ISRAEL JOURNAL OF MATHEMATICS, Vol. 28, Nos. 1-2, 1977

CYCLIC ALGEBRAS, COMPLETE FIELDS, AND CROSSED PRODUCTS

BY

LAWRENCE J. RISMAN

Dedicated to the memory of Richard Brauer

ABSTRACT

Let k be a field and n a positive integer. We construct a field extension K of k and a cyclic division algebra D of index n with center K.

THEOREM 1. *Let $q = \mathrm{char}(k)$. Let M be a subfield of D which is Galois over K of degree m with Galois group H.*

1) *If $q \mid m$ then H has a normal q-Sylow subgroup.*

2) *If $q \nmid m$ then H is an abelian group with one or two generators, an extension of a cyclic group by a cyclic group of order e where k contains a primitive e-th root of unity.*

Let $k(X)$ be the generic division ring over k of index n as defined by Amitsur.

THEOREM 2. *If n is divisible by the square of a prime $p \neq \mathrm{char}(k)$ and k does not contain a primitive p-th root of unity, then $k(X)$ is not a crossed product.*

1. Introduction

A division algebra is a division ring finite dimensional over its center. If D is a division algebra with center C, then the dimension $[D\colon C]$ is a square n^2. The integer n is called the index of D over C. A subfield M of D is maximal if and only if $[M\colon C] = n$. By a theorem of Noether and Jacobson, any division algebra D contains a maximal subfield which is separable over the center, and consequently D is equivalent in the Brauer group of C to a crossed product algebra. A division algebra D with center C is a crossed product if and only if D contains a maximal subfield which is Galois over C.

Our concern here is with maximal subfields of a division algebra, in particular with the problem of determining whether a division algebra is a crossed product. Any division algebra of index 2 is a crossed product. It was proven by

Received April 7, 1976 and in revised form February 4, 1977

Wedderburn, Albert, and Brauer that for $n = 2, 3, 4, 6$ or 12 any division algebra of index n is a crossed product [2, chap. 11, sections 5 and 6]. See [8] for a theorem in this connection for $n = 5$. By valuation theory, if C is a local field then any division algebra with center C is a crossed product and contains a maximal subfield cyclic over C. By the theorem of Brauer, Hasse, Noether, and Albert if C is a global field the same conclusion holds [2, chap. 9].

Much progress has been made recently. In *On central division algebras* Amitsur showed that there exist division algebras that are not crossed products [3]. For any field k and any integer n he defined $k(X)$, the generic division algebra of index n over k. The center of $k(X)$ is a function field over k. He proved that if k is the field of rational numbers and n is divisible by 8 or by p^2 for any odd prime p, then $k(X)$ is not a crossed product. Subsequently further results have been obtained by Schacher and Small [16], Amitsur [4], and Fein and Schacher [10], and Jacobson [11]. They have shown that $k(X)$ is not a crossed product in the following cases: 1) if n is divisible for p^3 for any prime $p \neq \mathrm{char}(k)$ for any field k, 2) if n is divisible by p^2 for any prime $p \neq \mathrm{char}(k)$ such that k does not contain a primitive p-th root of unity provided that k is a global field or a finite field.

Unlike the p^3 theorems, the proofs of the p^2 theorems cited above depend on properties of global and local fields. The extension of these results to the case n divisible by $\mathrm{char}(k)$ in [10] depends on the classification of division algebras over global fields given by the theorem of Brauer, Hasse, Noether, and Albert. Theorem 2 below extends the above results, removing restrictions on the field k in case 2, and simplifying the proof in previously known cases. Its proof does not depend on global fields. It depends on results of Amitsur and on Theorem 1 below. The proof of Theorem 1 depends on the theory of extension fields of a field complete in a discrete valuation. Theorem 1 yields Theorem 2 without the necessity of reducing to global fields in case q divides m and without appeal to global fields or the Dirichlet density theorem for the p^2 case.

2. Statement of theorems

Let k be a field and n be a positive integer. We construct a field extension K of k and a cyclic algebra D over K as follows. Let L_0 be the field of rational functions over k in n indeterminates $x_1, \cdots, x_n$. Let σ_0 be the automorphism of L_0 which leaves k fixed and permutes the x_i cyclically ($x_i \to x_{i+1}$, $x_n \to x_1$). Let K_0 be the subfield of L_0 fixed by σ_0. Note that L_0 is a Galois extension of K_0 with cyclic Galois group of order n generated by σ_0.

Let $K = K_0((t))$ be the field of formal Laurent series in one variable over K_0. Let $L = L_0((t))$, and let σ be the automorphism of L which leaves t fixed and whose restriction to L_0 is σ_0. Then L is a Galois extension of K with cyclic Galois group $G = \mathrm{Gal}(L/K)$ of order n generated by σ. Let D be the cyclic algebra over K, $D = (L, \sigma, t)$. Let q be the characteristic of k.

We show below that D is a division algebra of index and order n in the Brauer group of k.

THEOREM 1. *Let M be a subfield of D which is Galois over K of degree $m = [M:K]$ with Galois group $H = \mathrm{Gal}(M/K)$.*

1) *If q divides m then H has a normal q-Sylow subgroup.*

2) *If q does not divide m then H is an abelian group with one or two generators. In particular, H is an abelian extension of a quotient group of G by a cyclic group of order e where k contains a primitive e-th root of unity.*

The proof of this theorem turns on the facts that L is the unique unramified maximal subfield of D and that every root of unity in L lies in k.

COROLLARY 1. *If n is prime to q, p is a prime dividing n, and the field k does not contain a primitive p-th root of unity, then every subfield of D which is Galois over K has an abelian Galois group with cyclic p-Sylow subgroup.*

Let $k(X)$ be the generic division ring over k of index n, as defined by Amitsur [4]. Note that n may be divisible by $q = \mathrm{char}(k)$.

THEOREM 2. 1) *If n is divisible by p^3 for any prime $p \neq \mathrm{char}(k)$, then $k(X)$ is not a crossed product.*

2) *If n is divisible by p^2 for any prime $p \neq \mathrm{char}(k)$ such that k does not contain a primitive p-th root of unity, then $k(X)$ is not a crossed product.*

3. Complete fields

We investigate fields complete in a discrete valuation with a view towards proving Theorem 1. For an exposition of the relevant definitions and theory we refer to [20, chap. 3] or [6, chap. 4]. Some of the results of this section are generalizations of results which are well known for complete fields with finite residue class field. See [1] and the references contained therein. These results are proven here for a complete field with arbitrary residue class field. This fact, together with Proposition 4 below, makes possible the proof of Theorem 1.

Let F be a field complete in a discrete valuation v. Let 0 be the ring of integers of F, $0 = \{x \in F \mid v(x) \geqq 0\}$. Let t be a uniformizing parameter of v, an element of

F such that $v(t) = 1$. Let P be the prime divisor of F, $P = \{x \mid v(x) > 0\}$, the ideal of 0 generated by t. The residue class field $\bar{F} = 0/P$. Let q be the characteristic of $\bar{F}$. An extension field E of f is unramified if the degree $[E = F] = [\bar{E} : \bar{F}]$ and $\bar{E}$ is separable over $\bar{F}$. An extension field E of F is tamely ramified if q does not divide the ramification index of E over F and $\bar{E}$ is separable over $\bar{F}$. We require the following characterization of extension fields of F. Note that a Galois extension field is normal and separable.

Lemma 1. *Let E be a Galois extension of F. Let T, the inertia field, be the maximal unramified subextension of F. Let V, the ramification field, be the maximal tamely ramified subextension of E.*

1) *T is Galois over F, $\bar{E}$ is normal over $\bar{F}$, and the Galois groups* $\mathrm{Gal}(T/F)$, $\mathrm{Gal}(\bar{T}/\bar{F})$, *and* $\mathrm{Gal}(\bar{E}/\bar{F})$ *are isomorphic.*

2) *V is Galois over F.*

3) *V is a cyclic extension of T of degree e with q not dividing e, $V = T(\sqrt[e]{s})$ where $s \in T$ with $v(s) = 1$, T contains a primitive e-th root of unity, and $\bar{T}$ contains a primitive e-th root of unity.*

4) *The degree of E over V is a power of q.*

Proof. Assertion 1 is [20, theor. 3–5–3]. Note that $\bar{T}$ is the maximal subfield of $\bar{E}$ separable over $\bar{F}$, so that if $\bar{E}$ is separable over $\bar{F}$ then $\bar{E} = \bar{T}$. Assertion 2 follows from [20, props. 3–6–1 and 3–6–8]. That V is cyclic over T of degree e not divisible by q is [20, prop. 3–6–4]. That $V = T(\sqrt[e]{s})$ with $s \in T$ and $v(s) = 1$ follows from [20, props. 3–4–3 and 3–4–7]. The ratio of any two roots of $x^e - s$ is an e-th root of unity, and this polynomial has e distinct roots in V. Hence V contains a primitive e-th root of unity, $z = \sqrt[e]{1}$. Since q does not divide e, the polynomial $x^e - 1$ is separable over $\bar{F}$. Hence $\bar{E}$ contains a primitive e-th root of unity and z lies in T by [20, theor. 3–2–6], proving assertion 3. Assertion 4 follows from [20, prop. 3–4–7]. Q.E.D.

Remark. The above lemma is valid if E is merely assumed normal over F. In general a field extension obtained by adjoining an e-th root may be cyclic of degree e even if the ground field does not contain a primitive e-th root of unity.

If $1 \to C \to G \to H \to 1$ is an exact sequence of groups, we say that G is an extension of H by C. This terminology is motivated by Galois theory. It is not the only standard terminology.

Corollary 1. *Suppose E is a tamely ramified extension of F with ramification index e over F and residue class field $\bar{E}$.*

1) *If $\bar{E}$ does not contain a primitive e-th root of unity, then E is not normal over F.*

2) *If E is normal over F, then* $\mathrm{Gal}(E/F)$ *is an extension of* $\mathrm{Gal}(\bar{E}/\bar{F})$ *by a cyclic group of order e.*

PROOF. Assertion 1 is immediate from Part 3 of Lemma 1. Suppose E is normal over F. Let T be the inertia field of E. Let $C = \mathrm{Gal}(E/T)$. By Part 3 of Lemma 1, C is a cyclic group of order e. By Part 1 of the lemma, T is Galois over F and $\mathrm{Gal}(T/F)$ is isomorphic to $\mathrm{Gal}(\bar{E}/\bar{F})$. By Galois theory we have an exact sequence of groups $1 \to C \to \mathrm{Gal}(E/F) \to \mathrm{Gal}(T/F) \to 1$, and assertion 2 is proven. Q.E.D.

COROLLARY 2. *Suppose E is a tamely ramified extension Galois over F. Let T be the inertia field of E. Let p be a prime dividing* $[E:F]$. *Suppose a p-Sylow subgroup of $H =$* $\mathrm{Gal}(T/F)$ *is cyclic, and T does not contain a primitive p-th root of unity. Then any p-Sylow subgroup of $G =$* $\mathrm{Gal}(E/F)$ *is cyclic.*

PROOF. G is an extension of H by a group of order e and T contains a primitive e-th root of unity. Hence e is prime to p. An appropriately chosen pre-image of a generator of a cyclic p-Sylow subgroup of H generates a cyclic p-Sylow subgroup of G. As all p-Sylow subgroups of G are conjugate, the proof is complete. Q.E.D.

PROPOSITION 1. *Let E be a tamely ramified extension Galois over F with ramification index e. Let $G =$* $\mathrm{Gal}(E/F)$. *Let T be the inertia field of E,* $C = \mathrm{Gal}(E/T)$, *and* $H = \mathrm{Gal}(T/F)$.

1) *G is a central extension of H by C if and only if F contains a primitive e-th root of unity.*

2) *If H is cyclic, then G is an abelian group (with one or two generators) if and only if F contains a primitive e-th root of unity.*

PROOF. By Corollary 1 to Lemma 1, G is an extension of H by C. It remains to show that C is a central subgroup of G if and only if F contains a primitive e-th root of unity. Let s be a prime element of T with $E = T(\sqrt[e]{s})$ and let $r = \sqrt[e]{s}$ in E. T contains a primitive e-th root of unity by Part 3 of Lemma 1. Let σ be an automorphism in $H = \mathrm{Gal}(T/F)$. Since E is normal over F, $T(\sqrt[e]{s^\sigma}) = E$. Hence by Kummer theory $s^\sigma = s^i u_\sigma$ with u_σ an e-th power in T and $0 < i < e$. Since the extension of v from F to T is unique, $v(s^\sigma) = v(s) = 1$. As $v(u_\sigma)$ is divisible by e and $v(s^i) = i$, it follows that $i = 1$ and $v(u_\sigma) = 0$. Hence $s^\sigma/s = u_\sigma$ with u_σ an e-th power in the units of T. Let γ be a pre-image of σ in G, an extension of σ to

E. Then $(r^\gamma/r)^e = s^\sigma/s = u_\sigma$ so that $r^\gamma = ra_\gamma$ with $a_\gamma \in T$ and $a_\gamma^e = u_\sigma$. Let $\tau \in C = \mathrm{Gal}(E/T)$. It suffices to show that $\gamma\tau = \tau\gamma$ for all choices of γ and τ if and only if F contains a primitive e-th root of unity. Since γ maps T into T and τ fixes T elementwise, the restrictions of γ and τ to T clearly commute. As E is generated over T by r it suffices to check if $r^{\gamma\tau} = r^{\tau\gamma}$. Note that $r^\tau = rz$ with $z^e = 1$.

We compute $r^{\gamma\tau} = (ra_\gamma)^\tau = r^\tau a_\gamma^\tau = rza_\gamma^\tau$. Since $a_\gamma \in T$, $a_\gamma^\tau = a_\gamma$. Hence $r^{\gamma\tau} = rza_\gamma$. Now we compute $r^{\tau\gamma} = (rz)^\gamma = r^\gamma z^\gamma = ra_\gamma z^\gamma = ra_\gamma z^\sigma$. If F contains a primitive e-th root of unity, $z \in F$ and $z^\sigma = z$. Hence $r^{\tau\gamma} = ra_\gamma z = r^{\gamma\tau}$, and thus $\gamma\tau = \tau\gamma$. Conversely, suppose F does not contain a primitive e-th root of unity. Let τ be a generator of C so that $r^\tau = rz$ with z a primitive e-th root of unity in T. Let σ be an automorphism in $\mathrm{Gal}(T/F)$ such that $z^\sigma \neq z$. Let γ be a preimage of σ in G. Then the above computation shows that $r^{\tau\gamma} \neq r^{\gamma\tau}$ and therefore $\gamma\tau \neq \tau\gamma$. Assertion 1 is proven.

Suppose that H is cyclic. Let σ be a generator of H and γ a preimage of σ in G. Let τ be a generator of C. Then γ and τ generate G. By assertion 1 $\gamma\tau = \tau\gamma$ if and only if F contains a primitive e-th root of unity. Assertion 2 follows.

Q.E.D.

Remark. Any central extension of a cyclic group is abelian. A central extension of an abelian group by a cyclic group need not be abelian. Consider the quaternian group.

I am grateful to Jack Sonn for his contribution to the proof of the above proposition and for many enlightening conversations on valuation theory and Galois theory.

The proof of the above proposition yields the following lemma, which is pure Galois theory.

Lemma 2. *Let F be a field. Let T be a finite normal extension of F and $H = \mathrm{Gal}(T/F)$. Suppose e is prime to* char (F) *and T contains a primitive e-th root of unity $z = \sqrt[e]{1}$. Let $b \in T$ and $E = T(\sqrt[e]{b})$. Suppose $[E:T] = e$.*

1) *E is a Galois extension of T with cyclic Galois group C of order e.*

2) *E is normal over F if and only if for each automorphism $\sigma \in H$ $b^\sigma = b^{i_\sigma}u_\sigma$ with u_σ an e-th power in T.*

3) *If E is normal over F, then* $\mathrm{Gal}(E/F)$ *is a central extension of H by C if and only if for each $\sigma \in H$ $z^\sigma = z^{i_\sigma}$.*

4) *If for each $\sigma \in H$ b^σ/b is an e-th power in T,* $\mathrm{Gal}(E/F)$ *is a central extension of H by C if and only if $z \in F$.*

The above lemma and above proposition can also be formulated in terms of Galois cohomology. The above lemma can be extended to the case E an abelian Galois extension of T.

Proposition 2. *Let E be a tamely ramified extension Galois over F with ramification index e. Suppose F contains a primitive e-th root of unity. Let T be the inertia field of E and let $s = bt$ be a prime element of T with $E = T(\sqrt[e]{s})$. Then*

1) *$T(\sqrt[e]{b})$ is an unramified extension Galois over F with Galois group G_0 a central extension of* Gal(T/F) *by a cyclic group of order dividing e. Moreover G_0 is isomorphic to the Galois group of the residue class field extension $\overline{T(\sqrt[e]{b})}$ over $\bar{F}$.*

2) *$F(\sqrt[e]{t})$ is a totally and tamely ramified extension Galois over F with cyclic Galois group C of order e.*

3) *$T(\sqrt[e]{b})$ and $F(\sqrt[e]{t})$ are linearly disjoint over F and E is a subfield of their composite $T(\sqrt[e]{b}, \sqrt[e]{t})$.*

4) *The Galois group of $T(\sqrt[e]{b}, \sqrt[e]{t})$ over F is isomorphic to the direct product $G_0 \times C$ and* Gal(E/F) *is a quotient group of $G_0 \times C$.*

Proof. The minimal polynomial for $\sqrt[e]{b}$ over T is x^{e_1}-c with $c^{e_2} = b$, $e_1e_2 = e$. This follows by Kummer theory. See [13, prop. 1]. By hypothesis, t is a prime element of F so that b and c are units of T. Since e_1 is prime to char$(\bar{F})$, $x^{e_1} - \bar{c}$ is a separable polynomial over $\bar{F}$. Hence $T(\sqrt[e]{b})$ is unramified over T by [20, theor. 3–2–6]. As T is unramified over F, $T(\sqrt[e]{b})$ is unramified over F by [20, prop. 3–2–4]. We conclude, as in the proof of Proposition 1, that for each automorphism $\sigma \in$ Gal(T/F) s^σ/s is an e-th power in T. Since $t \in F$, $s^\sigma = b^\sigma t$ and $s^\sigma/s = b^\sigma/b$. Hence c^σ/c is an e-th power in T. The balance of assertion 1 follows from the above Lemma 2 and the first assertion of Lemma 1.

Assertion 2 is immediate from [20, theor. 3–3–1]. Since $T(\sqrt[e]{b})$ is unramified over F and $F(\sqrt[e]{t})$ is totally ramified over F, they are linearly disjoint. This follows from the equality $ef = n$, or even from the inequality $ef \leqq n$. Clearly E is a subfield of their composite. Assertion 3 is proven, and assertion 4 follows from assertion 3 by Galois theory. Q.E.D.

Corollary 1. *If G_0 is abelian, then* Gal(E/F) *is abelian.*

Proof. Immediate from assertion 4 of the proposition.

Corollary 2. *Suppose n is prime to* char$(\bar{F})$, *F contains a primitive n-th root of unity, and every Galois extension of $\bar{F}$ of degree dividing n is abelian. Then every Galois extension of F of degree dividing n is abelian.*

Proof. Note that since e_1 divides e the degree of $T\sqrt[e]{b}$ over F divides the degree of E over F. The stated result follows from Corollary 1 together with assertion 1 of the proposition. Q.E.D.

COROLLARY 3. (Schilling, Amitsur, et al.) *Let k be an algebraically closed field of characteristic q. Let $F = k\{t_1, \cdots, t_m\}$ be an iterated power series field over F in m variables. Then every Galois extension of F of degree prime to q has an abelian Galois group with $\leqq m$ generators.*

PROOF. Induction based on part 4 of Proposition 2.

Note that the proof in [9] can be easily corrected by appropriately modifying Proposition 2.2 which is false as stated. In fact, every extension of F of degree prime to q is Galois with such a Galois group. Cf. [17, theor. 3], [3, prop. 2], [16, lemma 1], or [11, chap. 2.5].

PROPOSITION 3. *Let E be a normal extension of F. Let $G = \mathrm{Gal}(E/F)$. Suppose $\mathrm{Gal}(\bar{E}/\bar{F})$ is cyclic. Let e be the index of tame ramification of E over F. Suppose F contains a primitive e-th root of unity.*

1) *G is an extension of an abelian group with one or two generators by a q-group.*

2) *The q-Sylow subgroup of G is normal.*

PROOF. Let V be the ramification field of E. By Lemma 1 V is Galois over F. Let $G_1 = \mathrm{Gal}(V/F)$. By Lemma 1 the degree $[E\colon V]$ is a power of q. Let $Q = \mathrm{Gal}(E/V)$. Note that $|Q| = q^i$ divides $[E\colon V]$. By Galois theory we have an exact sequence of groups $1 \rightarrow Q \rightarrow G \rightarrow G_1 \rightarrow 1$. By Proposition 1 G_1 is abelian, with at most two generators, and assertion 1 is proven.

Let N be the q-Sylow subgroup of G_1. Since G_1 is abelian, N is a normal subgroup of G_1. Let M be the preimage of N in G. Then M is a normal subgroup of G by the Noether isomorphism theorems. The order $|M| = |N| \cdot q^i$ and the order $|G| = |G_1| \cdot q^i$. Hence M is the q-Sylow subgroup of G, and assertion 2 is proven. Q.E.D.

REMARK. Any extension of a group with normal q-Sylow subgroup by a q-group has normal q-Sylow subgroup.

4. Cyclic division algebras

The hypotheses of the previous section remain in force. F is a field complete in a discrete valuation v with residue class field $\bar{F}$, $q = \mathrm{char}(\bar{F})$, and t is a uniformizing parameter of v. We construct a cyclic algebra A over F and study the subfields of A. For the relevant definitions and theory we refer to [5, chap. 8] or [2, chaps. 4 and 5]. Let S be a cyclic Galois extension of F of degree n. Let σ be an automorphism generating $\mathrm{Gal}(S/F)$. For non-zero $a \in F$ (S, σ, a) denotes the cyclic crossed product algebra. (S, σ, a) is a central simple algebra of dimension n^2 over F containing S as a maximal commutative subring and generated over S by x_σ satisfying $x_\sigma^n = a$ and $x_\sigma b x_\sigma^{-1} = b^\sigma$ for all $b \in S$.

Suppose, moreover, that S is unramified over F in the weak sense that the ramification index $e = e(S/F) = 1$. We do not require that $\bar{S}$ be separable over $\bar{F}$. Let A be the cyclic algebra (S, σ, t).

Proposition 4. *Let T be an algebraic extension field of F with ramification index $e(T/F) = 1$.*

1) *A is a division algebra of index and order n in the Brauer group of F.*

2) *Let ST be a field compositum of S and T over F, and let m be the degree $[ST : T]$. Then $A_T = A \otimes_F T$ is an algebra of index and order m in the Brauer group of T.*

3) *T is isomorphic over F to a subfield of A if and only if T is isomorphic over F to a subfield of S.*

Proof. The order of A divides the index of A which divides $n = [S : F]$. Hence for assertion 1 it suffices to prove the order of $A = n$. The order of A is the least positive i such that t^i is a norm from S to F, $t^i = N(b)$. For $b \in S$, $v(N(b)) = n \cdot v(b)$. Moreover, $v(t^i) = i$. Since $e(S/F) = 1$, $v(b)$ is an integer. Hence if $t^i = N(b)$ then n divides i, and assertion 1 follows.

For assertion 2 note that the degree $m = [ST: T] = [S: S \cap T]$, and S is cyclic over $S \cap T$ with $\mathrm{Gal}(S/S \cap T)$ generated by $\sigma^{n/m}$. Moreover, ST is cyclic over T with $\mathrm{Gal}(ST/T)$ generated by γ, the extension of $\sigma^{n/m}$ to ST leaving T fixed. The algebra A_T is equivalent in the Brauer group of T to the cyclic algebra (ST, γ, t) by [5, theor. 8.5D, p. 89] or [2, theor. 8, p. 73]. This fact is an instance of the compatibility of the restriction map on the Brauer group with the restriction map in Galois cohomology. That is, the factor set for A_T in $H^2(\mathrm{Gal}(ST/T), (ST)^*)$ is the restriction to this cohomology group of the factor set for A in $H^2(\mathrm{Gal}(S/F), S^*)$. Note that the ramification index $e(ST/T) = 1$ and t is a prime element of T. By assertion 1 (ST, γ, t) is a division algebra of index and order m in the Brauer group of T. Assertion 2 follows.

Clearly any subfield of S is a subfield of A. Suppose T is a subfield of A. Let $f = [T: F]$. Then f divides n and the index of A_T in the Brauer group of T is n/f by [2, theor. 24, p. 61]. By assertion 2, $n/f = [ST: T]$. Hence the degree $[ST: F] = [ST: T][T: F] = n$. That is, $[ST: F] = [S: F]$, so that $ST = S$, and assertion 3 is proven. Q.E.D.

REMARK. If $\bar{F}$ is perfect and the Brauer group of $\bar{F}$ is trivial, then every division algebra with center F is isomorphic to (S, σ, t) for some S, σ, and t. See [19, chap. 12, theor. 2 and Ex. 1, p. 194]. If $(i, n) = 1$ and $j = i^{-1} \pmod n$, then $(S, \sigma, t^i) = (S, \sigma^j, t)$.

PROPOSITION 5. *Let M be an extension field of F contained in A. Let T be the inertia field of M. Then T is isomorphic over F to a subfield of S, T is a cyclic Galois extension of F, and* $\mathrm{Gal}(T/F)$ *is isomorphic to a quotient group of* $\mathrm{Gal}(S/F)$.

PROOF. T is the maximal unramified subfield of M. By assertion 3 of Proposition 4, T is isomorphic over F to a subfield of S. By Galois theory T is cyclic over F and $\mathrm{Gal}(T/F)$ is a quotient group of $\mathrm{Gal}(S/F)$. Q.E.D.

COROLLARY 1. *Suppose $\bar{F}$ is perfect and the Brauer group of $\bar{F}$ is trivial. Let M be an extension field of F and let T be the inertia field of M. If T is not a cyclic Galois extension of F, then M can not be embedded in any division algebra with center F.*

PROOF. Immediate from the proposition and the above cited theorem of [19]. Q.E.D.

In the terminology of [15], the conclusion of the above corollary is that M is not F-adequate. Consider the following example. By Tsen's theorem a function field in one variable over an algebraically closed field has trivial Brauer group. In particular, let $\bar{F}$ be the field of rational functions in a variable x over the complex numbers. Let $\bar{T} = \bar{F}(\sqrt{x}, \sqrt{x+1})$. Let $F = \bar{F}((t))$ be the field of formal Laurent series in one variable over $\bar{F}$, and let $T = \bar{T}((t))$. Then by the above corollary, T is not F-adequate.

PROPOSITION 6. *Let r be the largest factor of n prime to q. Suppose that any r-th roots of unity in S lie in F. Let M be a subfield of A which is normal over F. Let T be the inertia field of M and let V be the ramification field of M. Then*

1) *V is Galois over F,* $\mathrm{Gal}(V/K)$ *is abelian, and* $\mathrm{Gal}(V/F)$ *is an extension of* $\mathrm{Gal}(T/F)$ *by a cyclic group of order e where F contains a primitive e-th root of unity.*

2) $\mathrm{Gal}(M/V)$ *is a q-group, and the q-Sylow subgroup Q of* $\mathrm{Gal}(M/F)$ *is normal.*

3) *Suppose M is Galois over K. Let W be the fixed field of Q. Then W is a subfield of V and* $\mathrm{Gal}(W/F)$ *is a quotient group of* $\mathrm{Gal}(V/F)$, *an abelian group with one or two generators.*

PROOF. By Proposition 5, T is isomorphic over F to a subfield of S. Hence T is cyclic over F and if T contains a primitive e-th root of unity z, then z lies in F.

Assertion 1 then follows from part 2 of Proposition 1 and parts 2 and 3 of Lemma 1.

$\mathrm{Gal}(M/V)$ is a q-group by part 4 of Lemma 1. $\mathrm{Gal}(M/F)$ is an extension of $\mathrm{Gal}(V/F)$ by $\mathrm{Gal}(M/V)$. It follows from assertion 1 above, together with part 2 of Proposition 3 that the q-Sylow subgroup Q of $\mathrm{Gal}(M/F)$ is normal, proving assertion 2.

Suppose M is Galois over K. $\mathrm{Gal}(M/V)$ is a subgroup of Q. By Galois theory W is a subfield of V, and assertion 3 follows. Q.E.D.

COROLLARY 1. *Let S be as in the proposition. Suppose n is prime to q, p is a prime dividing n, and the field F does not contain a primitive p-th root of unity. Then every subfield of A which is Galois over F has an abelian Galois group with cyclic p-Sylow subgroup.*

PROOF. Let M be a subfield of A which is Galois over F. Since $[M:F]$ divides n, q does not divide $[M:F]$. Hence $M = V$. The stated result follows from assertion 1 of the proposition and corollary 2 to Lemma 1. Q.E.D.

COROLLARY 2. *Suppose q does not divide n, and S does not contain any nontrivial n-th roots of unity. Then every subfield of A which is Galois over F is cyclic and is isomorphic over F to a subfield of S.*

PROOF. Let M be a subfield of A which is Galois over F. Since q does not divide $[M:F]$, $M = V$. Since S contains no nontrivial n-th root of unity it follows from part 1 of the proposition that $e = 1$. Hence $M = T$. The stated result follows by Proposition 5. Q.E.D.

5. The division algebra D

We now apply the above results to prove Theorem 1. Let the field extension K of k and the algebra $D = (L, \sigma, t)$ be as defined above. Recall that $q = \mathrm{char}(k)$. Note that every root of unity in L lies in k. In fact, k is algebraically closed in L. From Gauss's Lemma it follows that L_0 is algebraically closed in $L = L_0((t))$ and k is algebraically closed in $L_0 = k(x_1, \cdots, x_n)$.

We define the valuation v on K by the formula $v(\Sigma_{i=m}^{\infty} a_i t^i) = m$. Then v is a normalized discrete valuation on K with uniformizing parameter t and residue class field K_0. K is complete with respect to v. L is an unramified Galois extension of K with cyclic Galois group generated by σ.

It follows from Proposition 4 that D is a division algebra of index and order n in the Brauer group of K. This fact is also proven in [11, theor. 4, p. 84].

PROOF OF THEOREM 1. Let T be the inertia field of M, and let V be the ramification field of M. As observed above, every root of unity in L lies in k and hence, a fortiori, lies in K. Hence the hypotheses of Proposition 6 are satisfied. The q-Sylow subgroup of $\mathrm{Gal}(M/F)$ is normal by part 2 of Proposition 6, proving assertion 1. Note that if q does not divide $m = [M:K]$, then $M = V$. Assertion 2 follows from part 1 of Proposition 6. Q.E.D.

PROOF OF COROLLARY 1 TO THEOREM 1. If k does not contain a primitive p-th root of unity, then K does not contain a primitive p-th root of unity. The stated result follows from Corollary 1 to Proposition 6. Q.E.D.

Note that if n is odd and k is the field of rational numbers, Corollary 2 to Proposition 6 applies to D.

6. Generic division algebras

For the theory of polynomial identities and generic division algebras we refer to [3], [4], and [11]. Any division ring satisfying a polynomial identity is a division algebra finite dimensional over its center. A division algebra has index n if and only if it satisfies the polynomial identities of n by n matrices over its center. This is a consequence of a theorem of Kaplansky, Amitsur, and Levitski [11, p. 30].

Fix h with $2 \leqq h \leqq \infty$. Consider the n by n matrices X_r, $1 \leqq r \leqq h$, whose entries are distinct indeterminates over k, $X_r = (x^r_{ij})$. Let R be the ring of polynomials over k in the commuting variables x^r_{ij}. The subring $k[X]$ of the ring of n by n matrices over R generated over k by the X_r is the generic matrix algebra of degree n over k. The ring $k[X]$ satisfies the polynomial identities of n by n matrices, and is universal with respect to this property. By a theorem of Amitsur $k[X]$ is a domain, [3, theor. 3] or [11, theor. 2, p. 90]. Its ring of (central) quotients $k(X)$ is the generic division algebra of index n over k.

DEFINITION. If the following condition holds, a division algebra A is a *crossed product with the group* G: A contains a maximal subfield L which is Galois over the center C and $\mathrm{Gal}(L/C)$ is isomorphic to G.

We require the following theorems of Amitsur.

LEMMA 3. *If $k(X)$ is a crossed product with a group G, then any division algebra of index n whose center is a field extension of k is a crossed product with G.* See [3, p. 418–419] or [11, theor. 4, p. 93].

Lemma 4. *If* char(k) *does not divide* n, *then there exists a division algebra* A *of index* n *with center* C, *a field extension of* k, *such that every subfield of* A *containing* C *is Galois over* C *with abelian Galois group a direct product of cyclic groups of prime order.* See [3, theor. 3, p. 412] or [11, theor. 1, p. 102]. For an alternate treatment, see [14].

Proposition 7. *Suppose* q *does not divide* n.

1) *If* n *is divisible by* p^3 *for any prime* p, *then* $k(X)$ *is not a crossed product.*

2) *If* n *is divisible by* p^2 *for any prime* p *such that* k *does not contain a primitive* p*-th root of unity, then* $k(X)$ *is not a crossed product.*

Proof. Suppose $k(X)$ is a crossed product with a group G. Then by Lemma 3 and Lemma 4, G is a direct product of cyclic groups of prime order. By theorem 1 for each prime p dividing n the p-Sylow subgroup of G is either cyclic or a direct product of two cyclic groups. Hence n is not divisible by p^3 for any prime p, proving assertion 1. By Corollary 1 to Theorem 1, if k does not contain a primitive p-th root of unity, then the p-Sylow subgroup of G is cyclic. Hence n is not divisible by p^2, proving assertion 2. Q.E.D.

Remark. The proof of assertion 2 does not depend on the Dirichlet density theorem. It depends on Corollary 2 to Lemma 1, on Proposition 5, and on Lemmas 3 and 4.

It remains to treat the case n divisible by q. As noted in [10] Lemma 3 can be strengthened as follows.

Lemma 5. *If* $k(X)$ *has a subfield Galois over the center with Galois group* G, *then any division algebra of index* n *whose center is a field extension of* k *has a subfield Galois over the center with Galois group isomorphic to* G.

Sketch of Proof. The above cited proofs of Lemma 3 apply with the appropriate modifications. In the notation of [11, theor. 4, p. 93], the elements $\rho_{s,t}$ are in the centralizer of $F(\theta)$. That is $\theta\rho_{s,t} = \rho_{s,t}\theta$. Hence $\theta'\rho'_{s,t} = \rho'_{s,t}\theta'$, and therefore $(st)' = s't'$. It follows that G' is a group of automorphisms of $L(\theta')$ over L isomorphic to G. As θ' satisfies a polynomial of degree $= |G|$, $L(\theta')$ is Galois over L with Galois group G'. Q.E.D.

We require an elementary lemma on subfields of division algebras.

Lemma 6. *Suppose* $n = rs$ *and* $(r, s) = 1$. *Let* A *be a division algebra of index* n *with center* C. *Let* A_1 *be a subalgebra of* A *central over* C *of index* r. *Suppose* E *is an extension field of degree* m *over* C *and* m *divides* r. *If* E *is isomorphic over* F *to a subfield of* A, *then* E *is isomorphic over* F *to a subfield of* A_1.

Proof. By [2, theor. 24, p. 61] E is isomorphic to a subfield of A if and only if the index of A_E is n/r. Let A_2 be the centralizer of A_1 in A. Then $A = A_1 \otimes_C A_2$. Since $(r, s) = 1$ the index of A_{2_E} is s, by [2, theor. 20, p. 60], and the index of A_E is the product of the indices of A_{1_E} and A_{2_E}. Hence the index of A_{1_F} is r/m, and E is isomorphic over F to a subfield of A_1. Q.E.D.

Corollary 1. *Suppose $n = rs$ and $(r, s) = 1$. Let G be a group of order n, N a normal subgroup of order s, and $H = G/N$. Suppose there exists a division algebra A of index s with center C. If every division algebra of index n with center C is a crossed product with G, then every division algebra of index r with center C is a crossed product with H.*

Proof. Suppose B is a division algebra of index r with center C. Then $B \otimes_C A$ is a division algebra of index n with center C. By hypothesis there exists a maximal subfield M of $B \otimes_C A$ Galois over C with Galois group G. Let E be the subfield of M fixed by N. The result follows from Lemma 6. Q.E.D.

In the terminology of [10] the above corollary states that if the pair (C, G) has the crossed product property A then the pair (C, H) has the crossed product property A. In case C is a global field or a local field more can be proven. See [10, prop. 8].

Suppose F is a field of characteristic $q \neq 0$ with a discrete valuation and uniformizing parameter t. The polynomial $x^q - x - 1/t$ has no root in F. By Artin–Schreier theory it is irreducible and yields a cyclic Galois extension of degree q over F. By a theorem of Witt [18, corol. 1, p. II–5] the Galois group of the maximal q extension of any field of characteristic q is a free pro-q group. Hence for any $s = q^i$ there exists a cyclic Galois extension of F of degree s. As noted in [10] it follows from [6, p. 205] that every finite q group is realized as a Galois group over F, a fact which we do not require here.

Let $n = rs$ with r prime to q and $s = q^i$. Let A be Amitsur's division algebra of index r in Lemma 4 and C the center of A. C is a field of iterated power series in at least two variables over the algebraic closure of k. Let t_1 and t_2 be the last two variables. Then $C = F((t_2))$ and F is a field of characteristic q complete in a discrete valuation with uniformizing parameter t_1. As noted above there exists a cyclic extension E of degree s over F. Let S be the corresponding unramified extension of C, and let σ be a generator of $\mathrm{Gal}(S/C)$. By Proposition 4, $B = (S, \sigma, t_2)$ is a division algebra of index and order s in the Brauer group of C. Since $(r, s) = 1$, $A \otimes_C B$ is a division algebra central over C of index n containing A as a subalgebra.

For any integer s prime to q the cyclic extension $F(\sqrt[s]{t_1})$ of F yields, as above, a division algebra central over C of index and order s. Similarly, if C is a field of rational functions in two variables over a field containing enough roots of unity, for any s there exist division algebras central over C of index and order s. For further results see [7, section 4].

PROOF OF THEOREM 2. If q does not divide n, we are done by Proposition 7. Suppose $n = rs$ with $s = q^i$ and r not divisible by q. Suppose $k(X)$ is a crossed product with Group G. Let Z be the center of $k(X)$ and let M be a subfield of $k(X)$ Galois over Z with $\mathrm{Gal}(M/Z) = G$. By Lemma 5 and Theorem 1 the q-Sylow subgroup Q of G is normal. Let W be the fixed field of Q in M. Then W is Galois over Z of degree r with $H = \mathrm{Gal}(W/Z) = G/Q$. By Lemma 5 any division algebra of index n whose center is a field extension of k has a subfield Galois over the center with Galois group isomorphic to H. By Theorem 1, H is an abelian group with one or two generators. If p is a prime dividing r, the p-Sylow subgroup of H is cyclic or a product of two cyclic groups. If k does not contain a primitive p-th root of unity, the p-Sylow subgroup of H is cyclic.

Let A be the division algebra of index r of Lemma 4, and let $A \otimes_C B$ be the division algebra of index n containing A described above. By Lemma 5, $A \otimes_C B$ contains a subfield E Galois of degree r over C with Galois group H. By Lemma 6, E is isomorphic over C to a subfield of A. By Lemma 4, H is a direct product of cyclic groups of prime order. Theorem 2 follows. Q.E.D.

The above proof of Theorem 2 yields the following stronger statement.

PROPOSITION 8. *Suppose $k(X)$ contains a subfield Galois of degree m over the center. Then m is not divisible by p^3 for any prime $p \neq q$, and m is not divisible by p^2 for any prime $p \neq q$ such that k does not contain a primitive p-th root of unity.*

To discuss generic division algebra of various indices we expand our notation and let $k(X, n)$ denote the generic division algebra of index n over k. Suppose $n = rs$ with $(r, s) = 1$ and $k(X, n)$ has a subfield Galois over the center of degree r with Galois group G. It follows from Lemmas 5 and 6 that if there exists a central division algebra of index s over the center of $k(X, r)$, then $k(X, r)$ is a crossed product with group G. See [10, theor. 11]. Fein and Schacher have recently announced an improvement of this result. See in this connection [12, theor. 6.3, p. 95] and [7, section 4].

By [10, lemma 3] if A is a cyclic division algebra of index nm with center C, n is prime to $\mathrm{char}(C)$, and C contains a primitive n-th root of unity, then A is a crossed product for a direct product of a cyclic group of order m and a cyclic group of order n. The strength of non-crossed product results to be obtained by constructing cyclic division algebras is limited by this fact.

Added in proof. See *Twisted rational functions and series* by this author, preprint, April 1977, for an alternative proof of Proposition 5 and for further related results and generalizations.

References

1. Adrian A. Albert, *On p-adic fields and rational division algebras*, Ann. of Math. **41** (1940), 674–693.
2. Adrian A. Albert, *Structure of Algebras*, American Mathematical Society, Colloquium, Publications 29, 1961.
3. S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.
4. S. A. Amitsur, *The generic division rings*, Israel J. Math. **17** (1974), 241–247.
5. E. Artin, C. Nesbitt and R. Thrall, *Rings with Minimum Condition*, University of Michigan, Ann Arbor, 1944.
6. Emil Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.
7. M. Auslander and A. Brumer, *Brauer groups of discrete valuation rings*, Indag. Math. **30** (1968), 286–296.
8. Richard Brauer, *On normal division algebras of index* 5, Proc. Nat. Acad. Sci. U.S.A. **24** (1938), 243–246.
9. Chan-Nan Chang, *The Brauer group of an Amitsur field*, Proc. Amer. Math. Soc. **39** (1973), 493–496.
10. B. Fein and M. Schacher, *Galois groups and division algebras*, J. Algebra **38** (1976), 182–191.
11. Nathan Jacobson, *PI-Algebras. An Introduction*, Springer-Verlag, Lecture Notes in Mathematics 441, Berlin, 1975.
12. Claudio Procesi, *Rings with Polynomial Identities*, Marcel Dekker, New York, 1973.
13. Lawrence Risman, *On the order and degree of solutions to pure equations*, Proc. Amer. Math. Soc. **55** (1976), 261–266.
14. Lawrence Risman, *Non-cyclic division algebras*, to appear in J. Pure Appl. Algebra.
15. Murray Schacher, *Subfields of division rings*, J. Algebra **9** (1968), 451–477.
16. M. Schacher and L. Small, *Noncrossed products in characteristic P*, J. Algebra **24** (1973), 100–103.
17. O. F. G. Schilling, *Arithmetic in fields of formal power series in several variables*, Ann. of Math. **38** (1937), 551–576.
18. Jean-Pierre Serre, *Cohomology Galoissienne*, Springer-Verlag, Lecture Notes in Mathematics 5, Berlin, 1965.
19. Jean-Pierre Serre, *Corps Locaux*, Hermann, Paris, 1968.
20. Edwin Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

THE TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY
HAIFA, ISRAEL