NORMAL DIVISION ALGEBRAS OF DEGREE p^e OVER F OF CHARACTERISTIC p*

BY

A. ADRIAN ALBERT

1. Introduction. In a recent paper† I proved that a normal division algebra D of degree p, a prime, over a field F of characteristic not p, is cyclic if and only if D contains a sub-field $F(y)$, $y^p=\gamma$ in F. This result evidently leads to the *conjecture that any normal division algebra D of degree n over F is cyclic over F if and only if D contains a maximal sub-field, $F(y)$, $y^n=\gamma$ in F.*

The conjectured criterion given above would be of fundamental importance for the theory of the structure of normal division algebras. Without loss of generality we may assume that $n=p^e$, p a prime, and the theory then gives rise to two distinct cases according as F does or does not have characteristic p. We shall consider the former case here and give a brief simple proof of the criterion.

2. Cyclic fields of degree p^e. Let F be a field of characteristic $p\neq 0$. An equation

$$\lambda^p = \lambda + \alpha \qquad (\alpha \text{ in } F) \tag{1}$$

is called a *normed equation*. If x is a root of (1) so are $x+1, x+2, \cdots, x+p-1$, and we have the Artin-Schreier lemmas:‡

LEMMA 1. *A normed equation is either cyclic or has its roots in F. Every cyclic field of degree p over F may be generated by a root of a normed equation.*

LEMMA 2. *Let $Z=F(x)$ be cyclic of degree p over F,*

$$x^p = x + \alpha \qquad (\alpha \text{ in } F). \tag{2}$$

Then a quantity x_0 of Z satisfies a normed equation if and only if

$$x_0 = kx + b \qquad (k = 0, 1, \cdots, p-1;\ b \text{ in } F).$$

Let Z_e be cyclic of degree p^e over F so that

$$Z_e > Z_{e-1} > \cdots > Z_1 > Z_0 = F, \tag{3}$$

where Z_i is cyclic of degree p^i over F, cyclic of degree p over Z_{i-1}. I have proved‡ that $Z_i=F(x_i)$,

* Presented to the Society, April 20, 1935; received by the editors March 26, 1935.

† These Transactions, vol. 36 (1934), pp. 885–892.

‡ For the properties of this section see my paper in the Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 625–631.

$$x_i^p = x_i + a_i \qquad (a_i \text{ in } Z_{i-1}), \tag{4}$$

and that Z_e has a generating automorphism S given by

$$x_i \longleftrightarrow x_i^S = x_i + \beta_i, \tag{5}$$

where*

$$\beta_{i+1} = (x_1 x_2 \cdots x_i)^{p-1}, \qquad T_{Z_i/F}(\beta_i) = (-1)^i, \tag{6}$$

and

$$a_i^S - a_i = \beta_i^p - \beta_i. \tag{7}$$

Every quantity of Z_e has the form

$$a = \sum_{i_j=0}^{p-1} \alpha_{i_1 i_2, \cdots, i_e} x_1^{i_1} \cdots x_e^{i_e} \qquad (\alpha_{i_1, \cdots, i_e} \text{ in } F). \tag{8}$$

Write $\alpha_0 = \alpha_{p-1, \cdots, p-1}$ so that

$$a = \alpha_0 \beta_{e+1} + a_0.$$

I have proved that there exists a quantity c in Z_e such that $a_0 = c^S - c$. Then

$$T_{Z_e/F}(a_0) = 0, \qquad T_{Z_e/F}(a) = (-1)^e \alpha_0, \qquad a = \alpha_0 \beta_{e+1} + c^S - c.$$

If $T_{Z_e/F}(a) = 0$ then $\alpha_0 = 0$ and $a = c^S - c$, while conversely $a = c^S - c$ implies that $T_{Z_e/F}(a) = 0$. When also $a = d^S - d$ then $d - c = \gamma$ has the property $\gamma = \gamma^S$, γ is in F. We thus have

LEMMA 3. *Let Z_e be cyclic of degree p^e over F and with generating automorphism S. Then*

$$T_{Z_e/F}(a) = 0 \qquad (a \text{ in } Z_e), \tag{9}$$

if and only if

$$a = c^S - c \qquad (c \text{ in } Z_e). \tag{10}$$

Moreover (10) *has a unique solution c apart from an additive constant in F.*

LEMMA 4. *The field Z_e of Lemma 3 contains a quantity β_{e+1} such that*

$$T_{Z_e/F}(\beta_{e+1}) = (-1)^e \tag{11}$$

and every a of Z_e has the form

$$a = T_{Z/F}(a)(-1)^e \beta_{e+1} + c^S - c \qquad (c \text{ in } Z_e). \tag{12}$$

In particular I have proved that

$$T_{Z/F}(\beta_{e+1}^p - \beta_{e+1}) = 0 \tag{13}$$

* We write $T_{Z/F}(a)$ for the trace of the quantity a in Z over F.

so that $\beta_{e+1}^p - \beta_{e+1} = a_{e+1}^S - a_{e+1}$. Then I have shown that the field $F(x_{e+1})$ determined by

$$x_{e+1}^p = x_{e+1} + a_{e+1} \tag{14}$$

is cyclic of degree p^{e+1} over F with Z_e as sub-field and generating automorphism given by $x_{e+1}^S = x_{e+1} + \beta_{e+1}$ and that of Z_e.

3. **Cyclic algebras of degree p over F.** Consider n-rowed square matrices A with elements in an infinite field F of characteristic p.

Two n-rowed square matrices A, B with elements in F are similar in F if and only if they have the same invariant factors. The minimum equation of A is the equation obtained by setting its invariant factor $\phi(\lambda)$ of highest degree in λ equal to zero. When $\phi(\lambda)$ has degree n it coincides with the characteristic polynomial of A and every B such that $\phi(B) = 0$ is similar to A.

In particular let $n = p$ and $y^p = \gamma$ in F, y be in a total matric algebra M of degree p over F. By a proper choice of the representation of M by the algebra of all p-rowed square matrices with elements in F we may take

$$y = \begin{pmatrix} 0 & 1 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 1 \\ \gamma & 0 & \cdot & \cdot & \cdot & 0 \end{pmatrix}. \tag{15}$$

Since F is an infinite field there exists a quantity $\xi \neq 0, 1, \cdots, p-1$ in F and thus

$$x = \begin{pmatrix} \xi & & & \\ & \xi + 1 & & \\ & & \ddots & \\ & & & \xi + p - 1 \end{pmatrix} \tag{16}$$

is non-singular. A trivial computation gives

$$x^p = x + \alpha, \qquad yx = (x + 1)y, \tag{17}$$

where $\alpha = \xi^p - \xi$ is in F.

We now let D be a normal division algebra of degree p over F and let $y^p = \gamma$ in F for y in D but not in F. There exists a separable field $K = F(\eta)$ of degree p over F such that D_K is a total matric algebra over F. Then D is equivalent to an algebra of p-rowed square matrices with elements in K and the quantities $1, \eta, \cdots, \eta^{p-1}$ are linearly independent in D, the quantities

$1, y, \cdots, y^{p-1}$ are linearly independent in K. We have thus proved that there exists a quantity x in D_K such that $yx=(x+1)y$.

We write

$$x = x_0 + x_1\eta + \cdots + x_{p-1}\eta^{p-1} \qquad (x_i \text{ in } D) \tag{18}$$

and the equation $yx=(x+1)y$ is equivalent to

$$[xy_0 - (x_0+1)y] + (yx_1 - x_1y)\eta + \cdots + (yx_{p-1} - x_{p-1}y)\eta^{p-1} = 0. \tag{19}$$

Thus $yx_0=(x_0+1)y$ where $y\neq 0, x_0\neq 0$ are in D. The minimum equation of x_0 has degree p over F and x_0+1 in $F(x_0)$ as a root. The field $Z=F(x_0)$ is cyclic over F and D is a cyclic algebra. The converse is well known and we have

THEOREM 1. *Let D be a normal division* algebra of degree p over F of characteristic p. Then D is cyclic if and only if D contains an inseparable sub-field $F(y)$, $y^p=\gamma$ in F.*

4. **Cyclic fields over $K=F(y)$.** Let $K=F(y)$ be inseparable of degree p over F, $y^p=\gamma$ in F, and let $Z=Z_e$ be cyclic of degree p^e over K. Then (3)–(7) are satisfied with β_{i+1}, a_{i+1} in $Z_i=K(x_i)$. Write $a_1=\sum_{i=0}^{p-1}\alpha_iy^i$ with α_i in F so that $a_1^p=\sum\alpha_i^py^{ip}=\sum\alpha_i^p\gamma^i=a_{01}$ is in F. Then $x_{01}=x_1^p$ has the property $x_{01}^p-x_{01}=(x_1^p-x_1)^p=a_1^p=a_{01}$ is in F. But in fact $x_{01}=x_1+a_1$ generates $K(x_1)$. Hence

$$Z_1 = Z_{01} \times K$$

where Z_{01} is cyclic of degree p over F. We may in fact prove

THEOREM 2. *Let Z be cyclic of degree p^e over $K=F(y)$, $y^p=\gamma$ in F. Then Z is the direct product*

$$Z = Z_0 \times K, \qquad Z_0 = F(x), \qquad Z = K(x),$$

where Z_0 is cyclic of degree p^e over F.

For let the above theorem be true for the sub-field Z_{i-1} of Z_e. Then $Z_{i-1}=Z_{i-1,0}\times K$ and β_i of (6) is in $Z_{i-1,0}$. We also have $Z_i=Z_{i-1}(x_i)$, $x_i^p=x_i+a_i$ and may write $a_i=\sum a_{ij}y^j$, $a_{i0}=a_i^p=\sum a_{ij}\gamma^j$ in $Z_{i-1,0}$. The quantity $x_{i0}=x_i+a_i$ $=x_i^p$ generates Z_i over K and $x_{i0}^p=x_{i0}+a_{i0}$, $x_{i0}^s=x_{i0}+\beta_i$ where a_{i0} and β_i are in $Z_{i-1,0}$. Thus $Z_{i,0}=Z_{i-1,0}(x_{i0})$ and $Z_i=Z_{i0}\times K$. The induction is complete and Theorem 2 is proved.

5. **Cyclic algebras of degree p^e over F.** We shall now prove

THEOREM 3. *Let D be a normal division algebra of degree $n=p^e$ over F of characteristic p and let $F(y)$ be a maximal sub-field of D, $y^n=\gamma$ in F. Then D is a cyclic algebra*

* If F is a finite field there exist no normal division algebras of degree greater than unity over F.

$$(Z, S, \gamma)$$

where $yx = x^S y$ *for every* x *of* Z.

For assume that the theorem is true for algebras of degree $p^i < p^e$ and let D have degree p^e over F and contain y such that $y^n = \gamma$ in F, $F(y)$ is a maximal sub-field of D. Define

$$m = p^{e-1}, \qquad y_m = y^m,$$

so that the algebra B of all quantities of D commutative with y_m is a normal division algebra of degree m over $K = F(y_m)$. By the hypothesis of our induction there exists a cyclic field Z_0 of degree m over K in B such that $yz = z^S y$. Theorem 2 states that $Z_0 = Z_{e-1} \times K$ where Z_{e-1} is cyclic of degree m over F. Any change in the generating automorphism of Z_0 is accomplished by replacing y by y^r, r prime to p, so we may assume without loss of generality that $yz = z^S y$ for every z of Z_{e-1} where S generates the cyclic automorphism group of Z_{e-1}. Write $Z_{e-1} = F(x_{e-1})$.

The algebra G of all quantities of D commutative with x_{e-1} is a normal division algebra of degree p over Z_{e-1} and contains y_m. By the hypothesis of our induction there exists an x_{01} in G such that $y_m x_{01} = (x_{01} + 1) y_m$. Then $x_0 = (-1)^{e-1} x_{01}$ has the properties

$$x_0^p = x_0 + a_0, \qquad y_m x_0 = [x_0 + (-1)^{e-1}] y_m \equiv x_0^{S_0} y_m,$$

with a_0 in Z_{e-1}. The quantity y transforms x_0 in G into

$$y x_0 y^{-1} = x_{0y} \text{ in } G, \qquad x_{0y}^p = x_{0y} + a_0^S, \qquad y_m x_{0y} = (x_{0y} + \delta) y_m$$

where

$$\delta = (-1)^{e-1} = T_{Z_{e-1}/F}(\beta_e), \qquad y_m y = y y_m.$$

Write $x_{0y} = \sum_{i=0}^{p-1} b_i y_m^i$ with b_i in $Z_{e-1}(x_0)$ and have

$$\sum_{i=0}^{p-1} b_i(x_0 + \delta) y_m^{i+1} = \delta y_m + \sum_{i=0}^{p-1} b_i(x_0) y_m^{i+1}, \qquad b_i(x_0 + \delta) \equiv b_i^{S_0} \text{ in } Z_{e-1}(x_0).$$

Thus $b_i(x_0 + \delta) = b_i$ is in Z_{e-1} for $i = 1, \cdots, m$, $b_0(x_0 + \delta) = b_0 + 1$. By Lemma 2 we have $b_0 = kx_0 + \beta$ with k an integer and β in Z_{e-1}. Then $(x_0 + \delta)k + \beta = kx_0 + \beta + \delta$, $k = 1$, $b_0 = x_0 + \beta$,

$$x_{0y} = x_0 + P(y_m)$$

where* $P(y_m)$ is in $Z_{e-1}(y_m)$.

* Note the analogy between this result and the theorem that $y_0 x = x^S y_0$ if and only if $y_0 = Py$ with P in $F(x)$.

The field $Z_0=Z_{e-1}(y_m)=Z_{e-1}\times F(y_m)$ is cyclic of degree p^{e-1} over $K=F(y_m)$. Thus $yx_0y^{-1}=x_0+P$, $y^2x_0y^{-2}=x_0+P+P^S$, and finally

$$y^m x_0 y^{-m} = x_0 + T_{Z_0/K}(P) = y_m x_0 y_m^{-1} = x_0 + \delta, \qquad T_{Z_0/K}(P) = T_{Z_{e-1}/K}(\beta_e),$$

and, since $Z_0=Z_{e-1}\times K$,

$$T_{Z_0/K}(\beta_e - P) = 0.$$

We apply Lemma 3 and obtain a quantity g in Z_0 such that $g^S-g=\beta_e-P$. Define $x_{e0}=x_0+g$ and obtain $x_{e0}^p=x_{e0}+a_{e0}$,

$$yx_e = (x_{0y} + g^S)y = (x_0 + P + g + \beta_e - P)y = (x_e + \beta_e)y.$$

Then $x_{e0}^S=x_e+\beta_e$ satisfies $(x_{e0}^S)^p=x_{e0}^S+a_{e0}$, and $K(x_{e0})$ is cyclic of degree p^e over K. By Theorem 2 the field $K(x_{e0})=K\times Z_e$ where Z_e is cyclic of degree p^e over F and has the same generating automorphism as Z_{e0}. In fact $Z_e=F(x_e)$, $x_e=x_{e0}+a_{e0}=x_{e0}^p$, $x_e=x_e{}^S+\beta_e$. We have proved Theorem 3.

University of Chicago,
Chicago, Ill.