Invent. math. 77, 71-84 (1984)

Inventiones mathematicae
© Springer-Verlag 1984

Noether's problem over an algebraically closed field

David J. Saltman*

Department of Mathematics, The University of Texas at Austin, Austin, TX 78712, USA

In [8], Emmy Noether asked whether the following field extension was rational, that is, purely transcendental. Let G be a finite group, and F a field. Form the rational field $F(x(g)|g\in G)$. Let G act on this field via $g(x(h))=x(gh)$. The extension in question is $F(x(g)|g\in G)^G/F$, where the superscript denotes the fixed field. We denote $F(x(g)|g\in G)^G$ by $F(G)$.

Noether's problem can be phrased, then, as asking: for which F and G is $F(G)/F$ rational? Since [8], this question has been answered for various F and G. Virtually complete answers are known if G is abelian. To begin with, if G is abelian of exponent n, then Fischer, already in [6], showed that $F(G)/F$ is rational if F contains a primitive n^{th} root of one. In [13], Swan constructed the first example where $F(G)/F$ is not rational. In Swan's example, F is the rational field Q and G is the cyclic group of order 47. Voskresenski, Endo-Miyata, and Lenstra have classified the abelian groups G and global fields F for which $F(G)/F$ is rational.

The question we will deal with in this paper is the following case of Noether's problem. Is there a finite group G and an algebraically closed field F such that $F(G)/F$ is not rational? By Fischer's result, none of the previous counter-examples of Swan et al. can apply here. In this paper we construct groups, G, of prime power order q^9, such that $F(G)/F$ is not rational for F algebraically closed of characteristic prime to q.

Our proof makes essential use of the notion of retract rational (see [11]), whose definition we now recall. Let $F\subseteq K$ be fields. K/F is called retract rational if and only if K is the field of fractions of a domain S such that S satisfies the following. There is a localized polynomial ring $F[x_1,\dots,x_n](1/s)=R$ and F algebra maps $\varphi\colon S\to R$ and $\psi\colon R\to S$ such that $\psi\circ\varphi$ is the identity on S.

In this paper we, in fact, prove that $F(G)/F$ is not retract rational for the F, G referred to above. We construct an extension K/F with the property that

* The author is grateful for support from the Sloan Foundation and from the NSF grant #MCS-8303356

$F(G)/F$ and K/F are each retract rational if and only if G Galois extensions have the lifting property over local rings (see [11]). It then suffices to show that K/F is not retract rational. This is accomplished by using the explicit description of K/F to show that there is an element of the Brauer group of K which is unramified with respect to every discrete valuation F algebra domain with field of fractions K. This idea is a slight variant of the unramified Brauer group introduced in [12]. Actually, however, this phase of the argument is closely related to the proof by Artin and Mumford ([13]) that a certain unirational field is not rational.

It is important to note one more aspect of the proof in this paper. We construct the field K mentioned above by using an observation attributed to Hasse. Namely, assume G' has a normal central subgroup $N \subseteq G'$ and N has prime order q. Then extending a G'/N Galois extension to a G' Galois extension is equivalent to splitting a G'/N cyclotomic crossed product. The effect of this observation, detailed in section one, is that a description of G' Galois extensions can be put together from a description of G'/N Galois extensions and a generic splitting field. The above vague idea is made precise using the notions of dense representation and local projectivity introduced in [11]. This part of our argument should have further applications in Galois theory.

F is the base field throughout this paper and will always be assumed to be infinite. All algebras, rings or fields are F algebras. All maps between these objects, unless stated otherwise, are F algebra homomorphisms. We use $\rho(n)$ to denote a primitive n^{th} root of one. To say $\rho(n) \in F$ implies that the characteristic of F does not divide n. The $\rho(n)$ are chosen so that $\rho(nk)^k = \rho(n)$. For any ring R, R^* denotes the group of units of R. Local rings are displayed as T, M where $M \subseteq T$ is the maximal ideal. As a general rule, the restrictions or unique extensions of maps have the same symbol as the original.

In section one of this paper we assume a bit of familiarity with the Galois theory of commutative rings, for which [5] Chap. 3 is a good general reference. Let us now mention some special notation and terminology we employ. Saying that S/R is a Galois extension of commutative rings with group G includes a specified action of G on S. In keeping with this, an isomorphism of G Galois extensions is assumed to be a G map, that is, it preserves the G action. If $R = K$ is a field, then Galois extensions L/K need not have L a field; L, however, must be a direct sum of isomorphic fields. When L is not a field note that L/K could be a Galois extension in different ways and with different groups.

Let $\varphi: R \rightarrow R_1$ be a ring homomorphism. We let the symbol $\otimes_\varphi R_1$ mean tensoring by R_1 viewed as an R module via φ. If S/R is Galois, then $S \otimes_\varphi R_1/R_1$ is G Galois in a natural way. If S_1/R_1 is also G Galois and $S \otimes_\varphi R_1 \cong S_1$ as G Galois extensions, we say that φ realizes S_1/R_1.

In section one we will refer to the so-called embedding problem of Galois theory. For this the following definition is useful. Let G' be a finite group, N a normal subgroup and let $G = G'/N$. Suppose S/R is a G Galois extension. A $G' - S/R$ Galois extension is a G' Galois extension S'/R such that $S' \supseteq S$, $S = (S')^N$ and such that the induced action of G on S is the given one.

On several occasions we will use the following trick in order to show that certain G Galois extensions are isomorphic.

Lemma 0.1. *Let S/R, S_1/R_1 be G Galois extensions and $\varphi: R \to R_1$ a homomorphism. Then $S_1 \cong S \otimes_\varphi R_1$ if and only if φ extends to a G preserving homomorphism $\varphi: S \to S_1$.*

Proof. If $S_1 \cong S \otimes_\varphi R_1$, then the induced map $S \to S \otimes_\varphi R_1 \to S_1$ is G preserving. Conversely, let $\varphi: S \to S_1$ be a G map. φ induces a G map $\varphi_1: S \otimes_\varphi R_1 \to S_1$ such that φ_1 is the identity on R_1. If $I \subseteq S \otimes_\varphi R_1$ is the kernel of φ_1, then I is preserved by G and $I \cap R_1 = (0)$. An exercise using [5] page 81 shows that $I = (0)$ and so that φ_1 is injective. To show that φ_1 is surjective note that $\varphi_1(S \otimes_\varphi R_1)$ and S_1 must be equal modulo every maximal ideal of R_1 as they both have the same dimension. Q.E.D.

In constructing commutative ring extensions it is useful to make the following definition. Suppose R is a commutative ring and $f(z) \in R[z]$ is a polynomial. Set $R\{f(z)\} = R[z]/(f(z))$. The image of z in $R\{f(z)\}$ we call the canonical element. If $f_1(z), \ldots, f_s(z)$ are a set of polynomials, then we set $R\{f_1(z), \ldots, f_s(z)\}$ or $R\{f_i(z) | 1 \leqq i \leqq s\}$ to be $R[z_1, \ldots, z_s]/(f_1(z_1), \ldots, f_s(z_s))$. The canonical element of $R\{f_i(z) | 1 \leqq i \leqq s\}$ associated with $f_i(z)$ is the image of z_i.

Finally, we require some notation from the theory of Azumaya algebras and the Brauer group. If R is a commutative ring, $Br(R)$ will denote the Brauer group of R. If A/R is an Azumaya algebra, $[A]$ will denote the Brauer equivalence class of A. Crossed products will be written $\Delta(S/R, G, c)$ where S/R is G Galois and c is a 2-cocycle of G in S^*. If G is cyclic of order n, $R = K$ is a field, and $\rho(n) \in K$, then this crossed product also has the following form. Assume $a, b \in K^*$ and let $(a, b)_{n,k}$ be the algebra generated over K by α, β subject to the relations $\alpha^n = a$, $\beta^n = b$, and $\alpha\beta = \beta\alpha\rho(n)$. The subscripts n or K will be dropped if no confusion is possible.

Section one: Central extensions of Galois groups

We begin this section with a key observation attributed to Hasse. In order to make this observation, we must recall some elementary facts. Let G be a finite group and N the cyclic group of order q, a prime. We let G act on N trivially. Extensions of G by N are in one to one correspondence with the cohomology group $H^2(G, N)$. Explicitly, if G' is a group with central subgroup $N \subseteq G'$ such that $G'/N = G$, then an element of $H^2(G, N)$ is defined as follows. For each $g \in G$ choose a preimage $u(g) \in G'$. Now define $c(g, h)$, for $g, h \in G$, via the relation

$$u(g)u(h) = c(g, h)u(gh). \tag{1}$$

The elements $c(g, h)$ are in N and form a G 2-cocycle in N. Another choice of the $u(g)$'s yields a cohomologous 2-cocycle. The cohomology class of c in $H^2(G, N)$ is the element we are defining. Conversely, given an element of $H^2(G, N)$ one can choose a representative cocycle $c: G \times G \to N$ and then use (1) to define G'. For the rest of this section we fix $G', N, G = G'/N$, the $u(g)$'s, and the associated cocycle c. Since $u(1)$ can always be chosen to be 1, we can assume $c(1, g) = c(g, 1) = 1$ for all $g \in G$. In this paper, all cocycles will be assumed to be normalized in this way.

The above observation can be used in Galois theory to construct an obstruction to the so-called embedding problem. Let F be a field of characteristic not q, and containing $\rho(q)$. Choose a group embedding $\eta: N \rightarrow F^*$. Obviously, $\eta(N) \subseteq F^*$ is the set of q^{th} roots of one. Let $K \supseteq F$ be a field and L/K a G Galois extension. Denote by η^* the induced map $\eta^*: H^2(G, N) \rightarrow H^2(G, L^*)$. The embedding problem asks whether the G Galois extension L/K embeds in a $G' - L/K$ Galois extension L'/K. Since L' and L need not be fields, this problem has an easy answer which is essentially the observation of Hasse mentioned above. We include a proof because we will soon make use of the proof as well as the result.

Proposition 1.1. *Let G', L/K, etc. be as above. Then L' exists if and only if $\eta^*(\gamma) = 1$ in $H^2(G, L^*)$, where γ is the cohomology class of c.*

Proof. Suppose L' exists. Then L'/L has Galois group N. We can write $L' = L[z^q - a\}$ where $a \in L^*$. Denote by α the canonical element of L'. We can choose a and α such that $b(\alpha) = \alpha\eta(b)$ for all $b \in N$. As $N \subseteq G'$ is central, $(u(g))(\alpha) = \alpha d(g)$ for some $d(g) \in L^*$. Applying (1), we have that

$$u(g)(u(h)(\alpha)) = u(g)(\alpha d(h)) = \alpha d(g) g(d(h))$$

and

$$u(g)(u(h))(\alpha) = c(g, h) u(gh)(\alpha) = \alpha\eta(c(g, h)) d(gh).$$

Thus $d(g) g(d(h)) = \eta(c(g, h)) d(gh)$ and so the $d(g)$'s form a coboundary for $\eta(c)$. In consequence, $\eta^*(\gamma) = 1$.

Conversely, suppose $\eta^*(\gamma)$ is split. With $u(g)$ and $c(g, h)$ as above we can conclude that there are $d(g) \in L^*$ such that $d(g) g(d(h)) = \eta(c(g, h)) d(gh)$ for all $g, h \in G$. It follows that $d(g)^q$ is a 1-cocycle. Since $H^1(G, L^*) = (1)$, there is an $a \in L^*$ such that $g(a)/a = d(g)^q$. Set $L' = L\{z^q - a\}$ and let α be the canonical element of L'. Define $(u(g))(\alpha) = \alpha d(g)$ and $b(\alpha) = \alpha\eta(b)$ for $b \in N$. It is now easy to check that this defines an action of G' on L' extending that of G on L and that L'/K is G' Galois. Q.E.D.

The proof of 1.1 can be generalized in a number of ways. Contained in it is a construction of G' Galois extensions which can be done more generally and, over a field, is the only way to get G' extensions. For the first part, let S/R be a G Galois extension, where $F \subseteq R$. Defining $\eta: N \rightarrow S^*$ as above, assume that $\eta^*(\gamma) \in H^2(G, S^*)$ is split. The following lemma is an easy generalization of the argument in 1.1.

Lemma 1.2. *Let $d(g) \in S^*$ be such that $d(g) g(d(h)) = \eta(c(g, h)) d(gh)$. Assume $a \in S^*$ is such that $g(a)/a = d(g)^q$. If $S' = S\{z^q - a\}$, then S'/R is a G' Galois extension of S/R.*

Suppose the G Galois extension T'/T is given. We can use 1.2 to form a G' Galois extension in a very general way. Set $S''(T'/T) = T'[y(g) | g \in G](1/s)$ where s is the product of all the $y(g)$'s. The action of G on T' extends to an action on $S''(T'/T)$ via $g(y(h)) = y(gh)$. Change notation by setting $y = y(1)$, so $y(g) = g(y)$. Now form $S(T'/T) = S''(T'/T)\{z^q - g(y)/y | 1 \neq g \in G\}$. For $g \neq 1$, set $x(g) \in S(T'/T)$

to be the canonical element associated with the polynomial $z^q - g(y)/y$. Also set $x(1)=1$. The action of G on $S''(T'/T)$ extends to one on $S(T'/T)$ via

$$g(x(h)) = [x(gh)/x(g)]\,\eta(c(g,h)).$$

Finally, set $R(T'/T)$ to be $S(T'/T)^G$ and $S'(T'/T)$ to be $S(T'/T)\{z^q - y\}$. An exercise using [5] page 81 shows that $S(T'/T)/R(T'/T)$ is G Galois and so that $S(T'/T) \cong T' \otimes_T R(T'/T)$. By 1.2, $S'(T'/T)/R(T'/T)$ is Galois with group G'. Note that if T' is a domain then so are $S''(T'/T)$, $S(T'/T)$, and $S'(T'/T)$. In the rest of this section, when we make use of $S'(T'/T)$ etc. we will assume the elements y and $x(g)$ are the elements above and γ is the canonical element of $S'(T'/T)$ viewed as $S(T'/T)\{z^q - y\}$. We make this assumption even when the G Galois extension T'/T is denoted by different symbols.

The construction above is functorial in T'/T. That is, if $\varphi\colon T \to T_1$ is an F map, then φ induces a G preserving map $\varphi\colon T' \to T' \otimes_\varphi T_1$, and this extends, in an obvious way, to a G preserving map $\varphi'\colon S(T'/T) \to S(T' \otimes_\varphi T_1/T_1)$ and so to a G' map $\varphi'\colon S'(T'/T) \to S'(T' \otimes_\varphi T_1/T_1)$. Taking G (or G') fixed rings we have a map $\varphi'\colon R(T'/T) \to R(T' \otimes_\varphi T_1/T_1)$. Using this we conclude that,

$$S'(T' \otimes_\varphi T_1/T_1) \cong S'(T'/T) \otimes_{\varphi'} R(T' \otimes_\varphi T_1/T_1).$$

Consider, now, the case of a G Galois extension L/K where K is a field. Form $R = R(L/K)$, $S = S(L/K)$ and $S' = S'(L/K)$. Recall that F, and so K, are assumed infinite.

Lemma 1.3. *Suppose $L' \supseteq L \supseteq K$ is a $G' - L/K$ Galois extension. Then there is a $\varphi\colon R \to K$ such that $L' \cong S' \otimes_\varphi K$ and the induced G' map $\varphi\colon S' \to L'$ is the identity on L. If $0 \neq s \in R$, we can choose such a φ with $\varphi(s) \neq 0$.*

Proof. Examining the proof of 1.1, we see that $L' \cong L\{z^q - a\}$ where the canonical element α satisfies $u(g)(\alpha) = \alpha d(g)$, $g(d(h)) = [d(gh)/d(g)]\eta(c(g,h))$, and $g(a)/a = d(g)^q$. Define $\varphi\colon S' \to L'$ by setting φ to be the identity on L, $\varphi(y) = a$, $\varphi(x(g)) = d(g)$, and $\varphi(\gamma) = \alpha$. Recall that $y, x(g)$ and γ are as in the definition of S'. Anyway, φ is a well defined G' map and so taking the restriction of φ to R, we have $S' \otimes_\varphi K \cong L'$.

It remains to show that the density fact holds. For this purpose we set $V = \operatorname{Spec}(R)$. For any field $K' \supseteq K$, $\operatorname{Hom}_K(R, K')$ is in one to one correspondence with the G preserving maps $\varphi\colon S \to L \otimes_K K'$ which are the identity on L. In other words, the K' points of V correspond to choices $x'(g)$, $a' \in (L \otimes_K K')^*$ such that $g(a')/a' = x'(g)^q$ and $g(x'(h)) = [x'(gh)/x'(g)]\eta(c(g,h))$. Now consider $S_1 = L[w(g) \mid g \in G](1/t)$ where t is the product of all the $w(g)'s$ and G acts on S_1 via $g(w(h)) = w(gh)$. Set $w = w(1)$. If $R_1 = S_1^G$, then $U = \operatorname{Spec}(R_1)$ is a torus whose K' points are $(L \otimes_K K')^*$. If $(x'(g), a')$ is a K' point of V and w' is a K' point of U, then $(x'(g)g(w')/w', a'(w')^q)$ is another K' point of V. That is, there is an algebraic group action $U \times V \to V$. If $v \in V(K')$ and $u \in U(K')$, denote by uv the result of u acting on v. Note that, by working it through, if v corresponds to $\varphi\colon R \to K$ and uv corresponds to $\varphi''\colon R \to K$, then φ and φ'' realize isomorphic extensions L'.

From all of the above, it is clear that it suffices to prove that if $v \in V(K)$, $U(K)v \subseteq V(K)$ is Zariski dense. Recall that the ground field F is assumed infinite, and so K is an infinite field. If $\bar{K} \supseteq K$ is the algebraic closure, then one can check that $U(\bar{K})u = V(\bar{K})$. Also, R_1 is a localized polynomial ring so U is an open subset of affine space. It follows that $U(K)$ is dense in $U(\bar{K})$. Now the map $u \to uv$ is a regular map, so $U(K)v$ is dense in $U(\bar{K})v = V(\bar{K})$. Q.E.D.

Let S_0/R_0 be a G Galois extension, with R_0 an affine F algebra and S_0 a domain. We next will use the above lemma to show that $S'(S_0/R_0)/R(S_0/R_0)$ inherits nice properties of S_0/R_0. To be precise, let us repeat the definitions of two properties that appeared in [11] in connection with retract rational fields and lifting problems.

1) S_0/R_0 is called densely representing if for all fields $K \supseteq F$, all G Galois extensions L/K, and all $0 \neq s \in R_0$, there is a $\varphi: R_0(1/s) \to K$ such that φ realizes L/K.

2) S_0/R_0 is a local projective if the following holds. Let T, M be a local F algebra and let T'/T be G Galois. Set $L = T'/MT'$ and $K = T/M$. If φ: $R_0 \to K$ realizes L/K, there is a φ': $R_0 \to T$ such that φ' realizes T'/T and

$$\begin{tikzcd}
& T \arrow[dd] \\
R_0 \arrow[ur, "\varphi'"] \arrow[dr, "\varphi"'] & \\
& K
\end{tikzcd}$$

commutes.

The most important result of this section can now be stated.

Theorem 1.4. *Let S_0/R_0 be G Galois, $S' = S'(S_0/R_0)$ and $R = R(S_0/R_0)$. Assume S_0 is a domain.*

a) *If S_0/R_0 is densely representing for G Galois extensions, then S'/R is densely representing for G' Galois extensions.*

b) *If S_0/R_0 is a local projective for G Galois extensions, then S'/R is a local projective for G' Galois extensions.*

Proof. a) Let L'/K be G' Galois and set $L = (L')^N$. If $0 \neq s \in R$, then some coefficient of s, viewed as an element of $S(S_0/R_0)$, is nonzero. Call it s'. Choose φ_0: $R_0 \to K$ such that φ_0 realizes L/K and $\varphi_0(t) \neq 0$, where t is the G norm of s'. This implies that the induced map φ_1: $R(S_0/R_0) \to R(L/K)$ has $\varphi_1(s) \neq 0$. Now choose φ_2 as in Lemma 1.3 with $\varphi_2(\varphi_1(s)) \neq 0$. The map $\varphi_2 \circ \varphi_1$ is the one required.

b) Let T, M be a local F algebra and T'/T a G' Galois extension. Set $K = T/M$, $T'/MT' = L'$, $(T')^N = T''$ and $(L')^N = L = T''/MT''$. Suppose $\varphi: R \to K$ realizes L'/K. Then the restriction of φ to R_0 realizes L/K. Call this restriction φ_0. By assumption, there is a φ_0': $R_0 \to T$ which realizes T''/T and such that

$$\begin{tikzcd}
& T \arrow[dd] \\
R_0 \arrow[ur, "\varphi_0'"] \arrow[dr, "\varphi_0"'] & \\
& K
\end{tikzcd}$$

commutes. We also denote by φ''_0, φ'_0 and φ the corresponding G or G' maps $\varphi_0: S_0 \to L$, $\varphi'_0: S_0 \to T''$ and $\varphi: S' \to L'$. Identify T'' with $S_0 \otimes_{\varphi'_0} T$ and L with $S_0 \otimes_{\varphi_0} K$. The map $\varphi: S'(S_0/R_0) \to L'$ is determined by $x'(g) = \varphi(x(g))$, $a = \varphi(y)$, and $\alpha = \varphi(\gamma)$. Once again, $x(g)$, y and γ are as in the definition of $S'(S_0/R_0)$.

Since T is local, T'' is semilocal and so $T' \cong T''\{z^q - a'\}$. Let α' be the canonical element of T'. Then we can choose α' and a' so that $n(\alpha') = \alpha' \eta(n)$ for all $n \in N$. Arguing as before in the field case, $(u(g))(\alpha') = \alpha' e(g)$ for $e(g) \in (T'')^*$ with $g(e(h)) = [e(gh)/e(g)]\eta(c(g,h))$. If $\bar{e}(g)$ is the image of $e(g)$ in L, then $\bar{e}(g)$ and $x'(g)$ are both coboundaries for $\eta(c(g,h))$, so $\bar{e}(g)g(b)/b = x'(g)$ for some $b \in L^*$. Choose $b' \in (T'')^*$ a preimage of b, and change α' to $\alpha' b'$. The new $e(g)$ is a preimage of $x'(g)$. Also, set $\bar{\alpha}$ to be the image of α' in L'. One calculates that $\bar{\alpha}^{-1} u(g) n(\bar{\alpha}) = \eta(n) x'(g) = \alpha^{-1} u(g) n(\alpha)$, so $\bar{\alpha} = \alpha v$ where $v \in K^*$. Once again, there is a preimage $v' \in (T)^*$ and we can change α' to $\alpha' v'$. In other words, we can assume that α' is a preimage of α. Of course, then, a' is a preimage of a. Define $\varphi': S(S_0/R_0) \to T''$ by letting φ' be φ'_0 on S_0, setting $\varphi'(x(g)) = e(g)$, and setting $\varphi'(y) = a'$. Clearly φ' is a G map and its restriction to R is the desired lifting. Q.E.D.

The importance of 1.4 is that local projective densely representing G Galois extensions S/R are very well behaved for our purposes. The key fact is that G Galois extensions lift over local rings if and only if $q(R)/F$ is retract rational ([11]. 3.10). The actual theorem we prove in this paper is that there is a G such that $q(R)/F$ is not retract rational, for F algebraically closed. To this end, we must describe the construction of $S'(S_0/R_0)/R(S_0/R_0)$ in another way.

Theorem 1.5. *Let G, G' etc. be as above and assume S_0/R_0 is a G Galois extension with S_0 a domain. Let $c(g,h)$ be a normalized cocycle describing G' and let A be the central simple algebra $\Delta(q(S_0)/q(R_0), G, \eta(c))$. Then $q(R(S_0/R_0)) = K(A)(x)$ where $K = q(R_0)$, x is an indeterminant, and $K(A)$ is the generic splitting field of A defined in* [1] *and* [9].

Proof. Considering $K = q(R_0)$, it is easy to see that we may assume that $K = R_0$ is a field. Set $L = S_0$. Form the ring $T = L[z(g), z(g)^{-1} | 1 \neq g \in G]$ with G acting on T via $g(z(h)) = [z(gh)/z(g)]\eta(c(g,h))$. Here we have set $z(1) = 1$. Now $q(T^G) = q(T)^G = K(A)$ by [10] pages 212–213. Consider $S = S(L/K)$. Map $\varphi: T \to q(S)$ by setting $\varphi(z(g)) = x(g)$. As $x(g)^q = g(y)/y$, the $x(g)$'s are algebraically independent over L for $g \neq 1$, and so φ is an injection. Use φ to identify $q(T)$ with a subfield of $q(S)$. Choose $a \in q(T)$ with $g(a)/a = x(g)^q$. We have that a/y is G fixed; call it u. Then $q(T)(u)$ contains $x(g)$ for all $1 \neq g \in G$ and contains y, implying that $q(T)(u) = q(S)$. Also, $q(S)/F$ has transcendence degree the order of G, which is one more than the transcendence degree of $q(T)$. Hence u is transcendental over $q(T)$. Taking G fixed fields, we are done. Q.E.D.

Section two: Cyclotomic crossed products

Let μ be the group of units in the field F. We saw in the previous section that the Galois theory of central extensions leads one to consider crossed products with cocycles taking values in μ. We call these cyclotomic crossed products. If the cocycle takes values in $\mu(n)$, the n^{th} roots of one, we say the crossed product is n-cyclotomic. In this section we will characterize cyclotomic crossed products where the group is abelian. Some of these results are not actually needed but the results are suggestive and so worth writing down.

Before stating the first theorem, let us introduce some terminology. Consider a Kummer extension L/K where $L=K\{z^{n_i}-a_i|1\leqq i\leqq s\}$. We say $x\in K$ has an m^{th} root in L canonically if x has the form

$$y^m a_1^{r_1}\dots a_s^{r_s} \quad y\in K$$

where the r_i have the following property. If (m,n_i) is the g.c.d. of m and n_i, then r_i is a multiple of $m/(m,n_i)$. Of course, the point of all this is that x has an m^{th} root which is a product of an element of K^* and the canonical generators of L.

As a final bit of terminology, consider L/K the Kummer extension above. Assume $\rho(n_i)\in K$ for all i, and set α_i to be the canonical generator associated with the polynomial $z^{n_i}-a_i$. Then L/K is G Galois where G is abelian and generated by g_i defined as follows. Set $g_i(\alpha_j)=\alpha_j$ if $i\neq j$ and $g_i(\alpha_i)=\alpha_i\rho(n_i)$. In what follows, whenever we work with a Kummer extension L/K, this extension will be considered G Galois as above. (Remember L is not a field so this comment is not superfluous.) Also, the elements α_i and the automorphisms g_i will be as defined above.

Theorem 2.1. *Let A be the abelian crossed product $\Delta(L/K,G,c)$, where c takes values in μ. Then $[A]$ is a product of cyclic algebras $[(x\alpha,y\beta)_m]$ where x and y have m^{th} roots in L canonically, and α, β are in μ.*

Proof. Of course, we can write L/K as a Kummer extension which is G Galois as above. If the integers n_i are as above, we can assume that n_j divides n_i if $i\leqq j$.

We next use the description of abelian crossed products given in [2]. Let $z(g)\in A$ be such that $z(g)z(h)=c(g,h)z(gh)$, and $z(g)xz(g)^{-1}=g(x)$ for $x\in L$. We can assume that $z(1)=1$. Set $z_i=z(g_i)$. Now set, for $i\neq j$, $u_{ij}=z_iz_jz_i^{-1}z_j^{-1}$ and $b_i=(z_i)^{n_i}$. It was shown in [2] that the u_{ij}'s and b_i's are in L and completely describe A. In this case, the u_{ij}'s and b_i's are in μ because they are products of the $c(g,h)$'s.

The u_{ij}'s and b_i's satisfy relations which we now recall (see [2], page 78). Define $N_i(x)$ to be the norm of x with respect to the subgroup of G generated by g_i. Then one relation is that $N_j(u_{ij})=g_i(b_j)/b_j$. Also, $u_{ji}^{-1}=u_{ij}$. In our circumstance the u_{ij}'s and b_i's are G fixed so we have $(u_{ij})^n=1$ where $n=n_i$ or n_j.

The idea now is to change the u's and b's so as to construct a cyclic subalgebra of A. In general, one can replace $z(g)$ by any element of $z(g)L^*$. In particular, if $\gamma\in L^*$, we can change $z(g_1)$ to $\gamma z(g_1)$ and leave all other z's the same. One can then calculate that u_{1j} changes to $u_{1j}(\gamma/g_j(\gamma))$, b_1 changes to $N_1(\gamma)b_1$, u_j^1 becomes, of course, $(u_{1j}^{-1})(\gamma/g_j(\gamma))^{-1}$, and all other u's and b's remain the same. We saw above that each u_{1j} was an n_j root of one. It follows that we can choose γ to be a product of the α_i's for $i\neq 1$, so that $u_{1j}(\gamma/g_j(\gamma))=1$ for all $j\neq 1$. With this choice of γ, $N_1(\gamma)b_1$ will have the form

$$a_2^{r_2}\dots a_s^{r_s}b_1=(say) \quad yb_1 \tag{2}$$

since $N_1(\alpha_j)=(\alpha_j)^{n_1}$. Also, it is clear that y is an n_1 root in L canonically. Change notation so that u_{1j} and u_{j1} are 1, b_1 is (2), and all the other u's and b's are the same. Set A_1 to be the subalgebra of A generated by the new z_1 and α_1. Then $A_1 \cong (a_1, b_1)_{n_1}$ where a_1 and b_1 are as required. Let A_2 be the subalgebra generated by the z_i's and the α_i's for $i \geqq 2$. Since the u_{1j}'s are 1, A_1 and A_2 centralize each other. Checking degrees we have that $A \cong A_1 \otimes_K A_2$. Also, A_2 is a cyclotomic crossed product and we can proceed by induction. Q.E.D.

What we actually require in this paper is the converse to 2.1. That is, we are about to observe that products of cyclic algebras are similar to cyclotomic crossed products in the Brauer group.

Theorem 2.2. *Let $a_1, \dots, a_s \in K^*$, and set $L=K\{z^{n_i}-a_i \mid 1 \leqq i \leqq s\}$ for some n_i such that $\rho(n_i) \in F$. Assume that $(-1, -1)_{2,K}$ is split. Let $[A] \in Br(K)$ be such that $[A]$ is a product of algebras $[(x\alpha, y\beta)_m]$ where $\rho(m) \in F$, x and y have m^{th} roots in L canonically, and $\alpha, \beta \in \mu$. Let G be the (abelian) Galois group of L/K. Then A is Brauer similar to an n cyclotomic crossed product, where α, β and all the $\rho(n_i)$ are in $\mu(n)$.*

Proof. We will repeatedly use two reduction facts. If A_1, A_2 satisfy the conclusion, then so does $A_1 \otimes_K A_2$. Second, let $H \subseteq G$ be a subgroup, and $L' = L^H$. If $\Delta(L'/K, G/H, c')$ is an n cyclotomic crossed product, then so is the algebra $\Delta(L/K, G, c)$ gotten by inflation. It will also be useful to recall that, if d divides m, then $[(x^d, y)_m] = [(x, y^d)_m] = [(x, y)_{m/d}]$ and $[(x, -x)_m] = 1$.

Using the first reduction fact, we can assume that either $A = (a_i^r, a_j^q)_m$, $A = (a_i^r, \alpha)_m$ or $A = (\alpha, \beta)_m$ where $r = m/(m, n_i)$, $q = m/(m, n_j)$ and $\alpha, \beta \in \mu(n)$. In the last case, a straightforward exercise shows that $[A] = 1$ or $= [(-1, -1)_{2,K}]$. By assumption, then, $[A] = 1$ and so we can eliminate the last case.

For any x, $[(a_i^r, x)_m] = [(a_i, x)_{m'}]$ where $m' = (m, n_i)$. Since m' divides m, $m'/(m', n_j)$ divides $m/(m, n_j)$. Hence $[(a_i, a_j^q)_{m'}]$ is a power of $[(a_i, a_j^{q'})_{m'}]$ where $q' = m'/(m', n_j)$. This last algebra equals $[(a_i, a_j)_{m''}]$ where $m'' = (m', n_j)$. Althogether, we can assume that either $A = (\alpha_i, \alpha)_m$ for m dividing n_i or $A = (a_i, a_j)_m$ for m dividing n_i and n_j. In this last case, if $i = j$, then $(a_i, a_i)_m = (a_i, -1)$. Since this is covered by the first case, we may assume $i \neq j$.

If $L' = L\{z^m - a_i\}$, then we can identify L' with L^H for some subgroup $H \subseteq G$. The algebra $(a_i, \alpha)_m$ is clearly a cyclotomic crossed product with respect to L'/K, and so our inflation reduction fact eliminates this case. If $L' = L\{z^m - a_i, z^m - a_j\}$, L' is again of the form L^H. We set $u = \rho(m)$, $b_1 = b_2 = 1$ and use these to form the cyclotomic abelian crossed product $B = \Delta(L'/K, G/H, c)$. The proof of 2.1 shows that $[B] = [(a_i, a_j)_m]$. Once again, the inflation fact eliminates this last case. Q.E.D.

Remark. Hidden in the above proof is the following fact. If G is a finite abelian group of exponent n, and G acts on $\mathbf{Q}/\mathbf{Z}$ trivially, then $H^2(G, \mathbf{Q}/\mathbf{Z})$ has exponent dividing n. The exact sequence

$$0 \to \mathbf{Z}/n\mathbf{Z} \to \mathbf{Q}/\mathbf{Z} \xrightarrow{n} \mathbf{Q}/\mathbf{Z} \to 0$$

shows that the map $H^2(G,\mathbf{Z}/n\mathbf{Z})\to H^2(G,\mathbf{Q}/\mathbf{Z})$ is onto. Thus if F has enough roots of one, it can be seen directly that any cyclotomic crossed product using G is also an n cyclotomic one.

Section three: The unramified Brauer group and the example

We will show in this section that certain fields are not retract rational, and so not rational. We will do this by using the Brauer group to construct an invariant of fields which is zero for retract rational fields, and then show it is nonzero for our field. For convenience sake, from now on, assume F is an algebraically closed field.

The invariant we will define is almost identical to the invariant defined in [12]. To make the definition, recall the following fact. If R is a discrete valuation domain with field of fractions $q(R)=K$, then the Brauer group map $Br(R)\to Br(K)$ is a injection. Thus we can and will identify $Br(R)$ with a subgroup of $Br(K)$.

Definition 3.1. Suppose K/F is an extension of fields. Define $Br_v(K)\subseteq Br(K)$ to be the intersection of all $Br(R)$ where R is a discrete valuation domain with $q(R)=K$ and $F\subseteq R$.

Note that the above definition differs from the one in [12] because in [12] we considered all valuation domains, and not just the discrete ones. The two definitions coincide if K is the function field of a smooth proper F variety.

The following elementary properties of $Br_v(K)$ will be most useful to us.

Proposition 3.2. a) *If K/E is rational, $Br_v(K)=(0)$.*

b) *If $K\subseteq L$, then the natural map $Br(K)\to Br(L)$ sends $Br_v(K)$ into $Br_v(L)$.*

c) *If K/F is retract rational, then $Br_v(K)=(0)$.*

d) *If R is a smooth domain of finite type over F with $q(R)=K$, then $Br(R)\supseteq Br_v(K)$.*

Proof. All of the above facts were proved in [12] for the unramified Brauer group defined there. The proofs for $Br(K)$ are identical, and will mostly be left as an exercise. Let us simply recall that part d) above is a consequence of a result of Hoobler's ([7]), namely, that if R is a smooth domain of finite type over F, then $Br(R)=\cap Br(R_P)$, the intersection being over all height one primes of R.

Of course, considering 3.2c), it is clear that we intend to show a certain field is not retract rational by showing that Br_v of that field is not zero. The next lemma will give the form that our argument will take. But first, let us recall some notation and facts.

Let S be a discrete valuation domain and set $K=q(S)$. Let p be the characteristic of F. If A is an abelian group, let A' denote A if $p=0$ and denote the p prime part of A if $p\neq 0$. There is an exact sequence:

$$0\to Br(S)'\to Br(K)'\xrightarrow{\chi_S}\mathrm{Hom}_c(G_k,\mathbf{Q}/\mathbf{Z})'\to 0 \qquad (3)$$

where k is the residue field of S, G_k is the absolute Galois group of k, and Hom_c refers to continuous homomorphisms, where $\mathbf{Q}/\mathbf{Z}$ has the discrete topology. As G_k is compact, any $f \in \mathrm{Hom}_c(G_k, \mathbf{Q}/\mathbf{Z})$ has finite image. Since any finite subgroup of $\mathbf{Q}/\mathbf{Z}$ is cyclic, each element of $\mathrm{Hom}_c(G_k, \mathbf{Q}/\mathbf{Z})$ defines what we call the associated cyclic extension of k.

Lemma 3.3. *Let $L \supseteq K$ be an extension of fields and denote by* Res: *$Br(K) \to Br(L)$ the natural map. Recall that the kernel of* Res, *by definition, is the group $Br(L/K)$. Suppose that $\alpha \in Br(K)$ satisfies the following properties. First, if p is nonzero we assume that α has order prime to p. Also, that for any discrete valuation domain S, with $q(S) = K$, there is a $\beta \in Br(L/K)$ with $\chi_S(\alpha\beta) = 1$. Then* $\mathrm{Res}(\alpha) \in Br_v(L)$.

Proof. Let $R \subseteq L$ be any discrete valued domain with $q(R) = L$. Consider $S = K \cap R$. If $S = K$, $\mathrm{Res}(\alpha) \in Br(R)$ is clear. If $S \neq K$, then S is a discrete valuation domain with $q(S) = K$. Letting $\beta \in Br(L/K)$ be as above, we have by (3) that $\alpha\beta \in Br(S)$. Since $S \subseteq R$, $\mathrm{Res}(\alpha\beta) \in Br(R)$. Hence $\mathrm{Res}(\alpha) = \mathrm{Res}(\alpha\beta) \in Br(R)$. Since this is true for all R, we are done. Q.E.D.

With $S \subseteq K$ as above, and $a, b \in K^*$, it is quite easy to compute $\chi_S([(a,b)_n])$ if n is prime to p. To do this, we make use of the fact that $\mathrm{Hom}_c(G_k, \mathbf{Q}/\mathbf{Z})$ "measures" cyclic extensions of k. In fact, if we fix a root of one, $\rho(n)$, the n torsion part of $\mathrm{Hom}_c(G_k, \mathbf{Q}/\mathbf{Z})$ can be identified with $k^*/(k^*)^n$. Make this identification; let v be the normalized integer valued valuation of S; and denote by $\bar{x}$ the image in k of $x \in S$. Then $\chi_s([(a,b)_n])$ is exactly

$$\overline{(b^{v(a)}/a^{v(b)})}(-1)^{v(a)v(b)}.$$

The rest of this section has three parts. We will first construct a field and then use 3.3 to show that it is not retract rational. Next, we will relate this field to the construction of section one. And third, we will show how this proves that a certain $F(G)$, the field from Noether's problem, is not retract rational even though F is algebraically closed.

In order to describe the field we are going to construct, recall that if A/K is central simple, then we denoted by $K(A)$ the generic splitting field of A defined in [1] and [9]. It was proved in [1] that $Br(K(A)/K)$ was the group generated by $[A]$. If $A_1/K, \ldots, A_s/K$ are a set of central simple algebras, we can define, inductively, the generic splitting field $K(A_1, \ldots, A_s)$ to be the usual generic splitting field of $A_s \otimes_K K(A_1, \ldots, A_{s-1})$. We note two trivial properties. First, that $K(A_1, \ldots,, A_s)$ is independent of the order in which we list the A_i's. Second, that $Br(K(A_1, \ldots, S_s)/K)$ is the group generated by $[A_1], \ldots, [A_s]$.

We should reemphasize that F is assumed to be algebraically closed. Let q be a prime unequal to the characteristic of F.

Theorem 3.4. *Let $K = F(a,b,c,d)$ be the purely transcendental extension. Denote by L the generic splitting field $K\{(a,b)_q \otimes (c,d)_q, (a,c)_q, (a,d)_q, (b,c)_q, (b,d)_q\}$. Then L/F is not retract rational.*

Proof. It suffices to show that $[L] \neq [(a,b)_{q,L}] \in Br_v(L)$. Note that $(a,b)_{q,K} \otimes_K L \cong (a,b)_{q,L}$. Thus to show that $(a,b)_{q,L}$ is not trivial we must show that $[(a,b)_{q,K}]$ is not in the subgroup of $Br(K)$ generated by the above five algebras. Embed K into $\hat{K}=F((a,b,c,d))$, the iterated Laurent series field. Let $H\subseteq Br(\hat{K})$ be the subgroup of q torsion elements. By [4], H has rank 6. It is easy to see that $\{[(a,b)_q], [(a,c)_q], [(a,d)_q], [(b,c)_q], [(b,d)_q], [(c,d)_q]\}$ form a basis of H. This clearly implies what we want.

To prove $(a,b)_{q,L}\in Br_v(L)$, we, of course, use Lemma 3.3. So let $S\subseteq K$ be a discrete valuation ring with $q(S)=K$. Suppose that v and k are as above. We consider several cases. If $v(d)$ is prime to q, then

$$\chi_S([(b,d)_q])=\overline{(d^{v(b)}/b^{v(d)})} \bmod (k^*)^q \quad \text{and} \quad \chi_S([(a,d)_q])=\overline{(d^{v(a)}/a^{v(d)})} \bmod (k^*)^q.$$

Thus

$$\chi_S([(b,d)_q]^{v(a)}[(a,d)_q]^{-v(b)})=\overline{(b^{v(a)}/a^{v(b)})}^{-v(d)} \bmod (k^*)^q.$$

If $rv(d)\equiv 1\,(q)$,

$$\chi_S([(a,b)_q][(b,d)_q]^{v(a)r}[(a,d)_q]^{-v(b)r})=1.$$

As $[(b,d)_q]^{v(a)r}[(a,d)_q]^{-v(b)r}$ is in $Br(L/K)$, this case is done.

A similar argument applies if $v(c)$ is prime to q. Finally, if $v(c)$ and $v(d)$ are both divisible by q then $\chi_S([(c,d)_q])=1$ so $\chi_S([(a,b)_q][(a,b)_q\otimes(c,d)_q]^{-1})=1$. All together, Lemma 3.3 is satisfied in all cases and the theorem follows. Q.E.D.

The next step in our argument will show that the field L above is closely related to a densely representing local projective Galois extension S/R as studied in section one.

Theorem 3.5. *Let q be a prime unequal to the characteristic of F. Consider the field L defined above using this q. Then there is a q-group, G, and a densely representing local projective G Galois extension S/R such that $L\subseteq q(R)$ and $q(R)/L$ is rational.*

Proof. Let K be as in Theorem 3.4 and let $D_1,\ldots,D_5$ be the five central simple K algebras for which L is the generic splitting field $K(D_1,\ldots,D_5)$. Set $L_i=K(D_1,\ldots,D_i)$ and K' to be K with the qth roots of a,b,c, and d adjoined. The proof starts by observing that K is $q(R_0)$ where S_0/R_0 is a densely representing local projective Galois extension with Group G_0, the elementary abelian q-group of rank 4. In fact, $R_0=F[a,b,c,d](1/t)$ where $t=abcd$, and

$$S_0=R_0\{z^q-a, z^q-b, z^q-c, z^q-d\}.$$

Obviously $q(S_0)=K'$. An exercise shows that S_0/R_0 is densely representing and local projective as claimed.

By 2.2, D_1 is similar, in the Brauer group, to a q cyclotomic crossed product $A_1=\Delta(K'/K,G_0,c)$. Using 1.5 we see that there is a central extension of G_0 by $\mathbf{Z}/q\mathbf{Z}$, call it G_1, and a densely representing local projective G_1 Galois extension S_1/R_1, such that $q(R_1)=K(A_1)(x)$. Set K_1 to be $q(R_1)$. As $K(A_1)/K(D_1)$ is rational (see [9], page 413), we have that K_1/L_1 is rational.

By 2.2 again, D_2 is also similar to a q cyclotomic crossed product. Of course, the same is true of $D_2 \otimes_K K_1$. Using inflation, $D_2 \otimes K_1$ is similar to $A_2 = \Delta(q(S_1)/K_1, G_1, c)$ which is another q cyclotomic crossed product. Arguing as before, $K_1(A_2)(x) = q(R_2)$ where S_2/R_2 is a densely representing local projective G_2 Galois extension, G_2 being a central extension of G_1 by $\mathbf{Z}/q\mathbf{Z}$. Set $K_2 = q(R_2)$. Again, K_2/L_2 is rational. Proceeding in this way we are done. Q.E.D.

There are several things which should be noted in the above proof. First, each cocycle arises by inflation from a G_0 cocycle. It follows that the group G has a central subgroup N such that $G/N = G_0$ and N is an elementary abelian q-group of rank 5. However, the above construction does not uniquely determine G because the natural map $H^2(G_i, \mathbf{Z}/q\mathbf{Z}) \to H^2(G_i, \mu)$ is not injective. We can describe one group G fitting 3.5 as follows. G is generated by e, f, g, h, k, s, t, u, v such that all these elements have order q; e, f, g, h, k are all central, $sts^{-1}t^{-1} = e = uvu^{-1}v^{-1}$, $sus^{-1}u^{-1} = f$, $svs^{-1}v^{-1} = g$, $tut^{-1}u^{-1} = h$, and $tvt^{-1}v^{-1} = k$.

We can now state and quickly prove the example which is the whole point of this paper.

Theorem 3.6. *Let F be an algebraically closed field of characteristic unequal to the prime q. Let G be one of the q groups arising in* 3.5. *Set $K = F(x(g) \mid g \in G)$ and let G act on K in the usual way. Then $F(G) = K^G$ is such that $F(G)/F$ is not retract rational, and hence not rational.*

Proof. Let L be the field of 3.4 and S/R the densely representing local projective G Galois extension from 3.5. Since L/F is not retract rational, and $q(R)/L$ is rational, $q(R)/F$ is not retract rational ([11], 3.6). Hence G Galois extensions do not have the lifting property over local rings ([11], 3.10). But then by ([11], 3.12), $F(G)/F$ is not retract rational. Q.E.D.

Obviously, the method used will apply to more groups G than those covered by 3.5. For example, it applies to certain rank two nilpotent q groups with $N \subseteq G$ central and G/N elementary abelian of rank greater than or equal to five. What is lacking is a classification of the groups, even the rank two q groups, such that $F(G)/F$ is retract rational or even such that the above methods apply.

References

1. Amitsur, S.A.: Generic splitting fields of central simple algebras. Ann. Math. **62**, 8–43 (1955)
2. Amitsur, S.A., Saltman, D.J.: Generic abelian crossed products and p algebras. J. of Alg. **51**, 76–87 (1978)
3. Artin, M., Mumford, D.: Some elementary examples of unirational varieties which are not rational. Proc. London Math. Soc. **25**, 3rd series, 75–95 (1972)
4. Chang, C.: The Brauer group of an Amitsur field II. Proc. AMS **47** (no. 1), 22–24 (1975)
5. Demeyer, F., Ingraham, E.: Separable algebras over commutative rings. Lecture Notes of Mathematics, vol. 181. Berlin-Heidelberg-New York: Springer 1971
6. Fischer, E.: Die Isomorphie der Invarianten Körper der endlichen Abel'schen Gruppen linearen Transformationen. Gott. Nachr. pp. 77–80 (1915)

7. Hoobler, R.: A cohomological interpretation of the Brauer group of rings. Pac. J. Math. **86** (#1), 89–92 (1980)
8. Noether, E.: Gleichungen mit vorgeschriebener Gruppe. Math. Ann. **78**, 221–229 (1916)
9. Roquette, P.: On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras. Math. Ann. **150**, 411–439 (1963)
10. Roquette, P.: Isomorphisms of generic splitting fields of simple algebras. J. reine angew. Math. **214/215**, 207–226 (1964)
11. Saltman, D.: Retract rational fields and cyclic Galois extension. Israel J. Math. in press (1984)
12. Saltman, D.: Brauer groups and the center of generic matrices. J. of Algebra in press (1984)
13. Swan, R.: Invariant rational functions and a problem of Steenrod. Invent. Math. **7**, 148–158 (1969)

Oblatum 1-X-1983