

p -ALGEBRAS OF EXPONENT p^*

BY NATHAN JACOBSON†

A. A. Albert and O. Teichmüller have recently investigated the structure of p -algebras, that is, normal simple algebras of degree p^e and characteristic p .‡ In particular they showed that a necessary and sufficient condition that such an algebra have exponent p is that it be similar to an algebra A having a maximal subfield $C = F(c_1, c_2, \dots, c_m)$, where $c_i^p = \gamma_i \in F$, the underlying field. The latter algebra is cyclic. It is the purpose of this note to apply some results of my paper *Abstract derivation and Lie algebras*§ to obtain a new generation of A . For $m=1$ this generation is more symmetric than the cyclic generation. We obtain a condition that A be a matrix algebra in terms of the new generation, and when $m=1$ we have as a consequence a reciprocity law for fields of characteristic p .

Let A be a normal simple algebra of degree p^m (order p^{2m}) over a field F of characteristic p and suppose A contains the maximal subfield $C = F(c_1, c_2, \dots, c_m)$, $c_i^p = \gamma_i \in F$. Let D be an arbitrary derivation of C over F , that is, a mapping $x \rightarrow xD$ of C into itself such that

$$\begin{aligned}(x + y)D &= xD + yD, & (x\alpha)D &= (xD)\alpha, \\ (xy)D &= (xD)y + x(yD), & \alpha &\in F.\end{aligned}$$

It is known that D may be chosen so that the only elements z such that $zD=0$ are those of F ,|| and for a D of this type I have shown that

$$(1) \quad x(D^{p^m} + D^{p^m-1}\tau_1 + \dots + D\tau_m) = 0, \quad \tau_i \in F,$$

* Presented to the Society, April 10, 1937.

† National Research Fellow.

‡ A. A. Albert, *On normal division algebras of degree p^e over F of characteristic p* , Transactions of this Society, vol. 39 (1936), pp. 183–188, and *Simple algebras of degree p^e over a centrum of characteristic p* , Transactions of this Society, vol. 40 (1936), pp. 112–126. O. Teichmüller, *p Algebren*, Deutsche Mathematik, vol. 1 (1936), pp. 362–388.

§ Transactions of this Society, vol. 42 (1937), pp. 206–224, referred to as J.

|| R. Baer, *Algebraische Theorie der differentierbaren Funktionenkörper*. I, Sitzungsberichte Heidelberger Akademie, 1927, pp. 15–32.

or

$$x^{(p^m)} + x^{(p^{m-1})}\tau_1 + \dots + x'\tau_m = 0$$

for all $x \in C$, but no equation of the form

$$x^{(r)} + x^{(r-1)}b_1 + \dots + x'b_{r-1} + b_r = 0, \quad b_i \in C,$$

can hold if $r < p^m$.* I have shown also that any derivation in a simple subalgebra of a normal simple algebra may be extended to an inner derivation in the latter.† Thus there exists an element d in A such that $[x, d] \equiv xd - dx = xD$ for all $x \in C$.

We note that

$$(2) \quad xd^k = d^kx + C_{k,1}d^{k-1}x' + \dots + x^{(k)},$$

where the coefficients are those of the binomial theorem, and hence $xd^{p^j} = d^{p^j}x + x^{(p^j)}$. It follows from (1) that $(d^{p^m} + d^{p^{m-1}}\tau_1 + \dots + d\tau_m)$ commutes with every x , and since C is a maximal subfield of A , $(d^{p^m} + d^{p^{m-1}}\tau_1 + \dots + d\tau_m) = c \in C$. Deriving with respect to d (taking commutators), we have $[c, d] = 0$, and so $c = \delta \in F$ and

$$(3) \quad d^{p^m} + d^{p^{m-1}}\tau_1 + \dots + d\tau_m = \delta.$$

We assert that C and d generate the whole of A . Suppose

$$(4) \quad d^r + d^{r-1}b_1 + \dots + b_r = 0, \quad b_i \in C,$$

is an equation of least degree having coefficients in C and satisfied by d . If $x \in C$ by (2)

$$d^{r-1}x_1 + d^{r-2}x_2 + \dots + x_r = 0,$$

where, if we use the $C_{r,k}$ notation for binomial coefficients,

$$x_1 = C_{r,1}x', \quad x_2 = C_{r,2}x'' + C_{r-1,1}x'b_1, \dots, \\ x_r = x^{(r)} + x^{(r-1)}b_1 + \dots + x'b_{r-1}.$$

Since (4) has minimum degree, $x_1 = x_2 = \dots = x_r = 0$. But by (1) $x_r = 0$ is impossible for all x unless $r \geq p^m$. It follows that $r = p^m$ and $1, d, \dots, d^{p^m-1}$ are (right) independent over C . Thus C and d generate an algebra of order p^m over C and hence p^{2m} over F , and so C and d generate all of A . The field C , the derivation

* J, p. 218.

† J, p. 214.

D , and the equation (3) give a complete description of A .

Let $V(x)$ for $x \in C$ be the function

$$V_{p^m}(x) + V_{p^{m-1}}(x)\tau_1 + \cdots + V_1(x)\tau_m,$$

where

$$V_{p^i}(x) = x^{p^i} + (x^{(p-1)})^{p^{i-1}} + (x^{(p^2-1)})^{p^{i-2}} + \cdots + x^{(p^{i-1})}.$$

I have shown that $V(x) \in F$, and that it has properties analogous to the norm in cyclic fields.* Now suppose $\delta = V(x_0)$. If $d_1 = d - x_0$, then $[x, d_1] = xD$ for all x , and since

$$d_1^{p^j} = (d - x_0)^{p^j} = d^{p^j} - V_{p^j}(x_0),$$

we have

$$d_1^{p^m} + d_1^{p^{m-1}}\tau_1 + \cdots + d_1\tau_m = 0,$$

and so $A \cong F_{p^m}$, the algebra of all p^m -rowed square matrices with elements in F .†

Conversely suppose that $A \cong F_{p^m}$. Then there exists in A a field $\tilde{C} \cong C$ and an element \tilde{d}_1 such that $[\tilde{x}, \tilde{d}_1] = \tilde{x}\tilde{D}$ where $x \longleftrightarrow \tilde{x}$ in the isomorphism between C and \tilde{C} and

$$\tilde{d}_1^{p^m} + \tilde{d}_1^{p^{m-1}}\tau_1 + \cdots + \tilde{d}_1\tau_m = 0.$$

This isomorphism between C and \tilde{C} may be extended to an automorphism in A .‡ Hence there exists an element d_1 corresponding to \tilde{d}_1 such that $[x, d_1] = xD$ and

$$d_1^{p^m} + d_1^{p^{m-1}}\tau_1 + \cdots + d_1\tau_m = 0.$$

We observe that $d - d_1$ commutes with all the elements of C , and hence $d_1 = d - x_0$, $x_0 \in C$. It follows as before that $\delta = V(x_0)$.

THEOREM. *A necessary and sufficient condition that A be $\cong F_{p^m}$ is that $\delta = V(x_0)$, $x_0 \in C$.*

We now consider the special case where $m = 1$, $C = F(c)$, $c^p = \gamma$. Let D be the derivation such that $cD = 1$. It is easily seen that $D^p = 0$ and hence A is generated by c and d such that

* See J, p. 224.

† The symbol \cong denotes isomorphism. For the above equations and result see J, p. 223.

‡ M. Deuring, *Algebren*, 1935, p. 42.

$[c, d] = 1$ and $d^p = \delta$. Thus A has the basis $d^i c^j$ ($i, j = 0, 1, \dots, p-1$) such that

$$(5) \quad c^p = \gamma, \quad d^p = \delta, \quad cd - dc = 1.$$

The condition that $A \cong F_p$ is $\delta = V(x_0)$, $x_0 \in F(c)$. Here $V(x) = x^p + x^{(p-1)}$, and so if $x = \xi_0 + c\xi_1 + \dots + c^{p-1}\xi_{p-1}$, then

$$(6) \quad V(x) = (\xi_0^p - \xi_{p-1}) + \gamma\xi_1^p + \dots + \gamma^{p-1}\xi_{p-1}^p.$$

If δ is not a p -th power, (5) is essentially symmetric in c and d . We define the derivation $d \rightarrow dE = -1$ in $F(d)$. Since $E^p = 0$, the condition that $A \cong F_p$ is that

$$\gamma = V(y_0) = y_0 E^{p-1} + y_0^p, \quad y_0 \in F(d).$$

But if

$$y = \eta_0 + d\eta_1 + \dots + d^{p-1}\eta_{p-1},$$

then

$$V(y) = (\eta_0^p - \eta_{p-1}) + \delta\eta_1^p + \dots + \delta^{p-1}\eta_{p-1}^p.$$

Thus we have the following reciprocity theorem for arbitrary fields of characteristic p .

THEOREM. *If γ and δ are not p -th powers in F , then $(\xi_0^p - \xi_{p-1}) + \gamma\xi_1^p + \dots + \gamma^{p-1}\xi_{p-1}^p = \delta$ is solvable for $\xi_i \in F$ if and only if $(\eta_0^p - \eta_{p-1}) + \delta\eta_1^p + \dots + \delta^{p-1}\eta_{p-1}^p = \gamma$ is solvable for $\eta_i \in F$.*

UNIVERSITY OF CHICAGO