p-ALGEBRAS OVER A FIELD GENERATED BY ONE INDETERMINATE*

BY A. A. ALBERT

1. *Introduction.* The structure of all division algebras over the simplest type of non-modular field, the field of all rational numbers, has been determined.† The correspondingly simplest type of infinite modular field‡ is the simple transcendental extension $K = F(x)$ of a finite field F. Every division algebra D over such a K is a normal division algebra of degree n over a centrum G which is algebraic of finite degree over K. It is well known that the problem of determining the structure of D is reducible to the case where n is a power of a prime p. When p is the characteristic of F the algebra D is called a p-algebra and we shall solve the problem in this case. Our results will be valid if we replace the finite field F by any perfect field of characteristic p.

The theorem we shall obtain is remarkable not merely because of the character of the result thus derived but also because of the extremely elementary nature of the proof. By using a simple property of the field G described above we shall show that every p-algebra with centrum G is cyclic and of exponent equal to its degree. Moreover this result is due to the unusual fact that all cyclic algebras over G of the same degree p^e have a common pure inseparable splitting field.

2. *Simple Transcendental Extensions of F.* Consider any perfect field F of characteristic p. Then every a of F has the form $a = b^{p^k}$ for b in F. It is easily seen that in fact the correspondences

$$a \longleftrightarrow a^{p^k}, \qquad (k = 0, 1, \cdots),$$

are automorphisms of F.

We let x be an indeterminate over F, $J = F[x]$ be the set of

---

* Presented to the Society, September 7, 1937.

† Cf. the paper of H. Hasse and the author, Transactions of this Society, vol. 34 (1932), pp. 722–726.

‡ There is no structure problem for division algebras over finite fields as they are always finite fields.

all polynomials in x with coefficients in F. Then the rational function field $K=F(x)$ of all rational functions of x with coefficients in F is the quotient field of J. If α is in J such that

$$\alpha = a_0 + a_1x + \cdots + a_nx^n, \qquad (a_i \text{ in } F),$$

then $a_i=b_i^q$ with $q=p^k$ and b_i in F, and

$$\alpha = \beta^q, \qquad \beta = b_0 + b_1y + \cdots + b_ny^n$$

is in $F[y]$, $y^q=x$. Evidently every quantity of the field $K=F(x)$ is the p^k-th power of a quantity of $K_0=F(y)$. This result will be shown to imply the following theorem:

THEOREM 1. *Let x be an indeterminate over a perfect field F of characteristic p so that every algebraic extension G of degree n over $K=F(x)$ is inseparable of degree $t=p^e$ over its maximal separable sub-field $H=K(u)$ of degree $m=np^{-e}$ over K. Then*

$$(1) \qquad G = H(y) = K_0(u) = F(y, u), \quad K_0 = F(y), \quad y^t = x,$$

so that G is uniquely determined in the sense of equivalence by H and $t=p^e$. Conversely the field G of (1) *has degree p^e over H.*

If $q=p^k$ and $K(u^q)$ were a proper sub-field of $H=K(u)$, the field H would be inseparable. Hence every quantity of H of degree m over K is *uniquely* expressible in the form

$$(2) \qquad w = \alpha_0 + \alpha_1u^q + \cdots + \alpha_{m-1}u^{q(m-1)}, \qquad (\alpha_i \text{ in } K).$$

If $K(u, x^{1/p})$ did not have degree p over $K(u)$, the quantity x would have the form w^p with w in $K(u)$. Apply (2) with $k=0$ and obtain $x=w^p=\alpha_0^p+\alpha_1^pu^p+\cdots+\alpha_{m-1}^pu^{p(m-1)}$. The uniqueness of the expression (2) for $k=1$ implies that $\alpha_1=\cdots=\alpha_{m-1}=0$, $x=\alpha_0^p$ is the quotient of two polynomials in x^p, which is clearly impossible. Hence $H(x^{1/p})$ has degree p over H, and an evident induction implies that if $y^{p^e}=x$ then $H(y)=F(y, u)$ has degree p^e over H.

We now let G_1 be algebraic of finite degree over K so that G_1 has a maximal separable sub-field H and degree $t=p^e$ over H. It is conceivably not a simple extension of H. Without loss of generality we assume that G_1 is contained in a field which also contains the quantity y and hence the field $H(y)=G$. Every z of G_1 has the property $z^t=w$ in H, and if w has the form (2)

for $q=t$ then each $\alpha_i=\beta_i{}^t$ with β_i in $K_0=F(y)$, $w=v^t$, where $v=\beta_0+\beta_1 u+\cdots+\beta_{m-1}u^{m-1}$ is in $K_0(u)=G$. Thus $z^t=v^t$, $z=v$ is in G, $G_1\leqq G$. Since G and G_1 have the same degree over H, we have $G_1=G$.

An immediate corollary of our proof may be stated as follows:*

THEOREM 2. *Let H be separable of finite degree over $K=F(x)$ and g in H, $y^t=x$ where $t=p^e$. Then $g=d^t$ for d in $F(y)=K(y)$ of degree t over K.*

3. *The Determination.* The fundamental result on p-algebras over fields of our simple type may be thus stated:

THEOREM 3. *Let D be a normal division algebra of degree p^e over a field G which is algebraic of finite† degree over a simple transcendental extension of a perfect field F of characteristic p. Then G is separable of finite degree over $F(x)$, x an indeterminate over F, and D is a cyclic algebra*

$$(Z, S, x) \text{ over } G. \tag{3}$$

The exponent‡ of D is its degree p^e so that conversely the cyclic algebra (3) *is a division algebra if and only if x is not the norm of any quantity of the cyclic sub-field of Z of degree p over G.*

The now standard notation (3) in our case means that Z is a cyclic field of degree $p^e=t$ over G with generating automorphism

$$S: \qquad z \longleftrightarrow z^S, \qquad (z, z^S \text{ in } Z),$$

and that every quantity of D has the form

$$z_0 + z_1 y + \cdots + z_{t-1}y^{t-1}, \qquad (z_i \text{ in } Z).$$

* F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Characteristik p*, Mathematische Zeitschrift, vol. 33 (1931), pp. 1–32, p. 8, showed that every algebraic field of finite degree over a simple transcendental extension of a finite field F is separable over $F(x)$, for some indeterminate x. This inexplicit form of our Theorems 1, 2 is of course insufficient for our proof of Theorem 3.

† The results of Theorem 3 are also true for the case when G is algebraic but not of finite degree over K. For the method which leads to the reduction to the case of finite degree see the author's paper in this Bulletin, vol. 39 (1933), pp. 746–749.

‡ The result that the exponent and degree are equal was proved for *arbitrary degree n* by E. Witt, Mathematische Annalen, vol. 110 (1934), pp. 12–28. However his proof requires the same formidable machinery used for the analogous result on algebras over algebraic number fields, whereas the proof we give here is almost trivial.

Moreover $y^r z = z^{s^r} y^r$ for every z of Z, $y^t = x$. Thus (3) states that all cyclic algebras of degree $t = p^e$ over G have $G(y)$ as a common splitting field (equivalent to a maximal sub-field of all such algebras).

For proof we notice that the result concerning G is clearly part of Theorem 1. Let $A = (Y, T, g)$ be any cyclic algebra of degree $s = p^f \leqq p^e$ over G. By Theorem 2 we have $g = d^s$ with d in $L = G(x^{1/s})$, $A_L = (Y_L, T, 1)$ is a total matric algebra over L. Thus L is a splitting field* of every cyclic algebra of degree p^f. It is known* that D has exponent $p^f \leqq p^e$ over G and also that† then D is similar to a direct product of cyclic algebras A_i of degree p^f. But L splits each A_i and hence the algebra D. Since* the degree of every splitting field of D is divisible by the degree p^e of D it follows that $p^e \leqq p^f$, $t = p^e = p^f$. Thus D has exponent p^e and $L = G(x^{1/t})$ as a splitting field. But then it is known‡ that D has the form (3). The final statement in the theorem is a known§ consequence of the result that D of (3) is a division algebra if and only if its exponent is its degree.

UNIVERSITY OF CHICAGO

* These results are due to R. Brauer, E. Noether, and the author and are now well known. Their proofs with references may be found in the Ergebnisse tract of M. Deuring on *Algebren*.

† This is Theorem 18 of the author's paper in the Transactions of this Society, vol. 40 (1936), pp. 112–126.

‡ Loc. cit. See the proof of Theorem 12.

§ Cf. American Journal of Mathematics, vol. 54 (1932), pp. 1–13 for proof.