SIMPLE ALGEBRAS OF DEGREE p^e OVER A CENTRUM OF CHARACTERISTIC p*

BY

A. ADRIAN ALBERT

1. **Introduction.** The study of normal simple algebras A over a field F has been reduced to the case where the degree of A is a power of a prime p. The theory then splits sharply into two cases distinguished by the hypothesis that the characteristic of F is or is not p. We shall restrict our attention to the former case.

It is well known that every normal simple algebra A over F is similar to a crossed product B. But this result is of little aid in a study of A, since in fact the degree of B is in general not a power of p. We shall prove here, however, that in our case every A is *similar to a cyclic algebra whose degree is a power of* p.

If K is obtained from F by adjoining the p^eth roots of quantities of F to F, for fixed e, then K is said to have exponent e over F. We shall show that the *exponent* of an *algebra* A is p^e where e is the exponent of the above K of least exponent, which splits A. Moreover A has exponent p^e only if A is similar to a direct product of *cyclic division algebras* D_i whose *exponents and degrees are equal to* $p^{e_i} \leqq p^e$, D_1 of degree p^e.

2. **Commutative division algebras over F.** Let F be an infinite field of characteristic $p \neq 0$ and K be a commutative division algebra of order n over F. A quantity k of K is called separable† or inseparable according as its minimum equation has not or has multiple roots. We shall also say that K is separable or inseparable according as K does not or does contain inseparable quantities.

Every separable K is a simple algebraic extension $Z = F(\alpha)$ of F, where α is separable of degree n over F. Conversely if α is separable so is any polynomial in α, so that $Z = F(\alpha)$ is separable. We notice that then every subfield of Z is separable. Moreover if $F(\alpha^p) \neq F(\alpha) = Z$, then $\alpha^p = v$ has the property that $Z = Z_1(\alpha)$, $\alpha^p = v$ in Z_2. But the equation $\alpha^p = v$ is inseparable. Hence we have

---

* Presented to the Society, September 13, 1935; received by the editors July 22, 1935.

† For these definitions and elementary properties see B. L. van der Waerden, *Moderne Algebra*, vol. I. I believe they are due to E. Steinitz. See also Deuring's *Algebren*, Springer, 1935, for references to the numerous concepts used here. These are in the algebraic part of Deuring's book and the references are principally to work of Dickson, Wedderburn, Hasse, Brauer, Noether, and myself.

THEOREM 1. *Let $Z=F(x)$ be separable of degree n over F. Then $Z=F(x^p)$.*

The largest separable sub-field K_0 of an inseparable field K is a field whose degree n_0 is called* the reduced degree of K. Every quantity α of K has the property

$$\alpha^{p^e} = \alpha_0 \text{ in } K_0. \tag{1}$$

If moreover $\alpha^{p^{e-1}}$ is not in K_0 for some α of K we shall call e the *exponent* of K. The field K is obviously obtained by adjoining certain p^eth roots of quantities of K_0 to K_0. If $K_0=F$ *we shall call K a Kummer field over F.* We now prove

THEOREM 2. *Let Z be a separable field of degree m over a Kummer field K of exponent e over F, and Z_0 be the largest sub-field over F of Z, Z contain K. Then Z is the direct product*

$$Z = Z_0 \times K, \tag{2}$$

Z_0 has degree m over F, Z_0 is the field of all quantities α^{p^e} of Z, α in Z.

For $Z=K(\xi)$ where ξ is a root of a separable equation

$$f(x) = x^m + a_1x^{m-1} + \cdots + a_m = 0 \qquad (a_i \text{ in } K), \tag{3}$$

irreducible in K. Thus $\eta=\xi^{p^e}$ is a root of

$$g(y) = y^m + b_1y^{m-1} + \cdots + b_m = 0 \qquad (b_i \text{ in } F), \tag{4}$$

where $b_i=a_i^{p^e}$. By Theorem 1 we have $Z=K(\eta)$, so that $g(y)$ is irreducible in K. But then $Z_0=F(\eta)$ has degree n over F and (2) holds. The largest separable sub-field of Z must contain Z_0 and is a field $F(\zeta)=F(\zeta^{p^e})$ where ζ^{p^e} is obviously in Z_0. Hence Z_0 is the largest separable sub-field of Z.

The fields Z and Z_0 of Theorem 2 are equivalent under the correspondence (*not an isomorphism over F*)

$$\alpha \longleftrightarrow \alpha^{p^e} = \alpha_0 \qquad (\alpha \text{ in } Z). \tag{5}$$

If $\alpha\neq\beta$ then $\alpha_0\neq\beta_0$ since $\alpha^{p^e}-\beta^{p^e}=(\alpha-\beta)^{p^e}=0$ only when $\alpha=\beta$. Hence we have immediately

THEOREM 3. *Let Z and Z_0 be defined as in Theorem 2. Then Z is normal over K with automorphisms*

$$S: \qquad \alpha \longleftrightarrow \alpha^S$$

if and only if Z_0 is normal over F with automorphisms

$$S: \qquad \alpha_0 \longleftrightarrow \alpha_0{}^S, \qquad \alpha_0 = \alpha^{p^e}, \qquad \alpha_0 = (\alpha^S)^{p^e}.$$

* See van der Waerden, loc. cit.

COROLLARY I. *The field Z is cyclic over K if and only if Z_0 is cyclic over F.*

Let K be a simple Kummer extension of exponent e over F, so that $K=K_e=F(y)$, $y^{p^e}=\gamma$ in F. Then

$$K_e > K_{e-1} > \cdots > K_1 > K_0 = F, \tag{6}$$

where

$$y_i = y^{p^{e-1}}, \qquad K_i = F(y_i). \tag{7}$$

The field K_i has degree p^i over F, degree p over K_{i-1}, and $1, y_i, \cdots, y_i^{p-1}$ are linearly independent in K_{i-1}. In particular every quantity k of K has the form

$$k = k_0 + k_1 y + \cdots + k_{p-1}y^{p-1} \qquad (k_i \text{ in } K_{e-1}), \tag{8}$$

and, if $q=p^{e-1}$, then

$$k^q = k_0 + k_1^q y_1 + \cdots + k_{p-1}^q y_1^{p-1} \qquad (k_i^q \text{ in } F) \tag{9}$$

is in F if and only if $k_1=k_2=\cdots=k_{p-1}=0$. Thus we have proved

THEOREM 4. *A quantity k of K_e generates K_e if and only if k is not in K_{e-1}.*

We shall require

THEOREM 5. *Let Z be separable of degree m over $K=K_e=F(y)$, $y^{p^e}=\gamma$ in F. Then there exists a quantity c in Z such that*

$$w = N_{Z/K}(c) \tag{10}$$

has the property $K=F(w)$, that is, w generates K.

For $Z=Z_0\times K$, $Z_0=F(x)$, x is a root of

$$f(x) = \sum_{i=0}^{p-1} a_i(x^p)x^i = 0. \tag{11}$$

The polynomials $a_i(x^p)$ have coefficients in F and at least one $a_i(x^p)\neq 0$ for $i=r\neq 0$, since x is separable. Hence $a_r(\lambda^p y^p)$ is a polynomial in y^p with coefficients which are polynomials in λ with coefficients in F. These latter polynomials are not all identically zero, and thus there exists a λ_0 in F such that $a_r(\lambda_0^p y^p)\neq 0$,

$$f(\lambda_0 y) = \sum_{i=0}^{p-1} b_i y^i, \qquad b_i = a_i(\lambda_0^p y^p)\lambda^i \text{ in } K_{e-1}. \tag{12}$$

The quantity $f(\lambda_0 y)$ is not in K_{e-1} and, if $c=x-\lambda_0 y$, then

$$g(c) = f(c+\lambda_0 y) = c^m + B_1 c^{m-1} + \cdots + B_{m-1}c + f(\lambda_0 v) = 0. \tag{13}$$

But

$$N_{Z/K}(c) = (-1)^m f(\lambda_0 y) = w$$

is in K_e and not in K_{e-1}. By Theorem 4 we have $K = F(c)$.

The field K_e has degree p over $K_{e-1} = F(y^p)$ and, if δ is in K_{e-1}, and w is as above, then δw is not in K_{e-1}. This gives

THEOREM 6. *Let Z be as in Theorem 5 and δ be in K. Then there exists a quantity c of Z such that*

$$\delta_0 = N_{Z/K}(c)\delta \tag{14}$$

generates K, $K = F(\delta_0)$.

3. **Matrices with elements in F.** The theorems of the author's paper* *On normal simple algebras* hold for an arbitrary infinite field F although they were derived for the case where F is non-modular. The extension to the more general case may be made by the elementary considerations of the next three sections.

The matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ \alpha_n & \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_1 \end{pmatrix}, \qquad \alpha_i \text{ in } F, \tag{15}$$

has

$$|\lambda I - A| = \phi(\lambda) = \lambda^n - \alpha_1\lambda^{n-1} - \cdots - \alpha_n = 0 \tag{16}$$

as its characteristic equation. It may be easily verified that the identity matrix I, A, A^2, $\cdots$, A^{n-1} are linearly independent in any scalar field containing F and that $\phi(\lambda) = 0$ is actually the minimum equation of A. Moreover every n-rowed square matrix with $\phi(\lambda) = 0$ as *minimum* equation is similar in F to A.

Every matrix B with elements in F is similar to a matrix†

$$\begin{pmatrix} A_1 & & \\ & \cdot & \\ & & A_r \end{pmatrix} \tag{17}$$

where A_i is a matrix whose characteristic equation is its minimum equation. The characteristic determinants $D_i(\lambda)$ of the A_i are called the invariant fac-

* These Transactions, vol. 34 (1932), pp. 620–625.

† These are the classical results on matrices with elements in F.

tors of B and $D_{i-1}(\lambda)$ is divisible by $D_i(\lambda)$, $i=2, \cdots, \nu$. Thus $D_1(A)=0$, and $D_1(\lambda)=0$ is in fact the minimum equation of the matrix B. It is evident that a matrix $\overline{B}$ is similar to B if and only if $\overline{B}$ has the same invariant factors and hence the same canonical form given by (15), (17) as B.

When $D_1(\lambda)$ is irreducible we must have every $D_i(\lambda) \equiv D_1(\lambda)$, $n=m\nu$ where A_1 has m rows. Thus

$$B = \begin{pmatrix} A_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & A_1 \end{pmatrix}, \tag{18}$$

and $\overline{B}$ is similar to B if and only if $\overline{B}$ has the same *irreducible* minimum equation as B.

4. **Sub-fields of M_n.** Let M_n be the algebra of all n-rowed square matrices with elements in F. If Z is a *separable* sub-field of M_n and $\overline{Z}$ is equivalent to Z, then $Z=F(B)$, $\overline{Z}=F(\overline{B})$, where B and $\overline{B}$ have the same irreducible minimum equation. Hence $B=P\overline{B}P^{-1}$ where P is a non-singular quantity of M_n, and the inner automorphism of M_n, defined by the transformation of its quantities by P, carries B into $\overline{B}$. If $CB=BC$ then

$$C = (C_{ij}) \qquad (i, j = 1, \cdots, \nu) \tag{19}$$

and $C_{ij}A_1=A_1C_{ij}$. But it is known* that then C_{ij} is a polynomial in A_1 with coefficients in F. Hence the algebra of all quantities of M_n commutative with every quantity of Z is equivalent to a total matric algebra of degree ν over Z, $n=m\nu$, Z of degree m over F.

The above result cannot be extended to inseparable sub-fields K of M_n without further argument since the known proofs that $C_{ij}A_1=A_1C_{ij}$ if and only if C_{ij} is in $F(A_1)$ depend upon the hypothesis that A_1 has its characteristic roots all distinct. Hence we must treat this case here. We first prove

LEMMA 1. *Let $F(y)$ be a sub-field of M_p, $y^p=\gamma$ in F, F an infinite field of characteristic p. Then the only quantities of M_p commutative with y are quantities of $F(y)$.*

For we have seen that we may take

$$y = \begin{pmatrix} 0 & 1 & 0 \cdots 0 \\ 0 & 0 & 1 \cdots 0 \\ \cdot & \cdot & \cdot \cdots \cdot \\ 0 & 0 & 0 \cdots 1 \\ \gamma & 0 & 0 \cdots 0 \end{pmatrix}. \tag{20}$$

* Cf. the proof in Wedderburn's *Lectures on Matrices*, pp. 26–27.

Since F is infinite there exists a ξ in F such that $\xi \neq 0, 1, \cdots, p-1$. The matrix

$$x = \begin{pmatrix} \xi & & & \\ & \xi+1 & & \\ & & \ddots & \\ & & & \xi+p-1 \end{pmatrix} \tag{21}$$

is non-singular and has the property $yx=(x+1)y$. An elementary computation then gives

$$e_{11} = \frac{[x-(\xi+1)][x-(\xi+2)]\cdots[x-(\xi+p-1)]}{1\cdot 2\cdots(p-1)} \tag{22}$$

where e_{ij} is the matrix with unity in the ith row and jth column and zeros elsewhere. Moreover it is well known* that

$$e_{ij} = y^{1-i}e_{11}y^{j-1}. \tag{23}$$

But the relation $yx=(x+1)y$ then implies that every quantity of M_p is a linear combination of the p^2 quantities

$$x^i y^j \qquad (i, j = 0, 1, \cdots, p-1). \tag{24}$$

The algebra M_p has order p^2 over F and hence (24) are linearly independent in F. Thus $1, y, \cdots, y^{p-1}$ are *left linearly independent* in the commutative algebra $F(x)$. This latter algebra is not a field, however.

We now write $z=\sum_{i=0}^{p-1}a_i(x)y^i$ and have

$$zy - yz = \sum_{i=0}^{p-1}[a_i(x+1) - a_i(x)]y^{i+1} = 0, \tag{25}$$

so that $a_i(x)=a_i(x+1)$, $i=0, \cdots, p-1$. But then the element of the first row of $a_i(x)$ is $a_i(\xi)=a_i(\xi+1)$ so that $a_i(\xi)=a_i(\xi+1)=a_i(\xi+2)=\cdots=a_i(\xi+p-1)$ and $a_i(x)$ is a scalar matrix. Hence z is in $F(y)$.

We now prove

THEOREM 7. *Let Z be any sub-field of degree m of M_n. Then the sub-algebra of M_n commutative with Z is a total matric algebra M_ν of degree $\nu=nm^{-1}$ over Z, and any sub-field $\overline{Z}$ of M_n equivalent to Z may be carried into Z by an inner automorphism of M_n.*

The theorem is trivial when $n=1$. Hence assume it true for total algebras M_ν of degree $\nu<n$.

Let Z_0 be the largest separable sub-field of Z. Then we have proved the

* Cf. these Transactions, vol. 33 (1931), pp. 690–711, formula (20) on p. 702. Formula (18) was incorrectly printed there and should read $e_{11}y^{k-1}=e_{1k}$.

above theorem for Z_0 and hence may carry the sub-field $\overline{Z}_0$ of $\overline{Z}$ into Z_0. Hence we take $Z_0=\overline{Z}_0$ and have proved that the algebra of all quantities of M_n commutative with Z_0 of degree m_0 over F is a total matric algebra of degree $n_0=nm_0^{-1}$ over Z_0. Every inner automorphism of M_{n_0} over Z_0 is an inner automorphism of M_n leaving Z_0 invariant and M_{n_0} contains both Z and $\overline{Z}$. If $Z_0\neq F$ then $n_0<n$ and we may carry Z into $\overline{Z}$ by an inner automorphism of M_{n_0}; the algebra of all quantities of M_{n_0} commutative with Z is a total matric algebra of degree $n_0m_1^{-1}$ over Z. But Z has degree m_1 over Z_0, $m=m_1m_0$, $n_0m_1^{-1}=nm^{-1}=\nu$ and the algebra of all quantities of M_n commutative with Z is M_ν over Z. Hence let $Z_0=F$, Z be a Kummer field of degree $m=p\mu$ over F. Then Z has degree μ over $K=F(y)$, $y^p=\gamma$ in F.

The minimum equation of y is irreducible in F and $\overline{Z}>\overline{K}=F(\bar{y})$, $\bar{y}^p=\gamma$, $\bar{y}$ may be carried into y by an inner automorphism of M_n. Thus we take $y=\bar{y}$, $K=\overline{K}$, and y in the form (18) with A_1 given by (20). By Lemma 1 the sub-algebra of M_n commutative with y is M_{ν_0} of degree $\nu_0=np^{-1}$ over K. Moreover M_{ν_0} contains Z, $\overline{Z}$, and our induction states that there exists an inner automorphism of M_{ν_0} carrying $\overline{Z}$ into Z, the sub-algebra of M_{ν_0} commutative with Z is M_ν over Z, $\nu=\nu_0\mu^{-1}=nm^{-1}$. This inner automorphism of M_{ν_0} is an inner automorphism of M_n, and M_ν is obviously the sub-algebra of M_n commutative with Z. This proves Theorem 7.

5. **Simple algebras over F.** Let A be a simple algebra of degree n over its centrum F and let Z be a sub-field of degree m of A. If Z_0 is the maximum separable sub-field of Z then the sub-algebra B_0 over Z_0 of all quantities of A commutative with every quantity of Z_0 is well known to be a simple algebra of degree $\nu_0=nm_0^{-1}$ over its centrum Z_0 of degree m_0 over F. But we may in fact prove

THEOREM 8. *The sub-algebra of A commutative with Z is a normal simple algebra B of degree nm^{-1} over its centrum Z. Moreover if $\overline{Z}$ is a scalar field equivalent to Z then*

$$A_{\overline{Z}} = M_m \times \overline{B}, \tag{26}$$

where $\overline{B}$ over $\overline{Z}$ is equivalent to B over Z.

For it is obviously sufficient to prove the above theorem when $Z_0=F$. There exists a separable splitting field X of A and $A_X=M_n$ over X. But the composite $Z_X=(Z, X)$ is evidently an inseparable field of degree n over X and Theorem 6 states that the sub-algebra of A_X commutative with Z_X is M_ν over Z_X. Evidently $M_\nu=B_X$ so that B is normal simple of degree ν over Z. The remainder of the proof is as in the non-modular case quoted* in §3.

* These Transactions, vol. 34 (1932), pp. 620–625.

6. **Kummer splitting fields and cyclic algebras.** Let F have characteristic p and Ω be a perfect extension of F. Then if A is any normal simple algebra of degree p^e over F the algebra A_Ω is a total matric algebra.* The field Ω may be taken to consist of quantities δ such that δ^{p^s} is in F for some s depending on δ, and thus every sub-field of Ω of finite degree over F is a Kummer field over F. In particular the sub-field K of Ω, which contains all of the coefficients in the expression of an ordinary matric basis of A_Ω in terms of the basal units of A, has finite degree over F and splits A. We have proved

THEOREM 9. *Every normal simple algebra A of p^e over F of characteristic p has a Kummer splitting field.*

We next prove

THEOREM 10. *If there exist no cyclic fields of degree p over F then there exist no normal division algebras of degree p^e over F.*

For let D be a normal division algebra of degree p^e over F. Theorem 9 states that there exists a Kummer field K such that K does not split D but $K(y)$, $y^p=\gamma$ in K, does split D. Thus D_K is similar to a normal division algebra E of degree p over K which is split by $K(y)$. The author has then proved† that $E=(\gamma, Z, S)$ where Z is cyclic of degree p over K. By Theorem 2, $Z=Z_0\times K$ where Z_0 is cyclic of degree p over F.

If F possesses no cyclic extensions of degree p over F, then Theorem 10 implies that every normal simple algebra of degree p^e over F is a total matric algebra. This case is then complete, so we shall henceforth assume that there exist cyclic fields of degree p over F.

The author has shown‡ that our above assumption then implies that there exist cyclic fields Z_f of degree p^f over F for every f. Moreover if Z_f is given then there exists a cyclic Z_e, $e>f$, such that Z_e contains Z_f.

In particular let $f=e-1$. Then the author has proved† that

$$Z_e = F(x), \qquad x^p = x + a + \lambda \qquad (a \text{ in } Z_{e-1},\ \lambda \text{ in } F), \tag{27}$$

with generating automorphism S given by that of Z_e and

$$x^S = x + \beta. \tag{28}$$

The quantities a, β are uniquely determined quantities of Z_{e-1}, and the author

* These Transactions, vol. 36 (1934), pp. 388–394.

† See the paper *On normal division algebras of degree p^e over F of characteristic p*, these Transactions, vol. 39 (1936), pp. 183–188.

‡ Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 625–631.

has moreover proved that if a, β, λ are given, $x^p = x + a + \lambda$ is irreducible in Z_{e-1}, $F(x) = Z_e$ is cyclic of degree p^e over F.

Our hypothesis that there exist cyclic fields of degree p over F then implies that there exist cyclic algebras of arbitrary degree p^e over F. The author has proved*

LEMMA 2. *Let (γ, Z, S) be cyclic of degree $n = p^e$ over F and Y be the cyclic sub-field of Z of degree p^{e-1}. Then*

$$(\gamma, Z, S)^p = M_n^{p-1} \times M_p \times (\gamma, Y, S). \tag{29}$$

As an immediate application of Lemma 2 we obtain†

THEOREM 11. *Let $A = (\gamma, Z, S)$ be cyclic of degree p^e over F of characteristic p. Then Z is contained in a cyclic field $\overline{Z}$ of degree p^{e+1} over F, and the algebra*

$$B = (\gamma, \overline{Z}, S) \tag{30}$$

has the property

$$A \sim B^p. \tag{31}$$

7. **Theory of cyclic representations.** A field F of characteristic p is said to be perfect if there are no Kummer fields of degree p over F. Then there are no normal division algebras of degree p^e over F. This, combined with our previous discussion, shows that the theory of normal simple algebras of degree p^e over F becomes trivial except when there exist both Kummer and cyclic fields of degree p over F. We may therefore restrict our attention to this remaining‡ non-trivial case, and have seen that there now exist cyclic and Kummer fields of arbitrary degree p^e over F.

A total matric algebra of degree p over F contains fields isomorphic to any fields of degree p over F. Every normal simple algebra A of degree p over F is either a total matric algebra or a normal division algebra, and the author has shown§ that in the latter case A is a cyclic algebra if and only if it has a simple Kummer sub-field of degree p over F. Thus we have the case $e = 1$ of

---

* See the American Journal of Mathematics, vol. 54 (1932), pp. 1–13, for my proof holding for any field.

† Theorem 11 is false when F does not have characteristic p, since in fact the algebra $A = (1, i, j, ij)$, $i^2 = j^2 = -1$, $ji = -ij$, over the field R of rational numbers, is not similar to B^2 for any B of degree 4 over its centrum R. Note also that $A \sim B$, for normal simple algebras A and B, means $A = M \times D$, $B = M_0 \times D$ where D is a division algebra, M and M_0 are total matric algebras.

‡ We have actually assumed that the field F does not possess a certain type of algebraic closure. Such fields F of course exist and there do exist normal division algebras of degree p^e over some fields F.

§ These Transactions, vol. 39, loc. cit.

THEOREM 12. *A normal simple algebra A of degree p^e over F is cyclic if and only if A has a simple Kummer sub-field $K=F(y)$ of degree p^e over F.*

For we now assume the above theorem true for algebras of degree $p, p^2, \cdots, p^{e-1}$ and write $y_0=y^{p^{e-1}}$, $y_0{}^p=\gamma$ in F, $K=F(y)$ of degree p^e over F. The sub-algebra of A commutative with y_0 is a normal simple algebra C_{y_0} of degree p^{e-1} over $K_0=F(y_0)$ by Theorem 8. The algebra C_{y_0} contains the simple Kummer field $K_0(y)$ of degree p^{e-1} over K_0 and the hypothesis of our induction states that C_{y_0} is a cyclic algebra (g, X, S) where X is cyclic of degree p^{e-1} over K_0 and y is in K_0. If d is any quantity of X and

$$g' = N_{X/K_0}(d)g, \tag{32}$$

then $C_{y_0}=(g', X, S)$. Hence Theorem 6 states that we may choose g' to generate K_0. Obviously $C_{y_0}=C_{g'}$ so that we may write $C_{y_0}=(y_0, X, S)$,

$$yx = x^S y \qquad (x \text{ in } X), \tag{33}$$

without loss of generality.

Theorem 3 states that $X=X_0\times K_0$ where X_0 is cyclic of degree p^{e-1} over F and

$$yx_0 = x_0{}^S y \qquad (x_0 \text{ in } X_0). \tag{34}$$

The algebra C_{X_0} of all quantities of A commutative with every x_0 of X_0 is a normal simple algebra of degree p over F by Theorem 8. If C_{X_0} is a total matric algebra over X_0, then C_{X_0} contains fields equivalent to any field of degree p over X_0. But then A contains cyclic fields of degree p^e over F with X_0 as sub-field and is a cyclic algebra. Hence let C_{X_0} be a division algebra.

The algebra C_{X_0} contains the sub-field $K_0=F(y_0)$, $y_0{}^p=\gamma$, and the author has then proved* that $C_{X_0}=(\gamma, Z, S)$ where $Z=X_0(z)$ is cyclic of degree p over X_0,

$$z^p = z + a, \qquad y_0 z = (x_0 + \epsilon)y_0 \qquad (a \text{ in } X_0). \tag{35}$$

Also we may take

$$\epsilon = (-1)^{e-1} = T_{X_0/F}(\beta), \tag{36}$$

where β is given as in (28) and $T_{X_0/F}$ is the trace function. The quantity y transforms every quantity of X_0 into a quantity of X_0 and hence every quantity of C_{X_0} into a quantity of C_{X_0}. We thus write

$$yy_0 = y_0 y, \qquad yzy^{-1} = z_y = \sum_{i=0}^{p-1} b_i y_0{}^i \qquad (b_i \text{ in } Z). \tag{37}$$

* These Transactions, vol. 39, loc. cit.

But obviously $y_0 z_y = (z_y + \epsilon) y_0$ so that we have

$$\sum_{i=0}^{p-1} b_i(z+\epsilon) y_0^{i+1} = \epsilon y_0 + \sum_{i=0}^{p-1} b_i(z) y_0^{i+1}. \tag{38}$$

Thus $b_i(z+\epsilon) = b_i$ is in X_0 for $i = 1, \cdots, m$, while $b_0(x_0+\epsilon) = b_0 + \epsilon$. Then $b_0 = kz + \delta$ with k an integer and δ in X_0, $k(z+\epsilon)+\delta = kz + k\epsilon + \delta = kz + \delta + \epsilon$, $k = 1$,

$$z_y = z + P, \qquad P \text{ in } X = X_0(y_0). \tag{39}$$

The transformation of z by powers of y then gives $q = p^{e-1}$, $y^q = y_0$,

$$y^q z y^{-q} = z + \epsilon = z + T_{X/K}(P), \tag{40}$$

so that $T_{X/K}(P - \beta) = 0$. The author has then demonstrated* the existence of quantity Q in X such that

$$\beta = P + Q^S - Q. \tag{41}$$

We write

$$x_e = z + Q, \tag{42}$$

and have $y x_e y^{-1} = z + P + Q^S = x_e + \beta$. Thus $y_0 x_e y_0^{-1} = x_e + \epsilon$ satisfies a normed equation $x_e{}^p = x_e + a_e$ where $(x_e + \beta)^p = x_e + \beta + a_e{}^S$,

$$a_e{}^S - a_e = \beta^p - \beta. \tag{43}$$

But then $F(x_e)$ is cyclic of degree p^e over F and A is a cyclic algebra.

Conversely let $A = (\gamma, Z, S)$ be cyclic of degree p^e over F. From Lemma 2, $A = M \times (\delta, Y, S)$ where M is a total matric algebra and Y is the sub-field of Z of degree $q = p^f$ over F, $\delta \neq \lambda^p$ for any λ of F. The algebra (δ, Y, S) thus has a simple Kummer sub-field $F(y_0)$, $y_0{}^q = \delta$, and $M \times F(y_0)$ contains a simple Kummer field $F(y)$, $y^{p^e} = \gamma$, of degree p^e over F.

As a consequence of Theorem 12 we have

THEOREM 13. *Let A and B be cyclic algebras whose degrees are powers of the characteristic p of F. Then $A \times B$ is a cyclic algebra.*

For Theorem 12 states that B has a maximal simple Kummer sub-field $K_e = F(y)$. We write $A_K = (y_1, Z, S)$ where Z is cyclic of degree p over K. By Theorem 6 we may take y_1 to generate K and thus A_K has a simple Kummer sub-field $K_0 = K(y_0)$, $y_0{}^{p^e} = y_1$. Obviously $K_0 = F(y_0)$, $y_0{}^q = \delta$ in F, K_0 has degree $q = p^{e+f}$ over F. But the degree of $A \times B$ is q and $A \times B$ contains K_0. Hence Theorem 12 states that $A \times B$ is cyclic.

* These Transactions, vol. 39, loc. cit.

A further consequence of Theorem 12 is given by

THEOREM 14. *A normal division algebra D of degree p^f over F is similar to a cyclic algebra if and only if D has a Kummer splitting field of degree p^e over F.*

For by Theorem 12 algebra D has a Kummer splitting field of degree p^e over F when D is similar to a cyclic algebra.

Conversely let K split D. If $K=F(y)$ is simple of degree p^e over F, then $e>f$ and Theorem 12 states that D is similar to a cyclic algebra of degree p^e over F. Let then $K=F(y_1, \cdots, y_r)$ of degree p^e be a splitting field of D and assume as the basis of an induction on r that our theorem is true for algebras with Kummer splitting fields with at most $r-1$ generators. We may also assume that no sub-field of K splits D. Then $K_0=F(y_1)$ does not split D and has degree p^k over F, $K=K_0(y_2, \cdots, y_r)$ has degree p^{e-k} over K_0. Thus D is similar to a normal simple algebra A of degree p^e over F with K as maximal sub-field. The algebra B of all quantities of A commutative with y is a normal simple algebra of degree p^{e-k} over K_0 and is split by $K=K_0(y_2, \cdots, y_r)$. By the hypothesis of our induction B is a cyclic algebra (γ, Z, S) over K_0 with γ in K_0. Theorem 6 implies that we may take γ to generate K_0, $\gamma=y_1$, and thus B contains a sub-field $K(y)$, $y^{p^{e-1}}=y_1$, $y^{p^e}=\delta$ in F. By Theorem 12 algebra A is a cyclic algebra.

As an immediate corollary of Theorems 13 and 9 we have our principal result:

THEOREM 15. *Every normal division algebra of degree p^f over F of characteristic p is similar to a cyclic algebra of degree $p^e \geqq p^f$.*

8. **Theory of exponents.** A cyclic field Z of degree $\nu=p^n$ over F has the generation $Z=F(x)$ where x is a root of a (separable) cyclic equation of degree ν over F. Theorem 1 states that any quantity z of Z has the form

$$z = \sum_{i=1}^{\nu} \alpha_i x^{p(i-1)}, \qquad \alpha_i \text{ in } F. \tag{44}$$

As a consequence of (44) we may prove

THEOREM 16. *The exponent $\rho=p^\phi$ of a normal division algebra D of degree p^e over F is the least integer p^f such that f is the exponent of a Kummer splitting field of D.*

For D is similar to a cyclic algebra (γ, Z, S) of degree $\nu=p^n$ over F. Let K be a Kummer splitting field of D of least exponent f over F so that D_K is a total matric algebra. Then $\gamma=N_{Z_0/K}(z_0)$, where z_0 is in $Z_0=Z_K$. The

quantity $z=z_0^q$ is in Z if $q=p^f$ and hence $\gamma^q=N_{Z/F}(z)$. It is well known* that then the exponent $\rho=p^\phi$ is at most p^f, $\phi\leqq f$.

Conversely let $\rho=p^\phi$. If $\phi=1$ then $\gamma^p=N_{Z/F}(z)$ where z in Z has the form (44). Write

$$\beta_i = \alpha_i^{1/p}. \tag{45}$$

Not every β_i is in F, for otherwise $z_1=\sum_{i=1}^{p}\beta_i x^{i-1}$ is in Z, $z_0=z_1$, $\gamma^p=[N_{Z/F}(z_1)]^p$, γ must be the norm of z_1 when F has characteristic p. Then D is a total matric algebra contrary to hypothesis. But $K=F(\beta_1, \cdots, \beta_\nu)$ has exponent unity over F, $z=z_1^p$ where z_1 is in Z_K, $\gamma=N_{Z_1/K}(z_1)$, K splits D. Thus $f=\phi=1$.

We have proved Theorem 16 true for $\phi=f=1$. Assume it true for algebras of exponents p, p^2, $\cdots$, $p^{\phi-1}$, and let D have exponent p^ϕ. The algebra D^p has exponent $p^{\phi-1}$ and the hypothesis of our induction implies that D^p has a Kummer splitting field H of exponent $\phi-1$. The algebra $(D_H)^p$ is a total matric algebra so that D_H has exponent 1 or p. In either case D_H has a Kummer splitting field $K\geqq H$ of exponent at most unity over H, and K has exponent $\psi\leqq\phi$ over F. Obviously K splits D so that $\phi\geqq\psi\geqq f$. But we have proved that $\phi\leqq f$ so that $\phi=f$ and our theorem is proved.

Let K be a Kummer field of degree p^r and exponent unity over F. Then

$$K=K_r > K_{r-1} > \cdots > K_1 > K_0 = F, \tag{46}$$

where

$$K_i = F(\alpha_1^{1/p}, \cdots, \alpha_i^{1/p}) = K_{i-1}(\alpha_i^{1/p}), \quad \alpha_i \text{ in } F, \qquad (i=1, \cdots, r). \tag{47}$$

Obviously $K_r\neq F(\beta_1^{1/p}, \cdots, \beta_s^{1/p})$ for any β_j in F and $s<r$. We now prove

THEOREM 17. *Let A be a normal simple algebra of exponent p over F and p^r be the minimum degree of all Kummer splitting fields of A of exponent unity. Then A is similar to an algebra*

$$D_1 \times D_2 \times \cdots \times D_r, \tag{48}$$

where D_i is a cyclic division algebra of degree p over F.

For we may assume that A is a normal simple algebra of degree p^r over F with K as a maximal sub-field. If $r=1$ then $K=F(\alpha^{1/p})$ splits A and the author has shown† that then A is a cyclic algebra (γ, Z, S) of degree p over F.

We make an induction on r and let $H=K_{r-1}$. By hypothesis H does not split A, so that, by Theorem 8, the sub-algebra B of A of all quantities com-

* American Journal of Mathematics, loc. cit.

† These Transactions, vol. 39, loc. cit.

mutative with every quantity of H is a normal division algebra of degree p over H. By our above case $r=1$, $B=(\alpha_1, Z, S)$ over H and, since $Z=Z_0\times H$, algebra $B=(\alpha_1, Z_0, S)\times H=D_1\times H$ where D_1 is cyclic of degree p over F. Thus $A=D_1\times A_1$ where A_1 is a normal simple algebra of degree p^{r-1} with H as a maximal sub-field. If r_0 is the least integer for which A_1 has a Kummer splitting field of degree p^{r_0} over F and exponent unity, then the corresponding integer for A is at most r_0+1. Thus $r\leqq r_0+1$. But evidently $r_0\leqq r-1$, $r\geqq r_0+1$, $r_0=r-1$. By our induction $A_1=D_2\times\cdots\times D_r$, A has the form (48) as desired.

We shall finally prove

THEOREM 18. *Every normal simple algebra of exponent p^e is similar to a direct product of cyclic normal division algebras*

$$D_1\times\cdots\times D_t, \tag{49}$$

where the exponent and degree of D_i are equal and at most p^e, and where D_1 has exponent p^e.

For we have the above result when $e=1$. Let us then make an induction on e. The algebra A of exponent p^e is such that A^p has exponent p^{e-1}. By the assumption of our induction $A^p\sim B_1\times\cdots\times B_r$, where B_i is a cyclic normal division algebra of degree and exponent $p^{f_i}\leqq p^{e-1}$. If $p^{f_i}<p^{e-1}$ for all values of i, then the exponent of $B_1\times\cdots\times B_r$ is at most p^{e-2}, a contradiction. Hence we may assume that the exponent of B_1 is p^{e-1}. By Theorem 11 there exist cyclic normal division algebras D_i of degree p^{f_i+1} such that $D_i{}^p\sim B_i$. Evidently D_i has exponent p^{f_i+1}. Moreover

$$A^p\sim A_0{}^p,$$

where

$$A_0=D_1\times\cdots\times D_r.$$

But if A_0^{-1} is reciprocal to A_0, the algebra $(AA_0^{-1})^p$ is a total matric algebra. Either AA_0^{-1} is a total matric algebra and A is similar to A_0, or AA_0^{-1} has exponent p. In the latter case $AA_0^{-1}\sim D_{r+1}\times\cdots\times D_t$ where D_{r+j} has exponent and degree p. Then

$$A\sim D_1\times\cdots\times D_t,$$

as desired.

The above canonical form for A evidently yields an algebra of exponent p^e if and only if algebra B of exponent p given by $q=p^{e-1}$, $B=D_1{}^q\times\cdots\times D_t^q$, is not a total matric algebra. Hence in (49) we assume that $D_1, \cdots, D_s$ have

degree and exponent p^e while $D_{s+1}, \cdots, D_t$ have degree at most p^{e-1}. We write

$$D_i = (\gamma_i, Z_i, S_i), \qquad \gamma_i \text{ in } F,$$

where Z_i is cyclic of degree p^e over F. Then it is known* that the degree of D_i is its exponent if and only if

$$B_i = (\gamma_i, Y_i, S)$$

is a division algebra, where Y_i is the unique sub-field of degree p of Z_i. Thus A has exponent p^e if and only if $B_1 \times \cdots \times B_s$ is not a total matric algebra.

9. **A conjecture.** The structure of a normal division algebra relative to exponent has been in doubt since the author proved† the existence of *primary* normal division algebras of degree eight and exponent four. The results of §8 completely solve the problem for normal division algebras of degree p^e over F of characteristic p. The only remaining case is that of division algebras of degree p^e over F of characteristic not p, since the study of normal division algebras has been reduced to the case where the degree and exponent are a power of a prime. For this case we may hope to prove the

CONJECTURAL THEOREM. *A normal division algebra D has exponent p^e only if D is similar to a direct product of normal division algebras*

$$D_1 \times \cdots \times D_t,$$

where the exponent of D_i is its degree $p^{e_i} \leqq p^e$, and D_1 has degree p^e.

Thus the author's example of an algebra D of degree eight and exponent four *may possibly be* that of a normal division algebra D obtained by

$$M_2 \times D = D_1 \times D_2,$$

where D_1 and D_2 are normal division algebras of degree and exponent four, M_2 is a total matric algebra of degree two.

The author has not attempted to prove the above conjecture, but its proof is probably very difficult. It would be an important advance in the theory, however.

---

* American Journal of Mathematics, loc. cit.

† Bulletin of the American Mathematical Society, vol. 39 (1933), pp. 265–277.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.