PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 62, Number 2, February 1977

SPLITTINGS OF CYCLIC p-ALGEBRAS

DAVID J. SALTMAN[1]

ABSTRACT. In this note we investigate the finite p-groups appearing as Galois groups of maximal subfields of cyclic p-algebras and show that for a fixed cyclic p-algebra, all possible such groups appear.

In the following, a central simple algebra over a field of characteristic $p \neq 0$, and of degree a power of p, is called a p-algebra. A central simple algebra is called cyclic if it contains a maximal subfield which is a finite cyclic Galois extension of the center. We will assume that the reader is familiar with the theory of central simple algebras and the Brauer group.

If G is a finite group, and K is a field, we say G appears over K if there is a Galois extension L of K with Galois group $G(L/K) = G$. If, in addition, A is a finite dimensional central simple algebra over K, we say G appears over K in A if such an L can be found which is also a maximal subfield of A. The purpose of this note is to prove the following theorem. In this theorem, as in the rest of the note, K will always be a field of characteristic p.

THEOREM 1. *If A is a cyclic p-algebra of degree p^e over K and G is a group of order p^e appearing over K, then G appears in A.*

It is illuminating to take note of a result of Witt's at this point [5]. If K is a field of characteristic p and $\mathcal{P}$: $K \to K$ is the additive endomorphism $\mathcal{P}(k) = k^p - k$, then $K/\mathcal{P}(K)$ can be considered as a vector space over the field $F(p)$ of p elements. Let N_K be $\dim_{F(p)} K/\mathcal{P}(K)$ if this is finite and $N_K = \infty$ if not. Then Witt showed that a finite p-group G appears over K if and only if G is generated by $\leqslant N_K$ elements. We will make use later of the details of Witt's proof. Since we will show that the case N_K finite is trivial, the main substance of what we will prove is the following theorem.

THEOREM 1′. *If K is a field of characteristic p, N_K is infinite, and A is a cyclic p-algebra over K of degree p^e, then any group of order p^e appears over K in A.*

The degree p cyclic p-algebras are crucial to our proof. Let us recall some familiar facts about them. Any cyclic extension of K of degree p is of the form $K(\alpha)$ where $\mathcal{P}(\alpha) \in K$ but $\mathcal{P}(\alpha) \notin \mathcal{P}(K)$ and any such extension is cyclic of

Received by the editors March 16, 1976.
AMS (MOS) subject classifications (1970). Primary 16A40, 13A20; Secondary 12F10, 12F15.
Key words and phrases. Cyclic algebra, p-algebra, Galois group, Brauer group, characteristic p.
[1] The author was partially supported under N.S.F. Research Grant MPS72-04643.

degree p. If $a = \alpha^p - \alpha$ and $L = K(\alpha)$ is cyclic of degree p over K, then it can be shown that any p-algebra with maximal subfield L is of the form $K\{x,y\}/(x^p - x - a, y^p - b, xy - yx - y)$ where $K\{x,y\}$ is the noncommutative polynomial ring in x and y, $b \neq 0$ is in K. Call this algebra $[a,b)$ and call the images of x and y in $[a,b)$, α and β respectively. For any a and $b \neq 0$ in K, $[a,b)$ is a cyclic p-algebra over K. If $a \notin \mathcal{P}(K)$, then $K(\alpha)$, the subalgebra generated by α, is a cyclic field extension of K of degree p. If $b \notin K^p$, $K(\beta)$ is a simple purely inseparable extension of K. In either case, the field mentioned is a maximal subfield of $[a,b)$. On the other hand, if A is a p-algebra over K with maximal subfield $K(b^{1/p})$ then $A \cong [a,b)$ for some $a \in K$. Finally, if $a \in \mathcal{P}(K)$ or $b \in K^p$, $[a,b)$ is a trivial p-algebra, that is, a matrix algebra over K.

An elementary abelian p-group is a finite group of the form $C_p \oplus C_p \oplus \cdots \oplus C_p$, where C_p is the cyclic group of order p. If L/K is a Galois extension with Galois group an elementary abelian p-group, then $L = L_1 \otimes L_2 \otimes \cdots \otimes L_k$ where L_i/K is cyclic of degree p and so $L_i = K(\alpha_i)$ with $\mathcal{P}(\alpha_i) \in K$, $\notin \mathcal{P}(K)$. The images of the $\mathcal{P}(\alpha_i)$ in $K/\mathcal{P}(K)$ must be linearly independent over $F(p)$. Conversely, if $a_1, a_2, \ldots, a_k \in K$ are linearly independent in $K/\mathcal{P}(K)$, then there is a unique $L = K(\alpha_1, \alpha_2, \ldots, \alpha_k)$, Galois over K with group $C_p \oplus \cdots \oplus C_p$ (k times), such that $\mathcal{P}(\alpha_i) = a_i$ and $L = K(\alpha_1) \otimes \cdots \otimes K(\alpha_k)$. The facts stated above are well known and can be found, for example, in [3].

The main technique used in this note is the manipulation of the algebras $[a,b)$. The first lemma, of this form, is the following.

LEMMA 2. *If $K(\beta) \subseteq [a,b)$ is the K subalgebra generated by β, and $c = k_0 + k_1\beta + \cdots + k_{p-1}\beta^{p-1}$ is in $K(\beta)$, then $[a,b) \cong [a + \delta(c), b)$ where $\delta(c) = k_0^p - k_0 + k_1^p b + \cdots + k_{p-1}^p b^{p-1}$.*

PROOF. $[a,b)$ is generated by $\alpha + c$ and β, which satisfy the relations $\beta^p = b$ and $(\alpha + c)\beta - \beta(\alpha + c) = \beta$. We need only calculate $\mathcal{P}(\alpha + c)$ and show it equal to $\mathcal{P}(\alpha) + \delta(c)$.

Suppose z has the property $[z,\beta] = \beta$. Then $[z,\beta^i] = i\beta^i$. Using [2, p. 187], we see that

$$(z + k\beta^i)^p = z^p + (k\beta^i)^p + d_z^{p-1}(k\beta^i) = z^p + k^p b^i + (i)^{p-1}k\beta^i,$$

where d_z is the inner derivation determined by z. Thus if $1 \leqslant i < p$,

$$\mathcal{P}(z + k\beta^i) = (z + k\beta^i)^p - (z + k\beta^i) = \mathcal{P}(z) + k^p b^i.$$

We compute $\mathcal{P}(\alpha + c)$ by induction. If $c = k_0$, clearly

$$\mathcal{P}(\alpha + k_0) = \mathcal{P}(\alpha) + \mathcal{P}(k_0) = \mathcal{P}(\alpha) + \delta(k_0).$$

If $1 \leqslant i < p$ and $c = k_0 + k_1 + \cdots + k_i\beta^i$, set $z = \alpha + k_0 + \cdots + k_{i-1}\beta^{i-1}$. Then by above,

$$\mathcal{P}(\alpha + c) = \mathcal{P}(z + k_i\beta^i) = \mathcal{P}(z) + k_i^p b^i.$$

By induction, $\mathcal{P}(z) = \mathcal{P}(\alpha) + \delta(k_0 + k_1\beta + \cdots + k_{i-1}\beta^{i-1})$, and this does it. Q.E.D.

We can now deal with the case N_K is finite, as well as the case K is perfect. It is clear that a trivial p-algebra of degree p^e, i.e. a matrix algebra over K, contains as a maximal subfield *any* field extension of K of degree p^e. If K is perfect it is well known that all p-algebras are trivial and so Theorem 1 is obvious. Similarly, the next theorem will finish the case N_K is finite.

THEOREM 3. *If N_K is finite, then any p-algebra over K will be trivial.*

PROOF. It will suffice to show that the p-primary part of the Brauer group is zero. To show this, we need only show that any element of the Brauer group of exponent p is trivial. By [1, pp. 108–109], any such element is similar to a product of algebras $[a_i, b_i)$. Thus it will suffice to show that such an algebra is trivial.

Suppose $c_1, c_2, \ldots, c_n \in K$ are representatives of a basis for $K/\mathcal{P}(K)$ over $F(p)$. We can assume $c_i = d_i^p$, $d_i \in K$, since modulo $\mathcal{P}(K)$, c_i and c_i^p are the same. We can clearly assume K is not perfect and therefore infinite. We must show any algebra $[a, b)$ is trivial and we can assume $b \notin K^p$. Call $K' = K(b^{1/p}) = K(\beta) \subseteq [a, b)$. If $f \in K$, then $fc_i = \sum_j h_{ij}c_j + z$ where $z \in \mathcal{P}(K)$ and $h_{ij} \in F(p)$. Consider the mapping sending f to the $n \times n$ matrix $(h_{ij}) \in M_n(F(p))$. The quotient space $(K')^p/K^p$ is a vector space over $F(p)$ and so has some basis $\{\bar{b}_i\}_{i\in I}$. Choose representatives b_i in $(K')^p$ of the $\bar{b}_i$. Since K is infinite, K^p is infinite and so K^p is infinite dimensional as a vector space over $F(p)$. But $(K')^p/K^p$ is a nonzero vector space over K^p, and so it must be infinite dimensional over $F(p)$. That is, I is infinite. Since $M_p(F(p))$ is finite, there are two representatives b_i and b_j with the same associated matrix in $M_n(F(p))$. Then $b' = b_i - b_j$ has the properties $b'c_i \in \mathcal{P}(K)$ for all i and $b' \notin K^p$. Hence $b^* = 1 + b'$ has the properties $b^*c_i - c_i \in \mathcal{P}(K)$ for all i and $b^* \notin K^p$. Since $b^* \in K'^p$, $K' = K(b^{*1/p})$, and $[a, b) = [a^*, b^*)$ for some $a^* \in K$. $a^* = h_1c_1 + h_2c_2 + \cdots + h_nc_n + z$ for some h_i in $F(p)$ and z in $\mathcal{P}(K)$, so if we call $\beta' = b^{*1/p}$, $(h_id_i\beta')^p - h_ic_i \in \mathcal{P}(K)$. Thus by Lemma 2, if $c = h_1d_1\beta' + h_2d_2\beta' + \cdots + h_nd_n\beta'$, $[a^*, b^*) \cong [a^* + \delta(-c), b^*) = [z, b^*)$ where $z \in \mathcal{P}(K)$. But this last algebra is trivial. Q.E.D.

This next lemma is the central fact of this note. The idea of this lemma is to change b and then get "a" to be a desired value.

LEMMA 4. *Suppose $A = [a, b)$ is a cyclic p-algebra over K and $K' \subseteq K$ is a subfield of K such that $b \in K'$ and K/K' is finite. Let $a' \in K$ be arbitrary. Suppose q is a power of p strictly greater than the degree of K over K'. If $c \in K$ is such that $K'(c) = K'(c^q) = K$, $c \in K^q$ and $c^q = \sum k_ic^i$ where $k_i \in K'^q$, then $A \cong [a'', b + c)$ where $a'' - a' \in K'$.*

PROOF. As usual, we can assume b is not a pth power in K. Let d be the pth root of c. Then if $\beta^p = b$, $K(\beta) = K(\beta + d)$ and so $A = [a_1, b + c)$ for some

$a_1 \in K$. Use $\beta + d$ to define the δ operator as in Lemma 2. Define $x \equiv y$ to mean that $x - y$ is in $\delta(K(\beta + d))$. By Lemma 2, it suffices to show that $a_1 \equiv a' + k'$, $k' \in K'$. For this we need a sublemma.

SUBLEMMA 5. *Suppose* $K'' = K((b + c)^{1/p})$ *and* $(b + c)^{1/p}$ *is used to define the operator of Lemma* 2. *Then if* q *is a power of* p *greater than* n, *and* $c, m \in K^q$, $mc^n \equiv (-1)^n mb^n$.

PROOF. We will perform this proof by induction. Call $\beta = b^{1/p}$ and $d = c^{1/p} \in K$. Then $\delta((\beta + d)m^{1/p}) = (b + c)m$, so $mc \equiv (-1)mb$. Assume the result for all $j < n$. If $n < p$, then considering $\delta(m^{1/p}(\beta + d)^n)$, we get that

$$m \sum_{i=0}^{n} b^i c^{n-i} \binom{n}{i} \equiv 0. \tag{1}$$

By induction, $(-1)^{n-i} mc^{n-i} c^i \equiv mc^{n-i} b^i$. Thus we have that

$$m \sum_{i=0}^{n-1} b^i c^{n-i} \binom{n}{i} \equiv mc^n \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \right). \tag{2}$$

But $(\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} = (1 - 1)^n = 0$ so $\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} = -(-1)^n$. Combining equations (1) and (2) gives our result for $n < p$. Now if $n \geqslant p$ then $n = rp + i$ for $r \geqslant 1$ and $0 \leqslant i < p$ so $mc^n = mc^{rp} c^i$. For any x, $x^p \equiv x$, so

$$\begin{aligned} mc^{rp} c^i &\equiv m^{1/p} c^r d^i \equiv (-1)^r m^{1/p} b^r d^i \quad \text{(by induction)} \\ &\equiv (-1)^{rp} mb^{rp} c^i \equiv (-1)^{rp} mb^{rp} b^i (-1)^i \quad \text{(by the } n < p \text{ case).} \end{aligned}$$

Q.E.D.

We will now finish the proof of Lemma 4. Since $a_1 - a'$ is in K, $a_1 - a' = k_0 + k_1 c + \cdots + k_{n-1} c^{n-1}$ where n is the degree of K over K'. It is now easy to see that $(a_1 - a')^q = m_0 + m_1 c + \cdots + m_{n-1} c^{n-1}$ where all the m_i are in $(K')^q$. Thus

$$\begin{aligned} a_1 - a' &\equiv (a_1 - a')^q \\ &\equiv \text{(by the sublemma)} \quad m_0 + (-1)m_1 b + (-1)^2 m_2 b^2 \\ &\quad + \cdots + (-1)^{n-1} m_{n-1} b^{n-1} \end{aligned}$$

and this last expression is in K'. Q.E.D.

Our reason for proving Lemma 4 was to prove the following result.

LEMMA 6. *Suppose* $[a, b)$ *is a cyclic* p*-algebra of degree* p *over* K *and* $K' \subseteq K$ *is a subfield such that* K/K' *is finite and* $b \in K'$. *If* a' *is in* K *and separable over* K', *then there are* a'' *and* b' *in* K *such that* $[a, b) \cong [a'', b')$ *and* $a' - a'' \in K'$.

PROOF. Call L the separable closure of K' in K. Since $[a, b) \cong [a + a^p - a, b) = [a^p, b)$, we can assume $a \in L$. Thus $[a, b)$ is defined over L and we can assume $L = K$, that is, that K/K' is separable. Choose a $c \in K$ such that $K'(c) = K$. Choose p^e strictly greater than the degree of K over K'. By

separability, $K = K'(c^{p^e})$, so $c^{p^e} = \sum k_i c^i$, $k_i \in K'$. Thus using c^{p^e} we can apply Lemma 4. Q.E.D.

We will prove the main result, Theorem 1′, in two steps. The first step is embodied in the next result. As a preliminary, we must mention a theorem of Albert's [1, p. 107]. A p-algebra A, of degree p^n over its center K, is cyclic if and only if it is split by a simple purely inseparable extension K' of degree p^f, $f \leqslant n$. If K is not perfect, we can assume $f = n$. Thus, over a nonperfect field, a p-algebra is cyclic if and only if it has a simple purely inseparable maximal subfield.

PROPOSITION 7. *Let K be a field of characteristic p with N_K infinite, and A a cyclic p-algebra of degree p^e over K. Then the elementary abelian p-group of order p^e appears over K in A.*

PROOF. As usual, we may assume K is not perfect. Thus A contains a maximal subfield $L = K(\beta)$ such that $\beta^{p^e} \in K$ but $\beta^{p^{e-1}} \notin K$. We now proceed by induction on e. If $e = 1$, the result is trivial. Assume it for $e - 1$. Call $L' = K(\beta^{p^{e-1}})$ and $A' = A^{L'}$, the centralizer of L' in A. Then A' is central simple over L' of degree p^{e-1} with maximal subfield L, and thus A' is also cyclic. The p-power map induces an isomorphism from $L'/\mathcal{P}(L')$ to $K/\mathcal{P}(K)$, and so $N_{L'} = N_K$. By induction, A' contains a maximal subfield M' Galois over L' with Galois group the elementary p-group of order p^{e-1}. Since L'/K is purely inseparable, $M' = M \otimes L'$ where M/K is Galois with the same Galois group as M'/L'. Thus we can write $M = K(\alpha_1, \alpha_2, \ldots, \alpha_{e-1})$ where $\mathcal{P}(\alpha_i) = a_i \in K$ and the a_i's are linearly independent in $K/\mathcal{P}(K)$. M is a subfield of A of degree p^{e-1} and so $A^* = A^M$ is a p-algebra of degree p. Since L' commutes with M, $L' \subseteq A^*$. Thus for some $a \in M$, $A^* \cong [a, b)$ where $b = \beta^{p^e} \in K$. By Lemma 6, choosing $a' = 0$, $A^* = [a^*, b^*)$ where $a^* \in K$. Call $M^* = M(\alpha^*)$, where $\alpha^* \in A^*$ and $\mathcal{P}(\alpha^*) = a^*$. If a^* is linearly independent of the a_i's in $K/\mathcal{P}(K)$, then M^* is Galois over K with the required group. If not, then $a^* \in \mathcal{P}(M)$ and so A^* is trivial. Thus A^* contains any extension of degree p and the result is easy using the fact that N_K is infinite. Q.E.D.

We are now ready to deal with the case of arbitrary p-groups. If G is a finite p-group, define G^* to be the subgroup generated by the commutator subgroup G' of G and the set $G^p = \{g^p | g \in G\}$. Then G/G^* is an elementary abelian p-group and by Burnside's basis theorem (e.g. [4, p. 161]), the minimal number of generators of G and G/G^* are the same. The essence of the result of Witt's mentioned at the beginning was a proof of his that G appears over K if and only if G/G^* does. We will review his proof and show that it can be performed inside a fixed cyclic p-algebra.

Call $Z = Z(G)$ the center of G. We assume $G^* \neq (e)$. Then $Z \cap G^* \neq (e)$ (e.g. [4, p. 139]). Choose $g \in Z \cap G^*$ of order p and call H the subgroup generated by g. We have the extension $0 \to H \to G \to G/H \to 0$. Choose representatives u_σ for each $\sigma \in G/H$. As usual, define the group cohomology

2-cocycle $g_{\sigma,\tau}$ by the relation $u_\sigma u_\tau = g_{\sigma,\tau} u_{\sigma\tau}$. Being a 2-cocycle, $g_{\sigma,\tau} g_{\rho,\sigma\tau} = g_{\rho,\sigma} g_{\rho\sigma,\tau}$. Since H is central in G, $u_\sigma g' = g' u_\sigma$ for all $g' \in H$. These conditions completely determine G given H and G/H.

Suppose we have an extension L/K with Galois group G/H. Define $\chi \in \mathrm{Hom}(H, F(p))$ by $\chi(g) = 1$. Then $\chi(g_{\sigma,\tau}) + \chi(g_{\rho,\sigma\tau}) = \chi(g_{\rho,\sigma}) + \chi(g_{\rho\sigma,\tau})$. Thus $\chi(g_{\sigma,\tau})$ is a 2-cocycle of G/H into L^+. Since $H^2(G/H, L^+) = 0$, there is a $d\colon G/H \to L^+$ such that $\chi(g_{\sigma,\tau}) = d_\sigma + \sigma d_\tau - d_{\sigma\tau}$. Since $\chi(g_{\sigma,\tau}) \in F(p)$, we have that $\mathcal{P}(d_\sigma) + \sigma\mathcal{P}(d_\tau) - \mathcal{P}(d_{\sigma\tau}) = 0$. That is, $\mathcal{P}(d_\sigma)$ is a 1-cocycle. But $H^1(G/H, L^+) = 0$, so there is a $\gamma \in L$ such that $\mathcal{P}(d_\sigma) = (\sigma - 1)\gamma$. Define $L' = L(\alpha)$, where $\mathcal{P}(\alpha) = \gamma$. It is shown in [5] that L'/K is a Galois field extension with Galois group G. Note that if γ is changed to $\gamma + k$, with $k \in K$, the result still holds.

We are finally ready to prove Theorem 1′. Suppose A is a cyclic p-algebra of degree p^e over a field K with $N_K = \infty$, and G is a group of order p^e. We proceed by induction on e. As usual, we can assume K is not perfect. Define G^*, H, u_σ, and $g_{\sigma,\tau}$ as above. By Proposition 7 we can assume $G^* \neq (e)$. Suppose $L = K(\beta)$ is a simple purely inseparable maximal subfield of A of degree p^e and, as before, define $L' = K(\beta^{p^{e-1}})$ and $A' = A^{L'}$. Then A' is cyclic of degree p^{e-1} over L' and by induction contains a maximal subfield M' Galois over L' with Galois group G/H. As before, $M' = M \otimes L'$ where M/K is Galois with group G/H. Using M we can define χ, d_σ, and $\gamma \in M$ as above. Call $A^* = A^M$, so $A^* \cong [a, b)$ with $b \in K$. By Lemma 6, $A^* \cong [a^*, b^*)$ with $a^* - \gamma \in K$. If $\alpha^* \in A^*$ is such that $\mathcal{P}(\alpha^*) = A^*$, then $M(\alpha^*)$ is Galois over K with group G. This completes the theorem and the note.

Bibliography

1. Adrian Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R.I., 1961. MR **23** #A912.

2. Nathan Jacobson, *Lie algebras*, Interscience, New York, 1962. MR **26** #1345.

3. Paul J. McCarthy, *Algebraic extensions of fields*, Blaisdell, Waltham, Mass., 1966. MR **33** #5612.

4. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N.J., 1964. MR **29** #4785.

5. E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebner Gruppe de Ordnung p^f*, J. für Math. **174** (1936), 237–245.

Department of Mathematics, University of Chicago, Chicago, Illinois 60637