ISRAEL JOURNAL OF MATHEMATICS, Vol. 47, Nos. 2-3, 1984

RETRACT RATIONAL FIELDS AND CYCLIC GALOIS EXTENSIONS

BY

DAVID J. SALTMAN[†]

ABSTRACT

In [23], this author began a study of so-called lifting and approximation problems for Galois extensions. One primary point was the connection between these problems and Noether's problem. In [24], a similar sort of study was begun for central simple algebras, with a connection to the center of generic matrices. In [25], the notion of retract rational field extension was defined, and a connection with lifting questions was claimed, which was used to complete the results in [23] and [24] about Noether's problem and generic matrices. In this paper we, first of all, set up a language which can be used to discuss lifting problems for very general "linear structures". Retract rational extensions are defined, and proofs of their basic properties are supplied, including their connection with lifting. We also determine when the function fields of algebraic tori are retract rational, and use this to further study Noether's problem and cyclic 2-power Galois extensions. Finally, we use the connection with lifting to show that if p is a prime, then the center of the p degree generic division algebra is retract rational over the ground field.

Introduction

In [23], a series of results were proved consisting of statements that certain Galois extensions could be lifted over local rings, or could be pulled back from complete fields to dense subfields (the so-called approximation problem). This paper is a sequel to [23], in that here we raise and sometimes answer questions that arose out of [23].

One consequence of the methods of [23] was that a large "chunk" of the Grunwald–Wang theorem of algebraic number theory was, in fact, a special case of a result that applies to all fields (see also [17] and [26]; note that [17] predates [23]). The research that led up to this paper began by taking a closer look at the Grunwald–Wang Theorem and asking if "more" of it could be generalized to all fields. For example, let us consider Wang's counterexample. The unramified

[†] The author is grateful for NSF support under grant #MCS79-04473.

Received September 1, 1982 and in revised form November 1, 1983

cyclic extension L/Q_2 of degree 8 does not pull back to a cyclic extension of Q. But notice the following: $L = Q_2(\rho)$ where ρ is a primitive 17th root of one. And $Q(\rho)/Q$ is cyclic of degree 16. What this means is that $L \oplus L$ can be pulled back to a cyclic extension of Q of degree 16.

It turns out that this phenomenon is more general. It happens for all local and global fields and all 2 power cyclic groups (we reprove this). What's more, we can generalize the corresponding lifting result to purely transcendental extensions of local or global fields. But we also show that this phenomenon is not completely general; we construct a counterexample.

Several pieces of mathematical machinary are used to show the above results. One of them is an equivalence, for lifting and approximation questions, between 2 power cyclic Galois extensions and abelian crossed products. This equivalence is used to give a relatively elementary proof of a full version of the Grunwald–Wang theorem. In particular, Wang's counterexample is given another proof.

Going back to [23], we note that a relationship was traced between Noether's Problem and lifting problems. This relationship was one way. In order to give a converse, the notion of retract rational field extensions was introduced in [25]. Briefly, K/F is retract rational if K is the quotient field of S and S is a retraction of a localized polynomial ring $F[x_1, \cdots, x_n](1/r)$. The idea is that a retract rational extension is almost rational (i.e., purely transcendental). In [25], some properties of these extensions were sketched. A major goal of this paper is to give a fuller treatment of these extensions.

The point about retract rational field extensions is that they are naturally associated with lifting questions. In [25] this was claimed for Galois extensions and for central simple algebras. But it is true more generally, and one proof can show it all. In order to do this, we must use the appropriate general notion, that of linear structures. With this, and some other definitions, we can present our results in very general terms (and prove things once, instead of three times).

Much previous work on Noether's problem has used the function fields of algebraic tori. This culminates in the treatment of [6], where questions about the stable isomorphisms of these function fields are reduced to questions about integral representations of finite groups. In this paper, we ask parallel questions about these function fields and retract rationality. We can say precisely when these function fields are retract rational. In addition, we define a functor on the integral representations which is shown to be related to relative lifting problems. It is this machinery that allows us to present the counterexample in the lifting of 2 power cyclic Galois extensions mentioned above.

Throughout this paper, we will attempt to illustrate that the notion of retract rationality is a natural one. For example, we will prove the following result. Let A be a finite abelian group of exponent $2^r m$ for m odd. If F is a field of characteristic $\neq 2$, L is the field $F(x_g \mid g \in A)$, and ρ is a primitive 2^r root of one, then L^A/F is retract rational if and only if $F(\rho)/F$ is a cyclic extension. Compare this with the corresponding characterization of when L^A/F is rational ([16]). We can also extend our results to include all quotient fields of symmetric algebras of $F[A]$ modules which are faithful as A modules.

We spend a bit of time in this paper looking at the question of lifting crossed product algebras. As an outgrowth of that and our general theory, we prove the following: Let $Z(F, n, r)$ be the center of the generic division algebra $\mathrm{UD}(F, n, r)$ (e.g., [14], p. 92). If $n = p$ is a prime, then $Z(F, p, r)/F$ is retract rational. Compare this with [10], [11], and [20], where rationality is proved for $n = 2, 3, 4$.

In the previous papers [23], [24], and [25], both lifting problems and approximation problems are treated. Except for parts of §4, we will place the main emphasis on lifting problems. We believe the lifting questions to be more fundamental. The reader should note that these two sorts of questions are closely linked. In fact, using the argument of 4.20, a sort of equivalence could be proved between them. To do so, however, would require even more new terminology and does not seem, now, worth the effort.

In §1 we introduce the general terminology of linear structures, and the associated other definitions, §2 has the results about integral representations which we require, §3 is about retract rational fields and §4 is about cyclic Galois extensions. Also in §4 is the result about L^A mentioned above. Finally, §5 has the results about crossed products including the result about $Z(F, p, r)$.

Let us specify some terminology and notation. In this whole paper, F will be an infinite field, the "base" field. All rings will be F algebras. The term F map will denote an F algebra homomorphism. If G is a group, the symbol $F[G]$ will mean the group algebra, whereas if V is an F vector space, $F_+[V]$ will mean the symmetric algebra. A local F algebra will always be presented as T, M where $M \subset T$ is the maximal ideal. By assumption, local F algebras will be commutative. If V is an F vector space, $[V : F]$ is the dimension of V over F. We will fix an algebraic closure, $\bar{F}$, of F, and will denote by $\rho(n)$ a primitive nth root of one in $\bar{F}$, if meaningful. For any field K, $K(\alpha)$ will denote the field generated by K and α. The term "valuation on K" will refer to a real valued valuation. If K is a global field, we will (imprecisely) use the term valuation and prime interchangeably.

By a Galois extension we will mean a Galois extension of commutative rings

as in [7]. In particular, if K is a field and L/K is Galois, then L need not be a field (but L is a direct sum of fields). A Galois extension with group G will be abbreviated as a G-Galois extension. Note that such an extension is a ring extension S/R and a specified action of G on S. All isomorphisms of G-Galois extensions are assumed to preserve the G action.

We will make considerable use of the Brauer group, $\mathrm{Br}(R)$, of the commutative ring R, especially in the case R is a field. Of course, $\mathrm{Br}(R)$ consists of equivalence classes of Azumaya algebras. If A/R is Azumaya (this means R is the center of A), we will denote by $[A]$ the Brauer equivalence class of A. If $S \supseteq R$, $\mathrm{Br}(S/R)$ will denote the subgroup of $\mathrm{Br}(R)$ of all classes split by S. If A/R is Azumaya and A has constant rank as an R module, then this rank is a square. The square root of this rank is called the degree of A. Though we assume the reader is familiar with the Brauer group, we recall one important fact. If A/L, B/L are Azumaya, L is a field, $[A]=[B]$, and A, B have equal degrees, then $A \cong B$ as L algebras. Finally, if A is Azumaya, the exponent of A will be the order of $[A]$ in the Brauer group. We refer the reader to [1], [7], and [18] for the basic information about the Brauer group we will require.

Suppose S/R is G-Galois and S^* is the unit group of S. If $c(\sigma,\tau)\in S^*$ is a G 2-cocycle, we can form the crossed product $\Delta(S/R, G, c)$, which is Azumaya over R (e.g., [7], p. 121). If G is cyclic, the cocycle c is determined (up to coboundary) by a choice of generator $\sigma \in G$ and an element $d \in R^*$. The corresponding cyclic algebra will be denoted by $\Delta(S/R, \sigma, d)$.

All modules in this paper will be left modules. If R, S are commutative rings, if $\varphi : R \to S$ is a ring homomorphism, and if M is an R module, then $M \otimes_\varphi S$ will denote the tensor product where S is an R module via φ. If $f : N \to M$, $g : N \to M'$ are module homomorphisms (over some ring) we will denote the pushout by $M \oplus_N M'$. In the dual situation, $M \times_N M'$ will denote the pullback. In general, all maps which have, for one reason or another, unique extensions will have the same symbol used to designate the extension. And truly finally, if S is a domain, we will use $q(S)$ to denote the field of fractions of S.

§1. General nonsense

A major theme of this paper is the study of whether certain algebraic structures can be lifted over local rings. The purpose of this section is to develop a language with which we can discuss all of our lifting problems simultaneously. Of course, one can do this in many ways. Our choice here is a bit arbitrary, but it serves our purposes.

In the general definitions that will follow, it will be useful to keep in mind two examples of algebraic structures which we ultimately will deal with. They are Azumaya algebras and G-Galois extensions, for G a finite group (fixed). These examples have two important characteristics. First, they are both defined with respect to a base ring, either the center of the algebras or the fixed ring of the Galois group. Second, for both structures it makes sense to talk about base change via the tensor product. These two characteristics motivate our general definitions.

Let R be a commutative ring and M an R module. We set $M^{(0)} = R$ and we set $M^{(r)}$ to be the r-fold tensor product of M over R. We define a *linear structure* to be a tuple of the form

$$\mathcal{M} = \langle R, M, f_1, \cdots, f_r \rangle$$

where R, M are as above and $f_i : M^{(s_i)} \to M^{(t_i)}$ are R module maps. We will say such an $\mathcal{M}$ is over R and will occasionally write $\mathcal{M}/R$. The *type* of $\mathcal{M}$ is the sequence $(s_1, t_1), \cdots, (s_r, t_r)$. It is clear that R algebras can be thought of as linear structures over R. If G is a finite group, then G-Galois extensions S/R can be thought of as linear structures over R if we include among the f's the maps $\sigma : S \to S$ for each $\sigma \in G$. Finally, R modules with multilinear forms are also linear structures over R. In the rest of this paper, algebraic structures will be described as linear structures without explicitly stating how the identification is made.

The definition of a homomorphism of linear structures is the obvious one. That is, if

$$\mathcal{M} = \langle R, M, f_1, \cdots, f_r \rangle \quad \text{and} \quad \mathcal{N} = \langle S, N, g_1, \cdots, g_r \rangle$$

have the same type, we can define a homomorphism $\Psi : \mathcal{M} \to \mathcal{N}$ to be a pair (φ, ψ) where $\varphi : R \to S$ is a ring homomorphism, $\psi : M \to N$ is a φ-semilinear, and (φ, ψ) preserves the f_i and g_i as follows: Define $\psi^{(0)}$ to be φ, and $\psi^{(r)}$ to be the induced map $M^{(r)} \to N^{(r)}$. If $f_i : M^{(s)} \to M^{(t)}$ (and so $g_i : N^{(s)} \to N^{(t)}$), then we require that $g_i \circ \psi^{(s)} = \psi^{(t)} \circ f_i$. In this way the class of all linear structures of a fixed type form a catagory in the usual way. An isomorphism $(\varphi, \psi) : \mathcal{M}/R \to \mathcal{N}/S$ will be an invertible morphism which is R linear. That is, we insist that $S = R$, that φ is the identity, and that $\psi^{-1} : \mathcal{N} \to \mathcal{M}$ exists.

In the opposite direction, if $\mathcal{M} = \langle R, M, f_1, \cdots, f_r \rangle$ is a linear structure and $\varphi : R \to S$ is a ring homomorphism (and S is commutative), we can define

$$\mathcal{M} \otimes_\varphi S = \langle S, M \otimes_\varphi S, f_1 \otimes 1, \cdots, f_r \otimes 1 \rangle,$$

where $(M \otimes_\varphi S)^{(n)}$ is identified with $M^{(n)} \otimes_\varphi S$ and so $f_i \otimes 1$: $(M \otimes S)^{(s)} \to (M \otimes S)^{(t)}$ is well defined. Of course, $\mathcal{M} \otimes_\varphi S$ is a linear structure of the same type as $\mathcal{M}$ and the induced map $\mathcal{M} \to \mathcal{M} \otimes_\varphi S$ is a homomorphism.

In studying lifting problems, we will consider classes of structures over a fixed field as follows. Let F be a field. An F structure is a linear structure $\mathcal{M}/R$ such that $F \subset R$. The class of all F structures of a fixed type form a category where we insist that all homomorphisms be F linear. An F-class $\mathcal{C}$ is a class of F structures closed under (F linear) isomorphisms such that it has two additional properties. First, if $\mathcal{M}/R \in \mathcal{C}$, and $\varphi : R \to S$ is an F map with S commutative, then $\mathcal{M} \otimes_\varphi S \in \mathcal{C}$. Secondly, if $\mathcal{M}/R \in \mathcal{C}$ and $R' \subseteq R$ is a subring, then there is a $\mathcal{M}''/R'' \in \mathcal{C}$ such that $R' \subseteq R'' \subseteq R$; R'' is finitely generated as a ring over R', and $\mathcal{M}' \otimes_{R''} R \cong \mathcal{M}$. We are interested in several examples of F classes. If n is a positive integer, we denote by $\mathcal{A}(F, n)$ the F class of all Azumaya algebras A/R where A is of degree n. Let G be a finite group. We denote by $\mathcal{E}(G)$ the F class of all G-Galois extensions S/R where $F \subseteq R$. That both of these examples are F classes can be shown using [18], p. 35, [7], p. 85, and [22], p. 528. Later on in this paper we will describe other examples.

In [23] and [24], this author considered questions of the following sort. If C/K was a Galois extension, or an Azumaya algebra, and T was a local ring with residue field K, did C lift to a similar structure over T? In some cases, an affirmative answer to this question was obtained via the construction of a generic Galois extension or a pure generic algebra. Both this question, and this approach to an answer, are completely general and can be phrased in terms of F classes, which we now do. We say an F class $\mathcal{C}$ has the *lifting property* if whenever T, M is a local F algebra and $\mathcal{M} \in \mathcal{C}$ is over T/M, then there is a $\mathcal{M}'/T \in \mathcal{C}$ such that $\mathcal{M}' \otimes_T T/M \cong \mathcal{M}$, the isomorphism being T/M linear, by definition. $\mathcal{M}/R \in \mathcal{C}$ is a *representing object* for $\mathcal{C}$ if R is an affine F algebra and if whenever $\mathcal{N}/K \in \mathcal{C}$ with K a field, then there is an F map $\varphi : R \to K$ such that $\mathcal{N} \cong \mathcal{M} \otimes_\varphi K$. In this circumstance we say that $\mathcal{N}/K$ is a specialization of $\mathcal{M}/R$ and that φ realizes $\mathcal{N}/K$. Finally, a generic object $\mathcal{M}/R \in \mathcal{C}$ is a representing object such that R has the form $F[x_1, \cdots, x_n](1/r)$; that is, such that R is a localized polynomial ring.

In both the case of Galois extensions and of Azumaya algebras, there is a natural representing object. For Galois extensions, we (roughly speaking) refer to Noether's construction ([23], p. 274 for example). For Azumaya algebras, we refer to the generic division algebra $\mathrm{UD}(F, n, r)$. Considering, for example, this later case, the situation is the following. We set $R(F, n, r) \subseteq \mathrm{UD}(F, n, r)$ to be the ring of generic $n \times n$ matrices. If $C(F, n, r)$ is the center of $R(F, n, r)$, then there is a $0 \neq s \in C(F, n, r)$ such that $R(F, n, r)(1/s)/C(F, n, r)(1/s)$ is Azumaya of

degree n. If A/K is any central simple algebra of degree n, and $0 \neq t \in C(F, n, r)$, then there is a $\varphi : C(F, n, r)(1/st) \to K$ such that

$$R(F, n, r)(1/st) \otimes_{\varphi} K \cong A.$$

In other words, $R(F, n, r)(1/s)/C(F, n, r)(1/s)$ is not only a representing object, but is a densely representing object in the following sense. A representing object $\mathcal{M}/R \in \mathcal{C}$ is called *densely* representing if R is a domain and if for any $0 \neq s \in R$, then $\mathcal{M} \otimes_R R(1/s)$ is a representing object.

In [23] for Galois extensions, and in [24] for Azumaya algebras, a relationship was traced between generic objects and the lifting property. This relationship is quite general, and is stated in the next result. We will omit the proof because it is a trivial generalization of the argument of [23], p. 275.

PROPOSITION 1.1. *Let $\mathcal{C}$ be an F-class,*

(a) *if $\mathcal{C}$ has a generic object, then $\mathcal{C}$ has the lifting property;*

(b) *if $\mathcal{C}$ has a densely representing object, and $\mathcal{C}$ has the lifting property, then $\mathcal{C}$ has a generic object.*

Note that, arguing as in [23], p. 256, the existence of a generic object implies the more general lifting property over semilocal F algebras. Thus if $\mathcal{C}$ has a densely representing object, the lifting property for $\mathcal{C}$ implies the lifting property for $\mathcal{C}$ over semilocal F algebras.

Let us return to the F class, $\mathcal{A}(F, n)$, of Azumaya algebras and the ring $R(F, n, r)$. This ring is sort of a free object for $\mathcal{A}(F, n)$, but is not, itself, in $\mathcal{A}(F, n)$. The situation occurs again, so we introduce some terminology to cover it. Let $\mathcal{C}$ be an F class, $\mathcal{M}, \mathcal{N} \in \mathcal{C}$. A surjection $(\varphi, \psi) : \mathcal{M} \to \mathcal{N}$ is a morphism such that ψ, φ are surjections as set maps. Given this, it is clear how to define a projective. If $\mathcal{P}$ is an F structure of the same type as those in $\mathcal{C}$, then $\mathcal{P}$ is a *projective object* for $\mathcal{C}$ if whenever $\Delta : \mathcal{P} \to \mathcal{N}$ and $\Psi : \mathcal{M} \to \mathcal{N}$ are morphisms, where Ψ is a surjection and $\mathcal{M}$, $\mathcal{N} \in \mathcal{C}$, then there is a $\Delta' : \mathcal{P} \to \mathcal{M}$ such that $\Delta = \Psi \circ \Delta'$. We emphasize that, as with $R(F, n, r)$, we do not ask that $\mathcal{P}$ be in $\mathcal{C}$. We say that $\mathcal{P}$ is a projective object in $\mathcal{C}$ if $\mathcal{P} \in \mathcal{C}$.

We cite a few examples of projective objects, beginning with the easy fact that $R(F, n, r)/C(F, n, r)$ is a projective object for $\mathcal{A}(F, n)$. As another example, let $\mathcal{C}_0$ be the F class of all commutative F algebras R (each R is over itself). Then $R = F[x_1, \cdots, x_n]$ is a projective object in $\mathcal{C}_0$. We will give a third example in the next lemma.

LEMMA 1.2. *Let G be a finite group and V an $F[G]$ module such that*

$G \to \mathrm{End}_F(V)$ is injective. Then if $F_+[V]$ is the symmetric algebra, we have that $F_+[V]/F_+[V]^G$ is a projective object for $\mathscr{C}(G)$, the F class of G-Galois extensions.

PROOF. Suppose S/R and S'/R' are G-Galois extensions of commutative F algebras and $\psi : S \to S'$ is a G preserving F map surjection such that the restriction of ψ to R is onto R'. Let $\varphi : F_+[V] \to S'$ be any G preserving F map. By [5], p. 13, $(S')^+$ is a projective $R'[G]$ module, and so a projective $F[G]$ module. Hence there is a $F[G]$ module map $\delta : S' \to S$ such that $\psi \circ \delta$ is the identity on S'. Restricting $\delta \circ \varphi$ to V gives an $F[G]$ module map $\mu : V \to S$. This map μ induces a G preserving F algebra map $\mu'' : F_+[V] \to S$. Now $\varphi = \psi \circ \mu''$ because this relation holds on V. Q.E.D.

REMARK. I thank F. DeMeyer for this argument.

Though $R(F, n, r)$ is not Azumaya, we know that $R(F, n, r)(1/s)$ is Azumaya for some $0 \neq s \in C(F, n, r)$. This new algebra is no longer projective, but it is almost projective in the following sense. Define a morphism $(\varphi, \psi) : \mathscr{M}/R \to \mathscr{N}/S$ to be local if $\varphi^{-1}(S^*) = R^*$. That is, if the preimage of every unit in S is a unit in R. If $\mathscr{C}$ is a category of F structures, then $\mathscr{P} \in \mathscr{C}$ is a *local projective* if for all local surjections $\Psi : \mathscr{M} \to \mathscr{N}$, and all $\Delta : \mathscr{P} \to \mathscr{N}$, there is a $\Delta' : \mathscr{P} \to \mathscr{M}$ such that $\Delta = \Psi \circ \Delta'$. The use of the term local is, perhaps, justified by the following result.

THEOREM 1.3. (a) *Let $\mathscr{C}$ be an F class, and $\mathscr{P}/R \in \mathscr{C}$ a local projective. If $0 \neq s \in R$, then $\mathscr{P} \otimes_R R(1/s)/R(1/s) \in \mathscr{C}$ is a local projective.*

(b) *$S = F[x_1, \cdots, x_n](1/s)$ is a local projective for the class of all commutative F algebras.*

(c) *Let G be a finite group, and V a $F[G]$ module as in* 1.2. *Suppose $S = F_+[V](1/s)$ where $0 \neq s \in S$ is G fixed, and $R = S^G$. If S/R is G-Galois, then S/R is a local projective for $\mathscr{C}(G)$, the F class of G-Galois extensions.*

(d) *Let n be a positive integer and set $A' = R(F, n, r)$. If $s \in A'$ is in the center, and $A'(1/s) = A$ is Azumaya over its center C, then A/C is a local projective for $\mathscr{A}(n)$, the F class of Azumaya algebras of degree n.*

PROOF. (a) Let $\mathscr{M}/R$ and $\mathscr{N}/S$ be any objects, and let $0 \neq s \in R$. Then $\mathrm{Hom}(\mathscr{M} \otimes_R R(1/s), \mathscr{N}/S)$ can be identified with the subset of all $(\varphi, \psi) \in \mathrm{Hom}(\mathscr{M}/R, \mathscr{N}/S)$ such that $\varphi(s) \in S$ is a unit. With this observation (a) is easy. Using (a), parts (b), (c) and (d) are trivial. Q.E.D.

We end this section with just a little bit more terminology. Suppose $\mathscr{C}$ and $\mathscr{C}'$ are both F classes of the same type and $\mathscr{C} \subseteq \mathscr{C}'$. We say that $(\mathscr{C}, \mathscr{C}')$ have the lifting property if for every local F algebra T, M and every $\mathscr{M} \in \mathscr{C}$ over T/M there is a $\mathscr{M}'/T \in \mathscr{C}'$ such that $\mathscr{M}' \otimes_T T/M \cong \mathscr{M}$.

§2. Modules over a group

In later sections, we will be studying the function fields of algebraic tori, written $Q(L/K, M)$. They will be defined in §3, but note now that L/K here is a G-Galois extension, K is a field, and M is a $Z[G]$ module which is finitely generated free as an abelian group. In [27], [16], [8], [29] and [6], it was shown that $Q(L/K, M)$ can be studied via the G module properties of M. In this paper we will ask new questions about the $Q(L/K, M)$, and answer them by using some results on G modules. This section will deal exclusively with the necessary G module material.

In what follows, we will assume the reader is familiar with the basic reference [6], especially Section One. We will briefly review the definitions and some results. From now on all $Z[G]$ modules (also called G modules) will be assumed to be finitely generated free as abelian groups, unless stated otherwise. A *permutation* module is a $Z[G]$ module P such that P has a basis which is permuted by G. If $H \subseteq G$ is any subgroup, we can form the G module $Z[G/H]$ which has as a basis the cosets σH and upon which G acts in the obvious way. Any permutation module is a direct sum of the $Z[G/H]$'s for different H's. In what follows, the cohomology groups $H^n(G, M)$ will always be *Tate* cohomology groups and so will be defined for all integers n.

An *invertible* module is a direct summand of a permutation module. A *flasque* module is a G module M such that $H^{-1}(H, M) = 0$ for all subgroups $H \subseteq G$. If E is a flasque module, and $0 \to I \to M \to E \to 0$ is an exact sequence where I is invertible, then this exact sequence splits. It is shown in [6] that every G module M can be fitted into an exact sequence $0 \to M \to P \to E \to 0$ where P is a permutation module and E is a flasque module. Such a sequence is called a *flasque resolution* of M. For easy reference, we will state formally a result from [6], p. 181.

LEMMA 2.1. *Let $0 \to M \to P \to E \to 0$ be a flasque resolution and $f : M \to Q$ a G-map where Q is a permutation module. Then f extends to a G map $f' : P \to Q$.*

In [6], two modules M, M' were defined to be *similar* if $M \oplus P \cong M' \oplus P'$ for P, P' permutation modules. For our purposes, it is useful to define a slightly weaker equivalence relation. We will say that M, M' are *equivalent* if $M \oplus I \cong M \oplus I'$ for invertible G modules I, I'. We denote by $[M]$ the equivalence class of M under this equivalence relation. It was shown in [6] that if

$$0 \to M \to P \to E \to 0 \quad \text{and} \quad 0 \to M \to P' \to E' \to 0$$

are flasque resolutions, then E is similar to E'. Thus, if $\rho(M)$ is defined, as in [6],

to be the similarity class of E, ρ is well defined. We will modify this definition and set $\eta(M) = [E]$. Of course, η is also well defined. A large part of this section will be devoted to defining η on maps between G modules. The idea is that η is almost a functor. For technical reasons, we will define a genuine functor η' associated to η. It is the "quasi-functorial" properties of η that will allow us to settle some relative lifting problems.

Let M, M' be two G modules. Two G maps $f, f' : M \to M'$ are called equivalent if $f - f'$ factors through a permutation module. That is, if there is a permutation module P and G maps $g : M \to P$ and $h : P \to M'$ such that $h \circ g = f - f'$. We note without proof some easy facts about this relation. Let $g : M'' \to M$ and $h : M' \to M^*$ be G maps. If f is equivalent to 0 then so is $f \circ g$ and $h \circ f$. If $f', f : M \to M'$ are both equivalent to zero then so is $f + f'$ and $-f$. If $\mathrm{Id}_M : M \to M$ is the identity then Id_M is equivalent to 0 if and only if M is invertible. With these facts, it is easy to see that we have defined an equivalence relation on $\mathrm{Hom}_G(M, M')$. We denote by $[f]$ the equivalence class of f.

With this equivalence relation, we will define a quotient category as follows. Let $\mathcal{M}$ be the category of $\mathbf{Z}[G]$ modules which are finitely generated free over $\mathbf{Z}$. Let $\mathcal{E}$ be the full subcategory whose objects are flasque modules. Using the equivalence relation above, define $\mathcal{F}$ to be the quotient category of $\mathcal{E}$. That is, $\mathcal{F}$ has the same objects as $\mathcal{E}$ but $\mathrm{Hom}_{\mathcal{F}}(E, E')$ consists of equivalence classes, $[f]$, of maps. Note that $\mathcal{F}$ is an additive category and that 0 is the zero object for $\mathcal{F}$.

LEMMA 2.2. *Let E be a flasque module and I an invertible module. Denote by $i : E \to E \oplus I$ the canonical inclusion and $p : E \oplus I \to E$ the canonical projection. Then, in $\mathcal{F}$, $[i]$ is an isomorphism with inverse $[p]$.*

PROOF. $p \circ i$ is the identity on E and $i \circ p : E \oplus I \to E \oplus I$ maps E to E by the identity and maps I to 0. If $g = \mathrm{Id}_{E \oplus I} - i \circ p$, then g is 0 on E and so factors through I. Thus $[i] \circ [p] = [i \circ p] = [\mathrm{Id}_{E \oplus I}]$. Q.E.D.

The underlying idea is to try to define $\eta : \mathcal{M} \to \mathcal{F}$. This won't work because, in $\mathcal{F}$, equivalent things are isomorphic and not identical. Instead, we define $\eta' : \mathcal{M} \to \mathcal{F}$ as follows. For each M in $\mathcal{M}$, choose a flasque resolution (in an arbitrary way). If $f : M \to N$ is a morphism in $\mathcal{M}$, we have the following diagram where the horizontal maps are these chosen resolutions:

$$\begin{array}{ccccccccc} 0 & \to & M & \to & P & \to & E & \to & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} & & \\ 0 & \to & N & \to & Q & \to & D & \to & 0. \end{array}$$

Here g' exists by 2.1 and g is induced by g'. Then $\eta'(f)$ is $[g]$, by definition, and so $\eta'(M) = E$ and $\eta'(N) = E'$.

We must show η' does not depend on our choice of g'. So suppose $h' : P \to Q$ is another extension of f and $h : E \to D$ is the induced map. $g' - h'$ is zero on M and so induces a map $E \to Q$. $g - h$ is the composition of this map and the map $Q \to D$, and so $[g] = [h]$.

Next let us consider the dependence of η' on our choice of resolutions. Suppose $0 \to M \to P' \to E' \to 0$ and $0 \to N \to Q' \to D' \to 0$ are other flasque resolutions. We form the pushouts $P \oplus_M P'$ and $Q \oplus_N Q'$. By the basic properties of pushouts, there are exact sequences

$$0 \to P \to P \oplus_M P' \to E' \to 0 \quad \text{and} \quad 0 \to P' \to P \oplus_M P' \to E \to 0.$$

Since E and E' are flasque, $P \oplus_M P' \cong P \oplus E' \cong P' \oplus E$. Similarly, $Q \oplus_N Q' \cong Q \oplus D' \cong Q' \oplus D$. Also, there are exact sequences

$$0 \to M \to P \oplus P' \to P \oplus_M P' \to 0 \quad \text{and} \quad 0 \to N \to Q \oplus Q' \to Q \oplus_N Q' \to 0.$$

Let g', g be as above and choose $K' : P' \to Q'$ to be an extension of f. K' induces a G map $K : E' \to D'$. If we set

$$h' = g' \oplus k' : P \oplus P' \to Q \oplus Q',$$

then h' also extends f and induces a G map $h : P \oplus_M P' \to Q \oplus_N Q'$. An easy check shows that the following diagram commutes:

$$\begin{array}{ccccc} E & \longleftarrow & P \oplus_M P' & \longrightarrow & E' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle k} \\ D & \longleftarrow & Q \oplus_N Q' & \longrightarrow & D'. \end{array}$$

In $\mathcal{F}$, the horizontal maps are isomorphisms and so $[g]$ and $[k]$ differ by isomorphisms.

It is quite unpleasant to deal with η', since it depends on a choice of resolutions. What we will do, then, is abuse notation and write $\eta(M) = [\eta'(M)]$, $\eta(f) = [\eta'(f)]$ where we have identified morphisms in $\mathcal{F}$ which differ by isomorphisms. In the other sections of this paper, we will use η and not η'. This cannot lead to a contradiction because we are really only interested in whether $\eta(f)$ is $[0]$.

To summarize, then, $\eta(M) = [0]$ if and only if there is an exact sequence $0 \to M \to P \to I \to 0$ where P is a permutation module and I is invertible. Of

course, $\eta(\mathrm{Id}_M) = [0]$ if and only if $\eta(M) = [0]$. This next result gives a criterion for when $\eta(f) = [0]$ for any G map f.

THEOREM 2.3. *Let $f : M \to N$ be a G map. $\eta(f) = [0]$ if and only if there is a diagram, with the bottom row exact, as follows:*

$$\begin{array}{ccccccccc} & & & & M & & & & \\ & & & & {\scriptstyle f}\downarrow & \searrow & & & \\ 0 & \to & N & \to & N' & \to & Q & \to & 0 \end{array} \tag{2.4}$$

where P and Q are permutation modules.

PROOF. Suppose (2.4) is given. Let $0 \to M \to L \to E \to 0$ and $0 \to N' \to K \to D \to 0$ be flasque resolutions. By composition we can form the sequence $0 \to N \to K \to D' \to 0$. We note that D' is an extension of Q by D, so $D' \cong Q \oplus D$. Denote by f' the composition $M \to N \to N'$. If $g' : L \to K$ extends f', it also extends f. Thus if g' induces $g_1 : E \to Q \oplus D$ and $g_2 : E \to D$, then $\eta'(f)$ is $[g_1]$, up to isomorphism, and $\eta'(f')$ is $[g_2]$ up to isomorphism. We have:

$$\begin{array}{ccc} E & \longrightarrow & E \\ {\scriptstyle g_1}\downarrow & & \downarrow{\scriptstyle g_2} \\ Q \oplus D & \longrightarrow & D \end{array}$$

and so $[0] = [g_1]$ if and only if $[0] = [g_2]$. Now $\eta'(P)$ is isomorphic, in $\mathcal{F}$, to 0 and η' is a functor, so $\eta'(f') = [0]$ implying that $\eta'(f) = [0]$. By our abuse of notation (above), $\eta(f) = [0]$.

Conversely, suppose that $\eta(f) = [0]$. Choosing flasque resolutions for M and N we conclude that there is a diagram:

$$\begin{array}{ccccccccc} 0 & \to & M & \to & P & \to & E & \to & 0 \\ & & {\scriptstyle f}\downarrow & & \downarrow & & \downarrow{\scriptstyle P'} & & \\ 0 & \to & N & \to & Q & \to & D & \to & 0 \end{array}$$

where P, Q, and P' are permutation modules and E, D are flasque. Form the pullback $Q \times_D P'$ and insert it into the diagram. We have:

$$\begin{array}{ccccccccc} 0 & \to & M & \longrightarrow & P & \longrightarrow & E & \to & 0 \\ & & {\scriptstyle f}\downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & N & \to & Q \times_D P' & \to & P' & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & N & \longrightarrow & Q & \longrightarrow & D & \to & 0. \end{array}$$

Rewriting some of the maps above we have:

$$\begin{array}{ccccccc} 0 & \to & M & = & M & \to & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle P} & & \downarrow \\ 0 & \to & N & \to & Q \times_D P' & \to & P' \to 0. \end{array}$$

This proves the converse. Q.E.D.

We end this section with some calculations, the first of which will prove that $\eta(f) \neq [0]$ for a specific map f. Suppose $G' \subseteq G$ is a normal subgroup. Set $I_{G'} \subseteq Z[G]$ to be the left ideal generated by all elements of the form $\sigma - 1$ where $\sigma \in G'$.

PROPOSITION 2.5. *Let M be a G module, set $N = M/I_{G'}M$, and let $f : M \to N$ be the natural map. Then f factors through a permutation module if and only if N is invertible.*

PROOF. If N is invertible, then it is clear that f factors through a permutation module. Conversely, suppose f factors as $h \circ g$ where $g : M \to P$, $h : P \to N$, and where P is a permutation module. Since $I_{G'}N = 0$, h factors as $h_2 \circ h_1$ where $h_2 : P/I_{G'}P \to N$ and $h_1 : P \to P/I_{G'}P$. If $g' = h_1 \circ g : M \to P/I_{G'}P$, then g' factors through $N = M/I_{G'}M$. That is, $g' = g'' \circ f$ where $g'' : N \to P/I_{G'}P$. All in all, $h_2 \circ g'' = \mathrm{Id}_N$ since $h_2 \circ g'' \circ f = h_2 \circ g' = h \circ g = f$. Thus it suffices to show that $P/I_{G'}P$ is a permutation module. But $Z[G/H]/I_{G'}Z[G/H] = Z[G/G'H]$ and so we are done. Q.E.D.

For any finite group G, set J_G to be $Z[G]/Zt_G$ where $t_G = \Sigma_{\sigma \in G} \sigma$. If $N \subset G$ is a normal subgroup, there is a natural G map $J_G \to J_{G/N}$ where, of course, $J_{G/N}$ can be considered to be a G module. This map is defined by sending $1 + Zt_G \in J_G$ to $1 + Zt_{G/N} \in J_{G/N}$. The proof of the following result about the J_G's borrows a lot from the discussion in [6], p. 183.

THEOREM 2.6. *Let p be a prime and let G be a finite abelian p group of rank 2. Suppose $N \subset G$ is a subgroup such that G/N also has rank 2. If f is the map $J_G \to J_{G/N}$ defined above, then $\eta(f) \neq [0]$.*

PROOF. Let σ, τ be a basis for G such that $\sigma + N$ and $\tau + N$ are a basis for G/N. Consider the exact sequence $0 \to Z \to Z[G] \to Z[G] \oplus Z[G] \to E_G \to 0$ where Z is the G module with trivial action, $1 \in Z$ maps to $t_G \in Z[G]$ and $1 \in Z[G]$ maps to $(\sigma - 1, \tau - 1) \in Z[G] \oplus Z[G]$. E_G is defined by this sequence. Calling h the map $Z \to Z[G]$, we have that J_G is the cokernel of h. Thus we have two short exact sequences

$$0 \to Z \to Z[G] \to J_G \to 0 \quad \text{and} \quad 0 \to J_G \to Z[G] \oplus Z[G] \to E_G \to 0.$$

If $G' \subseteq G$ is a subgroup, $H^{-1}(G', E_G) = H^0(G', J_G) = H^1(G', Z) = (0)$. Hence E_G is flasque and $\eta(J_G) = [E_G]$. Similarly, there is a resolution

$$0 \to Z \to Z[G/N] \to Z[G/N] \oplus Z[G/N] \to E_{G/N} \to 0,$$

and $\eta(J_{G/N}) = [E_{G/N}]$. The natural map $Z[G] \oplus Z[G] \to Z[G/N] \oplus Z[G/N]$ induces a map $g : E_G \to E_{G/N}$ and $\eta(f) = [g]$. Explicitly, $E_G(E_{G/N})$ is $Z[G] \oplus Z[G]$ ($Z[G/N] \oplus Z[G/N]$) modulo the left submodule generated by $(\sigma - 1, \tau - 1)$ $((\sigma N - N, \tau N - N))$. It is now easy to see that $E_G / I_N E_G = E_{G/N}$ and g is the natural map. By 2.5, it suffices to show that $J_{G/N}$ is not invertible. This was shown in [6]. Simply outlined,

$$H^1(G/N, E_{G/N}) \cong H^2(G/N, J_{G/N}) \cong H^3(G/N, Z) \neq 0. \qquad \text{Q.E.D.}$$

In the theory of algebras, the following G module is of particular interest. Let G be a finite group and let P be a free $Z[G]$ module with basis $\{\tilde{c}(\sigma, \tau) \mid 1 \neq \sigma, \tau \in G\}$. Consider $R \subset P$ to be the left $Z[G]$ submodule generated by all expressions of the form

$$\tilde{c}(\sigma, \tau) + \tilde{c}(\sigma\tau, \eta) - \sigma(\tilde{c}(\tau, \eta)) - \tilde{c}(\sigma, \tau\eta) \qquad \text{for all } \sigma, \tau, \eta \in G,$$

where we have set $\tilde{c}(1, \sigma) = \tilde{c}(\sigma, 1) = 0$. Define $M_2(G) = P/R$. One should think of $M_2(G)$ as the module generated by a "generic" two cocycle of G.

Set $c(\sigma, \tau) = \tilde{c}(\sigma, \tau) + R \in M_2(G)$. The form of the relations in R makes it clear that $M_2(G)$ is a free Z module with basis $\{c(\sigma, \tau) \mid 1 \neq \sigma, \tau \in G\}$. Note that if $H \lhd G$ is a normal subgroup, there is a natural G module map $M_2(G) \to M_2(G/H)$ defined by sending $c(\sigma, \tau)$ to $c(\sigma H, \tau H)$. Our final result of this section will be a study of the $M_2(G)$'s in a special case. In [2], a study of abelian crossed product algebras was made using a description of abelian crossed products that is essentially due to Dickson. Here we are going to perform an analogous argument for G modules, but restricting ourselves to rank 2 abelian groups. So let G be an abelian group with generators σ, τ such that $G = \langle\sigma\rangle \oplus \langle\tau\rangle$. We first consider the following module. Let

$$H = \langle\sigma\rangle, \quad K = \langle\tau\rangle, \quad \text{and} \quad Q = Z[G] \oplus Z[G/H] \oplus Z[G/K].$$

Consider $R' \subset Q$ to be the left submodule generated by $(1 + \sigma + \cdots + \sigma^{n-1}, \tau H - H, 0)$ and $(1 + \tau + \cdots + \tau^{m-1}, 0, \sigma K - K)$, where n is the order of σ and m is the order of τ. Set $N = Q/R'$. We can think of N as the module generated by u, b, c subject to the relations

$$\sigma(b)=b, \quad \tau(c)=c, \quad (1+\sigma+\cdots+\sigma^{n-1})u=\tau(b)-b,$$

$$\text{and} \quad (1+\tau+\cdots+\tau^{m-1})u=\sigma(c)-c.$$

The result of Dickson (appearing in [2]) has as a special case that any crossed product algebra $\Delta(L/F, G, d)$ can be described via u', b', $c' \in L^*$ which satisfy exactly these relations. More precisely, let

$$\Delta(L/F, G, d)=\bigoplus_{\eta\in G} Lu_\eta$$

where $u_\eta u_\delta = d(\eta, \delta)u_{\eta\delta}$ and $u_\eta z = \eta(z)u_\eta$ for all $z \in L$. If we set

$$u'=u_\sigma u_\tau u_\sigma^{-1}u_\tau^{-1}, \quad b'=(u_\sigma)^{-n}, \quad \text{and} \quad c'=(u_\tau)^m,$$

then u', b', c' are as claimed (but note that L^* is a multiplicatively written G module). In terms of the cocycle d,

$$u'=d(\sigma,\tau)d(\tau,\sigma)^{-1}, \quad c'=d(\tau,\tau)d(t^2,\tau)\cdots d(\tau^{m-1},\tau)$$

$$\text{and} \quad b'=(d(\sigma,\sigma)d(\sigma^2,\sigma)\cdots d(\sigma^{n-1},\sigma))^{-1}.$$

In pure module terms, there is a G map $g: N \to M_2(G)$ defined by setting

$$g(u)=c(\sigma,\tau)-c(\tau,\sigma), \quad g(b)=-c(\sigma,\sigma)-c(\sigma^2,\sigma)-\cdots-c(\sigma^{n-1},\sigma)$$

and

$$g(c)=c(\tau,\tau)+\cdots+c(\tau^{m-1},\tau).$$

To show that g is well defined, one must show that these elements satisfy the relations defining R'. To avoid doing this directly, one can take L/K a G Galois extension of fields, set $K'=Q(L/K, M_2(G))$ (which will be defined in §3) and $L'=L\otimes_K K'$. Now use the $c(\eta,\delta)$ which generate $M_2(G)$ to define a crossed product $\Delta(L'/K', G, c)$, and then quote [2].

Next we consider $M_2(G)/g(N)=M'$. Set $c'(\eta,\delta)=c(\eta,\delta)+g(N)$. Considering the algebra case, we see that the cocycle c' must be split. In fact, an easy argument (one can use algebras again) shows that the necessary coboundary can be defined as follows. Set

$$d(1)=1, \quad d(\sigma)=1, \quad d(\tau)=1,$$

$$d(\sigma^i)=c'(\sigma,\sigma)c'(\sigma^2,\sigma)\cdots c'(\sigma^{i-1},\sigma) \qquad \text{for } i>1,$$

$$d(\tau^j)=c'(\tau,\tau)\cdots c(\tau^{j-1},\tau) \qquad \text{for } j>1,$$

and

$$d(\sigma^i\tau^j) = c'(\sigma,\sigma)\cdots c(\sigma^{i-1},\sigma)c(\tau,\tau)\cdots c(\tau^{j-1},\tau) \qquad \text{for } i,j>1.$$

Then for any ε, $\delta \in G$, $c'(\varepsilon,\delta) = d(\varepsilon) + \varepsilon d(\delta) - d(\varepsilon\delta)$. In particular, M' is generated over $Z[G]$ by the $d(\varepsilon)$'s.

We further analyse this situation as follows. Define $H : J_G \to N$ by setting $h(1+Zt_G) = u$. Then $N/h(J_G)$ is easily seen to be isomorphic to $Z \oplus Z$. Let q be the order of G. $M_2(G)$ has Z rank $(q-1)^2$. N is generated by $q+1$ elements over Z. Thus M' has Z rank greater than or equal to $(q-1)^2-(q+1) = q(q-3)$. It follows that M' is a free $Z[G]$ module with basis $\{d(\varepsilon) \mid \varepsilon \neq 1, \sigma, \tau\}$, g is an injection, N is a free Z module of rank $q+1$, and h is an injection.

THEOREM 2.7. *Let G be a finite abelian group $\langle\sigma\rangle \oplus \langle\tau\rangle$ as above.*

(a) $\eta(J_G) = \eta(M_2(G))$.

(b) *Suppose $H \subseteq G$ is a subgroup such that $G/H = \langle\sigma H\rangle \oplus \langle\tau H\rangle$. Let $f : J_G \to J_{G/H}$ and $g : M_2(G) \to M_2(G/H)$ be the canonical maps. Then $\eta(g) = \eta(f) \neq [0]$.*

PROOF. Part (a) is done above and (b) is an easy diagram chase. Q.E.D.

§3. Retract rational extensions

In this section we begin the core of this paper; the study of a class of field extensions called retract rational. These extensions were first introduced in [25], where some of the results we are about to present were stated, and occasionally given sketchy proofs. Here we will use the general language of §1 to give complete and very general proofs of the result in [25].

As we are about to see, the concept of retract rationality arises naturally when one studies lifting problems. To motivate the definition to come, recall that a rational (or purely transcendental) field extension K/F is one where K contains $x_1, \cdots, x_n$ algebraically independent over F and $K = F(x_1, \cdots, x_n)$. It is useful to think of K as a "free" object with basis $x_1, \cdots, x_n$. Retract rational extensions correspond to projective objects.

DEFINITION 3.1. Let $K \supseteq F$ be fields. K/F is called *retract rational* if and only if K is the quotient field of an F algebra domain $S \subseteq K$, such that there are F algebra maps

$$\varphi : S \to F[x_1, \cdots, x_n](1/w) \quad \text{and} \quad \psi : F[x_1, \cdots, x_n](1/w) \to S$$

where $F[x_1, \cdots, x_n](1/w)$ is a localized polynomial ring and $\psi \circ \varphi$ is the identity on S.

Retract rationality often corresponds to the lifting property of a single F class. Later on, we will study a relative lifting problem between two F classes. The corresponding field theory concept will be defined next.

DEFINITION 3.2. Let S, R be F algebra domains, and let $\varphi : S \to R$ be an F algebra map. We say φ *factors rationally* if and only if there is a localized polynomial ring $F[x_1, \cdots, x_n](1/w)$, a $0 \neq r \in R$, and F algebra maps

$$\psi : S \to F[x_1, \cdots, x_n](1/w) \quad \text{and} \quad \eta : F[x_1, \cdots, x_n](1/w) \to R(1/r)$$

such that $\varphi = \eta \circ \psi$.

Let us make a few elementary definitions and observe a few easy facts. If S, T are F algebras, and $\varphi : S \to T$; $\psi : T \to S$ are F algebra maps such that $\psi \circ \varphi = \mathrm{Id}_S$, we say that S is a (ψ, φ) retraction of T. If the maps need not be specified, S is just called a retraction of T. If T has the form $F[x_1, \cdots, x_n](1/w)$, we say S is a localized polynomial retraction. Suppose S, T are domains and S is a (ψ, φ) retraction of T. If $0 \neq s \in S$, then $S(1/s)$ is a retraction of $T(1/\varphi(s))$ via the unique extensions of ψ and φ. More generally, if $\varphi : S \to T$ factors rationally, and $s \in S$ satisfies $\varphi(s) \neq 0$, then the unique extension of φ to $\varphi : S(1/s) \to T(1/\varphi(s))$ factors rationally. Also, the relation of retraction is transitive. That is, if S is a retraction of T and T is of R, then S is a retraction of R, via the obvious maps. If S is a retraction of T, then clearly $S[x_1, \cdots, x_n]$ is a retraction of $T[x_1, \cdots, x_n]$.

The effect of the above observations is that, to some extent, the definitions 3.1 and 3.2 are independent of the domains involved. But to make this clearer, we present a result of Swan's. For convenience, we include a proof.

LEMMA 3.3. [27] *Let $F \subseteq K$ be fields, and let $S_1, S_2 \subset K$ be affine F subalgebras such that $q(S_i) = K$. Then there are $0 \neq s_1 \in S_1$ and $0 \neq s_2 \in S_2$ such that $S_1(1/s_1) = S_2(1/s_2)$.*

PROOF. Since S_1 is finitely generated, there is a $0 \neq s_2' \in S_2$ such that $S_1 \subseteq S_2(1/s_2')$. Since $S_2(1/s_2')$ is finitely generated, there is an $s_1 \in S_1$ such that $S_2(1/s_2') \subseteq S_2(1/s_1)$. But $s_1 = t/(s_2')^n$ for some positive integer n and some $0 \neq t \in S_2$. We now claim that $S_1(1/s_1) = S_2(1/s_2)$ where $s_2 = s_2't$. Note first that $S_2(1/s_2) = S_2(1/s_2')(1/t)$. So, in order to show that $S(1/s_1) \supseteq S_2(1/s_2)$, it suffices to note that

$$1/t = (1/s_1)(1/s_2')^n \in S_1(1/s_1).$$

In order to show that $S_1(1/s_1) \subseteq S_2(1/s_2)$, we observe that $1/s_1 = (s_2')^n/t \in S_2(1/s_2)$.

Q.E.D.

Combining this lemma and the observations preceding it, we conclude the following.

COROLLARY 3.4. *If K/F is retract rational, and $S \subseteq K$ is an affine F subalgebra such that $q(S) = K$, then for some $0 \neq s \in S$, $S(1/s)$ is a localized polynomial retract.*

Now is a good time to notice a useful fact which was part of the proof of 3.3. Let S'' be a domain with $q(S'') = K$. For some $0 \neq s'' \in S''$, set $S' = S''(1/s'')$. Repeat the process for some $0 \neq s' \in S'$. That is, set $S = S'(1/s')$. But now notice that S also has the form $S''(1/t)$. In fact, if $s' = t'/(s'')^n$ then $S = S''(1/s''t')$.

Up to now, we have implied that the concept of factoring rationally is a generalization of retract rationality. We make this precise in the next lemma.

LEMMA 3.5. *Let S be an affine F algebra domain and set $K = q(S)$. K/F is retract rational if and only if the identity $i : S \to S$ factors rationally.*

PROOF. If K/F is retract rational, it follows by 3.4 that for some $0 \neq s \in S$, $S(1/s)$ is a localized polynomial retract. In other words, the inclusion $i : S \to S(1/s)$ factors through a localized polynomial ring. Conversely, suppose that there are $0 \neq s \in S$,

$$\varphi : S \to F[x_1, \cdots, x_n](1/w) \quad \text{and} \quad \psi : F[x_1, \cdots, x_n](1/w) \to S(1/s)$$

such that $\psi \circ \varphi = i$. Set $v = \varphi(s)$ and note that $\psi(v) = s$. Thus φ extends uniquely to

$$\varphi : S(1/s) \to F[x_1, \cdots, x_n](1/wv)$$

and ψ extends uniquely to

$$\psi : F[x_1, \cdots, x_n](1/wv) \to S(1/s).$$

Now $\psi \circ \varphi$ must be the identity on $S(1/s)$, so $S(1/s)$ is a localized polynomial retract. Q.E.D.

We will now review some classical kinds of field extensions, and begin to see where retract rational extensions fit in. A field extension, K/F, is called unirational if $K \subseteq L$, where L/F is a rational field extension. An immediate consequence of the definition is that every retract rational extension is unirational. Already in [25], and again in Theorem 4.12 to come, examples are presented which show the converse false.

Two fields, K, L, are called stably isomorphic over F if there is an isomorphism $K(y_1, \cdots, y_n) \cong L(z_1, \cdots, z_m)$ over F, where the y's and z's are

indeterminants. An extension K/F is called stably rational if K is stably isomorphic, over F, to a rational extension of F. We are about to show that stably rational implies retract rational. More so, we are about to show that retract rationality respects stable isomorphism. But before we state the result, let us again point out that the converse is false. Swan showed that if $G = C_{47}$ is the cyclic group of order 47, and K is the field of invariants (under the obvious action) of G on $Q(x_g \mid g \in G)$ then K/Q is not stably rational. However, as was pointed out in [25], and will be stated below, K/Q is retract rational.

PROPOSITION 3.6. (a) *Let K, L be fields which contain F and are stably isomorphic over F. If L/F is retract rational, then so is K/F.*

(b) *Let S, T, and T' be F algebra domains, where $T \subseteq T'$. Assume $\varphi : S \to T$ is an F algebra map, and assume that $q(T')/q(T)$ is rational. If the composition $S \to T \to T'$ factors rationally, then so does φ.*

We begin this proof by stating and proving a lemma, which follows.

LEMMA 3.7. *Suppose S is an F algebra domain, and $T = S[x_1, \cdots, x_n](1/s)$ for some $0 \neq s \in S[x_1, \cdots, x_n]$. Then for some $0 \neq s' \in S$, $S(1/s')$ is a (ψ, φ) retraction of $T(1/s')$, where φ is the inclusion.*

PROOF OF LEMMA. Since F is infinite, there is an F algebra homomorphism $\psi : S[x_1, \cdots, x_n] \to S$ such that $s' = \psi(s) \neq 0$, and such that ψ is the identity on S. In fact, $\psi(x_i)$ can be chosen in F. This map ψ extends uniquely to an F algebra map

$$\psi : T = S[x_1, \cdots, x_n](1/s) \to S(1/s').$$

We may consider s' as an element of T and note that ψ extends to $\psi : T(1/s') \to S(1/s')$, where ψ is the identity on $S(1/s')$. In other words, if φ is the inclusion $S(1/s') \subset T(1/s')$, $S(1/s')$ is a (ψ, φ) retraction of $T(1/s')$. Q.E.D.

We now return to the proof of 3.6. To begin with (a), say $L = q(S)$ where S is a retraction of $F[x_1, \cdots, x_m](1/w)$. Hence $S[z_1, \cdots, z_n]$ is a retraction of $F[x_1, \cdots, x_m, z_1, \cdots, z_n](1/w)$. Of course,

$$q(S[z_1, \cdots, z_n]) = L(z_1, \cdots, z_n).$$

Thus we may assume $K(y_1, \cdots, y_n) = L$ where L/F is retract rational. Suppose $K = q(T)$ where T is an affine F algebra. By 3.4, there is a $0 \neq t \in T[y_1, \cdots, y_n]$ such that $T[y_1, \cdots, y_n](1/t)$ is a localized polynomial retract. But by Lemma 3.7, some $T(1/t')$ is a retraction of $T[y_1, \cdots, y_n](1/tt')$. By the basic properties

mentioned above of retractions, this later algebra is also a localized polynomial retraction. Then we are done by the "transitivity" of retractions.

To prove (b), assume $t' \in T'$ is such that the map $S \to T'(1/t')$ factors through a localized polynomial ring. By Swan's lemma, we may assume

$$T'(1/t') = T[y_1, \cdots, y_n](1/t) \qquad \text{for some } 0 \neq t \in T[y_1, \cdots, y_n].$$

To be explicit, assume the given map $\varphi' : S \to T[y_1, \cdots, y_n](1/t)$ factors into

$$\psi : S \to F[x_1, \cdots, x_m](1/w) \quad \text{and} \quad \eta : F[x_1, \cdots, x_m](1/w) \to T[y_1, \cdots, y_n](1/t).$$

For some $0 \neq s \in T$, we know by 3.7 that $T(1/s)$ is a (δ, i) retraction of $T[y_1, \cdots, y_n](1/ts)$, where i is the inclusion. Hence, as maps from S to $T(1/s)$, $\varphi = \delta \circ \varphi'$. Thus φ is the composition of ψ and

$$\delta \circ \eta : F[x_1, \cdots, x_m](1/w) \to T(1/s). \qquad \text{Q.E.D.}$$

We have now covered most of the (known) elementary or basic properties of retract rational fields. What is lacking is a clearer reason why retract rationality is analogous to projectivity. This is the point of the next result. Before presenting this result, let us make two comments. What the following result does not do is make retract rationality exactly projectivity in some category. This may be possible, and also may be fruitful. Second, the following result has a form that will be repeated. We will first state (for clarity) a result about retract rational fields, and then state an analogous, more general result for rationally factoring maps. Though the first statement will seem more intuitive, the second, more general statement, is necessary for one of our applications.

THEOREM 3.8. *Let K/F be an extension of fields. The following are equivalent:*

(i) *K/F is retract rational.*

(ii) *K is the quotient field of an affine F algebra S which satisfies the following condition. Suppose T, M is a local F algebra, $L = T/M$, $\rho : T \to L$ is the canonical map, and $\varphi : S \to L$ is an F algebra map. Then there is an F algebra map $\varphi' : S \to T$ such that $\rho \circ \varphi' = \varphi$.*

The proof of the above theorem will be encompassed in the following more general result.

THEOREM 3.9. *Let $\varphi : S \to R$ be an F algebra map between F algebra domains. Then the following are equivalent.*

(i) *φ factors rationally.*

(ii) *There is a $0 \neq r \in R$ such that the induced map $\varphi : S \to R(1/r)$ has the*

following property. Suppose T, M is a local F algebra, $L = T/M$, $\rho : T \to L$ is the canonical map, and $\psi : R(1/r) \to L$ is any F algebra map. Then there is an F algebra map $\psi' : S \to T$ such that $\rho \circ \psi' = \psi \circ \varphi$.

PROOF. First, let us show how 3.9 implies 3.8. If K/F is retract rational and $K = q(S)$ where S is a localized polynomial retract, then the identity $i : S \to S$ factors rationally. Quoting 3.9(ii), we have that some $S(1/s)$ has the property 3.8(ii). (Actually, S itself satisfies 3.8(ii), but this is not important and only occurs because of our choice for the form of 3.9.) Conversely, suppose 3.8(ii) holds for such S. By 3.9, the identity $i : S \to S$ factors rationally and 3.5 finishes the argument.

Turning now to the proof of 3.9, let us assume 3.9(i). Explicitly, we assume φ is the composition of

$$\eta : S \to F[x_1, \cdots, x_n](1/w) \quad \text{and} \quad \delta : F[x_1, \cdots, x_n](1/w) \to R(1/r).$$

If T, M, L, ρ, and ψ are as given in 3.9(ii), set $a_i = \psi(\delta(x_i))$. Choose $b_i \in T$ to be preimages of the a_i. Define $\mu : F[x_1, \cdots, x_n](1/w) \to T$ by $\mu(x_i) = b_i$. $\mu(w)$ is a unit because $\rho(\mu(w)) = \psi(\delta(w)) \neq 0$. If we now set $\psi' = \mu \circ \eta$, ψ' is the required map.

Conversely, assume 3.9(ii). Since $R(1/r)$ is affine, there is an F algebra surjection $\eta : F[x_1, \cdots, x_n] \to R(1/r)$. Let P be the kernel of η, and form the local ring $F[x_1, \cdots, x_n]_P = T$. If M is the maximal ideal of T, and K is the quotient field of R, then $T/M = K$. η extends to the map $\eta : T \to K$. Applying 3.9(ii) to the inclusion $i : R(1/r) \to K$, we have an F algebra map $\psi : S \to F[x_1, \cdots, x_n]_P = T$ such that $\eta \circ \psi = i \circ \varphi$. Since S is affine,

$$\psi(S) \subset F[x_1, \cdots, x_n](1/w) \qquad \text{for some } w \notin P.$$

Also, η yields a surjection

$$\eta : F[x_1, \cdots, x_n](1/w) \to R(1/rv) \qquad \text{where } v = \eta(w).$$

In all, $\varphi : S \to R(1/rv)$ is the composition of ψ and η. Q.E.D.

REMARK. Assume $q(R)/F$ is separably generated. Note that, in the proof that 3.9(ii) implies 3.9(i), it is then only necessary to consider T, M which are discrete valuation rings. This is because the T, M which occur in the proof are, first of all, nonsingular. But more so, by changing $R(1/r)$ to $R(1/rr')$ if necessary, we can write $R(1/r)$ as the image of some $F[x_1, \cdots, x_n](1/s)$ where n is less than or equal to one plus the Krull dimension of R. With this choice, the T, M that has to be treated is a discrete valuation ring.

Up to now, we have presented the properties of retract rational extensions without reference to lifting problems or F classes. However, 3.8 makes it clear that lifting problems are closely related to retract rationality. The next corollary states the precise connection. It is this connection, for some specific F classes, which led the author to consider retract rationality, and is the main justification for the concept's introduction. This next corollary is stated in the general language of §1. It should be thought of as an outline, which can be applied to proving lifting properties or retract rationality in some very concrete situations. Two examples will follow, and a third will come later in this paper. Once again, we will state the more intuitive fact about retract rationality first, and then the more general fact about rationally factoring maps.

COROLLARY 3.10. (a) *Let $\mathscr{C}$ be an F class, $\mathscr{P}/R \in \mathscr{C}$ a local projective object which is also densely representing. If K is the quotient field of R, then $\mathscr{C}$ has the lifting property if and only if K/F is retract rational.*

(b) *Let $\mathscr{C} \subseteq \mathscr{C}'$ be F classes of the same type, let $\mathscr{M}/R \in \mathscr{C}$ be a densely representing object, and let $\mathscr{P}/S \in \mathscr{C}'$ be a local projective object. Suppose r, S are F algebra affine domains, and $\varphi : S \to R$ is an F algebra map such that $\mathscr{M} \cong \mathscr{P} \otimes_\varphi R$ over R. Then $(\mathscr{C}, \mathscr{C}')$ has the (relative) lifting property if and only if φ factors rationally.*

PROOF. As before, (a) is a special case of (b). As for (b), assume $(\mathscr{C}, \mathscr{C}')$ has the lifting property. It is now very easy to see, using all the givens, that $\varphi : S \to R$ satisfies the condition 3.9(ii). Conversely, suppose φ factors rationally. Specifically, suppose $\varphi : S \to R(1/r)$ satisfies 3.9(ii). Every $\mathscr{N}/K \in \mathscr{C}$, for K a field, is a specialization of $\mathscr{M} \otimes_R R(1/r)$. Then 3.9(ii) implies that the lifting property holds. Q.E.D.

We can now give two examples of the use of 3.10. Our first example will involve the F class of Azumaya algebras of degree n, which we recall was labelled $\mathscr{A}(F, n)$. Also recall that $Z(F, n, r)$ is the center of the generic division algebra $\mathrm{UD}(F, n, r)$.

THEOREM 3.11. *$Z(F, n, r)/F$ is retract rational if and only if $\mathscr{A}(F, n)$ has the lifting property. That is, if and only if for every local commutative F algebra T, M, and every simple F algebra A of degree n over its center $K = T/M$, there is an Azumaya algebra B/T such that $B \otimes_T K \cong A$.*

PROOF. By 3.10, we must present an appropriate densely representing local projective object. Let $A' = R(F, n, r)$ be the ring of generic matrices with center

C'. There is a $0 \neq s' \in C'$ such that $A = A'(1/s')$ is Azumaya over its center $C = C'(1/s')$. As A is finite as a module over C, an exercise (called the Artin–Tate lemma) shows that C is affine. By 1.3, A/C is a local projective object. A/C is also densely representing. If $0 \neq t \in C$, we can write $C(1/t) = C'(1/s)$ for some $0 \neq s \in C'$. If B is a central simple algebra over $K \supseteq F$ of degree n, then by e.g. [13], page 92, there is an F algebra map $\psi : A' \to B$ such that $\psi(s) \in K$ is nonzero. Thus ψ extends to a map $\psi : A \otimes_C C(1/t) \to B$. Let $\varphi : C(1/t) \to K$ be the restriction of ψ. Since A/C is Azumaya, ψ induces an isomorphism $A(1/t) \otimes_\varphi K \cong B$. Q.E.D.

Our second application of 3.10 is to F classes of Galois extensions. Recall that the F class of all Galois extensions with group G was denoted $\mathscr{E}(G)$. Now let V be a finite dimensional left $F[G]$ module such that the map $G \to \mathrm{Hom}_F(V, V)$ is an injection. Form the symmetric algebra $F_+[V]$, and its quotient field $F_+(V)$. G acts on $F_+(V)$ in the obvious way.

THEOREM 3.12. *$F_+(V)^G/F$ is retract rational if and only if $\mathscr{E}(G)$ has the lifting property.*

PROOF. Once again, we must present a local projective densely representing object. By our assumptions, G acts faithfully on $F_+(V)$ and so $F_+(V)/F_+(V)^G$ is G Galois. Set $R'' = F_+[V]^G$. Since R'' has quotient field $F_+(V)^G$, there is an $0 \neq r'' \in R''$ and a subalgebra $S' \subseteq F_+(V)$ such that if $R' = R''(1/r'')$, then S'/R' is Galois with group G, R' is affine and $S'F_+(V)^G = F_+(V)$ (see [23], p. 274). By Swan's lemma, there are $0 \neq s' \in S'$ and $0 \neq s \in F_+[V]$ such that $S'(1/s') = F_+[V](1/s)$. Let r' be the G norm of s' and r the G norm of s. $S'(1/r')$ and $F_+[V](1/r)$ are both closed under the G action. It follows that $1/r' \in F_+[V](1/r)$ and $1/r \in S'(1/r')$. Hence $S'(1/r') = F_+[V](1/r)$. All in all we have $R = F_+[V]^G(1/r)$ and $S = F_+[V](1/r)$ such that S/R is Galois with group G and R is affine.

By 1.3, S/R is a local projective object. It remains to show that S/R is densely representing. As a first step, we note that it suffices to prove the following claim. Suppose $K \supseteq F$ is a field, L/K is G Galois, and $0 \neq s \in F_+[V]$. Then there is an F algebra map $\varphi : F_+[V] \to L$ such that φ preserves the G action and $\varphi(s) \neq 0$. This claim suffices because if $r_1 \in R$, we choose such a φ with $\varphi(rr_1) \neq 0$. Hence φ induces a G preserving map $\varphi : F_+[V](1/rr') \to L$ and φ restricts to a map $\psi : R(1/r') \to K$. Finally, φ induces a K linear epimorphism from $S \otimes_\psi K$ to L, which is an isomorphism by checking dimensions.

Thus it suffices to prove the claim. Using duality over F, it is easy to see that

there is a free $F[G]$ module W such that $V \subseteq W$. Since we can consider $F_+[V] \subseteq F_+[W]$, it suffices to prove the claim for the free module $W.K$ Also, since $F_+[W] \subseteq L_+[W]$, it suffices to prove the claim for $L_+[W]$. But $L_+[W]$ is nothing but a polynomial ring of the form $L[x_{i,g} \mid 1 \leqq i \leqq n \text{ and } g \in G]$, where G acts on the $x_{i,g}$'s in the usual way, and G acts on L. If W has rank one (i.e. $n = 1$), our claim is just the Dedekind independence theorem for L/K (see [13], p. 283). For general W, let $s \in L_+[W]$. By the rank one case, there are $a_g \in L$ such that

$$g(a_h) = a_{gh} \quad \text{and} \quad s(a_g, \cdots, a_h, x_{2,g}, \cdots, x_{2,h}, x_{3,g}, \cdots, x_{n,h}) \neq 0.$$

We can proceed by induction to prove the claim. Q.E.D.

Later on in this paper we will prove the lifting property for Azumaya algebras of prime degree and therefore, by 3.11, show that $Z(F, p, r)/F$ is retract rational. In [23], generic objects were constructed for Galois extensions with abelian Galois group over certain F. These F classes have the lifting property, and we have the following corollary.

COROLLARY 3.13. *Let A be a finite abelian group, and 2^r the highest power of 2 dividing the exponent of A. Assume F is a field such that either F has characteristic 2 or $F(\rho)/F$ is cyclic where ρ is a primitive 2^r root of one. Suppose V is a finitely generated $F[A]$ module such that $A \to \mathrm{Hom}_F(V, V)$ is injective. Then $F(V)^A/F$ is retract rational.*

In [23], it was shown that if the exponent of A is a multiple of 8, then there is no generic object for A-Galois extensions over the rational field Q. Thus, $Q(V)^A/Q$ is not retract rational. One is thus led to ask as to exactly when $F(V)^A/F$ is retract rational. The answer, to be given later, is that if $F(\rho)/F$ is not cyclic, then $F(V)^A/F$ is not retract rational.

Up till now, the only way to show that a field extension is not retract rational is to invoke 3.10 and some failed lifting problem. This does not, however, seem sufficient to product results like the one mentioned in the above paragraph. An examination of the previous work [16], [8], [29], [6], etc. makes it clear that it is important for these problems to examine so-called function fields of algebraic tori. In the rest of this section we will discuss these function fields and determine exactly when they are retract rational. This will allow us to solve problems of the type mentioned above.

For our purposes, it suffices to describe these function fields as follows. Let G be a finite group, and L/F a Galois extension with group G. Let M be a $Z[G]$ module. As in §2, this will always include the assumption that M is finitely

generated free as a Z module. Form the group algebra (not the symmetric algebra!) $L[M]$. This is a domain, with quotient field we denote by $L(M)$. G acts on $L[M]$ by acting on L and M, and so G acts on $L(M)$. The field we are interested in is denoted by $Q(L/F, M)$ and is equal to the fixed field $L(M)^G$.

It has been amply demonstrated in [27], [16], [8], [29], [6], that the fields $Q(L/F, M)$ can be studied via groups of units of affine subrings of $L(M)$. We now give an extremely brief summary of this theory, making use of the notation of §2. This summary will follow the exposition in [6], and we refer the reader to this source for further details. Recall that if M is a $Z[G]$ module, and $0 \to M \to P \to E \to 0$ is a flasque resolution of M, then $\rho(M)$ is defined to be the similarity class of E.

Before continuing, let us make some notational remarks. For any ring R, we denote by R^* the group of units of R. M, which in §2 was always written additively, is a subgroup of the multiplicative group $L[M]^*$. We therefore must make the convention that when viewed as contained in $L[M]$, M will be written multiplicatively. Otherwise, we will stick to the additive notation of §2.

The study of the fields $Q(L/F, M)$ starts with the observation that if $S = L[M]$, then as G modules, $S^*/L^* \cong M$. In fact, if $S \subset L(M)$ is any affine, G invariant unique factorization domain with quotient field $L(M)$, then $\rho(S^*/L^*) = \rho(M)$. Also, $Q(L/F, M)$ is stably isomorphic to $Q(L/F, N)$ over F if and only if $\rho(M) = \rho(N)$. In particular, $Q(L/F, M)$ is stably rational if and only if $\rho(M) = 0$. In the proof of these facts it is observed that if P is a permutation module, then $L[P]^G$ is a localized polynomial ring. Note now that the same argument shows that $L[P]^G$ is a localized polynomial ring over F even when L is not a field, but only Galois over F.

With the questions we wish to answer, it turns out to be appropriate to examine the relationship between the fields $Q(L/F, M)$ and the map η, as defined in §2. The main result along these lines is next.

THEOREM 3.14. *Let G, M, and L/F be as above.*

(a) *$Q(L/F, M)$ is retract rational if and only if $\eta(M) = [0]$.*

(b) *Let $f : M \to N$ be a map of G modules and $\varphi : L[M]^G \to L[N]^G$ the induced map of F algebras. Then φ factors rationally if and only if $\eta(f) = [0]$.*

PROOF. It suffices to prove (b), since (a) is the special case $f = \mathrm{Id}_M$. So assume φ factors rationally. That is, assume that there is a $0 \neq s \in L[N]^G$ and F algebra maps

$$\psi : L[M]^G \to F[x_1, \cdots, x_n](1/w), \quad \delta : F[x_1, \cdots, x_n](1/w) \to L[N]^G(1/s)$$

such that $\delta \circ \psi = \varphi$. Tensoring by L we have G preserving F algebra maps $\varphi' : L[M] \to L[N]$, $\psi' : L[M] \to L[x_1, \cdots, x_n](1/w)$ and

$$\delta' : L[x_1, \cdots, x_n](1/w) \to L[N](1/s)$$

such that $\delta' \circ \psi' = \varphi'$. All three of these maps restrict to G module maps on the groups of units modulo L^*. We note that $L[M]^*/L^* \cong M$, $L[x_1, \cdots, x_n](1/w)^*/L^*$ is a permutation module we will call P, and $N' = L[N](1/s)^*/L^*$ fits into an exact sequence $0 \to N \to N' \to Q \to 0$ of G modules where Q is a permutation module. All our maps together constitute the following diagram of G modules, with the row on the bottom being exact:

(3.15)
$$\begin{array}{ccccccccc} & & & & M & & & & \\ & & & & \downarrow f & \searrow P & & & \\ 0 & \longrightarrow & N & \longrightarrow & N' & \longrightarrow & Q & \longrightarrow & 0 \end{array}$$

Thus by 2.3 we have $\eta(f) = [0]$.

Conversely, suppose $\eta(f) = [0]$. By 2.3, there is a diagram (3.15). Let φ' be the induced map $L[M]^G \to L[N']^G$. φ' factors through $L[P]^G$, which is a localized polynomial ring. Finally, $L(N')^G/L(N)^G$ is a rational field extension (see proof of theorem 6.8 of [28]), so we are done by 3.6(b). Q.E.D.

In certain lifting problems, the following fields are relevant. Let G be a finite group, and let L/F be a finite extension of fields with Galois group G. Recall that a G module $M_2(G)$ was defined at the end of §2 as follows. $M_2(G)$ is generated by elements $c(\sigma, \tau)$ where $1 \neq \sigma, \tau \in G$, modulo the relations which make $c(\sigma, \tau)$ a 2-cocycle. The fields we are interested in are the ones of the form $Q(L/F, M)$ where $M = M_2(G)$.

The field $Q(L/F, M)$ will be shown to be related to the following F class. Denote by $\mathscr{A}(L/F)$ the F class of Azumaya algebras which are crossed products of the form $\Delta(L \otimes_F R/R, G, d)$ where R is any commutative F algebra and $d(\sigma, \tau)$ is a two cocycle of G in $(L \otimes_F R)^*$. In formally writing these crossed products as linear structures, we will assume that the structures specify the embedding of L in the algebra. We can do this because L has a finite basis over F and so we can specify the image of each basis element in the algebra. The effect of all of this is that the morphisms (ψ, φ):

$$\Delta(L \otimes_F R/R, G, d)/R \to \Delta(L \otimes_F S/S, G, d')/S$$

are exactly pairs (ψ, φ) of algebra morphisms where $\psi(L \otimes_F R) \subseteq L \otimes_F S$ and ψ restricted to $L \otimes_F R$ is just the map induced by φ. For example, an R isomorphism in $\mathscr{A}(L/F)$ can be specified by an algebra isomorphism

$$\psi : \Delta(L \otimes_F R/R, G, d) \to \Delta(L \otimes_F R/R, G, d')$$

such that ψ is the identity on $L \otimes_F R$. We are specifically not assuming that the morphisms preserve the cocycles.

We are about to apply 3.10 to the F class $\mathscr{A}(L/F)$. In order to make the application, we will describe a local projective densely representing object for $\mathscr{A}(L/F)$. Set $S = L[M]$, $R = L[M]^G$. Since $S = L \otimes_F R$, S/R, is G-Galois. Denote by c the G 2-cocycle which generates $M = M_2(G)$, and form the crossed product $A = \Delta(S/R, G, c)$. We consider A/R as an object in $\mathscr{A}(L/F)$.

LEMMA 3.16. *A/R is a local projective densely representing object for $\mathscr{A}(L/F)$.*

PROOF. We begin by showing local projectivity. Suppose $(\psi, \varphi) : B'/T \to B/V$ is a surjective map in $\mathscr{A}(L/F)$ such that $\varphi^{-1}(V^*) = T^*$. Let $(\mu, \delta) : A/R \to B/V$ be any map in $\mathscr{A}(L/F)$. Explicitly, write

$$B = \Delta(L \otimes_F V/V, G, d) \quad \text{and} \quad B' = \Delta(L \otimes_F T/T, G, d').$$

The restrictions $\psi' : L \otimes_F T \to L \otimes_F V$ and $\mu' : SL \otimes_F V$ are induced by φ and δ respectively. Using the norm of the extensions $L \otimes_F T/T$ and $L \otimes_F V/V$, it is easily seen that

$$(\psi')^{-1}((L \otimes_F V)^*) = (L \otimes_F T)^*.$$

Also, ψ' is surjective. Let $\{u_\sigma\}_{\sigma \in G}$ be the canonical S basis of A such that $u_\sigma u_\tau = c(\sigma, \tau) u_{\sigma\tau}$ and $u_\sigma s = \sigma(s) u_\sigma$. Let v_σ and w_σ be the corresponding elements of B and E'. Now $\mu(u_\sigma) v_\sigma^{-1}$ is a unit in $L \otimes_F V$ we call $g(\sigma)$, and $\psi(w_\sigma) v_\sigma^{-1}$ is a unit in $L \otimes_F V$ we call $f(\sigma)$. Note that

$$\mu(c(\sigma, \tau)) = g(\sigma)\sigma(g(\tau))g(\sigma\tau)^{-1} d(\sigma, \tau)$$

and

$$\psi(d'(\sigma, \tau)) = f(\sigma)\sigma(f(\tau))f(\sigma\tau)^{-1} d(\sigma, \tau).$$

Choose $g'(\sigma), f'(\sigma) \in (L \otimes_F T)^*$ such that $\psi(g'(\sigma)) = g(\sigma)$ and $\psi(f'(\sigma)) = f(\sigma)$. Set

$$w'_\sigma = g'(\sigma) f'(\sigma)^{-1} w_\sigma.$$

Then the (w'_σ)'s form an $L \otimes_F T$ basis of B', $w'_\sigma t = \sigma(t) w'_\sigma$ for $t \in L \otimes_F T$, and $d''(\sigma, \tau) = w'_\sigma (w'_\tau)(w'_{\sigma\tau})^{-1}$ satisfies $\psi(d''(\sigma, \tau)) = \mu(c(\sigma, \tau))$. We can now define a G map $h : M \to (L \otimes_F T)^*$ by $h(c(\sigma, \tau)) = d''(\sigma, \tau)$. The map h extends to a G preserving L algebra map $\gamma' : L[M] \to L \otimes_F T$. If we set $\gamma(u_\sigma) = w'_\sigma$, then γ'

extends to a map $\gamma : A \to B'$. If ε is the restriction of γ to $R = L[M]^G$, then $(\psi, \varphi) \circ (\gamma, \varepsilon) = (\mu, \delta)$. So local projectivity is proved.

To prove the densely representing property, we first state a lemma.

LEMMA 3.17. *Let K be a field, and $d(\sigma, \tau) \in (L \otimes_F K)^*$ a G 2-cocycle. Suppose $0 \neq s \in L[M]^G$. Then there is a G preserving L algebra map $\varphi : L[M] \to L \otimes_F K$ such that $\varphi(s) \neq 0$ and*

$$\varphi(c(\sigma, \tau)) = d(\sigma, \tau) g(\sigma) \sigma(g(\tau)) g(\sigma\tau)^{-1}$$

for some $g(\sigma) \in (L \otimes_F K)^*$.

PROOF. We begin by considering the G module $M = M_2(G)$. Let P be a free $Z[G]$ module with basis $\{b(\sigma) \mid 1 \neq \sigma \in G\}$. Define $f : M \to P$ by setting

$$f(c(\sigma, \tau)) = b(\sigma) + \sigma b(\tau) - b(\sigma\tau), \qquad \text{where } b(1) = 0.$$

This G map f is clearly well defined. Recall that if n is the order of G, then M has Z rank $(n-1)^2$. By a similar argument, $P/f(M)$ has Z rank $n-1$. Since $(n-1)^2 + (n-1) = n(n-1)$ is the rank of P, f must be an injection. Using f, we can assume $L[M]$ is a subalgebra of $L[P]$.

Now view $L[M]$ as a localized polynomial ring with the $c(\sigma, \tau)$'s as variables. To make the c's look more like variables, set $c(\sigma, \tau) = x_{\sigma,\tau}$. Let $s''(g(\sigma))$ be s with $d(\sigma, \tau) g(\sigma)(\sigma g(\tau)) g(\sigma\tau)^{-1}$ substituted for $x_{\sigma,\tau}$. The lemma exactly states that there are $g(\sigma) \in (L \otimes_F K)^*$ such that $s''(g(\sigma)) \neq 0$. View $L[P]$ and $(L \otimes_F K)[P]$ as localized polynomial rings with variables $\sigma(b(\tau))$. For the same reason as above, we set $y_{\sigma,\tau} = \sigma(b(\tau))$. Let $s' \in (L \otimes_F K)[P]$ be defined as s with $y_{1,\sigma} y_{\sigma,\tau} y_{1,\sigma\tau}^{-1} d(\sigma, \tau)$ substituted for $x_{\sigma,\tau}$. That is, let $\psi : L[M] \to (L \otimes_F K)[P]$ be the unique G preserving L algebra map such that

$$\psi(x_{\sigma,\tau}) = y_{1,\sigma} y_{\sigma,\tau} y_{1,\sigma\tau}^{-1} d(\sigma, \tau),$$

and set $\psi(s) = s'$. Since $s \in L[M]^G$, $s' \in (L \otimes_F K)[P]^G$. Suppose $s' \neq 0$. $(L \otimes_F K)[P]^G$ is a localized polynomial ring over K, so there is a K algebra map $\mu : (L \otimes_F K)[P]^G \to K$ such that $\mu(s') \neq 0$. Tensoring η by L yields a G preserving L algebra map

$$\mu' : (L \otimes_F K)[P] \to L \otimes_F K$$

such that $\mu'(s') \neq 0$. If $\varphi = \mu' \circ \psi$, then φ is the required map.

Thus we end the lemma's proof by showing that $s' \neq 0$. Let $K'' \supseteq K$ be a field extension splitting $d(\sigma, \tau)$. That is, there are $f(\sigma) \in (L \otimes_F K'')^*$ such that

$$d(\sigma,\tau)=f(\sigma)\sigma(f(\tau))f(\sigma\tau)^{-1}.$$

Viewing s as in $L[P]$, i.e. as a polynomial in the y's, we see that as an element of $(L\otimes_F K'')[P]$, s' is just s with $\sigma(f(\tau))y_{\sigma,\tau}$ substituted for $y_{\sigma,\tau}$. Since the $\sigma(f(\tau))$'s are units, $s'\neq 0$. Q.E.D.

Having proved this lemma, we return to our proof that A/R is densely representing. Let $B/K\in\mathscr{A}(L/F)$ be a crossed product $\Delta(L\otimes_F K/K,G,d)$, where K is a field. If $0\neq s\in L[M]^G$, choose $\varphi: L[M]\to L\otimes_F K$ as in the lemma. φ extends to a unique map $\varphi: L[M](1/s)\to L\otimes_F K$. Denote by $\varphi': R(1/s)\to K$ the restriction of φ (recall $R=L[M]^G$). By our choice of φ, $A(1/s)\otimes_{\varphi'} K\cong B$. Thus φ' realizes B and we have proved the proposition.

With 3.16 in hand, we can invoke 3.10. The following theorem is the result. Its proof being easy, we will omit it.

THEOREM 3.18. *Let L/F, G, and $M=M_2(G)$ be as above. Then the following are equivalent*:

(a) $\eta(M)=[0]$.

(b) $Q(L/F,M)$ *is retract rational.*

(c) $\mathscr{A}(L/F)$ *has the lifting property.*

(d) *For all local commutative algebras T, M, the natural map* $\mathrm{Br}(L\otimes_F T/T)\to\mathrm{Br}(L\otimes_F (T/M)/(T/M))$ *is a surjection.*

The curious thing about 3.18 is that one of the conditions, (a), is independent of L/F and only depends on G. Later on, we will use a Brauer group computation to add two more equivalent statements, namely:

(e) *For all local F algebras T, M and all G-Galois extensions S/T, the natural map* $\mathrm{Br}(S/T)\to\mathrm{Br}((S/MS)/(T/M))$ *is a surjection.*

(f) *All the Sylow subgroups of G are cyclic.*

There is a relative version of 3.18 which we can also state. Let G be a finite group, and $N\subseteq G$ a normal subgroup. Consider $M_2(G/N)=M'$ to be a G module, and let $f: M_2(G)\to M_2(G/N)$ be the canonical map. f induces an F algebra map $\varphi: L[M]^G\to L[M']^G$. Suppose L/F is a G Galois extension, and $K\subseteq L$ is the subfield associated with N.

THEOREM 3.19. *If M, M', N, G, L, and K are as above, then the following are equivalent*:

(a) $\eta(f)=[0]$.

(b) $\varphi: L[M]^G\to L[M']^G$ *factors rationally.*

(c) *Suppose T, P is a commutative local F algebra, and set $E = T/P$. Then the image of the natural map* $\mathrm{Br}(L \otimes_F T/T) \to \mathrm{Br}(L \otimes_F E/E)$ *contains* $\mathrm{Br}(K \otimes_F E/E)$.

PROOF. Let $n = |N|$. Set $\mathscr{A}'(K/F) \subseteq \mathscr{A}(L/F)$ to be the subclass of all $A/R \in \mathscr{A}(L/F)$ which are split by $K \otimes_F R$. In other words, $B/E \in \mathscr{A}'(K/F)$ for E a field are exactly algebras $M_n(B')$ where $B' = \Delta(K \otimes_F E, G/N, c)$.

Set R' to be the F algebra $L[M']^G$, $S' = L \otimes_F R'$. If $d(\sigma N, \tau N)$ is the G/N 2-cocycle which generates $M' = M_2(G/N)$, denote by $d'(\sigma, \tau) = d(\sigma N, \tau N)$ the induced G 2-cocycle. Set $A = \Delta(S'/R', G, d')$. Note that $K \otimes_F R'$ splits A.

We claim that A/R' is a densely representing object for $\mathscr{A}'(K/F)$. But, $[A] = [A']$ where $A' = \Delta(K \otimes_F R'/R', G/N, d)$. Also, R' is equal to $K[M']^{G/N}$. Thus by 3.16, A'/R' is a densely representing object for $\mathscr{A}(K/F)$. If $B/E \in \mathscr{A}'(K/F)$ for E a field, write $B = M_n(B')$ where $B' \in \mathscr{A}(K/F)$. For any $0 \neq s \in R'$, choose $\psi : R'(1/s) \to E$ such that $A'(1/s) \otimes_\psi E \cong B'$. Then $A(1/s) \otimes_\psi E \cong B$, and the claim is proved.

Next, set $R = L[M]^G$, $S = L[M]$ and $A_1 = \Delta(S/R, G, c)$ where c is the cocycle generating $M = M_2(G)$. Note that if $\varphi' : L[M] \to L[M']$ is the induced G preserving map, then $d'(\sigma, \tau) = d(\sigma N, \tau N) = \varphi'(c(\sigma, \tau))$. Hence $A_1 \otimes_\varphi R' \cong A$. All in all, 3.10(b) can be applied to show that (a) and (b) are equivalent to $(\mathscr{A}'(K/F), \mathscr{A}(L/F))$ having the relative lifting property. And (c) is clearly equivalent to this same property. Q.E.D.

§4. Cyclic extensions of 2 power order

In [23] it was seen that cyclic Galois extensions of 2 power order behave differently from odd order cyclic extensions. In this section we will further explore this difference. We will be able to use the machinery of the first three sections to settle some questions in this area. In turn, some of the machinery of those sections was motivated by the application here. In particular, we refer to 4.19.

To turn to specifics, let C_q be the cyclic group of order $q = 2^r$. Let F be a field and $\rho = \rho(q)$ a primitive qth root of unity ($\rho = 1$ if F has characteristic two). We already know ([23], p. 257) that if $F(\rho)/F$ is cyclic, then all C_q Galois extensions lift. What about the converse? If $F(\rho)/F$ is not cyclic, is there a counterexample to lifting? In [23] this sort of question was attacked using the related approximation problem and examples from algebraic number theory. But this approach cannot fully decide the issue; there are global fields F such that $F(\rho)/F$ is not cyclic but such that all relevant local-global problems are solvable. In fact, in

4.13, we characterize such F. Nonetheless, we can use the machinery of the first sections to show that there is a counterexample to lifting for such F.

To further study these cyclic extensions, we again turn to algebraic number fields for examples. In doing so, one discovers an interesting phenomenon. Suppose F is a global field and F' is one of its completions at a prime of F. Assume that L'/F' is a G Galois. Of course, L' may not pull back to a G Galois extension L/F. However, $L' \oplus L'$ can be thought of as a C_{2q} extension L''/F' via the induction operation of [23]. It can be shown that the C_{2q} extension L''/F' pulls back to a C_{2q} extension of F.

This phenomenon raises two questions. Does the same thing happen for lifting C_q Galois extensions? Also, is this phenomenon special to number fields or does it hold for all C_q Galois extensions? We prove two sorts of results. First, that for many fields the corresponding lifting problem is solvable. And second, that it is not always solvable.

Along the way, we will develop enough understanding of C_q Galois extensions to give new, perhaps more elementary, proofs of some relevant facts about C_q extensions of number fields. Included is another proof of Wang's counter example and a result that is a version of the full Grunwald–Wang Theorem.

Before investigating these questions directly, we must make a series of preliminary comments. The first such topic we mention is cyclic algebras. In [24], it was shown that cyclic algebras behave well. Unfortunately, the following easy result was not precisely proved there. We do so here for easy reference. Before stating this result, we specify some notation in a situation that will often recur. If K is a field, and v is a valuation on K, we will denote by K_v the completion of K with respect to v. If $v_1, \cdots, v_n$ are a set of valuations on K, then K_i will denote the completion of K with respect to v_i.

PROPOSITION 4.1. *Let σ be a generator of C_n.*

(a) *Suppose T, M is a local F algebra with $T/M = K$. Assume S/T is C_n Galois, and set $L = S \otimes_T K$. If $A = \Delta(L/K, \sigma, a)$ is a cyclic algebra, there is a cyclic algebra $B = \Delta(S/T, \sigma, a')$ such that $B \otimes_T K \cong A$.*

(b) *Suppose $v_1, \cdots, v_m$ are inequivalent real valued valuations on K. Let L/K be a C_n Galois extension and set $L_i = L \otimes_K K_i$. If $A_i = \Delta(L_i/K_i, \sigma, a_i)$ are cyclic algebras, there is an algebra $A = \Delta(L/K, \sigma, a)$ such that $A \otimes_K K_i \cong A_i$ for all i.*

PROOF. Part (a) is trivial. As for (b), note that one can use elementary arguments, or [23] p. 99, or [31], and conclude that there is an $\varepsilon > 0$ such that for any of the v_i, if $a_i' \in K_i$ satisfies $v_i(a_i - a_i') < \varepsilon$, then

$$\Delta(L_i/K_i, \sigma, a_i) \cong \Delta(L_iK_i, \sigma, a_i').$$

Use the weak approximation theorem (e.g. [3], p. 48) and choose $a \in K$ such that $v_i(a - a_i) < \varepsilon$ for all i. $A = \Delta(L/K, \sigma, a)$ is the algebra required by (b). Q.E.D.

Later on, we will need information about some approximation questions for abelian crossed products. The next result will settle the global field case of what we need. Let L, K be global fields, and L/K a Galois extension with Galois group $G = C_2 \oplus C_q$ where q is a power of 2. The following theorem gives precise conditions when elements of $\mathscr{A}(L/K)$ over local fields pull back to an element of $\mathscr{A}(L/K)$ over K itself. Note that the condition is given in terms of Hasse invariants (e.g. [21], p. 276).

THEOREM 4.2. *Let $v_1, \cdots, v_m$ be distinct valuations (or primes) on K, and set $L_i = L \otimes_K K_i$. Suppose $A_i = \Delta(L_i/K_i, G, c_i)$ has Hasse invariant $m_i/2q$. There is an $A = \Delta(L/K, G, c)$ such that $A_i \cong A \otimes_K K_i$ if and only if one or both of the following conditions hold:*

(i) *For some v not among the v_i, $L \otimes_K K_v$ is a field.*

(ii) *The sum of the m_i is divisible by 2.*

PROOF. The Brauer classes of the form $[\Delta(L/K, G, c)]$ are exactly those whose Hasse invariants at any valuation w have the form r/n where n is the local degree of L at w. Also, of course, the Hasse invariants of any Brauer class must sum to zero. Set $m/2q$ to be the sum of the Hasse invariants of the A_i. By Tchebotarev density (e.g. [12], p. 168), there are infinitely many primes not among the v_i's such that L has local degree q at those primes. If both (a) and (b) are false, and A exists, then the sum of the Hasse invariants of A at primes not among the v_i has the form r/q and $(m + 2r)/2q$ cannot be in Z, a contradiction. Conversely, if (a) holds, choose v not among the v_i such that $L \otimes_K K_v$ is a field. If (b) holds, let v be such that L has local degree q at v and v is again not among the v_i. Let $\alpha \in \mathrm{Br}(K)$ have Hasse invariants $-m/2q$ at v and $m_i/2q$ at v_i. α will have a representative A as required. Q.E.D.

It will be convenient to recall now some facts about the Brauer group of a rational function field $K(t)$ (see [9], [3]). Let $P \subset K[t]$ be a prime ideal, set $K_p = K[t]/P$, and let G_P be the absolute Galois group of K_P. That is, G_P is the Galois group of K_P^s/K_P, where K_P^s is the separable closure of K_P. We denote by $\chi(G_P)$ the group of continuous homomorphisms $\mathrm{Hom}_c(G_P, Q/Z)$, where G_P has the Krull topology and Q/Z has the trivial topology. If $f \in \chi(G_P)$, then

$N = \text{kernel}(f)$ is such that G_P/N is finite and cyclic. If L is the fixed field of N in K_P^s, we say that f defines L.

The Brauer group $\text{Br}(K(t))$ is described via the $\chi(G_P)$'s, at least away from the characteristic of K. Suppose p is the characteristic of K. If A is any torsion abelian group, set A' to be A if $p = 0$ and set A' to be the p prime part of A if $p \neq 0$. There is an exact sequence describing the Brauer group of $K(t)$ as follows:

$$0 \to \text{Br}(K)' \to \text{Br}(K(t))' \to \bigoplus \chi(G_P)' \to 0 \tag{4.3}$$

where the direct sum is over all primes $P \subseteq K[t]$. For $[A] \in \text{Br}(K(t))$, we denote by $\chi_P(A)$ the image of $[A]$ in $\chi(G_P)$. To work with (4.3), it is necessary to be able to compute the maps χ_P. This is done via an exact sequence for complete fields. Let L be a field of characteristic the same p (for notational convenience). Considering the Laurent series field $L((s))$, we have (e.g. [30], [3])

$$0 \to \text{Br}(L)' \to \text{Br}(L((s)))' \to \chi(G)' \to 0 \tag{4.4}$$

where G is the absolute Galois group of L. Moreover, the maps in (4.4) are functorial with respect to extensions of L. Finally, the map χ_L has the following properties. If M/L is a cyclic Galois extension, with Galois group generated by σ, then

$$f = \chi_L(\Delta(M((s))/L((s)), \sigma, s))$$

defines M and $f(\sigma) = 1/n$, $n = [M : L]$. On the other hand, if $u \in L((s))$ is a unit in the power series ring, then

$$\chi_L(\Delta(M((s))/L((s)), \sigma, u)) = 1.$$

Returning to the field $K(t)$, let $P \subseteq K[t]$ be a prime. Denote by $K(t)_P$ the completion of $K(t)$ at P. $K(t)_P$ is a Laurent series field over K_P, say $K_P((s))$. The map χ_P is just the composition of the map $\text{Br}(K(t)) \to \text{Br}(K(t)_P)$ and the map $\chi_{K_P} : \text{Br}(K_P((s))) \to \chi(G_P)$. This fact, along with the functoriality of (4.4), has the following consequence important to us. We will omit the easy proof.

LEMMA 4.5. *Suppose* $[A] \in \text{Br}(K(t))$ *and* $f_P = \chi_P(A)$. *Let* f_P *define the extension* L_P/K_P. *Assume* L/K *is such that* $L(t)$ *splits* A. *Then* $L \otimes_K K_P$ *contains an isomorphic copy of* L_P. *In other words, any field amalgamation* LK_P *contains* L_P.

As a final preliminary topic, we mention some facts about the induced Galois extensions defined in [23]. Suppose K is a field and L/K is Galois with group G. If G' is a finite group containing G, then there is an induced Galois extension $\text{Ind}_G^{G'}(L/K)$ which has Galois group G' over K. As a K algebra, $\text{Ind}_G^{G'}(L/K)$ is

just $L \oplus \cdots \oplus L$. As a $K[G']$ module, $\mathrm{Ind}_G^{G'}(L/K)$ is just $K[G'] \otimes_{K[G]} L$. Recall further that, if L/K is any G-Galois extension of a field K, then L/K has the form $\mathrm{Ind}_H^G(L'/K)$ where L' is a field, and $H = \mathrm{Gal}(L'/K)$. H is called a decomposition group of L/K; it is unique up to conjugation. In the next lemma we point out how decomposition groups and the Galois correspondence mix together.

LEMMA 4.6. *Let K be a field, and L/K Galois with group G and decomposition group H. Assume $N \subset G$ is a normal subgroup and that L' is the fixed ring of N. Then HN/N is a decomposition group for L'/K. Also, let L_1 and L_1' be the field direct summands of L and L' respectively. Assume that L_1/K has Galois group H. Then L_1' is isomorphic (as a K algebra) to the subfield of L_1 corresponding to $H \cap N$.*

PROOF. A decomposition group of L'/K can be described as a subgroup of G/N fixing some primitive idempotent of L'. Let $e \in L$ be a primitive idempotent which H fixes. Let $n_1, \cdots, n_r$ be coset representatives of $H \cap N$ in N. Set

$$f = n_1(e) + \cdots + n_r(e).$$

Then f is a primitive idempotent of L', and HN is exactly the subgroup of G fixing f. That is, HN/N is the subgroup of G/N fixing f. This proves the first claim.

L_1 is the field Le. There is an injection from $L'f$ to L_1 given by sending x to xe. Every element of this image must be fixed by $H \cap N$, since L' is fixed by N and e is fixed by H. Checking degrees, we have that the image is exactly the fixed field of $H \cap N$. Q.E.D.

We can now turn to the main body of this section, an examination of C_q extensions for q a power of 2. We fix some notation that will remain unchanged throughout this section. As always, F is the underlying field. For convenience, F will be assumed not to have characteristic 2. Set $\rho = \rho(q)$ to be a primitive qth root of unity. $F(\rho)/F$ will always be noncyclic with Galois group H. Let n be the order of H. H is generated by σ, τ where $\sigma(\rho) = \rho^{-1}$ and $\tau(\rho) = \rho^m$ for some m. The map τ and the integer m will be fixed according to the following lemma.

LEMMA 4.7. *We may choose τ, m such that $m - 1$ is a power of 2. Also, if s is the order of m modulo q, we may assume $m^s - 1 = kq$ where k is odd.*

PROOF. It suffices to show that if s divides $q/4$, then there is such an m with $m \not\equiv -1(q)$. This we prove by induction on q. If $q = 8$, $m = 5$ will do, as

$5^2 - 1 = 8 \cdot 3$. For general q, suppose first that $s \neq 2$. Choose $m = 1 + 2^r$ such that m has order $s/2$ modulo $q/2$, and such that $m^{s/2} = 1 + k(q/2)$ where k is odd. Now

$$m^s = (1 + k(q/2))^2 = 1 + kq + k^2(q^2/4) = 1 + (k + k^2(1/4))q.$$

We note that m has order s modulo q and that $k + k^2(q/4)$ is odd. This finishes the case $s \neq 2$. If $s = 2$ set $m = 1 + q/2$ and note that $m^2 = 1 + (1 + q^2/4)q$.

Q.E.D.

If $F(\rho)/F$ were cyclic, then C_q extensions over F could be described via the generic constructions of [23]. The basic idea is to adjoin ρ, and then to describe the resulting extensions. This method can also be used in our case, where $F(\rho)/F$ is not cyclic. The following theorem is the result. But first, let us recall a bit of notation from [23]. If R is a commutative ring, and $f(y) \in R[y]$ is monic, we set $R\{f(y)\} = R[y]/(f(y))$. The image of y in $R\{f(y)\}$ is called a canonical element. If R is a commutative F algebra, then σ and τ act naturally on $R' = R \otimes_F F(\rho)$. For $r \in R'$, set $N_\sigma(r) = r\sigma(r)$,

$$M_\tau(r) = \tau^{s-1}(r)\tau^{s-2}(r)^m \cdots r^{m^{s-1}},$$

and

$$N_{\sigma,\tau}(r) = r\tau(r) \cdots \tau^{s-1}(r)\sigma(r)\tau(\sigma(r)) \cdots \tau^{s-1}(\sigma(r)).$$

THEOREM 4.8. (a) *Assume T is a local F algebra and S/T is a C_q Galois extension. Consider $S' = S \otimes_F F(\rho)$ and $T' = T \otimes_F F(\rho)$. S'/T is Galois with group $C_q \oplus H$. $S' \cong T'\{y^q - a\}$, where the canonical generator $\alpha \in S'$ satisfies the following: $\tau(\alpha) = \alpha^m b^{-k}$, and $\sigma(\alpha) = \alpha^{-1} z^{-k}$ where $b, z \in (T')^*$, $\sigma(z) = z$ and $N_\sigma(b) = \tau(z)/z^m$. Also $a = M_\tau(b) = (\sigma(w)/w)z^{q/2}$ for some $w \in (T')^*$.*

(b) *Conversely, suppose R is a commutative F algebra, $R' = R \otimes_F F(\rho)$, and $b, z \in (R')^*$ satisfy $\sigma(z) = z$ and $N_\sigma(b) = \tau(z)/z^m$. Set $a = M_\tau(b)$. If $S' = R'\{y^q - a\}$ and $\alpha \in S'$ is a canonical generator, then one can define $\sigma(\alpha) = \alpha^{-1} z^{-k}$ and $\tau(\alpha) = \alpha^m b^{-k}$ so that $S' \cong S \otimes_R R'$ where S/R is C_q Galois.*

PROOF. We prove (b) first. If S' is as given, we must check that σ and τ are well defined on S'. But

$$\tau(a) = \tau(M_\tau(b)) = M_\tau(b)^m b^{-m^s+1} = a^m b^{-kq} = (\alpha^m b^{-k})^q = (\tau(\alpha))^q,$$

so τ is well defined. Now

$$N_\sigma(M_\tau(b)) = M_\tau(\tau(z)/z^m) = z^{-kq},$$

so

$$\sigma(a) = a^{-1}z^{-kq} = (\alpha^{-1}z^{-k})^q = (\sigma(\alpha))^q,$$

and σ is well defined. Also,

$$\tau^s(\alpha) = \alpha^{m^s}M_\tau(b)^{-k} = \alpha(\alpha^{m^{s-1}}M_\tau(b)^{-k}) = \alpha(a^kM_\tau(b)^{-k}) = \alpha,$$

and

$$\sigma^2(\alpha) = \sigma(\alpha^{-1}z^{-k}) = \alpha z^k\sigma(z)^{-k} = \alpha.$$

Hence σ, τ have orders 2, s respectively on S'. We check that

$$\sigma\tau(\alpha) = \sigma(\alpha^m b^{-k}) = \alpha^{-m}z^{-km}\sigma(b)^{-k} = \alpha^{-m}b^k\tau(z)^{-k} = \tau(\alpha^{-1}z^{-k}) = \tau(\sigma(\alpha)),$$

where we have used that $N_\sigma(b) = \tau(z)/z^m$. We conclude that σ, τ commute on S'. In all, the Galois group of R'/R extends to S'. Arguing exactly as in [23], p. 258, the Galois group of S'/R' commutes with this extension. If S is the fixed ring of σ and τ in S', then S/R is as desired.

As for (a), let S/T, S' and T' be as given. Since T is local, T' is semilocal and the Kummer description of C_q extensions can be applied to S'/T'. In particular, if η generates C_q, then $S' = T'\{y^q - a'\}$ where the canonical element $\alpha' \in S'$ satisfies $\eta(\alpha') = \rho\alpha'$. The maps σ and τ extend to S' via their action on $F(\rho)$, and commute with η. Since $\tau\eta = \eta\tau$, $\tau(\alpha') = \alpha'^m b'$ where $b' \in (T')^*$. Similarly, $\sigma(\alpha') = \alpha'^{-1}z'$ for $z' \in (T')^*$. As $\sigma^2(\alpha') = \alpha'$, $\sigma(z') = z'$. As $\tau^s(\alpha') = \alpha'$, we calculate that $M_\tau(b') = a'^k$. If we set $\alpha = (\alpha')^k$, $a = a'^k$, $b = b'^{-1}$, and $z = z'^{-1}$, then $\sigma(\alpha) = \alpha^{-1}z^{-k}$, $\tau(\alpha) = \alpha^m b^{-k}$. Finally $\tau(\sigma(\alpha)) = \sigma(\tau(\alpha))$ implies that $N_\sigma(b)^k = (\tau(z)/z^m)^k$. In other words, $N_\sigma(b) = (\tau(z)/z^m)\delta$ where $\delta^k = 1$. If we choose δ' a power of δ such that $\delta = (\delta')^2$, we have $N_\sigma(b\delta') = \tau(z)/z^m$. Since $m-1$ is a power of 2, $(m^s-1)/(m-1)$ is divisible by k and so $M_\tau(b\delta') = M_\tau(b)$. In all, we can change b to $b\delta'$ and completely satisfy the requirements of (a).

Q.E.D.

Consider now Theorem 4.8 applied to a C_q extension L/K where K is a field. The point of 4.8 is that L/K is determined by a solution of the equations $N_\sigma(b) = \tau(z)/z^m$ and $\sigma(z) = z$, in $K' = K \otimes_F F(\rho)$. Conversely, such a solution determines an extension L/K. As $m - 1 = 2'$, we can rewrite these equations as $N_\sigma(bz^{(m-1)/2}) = \tau(z)/z$ where $\sigma(z) = z$. If $c = bz^{(m-1)/2}$, then $N_{\sigma,\tau}(c) = 1$. Conversely, if $N_{\sigma,\tau}(c) = 1$, then by Hilbert's theorem 90 there is a z such that $N_\sigma(c) = \tau(z)/z$ where z is σ fixed. Setting $b = cz^{(1-m)/2}$, we have $N_\sigma(b) = \tau(z)/z^m$. All of which says that solving our original equation is almost equivalent to finding elements of K' of norm 1.

In old work of Dickson, repeated in [2], elements of norm 1 were seen to be key elements in a description of K'/K crossed products. We are about to derive, using essentially this observation, a very useful connection between C_q Galois extensions and K'/K crossed products. In particular, we will show that lifting one is equivalent to lifting the other.

To be precise, let L/K be a C_q Galois extension and let K_1 be the σ fixed subring of K'. The element z of Theorem 4.8 can be used to define a quaternion algebra $\Delta(K'/K_1, \sigma, z)$ which we will call $D(L/K)$. The next lemma will show that $D(L/K)$ is well defined. In this lemma, let D_K be the set of isomorphism classes of quaternion algebras B/K_1, split by K', and such that the τ transform B^τ of B is isomorphic to B.

LEMMA 4.9. *The mapping $L/K \to D(L/K)$ is well defined. Every element B of D_K is of the form $D(L/K)$ for some C_q Galois extension L/K. If $B = \Delta(K'/K_1, \sigma, z) = D(L/K)$, then there is a $b \in (K')^*$ such that b, z describe L/K.*

PROOF. We assume the notation of Theorem 4.8 and its proof, with R and T replaced by K. Note first that

$$\Delta(K'/K_1, \sigma, z) \cong \Delta(K'/K_1, \sigma, z') \qquad \text{where } z' = \alpha(\sigma(\alpha)).$$

Any other choice for α has the form $\alpha^t w$, where t is odd and $w \in (K')^*$. Now $\alpha^t w(\sigma(\alpha^t w)) = (z')^t N_\sigma(w)$, and

$$\Delta(K'/K_1, \sigma, z') \cong \Delta(K'/K_1, \sigma, (z')^t N_\sigma(w)).$$

Hence $D(L/K)$ is well defined.

Suppose $B = \Delta(K'/K_1, \sigma, z)$ is in D_K. Since $B^\tau \cong B$, $\tau(z)/z = N_\sigma(c)$ for some $c \in (K')^*$. Setting $b = cz^{(1-m)/2}$, we have $N_\sigma(b) = \tau(z)/z^m$. This b, z define a C_q extension L/K such that $D(L/K) \cong B$. To finish the lemma, we note that if $z' = N_\sigma(w)z$ for $w \in K_1^*$, and if $\alpha \in L'$ is the canonical generator as in the proof of 4.8, then $\alpha' = \alpha w^{-k}$ is a canonical generator of L' viewed as $K'\{y^q - aw^{-kq}\}$, and

$$\sigma(\alpha') = \alpha'^{-1} z'^{-k}, \qquad \tau(\alpha') = \alpha'^m (b\tau(w)/w^m)^{-k}. \qquad \text{Q.E.D.}$$

To the quaternion algebras in D_K one can associate a set of K'/K crossed products. More properly, let A_K be the set of isomorphism classes of crossed products $\Delta(K'/K, H, c)$. To each $A \in A_K$ we associate $B(A) \in D_K$ which is just the centralizer of K_1 in A. If $B \in D_K$, then the fact that $B^\tau \approx B$ implies that $[B]$ is in the image of the Brauer group of K and so that $B = B(A)$ for some $A \in A_K$.

Though it is not needed for our arguments, the above maps can be summarized as follows. Recall, from [2], that $A \in A_K$ can be described via u, c, c' such that $N_{\sigma,\tau}(u) = 1$, $N_\sigma(u) = \tau(c)/c$, and $N_\tau(u) = \sigma(c')/c'$. If b, z describe L/K, and $D(L/K) = B(A)$, then one of the u's describing A is the element $bz^{(m-1)/2}$ of norm 1.

Though the maps we have defined are not bijective, they are "equivalences" when it comes to lifting.

THEOREM 4.10. *Let T, M be a local F algebra, let $K = T/M$, and set $T' = T \otimes_F F(\rho)$. Denote by T_1 the σ fixed subring of T'. Assume L/K is C_q Galois, $A = \Delta(K'/K, H, c)$, and $D(L/K) = B(A)$. Then the following are equivalent:*

(a) *There is a C_q Galois extension S/T such that $S \otimes_T K \cong L$.*

(b) *There is an Azumaya algebra $A' = \Delta(T'/T, H, c')$ such that $A' \otimes_T K \cong A$.*

PROOF. Assuming (a), use 4.8 to describe S in terms of b', $z' \in (T')^*$. If b, $z \in K'$ are the images of b', z', then b, z describe L/K. Set $B' = \Delta(T'/T_1, \sigma, z')$. Since $\tau(z')/z'$ is a σ norm from T', $[B']$ is the image of some $[A''] \in \mathrm{Br}(T)$. $[A'' \otimes_T K]$ may not equal $[A]$, but they must be equal after tensoring up to K_1. Hence $[A'' \otimes_T K] = [A][D]$ where D has the form $\Delta(K_1/K, \tau, d)$. By 4.1, $D \cong D' \otimes_T K$ where $D' = \Delta(T_1/T, \tau, d')$. The Brauer class $[A''][D'] \in \mathrm{Br}(T)$ is split by T' and is a preimage of $[A]$. It follows that there is an algebra $A' = \Delta(T'/T, H, c')$ such that $[A']$ is a preimage of $[A]$. Since A' and A have equal degrees, we have $A' \otimes_T K \cong A$ and (b) is satisfied.

Next assume (b), and set B' to be the centralizer of T_1 in A'. We can write $B' = \Delta(T'/T_1, \sigma, z')$. Modulo M, z' has the form $zN_\sigma(w)$ where b, z describe L/K. Choosing $w' \in T'$ to be a preimage of w, we can change z' to $z'N_\sigma(w')$ and so assume that z' is a preimage of z. Now $\tau(z')/z' = N_\sigma(c')$ for some $c' \in T'$. Set $b' = c'z'^{(1-m)/2}$, so that $N_\sigma(b') = \tau(z')/z'^m$. Modulo M, b' and b have the same σ norm. Arguing exactly as before, we can assume b' is a preimage of b. We can now use b', z' to define a C_q extension S/T which satisfies (a). Q.E.D.

To put it all together, 4.10 says that the lifting problem for each $L/K \in \mathscr{E}(C_q)$ is equivalent to the lifting problem for some $A/K \in \mathscr{A}(K'/K)$, and vice versa. When $D(L/K) = B(A)$, and this equivalence holds, we write $L/K \sim A/K$ and say that L/K is equivalent to A/K.

We next observe that this equivalence also applies to approximation problems. Though we have decided not to emphasize approximation problems in this paper, the next result is necessary in order to show how the equivalence can also shed light on algebraic number fields.

THEOREM 4.11. *Let K be a field with valuations $v_1, \cdots, v_n$. Suppose L_i/K_i are C_q Galois extensions and $A_i = \Delta(K' \otimes_K K_i/K_i, H, c_i)$ are such that $L_i/K_i \sim A_i/K_i$. Then the following are equivalent:*

(a) *There is a C_q Galois extension L/K such that $L_i \cong L \otimes_K K_i$ for all i.*

(b) *There is an $A = \Delta(K'/K, H, c)$ such that $A \otimes_K K_i \cong A_i$.*

PROOF. Suppose (a) holds. Let L/K be given by b, $z \in K'$. Set $K_{i,1} = K_1 \otimes_K K_i$. By the same argument as in 4.10, we can find $A''/K \in \mathscr{A}(K'/K)$ such that $A'' \otimes_K K_{i,1} \cong A_i \otimes_{K_i} K_{i,1}$. Again, there are $C_i = \Delta(K_{i,1}/K_i, \tau, c_i)$ such that $[A_i] = [A'' \otimes_K K_i][C_i]$. By 4.1, there is a $C = \Delta(K_1/K, \tau, c)$ such that $C \otimes_K K_i \cong C_i$. Now $[A'' \otimes_K C] = [A']$ where $A' = \Delta(K'/K, H, c)$. We conclude that A satisfies (b).

Conversely, assume (b). Suppose $b_i, z_i \in K_i'$ define L_i/K_i. Arguing as in 4.10 again, there are $z'' \in K_1$ and $b'' \in K'$ such that $N_\sigma(b'') = \tau(z'')/z''^m$ and $z'' = z_i N_\sigma(c_i)$ for $c_i \in K_i' = K' \otimes_K K_i$. By the last sentence of Lemma 4.9, there are b_i' such that the pairs b_i', z'' define L_i/K_i. Of course, $b_i' = b''\sigma(d_i)/d_i$ for some $d_i \in K_i'$. Form $R' = K'[x_h \mid h \in H](1/t)$ where t is the product of the x_h's and H acts on R' in the usual way. Set R to be the invariant ring of H on R'. As has been observed before, R has the form $K[y_1, \cdots, y_m](1/t)$. Use $b''\sigma(x_1)/x_1$ and z'' to define the C_q Galois extension S/R. There are $\varphi_i : R \to K_i$ such that $S \otimes_{\varphi_i} K_i \cong L_i$. Arguing exactly as in [23], p. 279, there is a $\varphi : R \to K$ such that if $L = S \otimes_\varphi K$, then L satisfies (a). Q.E.D.

Theorems 4.10 and 4.11 can be quite useful because $\mathscr{A}(K'/K)$ can be easier to understand than $\mathscr{E}(C_q)$. As a first example of this, we provide the converse to 3.13. For this theorem, we will allow F to have characteristic 2.

THEOREM 4.12. *Let A be a finite abelian group of exponent $2'm$ where m is odd. Assume V is a finitely generated $F[A]$ module such that $A \to \mathrm{Hom}_F(V, V)$ is injective. Then $F_+(V)^A$ is retract rational over F if and only if either F has characteristic 2, or $F(\rho(2'))/F$ is cyclic.*

PROOF. What has to be shown is that if F has characteristic not 2 and $H = \mathrm{Gal}(\rho(2')/F)$ is not cyclic, then $\mathscr{E}(A)$ does not have the lifting property. But if it did, $\mathscr{E}(C_q)$ would have the lifting property for $q = 2'$ ([23], p. 265). This would imply by 4.10 that $\mathscr{A}(F(\rho(q)/F)$ had the lifting property. Hence by 3.18, $\eta(M_2(H)) = [0]$. But then $\eta(J_H) = [0]$ (2.7). This last statement is false for H noncyclic ([6], p. 183, mentioned in 2.6 above). Q.E.D.

Let me briefly mention an alternate proof for 4.12. As argued, it is equivalent

to the question of whether $\eta(J_H) = [0]$. Of course, this last statement is independent of F and only depends on H. But arguing backwards, we can conclude that $\eta(J_H) \neq [0]$ from the counterexamples in [23] for the case $F = Q$ (i.e., Wang's counterexample).

Another consequence of 4.11 is a version of the full Grunwald–Wang Theorem for number fields. Theorem 4.11 reduces the approximation problem for C_q extensions to the same problem for abelian crossed products. Theorem 4.2 answers this equation completely for these crossed products. The combination, then, is a complete answer as to when local C_q extensions can be pulled back to global ones. There seems to be little point to explicitly stating this version in a separate result, but one aspect should be noticed. The behavior of a local C_q extension depends completely on the parameter we have labelled z.

We will, however, draw two more limited consequences from the combination of 4.11 and 4.2, both well known facts in algebraic number theory. First, we can recover Wang's counterexample. If $F = Q$, $\rho = \rho(q)$ for q a power of 2 bigger than or equal to 8, then $Q(\rho) \otimes_Q Q_p$ is a field for the prime $p = 2$ and no other. It follows from 4.2 that if $A/Q_2 \in \mathcal{A}(Q(\rho)/Q)$ is a division algebra, then A cannot pull back to Q. Hence some C_q extension also cannot pull back.

More generally, the next proposition will give necessary and sufficient conditions on a global field K so that all local-global approximation problems for C_q extensions are solvable. The proof, being an easy combination of 4.11 and 4.2, is omitted.

PROPOSITION 4.13. *Suppose K is a global field. Then the following are equivalent:*

(a) *For all primes v of K, $K(\rho(q)) \otimes_K K_v$ is not a field.*

(b) *For all primes $v_1, \cdots, v_n$ of K and all C_q Galois extensions L_i/K_i, there is a C_q Galois extension L/K such that $L \otimes_K K_i \cong L_i$.*

In the beginning of this section, we mentioned that, over global fields, there was an interesting interaction between lifting questions and the induction operation on Galois extensions. In order to explore this, we first sort out the relationship between the induction operation and the equivalence of Theorem 4.10.

LEMMA 4.14. *Let $G = C_q$ be the cyclic group of order $q = 2^r$, viewed as a subgroup of $G' = C_s$ where $s = 2^r q = s'q$. Let $\rho = \rho(q)$ and $\rho' = \rho(s)$ where we assume $\rho'^{s'} = \rho$. Suppose $L/K \in \mathcal{C}(C_q)$, $A/K \in \mathcal{A}(K'/K)$, and $L/K \sim A/K$. Set $L_1 = \mathrm{Ind}_G^{G'}(L/K)$. Then $L_1/K \sim A_1/K$ where $A_1 \in \mathcal{A}(F(\rho') \otimes_F K/K)$ and $[A] = [A_1]$ in the Brauer group.*

PROOF. The automorphisms σ, $\tau \in H = \mathrm{Gal}(F(\rho)/F)$ extend to automorphisms σ, $\tau \in H' = \mathrm{Gal}(F(\rho')/F)$ where $\sigma(\rho') = \rho'^{-1}$ and $\tau(\rho') = \rho'^{m}$. The proof of Lemma 4.7 shows that σ, τ generate H' and that τ, m satisfies 4.7 with respect to s.

Suppose $b, z \in K'$ describe the C_q extension L/K. That is, if $L' = K' \otimes_K L$, suppose $L' \cong K'\{y^q - a\}$ where the canonical element $\alpha \in L'$ satisfies $\sigma(\alpha) = \alpha^{-1}z^{-k}$ and $\tau(\alpha) = \alpha^m b^{-k}$. Now set $k'' = F(\rho') \otimes_F K$ and $L'' = L_1 \otimes_K K''$. Then L'' has the form $K''\{y^s - a'\}$. Also, as a K'' algebra, l'' is isomorphic to

$$(L' \otimes_{K'} K'') \oplus (L' \otimes_{K'} K'') \oplus \cdots \oplus (L' \otimes_{K'} K'') \qquad (s' \text{ times}).$$

Identifying all these expressions, we find we can write the canonical element, β, of l'' as

$$\beta = (\alpha, \rho'\alpha, \cdots, (\rho')^{s'-1}\alpha).$$

We can compute that $\sigma(\beta) = \beta^{-1}z^{-k}$ and $\tau(\beta) = \beta^m b^{-k}$. In other words, $b, z \in K''$ describe L_1/K also. The lemma follows. Q.E.D.

Let K be a global field, $v_1, \cdots, v_n$ some primes of K, and let L_i/K_i be C_q Galois extensions. If $G = C_q$, $G' = C_{2q}$, and $L_i' = \mathrm{Ind}_G^{G'}(L_i/K_i)$, then 4.2 and 4.11 show that there always is a C_{2q} Galois extension L'/K such that $L_i' \cong L' \otimes_K K_i$. As noted before, we are interested in whether this is also true for all fields K. Also, we are interested in the corresponding lifting problem. That is, suppose T, M is a local F algebra, $K = T/M$, and L/K is Galois with group $G = C_q$. Does $\mathrm{Ind}_G^{G'}(L/K)$ lift to T?

In order to consider the lifting problem, we must ask when, in general, elements in $\mathscr{A}(K'/K)$ can be lifted. Let F, ρ, σ and τ be as always. Set F_1 to be the σ fixed subfield of $F(\rho)$, and set F_2 to be the τ fixed subfield. For any field $K \supseteq F$, we set $K_j = F_j \otimes_F K$. If $A/K \in \mathscr{A}(F(\rho)/F)$ is a tensor product $A_1 \otimes A_2$ such that K_i is a maximal commutative subring of A_i, we say that A decomposes. Note that by 4.1, if A decomposes then it can be lifted over any local F algebra. A similar property holds for the approximation problem.

It will be useful to have the following criteria for when A decomposes.

LEMMA 4.15. (a) *Suppose $A/K \in \mathscr{A}(F(\rho)/F)$ has the property that $[A]$ is a product of $[A_i]$ where each A_i is split by a cyclic extension L_i/K and $L_i \subset K'$. Then A decomposes.*

(b) *Suppose $A/K \in \mathscr{A}(F(\rho)/F)$ and $A'/K \in \mathscr{A}(K(\rho)/K)$ are such that $[A] = [A']$. If A' decomposes with respect to $K(\rho)/K$, or $K(\rho)/K$ is cyclic, then A decomposes.*

PROOF. We begin by proving (b). Suppose K_i' is the field direct summand of K_i. Then $K(\rho)$ is the field direct summand of $K_1' \otimes_K K_2'$. Assume, first of all, that $K(\rho)/K$ is not cyclic. Then $K(\rho) \cong K_1' \otimes_K K_2'$. If A'/K decomposes with respect to $K(\rho)/K$, then $A' = A_1' \otimes_k A_2'$ where K_i' is a maximal subfield of A_i'. But if K_i' splits A_i', then so does K_i. In other words, $[A_i'] = [A_i]$ where A_i is a crossed product with respect to K_i. We have that $[A] = [A_1][A_2]$. Checking degrees, we get that $A = A_1 \otimes_K A_2$ and A decomposes.

Next, assume that $K(\rho)/K$ is cyclic. $H' = \mathrm{Gal}(K(\rho)/K)$ can be considered to be a subgroup of $H = \mathrm{Gal}(F(\rho)/F)$. If $H' \supseteq \langle\sigma\rangle$, then $H' = \langle\sigma\rangle$ and $K(\rho) = K_2$. If $H' \cap \langle\sigma\rangle = (1)$, then 4.6 shows that $K(\rho)$ is isomorphic to a subfield of K_1. Hence either K_1 or K_2 splits A and clearly A decomposes.

Turning to (a), let A and the A_i, L_i be as given. Set L_i' to be the field direct summand of L_i. Then L_i' splits A_i, $L_i' \subset K(\rho)$, and L_i'/K is cyclic. All in all, we may assume that $F = K$. With this identification, then $\sigma, \tau \in H = \mathrm{Gal}(K(\rho)/K)$ have their usual meaning and the $L_i \subset K(\rho)$ are fields. By part (b), we may assume $K(\rho)/K$ is not cyclic. Enlarging L_i if necessary, we may assume $L_iK_j = K(\rho)$ for $j = 1$ or 2. In other words, $L_i \otimes_K K_j$ is a direct sum of copies of $K(\rho)$. For simplicity, we take $J = 1$, the other case being similar. If we write $A_i = \Delta(L_i/K, \eta, c)$, then

$$A_i \otimes_K K_1 = \Delta(L_i \otimes_K K_1/K_1, \eta, c).$$

Since $L_i \otimes_K K_1$ is a direct sum of copies of $K(\rho)$,

$$[A_i \otimes_K K_1] = [\Delta(K(\rho)/K_1, \sigma, c)]$$

(this is an easy calculation) and so

$$[A_i] = [\Delta(K_2/K, \sigma, c)][\Delta(K_1/K, \tau, d)] \qquad \text{for some } d \in K^*.$$

In other words, each $[A_i] = [A_{i,1}][A_{i,2}]$ where K_j splits $A_{i,j}$. Set $[B_j]$ to be the product of all the $[A_{i,j}]$'s. Since K_j splits B_j, we can assume that $B_j = \Delta(K_j/K, \eta, c_j)$ for the appropriate $\eta \in H$. Also, $[A] = [B_1][B_2]$, and so, checking degrees, we have $A \cong B_1 \otimes_K B_2$. Q.E.D.

As mentioned before, Theorem 4.10 is useful because sometimes $\mathscr{A}(F(\rho)/F)$ is easier to deal with than $\mathscr{C}(C_q)$. In particular, the machinery of the Brauer group can be used to show that certain $A/K \in \mathscr{A}(F(\rho)/F)$ decompose. The consequence is that we get lifting results for $\mathscr{A}(F(\rho)/F)$, and hence for $\mathscr{C}(C_q)$. The next proposition contains some of these Brauer group results.

PROPOSITION 4.16. *Let $F(\rho)/F$ be as above, and choose ρ' such that $\rho'^2 = \rho$.*

(a) *If K is any local or global field containing F, and $A/K \in \mathscr{A}(F(\rho)/F)$, then $M_2(A)/K \in \mathscr{A}(F(\rho')/F)$ decomposes.*

(b) *Now let K be an arbitrary field containing F. If for every $A/K \in \mathscr{A}(F(\rho)/F, M_2(A))$ decomposes as in* (a), *then the same is true for the rational function field $K(t)$.*

PROOF. First note that in both (a) and (b), by using 4.15 (b), we may assume that $K = F$ and thus that $K(\rho)/K$ is not cyclic. Turning to (a), suppose K is a local field. Assume that

$$\sigma, \tau \in H = \mathrm{Gal}(K(\rho)/K)$$

are as usual, and extend these maps to

$$\sigma, \tau \in H' = \mathrm{Gal}(K(\rho')/K)$$

just as in the proof of 4.14. Write $K(\rho') = K_1' \otimes K_2'$ in the usual way. Note that $[K(\rho): K] = [K_1': K]$. Since K is local, if A is split by $K(\rho)$, it is split by K_1'. So if $A/K \in \mathscr{A}(K(\rho)/K)$, then

$$M_2(A) = A' \otimes_K M_2(K) \qquad \text{where } A' = \Delta(K_1', \tau, c).$$

Thus $M_2(A)$ decomposes.

Next, suppose that, in (a), K is global. Let $v_1, \cdots, v_n$ be the primes of K where A ramifies. Let K_i be the completion of K at v_i, and $K(\rho') = K_1' \otimes_K K_2'$ the decomposition of $K(\rho')$ as above. Set $A_i = A \otimes_K K_i$ and $K_{i,j} = K_j' \otimes_K K_i$. By the above paragraph,

$$M_2(A_i) = A_{i,1} \otimes_{K_i} A_{i,2} \qquad \text{where } K_{i,j} \text{ splits } A_{i,j}.$$

Let $m_{i,j}/m$ be the Hasse invariant of $A_{i,j}$. For $j = 1, 2$, set m_j/m to be the sum of the $m_{i,j}/m$ over all i. Then $(m_1 + m_2)/m$ is in Z, since it is the sum of the Hasse invariants of A. Also, as $A_{i,2}$ is split by $K_{i,2}$ which has degree 2 over K_i, we have that m_2/m has the form $r_2/2$. By Tchebotarev density, there are infinitely many primes where K_1' and K_2' have local degree 2. In particular, there is such a v_{n+1} not among the other v_i's. Let $[A_j] \in \mathrm{Br}(K)$ have Hasse invariants $m_{i,j}/m$ at v_i and $r_2/2$ at v_{n+1}. Then $[A_j]$ is split by K_j' and we can write $M_2(A) = A_1 \otimes_K A_2$. This finishes (a).

To prove (b), we use the exact sequence (4.3), where $P \subset K[t]$, χ_p, G_p, K_p, etc. have the same meaning as in (4.3). Suppose $A/K(t) \in \mathscr{A}(K(\rho)/K)$. Set $f_P = \chi_P(A)$, and let f_P define the cyclic extension L_P/K_P. Since $K(\rho)(t)$ splits A, L_P is a subfield of $K(\rho) \otimes_K K_P$. That is, $L_P \subseteq K_P(\rho)$. By using 4.6 it is not hard to see

that $L_P \subseteq L'_P \otimes_K K_P$ where $L'_P \subseteq K(\rho)$ and L'_P/K is cyclic. Consider the cyclic algebra $B = \Delta(L'_P/K, \eta, g)$ where η generates the Galois group of L'_P/K and $g \in K[y]$ generates the prime ideal P. If Q is any other prime, then by the discussion after (4.4), we can compute that $\chi_Q(B) = 1$. On the other hand, if L''_P is the field amalgamation of L'_P and K_P, then $L_P \subseteq L''_P$ and $\chi_P(B) = f'_P$ defines $L''_P K_P$. It follows that $\chi_P(B') = f_P$ for some r.

Performing the above construction for all P such that $\chi_P(A) \neq 1$, we conclude that there are $[A_1], \cdots, [A_m]$ such that each A_i is split by some L_i/K where L_i/K is cyclic, $L_i \subseteq K(\rho)$, and $\chi_Q([A][A_1]^{-1} \cdots [A_m]^{-1}) = 1$ for all q. This implies that

$$[A] = [A_1] \cdots [A_m][B]$$

where $[B]$ is in the image of $\mathrm{Br}(K)$ and is split by $K(\rho)(t)$. If $B = B' \otimes_K K(t)$, then by our assumptions, $M_2(B')$ decomposes. By applying 4.15 we conclude that $M_2(A)$ decomposes. Q.E.D.

With 4.16 in hand, and using 4.10 and 4.11, we can now conclude some approximation and lifting properties for C_q extensions. We will limit ourselves to stating the lifting result because we believe it to be more natural.

COROLLARY 4.17. *Let $K \supseteq F$ be a field of the form $K_1(t_1, \cdots, t_r)$ where K_1 is a local or global field. Suppose T, M is a local F algebra and $T/M = K$. If L/K is a C_q Galois extension, then $L \oplus L$ lifts to a C_{2q} Galois extnsion of T.*

In [24], the lifting results of [23] were used to prove surjectivity results for the map from the Brauer group of a local ring to its residue field. However, the results of [24] were limited by the impossibility of lifting all 2 power cyclic extensions. The next corollary is an addition to corollary 3.6 of [24]. We omit its proof because it is a straightforward combination of 4.17 and the methods of [24].

COROLLARY 4.18. *Let T, M be a local F algebra. Set $K = T/M$. Assume $K = K_1(t)$ where K_1 is a local or global field. Then the map* $\mathrm{Br}(T) \to \mathrm{Br}(K)$ *is a surjection.*

Corollary 4.17 suggests that it would be worthwhile to ascertain whether this lifting property was special to the fields involved or was generally true. We next will observe that it is, in fact, special. The machinery of §2 will allow us to construct a C_q extension L/K such that $L \oplus \cdots \oplus L$ does not lift to any abelian extension.

THEOREM 4.19. *Suppose q, ρ are as above, and that $F(\rho)/F$ is not cyclic. Then*

there is a C_1 extension L/K such that the following holds. Let A be any finite abelian group containing C_q, and set $L' = \mathrm{Ind}_{C_q}^{A}(L/K)$. There is a local F algebra T, M with $T/M = K$ such that L' does not lift to T as an A-extension.

PROOF. First off, elementary group theory shows that it suffices to consider $A = C_s$ where $s = q2^r$. Theorem 4.10 and the calculation 4.14 show that it is equivalent to construct $A/K \in \mathscr{A}(F(\rho)/F)$ such that no $M_t(A)$ lifts to an element of $\mathscr{A}(F(\rho(s))/F)$. The choice of A is the obvious one. Let

$$H' = \mathrm{Gal}(F(\rho(s)/F), \qquad H = \mathrm{Gal}(F(\rho)/F)$$

and set N to be the $Z[H]$ module $M_2(H)$. Let K be the field $Q(F(\rho)/F, N)$. Use the "generic" cocycle c of $N = M_2(H)$ to form the crossed product

$$A = \Delta(F(\rho) \otimes K/K, H, c).$$

We will show that A/K is the desired algebra, for some T, M. Assume not. Then the proofs of 3.19 and 3.9 make it clear that the equivalent conditions of 3.19 hold for $F(\rho(s)) \supseteq F(\rho) \supseteq F$. Hence, if $f : M_2(H') \to M_2(H)$ is the natural map of H' modules, then $\eta(f) = [0]$. This being false by 2.7, we are done. Q.E.D.

Considering that the whole question started with an approximation property for global fields, it is worthwhile to state the approximation problem version of 4.19, which follows.

COROLLARY 4.20. *Suppose q, ρ are as above, and that $F(\rho)/F$ is not cyclic. Let A be a finite abelian group, with $A \supseteq C_q$. Then there is a field $K \supseteq F$, a discrete valuation v on K with completion K_v, and a C_q extension L/K_v, such that* $\mathrm{Ind}_{C_q}^{A}(L/K)$ *does not pull back to K.*

PROOF (outline). Assume not. Then there is a relative approximation property for $\mathscr{E}(C_q)$ and $\mathscr{E}(C_s)$, where $s = 2^r q$ and this has the obvious meaning. This immediately implies that if T, M is a discrete valuation F algebra, and $K = T/M$, then for any C_q extension L/K, some $L \oplus \cdots \oplus L$ would lift to a C_s extension of T. By the remark after 3.9, this implies the lifting for all T, M; which contradicts 4.19. Q.E.D.

§5. Lifting crossed products

Let G be a finite group, T, M a local F algebra, and S/T a G-Galois extension. In this section we will look at the question of whether $\mathrm{Br}(S/T) \to \mathrm{Br}((S/MS)/(T/M))$ is surjective. Note how a specific question of this

sort arose in §4, and how a partial answer was used to reach conclusions about cyclic Galois extensions. Our arguments have two highlights. First, we show how our question is related to older questions of whether algebras can be expressed in terms of cyclic algebras. Second, let p be a prime and let $Z(F,p,r)$ be the center of the generic division algebra $\mathrm{UD}(F,p,r)$. Then $Z(F,p,r)/F$ is retract rational.

To begin with, we must consider the corestriction map. We will use this map only in a limited context, so we will not give the most general definition. Suppose R is the semilocal F algebra and T/R is a G-Galois extension. There is an isomorphism $j_{T/R}: H^2(G,T^*)\to \mathrm{Br}(T/R)$ where j is defined via the crossed product construction. Suppose $H\subset G$ is a subgroup and S is the fixed ring of H in T. S is again semilocal. Cohomologically, one can define a transfer map $\mathrm{Tr}_{G/H}: H^2(H,T^*)\to H^2(G,T^*)$ (e.g. [4], p. 104). Using the isomorphisms $j_{T/R}$ and $j_{T/S}$, we have the corestriction map $\mathrm{Cor}_{S/R}: \mathrm{Br}(T/S)\to \mathrm{Br}(T/R)$. Note that the map we have defined is a special case of the construction in [15]. In particular, we can conclude that $\mathrm{Cor}_{S/R}$ does not depend on G or T but only on S/R.

From the basic properties of the transfer map (e.g. [4], p. 105), we conclude that if $[A]\in \mathrm{Br}(R)$, then $\mathrm{Cor}_{S/R}(S\otimes_R A)=[A]^n$ where $n=[G:H]$. Also, since the transfer map is a natural transformation, we conclude that if $\varphi: R\to R'$ is an F map of commutative F algebras, then

$$\begin{array}{ccc} \mathrm{Br}(T/S) & \longrightarrow & \mathrm{Br}(T'/S') \\ {\scriptstyle \mathrm{Cor}}\downarrow & & \downarrow{\scriptstyle \mathrm{Cor}} \\ \mathrm{Br}(T/R) & \longrightarrow & \mathrm{Br}(T'/R') \end{array} \tag{5.1}$$

commutes, where $T'=T\otimes_\varphi R'$ and $S'=S\otimes_\varphi R'$. Finally, if $S\supseteq S'\supseteq R$ then $\mathrm{Cor}_{S/R}=\mathrm{Cor}_{S'/R}\circ \mathrm{Cor}_{S/S'}$.

Turning to lifting questions, we have already seen that cyclic algebras behave well. Using the corestriction, we observe in the next proposition that this generalizes to groups with cyclic Sylow subgroups.

PROPOSITION 5.2. *Let T, M be a local F algebra. Set $K=T/M$. Suppose S/T is a G-Galois extension and $L=S\otimes_T K$. Assume $A=\Delta(L/K,G,c)$ has exponent a power, p^r, of a prime p. Further, assume that G has a cyclic p-Sylow subgroup of order p^s. then there is an Azumaya algebra $B=\Delta(S/T,G,c')$ such that $B\otimes_T K\cong A$ and B has exponent dividing p^s.*

PROOF. Let $P\subset G$ be a p-Sylow subgroup. Set $m=[G:P]$ and choose m'

such that $m'm \equiv 1(p^r)$. Let $A' = \Delta(L/K, G, d)$ be such that $[A'] = [A]^{m'}$. Denote by L', S' the fixed ring of P in L and S respectively. Note that we may assume $L' = S'/MS'$. We set A_1 to be the centralizer of L' in A'. Since P is cyclic, $A_1 = \Delta(L/L', \sigma, b)$ where σ generates P and $b \in (L')^*$. Since S' is semilocal, there is a $b' \in (S')^*$ such that b' is a preimage of b. Set $B_1 = \Delta(S/S', \sigma, b')$. Since $\mathrm{Cor}_{S'/R}([B_1]) \in \mathrm{Br}(S/T)$,

$$\mathrm{Cor}_{S'/R}([B_1]) = [B] \qquad \text{where } B = \Delta(S/T, G, d').$$

Using (5.1), $[B \otimes_T K] = \mathrm{Cor}_{L'/K}([A' \otimes_K L']) = [A']^m = [A]$. But A, B have equal degrees, so $B \otimes_T K \cong A$. Finally, $[B]$ is the image under the corestriction of an Azumaya algebra class with a representative of degree p^s, so $[B]$ has order dividing p^s, Q.E.D.

Now, as an immediate corollary of 5.2 we can prove the following.

COROLLARY 5.3. *Let $Z(F, p, r)$ be the center of the generic division algebra $\mathrm{UD}(F, p, r)$ of degree p, a prime. Then $Z(F, p, r)/F$ is retract rational.*

PROOF. By 3.11, we must show that Azumaya algebras of degree p have the lifting property. So let T, M be a local F algebra, set $K = T/M$, and let A/K be a central simple algebra of degree p. If $A = M_p(K)$, clearly A lifts. So we may assume A is a division algebra. Choose $L' \subseteq A$ to be a maximal separable subfield, so L'/K has degree p. Also choose $L_1 \supset L' \supset K$ such that L_1/K is Galois with group $G \subseteq S_p = G'$. Set $L = \mathrm{Ind}_G^{G'}(L_1/K)$. L splits A so $[A] = [A']$ where $A' = \Delta(L/K, S_p, c)$.

Extensions with group S_p have the lifting property. This can be seen in many ways, the most convenient is to note that if V is the standard degree p permutation representation of $F[S_p]$ and F' is the fixed field of S_p on $F_+(V)$, then F'/F is rational. Thus we can apply 3.11.

Using this, we choose an S_p Galois extension S/T such that $S \otimes_T K \cong L$. By 5.2, there is a $B' = \Delta(S/T, S_p, c')$ such that $B' \otimes_T K \cong A'$, and B' has exponent p. S_p has a subgroup, H, such that $[S_p : H] = p$. Let S' be the fixed ring of H in S. S' splits B' because, if r is the exponent of $B' \otimes_T S'$, then r divides $(p-1)!$ the degree of S/S'. But r divides p so $r = 1$. Hence ([7], p. 64) $[B'] = [B]$ where $S' \subseteq B$ is maximal commutative. In particular, B/T has degree p. Since $[B \otimes_T K] = [A]$, $B \otimes_T K \cong A$. Q.E.D.

We will end this paper by presenting a converse for 5.2. We do this by looking at concrete semilocal rings, and examining when algebras lift. So let K be a field, and L/K a G-Galois extension. Assume $P_1, \cdots, P_m \subseteq K[t]$ are maximal ideals

and $P = P_1 \cdots P_m$. Set R to be the localization $K[t]_P$, S to be $L \otimes_K R$, K_P to be $K[t]/P$, and $L_P = L \otimes_K K_P$. Note that $[A] \in \mathrm{Br}(K(t))$ is in the image of $\mathrm{Br}(R)$ if and only if $\chi_Q([A]) = 1$ for all $Q = P_j$. Also, R is Dedekind so we have the following exact sequence ([13]):

$$0 \longrightarrow \mathrm{Br}(R) \longrightarrow \mathrm{Br}(K(t)) \longrightarrow \bigoplus_{j=1}^{m} \chi(G_j) \longrightarrow 0$$

where G_j is the absolute Galois group of $K[t]/P_j$. We will identify $\mathrm{Br}(R)$ with its image in $\mathrm{Br}(K(t))$.

PROPOSITION 5.4. *$[A] \in \mathrm{Br}(L_P/K_P)$ is in the image of $\mathrm{Br}(S/R)$ if and only if $[A] = [B][B_1] \cdots [B_n]$ where:*

(i) *$[B]$ is in the image of $\mathrm{Br}(L/K)$.*

(ii) *Each $[B_i]$ has the form $\mathrm{Cor}_{L'/K}([\Delta(L''/L', \sigma, c)])$ where $H \subseteq G$ is a subgroup, L' is the fixed ring of H in L, and L'' is the fixed ring of $H' \subseteq H$ such that H/H' is generated by σ.*

PROOF. Suppose $[A]$ is the image of $[A'] \in \mathrm{Br}(S/R)$. We will use the comments and notation of (4.3). Since A' is Azumaya over R, $\chi_Q(A') = 1$ for all $Q = P_1, \cdots, P_m$. Let $Q_1, \cdots, Q_s$ be the primes such that A' has nontrivial characters at Q_i. Set f_i to be the character of A' at Q_i, and set $K_i = K[t]/Q_i$. The character f_i defines an extension L_i/K_i which is cyclic. Since S splits A', $L_i \subseteq L \otimes_K K_i$.

According to [9], p. 51, there is a cyclic algebra $A_i'' = \Delta(L_i(t)/K_i(t), \sigma, c)$ such that $\chi_Q(\mathrm{Cor}_{K_i(t)/K(t)}([A_i'])) = f_i$ if $Q = Q_i$ and $= 1$ otherwise. Note that from the argument in [9], one can see that c is in $K_i[t]$, and is, in fact, a product of the generators of the primes into which Q_i splits in $K_i[t]$. Set $[A_i']$ to be $\mathrm{Cor}_{K_i(t)/K(t)}([A_i''])$.

Since $\chi_Q([A_i']) = 1$ for any $Q = P_j$, $[A_i]$ can be considered to be in $\mathrm{Br}(R)$. We also claim that A_i' is split by S. Set $K_i' = K_i \cap L$. There is a cyclic extension L_i'/K_i' such that $L_i' \subset L$ and $L_i' \otimes_{K_i'} K_i \cong L_i$. An exercise in cohomology shows that $\mathrm{Cor}_{K_i(t)/K_i'(t)}([A_i''])$ has the form $[\Delta(L_i'(t)/K_i'(t), \sigma, N(c))]$ where N is the norm of $K_i(t)/K_i'(t)$. Since $L_i' \subseteq L$, $L(t)$ splits

$$[A_i'] = \mathrm{Cor}_{K_i'(t)/K(t)}(\mathrm{Cor}_{K_i(t)/K_i'(t)}([A_i'])).$$

Since $S \subseteq L(t)$ is Dedekind, $\mathrm{Br}(S) \to \mathrm{Br}(L(t))$ is injective so S splits $[A_i']$ considered as an element of $\mathrm{Br}(R)$.

Taken all together, $[A''] = [A'][A_1']^{-1} \cdots [A_m']^{-1}$ has trivial character at all primes and so is in the image of $\mathrm{Br}(K)$. Now we go modulo P. The image of A'' is

the B of the proposition. The naturality of the corestriction shows that the image of $[A_i']$ is $\mathrm{Cor}_{K_i'\otimes_K K_P/K_P}([\Delta(L_i'\otimes_K K_P/K_i'\otimes_K K_P, \sigma, d)])$ where d is the image of $N(c)$ under the natural map $K_i'\otimes_K R \to K_i'\otimes_K K_P$. Note that d is a unit by our description of c. If $H = \mathrm{Gal}(L_i'/K_i')$ and $H' = \mathrm{Gal}(L/L_i')$, and if $[B_i]$ is the image of $[A_i']^{-1}$, then $[B_i]$ satisfies 5.4(ii).

To prove the converse, note that an argument like that of 5.3 shows that the $[B_i]$'s lift to $\mathrm{Br}(S/R)$ and, of course, $[B]$ lifts because there is a map $\mathrm{Br}(K)\to \mathrm{Br}(R)$. Q.E.D.

With this calculation in hand, we can now prove:

THEOREM 5.5. *If F is a field and L/F is G-Galois, then $\mathscr{A}(L/F)$ has the lifting property if and only if every Sylow subgroup of G is cyclic.*

PROOF. Set $M = M_2(G)$, $K = Q(L/F, M)$, and $L_1 = L\otimes_F K$. If c is the "generic" cocycle of M, we form $A = \Delta(L_1/K, G, c)$. Our first claim is that A has exponent $n = [L : F]$. But if not, there is a $0 \neq r \in L[M]^G$ such that if U is the group $(L[M](1/r))^*/L^*$, then ε, considered as a cocycle of U, has exponent $m < n$. There is an exact sequence

$$0\to M \to U \to P \to 0$$

where P is a permutation module. Since $H^1(G, P) = (0)$, the map $H^2(G, M)\to H^2(G, U)$ is an injection. Hence, as a cocycle of M, c has exponent m. However, an exercise in cohomology shows that $H^2(G, M) = Z/nZ$, with the image of c forming a generator. This contradiction proves the claim.

With A/K as given, choose $P \subset K[t]$ such that $K[t]/P = K \oplus K$. Set $R = K[t]_P$. Let $A'/(K\oplus K)$ be the algebra $A \oplus M_n(K)$. If $\mathscr{A}(L/F)$ has the lifting property, then we observed in §1 that $\mathscr{A}(L/F)$ has the lifting property over semilocal rings. Hence $[A']$ is in the image of $\mathrm{Br}((L\otimes_F R)/R)$. By 5.4,

$$[A] = [A_1]\cdots[A_m]$$

where each $[A_i]$ has the form $\mathrm{Cor}_{K'/K}([\Delta(L'/K', \sigma, c)])$, with $L' \subseteq L\otimes_F K$ and with L'/K' being cyclic. Clearly, we may assume that all the L'/K' have prime power degree. Let $p \mid n$ and suppose p^r is the highest power of p dividing n. Since A has exponent n, some A_i must have exponent p^r, and the corresponding L'/K' then must have degree p^r. In other words, there must be subgroups $H' \lhd H \subset G$ such that H/H' is cyclic of order p^r. By elementary group theory, G has a cyclic p Sylow subgroup. As the converse follows easily from 5.2, we are done. Q.E.D.

REMARK. The proof of 5.5 can be modified to yield a converse to one of the basic observations of §4. Namely, suppose F, $\rho = \rho(q)$, $\rho' = \rho(s)$ are as in 4.14. If every $A/K \in \mathcal{A}(F(\rho)/F)$ has the property that $M_t(A)$ (for the appropriate t) lifts to an element of $\mathcal{A}(F(\rho')/F)$, then every such $M_t(A) \in \mathcal{A}(F(\rho')/F)$ decomposes.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Am. Math. Soc., Providence, 1961.

2. S. A. Amitsur and D. J. Saltman, *Generic abelian crossed products and p-algebras*, J. Algebra **51** (1978), 76–87.

3. M. Auslander and A. Brumer, *Brauer groups of discrete valuation rings*, Nederl. Akad. Wetensch. Proc., Ser. A, **71** (1968), 288–296.

4. J. W. S. Cassels and A. Frohlich, eds., *Algebraic Number Theory*, Thompson Book Co., Washington, D. C., 1967.

5. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Am. Math. Soc. **52** (1968), 1–19.

6. J.-L. Colliot-Thelene and J.-J. Sansuc, *La R-equivalence sur les Tores*, Ann. Sci. Ec. Norm. Sup. 4e serie **10** (1977), 175–230.

7. F. DeMeyer and E. Ingraham, *Separable Algebras Over Commutative Rings*, in Lecture Notes in Mathematics, No. 181, Springer-Verlag, Berlin/Heidelberg/New York, 1971.

8. S. Endo and T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975), 85–104.

9. B. Fein and M. Schacher, *Brauer groups of rational function fields over global fields*, in *Groupe de Brauer* (M. Kervaire and M. Ojanguren, eds.), Lecture Notes in Mathematics, No. 844, Springer-Verlag, Berlin/Heidelberg/New York, 1981.

10. E. Formanek, *The center of the ring of* 3×3 *generic matrices*, Linear Multilinear Algebra **7** (1979), 203–212.

11. E. Formanek, *The center of the ring of* 4×4 *generic matrices*, J. Algebra **62** (1980), 304–320.

12. L. Goldstein, *Analytic Number Theory*, Prentice Hall, Englewood Cliffs, N.J., 1971.

13. N. Jacobson, *Basic Algebra I*, W. H. Freeman, San Francisco, 1974.

14. N. Jacobson, *PI-Algebras*, Lecture Notes in Mathematics, No. 441, Springer-Verlag, Berlin/Heidelberg/New York, 1975.

15. M. A. Knus and M. Ojanguren, *A norm for modules and algebras*, Math. Z. **142** (1975), 33–45.

16. H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.

17. H. Miki, *On Grunwald–Hasse–Wang's theorem*, J. Math. Soc. Jpn. **30** (1978), 313–325.

18. M. Orzech and C. Small, *The Brauer Group of Commutative Rings*, Marcel Dekker, Inc., New York, 1975.

19. N. Popescu, *Abelian Categories with Applications to Rings and Modules*, Academic Press, London/New York, 1973.

20. C. Procesi, *Rings with Polynomial Indentities*, Marcel Dekker, New York, 1973.

21. I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

22. D. J. Saltman, *Azumaya algebras with involution*, J. Algebra **52** (1978), 526–539.

23. D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. **43** (1982), 250–283.

24. D. J. Saltman, *Generic algebras*, in *Brauer Groups in Ring Theory and Algebraic Geometry* (F. Oystaeyen and A. Verschoren, eds.), Lecture Notes in Mathematics, No. 917, Springer-Verlag, Berlin/Heidelberg/New York, 1982.

25. D. J. Saltman, *Generic structures and field theory*, in *Algebraists' Homage* (G. Seligman et al., eds.), American Mathematical Society, Providence, R.I., 1982.

26. Y. Sueyoshi, *A note on Miki's generalization of the Grunwald–Hasse–Wang theorem*, preprint.

27. R. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–58.

28. R. Swan, *Galois Theory*, in *Emmy Noether* (J. Brewer and M. Smith, eds.), Marcel Dekker, New York, 1981.

29. E. Voskrenskiy, *Stable equivalence of algebraic tori*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 3–10 (English transl.: Math. USSR Isv. **8** (1974), 1–7).

30. E. Witt, *Schiefkorper uber diskret bewerten Korpern*, J. für Math. **176** (1937), 31–44.

31. H. Zassenhaus, *On structural stability*, Commun. Algebra **8** (1980), 1799–1844.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY OF TEXAS
AUSTIN, TX 78712 USA