JOURNAL OF ALGEBRA 77, 97–103 (1982)

On the Generic Polynomial of Degree Two Algebras

ROBERT H. OEHMKE

Department of Mathematics, University of Iowa, Iowa City, Iowa 52242

Communicated by E. Kleinfeld

Received July 25, 1980

Let $\mathcal{A}$ be a finite dimensional algebra over a field $\mathcal{F}$ of characteristic not 2 or 3. We say that $\mathcal{A}$ is powerassociative if for every element y of $\mathcal{A}$ we have that $\mathcal{F}[y]$, the algebra of polynomials in y over $\mathcal{F}$, is associative. This provides, in particular, a well-defined notion of nilpotency of elements. If powerassociativity is preserved under scalar extensions of $\mathcal{A}$ we say that $\mathcal{A}$ is strictly powerassociative [1]. We assume $\mathcal{A}$ is commutative.

An algebra $\mathcal{A}$ is said to be of degree 2 if the maximal set of pairwise orthogonal, nonzero idempotents in any scalar extension of $\mathcal{A}$ is of cardinality 2. If $\mathcal{A}$ has an identity element 1 and e is an idempotent then so also is $1-e$. If $e \neq 0, 1$ then $\{e, 1-e\}$ is a maximal set of pairwise orthogonal, nonzero idempotents in an algebra of degree 2.

Let $u_1,..., u_n$ be a basis of the vector space $\mathcal{A}$ over $\mathcal{F}$ and $\delta_1,..., \delta_n$, $\varepsilon_1,..., \varepsilon_n$ and $\mu_1,..., \mu_n$ be algebraically independent elements over $\mathcal{F}$ in some extension field of $\mathcal{F}$. Let $\mathcal{K} = \mathcal{F}(\delta_1,..., \delta_n, \varepsilon_1,..., \varepsilon_n, \mu_1,..., \mu_n)$ and

$$x = \delta_1 u_1 + \cdots + \delta_n u_n.$$

The element x lies in the scalar extension $\mathcal{A}_{\mathcal{K}}$ of $\mathcal{A}$. The algebra $\mathcal{A}_{\mathcal{K}}$ is commutative, powerassociative, and finite dimensional and has the same basis over $\mathcal{K}$ as $\mathcal{A}$ does over $\mathcal{F}$. The element x is called a generic element of $\mathcal{A}$ [5, 6]. As an element in the finite dimensional algebra $\mathcal{A}_{\mathcal{K}}$ over $\mathcal{K}$, x satisfies a monic equation of degree n with coefficients in $\mathcal{K}$ and hence a minimal, monic equation over $\mathcal{K}$. This equation will be called the generic equation of $\mathcal{A}$ and written $m_x(\lambda) = 0$. If it is also assumed that $\mathcal{A}$ is Jordan, i.e.,

$$w^2(yw) = (w^2y)w$$

for all w and y in $\mathcal{A}$, and simple then Jacobson [5] has shown that the generic polynomial, $m_x(\lambda)$, is irreducible. From the literature on simple, commutative, powerassociative algebras [2, 3, 7, 9, 10] Jacobson's results prove that all simple, commutative, powerassociative algebras of charac-

0021-8693/82/070097-07$02.00/0

teristic not 2 or 3 have irreducible generic polynomials except possibly those of degree 2 with a non-nilstable idempotent [11]. We shall use the results of [11] to fill in this small gap in the literature and to obtain the best possible form (with respect to irreducibility) that the generic polynomial can take.

For every idempotent e of $\mathfrak{A}$ we have a vector space decomposition

$$\mathfrak{A} = \mathfrak{A}_e(1) + \mathfrak{A}_e(\tfrac{1}{2}) + \mathfrak{A}_e(0),$$

where

$$\mathfrak{A}_e(i) = \{ y \mid y \in \mathfrak{A} \text{ and } ey = iy \}.$$

Various multiplicative properties have been obtained [1] for these characteristic subspaces. In particular,

$$\mathfrak{A}_e(1)\,\mathfrak{A}_e(\tfrac{1}{2}) \subseteq \mathfrak{A}_e(\tfrac{1}{2}) + \mathfrak{A}_e(0),$$
$$\mathfrak{A}_e(0)\,\mathfrak{A}_e(\tfrac{1}{2}) \subseteq \mathfrak{A}_e(\tfrac{1}{2}) + \mathfrak{A}_e(1).$$

We shall call the idempotent e nilstable if for every $y \in \mathfrak{A}_e(1)$ and $z \in \mathfrak{A}_e(\frac{1}{2})$ the $\mathfrak{A}_e(0)$-component of the product yz is nilpotent.

We can now formally state the result we wish to prove.

THEOREM. *Let $\mathfrak{A}$ be a finite dimensional, commutative, strictly powerassociative, simple algebra over a field $\mathscr{F}$ of characteristic not 2 or 3 such that in some scalar extension of $\mathfrak{A}$ there is an idempotent that is not nilstable. The generic polynomial of $\mathfrak{A}$ is irreducible or of the form*

$$(\lambda^2 - \alpha(x)\lambda + \beta(x))^r,$$

where $\alpha(x)$ and $\beta(x)$ are forms in $\delta_1,..., \delta_n$ of degrees 1 and 2, respectively, $0 < r \leqslant p$, and $\lambda^2 - \alpha(x)\lambda + \beta(x)$ is irreducible.

Proof. If $\mathfrak{A}$ is simple then $\mathfrak{A}$ contains an identity element 1 [1]. Also the only simple non-nilstable algebras of this type are of characteristic $p \neq 0$ [10, 11]. Hence we shall assume $p \neq 0$. It has been shown [12] that the generic polynomial, $m_x(\lambda)$, is of the form

$$(\lambda^{2q} - \alpha(x)\,\lambda^q + \beta(x))^t,$$

where q is a power of p, t is a nonnegative integer and $\alpha(x)$ and $\beta(x)$ are homogeneous forms over $\mathscr{F}$ in $\delta_1, \delta_2,..., \delta_n$ of degrees q and $2q$, respectively, and $\lambda^{2q} - \alpha(x)\,\lambda^q + \beta(x)$ is irreducible over $\mathscr{K}$. In the subsequent work we do not need to work with the minimal polynomial. In fact the exponent t can be replaced by any positive integer s such that $t \leqslant s$. Hence we shall assume t is a power of p. We then have that exponentiation by t will be linear. Since the generic polynomial remains the same in scalar extensions we can assume $\mathscr{F}$ is algebraically closed.

Every element

$$x_0 = \delta_{10} u_1 + \cdots + \delta_{n0} u_n$$

can be considered as a specialization of x. If we write $\alpha(x_0)$ and $\beta(x_0)$ for the elements of $\mathscr{F}$ obtained when $\delta_{10},\dots,\delta_{n0}$ are substituted for $\delta_1,\dots,\delta_n$ then x_0 satisfies the equation

$$[x^{2q} - \alpha(x_0)\, x^q + \beta(x_0)]^t = 0$$

and the polynomial on the left has the same irreducible factors as the minimal polynomial satisfies by x_0 [5, 6]. Since $\mathfrak{A}$ has an idempotent $e \neq 0, 1$ we can take $x_0 = e - f$, where $f = 1 - e$. The minimal polynomial satisfied by x_0 is

$$\lambda^2 - 1$$

with the two distinct irreducible factors $\lambda - 1$ and $\lambda + 1$. Thus the generic polynomial $m_x(\lambda)$ must also have two distinct roots.

We let $\mathscr{L}$ be an extension of $\mathscr{K}$ that splits the polynomial

$$\lambda^2 - \alpha(x)\lambda + \beta(x) = (\lambda - b)(\lambda - a),$$

where $a, b \in \mathscr{L}$ and $a^t \neq b^t$. It follows easily that

$$e_x = \frac{x^{qt} - a^t}{b^t - a^t} \qquad \text{and} \qquad f_x = \frac{x^{qt} - b^t}{a^t - b^t}$$

are a pair of nonzero orthogonal idempotents whose sum is 1. These two elements lie in $\mathfrak{A}_{\mathscr{L}}$. We define

$$z_x = e_x - f_x = \frac{2x^{qt} - \alpha(x)^t}{b^t - a^t}.$$

If we let $L(z_x)$ be the linear transformation induced by left multiplication by z_x then $L(z_x)^2$ has two characteristic subspaces, $\mathfrak{A}_{e_x}(1) + \mathfrak{A}_{f_x}(1)$ and $\mathfrak{A}_{e_x}(\frac{1}{2})$, corresponding to the characteristic values 1 and 0.

Let $\bar{z}_x = (b^t - a^t)\, z_x$. We have $(b^t - a^t)^2 = (b^t + a^t)^2 - 4a^t b^t = \alpha(x)^{2t} - 4\beta(x)^t$; an element of $\mathscr{K}$. Also $\bar{z}_x = 2x^{qt} - \alpha(x)^t$ is in $\mathfrak{A}_K$. The linear transformation $L(\bar{z}_x)^2$ on the vector space $\mathfrak{A}_K$ has two characteristic subspaces $G_{\mathscr{K}}(1, 0)$ and $G_{\mathscr{K}}(\frac{1}{2})$ corresponding to the characteristic values $\alpha(x)^{2t} - 4\beta(x)^t$ and 0. It follows readily that

$$[G_{\mathscr{K}}(1, 0)]_{\mathscr{L}} = G_{\mathscr{L}}(1, 0),$$

$$[G_{\mathscr{K}}(\tfrac{1}{2})]_{\mathscr{L}} = G_{\mathscr{L}}(\tfrac{1}{2}),$$

where $G_{\mathscr{S}}(1,0)$ and $G_{\mathscr{S}}(\frac{1}{2})$ are the characteristic subspaces of $L(\bar{z}_x)^2$ acting on $\mathfrak{A}_{\mathscr{S}}$. We shall let $y = \varepsilon_1 u_1 + \cdots + \varepsilon_n u_n$ and $r = \mu_1 \mu_1 + \cdots + \mu_n \mu_n$. We write

$$y^* = yL(\bar{z}_x)^2,$$
$$r^* = rL(\bar{z}_x)^2.$$

Let e be a specialization of x that is an idempotent of $\mathfrak{A}$ not equal to 1 or 0. All of the elements of $\mathfrak{A}_e(1) + \mathfrak{A}_e(0)$ and $\mathfrak{A}_e(\frac{1}{2})$ can be obtained by a suitable specialization of y^* and $r - r^*$, respectively. If x is specialized to e then the corresponding specialization of $\bar{z}_x$ is $e - f$, where $f = 1 - e$. If the assumption is made that e_x is nilstable then there is a nonnegative integer u such that

$$[[y^*(r - r^*)]^*]^u = 0$$

and therefore

$$[[y_0^*(r_0 - r_0^*)]^*]^u = 0$$

for all specializations y_0 and r_0 of y and r, respectively. Thus all idempotents of $\mathfrak{A}$ would be nilstable, which contradicts our original assumptions. Therefore we must have that e_x is not a nilstable idempotent and the splitting of the polynomial $\lambda^{2qt} - \alpha(x)^t \lambda^{qt} + \beta(x)^t$ gives rise to this non-nilstable idempotent in $\mathfrak{A}_{\mathscr{S}}$.

Next we shall show that $\mathfrak{A}_{\mathscr{S}}$ is simple. Assume I is an ideal of $\mathfrak{A}_{\mathscr{S}}$ and, as an algebra over $\mathscr{S}$, has dimension $m < n$. Select a basis $v_1, \ldots, v_m$ of I in $\mathfrak{A}_{\mathscr{S}}$. Since $\mathscr{F}$ is an infinite field there must be a specialization such that not all the v_i's specialize to 0. Let this specialization of the v_i's generate the subspace J of $\mathfrak{A}$. This subspace will be of dimension less than or equal to m and greater than 0. Since I is closed under multiplication by elements in $\mathfrak{A}_{\mathscr{S}}$ it is certainly closed under multiplication by elements in $\mathfrak{A} \subseteq \mathfrak{A}_{\mathscr{S}}$. Therefore so also is J closed under multiplication by elements of $\mathfrak{A}$. Thus J is an ideal of $\mathfrak{A}$ and we have a contradiction. Thus $\mathfrak{A}_{\mathscr{S}}$ is simple.

We can now use the results of [11] to determine the structure of $\mathfrak{A}_{\mathscr{S}}$. The algebra $\mathfrak{A}_{\mathscr{S}}$ can be decomposed as

$$\mathfrak{A}_{\mathscr{S}} = \mathscr{B} + z\mathscr{B} + \mathfrak{A}_{e_x}(\tfrac{1}{2}).$$

The subspace $\mathscr{B}$ is a commutative, associative $\mathscr{D}$-simple algebra [11] for a nontrivial set of derivations $\mathscr{D}$ used in defining the multiplication of $\mathfrak{A}_{\mathscr{S}}$. Let $\mathscr{N}$ equal the set of all nilpotent elements in $\mathscr{B}$ and $\mathscr{N}^p$ the pth power of all the elements in $\mathscr{N}$. Since the characteristic of F is p, $\mathscr{N}^p$ forms a subalgebra of $\mathcal{B}$. Let I be $\mathcal{B}\mathcal{N}^p$, the set of all sums of products of an element in $\mathcal{B}$ times an element in $\mathcal{N}^p$. Clearly I is an ideal of $\mathcal{B}$. Also, if $D \in \mathcal{D}$ then $D(y) = 0$ for any $y \in \mathcal{N}^p$. Therefore I is a $\mathcal{D}$-admissible ideal of $\mathcal{B}$ and we must have $I = 0$ or $\mathcal{B}$. Since the elements of I are nilpotent we must have $I = 0$. Therefore $\mathcal{N}^p = 0$ and the nilindex of any nilpotent element of $\mathcal{B}$ is less than or equal to p.

The subspace $\mathcal{N}$ is the radical of $\mathcal{B}$. Therefore $\mathcal{B}/\mathcal{N}$ is a semisimple algebra over $\mathcal{K}$. Since $\mathcal{B}$ has only one idempotent $\mathcal{B}/\mathcal{N}$ must be a field. If b and b' are elements of $\mathcal{B}$ such that

$$b = b' + n$$

for some $n \in \mathcal{N}$ then $b^p = b'^p$. Therefore the mapping $b + \mathcal{N} \to b^p$ is well-defined and a homomorphism of rings. If $b + \mathcal{N} \to 0$ then $b^p = 0$ and $b \in \mathcal{N}$. Hence we have an isomorphism. Therefore $\mathcal{B}^p \cong \mathcal{B}/\mathcal{N}$ and $\mathcal{B}^p$ is a field. Actually $\mathcal{B}^p$ is an extension of $\mathcal{K}^p$. Let $M = \mathcal{K}^p(x^{pq})$. Since all nilpotent elements of $\mathcal{B}$ have nilindex less than or equal to p the same must be true of $G_\kappa(1, 0)$. Therefore x satisfies an equation of the form

$$[x^{2q} - \alpha(x)\, x^q + \beta(x)]^p = 0.$$

Therefore M is quadratic over $\mathcal{K}^p$. Now if $x^p - \alpha(x)^p = 0$ has a solution $\mathcal{Y}$ in M then this solution must lie in $\mathcal{K}^p$. Thus $\mathcal{Y}$ and $\alpha(x)$ would be in $\mathcal{K}$ and we would have to have $\mathcal{Y} = \alpha(x)$. A similar argument can be made relative to $\beta(x)$. Thus we can adjoin $\alpha(x)$ and $\beta(x)$ to M without danger of duplicating roots. If $q > 1$ we have the relationship

$$[x^{2q} - \alpha(x)\, x^q + \beta(x)]^p = 0$$

in $M(\alpha(x), \beta(x))$ and hence

$$x^{2q} - \alpha(x)\, x^q + \beta(x) = 0.$$

If $q = 1$ then of course we have $[x^2 - \alpha(x)x + \beta(x)]^t = 0$, where $t \leqslant p$. Thus we have completed the proof of the theorem.

We shall now give two examples of algebras of the type under consideration.

Let $\mathcal{B}$ be the associative algebra with identity generated by the nilpotent element n ($n^p = 0$) over the algebraically closed field $\mathcal{F}$. Let $\mathcal{A}$ be the vector space with basis over $\mathcal{F}$ consisting of

$$1, b, \ldots, b^{p-1}, z, b \circ z, \ldots, b^{p-1} \circ z, w, b \circ w, \ldots, b^{p-1} \circ w$$

and with products defined by

$$b^0 = 1, \qquad b^i b^j = b^{i+j}, \qquad (b^i \circ z)(b^j \circ z) = b^{i+j} \circ z, \qquad b^i(b^j \circ z) = b^{i+j} \circ z,$$
$$b^i(b^j \circ w) = (b^{i+j} \circ w) + ib^{i+j-1} \circ z, \qquad (b^i \circ z)(b^j \circ w) = -ib^{i+j-1},$$
$$(b^i \circ w)(b^j \circ w) = j(j-1)\, b^{i+j-2} + i(i-1)\, b^{i+j-2} - ijb^{i+j-2}.$$

This multiplication satisfies the condition of [11, Theorem 8] with D_0 defined by $D_0(b) = 1$ and $b_{00} = 0$.

We define the subspace N_i to be generated by all n^j, $n^j \circ z$, $n^j \circ w$ for $j \geqslant i$. If $i \geqslant 2$ it is straightforward to show that $N_i^2 \subseteq N_{i+1}$. Hence all the elements of N_i are nilpotent for $i \geqslant 2$. Now let $y = \lambda(z + n \circ w) + \delta n + \mu(n \circ z) + m$, where $m \in N_2$ and λ, δ, μ are in $\mathscr{F}$. We have $y^2 = 4\delta\lambda n \circ z + m'$, where $m' \in N_2$. If $\lambda = 0$ in the expression of y then $y^2 \in N_2$. Since λ is the coefficient of $z + n \circ w$ we see immediately that $(y^2)^2 \in N_2$. Thus y^2 is nilpotent and so also is y.

Now let $x = \delta_1 + \delta_2 z + \delta_3 w + \delta_4 n + \delta_5 n \circ z + \delta_6(n \circ w) + m_2$, where $m_2 \in N_2$. We determine the coefficients of $1, z, n \circ w$ and w in the expression $x^2 - \alpha(x)x + \beta(x)$, where $\alpha(x) = 2\delta_1$ and $\beta(x) = \delta_1^2 - \delta_2^2 + 2\delta_3\delta_5$. Again by a straightforward computation we have that the coefficients of 1 and w are 0 and that the coefficients of z and $n \circ w$ are equal in this expression. Thus, if we let $y = x^2 - \alpha(x)x + \beta(x)$ we have shown that y is nilpotent. Hence the generic polynomial for this algebra is

$$[x^2 - \alpha(x)x + \beta(x)]^p.$$

For a second example we let $\mathscr{F}$ be a field with an element a such that $x^p - a$ is irreducible over $\mathscr{F}$. Let $\mathscr{B} = \mathscr{F}(v)$, where v is a root of $x^p - a = 0$ in some extension field of $\mathscr{F}$. Let $\mathscr{A} = \mathscr{B} + \mathscr{B} \circ w + \mathscr{B} \circ z$. We define a linear transformation D on $\mathscr{B}$ by $D(v^i) = iv^{i-1}$ for all $i \geqslant 0$. It is easily shown that since $D(v^{i+p}) = D(av^i)$, D is well-defined and a derivation on $\mathscr{B}$. We use this derivation on $\mathscr{B}$ and define a multiplication on $\mathscr{A}$ according to Theorem 8 [11]. Now assume the generic polynomial of $\mathscr{A}$ is a divisor of

$$[x^2 - \alpha(x)x + \beta(x)]^p.$$

Since $v \in \mathscr{A}$ then specializing x to v we see that $[v^2 - \alpha(v)v + \beta(v)]^p = 0$. But v lies in the field $\mathscr{F}(v)$. Since $\alpha(v)$ and $\beta(v)$ are in $\mathscr{F}$ we see that v lies in a quadratic extension of $\mathscr{F}$. This contradicts our choice of v as a root of the irreducible equation $x^p - a = 0$. Thus the generic polynomial of $\mathscr{A}$ must be of the form $x^{2q} - \alpha(x)\, x^q + \beta(x)$.

These two examples demonstrate that each of two types of possible polynomials in the Theorem can occur.

REFERENCES

1. A. A. ALBERT, A theory of power-associative commutative algebras, *Trans. Amer. Math. Soc.* **69** (1950), 503–527.
2. A. A. ALBERT, On commutative power-associative algebras of degree two, *Trans. Amer. Math. Soc.* **74** (1953), 323–343.
3. A. A. ALBERT, On partially stable algebras, *Trans. Amer. Math. Soc.* **84** (1957), 430–443.
4. A. A. ALBERT, Addendum to the paper on partially stable algebras, *Trans. Amer. Math. Soc.* **87** (1958), 57–62.
5. N. JACOBSON, Generic norm of an algebra, *Osaka J. Math.* **15** (1963), 25–50.
6. N. JACOBSON, "Structure and Representation of Jordan Algebras," Colloquium Publications, Amer. Math. Soc., Providence, R.I., 1968.
7. L. A. KOKORIS, Power-associative commutative algebras of degree two, *Proc. Nat. Acad. Sci. USA* **38** (1952), 534–537.
8. L. A. KOKORIS, New results on power-associative algebras, *Trans. Amer. Math. Soc.* **77** (1954), 363–373.
9. L. A. KOKORIS, Simple power-associative algebras of degree two, *Ann. of Math.* **64** (1956), 544–550.
10. L. A. KOKORIS, Flexible nilstable algebras, *Proc. Amer. Math. Soc.* **13** (1962), 335–340.
11. R. H. OEHMKE, On commutative algebras of degree two, *Trans. Amer. Math. Soc.* **105** (1962), 295–313.
12. R. H. OEHMKE, On the generic polynomial of an algebra, *Scripta Math.* **29** (1972), 331–336.