22 November 2005

Generically algebraic Jordan algebras over commutative rings

Ottmar Loos
Institut für Mathematik
University of Innsbruck, A-6020 Innsbruck, Austria

Abstract. The theory of the generic minimum polynomial, norm and trace is developed for quadratic Jordan algebras which are finitely generated and projective modules over an arbitrary commutative base ring, using scheme-theoretic methods. We recover, with new proofs, most of the classical theory over fields, and also obtain a number of results which are new even in the classical setting.

Introduction

The theory of the generic minimum polynomial, norm and trace for linear and quadratic Jordan algebras of finite dimension over a field is well-known [**14**, **16**, **26**]. In this paper, we extend the theory to quadratic Jordan algebras which are finitely generated and projective modules over an arbitrary commutative base ring. With an appropriate definition of generically algebraic algebra, we are able to recover most of the results of the classical theory. Our methods involve scheme theory in an essential way. They yield new proofs of classical results as well as new ones even in the classical setting. The theory developed here applies to associative or alternative algebras by considering the associated Jordan algebra with quadratic operators $U_x y = xyx$. The results seem to be new even in this case.

Let k be an arbitrary commutative ring with unity, let J be a quadratic Jordan algebra which is finitely generated and projective as a k-module, and denote by A the algebra of polynomial laws on J. For a polynomial $f(\mathbf{t})$ in the indeterminate $\mathbf{t}$ with coefficients in A and an element x in a base ring extension $J \otimes_k R$ of J, we denote by $f(\mathbf{t}; x) \in R[\mathbf{t}]$ the polynomial obtained by evaluating the coefficients of f at x. We say J is *generically algebraic* (see 2.2) if there exists a locally monic polynomial $m(\mathbf{t}) \in A[\mathbf{t}]$ such that

(i) for all x in all base ring extensions, substitution of x for $\mathbf{t}$ in $m(\mathbf{t}; x)$ and $\mathbf{t}m(\mathbf{t}; x)$ yields zero,

(ii) for every prime ideal $\mathfrak{p}$ of k, the base change of $m(\mathbf{t})$ from k to the quotient field $\boldsymbol{\kappa}(\mathfrak{p})$ of $k/\mathfrak{p}$ is the classical generic minimum polynomial of $J \otimes_k \boldsymbol{\kappa}(\mathfrak{p})$.

These conditions are natural for the following reasons: (i) just says that every x satisfies its own generic minimum polynomial $m(\mathbf{t}; x)$. (Note that the condition $m(x; x) = 0$ is sufficient in (i) provided $J = B^+$ is the Jordan algebra associated to an associative or alternative algebra B). Condition (ii) is forced upon us if we wish the definition to be invariant under base change and consistent with that over fields. A polynomial $m(\mathbf{t})$ satisfying (i) and (ii) is unique (Prop. 2.7); it is called the *generic minimum polynomial of J*.

The question then arises which finitely generated and projective Jordan algebras are generically algebraic in this sense. It turns out that there always exist polynomials satisfying (i), for instance, $\det(\mathbf{t}^2 \mathrm{Id} - U_x)$. The well-known constructions of Jordan algebras from quadratic forms with base point and from cubic norm structures yield examples of polynomials of degree 2 and 3 satisfying (i) [**22**, **30**, **20**]. Condition (ii) is much more restrictive, and there are many examples of finitely generated and projective Jordan algebras which are not generically algebraic. On the other hand, the obvious analogues over rings of the simple finite-dimensional algebras over algebraically closed fields are all generically algebraic in this sense.

We now give a more detailed account of the contents. After a preliminary section collecting facts on locally monic polynomials, schemes and pure submodules, section 1 deals with *algebraic elements*. Let J be a quadratic Jordan algebra which is finitely generated and projective as a k-module. Ignoring for the moment the difficulties arising from the lack of power-associativity of quadratic Jordan algebras, we define an element $a \in J$ to be algebraic if the subalgebra $k[a]$ generated by a is a direct summand of J. (The actual definition in 1.4 is more involved and makes sense even without assumptions on the k-module structure of J). This is a much more stringent condition than that a be integral, i.e., that it satisfy some monic polynomial. Algebraic elements have well-defined minimum polynomials which behave well under base change. The functor of algebraic elements is a finitely presented quasi-affine k-scheme (Prop. 1.14).

In section 2, we develop the general theory of generically algebraic algebras, establish results on ascent and descent, and prove the uniqueness and the basic properties of the generic minimum polynomial (Prop. 2.7, Th. 2.11). An important tool is the fact that the *primitive elements*, i.e., the algebraic elements of highest degree, form an open dense subscheme (Lemma 2.6).

In Theorem 3.1 of section 3 we show that generically algebraic Jordan algebras are stable under isotopy and compute the generic minimum polynomial of an isotope. For algebras over fields, this is due to N. Jacobson [**12**] in the linear case, and to K. McCrimmon [**26**] in the quadratic case. For central separable algebras over rings containing $\frac{1}{2}$, it was proved by R. Bix [**2**] by a case-by-case verification. McCrimmon's proof made use of the composition law $N(U_x y) = N(x)^2 N(y)$ for the generic norm. Our proof is actually a simplification of McCrimmon's and yields the composition law as a corollary. Let us point out here that the classical proof of the composition law relies on the factoriality of the polynomial ring in several variables over a field and therefore does not carry over to base rings. We then prove the symmetry property of the coefficients of the generic minimum polynomial of an isotope and the fact that these coefficients are polynomial laws on $J \times J$ (Theorem 3.5). We finally derive in 3.11 explicit formulas for these coefficients which are new even for algebras over fields.

It is a curious phenomenon of quadratic Jordan algebras that they may contain elements which are not power-associative in the sense that the subalgebra generated by such an element is not special. As mentioned above, this brings complications in the definition of algebraic element. In section 4, we study this phenomenon in more detail and show in particular that algebraic elements of degree $\leqslant 3$ are automatically power-associative (Prop. 4.5). As a consequence, generically algebraic Jordan algebras of degree $\leqslant 3$ over fields are strictly power-associative (Cor. 4.4). This gives a partial answer to a question raised by K. McCrimmon in [**23**].

Finally, in section 5 we prove that a module isomorphism between generically algebraic Jordan algebras of degree 3 which preserves squares, traces and unit elements, is already an algebra isomorphism (Th. 5.1). As a consequence, the automorphism group of the exceptional Jordan algebra in characteristic 2 is isomorphic, by restriction, to the automorphism group of the 2-Lie algebra of its space of trace zero elements, and a similar result holds for derivations (Cor. 5.4).

Acknowledgements. I wish to thank H. P. Petersson who has read an earlier version of this paper and offered many valuable comments.

This paper was prepared in part while the author was a guest of the Department of Algebra, Geometry and Topology of the University of Málaga, and the Department of Mathematics of the University of Oviedo. The hospitality of these institutions is gratefully acknowledged.

0. Preliminaries

0.1. Notations and conventions. Throughout, k denotes an arbitrary commutative ring. $\mathrm{Spec}(k)$ is the set of prime ideals of k, with the Zariski topology, and for a ring homomorphism $\varrho\colon k \to k'$, $\mathrm{Spec}(\varrho)\colon \mathrm{Spec}(k') \to \mathrm{Spec}(k)$ is the continuous map $\mathfrak{q} \mapsto \varrho^{-1}(\mathfrak{q})$. The quotient field of $k/\mathfrak{p}$ ($\mathfrak{p} \in \mathrm{Spec}(k)$) is written $\boldsymbol{\kappa}(\mathfrak{p})$. We denote by k-**alg** the category of commutative associative k-algebras. Unsubscripted tensor products are understood over k. For $R \in k$-**alg** and X a k-module, we often abbreviate $X_R = X \otimes R$; for $x \in X$ we put $x_R := x \otimes 1_R \in X_R$, and for a homomorphism $h\colon X \to Y$ of k-modules, we denote by $h_R\colon X_R \to Y_R$ the R-linear extension of h; i.e., $h_R(x \otimes r) = h(x) \otimes r$, for all $x \in X$, $r \in R$. Thus we have $h_R(x_R) = h(x)_R$.

By a Jordan algebra J over k we always mean a unital quadratic Jordan algebra, unless otherwise specified. The unit element is written 1_J or simply 1, the set of invertible elements is $J^\times$. For an alternative (or associative) algebra B, the associated Jordan algebra with quadratic operators $U_x y = xyx$ is denoted B^+.

0.2. Vanishing sets. Let M be a k-module and $x \in M$. With x we associate the ideals

$$\mathfrak{a} := \mathrm{Ann}(x) = \{\lambda \in k : \lambda x = 0\} \quad \text{and} \quad \mathfrak{b} := \langle x, M^* \rangle = \{\langle x, \beta\rangle : \beta \in M^*\}$$

of k, where M^* is the dual module and $\langle\ ,\ \rangle\colon M \times M^* \to k$ is the canonical pairing. Clearly, $\mathfrak{a} \cdot \mathfrak{b} = 0$.

Now let M be finitely generated and projective. In geometric terms, M may then be considered as a vector bundle over the affine scheme $S = \mathrm{Spec}(k)$ and x as a section of this bundle. To carry this a bit further, let $x(\mathfrak{p}) := x \otimes 1_{\boldsymbol{\kappa}(\mathfrak{p})} \in M(\mathfrak{p}) := M \otimes \boldsymbol{\kappa}(\mathfrak{p})$, for all $\mathfrak{p} \in S$. Thus $M(\mathfrak{p})$ is the fibre of M and $x(\mathfrak{p})$ is the value of the section x at the point $\mathfrak{p}$. We claim that

$$x(\mathfrak{p}) = 0 \quad \iff \quad \mathfrak{b} \subset \mathfrak{p}. \tag{1}$$

Indeed, $M(\mathfrak{p})$ being a vector space over $\boldsymbol{\kappa}(\mathfrak{p})$, we have $x(\mathfrak{p}) = 0$ if and only if $\langle x(\mathfrak{p}), \alpha \rangle = 0$, for all $\alpha \in \big(M(\mathfrak{p})\big)^*$. Since M is finitely generated and projective, the canonical homomorphism $M^* \otimes R \to (M \otimes R)^*$ is an isomorphism, for all $R \in k$-**alg** [**4**, II, §4.2, Prop. 2(ii)]. Thus

$$\begin{aligned} x(\mathfrak{p}) = 0 \quad &\iff \quad \langle x, \beta\rangle \otimes 1_{\boldsymbol{\kappa}(\mathfrak{p})} = 0 \quad \text{for all } \beta \in M^* \\ &\iff \quad \langle x, \beta \rangle \in \mathfrak{p} \quad \text{for all } \beta \in M^* \\ &\iff \quad \mathfrak{b} \subset \mathfrak{p}. \end{aligned}$$

We may express (1) by

$$x^{-1}(0) = V(\mathfrak{b}), \tag{2}$$

where $V(\mathfrak{b}) = \{\mathfrak{p} \in S : \mathfrak{p} \supset \mathfrak{b}\}$ is the vanishing set of $\mathfrak{b}$, cf. [**3**, II, §4.3].

0.3. Unimodular elements. An element x of a k-module M is said to be *unimodular* if $k \cdot x$ is a free k-module of rank 1 and a direct summand of M, equivalently, if there exists an element $\beta \in M^*$ such that $\langle x, \beta \rangle = 1$, i.e., $\mathfrak{b} = k$. Thus 0.2.1 yields, in case M is finitely generated and projective,

$$x \quad \text{is unimodular} \quad \iff \quad x(\mathfrak{p}) \neq 0 \quad \text{for all } \mathfrak{p} \in S. \tag{1}$$

Let J be a Jordan algebra over k, finitely generated and projective as a k-module, with unit element 1_J. We claim that

$$J \text{ is a faithful } k\text{-module} \quad \iff \quad 1_J \text{ is unimodular.} \tag{2}$$

Indeed, $J = 0$ if and only if $1_J = 0$, and the unit element is compatible with base change: $1_{J_R} = (1_J)_R$, for all $R \in k$-**alg**. By general facts on finitely generated and projective modules, J is faithful if and only if $J(\mathfrak{p}) \neq 0$, for all $\mathfrak{p} \in S$. Now (2) follows from (1).

0.4. Lemma. *Let M be a finitely generated and projective k-module and $x \in M$. Then the following conditions are equivalent:*

(i) $x^{-1}(0)$ *is open in* $S = \mathrm{Spec}(k)$,
(ii) *there exists an idempotent* $\varepsilon \in k$ *such that* $\mathfrak{b} = k \cdot \varepsilon$,
(iii) $k \cdot x$ *is a direct summand of* M.

If these conditions hold, ε *is uniquely determined and is called the* support idempotent *of* x. *The annihilator of* x *is then* $\mathfrak{a} = k \cdot (1 - \varepsilon)$.

Proof. (i) $\Longrightarrow$ (ii) follows from well-known facts about the correspondence between open and closed subsets of S and idempotents of k [**3**, II, §4.3, Prop. 15].

(ii) $\Longrightarrow$ (iii): Choose $\beta \in M^*$ with $\langle x, \beta \rangle = \varepsilon$. Then we have $x = \varepsilon x$: Indeed, $\langle (1-\varepsilon)x, M^* \rangle = (1-\varepsilon)\mathfrak{b} = (1-\varepsilon)\varepsilon \cdot k = 0$. Since the canonical map $M \to M^{**}$ is injective, it follows that $(1-\varepsilon)x = 0$. Now one checks easily that $\pi(y) := \langle y, \beta \rangle x$ defines a projection of M with image $k \cdot x$.

(iii) $\Longrightarrow$ (i): Since M is finitely generated and projective so is $k \cdot x$. Hence the rank function of $k \cdot x$ is continuous on S, which implies that $x^{-1}(0) = \{\mathfrak{p} \in S : \mathrm{rk}_{\mathfrak{p}}(k \cdot x) = 0\}$ is open.

Uniqueness of ε follows from the fact that it is the unit element of $\mathfrak{b}$. Finally, $0 = \mathfrak{a}\mathfrak{b} = \varepsilon\mathfrak{a}$ implies $\mathfrak{a} \subset k \cdot (1-\varepsilon)$, and the reverse inclusion follows from $(1-\varepsilon)x = 0$.

0.5. Lemma. *Let J be a not necessarily unital Jordan algebra over k which is finitely generated and projective as a k-module, and let $e \in J$ be an idempotent of J. Then e satisfies the equivalent conditions of* 0.4.

Proof. Consider the Peirce decomposition $J = J_2(e) \oplus J_1(e) \oplus J_0(e)$ of J with respect to e. Then the $J_i(e)$, being direct summands of J, are finitely generated and projective. Moreover, Peirce decomposition is compatible with base change: For all $R \in k$-**alg**, we have $(J_R)_i(e) = J_i(e) \otimes R$. Finally, $e = 0$ if and only if $J_2(e) = 0$. Hence

$$e(\mathfrak{p}) = 0 \iff J_2(e) \otimes \boldsymbol{\kappa}(\mathfrak{p}) = 0 \iff \mathrm{rk}_{\mathfrak{p}}\, J_2(e) = 0.$$

Since the rank function of $J_2(e)$ is continuous on S, it follows that $e^{-1}(0)$ is open.

0.6. Lemma. *Let X be a k-module, let $x_1, \ldots, x_n \in X$ and let N be the k-span of $x_1, \ldots, x_n$. Then the following conditions are equivalent:*

(i) N *is free with basis* $x_1, \ldots, x_n$ *and a direct summand of* X,
(ii) $y := x_1 \wedge \cdots \wedge x_n$ *is unimodular in* $\bigwedge^n X$.

If X is finitely generated and projective these conditions are equivalent to

(iii) $x_1(\mathfrak{p}), \ldots, x_n(\mathfrak{p})$ *are linearly independent over* $\boldsymbol{\kappa}(\mathfrak{p})$, *for all* $\mathfrak{p} \in \mathrm{Spec}(k)$.

If these conditions hold, we have

$$x \in N \quad \iff \quad y \wedge x = 0, \tag{1}$$

for all $x \in X$.

Proof. (i) $\Longrightarrow$ (ii): Let $X = N \oplus P$ and define linear forms $\alpha_i \in X^*$ by $\langle x_i, \alpha_j \rangle = \delta_{ij}$ and $\langle \alpha_i, P \rangle = 0$. Let $\beta \in \big(\bigwedge^n X\big)^*$ be the image of $\alpha_1 \wedge \cdots \wedge \alpha_n$ under the canonical homomorphism $\bigwedge^n(X^*) \to \big(\bigwedge^n X\big)^*$. Then $\langle \beta, y \rangle = \det(\langle \alpha_i, x_j \rangle) = 1$.

(ii) $\Longrightarrow$ (i): Define $\alpha_i \in X^*$ by

$$\langle x, \alpha_i \rangle := \langle x_1 \wedge \cdots \wedge x_{i-1} \wedge x \wedge x_{i+1} \wedge \cdots \wedge x_n, \beta \rangle.$$

Then $\langle x_i, \alpha_j \rangle = \delta_{ij}$. This clearly implies that N is free with basis $x_1, \ldots, x_n$. Furthermore, $X = N \oplus P$ where $P = \bigcap_{i=1}^n \mathrm{Ker}(\alpha_i)$, so N is a direct summand of X.

(ii) $\iff$ (iii): Since exterior powers commute with base change, we have $y(\mathfrak{p}) = x_1(\mathfrak{p}) \wedge \cdots \wedge x_n(\mathfrak{p})$, so the assertion follows from 0.3.1. Finally, (1) follows from [**4**, III, §7.9, Prop. 13].

0.7. k-functors and schemes. Following [**6**], we will consider schemes over k as special functors from k-**alg** to the category of sets, also called k-functors. Morphisms between functors are natural transformations. To fix notations, we give some examples.

(a) Let $A \in k$-**alg**. The affine scheme defined by A is the k-functor $\mathbf{Spec}(A)$ given by

$$\mathbf{Spec}(A)(R) = \mathrm{Hom}_{k\text{-}\mathbf{alg}}(A, R).$$

Note the following special cases: For $A = \{0\}$ we obtain the "empty functor", mapping R to $\emptyset$ if $R \neq \{0\}$ and to a one-point set (consisting of the unique homomorphism $\{0\} \to \{0\}$) if $R = \{0\}$.

For $A = k$, $\mathbf{Spec}(k)$ is the "one-point" functor because $\mathrm{Hom}_{k\text{-}\mathbf{alg}}(k, R)$ consists of the unique homomorphism $k \to R$ making R a k-algebra.

For $A = k^I$ where I is a finite set, we obtain a functor denoted by I_k and called the *constant k-functor defined by I*, although "locally constant" would be more apt. It can be described as follows: For each $R \in k$-**alg**, $I_k(R)$ is the set of complete families of orthogonal idempotents $(\varepsilon_i)_{i \in I}$ in R. By the well-known relation between idempotents and open and closed subsets of $\mathrm{Spec}(R)$, $I_k(R)$ can also be considered as the set of continuous (= locally constant) maps $\mathrm{Spec}(R) \to I$, where I has the discrete topology.

(b) A k-scheme $\mathbf{X}$ is a local k-functor for which there exist open affine subschemes $\mathbf{U}_i$ covering $\mathbf{X}$ [**6**, I, §1, 3.11]. Refer to [**6**, I, §1, 3.6, §2, 4.1] for the notion of an open (closed) subfunctor. "Covering" means that $\mathbf{X}(K) = \bigcup \mathbf{U}_i(K)$ for all *fields* $K \in k$-**alg**. The union need not be disjoint, and when R is not a field, $\mathbf{X}(R)$ may be strictly bigger than the union of the $\mathbf{U}_i(R)$.

(c) The example k^I of (a) generalizes in the obvious way to the case of an arbitrary set I, where now an element of $I_k(R)$ is a family (ε_i) as before with only finitely many $\varepsilon_i \neq 0$. This corresponds to the fact that $\mathrm{Spec}(R)$ is quasicompact, and hence a continuous map to the discrete space I can take only finitely many values. If I is infinite, I_k is still a scheme but no longer affine.

(d) Let $\mathbf{X}_i$ ($i \in I$) be a family of k-functors with the property that $\mathbf{X}_i(\{0\})$ is a one-point set. We define $\coprod_{i \in I} \mathbf{X}_i$ to be the functor $\mathbf{X}$ given as follows: The elements of $\mathbf{X}(R)$ are the pairs (ε, x) where $\varepsilon = (\varepsilon_i)_{i \in I} \in I_k(R)$, and $x = (x_i)_{i \in I} \in \prod_{i \in I} \mathbf{X}_i(\varepsilon_i R)$. If the $\mathbf{X}_i$ are local, this means that $\mathbf{X}$ is the local functor associated to the functor $R \mapsto \dot{\bigcup}_{i \in I} \mathbf{X}_i(R)$. There is a unique morphism $\mathbf{deg}\colon \coprod_{i \in I} \mathbf{X}_i \to I_k$ such that $\mathbf{X}_i = \mathbf{deg}^{-1}(\{i\}_k)$, given by $(\varepsilon, x) \mapsto \varepsilon$.

0.8. Locally monic polynomials. Let $\mathbf{t}$ be an indeterminate. A polynomial $f(\mathbf{t}) \in k[\mathbf{t}]$ is called *locally monic* if it satisfies the following equivalent conditions:

(i) For all $\mathfrak{p} \in S = \mathrm{Spec}(k)$, the localizations $f(\mathbf{t})_\mathfrak{p} \in k_\mathfrak{p}[\mathbf{t}]$ are monic,

(ii) there exists a finite subset D of $\mathbb{N}$ and a family $(\varepsilon_d)_{d \in D}$ of orthogonal idempotents of k with sum 1 such that $f(\mathbf{t}) = \sum_{d \in D} \varepsilon_d f_d(\mathbf{t})$ where $f_d(\mathbf{t})$ is monic of degree d.

If these conditions hold, the function $\deg f\colon S \to \mathbb{N}$, $\mathfrak{p} \mapsto \deg f(\mathbf{t})_\mathfrak{p}$, is locally constant and called the *degree* of $f(\mathbf{t})$. It is given by

$$(\deg f)(\mathfrak{p}) = d \qquad \Longleftrightarrow \qquad \varepsilon_d \equiv 1 \bmod \mathfrak{p}. \tag{1}$$

(i) $\Longrightarrow$ (ii): Write $f(\mathbf{t}) = \sum_{j=0}^{n} \lambda_j \mathbf{t}^j$ where $\lambda_j \in k$ and let $S_d \subset S$ be the set of $\mathfrak{p}$ such that $\deg f(\mathbf{t})_\mathfrak{p} = d$, for $d \in D := \{0, \dots, n\}$. Then

$$S_d = \{\mathfrak{p} \in S : (\lambda_d)_\mathfrak{p} = 1 \ \text{ and } (\lambda_j)_\mathfrak{p} = 0 \text{ for } j = d+1, \dots, n\}$$

which shows that the S_d are open in S, being finite intersections of open sets. Here we use the following general fact: If M is any k-module and $x \in M$ then $\{\mathfrak{p} \in S : x_\mathfrak{p} = 0\}$ is the complement of the support of the monogenous k-module $k \cdot x$ and hence open in S, cf. [**3**, II, §4.4, Prop. 17]. By our assumption (i), $S = \dot{\bigcup}_{d \in D} S_d$. Hence the $(S_d)_{d \in D}$ form a decomposition of S into open and closed subsets, corresponding to a family $(\varepsilon_d)_{d \in D}$ of orthogonal idempotents with sum 1_k via

$$\mathfrak{p} \in S_d \qquad \Longleftrightarrow \qquad \varepsilon_d \equiv 1 \bmod \mathfrak{p}. \tag{2}$$

Let $f_d(\mathbf{t}) = \varepsilon_d f(\mathbf{t})$. Then $f(\mathbf{t}) = \sum_{d \in D} \varepsilon_d f_d(\mathbf{t})$ and $f_d(\mathbf{t})_\mathfrak{p} = \left\{ \begin{matrix} 0 & \text{if } \mathfrak{p} \notin S_d \\ f(\mathbf{t})_\mathfrak{p} & \text{if } \mathfrak{p} \in S_d \end{matrix} \right\}$. In particular, $f_d(\mathbf{t})_\mathfrak{p}$ is monic of degree d for all $\mathfrak{p} \in S_d$. By standard facts on localization [**3**, II, §3.3, Cor. 2 of Th. 1], this implies that $f_d(\mathbf{t})$ is monic of degree d. Moreover, $\deg f$ is constant equal to d on S_d and hence locally constant on S, and (1) follows from (2).

(ii) $\Longrightarrow$ (i): Let $S_d := \operatorname{Spec}(k\varepsilon_d)$. Then the S_d define a decomposition of S into open and closed subsets, and for $\mathfrak{p} \in S_d$ and $d \neq d'$ we have $f_{d'}(\mathbf{t})_\mathfrak{p} = 0$. Hence $f(\mathbf{t})_\mathfrak{p} = f_d(\mathbf{t})_\mathfrak{p}$ is monic for all $\mathfrak{p} \in S$.

Remark. The set D can be chosen as any finite subset of $\mathbb{N}$ containing the range of the function $\deg f$. In particular, by reducing D to the range of $\deg f$, all ε_d are non-zero and, correspondingly, the S_d non-empty. However, it would be inconvenient to require this condition, see, e.g., 1.8. To be consistent, we then must consider the unique element of the polynomial ring over the zero ring as monic.

Locally monic polynomials behave well under base change: Let $R \in k$-**alg** and $\varrho\colon k \to R$ the homomorphism making R a k-algebra. Then $f(\mathbf{t})_R \in R[\mathbf{t}]$, obtained by applying ϱ to the coefficients of $f(\mathbf{t})$, is locally monic and the degree functions are related by

$$(\deg f_R)(\mathfrak{q}) = (\deg f)(\varrho^{-1}(\mathfrak{q})), \tag{3}$$

i.e., the diagram

$$\begin{array}{ccc} \operatorname{Spec}(R) & \xrightarrow{\ \deg f_R\ } & \mathbb{N} \\ & {\scriptstyle \operatorname{Spec}(\varrho)} \searrow \quad \nearrow {\scriptstyle \deg f} & \\ & \operatorname{Spec}(k) & \end{array} \tag{4}$$

commutes. This follows easily from (ii) above because the $(\varrho(\varepsilon_d))_{d \in D}$ form a complete system of orthogonal idempotents in R.

We also note that *the property of being locally monic descends from faithfully flat base extensions*: If $R \in k$-**alg** is faithfully flat over k and $f(\mathbf{t}) \in k[\mathbf{t}]$ has $f(\mathbf{t})_R$ locally monic then $f(\mathbf{t})$ is locally monic. Indeed, for every $\mathfrak{p} \in \operatorname{Spec}(k)$ there exists $\mathfrak{q} \in \operatorname{Spec}(R)$ such that $\varrho^{-1}(\mathfrak{q}) = \mathfrak{p}$, and $R_\mathfrak{q}$ is faithfully flat over $k_\mathfrak{p}$. Since the localization of $f(\mathbf{t})_R$ at $\mathfrak{q}$ is monic and may be identified with the base extension of $f(\mathbf{t})_\mathfrak{p}$ from $k_\mathfrak{p}$ to $R_\mathfrak{q}$, it follows by faithfully flat descent that $f(\mathbf{t})_\mathfrak{p}$ is monic.

0.9. The copolynomial. Let $\delta\colon \operatorname{Spec}(k) \to \mathbb{N}$ be a locally constant function, corresponding to a family of orthogonal idempotents $(\varepsilon_d)_{d\in D}$ with sum 1 in k via $\delta(\mathfrak{p}) = d \iff \mathfrak{p} \in \operatorname{Spec}(k\varepsilon_d)$. For example, $\delta = \deg f$ could be the degree function of a locally monic polynomial. For $R \in k$-**alg** and $r \in R$, we define

$$r^\delta := \sum_{d\in D} \varepsilon_d r^d \qquad \text{and} \qquad \delta \cdot r := \sum_{d\in D} \varepsilon_d dr. \tag{1}$$

Now let $f(\mathbf{t})$ be locally monic and let $f(\mathbf{t}) = \sum_{d\in D} \varepsilon_d f_d(\mathbf{t})$ as in (ii) of 0.8. The *copolynomial of* $f(\mathbf{t})$ is defined by

$$\check{f}(\mathbf{t}) := \mathbf{t}^{\deg f} \cdot f(\mathbf{t}^{-1}) = \sum_{d\in D} \varepsilon_d \mathbf{t}^d f_d(\mathbf{t}^{-1}). \tag{2}$$

Clearly, $\check{f}(0) = \sum_{d\in D} \varepsilon_d = 1$, so the copolynomial is *comonic*. We define the *coefficients* c_i *of* f *in descending order* by the following ascending expansion of $\check{f}(\mathbf{t})$:

$$\check{f}(\mathbf{t}) = \sum_{i\in\mathbb{N}} (-1)^i c_i \mathbf{t}^i. \tag{3}$$

Of course, $c_0 = 1$ and $c_i = 0$ for $i > \max\deg f$. We can reconstruct $f(\mathbf{t})$ from $\check{f}(\mathbf{t})$ and $\deg f$ by the formula

$$f(\mathbf{t}) = \mathbf{t}^{\deg f} \cdot \check{f}(\mathbf{t}^{-1}), \tag{4}$$

which yields the expansion

$$f(\mathbf{t}) = \sum_{i\in\mathbb{N}} (-1)^i c_i \mathbf{t}^{(\deg f)-i} = \sum_{d\in D} \varepsilon_d \sum_{j=0}^{d} (-1)^j c_j \mathbf{t}^{d-j}. \tag{5}$$

This also shows why it is more convenient to define the coefficients of f in the roundabout manner using $\check{f}$ rather than f. We finally remark that

$$f(0) \in k^\times \quad \Longrightarrow \quad f(0)^{-1}\check{f}(\mathbf{t}) \text{ is locally monic of degree } \deg(f). \tag{6}$$

Indeed, this is easily reduced to the case where $\deg(f) = d$ is constant. Then $f(\mathbf{t}) = \sum_{i=0}^{d} (-1)^i c_i \mathbf{t}^{d-i}$ and hence $f(0)^{-1}\check{f}(\mathbf{t}) = \sum_{i=0}^{d} (-1)^{d-i} c_i c_d^{-1} \mathbf{t}^i$.

0.10. Example: Characteristic polynomials. Let M be a finitely generated and projective k-module and let $g \in \operatorname{End}(M)$. We refer to [**1**] for the notion of the determinant of g. The *characteristic polynomial of* g is defined by

$$\chi_g(\mathbf{t}) := \det(\mathbf{t}\mathrm{Id}_M - g). \tag{1}$$

This is locally monic, has degree $\deg \chi_g = \operatorname{rk} M$, and the associated copolynomial is

$$\check{\chi}_g(\mathbf{t}) = \det(\mathrm{Id}_M - \mathbf{t}g) = \sum_{i\in\mathbb{N}} (-1)^i c_i(g)\mathbf{t}^i, \tag{2}$$

where the coefficients are given by $c_i(g) = \operatorname{trace} \bigwedge^i g$. (Note that in [**1**], $\lambda_{\mathbf{t}}(g) := \check{\chi}_g(-\mathbf{t})$ is called the characteristic polynomial of g.)

The following lemma is probably well known but we give a proof for lack of a convenient reference.

0.11. Lemma. *The map associating with a polynomial $f \in k[\mathbf{t}]$ the quotient $E = k[\mathbf{t}]/\big(f\big)$ induces a bijection between the set of locally monic polynomials in $k[\mathbf{t}]$ and the set of quotient algebras of $k[\mathbf{t}]$ which are finitely generated and projective as k-modules. The inverse map is given by $E \mapsto \chi_{L(z)}(\mathbf{t})$, where $z := \mathrm{can}(\mathbf{t}) \in E$ and $L(z)$ is multiplication by z in the algebra E. The degree of f equals the rank of E (as functions on $\mathrm{Spec}(k)$), and f is monic of degree d if and only if E is free with basis $1, z, \dots, z^{d-1}$.*

Proof. (a) Let $f(\mathbf{t})$ be locally monic. After decomposing $1_k = \sum_{d\in D} \varepsilon_d$ as in 0.8, we may assume that $f(\mathbf{t})$ is monic of (constant) degree d. Then it follows from the usual division algorithm in $k[\mathbf{t}]$ that E is free of rank d with basis $z^0, \dots, z^{d-1}$. Now a standard computation shows that $\det(\mathbf{t}\mathrm{Id}_E - L(z)) = f(\mathbf{t})$.

(b) Conversely, let $\mathfrak{N}$ be an ideal in $k[\mathbf{t}]$, let $E = k[\mathbf{t}]/\mathfrak{N}$ be finitely generated and projective and let $f(\mathbf{t}) := \chi_{L(z)}(\mathbf{t})$. Then $f(\mathbf{t})$ is locally monic of degree $\mathrm{rk}\, E$, and by the Cayley-Hamilton Theorem [**1**, Th. 1.4], $0 = f(L(z)) \cdot 1_E = \mathrm{can}(f(\mathbf{t}))$ where can: $k[\mathbf{t}] \to E$ is the canonical map. Thus $f(\mathbf{t}) \in \mathfrak{N}$, so there exists a surjective homomorphism u: $E' := k[\mathbf{t}]/\big(f(\mathbf{t})\big) \to E$. By what we proved in (a), E' is finitely generated and projective, and $\mathrm{rk}\, E' = \deg f = \mathrm{rk}\, E$. By standard facts on finitely generated and projective modules [**3**, II, §3.3, Th. 1 and Cor. 5 of Th. 1], u is an isomorphism.

0.12. Schemes defined by modules. With any k-module M, we associate functors $M_{\mathbf{a}}$ and $M_{\mathbf{u}}$ defined by

$$M_{\mathbf{a}}(R) = M \otimes R, \qquad M_{\mathbf{u}}(R) = \{x \in M_{\mathbf{a}}(R) : x \text{ unimodular}\}.$$

If $M = k$, then $k_{\mathbf{u}}$ is just the functor of units, i.e., $k_{\mathbf{u}}(R) = R^\times$, so $k_{\mathbf{u}} = \mathbf{G}_m$, the multiplicative group (over k). Now suppose M is finitely generated and projective. Then $M_{\mathbf{a}} \cong \mathbf{Spec}(A)$ is an affine, smooth and finitely presented k-scheme with connected fibres over k, where $A = \mathcal{O}(M)$, the symmetric algebra over the dual module M^* of M [**6**, II, §1, 2.1]. Moreover, A is faithfully flat over k, so, denoting by ι: $k \to A$ the canonical homomorphism,

$$\mathrm{Spec}(\iota)\colon \mathrm{Spec}(A) \to \mathrm{Spec}(k) \text{ is open and surjective,} \tag{1}$$

cf. [**10**, Th. 2.4.6]. Also, $M_{\mathbf{u}}$ is open in $M_{\mathbf{a}}$, quasi-affine (but in general no longer affine) and also smooth, finitely presented and with connected fibres. Indeed, choose a generating set $\alpha_1, \dots, \alpha_n$ for M^*. Then $M_{\mathbf{u}}$ is the union of the open subschemes of $M_{\mathbf{a}}$ defined by $\alpha_1, \dots, \alpha_n$, i.e., $x \in M_{\mathbf{u}}(R)$ if and only if the ideal of R generated by $\alpha_1(x), \dots, \alpha_n(x)$ is all of R.

Note that $A = \mathcal{O}(M)$ is compatible with base ring extension: For all $R \in k$-**alg** there is a canonical isomorphism $A_R \cong \mathcal{O}(M_R)$ which will be treated as an identification. This comes from the canonical isomorphism $(M_R)^* \cong (M^*)_R$ (because M is finitely generated and projective) and the fact that the symmetric algebra commutes with base ring extension.

We may identify A with the algebra of k-valued polynomial laws on M in the sense of [**31**]. Thus if $g \in A$, then for all $x \in M_R$ we have $g(x) \in R$, and for all k-algebra homomorphisms ϱ: $R \to S$, we have $\varrho(g(x)) = g((\mathrm{Id}_M \otimes \varrho)(x))$. Usually, this will be simply written as $g(x)_S = g(x_S)$. Also, $A = \bigoplus_{n\in\mathbb{N}} A_n$ is a graded algebra, where A_n is the n-th symmetric power of M^*, corresponding to the homogeneous polynomial laws of degree n. In particular, $A_0 = k$, $A_1 = M^*$ and A_2 is naturally identified with the quadratic forms on M. We claim that

$$\text{an idempotent } \varepsilon \text{ of } A \text{ belongs to } A_0 = k. \tag{2}$$

Indeed, decompose $\varepsilon = \varepsilon_0 + \varepsilon_+$ where $\varepsilon_0 \in A_0$ and $\varepsilon_+ \in \sum_{i\geqslant 1} A_i$. Assume $\varepsilon_+ \neq 0$, and let $n \geqslant 1$ be maximal with the property that $\varepsilon_+ \in \bigoplus_{i\geqslant n} A_i$. Then $\varepsilon^2 = \varepsilon_0^2 + 2\varepsilon_0\varepsilon_+ + \varepsilon_+^2 = \varepsilon_0 + \varepsilon_+$ yields $\varepsilon_0^2 = \varepsilon_0$ and $\varepsilon_+ = 2\varepsilon_0\varepsilon_+ + \varepsilon_+^2$, or $(1-2\varepsilon_0)\varepsilon_+ = \varepsilon_+^2$. Now $(1-2\varepsilon_0)^2 = 1$ and hence $\varepsilon_+ = (1-2\varepsilon_0)\varepsilon_+^2 \in \bigoplus_{i\geqslant 2n} A_i$, contradiction.

0.13. Locally monic polynomials, continued. We keep the notations and conventions introduced in 0.12. Consider a polynomial $f(\mathbf{t}) = \sum_{i\geqslant 0} g_i\,\mathbf{t}^i \in A[\mathbf{t}]$ and an element $x \in M_R$. By evaluating the coefficients of f at x we obtain a polynomial in $R[\mathbf{t}]$, written

$$f(\mathbf{t};x) := \sum_{i\geqslant 0} g_i(x)\,\mathbf{t}^i \in R[\mathbf{t}]. \tag{1}$$

Conversely, specifying an element in $A[\mathbf{t}]$ amounts to specifying a polynomial $f(\mathbf{t};x) \in R[\mathbf{t}]$ for all $x \in M_R$ and all $R \in k$-**alg**, varying functorially with R, i.e., such that $f(\mathbf{t};x)_S = f(\mathbf{t};x_S)$ for all R-algebras S. Note also that, for $f(\mathbf{t}) \in A[\mathbf{t}]$ and any $R \in k$-**alg**,

$$f_R := f(\mathbf{t})_R := f(\mathbf{t}) \otimes_k 1_R = \sum_{i\geqslant 0} (g_i)_R\,\mathbf{t}^i \in A_R[\mathbf{t}] \tag{2}$$

is a polynomial with coefficients in A_R.

Now let $f(\mathbf{t}) \in A[\mathbf{t}]$ be locally monic, with degree function $\deg f\colon \mathrm{Spec}(A) \to \mathbb{N}$, and let $f(\mathbf{t}) = \sum_{d\in D} \varepsilon_d f_d(\mathbf{t})$ as in 0.8, where $(\varepsilon_d)_{d\in D}$ is a complete system of orthogonal idempotents of A and $f_d(\mathbf{t})$ is monic of degree d. By 0.12.2, the ε_d belong to k. Let $R \in k$-**alg** and let $\varrho\colon k \to R$ be the homomorphism making R a k-algebra. Then the $\varrho(\varepsilon_d) = \varepsilon_d \otimes 1_R$ form a family of orthogonal idempotents with sum 1_R, and $f(\mathbf{t})_R = \sum_{d\in D}(\varepsilon_d \otimes 1_R)\cdot f_d(\mathbf{t})\otimes 1_R$ shows that $f(\mathbf{t})_R$ is locally monic.

Let $\mathfrak{P} \in \mathrm{Spec}(A)$ and $\mathfrak{p} := k \cap \mathfrak{P} = \mathrm{Spec}(\iota)(\mathfrak{P}) \in \mathrm{Spec}(k)$. Then

$$\begin{aligned} (\deg f)(\mathfrak{P}) = d \quad &\Longleftrightarrow \quad \varepsilon_d \equiv 1 \bmod \mathfrak{P} && \text{(by 0.8.1)} \\ &\Longleftrightarrow \quad \varepsilon_d \equiv 1 \bmod \mathfrak{p} && \text{(by 0.12.2).} \end{aligned}$$

Thus there exists a unique locally constant function $\overline{\deg}\, f\colon \mathrm{Spec}(k) \to \mathbb{N}$ making the diagram

$$\begin{array}{ccc} \mathrm{Spec}(A) & \xrightarrow{\ \deg f\ } & \mathbb{N} \\ & {\scriptstyle \mathrm{Spec}(\iota)} \searrow \quad \nearrow {\scriptstyle \overline{\deg}\, f} & \\ & \mathrm{Spec}(k) & \end{array} \tag{3}$$

commutative. It can also be described as follows: $A_{\boldsymbol{\kappa}(\mathfrak{p})}$ is isomorphic to the polynomial algebra in $n = \mathrm{rk}_{\mathfrak{p}}\, M$ variables over $\boldsymbol{\kappa}(\mathfrak{p})$, in particular, it is an integral domain. Hence the locally monic polynomial $f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})} \in A_{\boldsymbol{\kappa}(\mathfrak{p})}[\mathbf{t}]$ is actually monic, and we have

$$\big(\overline{\deg}\, f\big)(\mathfrak{p}) = \deg f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}, \tag{4}$$

for all $\mathfrak{p} \in \mathrm{Spec}(k)$. Indeed, letting d be the unique element of D with $\varepsilon_d \equiv 1 \bmod \mathfrak{p}$ (which exists because $\mathfrak{p}$ is a prime ideal), we see that $f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})} = f_d(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}$ has degree d, as required.

Let again $R \in k$-**alg** and let $x \in M_R$. Then $f(\mathbf{t};x) = \sum_{d\in D} \varepsilon_d f_d(\mathbf{t};x) = \sum_{d\in D} \varrho(\varepsilon_d) f_d(\mathbf{t};x)$. Furthermore, for $\mathfrak{q} \in \mathrm{Spec}(R)$, $\varrho(\varepsilon_d) \equiv 1 \bmod \mathfrak{q}$ if and only if $\varepsilon_d \equiv 1 \bmod \varrho^{-1}(\mathfrak{q})$. Hence $f(\mathbf{t};x)$ is locally monic of degree

$$\deg f(\mathbf{t};x) = (\overline{\deg}\, f) \circ \mathrm{Spec}(\varrho). \tag{5}$$

In particular, for $R = k$ (and hence $\varrho = \mathrm{Id}$) we see that $\overline{\deg}\, f = \deg f(\mathbf{t};x)$ for any $x \in M$. Applying this to $f_R \in A_R[\mathbf{t}]$ (cf. (2)) and noting that $f_R(\mathbf{t};x) = f(\mathbf{t};x)$ for all $x \in M_R$ yields

$$\overline{\deg}\, f_R = (\overline{\deg}\, f) \circ \mathrm{Spec}(\varrho). \tag{6}$$

We finally remark that passing to the copolynomial commutes with evaluating the coefficients, i.e., we have the formula

$$\check{f}(\mathbf{t};x) = f(\mathbf{t};x)\check{}\,. \tag{7}$$

Indeed, by the definition of the copolynomial in 0.9, $f(\mathbf{t};x)\check{} = \sum \mathbf{t}^d \varrho(\varepsilon_d) f_d(\mathbf{t}^{-1};x)$, and $\check{f}(\mathbf{t}) = \sum \mathbf{t}^d \varepsilon_d f_d(\mathbf{t}^{-1})$. Evaluating this at x yields $\check{f}(\mathbf{t};x) = \sum \mathbf{t}^d \varepsilon_d f_d(\mathbf{t}^{-1};x)$. But since R is a k-algebra, $\varepsilon_d r = \varrho(\varepsilon_d) r$ for all $r \in R$, whence (7).

0.14. Density. A subfunctor $\mathbf{U}$ of a k-functor $\mathbf{X}$ is called *dense* if, for all open subfunctors $\mathbf{V} \subset \mathbf{X}$ and all closed $\mathbf{Z} \supset \mathbf{U} \cap \mathbf{V}$ we have $\mathbf{Z} = \mathbf{V}$, and this property remains valid in all scalar extensions. If $\mathbf{X}$ is a scheme then this notion agrees with "universally schematically dense" in the sense of [**11**, 11.10].

Let $\mathbf{X}$ be a smooth separated finitely presented k-scheme with connected non-empty fibres, and let $\mathbf{U}$ be an open subscheme of $\mathbf{X}$. We refer to [**7**, Exp. XVIII, 1.7] and [**11**, 11.10.10] for the equivalence of the following conditions:

(i) $\mathbf{U}$ is dense in $\mathbf{X}$,
(ii) there exists a faithfully flat and finitely presented $R \in k$-**alg** such that $\mathbf{U}(R) \neq \emptyset$,
(iii) $\mathbf{U}(K) \neq \emptyset$ for all algebraically closed fields $K \in k$-**alg**.

Note that the assumptions on $\mathbf{X}$ are in particular satisfied when $\mathbf{X} = M_{\mathbf{a}}$ is the k-scheme defined by a finitely generated and projective k-module M.

For example, let J be a Jordan algebra over k which is finitely generated and projective as a k-module, let $\mathbf{J} = J_{\mathbf{a}}$ be the affine scheme defined by J and $\mathbf{U} = \mathbf{J}^{\times}$ the subfunctor of invertible elements, defined by $\mathbf{U}(R) = J_R^{\times}$ for all $R \in k$-**alg**. Then $\mathbf{U}$ is open, being the inverse image of $k_{\mathbf{u}}$ under the morphism $x \mapsto \det U_x$ for all x in all base extensions of J, and it is dense because $1_J \in \mathbf{U}(k)$.

Density will be used mostly for the following type of argument: Suppose $\mathbf{U} \subset \mathbf{X}$ is dense, that $\mathbf{Y}$ is a separated k-functor, and that $f, g \colon \mathbf{X} \to \mathbf{Y}$ are morphisms which agree on $\mathbf{U}$. Then $f = g$. This is immediate from the definition applied to $\mathbf{V} = \mathbf{X}$ and $\mathbf{Z}$ the subfunctor of $\mathbf{X}$ where f and g agree.

0.15. Pure submodules. Recall [**18**, §4J] that a submodule P of a k-module X is called *pure* if for every k-module N, the map $u \otimes \mathrm{Id}_N \colon P \otimes N \to X \otimes N$ induced from the inclusion $u \colon P \subset X$ is injective. For example, this is so if P is a direct summand or if X/P is flat. We collect some facts on pure submodules.

(a) P is pure if and only if the map $P \otimes R \to X \otimes R$ is injective, for all $R \in k$-**alg**.

(b) If P is pure in X then P_R (canonically identified with $\mathrm{Im}(u_R)$) is a pure submodule of X_R, for all $R \in k$-**alg**.

(c) Conversely, if $R \in k$-**alg** is faithfully flat and P_R is pure in X_R then P is pure in X.

(d) Suppose X is projective and $P \subset X$ is pure and finitely generated. Then P is a direct summand of X (and hence both P and X/P are projective.)

(e) Suppose k is a principal ideal domain. Then P is pure in X if and only if $P \cap \lambda X = \lambda P$, for all $\lambda \in k$.

Proof. (a) The stated condition is obviously necessary. To see that it is sufficient, let N be an arbitrary k-module, and let $R := k \oplus N$ be the split null extension. Then the injectivity of $P \otimes R \to X \otimes R$ implies that also $P \otimes N \to X \otimes N$ is injective.

(b) See [**3**, I, Ex. 24(e) of §2] or [**18**, 4.84(f)].

(c) Let N be a k-module. Since R is faithfully flat, the map $P \otimes N \to X \otimes N$ is injective provided the map $(P \otimes N) \otimes R \to (X \otimes N) \otimes R$ is injective. Now $(P \otimes N) \otimes R \cong (P \otimes_k R) \otimes_R (N \otimes_k R)$ by [**4**, II, §5.1, Prop. 3], and similarly for X in place of P. Since P_R is pure in X_R, the map $(P_R) \otimes (N_R) \to X_R \otimes N_R$ is injective, whence our assertion.

(d) See [**18**, p. 164, Ex. 42(a)].

(e) See [**3**, I, Ex. 24(a) of §2] or [**18**, Cor. 4.93].

1. Algebraic elements

1.1. In this section, J always denotes a unital quadratic Jordan algebra over an arbitrary commutative ring k of scalars. Denote by $k[\mathbf{t}]$ the polynomial ring in the indeterminate $\mathbf{t}$ and let $a \in J$. It is well known that there is a unique homomorphism $j_a\colon k[\mathbf{t}]^+ \to J$ of Jordan algebras sending $\mathbf{t}$ to a. The image of j_a is the subalgebra $k[a]$ of J generated by (1 and) a. The kernel $\mathfrak{K}(a)$ of j_a is a Jordan, but in general not an associative ideal of $k[\mathbf{t}]$. In case k is a field, $\mathfrak{K}(a)$ contains a unique largest associative ideal [**16**, Section 1] which is of course principal. If k is arbitrary, we proceed in a somewhat different manner as follows.

Write the elements of $J^2 = J \times J$ as formal column vectors $\begin{pmatrix} x \\ y \end{pmatrix}$, $x, y \in J$, and correspondingly the endomorphisms of J^2 as 2×2-matrices with entries from $\operatorname{End} J$. For $a \in J$ and $i \in \mathbb{N}$, define $a^{[i]} \in J^2$ by

$$a^{[i]} := \begin{pmatrix} a^i \\ a^{i+1} \end{pmatrix}. \tag{1}$$

Let $h_a\colon k[\mathbf{t}] \to J^2$ be the unique k-linear map with $h_a(\mathbf{t}^i) = a^{[i]}$, and denote its kernel by $\mathfrak{N}(a)$ and its image by $M(a)$. Thus

$$h_a(f(\mathbf{t})) = \begin{pmatrix} j_a(f(\mathbf{t})) \\ j_a(\mathbf{t}f(\mathbf{t})) \end{pmatrix}, \tag{2}$$

whence $j_a = \mathrm{pr}_1 \circ h_a$ and $\mathfrak{N}(a) \subset \mathfrak{K}(a)$. Also, by definition, we have an exact sequence

$$0 \longrightarrow \mathfrak{N}(a) \xrightarrow{\ i_a\ } k[\mathbf{t}] \xrightarrow{\ h'_a\ } M(a) \longrightarrow 0 \tag{3}$$

of k-modules, where i_a is inclusion and h'_a is just h_a but with codomain $M(a) = \operatorname{Im}(h_a)$. If $\psi\colon J \to \tilde{J}$ is a homomorphism of unital Jordan algebras, one checks immediately that

$$\mathfrak{K}(a) \subset \mathfrak{K}(\psi(a)) \quad \text{and} \quad \mathfrak{N}(a) \subset \mathfrak{N}(\psi(a)). \tag{4}$$

1.2. Lemma and Definition. (a) *Let* $\theta_a := \begin{pmatrix} 0 & \mathrm{Id} \\ U_a & 0 \end{pmatrix} \in \operatorname{End}(J^2)$. *Then*

$$\theta_a^2 = \begin{pmatrix} U_a & 0 \\ 0 & U_a \end{pmatrix}, \tag{1}$$

$$\theta_a \cdot a^{[i]} = a^{[i+1]}, \tag{2}$$

$$h_a\big(f(\mathbf{t})g(\mathbf{t})\big) = f(\theta_a) \cdot h_a\big(g(\mathbf{t})\big), \tag{3}$$

for all $i \in \mathbb{N}$ *and* $f(\mathbf{t}), g(\mathbf{t}) \in k[\mathbf{t}]$. *Hence, regarding* J^2 *as a* $k[\mathbf{t}]$*-module by letting* $\mathbf{t}$ *act via* θ_a, h_a *is a homomorphism of* $k[\mathbf{t}]$*-modules and* $M(a)$ *is the* $k[\mathbf{t}]$*-submodule generated by* $a^{[0]}$.

(b) $\mathfrak{N}(a)$ *is the largest ideal of* $k[\mathbf{t}]$ *contained in* $\mathfrak{K}(a)$. *We define*

$$E(a) := k[\mathbf{t}]/\mathfrak{N}(a), \tag{4}$$

regarded as a commutative associative monogenous k*-algebra, generated by the element* $z := \operatorname{can}(\mathbf{t})$, *and denote by* $\pi\colon E(a)^+ \to J$ *the homomorphism of Jordan algebras induced from* j_a. *Then for all* $b \in \operatorname{Ker}(\pi) = \mathfrak{K}(a)/\mathfrak{N}(a)$, $b^2 = 2b = 0$.

(c) *Let* $M_0(a) = \{w \in M(a) : \mathrm{pr}_1(w) = 0\}$. *Then* $M_0(a) \cong \operatorname{Ker}(\pi)$ *as* k*-modules, and* $\mathrm{pr}_2(M_0(a)) \subset J$ *consists of absolute zero divisors.*

Remark. Of course, h_a induces a canonical isomorphism

$$\gamma_a\colon E(a) \xrightarrow{\cong} M(a)\,, \qquad \gamma_a(z^n) = a^{[n]}, \tag{5}$$

of k-modules and even of $k[\mathbf{t}]$-modules. Nevertheless, it is useful to distinguish $E(a)$ and $M(a)$, in particular, since the algebra structure of $E(a)$ does not correspond to a multiplication on $M(a)$ induced in a natural way from the Jordan algebra structure on J^2.

Proof. (a) (1) and (2) are immediate from the definitions and (3) follows easily from (2).

(b) It is clear from (3) that $\mathfrak{N}(a)$ is an ideal of $k[\mathbf{t}]$ and $\mathfrak{N}(a) \subset \mathfrak{K}(a)$ by 1.1.2. Now suppose I is an ideal of $k[\mathbf{t}]$ contained in $\mathfrak{K}(a)$, and let $f(\mathbf{t}) \in I$. Then also $\mathbf{t}f(\mathbf{t}) \in I$, and hence $h_a(f(\mathbf{t})) = 0$ by 1.1.2, showing $f(\mathbf{t}) \in \mathfrak{N}(a)$. If $g(\mathbf{t}) \in \mathfrak{K}(a)$ then, because $\mathfrak{K}(a)$ is a Jordan ideal, $g(\mathbf{t})^2$ and $\mathbf{t}g(\mathbf{t})^2 = U_{g(\mathbf{t})} \cdot \mathbf{t}$ belong to $\mathfrak{K}(a)$, whence $g(\mathbf{t})^2 \in \mathrm{Ker}(h_a) = \mathfrak{N}(a)$ by 1.1.2. Similarly, $2g(\mathbf{t}) = 1 \circ g(\mathbf{t})$ and $2\mathbf{t}g(\mathbf{t}) = \mathbf{t} \circ g(\mathbf{t})$ belong to $\mathfrak{K}(a)$, showing $2g(\mathbf{t}) \in \mathfrak{N}(a)$.

(c) The first statement follows easily from $\mathrm{pr}_1 \circ h_a = j_a$. An element $w = \begin{pmatrix} 0 \\ y \end{pmatrix}$ belongs to $M_0(a)$ if and only if there exists $f(\mathbf{t}) \in k[\mathbf{t}]$ such that $j_a(f(\mathbf{t})) = 0$, i.e., $f(a) = 0$, and $y = j_a(\mathbf{t}f(\mathbf{t})$. By [**15**, Cor. 3.3.3], $U_y = U_a U_{f(a)} = 0$.

1.3. Lemma. *Let $a \in J$ and $R \in k$-**alg**. We use the notations of* 1.2 *and* 0.1.

(a) *Identify $k[\mathbf{t}] \otimes R$ with $R[\mathbf{t}]$ in the canonical way. Then*

$$(h_a)_R = h_{a_R}\colon R[\mathbf{t}] \to J_R^2. \tag{1}$$

(b) *The image of $(i_a)_R$ is contained in $\mathfrak{N}(a_R)$ and hence induces a homomorphism $\varphi\colon \mathfrak{N}(a) \otimes R \to \mathfrak{N}(a_R)$, for which $\mathrm{Ker}(\varphi) = \mathrm{Ker}\big((i_a)_R\big)$. The image of the map $u_R\colon M(a) \otimes R \to J_R^2$ induced from the inclusion $u\colon M(a) \subset J^2$ is $M(a_R)$, whence a surjective homomorphism $u'_R\colon M(a) \otimes R \to M(a_R)$ of R-modules. The diagram*

$$\begin{array}{ccccccccc}
 & & \mathrm{Ker}(\varphi) & \longrightarrow & 0 & \longrightarrow & \mathrm{Ker}(u_R) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathfrak{N}(a)\otimes R & \xrightarrow{(i_a)_R} & R[\mathbf{t}] & \xrightarrow{(h'_a)_R} & M(a)\otimes R & \longrightarrow & 0\\
 & & {\scriptstyle\varphi}\downarrow & & \| & & \downarrow{\scriptstyle u'_R} & & \\
0 & \longrightarrow & \mathfrak{N}(a_R) & \xrightarrow[i_{a_R}]{} & R[\mathbf{t}] & \xrightarrow[h'_{a_R}]{} & M(a_R) & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Coker}(\varphi) & \longrightarrow & 0 & \longrightarrow & 0 & &
\end{array} \tag{2}$$

is commutative with exact rows and columns, and there is a canonical isomorphism

$$\partial\colon \mathrm{Ker}(u_R) \xrightarrow{\cong} \mathrm{Coker}(\varphi). \tag{3}$$

(c) *The unique R-module homomorphism $\eta\colon E(a) \otimes R \to E(a_R)$ making the diagram*

$$\begin{array}{ccc}
E(a)\otimes R & \xrightarrow{\eta} & E(a_R)\\
{\scriptstyle(\gamma_a)_R}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\gamma_{a_R}}\\
M(a)\otimes R & \xrightarrow[u'_R]{} & M(a_R)
\end{array} \tag{4}$$

commutative, is a homomorphism of R-algebras.

(d) *If R is flat over k then* $\mathrm{Ker}(u_R) = 0$ *and* u'_R *is an isomorphism.*

Proof. (a) The map $x \mapsto x_R$ from J to J_R is a homomorphism of Jordan algebras over k. Hence $(a^n)_R = (a_R)^n$ which implies

$$(h_a)_R(\mathbf{t}^n) = h_a(\mathbf{t}^n)_R = \big(a^{[n]}\big)_R = (a_R)^{[n]} = h_{a_R}(\mathbf{t}^n), \tag{5}$$

from which (1) follows.

(b) Let $f(\mathbf{t}) \in \mathfrak{N}(a)$ and $r \in R$. Then by (1),

$$h_{a_R}\big(f(\mathbf{t}) \otimes r\big) = (h_a)_R\big(f(\mathbf{t}) \otimes r\big) = h_a(f(\mathbf{t})) \otimes r = 0.$$

Since the elements of the form $f(\mathbf{t}) \otimes r$ span $\mathfrak{N}(a) \otimes R$, this proves the existence of φ. Next, let $f(\mathbf{t}) \otimes r \in k[\mathbf{t}] \otimes R = R[\mathbf{t}]$. Then

$$u_R\big(h'_a(f(\mathbf{t})) \otimes r\big) = h_a(f(\mathbf{t})) \otimes r = (h_a)_R\big(f(\mathbf{t}) \otimes r\big) = h_{a_R}\big(f(\mathbf{t}) \otimes r\big)$$

(by (1)) shows that the image of u_R equals the image of h_{a_R} which is, by definition, $M(a_R)$. This establishes the existence of u'_R.

It is easy to check that (2) is commutative. The exactness of the second row follows by tensoring 1.1.3 with R, while the exactness of the third row is just 1.1.3, but for a_R instead of a. Now (3) follows from the Snake Lemma [**3**, I, §1.4].

(c) Let $z = \mathrm{can}(\mathbf{t}) \in E(a)$ and $w = \mathrm{can}'(\mathbf{t}) \in E(a_R)$ (where $\mathrm{can}'\colon R[\mathbf{t}] \to E(a_R)$ is the canonical map) be the generators of $E(a)$ and $E(a_R)$, respectively. We show that $\eta(z^n \otimes 1_R) = w^n$ for all $n \in \mathbb{N}$, from which the homomorphism property of η follows easily. Now $\gamma_{a_R}(w^n) = (a_R)^{[n]}$ while $u_R\big((\gamma_a)_R(z^n \otimes 1_R)\big) = u_R\big(\gamma_a(z^n) \otimes 1_R\big) = u_R(a^{[n]} \otimes 1_R) = (a^{[n]})_R$, and these two are equal by (5).

(d) Obvious.

1.4. Definition. Let again J be a unital Jordan algebra over k. We will use the expression "a satisfies a polynomial $f(\mathbf{t})$" for the fact that $f(\mathbf{t}) \in \mathfrak{N}(a)$, i.e., that $j_a(f(\mathbf{t})) = j_a(\mathbf{t}f(\mathbf{t})) = 0$. An element $a \in J$ is called *integral* if it satisfies some monic polynomial. Just as in the case of associative algebras, we have:

$$a \text{ is integral} \quad\Longleftrightarrow\quad M(a) \text{ is finitely generated as a } k\text{-module.} \tag{1}$$

Indeed, the implication from left to right follows easily from 1.2.2 and induction. For the reverse, note that θ_a induces, by 1.2.2, an endomorphism

$$\zeta_a\colon M(a) \to M(a).$$

Then $M(a)$ is a faithful $k[\zeta_a]$-module. Hence by [**3**, V, §1.1, Lemma 1], there exists a monic $f(\mathbf{t}) \in k[\mathbf{t}]$ satisfying $f(\zeta_a) = 0$. It follows that $0 = f(\zeta_a) \cdot a^{[0]} = f(\theta_a) \cdot a^{[0]} = h_a(f(\mathbf{t}))$ (by 1.2.3), so a satisfies $f(\mathbf{t})$.

In general, integral elements do not have well-defined minimum polynomials, i.e., the ideal $\mathfrak{N}(a)$ need not be generated by a (locally) monic polynomial. For example, let $k = \mathbb{Z}/4\mathbb{Z}$, $J = \mathrm{Mat}_2(k)^+$ and $a = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$. Then $\mathfrak{N}(a)$ is generated by $2\mathbf{t}$ and $\mathbf{t}^2$ and $E(a) \cong k \oplus (k/2k)$ is not projective as a k-module. Therefore, we introduce the following notion. An element $a \in J$ is called *pre-algebraic* if $E(a)$ is a finitely generated and projective k-module. By Lemma 0.11, this is equivalent to $\mathfrak{N}(a)$ being the principal ideal generated by a unique locally monic polynomial, called the *minimum polynomial* of a and denoted by $\mu_a(\mathbf{t})$. Because $E(a) \cong M(a)$ by 1.2.5, we have

$$a \text{ is pre-algebraic} \iff M(a) \text{ is a finitely generated projective } k\text{-module.} \tag{2}$$

Obviously, by (1) and (2),

$$a \text{ pre-algebraic} \implies a \text{ integral.} \tag{3}$$

We note that, for a pre-algebraic,

$$\mu_a(\mathbf{t}) = \det(\mathbf{t}\mathrm{Id}_{M(a)} - \zeta_a), \qquad \check{\mu}_a(\mathbf{t}) = \det(\mathrm{Id}_{M(a)} - \mathbf{t}\zeta_a). \tag{4}$$

Indeed, we have the commutative diagram

$$\begin{array}{ccc} E(a) & \xrightarrow{L(z)} & E(a) \\ \gamma_a \downarrow \cong & & \cong \downarrow \gamma_a \\ M(a) & \xrightarrow[\zeta_a]{} & M(a) \end{array}$$

where γ_a is the isomorphism 1.2.5. Hence the assertion follows from 0.10.2, Lemma 0.11 and the fact that the determinant is compatible with isomorphisms [**1**, Prop. 1.3(iv)].

The *degree* of a pre-algebraic a is defined to be the degree of $\mu_a(\mathbf{t})$, i.e., the locally constant function

$$\deg a\colon \mathfrak{p} \mapsto \deg \mu_a(\mathbf{t})_{\mathfrak{p}} = \mathrm{rk}_{\mathfrak{p}}\, E(a) = \mathrm{rk}_{\mathfrak{p}}\, M(a) \tag{5}$$

on Spec(k). If a has constant degree d, i.e., if $\mu_a(\mathbf{t})$ is monic of degree d, then by Lemma 0.11, $E(a)$ is free as a k-module with basis $1, \ldots, z^{d-1}$. Hence 1.2.5 implies

$$a \text{ is pre-algebraic of degree } d \iff a^{[0]}, \ldots, a^{[d-1]} \text{ is a basis of } M(a). \tag{6}$$

Note that for a pre-algebraic $a \in J$, the exact sequence 1.1.3 splits because $M(a)$ is in particular projective. It therefore remains exact upon tensoring with any $R \in k$-**alg**, so we have, with the notations of Lemma 1.3(b):

$$a \text{ pre-algebraic} \implies \varphi\colon \mathfrak{N}(a) \otimes R \to \mathfrak{N}(a_R) \text{ injective.} \tag{7}$$

Hence, for a pre-algebraic a, we may and often will identify $\mathfrak{N}(a) \otimes R$ with its image in $\mathfrak{N}(a_R)$. However, even when also a_R is pre-algebraic, φ is not necessarily surjective, and hence $\mu_a(\mathbf{t})_R$ may be different from $\mu_{a_R}(\mathbf{t})$. For example, let $k = \mathbb{Z}$ and $J = B^+$ where B is the associative commutative $\mathbb{Z}$-algebra, free of rank 4, with basis $1, a, b, ab$ and multiplication table $a^2 = 2b$, $b^2 = 0$. Then $\mathfrak{K}(a) = \mathfrak{N}(a) = (\mathbf{t}^4)$ so $\mu_a(\mathbf{t}) = \mathbf{t}^4$. But for $R = \mathbb{Z}/2\mathbb{Z}$, J_R is the tensor product of the algebra of dual numbers over R with itself, and the minimum polynomial of a_R is $\mathbf{t}^2$. This leads to the following definition:

An element $a \in J$ is called *algebraic* if a_R is pre-algebraic and satisfies

$$\mu_{a_R}(\mathbf{t}) = \mu_a(\mathbf{t})_R, \tag{8}$$

equivalently,

$$\mathfrak{N}(a_R) = \mathfrak{N}(a) \otimes R, \tag{9}$$

for all $R \in k$-**alg**. The equivalence of (8) and (9) follows from the fact that $\mathfrak{N}(a)$ and $\mathfrak{N}(a_R)$ are, respectively, the principal ideals generated by $\mu_a(\mathbf{t})$ and $\mu_{a_R}(\mathbf{t})$. Of course, if k is a field, the three notions just introduced all coincide with the usual definition of an algebraic element. They hold for all $a \in J$ provided J is finite-dimensional over k.

1.5. Proposition. *Let $a \in J$ and $R \in k$-**alg** and denote by $\varrho\colon k \to R$ the ring homomorphism making R a k-algebra.*

(a) *a is algebraic if and only if $M(a)$ is a finitely generated and projective k-module and a pure submodule of J^2.*

(b) *If J is finitely generated and projective as a k-module, then a is algebraic if and only if $M(a)$ is a direct summand of J^2.*

(c) *Let a be algebraic. Then a_R is algebraic as well, and the homomorphisms φ, u'_R and η of Lemma 1.3 are isomorphisms. The degree functions of a and a_R are related by*

$$(\deg a_R)(\mathfrak{q}) = (\deg a)(\varrho^{-1}(\mathfrak{q})) \tag{1}$$

for all $\mathfrak{q} \in \operatorname{Spec}(R)$.

(d) *Conversely, let R be faithfully flat over k and assume that a_R is algebraic. Then a is algebraic.*

Proof. (a) If a is algebraic then it is in particular pre-algebraic, so $M(a)$ is finitely generated and projective by 1.4.2. Because of 1.4.9, the map φ of 1.3(b) is an isomorphism. Hence by 1.3.3, $u_R\colon M(a) \otimes R \to J_R^2$ is injective for all $R \in k$-**alg**, so $M(a)$ is pure by 0.15(a). Conversely, suppose $M(a)$ is finitely generated and projective and pure, and let $R \in k$-**alg**. Then $u_R\colon M(a) \otimes R \to J_R^2$ is injective, so $u'_R\colon M(a) \otimes R \to M(a_R)$ is an isomorphism. Finitely generated projective modules remain so under base change. Hence $M(a_R)$ is finitely generated and projective, so a_R is pre-algebraic by 1.4.2. Since in particular a itself is pre-algebraic, φ is injective. By 1.3.3, φ is surjective as well, so 1.4.9 holds.

(b) Direct summands of finitely generated and projective modules are themselves finitely generated and projective and of course pure, and pure submodules of projective modules are direct summands, by 0.15(d).

(c) From the definition of an algebraic element it is evident that a_R is algebraic along with a. The fact that φ, u'_R and η are isomorphisms follows from the proof of (a) and 1.3.4. Formula (1) follows from the definition of the degree function in 1.4.5 and 0.8.3.

(d) We use the characterization given in (a). By Lemma 1.3(d), $u'_R\colon M(a)\otimes R \to M(a_R)$ is an isomorphism. Since $M(a_R)$ is finitely generated and projective, the same is true of $M(a)$ by [**3**, I, §3.6, Prop. 12]. Purity of $M(a)$ follows from that of $M(a_R)$ by 0.15(c).

1.6. Power-associativity. An element $a \in J$ is called *power-associative* if the kernel $\mathfrak{K}(a) = \operatorname{Ker}(j_a)$ of the evaluation map $j_a\colon k[\mathbf{t}] \to J$ (cf. 1.1) is an ideal of the associative algebra $k[\mathbf{t}]$ (and not just a Jordan ideal). By Lemma 1.2, equivalent conditions are that $\mathfrak{N}(a) = \mathfrak{K}(a)$, or that $\mathrm{pr}_1\colon M(a) \to k[a]$ or $\pi\colon E(a) \to J$ be injective. We will say an element $a \in J$ is *strictly power-associative* if a_R is power-associative for all $R \in k$-**alg**. Any one of the following conditions is sufficient to guarantee that every element of J is power-associative:

(a) J has no 2-torsion,
(b) J contains no absolute zero divisors,

and any one of the following conditions implies that every element of J is strictly power-associative:

(c) $2 \in k^\times$,
(d) $J = B^+$ is the Jordan algebra associated with an associative or alternative algebra B.

Indeed, (a) and (b) follow from Lemma 1.2, and the rest is clear.

Let v: $k[a] \subset J$ be the inclusion, let $R \in k$-**alg** and denote by v'_R: $k[a] \otimes R \to R[a_R]$ the induced map. Then we have a commutative diagram of surjective maps

$$\begin{array}{ccc} M(a) \otimes R & \xrightarrow{\mathrm{pr}_1 \otimes \mathrm{Id}_R} & k[a] \otimes R \\ {\scriptstyle u'_R}\downarrow & & \downarrow{\scriptstyle v'_R} \\ M(a_R) & \xrightarrow[\mathrm{pr}_1]{} & R[a_R] \end{array} \tag{1}$$

where u'_R is as in Lemma 1.3. By 0.15(a), $k[a]$ is pure if and only if, for all $R \in k$-**alg**, v'_R is injective, while $M(a)$ is pure if and only if all u'_R are injective. Also, all top maps are bijective if and only if a is power-associative, and all bottom maps are bijective if and only if a is strictly power-associative. Thus we see that

$$\begin{aligned} &a \textit{ is power-associative and } k[a] \textit{ is pure} \quad \Longleftrightarrow \\ &a \textit{ is strictly power-associative and } M(a) \textit{ is pure.} \end{aligned} \tag{2}$$

If k is a field, the purity conditions are automatically satisfied, so power-associativity of an element a implies strict power-associativity of a, and by (c), only the case where the characteristic is 2 is of interest. But over rings there may exist power-associative elements which are not strictly power-associative.

Example. Let A be the associative commutative algebra over $\mathbb{Z}$ obtained from $\mathbb{Q}[\mathbf{t}]/(\mathbf{t}^4)$ by restricting scalars to $\mathbb{Z}$. Let $a := \mathrm{can}(\mathbf{t}) \in A$ and $b := a^2/2$ and define $J = \mathbb{Z}1 \oplus \mathbb{Z}a \oplus \mathbb{Z}b \oplus \mathbb{Z}a^3 \subset A$. Using the relations $a^2 = 2b$, $a \circ b = a^3$, $b^2 = 0$, one shows easily that J is a Jordan subalgebra of A; it is not an associative subalgebra of A because $ab \notin J$. Obviously, J is free of rank 4 as a $\mathbb{Z}$-module. Since J has no 2-torsion, every element of J is power-associative. But the element a is not strictly power-associative, because for $R = \mathbb{Z}/2\mathbb{Z}$ we have $a_R^2 = 0 \neq a_R^3$. We also see that $k[a]$ is not pure, because $2b \in k[a]$ but $b \notin k[a]$ (cf. 0.15(e)). On the other hand, $M(a)$ is a direct summand of J^2 (hence pure), a complementary submodule being spanned by $\begin{pmatrix} b \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 0 \\ a \end{pmatrix}$, $\begin{pmatrix} 0 \\ b \end{pmatrix}$. In particular, a is algebraic. The algebra J is also an example of a special but not strictly special Jordan algebra: It loses speciality after the base change from $\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$.

Remark. K. McCrimmon [**23**] has defined a Jordan algebra J over a field K to be power-associative if every element of J is power-associative. As remarked above, every element of J is then even strictly power-associative. But it is not clear if all elements of all field extensions $J \otimes_K L$ are power-associative, even when K is infinite.

In the presence of (strict) power-associativity, the conditions that an element a be pre-algebraic or algebraic can be reformulated as follows:

1.7. Corollary. (a) *Let $a \in J$ be power-associative. Then a is pre-algebraic if and only if $k[a]$ is finitely generated and projective.*

(b) *Let $a \in J$ be strictly power-associative. Then a is algebraic if and only if $k[a]$ is finitely generated and projective and a pure submodule of J.*

(c) *Let $a \in J$ be strictly power-associative and let J be finitely generated and projective. Then a is algebraic if and only if $k[a]$ is a direct summand of J.*

Proof. (a) Immediate from 1.4.2 because pr_1: $M(a) \to k[a]$ is now an isomorphism of k-modules.

(b) By strict power-associativity, the horizontal arrows in 1.6.1 are isomorphisms. Now the assertion follows from Prop. 1.5(a).

(c) This is immediate from (b) and Prop. 1.5(b).

Example. The reader may find it instructive to use (c) for showing that the element $a \in J = B^+$ of 1.4 is not algebraic. Here $k[a] = \mathbb{Z}1 \oplus \mathbb{Z}a \oplus \mathbb{Z}2b \oplus \mathbb{Z}2ab$ is not a direct summand of J, because $J/k[a] \cong \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^2$ is not projective as a $\mathbb{Z}$-module.

1.8. Example: Idempotents. We claim that an idempotent $e = e^2 \in J$ is strictly power-associative. Since e_R remains an idempotent in J_R for all $R \in k$-**alg**, it suffices to show e power-associative. Now $e^2 = e$ implies $e^3 = U_e e = U_e e^2 = e^4 = (e^2)^2 = e$, and then $e^i = e$ for all $i \geqslant 1$. Hence $e^{[i]} = \begin{pmatrix} e \\ e \end{pmatrix}$ for all $i \geqslant 1$, so $M(e) = k\begin{pmatrix} 1_J \\ e \end{pmatrix} + k\begin{pmatrix} e \\ e \end{pmatrix}$. If $w = \lambda\begin{pmatrix} 1_J \\ e \end{pmatrix} + \mu\begin{pmatrix} e \\ e \end{pmatrix} \in M(e)$ and $\mathrm{pr}_1(w) = \lambda 1_J + \mu e = 0$, then applying U_e to this equation yields $\lambda e + \mu e = 0$ and therefore $w = 0$. Hence $\mathrm{pr}_1\colon M(e) \to J$ is injective, as desired.

Now let us assume that J is finitely generated and projective as a k-module. We show that e is algebraic and compute its minimum polynomial. By 1.7(c), e will be algebraic if and only if $k[e]$ is a direct summand of J. Consider the Peirce decomposition $J = J_2 \oplus J_1 \oplus J_0$ of J with respect to e. Then $1_J = e \oplus (1_J - e) \in J_2 \oplus J_0$, and $k[e] = k \cdot 1_J + k \cdot e = k \cdot e \oplus k \cdot (1_J - e)$, so it suffices to show that $k \cdot e$ and $k \cdot (1 - e)$ are direct summands of J_2 and J_0, respectively. This follows from Lemma 0.5 since e and $1 - e$ are idempotents (in fact, the unit elements) of J_2 and J_0. Using the notations of 0.2, we define subsets of $S = \mathrm{Spec}(k)$ by

$$\begin{aligned}
\mathfrak{p} \in S_0 &\iff 1_J(\mathfrak{p}) = 0 \iff J(\mathfrak{p}) = \{0\},\\
\mathfrak{p} \in S_1' &\iff e(\mathfrak{p}) = 0 \neq 1_J(\mathfrak{p}),\\
\mathfrak{p} \in S_1'' &\iff e(\mathfrak{p}) = 1_J(\mathfrak{p}) \neq 0,\\
\mathfrak{p} \in S_2 &\iff 0 \neq e(\mathfrak{p}) \neq 1_J(\mathfrak{p}).
\end{aligned}$$

These sets are open and closed, disjoint, and their union is S. Indeed, let γ, δ and ε be the support idempotents of 1_J, $1_J - e$ and e, respectively (cf. 0.4 and 0.5). Then these subsets correspond to the following orthogonal idempotents with sum 1_k: $\varepsilon_0 = 1 - \gamma$, $\varepsilon_1' = \delta(1 - \varepsilon)$, $\varepsilon_1'' = \varepsilon(1 - \delta)$, and $\varepsilon_2 = \varepsilon\delta$. The minimum polynomial of e satisfies

$$\mu_e(\mathbf{t})_{\mathfrak{p}} = \left\{\begin{array}{ll} 1 & \text{if } \mathfrak{p} \in S_0 \\ \mathbf{t} & \text{if } \mathfrak{p} \in S_1' \\ \mathbf{t} - 1 & \text{if } \mathfrak{p} \in S_1'' \\ \mathbf{t}^2 - \mathbf{t} & \text{if } \mathfrak{p} \in S_2 \end{array}\right\}.$$

Put $S_1 = S_1' \cup S_1''$ and $\varepsilon_1 = \varepsilon_1' + \varepsilon_1''$. Then the degree function of e takes the value i on S_i, and the minimum polynomial of e and its copolynomial are given by

$$\mu_e(\mathbf{t}) = \varepsilon_0 + \varepsilon_1(\mathbf{t} - \varepsilon) + \varepsilon_2(\mathbf{t}^2 - \mathbf{t}), \qquad \check{\mu}_e(\mathbf{t}) = 1 - \varepsilon\mathbf{t}, \tag{1}$$

where of course some of the ε_i may be zero. We note the special cases $e = 1_J$ and $e = 0$:

$$\mu_{1_J}(\mathbf{t}) = \gamma(\mathbf{t} - 1) + (1 - \gamma), \qquad \mu_0(\mathbf{t}) = \gamma\mathbf{t} + (1 - \gamma). \tag{2}$$

When J is faithful as a k-module, i.e., when 1_J is unimodular or $\gamma = 1$ (cf. 0.3.2), these formulas simplify to $\mu_{1_J}(\mathbf{t}) = \mathbf{t} - 1$ and $\mu_0(\mathbf{t}) = \mathbf{t}$.

1.9. Lemma. (a) *Let $\lambda \in k^\times$ be a unit. Then an element $a \in J$ is (pre-)algebraic if and only if λa is so, and in this case,*

$$\mu_{\lambda a}(\mathbf{t}) = \lambda^{\deg a}\mu_a(\lambda^{-1}\mathbf{t}), \qquad \check{\mu}_{\lambda a}(\mathbf{t}) = \check{\mu}_a(\lambda\mathbf{t}). \tag{1}$$

(b) *Let $a, b \in J^\times$ be invertible and consider the isotopes $J^{(b)}$ and $J^{(a)}$. Then a is (pre-)algebraic in $J^{(b)}$ if and only if b is (pre-)algebraic in $J^{(a)}$, and then the respective minimum polynomials are related by*

$$\mu_a^{(b)}(\mathbf{t}) = \mu_b^{(a)}(\mathbf{t}). \tag{2}$$

Proof. (a) Put $\sigma_\lambda = \begin{pmatrix} \mathrm{Id} & 0 \\ 0 & \lambda\mathrm{Id} \end{pmatrix} \in \mathrm{GL}(J^2)$. From 1.1.1, we have $(\lambda a)^{[i]} = \lambda^i \sigma_\lambda\big(a^{[i]}\big)$ and hence $\sigma_\lambda(M(a)) = M(\lambda a)$. Thus $M(\lambda a)$ is finitely generated and projective (and pure) if and only if $M(a)$ is so. In view of 1.4.2 and Prop. 1.5(a), this proves the statement about λa being (pre-)algebraic. The diagram

$$\begin{array}{ccc} M(a) & \xrightarrow{\lambda\zeta_a} & M(a) \\ {\scriptstyle\sigma_\lambda}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\sigma_\lambda} \\ M(\lambda a) & \xrightarrow[\zeta_{\lambda a}]{} & M(\lambda a) \end{array}$$

is easily seen to commute. Hence by 1.4.4, $\check\mu_{\lambda a}(\mathbf{t}) = \det(\mathrm{Id}_{M(\lambda a)} - \mathbf{t}\zeta_{\lambda a}) = \det(\mathrm{Id}_{M(a)} - \lambda\mathbf{t}\zeta_a) = \check\mu_a(\lambda\mathbf{t})$, and then the first formula of (1) follows by 0.9.4.

(b) We indicate quantities computed in $J^{(v)}$ by a superscript (v); in particular, the ith power of an element x in the isotope $J^{(v)}$ is $x^{(i,v)}$. Induction shows

$$U_a b^{(i,a)} = a^{(i+1,b)} \quad \text{and} \quad U_b^{-1} b^{(i+1,a)} = a^{(i,b)}$$

for all $i \in \mathbb{N}$, equivalently,

$$\begin{pmatrix} 0 & U_b^{-1} \\ U_a & 0 \end{pmatrix} \begin{pmatrix} b^{(i,a)} \\ b^{(i+1,a)} \end{pmatrix} = \begin{pmatrix} a^{(i,b)} \\ a^{(i+1,b)} \end{pmatrix}. \tag{3}$$

Now $\phi := \begin{pmatrix} 0 & U_b^{-1} \\ U_a & 0 \end{pmatrix} \in \mathrm{GL}(J^2)$, and (3) says that ϕ induces an isomorphism ϕ: $M^{(a)}(b) \to M^{(b)}(a)$ of k-modules. One easily checks that the diagram

$$\begin{array}{ccc} M^{(a)}(b) & \xrightarrow{\zeta_b^{(a)}} & M^{(a)}(b) \\ {\scriptstyle\phi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\phi} \\ M^{(b)}(a) & \xrightarrow[\zeta_a^{(b)}]{} & M^{(b)}(a) \end{array}$$

is commutative. Now similar arguments as before complete the proof.

1.10. Invertibility. Let $a \in J$ be invertible. Then we define $a^{[i]}$ for all $i \in \mathbb{Z}$ by 1.1.1 and extend h_a to a map h_a: $k[\mathbf{t}, \mathbf{t}^{-1}] \to J^2$. It is immediately checked that $\theta_a \in \mathrm{GL}(J^2)$ with inverse

$$\theta_a^{-1} = \begin{pmatrix} 0 & U_a^{-1} \\ \mathrm{Id} & 0 \end{pmatrix}, \tag{1}$$

and that 1.2.2 holds for all $i \in \mathbb{Z}$. Thus J^2 becomes a module over the Laurent polynomial ring $k[\mathbf{t}, \mathbf{t}^{-1}]$ by letting again $\mathbf{t}$ act via θ_a, and formula 1.2.3 then holds for all $f(\mathbf{t}), g(\mathbf{t}) \in k[\mathbf{t}, \mathbf{t}^{-1}]$. The analogue of the usual formula $(a^{-1})^i = (a^i)^{-1}$ is

$$(a^{-1})^{[i]} = \omega\big(a^{[-i-1]}\big) \quad (i \in \mathbb{Z}), \tag{2}$$

where $\omega = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix} \in \mathrm{GL}(J^2)$ is the switch of factors. This is easily verified. We finally note that, when a is invertible, $M(a)$ is not necessarily a $k[\mathbf{t}, \mathbf{t}^{-1}]$-submodule of J^2. Indeed, 1.2.2 and the fact that $M(a)$ is spanned by all $a^{[i]}$, $i \geqslant 0$, implies that

$$\theta_a^{-1} \text{ stabilizes } M(a) \quad \iff \quad \theta_a^{-1}(a^{[0]}) = a^{[-1]} \in M(a). \tag{3}$$

1.11. Lemma. *For any polynomial* $f(\mathbf{t}) \in k[\mathbf{t}]$ *define* $f^\sharp(\mathbf{t})$ *by*

$$\mathbf{t}f^\sharp(\mathbf{t}) = f(\mathbf{t}) - f(0). \tag{1}$$

(a) *If* $a \in J$ *satisfies a polynomial* $f(\mathbf{t})$ *with invertible constant term then* a *is invertible in* J*, with inverse*

$$a^{-1} = -\frac{f^\sharp(a)}{f(0)}. \tag{2}$$

Moreover, $\theta_a^{-1} \in \mathrm{End}(J^2)$ *stabilizes* $M(a)$*, and* $M(a^{-1}) \subset \omega\big(M(a)\big)$ *where* $\omega \in \mathrm{GL}(J)$ *is as in* 1.10*. If in addition* a *is integral, then*

$$M(a^{-1}) = \omega\big(M(a)\big). \tag{3}$$

(b) *Suppose* $a \in J$ *is algebraic. Then* $a \in J^\times$ *if and only if* $\mu_a(0) \in k^\times$*. In this case,* a^{-1} *is algebraic as well, of the same degree as* a*, formula* (3) *holds, and the minimum polynomial of* a^{-1} *is*

$$\mu_{a^{-1}}(\mathbf{t}) = \frac{\check{\mu}_a(\mathbf{t})}{\mu_a(0)}. \tag{4}$$

Proof. (a) For fields, (2) is proved in [**16**, Sec. 1, Lemma 1], and the proof is identical in case of a base ring. For the convenience of the reader, we repeat the argument. Squaring (1) gives $\mathbf{t}^2 f^\sharp(\mathbf{t})^2 = f(\mathbf{t})^2 - 2f(0)f(\mathbf{t}) + f(0)^2$ and applying j_a to this yields $U_a f^\sharp(a)^2 = f(0)^2 \cdot 1_J$, or $U_a b^2 = 1_J$ where $b := -f^\sharp(a)/f(0)$. Hence 1_J is in the range of U_a so a is invertible. Now multiply (1) with $\mathbf{t}^2$ to obtain $\mathbf{t}^2 f^\sharp(\mathbf{t}) = \mathbf{t}f(\mathbf{t}) - \mathbf{t}f(0)$. As $\mathbf{t}f(\mathbf{t}) \in \mathfrak{N}(a)$, applying j_a yields $U_a f^\sharp(a) = -f(0)a$ or $U_a b = a$ and therefore $b = U_a^{-1} a = a^{-1}$.

We show that θ_a^{-1} stabilizes $M(a)$ by verifying the condition of 1.10.3. Apply h_a to (1) and use 1.2.3. Then $\theta_a \cdot h_a(f^\sharp(\mathbf{t})) = -f(0)a^{[0]}$, and hence $\theta_a^{-1} \cdot a^{[0]} = -f(0)^{-1} h_a(f^\sharp(\mathbf{t})) \in M(a)$, as desired. Thus all $a^{[i]}$ for $i < 0$ lie in $M(a)$. From 1.10.2, it follows that $M(a^{-1}) = \omega\Big(h_a\big(\sum_{j\geqslant 1} k \cdot \mathbf{t}^{-j}\big)\Big) \subset \omega\big(M(a)\big)$.

Now assume a is integral, so it satisfies a monic polynomial, say $a^{[n]} + \lambda_1 a^{[n-1]} + \cdots + \lambda_n a^{[0]} = 0$. Applying θ_a^{-n-1} to this and using 1.2.2 yields $\sum_{i=0}^n \lambda_i a^{[-i-1]} = 0$, and by 1.10.2, we obtain $\sum_{i=0}^n \lambda_i (a^{-1})^{[i]} = 0$, so a^{-1} satisfies the polynomial $1 + \lambda_1 \mathbf{t} + \cdots + \lambda_n \mathbf{t}^n$ with constant term 1. Thus we may switch the roles of a and a^{-1} and have $M(a) \subset \omega\big(M(a^{-1})\big)$. Now it follows from $\omega^2 = \mathrm{Id}$ that (3) holds.

(b) For the first statement, and by what we proved in (a), it remains to show that $a \in J^\times$ implies $\mu_a(0) \in k^\times$. Assume this is not the case. Then there exists a maximal ideal $\mathfrak{m} \subset k$ such that $\mu_a(0) \in \mathfrak{m}$. Let $K := k/\mathfrak{m}$. By 1.4.8, we have $\mu_{a_K}(0) = \mu_a(0) \otimes 1_K = 0$, whence a_K is not invertible in J_K by [**16**, Sec. 1, Lemma 1]. On the other hand, invertible elements remain so under base change, contradiction.

Now let a be algebraic and invertible. Then a is in particular integral and satisfies $\mu_a(\mathbf{t})$ whose constant term is invertible. Hence part (a) shows that (3) holds. Since $\omega \in \mathrm{GL}(J^2)$, it follows from (3) that $M(a^{-1})$ is finitely generated and projective and pure in J^2, so a^{-1} is algebraic by Prop. 1.5(a). From 1.10.2 one sees that the diagram

$$\begin{array}{ccc} M(a) & \xrightarrow{(\zeta_a)^{-1}} & M(a) \\ {\scriptstyle\omega}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\omega} \\ M(a^{-1}) & \xrightarrow[\zeta_{a^{-1}}]{} & M(a^{-1}) \end{array}$$

commutes. Hence $\mu_{a^{-1}}(\mathbf{t}) = \det(\mathbf{t}\mathrm{Id}_{M(a^{-1})} - \zeta_{a^{-1}}) = \det(\mathbf{t}\mathrm{Id}_{M(a)} - (\zeta_a)^{-1}) = \det(-\zeta_a)^{-1} \cdot \det(\mathrm{Id} - \mathbf{t}\zeta_a) = \mu_a(0)^{-1} \cdot \check{\mu}_a(\mathbf{t})$. Finally, $\deg a = \deg a^{-1}$ follows from (4) and 0.9.6.

1.12. Lemma. *Let J be a finitely generated and projective Jordan algebra over k and $a \in J$. Then a is algebraic of degree d if and only if*

$$a^{[0]} \wedge \cdots \wedge a^{[d-1]} \in \bigwedge^d J^2 \quad \textit{is unimodular, and} \tag{1}$$

$$a^{[0]} \wedge \cdots \wedge a^{[d]} = 0. \tag{2}$$

Proof. "Only if": As remarked in 1.4, $M(a)$ is free with basis $a^{[0]}, \ldots, a^{[d-1]}$. By 1.5(b), it is a direct summand of J^2, and obviously $a^{[d]} \in M(a)$. Thus (1) and (2) follow from Lemma 0.6.

"If": From (1) and (2) and Lemma 0.6, it follows that the span, say N, of $a^{[0]}, \ldots, a^{[d-1]}$ is a free direct summand of J^2 with basis $a^{[0]}, \ldots, a^{[d-1]}$, and that $a^{[d]} \in N$. Now 1.2.2 implies that N contains all $a^{[i]}$ and hence that $N = M(a)$. By 1.5(b), a is algebraic and obviously of degree d.

1.13. Definition. For a unital Jordan algebra J over k and $d \in \mathbb{N}$, we define the following subsets of J:

$$J_{\mathrm{alg}} := \{a \in J : a \ \text{ is algebraic}\}, \qquad J_{\mathrm{alg},d} := \{a \in J_{\mathrm{alg}} : \deg a = d\}.$$

Now let $\mathbf{J} = J_{\mathbf{a}}$ be the functor from k-**alg** to the category of sets defined by J as in 0.12, i.e., $\mathbf{J}(R) = J \otimes R$, for all $R \in k$-**alg**. We put

$$\mathbf{J}_{\mathrm{alg}}(R) := (J_R)_{\mathrm{alg}}, \qquad \mathbf{J}_{\mathrm{alg},d}(R) := (J_R)_{\mathrm{alg},d},$$

for all $R \in k$-**alg** and denote by $\mathbb{N}_k$ the constant functor determined by $\mathbb{N}$ as in 0.7(c).

1.14. Proposition. (a) *$\mathbf{J}_{\mathrm{alg}}$ and $\mathbf{J}_{\mathrm{alg},d}$ are hard subsheaves of $\mathbf{J}$ in the sense of* [**6**, III, §1, 3.3]*, in particular, they are local functors. The degree function $a \mapsto \deg a$ associated to an algebraic element a defines a morphism $\mathbf{deg}\colon \mathbf{J}_{\mathrm{alg}} \to \mathbb{N}_k$ such that $\mathbf{J}_{\mathrm{alg},d} = \mathbf{deg}^{-1}(\{d\}_k)$, for all $d \in \mathbb{N}$. The $\mathbf{J}_{\mathrm{alg},d}$ are open subfunctors of $\mathbf{J}_{\mathrm{alg}}$ which cover $\mathbf{J}_{\mathrm{alg}}$.*

(b) *Suppose J is finitely generated and projective as a k-module and let $P^{(n)} := \bigwedge^n J^2$. Then $\bigwedge^n (J_R^2) \cong (P^{(n)})_R$ for all $R \in k$-**alg**, and hence there are morphisms $p_n\colon \mathbf{J} \to P_{\mathbf{a}}^{(n)}$ given by $x \mapsto x^{[0]} \wedge \cdots \wedge x^{[n-1]}$, for all $x \in J_R$, $R \in k$-**alg**. Let $P_{\mathbf{u}}^{(n)}$ be the open subscheme of unimodular elements of $P_{\mathbf{a}}^{(n)}$, cf.* 0.12*. Then $\mathbf{J}_{\mathrm{alg}}$ and the $\mathbf{J}_{\mathrm{alg},d}$ are finitely presented quasi-affine k-schemes, given by*

$$\mathbf{J}_{\mathrm{alg},d} = p_d^{-1}\big(P_{\mathbf{u}}^{(d)}\big) \cap p_{d+1}^{-1}(0) \quad \textit{and} \qquad \mathbf{J}_{\mathrm{alg}} = \coprod_{d=0}^{r} \mathbf{J}_{\mathrm{alg},d},$$

where $r = \max \operatorname{rk} J^2$.

Proof. (a) Let $\mathbf{X} = \mathbf{J}_{\mathrm{alg}}$ or $\mathbf{X} = \mathbf{J}_{\mathrm{alg},d}$. We first show that $\mathbf{X}$ is a subfunctor of $\mathbf{J}$, i.e., that, for all homomorphisms $\varrho\colon R \to S$ of k-algebras, $\mathbf{J}(\varrho)\big(\mathbf{X}(R)\big) \subset \mathbf{X}(S)$. Since $\varrho\colon R \to S$ makes S an R-algebra, $a_S \in \mathbf{X}(S)$ follows from Prop. 1.5(c), (applied to J_R and S instead of J and R). To say that $\mathbf{X}$ is a hard sheaf just means that it commutes with finite direct products (which is obvious), and that for all $R \in k$-**alg** and all faithfully flat R-algebras S, the sequence of sets

$$\mathbf{X}(R) \longrightarrow \mathbf{X}(S) \rightrightarrows \mathbf{X}(S \otimes_R S)$$

is exact, where the arrows are induced from $R \to S$ and the two embeddings $S \to S \otimes_R S$ into the first and second factor. After changing the base ring from k to R, this is precisely the statement of Prop. 1.5(d).

It is easy to check that there is a morphism (i.e., a natural transformation of functors) $\mathbf{deg}\colon \mathbf{J}_{\mathrm{alg}} \to \mathbb{N}_k$ such that $\mathbf{deg}_R\colon \mathbf{J}_{\mathrm{alg}}(R) \to \mathbb{N}_k(R)$ is given by

$$\big(\mathbf{deg}_R(a)\big)(\mathfrak{p}) = (\deg a)(\mathfrak{p}),$$

for all $R \in k\text{-}\mathbf{alg}$, $a \in \mathbf{J}_{\mathrm{alg}}(R)$, $\mathfrak{p} \in \mathrm{Spec}(R)$. Clearly $a \in \mathbf{J}_{\mathrm{alg},d}(R)$ if and only if the function $\mathbf{deg}_R(a)\colon \mathrm{Spec}(R) \to \mathbb{N}$ is constant equal to d. This proves that $\mathbf{deg}^{-1}(\{d\}_k) = \mathbf{J}_{\mathrm{alg},d}$. Finally, if K is a field then $\mathrm{Spec}(K)$ is a one-point set, so the function $\mathbf{deg}_K(a)$ is constant, for every $a \in \mathbf{J}_{\mathrm{alg}}(K)$ (this is just saying that an algebraic element over a field has a well-defined (constant) degree). It follows that $\mathbf{J}_{\mathrm{alg}}(K)$ is the disjoint union of the $\mathbf{J}_{\mathrm{alg},d}(K)$, proving the last assertion.

(b) Let $r = \max\{\mathrm{rk}_{\mathfrak{p}}(J^2) : \mathfrak{p} \in \mathrm{Spec}(k)\}$. Then clearly $\mathbf{J}_{\mathrm{alg},d} = \emptyset$ for $d > r$. Hence, to prove the statement for $\mathbf{J}_{\mathrm{alg}}$, it suffices to show that the $\mathbf{J}_{\mathrm{alg},d}$ are finitely presented quasi-affine schemes. Since J is finitely generated and projective so are the exterior powers $P^{(n)}$, and hence they define affine finitely presented schemes $P^{(n)}_{\mathbf{a}}$ and open quasi-affine finitely presented subschemes $P^{(n)}_{\mathbf{u}}$ of unimodular elements. Also, exterior powers commute with base change, so the natural homomorphism $\bigwedge^n(J^2_R) \to P^{(n)}_R$ is an isomorphism. This proves the existence of p_n. Now Lemma 1.12 (which of course holds in all base ring extensions as well) shows that $\mathbf{J}_{\mathrm{alg},d} = \mathbf{Z} \cap \mathbf{U}$ where $\mathbf{Z} = p^{-1}_{d+1}(0)$ and $\mathbf{U} = p^{-1}_d(P^{(d)}_{\mathbf{u}})$ are, respectively, closed and open finitely presented subschemes of $\mathbf{J}$ [**6**, I, §3]. This completes the proof.

Remark. Let in particular k be a field and J finite-dimensional. Then every element of J is algebraic, so (b) shows J is the disjoint union of the $J_{\mathrm{alg},d}$. Over a ring, the union is still disjoint, but there may be non-algebraic elements.

2. Generically algebraic algebras

2.1. The function $\deg J$**.** In this section, J always denotes a unital quadratic Jordan algebra over an arbitrary ring k which is finitely generated and projective as a k-module, and $\mathbf{J} = J_{\mathbf{a}}$ the affine k-scheme defined by J as in 0.12. For every prime ideal $\mathfrak{p} \in \mathrm{Spec}(k)$, $J(\mathfrak{p}) = J \otimes \boldsymbol{\kappa}(\mathfrak{p})$ is finite-dimensional and therefore generically algebraic over $\boldsymbol{\kappa}(\mathfrak{p})$ [**16**, Sec. 2, Th. 2]. In particular, it has a well-defined generic minimum polynomial whose degree is, by definition, the degree $\deg J(\mathfrak{p})$ of $J(\mathfrak{p})$. We thus have a function $\deg J\colon \mathrm{Spec}(k) \to \mathbb{N}$ given by

$$(\deg J)(\mathfrak{p}) := \deg J(\mathfrak{p}).$$

This function is lower semicontinuous (where $\mathbb{N}$ has the discrete topology). Indeed, let $p_d\colon \mathbf{J} \to P^{(d)}_{\mathbf{a}}$ be as in 1.14 and let $\mathbf{Y} = p_d^{-1}(P^{(d)}_{\mathbf{u}})$. Then $\mathbf{Y}$ is open in $\mathbf{J}$. Let $\deg J(\mathfrak{p}) = d$ and let K be an algebraic closure of $\boldsymbol{\kappa}(\mathfrak{p})$. Then it follows from [**16**, Section 3] that there exists $x \in J_K$ such that $x^{[0]}, \dots, x^{[d-1]}$ are linearly independent, i.e., $\mathbf{Y}(K) \neq \emptyset$. Let $|\mathbf{Y}|$ be the open subset of $\mathrm{Spec}(A)$ underlying the open subscheme $\mathbf{Y}$, cf. [**6**, I, §1, No. 4]. Then by 0.12.1, $U := p(|\mathbf{Y}|) \subset \mathrm{Spec}(k)$ is an open neighbourhood of $\mathfrak{p}$, and for all $\mathfrak{q} \in U$ the fibre of $\mathbf{Y}$ over $\mathfrak{q}$ is not empty. Thus there exists $y \in J \otimes L$ where L is an algebraic closure of $\boldsymbol{\kappa}(\mathfrak{q})$, for which $y \in \mathbf{Y}(L)$, i.e., such that $y^{[0]}, \dots, y^{[d-1]}$ are linearly independent, and hence the degree of $J(\mathfrak{q})$ is at least d.

The degree of J behaves as expected under base change, namely,

$$\deg J_R = (\deg J) \circ \mathrm{Spec}(\varrho) \quad (R \in k\text{-}\mathbf{alg}), \tag{1}$$

where $\varrho\colon k \to R$ is the homomorphism making R a k-algebra. Indeed, if $\mathfrak{q} \in \mathrm{Spec}(R)$ and $\mathfrak{p} = \varrho^{-1}(\mathfrak{q}) \in \mathrm{Spec}(k)$, then $\boldsymbol{\kappa}(\mathfrak{q})$ is, via ϱ, an extension field of $\boldsymbol{\kappa}(\mathfrak{p})$, so by the invariance of the generic minimum polynomial of a Jordan algebra over a field under field extension, $\deg J(\mathfrak{p}) = \deg J(\mathfrak{p}) \otimes \boldsymbol{\kappa}(\mathfrak{q}) = \deg J_R(\mathfrak{q})$. — For later use, we note:

$$a \in J \quad \text{algebraic} \quad \Longrightarrow \quad \deg a \leqslant \deg J. \tag{2}$$

Indeed, for every $\mathfrak{p} \in \mathrm{Spec}(k)$, the degree of a at $\mathfrak{p}$ is the degree of $\mu_a(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}$ by 1.4.5, and by 1.4.8, this is the same as $\mu_{a(\mathfrak{p})}(\mathbf{t})$, which divides the generic minimum polynomial of $J(\mathfrak{p})$.

2.2. Definition. Let J be as above, let $A = \mathcal{O}(J)$ be the affine algebra of $\mathbf{J}$ (cf. 0.12), and let $f(\mathbf{t}) \in A[\mathbf{t}]$ be locally monic. Using the notations of 0.13, we say J *satisfies* $f(\mathbf{t})$ if, for all $R \in k$-**alg**, every $x \in \mathbf{J}(R)$ satisfies the polynomial $f(\mathbf{t}; x)$, i.e., $f(\mathbf{t}; x) \in \mathfrak{N}(x)$. Obviously, this condition is stable under base change, i.e., if J satisfies $f(\mathbf{t})$ then J_R satisfies $f(\mathbf{t})_R$, for all $R \in k$-**alg**. In particular, $J(\mathfrak{p})$ satisfies $f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}$ for all $\mathfrak{p} \in \mathrm{Spec}(k)$, so that $f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}$ is a multiple of the generic minimum polynomial of $J(\mathfrak{p})$. Thus by 0.13.4 and the definition of the degree function of J, we have:

$$J \text{ satisfies } f(\mathbf{t}) \quad \Longrightarrow \quad \deg J \leqslant \overline{\deg}\, f(\mathbf{t}). \tag{1}$$

Note that such f always exist. For example, $f(\mathbf{t}; x) = \det(\mathbf{t}^2\mathrm{Id} - U_x)$ is locally monic, and by the Cayley-Hamilton Theorem, $f(U_x; x) = 0$ in $\mathrm{End}(J_R)$ for all $R \in k$-**alg**. Hence $0 = f(U_x; x) \cdot 1_J = f(U_x; x) \cdot x$, cf. [**16**, Section 1, Lemma 2]. However, it is in general not true that J satisfies a locally monic f for which equality holds in (1). This leads to the following definition:

J is called *generically algebraic* if there exists a locally monic polynomial $m(\mathbf{t}) \in A[\mathbf{t}]$ such that

(i) J satisfies $m(\mathbf{t})$, i.e., for all $R \in k$-**alg** and all $x \in \mathbf{J}(R)$, x satisfies the polynomial $m(\mathbf{t}; x)$,

(ii) $\deg J = \overline{\deg}\, m(\mathbf{t})$; equivalently, that for all prime ideals $\mathfrak{p} \in \mathrm{Spec}(k)$, $m(\mathbf{t}) \otimes_k 1_{\boldsymbol{\kappa}(\mathfrak{p})}$ is the generic minimum polynomial of $J(\mathfrak{p})$.

An associative or alternative algebra B will be called generically algebraic if the associated Jordan algebra B^+ has this property. — It is useful to note that (ii) is equivalent to the condition

(ii)′ $m(\mathbf{t})_K$ is the generic minimum polynomial of J_K, for all fields $K \in k$-**alg**.

This follows easily from the fact that the kernel of the canonical map $k \to K$ is a prime ideal $\mathfrak{p}$ of k, so K is an extension field of $\boldsymbol{\kappa}(\mathfrak{p})$, and the well-known invariance of the generic minimum polynomial of a finite-dimensional Jordan algebra under base field extensions.

A polynomial $m(\mathbf{t})$ satisfying (i) and (ii) will be called a *generic minimum polynomial for* J. Actually, we will show below in 2.7(a) that $m(\mathbf{t})$ is uniquely determined by (i) and (ii).

2.3. Remarks. (a) The property of being generically algebraic is stable under base change (and descends from faithfully flat base extensions, see 2.7(b)): If J is generically algebraic over k and $m(\mathbf{t})$ is a generic minimum polynomial for J then J_R is generically algebraic over R and $m(\mathbf{t})_R$ is a generic minimum polynomial for J_R, for all $R \in k$-**alg**.

Indeed, by general facts, J_R is finitely generated and projective over R, and by 0.13, $m(\mathbf{t})_R$ is locally monic. As noted before, J_R satisfies $m(\mathbf{t})_R$. Hence condition (i) holds for $m(\mathbf{t})_R$, and condition (ii) follows from 0.13.6 and 2.1.1.

(b) By condition (ii) and 0.13.3, the degree function $\deg J$ of a generically algebraic J is locally constant on $\mathrm{Spec}(k)$. Thus we can decompose $k = \prod_{d\in D} k_d$ and correspondingly $\mathrm{Spec}(k) = \coprod_{d\in D} \mathrm{Spec}(k_d)$ such that $\deg J$ is constant equal to d on $\mathrm{Spec}(k_d)$; equivalently, that $J \otimes k_d$ is generically algebraic of constant degree d over k_d. In proofs, this fact will often be used by employing a phrase like "after decomposing the base ring, we may assume that J has constant degree equal to d." There are, however, natural examples of generically algebraic Jordan algebras whose degree functions are not constant, see 2.4(d).

(c) In the literature, the terminology "generically algebraic Jordan algebra of degree d", in particular for $d = 2$ and $d = 3$, has been used in an informal fashion for Jordan algebras over rings which possess a monic polynomial $m(\mathbf{t})$ of degree d satisfying condition (i), e.g., in [**29**, **30**, **20**]. Since condition (ii) does in general not hold for these examples, they are not necessarily generically algebraic in the present sense.

2.4. Examples. (a) If k is a field, every finite-dimensional Jordan algebra over k is generically algebraic in the present sense, and its generic minimum polynomial is the usual one.

(b) Let either $\mathcal{C}$ be a composition algebra of rank $\geqslant 2$ over k as defined in [**28**, 1.4] or let $\mathcal{C} = k$. (Note that k itself is not a composition algebra in the sense of [**28**] unless 2 is a unit in k). Consider the Jordan algebra $J = \mathrm{H}_d(\mathcal{C}, k)$ of hermitian $d \times d$-matrices over $\mathcal{C}$ with diagonal entries in k. Then it is easily seen from [**22**, pp. 501–503] that J is generically algebraic of degree d, provided $d \leqslant 3$. If $\mathcal{C}$ is associative, then $\mathrm{H}_d(\mathcal{C}, k)$ is generically algebraic of degree d for all $d \geqslant 1$.

(c) We leave it to the reader to show that J is generically algebraic of degree 0 if and only if $J = \{0\}$, and of degree 1 if and only if $J \cong k$. The generically algebraic algebras of degree 2 are precisely the Jordan algebras associated with quadratic forms with base point on finitely generated and projective k-modules of rank $\geqslant 2$, see 3.7. The generically algebraic Jordan algebras of degree 3 are all obtained by the "general cubic construction", see 3.9.

(d) Let M be a finitely generated and projective k-module. Then $J := \mathrm{End}(M)^+$ is generically algebraic, with generic minimum polynomial given by the characteristic polynomial

$$m(\mathbf{t}; x) = \det(\mathbf{t}\mathrm{Id} - x)$$

where det is the determinant of an endomorphism of a finitely generated and projective module, see [**1**]. The degree of J is given by $\deg(J) = \mathrm{rk}(M)$ and therefore is in general not constant. More generally, Azumaya algebras over k are generically algebraic [**17**, III, §1], as are central separable Jordan algebras over rings containing $\frac{1}{2}$ [**2**, §1].

(e) Let J' and J'' be generically algebraic with generic minimum polynomials m' and m''. Then it is easily seen that $J = J' \times J''$ is generically algebraic with generic minimum polynomial $m(\mathbf{t}; (x', x'')) = m'(\mathbf{t}; x') \cdot m''(\mathbf{t}; x'')$ and that $\deg J = \deg J' + \deg J''$.

(f) By 2.3(b), the degree function of a generically algebraic Jordan algebra J is locally constant on $\mathrm{Spec}(k)$. This necessary condition gives easy examples of finitely generated and projective Jordan algebras which are not generically algebraic. For example, let $J = B^+$ where B is as in 1.4. Then

$$(\deg J)(\mathfrak{p}) = \left\{ \begin{array}{ll} 2 & \text{if } \mathfrak{p} = (2) \\ 4 & \text{if } \mathfrak{p} \neq (2) \end{array} \right\}$$

is not constant on the connected space $\mathrm{Spec}(\mathbb{Z})$. On the other hand, there are examples of finitely generated and projective Jordan algebras of constant degree which are not generically algebraic, see 3.7.

2.5. Primitive elements. Let J be finitely generated and projective as a k-module. An element $a \in J$ is called *primitive* if a is algebraic and $\deg a = \deg J$. We define

$$J_{\mathrm{prim}} = \{a \in J : a \text{ primitive}\} \quad \text{and} \quad \mathbf{J}_{\mathrm{prim}}(R) := (J_R)_{\mathrm{prim}} \subset \mathbf{J}(R),$$

for all $R \in k$-**alg**. Then $\mathbf{J}_{\mathrm{prim}}$ is a subfunctor of $\mathbf{J}$ (actually, of $\mathbf{J}_{\mathrm{alg}}$): Indeed, let $R \to S$ be a homomorphism of k-algebras, and let $a \in \mathbf{J}_{\mathrm{prim}}(R)$. Then $a_S \in \mathbf{J}(S) = (J_R)_S$ is algebraic by Prop. 1.5(c), and from 1.5.1 and 2.1.1, it follows that $\deg a_S = \deg J_S$.

In case J is generically algebraic and $m(\mathbf{t})$ is a generic minimum polynomial of J, we have

$$a \text{ is primitive} \quad \Longleftrightarrow \quad a \text{ is algebraic and } \mu_a(\mathbf{t}) = m(\mathbf{t}; a). \tag{1}$$

Since $\deg a = \deg \mu_a(\mathbf{t})$ by definition, this is immediate from (ii) of 2.2 and the fact that $\mu_a(\mathbf{t})$ divides $m(\mathbf{t}; a)$. Also,

$$a \text{ primitive} \quad \Longrightarrow \quad \check{\mu}_a(\mathbf{t}) = \check{m}(\mathbf{t}; a) \tag{2}$$

which follows immediately from 0.13.7.

2.6. Lemma. *Let J be generically algebraic. Then $\mathbf{J}_{\mathrm{prim}}$ is an open dense finitely presented subscheme of $\mathbf{J}$, given as follows: Decompose $k = \prod_{d \in D} k_d$ such that $J_d := J \otimes k_d$ has constant degree d, cf.* 2.2(b)*. Then, in the notation of* 1.13 *and of* 0.7(d)*,*

$$\mathbf{J}_{\mathrm{prim}} = \coprod_{d \in D} (\mathbf{J}_d)_{\mathrm{alg},d}.$$

In particular, $\mathbf{J}_{\mathrm{prim}} = \mathbf{J}_{\mathrm{alg},d}$ if J has constant degree d.

Proof. Since $\mathbf{J} = \coprod_{d \in D} \mathbf{J}_d$ where $\mathbf{J}_d = (J_d)_{\mathbf{a}}$ is the affine scheme defined by J_d, we may assume that $\deg J = d$ is constant. Then by definition, $a \in \mathbf{J}_{\mathrm{prim}}(R)$ if and only if a is algebraic and has degree d, so $\mathbf{J}_{\mathrm{prim}} = \mathbf{J}_{\mathrm{alg},d}$.

Now we show that $\mathbf{J}_{\mathrm{alg},d}$ is open and dense in $\mathbf{J}$. Consider the morphisms $p_n \colon \mathbf{J} \to P_{\mathbf{a}}^{(n)}$ of 1.14(b). By (i) of 2.2, $x^{[d]}$ is a linear combination of $x^{[0]}, \ldots, x^{[d-1]}$ in all base ring extensions, which shows that $p_{d+1} = 0$. Hence by Prop. 1.14(b), $\mathbf{J}_{\mathrm{alg},d}$ is the inverse image of the open subscheme $P_{\mathbf{u}}^{(d)}$ of $P_{\mathbf{a}}^{(d)}$ under p_d and therefore open in $\mathbf{J}$. To prove that it is dense, it suffices by 0.14(iii) to show that $\mathbf{J}_{\mathrm{alg},d}(K) \neq \emptyset$, for all algebraically closed fields $K \in k$-**alg**. This follows from well-known results on Jordan algebras over fields, see [**16**, Section 3].

Remark. Although $\mathbf{J}_{\mathrm{prim}}$ is dense in $\mathbf{J}$, this does not imply that J itself contains any primitive elements. For example, let $k = \mathbb{F}_2$ and $J = k^3$, which by 2.4(e) is generically algebraic of degree 3. Then $a^n = a$ for all $n \geqslant 1$ and all $a \in J$, so $M(a)$ has dimension $\leqslant$2, while for a to be primitive, we must have $\dim M(a) = 3$. On the other hand, by 0.14(ii), there always exists a faithfully flat $R \in k$-**alg** such that $\mathbf{J}_{\mathrm{prim}}(R) \neq \emptyset$.

2.7. Proposition. (a) *The generic minimum polynomial $m(\mathbf{t})$ of a generically algebraic Jordan algebra J is uniquely determined. The coefficients m_i of $m(\mathbf{t})$, defined as in* 0.9.4 *by the expansion*

$$\check{m}(\mathbf{t};x)=\sum_{i\geqslant 0}(-1)^i m_i(x)\mathbf{t}^i, \tag{1}$$

are homogeneous of degree i. In particular, $m_0 = 1$ and m_1 is a linear form on J, called the generic trace *of J. The* generic norm, *defined by*

$$N(x) := m(0;-x) = (-1)^{\deg J} m(0;x), \tag{2}$$

is locally homogeneous of degree $\deg J$, i.e., it satisfies

$$N(rx) = r^{\deg J} N(x), \tag{3}$$

*for all $r \in R$, $x \in J_R$, $R \in k$-**alg**; see 0.9.1 for the notation $r^{\deg J}$. The m_i and hence also $m(\mathbf{t})$ and N are invariant under isomorphisms in the obvious sense and under derivations in the sense that*

$$\partial_{\Delta(x)} m_i\big|_x = 0, \tag{4}$$

for all $\Delta \in \mathrm{Der}(J)$.

(b) *(Descent) Let J be a Jordan algebra over k, let $R \in k$-**alg** be faithfully flat over k and suppose that $\tilde{J} := J_R$ is generically algebraic over R. Then J is generically algebraic over k.*

Remarks. (i) Despite appearances, the sum in (1) is finite, because $m_i = 0$ for $i > \max\deg J$. The derivative $\partial_v f\big|_x$ of a polynomial law f at x in direction v is defined by $f(x+\varepsilon v) = f(x) + \varepsilon\partial_v f\big|_x \in J \otimes k(\varepsilon)$, where $k(\varepsilon) = k[\mathbf{t}]/(\mathbf{t}^2)$ is the algebra of dual numbers.

(ii) In [**30**, Remark after 2.6], examples of isomorphisms are given which do not preserve norms. This is no contradiction to (a) because the "norms" in question are the cubic forms of a cubic norm structure. The algebras in these examples are not generically algebraic of degree 3 and hence have generic norms different from the cubic forms of the norm structure, see also the remark made in 3.9.

Proof. (a) Suppose $m(\mathbf{t})$ and $m'(\mathbf{t})$ are generic minimum polynomials for J. Then by 2.5.1, $m(\mathbf{t};a) = \mu_a(\mathbf{t}) = m'(\mathbf{t};a)$ for all $a \in \mathbf{J}_{\mathrm{prim}}(R)$ and all $R \in k$-**alg**, so $m(\mathbf{t}) = m'(\mathbf{t})$ follows from density of $\mathbf{J}_{\mathrm{prim}}$.

By [**31**, I, §8], m_i is homogeneous of degree i if and only if

$$m_i(rx) = r^i m_i(x), \tag{5}$$

for all $r \in R$, $x \in J_R$, $R \in k$-**alg**. Since $k_{\mathbf{u}}$ is dense in $k_{\mathbf{a}}$ and $\mathbf{J}_{\mathrm{prim}}$ is dense in $\mathbf{J}$, it suffices to show that this holds for all $r \in R^\times$ and $x \in \mathbf{J}_{\mathrm{prim}}(R)$. Then by Lemma 1.9, rx is algebraic and we have $\check{\mu}_{rx}(\mathbf{t}) = \check{\mu}_x(r\mathbf{t})$. Hence, using 0.13.7,

$$\check{m}(\mathbf{t};rx) = \check{\mu}_{rx}(\mathbf{t}) = \check{\mu}_x(r\mathbf{t}) = \check{m}(r\mathbf{t};x).$$

Now (5) follows by comparing coefficients at powers of $\mathbf{t}$ in (1). In particular, m_1 is homogeneous of degree 1 and thus a linear form on J [**31**, I, §11]. For (3), we may, after decomposing the base ring, assume that J has constant degree d. Then $N = m_d$ is homogeneous of degree d.

The invariance under isomorphisms is clear from the uniqueness. In particular, the m_i are invariant under all automorphisms. If $\Delta \in \mathrm{Der}(J)$ then $\Phi := \mathrm{Id} + \varepsilon\Delta \in \mathrm{Aut}(J_R)$ where $R = k(\varepsilon)$. As remarked in 2.2(a), J_R is generically algebraic with generic minimum polynomial $m(\mathbf{t})_R$. Hence $m_i(\Phi(x)) = m_i(x)$, which after expansion yields (4).

(b) Since $\tilde{J}$ is in particular finitely generated and projective so is J by [**3**, I, §3.6, Prop. 12]. Hence, $\deg J$ is well-defined.

Let $\tilde{A} = \mathcal{O}(\tilde{J}) = A \otimes R$ where $A = \mathcal{O}(J)$, and let $\tilde{m}(\mathbf{t}) \in \tilde{A}[\mathbf{t}]$ be the generic minimum polynomial of $\tilde{J}$. We show that $\tilde{m}(\mathbf{t})$ is "defined over k", i.e., of the form $m(\mathbf{t})_R$, obtained by base change from a (unique) polynomial $m(\mathbf{t}) \in A[\mathbf{t}]$. The algebra $S := R \otimes_k R$ can be considered as an R-algebra in two ways by means of the embeddings $\varrho_1, \varrho_2\colon R \to S$ into the first and second factor. We denote these R-algebra structures by S_1 and S_2, respectively. By general facts on faithfully flat descent [**17**, Ch. III], $\tilde{m}(\mathbf{t})$ is defined over k if and only if $\tilde{m}(\mathbf{t})_{S_1} = \tilde{m}(\mathbf{t})_{S_2}$. By 2.3(a) (applied to $\tilde{J}$ over the base ring R), $\tilde{J}_{S_i}$ is generically algebraic over S with generic minimum polynomial $\tilde{m}(\mathbf{t})_{S_i}$, for $i = 1, 2$. Since $\tilde{J} = J \otimes_k R$ is defined over k, we have $\tilde{J}_{S_i} = (J \otimes_k R) \otimes_R S_i = J \otimes_k S_i = J \otimes_k S$ (because $S_i = S$ as a k-algebra by restriction of scalars from R to k). Hence $\tilde{m}(\mathbf{t})_{S_1} = \tilde{m}(\mathbf{t})_{S_2}$ follows from the uniqueness of the generic minimum polynomial of $J \otimes_k S$ shown in (a). This proves the existence of $m(\mathbf{t}) \in A[\mathbf{t}]$ with $m(\mathbf{t})_R = \tilde{m}(\mathbf{t})$.

Now it is easy to see that $m(\mathbf{t})$ meets the requirements of Definition 2.2. First, $\tilde{A}$ is faithfully flat over A and $\tilde{m}(\mathbf{t})$ can be considered as obtained from $m(\mathbf{t})$ by base change from A to $\tilde{A}$. Hence $m(\mathbf{t})$ is locally monic, as noted in 0.8. From the fact that $\tilde{J}$ satisfies $m(\mathbf{t})_R$ and that R is faithfully flat, it follows easily that J satisfies $m(\mathbf{t})$. Finally, let $\varrho\colon k \to R$ be the homomorphism making R a k-algebra. Then $(\overline{\deg}\, m) \circ \operatorname{Spec}(\varrho) = \overline{\deg}\, \tilde{m}$ (by 0.13.6) $= \deg \tilde{J}$ (by condition (ii) of 2.2, because $\tilde{J}$ is generically algebraic over R) $= (\deg J) \circ \operatorname{Spec}(\varrho)$ (by 2.1.1). Now $\operatorname{Spec}(\varrho)$ is surjective because R is faithfully flat over k, so we conclude that condition (ii) of 2.2 holds for $m(\mathbf{t})$.

2.8. Lemma. *Let $E \in k$-**alg** be a commutative associative k-algebra which is finitely generated and projective as a k-module. Then the following conditions are equivalent:*

(i) *E is generically algebraic of degree* $\deg E = \operatorname{rk} E$*,*
(ii) *E becomes monogenous after a faithfully flat base change.*

If these conditions hold then the generic minimum polynomial of E is $m(\mathbf{t}; x) = \det(\mathbf{t}\mathrm{Id} - L(x))$ *and the primitive elements of E are precisely the generators of E as a k-algebra.*

Remark. Algebras satisfying these conditions play an important role in the theory of the norm functor [**8**] where the property (ii) is called "locally simple", see also [**9**].

Proof. (i) $\Longrightarrow$ (ii): Let $\mathbf{E} = E_{\mathbf{a}}$ be the k-scheme defined by E. By Lemma 2.6, $\mathbf{E}_{\mathrm{prim}}$ is open and dense in $\mathbf{E}$, so there exists a faithfully flat (and even finitely presented) $R \in k$-**alg** such that E_R contains a primitive element z. Since z is strictly power-associative, $R[z] \cong M(z)$ and $R[z] \subset E_R$ is a direct summand as an R-module by Cor. 1.7(c). It follows that $\operatorname{rk} R[z] = \operatorname{rk} M(z) = \deg(z) = \deg E_R$ (because z is primitive) $= \operatorname{rk} E_R$ (by 2.1.1). Thus $R[z] = E_R$ is monogenous, and we also see that primitive elements are generators.

(ii) $\Longrightarrow$ (i): By the descent property proved in Prop. 2.7(b) and the behaviour of the degree under base change (2.1.1), we may assume that E is monogenous, say, $E = k[z]$. Clearly, the indicated polynomial $m(\mathbf{t})$ is locally monic, and from the Cayley-Hamilton Theorem it follows that E satisfies $m(\mathbf{t})$. Hence $\deg E \leqslant \overline{\deg}\, m(\mathbf{t})$ by 2.2.1. By Lemma 0.11, $E \cong k[\mathbf{t}]/\big(m(\mathbf{t}; z)\big)$. Since E is an associative algebra, z is strictly power-associative in the sense of 1.6. Because $E = k[z]$, it follows from Cor. 1.7(c) that z is algebraic, and obviously $\mu_z(\mathbf{t}) = m(\mathbf{t}; z)$. Hence $\overline{\deg}\, m(\mathbf{t}) = \deg m(\mathbf{t}; z) =$ (by 0.13.5 in the special case $R = k$) $= \deg \mu_z(\mathbf{t}) = \deg z$ (by definition of the degree of an algebraic element in 1.4.5) $\leqslant \deg E$ (by

2.2.1). Thus $\deg E = \overline{\deg}\, m(\mathbf{t})$, so E is generically algebraic with generic minimum polynomial $m(\mathbf{t})$. As $\deg \mu_z(\mathbf{t}) = \operatorname{rk} E$ by Lemma 0.11, we have $\deg E = \operatorname{rk} E$. We also see that z is primitive because $\deg z = \deg E$.

2.9. Lemma. *Let J be generically algebraic with generic minimum polynomial $m(\mathbf{t})$, and let $a \in J$ be primitive. Let $E := E(a)$ and $\pi\colon E^+ \to J$ be as in* 1.2(b). *Then E is monogenous and finitely generated and projective, with $\operatorname{rk} E = \deg J$. For all $y \in E_R$ and $R \in k$-**alg**,*

$$m(\mathbf{t}; \pi(y)) = \det(\mathbf{t}\mathrm{Id} - L(y)), \qquad \check{m}(\mathbf{t}; \pi(y)) = \det(\mathrm{Id} - \mathbf{t}L(y)), \tag{1}$$

where $L(y)$ is left multiplication with y in E.

Proof. E is finitely generated and projective by 1.2.5 and 1.4.2, and it is generically algebraic with generic minimum polynomial

$$m^E(\mathbf{t}; y) = \det(\mathbf{t}\mathrm{Id}_E - L(y)) \tag{2}$$

by Lemma 2.8. The affine scheme $\mathbf{E} := E_{\mathbf{a}}$ defined by E is smooth, finitely presented and with connected fibres. By Lemma 2.6, $\mathbf{E}_{\mathrm{prim}}$ is open in $\mathbf{E}$ and $\mathbf{J}_{\mathrm{prim}}$ is open in $\mathbf{J}$. Hence $\mathbf{U}\colon = \mathbf{E}_{\mathrm{prim}} \cap \pi^{-1}(\mathbf{J}_{\mathrm{prim}})$ is open in $\mathbf{E}$. Moreover, $z = \mathrm{can}(\mathbf{t}) \in E$ is primitive by Lemma 2.8, and $\pi(z) = a \in J$ is primitive by assumption, whence $z \in \mathbf{U}(k)$. Thus $\mathbf{U}$ is dense in $\mathbf{E}$ by 0.14. We claim that

$$\mu_y(\mathbf{t}) = \mu_{\pi(y)}(\mathbf{t}) \text{ for all } y \in \mathbf{U}(R),\ R \in k\text{-}\mathbf{alg}. \tag{3}$$

Indeed, y and $b := \pi(y)$ are algebraic elements of E_R and J_R, respectively, so they have well-defined locally monic minimum polynomials, generating, respectively, the ideals $\mathfrak{N}(y)$ and $\mathfrak{N}(b)$ of $R[\mathbf{t}]$. Moreover, $\mathfrak{N}(y) \subset \mathfrak{N}(b)$ by 1.1.4, so $\mu_y(\mathbf{t})$ is a multiple of $\mu_b(\mathbf{t})$. Hence it suffices to show that both polynomials have the same degree, i.e., that $\deg b = \deg y$. Since y and b are primitive, $\deg y = \deg E_R = \operatorname{rk} E_R$ (by 2.8) and $\deg b = \deg J_R$. Also, since a is primitive, $\deg J = \deg a = \operatorname{rk} E$, cf. 1.4.5, and therefore also $\deg J_R = \operatorname{rk} E_R$. This implies $\deg y = \deg b$, so we have (3). It follows that $\det(\mathbf{t}\mathrm{Id}_E - L(y)) = m^E(\mathbf{t}; y)$ (by (2)) $= \mu_y(\mathbf{t})$ (because y is primitive) $= \mu_{\pi(y)}(\mathbf{t})$ (by (3)) $= m(\mathbf{t}; \pi(y))$ (because $\pi(y)$ is primitive). Hence the first formula of (1) holds for all $y \in \mathbf{U}(R)$ and all $R \in k$-**alg**. Since $\mathbf{U}$ is dense in $\mathbf{E}$, it holds for all $y \in \mathbf{E}(R)$. The second formula is clear from 0.10.1 and 0.10.2.

2.10. The adjoint. Let J be generically algebraic with generic minimum polynomial $m(\mathbf{t})$. We define the polynomial $m^\sharp(\mathbf{t}) \in A[\mathbf{t}]$ as in 1.11.1 by

$$\mathbf{t}m^\sharp(\mathbf{t}; x) = m(\mathbf{t}; x) - m(0; x), \tag{1}$$

and the *adjoint* of an arbitrary $x \in J_R$ ($R \in k$-**alg**) by

$$x^\sharp = m^\sharp(-x; -x). \tag{2}$$

From the homogeneity of the coefficients m_i of $m(\mathbf{t})$ it follows that $m(\mathbf{t}; x)$ is locally homogeneous of degree $\deg J$ in $(\mathbf{t}; x)$, i.e., $m(\lambda\mathbf{t}; \lambda x) = \lambda^{\deg J} m(\mathbf{t}; x)$. Hence $x \mapsto x^\sharp$ is a locally homogeneous polynomial law of degree $(\deg J) - 1$. If $\deg J = d$ is constant, we have

$$m^\sharp(\mathbf{t}; x) = \sum_{i=1}^{d} (-1)^{i-1} m_{i-1}(x)\mathbf{t}^{d-i}, \qquad x^\sharp = \sum_{i=1}^{d} m_{i-1}(x)(-x)^{d-i}. \tag{3}$$

We also note the formulas

$$U_x x^\sharp = N(x)x, \qquad U_x(x^\sharp)^2 = U_{x^\sharp} x^2 = N(x)^2 1_J, \tag{4}$$

which follow by applying j_{-x} to the equations $\mathbf{t}^2 m^\sharp(\mathbf{t}; -x) = \mathbf{t}m(\mathbf{t}; -x) - \mathbf{t}N(x)$ and $\big[\mathbf{t}m^\sharp(\mathbf{t}; -x)\big]^2 = \big[m(\mathbf{t}; -x) - N(x)\big]^2$.

2.11. Theorem. *Let J be a generically algebraic Jordan algebra over k. We use the notations introduced in* 2.7 *and* 2.10.

(a) *The generic minimum polynomial and copolynomial can be recovered from the generic norm by*

$$m(\mathbf{t};x) = N(\mathbf{t}1_J - x), \qquad \check{m}(\mathbf{t};x) = N(1_J - \mathbf{t}x). \tag{1}$$

In particular, $\check{m}(\mathbf{t};0) = N(1_J) = 1$, $\check{m}(\mathbf{t};1_J) = (1-\mathbf{t})^{\deg J}$ and

$$m_i(1_J) = \binom{\deg J}{i} \qquad (i \in \mathbb{N}). \tag{2}$$

(b) *For all $x \in J$, the generic norm is multiplicative on $k[x]$ in the sense that*

$$N\big((fg)(x)\big) = N(f(x))N(g(x)) \tag{3}$$

for all $f, g \in k[\mathbf{t}]$. In particular,

$$N(x^j) = N(x)^j \qquad (j \in \mathbb{N}). \tag{4}$$

(c) *The element $x \in J$ is invertible if and only if $N(x) \in k^\times$. In this case,*

$$x^{-1} = \frac{x^\sharp}{N(x)}, \tag{5}$$

$$m(\mathbf{t}; -x^{-1}) = \frac{\check{m}(\mathbf{t}; -x)}{N(x)}, \tag{6}$$

$$N(x^{-1}) = \frac{1}{N(x)}, \tag{7}$$

$$N(x^\sharp) = N(x)^{(\deg J)-1}, \tag{8}$$

$$x^{\sharp\sharp} = N(x)^{(\deg J)-2}x. \tag{9}$$

(d) *$x \in J$ is nilpotent if and only the $m_i(x) \in k$ are nilpotent, for all $i \geqslant 1$.*

(e) *The derivative of m_{i+1} in the direction of 1_J is*

$$\partial_{1_J} m_{i+1}\big|_x = \big((\deg J) - i\big)m_i(x). \tag{10}$$

Proof. (a) By density of $\mathbf{J}_{\mathrm{prim}}$ (Lemma 2.6), it suffices to prove this for all $x \in \mathbf{J}_{\mathrm{prim}}(R)$ and all $R \in k$-**alg**, and after changing the base from k to R to simplify notation, we may assume $x = a \in J$ is primitive. As in Lemma 2.9, let $a = \pi(z)$ and put $y := \mathbf{t}1_E - z \in E_{k[\mathbf{t}]}$. Then by 2.9.1,

$$N(\mathbf{t}1_J - a) = N(\pi(y)) = m(0; -\pi(y)) = \det L(y) = \det(\mathbf{t}\mathrm{Id} - L(z)) = m(\mathbf{t}; a).$$

The second formula of (1) is proved similarly. By specializing $\mathbf{t} \to 0$ and because the copolynomial is comonic (0.9) we see $1 = \check{m}(0;x) = N(1_J)$, and putting $x = 1_J$ yields $\check{m}(\mathbf{t};1_J) = N\big((1-\mathbf{t})1_J\big) = (1-\mathbf{t})^{\deg J}$ (by 2.7.3) $= \sum_{i \geqslant 0}(-1)^i m_i(1)\mathbf{t}^i$ (by 2.7.1). This proves (2).

(b) By the density argument employed above, it suffices to prove this for $x = a \in J$ primitive. Then the asserted formulas follow at once from the fact that $N(\pi(y)) = \det L(y)$ (by 2.9.1) and the multiplicativity of the determinant.

(c) If $N(x) = m(0; -x)$ is invertible, then x is invertible, and formula (5) holds by Lemma 1.11(a). Conversely, let $x \in J^\times$ but assume $N(x) \notin k^\times$. Then there exists a maximal ideal $\mathfrak{m} \subset k$ with $N(x) \in \mathfrak{m}$. Let $K = k/\mathfrak{m}$. Then $0 = N(x)_K = N(x_K)$, and hence x_K is not invertible in J_K, by [**16**, Theorem 2(iii)]. This contradicts the fact that invertible elements remain so under base change.

We prove (6). By density, we may assume x primitive. Then also x^{-1} is primitive because $\deg x = \deg x^{-1}$ by 1.11(b). Now it follows from 1.11.4 and 2.5.2 that

$$m(\mathbf{t}; x^{-1}) = \frac{\check{m}(\mathbf{t}; x)}{m(0; x)},$$

and replacing x by $-x$ in this formula yields (6). By specializing $\mathbf{t} \to 0$ we have (7).

Next, (8) and (9) are polynomial identities, so by density we may assume x invertible. Then $N(x)^{-1} = N(x^{-1}) = N(x^\sharp/N(x)) = N(x^\sharp)/N(x)^{\deg J}$ yields the first formula. For the second, one argues similarly, using the fact that $(x^{-1})^{-1} = x$ and that $x^\sharp$ is homogeneous of degree $(\deg J) - 1$.

(d) After decomposing the base ring, we may assume $\deg J = d$ constant. Then $x^d = \sum_{i=1}^{d} (-1)^{i-1} m_i(x) x^{d-i}$. Hence, if all $m_i(x)$ are nilpotent, it follows from the multinomial expansion that x is nilpotent. Conversely, if x is nilpotent then so is $x(\mathfrak{p})$, for all prime ideals $\mathfrak{p} \in \mathrm{Spec}(k)$. By [**16**, Theorem 2(vi)], $0 = m_i(x(\mathfrak{p})) = m_i(x) \otimes 1_{\boldsymbol{\kappa}(\mathfrak{p})}$, so $m_i(x)$ belongs to the intersection of all prime ideals of k and therefore is nilpotent.

(e) Let $R = k(\varepsilon)$ be the algebra of dual numbers. Then by (a), $\check{m}(\mathbf{t}; x + \varepsilon 1_J) = N(1_J - \mathbf{t}(x + \varepsilon 1_J)) = N((1 - \mathbf{t}\varepsilon)1_J - \mathbf{t}x)$. Now $1 - \mathbf{t}\varepsilon$ is invertible with inverse $(1 - \mathbf{t}\varepsilon)^{-1} = 1 + \mathbf{t}\varepsilon$. Hence by 2.7.3,

$$\check{m}(\mathbf{t}; x + \varepsilon 1_J) = (1 - \mathbf{t}\varepsilon)^{\deg J} N(1 - \mathbf{t}(1 + \mathbf{t}\varepsilon)x) = (1 - \mathbf{t}\varepsilon)^{\deg J} \check{m}(\mathbf{t} + \mathbf{t}^2\varepsilon; x).$$

Expanding both sides with formula 2.7.1 and comparing coefficients at $\varepsilon \mathbf{t}^{i+1}$ yields (10).

2.12. Generic elements. For finite-dimensional algebras Jordan algebras over fields, the generic minimum polynomial is simply the minimum polynomial of the generic element, see [**5**, **14**]. Does a similar statement hold over rings? It would be tempting to be able to say "J is generically algebraic if and only if the generic element of J is algebraic". Unfortunately, this is not the case. Let us first recall the notion of generic element for finitely generated and projective modules [**19**, §18].

Let J be finitely generated and projective and $A = \mathcal{O}(J)$. The generic element $\mathbf{x}$ of J is the element $\mathbf{x} \in J \otimes J^* \subset J \otimes A$ corresponding to Id_J under the canonical isomorphism $J \otimes J^* \cong \mathrm{End}\, J$. The name "generic element" is justified by the fact that $\mathbf{x}$ can be specialized to any $x \in J_R$, $R \in k$-**alg**, in the following sense: Evaluation of an element $g \in A$ at x defines a homomorphism $e_x \colon A \to R$, $e_x(g) = g(x)$, and hence a map $\mathrm{Id}_J \otimes e_x \colon J_A \to J_R$, which maps $\mathbf{x}$ to x. We thus have $g = g(\mathbf{x}) \in A$, for all $g \in A$. This implies that, for any $f(\mathbf{t}) \in A[\mathbf{t}]$, we have $f(\mathbf{t}; \mathbf{x}) = f(\mathbf{t})$, and that J satisfies a locally monic $f(\mathbf{t}) \in A[\mathbf{t}]$ (in the sense of 2.2) if and only if the generic element $\mathbf{x}$ satisfies $f(\mathbf{t})$.

2.13. Proposition. (a) *Let J be generically algebraic with generic minimum polynomial $m(\mathbf{t})$. Then the generic element $\mathbf{x}$ of J is pre-algebraic and its minimum polynomial is $m(\mathbf{t})$, but $\mathbf{x}$ is not an algebraic element of J_A, unless $J = \{0\}$.*

(b) *There are examples of finitely generated and projective Jordan algebras whose generic element is pre-algebraic but which are not generically algebraic.*

Proof. (a) After decomposing the base ring, we may assume $\deg J = d$ constant. Since every element $x \in J_R$ in every base ring extension R of k satisfies $m(\mathbf{t}; x)$, this is in particular so for $\mathbf{x}$, whence $m(\mathbf{t}) \in \mathfrak{N}(\mathbf{x})$. To prove $\mu_{\mathbf{x}}(\mathbf{t}) = m(\mathbf{t})$ it suffices to show that $\mathbf{x}^{[0]}, \ldots, \mathbf{x}^{[d-1]}$ are free over A in J_A^2. Thus assume a relation $\sum_{i=0}^{d-1} g_i(\mathbf{x})\mathbf{x}^{[i]} = 0$ in J_A^2. By specializing $\mathbf{x}$ to any $a \in \mathbf{J}_{\mathrm{prim}}(R)$, $R \in k$-**alg**, it follows that $\sum_{i=0}^{d-1} g_i(a)a^{[i]} = 0$. Since a is algebraic of degree d, the powers $a^{[0]}, \ldots, a^{[d-1]}$ are linearly independent over R, so that all $g_i(a) = 0$. Thus the g_i vanish on the open and dense subscheme $\mathbf{J}_{\mathrm{prim}}$ of $\mathbf{J}$ and are therefore zero. It follows that $\mathbf{x}$ is pre-algebraic of degree d, so its minimum polynomial is $m(\mathbf{t})$.

Now assume that $\mathbf{x}$ is algebraic. Then, for every A-algebra R, the degree of $\mathbf{x}_R$ is still d. On the other hand, $\mathbf{x}$ can be specialized to 0. Hence the element $0 \in J$ is algebraic of degree d. Since 0 is in particular an idempotent, the computation in 1.8 shows $\mu_0(\mathbf{t}) = \gamma\mathbf{t} + (1-\gamma)$ where γ is the support idempotent of 1_J. It follows that either $d = 0$ and then $\gamma = 0$ hence $J = 0$, or $d = 1$ whence $d = 1$ and $J = k$. But the second case is impossible, because then $\mathbf{x} = \mathbf{t} \in A = k[\mathbf{t}]$, and the A-submodule of A generated by $\mathbf{t}$ is $\mathbf{t}A$ which is not a direct summand of A (as an A-module).

(b) Let $J = B^+$ be the algebra of 2.4(f). Then it is easily seen that the generic element is pre-algebraic, but J is not generically algebraic because its degree function is not locally constant on $\mathrm{Spec}(\mathbb{Z})$.

3. The generic minimum polynomial of an isotope

3.1. Theorem. *Let J be a generically algebraic Jordan algebra over k, with generic minimum polynomial $m(\mathbf{t})$ and generic norm N. Let $v \in J^\times$ and let $J^{(v)}$ be the v-isotope of J, with unit element $1^{(v)} = v^{-1}$ and U-operators $U_x^{(v)} = U_xU_v$. Then also $J^{(v)}$ is generically algebraic, $\deg J^{(v)} = \deg J$, with generic minimum polynomial, copolynomial and generic norm given by*

$$m^{(v)}(\mathbf{t}; x) = N(v)N(\mathbf{t}v^{-1} - x), \tag{1}$$

$$\check{m}^{(v)}(\mathbf{t}; x) = N(v)N(v^{-1} - \mathbf{t}x), \tag{2}$$

$$N^{(v)}(x) = N(v)N(x). \tag{3}$$

Proof. We follow the idea of the proof of [**26**, Th. 1] but avoid the use of the composition law for the generic norm. Clearly $J^{(v)}$ is finitely generated and projective because $J = J^{(v)}$ as k-modules. For the remainder of the proof, we may assume, after decomposing the base ring, that $\deg J = d$ is constant, and it is no restriction to assume $d > 0$, for else $J = \{0\}$ by 2.4(c). Then N is homogeneous of degree d. Define polynomial laws $N_{i,d-i}$, bihomogeneous of degree $(i, d-i)$, on $J \times J$ by the expansion

$$N(\mathbf{s}x + \mathbf{t}y) = \sum_{i=0}^{d} \mathbf{s}^i\mathbf{t}^{d-i}N_{i,d-i}(x, y), \tag{4}$$

where $\mathbf{s}, \mathbf{t}$ are indeterminates and $x, y \in J_R$, $R \in k$-**alg**, cf. [**31**, II, §1]. Then $N_{i,d-i}(x, y) = N_{d-i,i}(y, x)$ and $N_{0,d}(x, y) = N(y)$. Define $f(\mathbf{t}) \in A[\mathbf{t}]$ (where $A = \mathcal{O}(J)$) by

$$f(\mathbf{t}; x) = N(v)N(\mathbf{t}v^{-1} - x) = \sum_{i=0}^{d}(-1)^iN(v)N_{i,d-i}(x, v^{-1})\mathbf{t}^{d-i}. \tag{5}$$

This is obtained from (4) by $\mathbf{s} \to -1$ and $y = v^{-1}$. Then the coefficient of $\mathbf{t}^d$ in $f(\mathbf{t})$ is $N(v)N_{0,d}(x, v^{-1}) = N(v)N(v^{-1}) = 1$ (by 2.11.7), so $f(\mathbf{t})$ is monic of degree d.

Now we show that $J^{(v)}$ satisfies $f(\mathbf{t})$ in the sense of 2.2, i.e., that $f(\mathbf{t};x)$ and $\mathbf{t}f(\mathbf{t};x)$ vanish upon substitution of x for $\mathbf{t}$, for all $x \in J_R^{(v)}$ and $R \in k$-**alg**. Since everything is compatible with base change, we may extend k to R and then write again k for R (for simpler notation), so it suffices to prove this for all $x \in J^{(v)}$. Consider the k-algebra $S = k(\lambda) = k[\mathbf{s}]/(\mathbf{s}^{d+2})$ which is free as a k-module with basis $1, \lambda, \dots, \lambda^{d+1}$ and satisfies $\lambda^{d+2} = 0$. Since λ is nilpotent, $1^{(v)} - \lambda x \in J_S^{(v)}$ is invertible. We compute its inverse in two ways. First, again by nilpotence of λ, the inverse is given by the geometric series:

$$(1^{(v)} - \lambda x)^{(-1,v)} = \sum_{j=0}^{d+1} \lambda^j x^{(j,v)}, \tag{6}$$

where $x^{(j,v)}$ is the jth power of x in $J^{(v)}$. On the other hand, an element a is invertible in $J^{(v)}$ if and only if it is invertible in J, and then

$$a^{(-1,v)} = \big(U_a^{(v)}\big)^{-1} a = \big(U_a U_v\big)^{-1} a = U_v^{-1} U_a^{-1} a = U_v^{-1} a^{-1}. \tag{7}$$

Since J is generically algebraic, $a^{-1} = a^\sharp / N(a)$ by 2.11.5. All this remains true in any base ring extension. In particular, let $a = 1^{(v)} - \lambda x = v^{-1} - \lambda x$. Substituting $a^\sharp/N(a)$ for a^{-1} in (6) and multiplying the resulting equation with $N(a)$ yields

$$U_v^{-1}(v^{-1} - \lambda x)^\sharp = N(v^{-1} - \lambda x) \cdot \sum_{j=0}^{d+1} \lambda^j x^{(j,v)}. \tag{8}$$

Now $x \mapsto x^\sharp$ is a homogeneous polynomial law of degree $d-1$ by 2.10. Hence the coefficients of λ^d and λ^{d+1} on the left hand side of (8) vanish, so they must vanish on the right hand side as well. From (4) we have the expansion $N(v^{-1} - \lambda x) = \sum_{i=0}^{d} (-\lambda)^i N_{i,d-i}(x, v^{-1})$. By collecting terms at λ^d and λ^{d+1} on the right hand side, we obtain the relations

$$\sum_{i=0}^{d} (-1)^i N_{i,d-i}(x, v^{-1}) x^{(d-i,v)} = \sum_{i=0}^{d} (-1)^i N_{i,d-i}(x, v^{-1}) x^{(d+1-i,v)} = 0.$$

After multiplying with $N(v)$, this says precisely that x satisfies $f(\mathbf{t};x)$ in the isotope $J^{(v)}$.

We have verified condition (i) of 2.2 for $J^{(v)}$, so it remains to show that $J^{(v)}$ has degree d, i.e., that $J^{(v)}(\mathfrak{p}) = J^{(v)} \otimes 1_{\boldsymbol{\kappa}(\mathfrak{p})}$ has degree d, for all $\mathfrak{p} \in \operatorname{Spec}(k)$. Now $\deg J^{(v)}(\mathfrak{p}) \leqslant d = \deg J(\mathfrak{p})$ because because $J^{(v)}(\mathfrak{p})$ satisfies the polynomial $f(\mathbf{t})_{\boldsymbol{\kappa}(\mathfrak{p})}$ of degree d. But $J(\mathfrak{p}) = \big(J^{(v)}(\mathfrak{p})\big)^{(v^{-2}(\mathfrak{p}))}$ is an isotope of $J^{(v)}(\mathfrak{p})$, and $J^{(v)}(\mathfrak{p})$ is generically algebraic, being finite-dimensional over $\boldsymbol{\kappa}(\mathfrak{p})$. Hence the above argument, applied to $J^{(v)}(\mathfrak{p})$ instead of J, yields $\deg J(\mathfrak{p}) \leqslant \deg J^{(v)}(\mathfrak{p})$. We have shown that $J^{(v)}$ is generically algebraic with generic minimum polynomial $f(\mathbf{t}) = m^{(v)}(\mathbf{t})$. The formulas for $\check{m}^{(v)}(\mathbf{t})$ and the generic norm are then an immediate consequence.

3.2. Corollary. (a) *The generic norm of a generically algebraic Jordan algebra J permits Jordan composition:*

$$N(U_x y) = N(x)^2 N(y), \tag{1}$$

*for all $x, y \in J_R$, $R \in k$-***alg**.

(b) *Let B be a generically algebraic associative or alternative algebra over k and let N be its generic norm, i.e., the generic norm of the associated Jordan algebra B^+. Then N is multiplicative:*

$$N(xy) = N(x)N(y), \tag{2}$$

*for all $x, y \in B_R$, $R \in k$-**alg**.*

Proof. (a) By density of $\mathbf{J}^\times$ (see 0.14) we may assume y invertible. Then $N(y)N(U_x y) = N^{(y)}(x^{(2,y)}) = N^{(y)}(x)^2$ (by 2.11.4) $= N(y)^2 N(x)^2$ (by 3.1.3).

(b) Again by density, we may assume x invertible. Then left multiplication L_x with x in B is an isomorphism $L_x\colon \big(B^{(x)}\big)^+ \to B^+$ of Jordan algebras [**24**, Prop. 4], and $\big(B^{(x)}\big)^+ = \big(B^+\big)^{(x)}$ by [**24**, (19)]. Since the generic norm is invariant under isomorphisms by Prop. 2.7(a), it follows that $N(xy) = N(L_x(y)) = N^{(x)}(y) = N(x)N(y)$.

The following lemma is the analogue over rings of [**26**, Th. 2].

3.3. Lemma. *Let J be generically algebraic and let $u, v \in J^\times$. Then the generic minimum polynomials of $u \in J^{(v)}$ and $v \in J^{(u)}$ are related by*

$$m^{(v)}(\mathbf{t}; u) = m^{(u)}(\mathbf{t}; v), \tag{1}$$
$$\check{m}^{(v)}(\mathbf{t}; u) = \check{m}^{(u)}(\mathbf{t}; v), \tag{2}$$

and the generic norm has the symmetry property

$$N(v)N(v^{-1} - u) = N(u)N(u^{-1} - v). \tag{3}$$

Proof. Let us first assume that u is primitive, hence in particular algebraic, in $J^{(v)}$. By Lemma 1.9(b), v is then algebraic in $J^{(u)}$, and $\mu_v^{(u)}(\mathbf{t}) = \mu_u^{(v)}(\mathbf{t}) = m^{(v)}(\mathbf{t}; u)$ (by 2.5.1). Hence $\deg \mu_v^{(u)}(\mathbf{t}) = \deg m^{(v)}(\mathbf{t}; u) = \deg J = \deg J^{(u)}$ by Th. 3.1. This shows that v is primitive in $J^{(u)}$, and hence (1) follows again from 2.5.1. Furthermore, (2) and (3) are immediate consequences.

In the general case, consider the subfunctor $\mathbf{U}$ of $\mathbf{J}^\times \times \mathbf{J}^\times$ defined by

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{U}(R) \quad \Longleftrightarrow \quad x \text{ is primitive in } (J_R)^{(y)},$$

for all $R \in k$-**alg**. Note that $(x, y) \in \mathbf{U}(R)$ if and only if $(y, x) \in \mathbf{U}(R)$ and that (1) – (3) hold on $\mathbf{U}(R)$, by what we proved above. Hence, it suffices to show that $\mathbf{U}$ is an open and dense subscheme of $\mathbf{J}^\times \times \mathbf{J}^\times$. After decomposing the base ring, we may assume $\deg J = d$ constant. Then also all isotopes of all J_R have degree d. Define a morphism $p\colon \mathbf{J}^\times \times \mathbf{J}^\times \to P_{\mathbf{a}}^{(d)}$ (cf. Prop. 1.14(b)) by

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x^{(0,y)} \\ x^{(1,y)} \end{pmatrix} \wedge \cdots \wedge \begin{pmatrix} x^{(d-1,y)} \\ x^{(d,y)} \end{pmatrix}$$

in all base ring extensions. Then $\mathbf{U}$ is the inverse image of $P_{\mathbf{u}}^{(d)}$ under p and therefore open. Furthermore, $\mathbf{J}^\times \times \mathbf{J}^\times$ is smooth, being open in $\mathbf{J} \times \mathbf{J}$, and it has connected fibres: Indeed, for all algebraically closed fields $K \in k$-**alg**, $J_K^\times \times J_K^\times$ is the complement of the hypersurface $N(x)N(y) = 0$ in $J_K \times J_K$ and the latter is isomorphic to affine $2n$-space over K where $n = \dim J_K$. Thus by 0.14, it suffices to have $\mathbf{U}(K) \neq \emptyset$. Since $\mathbf{J}_{\mathrm{prim}}(K) \neq \emptyset$ by density of $\mathbf{J}_{\mathrm{prim}}$ and $\mathbf{J}_{\mathrm{prim}} \times \{1_J\} \subset \mathbf{U}$, we are done.

3.4. Suppose J is generically algebraic of constant degree d. In view of 3.1.1 and 3.1.5, the symmetry formulas 3.3.1 – 3.3.3 are equivalent to

$$m_i^{(y)}(x) = N(y)N_{i,d-i}(x, y^{-1}) = N(x)N_{i,d-i}(y, x^{-1}) = m_i^{(x)}(y).$$

Here the two left hand sides are defined for all x while the two right hand sides are defined for all y. This suggests the existence of polynomial laws F_i on $J \times J$ such that $m_i^{(y)}(x) = F_i(x, y)$ for all x and all invertible y, and analogously with x and y interchanged. For $i = 0$ and $i = d$ this is of course trivially true, with $F_0 = 1$ and

$$F_d(x, y) = N(x)N(y). \tag{1}$$

For $i = d-1$, we have $N_{d-1,1}(z, v)$ linear in v, and hence, using 2.11.5, $m_{d-1}^{(y)}(x) = N(y)N_{d-1,1}(x, y^{-1}) = N_{d-1,1}(x, y^\sharp)$, so

$$F_{d-1}(x, y) = N_{d-1,1}(x, y^\sharp) \tag{2}$$

is such a polynomial law. We now show that such F_i exist for all i.

3.5. Theorem. *Let J be generically algebraic. Then there exist unique polynomial laws F_i $(i \in \mathbb{N})$ on $J \times J$ such that*

$$m_i^{(y)}(x) = F_i(x, y), \tag{1}$$

*for all $x \in J_R$, $y \in (J_R)^\times$, $R \in k$-**alg**. The F_i are symmetric and bihomogeneous of bidegree (i, i). In particular, F_1 is a symmetric bilinear form on J, called the* bilinear trace. *Explicitly, it is given by*

$$F_1(x, y) = m_1(x)m_1(y) - m_{1,1}(x, y) = -\partial_x\partial_y \log N\big|_{1_J} \tag{2}$$

where $m_{1,1}$ denotes the bilinear form associated to the quadratic form m_2, and satisfies

$$F_1(x, y^\sharp) = \partial_x N\big|_y, \tag{3}$$

*for all $x, y \in J_R$, $R \in k$-**alg**.*

Proof. After decomposing the base ring, we may assume $\deg J = d$ constant. Let $R \in k$-**alg** and consider the R-algebra $\tilde{R} = R[\mathbf{t}](\lambda) = R[\mathbf{t}, \mathbf{s}]/(\mathbf{s}^{d+1})$. Let $x, y \in J_R$ be arbitrary. Then $1 - \lambda x \in J_R \otimes_R \tilde{R}$ is invertible, with inverse given by the geometric series: $(1 - \lambda x)^{-1} = 1 + \lambda x + \cdots + \lambda^d x^d$. Since $\tilde{R}$ is a free R-module with basis $\lambda^i \mathbf{t}^j$ $(i = 0, \ldots, d,\ j \in \mathbb{N})$, we can write, using 3.1.2,

$$\check{m}^{(1-\lambda x)}(\mathbf{t}; y) = N(1 - \lambda x)N\big((1 - \lambda x)^{-1} - \mathbf{t}y\big) = \sum_{i,j=0}^{d} \lambda^i \mathbf{t}^j h_{ij}(x, y), \tag{4}$$

with uniquely determined $h_{ij}(x, y) \in R$. By "varying R", one sees that (4) defines polynomial laws h_{ij} on $J \times J$, and since the left hand side of (4) depends only on λx and $\mathbf{t}y$, it is clear that h_{ij} is bihomogeneous of bidegree (i, j). Now assume y invertible. Then by 2.7.1 and 3.3.2,

$$\sum_{i=0}^{d} (-1)^i m_i^{(y)}(1 - \lambda x)\mathbf{t}^i = \check{m}^{(y)}(\mathbf{t}; 1 - \lambda x) = \check{m}^{(1-\lambda x)}(\mathbf{t}; y) = \sum_{i,j=0}^{d} \lambda^i \mathbf{t}^j h_{ij}(x, y). \tag{5}$$

Since $m_i^{(y)}$ is homogeneous of degree i we have $m_i^{(y)}(1 - \lambda x) = (-1)^i \lambda^i m_i^{(y)}(x)$ plus terms with lower powers of λ. Substituting this into (5) and comparing coefficients at $\lambda^i\mathbf{t}^i$ yields $m_i^{(y)}(x) = h_{ii}(x,y)$ (and $h_{ij} = 0$ for $i > j$). Thus $F_i := h_{ii}$ has the asserted property. Symmetry and homogeneity of the F_i follow from the corresponding properties of the $m_i^{(y)}(x) = m_i^{(x)}(y)$ and the fact that $\mathbf{J}^\times \times \mathbf{J}^\times$ is dense in $\mathbf{J} \times \mathbf{J}$. In particular, F_1 is a bilinear form by [**31**, Prop. I.6].

We now determine $F_1 = h_{11}$ from (4) as the coefficient of $\lambda\mathbf{t}$. Computing modulo λ^2 and $\mathbf{t}^2$, we have $(1-\lambda x)^{-1} \equiv 1 + \lambda x$, hence

$$\begin{aligned}\check{m}^{(1-\lambda x)}(\mathbf{t}; y) &= N(1-\lambda x)N(1+\lambda x - \mathbf{t}y) = \check{m}(1;\lambda x)\check{m}(1;\mathbf{t}y - \lambda x) \quad \text{(by 2.11.1)}\\ &\equiv \big\{1 - m_1(\lambda x)\big\}\big\{1 - m_1(\mathbf{t}y - \lambda x) + m_2(\mathbf{t}y - \lambda x)\big\} \qquad \text{(by 2.7.1)}\\ &\equiv 1 - \mathbf{t}m_1(y) + \mathbf{t}\lambda\big\{(m_1(x)m_1(y) - m_{1,1}(x,y)\big\}.\end{aligned}$$

This proves (2). By density of $\mathbf{J}^\times$, it suffices to prove (3) for y invertible. Replace v by y^{-1} in 3.1.2 and multiply the result with $N(y)$. Then, because $N(y^{-1}) = N(y)^{-1}$ and $y^{-1} = y^\sharp N(y)^{-1}$ by Th. 2.11(c), it follows that

$$N(y - \mathbf{t}x) = N(y)\check{m}^{(y^{-1})}(\mathbf{t};x) \equiv N(y) - \mathbf{t}F_1(x, y^\sharp) \pmod{\mathbf{t}^2}.$$

On the other hand, $N(y - \mathbf{t}x) \equiv N(y) - \mathbf{t}\partial_x N\big|_y \pmod{\mathbf{t}^2}$, whence (3).

3.6. Corollary. *We keep the assumptions and the notation of Th.* 3.5. *Let* $\mathrm{Str}(J)$ *be the structure group of* J *and let* $g \mapsto g^*$ *be the antiautomorphism of* $\mathrm{Str}(J)$ *determined by* $U_{g(x)} = gU_xg^*$, *for all* $x \in J$.

(a) *The* F_i *are invariant under the structure group in the sense that, for* $g \in \mathrm{Str}(J)$,

$$F_i(g(x), y) = F_i(x, g^*(y)), \tag{1}$$

for all $x, y \in J_R$, $R \in k$-**alg**.

(b) *The generic norm is covariant under the structure group in the sense that*

$$N\big(g(x)\big) = N\big(g(1_J)\big)N(x) \tag{2}$$

for all $g \in \mathrm{Str}(J)$, $x \in J_R$, $R \in k$-**alg**. *The map* $g \mapsto N\big(g(1_J)\big)$ *is a character* $\chi\colon \mathrm{Str}(J) \to k^\times$ *satisfying* $\chi(g^*) = \chi(g)$ *and* $\chi(U_x) = N(x)^2$.

Proof. (a) By density of $\mathbf{J}^\times$, it suffices to prove (1) for invertible y, and after changing the base ring from k to R, we may assume $x, y \in J$. Then $g\colon J^{(g^*(y))} \to J^{(y)}$ is an isomorphism of Jordan algebras. Hence, by the invariance of the generic minimum polynomial under isomorphisms (Prop. 2.7(a)), $F_i(g(x), y) = m_i^{(y)}(g(x))$ $= m_i^{(g^*(y))}(x) = F_i(x, g^*(y))$.

(b) We may assume that J has constant degree d. Then by 3.4.1 and (1), $N\big(g(x)\big)N(y) = N(x)N\big(g^*(y)\big)$. By putting $x = y$ we see that $N\big(g(x)\big) = N\big(g^*(x)\big)$ and for $y = 1$ we obtain $N\big(g(x)\big) = N\big(g^*(1)\big)N(x) = N\big(g(1)\big)N(x)$. This easily implies that χ is a homomorphism. Finally, $\chi(U_x) = N(x)^2$ is clear from 3.2.1.

Remark. For a base field and $i = 1$, formula (1) is proved in [**26**, Th. 4]. An obvious rephrasing of (b) together with 3.1.3 shows that an isotopy between generically algebraic Jordan algebras is a strict norm similarity. The converse holds for central separable Jordan algebras over rings containing $\frac{1}{2}$ [**2**, Th. 4.4] but fails for rings where 2 is not invertible, e.g., for the $n \times n$ symmetric matrices over $k = K(\varepsilon)$ (dual numbers over a field K of characteristic 2), as discovered by Waterhouse [**32**].

3.7. Corollary. J *is a generically algebraic Jordan algebra of degree* 2 *if and only if* $J = \mathrm{Jor}(X, Q, 1)$ *is the Jordan algebra defined by a unital quadratic form* $(X, Q, 1)$ *as in* [**20**, 1.5], *where* X *is a finitely generated and projective* k*-module of rank* $\geqslant$2.

Proof. (a) Let $J = \mathrm{Jor}(X, Q, 1)$ with X finitely generated and projective of rank $\geqslant 2$. Thus

$$U_x y = B(x, \bar{y})x - Q(x)\bar{y}, \tag{1}$$

where B is the bilinear form associated with Q and $\bar{x} = T(x)1 - x$, with $T(x) = B(1, x)$. By [**20**, 1.5.2], J satisfies the polynomial $m(\mathbf{t}; x) = \mathbf{t}^2 - T(x)\mathbf{t} + Q(x)$, and we have $\deg J = 2$ because $\operatorname{rk} X \geqslant 2$, cf. 2.4(c). Hence J is generically algebraic of degree 2.

(b) Conversely, let J be generically algebraic of degree 2, with generic minimum polynomial $m(\mathbf{t}; x) = \mathbf{t}^2 - m_1(x)\mathbf{t} + m_2(x)$, and let X be the k-module underlying J. Because a Jordan algebra over a field is of degree 1 if and only if it is one-dimensional, the condition $\deg J = 2$ implies $\operatorname{rk} X \geqslant 2$. Hence the unit element $1_J = 1$ is a unimodular vector by 0.3.2. Next, $Q := m_2$ is a quadratic form, and $N(x) = m(0; -x) = Q(x)$, so $Q(1) = 1$ by Th. 2.11(a). Thus $(X, Q, 1)$ is a unital quadratic form in the sense of [**20**]. It remains to show that $J = \mathrm{Jor}(X, Q, 1)$ is the associated Jordan algebra, i.e., that (1) holds.

Let B be the bilinear form associated with Q and put $T(x) := B(1, x)$ as well as $\bar{x} := T(x)1 - x$. Now note that $m_1(x) = \partial_1 m_2\big|_x$ (by 2.11.10) $= B(1, x) = T(x)$, and $x^\sharp = m_1(x)1 - x$ (by 2.10.3) $= \bar{x}$. By density of $\mathbf{J}^\times$, it suffices to prove (1) for y invertible. Then $U_x y = x^{(2,y)} = m_1^{(y)}(x)x - m_2^{(y)}(x)1^{(y)} = F_1(x, y)x - F_2(x, y)y^{-1}$. Furthermore, $F_1(x, y) = F_1(x, \bar{\bar{y}}) = \partial_x N\big|_{\bar{y}} = B(x, \bar{y})$ by 3.5.3, and $y^{-1} = y^\sharp / N(y)$ (by 2.11.5) $= \bar{y}/Q(y)$, as well as $F_2(x, y) = Q(x)Q(y)$ by 3.4.1. Hence $U_x y$ is given by (1).

3.8. Example. Not every Jordan algebra J which is finitely generated and projective as a k-module and whose degree is constant equal to 2 is generically algebraic of degree 2 and (hence the Jordan algebra of a unital quadratic form). For example, let $J = k \cdot 1 \oplus k \cdot a$ be free of rank 2 as a k-module. It can be shown that there exists a unique Jordan algebra structure on J such that

$$a^2 = \beta a - \alpha 1, \quad a^3 = \beta a^2 - (\alpha + \delta)a + \gamma 1 \tag{1}$$

if and only if the constants $\alpha, \beta, \gamma, \delta$ in k satisfy the conditions

$$2\gamma = 2\delta = \beta\gamma = \beta\delta = \gamma^2 = \delta^2 = \gamma\delta = 0. \tag{2}$$

Suppose these conditions are satisfied. Then J has constant degree equal to 2. Indeed, by (2), γ and δ are nilpotent, so $\gamma_K = \delta_K = 0$ for all fields $K \in k$-**alg**. Thus J_K is just the commutative associative algebra $K[\mathbf{t}]/(\mathbf{t}^2 - \beta_K \mathbf{t} + \alpha_K 1)$ considered as a Jordan algebra, hence of degree 2. We claim that J is generically algebraic if and only if $\gamma = \delta = 0$. Indeed, assuming J to be generically algebraic, its generic minimum polynomial has the form $m(\mathbf{t}; x) = \mathbf{t}^2 - m_1(x)\mathbf{t} + m_2(x)1$. Now $0 = m(a; a) = a^2 - m_1(a)a + m_2(a)1$ shows, because 1 and a are a basis of J as a k-module, that $\beta = m_1(a)$ and $\alpha = m_2(a)$. Moreover, $0 = j_a\big(\mathbf{t}m(\mathbf{t}; a)\big) = a^3 - \beta a^2 + \alpha a$ implies, by (1), that $\gamma = \delta = 0$. Conversely, if $\gamma = \delta = 0$, then it is easy to see that J is the Jordan algebra associated with the unital quadratic form Q on J given by $Q(\lambda 1 + \mu a) = \lambda^2 + \lambda\mu\beta + \mu^2\alpha$, and is therefore generically algebraic of degree 2 by Cor. 3.7.

Since there are rings containing $\alpha, \ldots, \delta$ satisfying (2) with $(\gamma, \delta) \neq (0, 0)$, for example, $k = \mathbb{Z}/4\mathbb{Z}$ or the ring of dual numbers over a field of characteristic 2, this gives examples of Jordan algebras, free of rank 2 and of constant degree 2, which are not generically algebraic.

3.9. Corollary. (a) *Let J be generically algebraic of degree 3, with generic norm N and adjoint map $\sharp$. Then J is obtained by the general cubic construction* [**22**, Th. 1] *from the cubic norm structure* $(N, \sharp, 1)$.

(b) *Conversely, let $(N, \sharp, 1)$ be a cubic norm structure on a finitely generated and projective k-module X, let J be the Jordan algebra structure on X determined by $(N, \sharp, 1)$, and suppose that* $\deg J = 3$ *(as a function on* $\mathrm{Spec}(k)$*). Then J is generically algebraic of degree* 3.

Remark. In (b), $\deg J$ is a well-defined function on $\mathrm{Spec}(k)$ by 2.1, because X is finitely generated and projective. Unlike the degree 2 case, a blanket assumption on the rank of X is not sufficient to guarantee that $\deg J = 3$, cf. [**30**, 2.4 – 2.6].

Proof. (a) We first verify the conditions required for $(N, \sharp, 1)$: Condition (i) $x^{\sharp\sharp} = N(x)x$, holds by 2.11.9, and condition (ii) $F_1(x, y^\sharp) = \partial_x N\big|_y$, holds by 3.5.3. Condition (iii) says $1 \times y = m_1(y)1 - y$: By 2.10.3, $x^\sharp = x^2 - m_1(x)x + m_2(x)1$. Linearization yields $x \times y = x \circ y - m_1(x)y - m_1(y)x + \partial_x m_2\big|_y$, and putting $x = 1$ results in

$$\begin{aligned} 1 \times y &= 1 \circ y - m_1(1)y - m_1(y)1 + \partial_1 m_2\big|_y \\ &= 2y - 3y - m_1(y)1 + 2m_1(y) \qquad \text{(by 2.11.2 and 2.11.10)} \\ &= -y + m_1(y)1. \end{aligned}$$

The remaining conditions (iv) $1^\sharp = 1$ and (v) $N(1) = 1$ are clear from Th. 2.11. Now the same formal calculation as in [**23**, Th. 1] shows that $U_x y = F_1(x, y)x - x^\sharp \times y$.

(b) It only remains to show that J satisfies the polynomial $m(\mathbf{t}; x) = \mathbf{t}^3 - T(x)\mathbf{t}^2 + S(x)\mathbf{t} - N(x)$ (where we use the notations of [**22**]). Now $x^3 - T(x)x^2 + S(x)x - N(x)1 = 0$ is [**22**, (20)], and $x^4 = U_x x^2 = U_x\big(x^\sharp + T(x)x - S(x)1\big)$ (by [**22**, (21)]) $= N(x)x + T(x)x^3 - S(x)x^2$ (by [**22**, (24)]), as desired.

3.10. Corollary. *Let J be generically algebraic and $x \in J$. Then for all polynomials $f(\mathbf{t}), g(\mathbf{t}) \in k[\mathbf{t}]$,*

$$F_i\big(f(x), g(x)\big) = m_i\big((fg)(x)\big). \tag{1}$$

In particular,

$$m_i(x^{l+n}) = F_i(x^l, x^n), \tag{2}$$

for all $l, n \in \mathbb{N}$.

Proof. By the standard density argument, we may assume $x = a$ primitive. Then let $E = E(a) = k[\mathbf{t}]/(m(\mathbf{t}; a))$ and $\pi\colon E^+ \to k[a]$ be as in Lemma 2.9, and let $z = \mathrm{can}(\mathbf{t})$ be the generator of E. The elements of E are of the form $y = f(z)$ where $f \in k[\mathbf{t}]$. If $w = g(z)$ is a second element of E, then $\pi(y) = f(a)$, $\pi(w) = g(a)$, and $\pi(yw) = (fg)(a)$. Hence, (1) is equivalent to

$$F_i(\pi(y), \pi(w)) = m_i(\pi(yw)), \tag{3}$$

for all $y, w \in E$. By 2.9.1, $N(\pi(y)) = m(0; -\pi(y)) = \det L(y)$, and $\check{m}(\mathbf{t}; \pi(y)) = \det(\mathrm{Id} - \mathbf{t}L(y))$, for all $y \in E$. Again by density, it suffices to prove (3) for all invertible $w \in E$. Then also $\pi(w)$ is invertible in J with inverse $\pi(w^{-1})$, and we have

$$\begin{aligned} \check{m}^{(\pi(w))}(\mathbf{t}; \pi(y)) &= N(\pi(w))N(\pi(w^{-1}) - \mathbf{t}\pi(y)) \quad \text{(by 3.1.2)} \\ &= \det L(w) \det\big(L(w^{-1}) - \mathbf{t}L(y)\big) \\ &= \det(\mathrm{Id} - \mathbf{t}L(yw)\big) \text{ (because } E \text{ is commutative and associative)} \\ &= \check{m}(\mathbf{t}; \pi(yw)). \end{aligned}$$

Expanding both sides with 2.7.1 and using 3.5.1 yields (3).

3.11. An explicit formula for the F_i. Let J be generically algebraic of constant degree d. It is natural to ask for an explicit formula, expressing the F_i of Th. 3.5 in terms of the coefficients m_j of the generic minimum polynomial and generalizing 3.5.2 in case $i = 1$. The proof of 3.5 shows that $F_i = h_{ii}$ is the coefficient of $\lambda^i \mathbf{t}^i$ in 3.5.4. In order to free the index i for other purposes, we will use the letter p instead of i. In expanding the left hand side of 3.5.4, we are therefore only interested in terms containing $\lambda^p \mathbf{t}^p$. Thus, it is no restriction to assume $\lambda^{p+1} = 0$.

Define polynomial laws $g_{ip}(x, y)$ on $J \times J$, bihomogeneous of bidegree (i, p), by the expansion

$$N\big((1 - \lambda x)^{-1} - \mathbf{t}y\big) = N(1 + \lambda x + \cdots + \lambda^p x^p - \mathbf{t}y) \equiv (-\mathbf{t})^p \sum_{i=0}^{p} g_{ip}(x, y)\lambda^i, \quad (1)$$

where $\equiv$ means that both sides differ only by terms not involving $\mathbf{t}^p$. Then

$$\begin{aligned} N(1 - \lambda x)N\big((1 - \lambda x)^{-1} - \mathbf{t}y\big) &\equiv (-\mathbf{t})^p \Big(\sum_{i=0}^{p}(-1)^i m_i(x)\lambda^i\Big)\Big(\sum_{i=0}^{p} g_{ip}(x, y)\lambda^i\Big) \\ &= \lambda^p \mathbf{t}^p \Big(\sum_{i=0}^{p} g_{ip}(x, y)(-1)^i m_{p-i}(x)\Big) + \cdots \end{aligned}$$

where the dots indicate terms not involving λ^p, and therefore

$$F_p(x, y) = \sum_{i=0}^{p} g_{ip}(x, y)(-1)^i m_{p-i}(x). \quad (2)$$

It remains to compute the g_{ip}. Since $N(1 + z) = \check{m}(1; -z) = \sum_{j=0}^{d} m_j(z)$ by 2.7.1 and 2.11.1, we have

$$N(1 + \lambda x + \cdots + \lambda^p x^p - \mathbf{t}y) \equiv \sum_{j=p}^{d} m_j(-\mathbf{t}y + \lambda x + \cdots + \lambda^p x^p), \quad (3)$$

because $m_j = 0$ for $j > d$. Let $\mathbf{t}_0, \ldots, \mathbf{t}_p$ be indeterminates, and define the multihomogeneous polynomial laws $m_{i_0,\ldots,i_p}(x_0, \ldots, x_p)$ of multidegree $(i_0, \ldots, i_p)$ and total degree $j = i_0 + \cdots + i_p$ by the expansion

$$m_j(\mathbf{t}_0 x_0 + \cdots + \mathbf{t}_p x_p) = \sum_{i_0+\cdots+i_p=j} m_{i_0,\ldots,i_p}(x_0, \ldots, x_p)\mathbf{t}_0^{i_0} \cdots \mathbf{t}_p^{i_p},$$

cf. [**31**, Chap. II]. Note that the i_ν are $\geqslant 0$, and if $i_\nu = 0$ then $m_{i_0,\ldots,i_p}$ is independent of x_ν. Then we obtain from (3), putting $\tilde{x} = \lambda x + \cdots + \lambda^p x^p$ for short,

$$N(1 + \tilde{x} - \mathbf{t}y) \equiv (-\mathbf{t})^p \sum_{l=0}^{d-p} \sum_{i_1+\cdots+i_p=l} \lambda^{1i_1+2i_2+\cdots+pi_p} m_{p,i_1,\ldots,i_p}(y, x, x^2, \ldots, x^p). \quad (4)$$

Now collect the terms involving λ^i to obtain g_{ip}:

$$g_{ip}(x, y) = \sum_{l=0}^{d-p} \sum_{\substack{i_1+\cdots+i_p=l \\ 1i_1+2i_2+\cdots+pi_p=i}} m_{p,i_1,\ldots,i_p}(y, x, x^2, \ldots, x^p). \quad (5)$$

The sum over l in (5) actually runs only from 0 to $\min(p, d - p)$ because $l = i_1 + \cdots + i_p \leqslant 1i_1 + \cdots + pi_p = i$ and $0 \leqslant i \leqslant p$ by (1). Then formulas (2) and (5) together constitute the desired explicit expression for F_p. We note the following special cases:

$$F_2(x,y) = m_2(x)m_2(y) + m_{2,1}(y, x^2 - m_1(x)x) + m_{2,2}(x,y), \tag{6}$$

$$\begin{aligned} F_3(x,y) = {} & m_3(x)m_3(y) - m_{3,1}(y, x^3 - m_1(x)x^2 + m_2(x)x) \\ & + m_1(x)m_{3,2}(y,x) - m_{3,1,1}(y,x,x^2) - m_{3,3}(x,y). \end{aligned} \tag{7}$$

Finally note that, because the $F_i(x,y)$ are symmetric in x and y, so must be the right hand side of these formulas, which yields identities between the polarizations of the m_i.

Remark. An expansion similar to the right hand side of (4), but in a different context, occurs in [**27**, (1.13)] (personal communication by K. McCrimmon).

3.12. The exponential trace formula. Let J be generically algebraic. Switching x and y in Formula 3.5.3 we have $F_1(x^\sharp, y) = \partial_y N\big|_x$. For invertible x, this is equivalent to

$$\frac{\partial_y N\big|_x}{N(x)} = \partial_y \log N\big|_x = F_1(x^{-1}, y) \tag{1}$$

because $x^{-1} = x^\sharp/N(x)$. Let $k[[\mathbf{t}]]$ be the algebra of formal power series and put $\tilde{J} := J \otimes k[[\mathbf{t}]]$. Also let $x \in J$ be arbitrary. Then $1 - \mathbf{t}x \in \tilde{J}$ is invertible in $\tilde{J}$, with inverse given by $(1-\mathbf{t}x)^{-1} = \sum_{i=0}^\infty x^i \mathbf{t}^i$. Indeed, the formal sum on the right makes sense in $J[[\mathbf{t}]]$ (by which we mean the direct product of countably many copies $J \cdot \mathbf{t}^i$ ($i \in \mathbb{N}$) of J with the obvious operations making it a Jordan algebra) and has the right formal properties, so it suffices to show that $\tilde{J} = J[[\mathbf{t}]]$. Since J is finitely generated and projective there exist finitely many $v_j \in J$ and $\alpha_j \in J^*$ such that $\mathrm{Id}_J = \sum_{j=1}^l v_j \otimes \alpha_j$. Hence an element $\sum_{i=0}^\infty z_i \mathbf{t}^i \in J[[\mathbf{t}]]$ equals $\sum_{j=1}^l \varphi_j(\mathbf{t}) v_j$ where $\varphi_j(\mathbf{t}) = \sum_{i=0}^\infty \alpha_j(z_i)\mathbf{t}^i \in k[[\mathbf{t}]]$.

We now compute the logarithmic derivative with respect to $\mathbf{t}$ of

$$N(1 - \mathbf{t}x) = \check{m}(\mathbf{t}; x) = \sum_{i=0}^n (-1)^i m_i(x)\mathbf{t}^i$$

(by 2.7.1 and 2.11.1, with $n = \max\deg J$) in two ways. On the one hand,

$$\begin{aligned} \frac{d}{d\mathbf{t}} \log N(1-\mathbf{t}x) &= N(1-\mathbf{t}x)^{-1} \frac{d}{d\mathbf{t}} \check{m}(\mathbf{t}; x) \\ &= N(1-\mathbf{t}x)^{-1} \cdot \sum_{i=1}^n (-1)^i i\, m_i(x)\mathbf{t}^{i-1}. \end{aligned} \tag{2}$$

On the other hand, by (1), the chain rule and 3.10.2,

$$\begin{aligned} \frac{d}{d\mathbf{t}} \log N(1-\mathbf{t}x) &= F_1((1-\mathbf{t}x)^{-1}, -x) \\ &= -\sum_{i=0}^\infty F_1(x^i, x)\mathbf{t}^i = -\sum_{i=0}^\infty m_1(x^{i+1})\mathbf{t}^i. \end{aligned} \tag{3}$$

Combining (2) and (3), we have

$$\sum_{i=1}^n (-1)^i i\, m_i(x)\mathbf{t}^{i-1} = \Big(\sum_{i=0}^n (-1)^i m_i(x)\mathbf{t}^i\Big)\Big(-\sum_{i=0}^\infty m_1(x^{i+1})\mathbf{t}^i\Big).$$

By comparing coefficients at powers of $\mathbf{t}$, one sees recursively that $i!\,m_i(x)$ is a polynomial with coefficients in $\mathbb{Z}$ in $m_1(x), \ldots, m_1(x^i)$. The first two terms are

$$2m_2(x) = m_1(x)^2 - m_1(x^2), \tag{4}$$
$$6m_3(x) = m_1(x)^3 - 3m_1(x)m_1(x^2) + 2m_1(x^3). \tag{5}$$

Explicit formulas for all i are known and involve the cycle indicator polynomials, see, e.g., [**21**, §4].

Now assume k is a $\mathbb{Q}$-algebra. Then we can integrate and exponentiate formula (3) and obtain the *exponential trace formula*

$$N(1 - \mathbf{t}x) = \exp\Big(- \sum_{i=1}^{\infty} m_1(x^i) \frac{\mathbf{t}^i}{i} \Big). \tag{6}$$

Remark. In [**1**, Th. 1.10], formula (3) is proved in a different way for the special case $J = \mathrm{End}(M)$ (cf. 2.4(d)), and is referred to as the exponential trace formula, although (6) seems to be more deserving of this name.

4. Generically power-associative algebras

4.1. Definition. Let J be a Jordan algebra over k. For every $R \in k$-**alg** we define

$$\mathbf{J}_{\mathrm{pa}}(R) := \{a \in J_R : \ a \text{ strictly power-associative}\},$$

cf. 1.6. From the very definition of strict power-associativity it is evident that $\mathbf{J}_{\mathrm{pa}}$ is a subfunctor of $\mathbf{J}$. We claim that it is in fact a hard subsheaf of $\mathbf{J}$. After a base change, this just means that it has the following descent property: If $a \in J$ and a_R is strictly power-associative for some faithfully flat $R \in k$-**alg**, then a is strictly power-associative as well. Thus we must show that $\mathrm{pr}_1 \colon M(a_S) \to J_S$ is injective, for all $S \in k$-**alg**. Now the S-algebra $R_S = R \otimes S$ is in particular flat over S, so the canonical map $M(a_S) \otimes_S R_S \to M(a_S \otimes_S 1_{R_S})$ is an isomorphism by Lemma 1.3(d). We can consider $R_S \cong S \otimes R = S_R$ as an R-algebra, and then $a_S \otimes_S 1_{R_S} = a \otimes_k 1_{R \otimes S} = a_R \otimes_R 1_{S_R}$ are canonically identified. Also, since a_R is strictly power-associative, $\mathrm{pr}_1 \colon M(a_R \otimes_R 1_{S_R}) \to J_R \otimes_R S_R$ is injective. From the commutative diagram

$$\begin{array}{ccc} M(a_S) \otimes_S R_S & \xrightarrow{\mathrm{pr}_1 \otimes \mathrm{Id}_{R_S}} & J_S \otimes_S R_S \\ \cong \downarrow & & \downarrow \cong \\ M(a_R \otimes_R 1_{S_R}) & \xrightarrow[\mathrm{pr}_1]{} & J_R \otimes_R S_R \end{array}$$

we see that $M(a_S) \otimes_S R_S \to J_S \otimes R_S$ is injective. Since R_S is faithfully flat over S, it follows that $M(a_S) \to J_S$ is injective, as desired.

4.2. Lemma. *Let J be a Jordan algebra over k and let $a \in J$ be algebraic of degree d. Consider the following conditions:*

(i) *a is strictly power-associative,*
(ii) *$a^0, \ldots, a^{d-1}$ are k-free and span a direct summand of J,*
(iii) *$a^0 \wedge \cdots \wedge a^{d-1}$ is unimodular in $\bigwedge^d J$.*

Then (iii) $\iff$ (ii) $\implies$ (i)*. If J is finitely generated and projective as a k-module or if k is a field then all conditions are equivalent.*

Proof. (iii) $\iff$ (ii) follows from Lemma 0.6.

(ii) $\Longrightarrow$ (i): Since a is algebraic of degree d, $M(a)$ is free with basis $a^{[0]}, \dots, a^{[d-1]}$ by 1.4.6. Now $\mathrm{pr}_1(a^{[i]}) = a^i$ shows that $\mathrm{pr}_1\colon M(a) \to k[a]$ is a k-module isomorphism. Hence a is power-associative and $k[a]$ is pure, being a direct summand. By 1.6.2, a is strictly power-associative.

Now let J be finitely generated and projective, and suppose (i) holds. Then $M(a)$ is pure by Prop. 1.5(a), so $k[a]$ is pure by 1.6.2 and therefore a direct summand by 0.15(d). As $\mathrm{pr}_1\colon M(a) \to k[a]$ is an isomorphism and $a^{[0]}, \dots, a^{[d-1]}$ is a basis of $M(a)$, we have (ii). Finally, if k is a field, $k[a]$ is automatically a direct summand, so the same argument applies.

4.3. Lemma. *Let J be a Jordan algebra over a field K and let $a \in J$ be an algebraic element of degree $d \leqslant 3$. Then $a^0, \dots, a^{d-1}$ are linearly independent.*

Proof. There are the following cases:

$d = 0$: Then $J = \{0\}$ and the empty set is linearly independent.

$d = 1$: Then $J \neq \{0\}$ and $a^0 = 1_J \neq 0$ is linearly independent.

$d = 2$: Assume that 1 and a are linearly dependent. Then $a = \lambda 1$ for some $\lambda \in K$, hence, $a^2 = \lambda^2 1 = \lambda a$. This shows that a satisfies the polynomial $\mathbf{t} - \lambda$ of degree 1, contradicting the fact that $\mu_a(\mathbf{t})$ has degree 2.

$d = 3$: Assume again, by way of contradiction, that $1, a, a^2$ are linearly dependent. We must have 1 and a linearly independent, else $a = \lambda 1$ and $\mu_a(\mathbf{t}) = \mathbf{t} - \lambda$ as in the previous case. Thus $a^2 \in K \cdot 1 \oplus K \cdot a$, and since $\mu_a(\mathbf{t})$ has degree 3, a^3 is a linear combination of $1, a, a^2$, hence of 1 and a. It follows that $K[a] = K \cdot 1 \oplus K \cdot a$, so there exist unique $\alpha, \beta, \gamma, \delta \in K$ such that

$$a^2 = \alpha 1 + \beta a, \qquad a^3 = \alpha a + \beta a^2 + \gamma 1 + \delta a. \tag{1}$$

It suffices to show that $\gamma = \delta = 0$, because then (1) says that a satisfies the degree 2 polynomial $\mathbf{t}^2 - \beta \mathbf{t} - \alpha 1$, contradicting the fact that $\deg a = 3$. If K has characteristic $\neq 2$ then the first equation (1) implies $a \circ a^2 = 2a^3 = 2\alpha a + 2\beta a^2$, and we are done. If K has characteristic 2, we compute powers of a as follows, always using $2 = 0$ in K:

$$\begin{aligned} a^4 &= (a^2)^2 = (\alpha 1 + \beta a)^2 = \alpha^2 1 + \beta^2 a^2 && (2)\\ &= U_a a^2 = U_a(\alpha 1 + \beta a) = \alpha a^2 + \beta a^3 \\ &= \alpha a^2 + \alpha\beta a + \beta^2 a^2 + \beta\gamma 1 + \beta\delta a \\ &= \alpha^2 1 + 2\alpha\beta a + \beta^2 a^2 + \beta\gamma 1 + \beta\delta a. && (3) \end{aligned}$$

From (2) and (3) we see by comparing coefficients at 1 and a and using (1), that $\beta\gamma = \beta\delta = 0$. Thus we are done if $\beta \neq 0$. Now assume $\beta = 0$ and compute fifth and sixth powers:

$$\begin{aligned} a^5 &= U_{a^2} a = U_{\alpha 1} a = \alpha^2 a \\ &= U_a a^3 = U_a\big(\gamma 1 + (\alpha + \delta) a\big) \\ &= \gamma a^2 + (\alpha + \delta) a^3 = \alpha\gamma 1 + (\alpha + \delta)\big(\gamma 1 + (\alpha + \delta) a\big). \end{aligned}$$

Comparing coefficients at a shows $\alpha^2 = (\alpha + \delta)^2 = \alpha^2 + \delta^2$, whence $\delta = 0$. Next,

$$\begin{aligned} a^6 &= (a^2)^3 = \alpha^3 1 \\ &= (a^3)^2 = (\gamma 1 + \alpha a)^2 = \gamma^2 1 + \alpha^2 a^2 = (\gamma^2 + \alpha^3) 1, \end{aligned}$$

which implies $\gamma = 0$ and completes the proof.

4.4. Corollary. *Let J be a (possibly infinite-dimensional) Jordan algebra over a field K which is generically algebraic of degree $\leqslant 3$ in the sense of* [**16**]*. Then J is strictly power-associative in the sense of* [**23**]*; i.e., every element of every base field extension of J is power-associative.*

This is obvious from Lemma 4.2 and Lemma 4.3. Note, however, that it is not clear whether all elements of J_R, R a commutative K-algebra, are power-associative as well.

4.5. Proposition. *Let J be finitely generated and projective as a k-module.*

(a) $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{alg}}$ *is an open finitely presented subscheme of* $\mathbf{J}_{\mathrm{alg}}$.

(b) *Algebraic elements of degree $\leqslant 3$ are strictly power-associative, that is,* $\coprod_{d\leqslant 3} \mathbf{J}_{\mathrm{alg},d} \subset \mathbf{J}_{\mathrm{pa}}$.

Proof. (a) By Prop. 1.14(b), it suffices to show that $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{alg},d}$ is open and finitely presented, for all d. Define a morphism from $\mathbf{J}_{\mathrm{alg},d}$ to $(\bigwedge^d J)_{\mathbf{a}}$ by $x \mapsto x^0 \wedge \cdots \wedge x^{d-1}$ in all base extensions. Then Lemma 4.2(iii) says that $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{alg},d}$ is the inverse image of $(\bigwedge^d J)_{\mathbf{u}}$, whence the assertion.

(b) Let $a \in J$ be algebraic of constant degree $d \leqslant 3$ and let $\mathfrak{p} \in \mathrm{Spec}(k)$ be arbitrary. Then $a(\mathfrak{p}) \in J(\mathfrak{p})$ is algebraic of degree d as well, so Lemma 4.3 shows that $a(\mathfrak{p})^0, \ldots, a(\mathfrak{p})^{d-1}$ are linearly independent over $\boldsymbol{\kappa}(\mathfrak{p})$. Now Lemma 0.6 and Lemma 4.2 imply that a is strictly power-associative. Since the same argument works in all base ring extensions, it follows that $\mathbf{J}_{\mathrm{alg},d} \subset \mathbf{J}_{\mathrm{pa}}$ for $0 \leqslant d \leqslant 3$. Now $\coprod_{d\leqslant 3} \mathbf{J}_{\mathrm{alg},d} \subset \mathbf{J}_{\mathrm{pa}}$ follows because $\mathbf{J}_{\mathrm{pa}}$, being a hard sheaf (cf. 4.1), is in particular a local functor.

4.6. Definition. Let J be a generically algebraic Jordan algebra over k. By Lemma 2.6, $\mathbf{J}_{\mathrm{prim}}$ is an open dense subscheme of $\mathbf{J}$, contained in $\mathbf{J}_{\mathrm{alg}}$, and by Prop. 4.5(a), $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{alg}}$ is open in $\mathbf{J}_{\mathrm{alg}}$. Hence $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{prim}}$ is open in $\mathbf{J}$. We will say J is *generically power-associative* if $\mathbf{J}_{\mathrm{pa}} \cap \mathbf{J}_{\mathrm{prim}}$ is dense in $\mathbf{J}$. By 0.14 and Lemma 4.2, an equivalent condition is: For all $\mathfrak{p} \in \mathrm{Spec}(k)$, and letting K denote an algebraic closure of $\boldsymbol{\kappa}(\mathfrak{p})$, there exists an element $x \in J_K$ such that the powers $1, x, \ldots, x^{(\deg J(\mathfrak{p}))-1}$ are linearly independent over K.

4.7. Corollary. *Let J be generically algebraic over k. Any one of the following conditions is sufficient for J to be generically power-associative:*

(i) $2 \in k^\times$,
(ii) *$J = B^+$ where B is associative or alternative,*
(iii) $\deg J \leqslant 3$ *(as a function on* $\mathrm{Spec}(k)$*).*

Indeed, (i) and (ii) follow from (c) and (d) of 1.6, and (iii) is clear from Prop. 4.5(b).

4.8. Example. A Jordan algebra of degree 4 need not be generically power-associative, the simplest example being $J = k \cdot 1 \oplus k \cdot a \oplus k \cdot a^3$ where k is a ring with $2k = 0$. But there are such examples even over $\mathbb{Z}$. Let J be the algebra, free of rank 4 over $\mathbb{Z}$, with basis $1, a, b, a^3$ introduced in 1.6. It is easily seen that J is generically algebraic of degree 4, with generic minimum polynomial $m(\mathbf{t}; x) = (\mathbf{t} - \varphi(x))^4$ where φ is the linear form determined by $\varphi(1) = 1$ and $\varphi(a) = \varphi(b) = \varphi(a^3) = 0$. Then J is not generically power-associative, because for K a field of characteristic 2, the powers $1, x, x^2, x^3$ of any $x \in J_K$ are linearly dependent. Indeed, let us put $c = a^3$. The products in J are determined by the following relations:

$$U_a1 = a^2 = 2b, \quad U_a a = a^3 = a \circ b = c, \quad U_a b = U_a c = 0,$$
$$U_b = U_c = U_{a,c} = U_{b,c} = 0,$$
$$U_{a,b}1 = a \circ b = c, \quad U_{a,b}a = U_{a,b}b = U_{a,b}c = 0.$$

Now let R be an arbitrary commutative ring and denote the basis of J_R obtained by base change from $\mathbb{Z}$ to R again by $1, a, b, c$. Let $x = \lambda 1 + \alpha a + \beta b + \gamma c \in J_R$. Then the powers of x are

$$x^2 = \lambda^2 1 + 2\lambda\alpha a + 2(\lambda\beta + \alpha^2)b + (2\lambda\gamma + \alpha\beta)c,$$
$$x^3 = \lambda^3 1 + 3\lambda^2\alpha a + (3\lambda^2\beta + 6\lambda\alpha^2)b + (3\lambda^2\gamma + 3\lambda\alpha\beta + \alpha^3)c.$$

A straightforward computation shows that the determinant of the coefficients of $1, x, x^2, x^3$ with respect to the basis $1, a, b, c$ is

$$\det \begin{pmatrix} 1 & \lambda & \lambda^2 & \lambda^3 \\ 0 & \alpha & 2\lambda\alpha & 3\lambda^2\alpha \\ 0 & \beta & 2\lambda\beta + 2\alpha^2 & 3\lambda^2\beta + 6\lambda\alpha^2 \\ 0 & \gamma & 2\lambda\gamma + \alpha\beta & 3\lambda^2\gamma + 3\lambda\alpha\beta + \alpha^3 \end{pmatrix} = 2\alpha^6.$$

Hence J_R contains a power-associative element of degree 4 if and only if $2 \in R^\times$.

5. Algebras of degree 3

5.1. Theorem. *Let J and J' be generically algebraic Jordan algebras of degree 3 over a ring k and let m_1 and m_1' be the generic traces of J and J', respectively. Also let $f\colon J \to J'$ be an isomorphism of k-modules. Then the following conditions are equivalent:*

(i) *f is an isomorphism of Jordan algebras,*

(ii) *f preserves unit elements, squares and traces; i.e., $f(1_J) = 1_{J'}$, $f(x^2) = f(x)^2$, and $m_1'(f(x)) = m_1(x)$, for all $x \in J$.*

Remark. This theorem is of course only of interest in case 2 is not a unit in k, because otherwise the quadratic operators can be recovered from the squaring operation by the formula $2U_x y = x \circ (x \circ y) - x^2 \circ y$.

Proof. (i) $\Longrightarrow$ (ii): The first two conditions are obvious, and the third follows from Prop. 2.7(a).

(ii) $\Longrightarrow$ (i): First note that the conditions on f are preserved under arbitrary base change. We will show that f preserves third powers in all base ring extensions. Then the assertion will follow by differentiation, see also [**25**, Th. 1].

Let $\mathbf{U} := \mathbf{J}_{\rm prim} = \mathbf{J}_{\rm alg,3} \subset \mathbf{J}$ and $\mathbf{U}' := \mathbf{J}'_{\rm prim} = \mathbf{J}'_{\rm alg,3} \subset \mathbf{J}'$. By Lemma 2.6 these are open dense subschemes of $\mathbf{J}$ and $\mathbf{J}'$, respectively. Since f induces an isomorphism $f\colon \mathbf{J} \to \mathbf{J}'$ of schemes, $f^{-1}(\mathbf{U}')$ is dense in $\mathbf{J}$, hence $\mathbf{U} \cap f^{-1}(\mathbf{U}')$ is so as well. Thus it suffices to prove $f(x^3) = f(x)^3$ for all $x \in \mathbf{U}(R) \cap f^{-1}(\mathbf{U}'(R))$ and all $R \in k$-**alg**. Everything is invariant under base change, so we may replace R by k and assume $x \in J_{\rm prim} \cap f^{-1}(J'_{\rm prim})$.

Let $E = k[x]$ and $E' = k[y]$ where $y := f(x)$. By Prop. 4.5(b), x and y are strictly power-associative, so by Lemma 4.2, E and E' are free of rank 3 with bases $1 = 1_J, x, x^2$ and $1' = 1_{J'}, y, y^2$, respectively. Let $T = m_1$, $S = m_2$ and $N = m_3$ and denote the corresponding quantities for J' by T', S' and N'. Since x satisfies its generic minimum polynomial $m(\mathbf{t}; x) = \mathbf{t}^3 - T(x)\mathbf{t}^2 + S(x)\mathbf{t} - N(x)$, we have

$$x^3 = T(x)x^2 - S(x)x + N(x)1, \tag{1}$$
$$x^4 = T(x)x^3 - S(x)x^2 + N(x)x. \tag{2}$$

Substitution of (1) in (2) results in

$$x^4 = \big[T(x)^2 - S(x)\big]x^2 + \big[N(x) - S(x)T(x)\big]x + T(x)N(x)1. \tag{3}$$

Since f preserves squares and hence also fourth powers, f applied to (3) yields

$$y^4 = \big[T(x)^2 - S(x)\big]y^2 + \big[N(x) - S(x)T(x)\big]y + T(x)N(x)1'. \tag{4}$$

On the other hand, the analogue of (3) holds in J' for y, so we have

$$y^4 = \big[T'(y)^2 - S'(y)\big]y^2 + \big[N'(y) - S'(y)T'(y)\big]y + T'(y)N'(y)1'. \tag{5}$$

Since f preserves traces, we have $T(x) = T'(y)$. Hence it follows from (4) and (5) and the linear independence of $1', y, y^2$ that $S(x) = S'(y)$ and $N(x) = N'(y)$. Now f applied to (1) shows

$$f(x^3) = T(x)y^2 - S(x)y + N(x)1' = T'(y)y^2 - S'(y)y + N'(y)1' = y^3 = f(x)^3.$$

By our initial reduction, $f(x^3) = f(x)^3$ holds now for all $x \in \mathbf{J}(R)$ and all $R \in k$-**alg**. In particular, let $R = k(\varepsilon)$ (dual numbers) and let $x, y \in J$. Then $(x + \varepsilon y)^3 = x^3 + \varepsilon(x^2 \circ y + U_x y)$, and since f preserves squares and circle products, we also have $f(U_x y) = U_{f(x)} f(y)$. This completes the proof.

5.2. The characteristic 2 case. Let k be a commutative ring with $2k = 0$, and let J be a unital Jordan algebra over k. Then the k-module J becomes a 2-Lie algebra, denoted $\mathfrak{L}(J)$, with Lie bracket $[x, y] = x \circ y$ and second power operation $x^{[2]} = x^2$ [**13**, Ch. I, Th. 4].

From $1 \circ x = 2x = 0$ for all $x \in J$ it follows that $k \cdot 1_J$ is contained in the centre $Z(\mathfrak{L}(J))$ of $\mathfrak{L}(J)$. For a Jordan matrix algebra as in 2.4(b), it is easily seen that in fact

$$Z\big(\mathfrak{L}(\mathrm{H}_n(\mathcal{C}, k))\big) = k \cdot 1_J. \tag{1}$$

Now let J be generically algebraic of constant degree d and let $T = m_1$ be the generic trace. Then by 3.12.4, the trace commutes with the squaring operation:

$$T(x^2) = T(x)^2, \quad \text{for all } x \in J. \tag{2}$$

Linearization of (2) yields $T(x \circ y) = 2T(x)T(y) = 0$, which together with (2) shows that

$$J_0 = \operatorname{Ker} T \ \text{ is a 2-ideal of } \mathfrak{L}(J). \tag{3}$$

Assume in particular that d is odd. Then $T(1_J) = d \cdot 1_k$ (by 2.11.2) $= 1_k$, which implies

$$\mathfrak{L}(J) = k \cdot 1_J \oplus J_0 \tag{4}$$

is a direct sum of 2-Lie algebras.

Let $\mathfrak{g}$ and $\mathfrak{g}'$ be 2-Lie algebras over k. We denote the set of Lie algebra isomorphisms from $\mathfrak{g}$ to $\mathfrak{g}'$ by $\mathrm{Isom}_{\mathrm{Lie}}(\mathfrak{g}, \mathfrak{g}')$, and the set of 2-Lie algebra isomorphism by $\mathrm{Isom}_{\text{2-Lie}}(\mathfrak{g}, \mathfrak{g}')$, and employ similar notations for automorphism groups. Clearly, $\mathrm{Isom}_{\text{2-Lie}}(\mathfrak{g}, \mathfrak{g}') \subset \mathrm{Isom}_{\mathrm{Lie}}(\mathfrak{g}, \mathfrak{g}')$. Furthermore,

$$Z(\mathfrak{g}') = 0 \quad \Longrightarrow \quad \mathrm{Isom}_{\text{2-Lie}}(\mathfrak{g}, \mathfrak{g}') = \mathrm{Isom}_{\mathrm{Lie}}(\mathfrak{g}, \mathfrak{g}'). \tag{5}$$

Indeed, this follows easily from the formula $\mathrm{ad}(x^{[2]}) = (\mathrm{ad}\, x)^2$, valid in any 2-Lie algebra, and the fact that the adjoint representation of $\mathfrak{g}'$ is faithful.

5.3. Corollary. *We keep the assumptions of Theorem* 5.1 *and assume furthermore that* $2k = 0$*. Let* $\mathfrak{L}(J) = k \cdot 1_J \oplus J_0$ *and* $\mathfrak{L}(J') = k \cdot 1_{J'} \oplus J_0'$ *be the decompositions as in* 5.2.4*.*

(a) *The restriction map* res: $f \mapsto f_0 = f\big|J_0$ *is a bijection* res: $\mathrm{Isom}(J, J') \to \mathrm{Isom}_{2\text{-Lie}}(J_0, J_0')$*, and*

$$\text{res: } \mathrm{Aut}(J) \to \mathrm{Aut}_{2\text{-Lie}}(J_0) \tag{1}$$

is an isomorphism of groups.

(b) *Assume that in addition* $Z(\mathfrak{L}(J)) = k \cdot 1_J$ *and* $Z(\mathfrak{L}(J')) = k \cdot 1_{J'}$*; equivalently, that* J_0 *and* J_0' *have trivial centres. Then the assertions of* (a) *hold for* $\mathrm{Isom}_{\mathrm{Lie}}$ *and* $\mathrm{Aut}_{\mathrm{Lie}}$ *instead of* $\mathrm{Isom}_{2\text{-Lie}}$ *and* $\mathrm{Aut}_{2\text{-Lie}}$ *as well.*

Proof. (a) It is clear that an isomorphism f of Jordan algebras induces an isomorphism $f_0 = f\big|J_0$ of 2-Lie algebras. Conversely, let $f_0\colon J_0 \to J_0'$ be an isomorphism of 2-Lie algebras and extend f_0 to an k-module isomorphism $f\colon J \to J'$ by $f(1_J) = 1_{J'}$ and $f\big|J_0 = f_0$. Since $(\lambda 1_J + x_0)^2 = \lambda^2 1_J + 2\lambda x_0 + x_0^2 = \lambda^2 1_J + x_0^2$ for all $x_0 \in J_0$, we see that f satisfies the conditions (ii) of Th. 5.1, and therefore is an isomorphism of Jordan algebras.

(b) From 5.2.4 and the assumption on the centres of $\mathfrak{L}(J)$ and $\mathfrak{L}(J')$ it follows that J_0 and J_0' have trivial centres as Lie algebras. Now the assertion is clear from 5.2.5.

Using the fact that Δ is a derivation if and only if $\mathrm{Id} + \varepsilon\Delta$ is an automorphism (where $k(\varepsilon)$ is the ring of dual numbers), it is easy to formulate an infinitesimal version of Cor. 5.3 which we leave to the reader. In particular, 5.2.1 and Cor. 5.3(b) imply the following result:

5.4. Corollary. *Let* $J = \mathrm{H}_3(\mathcal{C}, k)$ *be the Jordan algebra of* 3×3 *hermitian matrices over a composition algebra* $\mathcal{C}$ *over* k *with scalar diagonal entries as in* 2.4(b)*, and assume that* $2k = 0$*. Then* $\mathrm{Aut}_{2\text{-Lie}}(J_0) = \mathrm{Aut}_{\mathrm{Lie}}(J_0)$ *and* $\mathrm{Der}_{2\text{-Lie}}(J_0) = \mathrm{Der}_{\mathrm{Lie}}(J_0)$*. The restriction maps* $\mathrm{Aut}(J) \to \mathrm{Aut}_{\mathrm{Lie}}(J_0)$ *and* $\mathrm{Der}(J) \to \mathrm{Der}_{\mathrm{Lie}}(J_0)$ *are isomorphisms of groups and of* 2*-Lie algebras, respectively.*

References

[**1**] G. Almkvist, *Endomorphisms of finitely generated projective modules over a commutative ring*, Ark. Mat. **11** (1973), 263–301.

[**2**] R. Bix, *Separable Jordan algebras over commutative rings. III*, J. Algebra **86** (1984), no. 1, 35–59.

[**3**] N. Bourbaki, *Commutative Algebra*, Hermann, Paris, 1972, Translated from the French.

[**4**] ———, *Elements of mathematics. Algebra, Part I: Chapters 1-3*, Hermann, Paris, 1974, Translated from the French.

[**5**] H. Braun and M. Koecher, *Jordan-Algebren*, Grundlehren der mathematischen Wissenschaften, vol. 128, Springer-Verlag, Berlin, 1966.

[**6**] M. Demazure and P. Gabriel, *Groupes algébriques*, vol. 1, Masson, Paris, 1970.

[**7**] M. Demazure and A. Grothendieck, *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin, 1962/1964.

[**8**] D. Ferrand, *Un foncteur norme*, Bull. Soc. Math. France **126** (1998), no. 1, 1–49.

[**9**] ———, *Monogenous algebras. Back to Kronecker*, Preprint, 2004.

[**10**] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 24, 231.

[11] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28, 255.

[12] N. Jacobson, *Generic norm of an algebra*, Osaka Math. J. **15** (1963), 25–50.

[13] ———, *Lectures on quadratic Jordan algebras*, Tata Institute of Fundamental Research, Bombay, 1969, Lectures on Mathematics, No. 45.

[14] ———, *Structure and Representations of Jordan Algebras*, Amer. Math. Soc. Colloq. Publ., vol. 39, Amer. Math. Soc., 1969.

[15] ———, *Structure theory of Jordan algebras*, University of Arkansas Lecture Notes in Mathematics, vol. 5, University of Arkansas, Fayetteville, Ark., 1981.

[16] N. Jacobson and J. Katz, *Generically algebraic quadratic Jordan algebras*, Scripta Math. **29** (1973), 215–227.

[17] M. A. Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991.

[18] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999.

[19] O. Loos, *Jordan pairs*, Lecture Notes in Math., vol. 460, Springer-Verlag, 1975.

[20] ———, *Tensor products and discriminants of unital quadratic forms over commutative rings*, Mh. Math. **122** (1996), 45–98.

[21] ———, *Trace and norm for reduced elements of Jordan pairs*, Comm. Algebra **25** (1997), no. 9, 3011–3042.

[22] K. McCrimmon, *The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras*, Trans. Amer. Math. Soc. **139** (1969), 495–510.

[23] ———, *The Freudenthal-Springer-Tits constructions revisited*, Trans. Amer. Math. Soc. **148** (1970), 293–314.

[24] ———, *Homotopes of alternative algebras*, Math. Ann. **191** (1971), 253–262.

[25] ———, *Quadratic Jordan algebras and cubing operations*, Trans. Amer. Math. Soc. **153** (1971), 265–278.

[26] ———, *The generic norm of an isotope of a Jordan algebra*, Scripta Math. **29** (1973), no. 3-4, 229–236.

[27] ———, *A characterization of the nondegenerate radical in quadratic Jordan triple systems*, Algebras Groups Geom. **4** (1987), no. 2, 145–164.

[28] H. P. Petersson, *Composition algebras over algebraic curves of genus zero*, Trans. Amer. Math. Soc. **337** (1993), 473–491.

[29] H. P. Petersson and M. L. Racine, *Radicals of Jordan algebras of degree 3*, Radical theory, Proc. 1st Conf., Eger/Hung. 1982, Colloq. Math. Soc. János Bolyai 38, 1985, pp. 349–377.

[30] ———, *Jordan algebras of degree 3 and the Tits process*, J. of Algebra **98** (1986), 211–243.

[31] N. Roby, *Lois polynomes et lois formelles en théorie des modules*, Ann. Sci. École Norm. Sup. (3) **80** (1963), 213–348.

[32] W. C. Waterhouse, *Symmetric determinants and Jordan norm similarities in characteristic* 2, Proc. Amer. Math. Soc. **93** (1985), no. 4, 583–589.