Jacobson, N.
Osaka Math. J.
15 (1963), 25–50.

GENERIC NORM OF AN ALGEBRA*

Dedicated to Professor K. Shoda on his sixtieth birthday

By

NATHAN JACOBSON

The notions of the rank or principal polynomial of an associative algebra and the corresponding notions of trace and norm are classical. These notions have been generalized recently by the author ([13, I]) to apply to strictly power associative algebras, and we have renamed these concepts the generic minimal polynomial, trace and norm, since this terminology appears to be more in keeping with present day usage in analogous situations. In our paper we investigated the groups of linear transformations which preserve the norms in special central simple Jordan algebras. This applies to central simple associative algebras as a special case. In a later paper ([13, III]) we studied the norm preserving groups of exceptional central simple Jordan algebras. The groups obtained in this way are generalizations of the complex Lie group E_6 and include certain geometrically defined subgroups of the collineation groups of Cayley planes.

In this paper we shall give a systematic study of generic norms for strictly power associative algebras. We shall first answer a question on the multiplicative property of the generic norm which was left open in our first paper: We shall prove that $M(ab)=M(a)M(b)$ holds if $M(x)$ is any irreducible factor of the generic norm $N(x)$ which is normalized so that $M(1)=1$, and a, b are contained in an associative subalgebra of the given algebra. Assuming the base field is large enough we shall determine all the homogeneous polynomials $Q(x)$, $x=\sum \xi_i u_i$, ξ_i indeterminates, (u_i) a basis, which satisfy multiplicative properties in a strictly power associative algebra. In particular, we shall show that if $\mathfrak{A}$ is associative simple and the base field is large enough then $Q(ab)=Q(a)Q(b)$ for all $a, b \in \mathfrak{A}$ implies that Q is a power of the generic norm.

This result is well known for $\mathfrak{A}=\Phi_n$ the algebra of $n\times n$ matrices

* This research has been supported by the U.S. Air Force under grant SAR-G-AFOSR-61-29.

over Φ and it includes a theorem on multiplicative polynomial functions on fields which is due to Flanders ([9]). Our results are applicable also to alternative algebras and will be used in a forthcoming paper by Schafer ([19]) on forms of degree n which permit composition.

A second aspect of the norm theory deals with Jordan algebras. For these we prove a Jordan multiplicative property: $M(\{aba\})=M(a)^2M(b)$ where $\{aba\}=2(ba)a-ba^2$ and $M(x)$ is any normalized irreducible factor of the generic norm $N(x)$. Again assuming Φ is large enough we can determine all homogeneous polynomials $Q(x)$ having this property. We shall consider also the question as to how completely an algebra is determined by its generic norm. In this connection we shall show that under mild restrictions on Φ, equivalence of generic norms for Jordan algebras one of which is separable implies u-isotopy of the algebras ([15]). This implies that if $\mathfrak{A}$ and $\mathfrak{B}$ are associative algebras, $\mathfrak{B}$ separable simple, and $\mathfrak{A}$ and $\mathfrak{B}$ have equivalent generic norms then $\mathfrak{A}$ and $\mathfrak{B}$ are either isomorphic or anti-isomorphic. The Jordan multiplicative property of the generic norm implies that this function is Lie invariant under multiplications by elements of generic trace 0. This and a result of Tits' ([21]) permit us to extend to the characteristic p case a result of [13, I] on the Lie algebra of linear transformations having N as Lie invariant.

1. Generic minimum polynomial. We recall that a (not necessarily associative) algebra $\mathfrak{A}$ is called power associative if the subalgebras generated by single elements are associative and $\mathfrak{A}$ is strictly power associative if $\mathfrak{A}_\Omega$, the algebra obtained by extending the base field Φ of $\mathfrak{A}$ to the extension field Ω ($\mathfrak{A}_\Omega=\Omega\otimes_\Phi\mathfrak{A}$) is power associative for every Ω. Throughout this paper we deal exclusively with algebras which are finite dimensional over a field, are strictly power associative, and have identity elements. Wherever the term "algebra" is used without modifiers in the sequel, it will be understood that all of these conditions hold. "Subalgebra" will mean subalgebra containing 1 and "homomorphism" will mean algebra homomorphism in the usual sense such that $1\to 1$.

Let $\mathfrak{A}$ be an algebra and let $(u_1, u_2, \cdots, u_n)$ be a basis for $\mathfrak{A}$ over Φ. Let $\xi_1, \xi_2, \cdots, \xi_n$ be indeterminates and $P=\Phi(\xi_1, \xi_2, \cdots, \xi_n)$ the field of rational expressions in the ξ_i with coefficients in Φ. We form the algebra $\mathfrak{A}_P$ and consider the element $x=\sum \xi_i u_i$ of the algebra. We call this a generic element of the algebra $\mathfrak{A}$ over Φ. Let

$$(1) \qquad m_x(\lambda) = \lambda^m-\sigma_1(x)\lambda^{m-1}+\cdots+(-1)^m\sigma_m(x)$$

be the minimum polynomial of x as element of the power associative

algebra $\mathfrak{A}_P$. Then it can be shown that the $\sigma_i(x)$ are polynomials in the ξ's, that is, $\sigma_i(x) \in \Phi[\xi_1, \xi_2, \cdots, \xi_n]$ ([13, I]). Of particular interest are the first and last coefficients which we denote also as $\sigma_1(x) = T(x)$, $\sigma_m(x) = N(x)$. The polynomial $\sigma_i(x)$ is homogeneous of degree i in the ξ's and $m_x(\lambda)$ is homogeneous of degree m in λ and the ξ's. A change of basis from (u_i) to (v_i) where $v_i = \sum \mu_{ij} u_j$ gives a new generic element $y = \sum \xi_i v_i = \sum \xi_i \mu_{ij} u_j$. It follows that $m_y(\lambda)$, $T(y)$, $N(y)$ are obtained from $m_x(\lambda)$, $T(x)$, $N(x)$ respectively by substituting $\xi_j \to \sum_i \xi_i \mu_{ij}$ in the latter polynomials. In this sense $m_x(\lambda)$, $T(x)$, $N(x)$ are determined by $\mathfrak{A}$ over Φ. Accordingly, we shall call these the *generic minimum polynomial*, *generic trace* and *generic norm of the algebra*. The degree m of $m_x(\lambda)$ in λ (or in λ and the ξ's) will be called the *degree of the algebra*.

Now let a be an element of $\mathfrak{A}$. We can write $a = \sum_1^n \alpha_i u_i$ and specialize $\xi_i \to \alpha_i$ in $m_x(\lambda)$, $T(x)$, $N(x)$. This will give a polynomial

$$(2) \qquad m_a(\lambda) = \lambda^m - \sigma_1(a)\lambda^{m-1} + \cdots + (-1)^m \sigma_m(a)$$

$\in \Phi[\lambda]$ and elements $T(a)$, $N(a) \in \Phi$. These are respectively the *generic minimum polynomial*, *generic trace* and *generic norm of the element a*. It is easily seen that these objects are unchanged under a change of basis for $\mathfrak{A}$ (and hence of the generic element) and that $m_a(a) = 0$. Hence $m_a(\lambda)$ is divisible by the minimum polynomial $\mu_a(\lambda)$ of a. It is clear also that $m_a(\lambda)$, $T(a)$, $N(a)$ are unchanged under extension of the base field: If Ω is an extension of Φ and we identify $\mathfrak{A}$ with a subset of $\mathfrak{A}_\Omega$ then $m_a(\lambda)$, $T(a)$, $N(a)$ are the same if a is considered as an element of $\mathfrak{A}$ or as an element of $\mathfrak{A}_\Omega$. On the other hand, these objects may change if $\mathfrak{A}$ is replaced by a subalgebra $\mathfrak{B}$ or the base field Φ is changed. Consequently, we shall sometimes require the more precise notations $m_{a,\mathfrak{A}|\Phi}(\lambda)$, $T_{\mathfrak{A}|\Phi}(a)$, $N_{\mathfrak{A}|\Phi}(a)$ or $m_{a,\mathfrak{A}}(\lambda)$, $T_{\mathfrak{A}}(a)$, $N_{\mathfrak{A}}(a)$ for $m_a(\lambda)$, $T(a)$, $N(a)$. We remark also that if we consider the algebra $\mathfrak{A}_P$, $P = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$ then $m_x(\lambda)$ is the generic minimum polynomial of the element x of this algebra. A similar statement can be made for $N(x)$, so $N(x) = N_{\mathfrak{A}_P}(x)$ and $T(x) = T_{\mathfrak{A}_P}(x)$.

The following result is known

Theorem 1. *Let $\mathfrak{A}$ be a finite dimensional strictly power associative algebra containing 1 and let $m_a(\lambda)$, $T(a)$, $N(a)$ be the generic minimum polynomial, trace and norm of a, $\mu_a(\lambda)$ the minimum polynomial of a. Then:*

(i) $T(\alpha a) = \alpha T(a)$, $\alpha \in \Phi$, $T(a+b) = T(a) + T(b)$

(ii) $N(\alpha a) = \alpha^m N(a)$, $N(ab) = N(a)N(b)$ *if a, b are in a subalgebra*

$\Phi[c]$ *generated by an element* c.

(iii) $N(\lambda 1-a)=m_a(\lambda)$

(iv) $T(1)=m$, $N(1)=1$

(v) *every irreducible factor of* $m_a(\lambda)$ *is a factor of* $\mu_a(\lambda)$

(vi) $m_{a^\eta}(\lambda)=m_a(\lambda)$ *if* η *is an isomorphism or anti-isomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{A}^\eta=\mathfrak{B}$.

(vii) *the coefficients of* $m_a(\lambda)$ *are Lie invariant under derivation.*

In (iii) the left hand side is the generic norm of the element $\lambda 1-a$ contained in the algebra $\mathfrak{A}_{\Phi(\lambda)}$ where $\Phi(\lambda)$ is the field of rational expressions in the indeterminate λ. The meaning of (vii) is that if $\sigma_i(x)\in\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ is one of the coefficients of $m_x(\lambda)$ as in (1) and D is a derivation in $\mathfrak{A}$ over Φ then the congruence $\sigma_i(a+(aD)t)\equiv\sigma_i(a) \pmod{t^2}$ holds in $\Phi[t]$, t an indeterminate. Parts (i)-(vi) of Th. 1 have been proved in [13, I]. Part (vii) is due to Tits and will appear in [21].

It is useful to introduce the analogue of the adjoint of a matrix. We define

$$(3)\qquad adj\, a = \sigma_{m-1}(a)1-\sigma_{m-2}(a)a+\cdots+(-1)^{m-1}a^{m-1}.$$

Then $\mathrm{adj}\, a\in\Phi[a]$ and the relation

$$(4)\qquad a(adj\, a) = N(a)1$$

is equivalent to $m_a(a)=0$.

Now assume the characteristic of Φ is either 0 or a prime $p>m$. Then we set

$$(4)\qquad (a_1, a_2, \cdots, a_m) = \frac{1}{m!}[N(a_1+a_2+\cdots+a_m) - \sum_i N(a_1+\cdots+\hat{a}_i+\cdots+a_m)+\sum_{i<j} N(a_1+\cdots+\hat{a}_i+\cdots+\hat{a}_j+\cdots+a_m)-\cdots+(-1)^{m-1}\sum N(a_i)]$$

where the $\wedge$ indicated omission of the term appearing directly below it. Then $(a_1, a_2, \cdots, a_m)$ is symmetric and multilinear and $N(a)=(a, a, \cdots, a)$. Hence

$$\begin{aligned} m_a(\lambda) &= \lambda^m-\sigma_1(a)\lambda^{m-1}+\cdots+(-1)^m\sigma_m(a) = N(\lambda 1-a)\\ &= (\lambda 1-a, \lambda 1-a, \cdots, \lambda 1-a). \end{aligned}$$

If we differentiate this with respect to λ $(m-i)$-times and set $\lambda=0$ we obtain the formula

$$(m-i)!\,(-1)^i\sigma_i(a)=(-1)^i\frac{m!}{i!}(\overbrace{a, \cdots, a}^{i}, 1, \cdots, 1).$$

Hence we have

$$\sigma_i(a) = \binom{m}{i}(\overbrace{a, \cdots, a}^{i}, 1, \cdots, 1) \tag{4}$$

In particular, $T(a) = m(a, 1, \cdots, 1)$.

2. Multiplicative properties of the generic norm. We shall now show that the multiplicative property of N given in Th. 1 (iii) is valid whenever a, b are contained in a associative subalgebra of $\mathfrak{A}$. This was conjectured in [13, I]. We shall in fact prove a stronger result on factors of $N(x)$. In general, we denote elements of $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ as $M(x)$, $Q(x)$, etc., where x is the generic element $x = \sum \xi_i u_i$. If $M(x)$ is a factor of $N(x)$ in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ then $N(1) = 1$ implies that $M(1) \neq 0$. Hence we can multiply $M(x)$ by a suitable element of Φ and obtain $M(1) = 1$. A polynomial having this property will be called *normalized.* Clearly $N(x)$ has a unique factorization in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ as a product of normalized irreducible factors. We shall show that these normalized irreducible factors are multiplicative on associative subalgebras of $\mathfrak{A}$. For the present the base field Φ is arbitrary.

Lemma 1. *Let x be a generic element of $\mathfrak{A}$ and let*

$$m_x(\lambda) = \pi_1(\lambda, x)\pi_2(\lambda, x) \cdots \pi_r(\lambda, x) \tag{5}$$

be the factorization of $m_x(\lambda)$ into irreducible factors with leading coefficient 1 in λ in $\Phi[\lambda, \xi_1, \cdots, \xi_n]$. Then

$$N(x) = \pi_1(0, x)\pi_2(0, x) \cdots \pi_r(0, x) \tag{6}$$

is a factorization of $N(x)$ into irreducible factors in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$.

Proof. We may assume $u_1 = 1$ in the basis $(u_1, u_2, \cdots, u_n)$. Set $\varphi_i(\xi_1, \xi_2, \cdots, \xi_n) = \pi_i(0, x)$. Then we have to show that every $\varphi_i(\xi_1, \xi_2, \cdots, \xi_n)$ is irreducible. If this is not the case, we may assume that $\varphi_1(\xi) = \eta(\xi)\zeta(\xi)$ where these are polynomials of positive degrees in the ξ's. Then

$$\begin{aligned}\varphi_1(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n) \\ = \eta(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n)\zeta(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n)\end{aligned}$$

and, since $m_x(\lambda) = N(\lambda 1 - x)$,

$$\begin{aligned}m_x(\lambda) = \eta(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n)\zeta(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n)\varphi_2(\lambda - \xi_1, \\ -\xi_2, \cdots, -\xi_n) \cdots \varphi_r(\lambda - \xi_1, -\xi_2, \cdots, -\xi_n).\end{aligned}$$

This is a factorization of $m_x(\lambda)$ as a product of $r+1$ factors of positive

degree in $\Phi[\lambda, \xi_1, \cdots, \xi_n]$. This contradicts the fact that (5) is a factorization into irreducible factors.

Lemma 2. *Let $\mathfrak{B}$ be a subalgebra of $\mathfrak{A}$ and let $y=\sum_1^r \eta_j v_j$ be a generic element of $\mathfrak{B}$, η's indeterminates, $x=\sum \xi_i u_i$ a generic element of $\mathfrak{A}$. If $v_j=\sum \rho_{ji} u_i$ then we let $m_y(\lambda)$ and $N(y)$ be the polynomials which are obtained from $m_x(\lambda)$ and $N(x)$ by the substitutions $\xi_i \to \sum_j \eta_j \rho_{ji}$. Then $m_y(\lambda)$ and $m_{y,\mathfrak{B}}(\lambda)$ have the same irreducible factors (except for multiplicities) in $\Phi[\lambda, \eta_1, \cdots, \eta_r]$ and $N(y)$ and $N_{\mathfrak{B}}(y)$ have the same irreducible factors in $\Phi[\eta_1, \cdots, \eta_r]$.*

Proof. We extend the base field to $\Delta=\Phi(\eta_1, \eta_2, \cdots, \eta_r)$. Then $m_y(\lambda)$ and $N(y)$ are respectively the generic minimum polynomial and norm of the element $y=\sum \eta_j v_j$ of $\mathfrak{A}_\Delta$. Since $m_{y,\mathfrak{B}}(\lambda)$ is the minimum polynomial of y, Th. 1 (v) shows that $m_{y,\mathfrak{B}}(\lambda)$ and $m_y(\lambda)$ have the same irreducible factors in $\Delta[\lambda]$. Since these are polynomials in λ and the η's with leading coefficient of λ equal 1, it follows that they have the same irreducible factors in $\Phi[\lambda, \eta_1, \cdots, \eta_r]$. By Lemma 1, the irreducible factors of $N_{\mathfrak{B}}(y)$ in $\Phi[\eta_1, \eta_2, \cdots, \eta_r]$ are associates of the polynomials $\pi(0, y)$ where $\pi(\lambda, y)$ is an irreducible factor of $m_{y,\mathfrak{B}}(\lambda)$. The proof of Lemma 1 shows also that a similar statement can be made for $N(y)$ and $m_y(\lambda)$. It follows that $N(y)$ and $N_{\mathfrak{B}}(y)$ have the same irreducible factors in $\Phi[\eta_1, \cdots, \eta_r]$.

Lemma 3. *Let $\mathfrak{A}$ be associative and let $M(x)$ be a normalized irreducible factor of $N(x)$ in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$. Then*

$$M(ab) = M(a)M(b) \tag{7}$$

for all $a, b \in \mathfrak{A}$.

Proof. Since the product of multiplicative functions is multiplicative, it suffices to prove (7) for Φ algebraically closed. We take 1-1 representation $a \to A$ $(1 \to 1)$ of $\mathfrak{A}$ by matrices in the $N \times N$ matrix algebra Φ_N. This can be taken in reduced form:

$$A = \begin{pmatrix} A_1 & & \\ & A_2 & * \\ & & \ddots \\ 0 & & \\ & & A_k \end{pmatrix}, \quad A_i \in \Phi_{n_i}, \tag{8}$$

where $a \to A_i$ are irreducible matrix representations. The generic element x of $\mathfrak{A}$ is represented by

$$X = \begin{pmatrix} X_1 & & & \\ & X_2 & & * \\ & & \ddots & \\ & 0 & & X_k \end{pmatrix}. \tag{9}$$

Now the generic norm in the matrix algebra Φ_N is the determinant. Hence, if we identify $\mathfrak{A}$ with its image in Φ_N, x with X, then Lemma 2 implies that $M(x)$ is an irreducible factor of $\det X = \det X_1 \det X_2 \cdots \det X_k$. We shall now show that every $\det X_i$ is irreducible in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$. Since Φ is algebraically closed, Burnside's theorem shows that we can choose n_i^2 elements $a^{(jk)} \in \mathfrak{A}$ such that the i-th component matrices $A_i^{(jk)}$ in (8) form a basis for the complete matrix algebra Φ_{n_i}. We may assume that the $a^{(jk)}$ are part of a basis for $\mathfrak{A}$ over Φ. If we set all the ξ's except those attached to the $a^{(jk)}$ equal 0 then X_i becomes a generic element of Φ_{n_i}. It is well known that $\det X_i$ is irreducible if X_i is generic. Hence $\det X_i$ is irreducible for x generic in $\mathfrak{A}$. It now follows that $M(x) = \det X_i$ for some i. Since $a \to A$ and the determinant are multiplicative, (7) is valid for all a, b in $\mathfrak{A}$.

We can now prove

Theorem 2. *Let $\mathfrak{A}$ be an algebra as in Th. 1 and let $M(x)$ be a normalized irreducible factor in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ of the generic norm $N(x)$. Then*

$$M(ab) = M(a)M(b) \tag{10}$$

holds if a and b are contained in an associative subalgebra $\mathfrak{B}$ of $\mathfrak{A}$.

Proof. Let $y = \sum_1^r \eta_j v_j$ be a generic element of $\mathfrak{B}$. Then $M(y)$ is a factor of $N(y)$ and so this is a product of normalized irreducible factors of $N(y)$. By Lemma 2, these are irreducible factors of $N_{\mathfrak{B}}(y)$. Hence, by Lemma 3, they are multiplicative for $a, b \in \mathfrak{B}$. Hence (10) holds for $a, b \in \mathfrak{B}$.

Evidently Th. 2 implies that if $M(x)$ is a product of normalized irreducible factors of $N(x)$ then $M(ab) = M(a)M(b)$ holds for a, b in any associative subalgebra $\mathfrak{B}$. If $\mathfrak{A}$ is alternative, any two elements generate an associative subalgebra. Hence $M(x)$ is multiplicative for all a, b in an alternative algebra.

We shall show next that the multiplicative properties given in Ths. 1 and 2 are characteristic of products of normalized irreducible factors of $N(x)$. The precise result we can prove is the following

Theorem 3. *Let $\mathfrak{A}$ be a strictly power associative finite dimensional*

algebra with an identity. Let $x=\sum_1^n \xi_i u_i$ *be a generic element of* $\mathfrak{A}$ *and* $Q(x)$ *a non-zero homogeneous polynomial of degree* q *in* $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$. *Let* $|\Phi|$ *be the cardinal number of* Φ, m *the degree of* $\mathfrak{A}$. *Assume either one of the following two sets of conditions*:

(α) $Q(ab)=Q(a)Q(b)$ *for all* a *and* $b\in\Phi[a]$, $|\Phi|>qm$

(β) $Q(ab)=Q(a)Q(b)$ *for all* a, b *and* $|\Phi|>q$.

Then $Q(x)$ *is a product of normalized irreducible factors of the generic norm* $N(x)$ *of* $\mathfrak{A}$.

Proof. Assume (α) and introduce additional indeterminates $\eta_1, \eta_2, \cdots, \eta_m$. Set $y=\eta_1+\eta_2 x+\cdots+\eta_m x^{m-1}\in\mathfrak{A}_\Omega$, $\Omega=\Phi(\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_m)$, and consider the polynomial $F(x, y)=Q(x)Q(y)-Q(xy)$. This is a polynomial of degree at most qm in the ξ's and q in the η's. The usual proof of the theorem on specialization of non-zero polynomials with coefficients in an infinite field shows that if F is a non-zero polynomial with coefficients in a field Φ and Φ contains more elements than the maximum degree of F in any of the indeterminates then values can be chosen for the indeterminates in Φ so that $F\neq 0$ for these values. Since (α) implies that $F(x, y)=0$ for all $x=a$, $y=b$ and $|\Phi|>qm$ we see that $F(x, y)=0$ in $\Phi[\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_m]$. Now consider the relation (4) for the generic element x: $x(adj\, x)=N(x)1$. We have $adj\, x=\sigma_{m-1}(x)-\sigma_{m-2}(x)x+\cdots+(-1)^{m-1}x^{m-1}$ and the $\sigma_i(x)$ are polynomials in the ξ's. Since $F(x, y)=0$ we have on specializing $\eta_1=\sigma_{m-1}(x)$, $\eta_2=-\sigma_{m-2}(x)$, etc. that $F(x, adj\, x)=0$. Thus we have the relation

$$
\begin{aligned}
(11)\qquad Q(x)Q(adj\, x) &= Q(x\ adj\, x)\\
&= Q(N(x)1)\\
&= Q(1)N(x)^q .
\end{aligned}
$$

The multiplicative property and the assumption that $Q(x)\neq 0$ imply that $Q(1)=1$. Also $Q(adj\, x)\in\Phi[\xi_1, \cdots, \xi_n]$; hence (11) shows that $Q(x)$ is a factor of $N(x)^q$ in $\Phi[\xi_1, \cdots, \xi_n]$. Since $Q(x)$ is normalized ($Q(1)=1$) it follows that $Q(x)$ is a product of normalized irreducible factors of $N(x)$. A similar argument applies to (β). Here we use indeterminates $\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_n$ and the elements $x=\sum \xi_i u_i$, $y=\sum \eta_i u_i$ of $\mathfrak{A}_\Omega$, $\Omega=\Phi(\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_n)$. We consider the polynomial $F(x, y)=Q(x)Q(y)-Q(xy)$ which is of degree q in the ξ's and η's. Assumption (β) implies $F(x, y)=0$. The rest of the argument is a repetition of that used in (α).

We consider next the special case of Th. 3 in which $\mathfrak{A}$ is simple alternative. Then $\mathfrak{A}$ is either associative or is a Cayley algebra. If $\mathfrak{A}$

is associative, then Dieudonné ([8]) has proved that $m_x(\lambda)$ is irreducible. Hence, by Lemma 1, $N(x)$ is irreducible in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$. Dieudonné's argument is also applicable in the alternative case. (We shall consider this more fully for Jordan algebras in § 4.) Theorem 3 and irreducibility of $N(x)$ have the following

Corollary. *Let $\mathfrak{A}$ be a finite dimensional simple alternative algebra and $Q(x)$, $x=\sum \xi_i u_i$, a homogeneous polynomial of degree q such that $Q(ab)=Q(a)Q(b)$ for all $a, b \in \mathfrak{A}$. Assume $|\Phi| > q$. Then $Q(x)$ is a power of the generic norm $N(x)$.*

3. Generic norms for Jordan algebras. In the remainder of this paper we restrict our attention to Jordan algebras. We recall that this class of algebras is defined by the identities:

$$ab = ba\,, \quad (a^2b)a = a^2(ba)\,, \tag{12}$$

and it is assumed that the characteristic is $\neq 2$. We shall assume also that every algebra is finite dimensional and has an identity element. If $\mathfrak{A}$ is an associative algebra over a field of characteristic $\neq 2$ than $\mathfrak{A}$ defines a Jordan algebra $\mathfrak{A}^+$ whose vector space is the same as that of $\mathfrak{A}$ and whose multiplication is $ab=\frac{1}{2}(a\times b+b\times a)$ in terms of the given associative multiplication $\times$ in $\mathfrak{A}$. Such algebras and their subalgebras are called special Jordan algebra. The associative algebra $\mathfrak{A}$ and the Jordan algebra $\mathfrak{A}^+$ have the same power structure, that is, the associative power $a^{\times k}$ concides with the Jordan power a^k. Hence it is clear that $\mathfrak{A}$ and $\mathfrak{A}^+$ have the same generic minimum polynomials, norms and traces. Hence it is clear that the generic norm theory for Jordan algebras has direct application to associative algebras of characteristic $\neq 2$. These remarks apply also to alternative algebras of characteristic $\neq 2$ since it is true also that if $\mathfrak{A}$ is alternative then $\mathfrak{A}^+$ is a Jordan algebra.

In any Jordan algebra $\mathfrak{A}$ one has the important ternary composition

$$\{abc\} = (ab)c+(bc)a-(ac)b\,. \tag{13}$$

This satisfies a number of identities, the most noteworthy being

$$\begin{aligned} &\{aub\} = \{bua\}\,, \\ &\{\{\{aua\}ub\}ua\} = \{\{aua\}u\{bua\}\}\,, \end{aligned} \tag{14}$$

$$\{a\{b\{aca\}b\}a\} = \{\{aba\}c\{aba\}\}\,. \tag{15}$$

These are easily checked in special Jordan algebras since $\{abc\} = \frac{1}{2}(a\times b\times c+c\times b\times a)$ in terms of the associative multiplication $\times$.

Their validity for arbitrary Jordan algebras then follows from a general principle due to I. G. MacDonald to the effect that any identity in three variables which is of degree at most one in one of these will hold for all Jordan algebras if it holds for all special Jordan algebras ([18] or [14]).

Identities (14) have the following significance. If we fix u we can consider $\{aub\}$ as a u-product $a_u b$ of a and b. Then (14) states that this u-product satisfies the defining identities for Jordan algebras. If u is regular in $\mathfrak{A}$ in the sense that u has an inverse v in $\Phi[u]$ then the algebra $(\mathfrak{A}, u)$ with the multiplication $a_u b = \{aub\}$ has the identity element v. (See [15] for this and the other results stated here without proof.) The Jordan algebra $(\mathfrak{A}, u)$ is called the u-isotope of $\mathfrak{A}$. The relation between $(\mathfrak{A}, u)$ and $\mathfrak{A}$ is a symmetric one. If $\mathfrak{A}$ is an associative algebra the u-isotope $(\mathfrak{A}^+, u)$ of the Jordan algebra $\mathfrak{A}^+$ is isomorphic to $\mathfrak{A}^+$. To see this we define the multiplication $a \times_u b = a \times u \times b$ in $\mathfrak{A}$. This gives another associative algebra $\mathfrak{A}_u$ and the mapping $y \to yv$ $(v = u^{-1})$ is an isomorphism of $\mathfrak{A}$ onto $\mathfrak{A}_u$. Also it is clear that the u-isotope $(\mathfrak{A}^+, u)$ is the special Jordan algebra $\mathfrak{A}_u^+$. Hence $y \to yv$ is an isomorphism of $\mathfrak{A}^+$ onto $\mathfrak{A}_u^+ = (\mathfrak{A}^+, u)$. We recall also that isotopic algebras are not always isomorphic.

If we denote the mapping $y \to ya$ in $\mathfrak{A}$ as R_a and the mapping $y \to \{aya\}$ as U_a then (13) gives the relation $U_a = 2R_a^2 - R_{a^2}$. Also the identity (15) can be written in operator form as

$$U_a U_b U_a = U_{\{aba\}} . \tag{15'}$$

We now take up the theory of the generic norm of Jordan algebras. In [13, I] we verified by case considerations that the generic norm $N(x)$ of a central simple Jordan algebra satisfies the *Jordan multiplicative property* $N(\{aba\}) = N(a)^2 N(b)$. We shall now prove the following general result.

Theorem 4. *If $\mathfrak{A}$ is a Jordan algebra and $M(x)$ is a normalized irreducible factor in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ of the generic norm $N(x)$, then*

$$M(\{aba\}) = M(a)^2 M(b) \tag{16}$$

for all $a, b \in \mathfrak{A}$.

Proof. Let $\mathfrak{B}$ be the subalgebra generated by a and b. By a theorem of Shirshov-Cohn ([20] or [14] and [7]), $\mathfrak{B}$ is special so $\mathfrak{B}$ can be regarded also as a subalgebra of a special Jordan algebra $\mathfrak{E}^+$, $\mathfrak{E}$ associative. Let $y = \sum_1^r \eta_j v_j$ be a generic element of $\mathfrak{B}$. Then we know that $N(y)$

and $N_{\mathfrak{B}}(y)$ have the same irreducible factors in $\Phi[\eta_1, \eta_2, \cdots, \eta_r]$ (Lemma 2). Since $M(x)$ is a factor of $N(x)$, $M(y)$ is a factor of $N(y)$. Hence $M(y)$ is a product of normalized irreducible factors of $N_{\mathfrak{B}}(y)$ so it is enough to prove (16) for these factors. Now we can pass to the Jordan algebra $\mathfrak{F}^+$ which contains $\mathfrak{B}$ as a subalgebra. Let N^* denote the generic norm for this algebra. Then the irreducible factors of $N_{\mathfrak{B}}(y)$ coincide with those of $N^*(y)$. Let $N^*(y)=P_1(y)P_2(y)\cdots P_k(y)$ be the factorization of $N^*(y)$ into normalized irreducible factors in $\Phi[\eta_1, \eta_2, \cdots, \eta_r]$. Then (16) will follow if we can prove $P_i(\{aba\})=P_i(a)^2P_i(b)$, $1\leq i\leq k$, $a, b\in\mathfrak{B}$. This will follow by specialization if $P_i(\{aya\})=P_i(a)^2P_i(y)$ holds for $y=\sum\eta_j v_j\in\mathfrak{F}_\Delta^+$, $\Delta=\Phi(\eta_1, \eta_2, \cdots, \eta_r)$ and a in $\mathfrak{B}$. Now $N^*(y)$ is the generic norm in the associative algebra $\mathfrak{F}_\Delta$ and $\{aya\}=a\times y\times a$ in terms of the associative multiplication. Hence, by Th. 2, $N^*(\{aya\})=N^*(a)^2N^*(y)$.

We now fix a and consider the subalgebra $\Phi[a]$ generated by a. We may assume also that Φ is infinite and we shall apply some results from the theory of algebraic groups. Let G be the group of units of the polynomial algebra $\Phi[a]$. Since G is defined by $N^*(c)\neq 0$, G is an open subset of $\Phi[a]$ in the Zariski topology. Hence it suffices to prove $P_i(\{cyc\})=P_i(c)^2P_i(y)$ for all $c\in G$. If $c\in G$ we let $\bar{R}_c$ denote the multiplication $z\to zc$ in $\Phi[a]$. The image $\bar{R}(G)$ is a group of linear transformations in $\Phi[a]$ and $c\to\bar{R}_c$ is an isomorphism. Since the set of right multiplications in the commutative associative algebra $\Phi[a]$ can be characterized as the set of linear transformations which commute with all these multiplications, it is clear that $\bar{R}(G)$ is an algebraic group of linear transformation in the space $\Phi[a]$. Since $c\to\bar{R}_c$ is a polynomial mapping and G is an open subset of $\Phi[a]$, $\bar{R}(G)$ is an irreducible algebraic group. If we express $\{cyc\}$ in terms of the associative multiplication in $\mathfrak{F}_\Delta$ we see that $\{c_1\{c_2yc_2\}c_1\}=\{(c_1c_2)y(c_2c_1)\}$ for $c_i\in G$ and $\{c^{-1}\{cyc\}c^{-1}\}=y$ for $c\in G$. Hence if we write $y'=\sum\eta'_j v_j=\{cyc\}$ then $\eta'_j=\sum_1^r\gamma_{jk}\eta_k$ where the matrix $\gamma(c)=(\gamma_{jk})$ is non-singular and $c\to\gamma(c)$ is a group homomorphism of G (or $\bar{R}(G)$). Also it is clear that the mapping $\bar{R}_c\to\gamma(c)$ is a polynomial mapping. The mapping $y\to y'=\{cyc\}$ can be extended to an automorphism $A(c)$ in $\Phi[\eta_1, \eta_2, \cdots, \eta_r]$ and $\gamma(c)\to A(c)$ is an isomorphism, so $c\to A(c)$ and $\bar{R}_c\to A(c)$ are homomorphisms. If $c\in G$, $N^*(\{cyc\})=N^*(c)^2N^*(y)$ and $N^*(y)=P_1(y)P_2(y)\cdots P_k(y)$. Hence $P_i(y)^{A(c)}=\rho_iP_{i'}(y)$ where $i\to i'$ is a permutation $\pi(c)$ of $1, 2, \cdots, k$ and ρ_i is a non-zero element of Φ. It is clear that $c\to\pi(c)$ is a homomorphism of G into a finite group so the kernel H is a subgroup of finite index in G and $\bar{R}(H)$ is a subgroup of finite index in $\bar{R}(G)$. If $c\in H$, $P_i(\{cyc\})=\rho_iP_i(y)$, $1\leq i\leq k$, and since $P_i(1)=1$ and $P_i(\{c1c\})=P_i(c^2)=P_i(c)^2$, by Th.

2, we have $\rho_i = P_i(c)^2$. Hence $P_i(\{cyc\}) = P_i(c)^2 P_i(y)$, $1 \leq i \leq k$, holds for all $c \in H$. Conversely, these conditions insure that $c \in H$. Now these conditions show that H is an algebraic subset of G. Hence $\bar{R}(H)$ is an algebraic subgroup of $\bar{R}(G)$. Since $\bar{R}(G)$ is irreducible and $\bar{R}(H)$ is of finite index in $\bar{R}(G)$ we must have $\bar{R}(G) = \bar{R}(H)$ ([6], p. 86). Then $G = H$ and $P_i(\{cyc\}) = P_i(c)^2 P_i(y)$ holds for all c in G. This completes the proof.

We observe that if $M(x)$ satisfies (16) then so does $-M(x)$. Hence any product of normalized irreducible factors of $N(x)$ or the negative of such a product satisfies (16). On the other hand, we have

Theorem 5. *Let $Q(x)$ be a non-zero homogeneous polynomial of degree q in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ such that $Q(\{aba\}) = Q(a)^2 Q(b)$ for all a, b in the Jordan algebra $\mathfrak{A}$. Assume $|\Phi| > q^2$. Then $Q(x)$ is either a product of normalized irreducible factors of the generic norm $N(x)$ of $\mathfrak{A}$ or the negative of such a product.*

Proof. If we take $a = b = 1$ in the assumed relation we obtain $Q(1) = Q(1)^3$. Also taking $a = 1$ gives $Q(b) = Q(1)^2 Q(b)$. Since we can choose b so that $Q(b) \neq 0$ we see that $Q(1) \neq 0$ and $Q(1)^2 = \pm 1$. If we replace Q by $-Q$, if necessary, then we may assume $Q(1) = 1$. Set $x = \sum \xi_i u_i$, $y = \sum \eta_i u_i$, where the ξ's and η's are indeterminates and consider the polynomial $F(x, y) \equiv Q(\{xyx\}) - Q(x)^2 Q(y)$ in $\Phi[\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_n]$. This is of degree q^2 in the ξ's and of degree q in the η's. Moreover, $F(a, b) = 0$ for all $a, b \in \mathfrak{A}$. Since $|\Phi| > q^2$ this implies that $F(x, y) = 0$. Specialize $y = adj\, x$. Then we obtain $Q(\{x(adj\, x)x\}) = Q(x)^2 Q(adj\, x)$. Since $\{x(adj\, x)x\} = N(x)x$ this gives

$$N(x)^q Q(x) = Q(x)^2 Q(adj\, x)\,.$$

Hence $N(x)^q = Q(x) Q(adj\, x)$ which shows that $Q(x)$ is a product of irreducible factors of $N(x)$. Since $Q(1) = 1$ these can be taken to be normalized.

We shall now consider a Jordan multiplicative function which has been introduced by M. Koecher ([17]). We define $K(a) = \det U_a$ and, for the generic $x = \sum \xi_i u_i$ in $\mathfrak{A}_{\Phi(\xi_1, \cdots, \xi_n)}$, we define $K(x) = \det U_x$ where $U_x = 2R_x^2 - R_{x^2}$. Clearly, the entries of the matrix of U_x relative to the basis $(u_1, u_2, \cdots, u_n)$ are homogeneous quadratic polynomials in the ξ's. Hence $K(x)$ is a homogeneous polynomial of degree $2n$ in the ξ's. By (15) and the multiplicative property of determinants, we have $K(\{aba\}) = K(a)^2 K(b)$. Also $K(1) = 1$ since $U_1 = 1$. Hence we can apply Th. 5 to conclude that $K(x)$ is a product of irreducible factors occuring in $N(x)$. However, we can obtain a better result in another way. We recall that an element a is regular (has an inverse) if and only if the operator U_a has an inverse ([15]). Also, since $m_a(\lambda)$ and the minimum polynomial

$\mu_a(\lambda)$ have the same irreducible factors and a is regular if and only if $\mu_a(\lambda)$ is not divisible by λ it is clear that a is regular if and only if $N(a)\neq 0$. Since U_a is regular if and only if $K(a)=\det U_a\neq 0$ it is clear that we have the following situation: $N(a)=0$ if and only if $K(a)=0$. This is valid also in $\mathfrak{A}_\Omega$ where Ω is the algebraic closure of Φ. Hence, by the Hilbert Nullstellensatz we have

Theorem 6. *The polynomials $N(x)$ and $K(x)=\det U_x$ have the same irreducible factors (not counting multiplicities).*

We remark that this result permits the use of $K(x)$ in place of N^* in the first part of the proof of Th. 4. We remark also that if Φ is the field of real numbers or the field of complex numbers then the second part of the proof of Th. 4 can be replaced by a classical argument using the connectedness of the group G used in the proof.

4. Generic norm of a simple Jordan algebra. We now give a list of "standard" simple Jordan algebras over a field Φ together with their generic norms. If Φ is algebraically closed then any simple Jordan algebra will be isomorphic to one of the algebras of our list.

$A(m)=\Phi_m^+$, Φ_m, the associative algebra of $m\times m$ matrices over Φ. The generic norm of $a\in\Phi_m^+$ is $N(a)=\det a$.

$B(m)$, the subalgebra of Φ_m^+ of symmetric matrices. Here $N(a)=\det a$.

$C(m)$, the subalgebra of Φ_{2m}^+ of symplectic symmetric matrices. These are defined by the condition $q^{-1}a'q=a$ where a' is the transpose of a and $q=\begin{pmatrix} 0 & 1_m \\ -1_m & 0 \end{pmatrix}$. The condition on a is equivalent to $(qa)'=-qa$. The generic norm is $N(a)$ is the Pfaffian $Pf(qa)$.

D, the Jordan algebra of a non-degenerate symmetric bilinear form (a, b) of maximal Witt index in a vector space $\mathfrak{M}$ over Φ with $\dim\mathfrak{M}>1$. Here $D=\Phi 1\oplus\mathfrak{M}$ and multiplication is defined by $(\alpha 1+a)(\beta 1+b)=(\alpha\beta+(a,b))1+(\alpha b+\beta a)$ for α,β in Φ, a,b in $\mathfrak{M}$. We have $N(\alpha 1+a)=\alpha^2-(a,a)$.

E, the exceptional (non-special) Jordan algebra of 3×3 hermitian matrices over a split Cayley algebra C. These have the form

$$a=\begin{pmatrix} \alpha_1 & a_3 & \bar{a}_2 \\ \bar{a}_3 & \alpha_2 & a_1 \\ a_2 & \bar{a}_1 & \alpha_3 \end{pmatrix} \tag{17}$$

where the $a_i\in C$, $\bar{a}_i$ is the conjugate of a_i, and the $\alpha_i\in\Phi$. The generic norm is

$$N(a)=\alpha_1\alpha_2\alpha_3+T((a_1a_2)a_3)-\alpha_1N(a_1)-\alpha_2N(a_2)-\alpha_3N(a_3) \tag{18}$$

where T and N are the generic trace and norm in C: $T(c)=c+\bar{c}$, $N(c)=c\bar{c}=\bar{c}c$.

Lemma 1. *The generic norm of any one of the standard simple algebras listed above is irreducible. For every $\alpha\in\Phi$ there exists an element v in the algebra whose generic minimum polynomial is $\lambda^{m-1}(\lambda-\alpha)$.*

Proof. It is well known that the determinant of a generic matrix and of a generic symmetric matrix are irreducible ([5], pp. 176–177). The irreducibility for the generic norm for the algebras $C(m)$ is proved in [10]. (We remark that this is equivalent to the irreducibility of the Pfaffian of a generic skew symmetric matrix.) Also it is well known that a non-degenerate quadratic form in more than two variables is irreducible ([5], p. 137). Hence the first statement holds for the algebras $A-D$. It is clear from (17) that a suitable specialization of the generic element of the exceptional Jordan algebra E gives a generic element of the algebra $B(3)$. Moreover, N as defined in E reduces to the determinant of the symmetric matrix. Since the latter is irreducible, it follows that $N(x)$ is irreducible for x generic in E. To prove the second statement we take v to be the matrix with single entry α in the (1, 1)-position for $A(m)$, $B(m)$ or E. In D there exist non-zero orthogonal idempotents e_1 and e_2 such that $e_1+e_2=1$. We take $v=\alpha e_1$. If b is any $n\times n$ matrix then $v=\begin{pmatrix} b & 0 \\ 0 & b' \end{pmatrix}\in C(m)$. Take b in v to be the matrix α in the (1, 1)-position with 0's elsewhere. It is easy to check that the generic minimum polynomial of v is $\lambda^{m-1}(\lambda-\alpha)$.

Lemma 2. *Let $\mathfrak{A}$ be a central simple Jordan algebra over Φ. Then there exists a finite dimensional separable extension field Λ of Φ such that $\mathfrak{A}_\Lambda$ is a standard simple algebra.*

Proof. If $\mathfrak{A}$ is of degree two then $\mathfrak{A}$ is the Jordan algebra of a non-degenerate symmetric bilinear form in $\mathfrak{M}$ over Φ with $\dim\mathfrak{M}>1$. A suitable extension field of the form $\Delta=\Phi(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \cdots, \sqrt{\alpha_k})$ will make the extension of (a, b) to $\mathfrak{M}_\Delta$ have maximal Witt index. Since the characteristic is not two it is clear that Δ is separable. Then $\mathfrak{A}_\Delta$ is an algebra D of our list. If $\mathfrak{A}$ is special and not of degree two, it is known that either $\mathfrak{A}$ has the form $\mathfrak{E}^+$ where $\mathfrak{E}$ is central simple associative or $\mathfrak{A}$ is the subalgebra of J-symmetric elements of a simple associative algebra $\mathfrak{E}$ with an involution J where $\mathfrak{E}$ is either central or J is of second kind and the center of $\mathfrak{E}$ is a quadratic extension of Φ ([16]). If $\mathfrak{A}=\mathfrak{E}^+$, $\mathfrak{E}$ central simple associative then $\mathfrak{E}$ has a finite dimensional separable splitting field Δ. Then $\mathfrak{E}_\Delta\cong\Delta_m$ and $\mathfrak{E}_\Delta^+\cong\Delta_m^+$ so $\mathfrak{A}_\Delta$ is an algebra $\mathfrak{A}$ of

our list. If $\mathfrak{A}$ is the Jordan algebra of J-symmetric elements in a central simple Jordan algebra $\mathfrak{E}$ and Δ is a splitting field for $\mathfrak{E}$ then $\mathfrak{A}_\Delta$ is either an algebra C or it is an algebra of γ-symmetric matrices of Δ_m where γ is a diagonal matrix and γ-symmetry means $\gamma^{-1}a'\gamma=a$. If we take a suitable extension $\Delta(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \cdots, \sqrt{\alpha_m})$ we may replace γ by 1 and obtain an algebra B. Since Δ can be taken finite dimensional separable it is clear the result holds in this case. If $\mathfrak{A}$ is the set of J-symmetric elements of $\mathfrak{E}$ with involution of second kind and center Δ a quadratic extension of Φ then $\mathfrak{A}_\Delta$ is of the form $\mathfrak{E}^+$, $\mathfrak{E}$ central simple over Δ. The result then follows from an earlier case. It remains to consider the central simple exceptional Jordan algebras. Such an algebra is either a division algebra or it is reduced ([2]). In the first case, the base field has to be infinite: It is known also that if a and b are elements of $\mathfrak{A}$ whose coordinates do not satisfy a certain finite set of algebraic equations then the subalgebra $\mathfrak{B}$ generated by a and b is nine-dimensional central simple ([3]). Also since $\mathfrak{B}$ is generated by two elements it is special. It follows that $\mathfrak{A}$ contains a nine-dimensional special central simple subalgebra $\mathfrak{B}$. Hence a suitable finite dimensional separable extension field Δ of Φ produces a non-trivial idempotent in $\mathfrak{B}_\Delta$, so in $\mathfrak{A}_\Delta$. Then $\mathfrak{A}_\Delta$ is reduced. Finally, assume $\mathfrak{A}$ is reduced. Then $\mathfrak{A}$ is the set of 3×3 γ-hermitian Cayley matrices for some Cayley algebra C. If the Cayley algebra is split then we may take $\gamma=1$ and obtain the algebra E ([3]). Otherwise, a suitable quadratic extension Δ of Φ will make C_Δ split. Then $\mathfrak{A}_\Delta$ is the algebra E. This completes the proof.

We can now prove

Theorem 7. *The generic norm of any simple Jordan algebra $\mathfrak{A}$ over Φ is irreducible.*

Proof. Let Γ be the center of $\mathfrak{A}$, so Γ is a field. We consider first the case in which Γ is purely inseparable of exponent p^e, p the characteristic, and $\mathfrak{A}$ is standard over Γ. Let $(v_1=1, v_2, \cdots, v_r)$ be a basis for $\mathfrak{A}$ over Γ, $(\gamma_1=1, \gamma_2, \cdots, \gamma_h)$ a basis for Γ over Φ. Then $(\gamma_i v_j)$ is a basis for $\mathfrak{A}$ over Φ and if ζ_{ij} are indeterminates then $z=\sum \zeta_{ij}\gamma_i v_j$ is a generic element of $\mathfrak{A}$ over Φ. Let $x=\sum \xi_j v_j$ be a generic element of $\mathfrak{A}$ over Γ, $\overline{m}_x(\lambda)$ its minimum polynomial (in $\mathfrak{A}_{\Gamma(\xi_1,\cdots,\xi_r)}$). Then z is a root of $\overline{m}_z(\lambda)$ which is obtained from $\overline{m}_x(\lambda)$ by the replacements $\xi_j \to \sum_i \zeta_{ij}\gamma_i$. The coefficients of $\overline{m}_z(\lambda)$ are polynomials in the ζ's with coefficients in Γ. By Lemma 1, $\overline{m}_x(\lambda)$ is irreducible in $\Gamma[\lambda, \xi_1, \cdots, \xi_r]$. Now the specialization $\zeta_{ij}=0$ for $i>1$ converts z to $z'=\sum \zeta_{ij}v_j$ and $\overline{m}_z(\lambda)$ to $\overline{m}_{z'}(\lambda)$ which is obtained from $\overline{m}_x(\lambda)$ by the replacement $\xi_j \to \zeta_{ij}$. Hence $\overline{m}_{z'}(\lambda)$ and, à fortiori,

$\overline{m}_z(\lambda)$ is irreducible in $\Gamma(\lambda, \zeta_{ij}]$. Since Γ is of exponent p^e over Φ, $\overline{m}_z(\lambda)^{p^e} \in \Phi[\lambda, \zeta_{ij}]$. Let q be the smallest exponent such that $\overline{m}_z(\lambda)^q \in \Phi[\lambda, \zeta_{ij}]$. Then $\overline{m}_z(z)=0$ implies $\overline{m}_z(z)^q=0$. Hence $\overline{m}_z(\lambda)^q$ is divisible in $\Phi[\lambda, \zeta_{ij}]$ by the minimum polynomial $\overline{m}_z(\lambda)$ of z over $\Phi(\zeta_{ij})$. Since $\overline{m}_z(\lambda)$ is irreducible in $\Gamma(\lambda, \zeta_{ij}]$ and q is minimal it follows that $m_z(\lambda)=\overline{m}_z(\lambda)^q$. Since Γ is of exponent p^e over Φ we can choose $\alpha \in \Gamma$ such that the minimum polynomial of α over Φ is $\lambda^{p^e}-\alpha^{p^e}$. By Lemma 1, there exists a $v \in \mathfrak{A}$ whose generic minimum polynomial $\overline{m}_v(\lambda)$ in $\mathfrak{A}$ over Γ is $\lambda^{m-1}(\lambda-\alpha)$. Then the generic minimum polynomial of v in $\mathfrak{A}$ over Φ is $\lambda^{(m-1)q}(\lambda-\alpha)^q$. Hence $\alpha^q \in \Phi$ and since $\lambda^{p^e}-\alpha^{p^e}$ is the minimum polynomial of α over Φ, $q \geq p^e$. Hence $m_z(\lambda)=m_z(\lambda)^{p^e}$. If $k(\lambda)$ is a factor of $m_z(\lambda)$ in $\Phi[\lambda, \zeta_{ij}]$ of positive degree then $k(\lambda)=\overline{m}_z(\lambda)^r \in \Phi[\lambda, \zeta_{ij}]$. Hence $r=q=p^e$ and $k(\lambda)=m_z(\lambda)$. Thus $m_z(\lambda)$ is irreducible and hence $N(z)$ is irreducible in $\Phi[\zeta_{ij}]$. Next assume Γ is purely inseparable over Φ, $\mathfrak{A}$ arbitrary over Γ. By Lemma 2, there exists a separable extension Δ of Γ such that $\Delta \otimes_\Gamma \mathfrak{A}$ is standard. Since Δ is a separable extension of the purely inseparable extension Γ of Φ, $\Delta = \mathrm{E} \otimes_\Phi \Gamma$ where E is separable over Φ. Then $\mathfrak{A}_\mathrm{E} = \mathrm{E} \otimes_\Phi \mathfrak{A}$ has Δ as center and this algebra is standard over Δ. Also Δ is purely inseparable over the base field E. Hence, by the result just proved, the generic norm of $\mathfrak{A}_\mathrm{E}$ over E is irreducible. Consequently the generic norm of $\mathfrak{A}$ over Φ is irreducible. Next let $\mathfrak{A}$ be any algebra over a field Γ which is finite dimensional separable over Φ and suppose the generic norm of $\mathfrak{A}$ over Γ is irreducible. We claim that the generic norm of $\mathfrak{A}$ over Φ is irreducible. We use the bases and notations z, x, $\overline{m}_x(\lambda)$, $\overline{m}_z(\lambda)$ of the first part of this proof. Thus z is a generic element of $\mathfrak{A}$ over Φ, x a generic element of $\mathfrak{A}$ over Γ, $\overline{m}_x(\lambda)$ is the minimum polynomial of x and $\overline{m}_z(\lambda)$ is obtained from $\overline{m}_x(\lambda)$ by specialization. Then $\overline{m}_z(\lambda) \in \Gamma[\lambda, \zeta_{ij}]$ and $\overline{m}_z(z)=0$. Let Ω be the normal closure of Γ over Φ and let $s_1=1, s_2, \cdots, s_l$ be the distinct isomorphisms of Γ over Φ into Ω over Φ. Then if θ is a primitive element of Γ over Φ, the minimum polynomial of θ over Φ is $g(\lambda)=\prod_{k=1}^{l}(\lambda-\theta^{s_k})$. Consider the polynomial $\prod_{k=1}^{l}\overline{m}_z(\lambda)^{s_k}$. This is invariant under every automorphism of the Galois group of Ω over Φ. Hence it belongs to $\Phi[\lambda, \zeta_{ij}]$. Let $\Pi'\overline{m}_z(\lambda)^{s_k}$ be a product of the conjugates $\overline{m}_z(\lambda)^{s_k}$ of least degree having coefficients in Φ and having the factor $\overline{m}_z(\lambda)$. Then $\Pi'\overline{m}_z(z)^{s_k}=0$, so $\Pi'\overline{m}_z(\lambda)$ is divisible by $m_z(\lambda)$. On the other hand, since $\theta \in \Gamma$, the generic minimum polynomial $\overline{m}_\theta(\lambda)=(\lambda-\theta)^m$ and so $\Pi' m_\theta(\lambda)^{s_k}=\Pi'(\lambda-\theta^{s_k})^m$. Since this polynomial has coefficients in Φ and has θ as a root it is divisible by a power of the separable irreducible polynomial $g(\lambda)$. This implies that

$\Pi' = \prod_{k=1}^{l} \overline{m}_z(\lambda)^{s_k}$ so $\prod_{k=1}^{l} \overline{m}_z(\lambda)^{s_k}$ is the product of the conjugates $\overline{m}_z(\lambda)^{s_k}$ of least degree having coefficients in Φ and divisible by $\overline{m}_z(\lambda)$. This implies that $\prod_{k=1}^{l} \overline{m}_z(\lambda)^{s_k}$ is irreducible in $\Phi[\lambda, \zeta_{ij}]$. Since it is divisible by $\overline{m}_z(\lambda)$ we see that $m_z(\lambda) = \prod_{k=1}^{l} \overline{m}_z(\lambda)^{s_k}$ is irreducible. Hence $N(z)$ is irreducible in $\Phi[\zeta_{ij}]$. We can now complete the proof. Let $\mathfrak{A}$ be simple with center Γ and let E be the maximal separable subfield of Γ over Φ. Then Γ is purely inseparable over E. Hence the generic norm of $\mathfrak{A}$ over E is irreducible. Since E is separable over Φ the result we have just proved shows that the generic norm of $\mathfrak{A}$ over Φ is irreducible.

A number of other results are implicit in the foregoing proof. We state these without explicit proofs: (1) If $\mathfrak{A}$ is a purely inseparable field over Φ of exponent p^e then the generic norm $N(a) = a^{p^e}$, $a \in \mathfrak{A}$. (2) If $\mathfrak{A}$ is a separable field over Φ the generic norm coincides with the usual norm $n_{\mathfrak{A}|\Phi}(a)$. (3) If $\mathfrak{A}$ is simple with center Γ then $N_{\Gamma|\Phi}(N_{\mathfrak{A}|\Gamma}(a)) = N_{\mathfrak{A}|\Phi}(a)$. (4) If $\mathfrak{A}$ is arbitrary and the generic norm of $\mathfrak{A}$ over Γ is irreducible and Γ is finite dimensional separable over Φ then $N_{\Gamma|\Phi}(N_{\mathfrak{A}|\Gamma}(a)) = N_{\mathfrak{A}|\Phi}(a)$.

The following two results are immediate consequences of Ths. 5, 6 and 7.

Corollary 1. *Let $\mathfrak{A}$ be a simple Jordan algebra over Φ and let $Q(x)$ be a non-zero homogeneous polynomial of degree q in $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ such that $Q(\{aba\}) = Q(a)^2 Q(b)$ for all a, b in $\mathfrak{A}$. Assume $|\Phi| > q^2$. Then $Q(x) = \pm N(x)^k$.*

Corollary 2. *Let $\mathfrak{A}$ be a simple Jordan algebra. Then the degree m of $\mathfrak{A}$ is a divisor of $2n$, $n = \dim \mathfrak{A}$ and $K(x) = \det U_x = N(x)^{2n/m}$.*

5. Separable Jordan algebras. A Jordan algebra is said to be *separable* if it is a direct sum of simple algebras which have separable centers. An equivalent condition is that $\mathfrak{A}_\Omega$ is semi-simple (has no non-zero solvable ideals) for every extension field Ω of the base field. The main tool for studying separable Jordan algebras is the following criterion.

Theorem 8. *A Jordan algebra is separable if and only if the trace bilinear form $(a, b) \equiv T(ab)$ is non-degenerate.*

Proof. We note first that (a, b) is associative:

$$(ab, c) = (a, bc) \tag{19}$$

This is equivalent to $T(A(a, b, c)) = 0$ for $A(a, b, c)) = (ab)c - a(bc) = b[R_a, R_c]$.

Now $D_{a,c}=[R_a, R_c]$ is a derivation in $\mathfrak{A}$ and $T(bD)=0$ follows from Th. 1 (vii) for every derivation D. Hence (19) is valid. This relation implies that the radical $\mathfrak{A}^\perp$ of (a, b) is an ideal. If $\mathfrak{R}$ is the radical (maximal solvable ideal) of the algebra then $z^n=0$ for every $z\in\mathfrak{R}$. Then $T(z)=0$ and since $\mathfrak{R}$ is an ideal, $(z, a)=0$ for all a. Hence $\mathfrak{R}\subseteq\mathfrak{A}^\perp$. Hence non-degeneracy of (a, b) implies $\mathfrak{R}=0$. Also, since non-degeneracy of (a, b) is invariant under extension of the base field, $\mathfrak{A}_\Omega$ is semi-simple for every extension of Φ. Coversely, assume $\mathfrak{A}_\Omega$ is semi-simple for Ω the algebraic closure of Φ. Then $\mathfrak{A}_\Omega=\mathfrak{A}_1\oplus\mathfrak{A}_2\oplus\cdots\oplus\mathfrak{A}_k$ where the $\mathfrak{A}_i$ are ideals. It is easily seen that if $a\in\mathfrak{A}_\Omega$ and $a=a_1+a_2+\cdots+a_k$, $a_i\in\mathfrak{A}_i$ then $T(a)=T_1(a_1)+\cdots+T_k(a_k)$, T_i the generic trace in $\mathfrak{A}_i$. Also it is known that the trace bilinear form on the simple $\mathfrak{A}_i$ is non-degenerate ([13, I]). Hence (a, b) is non-degenerate.*

For base fields Φ of characteristic 0 or $p>m$, the degree of $\mathfrak{A}$, we have defined $(a_1, a_2, \cdots, a_m)$ by (4), that is, by linearizing the generic norm $N(a)$. Following Schafer, we shall say that $N(x)$ is non-degenerate on $\mathfrak{A}$ if $(b, a_2, \cdots, a_m)=0$ for all $a_i\in\mathfrak{A}$ implies $b=0$. We shall show that this is also a condition for separability of $\mathfrak{A}$. We require first

Theorem 9. *The generic norm of a Jordan algebra $\mathfrak{A}$ is Lie invariant under the multiplication R_a, $a\in\mathfrak{A}$, if and only if the generic trace $T(a)=0$.*

Proof. This will be a consequence of

$$N(b+tab)\equiv N(b)+N(b)T(a)t \pmod{t^2}. \tag{20}$$

We have

$$N(\{(1+ta)b(1+ta)\} = N(1+ta)^2N(b) \tag{21}$$

by Th. 4. Also $N(1+ta)\equiv 1+tT(a) \pmod{t^2}$ follows from $N(\lambda 1-a)=\lambda^m-T(a)\lambda^{m-1}+\cdots$. Hence we have $N(1+ta)^2\equiv 1+2T(a)t \pmod{t^2}$. Next we have

$$\begin{aligned}\{(1+ta)b(1-ta)\} &= 2(b(1+ta))(1+ta)-b(1+ta)^2\\ &\equiv b+2bat \pmod{t^2}.\end{aligned}$$

Hence, by (21),

$$N(b+2bat)\equiv(1+2T(a)t)N(b) \pmod{t^2}.$$

Replacing a by $\frac{1}{2}a$ gives (20).

---

* It is possible to prove this in another way which does not make use of the structure theory. We shall give such a proof in a forthcoming paper on Cartan subalgebras of Jordan algebras.

We can now prove

Theorem 10. *Let $\mathfrak{A}$ be a Jordan algebra of characteristic 0 or $p>m$ the degree of $\mathfrak{A}$. Then $\mathfrak{A}$ is separable if and only if the generic norm $N(x)$ is non-degenerate.*

Proof. We can linearize the relation (20) to obtain

$$(22)\qquad \begin{aligned}&(a_1b, a_2, \cdots, a_m)+(a_1, a_2b, a_3, \cdots, a_m)\\ &\quad+\cdots+(a_1, a_2, \cdots, a_{m-1}, a_mb)\\ &=T(b)(a_1, a_2, \cdots, a_m).\end{aligned}$$

We recall also that $T(a)=m(a, 1, \cdots, 1)$ (4). Suppose first that N is degenerate: there exists a $z\neq 0$ such that $(z, a_2, \cdots, a_m)=0$ for all a_i in $\mathfrak{A}$. Taking $a_2=\cdots=a_m=1$ gives $T(z)=0$. Taking $a_1=a$, $a_2=\cdots=a_m=1$, $b=z$ in (22) gives $T(az)=0$. Hence $(a, z)=0$ for all a and the trace form (a, b) is degenerate. Conversely, assume there exists a $z\neq 0$ such that $(z, a)=0$ for all a. Then the radical $\mathfrak{A}^{\perp}$ of the trace form is $\neq 0$. We have $(z, 1, \cdots, 1)=0$ and suppose we have already proved that $(z, a_2, \cdots, a_k, 1, \cdots, 1)=0$ for all $a_i\in\mathfrak{A}$, $z\in\mathfrak{A}^{\perp}$. Since $\mathfrak{A}^{\perp}$ is an ideal we have $(za_{k+1}, a_2, \cdots, a_k, 1, \cdots, 1)=0$ for all a_i. Then (22) and the symmetry of $(a_1, a_2, \cdots, a_m)$ imply that $(z, a_2, \cdots, a_{k+1}, 1, \cdots, 1)=0$. Hence $(z, a_2, \cdots, a_m)=0$ for all $a_i\in\mathfrak{A}$, $z\in\mathfrak{A}^{\perp}$ and $N(x)$ is degenerate. The result now follows from Th. 8.

6. Norm equivalence. Two algebras $\mathfrak{A}$ and $\mathfrak{B}$ are called *norm equivalent* if there exists a 1-1 linear mapping $a\to a^{\eta}$ of $\mathfrak{A}$ onto $\mathfrak{B}$ such that $N(a^{\eta})=\rho N(a)$ for all $a\in\mathfrak{A}$, where ρ is a non-zero element of Φ. Let $\mathfrak{A}$ be Jordan, u a regular element of $\mathfrak{A}$. We denote the generic norm in the isotope $(\mathfrak{A}, u)$ of $\mathfrak{A}$ by $N^{(u)}(a)$. The identity mapping is a norm equivalence of $\mathfrak{A}$ and $(\mathfrak{A}, u)$ since we have the following

Lemma. $N^{(u)}(a)=N(u)N(a)$, $a\in\mathfrak{A}$.

Proof. We may assume the base field is algebraically closed. Then u has a square root v in $\mathfrak{A}$. To see this we decompose $\Phi[u]=\mathfrak{B}_1\oplus\mathfrak{B}_2\oplus\cdots\oplus\mathfrak{B}_m$ where $\mathfrak{B}_i$ is an ideal of the form $\mathfrak{B}_i=\Phi e_i+\mathfrak{N}_i$, e_i the identity of $\mathfrak{B}_i$ and $\mathfrak{N}_i$ a nil ideal. Then $u=\sum b_i$, where $b_i=\alpha_i(e_i-4z_i)$, $\alpha_i\neq 0$, $z_i\in\mathfrak{N}_i$. The power series expansion for $(1-4\lambda)^{\frac{1}{2}}$ is

$$(1-4\lambda)^{\frac{1}{2}}=1-\sum_1^{\infty}\frac{2(2k-2)!}{k!(k-1)!}\lambda^k$$

which has integer coefficients. Since z_i is nilpotent

$$v_i = \alpha_i^{\frac{1}{2}}\left(e_i - \sum \frac{2(2k-2)!}{k!(k-1)!} z_i^k\right)$$

is defined and satisfies $v_i^2 = b_i$. Hence $v^2 = u$ for $u = \sum v_i$. Hence $N(\{vav\}) = N(u)N(a)$. We have

$$\{vav\}^m - T(\{vav\})\{vav\}^{m-1} + \cdots + (-1)^m N(\{vav\}) = 0 . \tag{23}$$

The subalgebra generated by v and a is special, so it may be considered as a subalgebra of an algebra $\mathfrak{E}^+$ where $\mathfrak{E}$ is associative. We have $\{vav\} = v \times a \times v$ in terms of the associative multiplication in $\mathfrak{E}$ and powers are the same in $\mathfrak{E}$ and $\mathfrak{E}^+$. Hence

$$\{vav\}^k = v \times a \times u \times a \times \cdots \times a \times v , \quad k\ a's .$$

If we use this in (23) and multiply the resulting relation left and right by v^{-1} we obtain

$$\begin{aligned} a \times u \times a \times \cdots \times a - T(\{vav\}) a \times u \times \cdots \times a \\ + \cdots + (-1)^m N(\{vav\}) u^{-1} = 0 . \end{aligned} \tag{24}$$

Using $\{aub\} = \frac{1}{2}(a \times u \times b + b \times u \times a)$ we can prove by induction that the k-th power of a in $(\mathfrak{A}, u)$ is

$$a^{k,u} = a \times u \times a \times \cdots \times a , \quad k\ a's . \tag{25}$$

Hence (24) can be written as

$$a^{m,u} - T(\{vav\}) a^{m-1,u} + \cdots + (-1)^m N(\{vav\}) u^{-1} = 0 . \tag{26}$$

Since u^{-1} is the identity for $(\mathfrak{A}, u)$ this is a polynomial equation for a in $(\mathfrak{A}, u)$. Moreover, the same argument shows that we have

$$x^{m,u} - T(\{vxv\} x^{m-1,u} + \cdots + (-1)^m N(\{vxv\}) u^{-1} = 0 \tag{27}$$

for x generic. Since the relation between $\mathfrak{A}$ and $(\mathfrak{A}, u)$ is a symmetric one it is clear that this is the minimum polynomial of x in $(\mathfrak{A}, u)$. Hence $N^{(u)}(x) = N(\{vxv\}) = N(u)N(x)$. Specialization gives the required relation $N^{(u)}(a) = N(u)N(a)$.

In dealing with norm equivalence it is natural to assume that the degrees of the algebras are the same. We do this in the following

Theorem 11. *Assume* Φ *of characteristic* $\neq 3$ *and* $|\Phi| \geq m = \deg \mathfrak{A} = \deg \mathfrak{B}$. *Assume also that* $\mathfrak{B}$ *is a separable Jordan algebra. Then the Jordan algebras* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are norm equivalent if and only if* $\mathfrak{A}$ *is isomorphic to a* u*-isotope of* $\mathfrak{B}$.

Proof. The condition is clearly sufficient in view of the preceding lemma. Conversely, suppose η is a 1-1 linear mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ such that $N(a^\eta)=\rho N(a)$, $a\in\mathfrak{A}$. Let $v=1^\eta$. Then we have $N(v)=\rho N(1)=\rho\neq 0$, so $u=v^{-1}$ exists in $\mathfrak{B}$. We can form the u-isotope $(\mathfrak{B}, u)$ whose identity is v. We have $N^{(u)}(a^\eta)=N(u)N(a^\eta)=\rho^{-1}\rho N(a)=N(a)$ and $1^\eta=v$ the identity of $(\mathfrak{B}, u)$. We observe next that the radical of a Jordan algebra and any isotope coincide. This is clear since the radical is a nilpotent ideal. It follows that if an algebra is semi-simple or separable then any isotope is respectively semi-simple or separable. In particular, we see that $(\mathfrak{B}, u)$ is separable. Hence if we change our notation we can reduce the proof to showing that if η is a 1-1 linear mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ such that $N(a^\eta)=a$, $a\in\mathfrak{A}$ and 1^η is the identity of $\mathfrak{B}$ then η is an isomorphism. The proof of this is identical with the proof of the special case $\mathfrak{B}=\mathfrak{A}$ central simple treated in Th. 4 of [13, I]. We therefore omit the remainder of the argument.

We recall that if $\mathfrak{A}$ and $\mathfrak{B}$ are simple associative algebras then $\mathfrak{A}^+\cong\mathfrak{B}^+$ if and only if $\mathfrak{A}$ and $\mathfrak{B}$ are either isomorphic or anti-isomorphic ([4] or [11]). We recall also that $\mathfrak{A}$ and $\mathfrak{A}^+$ have the same generic norms and that any isotope of $\mathfrak{A}^+$ is isomorphic to $\mathfrak{A}^+$. These facts together with Th. 11 imply the following

Theorem 12. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be separable simple associative algebras of the same degree over a field Φ of characteristic $\neq 2, 3$ such that $|\Phi|\geq m=\deg\mathfrak{A}$. Then $\mathfrak{A}$ and $\mathfrak{B}$ are norm equivalent if and only if they are either isomorphic or anti-isomorphic.*

REMARK (added in proof). As has been shown by Landherr (Hamburg Abhandlungen, vol. 11 (1934), p. 53), it is easy to establish the existence of two associative central division algebras $\mathfrak{A}$ and $\mathfrak{B}$ of degree three over the rational field (or over an algebraic number field) which are neither isomorphic nor anti-isomorphic but $\mathfrak{A}_\Lambda$ and $\mathfrak{B}_\Lambda$ are either isomorphic or anti-isomorphic for Λ the field of real numbers or any p-acid field, $p=2, 3, 5, \cdots$. Let N_1 and N_2 denote the generic norms of $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Then Theorem 12 implies that N_1 and N_2 are homogeneous cubic forms in nine variables which are not rationally equivalent, but which are equivalent in the strict sense obtained by taking $\rho=1$ in our definition in the real field and in every p-adic field.

7. The Lie algebra $\mathfrak{L}(\mathfrak{A}, N)$. In this section we assume that $|\Phi|>m=\deg\mathfrak{A}$. Let $\mathfrak{L}(\mathfrak{A}, N)$ denote the set of linear transformations $\mathfrak{A}$ in $\mathfrak{A}$ having N as Lie invariant, that is, $N(a+(aA)t)\equiv N(a) \pmod{t^2}$. If x is generic, we have $N(x+(xA)t)=N(x)+N_1(x)t+N_2(x)t^2+\cdots$ where the

$N_i(x)$ are of degree $\leq m$. Since $A \in \mathfrak{L}(\mathfrak{A}, N)$ we have $N_1(a)=0$ for all $a \in \mathfrak{A}$ and since $|\Phi| > m$ this implies that $N_1(x)=0$. Hence the extension of $\mathfrak{A}$ to $\mathfrak{A}_\Omega$ where Ω is an extension field of Φ has N as Lie invariant also.

Assume for the moment that Φ is infinite and let $\mathfrak{P}(\mathfrak{A})$ be the algebra of polynomial functions on $\mathfrak{A}$. These can be defined intrinsically as the elements of the algebra of mappings of $\mathfrak{A}$ into Φ generated by the linear mappings. The latter constitute the conjugate space $\mathfrak{A}^*$ of $\mathfrak{A}$ and $\mathfrak{P}(\mathfrak{A})$ is isomorphic to the algebra of polynomials $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$, ξ_i indeterminates, $n=\dim \mathfrak{A}$. Then if A is a linear transformation in $\mathfrak{A}$ over Φ, the transpose $\mathfrak{A}^*$ has a unique extension to a derivation D_A in $\mathfrak{P}(\mathfrak{A})$. If t is an indeterminate any polynomial function φ on $\mathfrak{A}$ has a unique extension to $\mathfrak{A}_{\Phi(t)}$. If A is a linear transformation in $\mathfrak{A}$ we have $\varphi(a+(aA)t)=\varphi(a)+\varphi_1(a)t+\varphi_2(a)t^2+\cdots$ and we obtain a mapping $\varphi \to \varphi_1$ in $\mathfrak{P}(\mathfrak{A})$. One checks that this is a derivation in $\mathfrak{P}(\mathfrak{A})$. If A is linear then $\varphi_1(a)=\varphi(aA)$, so $\varphi_1=\varphi(aA)=\varphi A^*$, A^* the transpose of A. Thus the derivation $\varphi \to \varphi_1$ coincides with D_A on A^*. Consequently, $\varphi \to \varphi_1$ is D_A on $\mathfrak{P}(\mathfrak{A})$.

We can verify that $D_{A+B}=D_A+D_B$, $D_{\alpha A}=\alpha D_A$, $D_{[A,B]}=[D_B, D_A]$ where $[XY]=XY-YX$ for linear transformations X, Y. Also $D_A=0$ implies $A^*=0$ and $A=0$. Hence $A \to D_A$ is an anti-isomorphism of the Lie algebra of linear transformations in $\mathfrak{A}$ into the Lie algebra of derivations in $\mathfrak{P}(\mathfrak{A})$. If the base field is of characteristic $p \neq 0$ we have $D_{A^p}=D_A{}^p$ which means that $A \to D_A$ is an isomorphism for restricted Lie algebras. If φ is any element of $\mathfrak{P}(\mathfrak{A})$ the set of derivations of $\mathfrak{P}(\mathfrak{A})$ mapping φ into 0 is a subalgebra of the derivation algebra of $\mathfrak{P}(\mathfrak{A})$ which is restricted if the characteristic is $p \neq 0$. Hence the set $\mathfrak{L}(\mathfrak{A}, \varphi)$ of linear transformations A of $\mathfrak{A}$ such that $\varphi D_A=0$ is a subalgebra, restricted for characteristic p, of the Lie algebra of linear transformations in $\mathfrak{A}$. If we recall that $\varphi(a+(aA)t)=\varphi(a)+(\varphi D_A)(a)t+\cdots$ we see that $\mathfrak{L}(\mathfrak{A}, \varphi)$ is the set of linear transformations having φ as Lie invariant in the earlier sense ($\varphi(a+(aA)t) \equiv \varphi(a) \pmod{t^2}$).

Now consider the algebra $\mathfrak{A}$ again where we assume only that $|\Phi| > m$. We have seen that if $A \in \mathfrak{L}(\mathfrak{A}, N)$ then the linear extension A of A to $\mathfrak{A}_\Omega \in \mathfrak{L}(\mathfrak{A}_\Omega, N)$. If we take Ω infinite and use the results just indicated we see that $\mathfrak{L}(\mathfrak{A}, N)$ is a Lie algebra of linear transformations in $\mathfrak{A}$ which is restricted if the characteristic is $p \neq 0$.

Now assume the characteristic is either 0 or $p > m$ and let $(a_1, a_2, \cdots, a_m)$ be the symmetric multilinear form obtained from the norm form as before. Then $N(a)=(a, a, \cdots, a)$. Consequently,

$$\begin{aligned} N(a+(aA)t &= (a+(aA)t, a+(aA)t, \cdots, a+(aA)t) \\ &\equiv N(a)+m(aA, a, \cdots, a)t \pmod{t^2} \end{aligned}$$

which implies that $A\in\mathfrak{L}(\mathfrak{A}, N)$ if and only if $(aA, a, \cdots, a)=0$. If we linearize this relation we see that $A\in\mathfrak{R}(\mathfrak{A}, N)$ if and only if

$$(28)\qquad (a_1A, a_2, \cdots, a_m)+(a_1, a_2A, a_3, \cdots, a_m)+\cdots+(a_1, a_2, \cdots, a_{m-1}, a_mA)=0\,.$$

We have seen that $\mathfrak{L}(\mathfrak{A}, N)$ contains the Lie algebra of derivations $\mathfrak{D}(\mathfrak{A})$ (Th. 1, (vii)). Also if $\mathfrak{A}$ is Jordan then $\mathfrak{L}(\mathfrak{A}, N)$ contains $R(\mathfrak{A}')$ the set of multiplications R_b where b is in the subspace $\mathfrak{A}'$ of elements of generic trace 0 (Th. 9). If D is a derivation then $1D=0$ and if $b\in\mathfrak{A}'$ then $1R_b=b$. Hence $\mathfrak{D}(\mathfrak{A})\cap R(\mathfrak{A}')=0$. Hence for Jordan algebras we have

$$(29)\qquad \mathfrak{L}(\mathfrak{A}, N)\supseteq\mathfrak{D}(\mathfrak{A})+R(\mathfrak{A}'),\quad \mathfrak{D}(\mathfrak{A})\cap R(\mathfrak{A}')=0\,.$$

We shall now consider the situation for $\mathfrak{A}$ a separable Jordan algebra and we prove first the following

Lemma. *Let $\mathfrak{A}$ be a separable Jordan algebra over a field Φ of characteristic $\neq 3$ containing more than m elements, m the degree of $\mathfrak{A}$. Then a linear transformation A in $\mathfrak{A}$ over Φ is a derivation if and only if $\mathfrak{A}\in\mathfrak{L}(\mathfrak{A}, N)$ and $1A=0$.*

Proof. We have seen that any derivation satisfies the indicated conditions. Conversely, assume A satisfies the conditions. We write $m_a(\lambda)=\lambda^m-\sigma_1(a)\lambda^{m-1}+\cdots+(-1)^m\sigma_m(a)$. Then for $\rho\in\Phi$ we have

$$N(\rho 1-a)=m_a(\rho)=\rho^m-\sigma_1(a)\rho^{m-1}+\cdots+(-1)^m\sigma_m(a)\,.$$

Since $1A=0$ and N is Lie invariant for A, we have

$$\begin{aligned}N(\rho 1-(a+(aA)t) &= N((\rho 1-a)-((\rho 1-a)A)t)\\ &\equiv N(\rho 1-a)\pmod{t^2}\,,\end{aligned}$$

which gives

$$\begin{aligned}&\rho^m-\sigma_1(a)\rho^{m-1}+\cdots+(-1)^m\sigma_m(a)\\ &\quad\equiv\rho^m-\sigma_1(a+(aA)t)\rho^{m-1}+\cdots+(-1)^m\sigma_m(a+(aA)t)\pmod{t^2}\,,\end{aligned}$$

or

$$\begin{aligned}&[\sigma_1(a+(aA)t)-\sigma_1(a)]\rho^{m-1}+\cdots+(-1)^m[\sigma_m(a+(aA)t)-\sigma_m(a)]\\ &\quad\equiv 0\pmod{t^2}\,.\end{aligned}$$

If we choose m distinct values of ρ in (30), we see, by a Vandermonde determinant argument, that $\sigma_i(a+(aA)t)\equiv\sigma_i(a)\pmod{t^2}$, which shows that every $\sigma_i(a)$ is Lie invariant under A. We have shown in [13, I], p. 186

that $T(a^2)$ and $T(a_3)$ are expressible as polynomials in the σ_i with coefficients in Φ if $\mathfrak{A}$ is central simple. Since a separable algebra becomes a direct sum of central simple algebras on extending the base field to its algebraic closure this result is valid in the present situation also. It follows that $T(a^2)$ and $T(a^3)$ are Lie invariant under A. Since the characteristic is $\neq 2, 3$ a linearization such as we applied to obtain (28) shows that if $(a, b)=T(ab)$ and $(a, b, c)=T((ab)c)=T(a(bc))$ then

$$(30) \qquad \begin{aligned} (aA, b)+(a, bA) &= 0 \\ (aA, b, c)+(a, bA, c)+(a, b, cA) &= 0 \end{aligned}$$

for all $a, b, c \in \mathfrak{A}$. The first of these gives

$$((ab)A, c)+(ab, cA) = 0$$

and the second gives, on noting that $(a, b, c)=(ab, c)$,

$$((aA)b, c)+(a(bA), c)+(ab, cA) = 0 .$$

Hence

$$((ab)A-(aA)b-a(bA), c) = 0 .$$

Since (a, b) is non-degenerate this implies that $(ab)A=(aA)b+a(bA)$ which is the condition that A is a derivation.

We can now prove

Theorem 13. *If $\mathfrak{A}$ is a separable Jordan algebra over a field of characteristic $\neq 3$ which has more than m elements where m is the degree of $\mathfrak{A}$, then*

$$(31) \qquad \mathfrak{L}(\mathfrak{A}, N) = R(\mathfrak{A}') \oplus \mathfrak{D}(\mathfrak{A}) .$$

Proof. We know that $\mathfrak{L}(\mathfrak{A}, N)$ contains $R(\mathfrak{A}')$ and $\mathfrak{D}(\mathfrak{A})$ and the sum of the latter two spaces is direct. Now let $A \in \mathfrak{L}(\mathfrak{A}, N)$. Then $N(1+(1A)t) \equiv 1 \pmod{t^2}$ and the relation $m_a(\lambda)=N(\lambda 1-a)$ implies that $N(1+(1A)t) \equiv 1 + T(1A) \pmod{t^2}$. Hence $a=1A$ satisfies $T(a)=0$ so $a \in \mathfrak{A}'$ and $R_a \in R(\mathfrak{A}')$. Set $B=A-R_a$. This is in $\mathfrak{L}(A, N)$ and satisfies $1B=0$. Hence $B \in \mathfrak{D}(\mathfrak{A})$. Thus $A=R_a+B \in (\mathfrak{A}')+\mathfrak{D}(\mathfrak{A})$ and (31) holds.

We know that $(ab, c)=(a, bc)$ or $(aR_b, c)=(a, cR_b)$ which shows that R_b is symmetric (coincides with its adjoint) relative to (a, b). On the other hand, the Lie invariance of $T(a^2)$ relative to derivations show that $(aD, b)+(a, bD)=0$ for D any derivation. This shows that D is skew relative to (a, b). The decomposition (31) of $\mathfrak{L}(\mathfrak{A}, N)$ is therefore the unique decomposition of $\mathfrak{L}(\mathfrak{A}, N)$ as direct sum of the spaces of symmetric and skew elements relative to (a, b). Hence we have the following

characterization of multiplications by elements of generic trace 0 and of derivations.

Corollary. *Under the same hypothesis as in Th.* 13 *we have*: *A linear transformation A in $\mathfrak{A}$ has the form $A=R_a$, $a\in\mathfrak{A}'$ if and only if A has N as Lie invariant and A is symmetric relative to (a, b). A linear transformation A in $\mathfrak{A}$ is a derivation if and only if A has N as Lie invariant and A is skew relative to (a, b).*

If the characteristic is 0 it is known that $\mathfrak{D}(\mathfrak{A})$ coincides with the set $\mathfrak{J}(\mathfrak{A})$ of inner derivations, that is, the set of derivation of the form $x\to\sum A(a_i, x, b_i)$, $A(a_i, x, b_i)=(a_ix)b_i-a_i(xb_i)$. ([12]). It is clear from the decomposition $\mathfrak{A}=\Phi 1\oplus\mathfrak{A}'$ that we may take the a_i and b_i to satisfy $T(a_i)=0$, $T(b_i)=0$. Since $x\to A(a, x, b)=x[R_aR_b]$ and $[[R_aR_b]R_c]=R_{A(b,c,a)}$ it follows from Th. 13 that $\mathfrak{L}(\mathfrak{A}, N)$ is the Lie algebra of linear transformations generated by the R_a, $a\in\mathfrak{A}'$, if Φ is of characteristic 0. If the characteristic is p this need not be the case. For example, let $\mathfrak{A}=\Phi_m^+$ where $p\mid m$. It is easy to see that $\mathfrak{J}(\mathfrak{A})$ consists of the mappings $x\to[xb]$ where $T(b)=0$. On the other hand, if a is any element of Φ_n^+ then $x\to[xa]$ is a derivation and if $T(a)\neq 0$ then this cannot have the form $x\to[xb]$ with $T(b)=0$. Using the known results on the derivations of central simple algebras ([16]) and the structure of classical Lie algebras it is easy to sort out the cases in which $\mathfrak{D}(\mathfrak{A})=\mathfrak{J}(\mathfrak{A})$.

YALE UNIVERSITY

(Received March 7, 1963)

Bibliography

[1] A. A. Albert: *A theory of power associative commutative algebras*, Trans. Amer. Math. Soc. **69** (1950), 503–527.

[2] A. A. Albert: *A construction of exceptional Jordan division algebras*, Ann. of Math. **67** (1958), 1–28.

[3] A. A. Albert and N. Jacobson: *Reduced exceptional simple Jordan algebras*, Ann. of Math. **66** (1957), 400–417.

[4] G. Ancochea: *On semi-automorphisms of division algebras*, Ann. of Math. **48** (1947), 147–154.

[5] M. Bôcher: Introduction to Higher Algebra, New York, Macmillan, 1929.

[6] C. Chevalley: Théorie des Groupes de Lie, Tome II, Paris, Hermann, 1951.

[7] P. M. Cohn: *Special Jordan algebras*, Canad. J. Math. **6** (1954), 253–264.

[8] J. Dieudonné: *Sur le polynôme principal d'une algèbre*, Arch. Math. **8** (1957), 81–84.

[9] H. Flanders: *The norm function of an algebraic field extension*, I, Pacific J. Math. **3** (1953), 103–112; II ibid. **5** (1955), 519–528.

[10] N. Jacobson: *An application of E. H. Moores' determinant of a hermitian matrix*, Bull. Amer. Math. Soc. **45** (1939), 745–748.

[11] N. Jacobson: *Isomorphism of Jordan rings*, Amer. J. Math. **70** (1948), 317–326.

[12] N. Jacobson: *Derivation algebras and multiplication algebras of semi-simple Jordan algebras*, Ann. of Math. **50** (1949), 866–874.

[13] N. Jacobson: *Some groups of linear transformations defined by Jordan algebras*, I, J. Reine Angew, Math. **201** (1959), 178–195; II ibid. **204** (1960), 74–98; III ibid. **207** (1961), 61–95.

[14] N. Jacobson: *MacDonald's theorem on Jordan algebras*, Arch. Math. **13** (1962), 241–250.

[15] N. Jacobson: *A coordinatization theorem for Jordan algebras*, Proc. Nat. Acad. Sci. U. S. A. **48** (1962), 1154–1160.

[16] N. Jacobson and F. D. Jacobson: *Classification and representation of semi-simple Jordan algebras*, Trans. Amer. Math. Soc. **65** (1949), 141–169.

[17] M. Koecher: Jordan algebras and their applications, Multilithed notes, University of Minnesota, 1962.

[18] I. G. MacDonald: *Jordan algebras with three generators*, Proc. London Math. Soc. III, **10** (1960), 395–408.

[19] R. D. Schafer: *On forms of degree n permitting composition*, forthcoming in J. Math. and Mech.

[20] A. I. Shirshov: *On special J-rings*, Mat. Sb. **80** (1960), 149–166 (in Russian).

[21] J. Tits: forthcoming in Proc. Amer. Math. Soc.