PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 3, November 1988

METACYCLIC p-ALGEBRAS

MING-CHANG KANG

(Communicated by Donald Passman)

ABSTRACT. Let K be a field of char $K = p > 0$, m, r any positive integers with $(p, m) = 1$, and L a metacyclic extension of K with degree $p^r m$, i.e. $\mathrm{Gal}(L/K) = \langle \sigma, \tau : \sigma^{p^r} = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^e \rangle$ for some integer e. If A is a central simple K-algebra of degree p^r and is split by L, then A is a cyclic algebra. For $r = 1$, the theorem has been proved by A. A. Albert [1].

1. Introduction.

In [1], A. A. Albert proves the following theorem,

THEOREM. *Let K be any field of* char $K = p > 0$, *m any positive integer which is relatively prime to p, and L a metacyclic extension of K with degree pm, i.e.* $\mathrm{Gal}(L/K) = \langle \sigma, \tau : \sigma^p = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^e \rangle$ *for some integer e. If A is a central simple K-algebra of degree p and is split by L, then A is a cyclic algebra.*

The aim of this note is to generalize the above theorem to the case of p-algebras of degree p^r. Namely,

THEOREM. *Let K be any field of* char $K = p > 0$, *m, r any positive integer with $(p, m) = 1$, and L a metacyclic extension of K with degree $p^r m$, i.e.* $\mathrm{Gal}(L/K) = \langle \sigma, \tau : \sigma^{p^r} = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^e \rangle$ *for some integer e. If A is a central simple K-algebra of degree p^r and is split by L, then A is a cyclic algebra.*

2. The proof of the theorem.

LEMMA. *Let K be any field, m, n any positive integers which are relatively prime, and L a metacyclic extension of K with degree mn, i.e.* $\mathrm{Gal}(L/K) = \langle \sigma, \tau : \sigma^n = \tau^m = 1, \tau\sigma\tau^{-1} = \sigma^e \rangle$ *for some integer e. If A is a central simple K-algebra of degree n which is split by L and $F = \{a \in L : \sigma(a) = a\}$, then $A \otimes_K F$ is isomorphic to the cyclic algebra $(b, L/F, \sigma)$ for some $b \in F^\times$ with $\tau(b) = \lambda^n b^e$ where λ is some element in $F^\times$.*

PROOF. Let C be a central simple K-algebra of degree mn which is similar to A. Then L is a maximal subfield of C. Let the centralizer of F in C be B. Then $B \cong A \otimes_K F$. The automorphism τ^i on L, $0 \leq i \leq m-1$, can be extended to an automorphism on C; again we call it τ^i. Then $\tau^i(B) = B$.

Now L is a maximal subfield of B. Hence $B = (b, L/F, \sigma)$ for some $b \in F^\times$ [2, p. 71]. Then $\tau(B) = (\tau(b), L/F, \sigma^e)$ and $\tau^i(B) = (\tau^i(b), L/F, \sigma^{e^i})$. Let us denote the similarity classes of B and $(b, L/F, \sigma)$ by $[B]$ and $[b, L/F, \sigma]$ respectively. Let f be an integer with $ef = 1 \pmod n$. Then, by [2, Lemma 3, p. 72],

Received by the editors January 12, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16A39, 12E15.
Key words and phrases. Central simple algebra, cyclic algebra.
Partially supported by the National Science Council, Republic of China.

0002-9939/88 $1.00 + $.25 per page

$[B] = [\tau^i(B)] = [\tau^i(b), L/F, \sigma^{e^i}] = [\tau^i(b^{f^i}), L/F, \sigma^{e^i f^i}] = [\tau^i(b^{f^i}), L/F, \sigma]$. Therefore $m[B] = \sum_{0 \le i \le m-1} [\tau^i(B)] = [c, L/F, \sigma]$ where $c = \prod_{0 \le i \le m-1} \tau^i(b^{f^i})$.

Now

$$\frac{\tau(c)}{c^e} = \frac{b^{f^{m-1}}}{b^e} \prod_{1 \le i \le m-1} \tau^i \left(\frac{b^{f^{i-1}}}{b^{ef^i}} \right) \in F^{\times n}$$

since $ef = 1 \pmod{n}$.

Choose integer m_0 with $mm_0 = 1 \pmod{n}$. Then $[B] = m_0[c, L/F, \sigma] = [c^{m_0}, L/F, \sigma]$. Clearly $\tau(c^{m_0}) = \lambda^n (c^{m_0})^e$ for some $\lambda \in F^\times$. This completes the proof of the Lemma.

Now the proof of the theorem.

Let $n = p^r$ in the above Lemma. We have $A \otimes_K F$ is isomorphic to $(b, L/F, \sigma)$ for some $b \in F^\times$ with $\tau(b) = \lambda^{p^r} b^e$ where $\lambda \in F^\times$.

Note that the cyclic algebra $(b, L/F, \sigma)$ has a maximal subfield $F(v)$ with $v^{p^r} = b$ and $[F(v): F] = p^r$. (If the polynomial $X^{p^r} - b \in F[X]$ is not irreducible, apply [**2**, Lemma 8, p. 75] to reduce the degree of $A \otimes_K F$ and rework the Lemma.)

CLAIM. $F(v)$ is a normal extension of K. Since F is a Galois extension of K, it suffices to show that all conjugates of v over K are contained in $F(v)$. Let $f(X)$ be the minimal polynomial of b over K. Then v is a root of $f(X^{p^r}) = 0$. Hence, if u is a conjugate of v over K, then u is also a root of $f(X^{p^r}) = 0$. It follows that u^{p^r} is some conjugate of b, i.e. $u^{p^r} = \tau^i(b)$ for some i. But $\tau^i(b) = \lambda_i^{p^r} b^{e^i}$ for some $\lambda_i \in F^\times$. Hence $u^{p^r} = \lambda_i^{p^r} (v^{e^i})^{p^r}$. It follows that $u = \lambda_i v^{e^i} \in F(v)$.

Since $F(v)$ is normal over K, it follows that $F(v) = F \otimes_K E$ where E is the maximal purely inseparable extension in $F(v)$. Clearly, the purely inseparable exponent of $F(v)$ over F and that of E over K are the same, which is just r. Hence $E = K(w)$ for some w with $w^{p^r} \in K$.

Consider $A \otimes_K K(w)$. Since $F(v)$ splits $A \otimes K(w)$ and $[F(v) : K(w)]$ is relatively prime to the degree of $A \otimes_K K(w)$. It follows that $[A \otimes_K K(w)] = 0$ in $Br(K(w))$. By [**2**, Theorem 2, p. 108], A is a cyclic algebra.

REFERENCES

1. A. A. Albert, *A note on normal division algebras of prime degree*, Bull. Amer. Math. Soc. **44** (1938), 649–652.
2. P. K. Draxl, *Skew fields*, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1983.

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI, TAIWAN REPUBLIC OF CHINA