_{ij}(\Omega)_R \quad (1 \leq i, j \leq r).
\]

(b) For \( 1 \leq i \leq r \), the \( k \)-module \( J_i(\Omega) \) is a Jordan algebra over \( k \) with unit element \( c_i \) whose \( U \)-operator is derived from the \( U \)-operator of \( J \) by means of restriction. Moreover \( \bigoplus_{i=1}^r J_i(\Omega) \) is a direct sum of ideals and a subalgebra of \( J \).

(c) The Peirce components of \( J \) relative to \( \Omega \) satisfy the bilinear composition rules
\[
J_{ij}(\Omega) \circ J_{jl}(\Omega) \subseteq J_{il}(\Omega) \quad J_{ij}(\Omega) \circ J_{ij}(\Omega) \subseteq J_{ii}(\Omega) + J_{jj}(\Omega)
\]
for \( 1 \leq i \leq j \leq l \leq r \).

**Proof.** This is established in exactly the same manner as Cor. 34.3 has been derived from Thm. 34.2. \( \square \)

**Exercises.**

175. Show that \( J \) is linear at \( c \), for every idempotent \( c \in J \).

176. Let \( c \in J \) be an idempotent and suppose \( v \in J_1(c) \) is invertible in \( J \). Prove that \( U_v \) via restriction induces an isotopy from \( J_2(c) \) onto \( J_0(c) \). Moreover, this isotopy is an isomorphism if and only if \( v^2 = 1_J \).

177. Let \( c \) be an idempotent in \( J \) and put \( J_i := J_i(c) \) for \( i = 0, 1, 2 \). Then prove that
\[
\phi: J_2 \rightarrow \text{End}_k(J_1), \quad x \mapsto V_x|J_1,
\]
is a homomorphism of Jordan algebras. Conclude that, if the Jordan algebra \( J_2 \) is simple and \( J_1 \neq \{0\} \), then \( J_2 \) is special.

**Remark.** By a theorem of McCrimmon [81], if \( J \) is simple, then so is \( J_2 \). Moreover, if \( c \neq 0, 1_J \), then \( J_1 \neq \{0\} \) by Cor. 34.3 (b). Thus for a simple Jordan algebra \( J \) and an idempotent \( c \neq 0, 1 \) in \( J \), the Jordan algebra \( J_2(c) \) is special.

178. Show for a Peirce triple \( T := (ij, lm, np) \) that the following conditions are equivalent.

(i) \( T \) is not connected.

(ii) Always up to the identification of [34.10] either \( \{i, j\} \cap \{l, m\} = \emptyset \) or
\[
T = (ij, jm, jp), \quad m \neq i, j, p.
\]

Conclude that a Peirce triple \( (ij, jl, ij) \) is connected if and only if \( l = i \) or \( l = j \), in which case there is a unique positive integer \( m \) such that \( ij = lm \).

179. The multiple Peirce decomposition for alternative algebras (cf. Schafer [114]). Let \( A \) be a unital alternative algebra over \( k \) and \( \Omega := (c_1, \ldots, c_r) \) a complete orthogonal system of idempotents in \( A \).
260 5 Jordan algebras

(a) Put
\[ E_{ij} := E_{ij}(\Omega) := L_{v} R_{vj} \quad (1 \leq i, j \leq r) \]  
(2) ELCEAR

and show that \((E_{ij})_{1 \leq i, j \leq r}\) is a family of orthogonal projections of \(A\) whose sum is the identity. Conclude

\[ A = \bigoplus_{1 \leq i, j \leq r} A_{ij} \]  
(3) PECOA

as a direct sum of \(k\)-modules, where \(A_{ij} := A_{ij}(\Omega) = \text{Im}(E_{ij})\) for \(1 \leq i, j \leq r\). The \(A_{ij}\) are called the Peirce components of \(A\) relative to \(\Omega\).

(b) Show

\[ A_{ij} = \{ x \in A \mid c_{j} x = \delta_{ji} x, \quad x c_{j} = \delta_{ji} x \quad (1 \leq l \leq r) \} \]

(4) DEPECO

for \(1 \leq i, j \leq r\).

(c) Prove that the Peirce components of \(A\) relative to \(\Omega\) satisfy the following composition rules, for all \(i, j, l, m = 1, \ldots, r\).

\[ A_{ij} A_{jl} \subseteq A_{il}, \]
(5) A1JAJM

\[ A_{ij}^{l} \subseteq A_{jl}, \]
(6) A1JAIJ

\[ A_{ij} A_{lm} = \{ 0 \} \quad (j \neq l, \quad (i, j) \neq (l, m)) \]  
(7) A1JALM

Finally, prove \(x^{2} = 0\) for all \(x \in A_{ij}, 1 \leq i, j \leq r, i \neq j\).

(d) Note by Exc. [153] (b) that \(\Omega\) is a complete orthogonal system of idempotents in \(A^{(+)}\), with Peirce components \(A_{ij}^{(+)} := A_{ij}^{(+)}(\Omega) \quad (1 \leq i \leq j \leq r)\), and prove

\[ A_{ij}^{(+)} = A_{il} \quad (1 \leq i \leq r), \quad A_{ij}^{(+)} = A_{ij} \oplus A_{jl} \quad (1 \leq i < j \leq r). \]

PR.CONCOM 180. Connectedness in complete orthogonal systems of idempotents. (Jacobson [45 Prop. 5.3.3])

Let \(\Omega = (c_{1}, \ldots, c_{r})\) be a complete orthogonal system of idempotents in \(J\), with Peirce components \(J_{ij} = J_{ij}(\Omega), 1 \leq i, j \leq r\). Fix indices \(i, j, l, m = 1, \ldots, r\) with \(i \neq j\) and prove:

(a) For \(v_{ij} \in J_{ij}\), the following conditions are equivalent.

(i) \(v_{ij} \in J_{ij}(c_{i} + c_{j})^{*}\).
(ii) \(U_{ij} J_{ij}^{*} \subseteq J_{ij}^{*}, U_{ij}^{*} J_{ij} \subseteq J_{ij}^{*}\).
(iii) \(U_{ij} c_{i} \in J_{ij}^{*}, U_{ij} c_{j} \in J_{ij}^{*}\). 

In this case, \(c_{i}\) and \(c_{j}\) are said to be connected by \(v_{ij}\). We say \(c_{i}\) and \(c_{j}\) are connected if \(v_{ij} \in J_{ij}\) exists connecting \(c_{i}\) and \(c_{j}\). And finally, we say \(\Omega\) is connected if \(c_{i}\) and \(c_{j}\) are connected, for all \(i, j = 1, \ldots, r\) distinct.

(b) For \(v_{ij} \in J_{ij}\), the following conditions are equivalent.

(i) \(v_{ij}^{2} = c_{i} + c_{j}\).
(ii) \(U_{ij} c_{i} = c_{j}, U_{ij} c_{j} = c_{i}\)

In this case, \(c_{i}\) and \(c_{j}\) are said to be strongly connected by \(v_{ij}\). We say \(c_{i}\) and \(c_{j}\) are strongly connected if \(v_{ij} \in J_{ij}\) exists strongly connecting \(c_{i}\) and \(c_{j}\). And finally, we say \(\Omega\) is strongly connected if \(c_{i}\) and \(c_{j}\) are strongly connected, for all \(i, j = 1, \ldots, r\) distinct.

(c) Let \(1 \leq l \leq r\) and assume \(i \neq l \neq j\). If \(c_{i}\) and \(c_{j}\) are (strongly) connected by \(v_{ij} \in J_{ij}\), and \(c_{j}\) and \(c_{i}\) are (strongly) connected by \(v_{jl} \in J_{jl}\), then \(c_{i}\) and \(c_{j}\) are (strongly) connected by \(v_{ij} \circ v_{jl} \in J_{ijl}\).
181. Isotopes and complete orthogonal systems of idempotents. (Jacobson [45, Prop. 5.3.4]) Let
\( \Omega = (c_1, \ldots, c_r) \) be a complete orthogonal system of idempotents in \( J \), with Peirce components
\( J_{ij} := J_{ij}(\Omega) \), \( 1 \leq i, j \leq r \). Following Cor. 34.12 (b), consider the subalgebra of
\( J \) defined by
\[
\text{Diag}_\Omega(J) := \bigoplus_{i=1}^r J_{ii}
\]
as a direct sum of ideals. For \( 1 \leq i \leq r \), let \( p_i \in J_{ii} \) and put
\[
p := \sum_{i=1}^r p_i \in \text{Diag}_\Omega(J)^\times \subseteq J^\times.
\] (9) DIAINV

(a) Put \( c_i(p) := p_i^{-1} \in J_{ii} \) (the inverse of \( p_i \) in \( J_{ii} \)) for \( 1 \leq i \leq r \) and show that
\[
\Omega(p) := (c_1(p), \ldots, c_r(p))
\]
is a complete orthogonal system of idempotents in the isotope \( J(p) \) such that
\[
J_{ij}^{(p)} := (J(p))_{ij}(\Omega(p)) = J_{ij}
\]
for \( 1 \leq i, j \leq r \). In particular, \( \text{Diag}_{\Omega(p)}(J^{(p)}) = \text{Diag}_\Omega(J)^{(p)} \). (10) PECOP

(b) Let also \( q_i \in J_{ii}^\times \) for \( 1 \leq i \leq r \) and \( q := \sum_{i=1}^r q_i \in \text{Diag}_\Omega(J)^\times \). Then show \( (\Omega(p))^{(p)} = \Omega^{(p)} \).

(c) Assume \( c_1 \) and \( c_i \) are connected for \( 2 \leq i \leq r \) (cf. Exc. 180). Show that there exist \( p_i \in J_{ii}^\times \), \( 1 \leq i \leq r \), such that \( c_i(p) \) and \( c_i^{(p)} \) with \( p := \sum_{i=1}^r p_i \) are strongly connected in their capacity as members of the complete orthogonal system \( \Omega^{(p)} \) of idempotents in \( J^{(p)} \).

182. Lifting of complete orthogonal systems of idempotents. Let \( \varphi: J \to J' \) be a surjective homomorphism of Jordan algebras and suppose \( \text{Ker}(\varphi) \subseteq J \) is a nil ideal. Show that every complete orthogonal system \( (c_1', \ldots, c_r') \) of idempotents in \( J' \) can be lifted to \( J \): there exists a complete orthogonal system \( (c_1, \ldots, c_r) \) of idempotents in \( J \) such that \( \varphi(c_i) = c_i' \) for \( 1 \leq i \leq r \).

\( (M, q, e) \) be a non-zero pointed quadratic module over a field \( F \) and suppose \( q \) is non-degenerate. Show that the Jordan algebra \( J(M, q, e) \) is either simple or isomorphic to \( (F \oplus F)^{(+)}. \)
Chapter 6
Cubic Jordan algebras

Just as octonions fit naturally into the more general picture of composition algebras, the most efficient approach to Albert algebras consists in viewing them as special cases of cubic Jordan algebras. These, in turn, are best understood by means of cubic norm structures which, therefore, will have to be studied first. In the subsequent sections, we derive their most basic properties before we will be able to investigate cubic Jordan algebras in general, and Albert algebras in particular, over arbitrary commutative rings.

35. From cubic norm structures to cubic Jordan algebras

The natural habitat of cubic Jordan algebras is provided by the concept of a cubic norm structure, which will be introduced and investigated in the first half of the present section by closely following the treatment of McCrimmon [77]. This investigation will then be used in the second half to initiate the study of cubic Jordan algebras. We conclude the section by showing that the categories of cubic norm structures and of cubic Jordan algebras are isomorphic.

Throughout \( k \) stands for an arbitrary commutative ring. Relaxing on the conventions of the previous section, we do not distinguish anymore between the notation for a polynomial law \( f : M \to N \) and that for its induced set maps \( f_R : M_R \to N_R, R \in k\text{-alg} \). We begin with a preliminary concept of a more technical nature that will be included here only for convenience.

35.1. Cubic arrays. By a cubic array over \( k \) we mean a \( k \)-module \( X \) together with

- a distinguished element \( 1_X \in X \) (the base point),
- a quadratic map \( \sharp = \sharp_X : X \to X, x \mapsto x^\sharp \) (the adjoint, dependence on \( X \) most of the time being understood),
- a cubic form \( N_X : X \to k \) (the norm)

such that the following conditions are fulfilled.

(i) \( 1_X \in X \) is unimodular.
(ii) The base point identities hold:

\[
1_X^\sharp = 1_X, \quad N_X(1_X) = 1. \tag{1}
\]

Given another cubic array \( X' \) over \( k \), a homomorphism from \( X \) to \( X' \) is defined as a linear map \( \varphi : X \to X' \) preserving base points, adjoints and norms: \( \varphi(1_X) = 1_{X'}, \varphi(x^\sharp) = \varphi(x)^{\sharp_{X'}} \) for all \( x \in X \), and \( N_{X'} \circ \varphi = N_X \) as polynomial laws over \( k \). In
this way, we obtain the category of cubic arrays over $k$, denoted by $k$-	exttt{cuar}. For $R \in k$-	exttt{alg}, the $R$-module $X_R$ together with the base point $1_{X_R} := (1_X)_R \in X_R$, the adjoint $\sharp = \sharp_{X_R} = (\sharp_X)_R : X_R \to X_R$ defined as the $R$-quadratic extension of the adjoint of $X$, and the norm $N_{X_R} := N_X \otimes R : X_R \to R$ as a cubic form over $R$ is a cubic array over $R$, called the \textit{scalar extension} or \textit{base change} of $X$ from $k$ to $R$.

### 35.2. Traces of cubic arrays

Let $X$ be a cubic array over $k$. We write

$$x \times y = (D^2)(x,y) = (x+y)^2 \mp x^2 - y^2$$

for the bilinearization of the adjoint and, with regard to the norm, combine the notational simplifications of Exc. 58 with (13.14.2) and Cor. 13.20 to obtain not only

$$N_X(x,y) = (DN_X)(x,y) = (D^2N_X)(y,x) = (\partial_xN_X)(x)$$

but also

$$N_X(x,y,z) = (\partial_x\partial_yN_X)(x) = (\Pi^{(1,1,1)}N_X)(x,y,z)$$

for the total linearization of the cubic form $N_X$, which is therefore trilinear and totally symmetric in $x,y,z$ (cf. 13.8(c)). Recall further from Exc. 58 that

$$N_X(x+y) = N_X(x) + N_X(x,y) + N_X(y,x) + N_X(y),$$

$$N_X(x,y,z) = N_X(x+y,z) - N_X(x,z) - N_X(y,z).$$

The linear map

$$T_X : X \to k, \quad y \mapsto T_X(y) := N_X(1_X,y),$$

is called the \textit{linear trace} of $X$, while the quadratic form

$$S_X : X \to k, \quad y \mapsto S_X(y) := N_X(y,1_X)$$

is called the \textit{quadratic trace} of $X$. And finally, we define the \textit{bilinear trace} of $X$ as the symmetric bilinear form $T_X : X \times X \to k$ given by

$$T_X(y,z) = (\partial_xN_X)(1_X)(\partial_yN_X)(1_X) - (\partial_x\partial_yN_X)(1_X)$$

$$= N_X(1_X,y)N_X(1_X,z) - N_X(x,y,z,1_X),$$

which up to a sign agrees with the logarithmic Hessian of $N_X$ at $1_X$:

$$T_X(y,z) = -(\partial_y\partial_z\log N_X)(1_X) = -\partial_y\left(\frac{\partial_zN_X}{N_X}\right)(1_X).$$

In view of 5, 6, we may rewrite 7 as

$$T_X(y,z) = T_X(y)T_X(z) - S_X(y,z).$$
Combining all this with Euler’s differential equation (13.14.3) and (35.1.1), we obtain

\[ T_X(1_X) = S_X(1_X) = 3, \quad T_X(y, 1_X) = T_X(y) \]  \tag{11} \]

since (5) and (7) yield

\[ S_X(y, 1_X) = N_X(y, 1_X, 1_X) = N(1_X, 1_X, y) = 2N(1_X, y), \]  \tag{12} \]

If \( \varphi : X \to X' \) is a homomorphism of cubic arrays, then the chain rule (13.15.4) and (5) yield

\[ N_{X'}(\varphi(x), \varphi(y)) = N_X(x, y), \quad N_{X'}(\varphi(x), \varphi(y), \varphi(z)) = N_X(x, y, z). \]  \tag{13} \]

Combining this with (6–8) and the property of \( \varphi \) to preserve base points, we conclude that \( \varphi \) preserves (bi-)linear and quadratic traces:

\[ T_{X'}(\varphi(y)) = T_X(y), \quad T_{X'}(\varphi(y), \varphi(z)) = T_X(y, z), \quad S_{X'}(\varphi(y)) = S_X(y). \]  \tag{14} \]

### 35.3. Regular elements and non-singularity.

Let \( X \) be a cubic array over \( k \).

(a) An element \( x \in X \) is said to be **regular** if \( N_X(x) \in k \) is invertible.

(b) \( X \) is said to be **non-singular** if it is finitely generated projective as a \( k \)-module and its bilinear trace is non-singular as a symmetric bilinear form, i.e., if it induces a linear isomorphism from \( X \) onto its dual module \( X^* \) in the usual way.

Both notions defined in (a), (b), respectively, are invariant under base change: if \( x \in X \) is regular, then so is \( x_R \in X_R \), and if \( X \) is non-singular, then so is \( X_R \), for all \( R \in k\text{-alg} \).

### 35.4. The concept of a cubic norm structure.

By a **cubic norm structure** over \( k \) we mean a cubic \( k \)-array \( X \) satisfying the following identities **strictly**, i.e., in all scalar extensions:

\[
\begin{align*}
1 \times x &= T_X(x)1_X - x \quad &\text{(unit identity)}, \tag{1} \\
N_X(x, y) &= T_X(x^4, y) \quad &\text{(gradient identity)}, \tag{2} \\
x^3 &= N_X(x)x \quad &\text{(adjoint identity)}. \tag{3}
\end{align*}
\]

A homomorphism of cubic norm structures is defined as a homomorphism of them as cubic arrays. Thus cubic norm structures over \( k \) form a full subcategory, denoted by \( k\text{-cuno} \), of \( k\text{-cuar} \). By definition, cubic norm structures are stable under base change, so if \( X \) is a cubic norm structure over \( k \), then the cubic array \( X_R \) over \( R \) is, in fact, a cubic norm structure, for all \( R \in k\text{-alg} \).

### 35.5. Cubic norm substructures.

Let \( X \) be a cubic array over \( k \). By a **cubic subarray** of \( X \) we mean a cubic array \( Y \) such that \( Y \subseteq X \) is a \( k \)-submodule and the inclusion \( i : Y \to X \) is a homomorphism of cubic arrays. This is equivalent to requiring
(i) $1_X \in Y$, (ii) $Y^2 \subseteq Y$, i.e., $Y$ is stabilized by the adjoint of $X$, and (iii) $N_X \circ i = N_Y$ as polynomial laws over $k$, i.e., $(N_X)_R \circ i_R = (N_Y)_R$ as set maps $Y_R \rightarrow R$, for all $R \in k\text{-algebra}$. Thus any submodule $Y$ of $X$, with corresponding inclusion $i : Y \rightarrow X$, that contains $1_X$ and is stabilized by the adjoint of $X$ may canonically be regarded as a cubic subarray of $X$, with base point $1_Y = 1_X$, adjoint $\mathcal{A} : Y \rightarrow Y$ given by restricting the adjoint $\mathcal{A} : X \rightarrow X$ of $X$ to $Y$, and norm $N_Y := N_X|_Y := N_X \circ i$. In this case, the (bi-)linear and quadratic trace of $Y$ by \(35.2\) is just the corresponding object of $X$ restricted to $Y$ (resp. to $Y \times Y$).

Now suppose $X$ is a cubic norm structure over $k$ and let $Y \subseteq X$ be a cubic subarray. Then it follows either from Cor.\[3.9\] or from Exc.\[186\] that $Y$ is, in fact, a cubic norm structure, called a **cubic norm substructure** of $X$. If $E \subseteq X$ is an arbitrary subset, the smallest cubic norm substructure of $X$ containing $E$ is called the **cubic norm substructure generated by** $E$.

Our next aim will be to derive a number of basic identities for cubic norm structures. In order to do so, we require two preparations, the first one connecting cubic norm structures with para-quadratic algebras, the second one spelling out a sufficient condition for all regular elements of a cubic array to be unimodular.

### 35.6. Connecting with para-quadratic algebras.

Let $X$ be a cubic array over $k$. We define a $U$-operator, i.e., a quadratic map $U : X \rightarrow \text{End}_k(X)$, $x \mapsto U_x$, by

\[ U_x y := T_X(x, y)x - \lambda^2 \times y \quad (x, y \in X), \tag{1} \]

which in analogy to \(30.13\), \(30.15\) linearizes to the associated triple product

\[ \{xyz\} := V_{1, 2} z := U_{1, 2} y = T_X(x, y)z + T_X(y, z)x - (z \times x) \times y \tag{2} \]

for $x, y, z \in X$. Moreover, if $X$ is a cubic norm structure, then the unit identity \(35.4\) shows $U_{1_X} = 1_X$. Hence the $k$-module $X$ together with the $U$-operator \(1\) and the base point $1_X \in X$ forms a para-quadratic algebra over $k$, which we denote by $J(X)$ and will show in due course to be Jordan algebra. Passing from $X$ to $J(X)$ is clearly compatible with base change: $J(X_R) = J(X)_R$ for all $R \in k\text{-algebra}$.

### 35.7. Lemma.

Let $X$ be a cubic array over $k$ such that the identity

\[ \{xx^2y\} = 2N_X(x)y \]

holds strictly. Then every regular element of $X$ is unimodular.

**Proof.** Since $1_X \in X$ is unimodular by definition, there exists a linear form $\lambda : X \rightarrow k$ such that $\lambda(1_X) = 1$. Now suppose $x \in X$ is regular. Thanks to Euler’s differential equation combined with the hypothesis of the lemma, the linear form

\[ \lambda_x : X \rightarrow k, \quad y \mapsto N_X(x)^{-1}(N_X(x, y) - \lambda((yy^21_X))) \]

satisfies $\lambda_x(x) = 1$. Hence $x$ is unimodular. \(\square\)
35.8. Basic identities for cubic norm structures. Let \( X \) be a cubic norm structure over \( k \). Using the abbreviations \( 1 := 1_X, N := N_X, T := T_X, S := S_X \), we claim that the following identities hold strictly in \( X \) (in compiling the list below, we do not hesitate to include identities that have been introduced or derived earlier).
\[1^2 = 1, \quad N(1) = 1, \quad (1)\]
\[T(1) = S(1) = 3, \quad T(y, 1) = T(y), \quad S(y, 1) = 2T(y), \quad (2)\]
\[1 \times x = T(x)1 - x, \quad (3)\]
\[N(x, y) = T(x^2, y), \quad (4)\]
\[x^2 = N(x)x, \quad (5)\]
\[N(x + y) = N(x) + T(x^2, y) + T(x, y^2) + N(y), \quad (6)\]
\[T(x \times y, z) = T(x, y \times z), \quad (7)\]
\[x^2 \times (x \times y) = N(x)y + T(x^2, y)x, \quad (8)\]
\[(x \times y) \times (x \times z) + x^2 \times (y \times z) = \]
\[= T(x^2, y)z + T(x^4, z)y + T(x \times y, z)x, \quad (9)\]
\[x^2 \times y^2 + (x \times y)^2 = T(x^2, y)y + T(x, y^2)x, \quad (10)\]
\[T(x^2, x) = 3N(x), \quad (11)\]
\[S(x) = T(x^2), \quad (12)\]
\[S(x, y) = T(x \times y) = T(x)T(y) - T(x, y), \quad (13)\]
\[x^2 \times x = (T(x)S(x) - N(x))1 - S(x)x - T(x)x^2, \quad (14)\]
\[U_{xy} = T(x)yx - x^2 \times y, \quad (15)\]
\[U_x(x \times y) = T(x^2, y)x - N(x)y, \quad (16)\]
\[{xx^2y} = 2N(x)y, \quad (17)\]
\[N(x^2) = N(x)^2, \quad (18)\]
\[x \times (x^2 \times y) = N(x)y + T(x, y)x^2, \quad (19)\]
\[(U_{xy})^2 = U_x y^2 = T(x^2, y^2)x^2 - N(x)x \times y^2, \quad (20)\]
\[N(U_{xy}) = N(x)^2N(y), \quad (21)\]
\[x^2 = x^2 - T(x)x + S(x)1, \quad (22)\]
\[x \times y = y \times x = T(x)y - T(y)x + (T(x)T(y) - T(x, y))1, \quad (23)\]
\[T(x \circ y) = 2T(x, y), \quad (24)\]
\[(x \times y) \times (z \times w) + (y \times z) \times (x \times w) + (z \times x) \times (y \times w)\]
\[= T(x \times y, z)w + T(y \times z, w)x + T(z \times w, x)y + T(w \times x, y)z, \quad (25)\]
\[x \times (y \times (x \times z)) = T(x, y)yx \times z + T(x^2, z)y + T(y, z)x^2 - (x^2 \times y) \times z\]
\[= (U_{xy})y \times z + T(x^2, z)y + T(y, z)x^2, \quad (26)\]
\[x \times (y \times (z \times w)) + z \times (y \times (w \times x)) + w \times (y \times (x \times z))\]
\[= T(x, y)z \times w + T(z, y)w \times x + T(w, y)x \times z + T(x \times z, w)y, \quad (27)\]
\[x \times (x \times y) = (T(x)S(x, y) + S(x)T(y) - T(x^2, y))1 - \]
\[S(x, y)x - S(x)y - T(x)x \times y - T(y)x^2 - x^2 \times y, \quad (28)\]
\[N(x \times y) = T(x^2, y)T(x^2, y) - N(x)N(y), \quad (29)\]
\[\{xyz\} = V_{xy}z = U_{xz}y = T(x, y)z + T(y, z)x - (z \times x) \times y, \quad (30)\]
\[T(U_xz, z) = T(y, U_zz), \quad (31)\]
\[T \{xyz\}, w) = T(z, \{xyw\}), \quad (32)\]
\[T(x \circ y, z) = T(x, y \circ z). \quad (33)\]
Proof. It clearly suffices to verify these identities for all \( x, y, z, w \in X \). Moreover, thanks to Prop. [13.22], we may always assume if necessary that some of the variables involved are regular. Now, while the base point identities \([1]\) are valid even in arbitrary cubic arrays and \([3] - [5]\) belong to the very definition of a cubic norm structure, \([4]\) has been observed already in \([35.2.11], [35.2.12]\). Next, combining \([35.2.9]\) with the gradient identity \([4]\), we obtain \([6]\). Differentiating the gradient identity gives \( T(x, y, z) = N(x, y, z) \), which is totally symmetric in \( x, y, z \). Hence \([7]\) follows. To establish \([8]\), we differentiate the adjoint identity \([5]\) by making use of the chain and the product rule. Linearizing still further and using \([7]\) yields \([9]\), while \([10]\) follows from \([5]\) combined with the second order chain and product rules \([13.15.9], [13.15.10]\). To derive \([11]\), we combine the gradient identity \([4]\) with Euler’s differential equation \([13.3]\). The gradient identity \([1] \) for \( y = 1 \) and \([2]\) imply \([12]\). To establish \([13]\), we linearize \([12]\) and apply \([35.2.10]\). Similarly, specializing \( y = 1 \) in \([8]\) and observing \([3]\), we obtain \([14]\), while \([15]\) is just a repetition of \([35.6.1]\). To derive \([16]\), we combine \([7]\) with \([1], [8]\) and conclude \( U_{\lambda}(x \times y) = T(x, x \times y)y - x^2 \times (x \times y) = T(x, x \times y)x - N(x/y - T(x, y)x) \), hence \([16]\) since \( x \times x = 2x^2 \). Next, \([2], [8]\) and \([11]\) immediately imply \([17]\). Combining this with Lemma \([35.7]\), we can therefore conclude that all regular elements of \( X \) are unimodular. To establish \([18]\), we assume that \( x \) is regular, apply the adjoint identity \([5]\) and obtain

\[
N(x^2)x^2 = x^{\sharp\sharp} = N(x)^2x^2. \tag{34}
\]

Taking adjoints again, we deduce \( N(x^2)x = N(x)^4x \), hence \( N(x^2)^2 = N(x)^4 \in k^\times \) since \( x \) is unimodular. This shows that \( x^\sharp \) is regular, and \([18]\) follows from \([34]\). Turning to \([19]\), we again assume that \( x \) is regular, replace \( x \) by \( x^\sharp \) in \([8]\), observe \([18]\) and obtain \( N(x)x \times (x^2 \times y) = N(x^2)y + N(x)T(x, y)x^2 = N(x)(N(x)y + T(x, y)x^2) \), hence \([19]\). Now \([20]\) follows by expanding the left-hand side and observing \([19], [10]\) as well as the adjoint identity \([5]\). In \([21]\), we may assume that \( U_{\lambda}y \) is regular since \( U_1 = 1 \). Then \([20]\) and the adjoint identity yield \( N(U_{\lambda}y) = (U_{\lambda}y)^{\sharp\sharp} = U_{\lambda}y^{\sharp\sharp} = N(x)^2 N(y) U_{\lambda}y \), so the assertion follows from the unimodularity of \( U_{\lambda}y \). To derive \([22]\), we note that \( x^2 = U_1X = T(x, 1)x - x \times 1 \), whence the unit identity \([3]\) and \([12]\) lead to the desired conclusion. \([23]\) follows immediately from linearizing \([22]\) and observing \([13]\). Combining \([23]\) with \([13]\), we deduce

\[
T(x)T(y) - T(x, y) = T(x \circ y) = T(x \circ y) - 2T(x)T(y) + 3(T(x)T(y) - T(x, y)),
\]

hence \([24]\). Next, linearizing \([9]\), we obtain \( (w \times y) \times (x \times z) + (x \times y) \times (w \times z) + (x \times w) \times (y \times z) = T(x \times w, z) + T(y, x \times z) + T(x, y \times z) \), hence \([25]\) follows. Similarly, \([19]\) and \([4]\) imply \( z \times (x^2 \times y) + x \times ((x \times z) \times y) = T(x^2, z) \), hence \([26]\) gives \( x \times (y \times (w \times z)) + w \times (y \times (x \times z)) = T(w, y)x \times z + T(x, y)w \times z + T(x \times w, y)x \times z + T(y, z)x \times w - ((x \times w) \times y) \times z \), and after interchanging \( w \) with \( z \), we obtain \([27]\). Similarly, \([14]\) implies \( (x \times y) \times x \times x^2 \times y = T(y)S(x) + T(x)S(y) - T(x^2, y) \), hence \([28]\). Relation \([29]\) is less obvious. With independent indeterminates \( s, t \), we apply
\[ N(s^2x^2 + stx + y + t^2y^2) = N((sx + ty)^2) = N(sx + ty)^2 \]
\[ = (s^2N(x) + s^2tT(x^2, y) + stT(x, y^2) + t^2N(y))^2. \]

Expanding the very left-hand side by means of Exc. 58, (6), we conclude
\[ N(x \times y) + T(x^2 \times (x \times y), y^2) = 2N(x)N(y) + 2T(x^2, y)T(x, y^2), \]
where the second summand on the left by (8) and the Euler differential equation (11) agrees with \( N(x)T(y, x^2) + T(x^2, y)T(x, y^2) = 3N(x)N(y) + T(x^2, y)T(x, y^2). \) Hence (29) holds. (30) has already been noted in (35.6.2). To derive (31), we expand the left-hand side by (15) and, using (7), obtain the expression \( T(Ux, z) = T(T(x, y)x - x^2 \times y, z) = T(x, y)T(x, z) - T(x^2, y \times z), \) which is symmetric in \( y, z; \) hence (31) holds. Similarly, (30) yields \( T((xy), w) = T(x, y)T(z, w) + T(y, z)T(x, w) - T((z \times x) \times y, w), \) which by (7) remains unchanged under the substitution \( x \leftrightarrow y, z \leftrightarrow w. \) This yields (32), while (33) follows from (23) and the fact that the right-hand side of \( T(x \circ y, z) = T(x \times y, z) + T(x)T(y, z) + T(y)T(x, z) - T((T(x)T(y) - T(x, y))1, z) = T(x \times y, z) + T(x)T(y, z) + T(z)T(x, y) - T(x)T(y)T(z) \) is totally symmetric in \( x, y, z. \) \[ \square \]

After these preparations, we are ready for the first main result of this section.

35.9. **Theorem** (McCracken [77]). *Let \( X \) be a cubic norm structure over \( k. \) Then the para-quadratic algebra \( J(X) \) of 35.6 with base point \( 1_X \) and \( U \)-operator given by*

\[ U_{xy} = T_X(x, y)x - x^2 \times y \quad \text{(1)} \]

*is a Jordan algebra over \( k \) such that the identities*

\[ x^3 - TX(x)x^2 + S_X(x)x - N_X(x)1_X = 0 = x^2 - T_X(x)x^3 + S_X(x)x^2 - N_X(x)x, \quad \text{(2)} \]

\[ U_{x^2} = N_X(x)x, \quad U_{x^2} = N_X(x)^21_X, \quad \text{(3)} \]

*hold strictly in \( J(X). \) We call \( J(X) \) the Jordan algebra associated with or corresponding to \( X. \)*

**Proof.** For \( J = J(X) \) to be a Jordan algebra we must show that the identities

\[ U_{1x} x = x, \quad \text{(4)} \]
\[ U_{xy} z = U_x U_y U_z, \quad \text{(5)} \]
\[ U_x \{ yz \} = \{ xy U_z \} \quad \text{(6)} \]

hold for all \( x, y, z \in X. \) Here (4) follows immediately from the unit identity (35.8.3). To establish (5), we abbreviate \( 1 := 1_X, N := N_X, T := T_X, S := S_X \) and first combine (35.8.19) with (35.8.7) to conclude
Next we expand the left-hand side of (5), using the definition of the $U$-operator (1) and (35.8.20). A short computation gives

$$U_{1,2} = (T(x,y)T(x,z) - T(x^2, y)T(x,z))U_{xy}$$

$$- T(x^2, y^2)x^2 + N(x)(x^2) \times z.$$

Similarly, expanding the right-hand side of (5) and applying (35.8.11), (35.8.16), (35.8.19), we obtain

$$U_{1,2} = (T(x,y)T(x,z) - T(x^2, y)T(x,z))U_{xy} + N(x)T(y^2, x)$$

$$+ N(x)T(x,z)y^2 - x^2 \times (y^2 \times (x^2) \times z).$$

To establish (5), we therefore have to prove

$$x^2 \times (y^2 \times (x^2) \times z) = N(x)T(y^2, x) + N(x)T(x,z)y^2$$

$$+ T(x^2, y^2)x^2 + N(x)(x^2) \times z.$$

But this follows immediately from (35.8.26) combined with the adjoint identity (35.8.13). Finally, we must prove (6), which is less troublesome. One simply expands the left-hand side, using (1), (35.6.2), and applies (35.8.16) to obtain

$$U_x \{xyz\} = T(x,y)U_{xy} + (T(x,y)T(x,z) - T(x^2, x)z)$$

$$- T(x,z)x^2 \times y + N(x)y \times z.$$
In order to prove the third, we again apply (35.8.21) to obtain
\[ x^{-1} = N_X(x)^{-1}x, \quad (x^{-1})^\dagger = N_X(x)^{-1}x, \quad N_X(x^{-1}) = N_X(x)^{-1}. \] (1)

**Proof.** Put 1 := 1_X, N := N_X. If \( x \in J^X \), then (35.8.21) implies 1 = N(1) = N(U_xx^{-2}) = N(x)^2N(x^{-2}), hence \( N(x) \in k^\times \). Conversely, assume \( N(x) \in k^\times \) and put \( y := N(x)^{-1}x^2 \). From (35.9.3) we then deduce \( U_x = x, U_{xy}^2 = 1 \), hence \( x \in J^X \) and the first equation of (1). Taking adjoints, we immediately obtain the second. In order to prove the third, we again apply (35.8.21) to obtain \( N(x) = N(U_xx^{-1}) = N(x)^2N(x^{-1}) \) and therefore \( N(x^{-1}) = N(x)^{-1} \).

**35.11. Isotopes of cubic norm structures.** Isotopes of Jordan algebras have a counterpart on the level of cubic norm structures which we now proceed to discuss. Let \( X \) be a cubic norm structure over \( k \). Given a regular element \( p \in X \) and writing \( p^{-1} \) for its inverse in \( J = J(X) \) (cf. Cor. 35.10), we claim that the \( k \)-module \( X \) together with the base point \( 1_X(p) := 1_X^p \in X(p) \), the adjoint \( x \mapsto x^{(p)} \) (a quadratic map \( X \to X \)), and the norm \( N_X(p) := N_X^p \) (a cubic form \( X(p) \to k \)) defined respectively by

\[
1_X(p) := 1_X^p := p^{-1},
\]

\[
x^{(p)} := N_X(p)U_{p^{-1}x^2} = N_X(p)U_{p^{-1}x^2},
\]

\[
N_X(p)(x) := N_X^p(x) = N_X(p)N_X(x)
\]

in all scalar extensions is a cubic norm structure over \( k \), denoted by \( X^{(p)} \) and called the \( p \)-isotope of \( X \). Moreover, the (bi)-linear trace \( T_X(p) := T_X^p \) and the quadratic trace \( S_X(p) := S_X^p \) of \( X^{(p)} \) are given by

\[
T_X(p)(y,z) = T_X^p(y,z) = T_X(U_p y,z),
\]

\[
T_X(p)(y) = T_X^p(y) = T_X(p,y),
\]

\[
S_X(p)(y) = S_X^p(y) = T_X(p^2,y^2)
\]

for all for all \( y,z \in X \). Indeed, dropping the subscripts for convenience, (35.10.11) combined with (35.8.17) and Lemma 35.7 shows that \( X^{(p)} \) is a cubic array over \( k \) whose bilinear trace by (35.2.8), (35.8.8), (1) and the gradient identity (35.8.4) has the form

\[
T^{(p)}(y,z) = N^{(p)}(p^{-1},y)N^{(p)}(p^{-1},z) - N^{(p)}(p^{-1},y,z)
\]

\[
= N(p)^2T(p^{-1},y)T(p^{-1},z) - N(p)T(p^{-1} \times y,z)
\]

\[
= T(p,y)T(p,z) - T(p^2 \times y,z).
\]
Hence (4) holds, as do (5), (6). The defining conditions, (35.8.3), (35.8.4), (35.8.5), of a cubic norm structure are now straightforward to check, using the relation $y \times (x^{(p)} - z) = N(p)U_p^{-1}(y \times z)$ for the bilinearization of $(2, p)$. As an example, verifying the adjoint identity, we apply (35.10.1), (35.8.20) and obtain

\[ x^{(p)}(x^{(p)} - z) = N(p)U_p^{-1}(N(p)U_p^{-1}x^{(p)} - z) = N(p)^3U_p^{-1}U_p^{-1}x^{(p)}z^{(p)} \]

\[ = N(p)^3U_p^{-1}U_p^{-1}x_{p}^{(p)}z^{(p)} = N(p)U_p^{-1}U_p^{-1}x_{p}^{(p)}z^{(p)} \]

\[ = N(p)N(x)x = N(p)(x)x. \]

**35.12. Proposition** (McCrimmon [77]). Let $X$ be a cubic norm structure over $k$.

(a) If $p \in X$ is a regular element, then $J(X^{(p)}) = J(X)^{(p)}$ is the $p$-isotope of the Jordan algebra associated with $X$.

(b) If $p, q \in X$ are regular, then so is $U_p q$ and $(X^{(p)})(q) = X^{(U_p q)}$.

**Proof.** (a) Both algebras live on the same $k$-module and have the same unit element, so it remains to show that they have the same $U$-operator as well. To do so, we write $U'$ for the $U$-operator of $J(X^{(p)})$, abbreviate $T := T_X$ and obtain, combining (35.8.20), (35.11.1) with the fundamental formula,

\[ U'_{x, y} = T^{(p)}(x, y)x - x^{(p)} \times (p) y = T(U_p x, y)x - N(p)^2U_p^{-1}((U_p x)^2) \times y \]

\[ = T(U_p x, y)x - U_p^{-1}((U_p x)^2) \times y = T(U_p x, y)x - U_p^{-1}((U_p x)^2) \times y \]

\[ = U_p^{-1}(T(U_p x, y)U_p x - (U_p x)^2) \times y \]

\[ = U_p^{-1}U_p U_p x U_p y = U_p U_p y = U_p y, \]

which is exactly what we had to prove.

(b) The first part follows from (35.8.21) and Cor. 35.10; the rest from (a) and a straightforward computation.

In view of the preceding results, particularly Thm. 35.9, it is natural to ask for an intrinsic characterization of those Jordan algebras over $k$ that may be written in the form $J(X)$, for some cubic norm structure $X$. The key to such a characterization, taking (35.8.21), (35.9.2) as a guide, is provided by the most important concept of the present chapter.

**35.13. The concept of a cubic Jordan algebra.** In analogy to the concept of a conic algebra as presented in [19.1], we define a cubic Jordan algebra over $k$ as a Jordan $k$-algebra $J$ together with a cubic form $N_J: J \to k$ (the norm) such that the following conditions hold.

(i) $1_J \in J$ is unimodular.

(ii) The norm of $J$ satisfies $N_J(1_J) = 1$ and permits Jordan composition: the equation

\[ N_J(U_J y) = N_J(x)^2 N_J(y) \]
holds strictly in $J$.

(iii) For all $R \in k\text{-}\text{alg}$ and all $x \in J_R$, the monic cubic polynomial

$$m_{J,x}(t) := N_J(t1_R - x) \in R[t]$$

satisfies the equations

$$m_{J,x}(x) = (tm_{J,x})(x) = 0.$$

By definition, cubic Jordan algebras are invariant under base change. If $J'$ is another cubic Jordan algebra over $k$, a homomorphism $\phi: J \to J'$ is defined as a homomorphism of Jordan algebras preserving norms in the sense that $N_{J'} \circ \phi = N_J$ as polynomial laws over $k$. In this way we obtain the category of cubic Jordan algebras over $k$, denoted by $k\text{-cujo}$, the category of Jordan algebras over $k$, but not a full one, as we shall see in 35.22 below.

In order to make condition (iii) above more explicit, we imitate the procedure of 35.2 to define the linear trace of $J$ as the linear map

$$T_J: J \longrightarrow k, \quad x \longmapsto T_J(x) := N_J(1, x),$$

as well as the quadratic trace of $J$ as the quadratic form

$$S_J: J \longrightarrow k, \quad x \longmapsto S_J(x) := N_J(x, 1).$$

Then condition (iii) above is equivalent to the strict validity of the equations

$$x^3 - T_J(x)x^2 + S_J(x)x - N_J(x)1_J = 0,$$

$$x^4 - T_J(x)x^3 + S_J(x)x^2 - N_J(x)x = 0$$

in $J$. Note that (4) implies (5) if $\frac{1}{2} \in k$ since $J$ is then a linear Jordan algebra. Furthermore, (2), (3) combined with Euler’s differential equation imply

$$T_J(1_J) = S_J(1_J) = 3.$$

Inspired by (35.8.22), we define the adjoint of $J$ as the quadratic map $x \mapsto x^\sharp$ from $J$ to $J$ given by

$$x^\sharp := x^2 - T_J(x)x + S_J(x)1,$$

dependence on $J$ being understood. The adjoint linearizes to

$$x \times y := (x+y)^\sharp - x^\sharp - y^\sharp = x \circ y - T_J(x)y - T_J(y)x + S_J(x,y)1.$$

Combining (7) with (6), we conclude $1_J^\sharp = 1_J$, so the $k$-module $J$ together with the base point $1_J$, the adjoint $\sharp$ and the norm $N_J$ is a cubic array over $k$, denoted by $X(J)$. In particular, we have the bilinear trace of $X(J)$, which we call the bilinear trace of
35. From cubic norm structures to cubic Jordan algebras

$J$, denoted by $T_J: J \times J \to k$. Summing up, we conclude that not only the norm and adjoint but also the (bi-)linear and quadratic trace of $J$ and $X(J)$ are the same.

Clearly, every homomorphism of cubic Jordan algebras preserves not only norms but also (bi-)linear and quadratic traces. If there is no danger of confusion, we will always extend the notational conventions spelled out for cubic arrays in 35.1 to cubic Jordan algebras by writing their identity elements as $1$, their norms as $N$, and their (bi-)linear and quadratic traces as $T, S$, respectively.

Before we can proceed, we need a lemma.

**35.14. Lemma.** Let $X$ be a cubic array over $k$ such that the unit identity and the adjoint identity hold strictly in $X$:

$$1 \times x = T_X(x)1_X - x, \quad x^\sharp = N_X(x)x.$$  \hspace{1cm} (1) \hspace{1cm} \text{UNIADJ}

Then

$$S_X(x) = T_X(x^\sharp)$$  \hspace{1cm} (2) \hspace{1cm} \text{STCL}

for all $x \in X$.

**Proof.** Applying the second order chain and product rules to the second equation of (1), we obtain

$$x^\sharp \times y^\sharp + (x \times y)^\sharp = N_X(x,y)y + N_X(y,x)x.$$  

Putting $y = 1_X$ and combining with the first equation of (1), we obtain

$$S_X(x)1_X + T_X(x)x = T_X(x^\sharp)1_X - x^\sharp + (T_X(x)1_X - x)^\sharp$$

$$= T_X(x^\sharp)1_X - x^\sharp + T_X(x)^\sharp 1_X - T_X(x)(T_X(x)1_X - x) + x^\sharp$$

$$= T_X(x^\sharp)1_X + T_X(x)x,$$

and since $1_X$ is unimodular, the assertion follows. \hfill \Box

**35.15. Theorem.** Let $J$ be a cubic Jordan algebra over $k$. Then the cubic array $X := X(J)$ of 35.13 is a cubic norm structure over $k$ such that $J = J(X)$.

**Proof.** We always drop the subscript “$X$” for convenience and then proceed in several steps, where we try to read some of the arguments in our previous results backwards.

1. An element $x \in J$ is invertible if and only if $x$ is regular in $X$. In this case, $x^{-1} = N(x)^{-1}x^\sharp$ and $N(x^{-1}) = N(x)^{-1}$. Indeed, assume first $x \in J^\times$. Since $N$ permits Jordan composition, we obtain $1 = N(1) = N(U_x x^{-2}) = N(x)^2 N(x^{-2})$, hence $N(x) \in k^\times$, and $N(x) = N(U_x x^{-1}) = N(x)^2 N(x^{-1})$ implies $N(x^{-1}) = N(x)^{-1}$. Before proving the converse of our assertion, assume for the time being that $x$ is arbitrary. Combining 35.13(5) with 35.13(7) we obtain

$$U_x x^\sharp = N(x)x,$$  \hspace{1cm} (1) \hspace{1cm} \text{UXESH}
while Thm. 32.1 and (35.13.4) yield $U_x U_{x'} = N(x)^2 1_J$, hence

$$U_x x^2 = N(x)^2 1.$$  

(2) UXESC

Now suppose $N(x) \in k$. Then (1) and (2) show that $y := N(x)^{-1} x^2$ satisfies $U_x y = x$, $U_y y^2 = 1$, hence $x \in J^0$ and $y = x^{-1}$.  

20. The following identities hold strictly in $J$.

$$1 \times x = T(x) 1 - x,$$  

(3) JUNI

$$x^2 = N(x)x,$$  

(4) JADJI

$$N(x^2) = N(x)^2,$$  

(5) JNADJ

$$S(x) = T(x^2),$$  

(6) JEVESTH

$$\{xx y\} = 2N(x)y = \{x^2 y\},$$  

(7) JTRISH

$$U_x (x \times y) = N(x,y)x - N(x)y,$$  

(8) JUBADJ

$$(U_x y)^2 = U_{x'y} y^2,$$  

(9) JUADJ

$$N(U_{x'y} U_{x''}) = N(x)^2 N(y,z),$$  

(10) EUUX

$$N(x) U_{x'y} = N(x^2,y)x - N(x)x^2 \times y.$$  

(11) ENXU

We put $y = 1$ in (35.13.8) and obtain $1 \times x = 2x - T(x) 1 - 3x + S(1,1)1$, which implies (3) since $S(1,1) = T(x)T(1) - T(x,1) = 2T(x)$ by (35.2.10) (35.13.6). Turning to (4), (5), Prop. 13.22, and 10 allow us to assume that $x$ is invertible. Then $1^0$ implies $x^{10} = (N(x)x^{-1})^{10} = N(x)^2 (x^{-1})^{10} = N(x)^2 N(x^{-1}) (x^{-1})^{-1} = N(x)x$, hence (3).

But then (1) implies $N(x)^4 = N(N(x)x) = N(U_x x^2) = N(x)^2 N(x^2)$, and (5) drops out as well. (6) follows from (3), (4) and Lemma 35.14. For the first part of (7) we combine (35.13.7) with (32.4.4) and (35.13.4) and obtain

$$\{xx y\} = V_{x,x'y} = \left(V_{x,x'} - T(x)V_{x,x} + S(x)V_{x}\right)y$$

$$= \left(V_{x^3} - T(x)V_{x'} + S(x)V_{x}\right)y = (x^3 - T(x)x^2 + S(x)x) \circ y$$

$$= N(x)1 \circ y = 2N(x)y,$$

as desired. The second equation follows analogously. In order to derive (8), we differentiate (1) in the direction $y$, which yields $N(x,y)x + N(x)y = U_{x,x'} y^2 + U_{x'} (x \times y) = \{xx y\} + U_{x'} (x \times y)$, and (8) follows from (7). In (9), we apply Prop. 13.22 to the polynomial law $g$: $J \times J \to \text{End}(J)$ given by $g(x,y) := U_{xy}$. Hence we may assume that $x$ and $y$ are both invertible. Then so is $U_y$ by Prop. 33.3 and $1^0$ combined with (33.3.2) implies

$$(U_x y)^2 = N(U_{x'y}) (U_{x'y})^{-1} = N(x)^2 N(y) U_{x^{-1}y} - 1 = U_{N(x)x^{-1}N(y)^{-1}} = U_{x'y} y^2.$$  

Equation (10) follows by fixing $x$ and differentiating (35.13.1) at $y$ in the direction $z$. Finally, in order to derive (11), we replace $x$ by $x^2$ in (1) and obtain $N(x) U_{x^2 x} = N(x) x^2 x^2$, hence $U_{x^2 x} = N(x) x^2$ first for $x$ invertible and then in full
generality. Differentiating in the direction \( y \), we conclude \( N(x,y)x^2 + N(x)x \times y = U_{x^2}x + U_{x^2}y = \{ x^2(x \times y) \} + U_{x^2}y = 2N(x)x \times y + U_{x^2}y \) by \( (7) \). Thus

\[
U_{x^2}y = N(x,y)x^2 - N(x)x \times y.
\]

Here we replace \( x \) by \( x^2 \) to deduce \( N(x)^2 U_{x^2} = N(x)N(x^2,y)x - N(x)^2 x \times y \), which yields \( (11) \) first for \( x \in J^x \) and the in full generality.

3\(^{0}\). For \( p \in J^x \), the \( k \)-module \( J \) together with the base point \( 1(p) := p^{-1} \), the adjoint \( x \mapsto x(\sharp,p) := N(p)U_{p^{-1}}x^2 \) and the norm \( N(p) := N(p)N : J \rightarrow k \) is a cubic array \( X(p) \) whose linear and quadratic traces are given by

\[
T(p)(x) = N(p)N(p^{-1},x), \quad S(p)(x) = N(x,p^2).
\]

Moreover, \( X(p) \) strictly satisfies the unit and adjoint identities:

\[
1^{(p)} \times (p)x = T(p)(x)1^{(p)} - x, \quad x^{(p),p}(\sharp,p) = N(p)(x)x,
\]

where \( \times^{(p)} \) stands for the bilinearized adjoint of \( X(p) \). The straightforward verification that \( X(p) \) is a cubic array satisfying \( (12) \) is left to the reader. It therefore remains to check \( (13) \). First of all, \( 1^{(0)} \) and \( (8), (12) \) imply

\[
1^{(p)} \times (p)x = N(p)U_{p^{-1}}(p^{-1} \times x) = N(p)N(p^{-1},x)p^{-1} - N(p)N(p^{-1})x
\]

\[
= N(p)^{-1}N(p^2,x)p^{-1} - x = T(p)(x)1^{(p)} - x,
\]

while \( 1^{(0)}, (9), (13), (35.13.1) \) yield

\[
x^{(p),p}(\sharp,p) = (N(p)U_{p^{-1}}x^2)^{(p)} = N(p)U_{p^{-1}}(N(p)^{-1}U_{p^{-1}}x^2)^2 = N(p)U_{p^{-1}}(U_p x)^2 = N(p)^{-1}U_{p^{-1}}(N(U_p x)U_p x) = N(p)N(x)x = N(p)(x)x,
\]

as claimed.

4\(^{0}\). We can now show that \( X \) is a cubic norm structure. In view of \( (13), (4) \), we only have to verify the gradient identity. To this end, let \( p \in J^x \). Then \( 4^{0} \) and \( (35.14.2) \) imply \( S(p)(x) = T(p)(x^{(p),p}) \). But \( S(p)(x) = N(x,p^2) \) by \( (12) \), while \( (12) \) and \( (10) \) imply

\[
T(p)(x^{(p),p}) = N(p)N(p^{-1},N(p)U_{p^{-1}}x^2)) = N(p)^2N(U_{p^{-1}}p, U_{p^{-1}}x^2) = N(p,x^2).
\]

Thus \( N(x,p^2) = N(p,x^2) \), and in view of Prop. \( (13.22) \), we have shown that the identity

\[
N(x,y^2) = N(y,x^2)
\]

holds strictly in \( J \). Differentiating in the direction \( y \), we conclude...
\[ N(x, y \times z) = N(y, z, x^2). \]

Putting \( z = 1 \) and applying (35.13.3), (3), (35.1.10), (6), we therefore obtain
\[
T(y)S(x) - N(x, y) = T(y)N(x, 1) - N(x, y) = N(x, T(y)1 - y) = N(x, y \times 1)
\]
\[
= N(y, 1, x^2) = N(x^2, y, 1) = S(x^2, y) = T(x^2)T(y) - T(x^2, y)
\]
\[
= S(x)T(y) - T(x^2, y)
\]
and the adjoint identity is proved. It remains to show that \( J = J(X) \) is the Jordan algebra associated with \( X \). In (11), the gradient identity implies \( N(x^2, y, 1) = T(x^2)T(y) - T(x^2, y) \) and the formula \( U_A = T(x, y)x - x^2 \times y \) drops out for \( x \) invertible, hence in full generality. But this means \( J = J(X) \).

35.16. Corollary. Every invertible element of a cubic Jordan algebra is unimodular.

Proof. Let \( J \) be a cubic Jordan algebra over \( k \). Since Thm. 35.15 implies \( J = J(X) \) for some cubic norm structure \( X \), the assertion follows from Cor. 35.10 combined with Lemma 35.7 and (35.8.17).

35.17. Towards an isomorphism of categories. Let \( J \) be a cubic Jordan algebra over \( k \). Then Thm. 35.15 shows \( J = J(X(J)) \). Conversely, let \( X \) be a cubic norm structure over \( k \). By Thm. 35.9, combined with (35.8.21), \( J(X) \), always considered together with the norm of \( X: N_{J(X)} = N_X \), is a cubic Jordan algebra, and (35.8.22) implies \( X = X(J(X)) \). Now let \( \varphi: X \to X' \) be a homomorphism of cubic norm structures. Since \( \varphi \) preserves not only base points, adjoints and norms but also linear and quadratic traces, it is a homomorphism \( \varphi: J(X) \to J(X') \) of cubic Jordan algebras. Conversely let \( \varphi: J \to J' \) be a homomorphism of cubic Jordan algebras. Since \( \varphi \) preserves units, norms, linear and quadratic traces, it follows from (35.13.7) that it preserves adjoints as well. Thus \( \varphi: X(J) \to X'(J') \) is a homomorphism of cubic norm structures. Summing up, we have shown the following result.

35.18. Corollary. The formalism set up in 35.17 yields an isomorphism of categories between cubic norm structures and cubic Jordan algebras over \( k \).

35.19. Convention. From now on we will use Cor. 35.18 to identify cubic norm structures and cubic Jordan algebras over \( k \) canonically. Thus the two terms will henceforth be employed interchangeably.

35.20. Cubic alternative algebras. By a cubic alternative algebra over \( k \) we mean a unital alternative algebra \( A \) over \( k \) together with a cubic form \( N_A: A \to k \) (the norm) such that the following conditions are fulfilled.

(i) \( 1_A \in A \) is unimodular.
(ii) \( N_A(1_A) = 1 \).
(iii) For all $R \in k\text{-alg}$ and all $x \in A_R$, the monic polynomial

$$m_{A,x}(t) = N_A(t1_{AR} - x) \in R[t]$$

annihilates $x$:

$$m_{A,x}(x) = 0.$$ 

As in the case of cubic Jordan algebras, we then define the linear and the quadratic trace of $A$ by

$$T_A : A \longrightarrow k, \quad x \longmapsto T_A(x) := N_A(1_A, x), \quad (1)$$

$$S_A : A \longrightarrow k, \quad x \longmapsto S_A(x) := N_A(x, 1_A), \quad (2)$$

respectively. Condition (iii) may then be rephrased by saying that the equation

$$x^3 - T_A(x)x^2 + S_A(x)x - N_A(x)1_A = 0 \quad (3)$$

holds strictly in $A$. If $A'$ is another cubic alternative $k$-algebra, a homomorphism $\varphi : A \rightarrow A'$ of cubic alternative $k$-algebras is defined as a homomorphism of unital $k$-algebras that preserves norms: $N_{A'} \circ \varphi = N_A$ as polynomial laws over $k$. In this way we obtain the category of cubic alternative algebras over $k$, denoted by $k\text{-cual}$. If $A$ in the preceding discussion is even associative, then we speak of a cubic associative algebra over $k$. Cubic associative $k$-algebras may and always will be viewed canonically as a full subcategory, denoted by $k\text{-cua}$, of cubic alternative $k$-algebras. Similar conventions apply to commutative associative algebras.

A cubic alternative algebra $A$ as above is said to be multiplicative if the equation

$$N_A(xy) = N_A(x)N_A(y) \quad (4)$$

holds strictly in $A$. By definition arbitrary cubic alternative algebras (resp. multiplicative ones) are stable under base change. Moreover, combining Exc. 86 with Exc. 192 below, it follows that cubic alternative algebras need not be multiplicative, and their norms need not be uniquely determined by the algebra structure alone.

35.21. Proposition. Let $A$ be a multiplicative cubic alternative algebra over $k$. Then $A^{(+)}$ together with the norm $N_{A^{(+)}} := N_A$ is a cubic Jordan algebra over $k$ whose linear and quadratic trace agree with those of $A$: $T_{A^{(+)}} = T_A$, $S_{A^{(+)}} = S_A$. Moreover, the bilinear trace of $A^{(+)}$ is given by $T_{A^{(+)}}(x, y) = T_A(xy)$ for all $x, y \in A$.

Proof. Equation (35.13[4]) agrees with (35.20[3]), while (35.13[5]) follows after multiplying (35.20[3]) by $x$ in $A$. Moreover, from (35.20[3]) we deduce that $N := N_A = N_{A^{(+)}}$ permits Jordan composition: $N(U_{A'}) = N(xy) = N(x)^2N(y)$ holds strictly in $J := A^{(+)}$. Thus $J$ together with $N$ is a cubic Jordan algebra whose linear and quadratic trace by definition are the same as those of $A$. With $T := T_A$ (the linear trace of $A$, hence of $J$) and $T' := T_J$ (the bilinear trace of $J$), it remains to show $T'(x, y) = T(xy)$ for all $x, y \in A$. By Prop. 13.22 we may assume $p := y \in A^*$. From (35.11[5]) combined with Prop. 35.12 and Thm. 35.15 we therefore conclude that
$J^{(p)}$ is a cubic Jordan algebra with linear trace $T^{(p)}$ given by $T^{(p)}(x) = T'(x, p)$ for all $x \in A$. On the other hand, since $A$ is multiplicative, $R_p : J^{(p)} \to J$ by \[33.12\] is an isomorphism of cubic Jordan algebras. As such it preserves linear traces, which implies $T(xp) = T^{(p)}(x) = T'(x, p)$, as claimed. \[\Box\]

35.22. Cubic structures on the split quadratic étale algebra. Let $E := k \oplus k$ be the split quadratic étale $k$-algebra as in \[24.18\]. Define a cubic form $N : C \to k$ by

$$N(r_1 \oplus r_2) := r_1 r_2^2$$ (1)

for $R \in k\text{-alg}$ and $r_1, r_2 \in R$. If also $s_1, s_2 \in R$, then

$$N(r_1 \oplus r_2, s_1 \oplus s_2) = s_1 r_2^2 + 2r_1 r_2 s_2,$$

hence

$$T(r_1 \oplus r_2) = 2r_1 + r_2, \quad S(r_1 \oplus r_2) = 2r_1 r_2 + r_1^2. \tag{2}$$

It follows immediately from (1) that $N(1_c) = 1$ and $N$ is multiplicative. Moreover, a straightforward verification shows

$$x^3 - T(x)x^2 + S(x)x - N(x)1_c = 0$$

for $x = r_1 \oplus r_2 \in C_R = R \oplus R$. Thus $C$ together with the norm $N$ is a cubic alternative algebra over $k$, which we denote by

$$(k \oplus k)_\text{cub}.$$  

Note that

$$x^2 = r_1 r_2 \oplus r_1^2$$ (3)

for $x = r_1 \oplus r_2 \in C_R = R \oplus R$, which follows immediately from (2) and \[35.8.22\].

On the other hand, we may define a cubic form $N' : C \to k$ by

$$N'(r_1 \oplus r_2) = r_1 r_2^2$$

for $R \in k\text{-alg}$ and $r_1, r_2 \in R$. Arguing as before, it follows that $C$ together with the norm $N'$ is a cubic alternative algebra over $k$ as well, which we denote by

$$(k \oplus k)_{\text{cub}}.$$

Thus the algebra structure alone of a cubic alternative algebra will in general not determine its norm uniquely, even if the underlying module is free of finite rank. Returning to our example, the conjugation of $C$ is an automorphism of $C$ but neither one of $(k \oplus k)_{\text{cub}}$ nor one of $(k \oplus k)_{\text{cub}}^{\text{op}}$; in fact, it is an isomorphism from the former to the latter:

$$t_{k \oplus k} : (k \oplus k)_{\text{cub}} \xrightarrow{\sim} (k \oplus k)_{\text{cub}}^{\text{op}}.$$
In particular, \(k\)-\textbf{cual} is \textit{not} a full subcategory of \(k\)-\textbf{alt}, and neither is \(k\)-\textbf{cujo} one of \(k\)-\textbf{jord}, as may be seen from the present example by passing from \(C\) to \(C^{(+)}\).

35.23. \textbf{Example:} \(3 \times 3\)-\textbf{matrices}. \(\text{Mat}_3(k)\) is a cubic associative \(k\)-\textbf{algebra} with norm (resp. linear trace) given by the ordinary determinant (resp. trace) of matrices since \(\det(1_3, x) = \text{tr}(x)\) for all \(x \in \text{Mat}_3(k)\). On the other hand, the bilinear trace of \(\text{Mat}_3(k)^{(+)}\), viewed as a cubic \(\text{Jordan} \) \(\text{algebra} \), may be read off from Prop. 35.21: \(T(x, y) = \text{Tr}(xy)\). In particular, the cubic \(\text{Jordan} \) \(\text{matrix algebra} \) \(\text{Mat}_3(k)^{(+)}\) is non-singular. On the other hand, the adjoint of \(\text{Mat}_3(k)^{(+)}\) is the usual adjoint of \(\text{matrices} \).

35.24. \textbf{Examples:} \textbf{cubic} \(\text{étale} \) \textbf{algebras}. Let \(E\) be a unital commutative associative \(k\)-\textbf{algebra} that is finitely generated projective as a \(k\)-\textbf{module} and finite \(\text{étale} \) (in the sense of \ref{22.18}) as an \(\text{algebra} \) over \(k\). Then \(N(x) := \det(L_x)\) for \(x\) in every scalar extension of \(E\), where \(L\) stands for the \(\text{left multiplication of} \ E\), defines a cubic form \(N = N_E : E \to k\) which converts \(E\) into a \(\text{multiplicative} \) cubic \(\text{alternative} \) \(k\)-\textbf{algebra}; we speak of a \textbf{cubic \(\text{étale} \) \text{algebra}} in this context. The linear trace of \(E\) is then given by \(T(x) = \text{Tr}(L_x)\), while the bilinear one by Prop. 35.21 has the form \(T(xy) = \text{Tr}(L_{xy})\). It follows from \ref{22.18} therefore, that \(E^{(+)}\), viewed as a cubic \(\text{Jordan} \) \(\text{algebra} \) over \(k\), is non-singular.

A particularly simple case is that of the \textit{split cubic \(\text{étale} \) \textit{k-algebra}} defined by \(E = k \oplus k \oplus k\) as a direct sum of ideals, with identity element \(1_E = 1 \oplus 1 \oplus 1\) and norm \(N = N_E : E \to k\) given by

\[
N(x) = \xi_1 \xi_2 \xi_3
\]

for \(x = \xi_1 \oplus \xi_2 \oplus \xi_3 \in E_R\), \(R \in k\)-\textbf{alg}. The linear and quadratic trace of \(E\) have the form

\[
T(x) = \xi_1 + \xi_2 + \xi_3, \tag{2}
\]
\[
S(x) = \xi_2 \xi_3 + \xi_3 \xi_1 + \xi_1 \xi_2, \tag{3}
\]

while the adjoint and the bilinear trace of \(E^{(+)}\) are given by

\[
x^\dagger = \xi_2 \xi_3 \oplus \xi_3 \xi_1 \oplus \xi_1 \xi_2, \tag{4}
\]
\[
T(x, y) = \xi_1 \eta_1 + \xi_2 \eta_2 + \xi_3 \eta_3 \tag{5}
\]

for \(y = \eta_1 \oplus \eta_2 \oplus \eta_3 \in E_R\). It is sometimes convenient to identify \(E\) canonically with the algebra of \(3 \times 3\)-\textit{diagonal matrices} over \(k\):

\[
E = \text{Diag}_3(k) = \{\text{diag}(\gamma_1, \gamma_2, \gamma_3) \mid \gamma_1, \gamma_2, \gamma_3 \in k\}, \tag{6}
\]

viewed as a cubic \textit{commutative} \textit{associative} \textit{subalgebra} of \(\text{Mat}_3(k)\). For

\[
\Gamma = \text{diag}(\gamma_1, \gamma_2, \gamma_3) \in \text{Diag}_3(k)
\]
we have

\[ N(\Gamma) = \det(\Gamma) = \gamma_1 \gamma_2 \gamma_3, \]  
(7)  
\[ T(\Gamma) = \text{tr}(\Gamma) = \gamma_1 + \gamma_2 + \gamma_3, \]  
(8)  
\[ S(\Gamma) = \gamma_2 \gamma_3 + \gamma_1 \gamma_3 + \gamma_1 \gamma_2, \]  
(9)  
\[ \Gamma^2 = \text{diag}(\gamma_2 \gamma_3, \gamma_3 \gamma_1, \gamma_1 \gamma_2). \]  
(10)

Exercises.

184. Non-singular pointed cubic forms (Springer [118], McCrimmon [77]). By a pointed cubic form over \( k \) we mean a \( k \)-module \( X \) together with a distinguished element \( 1 = 1_X \in X \) (the base point) and a cubic form \( N = N_X : X \to k \) (the norm) such that \( N(1) = 1 \). We then define the associated (bilinear) trace of \( X \) as the symmetric bilinear form \( T = T_X : X \times X \to k \) given by

\[ T(y,z) := N(1,y)N(1,z) - N(1,y,z) \quad (y,z \in X). \]

A homomorphism of pointed cubic forms is a linear map preserving norms and base points. A pointed cubic form \( X \) with base point \( 1 \), norm \( N \) and trace \( T \) is said to be non-singular if \( X \) is a \( k \)-module and \( T \) is non-singular as a symmetric bilinear form, i.e., it induces an isomorphism from \( X \) onto its dual \( X^* \) in the usual way.

Now let \( X \) be a non-singular pointed cubic form over \( k \) as above.

(a) Show that there is a unique map \( x \mapsto x^2 \) from \( X \) to \( X \) satisfying the gradient identity

\[ T(x^2,y) = N(x,y) \quad (x,y \in X). \]

Conclude that \( X \) together with \( 1 \), \( \cdot \) and \( N \) is a cubic array satisfying the unit identity. In particular, \( X \) is a cubic norm structure if and only if the adjoint identity holds.

(b) Let \( \varphi : X \to X' \) be a surjective homomorphism of pointed cubic forms. Show that \( \varphi \) is an isomorphism of cubic arrays.

185. Let \( \varphi : J \to J' \) be a \( k \)-linear map of cubic Jordan algebras over \( k \). Prove that \( \varphi \) is

(a) an homomorphism of cubic Jordan algebras if it preserves unit elements and adjoints,
(b) an isomorphism of cubic Jordan algebras if \( J \) is non-singular and \( \varphi \) is surjective preserving unit elements and norms.

186. Show that a cubic array \( X \) over \( k \) is a cubic norm structure if and only if the identities

\[ 1 \times x = T(x)1 - x, \]  
(11)  
\[ N(x,y) = T(x^2,y), \]  
(12)  
\[ x^2 = N(x)x, \]  
(13)  
\[ x^2 \times y^2 + (x \times y)^2 = T(x^2,y)y + T(x,y^2)x, \]  
(14)  
\[ x^2 \times (x \times y) = T(x^2,y)x + N(x)y. \]  
(15)

hold for all \( x,y,z \in X \).

187. Rational cubic norm structures (Tits-Weiss [123], M"uhlherr-Weiss [88]). The following exercise characterizes cubic norm structures in terms of conditions that avoid scalar extensions. By a rational cubic norm structure over \( k \) we mean a \( k \)-module \( X \) together with

- a distinguished element \( 1 \in X \) (the base point),
- a map \( X \to X, x \mapsto x^2 \) (the adjoint),
35 From cubic norm structures to cubic Jordan algebras

- a bilinear map \( X \times X \to X \), \((x, y) \mapsto x \cdot y \) (the bilinearized adjoint),
- a symmetric bilinear form \( T : X \times X \to k \) (the bilinear trace),
- a map \( N : X \to k \) (the norm)
such that the following conditions are fulfilled.

(i) \( 1 \in X \) is unimodular.

(ii) The following equations hold for all \( \alpha \in k \) and all \( x, y, z \in X \).

\[
\begin{align*}
(\alpha x)^2 &= \alpha^2 x^2, \quad (16) \\
N(\alpha x) &= \alpha^3 N(x), \quad (17) \\
(x + y)^2 &= x^2 + x \cdot y + y^2, \quad (18) \\
N(x + y) &= N(x) + T(x^2, y) + T(x, y^2) + N(y), \quad (19) \\
T(x, x^2) &= 3N(x), \quad (20) \\
x^3 &= N(x)x, \quad (21) \\
x^3 \cdot y^3 + (x \cdot y)^3 &= T(x^2, y)x + T(x, y^2)x, \quad (22) \\
x^3 \cdot (x \cdot y) &= N(x)y + T(x^2, y)x, \quad (23) \\
1^3 &= 1, \quad (24) \\
1 \cdot x &= T(1, y)1 - y. \quad (25)
\end{align*}
\]

A homomorphism of rational cubic norm structures over \( k \) is defined as a linear map preserving base points, (bilinarianized) adjoints, traces and norms in the obvious sense. In this way we obtain the category of rational cubic norm structures over \( k \), noted by \( k\text{-racuno} \). Show for a rational cubic norm structure \( X \) over \( k \), with \( 1, \xi, \eta, T, N \) as above, that \( x \mapsto x^2 \) is a quadratic map and that there exists a unique cubic form \( \hat{N} : X \to \hat{X} \) which makes the \( k \)-module \( X \) together with \( 1, \xi, \eta, N \) a cubic norm structure over \( k \), written as \( \hat{X} \), having bilinear trace \( T \) and satisfying \( \hat{N} = N \). Conclude that the assignment \( X \mapsto \hat{X} \) on objects and the identity on morphisms yield an isomorphism of categories from \( k\text{-racuno} \) to \( k\text{-cuno} \).

188. (Brühne [17]) Let \( X \) be a cubic norm structure over \( k \). Show that the cubic norm substructure of \( X \) generated by arbitrary elements \( x, y \in X \) is spanned as a \( k \)-module by

\[
1, x, x^2, y, y^2, x \cdot y, x^2 \cdot y, x \cdot y^2, x^2 \cdot y^2.
\]

189. Norm ideals. Let \( X \) be a cubic array over \( k \). By a norm ideal of \( X \) we mean a \( k \)-submodule \( I \subseteq X \) such that the following conditions hold.

(i) \( 1 \) and \( I \) are linearly separated, i.e., there exists a linear form \( \lambda : X \to k \) such that \( \lambda(1) = 1 \) and \( \lambda(I) = \{0\} \).

(ii) \( N(x) = 0 \) for all \( x \in I \).

(iii) \( I^2 + X \cdot I \subseteq I \).

Prove:

(a) If \( \varphi : X \to X' \) is a homomorphism of cubic arrays, then \( \text{Ker}(\varphi) \subseteq X \) is a norm ideal.

(b) Conversely, if \( X \) is a cubic norm structure and \( I \subseteq X \) is a norm ideal, there is a unique way of viewing the quotient module \( X_1 := X/I \) as a cubic norm structure over \( k \) such that the canonical projection \( \pi : X \to X_1 \) is a homomorphism of cubic norm structures with kernel \( I \).

(Hint: Show \( T(x, y) = 0 \) for all \( x \in I, y \in X \) and apply Exc. [18])

190. Traceless cubic Jordan algebras. Let \( J \) be a cubic Jordan algebra over \( k \) which is traceless in the sense that its bilinear trace vanishes identically. Show \( 3 = 0 \) in \( k \) and that \( J \), viewed as a linear Jordan algebra, is commutative alternative.
191. (Petersson-Racine [101], Loos [71]) Let $J$ be a cubic Jordan algebra over $k$. Prove that an element $x \in J$ is nilpotent if and only if $T(x), S(x), N(x) \in k$ are nilpotent. Conclude that the nil radical of $J$ (Exc. 148) can be described as

$$\text{Nil}(J) = \{ x \in J \mid \forall y \in J : T(x,y), T(x^2,y), N(x) \in \text{Nil}(k) \},$$

(27) NILAR

$$\text{Nil}(J) = \{ x \in J \mid \forall y \in J : T(x,y), N(x) \in \text{Nil}(k) \}$$ (if $\frac{1}{2} \in k$),

(28) NILTWO

$$\text{Nil}(J) = \{ x \in J \mid \forall y \in J : T(x,y), T(x^2,y) \in \text{Nil}(k) \}$$ (if $\frac{1}{3} \in k$),

(29) NILTHR

$$\text{Nil}(J) = \{ x \in J \mid \forall y \in J : T(x,y) \in \text{Nil}(k) \}$$ (if $\frac{1}{6} \in k$).

(30) NILSIX

192. In this exercise, cubic Jordan (resp. alternative) algebras will be constructed out of Jordan algebras of Clifford type (resp. out of conic alternative algebras).

(a) Let $(M, q, e)$ be a pointed quadratic module with trace $t$ and conjugation $u \mapsto \bar{u}$ over $k$, and let $J := J(M, q, e)$ be the corresponding Jordan algebra of Clifford type. Show that

$$\hat{J} := k^+ \oplus M$$

as a direct sum of ideals in the category of para-quadratic $k$-algebras is a cubic Jordan algebra over $k$, with norm $N : \hat{J} \to k$ given by

$$N(r \oplus u) := rq(u) \quad (R \in k\text{-alg}, \ r \in R, \ u \in J)$$ (31) NOHA

Show further that the (bi-)linear and quadratic trace of $\hat{J}$ as well as its adjoint have the form

$$T(\alpha \oplus u, \beta \oplus v) = \alpha \beta + q(u, \bar{v}),$$

(32) BITHA

$$T(\alpha \oplus u) = \alpha + t(u),$$

(33) LITHA

$$S(\alpha \oplus u) = \alpha t(u) + q(u),$$

(34) QITHA

$$(\alpha \oplus u)^3 = q(u) \oplus \bar{a}$$

(35) ADRA

for all $\alpha, \beta \in k, u, v \in J$.

(b) Let $C$ be a conic alternative algebra over $k$. Show that

$$\hat{C} := k \oplus C$$

as a direct sum of ideals is a cubic alternative $k$-algebra, with norm $N : \hat{C} \to k$ given by

$$N(\hat{C}) := \bar{N}(C)$$ (31) NOHA

and trace and quadratic trace given by

$$\hat{t}(\alpha \oplus u) = \alpha t(u),$$

(34) QITH

and $\hat{q}(\alpha \oplus u) = \alpha q(u)$.

(35) ADRA

193. Cubic norm pseudo-structures (Petersson-Racine [101]). By a cubic norm pseudo-structure over $k$ we mean a $k$-module $X$ together with an element $1 \in X$, a quadratic map $x \mapsto x^2$ from $X$ to $X$ and a cubic form $N : X \to k$ such that all conditions of $35.1$ and $35.4$ hold, with the possible exception of the base point $1$ being unimodular. As in $35.2$ we can then speak of the (bi-)linear and the quadratic trace of $X$. Similarly, by a rational cubic norm pseudo-structure over $k$, we mean a $k$-module $X$ together with data $1, \frac{1}{2}, x, T, N$ as in Exc. 38 such that equations $16 - 23$ of that exercise hold for all $\alpha \in k, x, y, z \in X$ but the base point $1 \in X$ may fail to be unimodular.

(a) Show for a rational cubic norm pseudo-structure $X$ over $k$ that there exists a unique cubic form $\tilde{N} : X \to k$ making $X$ together with base point and adjoint a cubic norm pseudo-structure.

(b) Let $V, W$ be vector spaces over a field $F$ and suppose $V$ is finite-dimensional, with basis $(e_1, \ldots, e_n)$. Given a quadratic map $v \mapsto v^2$ from $V$ to $V$, with bilinearization $(v, v') \mapsto v \times v'$,
a symmetric bilinear map $\sigma: V \times V \to W$ and arbitrary elements $w_1, \ldots, w_n \in W$, show that the following conditions are equivalent.

(i) There exists a homogeneous polynomial law $\mu: V \to W$ of degree 3 such that $\mu(e_i) = w_i$ for $1 \leq i \leq n$ and $\mu(v, v') = \sigma(v^i, v')$ holds strictly in $V$.

(ii) $\sigma(e_i^i, e_i) = 3w_i$ for $1 \leq i \leq n$ and the trilinear map

$$V \times V \times V \to (v_1, v_2, v_3) \mapsto \sigma(v_1 \times v_2, v_3),$$

is totally symmetric.

In this case, $\mu$ is unique.

(c) Use (a), (b) to give an example of a cubic norm pseudo-structure $X$ such that the relation $N(x^i) = N(x)^2$ does not always hold and the bilinear trace of $X$ is different from zero. (Hint. The proof of [101, Thm. 2.10] contains a gap that should be filled by means of (a).)

### 36. Building up cubic norm structures

In this rather technical section, a number of basic tools will be provided that turn out to be of crucial importance in various constructions of cubic Jordan algebras. These tools are best described in the language of cubic norm structures. Accordingly, throughout this section, we fix an arbitrary commutative ring $k$ and a cubic norm structure $X$ over $k$. Generally speaking, we will be concerned with the question of which additional ingredients are needed in order to understand $X$ in terms of a given cubic norm substructure of $X$. These ingredients are based on a number of useful identities that are our main focus in the present section. In order to describe their range of validity in a precise manner, a peculiar conceptual framework will be needed that we now proceed to consider.

#### 36.1. The orthogonal complement of a cubic norm substructure

Let $X_0$ be a cubic norm substructure of $X$ and write

$$X_0^\perp := \{ u \in X \mid \forall x_0 \in X_0 : T(x_0, u) = 0 \}$$

for the orthogonal complement of $X_0$ relative to the bilinear trace of $X$. From [35.8.7] we obtain a well defined bilinear action

$$X_0 \times X_0^\perp \to X_0^\perp, \quad (x_0, u) \mapsto x_0 \cdot u := -x_0 \times u$$

that will be of fundamental importance later on. It seems worth noting, however, that the ingredients of this action are in general not compatible with base change: for $R \in k$-$\text{alg}$, the scalar extension $X_{0R}$ need not be a cubic norm substructure of $X$, and even if it is, $(X_{0R})^\perp$, its orthogonal complement in $X_R$ relative to the bilinear trace, need not be the same as $(X_0^\perp)_R$. To remedy this deficiency, the following concept will be introduced.
36.2. Pure cubic norm substructures. Let $X_0$ be a cubic norm substructure of $X$ and $R \in k$-alg. If the inclusion $i \colon X_0 \hookrightarrow X$ extends to an $R$-linear injection $i_R \colon X_{0R} \rightarrow X_R$, then $X_0$ is said to be $R$-pure. In this case, $X_{0R}$ can and always will be canonically regarded as a cubic norm substructure of $X_R$ over $R$. Furthermore, even though the $R$-module $(X_{0R})^\perp$ may still be distinct from $(X_0^\perp)_R$, the extended element $u_R = u \otimes 1_R \in X_R$, for any $u \in X_0^\perp$, belongs to $(X_{0R})^\perp$. We say that $X_0$ is pure if it is $R$-pure, for all $R \in k$-alg.

If $R$ is a flat $k$-algebra (so the functor $- \otimes R$ from $k$-modules to $R$-modules is exact [11, §2, Definition 1]), then every cubic norm substructure of $X$ is $R$-pure. On the other hand, if $X_0 \subseteq X$ is a cubic norm substructure which is a direct summand of $X$ as a $k$-module, then $X_0$ is pure.

36.3. The action of $X_0$ on $X_0^\perp$. Let $X_0$ be a cubic norm substructure of $X$ and write $N_0$ for the norm of $X_0$. We claim that the following relations hold, for all $R \in k$-alg making $X_0$ $R$-pure and all $x_0, y_0 \in X_{0R}$, all $u \in X_{0R}^\perp$.

\begin{align*}
1. & \quad u = u, \\
2. & \quad U_{x_0}u = x_0^\sharp \cdot u, \\
3. & \quad x_0 \cdot (y_0 \cdot (x_0 \cdot u)) = (U_{x_0}y_0) \cdot u, \\
4. & \quad x_0 \cdot (x_0^\sharp \cdot u) = N_0(x_0)u = x_0^\sharp \cdot (x_0 \cdot u), \\
5. & \quad N(x_0 \cdot u) = N_0(x_0)N(u).
\end{align*}

We may clearly assume $R = k$. Then (1) follows immediately from (36.1.2) and the unit identity (35.8.15), while the definition of the $U$-operator (35.8.15) combined with (36.1.2) and the relation $T(x_0, u) = 0$ gives (2). To derive (3), we apply (35.8.26) with $z = u$, observe $T(x_0^\sharp, u) = T(y_0, u) = 0$ and obtain $x_0 \cdot (y_0 \cdot (x_0 \cdot u)) = -(x_0 \times (y_0 \times (x_0 \times u)) = -(U_{x_0}y_0) \times u = (U_{x_0}y_0) \cdot u$, hence (3). Since $T(x_0, u) = T(x_0^\sharp, u) = 0$, we obtain (4) immediately from (36.1.2) and (35.8.17), (35.8.19). To prove (5), we observe that (35.8.29) reduces to $N(x_0 \cdot u) = N(x_0 \times u) = N(x_0)N(u)$, and this is (5).

Relations (1), (3) above are equivalent to saying that the linear map $\sigma : J_0 := J(X_0) \rightarrow \text{End}(X_0^\perp)^{(+)}$ given by $\sigma(x_0)u := x_0 \cdot u$ for $x_0 \in J_0$, $u \in X_0^\perp$ is a homomorphism of Jordan algebras. Thus if $k = F$ is a field, $J_0$ is simple as a Jordan algebra over $F$ and $X_0^\perp \neq \{0\}$, then $J_0$ is special.

36.4. Strong orthogonality. With $X_0$ as in 36.3, an element $u \in X$ is said to be strongly orthogonal (or strongly perpendicular) to $X_0$ if $u$ and $u^\sharp$ both belong to $X_0^\perp$. Following Petersson-Racine [105, 4.4], we call

$$X_0^\perp := \{ u \in X \mid u \in X_0^\perp, u^\sharp \in X_0^\perp \}. $$

the strong orthogonal complement of $X_0$ in $X$. Note that $X_0^\perp \subseteq X$ will not be a $k$-submodule in general and may, in fact, be empty. On the other hand, if $u \in X$ is strongly orthogonal to $X_0$, so is $u^\sharp$ by the adjoint identity. We now claim that the
following relations hold, for all $R \in k\text{-alg}$ making $X_0$ $R$-pure, all $x_0,y_0,z_0 \in X_{0R}$ and all $u \in (X_{0R})^\perp$.

\begin{align*}
(x_0 \cdot u)^\perp &= x_0^\perp \cdot u^\perp, \\
(x_0 \cdot u) \times (y_0 \cdot u) &= (x_0 \times y_0) \cdot u^\perp, \\
(x_0 \cdot u) \times u^\perp &= -N(u)x_0 = (x_0 \cdot u^\perp) \times u, \\
T(x_0 \cdot u, y_0 \cdot u) &= 0, \\
T(x_0 \cdot u, y_0 \cdot u^\perp) &= N(u)T_0(x_0, y_0), \\
(x_0 \cdot (y_0 \cdot u)) \times u^\perp + u \times (x_0 \cdot (y_0 \cdot u^\perp)) &= -N(u)x_0 \circ y_0, \\
(x_0 \cdot (y_0 \cdot u)) \times (x_0 \cdot u^\perp) &= -N(u)U_{x_0y_0}, \\
(x_0 \cdot (y_0 \cdot u)) \times (z_0 \cdot u^\perp) + (z_0 \cdot (y_0 \cdot u)) \times (x_0 \cdot u^\perp) &= -N(u)\{x_0y_0z_0\}, \\
(x_0 \cdot (y_0 \cdot u)) \times u^\perp &= u \times (y_0 \cdot (x_0 \cdot u^\perp)) = (x_0 \cdot u) \times (y_0 \cdot u^\perp), \\
(x_0 \cdot u) \times ((x_0 \cdot u) \times (y_0 \cdot u^\perp)) &= N(u)(U_{x_0y_0} \cdot u). \tag{11}
\end{align*}

\textit{Proof.} As before, we may clearly assume $R = k$. The relations $T(x_0^\perp, u) = T(x_0, u^\perp) = 0$ combined with \textcircled{35.8.10} imply \textcircled{1}, which immediately yields \textcircled{2} after linearizing with respect to $x_0$, while the first relation of \textcircled{3} follows from $(x_0 \cdot u) \times u^\perp = -(x_0 \times u) \times u^\perp$ and \textcircled{35.8.8}; the same argument replacing \textcircled{35.8.8} by \textcircled{35.8.19} also gives the second. To establish \textcircled{3}, \textcircled{5}, we apply \textcircled{36.1.1}, \textcircled{35.8.7} and \textcircled{2} to obtain $T(x_0 \cdot u, y_0 \cdot u) = -T(x_0 \cdot u, y_0 \cdot y) = -T((x_0 \times 1) \cdot u^\perp, y_0) = 0$ and $T(x_0 \cdot u, y_0 \cdot u^\perp) = T(x_0 \cdot u, y_0 \cdot u^\perp) = T((x_0 \times u) \times u^\perp, y) = N(u)T_0(x_0, y_0)$. Turning to \textcircled{6}, we put $x := u$, $y := x_0$, $z := y_0$ in \textcircled{35.8.26} and obtain $u \times (x_0 \cdot (y_0 \cdot u)) = u \times (x_0 \times (u \times y_0)) = T(u, x_0)u \times y_0 + T(u^\perp, x_0)u + T((x_0, y_0)u^\perp - (u^\perp \times x_0) \times y_0 = -T(x_0, y_0)u \circ u^\perp, y_0) = T((x_0 \cdot u) \times y_0, u^\perp) + T(x_0, y_0)u^\perp - y_0 \cdot (x_0 \cdot u^\perp)$; since $u$ is strongly perpendicular to $y_0$, \textcircled{6} follows. Similarly, setting $x := u^\perp$, $y := x_0$, $z := y_0$, $w := u$ in \textcircled{35.8.27} yields

\begin{align*}
&u^\perp \times (x_0 \times (y_0 \times u) + y_0 \times (x_0 \times (u \times u^\perp)) + u \times (x_0 \times (u^\perp \times y_0)) \\
&\quad = T(u^\perp, x_0)u_0 \times u + T(y_0, x_0)u \times u^\perp + T(u, x_0)u^\perp \times y_0 \\
&\quad \quad + T(u^\perp \times y_0, u)u_0.
\end{align*}

But $u \times u^\perp = -N(u)1$ by \textcircled{3}, which implies $T(u^\perp \times y_0, u) = T(y_0, u \times u^\perp) = -N(u)T(y_0)$, and we conclude

\begin{align*}
(x_0 \cdot (y_0 \cdot u)) \times u^\perp - N(u)(1 \times x_0) \circ y_0 + u \times (x_0 \cdot (y_0 \cdot u^\perp)) \\
&= -N(u)T(x_0, y_0)1 - N(u)T(y_0)x_0,
\end{align*}

where $(1 \times x_0) \times y_0 = T(x_0)1 \times y_0 - x_0 \times y_0 = T(x_0)T(y_0)1 - T(x_0)y_0 - x_0 \times y_0$. Thus
\[
(x_0 \cdot (y_0 \cdot u)) \times u^2 + u \times (x_0 \cdot (y_0 \cdot u))
\]
\[
= -N(u) \left( x_0 \times y_0 + T(x_0)y_0 + T(y_0)x_0 - (T(x_0)T(y_0) - T(x_0,y_0)) \right)
\]
\[
= -N(u)x_0 \circ y_0
\]
by (35.8.23). This proves (7). In (8) we may assume by Lemma 13.23 that \(x_0\) is invertible. Then (36.1.4) implies \(u = x_0, v = x_0^{-1} \in X_0^\perp\) by (1), and using (36.3.3), (1), (36.3.4), (3), (36.3.5), we obtain
\[
(x_0 \cdot (y_0 \cdot u)) \times (x_0 \cdot u^2) = \left( (U_{y_0}y_0) \times (x_0 \cdot (y_0 \cdot v)^2) \right)
\]
\[
= N_0(x_0)((U_{y_0}y_0) \times v)^2
\]
\[
= -N_0(x_0)N(v)U_{y_0}y_0 = -N_0(x_0 \cdot v)U_{y_0}y_0 = -N(u)U_{y_0}y_0,
\]
hence (8), which implies (9) after linearization. Comparing (2) for \(z_0 = 1\) with (7) we obtain \((x_0 \cdot (y_0 \cdot u)) \times u^2 + (y_0 \cdot u) \times (x_0 \cdot u^2) = -N(u)x_0 \circ y_0 = (x_0 \cdot (y_0 \cdot u)) \times u^2 + u \times (x_0 \cdot (y_0 \cdot u))\), giving the second relation of (10) with \(x_0\) and \(y_0\) interchanged. On the other hand, linearizing (36.3.3) we obtain \((x_0 \cdot (y_0 \cdot u)) \times u^2 + (y_0 \cdot (x_0 \cdot u)) \times u^2 = ((x_0 \circ y_0) \cdot u) \times u^2 = -N(u)x_0 \circ y_0\) by (3), and comparing with (7), we also obtain the first relation of (10) with \(x_0\) and \(y_0\) interchanged. Finally, to establish (11), we apply (35.8.28) to \(x_0, u, y_0, u^2\) instead of \(x, y, v\), respectively. Since \(x_0, u, y_0, u^2 \in X_0^\perp\) by (1), we have \(T(x_0, u) = T(y_0, u^2) = S(x_0, u) = 0, T((x_0 \cdot u)^2, y_0, u^2) = T(x_0 \cdot u^2, y_0, u^2) = 0\) by (2), \(S(x_0, u, y_0, u^2) = -T(x_0 \cdot u, y_0, u^2) = -N(u)T_0(x_0, y_0)\) by (3), and \((x_0 \cdot u^2) \times (y_0 \cdot u^2) = (x_0^2 \times y_0) \cdot u^2 = N(u)(x_0^2 \times y_0) \cdot u\) by (1). (2). Hence (35.8.28) yields \((x_0 \cdot u) \times ((x_0 \cdot u) \times (y_0 \cdot u^2)) = N(u)(T_0(x_0, y_0)x_0 - x_0 \circ y_0) \cdot u = N(u)(U_{y_0}y_0) \cdot u\), as desired.

36.5. Complemented cubic norm substructures. By a complemented cubic norm substructure of \(X\) we mean a pair \((X_0, V)\) such that \(X_0 \subseteq X\) is a cubic norm substructure, \(V \subseteq X\) is a \(k\)-submodule and the relations
\[
X = X_0 \oplus V, \quad V \subseteq X_0^\perp, \quad X_0 \cdot V \subseteq V
\]
(1)
hold. This concept is clearly compatible with base change, so if \((X_0, V)\) is a complemented cubic norm substructure of \(X\), then \((X_0, V)_R := (X_0 R, V_R)\) is one of \(X_R\), for all \(R \in k\text{-alg}\). In particular, \(X_0\) is pure.

36.6. Remark. If \(X_0 \subseteq X\) is a non-singular cubic norm substructure, then we deduce from Lemma 12.10 that \((X_0, X_0^\perp)\) is the unique complemented cubic norm substructure of \(X\) extended from \(X_0\). Conversely, suppose \(X\) itself is non-singular and \((X_0, V)\) is a complemented cubic norm substructure of \(X\). Then \(X_0\) is non-singular and \(V = X_0^\perp\).
For the remainder of this section, we fix a complemented cubic norm substructure \((X_0, V)\) of \(X\) and write \(N_0\) for the norm, \(T_0\) (resp. \(S_0\)) for the (bi-)linear (resp. quadratic) trace of \(X_0\).

### 36.7. Splitting the adjoint.

We use (36.5.1) to follow Springer’s approach to twisted compositions (Springer [119, p. 95], Springer-Veldkamp [121, 6.5], Knus-Merkurjev-Rost-Tignol [59, §38A, p. 527]) (where \(k\) is a field of characteristic not 2) or Petersson-Racine [102, (3.1)] (with a sign change and \(X_0\) coming from a cubic étale \(k\)-algebra) to define quadratic maps \(Q: V \to X_0, H: V \to V\) by

\[
u^\sharp = -Q(u) + H(u) \quad (u \in V, \ Q(u) \in X_0, \ H(u) \in V).
\]

We claim that the identities

\[
\begin{align*}
(x_0 + u)^2 &= \left(x_0^2 - Q(u)\right) + \left(-x_0 \cdot u + H(u)\right), \tag{2} \\
N(x_0 + u) &= N_0(x_0) - T_0(x_0, Q(u)) + N(u), \tag{3} \\
T(y_0 + v_0 + w) &= T_0(y_0, v_0) + T_0(Q(v, w)), \tag{4} \\
T(y_0 + v_0) &= T_0(y_0), \tag{5} \\
S(x_0 + u) &= S_0(x_0) - T_0(Q(u)) \tag{6}
\end{align*}
\]

hold strictly for \(x_0, y_0, z_0 \in X_0, u, v, w \in V\). Indeed, \(N(x_0 + u) = N_0(x_0) + T(x_0, u) + T(x_0, u) + N(u) = N_0(x_0) - T_0(x_0, Q(u)) + N(u)\) by (36.5.1) and (1) and \((x_0 + u)^2 = x_0^2 + x_0 \cdot u + u^2 = x_0^2 - x_0 \cdot u - Q(u) + H(u)\) by (36.1.2) and (1). Finally, \(T(y_0 + v_0 + w) = T_0(y_0, z_0) + T(v, w)\), and (35.8.13) yields \(T(v, w) = T(v)T(w) - T(v \times w) = -T(v \times w) = T(Q(v, w) - H(v, w)) = T_0(Q(v, w))\), giving (4), which immediately implies first (5) and then (6).

### 36.8. Identities for \(Q\) and \(H\).

The following identities hold strictly for all \(x_0, y_0, z_0 \in X_0, u, v, w \in V\).
\[ Q(x_0, u) = U_{x_0} Q(u), \]
\[ Q(x_0, u, y_0, u) = U_{x_0, y_0} Q(u), \]
\[ Q(x_0, u, x_0, v) = U_{x_0} Q(u, v), \]
\[ Q(x_0, u, y_0, v) + Q(x_0, v, y_0, u) = U_{x_0, y_0} Q(u, v), \]
\[ H(x_0, u) = x_0^2 + H(u), \]
\[ H(x_0, u, y_0, u) = (x_0 \times y_0). H(u), \]
\[ H(x_0, u, x_0, v) = x_0^2 + H(u, v), \]
\[ H(x_0, u, y_0, v) + H(x_0, v, y_0, u) = (x_0 \times y_0). H(u, v), \]
\[ Q(H(u)) = Q(u)^2, \]
\[ H(Q(u)) = N(u) u - Q(u). H(u), \]
\[ Q(x_0, u, H(u)) = N(u) x_0 = Q(u, x_0, H(u)), \]
\[ Q(H(u), v) + Q(u, H(u)) = T_0 \left( Q(H(u), v) \right) 1, \]
\[ H(x_0, u, H(u)) = T_0(x_0, Q(u)) u - Q(u). (x_0, u), \]
\[ H(u, x_0, H(u)) = (x_0 \times Q(u)). u, \]
\[ T_0(x_0, Q(u, v)) = T_0(Q(x_0, u, v)), \]
\[ Q(H(u), v) + Q(H(u), v) = Q(u, v)^2 + Q(u) \times Q(v), \]
\[ H(H(u), v) + H(H(u), v) = T_0 \left( Q(u, H(v)) \right) u + T_0 \left( Q(H(u), v) \right) v - Q(u). H(u), \]
\[ Q(u). H(u) - Q(u). H(u) - Q(v). H(u), \]
\[ N(H(u)) = N(u)^2 - 2N_0(Q(u)). \]

**Proof.** \[ 35.8 \] yields \((x_0, u)^2 = (x_0 \times u)^2 = T(x_0^2, u) u + T(x_0, u^2) x_0 - x_0^2 \times u^2 = -T_0(x_0, Q(u)) x_0 + x_0^2 \times Q(u) - x_0^2 \times H(u) = -U_{x_0} Q(u) + x_0^2 H(u), \) and comparing \(X_0^r\) and \(V\)-components by means of \(\text{(36.7.1)}, \) we obtain \(1\). (Repeatedly) linearizing \(1\) (resp. \(3\)) implies \(4\) (resp. \(6\)). Similarly, by the adjoint identity and \(\text{(36.7.2)}\), \(N(u) u - u^2 = (-Q(u) + H(u))^2 = Q(u)^2 - Q(H(u)) + \langle Q(u). H(u) + H(H(u)) \rangle, \) which leads to \(9\) (10). Applying \(35.8\) we obtain \(N(u) x_0 - T_0(x_0, Q(u)) u = N(u) x_0 + T(u^2, x_0) u = u^2 \times (u \times x_0) = -(x_0, u) \times (-Q(u) + H(u)) = -Q(u). (x_0, u) + Q(x_0, u, H(u)) - H(x_0, u, H(u)), \) hence \(15\) and the first relation of \(11\). Similarly, \(35.8\) implies \(N(u) x_0 = N(u) x_0 + T(u, x_0) u^2 = u \times (u^2 \times x_0) = u \times (-Q(u) + x_0 + H(u)) = (x_0 \times Q(u)). u + Q(u, x_0, H(u)) - H(u, x_0, H(u)) \) implies \(14\) and the second relation of \(11\). Linearizing \(11\) for \(x_0 = 1\) with respect to \(u\) and applying \(36.7\) gives \(Q(v, H(u)) + Q(u, H(u)) = T(u^2, v) 1 = T(H(u), v) 1 = T_0(Q(H(u), v)) 1, \) hence \(12\). To derive \(15\), we apply \(1\) and \(35.8\) to obtain \(T_0(x_0, Q(u, v)) = -T(0, x_0, v) = T(0, x_0, v) = T(x_0, u, v) = T_0(Q(x_0, u, v)) 1 \) by \(36.7.4\). Next \(16, 17\) will follow from \(9, 10\), respectively, by using the second order chain and product rules of the differential calculus for polynomial laws; we omit the details. And fi-
nally, turning to (18), we combine (35.8.18) with (36.7.1), (36.7.3), (9) and obtain
\[ N(u)^2 = N(u^2) = N(-Q(u) + H(u)) \]
\[ = -N_0(Q(u)) + T_0(Q(u), Q(H(u))) + N(H(u)) \]
\[ = -N_0(Q(u)) + T_0(Q(u), Q(u)^2) + N(H(u)) \]
\[ = -N_0(Q(u)) + 3N_0(Q(u)) + N(H(u)) \]
by Euler’s differential equation (35.8.11), and (18) follows. \qed

36.9. The build-up. The identities derived in the preceding subsection provide the opportunity of building up new cubic norm structures out of old ones. Let \( X_0 \) be a cubic norm structure over \( k \), with base point 1, adjoint \( x_0 \mapsto x_0^\ast \), norm \( N_0 \), (bi-)linear trace \( T_0 \) and quadratic trace \( S_0 \). Suppose we are given
(i) a \( k \)-module \( V \),
(ii) a bilinear action \( X_0 \times V \to V, (x_0, u) \mapsto x_0 \cdot u \),
(iii) quadratic maps \( Q : V \to X_0, H : V \to V \) such that \( Q(u, H(u)) \in R1_R \) for all \( u \in V_R, R \in k\text{-alg} \).
Since \( 1 \in X_0 \) is a unimodular vector, condition (iii) yields a unique cubic form \( \tilde{N} : V \to k \) such that
\[ \tilde{N}(u)1_R = Q(u, H(u)) \quad (u \in V_R, R \in k\text{-alg}). \]

Put \( X := X_0 \oplus V \) as a \( k \)-module, identify \( X_0, V \) canonically as submodules of \( X \) and define a cubic form \( \tilde{N} : X \to k \) as well as a quadratic map \( \tilde{\sharp} : X \to X \) by requiring that
\[ (x_0 \oplus u)^\ast := (x_0^\ast - Q(u)) \oplus (-x_0 \cdot u + H(u)), \]
\[ N(x_0 \oplus u) := N_0(x_0) - T_0(x_0, Q(u)) + \tilde{N}(u) \]
hold strictly for all \( x_0 \in X_0, u \in V \). Inspecting (2), (3), we see that the \( k \)-module \( X \) together with the base point 1, adjoint \( \tilde{\sharp} \) and norm \( \tilde{N} \) is a cubic array over \( k \) whose adjoint bilinearizes to
\[ (x_0 \oplus u) \times (y_0 \oplus v) = (x_0 \times y_0 - Q(u, v)) \oplus (-x_0 \cdot v - y_0 \cdot u + H(u, v)) \]
for all \( x_0, y_0 \in X_0, u, v \in V \). We also claim that the (bi-)linear and the quadratic trace of \( X \) are given by
\[ T(y_0 \oplus v, z_0 \oplus w) = T_0(y_0, z_0) + T_0(Q(v, w)), \]
\[ T(y_0 \oplus v) = T_0(y_0) \]
\[ S(x_0 \oplus u) = S_0(x_0) - T_0(Q(u)) \]
for \( x_0, y_0, z_0 \in X_0, u, v, w \in V \). Indeed, differentiating (3) implies
\[ N(x_0 \oplus u, y_0 \oplus v) = N_0(x_0, y_0) - T_0(x_0, Q(u, v)) - T_0(Q(u), y_0) + \hat{N}(u, v), \quad (8) \]

where putting \( x_0 = 1, \ u = 0 \) (resp. \( y_0 = 1, \ v = 0 \)) yields \( (6) \) (resp. \( (7) \)). Now \( (5) \) follows by linearizing \( (5) \) and applying \( (35.2.10) \).

**36.10. Proposition** (Petersson-Racine [102, Lemma 3.3]). *For \( X \) as defined in 36.9 to be a cubic norm structure over \( k \) it is necessary and sufficient that the following identities hold in all scalar extensions.*

1. \( u \equiv u \), \( (1) \)
2. \( x_0^2 \cdot (x_0 \cdot u) = N_0(x_0)u \), \( (2) \)
3. \( Q(x_0 \cdot u) = U_{x_0}Q(u) \), \( (3) \)
4. \( H(x_0 \cdot u) = x_0^2 \cdot H(u) \), \( (4) \)
5. \( Q(H(u)) = Q(u)^2 \), \( (5) \)
6. \( H(H(u)) = \hat{N}(u)u - Q(u) \cdot H(u) \), \( (6) \)
7. \( Q(x_0 \cdot u, H(u)) = \hat{N}(u)x_0 \), \( (7) \)
8. \( Q(H(u), v) + Q(u, H(u), v) = T_0 \left( Q(H(u), v) \right) 1, \) \( (8) \)
9. \( T_0(x_0, Q(u, v)) = T_0(Q(x_0 \cdot u, v)) \), \( (9) \)
10. \( H(x_0 \cdot u, H(u)) = T_0(x_0, Q(u))u - Q(u) \cdot (x_0 \cdot u). \) \( (10) \)

**Proof.** Assume first that \( X \) is a cubic norm structure. Then the set-up described in 36.9 shows that \( (X_0, V) \) is complemented cubic norm substructure of \( X \). Moreover, the identities \( (1) - (10) \), being a subset of the ones assembled in \( 36.3 \) and \( 36.8 \) hold strictly for \( x_0 \in X_0, \ u, v \in V \). Conversely, let this be so. We must show the unit, gradient, and adjoint identity. The unit identity is the least troublesome since the unit identity for \( X_0 \) combined with \( (36.9.2) \), \( (36.9.6) \) and \( (1) \) imply \( 1 \times x_0 = 1 \times x_0 - 1 \cdot u = T(x_0, u)1 - x_0 - u = T(x_0 \oplus u)1 - (x_0 \oplus u) \). In order to derive the gradient identity, we differentiate \( (36.9.1) \) and combine the result with \( (8) \) to obtain \( \hat{N}(u, v)1 = Q(v, H(u)) + Q(u, H(u), v) = T_0(Q(H(u), v))1, \) hence

\[ \hat{N}(u, v) = T_0 \left( Q(H(u), v) \right). \quad (11) \]

Now \( (36.9.8) \), the gradient identity for \( X_0 \) and \( (11), \ (9), \ (36.9.5), \ (36.9.2) \) imply
\[ N(x_0 \oplus u, y_0 \oplus v) = T_0(x_0^7, y_0) - T_0(x_0, Q(u), v) - T_0(Q(u), y_0) + T_0(Q(H(u), v) \]
\[ = T_0(x_0^7 - Q(u), y_0) - T_0(Q(x_0, u), v) + T_0(Q(H(u), v) \]
\[ = T_0(x_0^7 - Q(u), y_0) + T_0(Q(-x_0 \cdot u + H(u), v) \]
\[ = T((x_0^7 - Q(u)) \oplus (-x_0 \cdot u + H(u)), y_0 \oplus v) \]
\[ = T((x_0 \oplus u)^7, y_0 \oplus v), \]

as claimed. Finally, we apply the adjoint identity for \( X_0 \) and (36.9.2), (5), (3), (7), (2), (4), (10), (9), (35.8.15), (36.9.13) to derive
\[
(x_0 \oplus u)^{\#} = \left( (x_0^7 - Q(u)) \oplus (-x_0 \cdot u + H(u)) \right)^7 \]
\[ = \left( (x_0^7 - Q(u))^7 - Q(-x_0 \cdot u + H(u)) \right) \]
\[ \oplus \left( (x_0^7 - Q(u))^7 - Q(-x_0 \cdot u + H(u)) \right) \cdot (-x_0 \cdot u + H(u)) + H(-x_0 \cdot u + H(u)) \]
\[ = \left( x_0^7 - x_0^7 \times Q(u) + Q(u)^7 - Q(x_0 \cdot u) + Q(x_0 \cdot u, H(u)) - Q(H(u)) \right) \]
\[ \oplus \left( x_0^7 \cdot (x_0 \cdot u) - x_0^7 \cdot H(u) - Q(u) \cdot (x_0 \cdot u) + Q(u) \cdot H(u) + H(x_0 \cdot u) \right) \]
\[ = \left( N_0(x_0)x_0 - x_0^7 \times Q(u) - U_0^7 Q(u) + \hat{N}(u)x_0 \right) \]
\[ \oplus \left( N_0(x_0)u - T_0(x_0, Q(u))u + \hat{N}(u)u \right) \]
\[ = \left( N_0(x_0)x_0 - T_0(x_0, Q(u))x_0 + \hat{N}(u)x_0 \right) \]
\[ \oplus \left( N_0(x_0)u - T_0(x_0, Q(u))u + \hat{N}(u)u \right) \]
\[ = N(x_0 \oplus u)(x_0 \oplus u), \]

hence the adjoint identity for \( X \). □

### 36.11. Passing to isotopes

Let \( X_0 \) be a cubic norm substructure of \( X \) and \( p \) a regular element of \( X_0 \). Then \( X_0^{(p)} \), the \( p \)-isotope of \( X_0 \), is a cubic norm substructure of \( X^{(p)} \), and (35.11.4) shows
\[ X_0^{(p)}_{-1} = X_0^{-1} \quad (1) \]

as \( k \)-submodules of \( X \). Moreover, the natural action of \( X_0^{(p)} \) on \( X_0^{(p)}_{-1} \) as defined in (36.11.3) is given by the formula
\[ x_0 \cdot (p) u = p \cdot (x_0 \cdot u) \quad (2) \]
for \(x_0 \in X_0^{(p)}\) and \(u \in X_0^{(p)\perp}\). Indeed, (35.11.2) and (36.3.2) imply
\[
x_0^{(p)} u = -x_0 \times u = -N(p)U_{p^{-1}}(x_0 \times u) = N(p)U_{p^{-1}}(x_0 \cdot u)
= N(p^{-1})^{-1} p^{-1} \cdot (x_0 \cdot u) = (p^{-1})^{-1} \cdot (x_0 \cdot u) = p \cdot (x_0 \cdot u),
\]
as claimed. Similarly, one checks that \(u \in X^{(p)}\) is strongly orthogonal to \(X_0^{(p)}\) if and only if it is strongly orthogonal to \(X_0\), in which case
\[
u^{(2,p)} = p \cdot u^* .
\]

### 36.12. Complemented cubic norm substructures under isotopy
Let \((X_0, V)\) be a complemented cubic norm substructure of \(X\) and \(p\) a regular element of \(X_0\). From (36.5.11), (36.11.1) and (36.11.2) we conclude that \((X_0, V)^{(p)} := (X_0^{(p)}, V)\) is a complemented cubic norm substructure of \(X^{(p)}\). Writing \(Q^{(p)}, H^{(p)}\) for the analogues of \(Q, H\) as defined in 36.7 with \((X_0, V)\) replaced by \((X_0, V)^{(p)}\), we claim
\[
Q^{(p)}(u) = N(p)U_{p^{-1}}Q(u), \quad H^{(p)}(u) = p \cdot H(u) \quad (u \in V).
\]

Indeed, applying (36.7.1), (35.11.2), (36.11.2) we get
\[
-Q^{(p)}(u) + H^{(p)}(u) = u^{(2,p)} = N(p)U_{p^{-1}}u^* = -N(p)U_{p^{-1}}Q(u) + N(p)U_{p^{-1}}H(u)
= -N(p)U_{p^{-1}}Q(u) + N(p^{-1})^{-1}(p^{-1})^*H(u)
= -N(p)U_{p^{-1}}Q(u) + (p^{-1})^{-1}H(u)
= -N(p)U_{p^{-1}}Q(u) + p \cdot H(u),
\]
and comparing the components in \(X_0, V\), respectively, the assertion follows.

### Exercises

194. Cubic solutions to the eiconal equation

(Tkachev). Let \(k\) be a commutative ring containing \(\frac{1}{2}\). By an eiconal triple over \(k\) we mean a triple \((V, Q, N)\) consisting of a quadratic space \((V, Q)\) over \(k\) and a cubic form \(N: V \to k\) such that the quadratic map \(H: V \to V\) uniquely determined by the strict validity of
\[
Q(H(u), v) = \frac{1}{3} N(u, v)
\]
in \(V \times V\) strictly satisfies the eiconal equation
\[
Q(H(u)) = Q(u)^2
\]
in \(V\). Prove:

(i) If \((V, Q, N)\) is an eiconal triple over \(k\), then the \(k\)-module \(X := k \oplus V\) together with the base point \(1 \in X\), the adjoint \(X \to X, x \mapsto x^2\) and the norm \(N\): \(X \to k\) respectively defined by
for $R \in k$-alg, $r \in R$, $u \in V_k$, is a non-singular cubic norm structure over $k$.

(ii) Conversely, let $X$ be a non-singular cubic norm structure over $k$. Then $X_0 := kI \subseteq X$ is a non-singular cubic norm substructure, and if we put $V := X_0^\perp$ to define $Q : V \to k$ by the condition $Q(u) + u^2 \in V$ for all $u \in V$, then $(V, Q, N|_V)$ is an eiconal triple over $k$.

(iii) The constructions presented in (i), (ii) are inverse to each other.

(iv) If $(R^n, Q, N)$ is an eiconal triple over the field of real numbers, then the eiconal equation \( EICCO \) takes on the co-ordinate form

$$
\sum_{i,j=1}^n q_{ij} \frac{\partial N}{\partial x_i}(u) \frac{\partial N}{\partial x_j}(u) = 9 \left( \sum_{i,j=1}^n q_{ij}u_iu_j \right)^2 \tag{7}
$$

for

$$
u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{R}^n,
$$

where $Q = (q_{ij}) \in \text{Sym}_n(\mathbb{R}) \cap \text{GL}_n(\mathbb{R})$ corresponds to the quadratic form $Q$ and $Q^{-1} = (q^{ij})$.

## 37. Elementary idempotents and cubic Jordan matrix algebras

Elementary idempotents have been a useful tool in our study of composition algebras. As will be seen in the present section, the natural extension of this concept to cubic Jordan algebras turns out to be even more momentous. After introducing the concept itself, we describe the Peirce decomposition relative to elementary idempotents, and to complete orthogonal systems thereof, called elementary frames, purely in terms of cubic norm structures. We then proceed to define cubic Jordan matrix algebras, containing the diagonal elementary frame as a particularly useful constituent. This is underscored by the Jacobson co-ordinatization theorem, to be proved at the very end of this section, which basically says that every cubic Jordan algebra containing an elementary frame which is connected (cf. Exc. \[180\]) is isomorphic to a cubic Jordan matrix algebra.

Throughout this section, we let $k$ be a commutative ring and, unless other arrangements have been made, let $J$ be a cubic Jordan algebra over $k$, with adjoint $x \mapsto x^\dagger$, norm $N = N_J$, (bi-)linear trace $T = T_J$ and quadratic trace $S = S_J$.

### 37.1. The concept of an elementary idempotent

An element $e \in J$ is called an elementary idempotent if $e^2 = 0$ and $T(e) = 1$. In this case, $S(e) = T(e^2) = 0$, and \[35.8\] implies $e^2 = e$, so $e$ is indeed an idempotent and a unimodular one at that. In particular, the adjoint identity yields $N(e)e = e^{2i} = 0$, hence $N(e) = 0$. We also have $T(e,e) = T(e^2) = 2S(e)$ by \[35.8\], hence $T(e,e) = 1$. Note by the base point identities \[35.8\] that $1 = 1_J$ is an elementary idempotent if and only if
\[ k = \{0\} \text{ (hence } J = \{0\}) \text{. The property of being an elementary idempotent is clearly preserved by homomorphisms and scalar extensions of cubic Jordan algebras.}

### 37.2. Proposition

(cf. Racine [108], Petersson-Racine [104]). Let \( e \) be an elementary idempotent of \( J \).

(a) The complementary idempotent \( f = 1 - e \) satisfies \( f^2 = e \) and \( T(f) = 2 \).

(b) The Peirce components of \( J \) relative to \( e \) are orthogonal with respect to \( T \) and can be described as

\[
\begin{align*}
J_2(e) &= ke, \\
J_1(e) &= \{x \in J \mid T(x) = 0, e \times x = 0\}, \\
J_0(e) &= \{x \in J \mid e \times x = T(x)f - x\}.
\end{align*}
\]

(c) \( x^2 = S(x)e \) for all \( x \in J_0(e) \).

**Proof.**

(a) \( f^2 = (1 - e)^2 = 1^2 - 1 \times e + e^2 = 1 - T(e)1 + e = e \) and \( T(f) = T(1) - T(e) = 3 - 1 = 2 \).

(b) Let \( x_i \in J_i \) be \( J_i(e) \) for \( i = 0, 1, 2 \). We must show \( T(x_i, x_j) = 0 \) for \( i, j = 0, 1, 2 \) distinct. First of all, Thm. [34.2] and (35.8.31) yield \( T(x_2, x_1 + x_0) = T(U_e x_2, x_1 + x_0) = T(x_2, U_e (x_1 + x_0)) = 0 \), hence \( T(x_2, x_1) = T(x_2, x_0) = 0 \). Similarly, \( T(x_0, x_1) = T(U_f x_0, x_1) = T(x_0, U_f x_1) = 0 \) since \( J_i(f) = J_{2-i} \) by Cor. [34.3] (b). This proves the first part of (b).

As to the explicit description of the Peirce components, we have \( J_2(e) = \text{Im}(U_e) \) by (34.2) and \( U_e x = T(e, x)e - e^2 \times x = T(e, x)e \) \( e \in J \), hence \( J_2(e) \subseteq ke \).

Here the relation \( U_e e = e^3 = e \) gives equality. To prove (2), (3), we apply (35.8.23) to obtain \( e \times x = e \circ x - T(e)x - T(x)e + (T(e)T(x) - T(e, x))1 = e \circ x - x + T(x)f - T(e, x)1 \), hence

\[ e \circ x = x + e \times x - T(x)f + T(e,x)1 \quad (x \in J). \]

But \( x \in J_1 \) if and only if \( e \circ x = x \) by (34.2.7), and from (4) we conclude

\[ x \in J_1 \iff e \times x = T(x)f - T(e,x)1. \]

Now suppose \( x \in J_1 \). Then \( T(e, x) = T(f, x) = 0 \) by the first part, hence \( T(x) = T(e, x) + T(f, x) = 0 \), and (5) yields \( e \times x = 0 \) as well. Conversely, suppose \( e \times x = 0 \) and \( T(x) = 0 \). Taking traces of the first equation, we conclude \( 0 = T(e \times x) = T(e)T(x) - T(e, x) = -T(e, x) \), and (5) shows \( x \in J_1 \). This proves (2). Turning to (3), let \( x \in J_0 \). Then \( e \circ x = 0 \) by (34.2.6) and \( T(e, x) = 0 \) by the first part, forcing \( e \times x = T(x)f - x \) by (4). Conversely, if this relation holds, then \( T(x) = 2T(x) - T(x)T(f) - T(x) = T(e \times x) = T(e)T(x) - T(e, x) = T(e) - T(e, x) \), which implies \( T(e, x) = 0 \) and then \( T(x) = T(1, x) = T(e, x) + T(f, x) = T(f, x) \). Thus (a) gives \( U_f x = T(f, x)f - f^2 \times x = T(x)f - e \times x = x \), forcing \( x \in J_0 \), and the proof of (b) is complete.
(c) For $x \in J_0 = J_2(f)$ we have $x = U_j x$, and \((35.8.20)\) combined with (a) implies $x^2 = (U_j x)^2 = U_j x^2 = U_e x^2$. Hence $x^2 \in J_2 = ke$, and we find a scalar $\alpha \in k$ with $x^2 = \alpha e$. Taking traces, (c) follows. □

37.3. Corollary (Faulkner \[28\] Lemma 1.5]). With the notation and assumptions of Prop. 37.2 write $M_0$ for $J_0(e)$ as a $k$-module and $S_0$ for the restriction of $S$ to $M_0$. Then $(M_0, S_0, f)$ is a pointed quadratic module over $k$ and $J_0(e) = J(M_0, S_0, f)$ as Jordan algebras. Moreover, trace and conjugation of $(M_0, S_0, f)$ are respectively given by the restriction of $T$ to $J_0(e)$ and by the assignment $x \mapsto T(x) f - x$.

Proof. The relation $S_0(f) = T(f^2) = T(e) = 1$ shows that $(M_0, S_0, f)$ is a pointed quadratic module over $k$ with trace $x \mapsto S_0(f, x) = T(f^2 x) = T(f) T(x) - (f, x) = 2T(y) - T(y) = T(x)$ since $T(e, x) = 0$ by Prop. 37.2 (b). Hence the trace of $(M_0, S_0, f)$ is as indicated and, consequently, so is its conjugation, denoted by $x \mapsto \bar{x}$. Moreover, for $x, y \in M_0$, we compute $S_0(x, y) = T(x, y) = T(x) T(y) - T(x, y) = T(x, f) T(y) - T(x, y) = T(x, (y) f - y) = T(x, \bar{y})$, which combines with \((37.2.3)\) and Prop. 37.2 (c) to imply that the $U$-operator of $J_0$ agrees with $U_2 \bar{y} = T(x, y)x - y^2 = S_0(x, y)x - S_0(x) e \times y = S_0(x, y)x - S_0(x) (T(y) f - y) = S_0(x, \bar{y})x - S_0(x) \bar{y}$, hence with the $U$-operator of $J(M_0, S_0, f)$. □

In our subsequent computations, we conveniently subscribe to what we call

37.4. The ternary cyclicity convention. Unless explicitly stated otherwise, indices $i, j, l$ (or $m, n, p$) are always tacitly assumed to vary over all cyclic permutations $(i j l)$ (or $(m n p)$) of \((123)\). For example, given arbitrary elements $x_{ij}$ of an arbitrary $k$-module, this convention allows us to write $\sum x_{ij}$ for $x_{123} + x_{231} + x_{312}$.

37.5. Proposition. Elementary idempotents $e_1, e_2 \in J$ are orthogonal if and only if $e_1 \times e_2 = 1 - e_1 - e_2 =: e_3$. In this case, $(e_1, e_2, e_3)$ is a complete orthogonal system of elementary idempotents in $J$, and with the corresponding Peirce decomposition $J = \sum (J_{ii} + J_{jl})$, the following statements hold.

(a) $e_1 \times e_j = e_i$.
(b) $J_{ii} = ke_i$.
(c) The Peirce components of $J$ relative to $(e_1, e_2, e_3)$ are orthogonal with respect to the bilinear trace.
(d) The linear trace of $J$ vanishes on $J_{23} + J_{31} + J_{12}$.
(e) $x \circ y = x \times y$ for all $x \in J_{ij}, y \in J_{ji}$.
(f) $x^2 = -S(x)(e_j + e_l)$ for all $x \in J_{ji}$.

Proof. The very first assertion follows from \((37.2.3)\) and the following chain of equivalent conditions.

\[
e_1, e_2 \text{ are orthogonal } \iff e_2 \in J_0(e_1) \iff e_1 \times e_2 = T(e_2)(1-e_1) - e_2 \iff e_1 \times e_2 = e_3.
\]
In this case, \( T(e_3) = T(1) - T(e_1) - T(e_2) = 3 - 1 - 1 = 1 \), and applying (35.8.10) we obtain
\[
\begin{align*}
\hat{c}_3 &= (e_1 \times e_2)^2 = T(e_1^2, e_2) e_2 + T(e_1, e_2^2) e_1 - e_1^2 \times e_2^2 = 0.
\end{align*}
\]
Hence \( e_3 \) is an elementary idempotent, making \((e_1, e_2, e_3)\) a complete orthogonal system of the desired kind.

(a) is now clear by symmetry.

(b) This is just (34.11.2) and (37.2.1).

(c), (d) By (34.11.3), we have \( J_{ij} \subseteq J_i(e_i) \cap J_0(e_i) \). Therefore \( T(e_i, J_{ij}) = T(e_i, J_{ij}) = T(J_{ij}, J_{ij}) = \{0\} \), giving (c) and \( T(J_{ij}) = T(\sum e_i, J_{ij}) = \{0\} \), hence (d).

(e) By (c), (d), \( T(x) = T(y) = T(x, y) = 0 \), and (35.8.23) yields the assertion.

(f) We have \( x \in J_0(e_i) \) by (34.11.2), and Cor. 37.3 combined with (d) implies \( x^2 = T(x) x - S(x)(1-e_i) = -S(x)(e_j + e_i) \).

\[\square\]

37.6. The concept of an elementary frame. Adapting the terminology of Loos [67, 10.12] to the present set-up, we define an elementary frame of \( J \) to be a complete orthogonal system of elementary idempotents of length 3 in \( J \). By Prop. 37.5, an elementary frame of \( J \) has length 3 unless \( k = \{0\} \) and the length can be arbitrary.

If \((e_1, e_2, e_3)\) is an elementary frame of \( J \), then we write
\[ J = \sum (J_{ii} + J_{ij}) \]
for the corresponding Peirce decomposition. Combining Prop. 37.2(b) with (34.11.2), (34.11.3), we conclude
\[ J_{ii} = k e_i, \quad J_{ij} = \{x \in J \mid T(x) = 0, \ e_j \times x = e_i \times x = 0\}. \]

Elementary idempotents are intimately tied up with a particularly important class of cubic Jordan algebras, called cubic Jordan matrix algebras. Since the formal definition of this concept looks rather artificial at first, we begin by describing its intuitive background.

In Exc. [180], we have introduced the concept of (strong) connectedness for orthogonal systems of idempotents. In the present set-up, this concept allows a natural characterization by means of data belonging exclusively to the underlying cubic norm structure.

37.7. Proposition. Let \((e_1, e_2, e_3)\) be an elementary frame of \( J \) with the Peirce decomposition \( J = \sum (k e_i + J_{ij}) \). For elements \( u_{ij} \in J_{ij} \), the following conditions are equivalent.

(i) \( e_j \) and \( e_i \) are connected (resp. strongly connected) by \( u_{ij} \).

(ii) \( S(u_{ij}) \in k^\times \) (resp. \( S(u_{ij}) = -1 \)).

Proof. By Cor. 37.3, we have \( J_2(e_j + e_i) = J_0(e_i) = J(M_0, S_0, f) \), where \( M_0 = J_0(e_i) \) as \( k \)-modules, \( S_0 = S|_{M_0} \) and \( f = 1 - e_i = e_j + e_i \). Now \( e_j \) and \( e_i \) are connected by \( u_{ij} \) if and only if \( u_{ij} \in J_2(e_j + e_i)^\times \), which by Exc. [168] happens if and only if
$S(u_{ji}) = S_0(u_{ji}) \in k^\times$. On the other hand, $u_{ji}^2 = -S(u_{ji})(e_j + e_i)$ by Prop. 37.5 (f), so $e_j$ and $e_i$ are strongly connected by $u_{ji}$ if and only if $S(u_{ji}) = -1$. □

### 37.8. Twisted matrix involutions.

Let $C$ be a conic algebra over $k$ whose conjugation is an involution, and which is faithful as a $k$-module, allowing us to identify $k \subseteq C$ canonically as a unital subalgebra. If $m$ is a positive integer, then $\text{Mat}_m(k) \subseteq \text{Mat}_m(C)$ by Exc. 35 is a nuclear subalgebra. Twisting the conjugate transpose involution of $\text{Mat}_m(C)$ in the sense of 11.8 by means of a diagonal matrix $\Gamma = \text{diag}(\gamma_1, \ldots, \gamma_m) \in \text{GL}_m(k)$, we therefore conclude that the map

$$\text{Mat}_m(C) \to \text{Mat}_m(C), \quad x \mapsto \Gamma^{-1}x^t \Gamma$$

in the sense of 11.9, we therefore conclude that the map

$$\Gamma = \text{diag}(\gamma_1, \ldots, \gamma_m) \in \text{GL}_m(k)$$

is an involution, called the $\Gamma$-twisted conjugate transpose involution of $\text{Mat}_m(C)$. The elements of $\text{Mat}_m(C)$ remaining fixed under this involution are called $\Gamma$-twisted hermitian matrices, and simply hermitian matrices if $\Gamma = 1_m$ is the $m \times m$ unit matrix. The $\Gamma$-twisted hermitian matrices of $\text{Mat}_m(C)$ having diagonal entries in $k$ form a $k$-submodule of $\text{Mat}_m(C)$ which we denote by

$$\text{Her}_m(C, \Gamma);$$

in particular, we put

$$\text{Her}_m(C) := \text{Her}_m(C, 1_m).$$

If $\frac{1}{2} \in k$, then $\text{Her}_m(C, \Gamma)$ is the totality of all $\Gamma$-twisted hermitian matrices in $\text{Mat}_m(C)$, the condition on the diagonal entries being automatic since $H(C, C) = k1_C = k$ by (19.6.3).

Now assume $m = 3$. Writing $e_{ij}$, $1 \leq i, j \leq 3$ for the ordinary matrix units of $\text{Mat}_3(k) \subseteq \text{Mat}_3(C)$, we obtain a natural set of generators for the $k$-module $\text{Her}_3(C, \Gamma)$ by considering the quantities

$$u_{[jl]} := \gamma_{ij}e_{jl} + \gamma_{jl}u_{ij} \quad (u \in C, \ j, l = 1, 2, 3 \ \text{distinct}).$$

Indeed, a straightforward verification shows that $x \in \text{Mat}_3(C)$ belongs to $\text{Her}_3(C, \Gamma)$ if and only if it can be written in the form (necessarily unique)

$$x = \sum (\xi_i e_{ii} + u_{[jl]}) \quad (\xi_i \in k, \ u_i \in C, \ i = 1, 2, 3).$$

Thus we have a natural identification

$$\text{Her}_3(C, \Gamma) = \sum (ke_{ii} \oplus C[ji]) = (k \oplus C) \oplus (k \oplus C) \oplus (k \oplus C)$$

as $k$-modules.
With a few extra hypotheses on $C$, we wish to define a cubic norm structure on the $k$-module $\text{Her}_3(C, \Gamma)$ in a natural way that commutes with base change. Actually, we will be able to do so without any conditions on $C$ as a $k$-module, and without assuming that the diagonal matrix $\Gamma \in \text{Mat}_3(k)$ be invertible. This will be accomplished by formalizing the preceding set-up in a slightly different manner. We begin by introducing a convenient terminology.

**37.9. Co-ordinate pairs.** By a pre-co-ordinate pair over $k$ we mean a pair $(C, \Gamma)$ consisting of a multiplicative conic alternative $k$-algebra $C$ and a diagonal matrix $\Gamma \in \text{Mat}_3(k)$. In this case, it will always be tacitly assumed that $\Gamma$ has the form $\Gamma = \text{diag}(\gamma_1, \gamma_2, \gamma_3)$, with $\gamma_i \in k, 1 \leq i \leq 3$. If $\Gamma$ is invertible, we speak of a co-ordinate pair over $k$. For $\Gamma = 1_3$, we identify $C = (C, 1)$ and refer to this as a co-ordinate algebra over $k$. If $C$ is an octonion algebra, the terms octonionic (pre-)co-ordinate pair, octonionic co-ordinate algebra, respectively, will be used, ditto for $C$ being a quaternion or quadratic étale $k$-algebra.

**37.10. Towards a hermitian cubic norm structure.** Let $(C, \Gamma)$ be a pre-co-ordinate pair over $k$. By Prop. 20.2, $C$ is norm-associative (i.e., the identities (19.1.1)-(19.1.5) hold in $C$) and its conjugation is an involution. Guided by the formulas of (37.8), but abandoning their interpretation by means of hermitian matrices, we consider the $k$-module of all formal expressions

$$\sum (\xi_i e_{ii} + u_i[jl])$$

for $\xi_i \in k, u_i \in C$ and $i = 1, 2, 3$. Thanks to the formal character of these expressions, and in analogy of (37.8), this $k$-module, denoted by $X(C)$, may be written as

$$X(C) = \sum (ke_{ii} + C[jl]) = (k \oplus C) \oplus (k \oplus C) \oplus (k \oplus C),$$

and hence its dependence on $C$ is compatible with base change: $X(C)_R = X(C_R)$ for all $R \in k\text{-alg}$. Note, however, that the diagonal matrix $\Gamma \in \text{Mat}_3(k)$ has not yet entered the scene, which will happen only after we have given $X(C)$ the structure of a cubic array over $k$. In order to do so, we consider elements

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

of $X(C)_R$, with $x_i, \eta_i \in R, u_i, v_i \in C_R$ for $i = 1, 2, 3$, to define base point, adjoint and norm on $X(C)$ by the formulas

$$1 = 1_x := \sum e_{ii},$$

$$x^2 = \sum \left( (\xi_i e_{ii} - \gamma_i \nu_i \eta_i C(u_i)) e_{ii} + (- \xi_i u_i + \gamma_i u_i^3) [jl] \right),$$

$$N(x) := N_x(x) = \xi_1 \xi_2 \xi_3 - \sum \gamma_i \gamma_i \eta_i \nu_i \eta_i C(u_i) + \gamma_1 \gamma_2 \gamma_3 \nu_1 \nu_2 \nu_3 u_1 u_2 u_3,$$

the very last expression on the right of (5) being unambiguous by (19.1.1). One checks easily that these formulas make $X(C)$ a cubic array over $k$, which we denote
by \( \text{Her}_3(C, \Gamma) \) and which is clearly compatible with base change: \( \text{Her}_3(C, \Gamma)_R = \text{Her}_3(C_R, \Gamma_R) \) for all \( R \in \text{k-alg} \). Moreover, the adjoint bilinearizes to

\[
x \times y = \sum \left( (\xi_j \eta_i + \eta_j \xi_i - \gamma_{ij} \eta n_c(u_i, v_i)) e_{ii} \right) + (\xi_j v_i - \eta v_i) + \gamma_{ij} v_i (j \neq l),
\]

and we claim that the (bi-)linear and quadratic trace of \( X \) are given by

\[
T(x, y) = \sum (\xi_j \eta_i + \gamma_{ij} \eta n_c(u_i, v_i)),
\]

\[
T(x) = \sum \xi_j, \quad S(x) = \sum (\xi_j \xi_l - \gamma_{ij} \eta n_c(u_i)),
\]

Indeed, differentiating (5) at \( x \) in the direction \( y \), we obtain, using (19.12[1]),

\[
N(x, y) = \sum (\xi_j \xi_i \eta_i - \gamma_{ij} \eta (\eta n_c(u_i) + \xi_j \eta n_c(u_i, v_i)) + \gamma_{ij} \eta n_c(u_i, v_i)),
\]

and setting \( x = 1 \) gives (8), while setting \( y = 1 \) yields (9). On the other hand, linearizing (7) we deduce

\[
S(x) = \sum (\xi_j \eta_i + \eta_j \xi_i - \gamma_{ij} \eta n_c(u_i, v_i)).
\]

Finally, combining (11) with (8) and (35.2[10]), we end up with (7).

37.11. Theorem (Freudenthal [32, 33], McCrimmon [77]). Let \((C, \Gamma)\) be a pre-co-ordinate pair over \( k \). Then the cubic array \( \text{Her}_3(C, \Gamma) \) of \( 37.10 \) is a cubic norm structure over \( k \).

**Proof.** The unit (resp. gradient) identity follows from (37.10[5]), (37.10[6]), (37.10[8]) (resp. (37.10[4]), (37.10[7]), (37.10[11])) by a straightforward verification. It remains to prove the adjoint identity over \( k \). To this end we put

\[
x^2 = \sum (\xi_j^2 u_i + \eta_j^2 [j \neq l]),
\]

where \( \xi_j^2 \in k \) and \( \eta_j^2 \in C \) can be read off from (37.10[4]). We must show \( \xi_j^{12} = N(x) \xi_j \) and \( \eta_j^{12} = N(x) \eta_j \). We begin with the former by repeatedly applying (37.10[4]):

\[
\xi_j^{12} = \xi_j^2 \xi_j - \gamma_{ij} \eta n_c(u_i) = (\xi_j^2 \xi_j - \gamma_{ij} \eta n_c(u_i)) - \gamma_{ij} \eta n_c(-\xi_j u_i + \gamma_{ij} \eta u_j u_i).
\]

Expanding the terms on the right-hand side of the last equation and combining (19.5[7], 20.1[1], 19.5[5]) with the fact that the expression \( t_C(u_1 u_2 u_3) \) is invariant under cyclic permutations of its arguments, we conclude
as desired. Similarly, we expand
\[ u_i^{\ddagger} = -\xi_i^2 u_i + \gamma \xi_i \xi_j u_j - \gamma \xi_i \gamma \xi_j \xi_k u_k + \gamma \xi_i \gamma \xi_j \gamma \xi_k u_k + \gamma \xi_i \gamma \xi_j \gamma \xi_k u_k + \gamma \xi_i \gamma \xi_j \gamma \xi_k u_k \]

Here we combine the fact that the conjugation of \( C \) is an involution with Kirmse’s identities (20.31) to conclude
\[ u_i^{\ddagger} = (\xi_i^2 - \sum \gamma \xi_j \xi_k u_{jk} \xi_k) u_i + \gamma \xi_j \xi_k u_{jk} u_i + u_{ij} u_{ij} u_i = n_C u_i + t_C u_i \]

Thus \( u_i^{\ddagger} = N(x) u_i \), and the proof of the adjoint identity is complete. \( \Box \)

**37.12. The concept of a cubic Jordan matrix algebras.** The cubic Jordan algebra corresponding to the cubic norm structure \( \text{Her}_3(C, \Gamma) \) of Thm. 37.11 will also be denoted by \( J := \text{Her}_3(C, \Gamma) \) and is called a cubic Jordan matrix algebra. The justification of this terminology derives from the fact that, if \( 1_C \in C \) is unimodular and \( \Gamma \in \text{GL}_3(k) \), then the elements of \( J \) by 37.8 may be identified canonically with the \( \Gamma \)-twisted \( 3 \times 3 \) hermitian matrices having entries in \( C \) and scalars down the diagonal, i.e., with the matrices
\[ x = \sum (\xi_i e_i + u_i u_i) \]

for \( \xi_i \in k, u_i \in C, 1 \leq i \leq 3 \), and this identification is compatible with base change. Note, however, that the Jordan structure of \( J \) is not as closely linked to ordinary multiplication as one would naively expect. On the positive side, it follows from Exc. 19.17 below that the squaring of \( J \) and that of \( \text{Mat}_3(C) \) coincide on \( J \). Hence so do the circle product of \( J \) and the symmetric matrix product \( (x, y) \mapsto xy + yx \) of \( \text{Mat}_3(C) \). Thus, if \( \frac{1}{2} \in k \), then its linear Jordan structure make \( J \) a unital subalgebra of \( \text{Mat}_3(C)^+ \); in particular, the euclidean Albert algebra \( \text{Her}_3(\bar{\mathbb{O}}) \) of 5.5 is a (very important) example of a cubic Jordan matrix algebra over the reals. On the other
hand, returning to the case of an arbitrary base ring, if $C$ is properly alternative, then
the $k$-algebra $\text{Mat}_3(C)$ is not flexible, and the $U$-operator $U_{xy}$ of $J$ will in general
not be the same as $(xy)x$ or $x(yx)$ (Exc. [197](b)). On the other hand, the explicit formula
(7) of that exercise immediately implies the following useful observation.

37.13. Proposition. Let $(C, \Gamma)$ be a co-ordinate pair over $k$ such that $1_C \in C$ is
unimodular. If $C$ is associative, then the Jordan algebra $\text{Her}_3(C, \Gamma)$ is a subalgebra
of $\text{Mat}_3(C)^{(+)}$. □

37.14. Cubic Jordan matrix algebras and composition algebras. The most im-
portant cubic Jordan matrix algebras have the form $J = \text{Her}_3(C, \Gamma)$, where
$(C, \Gamma)$ is a co-ordinate pair and $C$ is a composition algebra. Since $C$ is finitely generated
projective as a $k$-module, so is $J$, by (37.10.1) and we deduce from (37.10.7) that
$J$ is non-singular if and only if $C$ is. Here is a special case.

37.15. Proposition. The map $\varphi : \text{Mat}_3(k)^{(+)} \to \text{Her}_3(k \oplus k)$ defined by
$$\varphi(x) := \sum (\xi_{ij} e_{ii} + (\xi_{ij} \oplus \xi_{ij})[jl])$$
for $x = (\xi_{ij})_{1 \leq i,j \leq 3} \in \text{Mat}_3(k)$ is an isomorphism of cubic Jordan algebras.

Proof. $\varphi$ is a linear bijection sending $1$ to $1_J$ with $J := \text{Her}_3(k \oplus k)$. By Ex. 35.23
and Exc. 185, therefore, it suffices to show that $\varphi$ preserves norms. Actually, since
$\varphi$ commutes with base change, we need only show $N_J(\varphi(x)) = \det(x)$ for all $x =
(\xi_{ij}) \in \text{Mat}_3(k)$. To this end we put $C := k \oplus k$ and note $n_C(\alpha \oplus \beta) = \alpha \beta$, $i_C(\alpha \oplus
\beta) = \alpha + \beta$ for $\alpha, \beta \in k$. Hence (37.10.5) implies
$$N_J(\varphi(x)) = N_J \left( \sum (\xi_{ij} e_{ii} + (\xi_{ij} \oplus \xi_{ij})[jl]) \right)$$
$$= \xi_{11} \xi_{22} \xi_{33} - \sum \xi_{ij} \xi_{lj} \xi_{ij} + \xi_{23} \xi_{31} \xi_{12} + \xi_{32} \xi_{13} \xi_{21}$$
$$- \xi_{31} \xi_{22} \xi_{13} - \xi_{32} \xi_{23} \xi_{11} - \xi_{33} \xi_{21} \xi_{12}$$
$$= \det(x),$$
as claimed. □

37.16. Elementary identities in cubic Jordan matrix algebras. Let $(C, \Gamma)$ be a
pre-co-ordinate pair over $k$. Then one checks that $\text{Her}_3(C, \Gamma)$ satisfies the identities
\[
\begin{align*}
\sum_{i=1}^{n} e_i^2 = 0, \quad T(e_i) &= 1, \quad e_i \times e_{ij} = e_{ij}, \\
e_j \times u_i[jl] &= e_l \times u_i[jl] = 0, \quad e_i \times u_i[jl] = -u_i[jl], \\
u_i[jl]^2 &= -\gamma_i \gamma_n C(u_i)e_{ll}.
\end{align*}
\] (1) (2) (3)

Moreover, for \( u \in J \):

**37.17. Proposition.** Let \((C, \Gamma)\) be a pre-co-ordinate pair over \( k \). Then \((e_{11}, e_{22}, e_{33})\) is an elementary frame in \( J := \text{Her}_3(C, \Gamma) \), called its diagonal frame, whose Peirce components are given by

\[
J_{ii} = ke_{ii}, \quad J_{jl} = C[jl].
\] (1) (PEDEI)

Moreover, for \( u \in C \), the orthogonal idempotents \( e_{jj} \) and \( e_{ll} \) are connected by \( u_i[jl] \in J_{ll} \) if and only if \( u_i \in C^\gamma \) and \( \gamma_j, \gamma_l \in k^\times \).

**Proof.** That the diagonal matrix units form an elementary frame of \( J \) follows immediately from \([37.16.1]\) combined with Prop. \([37.5]\) it remains to establish \([1]\), the first relation being obvious by \([37.6.2]\). As to the second, let

\[
x = \sum (\xi_m e_{mm} + u_m[np]) \in J \quad (\xi_m \in k, u_m \in C, m = 1, 2, 3).
\]

Then \([37.6.2], [37.16.1], [37.16.2]\) imply

\[
x \in J_{jl} \iff T(x) = 0, \quad e_{jj} \times x = e_{ll} \times x = 0 \\
\iff \sum \xi_m = 0, \\
\xi_j e_{ll} + \xi_l e_{ll} - u_j[jl] = 0 = \xi_j e_{ll} + \xi_l e_{jj} - u_l[ij] \\
\iff \xi_1 = \xi_2 = \xi_3 = 0, \quad u_j = u_l = 0 \\
\iff x = u_i[jl] \\
\iff x \in C[jl].
\]

The final statement follows immediately from Prop. \([37.5]\) and \([37.10.9]\), which implies \( S(u_i[jll]) = -\gamma_j \gamma_n C(u_i) \).

**37.18. Corollary.** The diagonal frame of \( \text{Her}_3(C, \Gamma) \) is connected if and only if \( \Gamma \in GL_3(k) \), i.e., \((C, \Gamma)\) is a co-ordinate pair over \( k \).
37.19. **Co-ordinate systems.** By a *co-ordinate system* of a cubic Jordan algebra $J$ over $k$ we mean a quintuple $\mathcal{S} = (e_1, e_2, e_3, u_{23}, u_{31}) \in J^5$ such that $(e_1, e_2, e_3)$ is an elementary frame of $J$, inducing the corresponding Peirce decomposition $J = \sum (ke_i + J_{ij})$, and for $i = 1, 2$, the orthogonal idempotents $e_j, e_l$ are connected by $u_{jl} \in J_{jl}$. We refer to $(e_1, e_2, e_3)$ as the elementary frame belonging to $\mathcal{S}$. A pair $(J, \mathcal{S})$ consisting of a cubic Jordan algebra $J$ over $k$ and a co-ordinate system $\mathcal{S}$ of $J$ will be called a *co-ordinated cubic Jordan algebra*.

37.20. **Example.** Let $(C, \Gamma)$ be a co-ordinate pair over $k$. Then Prop. 37.17 shows that

$$D(C, \Gamma) = (e_{11}, e_{22}, e_{33}, 1_C[23], 1_C[31])$$

is a co-ordinate system of the cubic Jordan algebra $\text{Her}_3(C, \Gamma)$, called its diagonal co-ordinate system. We write

$$\text{Her}_3(C, \Gamma) := (\text{Her}_3(C, \Gamma), D(C, \Gamma))$$

for the corresponding co-ordinated cubic Jordan algebra.

In the remainder of this section, we will show that, conversely, every co-ordinated cubic Jordan algebra is isomorphic to a cubic Jordan matrix algebra, under an isomorphism matching the given co-ordinate system of the former with the diagonal one of the latter. This will be the content of the Jacobson co-ordinatization theorem 37.25 below.

In order to accomplish this result, we begin with a series of preparations.

37.21. **Lemma.** We have

$$S(x \times y, z) = T(x)T(y)T(z) - T(x, y)T(z) - T(x \times y, z)$$

for all $x, y, z \in J$.

**Proof.** Applying (35.8.13) twice, we obtain

$$S(x \times y, z) = T(x \times y)T(z) - T(x \times y, z) = T(x)T(y)T(z) - T(x, y)T(z) - T(x \times y, z),$$

as claimed. \qed

37.22. **Proposition.** Let $(e_1, e_2, e_3)$ be an elementary frame of $J$ and $J = \sum (ke_i + J_{ij})$ the corresponding Peirce decomposition of $J$. Then $J_0 := \sum ke_i$ is a non-singular cubic subalgebra of $J$ canonically isomorphic to $E^+(+)$, where $E$ stands for the split cubic étale $k$-algebra. Moreover,

$$J_{ij} \times J_{jl} \subseteq J_{li},$$

and given
with $\xi, \eta \in k$, $u_{jl}, v_{jl} \in J_{jl}$, $i = 1, 2, 3$, the following relations hold.

\[
N(x) = \xi_1 \xi_2 \xi_3 + \sum \xi_i S(u_{ij}) + T(u_{23} \times u_{31}, u_{12}),
\]
\[
x^2 = \sum \left( (\xi_j \xi_i + S(u_{ij})) e_i + (- \xi_i u_{jl} + u_{jl} \times u_{ij}) \right),
\]
\[
x \times y = \sum \left( (\xi_j \eta_i + \eta_j \xi_i - T(u_{ij}, v_{jl})) e_i \right)
\]
\[
+ (- \xi_i v_{jl} - \eta_i u_{jl} + u_{jl} \times v_{ij} + v_{ij} \times u_{ij}) [jl],
\]
\[
T(x, y) = \sum \xi_i \eta_i + \sum T(u_{ij}, v_{jl}),
\]
\[
T(x) = \sum \xi_i,
\]
\[
S(x) = \sum (\xi_j \xi_i + S(u_{ij})),
\]
\[
S(x, y) = \sum (\xi_j \eta_i + \eta_j \xi_i - T(u_{ij}, v_{jl})).
\]

\[\text{Proof.} \quad \text{Relation (1)} \text{ follows from } J_{ij} \times J_{jl} = J_{ij} \circ J_{jl} \text{ (by Prop. 37.5(e)) and the Peirce rules. For the remaining assertions, we proceed in three steps.}\]

1. Noting that $J_0 = \sum k e_i$ is a direct sum of ideals by Cor. 34.12(b), our first aim will be to show that $J_0$ and $E^{(+)}$ are canonically isomorphic. Since $e_i^2 = 0$ by definition and $N(e_i) = 0$ by 37.1, combining equation (6) of Exc. 58 with Prop. 37.5(a) yields

\[
N(\sum \xi_i e_i) = \xi_1 \xi_2 \xi_3
\]

in all scalar extensions. Thus the map $\varphi: E^{(+)} \to J_0$ defined by

\[
\varphi(\xi_1 \otimes \xi_2 \otimes \xi_3) := \sum \xi_i e_i
\]

for $\xi_1, \xi_2, \xi_3 \in k$ is an isomorphism not only of Jordan algebras but, in fact, of cubic ones. Hence, 38.2+4, 38.2+5 yield

\[
(\sum \xi_i e_i)^2 = \sum \xi_j \xi_i e_i,
\]
\[
T(\sum \xi_i e_i, \sum \eta_i e_i) = \sum \xi_i \eta_i.
\]

2. We now apply the formalism of 36.7 to derive the relation

\[
V := X_0^+ = J_{23} + J_{31} + J_{12}
\]

from Prop. 37.5(c) and recall from Remark 36.6 that $(X_0, V)$ is a complemented cubic norm substructure of $J$, so it makes sense to compute the quadratic maps $Q, H$ of 36.7 in the special case at hand. Following (12), let

\[
u = u_{23} + u_{31} + u_{12} \in V, \quad u_{jl} \in J_{jl}.
\]
Prop. 37.5 (d), and (10), (14), (15) imply and combines with (3) to yield (7). Linearizing (7), we obtain giving (3). Applying Prop. 37.5 (c), we obtain (5), which immediately implies (6) since the expression \( T(x \times y, z) \) is totally symmetric in its arguments. Thus

\[
N(u)1 = Q(u, H(u)) = -\sum S(u_{ji}, u_{li} \times u_{ij})e_i,
\]

where Lemma 37.21 and Prop. 37.5 (d) imply

\[
S(u_{li} \times u_{ij}, u_{ji}) = -T(u_{li} \times u_{ij}, u_{ji}) = -T(u_{23} \times u_{31}, u_{12})
\]

since the expression \( T(x \times y, z) \) is totally symmetric in its arguments. Thus

\[
N(u) = T(u_{23} \times u_{31}, u_{12}).
\]

It is now easy to complete the proof of the proposition. Combining (36.7.3), (36.7.2) with (9), (11), (16), we obtain

\[
N(x) = N(\sum \xi_i e_i + u) = N(\sum \xi_i e_i) - T(\sum \xi_i Q(u_i) + N(u))
\]

\[
= \sum \xi_i \xi_2 \xi_3 + \sum \xi_i S(u_{ji}) + T(u_{23} \times u_{31}, u_{12}),
\]

giving (4), and

\[
x^2 = (\sum \xi_i e_i + u)^2 = \left( (\sum \xi_i e_i) - Q(u) \right) + \left( \sum \xi_i e_i \times u + H(u) \right).
\]

But \( u_{ji} \in J_0(e_i) \), while \( u_{li}, u_{ij} \in J_1(e_i) \). Hence \( e_i \times u = -u_{ji} \) by (37.2.2), (37.2.3), Prop. 37.5 (d), and (10), (14), (15) imply

\[
x^2 = \sum (\xi_j \xi_l + S(u_{ji})) e_i + \sum (-\xi_j u_{ji} + u_{li} \times u_{ij}),
\]

giving (3). Applying Prop. 37.5 (c), we obtain (5), which immediately implies (6) and combines with (3) to yield (7). Linearizing (7), we obtain

\[
S(x, y) = \sum (\xi_j \eta_l + \eta_j \xi_l + S(u_{ji}, v_{jl})).
\]

Since \( T(u_{ji}) = 0 \) by (6), we deduce \( S(u_{ji}, v_{jl}) = -T(u_{ji}, v_{jl}) \) from (35.8.13), and (8) follows, as does (4) by linearizing (3).
37.23. Lemma. Under the assumptions of Prop. 37.22 the relations

\[ S(u_{jl}, v_{jl}) = -T(u_{jl}, v_{jl}) , \]  
\[ u_{jl} \times (u_{jl} \times u_{li}) = -S(u_{jl})u_{li}, \]  
\[ (u_{li} \times u_{lj}) \times u_{ij} = -S(u_{lj})u_{li}, \]  
\[ u_{ji} \times (v_{jl} \times u_{li}) + v_{jl} \times (u_{jl} \times u_{li}) = T(u_{jl}, v_{jl})u_{li}, \]  
\[ (u_{li} \times u_{ij}) \times v_{ij} + (u_{ij} \times v_{ij}) \times u_{ij} = T(u_{ij}, v_{ij})u_{li}, \]  
\[ S(u_{jl} \times u_{li}) = -S(u_{jl})S(u_{li}) \]

hold for all \( u_{jl}, v_{jl} \in J_{jl}, u_{li} \in J_{li} \).

Proof. (1) is an immediate consequence of (37.22.8). In order to establish (2), we first note \( J_{lj} \subset J_1(e_j + e_l) \), \( J_{jl} \subset J_2(e_j + e_l) \). Hence Prop. 37.5 combined with (37.22.1) and Exc. 177 yields

\[ u_{jl} \times (u_{jl} \times u_{li}) = u_{jl} \circ (u_{jl} \circ u_{li}) = u^2_{jl} \circ u_{li} = -S(u_{jl})(e_j + e_l) \circ u_{li} = -S(u_{jl})u_{li}, \]

hence (2). An analogous computation yields (3). Linearizing (2) (resp. (3)) and combining with (1) gives (4) (resp. (5)). Finally, in order to establish (6), we apply (35.8) to conclude

\[ S(u_{jl} \times u_{li}) = T ((u_{jl} \times u_{li})^2) = T (T (u^2_{jl} \times u_{li})u_{li} + T (u_{jl}, u^2_{lj})u_{jl} - u^2_{jl} \times u^2_{li}), \]

which by Prop. 37.22 reduces to

\[ S(u_{jl} \times u_{li}) = -S(u_{jl})S(u_{li})T(e_i \times e_j) = -S(u_{jl})S(u_{li})T(e_i) = -S(u_{jl})S(u_{li}), \]

as claimed. \( \square \)

37.24. Proposition. Let \((J, \mathcal{G})\) be a co-ordinated cubic Jordan algebra over \( k \), with \( \mathcal{G} = (e_1, e_2, e_3, u_{23}, u_{31}) \) the corresponding co-ordinate system, and let \( J = \sum (ke_i + J_{jl}) \) be the Peirce decomposition of \( J \) relative to the elementary frame belonging to \( \mathcal{G} \). Then \( S(u_{jl}) \in k^x \) for \( i = 1, 2 \), and with

\[ \omega := \omega_{J, \mathcal{G}} := S(u_{23})^{-1}S(u_{31})^{-1} \in k^x, \]

the \( k \)-module

\[ C := C_{J, \mathcal{G}} := J_{12} \]

becomes a multiplicative conic alternative \( k \)-algebra with multiplication, norm, unit element, trace, conjugation respectively given by
Applying Lemma 37.23, (35.8.7), we then obtain

\[ uv := \omega(u \times u_{23}) \times (u_{31} \times v), \] 
\[ n_C(u) = -\omega S(u), \] 
\[ \omega u_{12} := u_{23} \times u_{31}, \] 
\[ \omega T(u_{12}, u), \] 
\[ \omega T(u_{12}, u) - u \]

for all \( u, v \in C \). Moreover,

\[(C, \Gamma) = (C_J, \Gamma_J, \omega) =: \text{Cop}(J, S)\]

with

\[ \Gamma := \Gamma_J := \text{diag}(\gamma_1, \gamma_2, \gamma_3), \gamma_1 = -S(u_{31}), \gamma_2 = -S(u_{23}), \gamma_3 = 1. \]

is a co-ordinate pair over \( k \), called the co-ordinate pair associated with \( (J, S) \).

**Proof.** We have \( S(u_{12}) \in k^x \) by Prop. 37.7, in particular, \( \omega \in k^x \) exists, and (3) by (37.22) defines a non-associative algebra structure on \( C = J_{12} \). It remains to show that \( C \) is a multiplicative conic alternative algebra with norm, unit element, trace, conjugation as indicated. Let \( u, v \in C \). The element \( u_{12} \in C \) by Lemma 37.23, (1) satisfies

\[ u_{12}v = \omega \left((u_{23} \times u_{31}) \times (u_{31} \times v)\right) = -S(u_{23})\omega u_{31} \times (u_{31} \times v) = S(u_{23})S(u_{31})\omega v = v, \]
\[ uu_{12} = \omega (u \times u_{23}) \times (u_{31} \times (u_{23} \times u_{31})) = -S(u_{31})\omega (u \times u_{23}) \times u_{23} = S(u_{23})S(u_{31})\omega u = u. \]

Thus \( C \) is unital with unit element \( 1_C = u_{12} \), and (5) holds. Defining the quadratic form \( n_C : C \to k \) by (4), we derive the relation \( n_C(1_C) = -\omega S(u_{23} \times u_{31}) = \omega S(u_{23})S(u_{31}) \), and (1) yields

\[ n_C(1_C) = 1. \]

In order to distinguish the squaring in \( J \) from the one in \( C \), we write \( u^2 \) for the latter. Applying Lemma 37.23, (35.8.7), (1), we then obtain

\[ u^2 = \omega (u \times u_{23}) \times (u_{31} \times u) \]
\[ = \omega T(u_{23}, u_{31} \times u)u - \omega (u \times (u_{31} \times u)) \times u_{23} \]
\[ = \omega T(u_{12}, u)u + \omega S(u_{31} \times u_{23}) = \omega T(u_{12}, u)u - n_C(u_{12}, u), \]

where (37.23) and (3) yield \( n_C(1_C, u) = -\omega S(u_{12}, u) = \omega T(u_{12}, u) \). Thus \( C \) is a conic \( k \)-algebra with norm, unit, trace given by (3), (5), (6), respectively. Relation (7) is now clear. Next we show alternativity, again by appealing to the relations of Lemma 37.23 and (6):
\[ u(v) = \omega^2(u \times u_{23}) \times (u_{31} \times ((u \times u_{23}) \times (u_{31} \times v))) \]
\[ = \omega^2T(u_{31}, u \times u_{23})(u \times u_{23}) \times (u_{31} \times v) - \]
\[ \omega^2(u \times u_{23}) \times ((u \times u_{23}) \times (u_{31} \times (u_{31} \times v))) \]
\[ = t_C(u)uv - \omega^2S(u \times u_{23})S(u_{31})v = t_C(u)uv + \omega^2S(u_{23})S(u_{31})S(u)v \]
\[ = t_C(u)uv - n_C(u)v = (t_C(u)u - n_C(u)1_C)v = u^2v, \]
\[ (uv)u = \omega^2\left( (v \times u_{23}) \times (u_{31} \times u) \times u_{23} \right) \times (u_{31} \times u) \]
\[ = \omega^2T(u_{23}, u_{31} \times u)(v \times u_{23}) \times (u_{31} \times u) - \]
\[ \omega^2\left( (v \times u_{23}) \times (u_{31} \times u) \right) \times (u_{31} \times u) \times u_{23} \]
\[ = t_C(u)vu - \omega^2S(u_{31} \times u)S(u_{23})v = t_C(u)vu + \omega^2S(u_{31})S(u_{23})S(u)v \]
\[ = t_C(u)vu - n_C(u)v = v(t_C(u)u - n_C(u)1_C) = vu^2. \]

Finally, by (37.23.6), (3), (4), the norm of \( C \) permits composition:
\[ n_C(uv) = -\omega^3S((u \times u_{23}) \times (u_{31} \times v)) \]
\[ = \omega^3S(u \times u_{23})S(u_{31} \times v) = \omega^2S(u)S(v) = n_C(u)n_C(v). \]

Summing up we have thus shown that \( C \) is a multiplicative conic algebra over \( k \).

\[ \square \]

**37.25. Theorem** (The Jacobson co-ordinatization theorem). Let \((J, \mathfrak{S})\) be a co-ordinated cubic Jordan algebra over \( k \). With the notation of Prop. 37.24, the map \( \phi_{J, \mathfrak{S}} : \text{Her}_3(C, \Gamma) \rightarrow J \) defined by
\[ \phi_{J, \mathfrak{S}}(x) := \sum (\xi_ie_i + v_j), \quad (1) \]

for
\[ x = \sum (\xi_ie_i + v_j)[j] \in \text{Her}_3(C, \Gamma) \quad (\xi_i \in k, v_i \in C, i = 1, 2, 3), \quad (2) \]

where
\[ v_{23} := -S(u_{31})^{-1}u_{31} \times \bar{v}_1, \quad v_{31} := -S(u_{23})^{-1}u_{23} \times \bar{v}_2, \quad v_{12} := v_3, \quad (3) \]
is an isomorphism of cubic Jordan algebras matching the diagonal co-ordinate system of \( \text{Her}_3(C, \Gamma) \) with the co-ordinate system \( \mathfrak{S} \) of \( J \).

**Proof.** Note by (37.24.2) that \( C = J_{12} \) as \( k \)-modules. Since the conjugation of any conic algebra leaves its norm invariant, (37.24.4) shows
\[ S(\bar{v}) = S(v) \quad (v \in C = J_{12}). \quad (4) \]

Putting \( \Phi := \phi_{J, \mathfrak{S}} \) and defining \( \Psi : J \rightarrow \text{Her}_3(C, \Gamma) \) by
\[ \Psi \left( \sum (\xi_i e_i + v_{jl}) \right) := \sum (\xi_i e_{ij} + v_i [jl]) \]
for \( \xi_i \in k, v_{jl} \in J_{jl}, i = 1, 2, 3, \) where
\[ v_1 := u_{31} \times v_{23}, \quad v_2 := u_{23} \times v_{31}, \quad v_3 := v_{12}. \]

(37.23.2), (37.23.3) imply \( \Phi \circ \Psi = 1_J \) and \( \Psi \circ \Phi := 1_{\text{Her}_3(C, \Gamma)}. \) Thus \( \Phi \) is a bijective linear map. It remains to show that \( \phi \) is a homomorphism of cubic Jordan algebras. Since \( \phi \) obviously preserves unit elements, the assertion will follow from Exc. 185(a) once we have shown that \( \phi \) preserves adjoints. In order to do so, we denote by \( x^\sharp \) the adjoint of \( x \in \text{Her}_3(C, \Gamma) \) as given by (2) and deduce from (37.10.4) that
\[ x^\sharp = \sum (\eta_i e_i + w_{jl}), \]
where
\[ \eta_i = \xi_j \xi_l - \gamma_j \gamma_l n_C(v_i), \quad w_i = -\xi_i v_i + \gamma_i v_j v_l. \]

Hence (2), (3) imply
\[ \phi(x^\sharp) = \sum (\eta_i e_i + w_{jl}), \]
where
\[ w_{23} := -S(u_{31})^{-1} u_{31} \times \bar{w}_1, \quad w_{31} := -S(u_{23})^{-1} u_{23} \times \bar{w}_2, \quad w_{12} := w_3. \]

Before we can proceed, we require the identity
\[ S(v_{jl}) = -\gamma_j \gamma_l n_C(v_i), \]
which follows by combining (5), (6), (37.23.6), (37.24.1), (37.24.4) and (37.24.9) with the computations
\[ S(v_{23}) = S(u_{31})^{-2} S(u_{31} \times \bar{v}_1) = -S(u_{31})^{-1} S(v_1) = -S(u_{23}) \omega S(v_1) = -\gamma_j \gamma_l n_C(v_1), \]
\[ S(v_{31}) = S(u_{23})^{-2} S(u_{23} \times \bar{v}_2) = -S(u_{23})^{-1} S(v_2) = -S(u_{31}) \omega S(v_2) = -\gamma_j \gamma_l n_C(v_2), \]
\[ S(v_{12}) = S(v_3) = -\omega^{-1} n_C(v_3) = -\gamma_j \gamma_l n_C(v_3). \]

Applying (10) and (6), we now conclude
\[ \eta_i = \xi_j \xi_l + S(v_{jl}). \]

On the other hand, combining (6), (7), (3), (37.24.9) gives
\[ w_{23} = -S(u_{31})^{-1}u_{31} \times \bar{w}_1 = S(u_{31})^{-1}\xi_1u_{31} \times \bar{v}_1 - S(u_{31})^{-1} \gamma_1 u_{31} \times (v_2v_3) = -\xi_1v_2 + u_{31} \times (v_2v_3), \]

where Lemma 37.23 and Prop. 37.24 imply

\[ u_{31} \times (v_2v_3) = \omega u_{31} \times ((v_2 \times u_{23}) \times (u_{31} \times v_3)) \]
\[ = \omega T(u_{31}, v_2 \times u_{23})u_{31} \times v_3 - \omega (v_2 \times u_{23}) \times (u_{31} \times (u_{31} \times v_3)) \]
\[ = t_C(v_2)u_{31} \times v_3 + S(u_{23})^{-1}(v_2 \times u_{23}) \times v_3 \]
\[ = -S(u_{23})^{-1}(t_C(v_2)(u_{23} \times u_{31}) \times u_{23} - v_2 \times u_{23}) \times v_3 \]
\[ = -S(u_{23})^{-1}(t_C(v_2)u_{23} - v_2) \times u_{31} \times v_3 \]
\[ = -S(u_{23})^{-1}(u_{23} \times \bar{v}_2) \times v_3 = v_{31} \times v_{12}. \]

Summing up,

\[ w_{23} = -\xi_1v_2 + v_{31} \times v_{12}. \]

Similarly,

\[ w_{31} = -S(u_{23})^{-1}u_{23} \times \bar{w}_2 = \xi_2 S(u_{23})^{-1}u_{23} \times \bar{v}_2 - S(u_{23})^{-1} \gamma_2 u_{23} \times (v_3v_1) = -\xi_2v_{31} + u_{23} \times (v_3v_1), \]

where

\[ u_{23} \times (v_3v_1) = \omega u_{23} \times ((v_3 \times u_{23}) \times (u_{31} \times v_1)) \]
\[ = \omega T(u_{23}, u_{31} \times v_1)v_3 \times u_{23} - \omega (u_{31} \times v_1) \times ((v_3 \times u_{23}) \times u_{23}) \]
\[ = t_C(v_1)v_3 \times u_{23} + S(u_{31})^{-1}(u_{31} \times v_1) \times v_3 \]
\[ = -S(u_{31})^{-1}(t_C(v_1)(u_{23} \times u_{31}) \times u_{23} - u_{31} \times v_1) \times v_3 \]
\[ = -S(u_{31})^{-1}(t_C(v_1)u_{23} - v_1) \times u_{31} \times v_3 \]
\[ = -S(u_{31})^{-1}(\bar{v}_1 \times u_{31}) \times v_3 = v_{23} \times v_{12}. \]

Thus

\[ w_{31} = -\xi_2v_{31} + v_{12} \times v_{23}. \]

Since

\[ w_{12} = w_3 = -\xi_3v_3 + \gamma_3\bar{v}_1v_2 = -\xi_3v_{12} + \bar{v}_2\bar{v}_1 \]
\[ = -\xi_3v_{12} + \omega(\bar{v}_2 \times u_{23}) \times (u_{31} \times \bar{v}_1) = -\xi_3v_{12} + v_{23} \times v_{31}, \]

our computations can be unified to

\[ w_{ij} = -\xi_i v_{ji} + v_{ii} \times v_{ij}. \]
Inserting (11) and (12) into (3), we may apply (37.22.3) and (1) to obtain

\[ \phi(x^2) = \sum (\xi_j^i + S(v_{ji})) e_i + \sum (-\xi_j v_{ji} + v_{ii} \times v_{ij}) = (\sum \xi_j e_i + \sum v_{ji})^2 = \phi(x)^2. \]

Hence \( \phi \) preserves adjoints and thus is an isomorphism of cubic Jordan algebras.

It remains to show that \( \phi \) matches the respective co-ordinate systems. To this end, we have to prove \( \phi(1_C[j]) = u_{ji} \) for \( i = 1, 2 \), which follows from (37.24.5) and

\[ \phi(1_C[23]) = -S(u_{31})^{-1} u_{31} \times 1_C = -S(u_{31})^{-1} u_{23} \times (u_{23} \times u_{31}) = u_{23}, \]

\[ \phi(1_C[31]) = -S(u_{23})^{-1} u_{23} \times 1_C = -S(u_{23})^{-1} u_{23} \times (u_{23} \times u_{31}) = u_{31}, \]

completing the proof of the entire theorem.

37.26. Remark. Versions of the Jacobson co-ordinatization theorem which in many ways are much more general than the one presented here may be found in the literature, see, e.g., Jacobson [43, 44, 45] and McCrimmon [75] for details. Given any integer \( m \geq 3 \), the most important difference is that instead of co-ordinate pairs one has to consider quadruples \( (D, \tau, D_0, \Delta) \) consisting of

- a unital alternative \( k \)-algebra \( D \),
- an involution \( \tau : D \to D \),
- a unital subalgebra \( D_0 \) of \( H(D, \tau) \) contained in the nucleus of \( D \) and being \( D \)-ample in the sense that \( uD_0 \tau(u) \subseteq D_0 \) for all \( u \in D \),
- an invertible diagonal matrix \( \Delta \in \text{Mat}_m(D_0) \).

With considerable effort, it can then be shown that the \( k \)-module

\[ \text{Her}_m(D, \tau, D_0, \Delta) \]

of all \( \Delta \)-twisted \( m \times m \) hermitian matrices with entries in \( D \) and diagonal ones in \( D_0 \), carries the structure of a Jordan algebra over \( k \) provided \( m = 3 \) or \( D \) is associative. Conversely, given a Jordan algebra \( J \) over \( k \) whose extreme radical is zero and a connected orthogonal system \( \Omega = (e_1, \ldots, e_m) \) of idempotents in \( J \), the Jacobson co-ordinatization theorem says that there exist a quadruple \( (D, \tau, D_0, \Delta) \) as above and an isomorphism from \( J \) onto \( \text{Her}_m(D, \tau, D_0, \Delta) \) matching the orthogonal system \( \Omega \) of the former with the diagonal one of the latter.

Here the condition on the extreme radical, being automatic for the algebras \( \text{Her}_m(D, \tau, D_0, \Delta) \), cannot be avoided. One may therefore wonder why it is absent from our version of the Jacobson co-ordinatization theorem. The answer rests on our formal definition of cubic Jordan matrix algebras in [37.10, 37.11, 37.12] which, for a co-ordinate pair \( (C, \Gamma) \), allows a concrete base change invariant interpretation of \( \text{Her}_3(C, \Gamma) \) in terms of \( \Gamma \)-twisted hermitian matrices only if \( 1_C \in C \) is unimodular. Indeed, dropping this hypothesis, the extreme radical of \( \text{Her}_3(C, \Gamma) \) may very well be different from zero, while otherwise it is not (Exc. 204).
Exercises.

195. Idempotents in cubic Jordan algebras. Let \( J \) be a cubic Jordan algebra over \( k \). An idempotent \( e \in J \) is said to be co-elementary if the complementary idempotent \( 1 - e \) is elementary. Now let \( e \) be any idempotent in \( J \). Prove that there exists a complete orthogonal system \((e^{(i)})_{0 \leq i \leq 3}\) of idempotents in \( k \), giving rise to decompositions

\[
k = k^{(0)} \oplus k^{(1)} \oplus k^{(2)} \oplus k^{(3)}, \quad J = J^{(0)} \oplus J^{(1)} \oplus J^{(2)} \oplus J^{(3)}
\]
as direct sums of ideals, where \( k^{(i)} = e^{(i)}k, J^{(i)} = e^{(i)}J = J^{(i)}e \) as cubic Jordan algebras over \( k^{(i)} \) for \( 0 \leq i \leq 3 \) such that

\[
e^{(i)} \text{ is an elementary idempotent of } J^{(i)} \text{ and } e^{(3)} \text{ is a co-elementary idempotent of } J^{(3)}.
\]

Show further that the \( e^{(i)} \) are unique and given by

\[
e^{(0)} = N(1 - e) = 1 - T(e) + S(e) - N(e),
\]

\[
e^{(1)} = T(e) - 2S(e) + 3N(e),
\]

\[
e^{(2)} = S(e) - 3N(e),
\]

\[
e^{(3)} = N(e).
\]

196. Ferrar’s lemma [28]. Let \( u_1, u_2, u_3 \) be elements of a cubic Jordan algebra \( J \) over \( k \) such \( u_i^2 = 0 \) for \( i = 1, 2, 3 \). Prove that \( q := \sum u_i \) is invertible in \( J \) if and only if \( T(u_1 \times u_2, u_3) \) is invertible in \( k \), and that, in this case, \((u_1, u_2, u_3)\) is an elementary frame in the isotope \( J^{(p)} \), \( p := q^{-1} \). Conclude that three elementary idempotents in \( J \) adding up to 1 form an elementary frame of \( J \).

197. The \( U \)-operator and matrix multiplication. Let \((C, \Gamma)\) be a co-ordinate pair over \( k \) and assume that \( 1_C \in C \) is unimodular. Let

\[
x = \sum (\xi_i e_i + u_i [j_1]), \quad y = \sum (\eta_i e_i + v_i [j_1]) \in J := \text{Her}_3(C, \Gamma)
\]

with \( \xi_i, \eta_i \in k, u_i, v_i \in C \) for \( i = 1, 2, 3 \) and write 1, \( x, x^2, x^3, \ldots \) for the powers of \( x \) in \( J \), while denoting matrix multiplication In Mat_3(C) by juxtaposition. Then prove

\[
x^2 = xx,
\]

\[
x^3 = x(xx) + \gamma_1 \gamma_2 \gamma_3 [u_1, u_2, u_3]1_3 = (xx)x - \gamma_1 \gamma_2 \gamma_3 [u_1, u_2, u_3]1_3,
\]

\[
U_{xy} = x(yy) - [x, x, x] + \gamma_1 \gamma_2 \gamma_3 ([u_1, u_2, v_3] + [u_2, u_3, v_1] + [u_3, u_1, v_2])1_3
\]

\[
= (xx)x + [x, x, x] - \gamma_1 \gamma_2 \gamma_3 ([u_1, u_2, v_3] + [u_2, u_3, v_1] + [u_3, u_1, v_2])1_3,
\]

\[
[x, x, x] = 2 \gamma_1 \gamma_2 \gamma_3 [u_1, u_2, u_3]1_3,
\]

\[
xx^2 = (N(x)1_C + \gamma_1 \gamma_2 \gamma_3 [u_1, u_2, u_3]1_3,
\]

\[
xx^2 = (N(x)1_C - \gamma_1 \gamma_2 \gamma_3 [u_1, u_2, u_3]1_3.
\]

Finally, writing \( x^3 \) as

\[
x^3 = \sum (\xi_i^2 + u_i^2 [j_1])\]

with \( \xi_i^2 \in k, u_i^2 \in C \) for \( i = 1, 2, 3 \), conclude that

\[
[u_1^2, u_2^2, u_3^2] = -N(x)[u_1, u_2, u_3].
\]

198. Let \((C, \Gamma)\) and \((C, \Gamma')\) with

\[
\Gamma = \text{diag}(\gamma_1, \gamma_2, \gamma_3), \quad \Gamma' = \text{diag}(\gamma_1', \gamma_2', \gamma_3') \in \text{Diag}_3(k).
\]
be two co-ordinate pairs over \( k \).

(a) View \( \text{Diag}_3(k) \) via \( [35.24] \) as the split cubic étale \( k \)-algebra and consider the following conditions, for any \( \Delta = \text{diag}(\delta_1, \delta_2, \delta_3) \in \text{Diag}_3(k) \).

(i) \( \gamma_i' = \delta_i^{-1} \gamma_i \) for \( i = 1, 2, 3 \) and \( \gamma_i' \gamma_j' = \delta_i \delta_j \gamma_j \gamma_i \), i.e., \( \Gamma'' = \Delta^2 \Gamma^x \) and \( N(\Gamma'') = N(\Delta) N(\Gamma') \).

(ii) \( \gamma_i' = \delta_i \delta_i^{-1} \gamma_i \) for \( i = 1, 2, 3 \), i.e., \( \Gamma' = \Delta^2 \Delta^{-1} \Gamma \).

(iii) The map

\[ \varphi_{C, \Delta} : \text{Her}_3(C, \Gamma) \longrightarrow \text{Her}_3(C, \Gamma') \]

defined by

\[ \varphi_{C, \Delta} (\sum (\xi_i e_{ii} + u_i [j]) ) = \sum (\xi_i e_{ii} + (\delta_i^{-1} u_i)[j]) \]  

(12) DIAFEL

for \( \xi_i \in k, u_i \in C, i = 1, 2, 3 \) is an isomorphism of cubic Jordan algebras.

Show that the implications

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

hold, and that all three conditions are equivalent if \( I_C \in C \) is unimodular.

(b) Conclude from (a) that the isomorphism class of \( \text{Her}_3(C, \Gamma) \) does not change if

(i) \( \Gamma \) is multiplied by an invertible scalar,

(ii) each diagonal entry of \( \Gamma \) is multiplied by an invertible square,

(iii) \( \Gamma \) is replaced by an appropriate diagonal matrix in \( \text{Mat}_3(k) \) of determinant 1.

199. **Diagonal isotopes of cubic Jordan matrix algebras.** Let \( (C, \Gamma) \) be a co-ordinate pair over \( k \).

Prove that

\[ p := \sum \gamma_i e_{ii} \in \text{Her}_3(C, \Gamma) \]

is invertible and that the map

\[ \varphi : \text{Her}_3(C, \Gamma)^{(p)} \longrightarrow \text{Her}_3(C) \]

defined by

\[ \varphi (\sum (\xi_i e_{ii} + u_i [j]) ) := \sum ((\gamma_i \xi_i) e_{ii} + (\gamma_i u_i)[j]) \]  

(13) DIIS

for \( \xi_i \in k, u_i \in C, i = 1, 2, 3 \) is an isomorphism of cubic Jordan algebras.

200. **Isotopes of pre-co-ordinate pairs.** Let \( (C, \Gamma) \) be a pre-co-ordinate pair over \( k \) and \( p, q \in C^\times \).

Put

\[ \Gamma^{(p, q)} := \text{diag}(\gamma_1^{(p, q)}, \gamma_2^{(p, q)}, \gamma_3^{(p, q)}), \]

so that

\[ (C, \Gamma)^{(p, q)} := (C^{(p, q)}, \Gamma^{(p, q)}) \]

is a pre-co-ordinate pair over \( k \), and show that the map

\[ \varphi : \text{Her}_3(C^{(p, q)}, \Gamma^{(p, q)}) \longrightarrow \text{Her}_3(C, \Gamma) \]

defined by

\[ \varphi (\sum (\xi_i e_{ii} + u_i [j]) ) := \sum (\xi_i e_{ii} + u'_{ij}) \]  

(14) ISOISC

for \( \xi_i \in k, u_i \in C, i = 1, 2, 3 \), where

\[ u'_1 := (pq)u_1(pq), \quad u'_2 := u_2 p, \quad u'_3 := qu_3 \]  

(15) OFFDI

is an isomorphism of cubic Jordan algebras.
201. Let \((C, \Gamma)\) be a co-ordinate pair over \(k\). Show that the cubic Jordan matrix algebra \(J = \text{Her}_3(C, \Gamma)\) over \(k\) is outer central.

202. Ideals of cubic Jordan matrix algebras. Let \((C, \Gamma)\) be a co-ordinate pair over \(k\) and suppose \(1_C \in C\) is unimodular, so that we obtain a natural identification \(k \subseteq C\) as a unital subalgebra which is stable under base change. Prove:

(a) The outer ideals of the Jordan algebra \(J := \text{Her}_3(C, \Gamma)\) are precisely of the form

\[ H_3(l_0, I, \Gamma) := \sum (l_0 e_i + I [j][l]) = \{ \sum (\xi_i e_i + u_i [j][l]) \mid \xi_i \in l_0, \ u_i \in I, \ 1 \leq i \leq 3 \}, \tag{16} \]

where \(I\) is an ideal in \((C, t_C)\) (viewed as an algebra with involution) and \(l_0\) is an ideal in \(k\), contained in \(I \cap k\) and weakly 1-ample in the sense that it contains the trace of arbitrary elements in \(I\):

\[ t_C(I) \subseteq l_0 \subseteq I \cap k. \tag{17} \]

(b) The ideals of \(J\) are precisely of the form \((16)\), where \(I\) as in (a) is an ideal in \((C, t_C)\) and \(l_0\) is an ideal in \(k\), contained in \(I \cap k\) and 1-ample in the sense that it contains norm and trace of arbitrary elements in \(I\):

\[ knc(I) + t_C(I) \subseteq l_0 \subseteq I \cap k. \tag{18} \]

(c) For \(l_0, I\) as in (a), we have \(2(I \cap k) \subseteq l_0\), hence \(l_0 = I \cap k\) if \(\frac{1}{2} \in k\).

(d) If \(C\) is a non-singular composition algebra, then the outer ideals of \(J\) are ideals and have the form \(AJ\) with \(A\) varying over the ideals of \(k\).

(e) If \(k = F\) is a field and \(C\) is a pre-composition algebra over \(F\), then the outer ideals of \(J = \text{Her}_3(C, \Gamma)\) are precisely of the form \(\{0\}\), \(\text{Rad}(T)\) (the radical of the bilinear trace), and \(I\). In particular, \(J\) is a simple Jordan algebra. Moreover, \(J\) is outer simple if and only if \(C\) is a non-singular composition algebra over \(F\).

203. Absolute zero divisors in cubic Jordan algebras. Let \(J\) be a cubic Jordan algebra over \(k\).

(a) Show that if \(x \in J\) is an absolute zero divisor, then so is \(x^2\).

(b) Assume that \(k\) is reduced and consider the following conditions on \(x \in J\).

(i) \(x\) is an absolute zero divisor.

(ii) \(x^2 = 0\) and \(T(x, y) = 0\) for all \(y \in J\).

(iii) \(N(x) = 0\) and \(T(x, y) = 0\) for all \(y \in J\).

Then prove that the implications

\[(i) \iff (ii) \implies (iii)\]

hold.

(c) Prove that every absolute zero divisor of \(J\) is contained in the nil radical of \(J\).

(d) (Weiss) Show that, contrary to what has been claimed in Petersson-Racine [103, p. 214], conditions (i), (ii), (iii) of part (b) are not equivalent, even if \(k = F\) is a field and \(J\) is a simple Jordan algebra.

(e) Show that the nil radical of \(J\) is zero if and only if \(k\) is reduced and \(J\) has no absolute zero divisors.

204. The extreme radical of co-ordinated cubic Jordan algebras. Let \(\mathcal{G} = (e_1, e_2, e_3, u_{23}, u_{31})\) be a co-ordinate system of the cubic Jordan algebra \(J\) over \(k\) and write \(J = \sum (k e_i + J_{jl})\) for the Peirce decomposition of \(J\) relative to the elementary frame \((e_1, e_2, e_3)\). Prove without recourse to the Jacobson co-ordinatization theorem that the extreme radical of \(J\) may be described as
Conclude for a co-ordinate pair \((C, \Gamma)\) over \(k\) that the extreme radical of \(\text{Her}_3(C, \Gamma)\) is zero if \(1_c \in C\) is unimodular but not in general.

205. A categorical set-up for the Jacobson co-ordinatization theorem. (a) Let \((C, \Gamma)\) and \((C', \Gamma')\) be co-ordinate pairs over \(k\). We define a homomorphism from \((C, \Gamma)\) to \((C', \Gamma')\) as a pair \((\eta, \Delta)\) consisting of

(i) a homomorphism \(\eta: C \to C'\) of conic \(k\)-algebras,
(ii) a matrix \(\Delta \in \text{Diag}_3(k)^{\times}\) such that \(\Gamma' = \Delta^t \Delta^{-1} \Gamma\).

In this way we obtain the category of co-ordinate pairs over \(k\), denoted by \(k\)-copia.

(b) Let \((J, \mathcal{S})\) and \((J', \mathcal{S}')\) be co-ordinated cubic Jordan algebras over \(k\) and write

\[
\mathcal{S} = (e_1, e_2, e_3, u_{23}, u_{31}) \in J^5, \quad \mathcal{S}' = (e_1', e_2', e_3', u_{23}', u_{31}') \in J'^5.
\]

We define a homomorphism from \((J, \mathcal{S})\) to \((J', \mathcal{S}')\) as a triple \((\varphi, \delta_1, \delta_2)\) consisting of

(i) a homomorphism \(\varphi: J \to J'\) of cubic Jordan algebras satisfying \(\varphi(e_i) = e_i'\) for \(i = 1, 2, 3\),
(ii) scalars \(\delta_1, \delta_2 \in k^{\times}\) such that \(\varphi(u_{ij}) = \delta_1^{-1} u_{ij}'\) for \(i = 1, 2\).

In this way we obtain the category of co-ordinated cubic Jordan algebras over \(k\), denoted by \(k\)-cocojo.

(c) Let \((\eta, \Delta): (C, \Gamma) \to (C', \Gamma')\) with \(\Delta = \text{diag}(\delta_1, \delta_2, \delta_3) \in \text{Diag}_3(k)^{\times}\) be a homomorphism of co-ordinate pairs over \(k\). Define

\[
\text{Her}_3(\eta, \Delta): \text{Her}_3(C, \Gamma) \longrightarrow \text{Her}_3(C', \Gamma')
\]

by

\[
\text{Her}_3(\eta, \Delta) \bigg( \sum \xi e_0 + u_j j! \bigg) := \sum \left( \xi e_0 + (\delta_1^{-1} \eta(u_i)) j! \right)
\]

(20)

for \(\xi_i \in k, u_i \in C, i = 1, 2, 3\) and show that

\[
\text{Her}_3(\eta, \Delta) := (\text{Her}_3(\eta, \Delta); \delta_1, \delta_2): \text{Her}_3(C, \Gamma) \longrightarrow \text{Her}_3(C', \Gamma')
\]

is a homomorphism of co-ordinated cubic Jordan algebras over \(k\), giving rise to a functor

\[
\text{Her}_3: \text{k-copia} \longrightarrow \text{k-cocojo}.
\]

(d) Let \((\varphi; \delta_1, \delta_2): (J, \mathcal{S}) \to (J', \mathcal{S}')\) be a homomorphism of co-ordinated cubic Jordan algebras over \(k\). Write \(J = \sum (ke_i + J_{ij})\) for the Peirce decomposition of \(J\) relative to the elementary frame belonging to \(\mathcal{S}\), ditto for \(J'\), and \(\varphi_{ij}\) for the linear map \(J_{ij} \to J'_{ij}\) induced by \(\varphi\) via restriction. Then prove that

\[
\text{Cop}(\varphi; \delta_1, \delta_2): \text{Cop}(J, \mathcal{S}) \longrightarrow \text{Cop}(J', \mathcal{S}'),
\]

where

\[
\text{Cop}(\varphi; \delta_1, \delta_2) := (\delta_1 \delta_2 \varphi_{ij}; \Delta = \text{diag}(\delta_1, \delta_2, \delta_3), \quad \delta_1 := \delta_1 \delta_2,
\]

(21)

is a homomorphism of co-ordinate pairs over \(k\), giving rise to a functor

\[
\text{Cop}: \text{k-cocojo} \longrightarrow \text{k-copia}.
\]

(e) Let \((C, \Gamma)\) be a co-ordinate pair over \(k\) and put
(C', Γ') := Cop(Her₃(C, Γ)). \hspace{1cm} (22)

Show C' = C[12] as k-modules and that

Ψ_{C, Γ} := (ψ_{C, Γ}, Λ_{C, Γ}) : (C, Γ) \cong (C', Γ'),

where

ψ_{C, Γ} : C \to C', \quad u \mapsto γ₃u[12], \hspace{1cm} (23)

Λ_{C, Γ} := \text{diag}(λ₁, λ₂, λ₃), \quad λ₁ = λ₂ = 1, \quad λ₃ = γ₃, \hspace{1cm} (24)

is an isomorphism of co-ordinate pairs over k.

(f) Let (J, S) be a co-ordinated cubic Jordan algebra over k and put

(J', S') := Her₃(Cop(J, S)). \hspace{1cm} (25)

Show with the terminology of Thm. 37.25 that

Φ_{J, S} := (\phi_{J, S}; 1, 1) : (J', S') \cong (J, S) \hspace{1cm} (26)

is an isomorphism of co-ordinated cubic Jordan algebras.

(g) Conclude that the functors

\[ k\text{-copa} \xrightarrow{\text{Her₃}} \text{Cop} \xrightarrow{\text{k-cuco}} \]

give an equivalence of categories.
Solutions

Chapter 1

Section 1

Putting \(x_1, x_2, x_3\) := \(a \oplus u\) for some \(a \in \mathbb{C}\), \(u \in \mathbb{C}^3\) and using (1.4.1), we obtain

\[
a \oplus u = [a_1 \oplus u_1, a_2 \oplus u_2, a_3 \oplus u_3]
\]

and an application of (1.4.1) yields

\[
a = a_1 a_2 a_3 - a_1^2 u_3 a_3 - a_1 u_2 a_3 - a_3^2 u_1 a_3 - (u_1 \times u_2)' u_3 - a_1 a_2 a_3
\]

First of all, (1.4.1) implies

\[
|2v| = \sqrt{2} |v|
\]

Multiplying the second equation with \(\bar{a}'\) from the left and applying the first combined with (1.4.1), we obtain

\[
0 = \bar{a}' (\bar{u} \times \bar{v}) + \bar{u} a b + \bar{u} \bar{v} a (\|u\|^2 + \|a\|^2) b = \|x\|^2 b,
\]

hence \(b = 0\). Thus (28) reduces to

\[
\bar{u}' \bar{v}' = 0, \quad \bar{u} \times \bar{v} = -\bar{v} \bar{u}.
\]

Here the second equation gives \(0 = \bar{v}' (\bar{u} \times \bar{v}) = -\|v\|^2 \bar{a}',\) 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, (28) yields \((\bar{u} \times \bar{v}) \times u = \bar{v}' \bar{u} - \bar{u}' \bar{v} = \|a\|^2 \bar{v},\) hence again \(v = 0\).
sol.INVAS  (a) For \( a, b \in \mathbb{C}, u, v \in \mathbb{C}^3, x = a \oplus u, y = b \oplus v \in \mathcal{O} \), we apply \( 1.4.1, 1.5.7 \) and conclude

\[
xy = (ab - \bar{u}v) \oplus (\bar{v}a + ab + \bar{u}x) = (ab - \bar{u}v) \oplus (-\bar{v}a - ub - \bar{u}x)
\]

\[
= \left( \bar{b}a - (-v)'(u) \right) \oplus \left( (-u)\bar{b} + (-v)a + (-\bar{v})x \right)
\]

\[
= (\bar{b} \oplus (-v))(\bar{a} \oplus (-u)) = \bar{x}',
\]

which proves (a).

(b) Let \( x = a \oplus u, y = b \oplus v \), with \( a, b \in \mathbb{C}, u, v \in \mathbb{C}^3 \). From \( 1.4.1 \) and \( 1.4.5 \) we conclude that \( t_0(xy) = ab + \bar{a}b - \bar{v}u - v'u = ab + \bar{a}b - \bar{v}u - v'u \) is symmetric in \( x, v \), giving the first equation. Moreover, the \( \mathbb{C} \)-component of the associator \([x_1, x_2, x_3] \) in Exc. \( 3 \) is purely imaginary. Hence the second equation follows from \( 1.5.5 \). Combined with \( 1.5.13 \) and (a) it implies

\[
n_0(xyz) = t_0((xy)z) = t_0(x(yz)) = n_0(x, zy) = n_0(x, z'y),
\]

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

(c) The first set of equations follows immediately from \( 1.5.10 \) and the definition of the conjugation. As to the remaining ones, we apply \( 1.5.12, 1.5.10, 1.5.6 \) to deduce

\[
xy = x(xy) - x^2v = t_0(x)xy + t_0(y)x^2 - n_0(x, y)x + n_0(x)y
\]

\[
= n_0(x, t_0(y)1_3 - y)x - n_0(x)\left( t_0(y)1_3 - y \right) = n_0(x, y)x - n_0(x)y,
\]

which completes the proof of (c).

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

\[
\text{tr} \left( \left( (u \times v)'w + (v \times w)'u + (w \times u)'v \right) A \right) = \lambda(A) \det(u, v, w) \quad (u, v, w \in \mathbb{C}^3)
\]

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 \( e_ie_i' = e_0 \) in terms of the ordinary matrix units for \( 1 \leq i \leq 3 \), we deduce \( \lambda(A) = \text{tr}(A) \), hence

\[
\text{tr} \left( \left( (u \times v)'w + (v \times w)'u + (w \times u)'v \right) A \right) = \text{tr} \left( \left( \det(u, v, w)1_3 \right) A \right).
\]

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

It remains to prove the Moufang identities. Since the conjugation of \( \mathcal{O} \) is an algebra involution (Exc. \( 3 \)(a)), the third Moufang identity immediately follows from the first.

We begin by proving the first Moufang identity, which by Exc. \( 3 \)(c) comes down to showing

\[
x(\{y(z)\}) = n_0(x, y)xz - n_0(x)yz.
\]

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. \( y = b \oplus 0, z = c \oplus 0, b, c \in \mathbb{C} \). Then \( 1.4.1 \) yields

\[
x(y(z)) = x(\{y((a \oplus u)(c \oplus 0))\}) = x((b \oplus 0)(ac \oplus uc)) = (a \oplus u)(abc \oplus ubc)
\]

\[
= (a^2bc - \bar{u}abc) \oplus u(ab + \bar{a}b)c.
\]

On the other hand, applying \( 1.5.1, 1.5.2 \) and \( 1.5.7 \) we obtain
Elementary idempotents and cubic Jordan matrix algebras

\[ n_{C}(x, y)zx - n_{C}(x)yz = n_{C}(a \oplus u, \bar{b} \oplus v)(a \oplus u)(c \oplus 0) - n_{C}(a \oplus u)(\bar{b} \oplus 0)(c \oplus 0) \]
\[ = (\bar{a}\bar{b} + ab)(ac \oplus uc) - (\bar{a}a + \bar{u}a)(\bar{b}c \oplus 0) \]
\[ = (\bar{a}abc + a^2 bc - \bar{a}abc - \bar{u}abc) \oplus u(abc + \bar{a}bc) \]
\[ = (a^2 bc - \bar{u}abc) \oplus u(ab + \bar{a}b)c. \]

Thus (2.27) holds.

**Case 2.** \( y = b \oplus 0, z = 0 \oplus w, b \in \mathbb{C}, w \in \mathbb{C}^1. \) Basically arguing as before, we obtain

\[ x(y(xz)) = x\left((a \oplus u)(0 \oplus w)\right) = x\left((b \oplus 0)((-\bar{u}w) \oplus (w\bar{a} + \bar{u} \times \bar{w}))\right) \]
\[ = \left(a \oplus u\right)((-b\bar{u}w) \oplus (w\bar{a}b + (\bar{a} \times \bar{w})\bar{b})) \]
\[ = (-ab\bar{u}w - \bar{u}w\bar{a}b - \bar{a}(\bar{u} \times \bar{w})\bar{b}) \]
\[ \oplus (w\bar{a}^2 \bar{b} + (\bar{u} \times \bar{w})\bar{a}b - ub\bar{u}w + (\bar{a} \times \bar{w})ab + \bar{u} \times (u \times w)\bar{b}). \]

Here (1.11) and the Grassmann identity (1.13) imply \( \bar{a}((- \bar{u} \times \bar{w}) = 0 \) as well as \( \bar{a} \times (u \times w) = (w \times u) \times \bar{u} = \bar{u}w - w\bar{u}w, \) hence

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

On the other hand,

\[ n_{C}(x, y)zx - n_{C}(x)yz = n_{C}(a \oplus u, \bar{b} \oplus 0)(a \oplus u)(0 \oplus w) - n_{C}(a \oplus u)(\bar{b} \oplus 0)(0 \oplus w) \]
\[ = (\bar{a}b + ab)((-\bar{u}w) \oplus (w\bar{a} + \bar{u} \times \bar{w})) - (\bar{a}a + \bar{u}a)(0 \oplus wb) \]
\[ = -(\bar{a}w)(ab + \bar{a}b) \oplus (w\bar{a}ab + \bar{a}^2 \bar{b}) + (\bar{a} \times \bar{w})(ab + \bar{a}b) - w\bar{a}ab - w\bar{a}ub \]
\[ = -(\bar{a}w)(ab + \bar{a}b) \oplus (w\bar{a}^2 \bar{b} + (\bar{u} \times \bar{w})(ab + \bar{a}b) - w\bar{u}ub) \]

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

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

\[ x(y(xz)) = x\left((a \oplus u)(c \oplus 0)\right) = x\left((0 \oplus v)(ac \oplus uc)\right) = (a \oplus u)\left(-\bar{v}uc \oplus (\bar{v} \times \bar{u})c\right) \]
\[ = (-a\bar{v}uc - \bar{v}vac - \bar{u}(\bar{v} \times \bar{u})c) \]
\[ \oplus (\bar{v}a\bar{c} + (\bar{v} \times \bar{u})\bar{a}e - u\bar{v}ec + (\bar{u} \times \bar{v})\bar{a}c + \bar{u} \times (v \times u)c). \]

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

\[ x(y(xz)) = \left(-ac(\bar{u}v \oplus \bar{v}u)\right) \oplus \left(v(\bar{a}a + \bar{u}u)c - u(\bar{u}v + \bar{v}u)c\right). \]

On the other hand,

\[ n_{C}(x, y)zx - n_{C}(x)yz = -n_{C}(a \oplus u, 0 \oplus v)(a \oplus u)(c \oplus 0) + n_{C}(a \oplus u)(0 \oplus v)(c \oplus 0) \]
\[ = -(\bar{a}v \oplus \bar{v}u)(ac \oplus uc) + (\bar{a}a + \bar{u}a)(0 \oplus vc) \]
\[ = -(ac(\bar{u}v \oplus \bar{v}u)) \oplus \left(-u(\bar{u}v + \bar{v}u)c + v(\bar{a}a + \bar{u}u)c\right). \]

and the discussion of Case 3 is complete.

**Case 4.** \( y = 0 \oplus v, z = 0 \oplus w, v, w \in \mathbb{C}^3. \) This is the most delicate case of them all.
\[ x(y(z)) = x\left( y((a \oplus u)(0 \oplus w)) \right) = x\left( (0 \oplus v)(-\tilde{v}w \oplus (\tilde{v} \times w)) \right) \\
= (a \oplus u) \left( -\tilde{v}w \oplus (-\tilde{v}w + (\tilde{v} \times w)a + (u \times w)) \right) \]

Since \( \tilde{v} \times (u \times w) = (w \times u) \times \tilde{v} = u\tilde{v}w - w\tilde{v}u \), we conclude

\[ x(y(z)) = (a \oplus u) \left( (u\tilde{v}w - w\tilde{v}u - (u \times w))a \right) \]

\[ = (a \times u)(v\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) + (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

\[ = \left( u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a \right) + (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

\[ = (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) + (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

Here \( \tilde{u} \times (v \times w) = (w \times u) \tilde{u} = v\tilde{u}w - w\tilde{u}v \), so that we obtain

\[ x(y(z)) = (v\tilde{u}w - w\tilde{u}v) \oplus (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

\[ = (v\tilde{u}w - w\tilde{u}v) \oplus (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

\[ = (v\tilde{u}w - w\tilde{u}v) \oplus (u\tilde{v}w - w\tilde{v}u - u\tilde{v}w - w\tilde{v}u - u\tilde{v}w + (u \times w)a) \]

On the other hand,

\[ x_0(x,y)z_0 - n_0(x)z_0 = -n_0(a \oplus u, 0 \oplus v)(a \oplus u)(0 \oplus w) + n_0(a \oplus u)(0 \oplus v)(0 \oplus w) \]

\[ = -n_0(a \times u)(v\tilde{u}w - w\tilde{u}v) \]

\[ = (a \times u)(v\tilde{u}w - w\tilde{u}v) \]

\[ = (a \times u)(v\tilde{u}w - w\tilde{u}v) \]

Comparing this with \( (31) \) we see that the \( \mathbb{C} \)-components are the same. Since \( u\tilde{v}w = w\tilde{u}v \), equality of the \( \mathbb{C} \)-components is equivalent to

\[ -u\tilde{v}w - v\tilde{u}w - u\tilde{v}w - v\tilde{u}w = -(u \times w)\tilde{u}w - (u \times w)\tilde{u}w = -(u \times w)\tilde{u}w - (u \times w)\tilde{u}w \]

which in turn is equivalent to

\[ \left( \det(\tilde{u}, \tilde{v}, w)1 \right) u = -u \det(\tilde{v}, \tilde{u}, w) = -(u \times w)\tilde{u}w + (u \times w)\tilde{u}w \]

But this relation holds by \( (1.4) \), 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.** \( y = b \oplus 0 \), \( z = c \oplus 0 \), \( b, c \in \mathbb{C} \). Then \( (1.4) \) yields

\[ (xy)(yz) = ((a \oplus u)(b \oplus 0))(c \oplus 0)(a \oplus u) = (ab \oplus ub)(ca \oplus uc) \]

\[ = (a^3bc - bc^3u) \oplus (uabc + uabc), \]

\[ x(yz)(z)x = ((a \oplus u)(bc \oplus 0)x = (abc \oplus uabc)(a \oplus u) \]

\[ = (a^2bc \oplus bc^2u) \oplus (uabc + uabc), \]

hence the assertion.

**Case 2.** \( y = b \oplus 0 \), \( z = 0 \oplus w \), \( b \in \mathbb{C} \), \( w \in \mathbb{C}^3 \). Then \( (1.4) \) and \( (1.1) \) yield
where the last summand may be written as

\[ (ab')u - \tilde{a}u' \tilde{v} - \tilde{a}/(u' \times \tilde{u})' \]

\[ + \left(\tilde{w}ab + (\tilde{u} \times \tilde{w})ab + (\tilde{u} \times \tilde{v})u + (\tilde{v} \times \tilde{w})\right)u \]

\[ - (ab')u - \tilde{a}u' \tilde{v} - \tilde{a}/(u' \times \tilde{u})' \]

Using (32) to compute the \( \mathbb{C}^3 \)-component of \((xy)(z)\), we obtain

\[ u_0 = -wa'd(u + v) - (w \times \tilde{u})'u - \tilde{a}/(u' \times \tilde{u})\]

\[ - \tilde{v}(w \times v) + (w \times \tilde{v})u + (w \times u) + (wa'v + (w \times u)(u' \times \tilde{u})u) \]

Here the last three terms may be written as

\[ \tilde{v}(w \times v)u = (u \times w) \times \tilde{u}u = wu'v + u'v \]

\[ (u \times v) \times \tilde{v}u = v(u' \times v)u + (u \times v) \times \tilde{v}u \]

Thus

\[ u_0 = -u'vwa - u'v\tilde{v}a + (\tilde{v} \times \tilde{w})a\tilde{a} - (\tilde{v} \times \tilde{u})u - \tilde{a}(u' \times \tilde{u})u - u'v \]

We now apply Exc. 3(c) to tackle the expression
Since $yz = (-v^t w) \oplus (v \times w)$, we deduce from (1.5.7) that

$$\overline{yz} = (-\overline{v^t w}) \oplus (-\overline{v \times w}).$$

(38) COYZ

When combined with (1.5.2), this implies

$$n_0(x, \overline{yz}) = n_0(\overline{yz}, x) = -\overline{v^t w} - v^t v \bar{a} - (v \times w)^t u - (\bar{v} \times \bar{w})^t \bar{u}$$

hence, in view of (37), (38), (35)

$$a_1 = n_0(x, \overline{yz}) a + n_0(x) \overline{v^t w}$$

$$= -\overline{v^t w} a - a^t v \bar{u} a - n(\overline{v^t w}) a + \overline{v^t v \bar{a}} + \overline{v^t v \bar{a}}^t u = a_0,$$

giving our first claim. It remains to prove the second, i.e., $u_0 = u_1$. Again by (37), (38), we obtain

$$u_1 = n_0(x, \overline{yz}) a + n_0(x) \overline{v^t w}$$

$$= -\overline{v^t w} a - a^t v \bar{u} a - \overline{n(\overline{v^t w}) a} + \overline{(v \times w)^t \bar{u}} + \overline{(\bar{v} \times \bar{w})^t u},$$

and comparing with (36) yields

$$u_1 - u_0 = (\bar{a} \times \bar{v}) \overline{v^t w} + (v \times w) \overline{a^t \bar{u}} + (\bar{v} \times \bar{w}) \overline{a^t \bar{u}},$$

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

Section 2

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 $\varphi_{\pm} : M \rightarrow N$ by

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

(40) CTPM

it suffices to show that (i) the assignments (10) 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 $r + i \equiv r + 3i \mod 7$. Then $2i \equiv 0 \mod 7$, hence $i \equiv 0 \mod 7$, a contradiction.

(ii) Let $(r, i), (s, j) \in M$. If $\varphi_+(r, i) = \varphi_+(s, j)$, then $r + i \equiv s + j \mod 7$ and $r + 3i \equiv s + 3j \mod 7$. Taking differences, we conclude $2i \equiv 2j \mod 7$, hence $i \equiv j \mod 7$ and then $i = j$. This implies $r \equiv s \mod 7$, hence $r \equiv s$, 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 $r + i \equiv s + 3j \mod 7$, $r + 3i \equiv s + j \mod 7$, and taking differences yields $2i \equiv -2j \mod 7$, hence $i \equiv j \equiv 0 \mod 7$, a contradiction. This proves (iii).

Combining (1.5.10) with (2.1.1), we deduce $t_0(u_i) = 0, n_0(c_j) = 1$ for $1 \leq r \leq 7$, so $u_i \in \Omega^8_1$ has euclidean norm 1, while (2) follows immediately from (2.1.2). Thus (ii) holds.

(iii) $\Rightarrow$ (iv). For $1 \leq r \leq 7$, $i = 1, 2, 4$, indices mod 7, we combine (4) with (1.5.13), (1.5.9) and obtain $t_0(u_{i+1}, u_{i+3}) = t_0(u_{i+1}, u_{i+3}) = t_0(u_{i+1}, u_{i+3}) = t_0(u_{i+1}, u_{i+3}) = 0$. By Exc. (3) therefore, $(u_1)_1 \leq r \leq 7$ forms an orthonormal basis of $\Omega^8_1$, giving the final assertion of the problem. The second set of equations in (5) is just (4) for $r \geq 4, i = 4$, and implies $n_0(u_{12}, u_3) = n_0(u_4, u_3) = 0$. Thus (iii) holds.
(iv) ⇒ (i). Systematically counting indices mod 7, we establish the desired implication by proving
the following intermediate assertions.

1. \( n_0(u_i) = 1 \) for \( 1 \leq r \leq 7 \). By (iii) this is clear for \( r \leq 3 \), and for \( r \geq 4 \) follows from \( 5 \) by
induction since the norm of \( \mathfrak{O} \) by Theorem \( 11 \) permits composition.

2. \( n_0(u_i, u_j) = 0 \) for \( 1 \leq r, s \leq 4 \) distinct. By (iii), we may assume \( s = 4, r \leq 2 \). Then \( 1.8 \) implies
\( n_0(u_i, u_j) = n_0(u_i, u_{i+2}) = n_0(u_j, u_{j+2}) = n_0(u_j, u_{j+4}) = 0 \), as claimed.

3. \( \mathfrak{O} \). Let \( 1 \leq r \leq 7 \) and \( i = 1, 2, 4 \) such that \( u_i = u_i u_{r+2} \). If \( u_{i+2} \) has trace zero, then \( u_i \) has
trace zero if and only if \( u_{i+2}, u_{r+2} \) are orthogonal. Moreover, if this is so and \( u_{i+2} \) as well as
\( u_{r+2} \) both have trace zero, then \( u_i = -u_{i+2} u_{r+2} \). Since \( u_{i+2} = -u_{i+4} \), we deduce from \( 1.5, 13 \)
that \( t_2(u_i) = -n_0(u_{i+2}, u_{r+2}) \), giving the first assertion. Since, under the final conditions stated,
\( u_i, u_{i+2}, u_{r+2} \) are all skew relative to the conjugation of \( \mathfrak{O} \), and this is an algebra involution, we
conclude \( u_i = -u_i = -u_{i+2} u_{r+2} = -u_{i+3} u_{r+3} \), as claimed.

4. \( u_i \in \mathfrak{O}^0 \) for \( 1 \leq i \leq 7 \). By (iii), this is automatic for \( r \leq 3 \), while it follows immediately from \( 2^0 \),
\( 3^0 \) (with \( i = 4 \) for \( r = 4, 5, 6 \). It remains to discuss the case \( r = 7 \). We have \( u_i = u_i u_{2i} \), and \( 3^0 \)
combined with \( 1.8 \) yields \( n_0(u_i, u_{2i}) = n_0(u_i u_{2i}, u_{2i+2}) = -n_0(u_{2i+2}, u_{2i+4}) = -n_0(u_{2i+4}, u_{2i+6}) = 0 \).
Hence the first part of \( 3^0 \) yields \( t_3(u_{2i}) = 0 \).

5. \( (u_{i+1} u_{j+3})_{i+1} \) is an orthonormal basis of \( \mathfrak{O}^0 \) and \( u_{i+1}^2 = -u_i u_{i+4} \) for \( 1 \leq i, j \leq 7 \) distinct.
The first part follows immediately from \( 1^0, 3^0, 4^0 \) combined with \( 5 \) while the second part is
now a consequence of \( 1^0 \) and \( 1.5.10, 1.5.13 \).

6. \( \mathfrak{O} \). Let \( 1 \leq r \leq 7 \) and \( i = 1, 2, 4 \) such that \( u_{i+2}, u_{r+3} = u_i \). Then

\[
\begin{align*}
\text{RTWI} & \quad u_{i+2} u_{r+3} = u_i, \\
\text{RFOI} & \quad u_{r+3} u_{i+2} = u_i,
\end{align*}
\]

(41) (42)

Since \( u_{i+2} u_{r+3} = u_i \) by \( 5 \) and \( \mathfrak{O} \) is an alternative algebra, \( u_{i+2} u_{r+3} = -u_{r+3} u_{i+2} = u_{i+2} \), and \( 41 \)
follows. \( 42 \) is proved similarly.

In view of \( 6^0 \), the proof of the implication (iv) ⇒ (i) will be complete once we have shown
\( 7^0 \). \( u_{i+4} u_{r+5} = u_i \) for \( 1 \leq r \leq 7 \). By \( 5 \), this is clear for \( 4 \leq r \leq 7 \), and \( 6^0 \) yields

\[
\begin{align*}
\text{ESONE} & \quad u_{i+1} u_{i+3} = u_i, \\
\text{ESTWO} & \quad u_{i+2} u_{i+3} = u_i
\end{align*}
\]

(43) (44)

Now let \( 1 \leq r \leq 2 \). Then \( 5 \) combined with \( 5^0 \), the middle Moufang identity (cf. Exc. \( 4 \)) and \( 43 \)
yields

\[
\begin{align*}
u_{i+4} u_{r+5} & = (u_{i+1} u_{i+2}) (u_{i+2} u_{r+3}) = (u_{i+2} u_{i+3}) (u_{i+3} u_{r+2}) = u_{i+2} (u_{i+3} u_{r+3}) u_{r+2} \\
& = u_{i+2} u_{i+3} u_{r+2} = -u_{i+3} u_{i+2} = -u_{i+2} u_{i+3} \equiv u_i,
\end{align*}
\]

so we are left with the case \( r = 3 \). Applying \( 43 \) for \( s = 1 \) and \( 44 \) for \( s = 3 \), we obtain

\[
\begin{align*}
u_{i} u_{s} & = (u_i u_s) u_1 = (u_i u_s) (u_2 u_4) = u_4 (u_i u_s) u_4 = u_4 (u_{i} u_{s} u_{4} u_{6}) u_4 \\
& = u_{i} u_{s} u_{4} u_4 = -u_4 (u_i u_s) = -u_4^2 u_3 = u_i,
\end{align*}
\]

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 \( 5 \) is the same as \( 2.11 \). As to the second, the alternative
laws combined with the fact that \( \mathfrak{O} \) is a division algebra yield the following chain of equivalent conditions.
Similarly, the third equation of (45) may be rephrased as
\[(u_3 u_{r+1}) u_{r+3} = -1 \Leftrightarrow (u_3 u_{r+1}) u_{r+3}^2 = -u_{r+3} \Leftrightarrow u_3 u_{r+1} = u_{r+3} \]
(46)

Hence (i) implies (ii). Conversely, suppose (ii) holds. Then the first equation of (3) combined with
(iii) shows that the elements \(u_r, 1 \leq r \leq 7\), belong to \(O^0\) and have length 1, while
(45), (46) yield \(u_1 u_{r+1} = u_{r+3}, u_{r+1} u_{r+3} = u_r\). Combining with (3), (4), (5) we deduce
\(n_0(u_1 u_{r+1}) = t_0(u_1 u_{r+1}) = -t_0(u_1 u_{r+1}) = t_0(u_{r+3}) = 0\) and, similarly, \(n_0(u_{r+1} u_{r+3}) = 0\). In
particular, \(u_1, u_2, u_3\) form an orthonormal system in \(O^0\) such that \(n_0(u_1 u_2, u_3) = n_0(u_3, u_4) = 0\),
and we have \(u_r = u_{r-3} u_{r-2}\) for \(4 \leq r \leq 7\). Since, therefore, condition (v) holds, so does (ii).

\[O^+\] is clearly a commutative real algebra with identity element \(1_{O^+} = 1_0\). Moreover, the squarings
\(\phi \in \text{Aut}(O)\) fixes \(1_0\) and preserves squares in \(O\). From
(1\(, 5\), 10) we therefore deduce \(t(x)x = n(x)1_0\) for all \(x \in O\), where \(t := t_0 \circ \phi - t_0, n := n_0 \circ \phi - n_0\).
Thus \(\phi\) is the union of the subspaces \(\text{Ker}(t)\) and \(\mathbb{R}1_0\). This implies first \(t = 0\) and then \(n = 0\), so \(\phi\)
is an orthogonal transformation of \(O\) fixing \(1_0\), hence stabilizing \(O^0 = (1_0)^{\perp}\). The assignment
\(\phi \mapsto \phi|_{O^0}\) clearly gives an injective group homomorphism from \(\text{Aut}(O^0)\) to \(\text{Aut}(O)\). Conversely,
the unique linear extension fixing \(1_0\) of \(\psi \in \text{O}(O^0)\) belongs to the orthogonal group of \(O\) and
leaves the trace invariant, hence is an automorphism of \(O^0\). 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, \(\text{Aut}(O)\) is trivially a
subgroup of \(\text{Aut}(O^+)\) which is closed since it may be realized via
\[\text{Aut}(O) = \bigcap_{x \in O} \{ \phi \in \text{GL}(O) \mid \phi(xy) = \phi(x)\phi(y) \}\]
as the intersection of a family of closed subsets of \(\text{GL}(O)\).

**Section 3**

**sol.CHALAT**

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 \(r_k(L) \leq r_k(L_1) = n\).

(ii) \(\Rightarrow\) (i). Let \(e = (e_1, \ldots, e_r)\), \(r \leq n\), be a \(\mathbb{Z}\)-basis of \(L\). Since \(L_0\) spans \(V\), so does \(e\), and we
conclude that \(e\) is an \(\mathbb{R}\)-basis of \(V\), forcing \(L \subseteq V\) to be a lattice.

**sol.LASTRU**

\(M + \sqrt{3}M \subseteq A\) is a free abelian subgroup of rank \(2 \dim_{\mathbb{R}}(A)\) which is obviously closed under
multiplication but not a lattice, hence not a \(\mathbb{Z}\)-structure of \(A\).

**sol.REONE**

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.

**Section 4**

**sol.HURCON**

By Thm. 4.2 (13, i, j, h) is an \(\mathbb{R}\)-basis of \(\mathbb{H}\) that is associated with \(\text{Hur}(\mathbb{H})\). Hence \(\text{Hur}(\mathbb{H})\)
consists of all linear combinations
Thus the preceding determinant formula reduces to

$$\det(\alpha 1_{\mathbb{H}} + \beta i + \gamma j + \delta h) = \det(\alpha 1_{\mathbb{H}} + \beta i + \gamma j + \delta h)$$

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.

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

\[
\begin{align*}
n_{\mathbb{H}}(x) &= \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \det(\alpha 1_{\mathbb{H}} + \beta i + \gamma j + \delta h), \\
n_{\mathbb{H}}(x) &= 2\alpha + \beta + \gamma + \delta, \\
n_{\mathbb{H}}(i, x) &= 2\beta + \delta, \\
n_{\mathbb{H}}(j, x) &= 2\gamma + \delta, \\
n_{\mathbb{H}}(h, x) &= \alpha + \beta + \gamma + 2\delta
\end{align*}
\]

are all integers. Multiplying \((51)\) by 2 and subtracting the sum of \((48), (49), (50)\) 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 \((47)-(50)\). Thus \(\alpha, \beta, \gamma \in (0, \frac{1}{2}]\), forcing \(\alpha = \beta = \gamma = \delta = 0\) as well.

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

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

To see this, we make use of the well known fact that \((52)\) holds for \(B = 0\) or \(C = 0\). Hence

\[
\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A) \det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A) \det\begin{pmatrix} \alpha & B \\ \beta & D \end{pmatrix} = \det(A) \det\begin{pmatrix} 1 & B \\ -CA^{-1} & D \end{pmatrix} = \det(A) \det(D - CA^{-1}B),
\]

as claimed. Turning to the matrix \(S\) of our problem, we now conclude

\[
\det(S) = \det(r \cdot 1_p) \det(s \cdot 1_q - T_2^{-1} \cdot 1_p) T_1 = \det(s \cdot 1_q - r^{-1} T_2 T_1) = \det(r^{-q} \cdot T_2 T_1) = \det(r^{-q} \cdot \text{char}_{T_2 T_1}(rs)),
\]

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

\[
T_2 T_1 = T^i T = \begin{pmatrix} v_1^T \\ \vdots \\ v_q^T \end{pmatrix} (v_1, \ldots, v_q) = (v_i v_j)_{1 \leq i, j \leq q} = \text{diag}(\|v_1\|^2, \ldots, \|v_q\|^2).
\]

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 \(i = 1, \ldots, q\), the second assertion stated in our problem drops out. Finally, assuming \(\|v_i\|^2 < rs\) for all \(i = 1, \ldots, q\), 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 \(1 \leq i \leq p + q\). For \(i \leq p\), the the \(i\)-th principal minor of \(S\) is 1, while for \(p < i \leq p + q\), it is the determinant of the matrix

\[
S' := \begin{pmatrix} r \cdot 1_p & T' \\ (T')^T & s \cdot 1_{p'-q} \end{pmatrix},
\]

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

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

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

\[\text{sol.UNIT}\]

(a) Since the norm of \(D\) permits composition by Thm. 17, the set of units in \(M\) is closed under multiplication and contains \(1_D\).

If (i) holds, then \(HUNI\) implies \(u\bar{u} = n_D(u)1_D = 1_D = \bar{u}u\). Thus (i) implies (ii) and (iii). Conversely, suppose (ii) holds. Then \(1 = n_D(u) = n_D(a)n_D(v)\), and since both factors on the right are integers by Prop. 3.9, we conclude \(u \in M\). This shows that (i) and (ii) are equivalent. The equivalence of (i) and (iii) is proved similarly. Moreover, for any \(v\) satisfying (iii) we apply Exc. 11, (i) and (ii) and obtain \(u = 1_D\bar{u} = n_D(u)v = v\) (by (i)), and the proof is complete.

(b) \(1_1, i_1, j_1, k_1\; (1_2, i_2, j_2, k_2)\) is an orthonormal basis of \(C\) associated with \(Ga(C)\). Hence \(Ga(C)^\times = \{\pm 1, \pm i\}\). Similarly, \(1_3, i_3, j_3, k_3\) is an orthonormal basis of \(H\) associated with \(Ga(H)\). Hence \(Ga(H)^\times = \{\pm 1_H, \pm i, \pm j, \pm k\}\). And, finally, any Cartan-Schouten basis \((u_r)_{0 \leq r \leq 7}\) of \(\mathfrak{O}\) is an orthonormal basis associated with \(Ga(\mathfrak{O})\). Hence \(Ga(\mathfrak{O})^\times = \{\pm u_r \mid 0 \leq r \leq 7\}\). Now we claim

\[
\text{Hur}(H)^\times = \{\pm 1_H, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1_H \pm i \pm j \pm k)\}. \tag{53} \]

To prove this, we note that the first eight elements of the right-hand side belong to \(Ga(H)^\times \subseteq \text{Hur}(H)^\times\). The remaining sixteen may all be obtained from adding a unit of \(Ga(H)\) to \(h\), hence belong to \(\text{Hur}(H)\). Since they also have norm 1, the right-hand side of (53) belongs to the left. Conversely, suppose \(u = a_01_H + a_1i + a_2j + a_3k\) with \(a_i \in \mathbb{R}\), \(0 \leq i \leq 3\), is a unit in \(\text{Hur}(H)\). By Exc. 11 there are two cases.

Case 1. \(a_i \in \mathbb{Z}, 0 \leq i \leq 3\). Then \(u \in Ga(H)^\times \subseteq \text{Hur}(H)^\times\).

Case 2. \(a_i = \frac{1}{2} + \beta_i, \beta_i \in \mathbb{Z}, 0 \leq i \leq 3\). Then

\[
1 = n_H(u) = \sum_{i=0}^3 \left(\frac{1}{4} + \beta_i + \beta_i^2\right) = 1 + \sum_{i=0}^3 (\beta_i^2 + \beta_i),
\]

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 \(0 \leq i \leq 3\). But this means \(a_i = \pm \frac{1}{2}\) for \(0 \leq i \leq 3\), and \(u\) belongs to the right-hand side of (53).

\[\text{sol.HURDE}\]

That the \(e_i, 1 \leq i \leq 4\), form an orthonormal basis of \(H\) relative to \((x, y)\) follows immediately from the fact that the vectors \(1_H, i, j, k\) of \(H\) are orthogonal of norm 1. Moreover, the latter vectors can be linearly expressed by the former according to the formulas

\[
e_1 - e_2 = j, \quad e_2 - e_3 = -h, \quad e_3 - e_4 = 1_H, \quad e_1 + e_4 = i.
\]

In particular, the second equation of the problem holds. Given \(\xi_i \in \mathbb{R}, 1 \leq i \leq 4\), we also obtain
Using (4.1.1), we therefore deduce

\[ \sum_{i=1}^{4} \xi_i e_i = \frac{1}{2} \left( (\xi_1 - \xi_4)1_{1\mathbb{H}} + (\xi_3 + \xi_4)i + (\xi_1 - \xi_2)j - (\xi_1 + \xi_2)k \right). \]

Using (4.1.1), we therefore deduce

\[ \sum_{i=1}^{4} \xi_i e_i = \frac{1}{2} \left( (\xi_1 - \xi_4)1_{1\mathbb{H}} + (\xi_3 + \xi_4)i + (\xi_1 - \xi_2)j - (\xi_1 + \xi_2)k \right) \]

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

\[ \sum_{i=1}^{4} \xi_i e_i \in \text{Hur}(\mathbb{H}) \iff \xi_1, \xi_1 + \xi_2 \in \mathbb{Z}, \quad \xi_1 + \xi_2 + \xi_3 \pm \xi_4 \in 2\mathbb{Z} \]

\[ \iff \xi_1, \xi_2 \in \mathbb{Z}, \quad \sum_{i=1}^{4} \xi_i \in 2\mathbb{Z}, \quad 2\xi_4 \in 2\mathbb{Z} \]

\[ \iff \xi_1, \xi_2, \xi_3, \xi_4 \in \mathbb{Z}, \quad \sum_{i=1}^{4} \xi_i \in 2\mathbb{Z}. \]

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

\[ \sum_{i=1}^{4} \xi_i e_i \in \text{Hur}(\mathbb{H})^\times \iff \frac{1}{4} \sum_{i=1}^{4} \xi_i^2 = 1 \iff \sum_{i=1}^{4} \xi_i^2 = 2, \]

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 Hur(\( \mathbb{H} \)) have the form stated at the very end of the problem.

(a) This follows immediately from the fact that Cartan-Schouten bases are orthonormal relative to \( n_{1\mathbb{H}} \) (Exc. 6). For example, \( n_{1\mathbb{H}}(e_1) = \frac{1}{4} (n_{1\mathbb{H}}(u_0) + n_{1\mathbb{H}}(u_2)) = \frac{1}{4} \), which implies \( \langle e_1, e_1 \rangle = 2n_{1\mathbb{H}}(e_1) = 1 \).

(b) We write \( L \) for the additive subgroup of \( \mathbb{O} \) generated by the quantities assembled in (4.1). We claim

\[ \text{Cox}(\mathbb{O}) \subseteq L \subseteq \frac{1}{2} \sum_{i=1}^{8} \mathbb{Z} e_i, \quad (54) \]

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

\[ a_0 = -e_1 + e_2, \quad a_1 = -e_3 + e_4, \quad a_2 = e_1 + e_2, \quad a_3 = -e_3 - e_4, \quad (55) \]

\[ a_4 = -e_3 + e_6, \quad a_5 = e_3 + e_6, \quad a_6 = e_7 + e_8, \quad a_7 = -e_7 + e_8 \]

all belong to \( L \). Moreover, (55) and (4.4.3)–(4.4.7) imply
Thus the basis $E'$ exhibited in (4.5), which is associated with $\text{Cox}(\mathcal{O})$ by Thm. 4.5, is entirely contained in $L$, and the first inclusion of (53) holds. From this and Exc. 8 we deduce that $L$ is a lattice in $\mathcal{O}$. Since Cox($\mathcal{O}$) is unimodular by Thm. 4.3 the proof of (b) will be complete once we have shown that the lattice $L$ is integral quadratic (Cor. 3.14). Since $n_\mathcal{O}(e_i) = \frac{1}{2}$ for $1 \leq i \leq 8$ by (a), equation (1) yields

$$n_\mathcal{O}(\pm e_i, \pm e_j) = n_\mathcal{O}\left( \frac{1}{2} \sum_{i=1}^{8} s_i e_i \right) = 1$$

for $1 \leq i < j \leq 8$ and all families $s = (s_i) \in \{\pm1\}^8$. Writing $M := \{1, 2, \ldots, 8\}$ and $M'_i := \{i \in M \mid s_i = \pm 1\}$, it remains to show

$$n_\mathcal{O}(\pm e_i, \pm e_i, \pm e_k, \pm e_l) \in \mathbb{Z}, \quad n_\mathcal{O}\left( \frac{1}{2} \sum_{i=1}^{8} s_i e_i, \frac{1}{2} \sum_{i=1}^{8} t_i e_i \right) \in \mathbb{Z}$$

for all $1 \leq i < j < k < l \leq 8$ and all families $s = (s_i), t = (t_i) \in \{\pm1\}^8$ such that $|M'_i|$ and $|M'_j|$ are both even. The first relation of (61) is obvious. In order to prove the second, we let $s = (s_i) \in \{\pm1\}^8$ be arbitrary and note $|M'_i| + |M'_j| = 8$, so $|M'_i|$ are either both even or both odd. Moreover, $-s := (-s_i) \in \{\pm1\}^8$ and $M''_i = M'_i$. Now, letting also $t = (t_i) \in \{\pm1\}^8$ be arbitrary and setting $s't := (s_it_i) \in \{\pm1\}^8$, we obtain

$$n_\mathcal{O}\left( \frac{1}{2} \sum_{i=1}^{8} s_i e_i, \frac{1}{2} \sum_{i=1}^{8} t_i e_i \right) = \frac{1}{4} \sum_{i=1}^{8} s_i t_i = \frac{1}{4} (|M''_i| - |M''_j|) = \frac{1}{2} - \frac{1}{2} |M''_i|,$$

and must show that if $|M''_i|$ and $|M''_j|$ are even, then so is $|M''_i|$. Suppose not. Then

$$|M''_i| = |M'_i \cup M'_j| + |M'_i \cup M'_j|$$

is odd. Replacing $s$ by $-s$, $t$ by $-t$ if necessary, we may assume that $|M'_i \cup M'_j|$ is odd and $|M'_i \cup M'_j|$ is even. But then

$$|M'_i| = |M'_i \cup M'_j| + |M'_i \cup M'_j|$$

shows that $|M'_i \cup M'_j|$ is odd, whence

$$|M'_i| = |M'_i \cup M'_j| + |M'_i \cup M'_j|$$

is odd as well, a contradiction.

(c) Write $L'$ for the right-hand side of (2). Inspecting (53)–(59), we conclude $\text{Cox}(\mathcal{O}) \subseteq L' \subseteq \frac{1}{2} \sum Z e_i$, so $L'$ is a lattice in $\mathcal{O}$ by Exc. 8. As before, we will be through once we have shown that $L'$ is integral quadratic. Let $x = \sum Z e_i \in L'$ with $\xi_1, \ldots, \xi_8 \in \mathbb{R}$. Then (3) implies $2\xi_1 \in \mathbb{Z}$, $\xi_i = \xi_1 + n_i$, $n_i \in \mathbb{Z}$ for $1 \leq i \leq 8$, 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 $N := \{i \in M \mid n_i \equiv 1 \text{ mod } 2\}$ contains an even number of elements. Now $n_\mathcal{O}(x) = \frac{1}{2} \sum Z e_i$ and
that the additive map from $\mathbb{Z}$ to $\mathbb{Z}$, now we use Exc. 13. (52)), and obtain

A straightforward verification using (63) shows by Exc. 8 that $u = \sum_{i=1}^{8} \xi_i e_i, \xi_i \in \mathbb{R}, 1 \leq i \leq 8,$ is a unit in $\text{Cox}(\mathcal{O}).$ Then (a) implies

$$\sum_{i=1}^{8} \xi_i^2 = 2n_\mathcal{O}(u) = 2. \quad (62)$$

If $\xi_i$ is an integer, then all $\xi_i, 1 \leq i \leq 8,$ are, and (62) shows that $u$ belongs to the first type of (1). On the other hand, if $\xi_i$ belongs to $\frac{1}{2} + \mathbb{Z},$ then all $\xi_i, 1 \leq i \leq 8,$ do, and (62) shows $\xi_i = \frac{1}{2},$ hence $\xi_i = \pm \frac{1}{2}$ for all $i = 1, \ldots, 8.$ Since $\sum_{i=1}^{8} \xi_i \in \mathbb{Z}$ by (2), the number if indices $i = 1, \ldots, 8$ having $\xi_i$ negative must be even, so $u$ is of the second type in (1).

The units of $\text{Cox}(\mathcal{O})$ belonging to the first type of (1) are in bijective correspondence with the quadruples of subsets of $M$ consisting of two elements, hence are $4 \cdot \binom{8}{2} = 4 \cdot 28 = 112$ in number. On the other hand, the units of $\text{Cox}(\mathcal{O})$ 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 $2^8 = 256$ in number. All in all, therefore, $\text{Cox}(\mathcal{O})$ has exactly $112 + 256 = 368$ units.

The inclusions $\text{Ga}(\mathcal{O}) \subset \text{Kir}(\mathcal{O}) \subset \frac{1}{2} \text{Ga}(\mathcal{O})$ follow immediately from the definition and show by Exc. 17 that $L := \text{Kir}(\mathcal{O})$ is a lattice in $\mathcal{O}.$ Since $(u_i)_{0 \leq i \leq 7}$ is an orthonormal basis of $\mathcal{O},$ we have $n_\mathcal{O}((\text{Ga}(\mathcal{O}), v_i) \subseteq \mathbb{Z}$ for $1 \leq i \leq 4,$ and a straightforward verification shows

$$n_\mathcal{O}(v_i) = 1, \quad n_\mathcal{O}(v_1, v_2) = 0, \quad n_\mathcal{O}(v_j, v_k) = 1 \quad (63)$$

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

Next we consider the family

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

of elements in $L.$ From $u_4 = 2v_1 - 1_\mathcal{O} - u_3 - u_2, u_5 = 2v_2 - 1_\mathcal{O} - u_3 - u_1, u_7 = -2v_3 + 1_\mathcal{O} + u_1 + u_3, u_9 = -2v_4 + u_3 + u_1 - u_2$ we deduce that $E_1$ spans $\mathcal{O}$ 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 $\mathcal{O}$ associated with $L.$

We now proceed to determine the discriminant of $L$ by computing the determinant of $Dn_\mathcal{O}(E_1).$ A straightforward verification using (63) shows

$$Dn_\mathcal{O}(E_1) = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$
Observing (4.4.3), we also put
\[ \phi \] is a model of the Hamiltonian quaternions matching 1
\[ \phi \] is an automorphism of \[ \mathbb{O} \]
\[ \phi \] the linear bijection
rules for Cartan-Shouten bases as depicted in Fig. 1 of 2.5.
\[ u \] coefficients of \[ \mathbb{Z} \]
\[ Z \]
\[ Z \] is a unimodular integral quadratic lattice in \[ \mathbb{O} \]
\[ Z \]
\[ Z \] is contained in \[ \mathbb{O} \]
\[ Z \]
\[ Z \] is odd.
\[ Z \] is odd
\[ Z \] are both odd. Thus \[ v_1v_3 \] does not belong to \( \text{Kir}(\mathbb{O}) \), as desired.

The idea of the solution is to imitate our construction of the Coxeter octonions with a different model of the Hamiltonian quaternions inside \[ \mathbb{O} \] and a different vector \[ q \in \mathbb{O} \] in place of \[ p \] such that the resulting \( \mathbb{Z} \)-structure agrees with \( R \). In doing so, repeated use will be made of the multiplication rules for Cartan-Shouten bases as depicted in Fig. 1 of 2.5.

On a more formal level, these multiplication rules as described in (2.1.1) and (2.1.2) show that the linear bijection \( \phi : \mathbb{O} \to \mathbb{O} \) determined by
\[ \phi(1) = 1 \cdot \mathbb{O}, \quad \phi(u_i) = u_{i+2}, \quad (1 \leq r \leq 7, \text{ indices mod } 7) \]
is an automorphism of \( \mathbb{O} \). With \( \mathbb{H} \subseteq \mathbb{O} \) as given in (4.4.1) we therefore conclude that
\[ B := \phi(\mathbb{H}) = \mathbb{R}1 + \mathbb{R}u_3 + \mathbb{R}u_4 + \mathbb{R}u_6 \subseteq \mathbb{O} \]
is a model of the Hamiltonian quaternions matching \( 1 \mathbb{H} = 1 \cdot \mathbb{O}, \mathbb{I} = u_3, \mathbb{J} = u_4, \mathbb{K} = u_6 \) and
\[ \text{Ga}(B) := \phi(\text{Ga}(\mathbb{H})) = \mathbb{Z}1 + Zu_3 + Zu_4 + Zu_6. \]

Observing (4.4.3), we also put
\[ q := \phi(p) = \frac{1}{2}(1 \cdot \mathbb{O} + u_3 + u_4 + u_5) \]
and deduce from Thm. 4.5 that
\[ R' := \phi(\text{Cox}(\mathbb{O})) = \text{Ga}(B) + \text{Ga}(Bq) \]
is a \( \mathbb{Z} \)-structure of \( \mathbb{O} \) isomorphic to \( \text{Cox}(\mathbb{O}) \). It therefore remains to show \( R' = R \).

We first note that \( \text{Ga}(\mathbb{O}) \) is contained in \( R \) (by definition) but also in \( R' \) (by Thm. 4.5). Moreover, invoking (4.4.4) – (4.3.7), we deduce
\[
\begin{align*}
\varphi(q) &= \frac{1}{2}(-10 + u_2 + u_3 + u_6), \\
\varphi(2q) &= \frac{1}{2}(-10 + u_4 - u_6 + u_7), \\
\varphi(3q) &= \frac{1}{2}(-u_1 - u_3 + u_4 + u_6).
\end{align*}
\]

Now an inspection shows
\[
\begin{align*}
v_1 + v_4 &= \frac{1}{2}(10 + u_3 + u_4 + u_5) \equiv q \mod \mathcal{O}, \\
v_2 + v_4 &= \frac{1}{2}(10 + u_2 + u_3 + u_6) \equiv u_5q \mod \mathcal{O}, \\
v_1 + v_2 + v_4 &= \frac{1}{2}(10 + u_4 + u_6 + u_7) \equiv u_6q \mod \mathcal{O}, \\
v_1 + v_2 + v_4 &= \frac{1}{2}(u_1 + u_3 + u_4 + u_6) \equiv u_6q \mod \mathcal{O}.
\end{align*}
\]

Since
\[
\varphi(E') = (10, u_3, u_4, u_5, q, u_5q, u_5q, u_6q)
\]
by (4.5.2) is a basis of \( \mathcal{O} \) associated with \( E' \), the preceding relations imply \( R' \subseteq R \). But they also yield
\[
\begin{align*}
u_5q - u_6q &\equiv v_3 \mod \mathcal{O}, \\
u_6q - u_5q &\equiv v_1 \mod \mathcal{O}, \\
u_6q - q &\equiv v_2 \mod \mathcal{O}, \\
q + u_5q - u_6q &\equiv v_4 \mod \mathcal{O}
\end{align*}
\]
and hence imply \( R \subseteq R' \). This shows \( R = R' \) and the proof is complete.

Let \( (u_5)_{0 \leq i \leq 7} \) be a Cartan-Schouten basis of \( \mathcal{O} \). In the language of Exc. 15, we have
\[
q := \frac{1}{2}(10 + u_3 + u_4 + u_6) = \frac{1}{2}(-e_1 + e_2 - e_3 - e_4 + e_5 + e_6),
\]
whence part (d) of that exercise shows that \( q \) is a unit in \( \text{Cox}(\mathcal{O}) \). 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 \( 1 \rightarrow 1, i \rightarrow u_i, j \rightarrow u_j, h \rightarrow q \) determine an additive embedding \( \text{Hur}(\mathcal{H}) \hookrightarrow \text{Cox} \mathcal{O} \) that preserves multiplication, hence is an embedding of \( Z \)-algebras.

**Section 5**

Computing the square of the matrix (5.4.2) in a straightforward manner yields (5.9.3). Linearizing and dividing by 2 immediately yields (5.9.4). Taking the trace of (5.9.4) and applying (5.8.3), we obtain
\[
T(x \cdot y) = \sum (\alpha_i \beta_i + \frac{1}{2} n_0(u_i, v_j) + \frac{1}{2} n_0(u_i, v_i)) = \sum \alpha_i \beta_i + \frac{1}{2} \left( \sum n_0(u_i, v_j) + \sum n_0(u_i, v_i) \right),
\]
and (5.9.5) follows. Writing
\[
z = \sum (\gamma_i e_i + w_i [j]), \quad (\gamma_i \in \mathbb{R}, w_i \in \mathcal{O}, \ 1 \leq i \leq 3),
\]

\[
\begin{align*}
\varphi(q) &= \frac{1}{2}(-10 + u_2 + u_3 + u_6), \\
\varphi(2q) &= \frac{1}{2}(-10 + u_4 - u_6 + u_7), \\
\varphi(3q) &= \frac{1}{2}(-u_1 - u_3 + u_4 + u_6).
\end{align*}
\]
we first note by (5.13) and Exc. (b) that, for all \(u, v, w \in \mathbb{O}\), the expression
\[
n_0[T(uv), w] = t_0(uvw)\]
is invariant under cyclic permutations of the variables. (67)

Combining (5.94) with (5.95), we therefore obtain
\[
T((x \ast y) \ast z) = \sum \left( (\alpha_j + \frac{1}{2}n_0(u, v)) \gamma + \frac{1}{2}n_0(u, v) \right) y_j
+ \frac{1}{2}n_0 \left( (\alpha_j + \alpha_i) n_0(u, v) + \beta_i \right) u + u_j v_i + v_j u_i, w_i \right) \]
\[
= \sum \left( (\alpha_j + \frac{1}{2}(\gamma_j + \gamma_i) n_0(u, v) + \beta_i \right) u + u_j v_i + v_j u_i \right)
+ \frac{1}{2} (\beta_i + \beta_j) n_0(w, u) + \frac{1}{2} (t_0(uv), w) + t_0(wv, u)) \right). \]

This expression obviously being symmetric in \(x, z\), we end up with (5.94).

We now turn to (5.97). Combining (5.83) with (5.95) we deduce
\[
T(x)T(y) - T(x \ast y) = \sum (\alpha_i)(\beta_j) - \sum (\alpha_i n_0(u, v)) \]
\[
= \sum (\alpha_j + \alpha_i n_0(u, v)), \]
which by (5.87) agrees with \(S(x, y)\). Similarly, by (5.93), (5.83), (5.86) and (5.84) we obtain
\[
x^2 - T(x) + S(x) = \sum \left( (\alpha_j^2 + n_0(u, v)) e_i + \left( (\alpha_j + \alpha_i) u_j + \beta_i \right) e_i \right)
- \left( \sum \alpha_i \right) \sum (\alpha_i e_i + u_i e_i) + \sum (\alpha_i n_0(u, v)) \left( \sum e_i \right) \]
\[
= \sum \left( (\beta_i n_0(u, v) + n_0(u, v)) e_i + \left( (\alpha_j + \alpha_i) u_j + \beta_i \right) e_i \right)
- \sum (\alpha_i n_0(u, v)) + \sum (\beta_i) n_0(u, v) \left( \sum e_i \right) \]
\[
= \sum \left( (\alpha_i \beta_i - n_0(u, v)) e_i + \left( - \alpha_i u_i + \beta_i \right) e_i \right) = x^2, \]
which completes the proof of (5.98).

Differentiating (5.82) at \(x\) in the direction \(y\) and observing (67), we obtain
\[
DN(x)(y) = \beta_i n_0(u) + \alpha_i n_0(u, v)) \]
\[
+ t_0(u v_1 u_2 u_3) + t_0(u_1 v_1 u_2 u_3) + t_0(u v_1 u_2 v_3) \]
\[
= \sum (\alpha_i \beta_i - n_0(u)) \beta_i - \alpha_i n_0(u, v) + t_0(u v_1 u_2 v_3), \]
while combining (5.95) with (5.84) and (67) yields
\[
T(x^2 \ast y) = \sum \left( (\alpha_i \beta_i - n_0(u)) \beta_i + n_0(u_i + \beta_i) \right) v_i \]
\[
= \sum (\alpha_i \beta_i - n_0(u)) \beta_i - \alpha_i n_0(u, v) + t_0(u v_1 u_2 v_3), \]
which proves the first equation of (5.99), while the second one derives from (5.98).

In order to prove (5.910), we apply (5.94) and (5.84) to compute
We end up with the fully linearized Jordan identity, which therefore holds in arbitrary real Jordan algebras. Differentiating at \( i \), changing notation and rearranging terms, we obtain

\[
x \cdot x^2 = \sum \left( \alpha_i \alpha_j \alpha_k - n_0(u_i) \right) + \frac{1}{2} n_0(u_j, -\alpha_j u_i + \overline{\alpha_i u_j}) + \frac{1}{2} n_0(u_j, -\alpha_j u_i + \overline{\alpha_i u_j}) e_{ij}
\]

Since the conjugation of \( \mathcal{O} \) is an involution and \( (u, u_j^i) \bar{a}_j = n_0(u) u_i, \  \bar{a}_i (u u_j) = n_0(u) u_i \) by Exc. ???, we conclude

\[
x \cdot x^2 = \sum \left( \alpha_i \alpha_j \alpha_k - n_0(u_i) \right) + \frac{1}{2} n_0(u_j, -\alpha_j u_i + \overline{\alpha_i u_j}) + \frac{1}{2} n_0(u_j, -\alpha_j u_i + \overline{\alpha_i u_j}) e_{ij}
\]

and plugging in (5.9.10) gives (5.9.11).

Finally, Differentiating \( x^3 = (x \cdot x) \cdot x \) at \( x \) in the direction \( y \), we find \( (y \cdot x) \cdot x + (x \cdot y) \cdot x + (x \cdot x) \cdot y = 2x \cdot (x \cdot y) + x^2 \cdot y \). Performing the same procedure on the right-hand side of (5.9.10), we therefore get (5.9.11).

We have \( \text{Her}_1(\mathcal{O}) \cong \mathbb{R}^3 \), while \( \text{Her}_2(\mathcal{O}) \) sits in the Euclidean Albert algebra via

\[
\text{Her}_2(\mathcal{O}) \cong \left\{ \begin{pmatrix} \alpha_1 & u_1 & 0 \\ \bar{u}_1 & \alpha_2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid \alpha_1, \alpha_2 \in \mathbb{R}, u_1 \in \mathcal{O} \right\}
\]

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

\[
w(u^2 y) + 2u((uv)w) = 2(uw)(uv) + u^2(wv).
\]

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 \( J := \text{Her}_n(\mathcal{O}) \) for some integer \( n \geq 4 \). For \( 1 \leq i, j, l, m \leq n \) mutually distinct and \( u, v \in \mathcal{O} \), we will make use of the obvious relations

\[
e_{il} \cdot u[lm] = \frac{1}{2} \left( \delta_{il} + \delta_{lm} \right) u[lm] = u[lm] \cdot e_{il},
\]

\[
u[j] = \bar{u}[j],
\]

\[
u[j] \cdot v[il] = \frac{1}{2} (uv)[il],
\]

\[
u;j] \cdot v[lm] = 0.
\]

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

\[
\frac{1}{4} ((uv)w)[14] = (u[12] \cdot v[23]) \cdot ((e_{33} + e_{44}) \cdot w[34])
\]

\[
= - (v[23] \cdot (e_{33} + e_{44}) \cdot u[12]) \cdot ((e_{33} + e_{44}) \cdot u[12]) \cdot (v[23] \cdot w[34])
\]

\[
+ u[12] \cdot ((v[23] \cdot (e_{33} + e_{44}) \cdot w[34]) + v[23] \cdot ((e_{33} + e_{44}) \cdot u[12]) \cdot w[34])
\]

\[
+ (e_{33} + e_{44}) \cdot ((u[12] \cdot v[23]) \cdot w[34])
\]

\[
= \frac{1}{8} (u(vw))[14] + \frac{1}{8} ((uv)w)[14].
\]
Thus we obtain the contradiction that \( \mathcal{O} \) is associative. Hence \( J \) cannot be a Jordan algebra.

(a) By hypothesis, \( \deg(\mu) = \dim_{R}[R[x]] = 3 \). Hence \( \mu := \det(11_{R[x]} - L_{0}^{3}) \) is monic of degree 3 as well. Moreover, \( \mu(x) = \mu(L_{0}^{3}) = 0 \), which proves the first assertion. The remaining ones now follow from \( \text{[5.13]2} \).

(b) We begin with preparations for a Zariski density argument. From \( \text{[5.9]10} \) we deduce \( x^{4} = T(x)x^{3} - S(x)x^{2} + N(x)x \), hence

\[
x^{4} = (T(x)x^{3} - S(x)x^{2}) - (T(x)S(x) - N(x))x + (T(x)N(x)1_{3}).
\]

(68) EXFO

Given \( \alpha, \beta \in \mathbb{R} \) for \( 0 \leq i \leq 2 \), we therefore conclude

\[
\left( \sum_{i=0}^{2} \alpha x^{i} \right) \left( \sum_{i=0}^{2} \beta x^{i} \right) = \sum_{i=0}^{3} y x^{i}
\]

with

\[
\begin{align*}
\gamma_{1} &= \alpha_{0}\beta_{0} + \alpha_{2}\beta_{2} T(x)N(x), \\
\gamma_{2} &= \alpha_{0}\beta_{1} + \alpha_{1}\beta_{0} - \alpha_{2}\beta_{1} (T(x)S(x) - N(x)), \\
\gamma_{2} &= \alpha_{0}\beta_{2} + \alpha_{1}\beta_{1} + \alpha_{2}\beta_{0} + \alpha_{2}\beta_{2} (T(x)^{2} - S(x)).
\end{align*}
\]

(69) PROX

Now assume \( 1_{3} \times x \times x^{2} \neq 0 \) in \( \Lambda^{2}(J) \) and put \( u := \sum_{i=0}^{2} \alpha x^{i} \). Then \( \text{[69]} \) implies that \( \mathbb{R}[u] = \mathbb{R}[x] \) if and only if

\[
\Delta(u) := \det\left( \begin{array}{ccc}
1 & \alpha_{0} & \alpha_{2}^{2} + \alpha_{2}^{2} T(x)N(x) \\
0 & \alpha_{0} & 2\alpha_{0}\alpha_{2} - \alpha_{2}^{2} (T(x)S(x) - N(x)) \\
0 & \alpha_{2} & 2\alpha_{2}\alpha_{0} + \alpha_{2}^{2} (T(x)^{2} - S(x)) \end{array} \right) \neq 0.
\]

On the other hand, by \( \text{[68]} \), we have \( \mathbb{R}[x^{2}] = \mathbb{R}[x] \) if and only if \( T(x)S(x) \neq N(x) \).

Then consider the set of 7-tuples

\[
(\alpha_{0}, \alpha_{1}, \alpha_{2}, \beta_{0}, \beta_{1}, \beta_{2}, x) \in \mathbb{R}^{6} \times J
\]

such that, setting \( u = \sum_{i=0}^{2} \alpha x^{i} \), \( v = \sum_{i=0}^{2} \beta x^{i} \), we have \( 1_{3} \times x \times x^{2} \neq 0 \) in \( \Lambda^{2}(J) \), \( T(x)S(x) \neq N(x) \), and the quantities \( \Delta(u) \), \( \Delta(v) \) and \( \Delta(u \bullet v) \) are all different from zero. By the preceding formulas, this set is Zariski-open \( \mathbb{R}^{6} \times J \). But it is also Zariski-dense since, for example, it contains

\[
(\xi_{0}, \xi_{1}, \xi_{2}, \xi_{0}, \xi_{1}, \xi_{2}, \frac{2}{3} \xi_{0} v_{u})
\]

for real numbers \( \xi_{i} \) such that the six quantities \( \pm \xi_{i}, \) \( 0 \leq i \leq 2 \), are mutually distinct.

Hence it suffices to prove the first claim under the additional hypotheses \( 1_{3} \times x \times x^{2} \neq 0 \) in \( \Lambda^{2}(J) \) and \( \mathbb{R}[x] = \mathbb{R}[u] = \mathbb{R}[v] = \mathbb{R}[u \bullet v] \). But then, since \( \mathbb{R}[x] \) is commutative associative, (a) gives

\[
N(u \bullet v) = \det(L_{0}^{u}L_{0}^{v}) = \det(L_{0}^{u}) \det(L_{0}^{v}) = \det(L_{0}^{u}) = N(u)N(v).
\]

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

\[
x := \sum \alpha_{i} e_{u}, \quad y := \sum v_{j} e_{l} \quad (\alpha_{i} \in \mathbb{R}, \ v_{j} \in \mathbb{O}, \ 1 \leq i \leq 3).
\]

Then \( \text{[5.8]2} \) and \( \text{[5.9]4} \) imply
which in general will be distinct from \( N(x)N(y) \).

(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 \( x \cdot x^{-1} = 1 \). Now (b) implies \( N(x)(x^{-1}) = 1 \) and, in particular, \( N(x) \neq 0 \). Conversely, let this be so. Combining \ref{5.9.9} with \ref{5.9.10}, we obtain \( x^2 \in \mathbb{R}[x] \) and \( x \cdot x^2 = N(x)1 \). But this implies \( x \cdot y = 1 \), where \( y := N(x)^{-1}x \in \mathbb{R}[x] \), so \( x \) is invertible in \( J \), and the inverse has the desired form.

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

\[
x = (x^{-1})^{-1} = (N(x)^{-1}x^2)^{-1} = N(x)x^2 = N(x)^{-1}x^2,
\]

and also the adjoint identity follows.

First let \( \phi \) be an automorphism of \( J \). Then \( \phi \) fixes \( 1 \) and in order to prove \( N(\phi(x)) = N(x) \) for \( x \in J \), we may assume, by Zariski density, that \( 1, x, x^2 \neq 0 \) in \( J(J) \). Since \( \phi \) preserves powers, \ref{5.9.9} implies

\[
T(\phi(x)) - S(\phi(x)) + N(\phi(x))1 = \phi(x)^3 = \phi(x^3)
\]

\[
= T(\phi(x))\phi(x)^2 - S(\phi(x))\phi(x) + N(\phi(x))1,
\]

and since \( 1, \phi(x), \phi(x)^2 \) are linearly independent, we conclude \( N(\phi(x)) = N(x) \), as claimed.

Conversely, suppose \( \phi \) preserves \( 1 \) and \( N \). Then \( \phi \) also preserves the directional derivative of \( N \) at \( x \) in the direction \( y \), i.e., in view \ref{5.9.9} we have

\[
T(\phi(x)\phi(y) = DN(\phi(x))(\phi(y)) = DN(x)(y) = T(x^2 \cdot y).
\]

Setting \( x = 1 \) implies \( T \circ \phi = T \), while setting \( y = 1 \) implies \( S \circ \phi = S \). Returning with this to \ref{5.9.10}, we conclude that \( \phi \) preserves cubes: \( \phi(x^3) = \phi(x)^3 \). Linearizing this gives \( 2\phi(x \cdot (x \cdot y)) + \phi(2x \cdot y) - 2\phi(x) \cdot (\phi(x) \cdot \phi(y)) + \phi(x)^2 \cdot \phi(y) \), and setting \( y = 1 \) shows that \( \phi \) preserves squares: \( \phi(x^2) = \phi(x)^2 \). Linearizing this yet again, we see that \( \phi \) preserves the product of \( J \), and the proof of the first part is complete.

As to the second part, the linear map \( \phi \) is clearly bijective and preserves the unit. Assume that \( \phi \) is an automorphism of \( J \). Then \ref{5.9.3} yields

\[
e_{22} + e_{33} = \phi((1_0[23]^2) = \phi(1_0[23]^2) = u^{-1}[23]^2 = n_0(u)^{-1}(e_{22} + e_{33}),
\]

and we conclude \( n_0(u) = 1 \). Conversely, let this be so. By the first part of the problem, it suffices to show that \( \phi \) preserves the norm. To this end, we compute

\[
N(\phi(x)) = N(\sum \alpha_i e_i + (u^{-1}u_i)[23] + (u_2 u^{-1})[31] + (u_1 u_2 u^{-1})[12])
\]

\[
= \alpha_1 e_{23} - \alpha_3 e_{31} - \alpha_2 e_{12} + (u^{-1}u_i) - \alpha_1 n_0(u_i u_1) - \alpha_3 n_0(u_2 u_1) + t_0((u^{-1}u_1)(u_2 u_1) - (u_2 u_1)(u_3 u_1)).
\]

But \( u \) has norm 1, \( n_0 \) permits composition, and the Moufang identities (Exc. \ref{4}) combined with Exc. \ref{3}(b) give
Thus \( \psi \) is a homomorphism.

Now define the left multiplication of \( \mathbb{O} \) as the linear map \( L : \mathbb{O}^+ \to \text{End}_\mathbb{R}(\mathbb{O})^+ \) sending \( x \in \mathbb{O}^+ \) to \( L_x : y \mapsto xy \). Since \( L_x : L_y = L_0 \) for all \( x, y \in \mathbb{O} \) by \( 1.6 \), \( L \) preserves squares and hence is a homomorphism of commutative algebras. It is also injective since \( L_x = 0 \) implies \( x = L_0 = 0 \). Thus \( L \) maps \( \mathbb{O}^+ \) isomorphically onto a subalgebra of \( \text{End}_\mathbb{R}(\mathbb{O}) \), and we conclude from \( 5.7(a) \) that \( \mathbb{O}^+ \) is a special Jordan algebra. As in Exc. 24(a), the verification of the formula for the \( \mathbb{U} \)-operator is straightforward: for \( x, y \in \mathbb{O} \) we obtain, using alternativity \( 1.6 \)

\[
U_x y = 2x \bullet (xy) - x^2 \bullet y = \frac{1}{2} ((xy) + (xy)x + x(xy)x - x^2 y - xy^2)
\]

as claimed. Finally, the Jordan algebra \( \mathbb{O}^+ \) is not euclidean since, given a Cartan-Shouten basis \( (u_i)_{0 \leq i \leq 7} \) of \( \mathbb{O} \), we have \( L_0 + u_i^2 = 0 \) for \( i = 1, \ldots, 7 \).
and Exc. [6] 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.

Exc. [25] (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. [25] (c)), and the relations \( 1_3 - c \in \mathbb{R} \), \( c(1_3 - c) = 0 \) yield \( c = 1_3 \), a contradiction. Thus \( N(c) = 0 \). Using this and (5.9.10), we deduce \( c = c^3 = (T(c) - S(c))c \), hence

\[
S(c) = T(c) - 1.
\]

Now (5.9.8) yields \( c^2 = (1 - T(c))c + S(c)1_3 = S(c)(1_3 - c) \), hence \( S(c)^2 = S(c)(3 - T(c)) = -S(c)^2 + 2S(c) \). Thus \( S(c)^2 = S(c) \), forcing \( S(c) \in \{0,1\} \), and (70) implies the assertion.

### Chapter 2

### Section 8

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 \( A = M_+ \cup M_- \), 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 \( B \).
For any subset $X \subseteq A$ and any homomorphism $\varphi : A \to B$ of $k$-algebras, one makes the following observations by straightforward induction:

(a) $\varphi(\text{Mon}_A(X)) = \text{Mon}_B(\varphi(X))$ for all integers $m > 0$.
(b) $\text{Mon}_A(Y) \subseteq \text{Mon}_B(\varphi(Y))$ for all $Y \subseteq \text{Mon}_A(X)$ and all integers $n, m > 0$.

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 $\varphi : A \to A'$ for the canonical epimorphism, any $x \in A$ makes $\varphi(x) \in A'$ nilpotent, so by (a), $\text{Mon}_A(\{x\})$ meets $I$ for some integer $n > 0$. But since $I$ is nil, we conclude that some $y \in \text{Mon}_A(\{x\})$ is nilpotent, leading to a positive integer $m$ such that $0 \in \text{Mon}_A(\{x\})$ by (b). Thus $x$ is nilpotent, forcing $A$ to be a nil algebra. Now write $\pi := \text{Nil}(A)$ for the sum of all nil ideals in $A$. Given $x \in n$, there are finitely many nil ideals $n_1, \ldots, n_k \subseteq A$ such that $x \in n_1 + \cdots + n_k$. 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 $(n_1 + n_2)/n_1 \cong n_2/(n_1 \cap n_2)$ combines with what we have proved earlier to yield the assertion.

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

(b) Let $x \in A$ be a pre-image of $c'$ under $\varphi$. Then $x^d - x$ is nilpotent, so some integer $n > 0$ has $0 = (x^d - x)^n = x^{dn} - \cdots - (-1)^{n-1}x^d$. Now (a) yields an idempotent $c \in k_d[x]$ satisfying $cx^d = x^d$. Writing $\tilde{a} := \varphi(a)$ for $a \in A$, we conclude $\tilde{a}c' - \tilde{a}cx^d = c\tilde{x} - \tilde{x} = c'$. On the other hand, $c = \sum_{i \geq 0} c_i x^i$ for some scalars $c_i \in k$, $i \geq 0$, so with $\alpha := \sum_{i \geq 0} c_i x^i$ we obtain $\tilde{e} = \tilde{ac} = \tilde{a}\tilde{c} = \tilde{cc} = c'$. Section 9

If $I_j$ are ideals in $A_j$ for $1 \leq j \leq n$, then $I := I_1 \oplus \cdots \oplus I_n$ is an ideal in $A$ since $A_1 + I_1 = \sum_j (A_1 I_j + I_1 A_j) \subseteq \sum_j I_1 = I$. Conversely, let $I$ be an ideal in $A$ and $e_j$ the identity element of $A_j$ for $1 \leq j \leq n$. Then $I_j = e_1 I = e_1 j$ is clearly an ideal in $A_j$ such that $I = \sum_j I_j$.

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

To complete the solution, let us assume that the $A_j$, $1 \leq j \leq n$, are simple $k$-algebras. By the first part of the exercise, the ideals of $A$ have the form {$(\bigoplus_{j \in N} A_j)$, where $N$ varies over the $2^n$ subsets of {1, ..., $n$}. Hence the $A_j$, $1 \leq j \leq n$, are precisely the minimal ideals of $A$. This description being independent of the decomposition chosen, the assertion follows.

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

$$v := x - \sum_{i=1}^r c_i 1_A c_i \in R. \quad (71)$$

Then the first relation of (2) trivially holds and

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

For $1 \leq i \leq r$,

$$(t - c_i)^n \mu_i f_i = (t - a_i)^n \mu_i (t - a_i)^{\nu - n} f_i = \mu_i (t - a_i)^{\nu - n} f_i$$

For $1 \leq i \leq r$,
is a multiple of $\mu$, and hence kills $x$. This shows $v^0 = 0$, and the proof of (2) is complete.

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

$$\text{Nil}(R) = \{u \in R \mid u \text{ is nilpotent}\}.$$  \hfill (72) \text{NILCAS}

Hence (2) implies, for all $m \in \mathbb{C}$,

$$x^m = \sum_{i=1}^{m} c_i^m \cdot v_i, \quad v_m \in \text{Nil}(R)$$

and then

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

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

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

But $c = c^2$, so $\sum (\beta_i^2 - \beta_i)c_i = v_f - v_f$ 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 $w := v_f \in \text{Nil}(R)$,

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

and we conclude

$$(1_A - 2c_I)w = w^2, \quad (1_A - 2c_I)^2 = 1_A.$$  \hfill (73) \text{CECI}

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 (73) that $(1 - 2c_I)w^m = w^m = 0$, 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 $v := ((t - \alpha_i)\mu_i)(x) \in R$. Then

$$v^h = ((t - \alpha_i)^h\mu_i)(x) = (\mu_i\mu_i^{n-1})(x) = 0,$$

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

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

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

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

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

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

(e) Let $\beta_i \in F^*$ satisfy $\beta_i^2 = \alpha_i$ for $1 \leq i \leq r$. Setting $z := \sum_{i=1}^r \beta_i e_i$, we obtain $z^2 = x = 1_A + w$, for some $w \in \text{Nil}(R)$. 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

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

The minimum polynomial of $w$ is $t^m$, 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

$$\gamma_0^2 = 2y_0 \gamma_1 = 1, \quad \sum_{l=0}^j \gamma_l \gamma_{j-l} = 0 \quad (2 \leq j < m).$$

This system of quadratic equations can be solved recursively by

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

This proves the assertion.

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

$$y = \sum_{i=0}^{m-1} \left( \frac{1}{2} \right) w^i,$$

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

We write $\mathcal{D}$ (resp. $\mathcal{E}$) 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 $(e_j)_{1 \leq j \leq n} \in \mathcal{E}$. For $1 \leq j, l \leq n$, centrality implies $(A e_j) (A e_l) = A^2 (e_j e_l)$, which is zero for $j \neq l$ and $A e_j$ for $j = l$. Moreover, $x = \sum x e_j \in \sum A e_j$ 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 $e_j$, $1 \leq l \leq n$, and deduce $x_j e_l = 0$. All this boils down to $A = \langle A e_j \rangle \oplus \cdots \oplus \langle A e_n \rangle$ as a direct sum of ideals. Thus the assignment $(e_j) \mapsto (A e_j)$ gives a map from $\mathcal{E}$ to $\mathcal{D}$.

Conversely, let $(I_j)_{1 \leq j \leq n} \in \mathcal{D}$. Then each $I_j$, $1 \leq j \leq n$, is a unital $k$-algebra in its own right, and setting $e_j := 1_{I_j}$, we deduce $x e_j = \sum e_j = 1_A$, $e_j e_l = \delta_{j,l}$ 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 $\text{Cent}(A) = \text{Cent}(I_j) \oplus \cdots \oplus \text{Cent}(I_n)$ as a direct sum of ideals. Thus the assignment $(I_j)_{1 \leq j \leq n} \mapsto (e_j)_{1 \leq j \leq n}$ determines a map from $\mathcal{D}$ to $\mathcal{E}$, and it is readily checked that the two maps constructed are inverse to each other.

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

$$[a e_{ij}, b e_{jm}, c e_{pq}] = \delta_{ij} \delta_{np} [a, b, c] e_{pq},$$  \hspace{1cm} (74)

$$[a e_{ij}, b e_{im}] = \delta_{ij} (ab) e_{im} - \delta_{im} (ba) e_{ij}.$$  \hspace{1cm} (75)

The inclusion $\text{Mat}_n(\text{Nuc}(A)) \subseteq \text{Nuc}(\text{Mat}_n(A))$ follows immediately from (74). Conversely, let $x = (a_{ij}) = \sum a_{ij} e_{ij} \in \text{Nuc}(\text{Mat}_n(A))$. Then (74) for $m = p$ implies $0 = [x, b e_{in}, c e_{pq}] = \sum [a_{ij}, b, c] e_{pq}$, hence $[a_{ij}, A, A] = \{0\}$. Similarly, $0 = [b e_{in}, c e_{pq}, x] = \sum [b, c, a_{ij}] e_{ij}$, forcing $[A, A, a_{ij}] = \{0\}$. And, finally, $0 = [b e_{in}, x, c e_{pq}] = [b, a_{ij}, c] e_{pq}$ implies $[b, a_{ij}, c] = 0$. Summing up, we conclude $a_{ij} \in \text{Nuc}(A)$ for $1 \leq i, j \leq n$, solving the first part of the problem.
Concerning the second one, let \( x = (a_{ij}) = \sum a_i e_{ij} \in \text{Cent}(\text{Mat}_n(A)) \). By the first part, \( a_{ij} \in \text{Nuc}(A) \) for \( 1 \leq i, j \leq n \). Moreover, \([75]\) for \( l = m \) yields \( 0 = [x, e_{ij}] = \sum a_{il} e_{lj} - \sum a_{lj} e_{il} \), hence \( a_{ij} = 0 \) for \( 1 \leq i, j \leq n, i \neq j \). Now let \( l \neq m \) in \([75]\). Then \([x, b e_{lm}] = (a_{ij} b) e_{lm} - (b a_{lm}) e_{lm} \), forcing \( a_{ij} = a_{lm} \in \text{Cent}(A) \), and we conclude \( x \in \text{Cent}(A) 1_n \). Conversely, it is clear that every element of \( \text{Cent}(A) 1_n \) belongs to \( \text{Cent}(\text{Mat}_n(A)) \).

Let \( t: A \rightarrow k \) be an associative linear form and suppose the corresponding bilinear form \( \sigma := \sigma_t \) (cf. \([89]\)) is non-singular (cf. \([12.9]\)). 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 \( t((xe)y) = t((yx)e) = t(e(yx)) = t(xy) = t(x(y)) \) for all \( x, y \in A \) combined with non-degeneracy of \( \sigma \) imply \( ex = x = xe \) for all \( x \in A \). Hence \( A \) is unital with \( 1_A = e \).

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 \( \text{det}(L_{x+y}) \in F[t] \) has degree \( n \), hence a root \( \alpha \in F \). But then left multiplication by the non-zero element \( x + \alpha y \in D \) has a non-trivial kernel, contradicting the property of \( D \) being a division algebra. Thus \( n = 1 \), and we conclude \( D = F e \) 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 \( F \rightarrow D, \xi \mapsto \alpha^{-1} \xi e \) is an isomorphism of \( F \)-algebras.

**Section 10**

Let \( m, n \in \mathbb{Z} \) such that \( u := mx + ny \in \text{Nuc}(A) \). Then \( 0 = [u, x, x] = m(x^2 x - xx^2) + n((yx)x - yx^2) = 2m(x - x) - 2ny = -2ny \), hence \( n = 0 \), and \( 0 = [u, x, y] = m(x^2 y - x(yx)) = 2ny \), hence \( m = 0 \). Thus \( \text{Cent}(A) = \text{Nuc}(A) = \mathbb{Z} 1_A \); in particular, \( A \) is central. On the other hand, passing to the base change \( A_R = \mathbb{Z}/2\mathbb{Z} \) and setting \( u := u_R \) for \( u \in A \), we conclude that \( 1_A, \bar{x}, \bar{y} \) 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 \( \text{Cent}(A_R) = \text{Nuc}(A_R) = A_R \) is a free \( R \)-module of rank 3, \( \text{Cent}(A_R)_k = (\text{Nuc}(A_R))_k = R 1_A \) is a free \( R \)-module of rank 1.

We proceed in several steps.

1°. Let can: \( k \rightarrow \kappa(p) \), \( \alpha \mapsto \alpha(p) \), be the natural map. Then the diagram

\[
\begin{array}{ccc}
k & \xrightarrow{\text{can}} & \kappa(p) \\
\downarrow & \ & \downarrow \psi \circ \iota_{\kappa(p)} \\
k' & \xrightarrow{\psi \circ \iota_{\kappa(p)}} & \kappa(p)
\end{array}
\]

commutes since

\[
(\psi \circ \iota_{\kappa(p)}) \circ \text{can}(\alpha) = (\psi \circ \iota_{\kappa(p)})(1 \circ \alpha(p)) = 1_{k'} \circ \alpha(p) = 1_{k'} \circ (\alpha \cdot 1_{\kappa(p)}) = (\alpha \cdot 1_{k'}) \circ 1_{\kappa(p)} = \psi(\alpha) \circ 1_{\kappa(p)} = \psi(\alpha)
\]

for all \( \alpha \in k \). Applying the contra-variant functor \( \text{Spec} \) to this diagram, we conclude that also

\[
\begin{array}{ccc}
\text{Spec}(k') & \xrightarrow{\text{Spec}(\psi)} & \text{Spec}(\kappa(p)) \\
\text{Spec}(\psi \circ \iota_{\kappa(p)}) & \xrightarrow{\text{Spec}(\psi \circ \iota_{\kappa(p)})} & \text{Spec}(\psi) \\
\text{Spec}(\psi) & \xrightarrow{\text{Spec}(\psi \circ \iota_{\kappa(p)})} & \text{Spec}(\kappa(p))
\end{array}
\]

commutes. But \( \text{Spec}(\kappa(p)) \) consists of a single point sent by \( \text{Spec}(\text{can}) \) to \( \text{can}^{-1}((0)) = \text{Ker}(\text{can}) = p \). Hence the image of \( \text{Spec}(\psi) \) belongs to the fiber \( \text{Spec}(\psi)^{-1}(p) \). Thus \( \text{Spec}(\psi) \) induces canoni-
cally a continuous map 
\[ \Psi : \text{Spec}(k' \otimes \kappa(p)) \to \text{Spec}(\varphi)^{-1}(p). \]

2. Let \( p' \in \text{Spec}(\varphi)^{-1}(p) \). Then \( \varphi^{-1}(p') = p \), and consulting 10.4.6, we find a unique homomorphism 
\[ \sigma_{p'} : k' \otimes \kappa(p) \to \kappa(p') \]

of \( \kappa(p) \)-algebras making a commutative diagram

\[ \begin{array}{ccc}
  k & \xrightarrow{\varphi} & k' \\
  \downarrow \text{can}_p & & \downarrow \text{can}_{p'} \\
  k_p & \xrightarrow{\psi'} & k'_p \\
  \downarrow \text{can}_{p}(p) & & \downarrow \text{can}_{p'}(p') \\
  \kappa(p) & \xrightarrow{\phi} & \kappa(p').
\end{array} \]

Thus \( \ker(\sigma_{p'}) \in \text{Spec}(k' \otimes \kappa(p)) \), and we obtain a map
\[ \Phi : \text{Spec}(\varphi)^{-1}(p) \to \text{Spec}(k' \otimes \kappa(p)) \]
given by
\[ \Phi(p') := \ker(\sigma_{p'}) \quad (p' \in \text{Spec}(\varphi)^{-1}(p)). \]

The definitions and 76 imply
\[ \Psi \circ \Phi(p') = \psi^{-1}(\sigma_{p'}^{-1}(\{0\})) = (\sigma_{p'} \circ \psi)^{-1}(\{0\}) = \{ \alpha' \in k' | \alpha'(p') = 0 \} = p' \]

for all \( p' \in \text{Spec}(\varphi)^{-1}(p) \), hence \( \Psi \circ \Phi = I_{\text{Spec}(\varphi)^{-1}(p)} \).

3. Let \( q \in \text{Spec}(k' \otimes \kappa(p)). \) Then
\[ \Phi \circ \Psi(q) = \Phi(p') = \ker(\sigma_{p'}), \quad p' := \psi^{-1}(q) \in \text{Spec}(\varphi)^{-1}(p). \]

By 10.4.6 again, we obtain a diagram

where the four squares commute. But so does the diagram
\[ \begin{array}{cc}
\psi \circ \sigma' & \psi = \text{can}_q(q) \circ \text{can}_q \\
\text{can}_p(p') & \in \text{can}_p(p') \\
\kappa(p') & \in \kappa(p)
\end{array} \]

which by (66) is clear for the upper triangle but holds true also for the lower one because \( \psi \circ \sigma' \circ \psi = \text{can}_q(q) \circ \text{can}_p(q) = \text{can}_q(q) \circ \text{can}_q \). We therefore conclude

\[ \Phi \circ \Psi(q) = \ker(\psi \circ \sigma') = \ker(\text{can}_q(q) \circ \text{can}_q) = q. \]

Summing up we have shown that \( \Psi \) is bijective with inverse \( \Phi \).

By (10) and (34), it remains to show that \( \Phi \) is continuous, equivalently, that \( \Psi \) is open. In order to see this, we first deduce from (10.3) and (10.2) the natural identifications

\[ k' \otimes \kappa(p) = (k' \otimes k_p) \otimes k_p = -k_p \otimes (k_p / p_p) = k_p / p_p k_p' \]

such that, with the natural maps \( i: k' \to k_p', \pi: k_p' \to k_p / p_p k_p' \), the triangle

\[ \begin{array}{ccc}
k' & \xrightarrow{i} & k_p' \\
\downarrow & & \downarrow \\
\pi & \xrightarrow{} & k_p / p_p k_p'
\end{array} \]

commutes. The proof will be complete once we have shown

\[ \Psi\left(D(\pi(f/s))\right) = D(f) \cap \text{Spec}(\varphi)^{-1}(p) \quad (77) \]

for all \( f \in k', s \in k \setminus p \). Let \( q \in \text{Spec}(k' \otimes \kappa(p)) = \text{Spec}(k_p' \otimes p_p k_p') \). Then the chain of equivalent conditions

\[ q \in D(\pi(f/s)) \iff \pi(f/s) \notin q \iff f/s \notin \pi^{-1}(q) \iff \psi^{-1}(q) \in D(f) \quad (78) \]

shows that the left-hand side of (77) is contained in the right. Conversely, let \( p' \in D(f) \cap \text{Spec}(\varphi)^{-1}(p) \). Then \( q := \psi^{-1}(p') \in \text{Spec}(k' \otimes \kappa(p)) \) and \( \psi^{-1}(q) = p' \in D(f) \). Consulting (78), we conclude \( q \in D(\pi(f/s)) \), hence \( p' = \Psi(q) \in \Psi(D(\pi(f/s))) \), and the proof of (77) is complete.

(a) We may assume \( \chi = 0 \). Let \( u_1, \ldots, u_m \) be a finite set of generators for the \( k \)-module \( M \). For \( p \in U \) and \( 1 \leq i \leq m \), we have \( \psi(u_i)/1 = \psi(u_i) = \psi(u_i) = 0 \) in \( N_p \). Hence there are \( f \in k \setminus p \), \( n \in \mathbb{N} \) such that \( f^n \psi(u_i) = 0 \) in \( N_f \) for all \( i = 1, \ldots, m \). But this means \( p \in D(f) \) and \( \psi(u_i)/1 = 0 \) in \( N_f \) for all \( i = 1, \ldots, m \), which in turn, by (10.5) amounts to \( \psi_q = 0 \) for all \( q \in D(f) \). Hence we have shown \( p \in D(f) \subseteq U \), and \( U \) is Zariski-open in \( X \).

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

\[ U_i := \{ p \in X \mid \psi_p = \chi_p \} \]

is Zariski-open in \( X \). Hence so is \( V = \cap_{i=1}^m U_i \).

In the solution to this problem, free use will be made of the formalism for the Zariski topology as explained, for example, in [11] II, § 4.3.
(a) For \( p \in X \), the chain of equivalent conditions
\[
p \in D(\epsilon) \iff \epsilon \notin p \iff \epsilon_p \notin p_p \iff \epsilon_p \in k_p \iff 1_p \iff (1-\epsilon)_p = 0
\]
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 \( p \in X \) that \( (\epsilon_p)_{i \in I} \) is an orthogonal system of idempotents in \( k_p \), whence \( \bigcup D(\epsilon_p) \neq 0 \) if and only if \( \epsilon_p \neq 0 \) for some \( i = 1, \hdots, r \). This proves \( \bigcup D(\epsilon_p) = D(\sum \epsilon_p) \), and the union on the left is disjoint since \( D(\epsilon) \cap D(\eta) = D(\epsilon \eta) = D(0) = \emptyset \) for \( i, j \in I, i \neq j \).

(b) Given a complete system \((\epsilon_i)_{i \in I}\) of orthogonal idempotents in \( k \), the subsets \( U_i := D(\epsilon_i) \subseteq X \), \( i \in I \), are open in \( X \) and by \((a)\) satisfy \( \bigcup U_i = D(\sum \epsilon_i) = D(1) = X \), where the union on the very left is disjoint and the \( U_i \) are empty for almost all \( i \in I \). Thus the assignment \((\epsilon_i) \mapsto (U_i)\) gives a map of the right kind, which is injective since the \( U_i \) by \((a)\) determine the \( \epsilon_i \) 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 \( \epsilon_i \in H^0(U_i, \mathcal{O}) = k \) 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 \( j \neq i \). It is then readily checked that the \( \epsilon_i \) form a complete orthogonal system of idempotents in \( k \), forcing the \( D(\epsilon_i) \) to be an open disjoint cover of \( X \). On the other hand, given \( p \in U_i \), we obtain \( \epsilon_p = 1_p \), which implies \( U_i \subseteq D(\epsilon_i) \) by \((a)\). Summing up, we have equality and surjectivity is proved.

Adopting a more direct approach based on the proof of [11, 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 \( U_i = V(a_i) \), \( Y_i = V(b_i) \) for some ideals \( a_i, b_i \subseteq k \). Since \( V(a_i + b_i) = V(a_i) \cap V(b_i) = U_i \cap Y_i = \emptyset \), we conclude \( a_i + b_i = k \), hence \( a_i = \beta_i \) for some \( \alpha_i \in \mathbb{A}_i, \beta_i \in b_i \). This implies \( \alpha_i = \alpha_i (\alpha_i + \beta_i) = \alpha_i^2 + \alpha_i \beta_i \equiv \alpha_i \mod b_i \), so \( \alpha_i \in a_i \) becomes an idempotent modulo \( b_i \). On the other hand, \( X = U_i \cup Y_i = V(a_i) \cup V(b_i) = V(a_i b_i) \), so \( a_i b_i \subseteq k \) is a nil ideal. Now [Exc.31] yields an idempotent \( \epsilon'_i \in a_i \) such that \( \epsilon'_i \equiv \alpha_i \mod a_i b_i \). Thus \( \epsilon_i := 1 - \epsilon'_i \in k \) is an idempotent as well satisfying \( \epsilon_i \equiv \beta_i \mod a_i b_i \), hence \( \epsilon_i \in b_i \). We conclude \( U_i = V(a_i) \subseteq V(\epsilon'_i) = D(\epsilon_i) \), \( Y_i = V(b_i) \subseteq V(\epsilon_i) = D(\epsilon'_i) \subseteq D(\epsilon_i) \cap \bigcup D(\epsilon'_i) = \emptyset \) by \((a)\). Therefore \( U_i = D(\epsilon_i) \), and it remains to show that \((\epsilon_i)_{i \in I}\) is a complete orthogonal system of idempotents. For \( i, j \in I, i \neq j \), we deduce \( D(\epsilon_i \epsilon_j) = D(\epsilon_i) \cap D(\epsilon_j) = U_i \cap U_j = \emptyset \), so the idempotent \( \epsilon_i \epsilon_j \) is also nilpotent, hence zero. Thus the \( \epsilon_i \) are orthogonal. For the same reason, \( \epsilon_i = 0 \) for almost all \( i \in I \) and (a) gives
\[
X = \bigcup U_i = \bigcup D(\epsilon_i) = \bigcup V(1-\epsilon_i) = V(\prod (1-\epsilon_i)) = V(1-\sum \epsilon_i),
\]
forcing the idempotent \( 1 - \sum \epsilon_i \) to be nilpotent, hence zero.

[42] Setting \( X := \text{Spec}(k) \), the subsets
\[
U_i := \{ p \in \text{Spec}(k) \mid \text{rk}_p(M) = i \} \subseteq X \quad (i \in \mathbb{N})
\]
form an open disjoint cover of \( X \) since \( X \) is quasi-compact [11, II, §4, Proposition 12], \( U_i \) is empty for almost all \( i \in \mathbb{N} \). This proves (a) while, in order to prove (b), we apply Exercise 41 to obtain a complete orthogonal system \((\epsilon_i)_{i \in \mathbb{N}}\) of idempotents in \( k \) such that \( U_i = D(\epsilon_i) \) for all \( i \in \mathbb{N} \). Given \( j \in \mathbb{N} \), let \( \pi_j : k \rightarrow k_j \) be the canonical projection induced by (1) and let \( p_j \in \text{Spec}(k_j) \). Then
\[
p := \text{Spec}(\pi_j)(p_j) = \pi_j^{-1}(p_j) = p_j \oplus \bigoplus_{i \neq j} k_i \in X,
\]
and [10.47] shows
\[
M_{p_j} = M_p \otimes_{k_v} k_{p_j}.
\]
Since $M_{ij}$ is free of rank $j$ over $k_{ij}$, it follows that $M_{[ij]}$ is free of rank $j$ over $k_{[ij]}$. This proves existence. In order to establish uniqueness, let $(\eta_l)_{l \in \mathbb{N}}$ be any complete orthogonal system of idempotents in $k$, giving rise, in analogy to (1), (2), to the decompositions

$$k = \bigoplus_{i \in \mathbb{N}} l_i, \quad l_i = k\eta_i \quad (i \in \mathbb{N}),$$

$$M = \bigoplus_{i \in \mathbb{N}} N_i, \quad N_i = N \otimes l_i \quad (i \in \mathbb{N}),$$

and making each $N_i$ a projective $l_i$-module of rank $i$. Again by Exercise 44, 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 $i \in I$. Fixing $j \in \mathbb{N}$ and $q \in V_j$, we apply 7 Exercise 32 and find a decomposition $q = \bigoplus_{i \in \mathbb{N}} q_i$, where $q_i = q \cap l_i$ is an ideal in $l_i$. But $q_i \neq q$ while $q_i q_j = 0 \in q$ for all $i \neq j$, forcing $q_i \in q \cap l_i = q$, and then $q_i = l_i$. Summing up we have shown

$$q = q_i \oplus \bigoplus_{i \neq j} l_i,$$

so $q_i$ is a prime ideal in $l_i$ and $\text{Spec}(\rho_j)(q_i) = q_i$, where $\rho_j : k \to l_j$ is the canonical projection induced by (80). Since

$$N_{l_j} = M_q \otimes_{k_q} l_{q_j}$$

has rank $j$ over $l_{q_j}$, the free $k_q$-module $M_q$ must have rank $j$ over $k_q$. This proves $q \in U_j$ by 79, and the solution is complete.

If $\phi : A \to A'$ is a unital algebra homomorphism, then so is $\phi(p) : A(p) \to A'(p)$, for each $p \in \text{Spec}(k)$. But since $A(p)$ is simple by hypothesis, $\phi(p)$ is injective and a dimension argument shows that it is, in fact, an isomorphism. Hence, by Nakayama’s lemma [65, §4], $\phi_p : A_p \to A'_p$ is an isomorphism, whence $\phi$ is one [11, II, Thm. 1].

---

**Section 11**

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

(b) By Prop. 10.15, the right multiplication of $A$ induces an isomorphism $R : \text{Cent}(A) \to \text{End}_{\text{Mult}(A)}(A)$. Hence it suffices to show that the elements of $\text{Cent}(A, G)$ correspond to the $\text{Mult}(A, G)$-linear maps $A \to A$ under this isomorphism, which follows from the relations $R_{g(a)}g = gR(a)$ for all $a \in \text{Cent}(A), g \in G$.

(c) If $(A, G)$ is a simple $k$-algebra with a group of automorphisms, 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, the first part follows from the Jacobson-Chevalley density theorem [65, Chap. XVII, §3, Cor. 3 of Thm. 1] and immediately implies necessity in the second part. Conversely, suppose $A \neq \{0\}$ and $M(A, G) = \text{End}_{k}(A)$. Then $A$ is an irreducible $M(A, G)$-module, forcing $(A, G)$ to be simple and $\text{Cent}(A, G)$ to be a field. Also, by (b), $\text{End}(A) = M(A, G) = \text{End}_{\text{Cent}(A, G)}(A)$ and a dimension count yields sufficiency as well.
The implications (iii) \(\Rightarrow\) (ii). Let \(k'\) be any extension field of \(k\) and put \((A', G') = (A, G) \otimes k'\) as a \(k'\)-algebra with a group of automorphisms. A moment’s reflection shows \(M(A', G') = M(A, G) \otimes k'\). Now the assertion follows from the second part of Exc. 44 (d).

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

(iv) \(\Rightarrow\) (i). This follows immediately from Exc. 44 (a), (c).

46. We follow standard arguments, reproduced in [15] 1 Satz 5.5, for example. First note that \(k\) is a field, by Exc. 44 (c) and central simplicity of \((A, G)\). Now 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

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

(82)

Then the elements \(x'_1, \ldots, x'_n\) are linearly independent over \(k\). Furthermore, a straightforward verification shows that the totality of elements \(u_i \in A\) such that

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

for some \(u_1, \ldots, u_n \in A\) forms an ideal \(I\) of \((A, G)\) which is non-zero since \(x_1 \in I\) and \(x_1 \neq 0\) by the minimality of \(n\). The simplicity of \((A, G)\) therefore implies \(I = A\), so in (82) 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 the 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, \([u, x_i, v] = [u, v, x_i] = [x, u] = 0\), forcing \(x_i \in \text{Cent}(A)\) for \(2 \leq i \leq n\). Applying \(g \otimes 1\) for any \(g \in G\) to (82) and again observing \(x_1 = 1\), we conclude

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

and the minimality of \(n\) implies \(\sum_{i=2}^{n} (x_i - g(x_i)) \otimes x'_i = 0\), hence \(x_i \in \text{Cent}(A, G)\) for \(2 \leq i \leq n\). But \((A, G)\) was assumed to be central simple, so \(\text{Cent}(A, G) = k1_A\), 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 \(x' \neq 0\). The simplicity of \((A', G')\) therefore implies \(I' = A'\), hence \(1_A \otimes x' \in J\) and \(J = A\), as claimed.

Section 12

The implications (iii) \(\Rightarrow\) (i) 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 \(h\), and writing \(e_0 = v_+^* \oplus v_+\), \(v_0 = L\), \(v_+^* \in L^*\), we apply (12.17.1) and obtain \((v_0^*, v_+^*, v_+, v_-) = h_2(e_+ + e_-) = 1\). Therefore \(v_+ + v_- \in L\) is a unimodular vector, hence a basis of \(L\) over \(k\), and (iii) follows.

The implications (ii) \(\Rightarrow\) (i) being obvious, let us assume that \((u_1, u_2)\) is a hyperbolic pair in \(h\). Writing \(u_j = \alpha_1 e_1 + \alpha_2 e_2\) (\(\alpha_j \in k\), \(i, j = 1, 2\)), we conclude

\[
\alpha_1 \alpha_2 = 0, \quad \alpha_1^2 + \alpha_2^2 = 1 \quad (j = 1, 2).
\]  

(83)
Thus \((\varepsilon_+, \varepsilon_-)\) is a complete orthogonal system of idempotents in \(k\), giving rise to a decomposition of \(k\) as in (ii) such that (2) holds. Moreover, setting \(\gamma_i := \alpha_1 \varepsilon_+ \in k^+\) with inverse \(\gamma_i^{-1} = \alpha_2 \varepsilon_+ \in k^+\) with inverse \(\gamma_i^{-1} = \alpha_2 \varepsilon_- \in k^-\), we apply (83) and obtain

\[
\begin{align*}
\gamma_1 = \varepsilon_+ & = \varepsilon_+ \\
\gamma_2 = \varepsilon_+ & = \varepsilon_+ \\
\gamma_3 = \varepsilon_+ & = \varepsilon_+
\end{align*}
\]

hence (3), (4).

We argue by induction on \(n\). The case \(n = 1\) has been settled in Cor. 12.5. Now suppose \(n > 1\) and assume that the assertion holds for \(n - 1\). For any \(u_n \in M_n\), the map

\[
F_{u_n} : M_1 \times \cdots \times M_{n-1} \to M, \quad (u_1, \ldots, u_{n-1}, u_n) \to F(u_1, \ldots, u_{n-1}, u_n)
\]

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

\[
F_{u_n}^R : M_{1R} \times \cdots \times M_{n-1R} \to M_R.
\]

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

\[
F_x : M_n \to M_R, \quad u_n \mapsto F_x(u_n) := (F_{u_n})^R(x).
\]

is \(k\)-quadratic. In order to see this, we put

\[
V := \text{Quad}(M_1, \ldots, M_{n-1}; M)
\]

and conclude from (84) that the map \(Q : M_n \to V, u_n \mapsto F_{u_n}\) is \(k\)-quadratic. On the other hand, (85) implies \(F_x(u_n) = Q(u_n, R)(x)\), so \(F_x\) is \(Q\) composed with two \(k\)-linear maps: the natural map

\[
\text{Quad}(M_1, \ldots, M_{n-1}; M) \to \text{Quad}(M_{1R}, \ldots, M_{n-1R}; M_R), \quad G \mapsto G_R,
\]

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

By Cor. 12.5 we therefore obtain an \(R\)-quadratic map

\[
(F_x)^R : M_{1R} \to (M_R)^R := M \otimes R \otimes R,
\]

which composes with the \(R\)-linear map

\[
\mu : M \otimes R \otimes R \to M \otimes R = M_R, \quad u \otimes r \otimes s \mapsto u \otimes rs
\]

(86) to yield a map \(F_k : M_{1R} \times \cdots \times M_{n-1R} \times M_{1R} \to M_R\) via

\[
F_k(x_1, \ldots, x_{n-1}, x_n) := \mu (\{F_x(x_1, \ldots, x_{n-1})\}^R(x_n))
\]

(87) for \(x_i \in M_{1R}\), \(1 \leq i \leq n\). By construction, \(F_k\) is quadratic in \(x_n\). Hence, writing \(x_n = \sum \tau_i u_{\tau_iR} r_i \in R\), \(u_{\tau_iR} \in M_R\), we obtain, after a straightforward computation,

\[
(F_k)^R u_n = \sum \tau_i^2 (F_{u_{\tau_iR}})^R + \sum \tau_i r_i (F_{u_{\tau_iR} u_{\tau_iR}})^R - (F_{u_{\tau_iR}})^R - (F_{u_{\tau_iR}})^R r_i)
\]

(87) which shows that the left-hand side of (87) is \(R\)-quadratic in \(x_i\), \(1 \leq i < n\). Thus \(F_k\) is an \(R\)-\(n\)-quadratic map. Next we show that (3) commutes. Indeed, given \(u_i \in M_i, 1 \leq i \leq n\), we apply (87), Cor. 12.5 (86), (85), the induction hypothesis and (84) to obtain
We first assume that

\[ F_R(u_1, \ldots, u_{n-1}, u_n) = \mu \left( (F_{n-1,R}(u_{n-1}R)(u_n))_R \right) = \mu \left( (F_{n,R}(u_1, \ldots, u_{n-1}, u_n))_R \right) = F_R(u_1, \ldots, u_{n-1}, u_n), \]

and commutativity of \( F_R \) is proved.

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

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

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

\[ G_{u_n} : H_{u_n} : M_{1R} \times \cdots \times M_{n-1,R} \to M_R \]

are \( R^{-n-1} \)-quadratic maps rendering the diagram

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

commutative. From the uniqueness part of the induction hypothesis, we therefore conclude \( G_{u_n} = H_{u_n} \). Now let \( x_i \in M_R \) for \( 1 \leq i \leq n \) and write \( x_n = \sum l_i u_{l_i}R, \ l_i \in R, u_{l_i} \in M \). Then what we have just shown implies

\[
G(x_1, \ldots, x_{n-1}, x_n) = \sum l_i^2 G(x_1, \ldots, x_{n-1}, u_{l_i}R) + \sum_{l \leq m} (G(x_1, \ldots, x_{n-1}, u_{l}R + u_{m}R) - G(x_1, \ldots, x_{n-1}, u_{m}R)
\]

\[
= \sum l_i^2 G_{u_{l_i}R}(x_1, \ldots, x_{n-1}) + \sum_{l \leq m} (G_{u_{l}R + u_{m}R}(x_1, \ldots, x_{n-1}) - G_{u_{m}R}(x_1, \ldots, x_{n-1})
\]

\[
= H(x_1, \ldots, x_{n-1}, x_n)
\]

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.

We first assume that \( M \) is free and let \( (e_i)_{i \in I} \) be an ordered basis of \( M \), so \( I \) is a totally ordered set with respect to some ordering. Let \( \beta : M \times M \to k \) be the unique bilinear form on \( M \) given by the values

\[
\beta(e_i, e_j) = \begin{cases} q(e_i) & \text{for } i = j \in I, \\ q(e_i, e_j) & \text{for } i, j \in I, i < j, \\ 0 & \text{for } i, j \in I, i > j \end{cases}
\]

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

\[
\beta(x, x) = \beta(\sum \xi_i e_i, \sum \xi_j e_j) = \sum_{i,j} \xi_i \xi_j \beta(e_i, e_j) = \sum \xi_i^2 q(e_i) + \sum_{i < j} \xi_i \xi_j q(e_i, e_j) = q(x),
\]
as claimed. Now let $M$ be an arbitrary projective module. Then there exists a $k$-module $M'$ making $N := M \oplus M'$ free. Let $q' : M' \to k$ be the zero quadratic form on $M'$ and consider the quadratic form $Q := q \oplus q' : N \to k$. By the special case just treated we find a bilinear form $B : N \times N \to k$ such that $Q(y) = B(y, y)$ for all $y \in N$. But this implies $q(x) = \beta(x, x)$, where $\beta : M \times M \to k$ is the restriction of $B$ to $M \times M$.

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

(ii) $\Rightarrow$ (i). 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 $\dim_k(\text{Rad}(Dq)) \leq 1$. Since the radical of a symmetric or skew-symmetric bilinear form over a field is compatible with base change, it suffices to show $\dim_k(\text{Rad}(Dq_k)) \leq 1$. But $q_k$ is non-degenerate by hypothesis, so its restriction to $\text{Rad}(Dq_k)$ 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 $\text{Rad}(Dq) = Fu$, and if $u \neq 0$, then $q(u) \neq 0$ since $q$ is non-degenerate. Now let $L/k$ be any field extension. Then $\text{Rad}(Dq_L) = Lu$. If $x' \in V_L$ satisfies $(q_L)(x') = (q_L)(x', y') = 0$ for all $y' \in V_L$ then, in particular, $x' \in \text{Rad}(Dq_L) = Lu$, so some $a \in L$ has $x' = a(u)$. 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 separable.
\[
\sum_{v \in \mathbb{N}} T^v(\Pi^{(\nu)} f)_R(x, y) = \sum_{v,v' \in \mathbb{N}^2, v' \geq v} t_{v}^{1} \cdots t_{v'}^{\nu} 0^{v_{\nu+1}} \cdots 0^{v_{\nu+p}} (\Pi^{(\nu')}) f_R(x, y) \\
= f_{\nu R}(\sum_{i=0}^{n} t_{x_i} + \sum_{j=1}^{p} 0_{x_{\nu + j}}) = f_R(\sum_{i=1}^{n} t_{x_i}) \\
= \sum_{v \in \mathbb{N}^p} T^v(\Pi^v f)_R(x),
\]
and comparing coefficients, the assertion follows.

For \(d \in \mathbb{N}\) define \(f_d := \Pi^{(d)} f\), which by Thm. 13.7 and 13.8 (a) is a homogeneous polynomial law \(M \to N\) of degree \(d\) over \(k\). Moreover, the family \((f_d)_{d \geq 0}\) is pointed finite, and for \(n = 1\), \(r_1 = 1_k\) implies \(f = \sum_{d \geq 0} f_d\). This proves the existence. Conversely, let \((f_d)_{d \geq 0}\) be any family of polynomial laws over \(k\) with the desired properties. For \(R \in k\text{-alg}\), \(r \in R, x \in M_R\) we deduce

\[
f_R(rx) = \sum_{d \geq 0} f_{dR}(rx) = \sum_{d \geq 0} r^d f_{dR}(x),
\]
and the uniqueness property of Thm. 13.7 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 \(f_d \neq 0\) 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 \(R \in k\text{-alg}\), define a set map \(f_{dR} : M_R \to R\) by

\[
f_{dR}(\sum_{i \in \mathbb{N}} r_i e_i) := r_d,
\]
where \((r_i)_{i \in \mathbb{N}}\) is an arbitrary sequence of finite support in \(R\). The family \((f_{dR})_{R \in k\text{-alg}}\) is clearly a homogeneous polynomial law \(f_d : M \to k\) of degree \(d\) over \(k\), and the family \((f_d)_{d \geq 0}\) is pointed finite. Hence, by 13.6 \(f := \sum_{d \geq 0} f_d : M \to k\) exists as a polynomial law over \(k\) and has the desired property.

The family of set maps \(\hat{w}: M_R \to N_R\) for \(w \in \mathbb{N}\) clearly varies functorially with \(R \in k\text{-alg}\) and hence is a polynomial law \(\hat{w}: M \to N\) such that \(\hat{w}_R(rx) = \hat{w}_R(x)\) for all \(r \in R, x \in M_R\). Thus \(\hat{w}\) is homogeneous of degree 0. Conversely, let \(f : M \to N\) be any homogeneous polynomial law of degree 0 over \(k\). Then \(w := f_k(0) \in N,\) and for all \(R \in k\text{-alg}, x \in M_R\), we apply 13.2.1 to obtain \(w_R = f_k(0)_R = f_R(0) = f_R(0)x = 0^d f_R(x) = f_R(x),\) hence \(\hat{w}_R = f_R\) and then \(\hat{w} = f\).

(a) The first part is obvious. To establish the second, we begin by treating the case \(n = 1\), so let \(f : M \to N\) be a homogeneous polynomial law of degree 1. Then 13.8 (c) implies \(\Pi^0 f = 0\) for all \(v \in \mathbb{N} \setminus \{(1,0),(0,1)\}\), and 13.7 (4) yields

\[
f_k(\alpha x + \beta y) = \alpha f((\Pi^{(1)}) f)_k(x, y) + \beta f((\Pi^{(0)}) f)_k(x, y)
\]
for all \(\alpha, \beta \in k\) and all \(x, y \in M\). Specializing \(\alpha = 1, \beta = 0\) and \(\alpha = 0, \beta = 1\), we conclude \((\Pi^{(1)}) f)_k(x, y) = f_k(x), (\Pi^{(0)}) f)_k(x, y) = f_k(y).\) Hence \(f_k : M \to N\) is a \(k\)-linear map. Since \(f \otimes R : M_R \to N_R\), for \(R \in k\text{-alg}\), is a homogeneous polynomial law of degree 1 over \(R\), it follows, therefore, that \(f_k : M_R \to N_R\) is an \(R\)-linear map. Moreover, for \(r \in R, x \in M,\) we deduce \(f_k(x \otimes r) = f_k(rx_k) = r f_k(x)\) for \(r \in R, x \in M,\) hence \(f_k = (f_k)k\). 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 \(\mu : M_1 \times \cdots \times M_n \to N\) be a multi-homogeneous polynomial law of multi-degree \(\hat{1} = (1, \ldots, 1)\). For \(1 \leq i \leq n\) and fixed \(v_j \in M_j (1 \leq j \leq n, j \neq i),\) it is straightforward to verify, using 13.4 (1), that \(f_i : M_i \to N\) defined by

\[
f_i(x) := \mu_R(v_1R, \ldots, v_{i-1}R, x, v_{i+1}R, \ldots, v_nR)
\]
for $R \in k\text{-alg}$, $x \in M_R$, is a homogeneous polynomial law of degree 1. Therefore, by the special case treated above, $f_{M_1} : M_1 \to N$ is a $k$-linear map, forcing $\mu_k : M_1 \times \cdots \times M_N \to N$ to be $k$-multilinear. Applying this to the extended polynomial law $\mu \otimes R : M_{kR} \times \cdots \times M_{kR} \to N_R$ over $R$, we conclude that $\mu_k : M_{kR} \times \cdots \times M_{kR} \to N_R$ is an $R$-multi-linear map. Hence, given $r_{ij} \in R, v_{ij} \in M_j$ for $1 \leq f \leq n$ and finitely many indices $i$, we obtain

$$
\mu_k(\sum r_{i1}v_{i1R}, \ldots, \sum r_{in}v_{inR}) = \sum_{i_1, \ldots, i_n} r_{i1} \cdots r_{in} \mu_k(v_{i1}, \ldots, v_{in}) R
$$

This proves $\mu_k = \mu_k \otimes R$ and completes the solution of (a).

(b) Let $Q : M \to N$ be a quadratic map. We show that $\tilde{Q} : M \to N$ is a polynomial law over $k$ by letting $\phi : R \to S$ be a morphism in $k\text{-alg}$ and $x, x' \in M, r, r' \in R$. The Cor. \[12.5\] implies

$$
(1_N \otimes \phi) \circ Q(x \otimes r) = (1_N \otimes \phi) \circ Q(xr) = (1_N \otimes \phi)(Q(x) \otimes r^2)
$$

and, similarly, $(1_N \otimes \phi) \circ Q(x \otimes r, x' \otimes r') = Q \circ (1_M \otimes \phi)(x \otimes r, x' \otimes r')$. This proves that $\tilde{Q}$ is indeed a polynomial law over $k$ and obviously homogeneous of degree 2. Conversely, let $f : M \to N$ be a homogeneous polynomial law of degree 2 over $k$ and consider the set map $Q := f_k : M \to N$. By \[13.8\] (c) and \[13.7\], we have

$$
Q(\alpha x + \beta y) = \alpha^2 f_k(x, y) + \alpha \beta f_k(x, y) + \beta^2 f_k(x, y)
$$

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 \[13.14\], 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 $(Df)_k = (f^{(1)})(f)_k$ is $k$-bilinear by \[13.8\] (a) and (a). This shows that $Q$ is a quadratic map with $DQ = (Df)_k$. For $R \in k\text{-alg}$, the $R$-quadratic map $Q_R : M_R \to N_R$ is uniquely determined by \[12.5\], which proves $Q_R = f_R$, hence $\tilde{Q} = f$.
Comparing coefficients of \(354 6\) Cubic Jordan algebras

(b) Let \(\nu\):

\[
\nu(x_1, \ldots, x_p, x, \ldots, x) = \sum_{\nu_{p+1} + \ldots + \nu_n = \nu} (\nu_{p+1}! \cdots \nu_n! (\Pi^{(\nu_{p+1}, \ldots, \nu_n)} f)_{R}(x_1, \ldots, x_p, x) \]

and comparing coefficients again completes the proof of (a).

(c) Let \(R \in \text{k-alg}\), \(t_1, t_2\) be independent variables and \(T = (t_1, t_2)\). For \(x, y_1, y_2 \in M_R\) we combine the Taylor expansion formula \([13.13]\) with Thm. \([13.7]\) and obtain

\[
\sum_{n \geq 0} t^n (D^p f)_{R[T]}(x, t_1 y_1 + t_2 y_2) = f_{R[L[T]}(x + t(t_1 y_1 + t_2 y_2)) = f_{R[L[T]}(x + (t_1) y_1 + (t_2) y_2)
\]

Comparing coefficients of \(t^n\), we therefore end up with the formula

\[
(D^p f)_{R[T]}(x, t_1 y_1 + t_2 y_2) = \sum_{j=0}^n t^{j} t_2^{n-j} \sum_{i=0}^j (\Pi^{(\nu_{i}, \ldots, \nu_j)} f)_{R}(x, t_1 y_1, t_2 y_2)
\]

This formula will now be applied in the special case \(n = 2\). From Exc. \([13.53]\) combined with \([13.8](a)\) we deduce, for all \(i \in \mathbb{N}\),

\[
\begin{align*}
(\Pi^{(\nu_1, \ldots, \nu_n)} f)_{R}(x, y_1, y_2) &= (\Pi^{(\nu_2)} f)_{R}(x, y_1), \\
(\Pi^{(\nu_1, \ldots, \nu_n)} f)_{R}(x, y_1, y_2) &= (\Pi^{(\nu_2, \ldots, \nu_n)} f)_{R}(x, y_2, y_1) = (\Pi^{(\nu_2)} f)_{R}(x, y_2).
\end{align*}
\]
Hence (89) for \( n = 2 \) implies

\[
(D^2 f)_{r_1 T}(x, t_1 y_1 + t_2 y_2) = t_1 [\xi T] \sum_{i \geq 0} (\Pi^{[i,2]} f)_{r_1 T}(x, y_1) + t_1 t_2 [\sum_{i \geq 0} (\Pi^{[i,1]} f)_{r_1 T}(x, y_1, y_2) + t_2^2 (D^2 f)_{r_1 T}(x, y_2)].
\]

In particular, applying Prop. 13.19,

\[
(\partial f)_{r_1 T}(x) = (D^2 f)_{r_1 T}(x, y) + (\partial f)_{r_1 T}(x, y_1) + (\partial f)_{r_1 T}(x, y_2) + \partial^2 f_{r_1 T}(x),
\]

which completes the proof of (c).

By (13.14.1) we have \( D^2 f = \Pi f \) and (13.8.1) implies \( (D^2 f)(x, y) = (\Pi f)(y, x) \), hence

\[
f(y, x) = (D^2 f)(y, x).
\]

Combining (13.14.2) for \( d = 3 \) with (13.13.3) and (2), (90), we obtain (3). In order to derive (4), we first let \( x, y \in M \). Then (90), Ex. 57(c) and Prop. 13.19 imply

\[
f(x + y, z) = (D^2 f)(z, x + y) = (\partial f)_{x+y}(z)
\]

\[
= (\partial f)(z) + (\partial f)(z) + (\partial f)(z)
\]

\[
= (D^2 f)(z, x) + (\Pi f)(y, z) + (D^2 f)(z, y)
\]

\[
= f(x, z) + f(x, y, z) + f(y, z),
\]

as claimed. The general case \( x, y \in M_R \) now follows by looking at \( f \otimes R \) rather than \( f \). Combining (3) for \( t = 1 \) and (4), we now obtain

\[
f(x + y + z) - f(x + y) - f(y + z) - f(z + x) + f(x) + f(y) + f(z)
\]

\[
= f(x + y) + f(x + y, z) + f(z, x + y) + f(z) - f(x + y) - f(y) - f(y, z)
\]

\[
- f(z, y) - f(z) - f(z, x) - f(x, z) + f(x) + f(x) + f(y) + f(z)
\]

\[
= f(x, z) + f(x, y, z) + f(z, x) + f(z, y) + f(z, z) + f(z) - f(y, z) + f(y, z) + f(y, z) - f(z, y) + f(z, y) - f(y, z) + f(z, y)
\]

\[
- f(z) - f(z) - f(z, x) - f(x, z) + f(x) + f(x) + f(y) + f(z)
\]

\[
= f(x, y, z),
\]

and this is (5). Before dealing with (6), we prove

\[
f(\sum_{i=1}^n r_i x_i, x) = \sum_{i=1}^n r_i^2 f(x_i, x) + \sum_{1 \leq i < j \leq n} r_i r_j f(x_i, x_j, x)
\]

for \( x \in M_R \) by induction on \( n \). For \( n = 1 \) there is nothing to prove. For \( n > 1 \), the induction hypothesis and (4) imply
as claimed. Hence zero. On the other hand, since $g_{x_i}$ for all $x_i$, this completes the induction and the proof of (a).

This completes the induction and the proof of (a).

(b) (i) $\Rightarrow$ (ii). From (i) we deduce $g_{F(e_i)} = 0$ for $1 \leq i \leq n$, while (i) implies $g_F(x,y,z) = 0$ for all $x,y,z \in F^n$. Moreover, from Euler’s differential equation $13.143$, we conclude $g_F(x,y) = (Dg)_F(x,y) + 3g_F(x) = 0$. It remains to show that $F$ consists of two elements and $g_F(x_0,y_0) \neq 0$ for some $x_0,y_0 \in F^n$. Replacing $f$ by $g$ and specializing $t$ to $\alpha \in F^n$ in (ii), 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 (i) and (ii) for $g$ in place of $f$ and $e_i \mapsto r_i$ in place of $x_i$ for $1 \leq i \leq n$ would lead to the contradiction $g = 0$ as a polynomial law over $F$. Thus (ii) holds.

(ii) $\Rightarrow$ (iii). By (i) and morcupmap (v) 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

$$S := \langle g_F(e_i,e_j) \rangle_{1 \leq i,j \leq n} \in \text{Mat}_n(F)$$

to be an alternating matrix and $S \neq 0$ by (ii). Now let

$$x = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in \sum_{i=1}^n r_i e_i \in R^n = (F^n)_R \quad \quad (r_1, \ldots, r_n \in R).$$

The (v) and (vi) imply

$$g_R(x) = g_R(\sum_{i=1}^n r_i e_i) = \sum_{i=1}^n r_i g_F(e_i) + \sum_{1 \leq i,j \leq n, i \neq j} r_i r_j g_F(e_i,e_j) + \sum_{1 \leq i \leq n} r_i r_i g_F(e_i,e_i) = \sum_{1 \leq i,j \leq n} r_i g_F(e_i,e_j) r_j^2 = x^t S x^2,$$

as claimed.

(iii) $\Rightarrow$ (i). Since $F \cong \mathbb{F}_2$ consists of two elements, the elements of $F^n$ as an $F$-algebra are all idempotents. Hence $g_F(x) = x^t S x = 0$ for all $x \in F^n$, whence the set map $g_F : F^n \to F$ is identically zero. On the other hand, since $S \neq 0$, there are elements $x_0, y_0 \in F^n$ such that $x_0^t S y_0 \neq 0$, 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

$$g_k(x_0 + \theta y_0) = (x_0 + \theta y_0)^3 S(x_0^2 + \theta y_0^2)$$
$$= (x_0 + \theta y_0)^3 S(x_0 + \theta^2 y_0) = (x_0 + \theta y_0)^3 S(x_0 + \theta y_0) + (x_0 + \theta y_0)^3 S y_0$$
$$= \delta_0 S y_0 \neq 0.$$

Thus $g_k \neq 0$, so $g : F^n \to F$ is a non-zero cubic form.

(a) If $f : M \to N$ and $f' : M' \to N'$ are polynomial laws over $k$, a morphism from $f$ to $f'$ in $k$-polaw is defined as a pair of linear maps $\varphi : M \to M'$, $\psi : N \to N'$ making a commutative diagram

$$
\begin{array}{ccc}
M & \xrightarrow{f} & N \\
\downarrow{\varphi} & & \downarrow{\psi} \\
M' & \xrightarrow{f'} & N'
\end{array}
$$

of polynomial laws over $k$.

(c) 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

$$f(x+y+z) - f(x+y) - f(y+z) - f(z+x) + f(x) + f(y) + f(z)$$
$$= g(x+y,z) + g(z,x+y) + f(z) - f(y) - g(y,z) - g(z,y) - f(z)$$
$$- f(z) - g(z,x) - g(x,z) - f(x) + f(x) + f(y) + f(z)$$
$$= g(x,y,z),$$

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, follows immediately by linearizing $g(y,x) = 0$ for $x \in \text{Rad}(f,g)$ with respect to $y \in M$ and using the total symmetry of $g$. Hence (iii) implies that $\text{Rad}(f,g)$ is a submodule of $M$. Finally, for a linear map $\pi$ as indicated, the maps $f_1 : M_1 \to N_1$ and $g_1 : M_1 \times M_1 \to N_1$ 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 are well defined, and it is straightforward to check that $(f_1, g_1) : M_1 \to N_1$ is a cubic map with the desired properties. This completes the proof of (c).

(d) If $(f,g) : M \to N$ and $(f',g') : M' \to N'$ are cubic maps over $k$, a morphism from $(f,g)$ to $(f',g')$ in $k$-cumap is defined as a pair of linear maps $\varphi : M \to M'$, $\psi : N \to N'$ making commutative diagrams

$$
\begin{array}{ccc}
M & \xrightarrow{f} & N \\
\downarrow{\varphi} & & \downarrow{\psi} \\
M' & \xrightarrow{f'} & N'
\end{array}
$$

and

$$
\begin{array}{ccc}
M \times M & \xrightarrow{g} & N \\
\downarrow{\varphi \times \varphi} & & \downarrow{\psi} \\
M' \times M' & \xrightarrow{g'} & N'
\end{array}
$$

of set maps.

Now let $f : M \to N$ be a homogeneous polynomial law of degree 3 over $k$. We combine equations (3), (4) of Exc. 58 with Euler’s differential equation (13.14.3) to conclude that $(f_k, (Df)_k)$ is a cubic map from $M$ to $N$. If $(\varphi, \psi) : f \to f'$ is a morphism in $k3$-holaw, then the chain rules (13.1.4), (13.1.5) applied to the commutative diagrams 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. We now proceed to show a functor in the opposite direction that is inverse to the previous one, and first claim that the assignment \( f \mapsto (f|_k, (Df)_k) \) gives a linear bijection from the homogeneous polynomial laws \( M \to N \) of degree 3 over \( k \) onto the cubic maps \( M \to N \) over \( k \). The map in question is clearly \( k \)-linear. But it is also injective since \( f_k = (Df)_k = 0 \) for a homogeneous polynomial law \( f : M \to N \) of degree 3 over \( k \) by equation (6) of Exc. 58 implies \( f = 0 \). It thus remains to show that it is surjective as well, so let \((f, g) : M \to N\) be any cubic map. Our task will be define set maps \( \tilde{f}_k : M_R \to N_k \) that vary functorially with \( R \in k\text{-alg} \), hence give rise to a polynomial law \( f : M \to N \) over \( k \), are homogeneous of degree 3, and have \( f_k = f \), \((Df)_k = g \).

We begin by extending \( g \) to a unique \( R \)-quadratic-linear map \( \tilde{g}_R : M_R \times M_R \to N_R \) such that

\[
\tilde{g}_R(x_R, y_R) = g(x, y)_R \quad (x, y \in M). \tag{94}
\]

In order to do so, let \( y \in M \). By Prop. [12.4] the \( k \)-quadratic map \( g(-, y) : M \to N \) extends uniquely to an \( R \)-quadratic map \( g(-, y)_R : M_R \to N_R \) such that \( g(-, y)_R(x_R) = g(x, y)_R \) for all \( x \in M \). Thus we obtain a map

\[
g' : M_R \times M \to N_R, \quad (x, y) \mapsto g'(x, y) := g(-, y)_R(x),
\]

which is clearly \( k \)-linear in the second variable and \( R \)-quadratic in the first. For \( x \in M_R \), therefore, \( g'_k(x, \cdot) : M \to N_k \) is \( k \)-linear and hence induces canonically an \( R \)-linear map \( g'_R(x, \cdot) : M_R \to N_R \).

Summing up, we can now define \( \tilde{g}_R : M_R \times M_R \to N_R \) by \( \tilde{g}_R(x, y) := g'_R(x, y) \) for \( x, y \in M_R \), which satisfies (94) since for \( x, y \in M \) we have

\[
\tilde{g}_R(x_R, y_R) = g'_R(x_R, y_R) = g'_R(x_R, -)(y) = g'(x_R, y) = g(-, y)_R(x_R) = g(x, y)_R.
\]

For finitely many \( r_i, s_i \in R \), \( x_i, y_i \in M \), we now conclude

\[
\tilde{g}_R \left( \sum_{i} r_ix_i, \sum_{i} s_iy_i \right) = \sum_{i} r_i^2 g(x_i, y_i)_R + \sum_{i<j} r_is_jg(x_i, x_j, y_i)_R \tag{95}
\]

from the fact that \( \tilde{g} \) is \( R \)-quadratic-linear and (94) holds. In particular, \( \tilde{g} \) is uniquely determined by these two conditions.

We now turn to the construction of \( f \). First we note

\[
f(\sum_{i} \alpha_i x_i) = \sum_{i} \alpha_i^2 f(x_i) + \sum_{i \neq j} \alpha_i \alpha_j g(x_i, x_j) + \sum_{i, j, l} \alpha_i \alpha_j \alpha_l g(x_i, x_j, x_l) \tag{96}
\]

for finitely many \( \alpha_i \in k \), \( x_i \in M \). The proof proceeds by induction on the number of non-zero summands along exactly the same lines as the one of formula (6) in Exc. 58. Let us now begin by assuming that \( M \) is free as a \( k \)-module, with basis \( (e_i)_{i \in I} \), indexed by a totally ordered set \( I \). In the spirit of (96), we then define a set map \( \tilde{f}_R : M_R \to N_R \) by

\[
\tilde{f}_R(\sum_{i} r_ie_i) := \sum_{i} r_i^2 f(e_i)_R + \sum_{i} r_ir_j g(e_i, e_j)_R + \sum_{i, j \in I} r_ir_j r_l g(e_i, e_j, e_l) \tag{97}
\]

for all families \( (r_i)_{i \in I} \) with finite support in \( R \). By definition, the set maps \( \tilde{f}_R \) vary functorially with \( R \in k\text{-alg} \), hence define a polynomial law \( \tilde{f} : M \to N \) over \( k \) which is obviously homogeneous of degree 3. For \( x = \sum r_ie_i, y = \sum s_ie_i \in M_R \), where the families \( (r_i), (s_i) \) in \( R \) have finite support, we obviously have

\[
(D\tilde{f})_R(x, y) = 3 \sum r_i^2 f(e_i)_R + \sum_{i, j} r_ir_j g(e_i, e_j)_R + \sum_{i, j, l} r_ir_j r_l g(e_i, e_j, e_l)_R. \tag{98}
\]

and

\[
\tilde{f}_R(\sum_{i} r_ix_i, \sum_{i} s_iy_i) = g(x, y)_R \tag{99}
\]
such that \( k \) of degree 3. By construction, we have \( \tilde{k} \) functorially with \( f \)

where \( g \)

Therefore, we find a cubic map \( \tilde{f} \) such that \( \tilde{f} \circ \pi = f \circ \pi \), hence \( \tilde{f} = f \), while \( [13,15] \) implies \( (Df)_{k} \circ (\pi \times \pi) = (D(f \circ \pi))_{k} = (Df)_{k} \circ g = g \circ (\pi \times \pi) = (Df)_{k} \circ g \). Thus the map in question is also surjective, which completes the proof of our intermediate assertion.

To every object \((f,g)\) of \( k\)-\textit{cubic map} we can thus associate a unique object \( f \circ g \) in \( k\)-\textit{holaw} such that \((f \circ g)_{k} = f \) and \( D(f \circ g)_{k} = g \), and we will be through once we have shown that every morphism \((\varphi, \psi) : (f,g) \rightarrow (f',g')\) in \( k\)-\textit{cubic map} is also a morphism \((\varphi, \psi) : f \circ g \rightarrow f' \circ g'\) in \( k\)-\textit{holaw}. By \([92]\) and \([93]\), we have

Thus \((f_{R},(Df)_{R}) = (\tilde{f}_{R},\tilde{g}_{R})\), and this is a cubic map \( M_{R} \rightarrow N_{R} \) over \( R \). In particular, for \( R = k \), we conclude \((f_{k},(Df)_{k}) = (f,g)\), which completes the proof in case \( M \) is free as a \( k\)-module.

Now assume that \( M \) is arbitrary. Then there exists a short exact sequence

of \( k\)-modules, where \( F \) is free. Since the functor \(- \otimes R \) is exact right, we obtain an induced exact sequence

Now observe that \((f_{1},g_{1}) := (f \circ \pi, g \circ (\pi \times \pi))\) is a cubic map from \( F \) to \( N \). By the special case treated before, we therefore obtain a homogeneous polynomial \( \text{Law}_{f_{1}} : F \rightarrow N \) of degree 3 and an \( R\)-quadratic-linear map \( \tilde{g}_{1R} : F_{R} \times F_{R} \rightarrow N_{R} \) satisfying \((\tilde{f}_{1R},(Df_{1})_{R}) = (f_{1R},\tilde{g}_{1R})\) and \( f_{1R} = f_{1}\), \( \tilde{g}_{1R} = g_{1R} \). We now claim

The last displayed exact sequence shows that any element of \( \text{Ker}(\pi_{R}) \) can be written as \( u_{k}(z) \), for some \( z = \sum r_{i}u_{iR} \in L_{R}, r_{i} \in R, u_{i} \in L \). Applying \([90]\) to the \( R\)-cubic map \((\tilde{f}_{1R},\tilde{g}_{1R})\), we conclude

where \( f_{1}(u_{i}(y)) = (f \circ \pi \circ t)(u_{i}) = 0, g_{1}(t(u_{i}), t(u_{i})) = g_{1}(\pi \circ t)(u_{i}), (\pi \circ t)(u_{i})) = 0 \) and, similarly, \( g_{1}(t(u_{i}), t(u_{i}), t(u_{i})) = 0 \). An analogous computation, involving \([95]\), shows \( \tilde{g}_{1R}(u_{k}(z), y) = \tilde{g}_{1R}(y, u_{k}(z)) = 0 \) for all \( y \in F_{R} \). Hence \( u_{k}(z) \in \text{Rad}(\tilde{f}_{1R},\tilde{g}_{1R}) \), and the proof of \([100]\) is complete. By \( a \), therefore, we find a cubic map \((\tilde{f}_{k},\tilde{g}_{k}) : M_{k} \rightarrow N_{k} \) such that \( \tilde{f}_{k} \circ \pi_{k} = f_{k} \) and \( \tilde{g}_{k} \circ (\pi_{k} \times \pi_{k}) = \tilde{g}_{1R} \). Since the linear maps \( \pi_{R} \), for all \( R \in k\text{-alg} \), are surjective, and the \( \pi_{R} \) vary functorially with \( R \), so do the \( \tilde{f}_{k} \). In other words, \( \tilde{f} : M \rightarrow N \) is a homogeneous polynomial law over \( k \) of degree 3. By construction, we have \( \tilde{f}_{k} \circ \pi = f_{k} = f \circ \pi \), hence \( \tilde{f}_{k} = f \), while \( [13,15] \) implies \( (Df)_{k} \circ (\pi \times \pi) = (D(f \circ \pi))_{k} = (Df)_{k} \circ g = g \circ (\pi \times \pi) = (Df)_{k} \circ g \). Thus the map in question is also surjective, which completes the proof of our intermediate assertion.

To every object \((f,g)\) of \( k\)-\textit{cubic map} we can thus associate a unique object \( f \circ g \) in \( k\)-\textit{holaw} such that \((f \circ g)_{k} = f \) and \( D(f \circ g)_{k} = g \), and we will be through once we have shown that every morphism \((\varphi, \psi) : (f,g) \rightarrow (f',g')\) in \( k\)-\textit{cubic map} is also a morphism \((\varphi, \psi) : f \circ g \rightarrow f' \circ g'\) in \( k\)-\textit{holaw}. By \([92]\) and \([93]\), we have
\( (\Psi \circ (f \ast g))_k = \Psi \circ (f \ast g)_k = \Psi \circ f = f' \circ \varphi = (f' \ast g')_k \circ \varphi = ((f' \ast g')_k \circ \varphi)_k. \)

\( (D(\Psi \circ (f \ast g)))_k(x,y) = \psi(D((f \ast g))_k(x,y)) = \psi(g(x,y)) = g'(\varphi(x),\varphi(y)) \)

\( = (D((f' \ast g'))_k(x,y))(\varphi(x),\varphi(y)) = (D((f' \ast g') \circ \varphi))_k(x,y). \)

Hence the uniqueness part of our intermediate assertion shows that \((\varphi, \psi) : f \ast g \to f' \ast g'\) is indeed a morphism in \(k\)-holaw.

**60** Fixing \(R \in k\text{-}\text{alg}, \) there is clearly a unique \(k\)-linear map

\[ \Psi_k : N \otimes \text{Pol}(M,k) \to \text{Map}(M_k,N_k) \]

given by

\[ \Psi_k(v \otimes f)(x) = v \otimes f_k(x) \]

for \(v \in N, f \in \text{Pol}(M,k), x \in M_k. \) For the first part of the problem, it will be enough to show that \(\Psi_k\) varies functorially with \(R, \) so let \(\varphi : R \to S\) be a morphism in \(k\text{-}\text{alg}. \) Since \(f\) is a scalar polynomial law, hence the diagram

\[
\begin{array}{ccc}
M_k & \xrightarrow{f_k} & R \\
\downarrow{1_M \otimes \varphi} & & \downarrow{\varphi} \\
M_k & \xrightarrow{f_k} & S
\end{array}
\]

commutes, so does

\[
\begin{array}{ccc}
M_k & \xrightarrow{\Psi_k(v \otimes f)} & N_k \\
\downarrow{1_M \otimes \varphi} & & \downarrow{1_{N_k} \otimes \psi} \\
M_k & \xrightarrow{\Psi_k(v \otimes f)} & N_k
\end{array}
\]

Hence we have shown that a \(k\)-linear map \(\Psi : N \otimes \text{Pol}(M,k) \to \text{Pol}(M,N)\) satisfying \((11)\) 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 \(\pi : N \otimes N' \to N, \pi' : N \otimes N' \to N', \) canonically regarded as homogeneous polynomial laws of degree 1 via Exercise 56 induce \(k\)-linear maps

\[ \pi : \text{Pol}(M,N \otimes N') \to \text{Pol}(M,N), \quad \pi' : \text{Pol}(M,N \otimes N') \to \text{Pol}(M,N') \]

given by \(f \mapsto \pi \circ f, f \mapsto \pi' \circ f, \) respectively, which in turn yield an isomorphism

\[ \pi \otimes \pi' : \text{Pol}(M,N \otimes N') \xrightarrow{\sim} \text{Pol}(M,N) \otimes \text{Pol}(M,N'). \]

After the natural identification \(M \otimes (N \otimes N') = M \otimes N \otimes M \otimes N',\) it is straightforward to check that the diagram

\[
\begin{array}{ccc}
(N \otimes N') \otimes \text{Pol}(M,k) & \xrightarrow{\psi \otimes \psi'} & \text{Pol}(M,N \otimes N') \\
\downarrow{\text{can}} & & \downarrow{\pi \otimes \pi'} \\
(N \otimes \text{Pol}(M,k)) \oplus (N' \otimes \text{Pol}(M,k)) & \xrightarrow{\psi \otimes \psi'} & \text{Pol}(M,N) \oplus \text{Pol}(M,N')
\end{array}
\]

\[(101)\]
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 (101), we are reduced to the case \( N = k. \) But then \( \Psi = \Psi^k = \mathbb{1}_{\mathbb{P}(M,k)} \), and the problem is solved.

We require the following easy lemma.

**Lemma.** Assume \( N \) is a \( K \)-module, \( N' \) is a \( K' \)-module and \( \varphi \colon M' \to M, \, \psi \colon N' \to N \) are \( \sigma \)-semi-linear maps. Then there exists a unique \( K \)-homomorphism in \( \mathbb{S}(M \otimes_K N) \).

**Proof.** Uniqueness is obvious. To prove existence, we note that \( \varphi \) (resp. \( \psi \)) may be viewed as a \( K' \)-linear map \( \varphi' \colon M' \to M^\sigma \) (resp. \( \psi' \colon N' \to N^\sigma \)) satisfying \( \varphi'(x') = \varphi(x')^\sigma \) for \( x' \in M' \) (resp. \( \psi'(y') = \psi(y')^\sigma \) for \( y' \in N' \)). Hence

\[
\varphi' \otimes_{K'} \psi' \colon M' \otimes_{K'} N' \to M^\sigma \otimes_{K'} N^\sigma
\]

exists as a \( K' \)-linear map. On the other hand, one checks easily, using (13.24.1), that the map

\[
M^\sigma \times N^\sigma \to (M \otimes_K N)^\sigma, \quad (x,y) \mapsto \left( \sigma_K(x) \otimes_K \sigma_N(y) \right)^\sigma
\]

is \( K' \)-bilinear, hence canonically induces a \( K' \)-linear map

\[
\phi \colon M^\sigma \otimes_{K'} N^\sigma \to (M \otimes_K N)^\sigma.
\]

Thus

\[
(\varphi \otimes \sigma \psi)' := \phi \circ (\varphi' \otimes_{K'} \psi') \colon M' \otimes_{K'} N' \to (M \otimes_K N)^\sigma
\]

is \( K' \)-linear and therefore determines a \( \sigma \)-semi-linear map

\[
\varphi \otimes_{\sigma} \psi := \sigma_M \otimes_{K,N} (\varphi \otimes_{\sigma} \psi)' \colon M' \otimes_{K'} N' \to M \otimes_K N
\]

with the desired properties. \( \square \)

Using this lemma, it suffices to put \( \varphi_k := \varphi \otimes_{\sigma} \sigma_K \) to obtain a \( \sigma \)-semi-linear map \( M'_{\sigma K} \to M_K \) satisfying (112), uniqueness again being obvious. For \( r, r_1 \in R \) and \( x' \in M' \), we apply (112) and obtain

\[
\varphi_k(r_1 \cdot (x' \otimes_{K'} r^\sigma)) = \varphi_k \left( x' \otimes_{K'} (r_1 r)^\sigma \right) = \varphi_k(x') \otimes_k (r_1 r) = r_1 \left( \varphi(x') \otimes_K (r_1)^\sigma \right) = \sigma_K(r_1^\sigma) \varphi_k(x' \otimes_{K'} r^\sigma),
\]

showing that \( \varphi_k \) is indeed \( \sigma_k \)-semi-linear.

We show that \( \varphi := (\varphi_k)_{R \in \mathbb{K}_{alg}} \) is a \( \sigma \)-semi-polynomial law by letting \( \lambda : R \to S \) be any morphism in \( K_{alg} \) to compute, for \( x' \in M' \), \( r \in R \),

\[
(1_M \otimes_k \lambda) \circ \varphi_k(x' \otimes_{K'} r^\sigma) = (1_M \otimes_k \lambda)(\varphi(x') \otimes_K \lambda(r)) = \varphi(x') \otimes_k \lambda(r) = \varphi_k(x' \otimes_{K'} \lambda(r)^\sigma) = \varphi_k(1_M \otimes_{K'} \lambda^\sigma)(x' \otimes_{K'} r^\sigma).
\]

Hence the set maps \( \varphi_k : M'_{\sigma K} \to M_K \) vary functorially with \( R \in K_{alg} \), whence \( \varphi : M' \to M \) is a \( \sigma \)-semi-polynomial law over \( k \).

(b) Let \( \lambda : R \to S \) be a morphism in \( K_{alg} \). The fact that \( \lambda^\sigma : R^\sigma \to S^\sigma \) is a morphism in \( K'_{alg} \) gives rise to the commutative diagram
and the first assertion follows. As to the second, let $\chi: K'' \to K''$ be another morphism in $k$-$\text{alg}$, $M''$ a $K''$-module and $h: M'' \to M''$ a $\chi$-semi-polynomial law over $k$. Then

$$(f \circ g) \circ h = (f \circ g)_R \circ h_{R^\sigma} = f_R \circ g_{R^\sigma} \circ h_{(R^\sigma)^\tau} = f_R \circ (g \circ h)_{R^\sigma} = (f \circ (g \circ h))_R.$$  

Hence $(f \circ g) \circ h = f \circ (g \circ h)$ as $\sigma$-$\chi$-semi-polynomial laws $M'' \to M$ over $k$.

(c) For $R \in k$-$\text{alg}$, $x' \in M''$, $r \in R$ we compute

$$(\varphi \circ \psi)_R (x') \otimes_{K'} r^\sigma = (\varphi \circ \psi)(x') \otimes_{K'} r = \varphi_R (\psi(x')) \otimes_{K'} r = \varphi_R \left( \psi_{R^\sigma} (x'' \otimes_{K'} r^\tau) \right) = (\varphi \circ \psi_{R^\sigma}) (x'' \otimes_{K'} r^\tau),$$

and this means $(\varphi \circ \psi)^{-1} = \tilde{\varphi} \circ \tilde{\psi}$.

(d) We have $\sigma \sigma^{-1} = 1_K$, $\sigma^{-1} \sigma = 1_K$ and (13.24) implies

$$1_M = (\sigma \sigma^{-1})_M = \sigma_M \circ (\sigma^{-1})_M,$$

$$1_{M^\sigma} = (\sigma^{-1} \sigma)_M = (\sigma^{-1})_M \circ \sigma_{(M^\sigma)^{e^{-1}}} = (\sigma^{-1})_M \circ \sigma_M.$$  

By (c), therefore, $(\sigma_M)^{-1} \circ ((\sigma^{-1})_M)^{-1}$ is the polynomial law over $K$ given by the identity of $M$, while $((\sigma^{-1})_M)^{-1} \circ (\sigma_M)^{-1}$ is the polynomial law over $K'$ given by the identity of $M^\sigma$. Hence if $g$ is a polynomial law satisfying the requirements of (d), then $g = ((\sigma^{-1})_M)^{-1} \circ f$. On the other hand, defining $g$ in this way and observing that

$$( (\sigma^{-1})_M)^{-1}: M = (M^\sigma)^{\sigma^{-1}} \to M^\sigma$$

is a $\sigma^{-1}$-semi-polynomial law over $k$, it follow from (b) that $g: M' \to M^\sigma$ is an ordinary polynomial law over $K'$ such that $f = (\sigma_M)^{-1} \circ g$.

Chapter 3

Section 14

63. Since the associator of $A$ is alternating, the first part follows immediately from 8.5.1. The second part is now obvious.

64. The implications (i)$\Rightarrow$(ii)$\Rightarrow$(iii)$\Rightarrow$(iv) and (i)$\Rightarrow$(v) are obvious, while (iv)$\Rightarrow$(v) follows from the fact that $L_x, R_x, U_x = L_x, R_x$ commute by pairs. We are thus left with the following implications. (iv)$\Rightarrow$(i). Given $y \in A$, we find an element $z \in A$ satisfying $z x = y$. Moreover, since (iii) holds by what we have just seen, there are $e, f \in A$ such that $e x = x = x f$. Now the Moufang identities
The remaining ones are now obvious. Next we establish (3) for $x \in A$ by definition, $x$ is bijective iff $x$ is invertible, so $L_x = 1_x - L_x = 1_x - R_x$ to arrive at the desired conclusion. Now let $i, j, l, m, n = 1, 2$ and put $E_{ij} := L_{ij} R_{ij}$. Then (102) yields $E_{ij} E_{lm} = L_{ij} R_{ij} L_{lm} R_{lm} = L_{ij} R_{ij} R_{lm} R_{lm} = \delta E_{il} E_{jm} R_{ij} = \delta E_{il} \delta R_{ij} E_{jm}$, so the $E_{ij}$ are indeed orthogonal projections that add up to $\sum_{i,j=1,2} E_{ii} = U_1$. This proves (1), where the $A_{ij} = A_{ji}(c)$ 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 $x_i \in A_{ij}$, $y_{lm} \in A_{lm}$ etc. and first prove

$$c_i x_j = \delta_i x_j, \quad x_i c_j = \delta_{ij} x_{ij}.$$ (103)

Indeed, by (2) the first relation is clear for $i = j$, while for $i \neq j$ we obtain $c_i x_j = x_i - c_j x_j = x_i x_j - x_j x_i = 0$, as claimed. The second relation is proved analogously. Combining now the linearized right alternative law (14.2.8) with (103), we obtain $(x_i y_j) c_l = x_i (y_j c_l + c_j y_l) - (x_i c_l) y_l = x_i y_j + \delta_{il} x_i y_l = \delta_{il} x_i y_l$ and, similarly, $c_j (x_i y_j) = x_i (c_j y_j + c_j x_j - x_j c_l) = x_i y_j - x_j x_i = 0$, as also have (3). In particular, $x_{ij} x_j = c_j x_{ij} = (c_j x_i) x_j = 0$, while the remaining assertion $A_{ij}^0 = \{0\}$ for $A$ associative is obvious.

### Section 16

By Prop. (14.6) $x \in A$ is invertible in $A^{(p,q)}$ iff $U_{(p,q)} = U_x U_{pq}$ (by (16.5.1)) is bijective iff $U_x$ is bijective iff $x$ is invertible in $A$, in which case its inverse in $A^{(p,q)}$ is $x^{(-1,p,q)} = (U_{(p,q)})^{-1} x = U_{pq} U_x^{-1} x = U_{pq} x$, as claimed.

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 $f(ux) = h(y), f(xy) = g(x)$, equivalently, $f \circ L_x = h \circ R_x = g$. Thus $L_x R_x : A \to A$ are linear bijections, forcing $A$ to be unital (Exc. 64) and $u, v \in A$ to be invertible (Prop. 14.6), with inverses $p := u^{-1}, q := v^{-1}$. This implies $f((xp)(yq)) = g(xp)h(yq) = f((xy)^{-1}y)(p(u^{-1}y)) = f(x)f(y)$. Thus $f : A^{(p,q)} \to B$ is an isomorphism; in particular, $B$ is alternative.
See [99, 2.2-2.8]. In particular $1_{\text{Str}(A)} = (1_A, 1_A, 1_A)$ is the unit element of Str$(A)$ and $(p, q, g)^{-1} = (g, -q, p^{-1}) \cdot (g, -q, p^{-1})^t$ is the inverse of $(p, q, g) \in \text{Str}(A)$.

The equation $(L_9 x) \cdot u - u^2 (L_9 y) = x u u \cdot u^{-2} (y u) = u (x (u^{-1} y)) = u (x y) = L_9 (x y)$ for all $x, y \in A$ shows that $L_9 : A \to A^{(u, u^{-2})}$ is an isomorphism. Hence $L_9 \in \text{Str}(A)$. Reading this in $A^{op}$ also yields $\tilde{R}_9 \in \text{Str}(A)$. Invoking (71) and Cor. 15.5 we now compute

$$L_9 \tilde{R}_9 \tilde{L}_9 = (u, u^{-2}, L_9) (v, v^{-2}, L_9) \tilde{L}_9 = (w, u^{-1} v^{-2} u^{-1}, L_9 \tilde{L}_9) (u, u^{-2}, L_9) \tilde{L}_9 = (w, z, \tilde{L}_9 \tilde{L}_9 \tilde{L}_9),$$

where

$$w = u u v^{-1} v^{-2} u^{-1} u u v = u v,$$

$$z = u^{-1} v^{-2} u^{-1} u u v^{-1} v^{-2} u^{-1} = u^{-1} v^{-1} u^{-2} v^{-1} u^{-1} = (u v)^{-2}.$$
The solution to Exc. 73 shows that right multiplication by pq yields an isomorphism from A(pq) to an appropriate unital isotope of A. It therefore suffices to show Nuc(A(pq)) = Nuc(A) and Cent(A(pq)) = Cent(A) for all p ∈ A**: actually, since A = (A(p))p−1, it will be enough to verify the inclusions Nuc(A) ⊆ Nuc(A(pq)), Cent(A) ⊆ Cent(A(pq)). Writing [−, −, −]p (resp. [−, −]p) for the associator (resp. the commutator) of A(p), this will follow once we have shown

\[ [x, y, z]^p = [x, y p^{-1}, p z] - [x, p^{-1}, (py)z], \quad [x, y]^p = [x, y] + [x, p^{-1}, py] - [y, p^{-1}, px] \quad (104) \]

for all \( x, y \in A \). In order to derive the first relation of (104), we compute

\[ [x, y, z]^p = \left( (xp^{-1})(py) \right)p^{-1}(pz) - (xp^{-1})(py)p^{-1}(pz) = [x, y p^{-1}, p z] - [x, p^{-1}, (py)z] \]

where the second summand on the right agrees with

\[ x \left( p^{-1} \left( p((py)z) \right) \right) = p^{-1}((py)z) = -[x, p^{-1}, (py)z] + (xp^{-1})(py)z. \]

Inserting this into the previous equation yields the first relation of (104). For the second, we obtain

\[ [x, y]^p = (xp^{-1})(py) - (yp^{-1})(px) = [x, p^{-1}, py] + xy - [y, p^{-1}, px] - xy = [x, y] + [x, p^{-1}, py] - [y, p^{-1}, px], \]

as claimed.

### Section 17

In order to get the terminology straight, let us denote by \( \text{paltinv}_p \) the category of \( p \)-pointed alternative algebras with involution as defined in Exc. 73. By contrast, let us denote by \( \text{alist}_p \) the category of alternative algebras with isotopy involution as defined in 17.4.

We begin by defining a functor \( \Phi: \text{paltinv}_p \to \text{alist}_p \). Let \( ((B, \tau), q) \) be an object of \( \text{paltinv}_p \). Then Cor. 17.8 shows that

\[ \Phi \left( ((B, \tau), q) \right) := (B^p, \tau^p, q) \]

is an object of \( \text{alist}_p \). If \( \varphi: ((B, \tau), q) \to ((B', \tau'), q') \) is a morphism in \( \text{paltinv}_p \), then it is straightforward to check that

\[ \varphi: (B^p, \tau^p, q) \to (B'^p, \tau'^p, q') \]

is a morphism in \( \text{alist}_p \). Hence we obtain a functor \( \Phi \) of the desired kind.

Next we define a functor \( \Psi: \text{alist}_p \to \text{paltinv}_p \) in the opposite direction. Let \( (B, \tau, q) \) be an object of \( \text{alist}_p \), i.e., an alternative \( k \)-algebra with isotopy involution. Then Prop. 17.7 and Lemma 17.1 show with \( p := q^{-1} \) that

\[ \Psi \left( ((B, \tau, q)) \right) := ((B^p, \tau^p), q) \]

is an object of \( \text{paltinv}_p \). If \( \psi: (B, \tau, q) \to (B', \tau', q') \) is a morphism in \( \text{alist}_p \) and \( p := q^{-1}, p' := q'^{-1} \), then \( \psi(p) = p' \), and it is straightforward to check that

\[ \psi: ((B^p, \tau^p), q) \to ((B'^{p'}, \tau'^{p'}), q') \]

is a morphism in \( \text{paltinv}_p \). Hence we obtain a functor \( \Psi \) of the desired kind.

Now we simply apply 17.7.5 to conclude that \( \Psi \circ \Phi \) is the identity on \( \text{paltinv}_p \) and \( \Phi \circ \Psi \) is the identity on \( \text{alist}_p \). Summing up
The map \( \epsilon_A \) has clearly period two and fixes \( p \). For the first part of the problem, it therefore suffices to show \([17.2]\) for \( \epsilon_A \) in place of \( \tau \). To this end, let \( x, x', y, y' \in A \). Then

\[
(\epsilon_A(y \oplus y')p^{-1})(p\epsilon_A(x \oplus x')) = ((y' \oplus y)(q \oplus q))((q^{-1} \oplus q^{-1})(x' \oplus x))
\]

\[
= ((qy') \oplus (sq^{-1}))(x'q^{-1} \oplus (q^{-1}q^{-1})(qx))
\]

\[
= ((qy') \oplus (sq^{-1}))((x'q^{-1} \oplus (q^{-1}x))
\]

\[
= (x'q^{-1})(qy') \oplus ((sq^{-1})(q(q^{-1}x)) = (x'q^{-1})(qy') \oplus yx
\]

\[
= \epsilon_A((x \oplus x')(y \oplus y')),
\]

as desired. Turning to the second part of the problem, we first note

\[
\text{Sym}(A^p \oplus A^q, \epsilon_A, p) = \{ (x, x) \mid x \in A \}.
\]

On the other hand, given \( x, x' \in A \), we have

\[
(\epsilon_A(x \oplus x')p)(x \oplus x') = ((x' \oplus x)(q^{-1} \oplus q^{-1}))(x \oplus x') = ((q^{-1}x') \oplus (xq^{-1}))(qq^{-1})(x \oplus x')
\]

\[
= x(q^{-1}x') \oplus (xq^{-1})(qx') = x(q^{-1}x') \oplus (xq^{-1})(qx').
\]

Combining, and using \([16.9.2]\), we obtain the following chain of equivalent conditions:

\[
\forall x, x' \in A: \ (\epsilon_A(x \oplus x')p)(x \oplus x') \in \text{Sym}(A^p \oplus A^q, \epsilon_A, p) \iff \forall x, x' \in A: \ (xq^{-1})(qx') = x(q^{-1}x')
\]

\[
\iff \forall x, x' \in A: \ (xq^{-1})(qx') = xx'
\]

\[
\iff A = A^p \iff q^2 \in \text{Nuc}(A).
\]

This solves the problem.

**Chapter 4**

**Section 19**

(a) We begin by deriving the following identities:

\[
n_c(x^2) = n_c(x)^2, \quad \text{(105) NOSQ}
\]

\[
n_c(x, x^2) = t_c(x)n_c(x), \quad \text{(106) NORASQ}
\]

\[
t_c(x^2) = t_c(x)^2 - 2n_c(x). \quad \text{(107) TRSQ}
\]

Indeed, the identities of \([19.5]\) yield \( n_c(x^2) = n_c(t_c(x)x - n_c(x)1_C) = t_c(x)^2n_c(x) - t_c(x)^2n_c(x) + n_c(x)^2 \), hence \([105]\), 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 \([106]\) and \( t_c(x^2) = t_c(t_c(x)x - n_c(x)1_C) = t_c(x)^2 - 2n_c(x) \) is \([107]\). Combining these identities with those of \([19.5]\) and writing \( y, z \in k[x] \) as \( y = \alpha_0 + \alpha_1x, y = \beta_0 + \beta_1x \) with \( \alpha_0, \alpha_1, \beta_0, \beta_1 \in k \), we now compute
37 Elementary idempotents and cubic Jordan matrix algebras

\[ n_C(\gamma z) - n_C(\gamma) n_C(z) = n_C((\alpha_1 x + \alpha_1 x)(t_0 1 e + \beta_1 x)) - n_C(\alpha_1 x + \alpha_1 x) n_C(t_0 1 e + \beta_1 x) \]
\[ = n_C(\alpha_1 t_0 1 e + (\alpha_1 t_0 1 e + \alpha_1 t_0 1 e) x + \alpha_1 \beta_1 x^2) \]
\[ - (\alpha_1^2 t_0^2 + \alpha_1 \alpha_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \alpha_1 \beta_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ = \alpha_1^2 t_0^2 + \alpha_1 \alpha_1 t_0 1 e(\alpha_1^2 t_0 1 e + \alpha_1 \beta_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ + (\alpha_1 \beta_1^2 + \alpha_1 \beta_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ - (\alpha_1^2 t_0^2 + \alpha_1 \alpha_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ = \alpha_1^2 t_0^2 + \alpha_1 \alpha_1 t_0 1 e(\alpha_1^2 t_0 1 e + \alpha_1 \beta_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ + (\alpha_1 \beta_1^2 + \alpha_1 \beta_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ - (\alpha_1^2 t_0^2 + \alpha_1 \alpha_1 t_0 1 e)(\alpha_1^2 t_0 1 e + \beta_1^2 t_0 1 e) \]
\[ = 0. \]

This completes the proof of (a).

(b) If \( x \) is invertible in \( k[x] \) with inverse \( x^{-1} \), then (a) yields

\[ n_C(x^n) n_C(x^{-1}) = n_C(1) = 1, \]

hence \( n_C(x) \in k^\times \). Conversely, if \( n_C(x) \in k^\times \), then \( y := n_C(x)^{-1} x \) by \([19,5,6]\) satisfies \( xy = 1 = yx \). Thus \( x \) is invertible in \( k[x] \) with inverse \( y \).

(c) If \( t_c(x), n_c(x) \in \text{Nil}(k) \), 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 \( x^0 = 0 \) 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 \( m := [\frac{n}{2}] + 1 > \frac{n}{2} \) 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 \([107]\)) and \( n_c(x)^2 = n_c(x)^2 \) (by \([105]\)) 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.

\[ n := n_C \circ \varphi : C \to k \] is a quadratic form such that \( Dn = (Dn_C) \circ (\varphi \times \varphi) \). Since \( \varphi \) preserves units, we conclude \( n(1_C) = 1 \) and \( i := (Dn)(1_C, -) = t_c \circ \varphi \). Now let \( x \in C \). Then

\[ \varphi(x^n - n(1_C)) = t_c(x^n) \varphi(x) - n_c(\varphi(x)) 1_C = \varphi(x)^2 - \varphi(x^2), \]

and since \( \varphi \) is injective, \( x^2 = t(x)x - n(1_C) \). 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.\([19,15]\)), 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 \( C := k \oplus k \), \( C' := k \) and \( \varphi : k \oplus k \to k \) be the projection onto the first summand. Then \([19,2\),(a),(b)\) yields \( n_k(\varphi(\alpha \oplus \beta)) = n_k(\alpha) = \alpha^2 \) for all \( \alpha, \beta \in k \), while \( n_k(\beta \oplus \alpha) = \alpha \beta \). Thus \( \varphi \) does not preserve norms, though being a unital algebra homomorphism, is not one of conic algebras.

(a) One verifies immediately that \( C \) is unital with identity element \( e \). Defining \( n_C : C \to k \) by

\[ n_C(\alpha e + x) := \alpha^2 + \alpha T(x) + B(x, x) \]

for \( \alpha \in k \), \( x \in M_k \), 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 $\alpha, \beta \in k, x, y \in M_k$. We have $n_C(e) = 1$, while $t_C := (Dn_C)(-, e)$ satisfies
\[ t_C(\alpha e + x) = 2\alpha + T(x) \]
for $\alpha \in k, x \in M_k$. Hence
\[
t_C(\alpha e + x)(\alpha e + x) - n_C(\alpha e + x)e = (2\alpha + T(x))(\alpha e + x) - (\alpha^2 + \alpha T(x) + B(x, x))e
= (\alpha^2 - B(x, x))e + ((\alpha + T(x))x + \alpha x)
= (\alpha e + x)^2,
\]
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 $M_k$, and (ii) $K$ is alternating. In order to establish (i), we let $x, y \in M_k = \ker(\lambda)$ and obtain
\[ \lambda(x \cdot y) = t_C(x)\lambda(y) - \lambda(xy)\alpha = -\lambda(xy) + \lambda(xy) = 0, \]
hence $x \cdot y \in M_k$. In order to establish (ii), we compute
\[ x \cdot x = t_C(x)x - x^2 + \lambda(x^2)e = n_C(x)e + \lambda(t_C(x)x - n_C(x)e)e = n_C(x)e - n_C(x)e = 0, \]
so $K$ is indeed alternating. We now denote by “−” the product in the conic algebra $C := Con(T, B, K)$ and obtain, for $\alpha, \beta \in k, x, y \in M_k$,
\[
(\alpha e + x) \cdot (\beta e + y) = (\alpha \beta + \lambda(xy))e + ((\alpha + t_C(x))y + \beta x - t_C(x)y + xy - \lambda(xy)e)
= \alpha \beta e + \alpha y + \beta x + xy = (\alpha e + x)(\beta e + y),
\]
\[ n_C(\alpha e + x) = \alpha^2 + \alpha t_C(x) - \lambda(x^2) = \alpha^2 + \alpha t_C(x) - t_C(x)\lambda(x) + n_C(x)\alpha(e)
= \alpha^2 + \alpha t_C(x) + n_C(x) = n_C(\alpha e + x). \]

Summing up, we have proved $C = Con(T_C, B_C, K_C)$. Finally, let $(T, B, K)$ be a conic co-ordinate system and $C := Con(T, B, K)$. Consulting the multiplication formula for $C$ (resp. the formula for the trace of $C$), we conclude
\[
T_C(x) = t_C(x) = T(x),
B_C(x, y) = -\lambda(xy) = B(x, y)
K_C(x, y) = t_C(x)y - xy + \lambda(xy)e = T(x)y - xy + \lambda(xy)e
= (B(x, y + \lambda(xy))e + (T(x)y - T(x)y + K(x, y)) = K(x, y),
\]
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.

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)
\[ 1_C \wedge y \wedge x^2 + 1_C \wedge x \wedge (x \circ y) = 0 \quad (x, y \in C). \tag{108} \]

Now put
\[ U := \{0\} \cup \{u \in \mathcal{C} \setminus k_1c \ | \ u^2 \in k_1c\} \tag{109} \]
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 $\alpha^2 1_C + 2\alpha \beta u + \beta^2 u^2 = \alpha 1_C + \beta u + \beta^2 u^2 = \alpha 1_C + \beta u$. 

\[ 1_C \wedge x \wedge x^2 + 1_C \wedge x \wedge (x \circ y) = 0 \quad (x, y \in C). \tag{108} \]

Now put
\[ U := \{0\} \cup \{u \in \mathcal{C} \setminus k_1c \ | \ u^2 \in k_1c\} \tag{109} \]

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 $\alpha^2 1_C + 2\alpha \beta u + \beta^2 u^2 = \alpha 1_C + \beta u + \beta^2 u^2 = \alpha 1_C + \beta u$. 

\[ 1_C \wedge x \wedge x^2 + 1_C \wedge x \wedge (x \circ y) = 0 \quad (x, y \in C). \tag{108} \]
Since conic algebras are stable under base change, they clearly satisfy the Dickson condition. Thus $1_C, u, v$ are linearly independent. On the other hand, setting $x = u, y = v$ (resp. $x = v, y = u$) in (108), and observing (109), 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 $n_C: C \to k$ 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

\[ n_C(\alpha 1_C + u, \beta 1_C + v) = 2\alpha \beta + n_C(u, v), \quad u \circ v = -n_C(u, v)1_C \quad (\alpha, \beta \in k, u, v \in U), \]

hence $t_C(\alpha 1_C + u) := n_C(1_C, \alpha 1_C + u) = 2\alpha$. Summing up, we obtain

\[
(\alpha 1_C + u)^2 = \alpha^2 1_C + 2\alpha u + u^2 = 2\alpha(\alpha 1_C + u) - (\alpha^2 + n_C(u))1_C
\
= w(\alpha 1_C + u)(\alpha 1_C + u) - n_C(\alpha 1_C + u)1_C. 
\]

Thus $C$ is a conic algebra over $k$ with norm $n_C$.

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

\[
C = k1_C \oplus M \tag{110}
\]

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 (110) give rise to quadratic maps $n: M \to k$ and $s: M \to M$ such that

\[
x^2 = s(x) - n(x)1_C \tag{111} \quad (x \in M). 
\]

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. 19.15 ensures that the norms $n_C$ glue to give a quadratic form $n: C \to k$. 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 $T = (t_i)_{i \in I}$ be a family of independent variables and write $k[T]$, for the corresponding polynomial ring. For a non-empty finite subset $E \subseteq I$, we consider the submodule

\[
M^E := \sum_{i \in E} k e_i \subseteq M \tag{112}
\]

which is a direct summand, and the element

\[
x^E := \sum_{i \in E} e_i \otimes t_i \in M^E_{k[T]} \subseteq M_{k[T]} \tag{113}
\]
We claim the annihilator of $x^6$ in $k[T]$ is zero; indeed, for $f(T) \in k[T]$ the relation $f(T)x^6 = 0$ implies $\sum c_i (t_i f(T)) = 0$, hence $t_i f(T) = 0$ for all $i \in E$ and then $f(T) = 0$ since $t_i$ is not a zero divisor in $k[T]$. Invoking the strict Dickson condition, we therefore find a unique polynomial $g(T) \in k[T]$ such that

$$s(x^6) = g(T)x^6.$$  

Specializing this relation with an additional variable $u$ to $uT$, we obtain $g(uT)ux^6 = u^5s(x^6) = (ug(T)u)x^6$, so the polynomial $g(T) \in k[T]$ is homogeneous of degree 1. Thus there exists a unique linear form $t^6 : M^6 \to k$ satisfying the relation $s(x) = t^6(x)x$ for all $x \in M^6$ because any such $t^6$ will be converted into the linear homogeneous polynomial $g(T)$ after extending scalars from $k$ to $k[T]$. Here the uniqueness condition implies that the linear forms $t^6$ as $E$ varies over the non-empty finite subsets of $I$ glue to give a linear form $t : M \to k$ such that $s(x) = t(x)x$ for all $x \in M$. Combining with (114), we obtain the relation

$$x^2 - t(x)x + n(x)1_C = 0$$  

for all $x \in M$. We now extend $t, n$ as given on $M$ to all of $C$ by

$$t(\alpha x + c) = 2\alpha + t(x), \quad n(\alpha x + c) = \alpha^2 + \alpha t(x) + n(x) \quad (\alpha \in k, x \in M)$$  

and then conclude from a straightforward computation that (114) holds for all $x \in C$. Since we also have $t = n(1C, \ldots)$, it follows that $C$ is a conic algebra.

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 (19.51) 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. 77 (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. 77 (b)), whence the relation $c(1_C - c) = 0$ implies $c = 1_C$, a contradiction. Hence $n_C(c) = 0$, and (19.51) 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 $p \subseteq k$, the ring $k_p$ is local, hence connected, and the first part of the problem yields $n_C(c)_p = n_{C_p}(c_p) = 0$, $t_C(c)_p = t_{C_p}(c_p) = 1_p$, and since this holds true for all $p \in \text{Spec}(k)$, condition (ii) 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 $R \in k\text{-alg}, R \neq \{0\}$, the elements $c_R$ and $1_C - c_R$ are both different from zero. Hence (i) holds.

We need an auxiliary 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 $a_1, \ldots, a_m \in I$ generate $I$ as an ideal and let $p \in \mathbb{Z}$, $p > 0$, satisfy $a_i^p = 0$ for all $i = 1, \ldots, m$. For any positive integer $n$, the ideal $I^n \subseteq k$ is generated by the expressions $a_1^i \cdots a_m^i$, where $1 \leq i_1 \leq \cdots \leq i_m \leq n$. If for all $i = 1, \ldots, m$, $q_i := \lfloor j \in \mathbb{Z}[1 \leq j \leq n, i_j = i] \rfloor \leq p - 1$,

then $n = \sum_{i=1}^{m} q_i \leq m(p-1)$. Thus for $n > m(p-1)$, some $i = 1, \ldots, m$ has $q_i \geq p$. But this implies first $a_{i_1} \cdots a_{i_p} = 0$ and then $I^n = \{0\}$. □

In the situation of our exercise, an element $x \in IC$ actually belongs to $I'C$ for some ideal $I' \subseteq C$ which is finitely generated and belongs to $I$. Hence $x^6 \in I'C$ for all positive integers $n$, where by the lemma $I'^n$ will eventually be zero. Thus $x$ is nilpotent, and we have shown that $IC \subseteq C$ is a nil ideal. By 8 (Exercise 31) therefore, we find an idempotent $c \in C$ satisfying $c = c'$. We claim that $c$ is elementary, i.e., by 19 (Exercise 82) that $n_C(c) = 0$ and $t_C(c) = 1$. Passing to the base change
from $k$ to $\tilde{k}$, we conclude

$$nc(c) = ne(c') = 0, \quad tc(c) = tc'(c') = 1_k,$$

hence $nc(c) \in I, tc(c) \in 1 + I \subseteq k^\times$ since $I \subseteq k$ is a nil ideal. Thus, thanks to Exercise 19, Exercise 77(a), $nc(c) \in k$ is a nilpotent idempotent, forcing $nc(c) = 0$, and applying the trace formula (115) for $x = c$, we see that $tc(c) \in k$ is an invertible idempotent, forcing $tc(c) = 1$. Summing up, $c$ is an elementary idempotent of $C$.

We begin with a short digression: let $e \in k$ be an idempotent. Then $R := k\epsilon$ becomes a member of $k\text{-alg}$ with identity elements $1_k = \epsilon$ and $k$-algebra structure given by the homomorphism $\alpha \mapsto \alpha \epsilon$ from $k$ to $R$. For a $k$-module $M$, scalar multiplication $k \times M \to M$ restricts to a bi-additive map $R \times E M \to E M$ making $E M$ an $R$-module. We claim that there is a natural identification $M_R = \epsilon M$ as $R$-modules such that $xR = x \otimes \epsilon = \epsilon x$ for all $x \in M$. In order to see this, we note that the map $x \mapsto \epsilon x$ from $M$ to $E M$ is $k$-linear, hence gives rise to an $R$-linear map $M_R \to \epsilon M$ satisfying $xR = x \otimes \epsilon = \epsilon x$. This map is clearly surjective, and it suffices to show that it is injective as well. Accordingly, let $x \in M$ and assume $\epsilon x = 0$. Then, setting $\epsilon' := 1 - \epsilon$, we have $xR = \epsilon x = \epsilon' x = \epsilon x = (\epsilon' \epsilon) x = 0$, as desired.

Returning now to the exercise itself, we prove (ii) $\Rightarrow$ (i). Obvious.

(i) $\Rightarrow$ (ii). If $c \in C$ is an idempotent, then (19.5.1) implies $tc(c) = tc(c)^2 = 2nc(c)$, hence

$$tc(c)(1 - tc(c)) = -2nc(c).$$

The quantities $\epsilon^{(i)}$, $i = 0, 1, 2$, as defined above obviously satisfy $\sum \epsilon^{(i)} = 1$, while the fact that $nc(c) \in C$ is an idempotent by Exc. 77(a) combined with (115) implies $\epsilon^{(i)} \epsilon^{(j)} = 0$ for $i, j = 0, 1, 2$ distinct. Thus they form a complete orthogonal system of idempotents in $k$. Our preliminary remark shows $C^{(i)} = C^{(j)}$ and $\epsilon = \sum \epsilon^{(i)}$, where $\epsilon^{(i)} = \epsilon^{(i)}(\epsilon)$ for $i = 0, 1, 2$. We now compute $\epsilon^{(0)} = \epsilon^{(0)}c = (1 - nc(c))(1 - tc(c))c$, where $(1 - tc(c))c = c^2 - tc(c)c = -nc(c)c$, which implies $\epsilon^{(0)} = 0$. Next we turn to

$$c^{(1)} = \epsilon^{(1)}c = (1 - nc(c))tc(c)c = (1 - nc(c))(c + nc(c)1_c) = (1 - nc(c))c,$$

which together with (115) implies

$$tc(c^{(1)}) = \epsilon^{(1)}tc(c) = (1 - nc(c))tc(c)^2 = (1 - nc(c))(tc(c) + 2nc(c))$$

$$= (1 - nc(c))tc(c) = \epsilon^{(1)} = 1_{C^{(1)}},$$

$$nc(c^{(1)}) = \epsilon^{(1)}nc(c) = (1 - nc(c))tc(c)nc(c) = 0.$$

Thus $c^{(1)} \in C^{(1)}$ is an elementary idempotent. Finally,

$$e^{(2)} = \epsilon^{(2)}c = nc(c)c,$$

which implies $nc(e^{(2)}) = \epsilon^{(2)}nc(c) = \epsilon^{(2)} = 1_{C^{(2)}}$. Thus $e^{(2)} \in C^{(2)}$ is an invertible idempotent in the sense of Exc. 77(b), forcing $e^{(2)} = 1_{C^{(2)}}$, as claimed. The statement just proved implies $tc(c^{(2)}) = 2$ in $k^{(2)}$. This can also be proved directly by noting

$$(2 - tc(c))\epsilon^{(2)} = 2nc(c) - tc(c)nc(c) = nc(c)\epsilon^{(2)} - tc(c)nc(c)$$

which is zero by (106) of the solution to Exc. 77.

It remains to prove uniqueness of the $\epsilon^{(i)}$, $i = 0, 1, 2$, be any complete orthogonal system of idempotents in $C$ satisfying mutatis mutandis the conditions of (ii), and define the $\epsilon^{(i)}$, $i = 0, 1, 2$, as in 19. Then $nc(e^{(i)}) = nc(\eta^{(i)}c) = \eta^{(i)}nc(c) = nc(c)_{\eta^{(i)}} = n_{c^{(1)}}(\epsilon^{(i)})$ and, similarly,
If \( C \) is a conic \( k \)-algebra with trivial conjugation, then \( 2x = t_C(x)1_C \) for all \( x \in C \) by (116).

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.

### 6. Cubic Jordan algebras

For the subsequent computations it is important to note

\[
(\alpha \beta_0)e = (\alpha \beta_0)e \quad (\alpha \in k, \beta_0 \in k_0)
\]

since, for \( \alpha = \alpha_0 + \alpha_3 \in k_0 \), the right-hand side becomes \((\alpha_0 \beta_0 + (\alpha_3 \beta_0))e = (\alpha_0 \beta_0)e = (\alpha \beta_0)e \), as claimed.

Turning to the exercise itself, we begin by showing associativity. Writing \( (e_1)_{1\leq i\leq 3} \) for the canonical basis of \( k_0^3 \) over \( k_0 \), we deduce from (1) that \([k_0^3, k_0^3] = k_0 \alpha, k_0^3 \) is a conic algebra.

Now let \( \alpha, \beta, \gamma \in k \) and \( u, v, w \in k_0^3 \).

Then

\[
(\alpha \beta)(v \gamma + w) = (\alpha \beta) v \gamma + \beta w + \gamma u, v + \alpha u, v + \gamma w + v, w
\]

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 \( 1_C = 1 \oplus 0 \), and the quadratic form \( n_t \) obviously satisfies \( n_t(1_C) = 1 \). Moreover, (116) yields

\[
n_t(\alpha \beta \gamma) = \alpha^2 + (\alpha \beta \gamma)e \quad (\alpha \in k, \beta, \gamma \in k_0^3),
\]

and we have

\[
n_t(\alpha \beta \gamma + \beta v + \gamma u) = 2\alpha \beta + (\alpha \beta \gamma + \beta v + \gamma u)e \quad (\alpha, \beta, v, \gamma \in k_0^3),
\]

hence

\[
t_2(\alpha \beta) := n_t(1_C, \alpha \beta) = 2\alpha \beta + (\alpha \beta \gamma)e.
\]

Comparing

\[
(\alpha \beta \gamma)e = \alpha^2 + 2(\alpha \beta \gamma)e
\]

with

\[
\]
we see that \( C \) is indeed a conic \( k \)-algebra with norm \( n_c \) and trace \( t_c \). We now turn to the equivalence of (i)–(iv). By Props. 20.2 and 19.13, 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 \( \text{Ann}(C) = \{0\} \), we conclude from Prop. 19.9 that \( t_c(xy) = n_c(x, \bar{y}) \) 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 (116) and obtain

\[
t_c(xy) = t_c((\alpha \beta) \oplus (\alpha v + \beta u + [u, v])) = 2\alpha \beta + (\bar{\alpha} (\bar{\alpha} v + \beta u + [u, v]))e
\]

\[
= 2\alpha \beta + (\bar{\alpha} (\bar{\alpha} v + \beta u + [u, v]) + \bar{\alpha} \bar{\alpha} e + \bar{\alpha} \beta u + \beta \bar{\alpha} v + \bar{\alpha} [u, v])e,
\]

\[
\bar{y} = t_c(\beta \oplus v)1_C - (\beta \oplus v) = (2\beta + (\beta v)e)(1 \oplus 0) - (\beta \oplus v) = (\beta + \beta v)e \oplus (\beta v)e + (\beta v)e \oplus (\beta v)e + (\beta v)e \oplus (\beta v)e,
\]

\[
n_c(x, \bar{y}) = n_c((\alpha \oplus u, \beta + \beta v)e \oplus (\beta v)e) = 2\alpha \beta + 2\alpha \bar{\alpha} e + \bar{\alpha} \beta u + \beta \bar{\alpha} v + \bar{\alpha} [u, v]e + \alpha e \oplus \beta \beta v e
\]

Comparing, we conclude \( \beta' [u, v] = 0 \) for all \( u, v \in k_0^3 \), and specializing \( u = e_1, v = e_2, (e_i)_{1 \leq i \leq 3} \) being the \( k_0 \)-basis of unit vectors in \( k_0^3 \), yields \( \delta = 0 \), hence (iv).

(iv) \( \Rightarrow \) (i). For \( \alpha, \beta \in k, u, v \in k_0^3 \), we compute

\[
n_c((\alpha \oplus u)(\beta \oplus v)) = n_c((\alpha \beta) \oplus (\alpha v + \beta u + [u, v]))
\]

\[
= (\alpha \beta)^2 + ((\alpha \beta \beta)^2 \bar{u} + (\alpha \beta \beta)^2 \bar{v} + (\alpha \beta \beta)^2 [u, v])e,
\]

\[
n_c(\alpha \oplus u)n_c(\beta \oplus v) = (\alpha^2 + (\alpha \bar{u})e)((\beta^2 + (\beta \bar{v})e)
\]

\[
= \alpha^2 \beta^2 + (\alpha \beta \beta)^2 \bar{v} + \alpha \beta \beta)^2 \bar{u}e.
\]

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 \( u \) by (iv). Hence \( \beta' [u, v] = 0 \), and we conclude that \( n_c \) permits composition, i.e., the conic algebra \( C \) with norm \( n_c \) is multiplicative.

\[\text{sol.NIRA}\] By Prop. 20.2(a), \( C \) is norm-associative. We put

\[N := \{x \in C \mid n_c(x), n_c(x, y) \notin \text{Nil}(k) \text{ for all } y \in C\}\]

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 \( x, y, z \in C \). By multiplicativity, \( n_c(xy) = n_c(x)n_c(y) \) is nilpotent, while norm-associativity yields the same for \( n_c(zx) = n_c(z)n_c(x) \) and \( n_c(zy) = n_c(z)n_c(y) \). Thus \( x \) and \( z \) 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. 77(c). Hence \( N \subseteq C \) is a nil ideal and as such contained in the nil radical. Conversely, let \( x \in \text{Nil}(C) \). Then \( x \) is nilpotent, as is \( x \bar{y} \in \text{Nil}(C) \) for all \( y \in C \). Consulting Exc. 77(c) again, we see that \( n_c(x) \) and \( n_c(x, y) = t_c(x \bar{y}) \) belong to \( \text{Nil}(k) \), which implies \( x \in N \) and completes the proof.

\[\text{sol.ARTCONALG}\] For the first part we must show that the submodule \( M \) of \( C \) spanned by the elements \( I_C, x, y, xy \) 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 19.5 and 20.12 to obtain...
\[ z^2 = t_c(z)z - n_c(z)1_c \in M \quad (z \in \{x, y, xy\}), \]
\[ x(xy) = x^2y = t_c(x)xy - n_c(x)y \in M, \]
\[ (xy)x = n_c(x,y)x - n_c(x)y = n_c(x,y)x - n_c(x)tc(y)x + n_c(x)y, \]
\[ xy = x \circ y - xy = t_c(x)y + t_c(y)x - n_c(x,y)1_c - xy \in M. \]

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. 

Abbreviating \( 1 := 1_c, n := n_c, t := t_c \) and expanding the norm of an associator, we obtain
\[
n([x_1, x_2, x_3]) = n((a_1 x_2) x_3) - n((a_1 x_2) x_3, x_1 (x_2 x_3)) + n((x_1 x_2) x_3),
\]
where multiplicity of the norm yields
\[
n((a_1 x_2) x_3) = 2n(x_1)a(n(x_2)n(x_3) - n((a_1 x_2) x_3, x_1 (x_2 x_3))). \tag{117} \]

Turning to the second summand on the right of (117), we obtain, by (20.11),
\[
n((a_1 x_2) x_3, x_1 (x_2 x_3)) = n(x_1 x_2, x_1)n(x_3, x_2 x_3) - n((a_1 x_2) (x_3 x_2), x_1 x_3).
\]

Since \( C \) is norm associative by Prop. 20.2, we may apply (19.11.2) to the first summand on the right, which yields
\[
n((a_1 x_2) x_3, x_1 (x_2 x_3)) = t(x_2)^2 n(x_3)n(x_1) - n((a_1 x_2) (x_3 x_2), x_1 x_3). \tag{118} \]

Manipulating the expression \( (a_1 x_2) (x_3 x_2) \) by means of (19.5.5) and the middle Moufang identity (14.3.3), we obtain
\[
(a_1 x_2) (x_3 x_2) = (x_1 x_2) \circ (x_2 x_3) - (x_2 x_3)(a_1 x_2)
= t(x_1 x_2) x_2 x_3 + t(x_2 x_3)x_1 x_2 - n(x_1 x_2, x_2 x_3)1 - x_2(x_3 x_2)x_2,
\]
where associativity of the trace (19.12), and (19.11), (20.3) yield
\[
(x_1 x_2) (x_3 x_2) = t(x_1 x_2) x_2 x_3 + t(x_2 x_3)x_1 x_2 - n(x_1 x_2, x_2 x_3)1 - t(x_1 x_2 x_3 x_2) + n(x_2)\tag{119}.
\]

Here we use (19.11), (19.5.5) to compute
\[
n(x_1 x_2, x_3 x_2) = n(x_1, x_2) x_3 x_2 = t(x_2) n(x_1, x_2 x_3) - n(x_1, x_2 x_3),
\]
and (19.11), (20.3) give
\[
n(x_1 x_2, x_3 x_2) = t(x_2) n(x_1, x_2 x_3) - t(x_2 x_3) n(x_1, x_2) + t(x_3) n(x_2)
= t(x_1) r(x_2) r(x_2 x_3) - t(x_2) r(x_1 x_2 x_3) - t(x_1) r(x_2) r(x_2 x_3) + t(x_1 x_2) r(x_2 x_3) + t(x_3) n(x_2),
\]
hence
\[
n(x_1 x_2, x_3 x_2) = t(x_1) r(x_2 x_3) - t(x_2) r(x_1 x_2 x_3) + t(x_3) n(x_2).
\]

Inserting this into (119), and (119) into the second term on the right of (118), we conclude
From Prop. 16.3 combined with 16.7 we deduce that

\[ n((x_1 x_2)(x_2 x_3), x_1 x_3) = t(x_1 x_2)n(x_2 x_1, x_1 x_3) + t(x_2 x_3)n(x_1, x_2 x_3) - t(x_1 x_2)n(x_1 x_2, x_1 x_3) - t(x_2 x_3)n(x_1, x_2 x_3) + n((x_2 x_3), x_1 x_3)n(x_2) \]

Thus

\[ \iota((x_1 x_2)(x_2 x_3))n(x_2 x_1, x_1 x_3) + \iota((x_2 x_3))n(x_1, x_2 x_3) - \iota((x_1 x_2))n(x_1 x_2, x_1 x_3) - \iota((x_2 x_3))n(x_1, x_2 x_3) + n((x_2 x_3), x_1 x_3)n(x_2), \]

where we may use \([19.12]\), \([19.5]\), \([19.11]\) to expand

\[ t(x_1 x_2)x_3n(x_2) = t(x_1 x_2)(x_3)n(x_2) \]

Inserting the resulting expression

\[ n((x_1 x_2)(x_2 x_3), x_1 x_3) = \sum t(x_1 x_2)x_1((x_2)n(x_2)) - t(x_1 x_2)x_1((x_2)n(x_2)) \]

into \([118]\) and \([119]\) into \([117]\), the assertion follows.

From Prop. 16.3 combined with 16.7 we deduce that \(C_{(\rho_0)}\) is a unital alternative \(k\)-algebra with identity element \(I_{C_{(\rho_0)}} = (pq)^{-1}\). Defining \(n_{C_{(\rho_0)}} := nC_{(pq)nC}\), Prop. 20.4 yields \(n_{C_{(\rho_0)}}(1_{C_{(\rho_0)}}) = 1\), and we have \(n_{C_{(\rho_0)}}(x, y) = nC_{(pq)nC}(x, y)\) for all \(x, y \in C\), which implies

\[ t_{C_{(\rho_0)}}(x) := n_{C_{(\rho_0)}}(1_{C_{(\rho_0)}}, x) = nC_{(pq)nC}(1_{C_{(\rho_0)}}^{-1}, x) = nC_{(pq)}(x, x). \]

Writing \(x^{(m, \rho_0)}\) for the \(m\)-th power of \(x \in C\) in \(C_{(\rho_0)}\), we apply \([16.2]\), the middle Moufang identity \([14.3]\) and \([20.3]\) to conclude

\[ x^{(2, \rho_0)} = (xp)(qx) = x(pq)x = nC_{(pq)}(x, x) = nC_{(pq)}(x) = t_{C_{(\rho_0)}}(x)x - n_{C_{(\rho_0)}}(x)1_{C_{(\rho_0)}}. \]

Thus \(C_{(\rho_0)}\) is a conic alternative \(k\)-algebra with norm and trace as indicated. Moreover,

\[ t_{C_{(\rho_0)}}(x) = t_{C_{(\rho_0)}}(x)1_{C_{(\rho_0)}} - x = nC_{(pq)}(x) - nC_{(pq)}(x)1_{C_{(\rho_0)}} = nC_{(pq)}(x)1_{C_{(\rho_0)}} - x = nC_{(pq)}(x)1_{C_{(\rho_0)}} = nC_{(pq)}(x)1_{C_{(\rho_0)}}, \]

giving the desired formula for the conjugation of \(C_{(\rho_0)}\). Finally, if \(C\) is multiplicative, then
for all \( x, y \in C \), and \( C^{(p,q)} \) is multiplicative as well.

By Prop. 20.2 the conjugation of \( C \) is an involution, and since \( q \) has trace zero, we have 
\[ q = -q. \]
Hence Lemma 17.3 shows that \( (C, \tau, q) \) is an alternative algebra with isotopy involution of negative type, i.e., an object of the category \( \text{alist} \) with \( \varepsilon = -\). By the solution to Exc. 75 the pointed alternative \( k \)-algebra with involution corresponding to \( (C, \tau, q) \) is
\[ \Psi((C, \tau, q)) = ((C^p, \tau^p), q), \]
where Prop. 20.4 yields \( p := q^{-1} = n_C(q)^{-1} \tau q = -n_C(q)^{-1} q \), hence \( C^p = C^q \). Similarly, Eq. 17.2 implies \( \tau^p = \tau^q \) and since \( \tau(q) = -q \), we deduce from Eq. 17.2 again that
\[ \tau^q(x) = -q^{-1} \tau(qx) = -q^{-1}(q^{-1} \tau(q)) = q^{-2} x q^{-1} = \bar{x} \]
for all \( x \in C \) since \( q^{1/2} \in k \). Thus \( \tau^p = \tau^q = \tau \), and we conclude that the pointed alternative algebra with involution corresponding to \( (C, \tau, q) \) via Exc. 75 is \( ((C^q, \tau), q) \). But actually it is also \( ((C, \tau), q) \) since we have an isomorphism
\[ \phi: ((C, \tau), q) \rightarrow ((C^q, \tau), q), \quad x \mapsto q^{-1} x q. \]
Indeed, \( \phi \) obviously fixes \( q \), and since \( q^3 = q^2 q = -n_C(q) q \), we have \( C^q = C^q \), forcing \( \phi: C \rightarrow C^q \) by Exc. 72 (b) to be an isomorphism such that
\[ \phi(x) = q \bar{x} q^{-1} = q \bar{x} q^{-1} = q^{-1} x q = \phi(x) \]
for all \( x \in C \). Thus \( \phi: (C, \tau) \rightarrow (C^q, \tau) \) is an isomorphism of alternative algebras with involution, as claimed.

Section 21

We put \( C := \text{Cay}(B, \mu) \) and let \( u_1, u_2, v_1, v_2 \in B \). Using the fact that \( B \) is norm associative by Prop. 20.7 (a) and applying 21.3 (1), we obtain
\[ n_C((u_1 + v_1)(u_2 + v_2)) = n_C((u_1 u_2 + \mu v_2 v_1) + (v_1 u_2 + v_2 u_1)) \]
\[ = n_B(u_1 u_2 + \mu v_2 v_1) - \mu n_C(v_1 u_2 + v_2 u_1) \]
\[ = n_B(u_1) n_B(u_2) + \mu n_B(u_1 u_2, v_2 v_1) + \mu^2 n_B(v_2) n_B(v_1) \]
\[ - \mu n_B(v_1) n_B(u_2) - \mu n_B(v_1 u_2, v_2 u_1) - \mu n_B(v_2 u_1) n_B(u_1) \]
\[ = (n_B(u_1) - \mu n_B(v_1)) (n_B(u_2) - \mu n_B(v_2)) \]
\[ + \mu n_B(v_2(u_1, u_2), v_1) - \mu n_B(v_2, [v_1, u_1 u_2]) \]
\[ = n_B(u_1 + v_1) n_B(u_2 + v_2) - \mu n_B([v_2, u_1 u_2], v_1), \]
from which the assertion can be read off immediately.

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. 20.2 (a) to compute
\[
\varphi(u_1 + v_1 j) \varphi(u_2 + v_2 j) = \left[(u_1 + (av_1)) + (u_2 + (av_2))\right] \\
= (u_1 u_2 + \mu a v_1) + ((av_2)u_1 + (av_1)a_2) + (u_2 v_1 + (v_2 u_1 + v_1 a_2)) \\
= \varphi\left((u_1 u_2 + n_{\phi}(a) a v_1) + (u_2 v_1 + v_1 a_2)\right) \\
= \varphi\left((u_1 + v_1 j)(u_2 + v_2 j)\right).
\]

Thus \(\varphi\) is an obviously unital algebra homomorphism. Moreover, setting \(C := \text{Cay}(B, n_{\phi}(a) \mu), \)
\(C' := \text{Cay}(B, \mu),\) we have, for all \(u, v \in B,\)
\[n_{C'} \circ \varphi(u + v j) = n_{C'}(u + (av) j) = n_{\phi}(u) - \mu n_{\phi}(v) = n_{C}(u) - n_{C}(v) \mu n_{\phi}(v) \]
since \(B\) is multiplicative. Thus \(\varphi\) is a homomorphism of conic algebras. The final statement is obvious.

\(\text{sol.ZERDIV}\) \(\text{sol.VARCD}\)
\( \Psi: \text{Cay}(B, \mu)^{op} \longrightarrow \text{Cay}(B^0, \mu), \quad u + vj \mapsto u + \bar{v}j, \)

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 \( \text{Cay}(B, \mu)^{op} \), we obtain, for all \( u_1, u_2, v_1, v_2 \in B \),

\[
\Psi(u_1 + v_1 j)\Psi(u_2 + v_2 j) = (u_1 + \bar{v}_1 j)(u_2 + \bar{v}_2 j) = (u_1 \cdot u_2 + \mu v_2 \cdot \bar{v}_1) + (\bar{v}_2 \cdot u_1 + \bar{v}_1 \cdot \bar{u}_2) j
\]

\[
= (u_2 u_1 + \mu \bar{v}_1 v_2) + (u_1 \bar{v}_2 + \bar{u}_2 \bar{v}_1) j
\]

\[
= (u_2 u_1 + \mu \bar{v}_1 v_2) + (u_1 \bar{v}_2 + v_1 \bar{u}_2) j
\]

\[
= \Psi([u_2 u_1 + \mu \bar{v}_1 v_2] + (u_1 \bar{v}_2 + v_1 \bar{u}_2) j)
\]

\[
= \Psi([u_2 + v_2 j]([u_1 + v_1 j]) = \Psi([u_1 + v_1 j] \cdot (u_2 + v_2 j) j),
\]

as claimed. Combining we obtain an isomorphism

\[ \phi \circ \Psi: \text{Cay}(B, \mu)^{op} \longrightarrow \text{Cay}^\prime(B, \mu)^{op}, \]

hence an isomorphism

\[ \phi \circ \Psi: \text{Cay}(B, \mu) \longrightarrow \text{Cay}^\prime(B, \mu), \quad u + vj \mapsto u + j^\prime \bar{v}, \]

of conic algebras.

**Section 22**

(i) \( \Rightarrow \) (ii). Since \((C, n, 1_C)\) by \(22.1.3\) is a pointed quadratic module, the implication follows from Lemma \(12.1.5\).

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

(iii) \( \Rightarrow \) (i). By \(22.1.2, 22.1.3\), the quantity \( \epsilon := n(1_C) \in k \) is an idempotent with \( \epsilon n(x) = n(x) \) for all \( x, y \in C \). Therefore the idempotent \( \epsilon' := 1 - \epsilon \in k \) satisfies \( n(\epsilon' 1_C) = \epsilon' \epsilon = 0, n(\epsilon' 1_C, y) = \epsilon' \epsilon n(1_C, y) = 0 \) for all \( y \in C \), which implies \( \epsilon' 1_C = 0 \) by non-degeneracy of \( n \), hence \( \epsilon' = 0 \) since \( 1_C \) is faithful. Thus \( n(1_C) = 1 \).

**Conil.** Let \( K \) be a unital \( F \)-algebra of dimension 2. Then \( K \) is quadratic, hence commutative associative \( [19.4] \), and we have \( K = F[u] \) for any \( u \in K \setminus F1K \). Writing \( \mu_u \in F[t] \) 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 \( \mu_u = (t - \alpha)(t - \beta) \) for some \( \alpha, \beta \in F, \alpha \neq \beta \). Here the Chinese Remainder Theorem \( [65, II, Cor. 2.2] \) implies

\[ K \cong F[t]/(\mu_u) \cong F[t]/(t - \alpha) \oplus F[t]/(t - \beta) \cong F \oplus F \]

as a direct sum of ideals, and we are in Case (ii).

3. \( \mu_u \) is irreducible and inseparable. Then \( \text{char}(F) = 2 \) and \( K/F \) is an inseparable quadratic field extension. Hence we are in Case (iii).

4. \( \mu_u \) is reducible and inseparable. Then \( \mu_u = (t - \alpha)^2 \) 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 \( F[e] \to K \) sending \( e \) 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 \( \text{Ker}(t_C) = F1C \), where the inclusion “\( \supseteq \)” is obvious. Conversely, let \( u \in \text{Ker}(t_C) \) and assume \( u \notin F1C \). 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) hold, then the trace of \( K \) kills \( 1_k = 1_C \) but is not identically zero. Thus \( \text{Ker}(t_k) = F1C \), forcing \( t_k(u) = t_k(u) \neq 0 \), 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.
We first show that \( C \) is a division algebra, then \( C \) is a commutative \( \mathbb{C} \)-algebra and hence is a unital \( A \)-algebra. Here Prop. 11.5 shows that either \( C \) is a division algebra, then \( \mathbb{C} \) is a non-zero scalar, \( \mathbb{C} \) is anisotropic, forcing \( C \) to be an octonion algebra over \( \mathbb{C} \), and \( \mathbb{C} = \text{Cay}(B, \mu) \).

(a) Isotropic non-singular quadratic forms over \( F \) are known to be universal. The assumption \( \mu \notin n_B(B^*) \) therefore implies that \( n_B \) is anisotropic, forcing \( B \) to be an octonion division algebra by Thm. 22.8 combined with Prop. 20.4. Now 21.31 implies

\[
x_1x_2 = (u_1u_2 + \mu \bar{v}_1v_1) + (v_2u_1 + \bar{v}_1u_2),
\]

and we conclude

\[
x_1x_2 = 0 \iff u_1u_2 = -\mu \bar{v}_1v_1, \quad v_2u_1 = -\bar{v}_1u_2.
\]

Suppose first \( x_1x_2 = 0 \). If \( u_1 = 0 \), then \( v_1 \neq 0 \) and (120) implies \( v_2 = u_2 = 0 \), hence \( x_2 = 0 \), a contradiction. Thus \( u_1 \neq 0 \). If \( u_2 = 0 \), then (120) again implies \( v_2 = 0 \). This contradiction shows \( u_2 \neq 0 \). Since \( B \) is a division algebra, the first equation of (120) now implies \( v_1 \neq 0 \). We have thus shown \( u_i \neq 0 \neq v_i \) for \( i = 1, 2 \). Next, since the norm of \( B \) is multiplicative, (120) yields first

\[
n_B(u_1)n_B(u_2) = \mu^2n_B(v_1)n_B(v_2) \quad \text{and}
\]

\[
n_B(u_1)^2n_B(u_2) = \mu^2n_B(v_1)^2n_B(v_2).
\]

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 \( \mu \in n_B(B^*) \). Hence (i) holds. Turning to (ii), we use (120), (i) and Kirmse’s identities (20.31) to compute

\[
(u_1u_2)v_1 = -\mu(\bar{v}_1v_1) - \mu n_B(v_1)v_2 = n_B(u_1)v_2 = u_1(\bar{u}_1v_2) = -u_1v_1u_2 = -u_1(u_2v_1),
\]

and this is (ii). Finally, (iii) is equivalent to the second equation of (120). Conversely, suppose \( u_i \neq v_i \) for \( i = 1, 2 \) and (i)–(iii) hold. Then so does the second equation of (120), and (i), (ii) imply

\[
(u_1u_2)v_1 = -u_1(u_2v_1) = -u_1v_1u_2 = u_1(\bar{u}_1v_2) = n_B(u_1)v_2 = -\mu n_B(v_1)v_2 = -\mu(\bar{v}_1v_1)v_1.
\]

But \( \bar{v}_1 \), being different from zero, is invertible in \( B \). Hence the first equation of (120) 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 \( n_C = n_B \oplus (-\mu)n_B \) (cf. Remark 21.4) is anisotropic. Assuming \( \mu = n_B(u) \) for some \( u \in B^* \) would lead to the contradiction \( n_C(u + j) = 0 \). Thus \( \mu \notin n_B(B^*) \). If \( C \) were not a division algebra, some \( x_i = u_i + v_i, \quad u_i, v_i \in B, \quad i = 1, 2 \), 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 \( x, y \in A, z \in A^+ \) for some quaternion subalgebra \( A \subseteq B \) and \( x \circ y = 0 \). Equivalently, \( xy = -yx \). Then we may identify \( B = \text{Cay}(A, v) = A \oplus Ai \) for some non-zero scalar \( v \in F \) (Thm. 22.15 (b)) and have \( A^+ = Ai \), hence \( z = wi \) for some \( w \in A \). Now we use (21.3.11) and compute

\[
(xy)z = (xy)(ui) = (uxy)i,
\]

\[
x(yz) = x(y(wi)) = x((uv)i) = (uxy)i = -(uxy)i.
\]

Hence \((xy)z = -x(yz)\), as desired. Conversely, let this be so. Since \( \text{char}(F) \neq 2 \) 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 non-singular. Since, therefore, \( A \) is a composition algebra of dimension at least 3 and at most 4 (Exc. \( \ref{exc:composition-algebra} \)), it must, in fact, be a quaternion algebra. As before, we may assume \( B = \text{Cay}(A, v) = A \oplus Ai \) for some \( v \in F^+ \). Then \( z = u + vi, u, v \in A \), and we conclude

\[
(xy)z = xyu + (uxy)i,
\]

\[
-x(yz) = -x(yw + (vy)i) = -xyu - (vyx)i.
\]

Comparing coefficients, this implies \( xyu = v(x \circ y) = 0 \), hence \( u = 0 \). But then \( v \neq 0 \), forcing \( x \circ y = 0 \) and \( z = vi \in A^+ \).

(d) Suppose first that \( C \) is a division algebra. Then its norm is anisotropic, and we have seen in (b) that this implies \( \mu \notin n_B(B^+) \). Assume now \( -\mu = n_B(z) \) for some element \( z \in B \) of trace zero. Pick any non-zero element \( y \in F[z] \) 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 \( x \in A'^+ \subseteq F[y] \). 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) \( n_B(z, xy) = n_B(z, y) \in n_B(A', x) = 0 \). Thus \( z \in A^+ \), while \((19.5.5)\) yields \( x \circ y = 0 \). Setting \( u_i := x, \)

\[
u_3 := y, v_1 := u_3 z^{-1} = -n_B(z^{-1})u_3 \in A^+, v_2 := -v_1 u_2 \in A^+, \]

we have \( v_1 = -v_1 \in A^+ \), whence it is clear that conditions (i)–(iii) of (a) hold. Hence (a) produces zero divisors in \( C \), a contradiction.

Conversely, suppose \( \mu \notin n_B(B^+) \), \( -\mu \notin n_B(B^+ \cap B^+) \). 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 \( u_1, u_2 \in A, v_1 \in A^+ \) and \( u_1 \circ u_2 = 0 \). This would imply \( v_1 = -v_1 \in A^+ \) and \( -\mu = n_B(z), z := u_1 v_1^{-1} \in A^+ \), and, in particular, \( l_B(z) = 0 \). This contradiction completes the proof.

(e) The algebra in question is the same as \( \text{Cay}(\mathbb{O}, -1) \). 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 \( \mathbb{O} \).

---

**sol.FROBTHE**

100 Let \( C \) be a finite-dimensional alternative division algebra over \( \mathbb{R} \). Then Exc. \( \ref{exc:finite-dim-alternative} \) 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 \( 1_x, x, x^2 \) are linearly dependent over \( \mathbb{R} \), and we deduce from Exc. \( \ref{exc:conic-algebra} \) that \( C \) is a conic algebra. Since the non-zero elements of \( C \) are invertible, Prop. \( \ref{prop:invertible-elements} \) 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. \( \ref{thm:composition-algebra} \) shows that \( C \) is a composition division algebra over \( \mathbb{R} \). By Cor. \( \ref{cor:composition-algebra} \), therefore, \( C \cong \text{Cay}(\mathbb{R}, \alpha_1, \ldots, \alpha_n) \) for some \( n = 0, 1, 2, 3 \) and \( \alpha_1, \ldots, \alpha_n \in \mathbb{R}^+ \). Here the assumption \( \alpha > 0 \) for some \( i = 0, \ldots, n \) would contradict Remark \( \ref{rem:positive-definite} \) in conjunction with the property of \( n_C \) to be positive definite. Thus \( \alpha_i < 0 \) for \( 0 \leq i \leq 3 \), and invoking Exc. \( \ref{exc:conic-algebra} \) 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.

**sol.ISOT**

101 For the first part of the problem, put \( C := \text{Cay}(B, \mu) \) and write \( \varphi: C \to C^0 \) for the map defined by
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 (21.3.1) and associativity of $B$ with the fact that its conjugation is an involution (Prop. 22.5), we obtain

$$\varphi(u + vj) := (p^{-1}up) + vj \quad (u, v \in B),$$

But $\tilde{\varphi} = n_\varphi(p)^{-1}$, $\tilde{\varphi}^{-1} = n_\varphi(p)^{-1}$. Hence

$$\varphi(u_1 + v_1j) \cdot \varphi(u_2 + v_2j) = \left((p^{-1}u_1p) + v_1j\right) \cdot \left((p^{-1}u_2p) + v_2j\right)$$

$$= \left((p^{-1}u_1p) + v_1j\right) \cdot \left(p((p^{-1}u_2p) + v_2j)\right)$$

$$= \left(p^{-1}u_1 + (v_1\tilde{\varphi}^{-1})j\right)(u_2p + (v_2\tilde{\varphi}j))$$

$$= \left(p^{-1}u_1u_2p + \mu\tilde{\varphi}u_1v_2\tilde{\varphi}^{-1}\right) + \left(v_2p^{-1}u_1 + v_1\tilde{\varphi}^{-1}\tilde{\varphi}u_2\right).$$

as desired.

Turning to the second part of the problem, let $C$ be an octonion algebra over $k$ and suppose $p, q \in C^p$ have the property that $pq^2$ belongs to some quaternion subalgebra $B \subseteq C$. By Exc. 73 (a) and its solution, it will be enough to show for $p = 1$ that $B$ is isomorphic to $C$. This assertion is local on $k$ by $\varphi$ and so we may assume that $k$ is a local ring. By Thm. 22.15 (a), we may identify $C = \text{Cay}(B, \mu) = B \otimes B$, where the relation $B^2 = B^\perp$ can be read off from (21.3.4) and the non-singularity of $n_\varphi$. Thus our new map $\varphi$ agrees with the one defined in the first part and hence must be an isomorphism of conic algebras.

(a) We begin by showing that for a quadratic $k$-algebra $R$ and $u \in R$,

$$n_R(u - \bar{u}) = 4n_R(u) - t_R(u)^2, \quad (121)$$

which follows from

$$n_R(u - \bar{u}) = n_R(u) - n_R(u, \bar{u}) + n_R(\bar{u}) = 2n_R(u) - t_R(u)^2 + n_R(u, u) = 4n_R(u) - t_R(u)^2.$$

Now suppose that $u - \bar{u}$ is invertible in $R$. Then Prop. 22.5 and (121) show that $D := k[u] \subseteq R$ is a quadratic étale subalgebra. By Lemma 42.10, therefore, we obtain the decomposition $D = D \oplus D^\perp$ as $k$-modules and conclude, by comparing ranks, that $R = D$ is quadratic étale.

Next suppose $k$ is a semi-local ring and $D$ is a quadratic étale $k$-algebra. Then Thm. 22.15 (b) yields an element $u \in D$ of trace 1 such that $D' := k[u] \subseteq D$ is a quadratic étale subalgebra. As before, we have $D = D' \oplus D' \perp$ as $k$-modules, and comparing ranks yields $D = D' = k[u]$. Now Prop. 22.5 combined with (121) shows $n_R(u - \bar{u}) = k^p$, hence $u - \bar{u} \in D^\perp$.

Finally, returning to an arbitrary base ring $k$ and a quadratic étale $k$-algebra $D$, it remains to show $H(D, t_D) = k1_D$. In order to do so, we may assume $D = k[u]$ for some $u \in D$ such that $u - \bar{u} \in D^\perp$. In particular, by Prop. 22.5 $D$ is free (of rank 2) as a $k$-module with basis $1_D, u$. We clearly have $1_D \subseteq H(D, t_D)$. Conversely, write $x \in H(D, t_D)$ as $x = \alpha 1_D + \beta u$ for some $\alpha, \beta \in k$. Then $x = \bar{x} = \alpha 1_D + \bar{\beta} \bar{u}$ 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 $x = \alpha 1_D \subseteq 1_D$.

(b) Let $B$ be a quaternion algebra over $k$. We must show that an element $x \in B$ satisfying $[x, x] = 0$ for all $y \in B$ is a scalar multiple of $1_B$. This assertion being local on $k$, we may assume that $k$ is a local ring. By Cor. 22.10 we may further assume $B = \text{Cay}(D, \mu) = B \oplus B^\perp$ for some quadratic étale
$k$-algebra $D$ and some $\mu \in k$. From Thm. 22.10, 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 $x = u_1 + v_1j$, $u_1, v_1 \in D$. By hypothesis we have $[x, u_2 + v_2j] = 0$ for all $u_2, v_2 \in D$, which by (21.12.1) implies

$$0 = [u_1, u_2] + \mu(v_2v_1 - \bar{v}_1v_2) = \mu(v_2v_1 - \bar{v}_1v_2).$$

Since $\mu$ is invertible, we conclude $\bar{v}_2v_1 = v_1v_2$ for all $v_2 \in D$. Setting $v_2 = 1_B$ gives $v_1 = v_1$, 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 (21.12.3), 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

$$k1_C \subseteq \{x \in C \mid \forall y \in C : xy = yx\} \cap \text{Nuc}(C),$$

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. 22.16, $C = \text{Cay}(\mu) = B \otimes \mathcal{B}$ up to isomorphism, for some quaternion subalgebra $\mathcal{B} \subseteq C$ and some scalar $\mu \in k^\times$ (Thm. 22.10). Now let $x = u_1 + v_1j \in C$ with $u_1, v_1 \in B$ and first assume $[x, u_2 + v_2j] = 0$ for all $u_2, v_2 \in B$. From (21.12.1), (21.12.2), we conclude

$$[u_1, u_2] + \mu(v_2v_1 - \bar{v}_1v_2) = 0 = v_2(u_1 - \bar{u}_1) - v_1(\bar{u}_2 - u_2),$$

for all $u_2, v_2 \in B$. By what we have seen before, the first of these equations for $v_2 = 0$ shows $u_1 \in \text{Cent}(B) = 1_B$. Now the second one implies $v_1(u_2 - \bar{u}_2) = 0$ for all $u_2 \in B$. By Thm. 22.15 (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 $x \in \text{Nuc}(C)$. Applying (21.12.3), for $u_2 = v_2 = 0$, we obtain $(v_2v_1)u_3 = (u_3)v_2v_1$ for all $v_2, u_3 \in B$. Setting $v_2 = 1_B$, this implies $v_1u_3 = u_3v_1$ for all $u_3 \in B$, hence $v_1 \in \text{Cent}(B) = k1_B$. Thus $v_1 = \beta 1_B$ for some $\beta \in k$, and our original equation reduces to $(\beta v_2)u_3 = u_3(\beta v_1)$ for all $v_2, u_3 \in B$ This means $\beta v_2 \in \text{Cent}(B) = k1_B$ 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 $v_1$ one of the basis vectors distinct from $1_B$, we conclude $\beta = 0$, hence $v_1 = 0$. Now we consider (21.12.4) 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 $u_1 \in \text{Cent}(B) = k1_B$, hence $x \in k1_C$, and completes the proof.

**Sol. ETAUT.** If $k$ allows a decomposition of the desired kind, then $\phi$ is clearly an automorphism of $D$. Conversely, let this be so. We first treat the case that $k$ is a local ring. Then $D$ is free of rank 2 as a $k$-module and Theorem 22.15 (b) implies $D = k[u]$ for some element $u \in D$ of trace 1. By Proposition 22.5, therefore $(1_D, u)$ is a basis of $D$, and there are $\alpha, \beta \in k$ such that $\phi(u) = \alpha 1_D + \beta u$. But $\phi$, being an automorphism of $D$, preserves norms, traces and unit. Hence

$$2\alpha + \beta = t_D(\phi(u)) = t_D(u) = 1,$$

$$\alpha^2 + \alpha \beta + \beta^2 n_D(u) = n_D(\phi(u)) = n_D(u),$$

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, Proposition 22.5 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 $\phi = 1_D$ in the first case, $\phi = t_D$ in the second.

Now let $k$ be arbitrary and put $X := \text{Spec}(k)$. Since $D$ is finitely generated as a $k$-module,

$$X^+ := \{p \in X \mid \phi_p = 1_{D_p}\}, \quad X^- := \{p \in X \mid \phi_p = t_{D_p}\},$$

and $X^+$ is open in $X$. This proves that $\phi$ is an automorphism of $D$. The converse follows by replacing $D$ by $\text{Cay}(\mu)$.
by §10 Exercise 102 are Zariski-open subsets of $X$. Moreover, they are disjoint by Exercise 102(a) and cover $X$ by the special case just treated. Hence §10 Exercise 102 yields a complete orthogonal system $(\epsilon_+, \epsilon_-)$ of idempotents in $k$ such that $X_{\pm} = D(\epsilon_\pm)$. Put $k_\pm := \epsilon_\pm k$. Then $k = k_+ \oplus k_-$. as a direct sum of ideals, and with the canonical projection $\pi_+: k \rightarrow k_+$, we consult (10.6.6) to conclude $p := \text{Spec}(\pi_+)(p_+) = p_+ \oplus k_- \in D(\epsilon_+)$. For any prime $p_+ \in k_+$, let $\pi_+ : k \rightarrow k_+$ be non-singular, and let $\Phi : I \rightarrow k$ be injective. Given $z \in C_\pm$, the relations

$$t_\epsilon((xz)w) = t_\epsilon(x(zw)), \quad t_\epsilon(xz) = t_\epsilon(zx)$$

therefore imply $(xz)w = x(zw), xz = zx$, so $x$ belongs to the centre of $C$, which is $k$ by Exc. 102(b). Hence $I \subseteq I \cap k = \{0\}$, which proves our claim.

Turning to the problem in its proper sense, we put

$$\mathcal{J}(k) := \{a \mid a \subseteq k \text{ is an ideal}\},$$

$$\mathcal{J}(C, t_\epsilon) := \{I \mid I \subseteq (C, t_\epsilon) \text{ is an ideal}\},$$

$$\mathcal{J}(C) := \{I \mid I \subseteq C \text{ is an ideal}\}.$$

In particular, $\mathcal{J}(C, t_\epsilon)$ consists of the ideals in $C$ that are stable under conjugation. Besides the inclusion $j : \mathcal{J}(C, t_\epsilon) \hookrightarrow \mathcal{J}(C)$, we now define maps

$$\Phi : \mathcal{J}(k) \rightarrow \mathcal{J}(C, t_\epsilon), \quad a \mapsto \Phi(a) := aC,$$

$$\Psi : \mathcal{J}(C) \rightarrow \mathcal{J}(k), \quad I \mapsto \Psi(I) := I \cap k,$$

which may all be depicted in the following diagram:

$$\mathcal{J}(k) \xrightarrow{\Phi} \mathcal{J}(C, t_\epsilon) \xrightarrow{j} \mathcal{J}(C).$$

The theorem will follow once we have shown

$$\Psi \circ j \circ \Phi = 1_{\mathcal{J}(k)}, \quad \Phi \circ \Psi \circ j = 1_{\mathcal{J}(C, t_\epsilon)}, \quad j \circ \Phi \circ \Psi = 1_{\mathcal{J}(C)} \quad (123) \quad (124)$$

The sol.IDEALSCOAL is as follows.
To do so, let $\mathfrak{a}$ be an ideal in $k$. Since $1_C \in C$ is unimodular, we find a $k$-submodule $M \subseteq C$ such that

$$C = k \oplus M$$  \hfill (125)

This gives $aC = a \oplus aM$, hence

$$(\Phi \circ j \circ \Phi)(a) = (aC) \cap k = (a \oplus aM) \cap k = a$$

and we have established the first relation of (123). We derive the second one along with (124) by letting $I$ be an ideal of $(C, I_C)$ (resp. of $C$ if $C$ has rank $r > 2$). Then $(\Phi \circ \Psi \circ j)(I) = (I \cap k)C \subseteq I$ (resp. $(j \circ \Phi \circ \Psi)(I) = (I \cap k)C \subseteq I$), so it remains to show

$$I \subseteq (I \cap k)C.$$  \hfill (126)

**Case 1.** $I \cap k = \{0\}.$

Then we have to prove $I = \{0\}$, which follows from our claim above.

**Case 2.** $a := I \cap k$ is arbitrary.

Then we pass to the base change $k' := k/a$, so we look at the composition algebra $C' := C \otimes k' = C/aC$ over $k'$, denote by $I' = I/aC$ the image of $I$ under the canonical map

$$C \rightarrow C', \quad x \mapsto x',$$

which belongs to $\mathfrak{I}(C')$, and claim that $a' := I' \cap k'$ satisfies

$$a' = \{0\}.$$  \hfill (127)

To see this, we first note that (125) implies

$$C' = k' \oplus M', \quad M' := M \otimes k'/aM.$$  \hfill (128)

Given $a_1 \in a' \subseteq I'$, we can therefore find elements $\xi, \eta \in k$, $y \in M$ satisfying $x := \xi + y \in I$ and $x' = \alpha_1$. In view of (128), this yields $\xi' = \alpha_1, y' = 0$, hence $y \in aM \subseteq aC \subseteq I$ and $\xi - x - y \in I \cap k = a$. But then $a_1 = \xi' = 0$ and the proof of (127) is complete. Now we are in a position to apply case 1, which yields $I' = \{0\}$, hence $I \subseteq aC$, as claimed in (126).

**sol.PEIRCEELID** 105. We begin by proving (2) and first note that not only $c_1 = c$ but also $c_2 = 1_C - c$ is an elementary idempotent (cf. Exc. 82, particularly (iv)). Let $i = 1, 2$ and $x \in \mathfrak{C}_i$. Then $c_1 x = x c_i$, and (20.1.2) yields $x = c_1 x = n(c_1 x) c_i = n(c) c_i x = n(c) c_i x_i c_i = n(c) x_i c_i \subseteq C_i$, and (2) holds. In view of this, arbitrary elements $x, y \in C$ can be written as in (3). Expanding the norm of $x$ in the obvious manner, we obtain

$$nC(x) = nC(c_1 x_1 + x_2 + x_3 + c_2)$$

$$= \alpha_1 nC(c_1) + \alpha_1 nC(c_1 x_1) + \alpha_1 nC(x_1) + \alpha_2 nC(c_2) + nC(x_2) + nC(x_3) + \alpha_2 nC(x_2) + \alpha_2 nC(c_2).$$

Applying (20.1.3), (20.1.2) and observing $nC(c_1) = nC(c_2) = 0$, we obtain, for $\{i, j\} = \{1, 2\},$

$$nC(c_1) = 0,$$

$$nC(c_i, x_{ij}) = nC(c_i, x_{ij}) = nC(c_i) nC(c_i) = 0,$$

$$nC(c_i, x_{ij}) = nC(c_i) nC(x_i c_i) = nC(c_i, x_{ij}) nC(c_i) = 0,$$

$$nC(c_i, c_2) = nC(c_i, 1_C - c) = tC(c) - 2nC(c) = 1,$$

$$nC(x_{ij}) = nC(c_i x_{ij}) = nC(c_i) nC(x_{ij}) = 0.$$
Inserting these relations into the preceding equation, we end up with \( \text{(5)}, \) while linearizing \( \text{(4)} \) gives \( \text{(5)}. \) Finally, \( \text{(5)} \) 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 \( \text{(5)} \) yields

\[
n_C(x_{ij}, C) = n_C(x_{ij}, k_{ij} + C_{ji} + k_{ji}) = n_C(x_{ij}, C_{ji}) = \{0\}
\]

hence \( x_{ij} = 0 \) since \( n_C \) is non-singular. Next let \( \lambda_{ij} : C_{ij} \to k \) be a linear form and \( \lambda : C \to k \) the linear extension of \( \lambda_{ij}. \) By non-singularity of \( n_C, \) there exists \( x \in C \) such that \( \lambda = n_C(x, -). \) Writing \( x \) in the form \( \{3\} \) and choosing \( y_{ij} \in C_{ji}, \) we apply \( \text{(5)} \) and obtain \( \lambda_{ij}(y_{ij}) = \lambda(y_{ij}) = n_C(x, y_{ij}) = n_C(x_{ij}, y_{ij}). \) 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 \( trC(x^2) = trC(xy^2) = 0 \) for all \( x, y, z \in C_{ij}. \) This follows from the final statement in \( \text{[15]} \) Exercise \( \text{[67]} \)

106. (a) Since scalar multiplication by \( D \) acts on the second factor of \( D \times D, \) the map \( \varphi \) is a unital homomorphism of \( D \)-algebras. Moreover, for \( u \in D \) we have

\[
\varphi(u \circ 1 : D - 1_D \otimes \tilde{u}) = (u \circ \tilde{u}) - (\tilde{u} \circ \tilde{u}) = (u - \tilde{u}) \otimes 0,
\]

\[
\varphi(1_D \circ u - u \circ 1_D) = (u \circ u) - (u \circ \tilde{u}) = 0 \oplus (u - \tilde{u}).
\]

In order to prove that \( \varphi \) is an isomorphism, we may assume that \( k \) is a local ring. By Exc. \( \text{[102]} \) (a), the element \( u \) may be so chosen that \( u - \tilde{u} \in D^\times. \) The preceding equations therefore show that \( 1_D \oplus 0 \text{ and } 0 \oplus 1_D \) both belong to \( \text{Im}(\varphi). \) But \( D \) is generated by these elements as a \( D \)-algebra. Hence \( \varphi \) is surjective. On the other hand, combining Exc. \( \text{[102]} \) (a) with Prop. \( \text{[22.3]} \) we conclude that \( D \) is a free \( k \)-module with basis \( \{1_D, u\}. \) Hence \( D \otimes D \) is a free \( D \)-module with basis \( \{1_D \otimes 1_D, u \otimes 1_D\}. \)

Hence an arbitrary element of \( \text{Ker}(\varphi) \) can be written in the form \( d_0(1_D \otimes 1_D) + d_1(u \otimes 1_D) \) with \( d_0, d_1 \in D, \) and we conclude

\[
0 = \varphi(d_0(1_D \otimes 1_D) + d_1(u \otimes 1_D)) = \varphi(1_D \otimes d_0 + u \otimes d_1) = (d_0 \otimes d_0) + (ud_1 \otimes \tilde{ud}_1) = (d_0 + ud_1) \oplus (d_0 + \tilde{ud}_1).
\]

Thus \( d_0 + ud_1 = d_0 + \tilde{ud}_1 = 0. \) Subtracting gives \( u - \tilde{u}d_1 = 0, \) hence \( d_1 = 0 \) and then \( d_0 = 0 \) as well. This shows that \( \varphi \) is injective, and the proof of (a) is complete.

(b) By definition, we have \( \sigma' \circ \varphi = \varphi \circ \sigma'. \) Hence, for \( x, d \in D, \)

\[
\sigma'(\langle xd \rangle \oplus \langle \tilde{xd} \rangle) = \sigma'((\varphi(x \circ d)) = \varphi((\sigma(x \circ d)) = \varphi((x \circ \tilde{d})) = \langle xd \rangle \oplus \langle \tilde{xd} \rangle = \langle xd \rangle \oplus \langle \tilde{xd} \rangle,
\]

which proves the assertion since, by (a), any element of \( D \otimes D \) can be written as a finite sum of expressions of the form \( \langle xd \rangle \oplus \langle \tilde{xd} \rangle \) with \( x, d \in D. \)

107. (a) Let \( x, y \in R. \) Since \( R \) by Prop. \( \text{[20.2]} \) (b) is a multiplicative conic algebra, we may apply \( \text{[19.11.3]} \) \( \text{[19.5.10]} \) and \( \text{[20.1.3]} \) to obtain

\[
t_R(exy) = nR(ex)ey - nR(ex), ey = nR(ex)ey - nR(ex, ey) = nR(ex, ey) = nR(ex)ey.
\]

Hence \( t_R \circ I_C : R \to k \) is an algebra homomorphism, which by Exc. \( \text{[62]} \) 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

\[
q(x)q(y) = (t_R(ex^2 + en_R(x))(t_R(ey^2 + en_R(y)))
\]

\[
= en_R(x)en_R(y) + t_R(ex^2)en_R(y) + en_R(x)t_R(ey^2) + t_R(ex^2)en_R(y) + en_R(x)en_R(y)
\]

\[
= t_R(en_R(x) + en_R(x)) = t_R(y) + t_R(ex)en_R(y) + n_R(x)en_R(y) + en_R(x)en_R(y)
\]

\[
= t_R(en_R(x) + en_R(x)) = t_R(x^2) + en_R(x) = q(x).
\]
Hence $q$ permits composition.

(c) The condition is clearly sufficient. Conversely, suppose $q$ permits composition. We put $e_1 := 1 \otimes 0, e_2 := 0 \otimes 1$ and

$$e_1 := q(e_1), \quad e_2 := q(e_1, e_2), \quad e_3 := q(e_2).$$

Then (8) holds. Moreover, since $q$ permits composition, $(e_1, e_3)$ is an orthogonal system of idempotents such that $e_1 e_2 = q(e_1) q(e_1, e_2) = q(e_1, e_2) = 0$ and, similarly, $e_2 e_3 = 0$. On the other hand, $\varepsilon := q(1_D) = \sum e_i$ 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 $\varepsilon e_i = e_i$ for $i = 1, 2, 3$, whence $e_2 = \varepsilon - e_1 - e_3$ must be an idempotent as well.

(d) Let $q: D \to k$ be a quadratic form permitting composition. Since, therefore, its scalar extension $q_D: D \otimes D \to D$ permits composition, so does $q' := q_D \circ \varphi^{-1}: D \otimes D \to D$, where $\varphi$ is the isomorphism of Exc. [106] (a). Hence (c) yields an orthogonal system $(d_1, d_2, d_3)$ of idempotents in $D$ such that

$$q(a \oplus b) = d_1 a^2 + d_2 ab + d_3 b^2$$

for all $a, b \in D$. With $\sigma$ as in Exc. [106] (b), we now claim

$$q_D \circ \sigma = t_D \circ q_D.$$  \hspace{1cm} (129) \hspace{1cm} QUDE

In order to prove this, we let $x, x', d, d' \in D$ and compute

$$(q_D \circ \sigma)(x \otimes d) = q_D(x \otimes d) = q(x)d^2,$$

$$(t_D \circ q_D)(x \otimes d) = t_D(q_D(x \otimes d)) = q(x)d^2 = q(x)d^2,$$

$$(q_D \circ (\sigma \times \sigma))(x \otimes d, x' \otimes d') = q_D(x \otimes d, x' \otimes d') = q(x, x')d^2d',$$

$$(t_D \circ q_D)(x \otimes d, x' \otimes d') = t_D(q_D(x \otimes d, x' \otimes d')) = q(x, x')d^2d'.$$

Hence (129) holds. Using this, and keeping the notation of Exc. [106] (b), we conclude

$$q' \circ \sigma' = q_D \circ \varphi^{-1} \circ \sigma \oplus \varphi^{-1} = q_D \circ \varphi^{-1} = t_D \circ q_D \circ \varphi^{-1} = t_D \circ q'.$$

deviating slightly from the notation used in (c), we now put $e_1 := 1_D \otimes 0, e_2 := 0 \otimes 1_D$ and obtain

$$\tilde{d}_1 = \tilde{q}'(e_1) = (t_D \circ q')(e_1) = (t_D \circ q')(e_1) =$$

hence $\tilde{d}_1 = d_1$. Similarly,

$$\tilde{d}_2 = (t_D \circ q')(e_1, e_2) = q' \left( (\sigma'(e_1), \sigma'(e_2)) \right) = q'(e_2, e_1) = d_2.$$

Thus $d_2 \in H(D, t_D) = k1_D$ (by Exc. [102] (a)). Since $1_D$ is unimodular, we find a unique idempotent $\varepsilon \in k$ such that $d_2 = \varepsilon 1_D$. Then $\varepsilon i = d_1$ is an idempotent in $D$ such that $\varepsilon e = d_2 d_1 = 0$, while the relation $q_D(e) 1_D = \varepsilon e = d_1 d_3 = 0$ implies $q_D(e) = 0$. Finally, for $x \in D$, we compute

$$q(x) 1_D = q_D(x \otimes 1_D) = q'(x \otimes 1_D) = q'(x \otimes \tilde{e}) = e x^2 + e \tilde{x} + \tilde{e} x^2$$

$$= (t_D(e x^2) + \varepsilon q_D(x)) 1_D,$$

and the assertion follows.
is exact, equivalently, that the linear map $\Phi$ is surjective. Let $q : M \to k$ be any quadratic form. By Exercise 59 there exists a bilinear form $b : M \times M \to k$ (possibly not symmetric) such that $q(x) = b(x, x)$ for all $x \in M$, and since $Q$ is non-singular, we find an element $f \in \text{End}_k(M)$ satisfying $b(x, y) = Q(f(x), y)$ for all $x, y \in M$. This implies $q = \Phi(f)$, and surjectivity of $\Phi$ is proved.

$q = \epsilon q_\mathcal{C}$ for some idempotent $\epsilon \in k$ clearly implies that $q$ permits composition. Conversely, suppose $q : C \to k$ is a quadratic form permitting composition. The case $r = 1$ being trivial, we may assume $r > 2$, so $C$ is either a quaternion or an octonion algebra; in any event, it is non-singular. Since $q$ permits composition, we obtain

$$q(x) = \epsilon q(x). \quad (x \in C, \, \epsilon := q(1_C) = \epsilon^2 \in k) \quad (130)$$

We now proceed in several steps.

1. Our first aim will be to show that if the bilinearization of $q$ vanishes, so does $q$ itself. Indeed, if $q(x, y) = 0$ for all $x, y \in C$, then $q : C \to k$ is a (possibly non-unital) homomorphism of $\mathbb{Z}$-algebras, forcing

$$I := \text{Ker}(q) = \{x \in C \mid q(x) = 0\} \subseteq C$$

to be an ideal. From Exc. 104 we therefore deduce $I = aC$ for some ideal $a \subseteq k$. It suffices to show $a = k$. Otherwise, the base change $C' = C/I = C \otimes k'$ would continue to be a composition algebra of rank $r > 2$ over the non-zero ring $k' = k/a$, and $q$ would induce an injection $C' \to k$ of $\mathbb{Z}$-algebras, which would make $C'$ a commutative associative $k'$-algebra, a contradiction.

2. Since the norm of $C$ is non-singular, the preceding exact sequence yields a $k$-linear map $f : C \to C$ satisfying

$$q(x) = n_C\big(f(x), x\big) \quad (x \in C), \quad (131)$$

which implies

$$q(x, y) = n_C(g(x, y), \quad g := f + f^*, \quad (132)$$

for all $x, y \in C$, where $f^*$ stands for the adjoint of $f$ relative to $Dn_C$. Obviously, $g$ is uniquely determined by $q$. Combining (132) with (19.11.4) and the property of $q$ to permit composition, we now obtain $n_C(\tilde{x}g(xy), z) = n_C(g(xy), xz) = q(xy, xz) = q(x)q(y, z) = n_C(q(x)g(y), z)$, hence

$$\tilde{x}g(xy) = q(x)g(y), \quad (133)$$

since $n_C$ is non-singular. Linearizing (133) and consulting (132) again, we conclude

$$\bar{x}g(\bar{y}) + i\tilde{x}g(xy) = n_C(g(x, z)g(y), \quad (134)$$

where we set $z = 1_C$ to conclude

$$g(xy) = \bar{\lambda}(x)g(y) + \tilde{x}g(y), \quad \bar{\lambda} := t_C \circ g - t_C. \quad (135)$$

For $y = 1_C$, this implies

$$g(x) = \bar{\lambda}(x)u + xu, \quad u := g(1_C). \quad (136)$$

Now observe that $C^\mathbb{P}$ is a composition algebra over $k$ having the same norm as $C$ and satisfying all of our previous hypotheses. Also, $q : C^\mathbb{P} \to k$ permits composition and passing from $C$ to $C^\mathbb{P}$ neither affects $g$ nor $\bar{\lambda}$ and $u$. Hence (136) yields

$$g(x) = \bar{\lambda}(x)u + ux. \quad (137)$$

Comparing (136) and (137), we obtain $ux = xu$ for all $x \in C$, so Exc. 102(b) implies...
This implies that one can therefore find an element \( u \) such that the inclusion \( C \to C' \) extends to a basis \( e_0 = 1_C, e_1, \ldots, e_{r-1} \) of \( C \) as a \( k \)-module. Setting \( x = e_i, y = e_j \) in (140) \((1 \leq i, j \leq r - 1, i \neq j)\), we conclude \( \epsilon' \lambda(e_i) = 0 \), while \( \epsilon' \lambda(1_C) = 0 \) follows from (139), (136) by specializing \( x \) to \( 1_C \). Summing up, all this yields \( \epsilon' \lambda = 0 \) and (139) reduces to

\[
g = \epsilon' 1_C.
\]

3. Setting \( y = 1_C \) in (133) and observing (141), we conclude

\[
\epsilon' n_C(x) = \epsilon' y q(x),
\]

which implies

\[
\epsilon \epsilon' = \epsilon'
\]

for \( x = 1_C \). On the other hand, linearizing (142) and consulting (141) again yields \( n_C(\epsilon' x, y) = \epsilon' n_C(x, y) = \epsilon' y q(x, y) = \epsilon' n_C(\epsilon' x, y) = n_C(\epsilon' x, y) \), and \( \epsilon' \epsilon^2 \) is an idempotent in \( k \). By (143), so is \( \epsilon_1 = \epsilon - \epsilon' \), allowing us to analyze the base change of \( q \) from \( k \) to \( k_1 = k \epsilon_1 \). Since \( \epsilon' \lambda = \epsilon' \epsilon_1 = 0 \), we conclude \( g \otimes k_1 = 0 \) from (141), so \( q_1 = q \otimes k_1 \) has zero bilinearization, hence by 1\(^\circ\) must be zero itself. Using (139), (143), this implies

\[
0 = q_1(1_C x, y) = \epsilon_1 x = \epsilon^2 - \epsilon \epsilon' = \epsilon - \epsilon',
\]

hence \( \epsilon = \epsilon' \). Now we may use (139), (142) to conclude \( \epsilon n_C(x) = \epsilon q(x) = q(x) \) for all \( x \in C \), and the proof is complete.

We first treat the case that \( k = F \) is a field. Then \( R \) is a two-dimensional \( F \)-algebra. If \( R \) is quadratic \( \tilde{a} \), then Thm. 22.13(a) yields a scalar \( \mu \in k^\times \) such that the inclusion \( R \to R' \) extends to an embedding from \( \text{Cay}(B, \mu) = B \oplus B \) to \( C \). Its image, therefore, is a quaternion subalgebra of \( C \) generated by \( R \) and the image of \( j \) in \( C \). Hence we may assume that \( R \) is not quadratic \( \tilde{a} \). Then Exc. 97 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 \( R = F u_0 \oplus F u_1 \) and \( n_C(u_0, u_1) = \lambda_0(\bar{u}_1) = 2 \alpha = 0 \), where \( \alpha := n_C(u_1) \). For any \( \beta \in F \), we can therefore find an element \( u_2 \in C \) such that \( n_C(u_0, u_2) = \lambda_0(u_2) = 1 \) and \( n_C(u_1, u_2) = \beta \). Setting \( \gamma := n_C(u_2) \) and \( u_3 := u_1 u_2 \), we conclude

\[
\begin{align*}
n_C(u_0, u_2) &= n_C(1_C, u_1 u_2) = n_C(\bar{u}_1, u_2) = -n_C(u_1, u_2) = -\beta, \\
n_C(u_1, u_1) &= 2 \alpha = 0, \\
n_C(u_1, u_2) &= n_C(u_1, u_1 u_2) = n_C(u_1) = \lambda_0(\bar{u}_1) = \lambda_0(u_2) = \alpha, \\
n_C(u_2, u_2) &= 2 n_C(u_2) = 2 \gamma, \\
n_C(u_2, u_3) &= n_C(u_2, u_1 u_2) = n_C(u_2) = \lambda_0(\bar{u}_1) = 0, \\
n_C(u_3, u_3) &= 2 n_C(u_3) = 2 n_C(u_1 u_2) = 2 n_C(u_1) = 2 \epsilon n_C(u_2) = 0.
\end{align*}
\]

This implies
The $R$ indicated above becomes a unit after reduction mod $\text{Jac}(a)$. Let $110$. quaternion algebra containing $R^b$ (resp. $k$) making $B_k := F_j \subset C_j$ (for some $a_j \in C_j, 1 \leq j \leq m$) is a quadratic subalgebra, so the preceding case yields an element $b_j \in C_j$ making $B_j := F_j \subset C_j$. This shows that $R \subset \bar{R}$ is a quaternion subalgebra containing $R$. Next assume that $k = F_1 \oplus \cdots \oplus F_m$ is a direct sum of finitely many fields $F_j, 1 \leq j \leq m$. Then $C = C_1 \oplus \cdots \oplus C_m$ with octonion algebras $C_j = C \otimes F_j$ over $F_j$ for $1 \leq j \leq m$, and $R = R_1 \oplus \cdots \oplus R_m$ with quadratic rings $R_j = R \otimes F_j$ over $F_j$ for $1 \leq j \leq m$. Then, clearly, $R_j = F_j[a_j] \subset C_j$ (for some $a_j \in C_j, 1 \leq j \leq m$) is a quadratic subalgebra, so the preceding case yields an element $b_j \in C_j$ making $B_j := F_j \subset C_j + F_j[a_j] + F_j[b_j + F_j a_j b_j] \subset C_j$ a quaternion subalgebra containing $R_j$. Now put $a := a_1 \oplus \cdots \oplus a_m$, $b := b_1 + \cdots + b_m$, $B := B_1 + \cdots + B_m$. The $R = k[a]$ and $B = k^1 + ka + kb + kab \subset C$ is a quaternion subalgebra generated by $R$ and $b$.

Finally, we are able to treat the general case. The property of $R$ to be a direct summand of $C$ as a $k$-module is preserved under scalar extensions. Hence, setting $\bar{k} := k/\text{Jac}(k), \bar{C} := C \otimes \bar{k} = C/\text{Jac}(k)C$, it follows from the previous case that $\bar{R} := R \otimes \bar{k} = R/\text{Jac}(k)R \subset \bar{C}$ is a quadratic subalgebra generated by some element $a' \in \bar{R}$ and that there is an element $b' \in \bar{C}$ making $B := k^1 + ka' + kb' \subset \bar{C}$ a quaternion subalgebra containing $R$. Lift $a'$ (resp. $b'$) to elements $a$ (resp. $b$) in $C$. Then $B := k^1 + ka + kb + kab$, the unital subalgebra of $C$ generated by $a, b$, is a quaternion algebra containing $R$ since the determinant of $D_{ab}$ evaluated at the bunch of generators indicated above becomes a unit after reduction mod $\text{Jac}(k)$, hence must have been one all along. 

\[\det\left(\frac{nc(u_i u_j)}{0 \leq i, j \leq 3}\right) = \det\left(\begin{array}{ccc} 2 & 0 & -\beta \\ 0 & 0 & \beta \alpha \\ 1 & 2\gamma & 0 \end{array}\right) = \det\left(\begin{array}{ccc} 0 & -2\beta & 1 - 4\gamma - \beta \alpha \\ 0 & 0 & \beta \alpha \\ 1 & 2\gamma & 0 \end{array}\right) = \det\left(\begin{array}{ccc} -2\beta & 1 - 4\gamma - \beta \alpha \\ 0 & \beta \alpha \\ \alpha + \beta^2 & 2\beta \gamma & 0 \end{array}\right) = \alpha(\alpha + \beta^2)(1 - 4\gamma) + (\alpha + \beta^2)\beta^2 + 4\alpha\beta^2 \gamma = (\alpha + \beta^2)(\alpha + \beta^2) = (\alpha + \beta^2)^2\] 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, forcing $\langle u_i \rangle_{0 \leq i \leq 3}$ to be linearly independent and $\sum F_{u_i} \subset C$ by Exc. 85 to be a quaternion subalgebra containing $R$.

Here the first inclusion is obvious, while the second and third one follow from the fact that $C$ is norm associative, particularly from (19.11.3), (19.11.4). Finally, in order to establish the fourth inclusion, we may assume that $k$ is a local ring, in which case Thm. 22.13(a) yields an identification $C = \text{Cay}(B, \mu) = B \oplus B_j$ for some $\mu \in k^x$ and then $B_i = B_j$ by (21.3.3). But now the assertion follows from (19.3.1). By (19.4.1), the map $\sigma_{B} := \sigma_{B} \oplus (-1_{B_j})$ is a reflection of $C$, and it is straightforward to check that the assignments $\sigma \mapsto \text{Fix}(\sigma), B \mapsto \sigma_{B}$ define inverse bijections between the set of reflections of $C$ and the set of composition subalgebras of $C$ having rank $\frac{1}{2}$. 

Here the first inclusion is obvious, while the second and third one follow from the fact that $C$ is norm associative, particularly from (19.11.3), (19.11.4). Finally, in order to establish the fourth inclusion, we may assume that $k$ is a local ring, in which case Thm. 22.13(a) yields an identification $C = \text{Cay}(B, \mu) = B \oplus B_j$ for some $\mu \in k^x$ and then $B_i = B_j$ by (21.3.3). But now the assertion follows from (19.3.1). By (19.4.1), the map $\sigma_{B} := \sigma_{B} \oplus (-1_{B_j})$ is a reflection of $C$, and it is straightforward to check that the assignments $\sigma \mapsto \text{Fix}(\sigma), B \mapsto \sigma_{B}$ define inverse bijections between the set of reflections of $C$ and the set of composition subalgebras of $C$ having rank $\frac{1}{2}$. 

\[\det\left(\frac{nc(u_i u_j)}{0 \leq i, j \leq 3}\right) = \det(\begin{array}{ccc} 2 & 0 & -\beta \\ 0 & 0 & \beta \alpha \\ 1 & 2\gamma & 0 \end{array}) = \det(\begin{array}{ccc} 0 & -2\beta & 1 - 4\gamma - \beta \alpha \\ 0 & 0 & \beta \alpha \\ 1 & 2\gamma & 0 \end{array}) = \det(\begin{array}{ccc} -2\beta & 1 - 4\gamma - \beta \alpha \\ 0 & \beta \alpha \\ \alpha + \beta^2 & 2\beta \gamma & 0 \end{array}) = \alpha(\alpha + \beta^2)(1 - 4\gamma) + (\alpha + \beta^2)\beta^2 + 4\alpha\beta^2 \gamma = (\alpha + \beta^2)(\alpha + \beta^2) = (\alpha + \beta^2)^2\]
Let $\rho \in \text{Aut}(C)$. If $\sigma$ is a reflection of $C$, then so is $\sigma^\rho := \rho^{-1} \circ \sigma \circ \rho$ and $\text{Fix}(\sigma^\rho) = \rho^{-1}(\text{Fix}(\sigma))$. On the other hand, if $B \subseteq C$ is a composition subalgebra of rank $\frac{1}{2}$, then $\sigma_{\rho^{-1}(B)} = (\sigma_B)^\rho$. This shows that two reflections of $C$ are conjugate under $\text{Aut}(C)$ 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 $C^{\sigma_0}$ have the same unit, norm and trace, Exc. [78] shows that they are preserved by $\tau$. For $x \in C$, this implies

$$\tau(x) = \tau(t_c(x))1_C - x = t_c(\tau(x))1_C - \tau(x) = \overline{\tau(x)}.$$ 

Thus $\tau$ commutes with $t_c$.

Now let $\tau$ be an involution of $C$ distinct from $t_c$. Since $\tau$, as we have just seen, commutes with $t_c$, the map $\tau_c := \tau \circ t_c = t_c \circ \tau$ is a reflection of $C$. Conversely, let $\sigma$ be a reflection of $C$. Being an automorphism of $C$, $\sigma$ preserves conjugation, forcing $\tau_\sigma := \sigma \circ t_c = t_c \circ \sigma$ to be an involution other than $t_c$. It is clear that the assignments $\tau \mapsto \tau_c$ and $\sigma \mapsto \tau_\sigma$ define inverse bijections between the set of involutions of $C$ distinct from $t_c$ and the set of reflections of $C$. Moreover, the identities $\tau_\sigma = \rho^{-1} \circ \tau_\rho \circ \rho$ and $\tau_{\rho^{-1} \circ \tau_\rho} = (\sigma_c)^\rho$ are immediately verified. Invoking (a), the aforementioned bijections, therefore, induce canonically inverse bijections between the isomorphism classes of involutions of $C$ other than $t_c$ and the conjugacy classes under $\text{Aut}(C)$ of the composition subalgebras of $C$ having rank $\frac{1}{2}$.

Finally, let $\tau \neq t_c$ be an involution of $C$ and $B \subseteq C$ the corresponding composition subalgebra of rank $\frac{1}{2}$. Then $\tau = \sigma_B \circ t_c$, and for $x, y \in B^\perp$, we obtain $\tau(x+y) = \sigma_B(x-y) = x+y$, hence

$$H(C, \tau) = H(B, t_B) \oplus B^\perp = k1_B \oplus B^\perp \cong k \oplus B^1,$$

and since $B^1$ is finitely generated projective of rank $\frac{1}{2}$, the final assertion follows.

**Section 2A**

(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.

In order to see this, we argue indirectly and assume $h(x, x) = 0$ for all $x \in M$. Linearizing this relation yields

$$t_B(h(x, y)) = h(x, y) + h(x, y) = h(x, y) + h(y, x) = 0$$

for all $x, y \in M$, where we may replace $x$ by $xa$, $a \in D$, to obtain $nt_B(a, h(x, y)) = t_B(\tilde{a}h(x, y)) = t_B(\tilde{h}(xa, y)) = 0$ 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 local ring $k$, with maximal ideal $\mathfrak{m}$ and residue field $\mathfrak{k} := k/\mathfrak{m}$, we argue by induction on $n$ and have nothing to prove for $n = 0$. If $n > 0$, we pass to the base change from $k$ to $\mathfrak{k}$ and put $(M, h) := (M, h)_{\mathfrak{k}}$, which is a hermitian space of rank $n$ over the field $\mathfrak{k}$. Hence our preceding claim yields an element $\tilde{x} \in M = M/\mathfrak{m}M$ such that $h(\tilde{x}, \tilde{x}) \neq 0$. Lifting $\tilde{x}$ to an element $e_1 \in M$ under the natural map $M \to \tilde{M}$, we deduce $\alpha_1 := h(e_1, e_1) \in \mathfrak{k}^\times$. Now we put

$$N := (e_1D)^\perp = \{y \in \mathfrak{m} | h(e_1, y) = 0\} = \{x \in M | h(x, e_1) = 0\}$$

and see by a straightforward verification that $M = (e_1D) \oplus N = (e_1D) \perp N$ relative to $h$. It follows that $(N, h|_{N, N})$ 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 $e_i \in M$, $\alpha_i \in k$, $1 \leq i \leq n$, 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 $h(e_iD,e_jD) = \delta_{ij}\alpha_i\alpha_j$ for
\(d, d' \in D, 1 \leq i, j \leq n\) show that the preceding decomposition is an orthogonal one relative to \(h\), hence relative to \(q\) as well, and \(q(e, d) = h(e, d, e, d) = \alpha_dd = \alpha_dd(d)\) for \(d \in D, 1 \leq i \leq n\). Thus 
\[q \cong \alpha_dd \perp \cdots \perp \alpha_dd \cong \langle \alpha_1, \ldots, \alpha_n \rangle \otimes n_D\]
is the finite orthogonal sum of non-singular quadratic forms over \(k\), hence must be non-singular itself.

We put \(C := \text{Ter}(D; M, h, \Delta)\) and have \(C = D \oplus M\) as \(k\)-modules. After the natural identification \(D \subseteq C\), we obtain \(p^{n+1} = p^{n+1} \oplus 0\), and writing "\(^-\)" for the product in \(C^\ast\), we conclude, for \(a, b \in D, x, y \in M\),
\[(a \oplus x) \cdot (b \oplus y) = ((a \oplus x)(p^{n+1} \oplus 0))((p \oplus 0)(b \oplus y))\]
\[= ((ap^{-1}) \oplus (xp^{-1}))(pb \oplus (yp^{-1}))\]
\[= (ap^{-1}pb - h(xp^{-1}, yp^{-1})) \oplus (yp^{-1}ap^{-1} + xp^{-1}pb + (xp^{-1}) \Delta)\]
\[= (ab - \bar{p}^{-1}h(x, y)p) \oplus (y \bar{a} + xb + (x \Delta)y \bar{p}^{-1}p)\]
Hence
\[(a \oplus x) \cdot (b \oplus y) = (ab - h(x, y)) \oplus (y \bar{a} + xb + (x \Delta)y \bar{p}^{-1}p) \quad (a, b \in D, x, y \in M). \quad (145)\]

We will now be able to compute the constituents of \(C^\circ = \text{Ter}(D; M^p, h^p, \Delta^p)\) by appealing to Thm. 24.11 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. 90 agrees with the bilinearized norm of \(C\). Thus \(M^p = M\) as \(k\)-modules. Consulting \((145)\), the right action of \(D^p = D\) on \(M^p = M\) may be read off from
\[(x, a) \mapsto (0 \oplus x) \cdot (a \oplus 0) = 0 \oplus (xa),\]
which amounts to \(M^p = M\) as right \(D\)-modules.

For \(x, y \in M\), we deduce from \((145)\) that \(h^p(x, y)\) is the negative of the \(D\)-component of
\[(0 \oplus x) \cdot (0 \oplus y) = (-h(x, y)) \oplus ((x \Delta)y \bar{p}^{-1}p), \quad (146)\]
hence agrees with \(h(x, y)\). Thus \(h^p = h\).

Finally, let \(a \in D^\ast\). Then \(a\Delta : \Lambda^3 M \to D\) is a volume element of \(M\), and \((24.8)\) shows
\[h(x \Delta y \Delta z, z) = a(h(x \Delta y \Delta z) = ah(x \Delta y \Delta z) = h((x \Delta y) \bar{a}, \bar{z})\]
for all \(x, y, z \in M\), which is equivalent to
\[x \Delta y \Delta z = (x \Delta y) \bar{a} \quad (x, y \in M, a \in D^\ast). \quad (147)\]

Now by Thm. 24.11 \(x \Delta y \Delta z\) is the \(M\)-component of \((0 \oplus x) \cdot (0 \oplus y)\), hence by \((146)\) agrees with \((x \Delta y) \bar{p}^{-1}p\). Since, fixing \(h\), the hermitian vector product uniquely determines the volume element it corresponds to, we conclude from this and \((147)\) that \(\Delta^p = \bar{p}^{-1} \Delta\).

Summing up, we have proved
\[C^p = \text{Ter}(D; M, h, \bar{p}^{-1} \Delta). \quad (148)\]

Finally, we wish to understand what all this means for the algebra \(C = \text{Zor}(k)\) of Zorn vector matrices over \(k\). By \((24.17)\) we have
\[C = \text{Ter}(D; D^3, h, \Delta), \quad D = k \oplus k, \quad D^3 = k_1 \oplus k_2 \oplus k_3, \quad h = \epsilon_1 \otimes 1_3, \\Delta(e_1 \wedge e_2 \wedge e_3) = 1, \quad e_i = e_i \otimes e_i \quad (1 \leq i \leq 3),\]
where \( (e_i)_{1 \leq i \leq 3} \) 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 \( \gamma \otimes \bar{\gamma} - 1 \) 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 (24.17) and obtain

\[
(x \times_h A^p y) = (x \times_h A^p y) \bar{p}^{-1} p = ((u_2 \times v_2) \oplus (u_1 \times v_1)) (\gamma \otimes \bar{\gamma} - 1) = (\gamma(\bar{u}_2 \times v_2)) \oplus (\bar{\gamma}^{-1}(u_1 \times v_1)).
\]

Repeating the computations of (24.17) we therefore conclude that \( \text{Zor}(k)^p \) is the \( k \)-module

\[
\begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix}
\]

under the multiplication

\[
\begin{pmatrix} \alpha_1 & u_2 \\ u_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} \beta_1 & v_2 \\ v_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \beta_1 - u_2^* v_1 & \alpha_1 v_2 + \beta_2 u_2 + \gamma^{-1}(u_1 \times v_1) \\ \beta_1 u_1 + \alpha_2 v_1 + \gamma(\bar{u}_2 \times v_2) & \alpha_2 \beta_2 - \bar{u}_1^* v_2 \end{pmatrix}
\]

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

\[
\begin{pmatrix} k & k e_1 \\ k e_1 & k \end{pmatrix} \subseteq \text{Zor}(k),
\]

it follows from Exc. [10] that \( \text{Zor}(k) \) and \( \text{Zor}(k)^p \) are isomorphic.

We proceed in several steps.

1\(^{st} \). We write \( (e_i)_{1 \leq i \leq 3} \) for the canonical basis of unit vectors in \( k^3 \) and put

\[
E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ X_1 := \begin{pmatrix} 0 & -e_1 \\ e_1 & 0 \end{pmatrix}, \ X_2 := \begin{pmatrix} 0 & -e_2 \\ e_2 & 0 \end{pmatrix}.
\]

Then (24.17) implies

\[
X_1 := X_1 X_2 = \begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix}, \ X_1^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_c = X_2^2,
\]

\[
X_1 X_2 X_1 = X_2 X_1 = \begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix} \begin{pmatrix} 0 & -e_1 \\ e_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & e_2 \\ e_2 & 0 \end{pmatrix} = -X_2.
\]

Moreover, since \( E \) is an elementary idempotent, we have

\[
\bar{E} = 1_c - E = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},
\]

and using (20.3), 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 (24). Now observe that an easy computation yields

\[
E X_i = \begin{pmatrix} 0 & -e_i \\ 0 & 0 \end{pmatrix}, \ E X_3 = \begin{pmatrix} 0 & e_3 \\ 0 & 0 \end{pmatrix} \quad (i = 1, 2),
\]

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\(^{nd} \). Now let \( A \) be any unital \( k \)-algebra and suppose that \( e, x_1, x_2 \in A \) satisfy the relations
Then we put
\[ e_{12} := 1, \quad e_{21} := -1, \quad x_3 := x_1x_1. \]

Since (149), (150) yield \( x_2x_1x_2 = x_2x_1x_2x_1 = x \) and \( x_2x_1 = x_2^2x_3x_1 = -x_1x_2 = -x_3 \),
we obtain
\[ e_{ij} = -\delta_{ij}, \quad e^2 = e, \quad x_i^2 = 1_C, \quad x_i^3 = -1_C, \quad y_i^2 = y_i^3 = 0 \]
\[ x_iy_j = x_jy_i, \quad x_iy_i = e, \quad x_3y_3 = -e, \quad y_3x_3 = -e \]
\[ x_i = 0, \quad y_i = 0, \quad x_{i+j} = 0, \quad y_{i+j} = 0 \]
Next we put
\[ B := \ker + k\bar{e} + \sum_{i=1}^3 kx_i + \sum_{i=1}^3 ky_i \subseteq A \]
\[ (y_i := e_{xi}, \ 1 \leq i \leq 3) \]

and claim that the spanning elements of \( B \) as a \( k \)-module displayed in (152) satisfy the following multiplication rules.
\[ e^2 = e, \quad \bar{e}^2 = \bar{e}, \quad x_i^2 = 1_C, \quad x_i^3 = -1_C, \quad y_i^2 = y_i^3 = 0 \]
\[ (i, j) = (1, 2), \quad (i, j) = (1, 2), \quad (i, j) = (1, 2), \quad (i, j) = (1, 2), \quad (i, j) = (1, 2), \quad (i, j) = (1, 2) \]
\[ (i, j) = (1, 2), \quad (i, j) = (1, 2), \quad (i, j) = (1, 2) \]
\[ (i, j) = (1, 2), \quad (i, j) = (1, 2) \]

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 \( C \rightarrow A \) acting on the basis vectors of \( C \) exhibited in (10) according to
\[ E \rightarrow e, \quad \bar{E} \rightarrow \bar{e}, \quad X_i \rightarrow x_i, \quad EX_i \rightarrow y_i \]
\[ (1 \leq i \leq 3) \]
is the unique unital homomorphism satisfying the conditions of the problem. The kernel of this homomorphism is an ideal in \( C \), which, by Exc. 114, has the form \( \alpha C \) for some ideal \( \alpha \subseteq k \). Hence \( B \cong C/\alpha C \cong C \otimes (k/\alpha) \cong \text{Zor}(k/\alpha) \) as \( k \)-algebras.

3. It remains to establish (153)–(162), which we now proceed to do by making use, among other things, of Artin’s theorem (Cor. 155) allowing us to drop parentheses in products with at most two distinct factors.

**Proof of (153).** The first four relations are clear in view of (151). Moreover, by (149), (150),
\[ x_i^2 = x_1x_2x_1x_2 = -x_i^2 = -1_C, \quad y_i^2 = ex_iex_i = e\bar{e} = 0 \]
for \( i = 1, 2 \) and \( y_j^3 = ex_3ex_3 = -e\bar{e} = 0 \), which completes the proof.
Thus (i61).

Proof of (154). For $i = 1, 2$, the definitions and (151) yield $x_i y_i = x_i e x_i = \bar{e}, y_i x_i = e x_i^2 = e$, $x_3 y_3 = x_3 e y_3 = -\bar{e}, y_3 x_3 = e x_3^2 = -e,$ as desired.

Proof of (155). The first relation is obvious, the next three hold by definition (cf. (152)), while the remaining ones follow from $e y_i = e x_i = e y_i$ for $i = 1, 2, 3.$

Proof of (156). The first equation is again obvious. As to the next three, we apply (151), (153) to obtain $x_i e = e x_i^2 = \bar{e} x_i = x_i - e x_i = x_i - y_i$ for $i = 1, 2$ and $x_3 e = -x_3 e x_3^2 = \bar{e} x_3 = x_3 - e x_3 = x_3 - y_3$, as claimed.

Proof of (157) We have $\bar{e} x_i = x_i - e x_i = y_i, y_i \bar{e} = y_i - y_i e = y_i$ for $1 \leq i \leq 3$, hence the first three equations of (157), while (156) yields $y_i e = y_i - y_i e = y_i$ for $1 \leq i \leq 3$, which completes the proof.

Proof of (159). From (156) we deduce $x_i \bar{e} = x_i - x_i e = y_i, y_i \bar{e} = y_i - y_i e = y_i$ for $1 \leq i \leq 3$, and the assertion follows.

Proof of (159). Let $\{i,j\} = \{1,2\}.$ The first equation is already in (151). By the same token, $x_i x_j = e_j x_i x_j = e_j x_j$ yields the second equation. Applying (151), (157) and the left Moufang identity, we obtain $x_3 y_j = x_3 (e x_j) = e_j x_3 (e x_j) = e_j (x_3 e x_j) x_3 = e_j (e x_3 x_j) = e_j (x_3 x_j x_3) = e_j (x_3 x_j x_3)$, which completes the proof of (159).

Proof of (160). Let $i, j \in \{1,2\}$. Then (159) yields $x_i x_j = e_j x_i x_j = e_j x_j$, while this, (151), (158) imply $x_i \bar{x}_j = x_i x_j - (x_i e) x_i = e_j x_i + e_j (x_3 x_i x_i) = e_j (x_3 x_3 x_i) = e_j (x_3 x_3 x_i)$, which completes the proof.

Proof of (161). Let $\{i,j\} = \{1,2\}$. Then (153), (159), (156), (160) yield

$$x_i y_i = -x_i (e x_i) x_i^2 = - (x_i (e x_i) x_i^2) x_i = -(x_i (e x_i) x_i^2) x_i = -e_j (x_i (e x_i) x_i^2) x_i$$

$$= -e_j x_i x_j + e_j e x_j = -e_j x_i x_j - e_j x_i x_j,$$

$$y_i x_j = [x_i (e x_i) x_i^2 = x_i [x_i (e x_i) x_i^2] = x_i (x_i e) x_i = e_j x_i (x_i e) x_i = e_j x_i (x_i e) x_i]$$

$$= e_j (x_i x_j - x_i (y_j x_j)) = e_j (x_i x_j - x_i (y_j x_j)) = e_j (x_i x_j - x_i x_j + x_j x_3)$$

$$= e_j x_i - e_j x_j + e_j x_j - x_i x_j - y_i x_j,$$

hence (161).

Proof of (162). Again, let $\{i,j\} = \{1,2\}$. Then (156), (160), (155) yield $y_i y_j = y_i x_j - (e x_i) x_j e = e_j (x_i - y_j) - e (e x_i) x_j e = e_j (x_i - y_j) - e (e x_i) x_j e = e_j (x_i - y_j)$, and finally, $y_j y_1 = y_j x_3 - x_3 e = y_j x_3 - e x_3)$, which completes the entire proof.

$$h_2 (\chi (x) \times h_{b, \Delta} \chi (y), \chi (z)) = \Delta_2 (\chi (x) \wedge \chi (y) \wedge \chi (z)) = (\Delta_2 (\chi (x) \wedge \chi (y) \wedge \chi (z)) = \Delta_1 (x \wedge y \wedge z) = h_1 (x \wedge h_{b, \Delta} y, z) = h_1 (x \wedge h_{b, \Delta} y, z) \chi (z).$$

But $h_2$ is non-singular and $\chi$ is bijective. Hence (ii) holds.

(ii) $\implies$ (iii). We put $\varphi := I_0 \oplus \chi$ and use (ii) to compute, for all $a, b \in D, x, y \in M_1$,

$$\varphi (a \odot x) \varphi (b \odot y) = (a \odot \chi (x)) (b \odot \chi (y))$$

$$= (ab - h_2 \chi (x), \chi (y)) \odot (\chi (y) a + \chi (x) b + \chi (x) \times h_{b, \Delta} \chi (y))$$

$$= (ab - h_2 \chi (x), \chi (y)) \odot (\chi (y) a + x b + x \times h_{b, \Delta} y)$$

$$= \varphi ((a \odot x) (b \odot y)).$$

Thus $\varphi$ is an algebra homomorphism. Being obviously bijective, it satisfies (iii).
For the first part of the problem, we begin by assuming that $c$ is absolutely primitive. Then we have to show that a decomposition (1) with the properties stated thereafter exists. In order to do so, we consider the following cases.

**Case 1.** $C$ has rank $r$, for some $r = 1, 2, 4, 8$.

**Case 1.1.** $r = 1$. Then $C = k$, and $ε := c ∈ k$ is an absolutely primitive idempotent. By Prop. 25.4 the ideal $kε ⊆ k$ is free of rank one with basis $ε$ as a $k$-module. Hence the equation $(1 − ε)ε = 0$ implies $ε = ε = 1$. But then the assertion follows by setting $k^{(1)} := \{0\}, k^{(2)} := k, C^{(1)} := \{0\}, C^{(2)} := k, e^{(1)} := 0, e^{(2)} := 1$.

**Case 1.2.** $r > 1$. Then Lemma 22 shows that the idempotent $c ∈ C$ is elementary, so we have $nc(c) = 0, tc(c) = 1$. Employing the language of Exc. 84 we therefore conclude $ε^{(0)} = ε^{(2)} = 0, ε^{(1)} = 1$. This gives $k^{(0)} = k^{(2)} := \{0\}, k^{(1)} := k, C^{(0)} = C^{(2)} := \{0\}, C^{(1)} := C$, and the decomposition $C = C^{(1)} ⊕ C^{(2)}, e = e^{(1)} ⊕ 1_{C^{(2)}}$ yields the assertion.

**Case 2.** The rank function of $C$ is locally constant (see 10.4). There exists a decomposition of $X := Spec(k)$ into the disjoint union of finitely many non-empty open subsets $U_i ⊆ X, 1 ≤ i ≤ n$, such that the rank of $C$ is constant on each $U_i$ for $1 ≤ i ≤ n$. Here Exc. 21 yields a complete orthogonal system $\{ε_i\}_{1 ≤ i ≤ n}$ of $n$-zero idempotents in $k$ such that $U_i = D(ε_i) = Spec(ke_i)$ for $1 ≤ i ≤ n$. Observing the beginning of the solution to Exc. 84 we also obtain a natural identification $C_i := C_i = C ⊕ ke_i$ as $ke_i$-modules. Applying Case 1 to this set-up, we now find, for $1 ≤ i ≤ n$, a decomposition $ke_i = (ke_i)^{(1)} ⊕ (ke_i)^{(2)}$ as a direct sum of ideals, as well as a composition algebra $C_i^{(1)}$ over $(ke_i)^{(1)}$ and an elementary idempotent $c_i^{(1)} ∈ C_i^{(1)}$ such that $C_i = C_i^{(1)} ⊕ (ke_i)^{(2)}$ and $c_i := ε_iC = c_i^{(1)} ⊕ 1_{ke_i}^{(2)}$. Now it suffices to put

$$k^{(j)} := \sum_{i=1}^n (ke_i)^{(j)}, \quad C^{(1)} := \sum_{i=1}^n c_i^{(1)}, \quad c^{(1)} := \sum_{i=1}^n c_i^{(1)} (j = 1, 2)$$

and to note that, since the $c_i^{(1)} ∈ C_i^{(1)}$ are elementary idempotents for $1 ≤ i ≤ n$, so is $c^{(1)} ∈ C^{(1)}$. 

**Section 25**
Conversely suppose we have a decomposition \([1]\) with the properties stated thereafter, particularly \([2]\). Then \(c^{(1)} \in C^{(1)}\), being an elementary idempotent, is an absolutely primitive one by Prop. \([25, 6]\), while the idempotent \(1_i \otimes 2_i \in k^{(2)}\) is absolutely primitive for trivial reasons. In order to show that \(c \in C\) is absolutely primitive, it will therefore be enough to establish the following

Claim. Let \(k = k_1 \oplus k_2\) be a direct sum of ideals, \(A_i\) a \(k_i\)-algebra and \(c_i \in A_i\), an absolutely primitive idempotent for \(i = 1, 2\). Viewing \(A := A_1 \oplus A_2\) as a \(k\)-algebra in a natural way, \(c := c_1 \oplus c_2\) is an absolutely primitive idempotent in \(A\).

The straightforward verification of this claim is left to the reader.

It remains to show that the rank of \(C^{(1)}\) is nowhere equal to 1. Otherwise we would have \(c^{(1)}_p = k^{(1)}_p\) for some prime ideal \(p \subseteq k\), whence Case 1.1 above would imply that

\[
c^{(1)}_p = 1^{(1)}_p,
\]

is be an elementary idempotent of \(k^{(1)}_p\), a contradiction.

\(\text{Claim.}\) Let \(M \in \text{Spec}(k)\), \(L_c := \text{Im}(c), \tilde{L}_c := \text{Ker}(c) = L_c\), we then have

\[
k \otimes L_0 = L_c \otimes \tilde{L}_c = L_c \oplus L_{\tilde{c}}
\]

as a direct sum of submodules. Hence \(L_c\) and \(L_{\tilde{c}}\) are both finitely generated projective \(k\)-modules.

For \(p \in \text{Spec}(k)\), we have \(c_p \neq 0 \neq \tilde{c}_p\) since \(c\) is elementary, so \((L_c)_p = L_{c_p}\) and \((L_{\tilde{c}})_p = L_{\tilde{c}_p}\) are both free \(k_p\)-modules of positive rank. On the other hand, \([163]\) yields \(\text{rk}_p(L_c) + \text{rk}_p(L_{\tilde{c}}) = 2\), which altogether implies \(\text{rk}_p(L_c) = \text{rk}_p(L_{\tilde{c}}) = 1\). Hence \(L_c\) is a line bundle, as claimed.

(ii) \(\Rightarrow\) (iii). Regardless of whether the idempotent \(c\) is elementary or not, \([163]\) holds, forcing \(L_c\) and \(L_{\tilde{c}}\) to be finitely generated projective \(k\)-modules. Now suppose as in (ii) that \(L_c\) is a line bundle. Then \([12, \text{III, } \S 7, \text{Cor. of Prop. } 10]\) implies

\[
L_0 \cong k \otimes L_0 \cong \bigwedge^2_k(k \otimes L_0) \cong \bigwedge^2(L_c \otimes L_{\tilde{c}}) \cong L_c \otimes L_{\tilde{c}}.
\]

Thus \(L_{\tilde{c}} \cong L_0 \otimes L_{\tilde{c}}^*\) is a line bundle as well, and we have established \([3]\). At this stage, we require the following well known

Fact. Let \(M, N\) be finitely generated projective \(k\)-modules. Then there is a natural identification \(\text{Hom}_k(M, N) = N \otimes M^*\) such that \((y \otimes x')(x') = (x', x')y\) for all \(x' \in M, y \in N, x' \in M^*\).

Using this and \([3]\), we now obtain a chain of natural isomorphisms as follows:

\[
B \cong \text{End}_k(k \otimes L_0) \cong \text{End}_k(L_c \oplus L_{\tilde{c}}) \cong \text{End}_k\left(\begin{array}{c}
L_c \\
L_{\tilde{c}}
\end{array}\right)
\]

\[
\cong \left(\begin{array}{c}
\text{Hom}_k(L_c, L_c) & \text{Hom}_k(L_c, L_{\tilde{c}}) \\
\text{Hom}_k(L_{\tilde{c}}, L_c) & \text{Hom}_k(L_{\tilde{c}}, L_{\tilde{c}})
\end{array}\right) \cong \left(L_c \otimes L_{\tilde{c}}^* \ L_c \otimes L_{\tilde{c}}^* \ L_{\tilde{c}} \otimes L_{\tilde{c}}^* \ L_{\tilde{c}} \otimes L_{\tilde{c}}^*\right) \cong B' := \text{End}_k(k \otimes L)
\]

with \(L := L_0 \otimes L_{\tilde{c}}^*\) an appropriate line bundle over \(k\). Writing \(\Phi : B \to B'\) for the composite of these isomorphisms, and following step-by-step their effect on the idempotent \(c\), we conclude

\[
\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},
\]

which completes the proof of (ii). Now suppose \(L\) is any line bundle over \(k\) such that there exists an isomorphism \(\Phi : B \to B' := \text{End}_k(k \otimes L)\) satisfying \([164]\). Then \(L \cong \mathcal{B}_2^1(\Phi(c)) \cong \mathcal{B}_2^1(c), L^* \cong \mathcal{B}_2^1(\Phi(c)*) \cong \mathcal{B}_2^1(c*)\).
$B'$, which not only shows that $L$ is unique up to isomorphism but also completes the proof of (3).

(iii) $\Rightarrow$ (4). Since $\Phi(c)$ is obviously elementary, so is $c$.

(b) Let $g \in \text{GL}(k \oplus L_0) = B^e$ such that $d = gcg^{-1}$. Then

$$L_d = d \left( \begin{array}{c} k \\ L_0 \end{array} \right) = gcg^{-1} \left( \begin{array}{c} k \\ L_0 \end{array} \right) = gc \left( \begin{array}{c} k \\ L_0 \end{array} \right) = g(L_0).$$

Hence $g$ determines via restriction an isomorphism $L_0 \xrightarrow{\sim} L_d$. Conversely, suppose $L_0$ and $L_d$ are isomorphic. Then, by (3), so are $L_0$ and $L_d$. Let

$$\rho : L_0 \xrightarrow{\sim} L_d, \quad \bar{\rho} : L_0 \xrightarrow{\sim} L_d$$

be isomorphisms. Then so is

$$g := \rho \oplus \bar{\rho} : k \oplus L_0 = L_0 \oplus L_0 \xrightarrow{\sim} L_d \oplus L_d = k \oplus L_0,$$

which amounts to $g \in \text{GL}(k \oplus L_0) = B^e$. Moreover, for $x \in L_d$, $y \in L_d$ we have $\rho^{-1}(x) \in L_e$, $\rho^{-1}(y) \in L_e$, hence

$$gcg^{-1}(x+y) = gc(\rho^{-1}(x) + \rho^{-1}(y)) = (\rho \oplus \bar{\rho})(\rho^{-1}(x)) = x.$$

But this means $gcg^{-1} = d$, and $c, e$ 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 (3) implies $L^{22}_e \cong L^{22}_d$.

Conversely, let this be so and put $L := L_0 \oplus L_0$. Then (iii) yields isomorphisms $\Phi : B \xrightarrow{\sim} B' := \text{End}_k(k \oplus L)$, $\Psi : B \xrightarrow{\sim} B'$ such that

$$\Phi(c) = \left( \begin{array}{c} 1 \\ 0 \\ 0 \\ 0 \end{array} \right) = \Psi(d).$$

Hence $\varphi := \Psi^{-1} \circ \Phi$ is an automorphism of $B$ sending $c$ to $d$.

(c) By (3), the line bundle $L_e$ is a direct summand of $k \oplus L_0$. Conversely, let $L$ be a direct summand of $k \oplus L_0$. 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.

117. (a) Let $x_i/1$ be a basis of $L_i$ over $k$, for $i = 1, \ldots, n$. Given $x \in L$, there exist $m \in \mathbb{N}$ and $a_1, \ldots, a_n \in k$ such that $x/1 = (a_i/f_i^{m_i})x_i/1 = (a_i/x_i)^{f_i^{m_i}}$ in $L_i$ for all $i = 1, \ldots, n$. Hence for some integer $p \geq m$ and all $i = 1, \ldots, n$, $f_i^{p}x = \beta_i x_i$, $\beta_i := f_i^{p - m}a_i$. Since the $f_i^{p}$ continue to generate $k$ as an ideal, we find $g_1, \ldots, g_n \in k$ such that $\sum f_i^{p}g_i = 1$. This implies $x = \sum \beta_i g_i x_i$, so $L = \sum k x_i$ is generated by $x_1, \ldots, x_n$.

(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 ($= \text{second exterior powers}$), we obtain $L \oplus L' \cong k$, i.e., $L' \cong L^e$.

(ii) $\Rightarrow$ (iii). This is Exc. 116 for $L_0 := k$.

(iii) $\Rightarrow$ (iv). Write

$$c = \begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix}$$

with $a, b, \gamma, \delta \in k$. Since $c$ has trace 1 and determinant 0, we have

$$a + \delta = 1, \quad a\delta = b\gamma.$$  (165)
From Exc. \[116\] we deduce
\[
\mathcal{L} \cong \mathcal{L}_c = \text{Im}(c) = k \left( \frac{\alpha}{\gamma} \right) + k \left( \frac{\beta}{\delta} \right).
\]

Observing
\[
\beta \left( \frac{\alpha}{\gamma} \right) = \alpha \left( \frac{\beta}{\delta} \right), \quad \delta \left( \frac{\alpha}{\gamma} \right) = \gamma \left( \frac{\beta}{\delta} \right),
\]
we now put \(f_1 = \alpha, f_2 = \delta\). Then \(k f_1 + k f_2 = k\) by \[165\], and \[166\] shows that \(L_{f_1}\) is the free \(k f_1\)-module of rank 1 with basis \(\left( \frac{\alpha}{\beta} \right)\), while \(L_{f_2}\) is the free \(k f_2\)-module of rank 1 with basis \(\left( \frac{\beta}{\gamma} \right)\).

Thus (iv) holds.

(iv) \(\Rightarrow\) (i). This is just a special case of (a).

Now suppose \(\mathcal{L}\) satisfies one (hence all) of the preceding four conditions. Then, by (ii), so does \(\mathcal{L}'\), allowing us to assume \(n > 0\). But then (iv) holds for \(\mathcal{L}^{\otimes n}\). In particular, by (ii), an elementary idempotent \(c^{(n)} \in \text{Mat}_2(k)\) satisfying \(\mathcal{L}^{\otimes n} \cong \mathcal{L}_{c^{(n)}}\) exists for any \(n \in \mathbb{Z}\) and is unique up to conjugation by inner automorphisms (Exc. \[116\] (b)). Since \(\mathcal{L}^{\otimes 0} \cong k\) is free of rank 1, we may put \(c^{(0)} = \left( \begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix} \right)\). Moreover, combining (ii) with (3) in Exc. \[116\] we may also put \(c^{-1} := \bar{c} = 1 - c\), and it will be enough to treat the case \(n > 0\).

We begin by proving (167), which follows from the computation
\[
\alpha^n a_n + \delta^n \delta_n = 1,
\]
where
\[
a_n := \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i, \quad \delta_n := \sum_{i=0}^{n-1} \binom{2n-1}{n+i} \alpha^{2n-1-i} \delta^i,
\]
and
\[
c^{(n)} := \left( \begin{array}{cc} \alpha^n a_n & \beta^n \delta_n \\ \gamma^n a_n & \delta^n \delta_n \end{array} \right) \in \text{Mat}_2(k)
\]
is an elementary idempotent satisfying \(\mathcal{L}_{c^{(n)}} \cong \mathcal{L}_{c^{(n)}}^{\otimes n}\).

We begin by proving (167), which follows from the computation
\[
\alpha^n a_n + \delta^n \delta_n = \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i + \sum_{i=0}^{n-1} \binom{2n-1}{n+i} \alpha^{2n-1-i} \delta^i
\]
\[
= \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i + \sum_{j=0}^{n-1} \binom{2n-1}{j} \alpha^{2n-1-j} \delta^j
\]
\[
= \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{2n-1-i} \delta^i = (\alpha + \delta)^{2n-1} = 1.
\]

Combining (167) with (166), we conclude that \(c^{(n)}\) as defined in (168) has trace 1 and determinant 0, hence is an elementary idempotent. Moreover,
\[
\beta^n \left( \frac{\alpha^n}{\gamma^n} \right) = \alpha^n \left( \frac{\beta^n}{\delta^n} \right), \quad \delta^n \left( \frac{\alpha^n}{\gamma^n} \right) = \gamma^n \left( \frac{\beta^n}{\delta^n} \right).
\]

We now put
\[
f^{(n)} := \alpha^n a_n, \quad g^{(n)} := \delta^n \delta_n
\]
and have \( f(i) + g(i) = 1 \) by (167). Setting \( L := L_e \), \( L_{c(i)} \), we must show \( L_{\alpha(n)} \cong L_{\beta(n)} \). To this end, we examine the situation of \( k_{\alpha(n)} \) and \( k_{\beta(n)} \).

Over \( k_{\alpha(n)} \), the quantities \( \alpha, \alpha_e, \) are both invertible. By (166), therefore, \( L_{\alpha(n)} \) is the free \( k_{\alpha(n)} \)-module with basis \( (\frac{\alpha_r}{l_r}) \). Consequently, \( (L_{\alpha(n)})_{\alpha(n)} = (L_{\alpha(n)})_{\beta(n)} \) is the free \( k_{\beta(n)} \)-module with basis \( (\frac{\alpha_r}{l_r}) \). By the same token, \( (L_{\alpha(n)})_{\beta(n)} = (L_{\alpha(n)})_{\alpha(n)} \) is the same as the free \( k_{\alpha(n)} \)-module with basis \( (\frac{\alpha_r}{l_r}) \)

\[ \Phi^{(\alpha)} : (L_{\alpha(n)})_{\alpha(n)} \cong (L_{\beta(n)})_{\beta(n)} \text{ such that } \Phi^{(\alpha)}((\frac{\alpha_r}{l_r})) = (\frac{\alpha_r}{l_r}). \]

Similarly, by (170), the quantities \( \delta, \delta^{(\alpha)} \) are invertible over \( k_{\beta(n)} \), and there is a unique isomorphism

\[ \Psi^{(\beta)} : (L_{\beta(n)})_{\beta(n)} \cong (L_{\alpha(n)})_{\alpha(n)} \text{ such that } \Psi^{(\beta)}((\frac{\beta_r}{l_r})) = (\frac{\beta_r}{l_r}). \]

Over \( k_{\beta(n)} \), the quantities \( \alpha, \alpha_0, \delta, \delta, \beta, \gamma \) become invertible, and we have \( (\frac{\beta}{l_r}) = \gamma^{-1} \delta (\frac{\gamma}{l_r}) \), hence \( (\frac{\beta}{l_r}) = \gamma^{-1} \delta^{(\alpha)} (\frac{\gamma}{l_r}) \). Hence the isomorphisms \( \Phi^{(\alpha)}, \Psi^{(\beta)} \) agree over \( k_{\beta(n)} \) and thus glue to an isomorphism \( L_{\alpha(n)} \cong L_{\beta(n)} \). This completes the proof.

Remark. The final proof of this exercise would have become much more natural if we had used the identification of \( \text{Pic}(k) \) with \( H_2(k, GL_1) \).

(i) \( \Rightarrow \) (ii). Let \( L \) be any line bundle over \( k \) that is a direct summand of \( k \oplus L_0 \). By Exc. 116(c), there exists an elementary idempotent \( e \in B \) such that \( L \cong L_e \). Using (i) to select an isomorphism \( \Phi : B \cong B' \), we obtain an elementary idempotent \( e' := \Phi(e) \in B' \) and, again by Exc. 116, we find \( L' := L_e \) a line bundle over \( k \) that is a direct summand of \( k \oplus L_0' \), and \( B' \cong B \). Set \( L_0 \cong L_{c(i)} \cong L_{c(i)}^\oplus \langle 0 \rangle \cong k \oplus L_0' \), \( B' \cong B \), and \( B' \cong B \). Hence the isomorphisms \( \Phi^{(\alpha(n))}, \Psi^{(\beta(n))} \) agree over \( k_{\beta(n)} \) and thus glue to an isomorphism \( L_{\alpha(n)} \cong L_{\beta(n)} \). This completes the proof.

(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 (ii). By Exc. 116(c), there exist elementary idempotents \( e \in B, e' \in B' \) such that \( L \cong L_e, L' \cong L_{c(i)} \). Now (i) holds.

and Exc. 116(a) produces isomorphisms \( \Phi : B \cong C := \text{End}_k(k \oplus M), \Phi' : B' \cong C \) sending \( e, e' \) to \( \{ 0 \} \), respectively. In particular, \( \Phi^{-1} \circ \Phi \) is an isomorphism from \( B' \) to \( B \), and (i) holds.

We apply Exc. 118 to \( B : = \text{End}_k(k \oplus L_0), L_0 \cong L, B' := \text{Mat}_2(k) \cong \text{End}_k(k \oplus L'_0), L'_0 := k \).

Then \( M := k \oplus \{ 0 \} \cong (k \oplus L_0) \) 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. 118 yields a line bundle \( M' \cong k \oplus L_0' = k \oplus k \), which is a direct summand of \( k \oplus k \) and satisfies \( L_0 \cong M_0 \oplus M_0 \cong L_0' \oplus M_0 \). This means \( L_0 \cong M_0 \oplus M_0 \). Moreover, \( k \oplus M = M_0 \oplus M_0 \) as well, and taking determinants (= second exterior powers), we obtain \( M_0 \cong M_0 \cong k \). Hence \( M_0 \cong M_0 \), being a homomorphic image of \( k \oplus k \), is generated by two elements.

Conversely, suppose \( L_0 \cong M_0 \) for some line bundle \( M_0 \) on two generators over \( k \). Then Exc. 117(b) implies \( M_0 \cong M_0 \cong k \). Since \( L_0 \cong M_0 \oplus k \cong k \), we deduce from Exc. 118 that \( B \) and \( B' = \text{Mat}_2(k) \) 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 \( \text{Pic}(k) \). By what we have just shown, the quaternion algebra
Let \( B := \text{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix} \)

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. [117](b).

By Exc. [119] the quaternion algebra

\[ B := \text{End}_k(k \oplus L^*) = \begin{pmatrix} k & L^* \\ L^* & k \end{pmatrix} \]

is split since \( L^* \) is the square (in \( \text{Pic}(k) \)) of some line bundle on two generators over \( k \). Computing the norm of \( B \) in two ways by means of \([25.9][1]\), we deduce \( h_l h_r \cong h_l \triangleleft (-h_l) \cong h_l h_l^* \) and hence obtain the first assertion. As to the second, it suffices to consult Exc. [47] which shows that the hyperbolic plane \( h_l \) is not split.

Localizing if necessary, we may assume that \( M \) is free (of rank 3). Let \( (e_i)_{1 \leq i \leq 3} \) be a basis of \( M \) and \( (e_i^*)_{1 \leq i \leq 3} \) the corresponding dual basis of \( M^* \). Setting \( \alpha := \theta(e_i \wedge e_j \wedge e_k) \), \( \beta := \theta^{-1}(e_i^* \wedge e_j^* \wedge e_k^*) \), we apply \([25.11][1]\) to conclude \( \alpha \beta = 1 \). In particular, \( \alpha \) and \( \beta \) are both invertible.

Letting \((i j l)\) vary over the cyclic permutations of \((123)\) and \( s = 1, 2, 3 \), we now apply \([25.11][2]\) to obtain \( (e_i \times_0 e_j, e_k) = \theta(e_i \wedge e_j \wedge e_k) = \alpha \delta_{ij} = (\alpha e_i^*, e_k) \) and \( (e_i^*, e_j^* \times_0 e_k^*) = \theta^{-1}(e_i^* \wedge e_j^* \wedge e_k^*) = \beta \delta_{ij} = (\beta e_i, e_j) \), which amounts to

\[ e_i \times_0 e_j = \alpha e_i^*, \quad e_i^* \times_0 e_j^* = \beta e_i. \quad (171) \]

Now observe that our asserted equations are alternating in \( u, v \) (resp. \( u^*, v^* \)). For the first equation, we may therefore assume \( u = e_i, v = e_j, w^* = e_l \). Then \([171]\) yields

\[
(e_i \times_0 e_j) \times_0 e_k^* = \alpha e_i^* \times_0 e_j^* = \begin{cases} \alpha \beta e_j & \text{for } s = i, \\ -\alpha \beta e_l & \text{for } s = j, \\ 0 & \text{for } s = l \end{cases}
\]

\[ = \begin{cases} e_j & \text{for } s = i, \\ -e_l & \text{for } s = j, \\ 0 & \text{for } s = l \end{cases}
\]

\[ = (e_i^*, e_j) - (e_i^* e_j) e_l,
\]

as claimed. Similarly, for the second equation, we may assume \( u^* = e_i^*, v^* = e_j^*, w = e_l \) and obtain

\[
(e_i^* \times_0 e_j^*) \times_0 e_k = \beta e_i \times_0 e_k = \begin{cases} \alpha \beta e_j^* & \text{for } s = i, \\ -\alpha \beta e_l^* & \text{for } s = j, \\ 0 & \text{for } s = l \end{cases}
\]

\[ = \begin{cases} e_j^* & \text{for } s = i, \\ -e_l^* & \text{for } s = j, \\ 0 & \text{for } s = l \end{cases}
\]

\[ = (e_i^*, e_j) - (e_i^* e_j^*) e_l^*.
\]

This completes the proof.

Let \( D := k \oplus k \) be the split quadratic étale \( k \)-algebra, \((M, h)\) a ternary hermitian space over \( D, \Delta : \otimes^3(M) \to D \) a volume element of \( M \) and \( C := \text{Ter}(D, M, h, \Delta) \) the octonion algebra over \( k \) arising from these data by means of the ternary hermitian construction. We wish to relate \( C \) to an octonion algebra of appropriately defined twisted Zorn vector matrices. In order to do so, we
perform the following steps.

1. We put \( c_1 := 1 \oplus 0 \in D, \ C_2 := \bar{c}_1 = 0 \oplus 1 \in D \) and have

\[
D = \kappa c_1 \oplus \kappa c_2
\]
as a direct sum of ideals. Moreover, \( k c_i = D c_i \) for \( i = 1, 2 \) are \( D \)-algebras in a natural way, and \( k c_i \cong k \) as \( k \)-algebras.

2. From 1 and what we have seen in the solution to Exc. 84, we deduce

\[
M = M_1 \oplus M_2, \quad M_i := M \otimes_D (k c_i) = M c_i \quad (i = 1, 2)
\]
as a direct sum of ideals. Moreover, \( \kappa c_i \) is a \( D \)-module of \( \kappa \)-submodules. In obvious notation, we now claim

\[
\bigwedge^3(M) = \bigwedge^3(M_1) \oplus \bigwedge^3(M_2)
\]
as right \( D \)-modules, where \( D \) acts diagonally on the right-hand side. Indeed, since taking exterior powers is compatible with base change \([12, III, \S 7, Prop. 8]\), we apply (172) and obtain

\[
\bigwedge^3(M) = \bigwedge^3(M \otimes_D (k c_i)) = \bigwedge^3(M) \otimes_D (k c_i) = \bigwedge^3(M) c_i \quad (i = 1, 2)
\]
hence the assertion. Note by (172) that \( M_i \) for \( i = 1, 2 \) is a finitely generated projective \( k \)-module of rank 3.

3. We now examine how the hermitian form \( h \) behaves with respect to the decomposition (172). For \( i, j = 1, 2, x_i \in M_i, y_j \in M_j \), the equation

\[
h(x_i, y_j) = h(x_i c_1, y_j c_2) = \bar{c}_1 h(x_i, y_j) c_j = h(x_i, y_j)(1 - c_1) c_j = (1 - \delta_j) h(x_i, y_j) c_j
\]
amounts to

\[
h(M_i, M_i) = \{0\}, \quad h(M_{3-i}, M_i) \subseteq k c_i \quad (i = 1, 2)
\]
In particular, there exists a \( k \)-bilinear form \( \beta : M_1 \times M_2 \to k \) such that \( h(x_1, y_2) = \beta(x_1, y_2) c_2 \), hence

\[
h(x_2, x_1) = \bar{h}(x_1, y_2) = \bar{\beta}(x_1, y_2) c_2 = \beta(x_1, y_2) \bar{c_2} = \beta(x_1, y_2) c_1
\]
for all \( x_1 \in M_1, y_2 \in M_2 \). Summing up, and consulting (175) again, we conclude

\[
h(x_1 \oplus y_1, x_2 \oplus y_2) = \beta(x_2, y_1) c_1 + \beta(x_1, y_2) c_2 = \beta(x_2, y_1) \oplus \beta(x_1, y_2)
\]
for \( x_i \in M_1, y_i \in M_2, i = 1, 2 \).

4. Suppose \( y_2 \in M_2 \) satisfies \( \beta(M_1, y_2) = \{0\} \). Then (176) yields \( h(x_1 \oplus y_1, 0 \oplus y_2) = 0 \) for all \( x_1 \in M_1, y_1 \in M_2 \), hence \( y_2 = 0 \). On the other hand, let \( \lambda : M_1 \to k \) be any \( k \)-linear form. Then

\[
\lambda \oplus 0 : M = M_1 \oplus M_2 \to k \oplus k = D
\]
is a \( D \)-linear form, and non-singularity of \( h \) yields unique elements \( x_1 \in M_1, y_1 \in M_2 \) such that \( (\lambda \oplus 0)(x_2 \oplus y_2) = h(x_1 \oplus y_1, x_2 \oplus y_2) \) for all \( x_2 \in M_1, y_2 \in M_2 \). By (176) this means \( \lambda(x_2) = \beta(x_2, y_1) \) for all \( x_2 \in M_1 \), and we have shown that the natural map

\[
M_2 \overset{\lambda}{\longrightarrow} M_1^*, \quad y \longmapsto \beta(-, y)
\]
induced by \( \beta \) is an isomorphism. Since the ternary hermitian construction is functorial (Exc. 113), we may identify \( M_2 \cong M_1^* \), and then have \( \beta(x, y^*) = (y^*, x) \) for all \( x \in M_1, y^* \in M_1^* \). Hence (172) and (176) imply
\[ M = M_1 \oplus M_2'. \quad h(x_1 \oplus y_1', x_2 \oplus y_2') = (y'_1, x_2) \oplus (y'_2, x_1) \quad (x_i \in M_1, y'_i \in M_2', i = 1, 2). \]  \hspace{1cm} (177)

Incidentally, it is straightforward to check that, conversely, the right-hand side of (177) determines a non-singular hermitian form on the right D-module \( M_1 \oplus M_2'. \)

5. We now turn to the volume element \( \Delta \) of \( M \). By (173), we obtain induced volume elements \( \theta: \wedge^3(M_1) \to k, \theta': \wedge^3(M_2') \to k \) such that

\[ \Delta \left( (x_1 \oplus y_1') \wedge (x_2 \oplus y_2') \wedge (x_3 \oplus y_3') \right) = \theta(x_1 \wedge x_2 \wedge x_3) \oplus \theta'(y_1' \wedge y_2' \wedge y_3') \]  \hspace{1cm} (178)

for all \( x_i \in M_1, y'_i \in M_2', i = 1, 2, 3 \). Note that \( \wedge^3(M_1') = (\wedge^3(M_1))^* \) under the identification (24.6).

Since the \( \Delta \)-determinant of \( h \) is 1, consulting (24.7) and (24.4) yields

\[ \theta(x_1 \wedge x_2 \wedge x_3) \theta'(v_1' \wedge v_2' \wedge v_3') \oplus \theta(u_1 \wedge u_2 \wedge u_3) \theta'(y_1' \wedge y_2' \wedge y_3') = \theta \theta' \]  \hspace{1cm} (179)

Comparing the first components of both sides, we conclude \( \theta(x_1 \wedge x_2 \wedge x_3) \theta'(v_1' \wedge v_2' \wedge v_3') = \det(\langle v'_i, x_j \rangle)_{1 \leq i, j \leq 3} \), which in view of (25.11.1) shows \( \theta' = \theta^{-1} \). Thus, taking into account (178) and the identification (173), we finally end up with

\[ \Delta = \theta \oplus \theta^{-1}. \]  \hspace{1cm} (179)

6. The preceding formula will enable us to decompose the vector product with respect to \( h, \Delta \) relative to the splitting (177). In order to do so, we let \( x_i \in M_1, y'_i \in M_2' \) for \( i = 1, 2, 3 \) and define \( u \in M_1, v = M_2' \) by

\[ (x_1 \oplus y_1') \times_{h, \Delta} (x_2 \oplus y_2') = u \oplus v. \]

Then \( \ldots \) yield

\[ \theta(x_1 \wedge x_2 \wedge x_3) \oplus \theta^{-1}(v'_1 \wedge v'_2 \wedge v'_3) = \Delta \left( (x_1 \oplus y_1') \wedge (x_2 \oplus y_2') \wedge (x_3 \oplus y_3') \right) \]

\[ = h \left( (x_1 \oplus y_1') \times_{h, \Delta} (x_2 \oplus y_2'), x_3 \oplus y_3' \right) \]

\[ = h(u \oplus v', x_3 \oplus y_3') = (v', x_3) \oplus (y'_3, u). \]

By \( \ldots \), therefore,

\[ \langle v', x_3 \rangle = \theta(x_1 \wedge x_2 \wedge x_3) = \langle x_1 \times \theta x_2, x_3 \rangle, \quad \langle y'_3, u \rangle = \theta^{-1}(y'_1 \wedge y'_2 \wedge y'_3) = \langle y'_3, y'_1 \times \theta y'_2 \rangle, \]

and since \( x_3, y'_3 \) are arbitrary, we deduce the final decomposition formula

\[ (x_1 \oplus y_1') \times_{h, \Delta} (x_2 \oplus y_2') = (y'_1, x_2) \oplus (x_1, y'_2) \]

\[ (x_i \in M_1, y'_i \in M_2', i = 1, 2). \]  \hspace{1cm} (180)

7. Finally, let \( \alpha, \beta \in k, \quad x_i \in M_1, \quad y'_i \in M_2' \) for \( i = 1, 2 \). Applying \( \ldots \), we obtain
Comparing this with \((25.11.3)\), we see that the map for \(I\) satisfying \(I = I_1\) thus there exists a natural number \(\ell\) such that \(I\) is an isomorphic of octonion algebras. This done, it is now clear that and how Thm. \([25.12]\) follows immediately from Thm. \([24.13]\).

Let \(C\) be a reduced octonion algebra over the Dedekind domain \(k\). By Thm. \([25.12]\) there exist a finitely generated projective \(k\)-module \(M\) of rank 3 and a volume element \(\theta\) of \(M\) such that \(C \cong \text{Zor}(M, \theta)\) in the sense of \([25.11]\). By [65, III, Exc. 13 (c)], we can find an ideal \(\alpha \subseteq k\) satisfying \(M \cong k^2 \oplus \alpha\). But \(\text{N}^\text{op}(M) \cong k\) by means of \(\theta\). By [12, III, Cor. of Prop. 10], therefore, \(\text{N}^\text{op}(k^2) \oplus \alpha \cong k \oplus \alpha\) is free of rank 1, forcing \(M\) to be free of rank 3. This yields identifications \(M = M^* = k^3\) that match \(\langle y, x \rangle\) with \(x^* y^*\) for \(x, y^* \in k^3\) and then lead to an isomorphism \(C \cong \text{Zor}(M, \theta) \cong \text{Zor}(k)\). Thus \(C\) is split.

For an ideal \(\alpha \subseteq k\), \(I := \alpha C \subseteq C\) is even a two-sided ideal. Conversely, passing from \(C\) to \(C^\text{op}\) if necessary, it will be enough to show that any right ideal \(I \subseteq C\) has the form as indicated. To this end, we consider the following cases.

Case 1. \(k = F\) is a field. Then we must show \(I = \{0\}\) or \(I = C\). If \(I\) contains invertible elements, then, clearly, \(I = C\). Otherwise, since \(C\) is conic alternative, Prop. \([20.4]\) shows that \(I \subseteq C\) is a totally isotropic subspace relative to \(nC\).

Case 1.1. \(t\text{c}\) vanishes identically on \(I\). Then \([19,5.5]\) shows \(I = I\), so the conjugation of \(C\) being an involutive implies that \(I \subseteq C\) is, in fact, a two-sided ideal. But then \(I = \{0\}\) by Exc. \([10]\).

Case 1.2. \(t\text{c} \neq 0\) on \(I\). Then some \(c \in I\) satisfies \(t\text{c}(c) = 1\), \(n\text{c}(c) = 0\). Thus \(c \in C\) is an elementary idempotent, and since we are working over a field, Thm. \([25.12]\) yields an identification \(C = \text{Zor}(k)\) such that

\[
c = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.
\]

Write \(C_{ij}\), \(i, j = 1, 2\), for the Peirce components of \(C\) relative to \(c\). Then \(C_{11} = kC \subseteq I, C_{12} = cC_{12} \subseteq I, \) which implies

\[
C_{21} = \begin{pmatrix} 0 & 0 \\ 0 & k^3 \end{pmatrix} = \begin{pmatrix} 0 & k^3 \\ 0 & 0 \end{pmatrix} = C_{12}C_{12} \subseteq I.
\]

But now \(\tilde{c} \in C_{22} = C_{22}C_{12} \subseteq I, \) hence \(I = C = C + \tilde{c} \subseteq I,\) and we conclude \(I = C\), as desired.

Case 2. \(k = \delta\) is a discrete valuation ring. We write \(p \subseteq \delta\) for the corresponding valuation ideal and \(k = \delta / p\) for the corresponding residue field. We may assume \(I \neq \{0\}\) and must show \(I = C\). Since \(\bigcap_{p \subseteq \delta} p = \{0\}\) and \(C\) is a free \(\delta\)-module of finite rank, we conclude \(\bigcap_{p \subseteq \delta} pC = \{0\}\) as well. Thus there exists a natural number \(r\) which is maximal with respect to the property \(I \subseteq p^rC\). In particular, \(I' := p^{-r}I \subseteq \delta\) is a right ideal, and the assumption \(I' \subseteq pC\) would imply the contradiction \(I = pI' \subseteq p^{r+1}C\). Hence \(I' \not\subseteq pC\). Consequently, \((I' + pC)/pC\) is a non-zero right ideal in the octonion algebra \(C(p)\) over the field \(k\), which by Case 1 must be all of \(C(p)\). Thus \(I' + pC = C\), and Nakayama’s lemma \([65, X, Lemma 4.2]\) implies \(I' = C\), hence \(I = pI' = pC\).

Case 3. The general case. By Exc. \([10]\) it will be enough to show that \(I \subseteq C\) is, in fact a two-sided
ideal, equivalently, that $I_p \subseteq C_p$ is a two-sided ideal for any prime ideal $p \subseteq k$. In order to do so, we may assume $I_p \neq \{0\}$, in which case the assertion follows immediately from Case 2.

### Section 25

The cases $s = 1$ and $s = r$ are obvious. Hence we may assume $1 < s < r$, which by Cor. 22.17 implies that $C, B, B'$ are all non-singular. Arguing by induction on $r - s$, we let $\varphi : B \rightarrow B'$ be an isomorphism. Then $C = B \sqcup B^\perp = B' \sqcup B'^\perp$, 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 (Cor. 26.6), $n_C_{|B^\perp}$ and $n_C_{|B'^\perp}$ are isometric. Since $s < r$, we have $\text{Supp}(B^\perp) = \text{Spec}(k)$, and applying Lemma 22.14 we find 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. 21.8 yields unique isomorphisms $h : \text{Cay}(B, \mu) = B \oplus B_1 \rightarrow B_1$ (resp. $h' : \text{Cay}(B', \mu) = B' \oplus B'_1 \rightarrow B'_1$) extending the identity of $B$ (resp. $B'$) and sending $j$ (resp. $j'$) to $l$ (resp. $l'$). The isomorphisms thus obtained fit into the diagram

$$
\begin{array}{ccc}
\text{Cay}(B, \mu) & \xrightarrow{h} & B_1 \\
\text{Cay}(B, \varphi) \cong & \cong & \cong \varphi_1 \\
\text{Cay}(B', \mu) & \xrightarrow{h'} & B'_1,
\end{array}
$$

which can be completed uniquely to a commutative square by the dotted isomorphism $\varphi_1 : B_1 \rightarrow B'_1$ 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 $B \subseteq \mathfrak{O}$ be a non-zero subalgebra and let $0 \neq x \in \mathfrak{O}$. Then $n_\mathfrak{O}(x) \neq 0$ and $B$ contains the element $x^2 = t_0(x)x - n_\mathfrak{O}(x)1_\mathfrak{O}$, hence $1_{\mathfrak{O}}$. Thus $B$ is a unital subalgebra of $\mathfrak{O}$ on which $n_\mathfrak{O}$ continues permit composition and to be anisotropic, hence non-singular as well since the characteristic is not 2. Summing up, therefore, $B \subseteq \mathfrak{O}$ is a composition division subalgebra. Form [26.11] we now conclude that $B$ is isomorphic to one of the algebras $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathfrak{O}$, and the Skolem-Noether theorem completes the proof.

### Section 26

Since $k$ is an integral domain, Exc. [54] yields a non-zero element $u \in C$ such that $n_C(u) = 0$. On the other hand, $k$ being a PID, $C$ is free of finite rank as a $k$-module. Letting $(\alpha_i)_{1 \leq i \leq r}$ be a $k$-basis of $C$, we write $u = \sum \alpha_i \epsilon_i$ for some $\alpha_1, \ldots, \alpha_r \in k$ not all zero. In fact, dividing by their greatest common divisor, we may assume that they are mutually prime, so we can find $\beta_1, \ldots, \beta_r \in k$ such that $\sum \alpha_i \beta_i = 1$. Since $C$ has rank $> 1$, it is non-singular, allowing us to consider the $Dn_C$-dual basis $(f_i)_{1 \leq i \leq r}$ of $C$ relative to $(\epsilon_i)$. Setting $\nu := \sum \beta_i f_i \in C$, we therefore obtain $n_C(u, \nu) = 1$. Thus $c := u\nu$ satisfies $nc(c) = 1$, $nc(c) = nc(u)uc(\nu) = 0$ and hence is an elementary idempotent. By Prop. 25.6, our composition algebra $C$ is therefore reduced. By Cor. 25.8 it is split if the rank is $2$. But by Prop. 25.10 and Thm. 25.12, the same conclusion holds also in ranks 4 and 8 since finitely generated projective $k$-modules are free.

### Section 27

By Prop. 26.2(b), $f$ preserves not only norms and units, but also traces and conjugations.

(a) Applying (20.3.2), we obtain

$$f(Ux) = nc(x, f(x) - nc(x)f(y) = nc(f(x), f(y))f(x) - nc(f(x))f(y) = Uf(x)f(y),$$

hence \([4]\). In order to prove \([5]\), we first note

$$\lambda^2 = U_1\lambda, \quad (U_{xy} - U_x - U_y)z = x(yz) + z(xy),$$

...
so by \( \mathbf{1} \), \( f \) preserves squares and the expression \( x(yz) + z(xy) \). Abbreviating the left-hand side of \( \mathbf{2} \) by \( A \) and using the fact that the associator of \( C \) is alternating, we can now compute

\[
A = f(xy)^2 - f(xy)(f(y)f(x)) - (f(x)f(y))f(xy) + f(x)f(y)^2f(x)
\]

\[
= f((xy)^2) - f(xy)(f(y)f(x)) - f(x)(f(y)f(xy)) - [f(x), f(y), f(xy)] + f(xy)^2x
\]

\[
= f(x, f(y), f(x)) + f((xy)^2 - (xy)(yx) - x(y(xy)) + xy^2x) = [f(x), f(xy), f(y)]
\]

since, thanks to Artin’s Theorem (Cor. 15.5), the subalgebra of \( C \) generated by two elements is associative. This completes the proof of \( \mathbf{2} \). In order to complete the proof of \( \mathbf{a} \), we will therefore suffice to show that the right-hand side of \( \mathbf{2} \) 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

\[
[f(y), f(xy), f(x)] = [f(y), f(x \circ y), f(x)] - [f(y), f(xy), f(x)] = [f(y), f(x) \circ f(y), f(y)] + [f(x), f(xy), f(y)] = [f(x), f(xy), f(y)]
\]

again by Artin’s Theorem, and the assertion follows.

(b) Since \( f \) preserves norms and traces, we have \( t_c(c') = t_c(f(c)) = t_c(1) = n_{c'}(c') = n_c(c) = 0 \), so \( c' \in C^\ast \) 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, \( f(x \circ y) = c' \circ f(y) \). Hence, writing \( \mathbf{C} \), \( i, j = 1, 2 \), for the Peirce components of \( C \) relative to \( c \), it will be enough to show

\[
\mathbf{C} = \{ x \in C \mid c \circ x = x \}
\]

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 \( \mathbf{1} \) is proved.

(a) We begin by assuming that the case of a local ring has been settled and then let \( k \) be arbitrary. We put \( X := \text{Spec}(k) \) and deduce from Exercise 40 (b), that

\[
X_+ := \{ p \in X \mid f_p : B_p \to B'_p \text{ is an isomorphism} \},
\]

\[
X_- := \{ p \in X \mid f_p : B_p \to B'_p \text{ is an anti-isomorphism} \}
\]

are Zariski-open subsets of \( X \). Since a quaternion algebra is not commutative, they are also disjoint, and our assumption implies that they cover \( X \). Now Exercise 41 yields a complete orthogonal system \( \{ e_i, e_\perp \} \) of idempotents in \( k \) satisfying \( X_+ = D(e_i) \). Now it suffices to put \( k_\pm = k e_\pm \) and to invoke (10.6)(b), which implies for any \( p_\pm \in \text{Spec}(k_\pm) \) that \( p := p_\perp \oplus k_\pm \in D(e_\perp) \) makes \( f_{p_\pm} = (f_p)_{e_\perp} \) (by (10.4)(b)) an isomorphism in case of the plus-sign and an anti-isomorphism in case of the minus-sign. Hence \( f_\pm \) is an isomorphism and \( f_\perp \) 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. Theorem 22.15(b) yields 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 Proposition 26.2, we conclude that \( D' := f(D) = k[u'] \), \( u' := f(u) \), is a quadratic étale subalgebra of \( B' \) (Proposition 22.5), and \( f|_D : D \to D' \) is an isomorphism (Proposition 26.4). Now apply Theorem 22.15(a) to reach \( B \) from \( D \) by means of the Cayley-Dickson construction; there exists a unit \( \mu \in k^\ast \) such that the inclusion \( D \to B \) extends to an identification \( B = \text{Cay}(D, \mu) = D \oplus D_j, j \in D^1, n_B(j) = -\mu \). Setting \( \tilde{f} := f(j) \in D' \subseteq B' \), we obtain \( n_B(\tilde{f}) = -\mu \) and from Proposition 26.6 we conclude that \( \tilde{f}|_D \) extends to a homomorphism \( g : B \to B' \) of conic algebras satisfying \( g(j) = \tilde{f} \). By Corollary 21.8 therefore, \( g \) is an isomorphism from \( B \) onto the subalgebra of \( B' \) generated by \( D' \) and \( \tilde{f} \). Counting ranks we conclude that \( g \) is in fact an isomorphism from \( B \) onto \( B' \). Hence \( f_1 := g^{-1} \circ f : B \to B \) is
a unital norm equivalence inducing the identity on $D$ and satisfying $f_1(j) = j$. Since $f_1$ stabilizes \( D^1 = D j \), we find a $k$-linear bijection $\varphi:\ D \to D$ such that $f_1(vj) = \varphi(v)j$ for all $v \in D$. Then $\varphi(1_D) = 1_D$, and since $n_D$ permits composition, $\varphi$ leaves $n_D$ invariant and is thus a unital norm equivalence of $D$, hence an automorphism (Proposition 26.4(b)). By §22 Exercise 103 therefore, we are left with the following cases.

Case 1. $\varphi = 1_D$. Then $f_1 = 1_D$, and $f = g: B \to B'$ is an isomorphism.

Case 2. $\varphi = t_B$. By §21 Exercise 93 the map $\psi: B \to B$ defined by $\psi(v + wj) := v - wj$ for all $v, w \in D$ is an automorphism, and one checks that $f_1 = \psi \circ \text{Int}(j) \circ t_B$, where $\text{Int}(j)$ stands for the inner automorphism $x \mapsto jxj^{-1}$ of $B$ affected by $j$. Hence $f = g \circ \psi \circ \text{Int}(j) \circ t_B: B \to B'$ is an anti-isomorphism.

(b) The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are obvious, so let us prove (i) under the assumption (iii).

By Corollary 26.3 there exists a unital norm equivalence $f: B \to B'$. With the notation of (3), we apply (a) to conclude that $g := f_\circ (f_\circ t_B): B \to B'$ is an isomorphism.

By Prop. 26.3(a), every automorphism of $B$ is a unital norm equivalence. Hence it suffices to show that, conversely, if $f: B \to B$ is a unital norm equivalence sending $e_{11}$ to $c$, then an automorphism of $B$ exists having the same property. From Exc. 127(b) we deduce that $c$ is an elementary idempotent in $B$. Hence Exc. 116(a) yields a line bundle $L$ over $k$ and an isomorphism

$$\Phi: B \xrightarrow{\sim} B':= \text{End}_k(k \oplus L) = \begin{pmatrix} k & L^* \\ L & k \end{pmatrix}$$

such that $\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Viewing $B_{12}(c) \oplus B_{21}(c)$ (resp. $L^* \oplus L$) canonically as quadratic submodules of $(B, n_B)$ (resp. $(B', n_{B'})$),

$$\Phi: B_{12}(c) \oplus B_{21}(c) \xrightarrow{\sim} L^* \oplus L$$

is an isometry and by \cite{25.11}, \cite{12.17}, there is a natural identification of $L^* \oplus L$ with the hyperbolic plane $\mathbb{H}_B$. On the other hand, $f$, being a unital norm equivalence, by Exc. 127(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 $\mathbb{H}_B$ is split, which by Exc. 47 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 $c$.

(a) By Prop. 26.2(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 $C = C^\varphi$, which by \cite{16.23} is equivalent to $q \in \text{Nuc}(C) = k_1C$ (Exc. 102(b)), hence to $p^3 = q^{-1} \in k_1C$.

(c) Assume $\varphi$ is an anti-automorphism of $C$. Then $C^{\varphi} = C^\varphi$, so we have $xy = (x^{\varphi^{-1}})(q^{\varphi})$, equivalently, $y(xq) = x(qy)$, for all $x, y \in C$. Setting $x = 1_C$ gives $qy = qy$ for all $y \in C$. By Exc. 102(b), this implies $q \in k_1C$ and then $xy = yx$ for all $x, y \in C$, a contradiction.

Let $p, q \in C^x$. By Exc. 90 $C(p, q)$ is a multiplicative conic alternative $k$-algebra with norm $n_{c(p, q)} = nc(pq)n_{c}$. By multiplicity, $L_{pq}$ is an isometry from $n_{c(p, q)}$ to $n_c$. Hence $C(p, q)$ is a composition algebra which is non-singular if $C$ is. Moreover, if $k$ is a semi-local ring, the norm equivalence theorem 26.7 shows that $C$ and $C(p, q)$ are isomorphic.

Let $x_i = u_i + v_i$, $u_i, v_i \in \mathcal{O}$, $i = 1, 2$ be non-zero elements of $\mathcal{O}$, then Exc. 99(a) for $\mu = -1$ shows that $x_iy_0 = 0$ if and only if $u_i \neq 0 = v_i$ for $i = 1, 2$ and

$$n_{c}(u_1) = c_{c}(v_1), \quad (u_1u_2)v_1 = -(u_1v_2)\bar{v}_1, \quad v_2 = (v_1\bar{u}_2)u_1^{-1}. \quad (182)$$

Now let $(w_i)_{1 \leq i \leq 7}$ be a Cartan-Shouten basis of $\mathcal{O}$ in the sense of \cite{2.1}. Combining \cite{21.34} with Fig. 1 of \cite{2.3} we compute

$$\begin{align*}
(w_1 + w_3)(w_2 - w_6j) &= (w_1w_2 - (-\bar{w}_6)w_3) + (w_3\bar{w}_2 - w_6w_1) \\
&= (w_1w_2 - w_6w_3) + (w_3w_2 - w_6w_1),
\end{align*}$$

where
where \( w_6 w_3 = w_4 = w_1 w_2 \) and \( w_6 w_4 = w_5 = -w_3 w_2 \). 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 \( (a, b) \in \text{Zer}(\mathbb{S}) \), while \( (182) \) (or the property of \( (w_i) \) being a Cartan-Shouten basis) yields
\[
w_6 = -(w_3 w_2) w_1^{-1} = -(w_3 w_2) w_1. \tag{183}
\]

We must show that the action of \( G \) on \( \text{Zer}(\mathbb{S}) \) is simply transitive. Let \( (x_1, x_2) \in \text{Zer}(\mathbb{S}) \) and write \( x_i = u_i + v_i \) with \( u_i, v_i \in \mathcal{O} \) for \( i = 1, 2 \) as before. Then \( (182) \) shows \( n_2(u_i) = n_2(v_i) \) for \( i = 1, 2 \), whence the relations \( n_2(x_i) = 2 \) imply \( n_2(u_i) = n_2(v_i) = 1 \). Consulting Exc. \( 29 \) (b), we also get \( n_2(u_1 u_2, v_1) = 0 \). By Exc. \( 3 \) therefore, the quantities \( u_1, u_2, v_1 \) can be extended to a Cartan-Shouten basis of \( \mathcal{O} \). Hence there exists an automorphism \( \sigma \) of \( \mathcal{O} \) sending \( u_1, u_2, v_1 \) respectively to \( w_1, w_2, w_3 \). Consulting \( (182), (183) \), 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 \( \sigma = 1_\mathcal{O} \). But this is clear since we then have \( \sigma(w_j) = w_j \) for \( i = 1, 2, 3 \), and \( w_1, w_2, w_3 \) by Exc. \( 6 \) generate the octonion algebra \( \mathcal{O} \).

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
\[
q^{2n-1}(q-1)(q^n - 1).
\]

In order to see this, we identify \((V, Q) = (\mathbb{F}_q^n \oplus \mathbb{F}_q^n, x \oplus y \mapsto x'y)\) and note for \( x \in \mathbb{F}_q^n \) that
\[
|\{ y \in \mathbb{F}_q^n | x'y = 0 \}| = \begin{cases} q^n & \text{for } x = 0, \\ q^{n-1} & \text{for } x \neq 0. \end{cases}
\]

Thus \( |\{ v \in V | Q(v) = 0 \}| = q^n + (q^n - 1)q^{n-1}, \) and we conclude that \((V, Q)\) contains precisely
\[
q^{2n} - q^n - (q^n - 1)q^{n-1} = q^n(q^n - 1) - (q^n - 1)q^{n-1} = (q^n - q^{n-1})(q^n - 1) = q^{n-1}(q-1)(q^n - 1)
\]
anisotropic vectors. The claim is proved.

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. \( 20.4 \)), and the norm of the split octonions is hyperbolic (Cor. \( 25.14 \)), the preceding claim reduces to the first equation for \( n = 3 \).

To prove the second equation, we note that \( n: C^\times \to \mathbb{F}_q^\times, x \mapsto n(x) := n_C(x) \), is a surjective multiplicative map. Writing \( N := \{ x \in C | n_C(x) = 1 \} \) for its “kernel”, we let \( x, y \in C^\times \), use Prop. \( 14.6 \) and obtain
\[
y \in n^{-1}(n(x)) \iff n(y) = n(x) \iff n(x^{-1}y) = 1 \iff x^{-1}y \in N \iff y \in xN,
\]
so the fibers of \( n \) all have the same cardinality. This shows \( |N| = |C^\times|/|\mathbb{F}_q^\times| = q^3(q^4 - 1). \)

(a) is trivial: if \( x \in M \) is not minimal, the \( x = y + z \) 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.** (a) If \( N \subseteq M \) is a submodule, then \( \text{Min}(M, Q) \cap N \subseteq \text{Min}(N, Q|_N) \).

(b) 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 \( \text{Min}(M, Q) = \text{Min}(N, Q|_N) \cup \text{Min}(N', Q|_{N'}) \).

In order to prove (a), let \( x \in \text{Min}(M, Q) \cap N \) 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 \( x \in \text{Min}(N, Q|_N) \). But note for \( x \in \text{Min}(N, Q|_N) \), that it is con-
ceivable 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 (a).

In order to prove (b), let \(x \in \text{Min}(M, Q)\) 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 \(\text{Min}(M, Q) \subseteq N \cup N'\), which implies

\[
\text{Min}(M, Q) = \text{Min}(M, Q) \cap (N \cup N') = (\text{Min}(M, Q) \cap N) \cup (\text{Min}(M, Q) \cap N').
\]

By symmetry and (a), it therefore suffices to show \(\text{Min}(N, Q|N) \subseteq \text{Min}(M, Q)\). Let \(x \in \text{Min}(N, Q|N)\) 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 \(x \in \text{Min}(M, Q)\).

We can now prove (c). Let \(x, y \in \text{Min}(M, Q)\) be inequivalent. For \(u \in [x], v \in [y]\), the assumption \(Q(u, v) \neq 0\) would imply that \(u, v \in \text{Min}(M, Q)\) are equivalent. Since \(M_q\) is spanned as a \(\mathbb{Z}\)-module by the minimal elements of \((M, Q)\) belonging to \([x]\), ditto for \(M_q\), this contradiction shows that \(M_q\) and \(M_q\) are orthogonal. But every \(x \in \text{Min}(M, Q)\) belongs to \(M_q\), and \(M\) is spanned by \(\text{Min}(M, Q)\) as a \(\mathbb{Z}\)-module. Thus \(M\) is the orthogonal sum of the distinct \(M_q\)'s, \(x \in \text{Min}(M, Q)\), and it remains to show that each \(M_q\) is indecomposable. Thanks to the obvious extension of (b) in the preceding lemma to more than two orthogonal summands, we may assume that each \(M_q\) is indecomposable. Indeed, suppose we have an orthogonal decomposition \(M = N \perp N'\) relative to \(Q\), with submodules \(N, N' \subseteq M\), and let \(x, y \in \text{Min}(M, Q)\). By part (b) of the lemma, we may assume \(x \in \text{Min}(N, Q|N)\), 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 \(Q(x_i, x_{i+1}) \neq 0\) for \(1 \leq i \leq k\). We claim \(x_i \in \text{Min}(N, Q|N)\) for all \(i = 0, \ldots, k\) and 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 (b) of the lemma implies \(x_i \in \text{Min}(N, Q|N)\), and the induction is complete. In particular, \(y \in \text{Min}(N, Q|N)\), and we have shown \(\text{Min}(M, Q) = \text{Min}(N, Q|N)\), which obviously implies \(M = N, N' = \{0\}\).

We put \(C^\perp = C/2C = C \otimes \mathbb{Z} \mathbb{F}_2\) as a conic algebra over \(\mathbb{F}_2\) and write \(x \mapsto x^3\) for the natural epimorphism from \(C\) to \(C^\perp\). This epimorphism canonically induces a map from \(C^\perp\) to \(C^\perp\), which may or may not be surjective. Note that, since the discriminant of \(C\) is odd, \(C^\perp\) is a composition algebra of dimension 8 over \(\mathbb{F}_2\), hence an octonion algebra and thus isomorphic to \(\text{Zor}(\mathbb{F}_2)\) (Cor. 25.14).

**Lemma 1.** For \(x, y \in C^\perp\) we have \(x^3 = y^3\) if and only if \(y = \pm x\).

Indeed, \(y = \pm x\) clearly implies \(x^3 = y^3\). 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

\[
1 = nc(x + 2z) = 1 + 2nc(x, z) + 4nc(z),
\]

hence \(nc(x, z) = -2nc(z)\), and applying the Cauchy-Schwarz inequality yields

\[
4nc(z)^2 = nc(x, z)^2 \leq nc(x, x)nc(z, z) = 4nc(z).
\]

But \(nc(z)\) is a positive integer, forcing \(nc(z) = 1\). 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 a unit in \(C\). Hence \(\alpha = -1\) and \(y = -x\).

We can now establish the first part of the problem. By Exc. 135 for \(q = 2\), we have \(|C^\perp| = 120\), while by Lemma 1, the fiber of an arbitrary element \(u \in C^\perp\) under the natural map \(C^\perp \to C^\perp\) is either empty or consists of two elements. Hence \(|C^\perp| \leq 240\).

For the rest of the proof, we may assume that \(|C^\perp| = 240\). Writing \(C^\perp\) for the image of \(C^\perp\) under the natural map \(C^\perp \to C^\perp\), and putting \(r := |C^\perp|\), we note that the fiber of any point in \(C^\perp\) consists of two elements. Thus \(2r = 240\), hence \(r = 120 = |C^\perp|\), and we conclude \(C^\perp = C^\perp\). In other words, the natural map \(C^\perp \to C^\perp\) is surjective.
37 Elementary idempotents and cubic Jordan matrix algebras

409

We can now prove that the positive definite integral quadratic lattice \((C, n_C)\) is indecomposable. We have \(C^\times = \{ x \in C | n_C(x) = 1 \} \subseteq \text{Min}(C, n_C)\), and for \(x, y \in C^\times\), Exc. 52 (b) yields a sequence \(x^1 = x_0, x_1, \ldots, x_i = y^1\) of elements in \(C^\times\) such that \(k \leq 2\) and \(n_C(x_{i-1}, x_i) \neq 0\) for \(1 \leq i \leq k\).

Since the natural map \(C^\times \to C^\times\) is surjective, each \(x_i\), \(1 \leq i \leq k\), lifts to an invertible element \(x_i \in C\), so we have a subsequence \(x = x_0, x_1, \ldots, x_k = y\) 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 \(C^\times \subseteq \text{I}_{C^\times}\). Now suppose that \(x \in \text{Min}(C, n_C)\) is not equivalent to \(1\).

From Exc. 134 (c) we deduce \(n_C(C^\times, x) = \{0\}\), which implies \(n_C(C^\times, x^1) = n_C(C^\times, x^1) = \{0\}\).

But \(C^\times\) is an octonion algebra over \(F\), which is spanned as a vector space by \(C^\times\) (Exc. 52 (a) and Prop. 20.4). Thus \(x^1 = 0\), hence \(x \in 2C\), and we conclude that the indecomposable submodules \(C_{[x]} \subseteq C\), with \(x \in \text{Min}(C, n_C)\) not equivalent to \(1\), 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. 134 (c), implies that \((C, n_C) = C_{[x]}\) is indeed indecomposable.

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 22.11 the trace form of \(R\) is surjective. Since \(\text{tr}(1_R) = 2\), we conclude that \(\text{tr}_C(u) = 2n + 1\) (for some integer \(n\)) is odd. In fact, replacing \(u\) by \(u - n \cdot 1_R\), we may assume \(\text{tr}_C(u) = 1\). Now Prop. 22.3 shows \(1 - 4n\) is ±1, which implies \(n = 0\) or \(n = \frac{1}{2}\). The latter option obviously being impossible, we conclude that \(R\) has zero divisors (Exc. 34), hence is split (Exc. 126). This solves the first part of the problem.

As to the second, assume \(\text{Hur}(\mathbb{H}) \cong \text{Cay}(R, \mu)\) 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 21.4 we conclude with \(d := \text{disc}(R)\) that \(d = 4d^2\mu^2\). On the other hand, since the norm of \(R \subseteq \text{Hur}(\mathbb{H})\) 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 \(2 = n\mu^2 = 4\mu(n\mu)^2 = 4n\mu(n\mu)^2 = 4n\mu\).

Hence neither \(C^\times\) is an octonion division algebra over the rationals, up to isomorphism actually the only one (Cor. 26.20). This shows \(C^\times \cong \text{Cay}(\mathbb{Q}, -1, -1, -1)\). In particular, the norm of \(C^\times\) 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 12 (c), up to isometry there is only one. Hence, by Cor. 26.2 we obtain a unit norm equivalence \(f: \text{Cox}(\mathbb{O}) \to \text{Cox}(\mathbb{O})\) by means of \(f\), we may actually assume \(C = \text{Cox}(\mathbb{O})\) as additive groups with \(1_C = 1_{\mathbb{O}}\) and \(n_C = n_{\text{Cox}(\mathbb{O})}\). In particular \(\text{Cox}(\mathbb{O}) = 240\) (Exc. 16 (d)).

(b) Put \(D := \text{Cox}(\mathbb{O})\). Then \(C^\times := C/2C = C \otimes_{\mathbb{Z}} \mathbb{F}_2\) and \(D^1 = D/2D = D \otimes_{\mathbb{Z}} \mathbb{F}_2\) are both octonion algebras over \(\mathbb{F}_2\), hence split (26.12) and, in particular, isomorphic. We therefore find an isomorphism \(\psi: C^\times \to D^1\) of \(\mathbb{F}_2\)-algebras. Note by the normalization provided in (a) that \((C^\times, n_C, 1_C) = (D^1, n_{\mathbb{O}}, 1_{\mathbb{O}})\) as “pointed” quadratic spaces over \(\mathbb{F}_2\). In particular, \(\psi\) is a bijection of the quadratic space \((C^\times, n_C)\). Applying 24 (Prop. 14), we see that the orthogonal group of this space is generated by the orthogonal transvections

\[ \tau_y: \quad x \mapsto x - \frac{n_C(a, x)}{n_C(a)} \]  

(a \in C^\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. 135 the natural map from \(C^\times\) to \(C^\times\) is surjective. Hence we can also lift \(\psi\) to an orthogonal transformation \(\phi\) of \((C, n_C)\). In other words, \(\phi: C \to \text{Cox}(\mathbb{O})\) is a linear bijection preserving norms such that the diagram
Commutes. Writing \( x^t := \text{can}(x) \) for \( x \in C^* \) and using the fact that \( \psi \) is an algebra isomorphism, we therefore obtain, for all \( x, y \in C^* \):

\[
(\varphi(x \cdot y)^t)^t = \psi((x \cdot y)^t) = \psi(x^t \cdot y^t) = (\varphi(x)^t)^t \omega(\psi(y)) = (\varphi(x)^t) (\varphi(y)^t)^t.
\]

But for \( x \in C^* \), the fiber of \( x^t \in C^* \) 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 \( \varepsilon : C^* \times C^* \to \{ \pm 1 \} \) such that \( \varphi(x \cdot y) = \varepsilon(x, y) \varphi(x) \varphi(y) \) for all \( x, y \in C^* \). We claim that \( \varepsilon \) is constant. Indeed, let \( x, y, z \in C^* \). Since \( \varphi \) preserves norms, and these are the same for \( C \) and \( \text{Cox}(\mathbb{O}) \), an application of (20.1.3) yields

\[
\varepsilon(x, y)\varepsilon(x, z) n_c(x)n_c(y, z) = \varepsilon(x, y)\varepsilon(x, z) n_c(\varphi(x), \varphi(y)),
\]

which in turn implies \( \varepsilon(x, y) = \varepsilon(x, w) = \varepsilon(x, z) \). Thus \( \varepsilon(x, y) \) does not depend on \( y \in C^* \). Interchanging the role of \( x \) and \( y \), and replacing \( (20.1.3) \) by (20.1.2) in the process, the same argument shows that \( \varepsilon(x, y) \) is also independent of \( x \in C^* \), 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 \( x, y \in C^* = \text{Cox}(\mathbb{O})^* \). But since \( C \) is generated by \( C^* \) as an additive group (Exercise 16 (b), (d)), this means that \( \varphi : C \to \text{Cox}(\mathbb{O}) \) is an isomorphism of octonion algebras.
hence \( n_c(u) = \beta n_c(v) \) and \( n_c(u, v) = \alpha n_c(v) \). This implies \( v \in C^c \) and with \( x := uv^{-1} \) we deduce \( \beta = n_c(x) \), \( \alpha = n_c(u, n_c(v)^{-1}) = n_c(x) \). Summing up, \( F[x] \subseteq C \) is a subalgebra isomorphic to \( K \), and we have found an embedding \( K \hookrightarrow C \).

(b) Since the property of being a composition algebra is stable under base change, we may assume that \( F \) itself is separably closed and must show that \( C \) is split. The case \( C \cong F \) being obvious, we may assume that \( C \) has dimension at least 2 and hence is non-singular. Assume \( C \) is a division algebra. Since \( F \) is separably closed, hence infinite, Zariski density leads to an element \( x \in C \setminus F \setminus \mathcal{I}_C \) having \( \mathcal{I}_C(x) \neq 0 \). But then \( F[x] \subseteq C \) is a separable quadratic field extension of \( F \), a contradiction to \( F \) being separably closed.

Section [28]

(a) Let \( R \in k\text{-alg} \) be the split-null extension of \( M \), living on the \( k \)-module \( k \oplus M \) under the multiplication \((\alpha \oplus u)(\beta \oplus v) = \alpha \beta \oplus (\alpha v + \beta u) \) for \( \alpha, \beta \in k \), \( u, v \in M \). One check easily that \( M \) is finitely generated as a \( k \)-module if and only if \( R \) is finitely generated as a unital \( k \)-algebra. Also, passing to the split-null extension is compatible with base change. Hence the assertion follows from Corollary [28.14].

(b) By [11, II, §5, Thm. 1], there is a finite family \((f_i)_{i \in I} \) of elements in \( k \) such that \( \sum_{i \in I} f_i = k \) and \( M_\mathcal{I} \) is a free \( k \)\text{-module of rank} \( r \). Put \( R := \bigoplus_{i \in I} k f_i \in k\text{-alg} \). Then \( M_\mathcal{I} \) is a free \( R \)-module of rank \( r \) and since \( R \) is faithfully flat over \( k \), by [11, [5, Prop. 3], the assertion is proved.

(a) Let \( R' \) be a finitely presented \( R \)-algebra. Then there are presentations

\[
0 \longrightarrow I \longrightarrow k[S] \xrightarrow{\pi} R \longrightarrow 0 , \quad (184) \quad \text{IKIK}
\]

\[
0 \longrightarrow J \longrightarrow R[T] \xrightarrow{\rho} R' \longrightarrow 0 \quad (185) \quad \text{JERT}
\]

of \( R \) over \( k \), \( R' \) over \( R \), respectively, with chains \( S = (s_1, \ldots, s_m) \), \( T = (t_1, \ldots, t_n) \) of independent variables and finitely generated ideals \( I \subseteq k[S] \), \( J \subseteq k[T] \). Extending \( (184) \) from \( k \) to \( k[T] \), we conclude that the sequence

\[
0 \longrightarrow I \otimes k[T] \longrightarrow k[S, T] \xrightarrow{\pi_{k[T]}} R \otimes k[T] = R[T] \longrightarrow 0 \quad (186) \quad \text{IKIK}
\]

is exact, whence

\[
\varphi := \rho \circ \pi_{k[T]} : k[S, T] \longrightarrow R'
\]

is a surjective morphism in \( k\text{-alg} \) which by \( (185) \) satisfies

\[
\text{Ker}(\varphi) = \pi_{k[T]}^{-1}(\text{Ker}(\rho)) = \pi_{k[T]}^{-1}(J) . \quad (188) \quad \text{PINV}
\]

Now pick \( g_1, \ldots, g_r \in R[T] \) such that \( J = \sum_{j=1}^r R[T]g_j \) and use \( (186) \) to find a lift \( h_j \) of \( g_j \) in \( k[S, T] \) under \( \pi_{k[T]} \). Then \( \pi_{k[T]}(h_j) = g_j \) for \( 1 \leq j \leq r \). By \( (186) - (188) \), this is easily seen to imply

\[
\text{Ker}(\varphi) = I \otimes k[T] + \sum_{j=1}^r k[S, T]h_j .
\]

But \( I \otimes k[T] \) is a finite \( k[T] \)-module, forcing \( \text{Ker}(\varphi) \subseteq k[S, T] \) 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 \( E := k[T]/(ft - 1) \) is clearly finitely presented, it suffices to show that \( k[T] \) and \( E \) are canonically isomorphic. Note first that the natural
projection $\pi : k[t] \to E$ makes $f$ invertible: $\pi(f) \in E^*$ with inverse $\pi(t)$. Hence the unit homomorphism $k \to E$ extends to a homomorphism $\varphi : k_f \to E$ such that $\varphi(1/f) = \pi(t)$. On the other hand, the $k$-homomorphism $k[t] \to k_f$ sending $t$ to $1/f$ kills $ft - 1$ and hence induces a $k$-homomorphism $\psi : E \to k_f$. One checks that $\varphi$ and $\psi$ are inverse to one another, and the assertion follows.

(a) Let $\pi : k[T] \to R$ be a surjective morphism in $k\text{-alg}$, giving rise to a presentation

\[
\begin{array}{cccccc}
0 & \to & I & \to & k[T] & \xrightarrow{\varphi \circ \pi} & R' & \to & 0
\end{array}
\]

of $R'$ as a $k$-algebra. By Proposition 28.13 therefore, $I \subseteq k[T]$ is a finitely generated ideal. But $I = \pi^{-1}(\ker(\varphi))$, and we conclude that $\ker(\varphi) = \pi(I) \subseteq R$ is a finitely generated ideal.

(b) Let

\[
\begin{array}{cccccc}
0 & \to & I & \to & k[T] & \xrightarrow{\pi} & R & \to & 0
\end{array}
\]

be a finite presentation of $R$. Setting $J := \ker(\varphi)$, this induces a presentation

\[
\begin{array}{cccccc}
0 & \to & \pi^{-1}(J) & \to & k[T] & \xrightarrow{\varphi \circ \pi} & R' & \to & 0
\end{array}
\]

of $R'$. Apply (189) and let $\pi(f_i), f_i \in k[T], 1 \leq i \leq m$, be finitely many generators of $J$ as an ideal in $R$. Then one checks that

\[
\pi^{-1}(J) = I + \sum_{i=1}^{m} k[T]f_i,
\]

so (190) makes $R'$ a finitely presented $k$-algebra.

By 27.19 $k[M_a] \cong S(M^*)$ 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 (10) Exercise 42 we find a complete orthogonal system $(e_i)_{i \in \mathbb{N}}$ 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 $k_i := k \otimes k_i$. Note that $e_i = 0$, 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 [12, III, §6, Prop. 7], we conclude

\[
S(M) = \bigoplus_{i \in \mathbb{N}} S(M_i)
\]

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 Exercise 139 (b) produces a faithfully flat $k$-algebra $k'$ making $M_k'$ a free $k'$-module of rank $r$. Since $S(M)_j' = S(M_j')$, therefore being a polynomial ring in $r$ variables [12, III, §6], hence finitely presented over $k'$, so is $S(M)$ over $k$, by Corollary 28.14.

It is straightforward to verify that $\tilde{w}$ is a subfunctor of $M_a$. 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

\[
f_{u^*}(R) : M_R \to R, \quad x \mapsto (u^*_R x - w_R)
\]

vary functorially with $R \in k\text{-alg}$ and hence define an element $f_{u^*} \in k[M_a]$. Since $M^*$ is finitely generated projective as well, and the canonical pairing $M' \times M \to k$ is non-singular, we conclude that $x \in M_k$ agrees with $w_k$ if and only if $f_{u^*}(R)(x) = 0$ for all $u^* \in M^*$. By Exercises 141, 142 therefore, $\tilde{w} \subseteq M_a$ is a finitely presented closed affine subscheme.

Let $K$ be a field. We have to prove that the quadratic form $q_k : M_k \to K$ over $K$ is non-degenerate. Write $\vartheta_k : k \rightarrow R$ (resp. $\vartheta_k : k \rightarrow K$) for the unit morphism of $R$ (resp. $K$). Then $p := \ker(\vartheta_k) \subseteq \text{Spec}(k)$, and since $R$ is faithfully flat over $k$, Proposition 28.8 yields a prime
ideal \( q \in \text{Spec}(R) \) such that \( p = \text{Spec}(\mathfrak{p}_R(q)) = \mathfrak{p}^{-1}_R(q) \). By \cite{10.4} not only \( K \) but also \( \kappa(q) \) is an extension field of \( \kappa(p) \). Let \( L \) be a free compositum of \( \kappa(q) \) and \( K \) over \( \kappa(p) \) \cite{17} pp. 551–2.

Since \( L \in R\text{-alg} \) is a field and \( q_k \) is separable, the quadratic form \( (q_k)_L \cong q_L \cong (q_R)_L \) over \( L \) is non-degenerate. Hence so is \( q_k \) over \( K \).

(a) For \( i = 1, 2, T \in S\text{-alg} \) and all \( k \)-modules \( P \), we have the natural identifications

\[
(P_k)_T = P_T = P_i = (P_k)_T
\]

via \cite{10.31}, so \( g_{ij} \) is a set map from \( (M_k)_T \) to \( (N_k)_T \), 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 \( \phi : T \to T' \) in \( S\text{-alg} \), we therefore obtain a morphism \( \phi_i : T_i \to T'_i \) in \( R\text{-alg} \) by defining \( \phi_i(t_i) := \phi(t) \), for all \( t \in T \). One checks that \( 1_{M_k} \otimes_R \phi_i = 1_{M_k} \otimes_R \phi \), and it follows that the diagram

\[
\begin{array}{ccc}
(M_k)_T & \xrightarrow{\phi} & (N_k)_T \\
1_{M_k} \otimes_R \phi & \downarrow & 1_{N_k} \otimes_R \phi \\
(M_k)_{T'} & \xrightarrow{\phi} & (N_k)_{T'}
\end{array}
\]

commutes. Hence \( g_{ij} : M_k \to N_k \) is a polynomial law over \( S \).

(b) If \( f : M \to N \) is a polynomial law over \( k \) such that \( f \otimes R = g \), then for all \( T \in S\text{-alg} \) we deduce that \( g_{ij} = g_{2j} = (f \otimes R)_{ij} = f_{ij} = f_T \) is independent of \( i = 1, 2 \). Thus \( g_1 = g_2 \). Conversely, assume \( g_1 = g_2 \). We first prove uniqueness of \( f \) and let \( k' \in k\text{-alg} \). One checks that the outer squares in (3) commute. Hence so does the inner one since \( g_{ij} = f_{ij} \) by hypothesis. Moreover, the vertical arrows in (3) are injective by Proposition \cite{28.4}, proving uniqueness of the set maps \( f_{ij} \), hence of \( f \) as a polynomial law over \( k \).

In order to prove existence, let \( k' \in k\text{-alg} \). To simplify notation, we indicate the base change from \( k \) to \( k' \) simply by a dash, for example \( M' = M_{k'}, R' = R \otimes k', S' = S \otimes k' = R' \otimes k' \otimes R' \). 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 \( R'\text{-alg} \) \( S'_i \) \((i = 1, 2) \) yield morphisms

\[
\sigma^R_i : R' \longrightarrow S'_i, \quad r' \longmapsto \sigma^R_i (r') := p^R_i (r')
\]

in \( R'\text{-alg} \subseteq R\text{-alg} \). Now we consider the following diagram.

\[
\begin{array}{ccc}
0 & \xrightarrow{\gamma} & 0 \\
\downarrow & & \downarrow \\
M' & \xrightarrow{\gamma f_{ij}} & N' \\
\downarrow & & \downarrow \\
M'_{k'} & \xrightarrow{\gamma f_{ij}} & N'_{k'} \\
\downarrow & & \downarrow \\
(M_{k'})_{R'} & \xrightarrow{\gamma} & (N_{k'})_{R'} \\
\downarrow & & \downarrow \\
(M_{k'})_{S'} & \xrightarrow{\gamma} & (N_{k'})_{S'}
\end{array}
\]

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 \( x \in M, r \in R, \alpha', \beta' \in k' \):
\[ \rho_{1}^{E,M}((x \otimes \alpha') \otimes_{V} (r \otimes \beta')) = (x \otimes \alpha') \otimes_{V} ((r \otimes \beta') \otimes_{V} (1_{k} \otimes 1_{V})) \]
\[ = (x \otimes \alpha') \otimes_{V} ((r \otimes 1_{k}) \otimes \beta') = x \otimes ((r \otimes 1_{k}) \otimes \alpha' \beta') \]
\[ = x \otimes ((r \otimes 1_{k}) \otimes \alpha' \beta')_{1} = (x \otimes 1_{k}) \otimes_{K} ((r \otimes \alpha' \beta')_{1}) \]
\[ = (x \otimes 1_{k}) \otimes_{K} (r \otimes \alpha' \beta') \]
\[ = (1_{M_{k}} \otimes_{K} \alpha' \beta')(x \otimes (\alpha' (r \otimes \beta'))) \]
\[ = (1_{M_{k}} \otimes_{K} \alpha' \beta')((x \otimes \alpha') \otimes_{V} (r \otimes \beta')). \]

The universal property \[28.5\] of the equalizer \(\text{can}_{W,K}^{E,N}\) of \(\rho_{1}^{E,N}\), \(\rho_{2}^{E,N}\) (Proposition \[28.6\]), applied to the map \(u := g_{E} \circ \text{can}_{W,K}^{E,N}: M' \to N_{E}^{'}\), by \[191\] implies that there exists a unique set map \(f_{U} : M' \to N'\) making \[191\] totally commutative. In other words, we have a commutative diagram

\[ \begin{array}{ccc}
M' & \xrightarrow{f_{U}} & N' \\
\downarrow \text{can}_{W,K}^{E,N} & & \downarrow \text{can}_{W,K}^{E,N} \\
M_{K}^{'} = (M_{k})_{E} & \xrightarrow{g_{E}} & (N_{k})_{E} = N_{E}^{'}.
\end{array} \] \[192\]

Next we show that \(f_{U}\) depends functorially on \(k'\), so let \(\varphi : k' \to k''\) be a morphism in \(k\)-\text{alg}. Indicating the base change from \(k\) to \(k''\) by a double dash, we see that

\[ \varphi_{k} := 1_{k} \otimes \varphi : R' \longrightarrow R'' \]

is a morphism in \(R\)-\text{alg}, and one checks that the diagram

\[ \begin{array}{ccc}
M' & \xrightarrow{1_{k} \otimes \varphi} & M'' \\
\downarrow \text{can}_{W,K}^{E,N} & & \downarrow \text{can}_{W,K}^{E,N} \\
M_{K}^{'} = (M_{k})_{E} & \xrightarrow{1_{k} \otimes \varphi} & (M_{k})_{E''} = M_{K}^{''}.
\end{array} \] \[194\]

commutes. Now consider the cube

\[ \begin{array}{ccc}
M' & \xrightarrow{f_{U}} & N' \\
\downarrow \text{can}_{W,K}^{E,N} & & \downarrow \text{can}_{W,K}^{E,N} \\
M_{K}^{'} = (M_{k})_{E} & \xrightarrow{g_{E}} & (N_{k})_{E} = N_{E}^{'} \\
\downarrow \text{can}_{W,K}^{E,N} & & \downarrow \text{can}_{W,K}^{E,N} \\
M_{K}^{''} = (M_{k})_{E''} & \xrightarrow{g_{E''}} & (N_{k})_{E''} = N_{E}^{''}.
\end{array} \]
where by \([192]\)–\([194]\) all rectangles commute, with the possible exception of the top one. By diagram chasing, therefore, so does the top one after being composed with \(\text{can}_{k'}\). But \(R''\) is faithfully flat over \(k'\), forcing \(\text{can}_{k'}\) by Proposition \([28.4]\) to be injective, and we have proved that the top rectangle commutes as well. Summing up, \(f: M \to N\) is a polynomial law over \(k\). Hence the solution of the problem will be complete once we have shown \(f \otimes_R g = 0\). In order to see this, let \(k' \in R\text{-alg}\) and \(\rho: R \to k'\) the corresponding unit morphism in \(k\text{-alg}\). With the notational simplifications introduced before, we obtain an induced morphism \(\rho': R' \to k'\) 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 \(R\text{-alg}\), and we obtain a diagram

\[
\begin{array}{cccc}
M' & \xrightarrow{\rho'} & N' \\
\text{can}_{k'}' & & \\
M'_R = (M_R)_{k'} & \xrightarrow{g_{k'}} & (N_R)_{k'} = N'_R \\
\text{can}_{k'}' & & \\
M' = (M_R)_{k'} & \xrightarrow{g_R} & (N_R)_{k'} = N',
\end{array}
\]

where the outer triangles are easily seen to be commutative. Hence \(f_{k'} = g_{k'}\), as desired.

**sol.FFCON** \([147]\) We systematically adhere to the notation and terminology of Exercise \([145]\).

(a) Let \(e\) be the unit element of \(C_R\) and write \(g := e: C_k \to C_R\) for the constant polynomial law over \(R\) determined by \(e\), as defined in §\([13]\) Exercise \([15]\). For \(T \in S\text{-alg}\) and \(i = 1, 2\), \(e_T \in (C_T)_R = (C_T)_R\) is the unit element of \((C_T)_R\), and we conclude \(e_T = e_T\). Thus \(g_1 = g_2\) as polynomial laws \(C_k \to C_k\) over \(S\). Applying Exercise \([145]\) we find a unique polynomial law \(f: C \to C\) over \(k\) such that \(f \otimes_R g = 0\). Put \(e_0 := f_2(0) \in C\). Since the vertical arrows in \([3]\) are injective, we conclude not only \(e_0 = e\) but also that \(C\) is unital with \(1_C = e_0\).

(b) Let \(n: C_R \to R\) be a quadratic form over \(R\) making \(C_R\) an conic \(R\)-algebra. For \(T \in S\text{-alg}\) and \(i = 1, 2\), there are two quadratic forms over \(T\) making \((C_T)_R\) a conic \(T\)-algebra, namely, \(n_T\). Hence Proposition \([19.14]\) implies \(n_{k} = n_{k}\). Viewing \(n\) as a homogeneous polynomial law \(g: C_k \to C_k\) of degree \(2\) over \(k\), we have \(g_1 = n_{k} = n_{k} = g_2\). Thus Exercise \([145]\) yields a unique polynomial law \(f: C \to k\) over \(k\) such that \(f \otimes_R g = 0\). Hence the set map \(n_0 := f_2: C \to k\) 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 \(C_k\) as a conic \(R\)-algebra with norm \(n\).

**sol.FFSPLIQ** \([147]\) By Exercise \([142]\) the \(k\)-functor \(M^2_k = (M^2)_k\) of Example \([27.13]\) is a finitely presented \(k\)-scheme. Hence so is \(X := \text{Hyp}(Q)\), defined as a closed subsheaf of \(M^2_k\) by finitely many equations (cf. \([6]\) and Exercise \([31]\)\(b)\)). After an appropriate base change, it therefore remains to show that the natural set map \(X(k) \to X(k)\) is surjective, where \(k := k/I\) and \(I \subseteq k\) is an ideal satisfying \(I^2 = \{0\}\). Note that \([10.2]\) and Corollary \([12.5]\) imply \(M := M_k = M/IM_k\), and the quadratic form \(\bar{q} := q_\ast: M \to k\) over \(k\) is given by \(\bar{q}(\bar{x}) = q(x)\) for all \(x \in M\), where \(\alpha \mapsto \bar{\alpha}\) (resp. \(x \mapsto \bar{x}\)) stand for the natural maps \(k \to k\) (resp. \(M \to M\)). We first note that a hyperbolic basis is indeed a basis of the underlying module and must show that any hyperbolic basis of \(\bar{Q} := (M, \bar{q})\) can be lifted to one of \(Q\), so let \((u^i)_{1 \leq i \leq 2n}\) 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 \([12.16]\) 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 \(q(a), q(b) \in I, q(a, b) = 1 + l \subseteq k^*\), and since \(l\) squares to zero, one checks that

\[
u := -q(a, b)^{-2}q(b)a + q(a, b)^{-1}b \]
form a hyperbolic pair of $Q$ lifting $(u',v')$. Now assume $n > 1$. By what we have just seen, the hyperbolic pair $(w'_k, w''_k)$ of $Q$ can be lifted to a hyperbolic pair $(w_k, w_{2k})$ of $Q$. Put $V := kw_k \oplus kw_{2k}$ and $M_0 := V^\perp$ (relative to $D_q$). Then Lemma 2.10 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, $\bar{Q}_0 = (M_0, \bar{q}'|M_0)$ contains $(w'_k)_{1 \leq 2(n - 1)}$ as a hyperbolic basis, which, by the induction hypothesis, can be lifted to a hyperbolic basis $(w_k)_{1 \leq 2n}$ of $Q_0$. Hence $(w_k)_{1 \leq 2n}$ is the desired lift of $(w'_k)_{1 \leq 2(n - 1)}$.

(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 $\eta : M \rightarrow M'$ satisfying $q' \circ \eta = q$. We define the set

$$\text{Isom}(Q, Q') := \{ \eta \mid \eta : Q \rightarrow Q' \text{ is an isometry} \},$$

which in general will be empty but gives rise to a $k$-functor

$$\text{Isom}_k(Q, Q') := \text{Isom}(Q, Q') : k\text{-alg} \rightarrow \text{set}$$

by defining

$$\text{Isom}(Q, Q')(R) := \text{Isom}_k(Q_R, Q'_R)$$

for all $R \in k\text{-alg}$ and by

$$\text{Isom}(Q, Q') \mathrel{\varphi} \text{Isom}(Q, Q')(R) \rightarrow \text{Isom}(Q, Q')(S),$$

for all morphisms $\varphi : R \rightarrow S$ in $k\text{-alg}$. The $k$-group functor $\text{O}(Q)$ of Example 27.24 acts canonically in a simply transitive manner on $\text{Isom}(Q, Q')$ from the right via

$$\text{Isom}_k(Q_R, Q'_R) \times \text{O}(Q_R) \rightarrow \text{Isom}_k(Q_R, Q'_R), \quad (\eta, \zeta) \mapsto \eta \circ \zeta$$

for all $R \in k\text{-alg}$.

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 $h^{2n}_k$ the split hyperbolic quadratic space of rank $2n$ over $k$ defined on $k^{2n} = (\binom{2n}{n})$ by the quadratic form

$$\langle S \rangle_{\text{quad}}, \quad S := \begin{pmatrix} 0 & 1_s \\ 0 & 0 \end{pmatrix}$$

in the sense of (12.72). The canonical basis of $k^{2n}$ is a hyperbolic basis for $h^{2n}_k$ and obviously compatible with base change. It follows immediately from the definitions that the assignment

$$\eta \mapsto (\eta(e_i))_{1 \leq 2n}$$

defines a bijection

$$\Phi = \Phi(k) : \text{Isom}(h^{2n}_k, Q) \rightarrow \text{Hyp}(Q).$$

3. Putting $X := \text{Isom}(h^{2n}_k, Q)$, the set maps

$$\Phi(R) : X(R) \rightarrow \text{Hyp}(Q)(R)$$

given by (198), (199) for all $R \in k\text{-alg}$ are bijective and obviously compatible with base change, hence give rise to an isomorphism

$$\Phi : X \rightarrow \text{Hyp}(Q)$$
of $k$-functors. By (a), therefore, $X$ is a smooth affine $k$-scheme. Moreover, $X$ is faithful in the sense of \cite{23}, since non-singular even-dimensional quadratic forms over an algebraically closed field are (split) hyperbolic \cite{22}. Summing up, \cite{28,17} (ii) implies that there exists a faithfully flat étale (split) hyperbolic \cite{27,Exercise 7.34}. Summing up, \cite{28,17} (ii) implies that there exists a faithfully flat étale $k$-algebra $R$ satisfying $X(R) \neq \emptyset$. But this means that $Q_R$ is split hyperbolic. Furthermore, $X$ is a torsor with structure group $O(h^{2n}_R)$ in the étale topology, forcing

$$O(Q)_R \cong O(Q)_k \cong O(h^{2n}_R) \cong X_R$$

to be smooth over $R$. By \cite{28,17} (iii), therefore $O(Q)$ is smooth over $k$.

**Chapter 5**

**Section 30**

\textbf{sol.PARNIL}  \textbf{[148]} (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 $x^m = U_i x^{m-2} \in \text{Mon}_m(\{x\})$. Conversely, let $x \in \text{Mon}_m(\{x\})$. Then $x = U_i z, y \in \text{Mon}_n(\{x\})$, $z \in \text{Mon}_n(\{x\}), n, p \in \mathbb{N}, n > 0, 2n + p = m$. By the induction hypothesis, $y = x^r, z = x^s$, and power associativity yields $x = U_r x^p = x^{n+s} = x^m$, as claimed.

(b) For any subset $X \subseteq J$ and any homomorphism $\phi: J \rightarrow J'$ of para-quadratic $k$-algebras, one makes the following observations by straightforward induction:

(i) $\phi(\text{Mon}_m(X)) = \text{Mon}_m(\phi(X))$ for all $m \in \mathbb{N}$.

(ii) $\text{Mon}_n(Y) \subseteq \text{Mon}_m(X)$ for all $Y \subseteq \text{Mon}_m(X)$ and all $m, n \in \mathbb{N}$.

If $x \in J$ is nilpotent, then (i) implies that $\phi(x) \in J'$ is nilpotent. Hence if $I$ is a nil ideal in $J$, then $I'$ is nil ideal in $J$ and $J'/I'$, respectively. Conversely, let this be so. Writing $\pi: J \rightarrow J'$ for the canonical epimorphism, any $x \in I$ makes $\pi(x) \in I'/I$ nilpotent, so by (i), $\text{Mon}_m(\{x\})$ meets $I$ for some $n \in \mathbb{N}$. But since $I'$ is nil, we conclude that some $y \in \text{Mon}_n(\{x\})$ is nilpotent, leading to a positive integer $m$ such that $0 \in \text{Mon}_m(\{x\})$ by (ii). Thus $x$ is nilpotent, forcing $I$ to be a nil ideal. Now write $n := \text{Nil}(J)$ for the sum of all nil ideals in $J$. Given $x \in n$, there are finitely many nil ideals $n_1, \ldots, n_r \subseteq J$ such that $x \in n_1 + \cdots + n_r$. 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 $(n_1 + n_2)/n_1 \cong n_2/(n_1 \cap n_2)$ combines with what we have proved earlier to yield the assertion.

(c) It suffices to prove that $\text{Nil}(k)/J \subseteq J$ is a nil ideal. The ideal property being obvious, we are reduced to showing that $\text{Nil}(k)/J$ consists entirely of nilpotent elements. An arbitrary element $x \in \text{Nil}(k)/J$ actually belongs to $IJ$, where $I \subseteq \text{Nil}(k)$ 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 \cite{19}. Exercise 83.

\textbf{sol.EVALPOL}  \textbf{[149]} (a) For the first assertion, since $\epsilon(1) = 1_J$, we need only show $(f^2 g)(x) = U f(x) g(x)$ for all $f, g \in k[x]$. By linearity, we may assume $g = t^u$ for some $n \in \mathbb{N}$ and, writing $f = \sum a t^i$ with coefficients $a_i \in k$, we obtain

$$f^2 g = \left( \sum a_i t^i + \sum a_i a_j t^{i+j} \right) t^u = \sum a_i^2 t^{2i+n} + \sum a_i a_j t^{i+j+n},$$

hence, as $J$ is power-associative,
(f^2g)(x) = \sum_{i,j} a_i^2 x^{2i+j} + \sum_{i,j} a_i a_j 2x^{i+j} = \sum_{i,j} a_i^2 U_{i,j} x^i + \sum_{i,j} a_i a_j \{x^i, x^j\}

= (\sum_{i,j} a_i^2 U_{i,j} + \sum_{i,j} a_i a_j U_{i,j},) x^i = U_{\Sigma a_i^2} x^i = U_{f(x)} g(x).

Thus \( \varepsilon_k \) is a homomorphism of para-quadratic algebras, and we conclude that \( I \subseteq k[t]^{(+)} \) is an ideal. Our next aim will be to show that \( I \) is an ideal in \( k[t] \). By linearity, it suffices to show for \( f \in I \) that \( t^n f \) belongs to \( I \) 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 \( \varepsilon_k \) is a homomorphism of para-quadratic algebras, the induction hypothesis yields not only \( (t^n f)(x) = 0 \), but also \( (t^{n+1} f)(x) = (t^n t f)(x) = U_{i,j}(t^{n-1} f)(x) = 0 \), and we have shown \( t^n f \in I \). Next let \( \mathcal{P} \) be any ideal of \( k[t] \) contained in \( I \). Given \( f \in \mathcal{P} \subseteq I \), we also have \( tf \in \mathcal{P} \subseteq I \), hence \( f(x) = (tf)(x) = 0 \), which shows \( t^n f \subseteq \mathcal{P} \), so \( \mathcal{P} \) is indeed the largest ideal of \( k[t] \) contained in \( I \). Finally, let \( f \in \mathcal{P} \). Then \( f^2(x) = U_{f(x),1} f(x) = 0 \) and \( (t f^2)(x) = U_{f(x),1} f(x) = 0 \), hence \( f^2 \in I \). Similarly, not only \( 2 f \in I \) but also \( 2(f^2)(x) = x \circ \varepsilon_k(x) = 0 \), hence \( 2 f \in \mathcal{P} \). 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 \( \ker(\pi) = I/I^{(0)} \) follows immediately from the fact that \( f^2 \) and \( 2 f \) belong to \( I^{(0)} \) for all \( f \in I \). This completes the solution to (a).

(b) Write \( f = \alpha_0 t^n + h \in k[t] \) with \( \alpha_0 \in k \) and \( h \in t^{n+2} k[t] \). Since \( 2 = 0 \) in \( k \) and \( n \geq 2 \), we have \( f^2 = \alpha_0^2 t^{2n} + h^2 \in t^{n+2} k[t] \), which is an ideal in \( k[t] \). Thus \( U_{f(x),g(x)} = f^2 g \in t^{n+2} k(t) \subseteq I \) for all \( g \in k[t] \). Conversely, let \( g = \sum \beta_j t^j \in k[t] \) with coefficients \( \beta_j \in k \) for \( j \in \mathbb{N} \). Then \( U_{f(x),g(x)} = f^2 g \equiv \alpha_0 \beta_j t^n \mod t^{n+2} k[t] \) and hence \( U_{f(x),g(x)} = U_{f(x)} g(x) \). Since \( \{g(x) f(x)\} = 2 f g \in I \subseteq k[t] \), it follows that \( I \) is an ideal in \( k[t]^{(+)} \). But it is not an ideal in \( k[t] \) since \( t \) belongs to \( k[t] \) but \( t^n \) 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.

(a) In the para-quadratic k-algebra \( k[t]^{(+)} \) we have \( U_{f,g} h = (f g)^2 h = f^2 g^2 h = U_{f,h} U_{g,h} \) for all \( f,g,h \in k[t] \), hence

\[ U_{f,g} = U_f U_g \quad \text{for} \quad f,g \in k[t]. \tag{200} \]

Since \( J \) is power-associative, the evaluation at \( x \) (Exc. 149) is a homomorphism \( k[t]^{(+)} \to J \) of para-quadratic algebras with image \( k[x] \). Applying this homomorphism to \( f \), \( g \in k[t] \), therefore gives \( \{f, g\} \), hence not only the first equation of \( 2 \) but also

\[ U_{U_{f(x),g(x)}} = U_{f^{(2)}(x)} U_{g^{(2)}(x)} - U_{f^{(2)}(x),g^{(2)}(x)}, \]

\[ U_{f^{(2)}} = U_{g^{(2)}} \quad \text{for} \quad f,g \in k[t]. \]

and the proof of (a) is complete.

(b) The polynomial

\[ f := \alpha_0 t^n + \cdots + \alpha_{n-1} t^{n-1} + t^n \quad \text{in} \quad k[t] \]

kills \( x \) and hence belongs to \( I := \ker(\varepsilon_k) \). From Exc. 149 (a) we therefore conclude that

\[ f^2 = \alpha_0^2 t^{2n} + \cdots + t^{2n} \in k[t] \]

belongs to \( I \), so by Exc. 149 (a) we have \( (t^2 f^2)(x) = 0 \), i.e.,

\[ \alpha_0^2 \alpha_i^2 \cdots \alpha_{i-1}^2 \alpha_i^2 \cdots \alpha_{i-1}^2 = 0 \quad \text{for} \quad i \in \mathbb{N}. \tag{201} \]

Now, setting \( k_r[x] := \sum_{i=r}^n k^i x^i \) for \( r \in \mathbb{N} \), we find in \( (k_r[x])_{r \in \mathbb{N}} \) a descending chain of submodules of \( k[x] \). Invoking \( 38 \), we therefore conclude that \( k_{2d^{(1)}}[x] = k_{2d^{(d+1)}}[x] \) is a finitely generated k-module. Thus the linear map \( U_{f^{(2)}(x)} : k_{2d^{(1)}}[x] \to k_{2d^{(d+1)}}[x] \), being surjective, is in fact bijective. Thus \( k_{2d^{(d+1)}}[x] \) has the same property and hence there exists a unique
element $v \in k_2[x]$ such that $U'_i v = x^{2d}$. Here (a) implies $U'_i U'_j = U'_j U'_i$, and we conclude that $U_v$ is the identity on $k_2[x]$. With $c := v^2$, this means $U_v = (U_v)^2 = 1$ on $k_2[x]$ and $c^2 = v = U_v v^2 = c$, $c^3 = U_v c = c$, so $c \in k_2[x]$ is an idempotent of the desired kind.

(c) Let $x \in J$ be a pre-image of $c'$ under $\phi$. 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 $v \in k_2[x]$ as in (b) and put $c := v^2$. Writing $\bar{u} := \phi(u)$ for $u \in J$, we conclude $U'_v \bar{v} = U \bar{v} = U \bar{d} \bar{v} = x^{2d} = c'$. 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 $\bar{v} = \alpha c'$, hence $c' = U'_v \bar{v} \bar{v} = \bar{a} U_v c' = \bar{a} c' = \bar{v}$. But this implies $\bar{v} = v^2 = c^2 = c'$, and the problem is solved.

\[\text{sol.OUTCEN}\]

(a) Since $J$ is outer simple, $\text{Mult}(J)$ acts irreducibly on $J$. Thus the assertion follows from Schur’s lemma \[47,\ p.\ 118\].

(b) Since $\text{Mult}(J)$ acts faithfully and irreducibly on $J$, it is a primitive Artinian $k$-algebra. \[47,\ Def.\ 4.1\]. Moreover, by definition, its centralizer in $\text{End}_k(J)$ is $\text{Cent}_k(J)$. Thus the assertion follows from the double centralizer theorem \[47,\ Thm.\ 4.10\].

(c) If $J$ is outer central and outer simple, the assertion follows from (b). Conversely, suppose $J \neq \{0\}$ and $\text{Mult}(J) = \text{End}_k(J)$. Then $J$ is outer simple, and (b) implies that $\text{Cent}_k(J)$ belongs to the centre of $\text{End}_k(J)$. Hence $J$ is outer central.

\[\text{sol.COS}\]

(a) Setting $c := \sum_{i=1}^r c_i$, we have

$$c^2 = \sum_{i=1}^r c_i^2 + \sum_{i<j} c_i c_j = \sum_{i=1}^r c_i = c,$$

$$c^3 = U_v c = \sum_{i=1}^r U_v c_i + \sum_{i+j=1}^{r-r} \{c_i c_j c_i\} = \sum_{i=1}^r c_i = \sum_{i=1}^r c_i = c,$$

and we have shown that $c$ is an idempotent in $J$. Hence so is $c_{r+1} := I_J - c$. \[30.9\] and it remains to show that $(c_1, \ldots, c_r, c_{r+1})$ is an orthogonal system of idempotents, completeness being obvious. For $1 \leq i, l \leq r$ distinct, we compute
\[ U_{i, j} = \sum_{k=1}^{r} U_{i, k} U_{j, k} = x_i - U_i c_i = c_i - \xi_i = 0, \]
\[ \{ U_{i, j} \} = c_i - U_i c_i = \xi_i = 0, \]
\[ \{ U_{i, j} \} = \{ (1 - c)(1 - c) \} = 2c_i = -2c_i = 0, \]
\[ \{ U_{i, j} \} = \{ c_i - c_j \} = -2c_i = -2c_i = 0, \]
\[ \{ U_{i, j} \} = c_i - \xi_i = 0. \]

Hence \((c_1, \ldots, c_r, \xi_{r+1})\) is a complete orthogonal system of idempotents in \(J\).

(b) If \((c_1, \ldots, c_r)\) 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 \((\xi)\) with \((3.10)\), we see that the idempotents \(c_i, \xi_i, 1 \leq i \leq r\), are orthogonal in \(J\), hence, as we have seen in \((30.9)\) in \(A\). But this means that \((c_1, \ldots, c_r)\) is a (complete) orthogonal system of idempotents in \(A\).

Section 31

(iii) \(\Rightarrow\) (iii). Obvious by the definition of a Jordan algebra.

(iii) \(\Rightarrow\) (ii). This follows from the arguments of \(31.3\) since the identities \(5\) – \(8\) are respectively the same as (resp. part of) \(31.3\) – \(31.3\).

(ii) \(\Rightarrow\) (i). Let \(R \in \mathcal{K} \mathcal{g} \mathcal{a} \mathcal{r} \). The left (resp. right) of \(6\) defines a \(k\)-3-quadratic map \(F\) (resp. \(G\)) from \(J^3\) to \(\text{End}_k(\mathcal{J})\), and we have \(F = G\) by hypothesis. Thus \(F_{R^k} = G_{R^k}\) by \(30.12\) which by \(31.12\) implies that \(6\) holds in \(J_{R^k}\). For analogous reasons, \(7\), \(8\) holds in \(J_{R^k}\) as well.

**Proof of (5).** By linearity in \(z\), we may assume \(z = wR, w \in J\). Assume first \(x = uR, u \in J\). Since both sides of \(5\) are quadratic in \(y\) and agree for \(y = vR, v \in J\), by hypothesis, it follows that \(5\) holds for all \(y \in J_{R^k}\). Now fix \(y \in J_{R^k}\) and put

\[ M := \{ x \in J_{R^k} \mid U_i U_j U_k = U_k U_j U_i \}, \]

which is obviously closed under multiplication by scalars in \(R\) and, as we have just seen, contains all elements \(uR, u \in J\). Hence \(5\) will follow once we have shown that \(M\) is closed under addition. But this is implied by \(7\) and a straightforward computation.

**Proof of (4).** By linearity in \(y\), we may assume \(y = vR, v \in J\). Arguing as before, it suffices to show that

\[ M := \{ x \in J_{R^k} \mid U_i V_{i,j} = V_{i,j} U_i \} \]

is closed under addition. But this is immediate, by \(3\) and a straightforward computation.

**Proof of (3).** Since \(3\) is quadratic in \(y\), it suffices to prove it for \(y = vR, v \in J\). Again we will be through once we have shown that

\[ M := \{ x \in J_{R^k} \mid U_i U_j = U_j U_i \} \]

is additively closed. This follows from \(5\), \(6\) by a lengthy, but still straightforward, computation.
Since a Jordan algebra satisfies (3)–(5), so do all its subalgebras and homomorphic images. By what we have just shown, therefore, they are all Jordan algebras.

(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 \( x, y \in I \), we have \( U_j x, U_j y \in I \) and given \( z \in I \), equations \((31.3.14), (31.3.15)\)

\[
\{xyz\} = V_{x,y} z = V_{y,z} x - U_{x,y} z = U_{x,y} z - U_{x,y} z \in I,
\]

which shows \( \{III\} \subseteq I \) and completes the proof.

(b) If \( c^2 = c \), then, \( U_c^2 = U_c \) by \((31.3.11)\), hence \( c^2 = U_c c = U_c^2 = U_c^2 \). Thus \( c \) is an idempotent.

(c) Let \( x, y \in J \) and \( z \in 3(J) \). Then \((31.3.14)\) implies \( V_{x,z} = V_{z,y} = U_{x,y} z = U_{x,y} z = 0 \) and, similarly, \( V_{y,z} = 0 \). From the fundamental formula \((31.3.2)\) we deduce \( U_{x,z} = 0 = U_{x,z} \). And, finally, applying \((31.3.9)\), we obtain

\[
U_{x,z} = U_{x,y} z = U_{x,z} V_{x,y} + U_{x,y} z - U_{x,y} z = -U_{x,y} z = 0,
\]

\[
U_{x,y} = U_{x,y} z = U_{x,y} V_{x,y} + U_{x,y} z - U_{x,y} z = -U_{x,y} z = 0.
\]

Hence \( U_j (3(J)) + U_j (3(J)) \subseteq 3(J) \), and we have shown by (a) that \( 3(J) \subseteq J \) is an ideal. Now suppose that \( J \) is simple. Then \( J \neq \{0\} \) by definition, hence \( U_{ij} \neq 0 \), which implies \( 3(J) = \{0\} \) by simplicity. The final statement now follow from Thm. \((30.17)\).

Let \( a \in \text{Cent}(J) \). Then \( L_{a} L_{x} = L_{a} L_{y} = L_{a x} \) for all \( x \in J \). Since, therefore, \( L_{a} \) and \( L_{x} \) commute, so do \( L_{a} \) and \( L_{x} = 2L_{a} - L_{a} \), for all \( x \in J \). Moreover, this and \( a^2 \in \text{Cent}(J) \) imply

\[
U_{a x} = 2L_{a} - L_{a} = 2L_{a} - L_{a} = 2L_{a} - L_{a} L_{x} = L_{a} U_{x},
\]

\[
U_{a x} = 2L_{a} L_{x} + L_{a} - L_{a} = L_{a} U_{x}.
\]

for all \( x, y \in J \), whence \((30.13)\) yields \( L_{a} \in \text{Cent}(J^{\text{quad}}) \). Conversely, let \( \psi \in \text{Cent}(J^{\text{quad}}) \). By \((30.13)\) we have \( \psi V_{x} = V_{x} \psi \) for all \( x \in J \), and from \((31.3.4)\) we deduce \( \psi L_{x} = L_{x} \phi \), hence \( \psi(x,y) = x \phi(y) \) for all \( x, y \in J \). Setting \( y = 1 \), we obtain \( \psi = L_{a} \) with \( \phi = \phi(1) \). In particular, \( L_{a} \) commutes with \( L_{a} \) for all \( x \in J \), whence \( a \) belongs to the centre of \( J \). Summing up we have shown that the injective algebra homomorphism \( f: \text{Cent}(J) \to \text{End}(J) \) has image \( \text{Cent}(J^{\text{quad}}) \), and the assertion follows.

If \( J = J(M, q, e) \), then \((9)\) holds strictly by \((31.12.5), (31.12.6)\). Conversely, suppose \((9)\) holds strictly. Then the second equation of \((9)\) may be written as \( U_{x} x = t(x) x^{2} - q(x) x, \) and linearizing we may apply \((31.3.15)\) to conclude

\[
x^{2} y + U_{x} y = U_{x} x + U_{x} y = t(x) x^{2} - q(x) x = q(x,y) x - q(x,y) y.
\]

Applying the trace (resp. \( q(-x,y) \)) to the first equation of \((9)\), we obtain

\[
t(x)^{2} = t(x) x^{2} - 2q(x), \quad q(x,y) = t(x) q(x,y) - q(x,y) t(y),
\]

while linearizing it yields

\[
x o y = t(x) y + t(y) x - q(x,y) e.
\]

Hence on the one hand

\[
x^{2} o y + U_{x} y = U_{x} y + t(x)^{2} y + t(y) x^{2} - q(x^{2}, y) e
\]

\[
= U_{x} y + t(x)^{2} y + t(x) t(y) x - q(x) t(y) e - t(x) q(x,y) e + q(x) t(y) e
\]

\[
= U_{x} y + t(x)^{2} y + t(x) t(y) x - t(x) q(x,y) e,
\]

while on the other
Comparing by means of (202) and writing \( x \mapsto \bar{x} \) for the conjugation of \((M, q, e)\), we obtain

\[
U_{xy} = q(xy) + t(x)q(y)x - q(x)t(y)e - q(x,y)x = q(x,y)x - q(x)y
\]

Thus \( J \) and \( J(M, q, e) \) not only have the same unit element but also the same \( U \)-operator, which implies \( J = J(M, q, e) \).

Concerning the first part, assume that \( x \in J \) is nilpotent. Then (31.12.11) shows that \( q(x) \) is nilpotent, while Exc.[150] yields a positive integer \( m \) satisfying \( x^m = 0 \) 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 (31.12.12) that \( t(x)^2 = 2q(x) \) is nilpotent. Hence so is \( t(x) \). We may therefore assume \( m \geq 3 \). Since \( \left[ \frac{m}{2} \right] \leq \frac{m}{2} < \frac{m}{2} + 1 \) and \( m > 2 \), we deduce

\[
\left[ \frac{m}{2} \right] + 1 \leq m + 1 - m + \frac{m}{2} < m + 1 = m,
\]

and if \( n \geq \left[ \frac{m}{2} \right] + 1 \), then \( 2n \geq 2 \left[ \frac{m}{2} \right] + 1 \) and \( \left[ \frac{m}{2} \right] < \frac{m}{2} = m \). On the other hand, (30.8.3) yields \( (x^2)^n = x^{2n} = 0 \), and the induction hypothesis implies that \( (x^2) \) is nilpotent. But then so is \( t(x)^2 = t(x^2) = 2q(x) \) by (31.12.12), 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.[31.15] Exc.[150] 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

\[
N := \{ x \in M \mid q(x), q(x,y) \in \text{Nil}(k) \quad \text{for all} \quad y \in M \}
\]

and let \( x \in N, y \in M \). Then (31.12.11) yields \( q(U_{x}, z) = q(x)^2q(z) \in \text{Nil}(k) \) and, similarly, \( q(U_{x}) \in \text{Nil}(k) \). Moreover, since the conjugation of \( J \) leaves \( q \) invariant, the definition of the \( U \)-operator implies

\[
q(U_{x} + U_{x}, y) = q(x, \bar{z})q(x, y) + q(z, \bar{y})q(z, y) - q(x,q(\bar{z}, y) + q(z,q(\bar{y}, x) + q(x,y), \bar{z}) = q(x,q(z + y) - q(x,q(z) - q(x,y)q(z) \in \text{Nil}(k).
\]

Thus \( U_{x} + U_{x} \subseteq N \), and we have shown in view of Exc.[155](a) that \( N \subseteq J \) is an ideal which, by the first part of this problem, is nil. This proves \( N \subseteq \text{Nil}(J) \). Conversely, let \( x \in \text{Nil}(J) \). Then \( q(x) \) and \( t(x) \) are nilpotent and \( \text{Nil}(J) \) contains \( x \circ y = t(x)y + t(y)x - q(x,y)1_J \). Hence \( t(x)y - q(x,y)1_J \in \text{Nil}(J) \), forcing

\[
q(t(x)y) = t(x)^2q(y) - t(x)q(x,y)1_J + q(x,y)^2
\]

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 \( \text{Nil}(J) \subseteq N \) and completes the proof.

We begin with a simple lemma.

**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 \( x^3 = -q(x)x \).

**Proof.** By (31.12.5), we have \( t(x) = q(x)1_J \), which by taking traces implies \( t(x)^2 = 2q(x) \). Applying (31.12.4), we therefore obtain

\[
x^3 = U_{x}x = q(x, \bar{x})x - q(x)x = (t(x)^2 - 2q(x)x - t(x)q(x)1_J + q(x)x
\]

\[
= (-t(x)^2 + q(x)x, \bar{x})x = -q(x)x
\]
as claimed. □

(a) We have \( I_2 = k^2 \oplus k^d \oplus k^d \oplus \cdots \). Hence, writing \( x \) for the image of \( t \) under the canonical map \( k[t]^{(+)} \rightarrow I_2 \), we conclude that \( I_2 \) is free as a \( k \)-module, with basis \( 1_{I_2} , x , x^2 \). In particular, \( x \) and \( x^2 \) are linearly independent. Since \( x^2 = 0 \), and by the preceding lemma, therefore, \( I_2 \) 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 \( k = k_0[e] , , e^2 = 0 \), be the \( k_0 \)-algebra of dual numbers. As in Exc. \[ \text{slo.DEPOQUA} \] we may view \( k_0 \) as a \( k \)-algebra by means of the homomorphism \( k \rightarrow k_0 , \alpha \mapsto \alpha \), given by \( \tilde{\varepsilon} = 0 \). Now let \( n \) be a positive integer, write \( (e_1 , \ldots , e_n) \) for the canonical basis of \( k^n \) over \( k \), put \( M := k_0 \oplus k^n \) as a \( k \)-module, define \( q : M \rightarrow k \) by

\[
q(\tilde{\alpha} \oplus \sum_{i=1}^n \alpha_i e_i) := \alpha^2 + e \alpha_1^2 + \sum_{i=2}^n \alpha_i^2 \quad (\alpha_0 , \alpha_1 , \ldots , \alpha_n \in k),
\]

and put \( e := 1_{k_0} \oplus 0 \). We claim that the map \( q \) is well defined. Indeed, if \( \alpha , \beta \in k \) satisfy \( \tilde{\alpha} = \tilde{\beta} \), then \( \alpha = \beta + e \gamma \), for some \( \gamma \in k \), hence \( \alpha^2 = \beta^2 + e^2 \gamma^2 = \beta^2 \), 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 \( \tilde{x} := 1 \), we have \( t(x) = 0 \) and \( q(x) = e \), hence \( q(x) 1_J = e (1_{k_0} \oplus 0) = e = 0 = t(x), \) so \((31.12.5)\) implies \( x^2 = 0 \). Now the preceding lemma yields \( x^3 = -q(x)x = -e e_1 \neq 0 \), and we have obtained an example of the desired kind.

\[ \text{slo.IDPOQUA} \]

Our solution is basically the same as the one to Exc. \[ \text{slo.DEPOQUA} \] First of all, assume that \( k \neq \{0\} \) is connected, so 0 and 1 are the only idempotents of \( k \). If \( c \in J \) has \( t(c) = 1 \) and \( q(c) = 0 \), then \( (31.12.5) \) shows \( c^2 = c \), so \( c \in J \) is an idempotent, which cannot be zero since \( t(c) = 1 \neq 0 \) and cannot be 1 since \( q(c) = 0 \neq 1 \). Conversely, let \( c \in J \) be an idempotent \( \neq 0 , 1 \). Then \( q(c) \) by \((31.12.1)\) is an idempotent in \( k \), and since \( k \) is connected, we either have \( q(c) = 1 \) or \( q(c) = 0 \). In the former case, \( c = c^2 = t(c)c - 1_J \), hence \( 1_J = (t(c)-1)c \), and taking norms we conclude \( (t(c)-1)^2 = 1 \). But this implies \( c = \alpha 1_J \) with \( \alpha = t(c)-1 , \alpha^2 = 1 \). We therefore obtain \( 1_J = \alpha^2 1_J = c^2 = c \), a contradiction. Hence \( q(c) = 0 \). Then \((31.12.5)\) implies \( c = c^2 = t(c)c \), and taking traces gives \( t(c)^2 = t(c) \). Thus \( t(c) \in k \) is an idempotent which cannot be zero since this would imply the contradiction \( c = 0 \). Thus \( t(c) = 1 \), as claimed.

The remainder of this exercise is established in exactly the same way as the corresponding part of Exc. \[ \text{slo.COBRLP} \]

\[ \text{slo.IDPOQUA} \]

The solution to this exercise is exactly the same as the one to Exc. \[ \text{slo.DEPOQUA} \]

\[ \text{slo.COBRLP} \]

If \( C \) is alternative, then \((20.3.2)\) shows \( C^{(+)} = J(C,n_C,1_C) \). Conversely, let this be so. For \( x,y \in C \) we apply \((19.5.5),(19.5.10),(19.5.14)\) and obtain

\[
n_C(x,y)x - n_C(x,y)\tilde{y} = xyx = (x \circ y)x = (yx)x = t_C(x)yx + t_C(y)x^2 - n_C(x,y)x - (yx)x
\]

\[
= t_C(x)y + (t_C(x)t_C(y) - n_C(x,y))x - t_C(y)n_C(x)C - (yx)x = n_C(x,y)x - n_C(x)\tilde{y} - n_C(x)y + (\tilde{y}x)x.
\]

Comparing, we arrive at one of Kirmse’s identities \((20.3.1)\), i.e., \((\tilde{y}x)x = n_C(x)\tilde{y}\). But this means that \( C \) is right alternative. Since it is also flexible by hypothesis, it is, in fact, alternative.

\[ \text{sol.POJCQAT} \]

Homomorphism of pointed quadratic modules are clearly homomorphisms of the corresponding Jordan algebras. Hence the assignment in question defines a functor from \( \text{slo.POJOUA}_{00} \) to \( k\text{-jord}_{01} \), 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 \([12.14]\) the proof of Prop. \([19.13]\) 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 \(\varphi: J(M, q, e) \to J(M', q', e')\) 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 \(\varphi: (M, q_1, e) \to (M', q', e')\) is a homomorphism of pointed quadratic modules. Hence \(\varphi: J(M, q_1, e) \to J(M', q', e')\) is an isomorphism 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 \(\varphi: (M, q, e) \to (M', q', e')\) is an isomorphism of pointed quadratic modules. Thus the functor in question is full.

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 \(q = (1, \delta, \delta e)\) for some \(\delta, e \in F^\times\). Now put

\[
K := \text{Cay}(F, -e) = F \oplus F 1, \quad B := \text{Cay}(K, -\delta) = K \oplus K 2.
\]

as in \([21.2]\). 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.\(110\)\(b\). Then \(\tau(a + b j) = a + b j2\) for all \(a, b \in K\), which implies \(H(B, \tau) = W := F 1 \oplus K 2 = F 1 \oplus F 2 = F 1 F 2 j 2\). By Exc.\(102\) we have \(B^{(\tau)} = J(B, n g, 1)\) and therefore \(H(B, \tau) = J(W, n g w, 1)\). By standard properties of the Cayley-Dickson construction, the vectors \(1_B, j 2, j 1 j 2\) are orthogonal relative to \(n g\) and satisfy \(n g(1_B) = 1, n g(j 2) = \delta, n g(j 1 j 2) = n g(1_B) n g(j 2) = \delta e\). Hence the pointed quadratic modules \((V, q, e)\) and \((W, n g w, 1)\) are isometric, forcing \(J\) and \(H(B, \tau)\) as the corresponding Jordan algebras by Exc.\(103\) 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 \(W \subseteq (B, n g)\), \(W' \subseteq (B', n g')\) are non-singular subspaces of co-dimension 1. If \(W\) and \(W'\) are isometric, then \(B\) and \(B'\) are isomorphic.

**Proof.** By Lemma\(12.10\) we have \(B = W \perp F u, B' = W' \perp F u'\) for some non-zero \(u \in B, u' \in B'\). Recall that the determinant of a quadratic space like \((B, n g)\) (resp. \((B', n g')\)) is unique up to non-zero square factors in \(F\). As a matter of fact, we deduce from \([22.19]\) that this determinant is a square. On the other hand, it agrees with \(\det(W)n g(u)\) (resp. \(\det(W')n g'(u')\)). On the other hand, \(W\) and \(W'\) being isometric, their determinants differ by a square factor in \(F\). Hence so do \(n g(u)\) and \(n g'(u')\). But this means that \(B\) and \(B'\) are norm-equivalent. By the norm equivalence theorem\(26.7\), therefore, they are isomorphic.

Now let \((B', \tau')\) be another quaternion algebra with involution \(\tau'\) having \(W' := H(B', \tau') \cong J(V, q, e)\). By Exc.\(163\) the quadratic subspaces \(W \subseteq (B, n g)\) and \(W' \subseteq (B', n g')\) are not only non-singular but also isometric. Our preceding lemma therefore implies that \(B\) and \(B'\) are isomorphic. We may thus assume \(B = B'\). Let \((j 1, j 2, j 3)\) be an orthogonal basis of \(W\) such that \(n g(j 2) = \delta, n g(j 1 j 2) = \delta e\), with \(\delta, e\) as above. Since \((B, n g)\) has trivial determinant, we conclude \(W^\perp = F j 1, n g(j 1 j 2) = e\). Then \(F j 1 = \text{Cay}(F, -e) = K\). Now \(19.35\) implies for \(i = 2, 3\):

\[
0 = \tau'(j 1, j 2, j 3) + n g(j 1, j 2, j 3) 1_B = \tau'(j 1) j 2 + n g(j 1 j 2) j 1_B = -n g(j 1 j 2) j 1_B.
\]

Thus \(n g(j 1 j 2) = 0\), and since we trivially have \(n g(j 1 j 2) 1_B = 0\), we deduce \(\tau'(j 1) j 2 = 0\). Here \(\tau'(j 1) j 2 = j 1 j 3\) would imply \(\tau' = 1_B\), a contradiction. Hence \(\tau'(j 1) j 2 = j 1 j 3\). Thus \(\tau' = 1_B\), corresponding to \(F j 1 \cong K\), which implies \((B, \tau) \cong (B, \tau')\) by Exc.\(110\)\(b\).

**Section 32**

(a) \(x \in \text{Rad}(q)\) implies \(U_1Y = q(x, \bar{y})x - q(x)\bar{y} = 0\) for all \(y \in J\), hence \(U_1 = 0\), and \(x\) is an absolute zero divisor of \(J\). Conversely, let this be so. Then \(31.12\) yields \(q(x)^2 = U_1x^2 = 0\), 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 $0 = U_j \tilde{x} = q(x, y)x$ and then $q(x, y)x^2 = q(q(x, y)x, y) = 0$. Thus $q(x, y) = 0$, and we have proved $x \in \text{Rad}(q)$.

(b) Here $k$ is arbitrary. Then $\tilde{k} := k/\text{Nil}(k) \in k\text{-alg}$ is reduced, and we have a canonical identification $J_\ell = J := J/\text{Nil}(k)J$ via $10.2$ matching $\tilde{z}_q$ for $z \in J$ with $\tilde{z}$, the image of $z$ under the natural map $J \to J$. Since $x$ is an absolute zero divisor in $J$, $\tilde{x}$ is one in $J$, so by the special case just treated we have $\tilde{q}(\tilde{x}) = \tilde{q}(\tilde{x}, y) = 0$ for all $y \in J$, where $\tilde{q} = q_1$ is the $k$-quadratic extension of $q$. But this means that $q(x)$ and $q(x, y)$ are nilpotent elements of $\tilde{k}$, for all $y \in J$, which implies $x \in \text{Nil}(J)$ by Exc.[158]

Section 33

(a) By the results of §§31, 32, equations (2)–(8) hold for all $i, j, m, n, p \in \mathbb{N}$. For $n \in \mathbb{N}$, $n > 0$, we combine (1) with (3, 3), and obtain $U_{i+1} = U_{i+1} = U_{i+1} = (U_{i+1})^{m} = U_{i+1}$. 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 $U_{i+1} = U_{i+1} = U_{i+1}$ for all $n \in \mathbb{N}$ and we do so by induction on $n$. For $n = 0$, there is nothing to prove. For $n \geq 2$, assuming the validity of the assertion for $n - 2$ yields $U_{i+1} = U_{i+1} = U_{i+1}(x^{n-1}) = U_{i+1}(x^{n-1})$, as claimed. Thus (3) holds.

Turning to (4), we first assume $n \in \mathbb{N}$ and then argue by induction. For $n = 0$, there is nothing to prove. Now let $n \geq 1$ and assume the assertion is valid for $n - 2$. Then $(x^{m})^{n} = U_{i+1}(x^{m})^{n} = U_{i+1}(x^{m})^{n}$, as claimed. Next assume $n < 0$. The case just treated and (2, 3) yield $U_{i+1}(x^{m})^{n} = (x^{m})^{n} = x^{m} = U_{i+1}(x^{m})^{n} = U_{i+1}(x^{m})^{n}$, and since $U_{i+1}(x^{m})^{n}$ is bijective, the proof of (4) is complete.

Next we establish (7). For $l \in \mathbb{N}$ such that $2l + m, 2l + n \in \mathbb{N}$, we obtain, using (2, 3, 3), (3, 3, 3),

$$U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1}$$

and, similarly, $U_{i+1}U_{i+1} = U_{i+1}U_{i+1}$. 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

$$U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p})$$

and

$$U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p}) = U_{i+1}(x^{m}x^{n}x^{p})$$

Thus (5) holds.

Turning to (6), we use (3, 3), (3, 3), (3), (3, 3) and obtain

$$V_{i+1}U_{i+1} = V_{i+1}U_{i+1} = V_{i+1}U_{i+1} = V_{i+1}U_{i+1} = V_{i+1}U_{i+1} = V_{i+1}U_{i+1}$$

Hence (6) follows.

Finally, in order to establish (9), we let $l \in \mathbb{N}$ satisfy $l + i, l + j, l + m, l + n \in \mathbb{N}$. Then, by (3, 3, 3, 3)

$$U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1} = U_{i+1}U_{i+1}$$

as claimed.

(b) Arguing as in the solution to Exc.[148](a), it follows that $g_{x}^{*} : k[t, t^{-1}] \to J$ is a homomorphism of Jordan algebras forcing $k[x, x^{-1}] \subseteq J$ to be a subalgebra containing $g_{x}^{*}(t^{1}) = x^{1}$.
Writing $J'$ for the subalgebra of $J$ containing $x$ 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 Sol. 32.3 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. 32.11.

(a) By (29.3.2) we have
\[ [L_x, L_y] = 0 \iff [L_x, L_{xy}] = 0. \]

(b) (i) $\Rightarrow$ (ii). Let $y := x^{-1}$. Then $2xy = x \circ y = \{x_1x^{-1}\} = 2 \cdot 1_J$ by Exc. 166 [5]. Hence $xy = 1_J$. Moreover, Exc. 166 [5] shows $4[L_x, L_y] = [U_{x_1}, U_{x_2}] = 0$, so $x$ and $y$ operator commute.

(ii) $\Rightarrow$ (iii). We have $xy = 1_J$, and since $x$ and $y$ operator commute, we also obtain $x^2y = y(x)x = x(y)x = x$.

(iii) $\Rightarrow$ (i). Since $x$ and $y$ operator commute, so do $x^2$ and $y$, by (a). For the same reason $y^2$ and $x$ operator commute. Hence
\[ U_{x^2} = 2x(y^2x) - x^2y^2 = y(x^2y) = yx = 1_J, \]
and $x$ is invertible in $J$ by Prop. 33.2.

Next suppose $y \in J$ satisfies (ii). Then $x$ is invertible and $U_{xy} = 2x(xy) - y(xy) = 2x - y(xy) = x$, hence $y = U_{x_1}^{-1}x = x^{-1}$. Similarly, if $y$ satisfies (iii), then $U_{xy} = 2x(xy) - x^2y = x$ and again $y = x^{-1}$.

(a) $q^{(f)} : M \to k$ is a quadratic form and $e^{(f)} \in M$ satisfies $q^{(f)}(e^{(f)}) = q(f)q(f^{-1}) = 1$ by Exc. 168 [10]. Hence $(M, q, e^{(f)})$ is a pointed quadratic module over $k$. For $x \in M$, the definitions imply
\[ e^{(f)}(x) = q^{(f)}(e^{(f)}x) = q(f)q(f^{-1}f, x) = q(f, x), \]
\[ e^{(f)} = e^{(f)}(x)e^{(f)} - x = q(f^{-1}f, f, x) - x, \]
hence (12) and (13). In (14), 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. $U_x^f$) for the $U$-operator of $J(M, q, e^{(f)})$ (resp. $J((M, q, e^{(f)})$). We first note
\[ U_{f^2} = U_{f^2} = x \cdots \]
Setting $1^{(l)} := 1_{p(l)}$ as in (33.8.1), we apply (33.8.2) and obtain $U_{z^{-1}}U_y = U_{z^{-1}(x^{-1})}^{-1} = U_{z^{-1}}x$, hence $U_yz^{-1} = x$. Using Exc. [166,9], we therefore conclude

$$
U_jU_{z^{-1}}U_y = U_jU_{z^{-1}(x^{-1})} = U_jU_{z^{-1}}U_y = U_jU_{z^{-1}(x^{-1})} = U_jU_{z^{-1}}x = U_yz^{-1} = x.
$$

We have $xx^{-1} = L_xL_x^{-1}1_j = 1_j$, and the Jordan identity (29.1.2) yields $x^2(x^{-1}) = x^2(x^{-1}) = x^{-1}$, hence $x^2x^{-1} = x$ since $L_x$ is bijective. We therefore conclude from Exc. (167) that $x$ is invertible in $J$ with inverse $x^{-1}$. Now (33.3.1) and (29.9.1) imply that $L_{x^{-1}} = \frac{1}{2}V_{x^{-1}} = \frac{1}{2}U_xU_x = U_x^{-1}L_x$ 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. (29) 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. (168). Assume $J$ has dimension $n \geq 3$ and extend $1_j$ to an orthogonal basis $(e_1, e_2, e_3, \ldots, e_n)$ of $J$ relative to $Dq$. Applying (31.12.8), 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.

(a) Let $\eta: J \to J'$ be a strong homotopy, so some $p \in J^*$ makes $\eta: J^p \to J'$ a homomorphism. Hence $\eta: J \to J'$ is a homotopy by Prop. (33.16)(b). Conversely, let $\eta: J \to J'$ be a homotopy such that $\eta(J^p') = J'^p'$. Then there exists a $p' \in J^*$ such that $\eta: J \to J^{p'}$ is a homomorphism. By hypothesis, we find an element $p \in J^*$ satisfying $\eta(p) = p'^{-2}$. Then (33.8)(ii) and Cor. (33.11) show that

$$
\eta: J^{p'} \to J^{p'(\eta(p))} = J^{p'(p'^{-2})} = J'
$$

is a homomorphism, forcing $\eta: J \to J'$ to be a strong homotopy.

(b) Let $F$ be a field and $\mu \in F[t]$ be an irreducible polynomial of degree at least 2, making $K := F[t]/(\mu)$ a finite algebraic extension field of $F$. We denote by $\pi: F[t] \to K$ the canonical projection and put $J := F[t]^{K^{-1}}$, $J': K^{-1}$. Pick an element $p' \in K \setminus F \pi x$. Then $p' \in J^\infty$ and the linear map

$$
\eta: J \to J', \quad f \mapsto \eta(f) := \pi(f)p'^{-1}
$$

fits into the commutative diagram

$$
\begin{array}{ccc}
J & \xrightarrow{\eta} & J' \\
\pi \downarrow & \simeq & \downarrow \rho_{p'}^{-1} \\
J & \xrightarrow{\rho_{p'}^{-1}} & J'.
\end{array}
$$

where, by (33.12.6), the horizontal arrow is a homomorphism. Thus $\eta: J \to J'$ is a homotopy. Assume that this homotopy is strong. Then there exists a $p \in J^*$ such that $\eta: J^p \to J'$ is a homomorphism. But Ex. (33.6) shows $J^\infty = F[t]^\infty = F^\infty$, hence $p \in F^\infty$. By (204), therefore,

$$
1_k = 1_{p'} = \eta(1_{p'}(J)) = \eta(p^{-1}) = p^{-1}\eta(1) = p^{-1}p'^{-1}.
$$
and we arrive at the contradiction \( p' = p^{-1}1_k \in F1_k \). Thus \( \eta \) is not a strong homotopy.

(a) We argue by induction if \( n \geq 0 \). For \( n = 0 \), we have to show \( \lambda (1_j) = 0 \), which follows from (15) by setting \( x = y = 1_j \); \( \lambda (1_j) = \bar{\lambda} (U_{1_j}1_j) = 3\lambda (1_j) \), 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 (16) implies \( \lambda (x^n) = \lambda (U_{x^n-2}) = 2\lambda (x) + \lambda (x^{n-2}) = 2\lambda (x) + (n - 2)\lambda (x) = n\lambda (x) \). If \( n = -1 \), we obtain \( \lambda (x) = \bar{\lambda}(U_{x^{-1}}) = 2\lambda (x) + \bar{\lambda}(x^{-1}) \), hence \( \lambda (x^{-1}) = -\lambda (x) \). And finally, for any integer \( n > 0 \), the definition (cf. Exc. 166 (1)) implies \( \lambda (x^n) = \bar{\lambda} ((x^{-1})^n) = n\lambda (x^{-1}) = -n\lambda (x) \). This completes the proof.

(b) We have \( (vw)^2 = v^2w^2 = U_{i}w^2 \). Hence (a) implies \( 2\lambda (vw) = \bar{\lambda} ((vw)^2) = \bar{\lambda} (U_{i}w^2) = 2\lambda (v) + \bar{\lambda} (w^2) = 2(\lambda (v) + \bar{\lambda} (w)) \), 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 \( 2m \subseteq \Gamma \). 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 \( jm + l = -(2lm - \lambda (x)) \in \Gamma \) since \( \Gamma \) by (16) and (a) is closed under the operation \( (\alpha, \beta) \rightarrow 2\alpha - \beta \). 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, \( \lambda (x) = (2i + j)m \in 2m \), which completes the proof.

(e) We have to verify (15) - (17) and do so by a straightforward computation: For \( x, y \in J \) we obtain

\[
\lambda \circ \rho (x) = \infty \iff \lambda (p) + \lambda (x) = \infty \iff \lambda (x) = \infty \iff x = 0,
\]

\[
\lambda \circ \rho (U_{i}y) = \lambda (p) + \lambda (U_{i}y) = \lambda (p) + 2\lambda (x) + 2\lambda (p) = 2\lambda (p) + 2\lambda (y) = 2\lambda \circ \rho (x) + 2\lambda \circ \rho (y),
\]

and finally,

\[
(\lambda \circ \rho)^{y}(x) = \lambda \circ \rho (q) + \lambda \circ \rho (x) = \lambda (p) + \lambda (q) + \lambda (x) + 2\lambda (p) + \lambda (q) + \lambda (x) = 2\lambda (p) + \lambda (q) + \lambda (x) = \lambda \circ \rho \circ \rho^{y} (x).
\]

(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

\[
\lambda (x \circ z) \geq \lambda (x) + \lambda (z) \hspace{1cm} (x, z \in J), \tag{205}
\]

and let \( y \in J^\times \) be arbitrary. Then we pass to the \( y \)-isotopes \( J^{(y)} \) and \( \lambda \circ \rho \) and combine (33.8) with (205) to conclude

\[
\lambda (y) + \lambda \circ \rho \circ \rho^{y} (x) = \lambda \circ \rho (x \circ y) \geq \lambda \circ \rho (x) + \lambda \circ \rho (z) \geq 2\lambda (y) + \lambda \circ \rho (z) + \lambda \circ \rho (x).
\]

Hence (19) follows. We are thus reduced to the case \( y = 1_j \) and have to prove (205). Fixing \( x \in J^\times \) and letting \( z \in J^\times \) be arbitrary, the estimate

\[
\lambda \circ \rho (x) = \lambda (U_{i}1_j) \geq \min \{ 2\lambda (x + 1_j), 2\lambda (x) + \lambda (z), \lambda (z) \}
\]

\[
\geq \min \{ 2\lambda (x, 0) + \lambda (z) = \min \{ \lambda (x), -\lambda (x) \} \}
\]

and finally, for any integer \( n > 0 \), the definition (cf. Exc. 166 (1)) implies \( \lambda (x^n) = \bar{\lambda} ((x^{-1})^n) = n\lambda (x^{-1}) = -n\lambda (x) \). This completes the proof.
shows that there exists a constant \( \kappa \geq 0 \), depending on \( x \), such that 
\[
\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \kappa \\
(z \in J^\circ).
\] (206)
We now consider \([31,3,15]\) for \( z \) in place of \( y \) and apply the result to \( 1_J \). Then 
\[
(x \circ z)^2 + z \circ U_xz = U_xz^2 + U_x^2 + 2x \circ U_xz,
\]
which in turn may be combined with \([31,3,17]\) to yield 
\[
(x \circ z)^2 = U_xz^2 + U_x^2 + x \circ U_xz.
\]
This and \eqref{206} imply 
\[
2\lambda(x \circ z) = 2(\lambda(x \circ z)^2) = 2(\lambda(U_xz^2 + U_x^2 + x \circ U_xz)) \\
\geq \min \{ 2(\lambda(x) + \lambda(z)), 2(\lambda(z) + \lambda(x)), \lambda(x \circ U_xz) \} \\
\geq \min \{ 2(\lambda(x) + \lambda(z)), 2(\lambda(x) + \lambda(z)) - \kappa \} \\
= 2(\lambda(x) + \lambda(z)) - \kappa.
\]
Thus 
\[
\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \frac{\kappa}{2} \\
(z \in J^\circ),
\]
and iterating this procedure, we end up with 
\[
\lambda(x \circ z) \geq \lambda(x) + \lambda(z) - \frac{\kappa}{2^n} \\
(z \in J^\circ, n \in \mathbb{N}).
\]
Hence, as \( n \to \infty \), we arrive at \eqref{205}.

(a) Since \( J \) by Thm. \([32,11]\) is locally linear, \( F[x] \subset J \) is a commutative associative \( F \)-algebra. Every \( y \neq 0 \) in \( F[x] \) is invertible in \( J \) and hence \( U_y : J \to J \) is bijective (Prop. \([33,2]\)). Thus \( U_y \) via restriction induces a linear injection \( F[x] \to F[y] \), and a dimension argument shows that \( U_y : F[x] \to F[y] \) is, in fact, bijective. Since, therefore, \( y \in F[x]^\circ \), 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 \( J = F : 1_J \).

(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. \([80]\) 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 \([31,12,8]\) and \([29,8,1]\) imply \( J = J(M,q,e) \). Since by Exc. \([168]\), 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.

Section 34

(a) \( J \) is a commutative associative \( F \)-algebra. Every \( y \neq 0 \) in \( F[x] \) is invertible in \( J \) and hence \( U_y : J \to J \) is bijective (Prop. \([33,2]\)) and \( U_y \) via restriction induces a linear injection \( F[x] \to F[y] \), and a dimension argument shows that \( U_y : F[x] \to F[y] \) is, in fact, bijective. Since, therefore, \( y \in F[x]^\circ \), 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 \( J = F : 1_J \).

(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. \([80]\) 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 \([31,12,8]\) and \([29,8,1]\) imply \( J = J(M,q,e) \). Since by Exc. \([168]\), 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.

Section 34

Let \( f = \sum_{i \geq 0} \alpha t^i \in \mathbb{k}[t] \) and suppose \( f(c) = 0 \). By Prop. \([32,7]\), we must show \( (tf)(c) = 0 \). With \( d := 1_J - c \) and \( \alpha := \sum_{i \geq 1} \alpha_i \in k \) we have \( 0 = f(c) = \alpha_0 (1_J - c) + \alpha c = (\alpha_0 + \alpha)c, \) \( \alpha_0 + \alpha \) is an orthogonal idempotent, we conclude \( (\alpha_0 + \alpha)c = \alpha_0 d = 0 \), hence \( (tf)(c) = (\sum_{i \geq 0} \alpha) c = (\alpha_0 + \alpha)c = 0, \) as desired.

Write \( J_i := J_i(c) \) for \( i = 0, 1, 2 \) and put \( d := 1_J - c \). Applying \([34,2,8]\), we see that \( U_x \) maps \( J_2 \) to \( J_0 \), hence via restriction induces a linear map \( \phi : J_2 \to J_0 \). Write \( w := v^{-1} \) as \( w = w_2 + w_1 + w_0 \), \( w_i \in J_i \) for \( i = 0, 1, 2 \). Then \([33,2,1]\) and \([34,2,8]\) again yield 
\[
v = U_x w = U_x w_2 + U_x w_1 + U_x w_0, \quad U_x w_i \in J_2-i \quad (i = 0, 1, 2).
\]
Comparing Peirce components and using bijectivity of $U$, (Prop. 34.2), we conclude $w_2 = w_0 = 0$. Thus $w \in J_1$, and by (34.2.8) combined with Cor. 34.3 (b) we have
\[ w^2 = p + q, \quad p := U_w d \in J_2^0, \quad q := U_w e \in J_0^0, \] (207)
which implies
\[ U_v p = d, \quad U_v q = c. \] (208)

Next, writing $p^{-1}$ (resp. $q^{-1}$) for the inverse of $p$ (resp. $q$) in $J_2$ (resp. $J_0$), we claim
\[ U_v d = p^{-1}, \quad U_v e = q^{-1}. \] (209)

Indeed, from (207), (208), Cor. 34.3 (b) and Exc. 166 we deduce $U_v U_i e = U_q U_i z q = U_q U_{i(w_2)} q = -U_q U_{p-1+i(q^{-1})} q = U_q U_{q^{-1}} = U_q q^{-1}$, and since $U_q : J_0 \to J_0$ is bijective, the second equation of (209) is proved. The first one follows analogously. In particular, $\varphi$, viewed as a linear map $J_2 \to J_0^{(0)}$, preserves units. But it also preserves $U$-operators since for $x, y \in J_2$ we may apply (208) to obtain
\[ U^{(0)}_{\varphi(x)} y = U_{\varphi(x)} U_{\varphi(y)} = U_{\varphi(x)} U_{\varphi(y)} \varphi = U_{\varphi(x)} \varphi(y) = \varphi(U_{\varphi(x)} y) = \varphi(U_{\varphi(y)}), \]
as claimed. Thus $\varphi : J_2 \to J_0^{(0)}$ is a homomorphism. Interchanging the role of $c$ and $d$, we also obtain a homotopy $\psi : J_0 \to J_2$ induced by $U_w = U_{c^{-1}}$. 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 (207) yields $p = c, q = d$. Hence $\varphi : J_2 \to J_0$ is an isomorphism. Conversely, let this be so. By what we have just shown, $1_J = \varphi(1_J) = q^{-1}$, forcing $q = d$. On the other hand, $\varphi^{-1} : J_0 \to J_2$ is an isomorphism induced by $U_{c^{-1}}$, and from (207) we conclude $p = U_{c^{-1}} d = \varphi^{-1}(d) = c$. Now (207) again implies first $w^2 = 1_J$ and then $v^2 = (w^2)^{-1} = 1_J$ as well.

From Cor. 34.3 (c) we deduce for $x \in J_2$ that $V_x$ stabilizes $J_1$, so the map $\varphi$ is well defined and linear. Moreover, $\varphi(1_J) = \varphi(c) = 1_{J_1}$ by (34.2.7). Now let $x, y \in J_2, z \in J_1$. Then (34.3.19) yields
\[ U_{\varphi(x)} \varphi(y) z = V_x V_y z = V_{x+y} z + V_{x+y} z, \]
where $U_{x+y} z \in \{ J_2 J_1 \} = \{ 0 \}$ by (34.2.9). Applying (34.3.19), we therefore conclude
\[ U_{\varphi(x)} \varphi(y) z = V_{x+y} z = V_{x+y} z + U_{x+y} z \]
since $U_{x+y} z = U_{x+y} = \{ 0 \}$ by (34.2.8). 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 $\text{Ker}(\varphi) \subseteq J_1$ is an ideal if $J_2$ since $\varphi(c) = 1_J \neq 0$. Thus $\text{Ker}(\varphi) = \{ 0 \}$ and $\varphi$ is injective.

(ii) $\Rightarrow$ (i). Clear.
(i) $\Rightarrow$ (ii). We may assume
\[ \{ i, j \} \cap \{ l, m \} \neq \emptyset \] (210)
and then consider the following cases.

Case 1. $\{ i, j \} \cap \{ l, m \} \cap \{ n, p \} = \emptyset$. We may assume $l = j$ by (210), 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 $T = (n, p, j, i)$ with $\{ n, p \} \cap \{ i, j \} = \emptyset$, 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 $T = (i, j, m, j, p)$ 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 \( ij = \{i, j\} = \{l, m\} = lm. \)

Let \( R := \langle t_1^{\pm 1}, \ldots, t_r^{\pm 1} \rangle \) be the ring of Laurent polynomials in the variable \( t_1, \ldots, t_r \). As in the proof of Thm. [34.11] (c), we have

\[
A \subseteq A_R = \bigoplus_{i_1, \ldots, i_r \in \mathbb{Z}} (t_1^{i_1} \cdots t_r^{i_r} A),
\]

\[
\text{End}_k(A) \subseteq \text{End}_k(A_R) = \bigoplus_{i_1, \ldots, i_r \in \mathbb{Z}} (t_1^{i_1} \cdots t_r^{i_r} \text{End}_k(A)) \subseteq \text{End}_k(A_R).
\]

(a) First of all, we have

\[
1_A = L_{\lambda_1} R_{\lambda_1} = L_{\Sigma_{i,j}} R_{\Sigma_{i,j}} = \sum_{i,j=1}^r L_{i,j} R_{i,j} = \sum_{i=1}^r E_{i,i}.
\]

It remains to show that the \( E_{i,j} \) are orthogonal projections. Since every base change of \( A \) is flexible, we conclude

\[
\sum_{i,j=1}^r t_i t_j L_{i,j} R_{i,j} = L_{\Sigma_{i,j}} R_{\Sigma_{i,j}} = R_{\Sigma_{i,j}} L_{\Sigma_{i,j}} = \sum_{i,j=1}^r t_i t_j L_{i,j} R_{i,j},
\]

and comparing coefficients yields

\[
E_{i,j} = L_{i,j} R_{i,j} = R_{i,j} L_{i,j} \quad (1 \leq i, j \leq r). \tag{211}
\]

Similarly,

\[
\sum_{i=1}^r t_i L_{i,i} = L_{\Sigma_{i}} R_{\Sigma_{i}} = R_{\Sigma_{i}} L_{\Sigma_{i}} = \sum_{i=1}^r t_i L_{i,j} R_{i,j},
\]

and the analogous relation for the right multiplication imply

\[
L_{i,j} L_{i,i} = \delta_{ij} L_{i,i}, \quad R_{i,j} R_{i,i} = \delta_{ij} R_{i,i} \quad (1 \leq i, j \leq r). \tag{212}
\]

Given \( i, j, l, m = 1, \ldots, r \), we now apply (211), (212) and obtain

\[
E_{i,l} E_{i,m} = L_{i,j} R_{i,j} L_{j,m} R_{j,m} = \delta_{ij} L_{j,m} R_{j,m} = \delta_{ij} \delta_{jm} R_{i,j} = \delta_{ij} \delta_{jm} E_{i,j}.
\]

Hence the \( E_{i,j} \) are orthogonal projections of \( A \), as claimed.

(b) Let \( 1 \leq i, j \leq r \) and \( x \in A_{i,j} \). For \( 1 \leq l \leq r \), we apply (212) to obtain

\[
c_{j,l} x = L_{j,l} E_{j,l} x = L_{j,l} R_{j,l} x = \delta_{jl} E_{j,j} x = \delta_{jl} x
\]

and, similarly, \( x c_l = \delta_{jl} x \). Thus the left-hand side of (4) is contained in the right. Conversely, let \( x \in A \) and assume \( c_{j,l} x = \delta_{jl} x, x c_l = \delta_{jl} x \) for \( l = 1, \ldots, r \). Then this holds, in particular, for \( l = i \) and \( l = j \), which implies \( E_{i,j} x = c_{i,j}(x c_{j,l}) = x \), hence \( x \in A_{i,j} \). This completes the proof of (b).

(c) Since \( t_{\lambda} \in R^* \) for \( 1 \leq \lambda \leq r \), we have

\[
w := \sum_{\lambda=1}^r t_{\lambda} c_{\lambda} \in J_R^0, \quad w^{-1} = \sum_{\lambda=1}^r t_{\lambda}^{-1} c_{\lambda} \tag{213}
\]

For \( 1 \leq i, j \leq r \), we now claim

\[
A_{i,j} = \{ x \in A \mid L_{i} x = t_j x, \ R_{i} x = t_j^{-1} x \} = \{ x \in A \mid L_{i} x = t_j x, \ R_{i} x = t_j^{-1} x \} \tag{214}
\]
where the second equation follows from the first since $L_{w-1} = L^{-1}_w$, $R_{w-1} = R^{-1}_w$ by \([1.4, 6, 2]\). In order to prove the first, we decompose $x$ as $x = \sum_{l,m} x_{lm} \in A_{lm}$ and apply \([4]\) to obtain
\[
L_w x = \sum_{k, l, m} t_k x_{lm} c_k = \sum_{l,m} t_l x_{lm} = R_w x.
\]
(215) ELNEX
Thus $L_w x = t_i x$ and $R_w x = t_i x$ if and only if $x = x_{ij}$, which completes the proof. In analogy to the proof of Thm. \([34.1]\) we now put
\[
T := \{ t_1^i \cdots t_r^i \mid i_1, \ldots, i_r \in \mathbb{Z} \}, \quad T_i := \{ t_i^1, \ldots, t_i^r \}
\]
and claim:

(*) If $s, t \in T$ admit an element $x \neq 0$ 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 $x = \sum_l x_{lm} \in A_{lm}$. Then \((215)\) implies
\[
\sum_l x_{lm} = sx = L_w x = \sum_l t_l x_{lm}, \quad \sum_l t^*_l x_{lm} = tx = R_w x = \sum_l t_1 x_{lm},
\]
and comparing components yields unique indices $i, j = 1, \ldots, r$ satisfying $s = t_i, t = t_j$ and $x = x_{ij}$.

For $1 \leq i, j, m \leq r$, $x_{ij} \in A_{ij}, y_{lm} \in A_{lm}$, we now obtain
\[
L_w (x_{ij} y_{lm}) = t_i t_j x_{ij} y_{lm}, \quad R_w (x_{ij} y_{lm}) = t_j^{-1} t_i t_m x_{ij} y_{lm},
\]
(216) ELNEXI
since the left and right Moufang identities \([34.3.1]\) and \([34.3.2]\) combined with \([34.6.2]\) and \((214)\) imply
\[
L_w (x_{ij} y_{lm}) = w (x_{ij} (w^{-1} w y_{lm})) = (wx_{ij} w) (w^{-1} y_{lm}) = t_i t_j x_{ij} y_{lm},
\]
\[
R_w (x_{ij} y_{lm}) = \left( (x_{ij} w^{-1}) w y_{lm} \right) w = (x_{ij} w^{-1}) (w y_{lm} w) = t_j^{-1} t_i t_m x_{ij} y_{lm},
\]
as claimed. Specializing $l \mapsto j$, $m \mapsto i$ in \((216)\) yields $L_w (x_{ij} y_{ij}) = t_i t_j x_{ij} y_{ij}, R_w (x_{ij} y_{ij}) = t_i t_j x_{ij} y_{ij}$, hence \([5]\). Similarly, \((216)\) for $l = i, m = j$ yields \([6]\), while \((7)\) follows from \((*)\) and \((216)\) since $j \neq l$ and $(i, j) \neq (l, m)$ imply that $t_i t_j t_l$ or $t_j^{-1} t_l t_m$ does not belong to $T_1$. Finally, for $1 \leq i, j \leq r$, $i \neq j$, and $x \in A_{ij}$, we apply \([6]\) to obtain $x^2 = A_{ij}$. But then \((211)\), \([4]\) and right alternativity yield $x^2 = E_{ij} x^2 = R_{ij} x^2 = (c_{ij} x) x = 0$, as claimed.

(d) Write $E_{ij}^{(\perp)}$, $1 \leq i \leq j \leq r$, for the Peirce projections of $\Omega$, viewed as a complete orthogonal system of idempotents in $A^{(\perp)}$. Comparing \([34.8.1]\) with \((211)\), we let $1 \leq i \leq j \leq r$ and conclude
\[
E_{ii}^{(\perp)} = U_{i i} = L_{ii} R_{ii} = E_{ii}, \quad E_{ij}^{(\perp)} = U_{i j} = L_{ij} R_{ij} + L_{i j} R_{ij} = E_{ij} + E_{ji}.
\]
The assertion follows.

Since the Peirce triples $(ij, ii, ij)$ and $(ij, jj, ij)$ are connected, \([34.11, 6]\) implies $U_{ij} J_{ij} \subseteq J_{jj}$ and $U_{ij} J_{ij} \subseteq J_{ii}$.

(a) $(i) \implies (ii)$. Applying Exc. \((17b)\) to $J' := J_1(c_1 + c_i)$, we conclude that $U_{ij} : J_{ij} \to J_{ij}$ is an isotopy. The first inclusion of $(ii)$ now follows from Prop. \([33.5]\) combined with Thm. \([33.10]\)(b). The second one follows by symmetry.

(a) $(ii) \implies (iii)$. Clear since $c_i \in J_{ij}$ and $c_{ij} \in J'_{ij}$.

(a) $(iii) \implies (i)$. Since the Peirce triples $(ij, ii, ij)$ are not connected for $l = 1, \ldots, r$, $i \neq l \neq j$, we have $v_{ij}^2 = \sum_{l \neq j} U_{ij} c_l = U_{ij} c_{ij} + U_{ij} c_{lj} \in J'^{\perp}$. Hence $v_{ij} \in J'^{\perp}$, and this is (a)(i). Basically the same argument also yields (b)(ii) $\implies$ (ii), while (b)(ii) $\implies$ (i) is obvious.

(c) \([31.3, 7]\) for $x = v_{ij}, y = v_{ji}, z = 1$ yields
Since $i, j, l$ are mutually distinct, the Peirce triples $(jl, iii, jll), (jll, jli, jlj)$ and $(jjl, jli, jlj)$ are not connected. Moreover, $V_j, c_1 = c_1, v_jj = v_{j1j}$ by (34.11.13) and (34.2.6). Summing up, therefore, (217) collapses to $U_{v_jj} c_i = U_j U_v c_i$ and, similarly, $U_{j} c_{i} = U_{j} U_{v} c_{i}$. Combining this with the characterization of (strong) connectedness in (a) (resp. (b)), the assertion follows.

(a) Free use will be made of the Peirce multiplication rules assembled in the present section. Let $1 \leq i, j \leq r$. Setting $d_k := c_j^{(p)}$ for $k = 1, \ldots, r$, we apply (33.8.8) and deduce $d_1^{(2, p)} = U_{p-1} \sum_{k=1}^{r} p_k = p_{1-1} = d_1$, so $d_i$ is an idempotent in $f^{(p)}$. Now assume $i \neq j$. Since $\sum_{k=1}^{r} \lambda_k$ is a direct sum of ideals, we obtain $d_i^{(p)} d_j = U_{d_i d_j} \sum_{k=1}^{r} p_k = U_{d_i d_j} = 0$, while (33.8.5) yields $d_i \delta_j = [d_i d_j] = 0$. Thus the idempotents $d_i, d_j$ are orthogonal in $f^{(p)}$. The equation $\sum_{k=1}^{r} \lambda_k = p - 1 = 1_{f^{(p)}}$ shows, therefore, that $\Omega^{(p)}$ is a complete orthogonal system of idempotents in $f^{(p)}$. Write $E_{im} \left(\text{resp. } E_{im}^{(p)}\right)$ for the Peirce projections of $E$ (resp. $\Omega^{(p)}$ in $f^{(p)}$). Then $E_{im}^{(p)} = E_{im} U_{p}$ by (34.8.1), hence $E_{im}^{(p)} = E_{i} U_{p} = E_{i} = J_{i}$, and the proof of (a) is complete.

(b) For $1 \leq i \leq r$ we have $(c_i^{(p)} q) = q c_i - 1 = (U_{p} q) c_i^{(p)} = 1$, and the assertion follows.

(c) Suppose $v_j, c_j$ connects $c_1$ and $c_2$. Put $c_3 := v_{j1}$ and $p_i := \sum_{k=1}^{r} p_k \in \text{Diag}(J)^{\infty}$. By the solution to (34.7.1) we see that $v_{j1} c_i = v_{j1} c_i$, and hence $w_{i1} = (v_{j1} c_i)$ is an idempotent in $f^{(p)}$. Hence (33.8.8) implies

$$w_{i1}^{(2, p)} = U_{w_{i1}}(p_1 + p_2) = U_{w_{i1}} p_1 + U_{w_{i1}} c_1 = c_1 + U_{w_{i1}} p_1 = c_1 + p_1^{-1}.$$

Thus $c_1^{(p)}$ and $c_2^{(p)}$ are strongly connected by $w_{i1} c_i$. We argue by induction on $r$. For $r = 1$, the assertion agrees with Exc. 151(c). Now let $r > 1$ and assume the statement holds for $r - 1$ in place of $r$. Put $c_{r} := c_{r}^{(p)}$ and use Exc. 151(c) again to find an idempotent $c_{r} = c_{r}^{(p)}$ in $J$ satisfying $\varphi(c_{r}) = c_{r}^{(p)}$. Write $E_{i} \left(\text{resp. } E_{i}^{(p)}\right)$ for the Peirce projections (resp. components) of $J$ relative to $c$ and $E_{i}^{(p)} \left(\text{resp. } E_{i}^{(p)}\right)$ for the Peirce projections (resp. components) of $J'$ relative to $c'$, where $i = 0, 1, 2$. We have $\varphi \circ E_{i} = E_{i}^{(p)} \circ \varphi$ and hence $\varphi(J) = \langle \varphi \circ E_{i} \rangle(J) = E_{i}^{(p)} \circ \varphi(J) = E_{i}^{(p)}(J) = E_{i}^{(p)}(J') = J_{i}$. In particular, $\varphi_{J_{i}} := \varphi|_{J_{i}} : J_{i} \rightarrow J_{i}$ is a surjective homomorphism of Jordan algebras whose kernel, $\text{Ker}(\varphi_{J_{i}}) = J_{0} \cap \text{Ker}(\varphi) \subseteq \text{Ker}(\varphi)$ is a nil ideal in $J_{i}$. Moreover, $J_{i}^{(p)}$ contains $(c_{1}, \ldots, c_{i-1})$ is a complete orthogonal system of idempotents. Hence the induction hypothesis yields a complete orthogonal system $(c_{i}, \ldots, c_{r}, c_{r}^{(p)})$ of idempotents in $J_{i}$ such that $\varphi(c_{i}) = c_{i}^{(p)}$ for $1 \leq i \leq r$. By Prop. 34.6(c) and Cor. 34.7 therefore, $(c_{1}, \ldots, c_{r}, c_{r}^{(p)})$ is a complete orthogonal system of idempotents in $J$ with the desired properties.
(Exc. 168), hence \( c = 1 \), \( \tilde{c} = 0 \), a contradiction. Hence \( q(c) = 0 \) (since \( q(c) \in F \) by (31.12) is an idempotent), and \( 31.12[5] \) reduces to \( 0 \neq c = c^2 = (t(c)c)^2 \). Taking traces, we conclude \( 0 \neq t(c) = t(c)^2 \), hence \( t(c) = 1 \). Summing, we have shown that \( c \) and \( \tilde{c} \) are elementary idempotents of \( J \), whence the corresponding Peirce decomposition by Prop. 34.5 implies \( I = J_0(c) = Fc, \tilde{I} = J_0(\tilde{c}) = F\tilde{c} \). Thus the assignment \( \alpha \oplus \beta \mapsto \alpha c + \beta \tilde{c} \) defines an isomorphism from \( F \oplus F \) onto \( J \).

Chapter 6

Section 35

184. (a) For \( x \in X \), the assignment \( y \mapsto N(x,y) \) defines linear form on \( X \). By non-singularity, therefore, we find a unique element \( x^2 \in X \) such that \( T(x^2,y) = N(x,y) \) for all \( y \in X \). On the other hand, given \( y \in X \), the assignment \( x \mapsto N(x,y) \) for \( R \in k\text{-alg} \), \( x \in X_k \) defines a polynomial law \( N(-,y) : X \to k \) which is homogeneous of degree 2, hence a quadratic form (Exc. 55(b)). But then \( x \mapsto x^2 \) must be a quadratic map since \( T \) is non-singular, and the gradient identity holds in all scalar extensions. Next we prove that \( X \) together with 1, \( \tilde{x}, N \) is a cubic array. By Euler's differential equation and Exc. 55[4], 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 \( T(1) = 1 \), 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

\[
T(x,1 \times y) = T(x \times y,1) = N(1,x,y) = N(1,x)N(1,y) - T(x,y) = T(y)T(x) - T(x,y)
\]

and the unit identity follows again from the non-singularity of \( T \).

(b) Let \( 1', \tilde{x}', N' \) be the base point, adjoint, norm, respectively, of \( X' \). We must show that \( \varphi \) preserves adjoints. Since \( \varphi \) is linear, the chain rule in the form 13.15[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 preserves bilinear traces as well: \( T'(\varphi(x), \varphi(y)) = T(x,y) \). But now the gradient identity gives

\[
T'(\varphi(x^2), \varphi(y)) = T(x^2, y) = N(x,y) = N'(\varphi(x), \varphi(y)) = T'(\varphi(x^2), \varphi(y))
\]

and the non-singularity of \( T' \) combines with the surjectivity of \( \varphi \) to yield \( \varphi(x^2) = \varphi(x)^2 \), as claimed.

185 (a) Since cubic Jordan algebras and cubic norm structures are identified via Cor. 35.18 \( \varphi \) 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. 13.22[22] to the polynomial law \( g := N_j \circ \varphi : J \to k \), we see that it suffices to prove \( N_j(\varphi(x)) = N_j(x) \) for all \( x \in J \) having \( \varphi(x) \in J' \). But then the adjoint identity combined with the fact that \( \varphi \) preserves adjoints implies \( N_j(x)\varphi(x) = \varphi(x^2) = \varphi(x)^2 = N_j(\varphi(x))\varphi(x) \), hence the assertion since \( \varphi(x) \) by Cor. 35.16[10] is unimodular.

(b) Since \( \varphi \) preserves unit elements and norms, it is a surjective homomorphism of pointed cubic forms in the sense of Exc. 15[22]. By part (b) of that exercise, therefore, \( \varphi \) is an isomorphism of cubic arrays, hence of cubic Jordan algebras.

186. If \( X \) is a cubic norm structure over \( k \), then 11–13 hold by definition, while 4, 15 have been recorded in 35.8.10, 35.8.8, respectively. Conversely, suppose 11–15 hold for all \( x,y,z \in X \) and let \( R \in k\text{-alg} \). Since 11, 12, 14 are homogeneous of degree at most 2 in each variable, they continue to hold in \( X_k \), so it remains to verify 13, 15 over \( R \). We first linearize

187.
to conclude that $T(x \times y, z) = N(x, y, z)$ is totally symmetric in $x, y, z \in X$. Hence linearizing
with respect to $y$ implies
\[ x^2 \times (y \times z) + (x \times y) \times (x \times z) = T(x^2, y)z + T(x^2, z)y + T(x \times y, z)x \]  
(218)
for all $x, y, z \in X$. Turning now to the proof of (15), linearity allows us to assume $y = v_R$ for some
$v \in X$; we then put
\[ M := \{ x \in X_R \mid x^2 \times (x \times y) = T(x^2, y)x + N(x)y \} . \]
By homogeneity, we have $rx \in M$ for all $x \in M$, $r \in R$. Moreover, for $u \in X$, the validity of (15)
over $X$ yields
\[ (u_R)^2 \times (u_R \times v_R) = (u^2_R) \times (u_R \times v_R) = (u^2 \times (u \times v))_R \]
\[ = T(u^2, v)u + N(u)v = T((u_R)^2, v_R)u_R + N_R(u_R)v_R , \]
hence $u_R \in M$. But the elements $u_R, u \in X_R$ span $X_R$ as an $R$-module. Therefore (15) 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 (218) yield
\[ (x + z)^2 \times ((x + z) \times y) = (x^2 + x \times z + z^2) \times (x \times y + z \times y) \]
\[ = x^2 \times (x \times y) + x^2 \times (z \times y) + (x \times z) \times (x \times y) + \]
\[ (x \times z) \times (z \times y) + z^2 \times (x \times y) + z^2 \times (z \times y) \]
\[ = T(x^2, y)x + N(x)y + T(z^2, y)z + T(x \times z, y)z + N(z)y \]
\[ = T((x + z)^2, y)(x + z) + N((x + z)y) \]
forcing $x + z \in M$, and the proof of (15) is complete. Now (13) will be treated in a similar manner
by putting
\[ M' := \{ x \in X_R \mid x^{2R} = N(x)x \} \subseteq X_R . \]
Since both sides of (13) are homogeneous of the same degree, $N$ is stable under scalar multiplica-
tion: $x \in M'$ and $r \in R$ implies $rx \in M'$. Moreover, for $x \in X$ we conclude, using the fact that $N$
 is a polynomial law,
\[ (x_R)^{2R} = (x^{2R})_R = (N(x)x)_R = (N(x)1_R)x_R = N(x_R)x_R , \]
hence $x_R \in M'$. But the elements $x_R, x \in X_R$ span $X_R$ as an $R$-module. Therefore (13) 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
(12), (14), (15) and the definition of $M'$ imply
\[ (x + y)^{2R} = (x^2 + x \times y + y^2)^2 \]
\[ = x^{2R} + x^2 \times (x \times y) + x^2 \times y^2 + (x \times y) \times y^2 + y^{2R} \]
\[ = N(x)x + T(x^2, y)x + N(x)y + T(x^2, y)y + \]
\[ T(x, y^2)x + T(x, y^2)y + N(y)x + N(y)y \]
\[ = (N(x) + T(x^2, y) + T(x, y^2) + N(y))(x + y) = N(x + y)(x + y) , \]
forcing $x + y \in M'$, as desired.
Let $X$ be a rational cubic norm structure over $k$, with base point 1, adjoint $x \mapsto x^2$, bilinearized
adjoint $(x,y) \mapsto x \times y$, bilinear trace $T$ and norm $N$. Combining (19) and (20) with the bilinearity
of $\times$, we conclude that $\sharp : X \to X$ is indeed a quadratic map with bilinearization $\times$. Beside the
map $N : X \to k$, we now consider the map $g : X \times X \to k$ defined by $g(x,y) := T(x^2, y)$ for $x,y \in X$.
Since the adjoint is a quadratic map with bilinearization $\times$, we deduce from (17), (19), (20) that
conditions (i)–(iv) of Exc. 59(b) hold for $(N, g)$, so $(N, g) : X \to k$ is a cubic map. By part (c) of
that exercise, therefore, we find a unique cubic form $\tilde{N} := N \ast g : X \to k$ such that $\tilde{N}(x) = N(x)$
and $\tilde{N}(x,y) = T(x^2, y)$ for all $x,y \in X$. Here (21) and (24) imply $1 = 1^2 = N(1)$, hence $N(1) = 1$
since 1 is unimodular. Thus $X$ together with the base point 1, the adjoint $\sharp$ and the norm $N$ 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 $\tilde{X}$. In view of
(25), we have $\tilde{T}(x) := \tilde{N}(1, x) = T(1, x)$ and $\tilde{S}(x) = \tilde{N}(x, y) = \tilde{T}(1, x^2)$ for $x \in X$, while Exc. 59(c)
implies $\tilde{T}(x \times y, z) = \tilde{T}(x, y \times z) = \tilde{T}(x, y) \tilde{T}(x, z)$ for all $x,y,z \in X$. Putting $x = 1$ and combining (35.8.10)
with (25), we conclude $\tilde{T}(y,z) = \tilde{T}(y)\tilde{T}(z) - \tilde{S}(y,z) = \tilde{T}(1, y)\tilde{T}(1, z) - \tilde{T}(1, y \times z) = \tilde{T}(y, z)$. Thus
$\tilde{T}$ is the bilinear trace of $\tilde{X}$. Hence equation (12) of Exc. 186 holds over $k$. But so do (11), (13),
and (15) of that exercise, by (25), (21)–(23), respectively. Thus all equations of Exc. 186 hold over $k$,
forcing the cubic array $\tilde{X}$ to be, in fact, a cubic norm structure.

If $\phi : X \to Y$ is a homomorphism of rational cubic norm structures, then $\phi : \tilde{X} \to \tilde{Y}$ is a linear
map preserving base points and adjoints. By Exc. 185(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 $x \mapsto x^2$, bilinear trace
$T$ and norm $N$. We claim that $1, x \mapsto x^2, (x,y) \mapsto x \times y, T$ and the set map $N : X \to k$ make $X$ a
rational cubic norm structure over $k$, denoted by $\text{Rat}(X)$, i.e., equations (16)–(25) hold. Indeed,
(19)–(20) are obvious, while (19)–(25) have been established in this order in (35.8.6), (35.8.11), (35.8.12), (35.8.13),
and (35.8.14), respectively. If $\phi : X \to Y$ is a homomorphism of cubic norm structures, then $\phi : \text{Rat}(X) \to \text{Rat}(Y)$ is trivially
one of rational cubic norm structures. Thus we obtain a functor from $k$-cuno to $k$-racuno which by Exc. 59(d) is
easily seen to be inverse to the functor $k$-cuno $\to k$-racuno constructed before. This completes the proof.

We first linearize (35.8.28) and obtain
\[
\sum_{u,v,w} a(u,v) + v \times (w \times u) + w \times (u \times v) = \left( \sum_{u,v} \tilde{T}(u \times v, w) \right) + \left( \sum_{v,w} T(v \times w) \right) - \left( \sum_{u,v} T(u \times v) \right)
\]
for all $u,v,w \in X$. We must show that the submodule $M \subseteq X$ spanned by the elements assembled
in (26) is stable under the adjoint map. First of all, we have $1^2 = 1 \in M$ by the base point identities
(35.8.11) and $1 \times 1 \in M$ by the unit identity (35.8.3). Moreover, $M$ is spanned by the elements
$x,s,t,s \times t, s \in \{x,x^2\}, t \in \{y,y^2\}$. Hence it will be enough to show that, for all $s,s' \in \{x,x^2\}$,
$t,t' \in \{y,y^2\}$,
\[
\begin{align*}
\tilde{T}(s \times t, (s \times t)^2) & \in M, \\
\tilde{T}(s \times t, (s' \times t)^2) & \in M, \\
\tilde{T}(s \times t', (s \times t')^2) & \in M, \\
\tilde{T}(s \times t, (s' \times t')^2) & \in M.
\end{align*}
\]

The adjoint identity (35.8.5) implies $s^2 \in \{N(x)x,x^2\}$, $s'^2 \in \{N(x)y,y^2\}$, hence not only the first two
inclusions of (220) but also $s^2 \times t' \in M$, while the third one now follows from (35.8.10). In the
first inclusion of (221) we may assume $s = x, s' = x^2$, whence the assertion follows from (14). The
second relation of (221) follows from (25), (220) for $s = s'$ and from (19), (8) for $s \neq s'$. Next,
(222) is (224) with $x$ and $y$ interchanged, so we are left with (223). We first note that $1 \times M \subseteq M$
and (221), (222) imply
\[ s \times M + t \times M \subseteq M. \quad (224) \]

Then we combine (219) with (220)–(222) to conclude

\[ (s \times t) \times (s' \times t') \equiv -s' \times (t' \times (s \times t)) - t' \times ((s \times t) \times s') \mod M, \]

and (224) implies (223).

sol.NORID

(a) The straightforward verification is left to the reader.

(b) We first show \( \mathcal{T}(x,y) = 0 \) for all \( x \in \mathcal{X} \) and all \( y \in \mathcal{Y} \). By condition (i), we find a linear form \( \lambda \) on \( \mathcal{X} \) separating \( 1 \) from \( \mathcal{I} : \lambda(1) = 1, \lambda(\mathcal{I}) = \{0\} \). From condition (iii) and the unit identity (35.8.3), we conclude that \( x \times y = \mathcal{T}(y)1 - y \) is contained in \( \mathcal{I} \), forcing \( 0 = \lambda(\mathcal{T}(y)1 - y) = \lambda(\mathcal{T}(y)) - \lambda(y) = \mathcal{T}(y) \). Thus the linear trace vanishes on \( \mathcal{I} \). This combined with condition (i) and (35.8.13) implies \( 0 = \mathcal{T}(x \times y) = \mathcal{T}(x)\mathcal{T}(y) - \mathcal{T}(x,y) = -\mathcal{T}(x,y) \), as claimed. Next consider the set maps \( f: \mathcal{X} \to \mathcal{K} \) and \( g: \mathcal{X} \times \mathcal{Y} \to \mathcal{K} \) defined respectively by \( f(x) = \mathcal{N}(x) \), \( g(x,y) = \mathcal{N}(x,y) = \mathcal{T}(x^2,y) \) for all \( x,y \in \mathcal{X} \). Then \( (f,g): \mathcal{X} \to \mathcal{K} \) is a cubic map, and conditions (ii), (iii) for a norm ideal combined with what we have just proved imply \( \mathcal{I} \subseteq \text{Rad}(f,g) \). Hence Exc. 59(a) yields a unique cubic map \( (f_1,g_1): \mathcal{X}_1 \to \mathcal{K} \) such that \( f_1 \circ \pi = f \), \( g_1 \circ (\pi \times \pi) = g \). Put \( \lambda_1 := \pi(1) \). By condition (iii) for a norm ideal, the adjoint \( \pi : \mathcal{X} \to \mathcal{X} \) induces canonically a unique quadratic map \( \mathfrak{z}_1 : \mathcal{X}_1 \to \mathcal{X}_1 \) satisfying \( \pi(x)\mathfrak{z}_1 = \pi(x^2) \) for all \( x \in \mathcal{X} \). Moreover, for \( x, y \in \mathcal{X} \) we have \( \pi(x) = \pi(y) = \pi(x \times y) \), where \( \times \) stands for the bilinearization of \( \mathfrak{z}_1 \). Finally, the bilinear trace of \( \mathcal{X} \) induces canonically a symmetric bilinear form \( \mathcal{T}_1 : \mathcal{X}_1 \times \mathcal{X}_1 \to \mathcal{K} \) such that \( \mathcal{T}_1(\pi(x),\pi(y)) = \mathcal{T}(x,y) \) for all \( x, y \in \mathcal{X} \). Setting \( \mathcal{N}_1 := \mathcal{N}_1 : \mathcal{X}_1 \to \mathcal{K} \), it is now straightforward to verify that the identities \( (16) \to (25) \) of Exc. 187 hold for \( \mathcal{N}_1 \) since they do for \( \mathcal{X} \). As the linear form \( \lambda \) kills \( \mathcal{I} \), it induces canonically a linear form \( \lambda_i : \mathcal{X}_1 \to \mathcal{K} \) having \( \lambda_1(1_1) = 1 \) and thus making \( 1_1 \in \mathcal{X}_1 \) unimodular. Summing up, Exc. 187 converts \( \mathcal{N}_1 \) into a cubic norm structure over \( \mathcal{K} \) such that \( \pi \) preserves base points and adjoints, hence by Exc. 188 is a homomorphism of cubic norm structures with kernel \( \mathcal{I} \).

sol.TRACUJO

We have \( 3 = \mathcal{T}(1,1) = 0 \) in \( \mathcal{K} \), hence \( 2 = -1 \in k^\times \). Thus \( \mathcal{J} \) may be viewed as a linear Jordan algebra whose bilinear multiplication by \( 31.4 \) and (35.13.8) is given by

\[ xy = \frac{1}{2} x \circ y = -x \circ y = -xy \]

since not only the bilinear trace but also the linear (by (35.8.2)) and the quadratic one (by (35.8.12)) are identically zero. We conclude \( x^2 = x^2 \) (which follows also from (35.13.7)), while (29.9.1) and (35.6.1) imply

\[ 2(x \circ y) - x^2 y = U_{xy} = \mathcal{T}(x,y) \circ x - x^2 \circ y = -x^2 \circ y = x^2 y, \]

hence the left alternative law \( x(xy) = x^2 y \). Being also commutative, \( \mathcal{J} \) is in fact alternative.

sol.CUBNIL

For the first part of the problem, if \( \mathcal{T}(x), \mathcal{S}(x), \mathcal{N}(x) \in \mathcal{K} \) are nilpotent, then so are \( \mathcal{T}(x) x^2, \mathcal{S}(x) x, \mathcal{N}(x) \mathcal{I} \in \mathcal{J} \). By (35.9.2) and Exc. 150, \( x^3 \) is nilpotent, whence \( x \in \mathcal{N}(x) \). Conversely, \( \mathcal{N}(x) \) is nilpotent. Since \( \mathcal{N} \) permits Jordan composition, it commutes with taking powers, and we conclude \( \mathcal{N}(x) \in \text{Nil}(k) \). Moreover, applying Exc. 150 again, there exists a positive integer \( m \) such that \( x^m = 0 \) for all integers \( n \geq m \). We now show \( \mathcal{T}(x), \mathcal{S}(x) \in \text{Nil}(k) \) 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 \( x^2 m = x^{2n} = 0 \) for all integers \( n > m - 1 \), the induction hypothesis implies that \( \mathcal{T}(x^2) \) and \( \mathcal{S}(x^2) \) are nilpotent. On the other hand, from (35.8.22) and the adjoint identity (35.8.5) we deduce

\[ \mathcal{T}(x^2) = 2\mathcal{S}(x) + T(x^2), \quad \mathcal{S}(x^2) = 2T(x)\mathcal{N}(x) + \mathcal{S}(x^2). \]

Since \( \mathcal{N}(x) \) is nilpotent, the induction hypothesis and the second equation imply that \( \mathcal{S}(x^2) \) is nilpotent, which combines with the first equation to show that \( \mathcal{T}(x) \) is nilpotent as well. This completes the proof of the first part.

In order to establish the second part, we put...
\[ I := \{ x \in J \mid \forall y \in J : T(x,y), T(x^2,y), N(x) \in \text{Nil}(k) \} \] (225)

and have to show \( I = \text{Nil}(J) \). For \( x, y \in I \) and \( z \in J \), we apply (35.8.10), (35.8.11) and obtain
\[ N(x+y) = N(x) + T(x^2,y) + T(x,y^2) + N(y) \in \text{Nil}(k), \]
\[ T(x+y,z) = T(x,z) + T(y,z) \in \text{Nil}(k), \]
\[ T((x+y)^2,z) = T(x^2,z) + T(x,y \times z) + T(y^2,z) \in \text{Nil}(k), \]

hence \( x+y \in I \). Thus \( I \subseteq J \) is a \( k \)-submodule. Next we claim
\[ \hat{I} + I \times J \subseteq I. \] (226)

The inclusion \( \hat{I} \subseteq I \) follows immediately from (225), the adjoint identity (35.8.1) and (35.8.18). It remains to show \( x \times y \in I \) for all \( x \in I, y \in J \). Given \( z \in J \), we apply (35.8.9), (35.8.10), (35.8.11)
\[ N(x \times y) = T(x^2,y) - N(x)N(y) \in \text{Nil}(k), \]
\[ T(x \times y,z) = T(x,y \times z) \in \text{Nil}(k), \]
\[ T((x \times y)^2) = T(x^2,y)T(y,z) + T(x,y^2)T(z,x) - T(x^2,y^2 \times z) \in \text{Nil}(k). \]

Hence \( x \times y \in I \) and (226) holds. Now let \( x \in I \) and \( y \in J \). Then \( U_0y = T(x,y)x - x^2 \times y \in I \) by (226), so \( I \subseteq J \) is an inner ideal. But since
\[ T(U_0x,z) = T(x,U_0z) \in \text{Nil}(k), \]
\[ T((U_0x)^2,z) = T(U_0x^2,z) = T(x^2,U_0z) \in \text{Nil}(k), \]
\[ N(U_0x) = N(y)N(x) \in \text{Nil}(k) \]
for all \( z \in J \) by (35.8.11), (35.8.12), (35.8.13) and (226), we also have \( U_0x \in I \) by (225), so \( I \subseteq J \) is an outer ideal altogether, therefore, an ideal in \( J \) which by the first part of the problem consists entirely of nilpotent elements. This proves \( I \subseteq \text{Nil}(J) \).

Conversely, let \( x \in \text{Nil}(J) \). Then \( T(x), S(x), N(x) \in \text{Nil}(k) \) by the first part of the problem, and we have \( \text{Nil}(k) \cap \text{Nil}(J) \subseteq \text{Nil}(J) \) by Ex. 148(c). Furthermore, for all \( y \in J \), \( \text{Nil}(J) + U_0y = T(x,y)x - x^2 \times y \), hence \( x^2 \times y \in \text{Nil}(J) \), which by (35.8.12), (35.8.13) implies \( S(x)T(y) - T(x^2,y) = T(x^2 \times y) \in \text{Nil}(k) \). Thus \( T(x^2,y) \in \text{Nil}(k) \). Since \( z := U_0x - T(x,y)x^2 - y^2 \times x \) belongs to the ideal \( \text{Nil}(J) \), so does \( x+z \), which by (35.8.1), (35.8.13), implies
\[ T(x,y)^2 - 2T(x^2,y) = T(x,y^2) - T(x \times x,y^2) - T(x^2,y^2 \times x) = T(x,U_0x), \]
\[ = T(x,z) = T(x)T(z) = S(x,z) \]
\[ = T(x)T(z) + S(x) + S(z) = S(x+z) \in \text{Nil}(k). \]

Thus \( T(x,y) \in \text{Nil}(k) \) and summing up we have shown \( x \in I \). This completes the proof of (27).

Finally, let \( x, y \in J \). If \( \frac{1}{2} \in k \), then \( T(x,y) = \frac{1}{2}T(x \times x,y) = \frac{1}{2}T(x,x \times y) \) by (35.8.7), so (27) implies (28). Similarly, if \( \frac{1}{2} \in k \), then \( N(x) = \frac{1}{2}T(x,x^2) \) by (35.8.11), so (27) implies (29). Finally, (30) follows by combining (28) and (29).

(a) \( N \) as defined by (31) is clearly a cubic form such that
\[ N(r \oplus u, s \oplus v) = sq(u) + rq(u,v) \]
for \( R \in k\text{-alg}, r, s \in R, u, v \in J_R \). 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 \( x \in J \), we therefore conclude that (35), (34) hold. For \( x = r \oplus u \in J_R \), this and (31.12.5), (31.12.6) imply
\[ x^3 - T(x)x^2 + S(x)x - N(x)1_{J} = \left( r^3 - (r + t(u))r^2 + (rt(u) + q(u))r - rq(u) \right) \]
\[ \oplus \left( u^3 - (r + t(u))u^2 + (rt(u) + q(u))u - rq(u)e \right) \]
\[ = 0 \oplus \left( u^3 - t(u)u^2 + q(u)u - r(u^2 - t(u)u + q(u)e) \right) \]
\[ = 0, \]
\[ x^4 - T(x)x^3 + S(x)x^2 - N(x)x = \left( r^4 - (r + t(u))r^3 + (rt(u) + q(u))r^2 - rq(u)r \right) \]
\[ \oplus \left( u^4 - (r + t(u))u^3 + (rt(u) + q(u))u^2 - rq(u)u \right) \]
\[ = 0 \oplus \left( u^4 - t(u)u^3 + q(u)u^2 - r(u^3 - t(u)u^2 + q(u)e) \right) \]
\[ = 0. \]

Since \( q \) permits Jordan composition by (31, 12), so does \( N \) by (31), and we have shown that \( \hat{J} \)

is a cubic Jordan algebra with norm \( N \) over \( k \) such that (31, 33, 34) hold. Linearizing (34) and

applying (55, 210), we also obtain (32). Finally, (55, 8, 22) implies, for \( x = \alpha \oplus u, \alpha \in k, u \in J \).

\[ x^2 = x^2 - T(x)x + S(x)1_J = \left( \alpha^2 - (\alpha + t(u))\alpha + (\alpha t(u) + q(u)) \right) \]
\[ \oplus \left( u^2 - (\alpha + t(u))u + (\alpha t(u) + q(u))e \right) \]
\[ = q(u) \oplus \left( \alpha(tu)e - u \right) \]
\[ = q(u) \oplus \alpha u. \]

This proves (35), and (a) is solved.

(b) Applying Exc. 162, 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

\[ \hat{C}(+) = k^{(+)} \oplus C^{(+)} = k^{(+)} \oplus J = \hat{J} \]

is a cubic Jordan algebra over \( k \) with norm \( N \): \( \hat{C} \to k \) given by

\[ N(r \oplus u) = r_{n_C}(u) \quad (R \in k\text{-alg}, \ r \in R, \ u \in C_R). \]

(227) NOHAC

Hence \( \hat{C} \) is a cubic alternative \( k \)-algebra with norm \( N \) which by (227) is multiplicative if and only if \( C \) is. Finally, Example (35, 22) fits into this picture by setting \( C := k \).

(a) The arguments solving Exc. 187 go through for rational cubic norm pseudo-structures without change and prove (a).

(b) (i) \( \Rightarrow \) (ii). Let \( 1 \leq i \leq n \). Then (i) and Euler’s differential equation imply \( \sigma(e_i^2, e_i) = \mu(e_i, e_i) = 3\mu(e_i) = 3w_i \). Moreover, linearizing the relation \( \mu(v, v') = \sigma(v^2, v') \), 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 \( R \in k\text{-alg} \), we define a map \( \mu_R : V_R \to W_R \) by setting

\[ \mu_R \left( \sum_{i=1}^{n} r_i e_i R \right) := \sum_{i=1}^{n} r_i^3 w_{i R} + \sum_{1 \leq i < j < n} r_i^2 r_j \sigma(e_i, e_j)_{R} + \sum_{1 \leq i < j < n} r_i r_j r_k \sigma(e_i \times e_j, e_k)_{R} \]

(228) MUAR

for \( r_1, \ldots, r_n \in R \). Then \( \mu := (\mu_R)_{R \in k\text{-alg}} : V \to W \) is obviously a homogeneous polynomial law of degree 3 satisfying \( \mu(e_i) = w_i \) for \( 1 \leq i \leq n \). Now let \( v = \sum_{i=1}^{n} r_i e_i R, v' = \sum_{i=1}^{n} r_i' e_i R \in V_R \) with \( r_i, r_i' \in R \) for \( i = 1, \ldots, n \). Then (228) implies
\[\mu(v,v') = \sum_i 3r_i^2 r_i w_{ij} + \sum_{i\neq j} (2r_i r_j + r_i^2 r_j) \sigma(e_i^e, e_j) + \sum_{i<j} (r_i r_j r_i + r_j r_i r_j) \sigma(e_i \times e_j, e_i) R.\]

On the other hand
\[v^2 = \sum_i r_i^2 e_i^R + \sum_{i<j} r_i r_j e_i \times e_j R,\]

and hence (ii) gives
\[\sigma(v^2, v') = \sum_i r_i^2 r_i' \sigma(e_i^e, e_i) + \sum_{i\neq j} r_i r_j r_i' \sigma(e_i \times e_j, e_i) R + \sum_{i<j} (r_i r_j r_i + r_j r_i r_j) \sigma(e_i \times e_j, e_i) R\]
\[= \sum_i r_i^2 r_i' \sigma(e_i^e, e_i) + \sum_{i\neq j} r_i r_j r_i' \sigma(e_i \times e_j, e_i) R + \sum_{i<j} (r_i r_j r_i + r_j r_i r_j) \sigma(e_i \times e_j, e_i) R\]
\[= \sum_i 3r_i^2 w_{ij} + \sum_{i\neq j} (r_i r_j r_i + r_j r_i r_j) \sigma(e_i \times e_j, e_i) R\]
\[= 0 = \mu(v, v'),\]

and (i) holds. Finally, uniqueness of \(\mu\) follows immediately from (6) of Exc. 58.

(c) Since a pseudo cubic norm pseudo-structure \(X\) over \(k\) is automatically a cubic norm structure if \(\frac{1}{2} \in k\) (\(\lambda := \frac{1}{2} T\) 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 \(a \in K\). Then \(F\) is infinite and \(J_0 := K^+\) is a cubic Jordan algebra over \(F\), with norm \(N_0 : K \to F\) (by Prop. 13.11 an honest-to-goodness polynomial function) given by \(N_0(v) = v^3\) for all \(v \in J_0\). For \(R \in F\)-alg and \(v, v' \in J_0\), we conclude \(N_0(vv') = 3v^2 v' = 0\), so the (bi-)linear and quadratic traces of \(J_0\) are both zero, and \(v^2 = v^2\) by 35.8.22 as well as \(v \times v' = 2v' = -v'\) 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 \(A : J_0 \to W\) be a non-zero linear map satisfying \(A(1) = 0\). Define a symmetric bilinear map \(\sigma : J_0 \times J_0 \to W\) by \(\sigma(v, v') := A(vv')\) for \(v, v' \in J_0\). Then \(\sigma(v^2, v) = A(v^3) = A(1) = 0\) for all \(v \in J_0\), and \(\sigma(v_1 \times v_2, v_3) = A(v_1 v_2 v_3)\) is totally symmetric in \(v_1, v_2, v_3 \in J_0\). Thus (b) yields a homogeneous polynomial law \(\mu : J_0 \to W\) of degree 3 such that \(\mu(1) = 0, \mu(a) = w_1, \mu(a^2) = \mu(w_1^2) = w_2\).

Now let \(k := F \oplus W\) be the “split-null extension” of \(F\) by \(W\), so \(W \subset k\) is an ideal that squares to zero and \(F\) acts canonically on \(W\). In other words, the multiplication of \(k\) obeys the rule
\[(\alpha \oplus w)(\alpha' \oplus w') := (\alpha \alpha') \oplus (\alpha w' + \alpha' w)\]
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 \(T : J \times J \to k\)
\[T(v, v') := 0 \oplus \sigma(v, v') = 0 \oplus A(vv')\]
for \(v, v' \in J\), which is in fact a \(k\)-bilinear form since
\[T((\alpha \oplus w)v, v') = T(\alpha v, v') = \alpha T(v, v') = (\alpha \oplus w)(0 \oplus A(vv')) = (\alpha \oplus w)T(v, v')\]
for all \(\alpha \in F, w \in W, v, v' \in J\). Similarly, we obtain a map
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 \([16]–[25]\) of Exc. \([187]\) To show this, let $\alpha \in F$, $w \in W$ and $v, v' \in J$. Then

\[
((\alpha \oplus w)v)^2 = (\alpha v)^2 = (\alpha \oplus 2\alpha w)v^2 = (\alpha \oplus w)^2v^2 \quad (229) \tag*{SHARK}
\]

proves \([16]\) and

\[
N((\alpha \oplus w)v) = N(\alpha v) = \alpha^2(N_0(v) \oplus \mu(v)) = (\alpha \oplus w)^2(N_0(v) \oplus \mu(v)) = (\alpha \oplus w)^2N(v)
\]

proves \([17]\). The equations \((229)\) and

\[
((\alpha \oplus w)v) \times v' = (\alpha v) \times v' = \alpha(v \times v') = (\alpha \oplus w)(v \times v')
\]

show that the adjoint $v \mapsto v^2$ is not only $F$-quadratic but, in fact, $k$-quadratic. Moreover, the bilinearized adjoint is the $k$-bilinearization of the adjoint, and we have \([18]\). Next we compute

\[
N(v+v') = N_0(v+v') \oplus \mu(v+v') = (N_0(v)+N_0(v')) \oplus (\mu(v)+\mu(v')) + \mu(v',v)+\mu(v',v')
\]

\[
= (N_0(v) \oplus \mu(v)) + (0 \oplus \sigma(v^2,v')) + (0 \oplus \sigma(v'^2,v)) + (N_0(v') \oplus \mu(v'))
\]

\[
= N(v) = T(v^2,v') + T(v'^2,v) + N(v'),
\]

and \([19]\) holds. Since $3 = 0$ in $k$, we have $T(v^2,v) = 0 \oplus \sigma(v^2,v) = 0 = 3N(v)$, hence \([20]\). Since the adjoint identity holds in $J_0$, we obtain

\[
v^{22} = N_0(v)v = (N_0(v) \oplus \mu(v))v = N(v)v,
\]

hence \([21]\). Similarly,

\[
v^{2} \times v^{2} + (v \times v')^{2} = -v^{2}v^{2} + (vv')^{2} = 0 = (0 \oplus \lambda(v^{2}v'))v' + (0 \oplus \lambda(vv'^{2}))v
\]

\[
= T(v^{2},v')v' + T(v,v')v
\]

gives \([22]\) and

\[
v^{2} \times (v \times v') = v^{2}(vv') = (v^{2})v' = (0 \oplus \lambda(v^{2}v'))v + N_0(v)v' = (N_0(v) \oplus \mu(v))v'
\]

\[
= T(v^{2},v')v' + N(v)v'
\]

gives \([23]\). While \([24]\) is obvious, the unit identity for $J_0$ implies $1 \times v = -v = (0 \oplus \lambda(v))1 - v = T(1, v)1 - v$, hence \([25]\).

By Exc. \([187]\) therefore, we find a cubic form $\tilde{N} : X \to k$ making $X$ a cubic norm pseudo-structure over $k$. Now consider the element $a \in J$. By construction we have

\[
N(a^2) = N_0(a^2) + \mu(a^2) = N_0(a)^2 + w_2.
\]

\[
N(a)^2 = (N_0(a) + \mu(a))^2 = N_0(a)^2 + 2N_0(a)\mu(a) = N_0(a)^2 - N_0(a)w_1,
\]

hence $N(a^2) \neq N(a)^2$ since $w_1, w_2$ are linearly independent over $F$.

Section \([36]\)

(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 eiconal triple structure provides us with quadratic maps $Q : V \to k, H : V \to V$. Moreover, setting $v = u$ in \([2]\), Euler’s differential equation implies
\[ Q(u, H(u)) = N(u) \quad (R \in k\text{-alg, } u \in V_k). \quad (230) \]

By \ref{36.9}, therefore, formulas (4)–(6) define a cubic array \( X \) over \( k \) whose bilinear trace by \ref{36.9.5} is non-singular. 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. \ref{36.10}, that the identities (36.10.1)–(36.10.9) hold strictly in \( X \). Here (36.10.5) is just the eiconal equation, while (36.10.7) has been established in (230) with \( N = N \). Since (36.10.1)–(36.10.4), (36.10.6), (36.10.9) are obvious in the special case at hand, we are left with (36.10.6), (36.10.8), (36.10.9), i.e., with

\[
\begin{align*}
H(H(u)) &= N(u)u - Q(u)H(u), \quad (231) \\
Q(u, H(u, v)) &= 2Q(H(u), v), \quad (232) \\
H(u, H(u)) &= 2Q(u)u. \quad (233)
\end{align*}
\]

We begin with (233) by linearizing (3) to conclude that

\[
Q(H(u,v), w) = \frac{1}{3} N(u, v, w) \quad (234)
\]

is totally symmetric in \( u, v, w \in V \). Combining this with the linearization of (3), i.e., with

\[
Q(H(u), H(v)) = 2Q(u)Q(v), \quad (235)
\]

we conclude \( Q(H(u, H(u))), v = Q(H(u, v), H(u)) = 2Q(u)Q(v, u, v), \) and (235) drops out since \( Q \) is non-singular. Setting \( w = u \) and using symmetry of (234) again, we obtain \( Q(H(u,v), u) = Q(H(u), v) = 2Q(u,v) \), hence (232). And finally, linearizing (233), we deduce

\[
H(u, H(u)) + H(u, H(u)) = 2Q(u,v)u + 2Q(u)u. \quad (236)
\]

Here we put \( v = H(u) \) apply (233), (230) and obtain

\[
\begin{align*}
2H(H(u)) + 4Q(u)H(u) &= H(H(u), H(u)) + 2H(u, Q(u)u) \\
&= H(H(u), H(u)) + H(u, H(u, H(u))) = 2Q(u, H(u))u + 2Q(u)H(u) \\
&= 2N(u)u + 2Q(u)H(u),
\end{align*}
\]

hence (231).

(ii) The cubic norm substructure \( X_0 \subseteq X \) is non-singular since \( \frac{1}{2} \in k \). Hence \( (X_0, V) \) is a complemented cubic norm substructure of \( X \). Defining a quadratic map \( H : V \rightarrow V \) by \( H(u) := Q(u)u^2 \) for \( u \in V \), we are in the situation \ref{36.7} and conclude that the identities (36.7.1)–(36.7.3), (36.7.1)–(36.8.18) hold strictly in \( X \). In particular, by (36.7.4) 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 \( 3Q(H(u), v) = T(H(u), v), \) whence \( (V, Q) \) is a quadratic space over \( k \). Finally, \ref{36.8.19} shows that the eiconal equation (3) holds strictly in \( V \). Summing up we have proved that \( (V, Q, N|_V) \) is an eiconal triple over \( k \).

(iii) follows by a straightforward verification.

(iv) The gradient of \( N \) at \( u \in \mathbb{R}^n \) is defined by

\[
\left( \text{grad}(N) \right)(u) = \begin{pmatrix}
\frac{\partial N}{\partial u_1}(u) \\
\vdots \\
\frac{\partial N}{\partial u_n}(u)
\end{pmatrix} \in \mathbb{R}^n
\]

and can be characterized by

\[
\left( \text{grad}(N) \right)(u)^T v = N(u, v) \quad (v \in \mathbb{R}^n).
\]
This and (2) imply
\[ H(u)^{\top}Qv = Q(H(u), v) = \frac{1}{3} (\text{grad}(N))(u)^{\top}v, \]
and we conclude \( H(u)^{\top}Q = \frac{1}{3}(\text{grad}(N))(u)^{\top}, \) hence
\[ H(u)^{\top} = \frac{1}{3}(\text{grad}(N))(u)^{\top}Q^{-1}, \quad H(u) = \frac{1}{3}Q^{-1}(\text{grad}(N))(u). \]
Now the left-hand side of (3) becomes
\[ H(u)^{\top}QH(u) = \frac{1}{9}(\text{grad}(N))(u)^{\top}Q^{-1}QQ^{-1}(\text{grad}(N))(u) = \sum_{i,j=1}^{n} q_{ij} \frac{\partial N}{\partial x_i}(u) \frac{\partial N}{\partial x_j}(u), \]
while the right-hand side of (3) is
\[ \left( \sum_{i,j=1}^{n} q_{ij}u_i u_j \right)^{2}. \]
Hence (3) follows.

Section 37

(a) We provide the solution to Exc. 84 with the following supplement. Let \( f: M \to N \) be a polynomial law over \( k, \epsilon \in k \) an idempotent and \( x \in M \). Then the identifications
\[ M_{R} = \epsilon M, \quad x_{R} = x \otimes \epsilon = \epsilon x \quad (R = \epsilon k \in k \text{-alg}, \ x \in M), \]
ditto for \( N \), imply \( f_R(\epsilon x) = f_R(x_R) = f(x) = \epsilon f(x) \), hence
\[ f_R(\epsilon x) = \epsilon f_R(x) \quad (x \in M). \quad (236) \]

(b) Before dealing with the problem itself, we characterize the various types of idempotents \( e \in J \) in the following way.
\[
\begin{align*}
e = 0 & \iff T(e) = S(e) = N(e) = 0, \quad (237) \\
e \text{ is elementary} & \iff T(e) = 1, \ S(e) = N(e) = 0 \iff T(e) = 1, \ S(e) = 0, \quad (238) \\
e \text{ is co-elementary} & \iff T(e) = 2, \ S(e) = 1, \ N(e) = 0 \\
& \iff T(e) = 2. \quad (239) \\
e = 1 & \iff T(e) = S(e) = 3, \ N(e) = 1 \iff N(e) = 1. \quad (240)
\end{align*}
\]
In (237), the implication from left to right is obvious. Conversely, assume \( T(e) = S(e) = N(e) = 0 \). Then (35.9.2) implies \( e = e^3 = 0 \). If \( e \) is elementary, then \( T(e) = 1, e^2 = 0 \), hence \( S(e) = T(e^2) = 0 \), while \( N(e) = 0 \) has been noted in 37.1. Conversely, assume \( T(e) = 1, S(e) = 0 \). Then (35.8.22) yields \( e^2 = e^3 - e = 0 \), and \( e \) is elementary, proving (238). In (239), we have
\[
e \text{ is co-elementary} \iff 1 - e \text{ is elementary} \iff T(1-e) = 1, \ S(1-e) = N(1-e) = 0.
\]
But \( T(1-e) = 3 - T(e) \) and \( S(1-e) = S(1) - S(e) = 3 - 2T(e) + S(e) \) by (35.8.2), while \( N(1-e) = 1 - T(e) + S(e) - N(e) \) by (35.8.6), (35.8.11). This proves (239). Finally, if \( e = 1 \) in (240), then \( T(e) = S(e) = 3 \) and \( N(e) = 1 \) by (35.8.1), (35.8.12). Conversely, if \( N(e) = 1 \), then \( e \in J \) by Cor. 35.10. Hence \( U_e \) is a bijective projection by Prop. 33.2 and Thm. 54.2 which implies \( U_e = 1 \), hence \( e^2 = e^3 = U_e 1 = 1 \).

(c) Turning, finally, to the solution of the problem, we begin by showing uniqueness, so let \( (\epsilon^{(i)})_{0 \leq i \leq 3} \) 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 (246), (247), (248), we obtain
\[
T(e) = \sum e^{(i)}T(e) = \sum T^{(i)}(e^{(i)})e = \sum T^{(i)}(e^{(i)}) = \varepsilon^{(1)} + 2\varepsilon^{(2)} + 3\varepsilon^{(3)}
\]
and, similarly,
\[
S(e) = \sum S^{(i)}(e^{(i)}) = \varepsilon^{(2)} + 3\varepsilon^{(3)}, \quad N(e) = \sum N^{(i)}(e^{(i)}) = \varepsilon^{(3)}.
\]
Solving this system of linear equations in the unknowns \( \varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)} \), we obtain (249). Now (1) follows from the completeness of the orthogonal system \( \{\varepsilon^{(i)}\} \).

(d) In order to prove existence, we define the \( \varepsilon^{(i)} \), \( 0 \leq i \leq 3 \) 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 \( 0 \leq i, j \leq 3 \), \( i \neq j \). To begin with, since \( N \) preserves powers by (35.8.21), and \( e, 1 - e \) are idempotents, so are \( \varepsilon^{(0)}\varepsilon^{(3)} \). Moreover, \( \varepsilon^{(0)}\varepsilon^{(3)} = N(e)^2N(1 - e) = N(U_6(1 - e)) = 0 \). Summing up, we have proved
\[
\varepsilon^{(0)2} = \varepsilon^{(0)}, \quad \varepsilon^{(3)2} = \varepsilon^{(3)}, \quad \varepsilon^{(0)}\varepsilon^{(3)} = 0. \tag{241}
\]
Next we apply (35.9.2) 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 (241) is an idempotent, applying \( T \) and \( S \) to the preceding equation, we end up with
\[
N(1 - e)e = 0, \quad T(e)N(1 - e) = S(e)N(1 - e) = 0. \tag{242}
\]
Combining with (2), (3), (231), we conclude
\[
\varepsilon^{(0)2} = \varepsilon^{(0)}, \quad \varepsilon^{(3)2} = \varepsilon^{(3)} \tag{243}
\]
On the other hand, replacing \( e \) by \( 1 - e \) in (242) 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
\[
T(e)N(e) = S(e)N(e) = 3N(e). \tag{244}
\]
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
\[
\varepsilon^{(1)}\varepsilon^{(3)} = \varepsilon^{(3)2} = 0. \tag{245}
\]
In view of (241), (244), (245), the \( \varepsilon^{(i)} \) will form a complete orthogonal system of idempotents in \( k \) once we have shown \( \varepsilon^{(1)}\varepsilon^{(3)} = 0 \). To this end, we first note \( T(e) = T(e, e) + T(1 - e, U_6) = T(e, e) + T(U_6(1 - e), e) = T(e, e) \) by (35.9.2) and then apply (35.8.13) to conclude \( 2S(e) = S(e, e) = T(e)^2 - T(e, e) \), hence
\[
2S(e) = T(e)^2 - T(e). \tag{246}
\]
Now we expand the last two equations of (242) by using (244) and (246). We obtain \( 0 = T(e) - T(e)^2 + T(e)S(e) - 3N(e) \), hence
\[
T(e)S(e) = 2S(e) + 3N(e), \tag{247}
\]
and \( 0 = S(e) - 2S(e) - 3N(e) + S(e)^2 - 3N(e) \), hence
\[
S(e)^2 = S(e) + 6N(e). \tag{248}
\]
Using (244), (247), (248), we can now compute
\[\epsilon^{(1)}(\epsilon^{(2)}) = T(e)S(e) - 3T(e)N(e) - 2S(e)2 + 6S(e)N(e) + 3S(e)N(e) - 9N(e)\]
\[= 2S(e) + 3N(e) - 9N(e) - 2S(e) - 12N(e) + 27N(e) - 9N(e)\]
\[= 0.\]

Thus \((\epsilon^{(1)})_{i,j,j} \in J^{(1)}\) is a complete orthogonal system of idempotents in \(k\). In particular, we have \(\epsilon = \sum\epsilon^{(i)}\), \(\epsilon^{(0)} = \epsilon^{(1)}\) if \(0 \leq i \leq 3\). From (35.8.18) we deduce \(\epsilon^{(0)} = N(1 - e) = 0\), while (35.8) implies \(N^{(3)}(\epsilon^{(3)}) = N^{(3)}(\epsilon^{(3)}) = \epsilon^{(0)}(\epsilon^{(3)}) = \epsilon^{(3)}\), hence \(\epsilon^{(3)} = 1_{\epsilon^{(3)}}\) by (24b). It remains to show that \(\epsilon^{(1)} \in J^{(1)}\) is elementary and \(\epsilon^{(2)} \in J^{(2)}\) is co-elementary, which follows from

\[T^{(1)}(\epsilon^{(1)}) = T^{(1)}(\epsilon^{(1)}) = T^{(1)}(T(e) + 2T(e)S(e) + 3T(e)N(e)\]
\[= T(e)^2 - 4S(e) - 6N(e) + 9N(e) = T(e) - 2S(e) + 3N(e) = \epsilon^{(1)} = 1_{\epsilon^{(1)}}\],
\[S^{(1)}(\epsilon^{(1)}) = S^{(1)}(\epsilon^{(1)}) = T^{(1)}(S(e) - 2S(e)^2 + 3S(e)N(e)\]
\[= 2S(e) + 3N(e) - 2S(e) - 12N(e) + 9N(e) = 0\]

and (238) in the first case, and from

\[T^{(2)}(\epsilon^{(2)}) = T^{(2)}(\epsilon^{(2)}) = \epsilon^{(2)}T(e) - T(e)S(e) - 3T(e)N(e)\]
\[= 2S(e) + 3N(e) - 9N(e) = 2(S(e) - 3N(e)) = 2\epsilon^{(2)} = 2 \cdot 1_{\epsilon^{(2)}}\],
\[S^{(2)}(\epsilon^{(2)}) = S^{(2)}(\epsilon^{(2)}) = 2(\epsilon^{(2)}S(e) - 3S(e)N(e) = S(e) + 6N(e) - 9N(e)\]
\[= S(e) - 3N(e) = \epsilon^{(2)} = 1_{\epsilon^{(2)}}\]

and (239) in the second.

Applying equation (6) of Exc. 58 and the (bilinearized) gradient identity, we expand
\(N(q) = N(q) + \sum N(u_i) + e_i T(u_i, u_j) + T(u_i \times u_j, u_j) + \sum N(u_i) + T(u_i \times u_j, u_j)\), where (35.8.18) implies \(N(u_i)^2 = N(u_i^2) = 0\). Since, therefore, the scalars \(N(q)\) and \(T(u_i \times u_j, u_j)\) 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 \(q \in J^+\) and \(T(u_i \times u_j, u_j) \in k^+\). From (35.8) we deduce \(T(u_i \times u_j, u_j) = T(u_i \times u_j, u_j)\). Hence the linear form \(x \rightarrow T(u_i \times u_j, x)\) from \(J\) to \(k\) takes \(u_i\) to an invertible element in \(k\), forcing \(u_i \in J\) to be unimodular. The adjoint identity (35.8.5) in the special form \(N(u_i) u_i = u_i^2 = 0\) therefore yields \(N(u_i) = 0\), so we have

\[N(q) = T(u_i \times u_j, u_j);\] (249)

in particular,

\[p = q^{-1} = N(q)^{-1} q^2 = T(u_i \times u_j, u_j)^{-1} \sum (u_j \times u_l)\] (250)

since the \(u_i, 1 \leq i \leq 3\), have \(u_i^2 = 0\). From (35.8.7) we deduce \(T(u_i \times u_j, u_i) = 2T(u_i^2, u_i) = 0\) and, similarly, \(T(u_i \times u_j, u_i) = 0\). Applying (35.11.3), (35.11.5) and (250), we not only conclude \(u_i^{(p)} = N(p) u_i \neq 0\) but also \(T(p, u_j) = T(p, u_j) = N(q)^{-1} T(u_i \times u_i, u_j) = N(q)^{-1} T(u_i \times u_i, u_j)\) by (249). Thus \(u_i, u_j, u_i\) are elementary idempotents in \(J^0\). That they do, in fact, form an elementary frame in that algebra will follow from Prop. 37.5 once we have shown \(u_i \times \epsilon^{(p)} u_j = T(u_i \times u_j, u_j) = q - u_i \times u_j\). In order to do so, we first linearize (35.11.3) and apply (249), (250) to obtain

\[u_i \times \epsilon^{(p)} u_j = N(q)^{-1} U_p (u_i \times u_j)\]
\[= N(q)^{-1} T(q, u_i \times u_j) q - N(q)^{-1} q^2 (u_i \times u_j)\]
\[= q - T(u_i \times u_j, u_j)^{-1} \sum (u_j \times u_l) (u_i \times u_l)\] (251)
The term for \( i = 3 \) in the sum on the very right of (251) by (35.8.10) gives 
\[ (u_1 \times u_2)^3 = 2(u_1 \times u_2)^2(u_3) + T(u_1, u_2, u_3)u_1 - u_1^2 \times u_2^2 \] = 0. On the other hand, invoking (35.8.22), (35.9.2) and (5), (6), we deduce
\[ (u_1 \times u_2) = T(u_1, u_2, u_3)u_1 - u_1^2 \times u_2^2 \]
so the second formula of (7) follows from this and the first. Subtracting the middle term of (6) from (198) we obtain (6). Invoking (35.8.10), (35.9.2) and (5), (6), we derive
\[ (a) \quad (i) \]
197. The tedious but straightforward verifications of (5) and the first equation of (6) are left to the reader. The former amounts to saying that the squaring of Mat_3(C) restricts to the squaring of \( J \). After linearizing, therefore, the symmetric matrix product \( xy + yx \) of Mat_3(C) restricts to the circle product \( x \circ y \) of (J). Hence (31.15.2), (5) and the first equation of (6) imply
\[ 2x^3 = x \circ x^2 = x(x(x)) + (xx)x = x^3 - \gamma y_2 y_1 [u_1, u_2, u_3] + (xx)x, \]
which yields the second equation of (6). In order to derive (7), we note that (6) 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 \( x^3 = Ux \), we apply (35.9.13) and obtain \( Ux \circ y + Uy \circ x = Uy(x) + (xx)y + yx^2. \) Since the associator of \( C \) is alternating, the same procedure applied to the middle term of (6) yields the expression
\[ xy^3 + x(yx) + x(y) + (xy) + y(x) + y(x)x - (xx)y - y(xx) = (y(xy) + (xy)x - [x, x, y] + [y, x, x]), \]
so the second formula of (7) follows from this and the first. Subtracting the middle term of (6) from (198), we obtain (35.8.10). Invoking (35.8.22), (35.9.2) and (5), (6), we deduce
\[ x^3 = (xx)x - T(x)x + S(x)x = x^3 - T(x)x^2 + S(x)x + \gamma y_2 y_1 [u_1, u_2, u_3] \]
\[ = (N(x)x^2 + \gamma y_2 y_1 [u_1, u_2, u_3]x)1 \]
\[ = (N(x)x^2 + \gamma y_2 y_1 [u_1, u_2, u_3]x)1 \]
hence (7), while (10) follows from (7) and \( x^3 + x^2 = x \circ x^2 = 2N(x)1 \). Finally, turning to (11), we replace \( x \) by \( x^2 \) in (10) and apply (35.8.10) to conclude
\[ x^2N(x)1 = (N(x)x^2 + \gamma y_2 y_1 [u_1, u_2, u_3]x)1 \]
On the other hand, the adjoint identity and (7) yield
\[ x^2N(x)1 = UUXYVN(x)x^2 = (N(x)x^21 + \gamma y_2 y_1 N(x))1 \]
hence (11).

198. (a) \( i \) \( \iff \) \( (ii) \). Condition (i) implies \( \Gamma \Delta^2 \Gamma^2 \Gamma = \Gamma \Delta^2 \Gamma^2 = N(\Delta)N(\Gamma)13 = N(\Delta)N(\Gamma)13 = \Delta^2 \Gamma \Gamma^2 \Gamma^2 \). Canceling yields \( \Gamma^2 = \Delta^2 \Gamma^2 \), hence (ii). Thus (i) implies (ii). Conversely, suppose (ii) holds. Then \( \Gamma^2 = \Delta^2 \Gamma^2 \), and taking norms we conclude \( N(\Gamma')N(\Delta') = N(\Delta)N(\Gamma)13 = \Delta^2 \Gamma \Gamma^2 \), hence the second relation of (i). Moreover, \( \Gamma^2 \Delta^2 = (\Gamma^2 \Delta)^2 = (\Delta^2 \Gamma)^2 \Delta^2 \Gamma = N(\Delta) \Delta^2 \Gamma = \Delta^2 \Delta^2 \Gamma = \Delta^2 \Delta^2 \Gamma = \Delta^2 \Delta^2 \Gamma \), which implies \( \Gamma^2 = \Delta^2 \Gamma^2 \), hence the first relation of (i). Thus (i) holds.
Moreover, from Exc. 90 we recall (252) gives the assertion.

Finally, let us assume that (iii) holds and $1_C \in C$ is unimodular. We wish to establish (ii), 
apply \[37.16\] to compute $\varphi(1C[i]) = \varphi(1C[j])$ and obtain $\delta_i^{-1}1_C[j] = \delta_i^{-1}1_C[i] \in C$. Hence $\varphi(1C) = \delta^{-1}C\delta^{-1}1_C$, and (ii) follows.

(b) Let $e_i, e_j, e_k \in k^*$. For (i), it suffices to put $\delta_i = \delta_j = e_i$ in (a), while (ii) follows by setting $\delta_i = e_i e_j$ in (a) since this implies $\delta_i \delta_j^{-1} = e_ie_i e_j e_j e_j^{-1} = e_i^2$. Finally, in (iii), we put $\delta_i = e_i^2$ and have $\gamma_i = \gamma_i^2$.

\[37.10\] $\varphi$ is a linear bijection which obviously preserves units. By Exc. 185 (a), therefore, it suffices to show that $\varphi$ preserves adjoints. For

$$x = \sum (\xi e_i + u_i [j]) \in J := \text{Hers}_2(C, \Gamma),$$

we note $p^{-1} = \sum \gamma_i^{-1} e_i$ and apply \[37.16\] to conclude

$$x^{(p)} = N(p) U_{p^{-1}x} = N(p) \sum \gamma_i^{-1} e_i x^2 = \gamma_i \sum \gamma_i^{-1} e_i u_i x^2 + \gamma_i \sum \gamma_i^{-1} e_i u_i x^2$$

$$= \gamma_i \sum \left( \gamma_i^{-1} (\xi e_i - \gamma_i u_i) e_i + (\gamma_i^{-1} u_i - \gamma_i u_i) \right)$$

$$= \sum \left( \gamma_i^{-1} (\xi e_i - \gamma_i u_i) e_i + (\gamma_i^{-1} u_i - \gamma_i u_i) \right),$$

hence

$$\varphi(x^{(p)}) = \sum \left( \gamma_i (\xi e_i - \gamma_i u_i) e_i + (\gamma_i^{-1} u_i - \gamma_i u_i) \right) = \varphi(x)^2,$$

as claimed.

Put \[(D, \Delta) := (C, \Gamma)^{(p, q)}, \quad \Delta = \text{diag}(\delta_1, \delta_2, \delta_3), \quad \delta_i = \delta_i^{(p, q)}\]

for $i = 1, 2, 3$. Then $C = D$ as $k$-modules, and we have

$\delta_1 = n_C(pq)^{-1} \gamma_1, \quad \delta_2 = n_C(q)^{-1} \gamma_2, \quad \delta_3 = n_C(p)^{-1} \gamma_3.$

Moreover, from Exc. 90 we recall

$$n_D(u) = n_C(pq)n_C(u), \quad \tilde{n}^{(p, q)} = n_C(pq)^{-1} \tilde{p} q \tilde{q} \tilde{p} = n_C(pq)^{-1} (pq) u (pq) (u \in C).$$
Now let
\[ x = \sum (\xi_{i} e_{ii} + u_{i} [jl]) \in \text{Her}_{3}(D, \Delta) \] (255)
and write \( u'_{i} v'_{i} \) for the adjoint of the cubic Jordan matrix algebra \( \text{Her}_{3}(D, \Delta) \). Furthermore, denote by \( \eta_{i}, \xi_{i} \in k, v_{i}, w_{i} \in C \) the quantities satisfying
\[ x'^{*} x = \sum (\eta_{i} e_{ii} + v_{i} [jl]) \in \text{Her}_{3}(D, \Delta), \quad \phi(x)^{2} = \sum (\xi_{i} e_{ii} + w_{i} [jl]) \in \text{Her}_{3}(C, \Gamma). \] (256)
Since
\[ \phi(x) = \sum (\xi_{i} e_{ii} + u_{i} [jl]) \in \text{Her}_{3}(C, \Gamma), \quad \phi(x'^{*} x) = \sum (\eta_{i} e_{ii} + v'_{i} [jl]) \in \text{Her}_{3}(C, \Gamma), \] (257)
where the \( u'_{i}, v'_{i} \) are to be determined by \( u_{i}, v_{i} \), respectively, via (15), we have to show
\[ \eta_{i} = \xi_{i}, \quad v'_{i} = w_{i} \quad (i = 1, 2, 3). \] (258)

Reading (37,104) in \( \text{Her}_{3}(D, \Delta) \) and invoking (253), (254), we compute
\[ \eta_{1} = \xi_{1} = \xi_{1} - \partial_{2} \delta_{i} \xi_{1} \cdot \delta_{i} \xi_{1} \cdot \delta_{i} \xi_{1} \cdot \delta_{i} \xi_{1} \cdot \delta_{i} \xi_{1} = \xi_{1}, \]
\[ \eta_{2} = \xi_{2} - \partial_{2} \delta_{i} \xi_{2} \cdot \delta_{i} \xi_{2} \cdot \delta_{i} \xi_{2} \cdot \delta_{i} \xi_{2} \cdot \delta_{i} \xi_{2} = \xi_{2}, \]
\[ \eta_{3} = \xi_{3} - \partial_{2} \delta_{i} \xi_{3} \cdot \delta_{i} \xi_{3} \cdot \delta_{i} \xi_{3} \cdot \delta_{i} \xi_{3} \cdot \delta_{i} \xi_{3} = \xi_{3}. \]
This proves the first set of equations in (258). In the second one, we have to show \( v'_{i} = w_{i} \) for \( i = 1, 2, 3 \). The case \( i = 1 \) is comparatively harmless since
\[ v'_{1} = (pq) v_{1} (pq) = (pq) \left( - \xi_{1} u_{1} + \partial_{2} \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \right) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) = - \xi_{1} u_{1} + \partial_{2} \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) \cdot \delta_{i} (u_{1}) = w_{1}, \]
as desired. But the remaining cases \( i = 2, 3 \) are considerably more involved. At a crucial stage, they require an application of (14,514) combined with the Moufang identities:
\[ v'_{2} = v_{2} p = (- \xi_{2} u_{2} + \partial_{2} \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) p) = - \xi_{2} u_{2} + \partial_{2} \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) p, \]
where
\[ (pq)(u_{3})/(q_{1})/(p_{1}) = ((pq)(u_{3})/(q_{1})/(p_{1})) = (p(q_{1})) \cdot (q_{1})/(p_{1}) q_{1} = p(q_{1}) \cdot (q_{1})/(p_{1}) q_{1} = p(q_{1}) \cdot (q_{1})/(p_{1}) q_{1} \]
\[ = p(u_{1} u_{1}). \]
Hence Kirmse’s identities (20,31) yield
\[ v'_{2} = - \xi_{2} u_{2} + \partial_{2} \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) p = - \xi_{2} u_{2} + \partial_{2} \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) p = - \xi_{2} u_{2} + \partial_{2} \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) \cdot \delta_{i} (u_{2}) p = w_{2}. \]
Similarly,
where
\[ (pq)((u_1p)(qu_2))((pq)) = ((pq)(u_1p))((qu_2))p)q = (p(qu_1)p)(qu_2)q = [(p(qu_1)p)(u_2)p]q = (u_1'u_2')q. \]

Thus
\[ v'_3 = -\xi_3u_3 + \gamma_3nc(q)^{-1}q(u_1'u_2')q = -\xi_3u_3 + \gamma_3nc(q)^{-1}q(u_1'u_2')q. \]

By (260) and (263), therefore, we have
\[ \text{Combining (261), (262), we have} \]

On the other hand, (259) and (37.16.5) imply
\[ \alpha\gamma \phi \text{ commute with the Peirce projections relative to the diagonal frame of } J, \]

Applying (37.16.6) and (259), we obtain
\[ \text{Thus} \]

\[ u_i'j = \phi_i'(u_j) - \phi_j'(u_i). \]

Applying (37.16.6) and (259), we obtain
\[ \gamma_i\gamma \phi \xi = U_i\gamma_i\xi = U_i\gamma_i\xi = \alpha U_i\gamma_i\xi, \]

\[ = U_i\gamma_i\xi = \xi_i. \]

Similarly, since
\[ u_i'j = \phi_i'(u_j) - \phi_j'(u_i), \]

On the other hand, (259) and (37.16.5) imply
\[ \gamma_i\gamma \phi \xi = U_i\gamma_i\xi = U_i\gamma_i\xi = \alpha U_i\gamma_i\xi, \]

Combining (260), (262), we have
\[ \phi_i = \phi_2 = \phi_3 = \phi. \]

By (260) and (263), therefore, \( \phi(u_i)[23] = \alpha u_i[23] = \alpha V_{u_i}[23] = V_{u_i}[23] = \xi u_i[23] \alpha_{e_{23}} = \xi u_i[23] \alpha_{e_{23}} = \xi u_i[23]. \]

Thus \( \phi = \xi I_C, \) and we have shown \( \alpha = \xi I, \) as claimed.

(a) We consider arbitrary elements
\[ x = \sum (\xi_i e_i + u_i[j]), \quad y = \sum (\eta_i e_i + v_i[j]) \]

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 \( (C, t_C) \) and \( I_0 \subseteq I \neq k \) is a weakly \( I \)-ample ideal in \( k, \) we must show that \( H: = H_I(I_0, I, \Gamma) \) is an outer ideal in \( J. \) For \( u \in I \) and \( v \in C \) we first note \( nc(u, v) = t_C(uv) \in I_0 \) 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 (37.10.7) and applying the preceding observation, we conclude \( T(x, y) \in I_0, \) hence \( T(x, y) = T(x, y) = T(x, y) = I_0 \subseteq IC \subseteq I. \) Thus \( T(x, y) = H \subset I. \) Moreover, since \( I \) is stabilized by \( t_C, \) and by (37.10.10), we have \( x \times y \in H, \) which after replacing \( x \) by \( x^2 \) 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., $U_{e_i}$ and $U_{e_{ij} e_k}$ for $i = 1, 2, 3$ stabilize $H$ and Prop. [37.17] yields
\[ H = \sum ((H \cap ke_i) + (H \cap C[j])]. \tag{264} \]  
We now put
\[ I := \{ u \in C \mid u[23] \in H \}, \quad I_0 := \{ \xi \in k \mid \xi e_{11} \in H \}, \tag{265} \]
which are $k$-submodules of $C, k$, respectively. For $u \in I$, we apply [37.16.3] and obtain $\gamma \gamma u[23] = \gamma u[23] \in H$, hence $u[23] \in H$. Thus $I = I_0$. From [37.16.4] we conclude that $u[jf] \in H$ belongs to $H$ if one of the "factors" does. We now claim
\[ H \cap C[j] = I[j]. \tag{266} \]
for $i = 1, 2, 3$. This follows from [265] for $i = 1$. Arguing by "cyclic induction mod 3", suppose [266] holds for some $i \in \{ 1, 2, 3 \}$ and let $u \in C$. If $u \in I$, then $\bar{u} \in I$, and [37.16.4] yields $\gamma \gamma u[23] = \gamma u[23] \in H$, hence $u[23] \in H$. Conversely, if $u[23] \in H$, the $H$ contains $u[23] = \gamma u[23]$, which implies $\bar{u} \in I$, hence $u \in I$. Thus [266] holds for $i$ instead of $i$, which completes its proof. Next we claim
\[ H \cap ke_{ij} = I_0 e_{ij} \tag{267} \]
for $i = 1, 2, 3$. Thanks to [265], the case $i = 1$ is again obvious. Next suppose [267] 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 $\xi e_{ij} \in H$, so $H$ by [37.16.6] contains $U_{e_{ij}} \xi e_{ij} = \gamma \gamma e_{ij}$, hence $\xi e_{ij} \in H$. Conversely, if $\xi e_{ij} \in H$, then $H$ contains $U_{e_{ij}} \xi e_{ij} = \gamma \gamma e_{ij}$, and we conclude $\xi \in I_0$. This completes the proof of [266]. Combining [264] with [266], [267], we obtain
\[ H = \sum (I_0 e_{ij} + I[j]), \tag{268} \]
and it remains to show that (i) $I$ is an ideal in $(C, \tau_c)$, (ii) $I_0 \subseteq I \cap k$, and (iii) $I_0$ is weakly $I$-ample.

For $u \in I, v \in J$, we combine [37.16.4] with [266] to obtain $\gamma u v[23] = v[23] \in H$, hence $uv \in I$. Thus $I$ is closed under conjugation, is an ideal in $(C, \tau_c)$, and (i) is proved. Turning to (ii), let $\xi \in I_0$. Then [37.16.2], [34.11.3], [34.27] imply $\xi [23] = \gamma [23] = \gamma \gamma e_{ij} = \gamma \gamma e_{ij} \in H$, hence $\xi \in I$. This proves (ii). Finally, turning to weak $I$-ampleness, let $u \in I$. Then $H$ contains $u[23] = \gamma \gamma u[23]$ (by [37.16.6] linearized), which implies $\tau_c(u) \subseteq I_0$ by [267] and completes the proof (iii).

(b) Let $I$ be an ideal in $(C, \tau_c)$ 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 $H := H(I_0, I, I')$ is an inner ideal of $I$ if and only if $I_0 I$ is $I$-ample. Suppose first that $H \subseteq J$ is an inner ideal and let $u \in I$. Then $H$ contains $U_{e[23]} e_{22}$, which by [37.16.9] agrees with $\gamma \gamma \gamma \gamma_{\tau_c}(u) e_{33}$, and we conclude $\gamma_{\tau_c}(u) \subseteq I_0$. Thus $I_0$ is $I$-ample. Conversely, let this be so. For $x \in H$, i.e., $\xi \in I_0$ and $u \in I$, $i = 1, 2, 3$, we obtain $T(x, y) \xi = \xi I_0, T(x, y) u I_1, I'$, hence $T(x, y) \in H$. Moreover, $x \in H$ by [37.10.4] since $I_0$ is $I$-ample. But then $x \in \tau_c(I)$ after inspecting [37.10.6], and we conclude $U_{\tau_c} \subseteq H$. Summing up, we have shown that $H \subseteq J$ is an inner ideal.

(c) For $\xi \in I \cap k$ we obtain $2 \bar{\xi} = \tau_c(\bar{\xi} \gamma) = I_0$. Thus $2(I \cap k) \subseteq I_0$. The rest is clear.

(d) Let $H$ be an outer ideal in $J$. The (a) implies $H = H(I_0, I, I')$ for some ideal $I \subseteq (C, \tau_c)$ and some weakly $I$-ample ideal $I_0$ of $k$ contained in $I \cap k$. By Exc. [23.13] there exists an ideal $a \subseteq k$ such that $I = a C$ and $I_0 \subseteq a \cap k = a$. Since $C$ is non-singular, its trace form is surjective (Lemmas [22.11]), and $\gamma_{\tau_c}(u) = 1$. For $\xi \in a$, we obtain $\xi \in I$ and therefore $\xi = \tau_c(\bar{\xi} u) \in \tau_c(I) \subseteq I_0$ by weak $I$-ampleness. This proves $I_0 = a$, hence $H = a I$ by [16].

(e) By Kaplansky’s theorem (Prop. [22.6]), $C$ is either a non-singular 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 $\text{Rad}(T) = H(\{0\}, K, I, \Gamma)$ 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 $I \neq K$, while $I_0 \subseteq I \cap F = F$ is an ideal in $F$, weak $I$-ampleness being automatic. If $I_0 = \{0\}$, then $H = \text{Rad}(T)$, and if $I_0 = F$, then $H = J$. Thus $J$ is simple but not outer simple.

203. (a) We have $U_1 = 0$ and must show $U_2 = 0$, i.e., $U_2 y = 0$ for all $y \in J$. Since cubic Jordan algebras are invariant under base change, viewing $U_2$ as a polynomial law over $k$ and applying Prop. 3.22 allow us to assume $y \in J^\circ$. Then $35.10$ for $x = y^{-1}$ and $35.8$ imply $U_2 y = N(y)[U_2 y^{-1}] = N(y)(U_2 y)^{-1} = 0$.

(b) (i) $\Rightarrow$ (ii). By (i) we have $x^2 = U_1 1 = 0$, and since $k$ is reduced, Exc. 191 shows $T(x) = S(x) = N(x) = 0$. By $35.8$, therefore, $x^2 = T(x)x + S(x)1 = 0$. Thus $T(x)y = U_2 y = 0$, 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 $N(x)x = x^2 = 0$, and applying the norm we obtain $N(x)^2 = 0$, hence $N(x) = 0$.

(c) Let $x \in J$ be an absolute zero divisor and assume first that $k$ is reduced. Then (b) implies $T(x,y) = T(x^2,y) = N(x) = 0$ for all $y \in J$, and Exc. 191 shows $x \in \text{Nil}(J)$.

Next assume that $k$ is arbitrary. Then $k : = k/\text{Nil}(k) \in k$-alg is reduced, and we have a canonical identification $J_\natural = J : = J/\text{Nil}(k)$ via $10.2$ matching $\xi$ for $\xi \in J$ with $\xi$, the image of $\xi$ under the natural map $J \to J_\natural$. Since $x$ is an absolute zero divisor in $J$, $\bar{x}$ is one in $J_\natural$, so by the special case just treated we have $T(\bar{x},y) = T(\bar{x}^2,y) = \bar{N}(\bar{x}) = 0$ for all $y \in J$, where $\bar{T} = T_1$ (resp. $\bar{N} = N_1$) is the bilinear trace (resp. norm) of $J_\natural$ over $k$. But this means that $T(x,y), T(x^2,y)$, $N(x)$ are nilpotent elements of $k$, for all $y \in J$, which means $x \in \text{Nil}(J)$.

(d) Let $F$ be a field of characteristic $2$, $K/F$ a purely inseparable field extension of exponent at most $1$, $I = \text{diag}(y_1, y_2, y_3) \in \text{GL}_3(F)$ and $J = \text{Her}_3(K, I)$. By Exc. 202 $J$ is a simple Jordan algebra over $F$. If $u_1, u_2, u_3 \in K$ are not all zero, neither is $x : = \sum u_i [j^2] \in J$. Moreover, since the bilinear norm of $K/F$ is zero, (37.10) and (37.107) show $N(x) = 0$ and $T(x,y) = 0$ for all $y \in J$, so $x$ satisfies condition (ii) of (b). On the other hand, $x^2 = \sum (\eta y_\gamma^n u_\gamma u_i + y u_i u_\gamma [j^2]) \neq 0$,

whence (b) shows that $x$ is not a zero divisor of $J$.

(e) First assume $\text{Nil}(J) = \{0\}$. We have seen in Exc. 148(c) that $\text{Nil}(k)J$ is a nil ideal in $J$. This proves $\text{Nil}(k)J = \{0\}$, and in particular $\text{Nil}(k)1 = \{0\}$. 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 $N(x) = T(x,y) = T(x^2,y) = 0$ for all $y \in J$. From Exc. 191 we therefore deduce $x \in \text{Nil}(J)$, hence $x = 0$, and $J$ has no absolute zero divisors. Conversely, let $k$ be reduced and suppose $J$ has no absolute zero divisors. For $x \in \text{Nil}(J)$ and $y \in J$, we have $T(x,y) = T(x^2,y) = N(x) = 0$. This implies $x^2 = N(x) = 0$, so $x^2$ is an absolute zero divisor by (b), forcing $x^2 = 0$ by hypothesis. But then, again by (b), $x$ is an absolute zero divisor, and we conclude $x = 0$, as desired.

We put

\[ M : = \{ \xi e_i : \xi \in k, \; J_{ij} = \{0\} \; \text{for} \; i, j = 1, 2, 3 \}, \]

\[ N : = \{ \xi e_i : \xi^2 = 0 \; \text{for} \; i = 1, 2, 3 \}. \]

By Exc. 154(c), $\text{Re}(J) \subseteq J$ is an ideal. Thus, given $x = \sum (\xi e_i + v_{ij}) \in \text{Re}(J)$, $\xi \in k$, $v_{ij} \in J_{ji}$, its Peirce components relative to $(e_1, e_2, e_3)$ by Prop. 34.8 belong to $\text{Re}(J)$ as well, so we have $\xi e_i, v_{ij} \in \text{Re}(J)$ for $1 \leq i \leq 3$. Here $34.12$ and $34.11$ imply $v_{ij} = e_j v_{ij} = U_{\xi e_i, e_j} e_j = 0$, hence $x = \sum \xi e_i$. Similarly, $\xi e_{ij} = \xi e_i o J_{ij} = \bar{U}_{\xi e_i, e_j} = \{0\}$, and we have shown $\text{Re}(J) \subseteq M$. Now suppose $x = \sum \xi e_i \in k$, satisfies $x \in M$, i.e., $\xi e_{ij} = \{0\}$ for $1 \leq i \leq 3$. Setting $u_{ij} : = u_{ij} \in M$, we have $u_{ij} \in J_{ji}$ by Prop. 37.22 and $S(u_{ij}) \in k^\times$ by Lemma 37.23 for $i = 1, 2, 3$. In particular, $\xi e_{ij} S(u_{ij}) = S(\xi e_{ij}) = 0$ and $2\xi e_{ij} S(u_{ij}) = S(2\xi e_{ij}) = 0$ imply $M \subseteq N$, and we have $U_{\xi e_i} = 0$.

Moreover, the assignment $x \mapsto x \times u_{ij}$ by Lemma 37.23 gives a linear bijection from $J_{ij}$ to $J_{ii}$. 

\[ \text{sol.ABZECU} \]
\[ 37. \text{Elementary idempotents and cubic Jordan matrix algebras} \]
\[ 451 \]
Hence \( \xi J_i = \xi_i J_i \times u_i = \{0\} \) and then \( \xi J_{ii} = \xi_i J_i \times u_i = \{0\} \). Summing up, we have shown

\[
\xi J = \sum_m (k \xi_i) e_m,
\]

and from the Peirce rules we conclude

\[
\{(\xi_i e_i) J\} = \{e_i (\xi_i J)\} = \sum_m \{e_i (k \xi_i) e_m\} = \sum_m \{e_i e_i (k \xi_i) e_m\}
\]

\[
= k \xi_i \{e_i e_i\} = 2k \xi_i e_i = \{0\}.
\]

But this means \( U_{\xi, e_i} = \{0\} \), and we have shown \( x = \sum \xi_i e_i \in \text{Rex}(J) \). This completes the proof of (19). Now let \((C, \Gamma)\) be a co-ordinate pair over \( k \) and put \((J, \mathcal{S}) := \text{Her}_3(C, \Gamma)\) as a co-ordinated cubic Jordan algebra over \( k \). By (19), and with the notation used before, the elements of \( \text{Rex}(J) \) have the form \( \sum \xi_i e_i, \xi_i \in k, \xi_i J_i = 0 \) for \( 1 \leq i \leq 3 \). But \( J_{ii} = C[j_i] \) by Prop. [37, 17] and we conclude \( \xi C = \{0\} \). In particular, \( \xi_1 C = 0 \), 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 \( C \in k\text{-alg} \) under the homomorphism \( k \to k_0 \) satisfying \( \varepsilon \mapsto 0 \). The squaring \( \alpha_0 \to \alpha_0^2 \) may be regarded as a \( k_0 \)-quadratic map \( n_C : C \to k \) with zero bilinearization, which is in fact \( k \)-quadratic since

\[
n_C((\beta_0 + \gamma \varepsilon) \alpha_0) = n_C(\beta_0 \alpha_0) = \beta_0^2 n_C(\alpha_0) = (\beta_0 + \gamma \varepsilon)^2 n_C(\alpha_0)
\]

for all \( \alpha_0, \beta_0, \gamma \in C \). 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.
for \( \xi_i \in k, u_i \in C, i = 1, 2, 3 \). Since \( \eta \) by definition preserves units, norms, traces and conjugations, we easily deduce from (37.10.3)–(37.10.5) that \( \text{Her}_3(\eta) \) is a homomorphism of cubic Jordan algebras. Given homomorphisms

\[
\begin{align*}
C & \xrightarrow{\eta} C' & \text{Her}_3(\eta) & \text{Her}_3(\eta') & \text{Her}_3(\eta'')
\end{align*}
\]

of multiplicative conic alternative algebras, (271) easily implies \( \text{Her}_3(\eta' \circ \eta) = \text{Her}_3(\eta') \circ \text{Her}_3(\eta) \).

Now let \( (\eta, \Delta) : (C, \Gamma) \to (C', \Gamma') \) with \( \Delta = \text{diag}(\delta_1, \delta_2, \delta_3) \in \text{Diag}_3(\kappa) \) be a homomorphism of co-ordinate pairs. We claim that

\[
\text{Her}_3(\eta, \Delta) = \text{Her}_3(\eta \circ \Delta) : \text{Her}_3(\eta) \circ \text{Her}_3(\Delta) : \text{Her}_3(C, \Gamma) \to \text{Her}_3(C', \Gamma')
\]

is a homomorphism of co-ordinated cubic Jordan algebras. Indeed, since \( \Gamma' = \Delta' \Gamma \); by (a), (ii), Exc. 198 shows that \( \text{Her}_3(\eta, \Delta) : \text{Her}_3(\eta) \circ \text{Her}_3(\Delta) \) is a homomorphism of the underlying cubic Jordan algebras and by (20) satisfies \( \text{Her}_3(\eta, \Delta)(e_{i0}) = e_{i0} \) for \( i = 1, 2, 3 \) and \( \text{Her}_3(\eta, \Delta)(e_{ij}[jl]) = (\delta_{i1}^{-1} \delta_{j1}^{-1} \delta_{k1}^{-1}) \delta_{ij}[jl] \) for \( i, j, k = 1, 2, 3 \).

It is straightforward to check using (20) that in this way we obtain a functor

\[
\text{Her}_3 : k\text{-copa} \to k\text{-cojuco}.
\]

(d) Writing \( T', S' \) for the trace, quadratic trace of \( J' \), we put

\[
\mathbb{S} = (e_1, e_2, e_3, u_{23}, u_{31}), \quad \omega := \omega_{\mathbb{S}, \mathbb{G}},
\]

\[
(C', \Gamma') := \text{Cop}(J', \mathbb{S}) = (C_j, \Gamma_j), \quad \Gamma = \text{diag}(\gamma_1, \gamma_2, \gamma_3),
\]

\[
\mathbb{G}' = (e_1', e_2', e_3', u_{23}', u_{31}'), \quad \omega' := \omega_{\mathbb{G'}, \mathbb{S'}},
\]

\[
(C', \Gamma') := \text{Cop}(J', \mathbb{S'}) = (C_j, \Gamma_j), \quad \Gamma' = \text{diag}(\gamma_1', \gamma_2', \gamma_3'),
\]

to deduce from (37.24.1) and (b), (ii)

\[
u' = S'(u_{23}')^{-1}S'(u_{31}')^{-1} = S'(\delta_1 \phi(u_{23}))[\delta_1 \phi(u_{31})]^{-1}
\]

\[
= \delta_1^{-1} \delta_2^{-1} \delta_3^{-1} S(u_{23})^{-1} S(u_{31})^{-1},
\]

which amounts to

\[
\omega' = \delta_1^{-1} \delta_2^{-1} \delta_3^{-1} \omega.
\]

Now let \( v, w \in C = J_{12} \). Then (274) combines with (37.24.3) to imply

\[
\phi_{12}(v) \phi_{12}(w) = \omega'(\phi(v) \times u_{23}) \times (u_{31}' \times \phi(w))
\]

\[
= \delta_1^{-1} \delta_2^{-1} \delta_3^{-1} \omega(\phi(v) \times u_{23}) \times (\phi(v) \times u_{23}) \times (\phi(u_{31}) \times \phi(w))
\]

\[
= \delta_1^{-1} \delta_2^{-1} \delta_3^{-1} \omega(\phi(v) \times u_{23}) \times (u_{31} \times w) \times \phi(v) \times u_{23} \times (u_{31} \times w)
\]

\[
= \delta_1^{-1} \delta_2^{-1} \delta_3^{-1} \phi_{12}(vw),
\]

and we conclude

\[
\phi_{12}(vw) = \delta_1 \delta_2 \phi_{12}(v) \phi_{12}(w), \quad (v, w \in C = J_{12}).
\]

In accordance with (21), we now define \( \eta := \delta_1 \delta_2 \phi_{12} : C \to C' \). Given \( v, w \in C \) and applying (275), we deduce \( \eta(vw) = \delta_1 \delta_2 \phi_{12} \phi_{12}(vw) = \delta_1 \delta_2 \delta_1 \phi_{12}(v) \delta_1 \delta_2 \phi_{12}(w) = \eta(v) \eta(w) \), so \( \eta \) is an algebra homomorphism which by (37.24.3), (37.24.4), (274) satisfies \( \eta(1_C) = \delta_1 \delta_2 \phi_{12}(u_{23} \times u_{31}) = \delta_1 \delta_2 \phi_{12}(u_{23} \times u_{31}) = 1_C \), \( n_C(\eta(v)) = -\omega S' \delta_1 \phi_{12}(v) = -\delta_1^{-1} \delta_2^{-1} \omega S' \phi(v) = -\omega S(v) = n_C(v) \).

Summing up we have thus shown that \( \eta : C \to C' \) is a homomorphism of conic algebras, so condition (a), (ii) holds for \( (\eta, \Delta) \). We now verify condition (a), (ii). An application of (37.24.7) yields

\[
\delta_1 = -\delta_1 S'(u_{31}) = -\delta_1^2 S'(\phi(u_{31})) = -\delta_1^2 S(u_{31}), \quad \delta_2 = -\delta_2 S'(u_{23}) = -\delta_2^2 S'(\phi(u_{23})) = -\delta_2^2 S(u_{23}),
\]

and...
Similarly, using (37.24.4), (37.10.9), we obtain

\[ \gamma'_i = \delta'_i^2 \gamma_i, \quad \gamma'_j = \delta'_j^2 \gamma_j, \quad \gamma'_k = \gamma_k = 1. \]  

(276) GAPRGA

In view of (21), (276), we therefore have \( \delta_i \delta_j \delta_k^{-1} \gamma_i = \delta_i \delta_j \delta_k^{-1} \gamma_j = \delta_i^2 \gamma_i = \gamma'_i \), \( \delta_i \delta_j \delta_k^{-1} \gamma_j = \delta_i^2 \gamma_j = \gamma'_j \), which comes down to \( \delta_i \delta_j \delta_k^{-1} \gamma_i = \gamma'_i \) for \( i = 1, 2, 3 \), hence to \( I' = \Delta^i \Delta^{-1} I \), and we have shown that condition (a), (ii) holds as well. Thus \( \text{Cop}(\psi; \delta_i, \delta_j) \) is indeed a morphism of co-ordinate pairs. It remains to show compatibility with compositions, so let

\[ (J, \mathfrak{S}) \xrightarrow{(\varphi, \delta_i, \delta_j)} (J', \mathfrak{S}') \xrightarrow{(\varphi', \delta'_i, \delta'_j)} (J'', \mathfrak{S}''), \]

be morphisms of co-ordinated cubic Jordan algebras. Setting \( \Delta' := \text{diag}(\delta'_i, \delta'_j, \delta'_k) \), \( \bar{\delta}'_i := \delta'_i \delta'_j \), gives

\[ \Delta' \Delta = \text{diag}(\delta'_i, \delta'_j, \delta'_k, (\delta'_i \delta'_j \delta'_k)) \]

Applying (21), we therefore conclude

\[
\text{Cop}(\psi'; \bar{\delta}'_i, \bar{\delta}'_j) \circ \text{Cop}(\psi; \delta_i, \delta_j)
= (\delta'_i \delta'_j \delta'_k \phi_{12} \circ \phi_{12}, \Delta')
= \left( \left( \delta'_i \delta'_j \delta'_k \phi_{12} \circ \phi_{12}, \text{diag}(\delta'_i \delta'_j \delta'_k, (\delta'_i \delta'_j \delta'_k)) \right) \right)
= \text{Cop}(\psi' \circ \phi; \delta'_i, \delta'_j) = \text{Cop}(\psi'; \delta'_i, \delta'_j) \circ (\phi; \delta_i, \delta_j), \]

and the assertion follows. Thus we have indeed a functor

\[ \text{Cop}: k-\text{cocojo} \rightarrow k-\text{coca} \]

(e) We employ the standard notation of (37.19) for the co-ordinated cubic Jordan algebra \((J, \mathfrak{S}):= \text{Her}_3(C, \Gamma)\) and then combine (37.24.4) with Prop (37.17) to conclude \( C' = J_{12} = C[12] \) as \( k \)-modules, giving the first assertion. Applying (37.20.1), (37.20.2), (37.24.1), (37.10.9), we obtain

\[ \omega = S(1_C[23])^{-1} S(1_C[31])^{-1} = (-\gamma'_1 \gamma_n(1_C))^{-1}(-\gamma'_3 \gamma_n(1_C))^{-1}, \]

hence

\[ \omega = \gamma'_1^{-1} \gamma'_2^{-1} \gamma'_3^{-1}. \]  

(277) CMDIAG

Now, for \( v, w \in C \), the multiplication in \( C' \) by (37.24.5), (277), (37.16.4) may be expressed as

\[ v[12] w[12] = \omega(v[12] \times 1_C[23]) \times (1_C[31] \times w[12]) = \gamma'_1^{-1} \gamma'_2^{-1} \gamma'_3^{-1} \gamma_n \bar{v}[31] \times \bar{w}[23] \]

\[ = \gamma'_1^{-1} \gamma_n \bar{v}[12] = \gamma'_1 \gamma'_3^{-1} (vw)[12], \]

which amounts to

\[ (vw)[12] = \gamma'_1 \gamma_n[12][12] \quad \text{for } v, w \in C. \]  

(278) PROPRI

Similarly, combining (37.24.5) and (37.20.1) with (37.16.4) yields \( l_C = 1_C[23] \times 1_C[31] = \gamma'_1 C[12] \), hence

\[ l_C = \gamma'_1 C[12]. \]  

(279) UNPRI

Similarly, using (37.24.4), (37.10.9), we obtain

\[ n_C(v[12]) = -\omega S(v[12]) = -\gamma'_1^{-1} \gamma'_2^{-1} \gamma'_3^{-1} (-\gamma'_2 n_C(v)), \]
which may be summarized to

\[ n^C(v[12]) = \gamma_3^2 n^C(v) \quad (v \in C). \] (280)

Invoking (278) – (280), the map \( \psi := \psi_{C, F} \) satisfies

\[ \psi(vw) = \gamma_3(vw[12]) = \gamma_3 v[12] \gamma_3 w[12] = \psi(v) \psi(w), \]

\[ \psi(1_C) = \gamma_3 1_C[12] = 1_C', \]

\[ n^C (\psi(v)) = n^C (\gamma_3 v[12]) = \gamma_3^2 \gamma_3^{-2} n^C(v) = n^C(v) \]

for all \( v, w \in C \). Hence \( \psi : C \to C' \) is an isomorphism of conic algebras. Finally, setting \( \Gamma' = \text{diag}(\gamma_1', \gamma_2', \gamma_3') \) and observing (37.25) – (37.27), we deduce \( \gamma_3' = -S(1_C[31]) = \gamma_1 n(1_C), \gamma_2' = -S(1_C[23]) = \gamma_3 n(1_C) \), which yields

\[ \gamma_1' = \gamma_2 n, \quad \gamma_2' = \gamma_3 n, \quad \gamma_3' = 1. \] (281)

Combining (281) with (24), we obtain \( \lambda_1 \lambda_2 \lambda_3^{-1} \gamma_1 = \gamma_3 \gamma_1 = \gamma_1', \lambda_1 \lambda_2 \lambda_3^{-1} \gamma_2 = \gamma_3 \gamma_2 = \gamma_2', \lambda_1 \lambda_2 \lambda_3^{-1} \gamma_3 = \gamma_3 \gamma_3 = \gamma_3' \), which may be unified to \( \lambda_1 \lambda_2 \lambda_3^{-1} \gamma = \gamma' \). Thus, setting \( \Lambda := \Lambda_{C, F} \), we see \( \Gamma' = \Lambda^2 \Lambda^{-1} \Gamma \). Hence \( \Psi_{C, F} \) is an isomorphism of co-ordinate pairs, as claimed.

(f) This is clear since \( \Phi = \Phi_{J, \Theta} \) as defined in Thm. 37.25 matches exactly the diagonal co-ordinate system of \( \text{Hers}(C, \Gamma) \) with the co-ordinate system \( \Theta \) of \( J \).

(g) It suffices to show

(i) that the \( \Phi_{J, \Theta} \) for all co-ordinated cubic Jordan algebras \( (J, \Theta) \) over \( k \) determine an isomorphism

\[ \text{Her}_3 \circ \text{Cop} \xrightarrow{\sim} \text{Id}_{k \text{-cocoa}} \]

of functors from \( k \text{-cocoa} \) to itself and, similarly,

(ii) that the \( \Psi_{C, F} \) for all co-ordinate pairs \( (C, \Gamma) \) over \( k \) determine an isomorphism

\[ \text{Id}_{k \text{-coca}} \xrightarrow{\sim} \text{Cop} \circ \text{Her}_3 \]

of functors from \( k \text{-coca} \) to itself.

We begin with (i). Given a co-ordinated cubic norm structure \( (J, \Theta) \) over \( k \), Theorem 37.25 shows that

\[ \Phi_{J, \Theta} : \big( \text{Her}_3 \circ \text{Cop} \big) (J, \Theta) \to (J, \Theta) \]

is an isomorphism in \( k \text{-cocoa} \). Thus, by [47] Def. 1.3, p. 23, the proof will be complete once we have shown that any homomorphism \( (\phi; \delta_1, \delta_2) : (J, \Theta) \to (J', \Theta') \) of co-ordinated cubic Jordan algebras gives rise to a commutative diagram

\[ \begin{array}{ccc}
\text{(Her}_3 \circ \text{Cop})(J, \Theta) & \xrightarrow{\Phi_{J, \Theta}} & (J, \Theta) \\
\text{(Her}_3 \circ \text{Cop})(\phi; \delta_1, \delta_2) & \downarrow & (\phi; \delta_1, \delta_2) \\
\text{(Her}_3 \circ \text{Cop})(J', \Theta') & \xrightarrow{\Phi_{J', \Theta'}} & (J', \Theta').
\end{array} \] (282)

In order to establish the commutativity of (282), we write \( S \) (resp. \( S' \)) for the quadratic trace of \( J \) (resp. \( J' \)); moreover, we put \( \Theta = (e_1, e_2, \ldots, u_3), \Theta' = (e_1', e_2', \ldots, u_3') \).

Applying (26), we first obtain \( (\phi; \delta_1, \delta_2) \circ \Phi_{J, \Theta} = (\phi; \delta_1, \delta_2) \circ (\Phi_{J, \Theta}; 1, 1) \), hence
Summing up, this completes the proof of (285), and we have shown that the diagram (282) com-

On the other hand, setting

we deduce from (272), (284) that

so in view of (283), it suffices to show

In order to do so, we write \((C, \Gamma) := \text{Cop}(J, \mathcal{E})\) (resp. \((C', \Gamma') = \text{Cop}(J', \mathcal{E}')\)). Combining (37.25) with condition (a), (i) of Exc. 198 we obtain \(\phi \circ \phi_{J, \mathcal{E}}(e_i) = \psi \circ \phi_{J, \mathcal{E}}(e_i) = \phi_{J', \mathcal{E}'} \circ \text{Her}_3(\eta, \Delta)\) for \(i = 1, 2, 3\), so it remains to show that both sides of (285) agree on \(v_i\), for all \(v_i \in C = J_2\), \(i = 1, 2, 3\). Since \(\eta\) as defined in (284), being an isomorphism of conic algebras, preserves conjugations, so does every scalar multiple of it, in particular \(\psi\). With this in mind, we apply (37.25), (284) and obtain

Similarly,

And, finally,

Summing up, this completes the proof of (285), and we have shown that the diagram (282) com-

It remains to establish (ii). To this end, we let \((\eta, \Delta) : (C, \Gamma) \to (C', \Gamma')\) be a morphism of co-ordinate triples and must show that the diagram
From \( (\mathcal{H}, \Gamma) \xrightarrow{\triangle} (\text{Cop} \circ \text{Her})_3(\mathcal{H}, \Gamma) \),

\[
\begin{array}{c}
\eta \circ \hat{\eta} = (\mathcal{H}, \Gamma) \\
\eta \circ \hat{\eta} = (\mathcal{H}, \Gamma) \\
\eta \circ \hat{\eta} = (\mathcal{H}, \Gamma)
\end{array}
\]

We abbreviate \( \Psi_{\mathcal{C}, \mathcal{F}} = (\psi, \Lambda), \Psi_{\mathcal{C}, \mathcal{F}} = (\psi', \Lambda') \) and deduce from (24) that

\[
\Lambda = \text{diag}(\lambda_1, \lambda_2, \lambda_3), \quad \Lambda' = \text{diag}(\lambda_1', \lambda_2', \lambda_3'), \quad \lambda_1 = \lambda_2 = 1, \quad \lambda_3 = \gamma_1.
\]

Hence \( \Psi_{\mathcal{C}, \mathcal{F}} \circ (\eta, \Delta) = (\psi', \Lambda') \circ (\eta, \Delta), \) and (269) implies

\[
\Psi_{\mathcal{C}, \mathcal{F}} \circ (\eta, \Delta) = (\psi' \circ \eta, \Lambda' \Delta),
\]

where (27) yields

\[
(\psi' \circ \eta)(v) = \gamma_1' \eta(v)[12], \quad (v \in \mathcal{C}).
\]

On the other hand, writing \( \Delta = \text{diag}(\delta_1, \delta_2, \delta_3) \) and invoking (291), we obtain

\[
\Lambda' \Delta = \text{diag}(\delta_1, \delta_2, \gamma_1' \delta_3).
\]

Next we use (272) to compute

\[
\text{Cop} \left( (\text{Her}_3(\eta, \Delta)) \right) = \text{Cop} \left( (\text{Her}_3(\eta, \Delta); \delta_1, \delta_2) \right),
\]

where

\[
\text{Cop} \left( (\text{Her}_3(\eta, \Delta)) \right) = (\hat{\eta}, \hat{\Delta}), \quad \hat{\eta} := \delta_1 \delta_2 \text{Her}_3(\eta, \Delta)_{12}, \quad \hat{\Delta} := \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2).
\]

From \( (\hat{\eta}, \hat{\Delta}) \circ \Psi_{\mathcal{C}, \mathcal{F}} = (\hat{\eta}, \hat{\Delta}) \circ (\psi, \Lambda) \) we therefore deduce

\[
(\text{Cop} \circ \text{Her}_3)(\eta, \Delta) \circ \Psi_{\mathcal{C}, \mathcal{F}} = (\hat{\eta} \circ \psi, \hat{\Delta} \Lambda).
\]

Given \( v \in \mathcal{C} \), we observe \( \Gamma' = \Lambda'^{-1} \Gamma \) (since \( (\eta, \Delta) \) is a morphism in \( k \)-\text{copa}), which yields

\[
(\hat{\eta} \circ \psi)(v) = \hat{\eta}(\psi_{\mathcal{C}, \mathcal{F}}(v)) = \gamma_1' \eta(v)[12] = \delta_1 \delta_2 \gamma_1 \text{Her}_3(\eta, \Delta)_{12}(v)[12]
\]

Thus \( \hat{\eta} \circ \psi = \psi' \circ \eta \). Moreover, by (295), (290), (291)

\[
\hat{\Delta} \Lambda = \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2) \text{diag}(1, 1, \gamma_1) = \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2 \gamma_1)
\]

Thus \( \hat{\eta} \circ \psi = \psi' \circ \eta \). Moreover, by (295), (290), (291)

\[
\hat{\Delta} \Lambda = \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2) \text{diag}(1, 1, \gamma_1') = \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2 \gamma_1') = \text{diag}(1, 1, \gamma_1') \text{diag}(\delta_1, \delta_2, \delta_1 \delta_2) = \Lambda' \Delta.
\]
Comparing now (292) with (296), we see that the diagram (286) commutes, which completes the proof of (ii).
References

1957. MR 0082628 (18,583c)
20. J.H. Conway and D.A. Smith, On quaternions and octonions: their geometry, arithmetic, and
(8,370b)
22. M. Demazure and P. Gabriel, Groupes algébriques. Tome I: Géométrie algébrique,
généralités, groupes commutatifs, Masson & Cie, Éditeur, Paris, 1970, Avec un appendice
Corps de classes local par Michiel Hazewinkel. MR 0302656 (46 #1800)
113–125.
Univ. Strasbourg (N.S.) no. 1 (1945), Hermann et Cie., Paris, 1948. MR 0024439 (9,494c)
27. R. Elman, N. Karpenko, and A. Merkurjev, The algebraic and geometric theory of quadratic
28. J.R. Faulkner, Octonion planes defined by quadratic Jordan algebras
1967), 506–514. MR 0212063
31. S. Garibaldi and H.P. Petersson, Wild Pfister forms over Henselian fields, K-theory, and conic
57 (2014), no. 2, 303–309. MR 3194176
34. A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes
36. R. Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977, Graduate Texts in
Mathematics, No. 52. MR 0463157 (57 #3116)
37. R. Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977, Graduate Texts in
Mathematics, No. 52. MR 0463157 (57 #3116)
39. N. Jacobson, Composition algebras and their automorphisms, Rend. Circ. Mat. Palermo (2)
7 (1958), 55–80. MR 0101253 (21 #66)
40. N. Jacobson, Lie algebras, Interscience Tracts in Pure and Applied Mathematics, No. 10, Inter-
41. N. Jacobson, Structure and representations of Jordan algebras, American Mathematical Society
Colloquium Publications, Vol. XXXIX, American Mathematical Society, Providence, R.I.,
1968. MR 0251099
References

44. , Lectures on quadratic Jordan algebras, Tata Institute of Fundamental Research, Bombay, 1969, Tata Institute of Fundamental Research Lectures on Mathematics, No. 45. MR 0325715
49. and , Jordan homomorphisms of rings, Trans. Amer. Math. Soc. 35 (1934), no. 1, 29–64. MR 1503141
51. , On an algebraic generalization of the quantum mechanical formalism, Ann. of Math. (2) 35 (1934), no. 1, 29–64. MR 1503141
53. , Projective modules, Ann. of Math (2) 68 (1958), 372–377. MR 0100017 (20 #6453)
57. , Quadratische Formen, Springer-Verlag, Berlin, 2002, Revised and edited in collaboration with Rudolf Scharlau. MR 2788987
References

90. O.T. O'Meara, Introduction to quadratic forms, Die Grundlehren der mathematischen Wissenschaften, Bd. 117, Springer-Verlag, New York, 1963. MR 0150179 (27 #2485)
93. H.P. Petersson, Composition algebras over commutative rings, In preparation.
102. Classification of algebras arising from the Tits process, J. Algebra 98 (1986), no. 1, 244–279. MR 87h:17038b


130. ______, *Alternative rings and related questions I: existence of the radical*, Ann. of Math. (2) 42 (1941), 676–686. MR 0005098 (3,100c)