

CYCLIC ALGEBRAS, SCHUR INDICES, NORMS AND GALOIS MODULES

JÁN MINÁČ, ANDREW SCHULTZ AND JOHN SWALLOW

To Paulo Ribenboim.

RÉSUMÉ. Soit p un nombre premier et supposons que K/F est une extension cyclique de degré p^n avec $\text{car}(F) \neq p$, dont le groupe de Galois est G . Au cours d'un article récent, nous avons établi des conditions précises pour que le $\mathbb{F}_p G$ -module $K^\times/K^{\times p}$ contienne une composante directe indécomposable de dimension qui n'est pas une puissance de p . Il existe au plus une telle composante et sa dimension doit être $p^i + 1$ avec $0 \leq i < n$ et, de plus, tout i avec $0 \leq i < n$ est possible. Notre théorème principal est un lien intéressant entre cette dimension et l'indice de Schur d'une certaine algèbre cyclique cyclotomique.

ABSTRACT. Let p be a prime and suppose that K/F is a cyclic extension of degree p^n with Galois group G , with $\text{char } F \neq p$. Let J be the $\mathbb{F}_p G$ -module $K^\times/K^{\times p}$ of p -th-power classes. In our previous paper we established precise conditions for J to contain an indecomposable direct summand of dimension not a power of p . At most one such summand exists, and its dimension must be $p^i + 1$ for some $0 \leq i < n$. We show that for all primes p and all $0 \leq i < n$, there exists a field extension K/F with a summand of dimension $p^i + 1$. The main theme is the investigation of an interesting link between this dimension and the Schur index of a certain cyclotomic cyclic algebra.

Introduction

Central simple algebras, representation theory, and Galois theory are among the favorite topics of Paulo Ribenboim. With the infectiousness of his enthusiasm, Paulo conveyed the beauty of these topics to his students, friends, colleagues, and to the readers of his work. Here we show an example of the natural interactions between these topics.

Let p be a prime and K/F a cyclic extension of fields of degree p^n with Galois group G . Assume further that $\text{char } F \neq p$. Let $K^\times$ be the multiplicative group of nonzero elements of K and

$$J = J(K/F) := K^\times / K^{\times p}$$

the group of p -th-power classes of K . We see that J is naturally an $\mathbb{F}_p G$ -module. In our previous paper [MSS1] we established the decomposition of J into indecomposables, as follows.

For $i \in \mathbb{N}$ let ξ_{p^i} denote a primitive p^i -th root of unity, and for $0 \leq i \leq n$ let K_i/F be the subextension of degree p^i , with $G_i = \text{Gal}(K_i/F)$. We adopt the convention that for all i , $\{0\}$ is a free $\mathbb{F}_p G_i$ -module.

Theorem ([MSS1, Theorems 1, 2, and 3]). *Suppose that*

- (1) F does not contain a primitive p -th root of unity or
- (2) $p = 2, n = 1$, and $-1 \notin N_{K/F}(K^\times)$.

Then

$$J \simeq \bigoplus_{i=0}^n Y_i,$$

where each Y_i is a free $\mathbb{F}_p G_i$ -module. Otherwise, let

$$m = m(K/F) := \begin{cases} -\infty & \text{if } \xi_p \in N_{K/F}(K^\times), \\ \min\{s : \xi_p \in N_{K/K_s}(K^\times)\} - 1 & \text{if } \xi_p \notin N_{K/F}(K^\times). \end{cases}$$

Then

$$J \simeq X \oplus \bigoplus_{i=0}^n Y_i,$$

where each Y_i is a free $\mathbb{F}_p G_i$ -module and X is an indecomposable $\mathbb{F}_p G$ -module of $\mathbb{F}_p$ -dimension $p^m + 1$ if $m \geq 0$ and 1 if $m = -\infty$.

It is not difficult to show directly that the decomposition is unique. (Alternatively, see the result of Azumaya [AF, p. 144].) This theorem is an extension of the main theorems in [MS1], and these results have already been applied to Galois embedding problems in [MS2] and [MSS2].

From the well-known result of Albert [A] concerning embedding a cyclic extension of degree p^i to a cyclic extension of degree p^{i+1} , we see that $\xi_p \in N_{K/K_s}(K^\times)$ for all $s \in \{0, 1, \dots, n\}$ if $m(K/F) = -\infty$ and $\xi_p \in N_{K/K_s}(K^\times)$ for all $s \in \{m+1, \dots, n\}$ if $m(K/F) > -\infty$. (In fact it is an easy exercise to show that $N_{K/K_i}(K^\times) \subseteq N_{K/K_j}(K^\times)$ if $i \leq j$ directly without referring to Albert's result.)

The submodules Y_i are produced naturally using norms from different layers of the tower of field extensions. However, the remaining submodule X is more mysterious, and we consider a first problem concerning the classification of all $\mathbb{F}_p G$ -modules occurring as $J(K/F)$.

Given $n \geq 1$ and d an element of the set

$$\{1, p^0 + 1, \dots, p^{n-1} + 1\},$$

does there exist a cyclic extension K/F with $\xi_p \in F^\times$ such that the exceptional summand X has dimension d ? (We remark that in the case of $n = 1$, $\xi_p \in F^\times$, the full realization problem—realizing all possible isomorphism classes for the $\mathbb{F}_p G$ -module $J(K/F)$ —has been solved [MS2].)

It turns out that we may answer this question in the affirmative using a construction of cyclic division algebras due to Brauer-Rowen. For a particular extension K/F with

$\text{Gal}(K/F) = \langle \sigma \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$, the cyclic algebra

$$A(K/F) = (K/F, \sigma, \xi_p)$$

will be investigated for its connection to the module-theoretic structure of $K^\times/K^{\times p}$. For instance, we will see in Section 1 that the invariant $m(K/F)$ above can be recast as

$$(1) \quad m(K/F) = \begin{cases} -\infty & \text{if } A(K/F) \text{ splits,} \\ \min\{s : K_s \text{ splits } A(K/F)\} - 1 & \text{otherwise.} \end{cases}$$

In Section 1 we begin by recalling basic facts about cyclic algebras, including the algebra $A(K/F)$. We go on to describe how the Schur index of $A(K/F)$ is bounded by $m(K/F)$. In some important cases these two invariants coincide; however, we show in Section 5 that we can have a strict inequality. Thus it appears that $m(K/F)$ is a genuinely new invariant of K/F .

Further investigation of $m(K/F)$ and its relation with the associated cyclotomic algebra $A(K/F)$ is of considerable interest. The case when this algebra is a division algebra is considered in the last section. We also highlight in Section 3 the interesting relations between the integer part function and the basic rule for cyclic algebras when passing to a cyclic extension. In Section 2 we show that $m(K/F) \in \{-\infty, 0\}$ in the case of local fields, and we provide examples for both cases. Finally, in Section 4 we show how to use just a simple observation about norms to bypass cyclic algebras and get a direct proof of Theorem 1.1. However, we stress the intrinsic interest of the relationship between $m(K/F)$ and the Schur index, and we hope that this paper will promote its further investigation.

1. Cyclic cyclotomic algebras, $m(K/F)$, Schur's index, and norms

First we reformulate $m(K/F)$ in terms of cyclic algebras and then we use the construction of Brauer-Rowen of suitable cyclic algebras. We will then prove the following theorem.

Theorem 1.1. *Let $n \in \mathbb{N}$ and $t \in \{-\infty, 0, 1, \dots, n-1\}$. Then there exists a cyclic extension K/F of degree p^n with $\xi_p \in F^\times$ and $m(K/F) = t$.*

Before turning to the proof of the theorem, we recall some basic facts about cyclic algebras. If L/E is a cyclic extension of degree $r > 1$, with Galois group $G = \text{Gal}(L/E) = \langle \tau \rangle$, and $b \in E^\times$, then

$$B = (L/E, \tau, b)$$

is a central simple algebra such that

$$B = \bigoplus_{0 \leq j < r} u^j L,$$

where $u^{-1}du = \tau(d)$ for all $d \in L$ and $u^r = b$. Thus B is an E -algebra of dimension r^2 over E . We say that $\deg B =: r$. If $B \simeq M_s(D)$, the matrix algebra containing

matrices of size $s \times s$ over some division algebra D , then we set $\text{ind } B = \sqrt{\dim_E D}$. We call $\text{ind } B$ the Schur index of B . We denote the order of $[B]$ in the Brauer group $\text{Br}(E)$ by $\exp B$. Finally, we observe the following important connection:

$$(2) \quad [B] = 0 \text{ in } \text{Br}(E) \iff b \in N_{L/E}(L^\times).$$

In this case, we say that B splits. For further details on cyclic algebras, we refer the reader to [P, Chapter 15] and [R, Chapter 7].

The particular cyclic algebra in which we will be most interested is the cyclotomic cyclic algebra

$$A(K/F) := (K/F, \sigma, \xi_p),$$

where here $\text{Gal}(K/F) = \langle \sigma \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$ and $\xi_p \in F$. Notice that equivalence (2) serves as justification for equation (1) from the introduction.

Proof of Theorem 1.1. We begin with a construction of Brauer-Rowen. (See [Br] for the original construction and see [R, § 7.3] and [RT, § 6] for some nice variations of Brauer's construction.)

First suppose $0 \leq t < n$. Set $q = p^{n-t}$ and let $K = \mathbb{Q}(\xi_q)(\mu_1, \dots, \mu_{p^n})$, where ξ_q is a primitive q -th root of unity and the μ_i 's are indeterminates over $\mathbb{Q}$. Observe that K has an automorphism σ of order p^n fixing $\mathbb{Q}(\xi_q)$ and permuting the μ_i cyclically.

Let $F = K^{\langle \sigma \rangle}$ be the subfield of K fixed by $\langle \sigma \rangle$ and, for each $1 \leq i \leq n$, let $K_i = K^{\langle \sigma^{p^i} \rangle}$. Then K/F is a cyclic extension of degree p^n satisfying $\mathbb{Q}(\xi_p) \subseteq F$, and $G = \langle \sigma \rangle = \text{Gal}(K/F)$. Denote by $\bar{\sigma}$ the restriction of σ to the subfield K_{t+1} .

Now $A = A(K/F)$ is Brauer-equivalent to the cyclic algebra $R = (K_{t+1}/F, \bar{\sigma}, \xi_q)$ by [P, Corollary 15.1b]. (See also Section 3 below.) Moreover, the construction of Brauer-Rowen shows that R is a division algebra of degree p^{t+1} and exponent p [R, Theorem 7.3.8]. Since $[A] = [R] \neq 0$, we have $\xi_p \notin N_{K/F}(K^\times)$.

For all $0 \leq i \leq n$, we have

$$(K/F, \sigma, \xi_p) \otimes_F K_i \simeq (K/K_i, \sigma^{p^i}, \xi_p)$$

by [D, Lemma 6, p. 74]. Therefore, since K_{t+1} is a maximal subfield of R , K_{t+1} splits A :

$$[A \otimes_F K_{t+1}] = 0 \in \text{Br}(K_{t+1}).$$

Therefore $\xi_p \in N_{K/K_{t+1}}(K^\times)$. Hence $m(K/F) \leq t$.

Suppose $m = m(K/F) < t$. We have seen that K_{m+1}/F splits A , but $m < t$ implies $p^{t+1} = \text{ind } A \leq [K_{m+1} : F] < p^{t+1}$, a contradiction (see [P, 13.4]). Hence $m(K/F) = t$.

Now suppose that $t = -\infty$. Let F be a number field containing ξ_p and, if $p = 2$, ξ_4 . Then the extension F^c/F obtained by adjoining all p -th-power roots of unity is the cyclotomic $\mathbb{Z}_p$ -extension of F . Let K/F be the subextension of degree p^n of F^c/F . Then $G = \text{Gal}(K/F)$ is cyclic and K/F embeds in a cyclic extension of F of degree p^{n+1} . Therefore $\xi_p \in N_{K/F}(K^\times)$, by a result of Albert [A], and hence $m(K/F) = -\infty$. $\square$

Example 1.2 (The case $n = 1$). We briefly describe how the case $n = 1$ may be handled quite simply. For the case $m(K/F) = 0$, we set $F = \mathbb{Q}(\xi_p)(X)$, where X is a transcendental element over $\mathbb{Q}(\xi_p)$, and $K = F(\sqrt[p]{X})$. Write $G = \text{Gal}(K/F)$ as $\langle \sigma \rangle$ with $\sigma(\sqrt[p]{X}) = \xi_p \sqrt[p]{X}$. Then the cyclic algebra $A = A(K/F)$ is a symbol algebra $A = \left(\frac{X, \xi_p}{F, \xi_p} \right)$. (See, for instance, [P, p. 284].) Furthermore,

$$-[A] = \left[\left(\frac{\xi_p, X}{F, \xi_p} \right) \right] = [(E/F, \tau, X)] \in \text{Br}(F),$$

where $E = F(\xi_{p^2})$ and $\tau(\xi_{p^2}) = \xi_p \xi_{p^2}$. However, it is an easy exercise (solved in [P, p. 380]) to show that $[(E/F, \tau, X)] \neq 0$. Hence A is not split, and $m(K/F) = 0$ as required. The $m(K/F) = -\infty$ case follows as in the end of the proof of Theorem 1.1.

2. Local fields

For extensions K/F of local fields, we may deduce that $m(K/F) \in \{-\infty, 0\}$, confirming [B]. In fact, since we need only the main theorem of local class field theory (see [Iw, Theorem 7.1]), our conclusion that $m(K/F) \in \{-\infty, 0\}$ is valid for all fields containing ξ_p which satisfy this theorem. A family of such fields was investigated by Neukirch and Perlis: fields k such that the pair $(G_k, \bar{k}^\times)$ is class formation in the sense of Artin-Tate [AT, Chapter 14]. In [NP, Theorem 2, p. 532], they prove that all such fields possess local class field theory. In particular, they point out that the field $\mathbb{Q}_p^a$ of all algebraic numbers in $\mathbb{Q}_p$, and similarly the field $\mathbb{R}^a$ of all real algebraic numbers, are examples of such fields.

First, we approach the conclusion with a continuation of our consideration of cyclic algebras, again writing A for the algebra $A(K/F)$ defined in Section 1. If $[A] = 0 \in \text{Br}(F)$, then $m(K/F) = -\infty$. Otherwise, since $\text{ind } A = \exp A$ for local fields (see [P, Corollary 17.10b]), the local invariant $\text{inv}_F A$ of A is s/p with $s \in \mathbb{N}, p \nmid s$. Because

$$\text{inv}_E(A \otimes_F E) = [E : F] \text{inv}_F A$$

(see [P, Proposition 17.10]), we obtain that $\text{inv}_{K_1}(A \otimes_F K_1) = 0$. Hence

$$[A \otimes_F K_1] = 0 \in \text{Br}(K_1)$$

and $m(K/F) = 0$, as desired. (Indeed, this same argument shows that any exponent p central simple algebra over a local field is split by every extension of degree p .)

Alternatively, we prove that $m(K/F) \in \{-\infty, 0\}$ directly, without using cyclic algebras. Suppose that K/F is a cyclic extension of local fields of degree p^n . Assume that $\xi_p \in F$ and $\xi_p \notin N_{K/F}(K^\times)$. We want to show that $\xi_p \in N_{K/K_1}(K^\times)$.

Consider the natural map

$$F^\times / N_{K/F}(K^\times) \longrightarrow K_1^\times / N_{K/K_1}(K^\times),$$

induced by the inclusion $F^\times \hookrightarrow K_1^\times$. (Recall that under the inclusion map, we have $N_{K/F}(K^\times) \subseteq N_{K/K_1}(K^\times)$.) From [Iw, Theorem 7.1], we see that

$$F^\times / N_{K/F}(K^\times) \simeq \text{Gal}(K/F) = C_{p^n}$$

and

$$K_1^\times / N_{K/K_1}(K^\times) = \text{Gal}(K/K_1) \simeq C_{p^{n-1}}.$$

The natural map is therefore a group homomorphism with nontrivial kernel. Because the element

$$\xi_p N_{K/F}(K^\times) \in \frac{F^\times}{N_{K/F}(K^\times)}$$

generates the smallest nontrivial subgroup of $\frac{F^\times}{N_{K/F}(K^\times)}$, we see that $\xi_p N_{K/F}(K^\times)$ belongs to the kernel of this map and $\xi_p \in N_{K/F}(K^\times / K_1^\times)$, as required.

Now suppose F is a local field containing $\xi_{p^{n+1}}$ and suppose $a \in F^\times$ is such that $a \notin F^{\times p}$ if $p > 2$ or $a \notin -4F^{\times 4}$ if $p = 2$. Let $K = F(\sqrt[n]{a})$. Then we see that K/F is a cyclic extension of degree p^n . (See [La, Theorems 8.1 and 9.1].) Furthermore, because $N_{K/F}(\xi_{p^{n+1}}) = \xi_p$, we conclude that $m(K/F) = -\infty$.

Example 2.1 (A case of $m(K/F) = 0$). Following [HS, § 3], we provide a simple example of a local field extension with $m(K/F) = 0$. Dirichlet's theorem shows that there exists a prime q such that

$$q = 1 + p^n + kp^{n+1} = 1 + p^n(1 + kp)$$

for some $k \in \mathbb{N} \cup \{0\}$. For such q we know on the one hand that $\xi_{p^n} \in \mathbb{Q}_q$ and $\xi_{p^{n+1}} \notin \mathbb{Q}_q$ (see [Ko, § 3.3]). On the other hand, by [Ko, § 3.3], we know that $\mathbb{Q}_q(\xi_q)$ is a totally ramified cyclic extension of $\mathbb{Q}_q$ of degree $q - 1$. Let $K/\mathbb{Q}_q$ be the cyclic extension $K \subseteq \mathbb{Q}_q(\xi_q)$ of degree p^n . Then by [HS, Proposition 4.1], we see that K cannot be embedded into a cyclic extension $L/\mathbb{Q}_q$ of degree p^{n+1} . Hence $m(K/\mathbb{Q}_q) = 0$.

3. Cocycles, carrying, and cyclic algebras

In the proof of Theorem 1.1, we used [P, Corollary 15.1b]: *Let $F \subseteq K \subseteq E$ be a tower of cyclic extensions such that $G = \text{Gal}(E/F) = \langle \sigma \rangle$, $\bar{\sigma}$ be the restriction of σ on K , and $[E : F] = a = bq$, where $b = [K : F]$ and $q = \frac{a}{b}$. Then*

$$[(K/F, \bar{\sigma}, \alpha)] = [(E/F, \sigma, \alpha^q)] \in \text{Br}(F)$$

for each $\alpha \in F^\times$.

In [P] the proof of this corollary uses a case-by-case calculation of cocycles. We feel that because of this, a beautiful and interesting connection between the integer parts of rational numbers and cohomology may be lost. We shall here highlight this connection.

For $r \in \mathbb{Q}$, let $[r] \in \mathbb{Z}$ denote the integer part of $r \in \mathbb{Q}$, that is, the value $[r]$ satisfying $[r] \leq r < [r] + 1$. As in [P, p. 278], the essential part of the proof of this statement is to prove that the following two cocycles Ψ_α and Φ_{α^q} determine the same cohomology class in $H^2(G, E^\times)$:

$$\Psi_\alpha(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } k + l < b, \\ \alpha & \text{if } k + l \geq b, \end{cases}$$

where $i = b\left[\frac{i}{b}\right] + k$ and $j = b\left[\frac{j}{b}\right] + l$, and

$$\Phi_{\alpha^q}(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < a, \\ \alpha^q & \text{if } i + j \geq a, \end{cases}$$

where $0 \leq i, j < a$.

Let $M = \langle \alpha \rangle$ be the subgroup of $F^\times$ (and therefore also $E^\times$) generated by α . Then we show that our cocycles Ψ_α and Φ_{α^q} already determine the same cohomology class in $H^2(G, M)$ and therefore by naturality also the same class in $H^2(G, E^\times)$.

Both classes in $H^2(G, M)$ determine the group extensions $[\Psi_\alpha]$ and $[\Phi_{\alpha^q}]$ of shapes

$$1 \longrightarrow M \longrightarrow H_\Psi \longrightarrow G \longrightarrow 1$$

and

$$1 \longrightarrow M \longrightarrow H_\Phi \longrightarrow G \longrightarrow 1.$$

Choose lifts $\hat{\sigma} \in H_\Psi$ and $\tilde{\sigma} \in H_\Phi$ for $\sigma \in G$, and let $0 \leq i, j < a$ be given. As above, write $i = b\left[\frac{i}{b}\right] + k$ and $j = b\left[\frac{j}{b}\right] + l$, and also write $i + j = a\left[\frac{i+j}{a}\right] + \bar{i} + \bar{j}$. On the one hand, notice that if $k + l < b$, then we have both $\left[\frac{i}{b}\right] + \left[\frac{j}{b}\right] = \left[\frac{i+j}{b}\right]$ and $\hat{\sigma}^i \hat{\sigma}^j = \hat{\sigma}^{i+j}$, so

$$\hat{\sigma}^i \alpha^{\left[\frac{i}{b}\right]} \hat{\sigma}^j \alpha^{\left[\frac{j}{b}\right]} = \hat{\sigma}^{\bar{i} + \bar{j}} \alpha^{\left[\frac{i+j}{b}\right]}.$$

If, on the other hand, we have $k + l \geq b$, then $\left[\frac{i}{b}\right] + \left[\frac{j}{b}\right] + 1 = \left[\frac{i+j}{b}\right]$; since

$$\hat{\sigma}^i \hat{\sigma}^j = \hat{\sigma}^{\bar{i} + \bar{j}} \alpha$$

by our cocycle condition, this gives

$$\hat{\sigma}^i \alpha^{\left[\frac{i}{b}\right]} \hat{\sigma}^j \alpha^{\left[\frac{j}{b}\right]} = \hat{\sigma}^i \hat{\sigma}^j \alpha^{\left[\frac{i}{b}\right] + \left[\frac{j}{b}\right]} = \hat{\sigma}^{\bar{i} + \bar{j}} \alpha^{\left[\frac{i}{b}\right] + \left[\frac{j}{b}\right] + 1} = \hat{\sigma}^{\bar{i} + \bar{j}} \alpha^{\left[\frac{i+j}{b}\right]}.$$

From this calculation we learn two things: first, that the map $\gamma : H_\Phi \rightarrow H_\Psi$ defined by

$$\begin{cases} \gamma(\tilde{\sigma}^i) &= \hat{\sigma}^i \alpha^{\left[\frac{i}{b}\right]}, \\ \gamma(\alpha) &= \alpha, \end{cases}$$

is an isomorphism between $[\Phi_{\alpha^q}]$ and $[\Psi_\alpha]$, thus completing our proof; and, second, that the cocycle Ψ_α is essentially the difference $\left[\frac{i+j}{b}\right] - \left[\frac{i}{b}\right] - \left[\frac{j}{b}\right]$. More specifically, this difference is the logarithm of Ψ_α with base α . (That “carrying” is a cocycle was already observed in [Is].)

The referee of this article introduced us to the following elegant and conceptual alternative proof of the main result of this section. This proof also shows that this statement is a straightforward consequence of the bilinearity of the cup product.

Let Γ be the Galois group of a separable closure F_s of F containing E . Let $\chi \in H^1(\Gamma, \mathbb{Q}/\mathbb{Z})$ be the character of Γ given by $\chi(\gamma) = k/a$, where the restriction of γ to E is σ^k . Let $\partial\chi$ be the image of χ under the connecting map ∂ ,

$$\partial : H^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \rightarrow H^2(\Gamma, \mathbb{Z})$$

associated with $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$. Viewing a given $\beta \in F^\times$ as an element in $H^0(\Gamma, F_s^\times)$, one can then check through explicit cocycle calculations that

$$\partial\chi \cup \beta = [(E/F, \sigma, \beta)] \in \text{Br}(F) \simeq H^2(\Gamma, F_s^\times).$$

In the case where $\beta = \alpha^q$, we have on the one hand $\partial\chi \cup \alpha^q = [(E/F, \sigma, \alpha^q)]$. On the other hand, the cup product's bilinearity gives $\partial\chi \cup \alpha^q = \partial(q\chi) \cup \alpha$, and since $q\chi$ is the character of Γ associated with K/F (and its generator $\bar{\sigma}$), we therefore have $\partial(q\chi) \cup \alpha = [(K/F, \bar{\sigma}, \alpha)]$, as desired.

4. Bypassing cyclic algebras with a norm calculation

Brauer-Rowen's construction of the cyclic algebras above suggests replacing $\mathbb{Q}(\xi_q)(\mu_1, \dots, \mu_{p^n})$ by any quotient field L of a unique factorization domain D . Let $U(D)$ be the group of units of D . In this case we have the following proposition.

Proposition 4.1. *Let G be a group of order n acting on a unique factorization domain D as a group of n distinct automorphisms of D . Assume also that $U(D)$ is a G -invariant subgroup of D . Then*

$$N_{L/L^G}(L) \cap U(D) = U(D)^n.$$

Proof. If $u = w^n \in U(D)^n$ for some $w \in U(D)$, then $u = N_{L/L^G}(w)$ and therefore

$$U(D)^n \subseteq N_{L/L^G}(L) \cap U(D).$$

Assume now that $u \in U(D) \cap N_{L/L^G}(L)$. Then $u = N_{L/L^G}(w)$, where

$$w = d \frac{p_1 \cdots p_t}{q_1 \cdots q_s},$$

$d \in U(D)$ and $p_1, \dots, p_t, q_1, \dots, q_s$ are primes in D .

Therefore

$$\left(\prod_{g \in G} \prod_{i=1}^s g(q_i) \right) N_{L/L^G}(w) = d^n \prod_{g \in G} \prod_{i=1}^t g(p_i).$$

From the unique factorization property of D , we conclude that $t = s$ and for each $i \in \{1, \dots, t\}$ there exists $g \in G, j \in \{1, \dots, t\}$ and $d_i \in U(D)$ such that

$$p_i = d_i g(q_j).$$

Hence $N_{L/L^G}(p_i) = d_i^n N_{L/L^G}(q_j)$, and we see that

$$u = N_{L/L^G}(w) = d^n \prod_{i=1}^t d_i^n \in U(D)^n. \quad \square$$

Using the proposition above, one can directly see, without the use of cyclotomic cyclic algebras, that the example employed in our original proof, namely

$$K/F = \mathbb{Q}(\xi_q)(\mu_1, \dots, \mu_{p^n}) / (\mathbb{Q}(\xi_q)(\mu_1, \dots, \mu_{p^n}))^{(\sigma)},$$

with $q = p^{n-t}$, works. In fact the following alternative theorem provides more examples. (We leave out the easy case when $t = -\infty$.)

Theorem 4.2. Let $\xi_{p^{n-t}} \in F$ but $\xi_{p^{n-t+1}} \notin F$, where $t \in \{0, 1, \dots, n-1\}$. Let C_{p^n} act on $L = F(\mu_1, \dots, \mu_{p^n})$ by extending a faithful linear representation $\psi : C_{p^n} \rightarrow GL_{p^n}(F)$ on an F -vector space $V \subseteq L$ generated by $\mu_1, \dots, \mu_{p^n}$. Let E be a fixed field of C_{p^n} . Then $m(L/E) = t$.

Proof. Set

$$D = F[\mu_1, \mu_2, \dots, \mu_{p^n}].$$

Then D is a unique factorization domain. Moreover, $L = F(\mu_1, \dots, \mu_{p^n})$ is the quotient field of D , and C_{p^n} acts naturally on L via an extension of the action from V to L . Then by Galois theory we obtain a chain of fields

$$E = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n = L,$$

where L_i is the fixed subfield of L under the cyclic subgroup C_i of order p^{n-i} . Then we deduce

$$\begin{aligned} \xi_p \in N_{L/L_i} &\iff \xi_p \in D^{p^{n-i}} \\ &\iff \xi_{p^{n-i+1}} \in F \\ &\iff n-i+1 \leq n-t \\ &\iff t+1 \leq i. \end{aligned}$$

Hence $m(L/E) = t$. □

5. Invariants m and $\text{ind } A$

The proof of Theorem 1.1 turns on the fact that for the particular extension K/F we have $\text{ind } A = p^{m+1}$. It is interesting to ask whether this equality holds generally. We show in this section that the answer is negative.

We begin with the inequality

$$\text{ind } A \leq p^{m+1}$$

as follows. Observe that by the definition of $m(K/F)$,

$$[A \otimes_F K_{m(K/F)+1}] = 0 \in \text{Br}(K_{m(K/F)+1})$$

for $m(K/F) \neq -\infty$. Hence the inequality holds in the case $m(K/F) \neq -\infty$. The statement also holds for $m(K/F) = -\infty$, since A splits if and only if $m(K/F) = -\infty$; in fact, in this case we obtain an equality.

We show that equality does not always hold by considering the following example in the number field case. Recall first that for number fields $\exp A = \text{ind } A$. (See, for instance, [P, Theorem 18.6].) Therefore $\text{ind } A$ is either 1 or p , since the exponent of A divides p :

$$[\otimes^p A] = [(K/F, \sigma, 1)] = 0 \in \text{Br}(F).$$

Hence it is enough to produce a case when $m(K/F) > 0$.

Let $p = 2$, $c \in 4\mathbb{Z} \setminus \{0\}$, $a = 1 + c^2 \notin \mathbb{Z}^2$, and $d \in \{1, -1\}$ such that $d(a + \sqrt{a})$ is not a sum of two squares in $\mathbb{Q}_2$. (For example, take $a = 17$ and $d = -1$.) It is

well-known that

$$F = \mathbb{Q} \subseteq K_1 = \mathbb{Q}(\sqrt{a}) \subseteq K_2 = \mathbb{Q}\left(\sqrt{d(a + \sqrt{a})}\right)$$

is then a tower of fields with K_2/F cyclic of order 4. (See [JLY, p. 33].)

Let $\hat{K}_i$, with $i = 1, 2$, denote the completion of K_i with respect to any valuation v on K_i which extends the 2-adic valuation on $\mathbb{Q}$. Since $8 \mid a - 1$, we have $\hat{K}_1 = \mathbb{Q}_2$ and then we may and do assume that $\hat{K}_1 = \mathbb{Q}_2 \subseteq \hat{K}_2$.

Since $d(a + \sqrt{a})$ is not a sum of two squares in $\mathbb{Q}_2$, the quaternion algebra

$$(d(a + \sqrt{a}), -1)_{\mathbb{Q}_2}$$

is nonsplit. Hence $-1 \notin N_{\hat{K}_2/\mathbb{Q}_2}(\hat{K}_2)$ and therefore $-1 \notin N_{K_2/K_1}(K_2^\times)$. (See [P, p. 353].) We then obtain that $m(K/F) = 1$.

6. When A is a division algebra

Observe that if A is a division algebra, then $\text{ind } A = p^n$ and the chain of inequalities

$$p^n = \text{ind } A \leq p^{m+1} \leq p^n$$

forces the equality $\text{ind } A = p^{m+1}$. In this section we show how a natural construction gives additional field extensions L_{n-k}/F_{n-k} with $\text{ind } A = p^{m+1} = p^{k+1}$ for every $k < n$.

More precisely, we shall construct a tower of extensions

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

and a corresponding tower of induced extensions $L_i := KF_i$ with the following properties: $[F_{i+1} : F_i] = p$, for $i < n$; $[L_i : F_i] = p^n$; and L_i/F_i is a cyclic extension with $\text{Gal}(L_i/F_i) = \langle \sigma_i \rangle$. Since the extensions L_i and F_{i+1} are linearly disjoint over F_i , the cyclotomic algebras

$$A_i = (L_i/F_i, \sigma_i, \xi_p) \quad \text{and} \quad A_{i+1} = (L_{i+1}/F_{i+1}, \sigma_{i+1}, \xi_p)$$

are related by $A_{i+1} = A_i \otimes_{F_i} F_{i+1}$. (See [D, Lemma 7, p. 74].) Then, passing from A_i to A_{i+1} , the index of A_{i+1} will either remain that of A_i or drop by a factor of p . We shall choose F_{i+1} in such a way that ξ_p will be a norm from L_{i+1} to a subfield whose codimension's p -factor is one larger than at the i -th step. This will guarantee that $p \cdot \text{ind } A_{i+1} = \text{ind } A_i$, and we shall have full control of the behavior of $\text{ind } A_i$ for each i .

Proposition 6.1. *Suppose that A is a division algebra. Set $F_i = F(\xi_{p^i})$ and $L_i = K(\xi_{p^i})$ for each $i = 1, 2, \dots, n$. Further set $A_i = A \otimes_F F_i$. Then L_i is linearly disjoint from F_n over F_i and*

$$\text{ind } A_i = p^{m(L_i/F_i)+1} = p^{n-i+1}$$

for $i = 1, 2, \dots, n$.

Proof. We proceed by induction on i . The base $i = 1$ is simply the case

$$K_1/F_1 = K/F,$$

which follows from the observation at the beginning of the section. Hence we assume that A is a division algebra and, for some $i \in \{1, 2, \dots, n-1\}$, we have $[L_i : F_i] = p^n$, $\text{ind } A_i = p^{n-i+1}$, and $m(L_i/F_i) = n-i$.

We claim that $\xi_{p^{i+1}} \notin L_i$. Otherwise, since $F_i(\xi_{p^{i+1}})/F_i$ is an extension of degree 1 or p , we deduce that $\xi_{p^{i+1}} \in T_i$, where T_i is the subfield of L_i/F_i with $[L_i : T_i] = p^i$. Without loss of generality, we may assume that $\xi_{p^{i+1}}^{p^i} = \xi_p$. Then $\xi_p = N_{L_i/T_i}(\xi_{p^{i+1}})$, and we obtain $m(L_i/F_i) \leq n-i-1$, a contradiction.

Hence L_i and F_{i+1} are linearly disjoint over F_i . Therefore L_{i+1}/F_{i+1} is a Galois extension of degree p^n and

$$G = \text{Gal}(L_i/F_i) \simeq \text{Gal}(L_{i+1}/F_{i+1}).$$

Now choose $\sigma_{i+1} \in \text{Gal}(L_{i+1}/F_{i+1})$ such that the restriction of σ_{i+1} to L_i is σ_i . (We assume that σ_i is already defined by induction, where $\sigma_1 = \sigma$.) Then we see that

$$A_{i+1} = A_i \otimes_{F_i} F_{i+1} \simeq (L_{i+1}/F_{i+1}, \sigma_{i+1}, \xi_p).$$

We therefore obtain from [P, Proposition 13.4(v)] that, on the one hand,

$$\text{ind } A_{i+1} \geq \frac{\text{ind } A_i}{p} = p^{n-i}.$$

On the other hand, we show that $p^{m(L_{i+1}/F_{i+1})+1} \leq p^{n-i}$, as follows. Since $\xi_{p^{i+1}} \in F_{i+1}^\times$, we have

$$\xi_p \in N_{L_{i+1}/T_{i+1}}(L_{i+1}^\times),$$

where $F_{i+1} \subseteq T_{i+1} \subseteq L_{i+1}$ and $[L_{i+1} : T_{i+1}] = p^i$. Hence $m(L_{i+1}/F_{i+1}) \leq n-i-1$.

Putting these last two inequalities together with the inequality $\text{ind } A \leq p^{m+1}$ observed at the beginning of Section 5, we reach the following chain:

$$\text{ind } A_{i+1} \leq p^{m(L_{i+1}/F_{i+1})+1} \leq p^{n-i} \leq \text{ind } A_{i+1}.$$

We obtain

$$m(L_{i+1}/F_{i+1}) = n - (i+1) \quad \text{and} \quad p^{m(L_{i+1}/F_{i+1})+1} = \text{ind } A_{i+1},$$

as desired. $\square$

To include $m(K/F) = -\infty$ in the proposition, it is sufficient to continue the induction one step further. Set $F_{n+1} = F(\xi_{p^{n+1}})$ and $L_{n+1} = K(\xi_{p^{n+1}})$. Then again L_{n+1}/F_{n+1} is a cyclic extension of degree p^n and $A_{n+1} = A \otimes_F F_{n+1}$ splits. We conclude that $m(L_{n+1}/F_{n+1}) = -\infty$.

The referee of this article pointed out an alternative proof of Proposition 6.1. Suppose $F_i \cap K = F$ is given (this is not difficult to see, especially when $p > 2$), and write

$$A = \bigoplus_{0 \leq j < p^n} \mu^j K,$$

where $\mu^{p^n} = \xi_p$ and $\mu^{-1}k\mu = \sigma(k)$ for each $k \in K$. Then we have

$$F_i := F(\xi_{p^i}) = F(\mu^{p^{n-i}}) \subset A.$$

The centralizer of F_i in A , written $C_A(F_i)$, is Brauer equivalent to A_i (see [P, Lemma 13.3]). Observe that $C_A(F_i)$ is a division algebra and hence

$$\text{ind } C_A(F_i) = \sqrt{\dim_{F_i} C_A(F_i)}.$$

From the double centralizer theorem ([P, Theorem 12.7(ii)]), we see that

$$\dim_F C_A(F_i) \cdot \dim_F F_i = \dim_F A.$$

We may write

$$\dim_F C_A(F_i) = \dim_{F_i} C_A(F_i) \cdot \dim_F F_i,$$

and by using $\dim_F A = p^{2n}$ and assuming $\dim_F F_i = p^{i-1}$, we obtain

$$\dim_{F_i} C_A(F_i) = p^{2(n-i+1)}.$$

Hence we have $\text{ind } A_i = p^{n-i+1}$, as required.

It remains to prove that $\dim_F F_i = p^{i-1}$. One can find that $x^{p^{i-1}} - \xi_p$ is irreducible for odd p in [La, Chapter 6, Theorem 9.1], hence giving the necessary equality. The case for $p = 2$ is resolved in [P, Lemma 15.4], where the polynomial $X^{2^n} + 1$ is shown to be irreducible, so that $[F(\xi_{2^{n+1}}) : F] = 2^n$. Since $[F(\xi_{2^{i+1}}) : F(\xi_{2^i})] \leq 2$ for each $1 \leq i \leq n$, it therefore follows that $[F_i : F] = 2^{i-1}$. This gives rise to the following interesting corollary.

Corollary 6.2. *Suppose that $n \geq 2$. Then $\sqrt{2} \notin F$.*

Proof. Suppose that $\sqrt{2} \in F$. Then

$$[F(\xi_8) : F] = [F(\sqrt{-1}) : F] = 2 < 2^{3-1},$$

a contradiction. □

Acknowledgements. We thank John Labute for his interest and for his valuable remarks related to this paper. We also thank the referee of this paper for providing us with elegant proofs in sections 3 and 6. We would also like to thank the referee of a previous version of this paper who suggested the approach considered in section 4. The research of the first author was supported in part by NSERC grant R0370A01. The research of the third author was supported in part by National Science Foundation grant DMS-0600122.

REFERENCES

- [A] A.A. Albert, *On cyclic fields*, Trans. Amer. Math. Soc. **37** (1935), no. 3, 454–462.
- [AF] F.W. Anderson and K.R. Fuller, *Rings and categories of modules*, Graduate Texts in Mathematics, Vol. 13, Springer-Verlag, New York-Heidelberg, 1974, viii+339 pp.
- [AT] E. Artin and J. Tate, *Class field theory*, Reprinted with corrections from the 1967 original, AMS Chelsea Publishing, Providence, RI, 2009, viii+194 pp.

- [B] Z.I. Borevič, *The multiplicative group of cyclic p -extensions of a local field* (Russian), Trudy Mat. Inst. Steklov **80** (1965), 16–29. English translation, in Proceedings of the Steklov Institute of Mathematics, no. 80 (1965): Algebraic number theory and representations, edited by D.K. Faddeev, 15–30, American Mathematical Society, Providence, RI, 1968.
- [Br] R. Brauer, *Über den Index und den Exponenten von Divisionalgebren*, Tôhoku Math. J. **37** (1933), 77–87.
- [D] P.K. Draxl, *Skew fields*, London Mathematical Society Lecture Notes Series, 81, Cambridge University Press, 1983, ix+182 pp.
- [HS] T. Hanke and J. Sonn, *Noncrossed products in Witt's theorem*, arXiv:0905.2668v2 [math.RA]. Available: <http://arxiv.org/abs/0905.2668>. To appear in Math. Ann.
- [Is] D.C. Isaksen, *A cohomological viewpoint on elementary school arithmetic*, Amer. Math. Monthly **109** (2002), no. 9, 796–805.
- [Iw] K. Iwasawa, *Local class field theory*, Oxford Science Publications, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1986, viii+155 pp.
- [JLY] C.U. Jensen, A. Ledet, and N. Yui, *Generic polynomials: Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, 45, Cambridge University Press, 2002, x+258 pp.
- [Ko] N. Koblitz, *p -adic numbers, p -adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics, 58, Springer-Verlag, New York, 1984, xii+150 pp.
- [La] S. Lang, *Algebra*, rev. 3rd ed., Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002, xvi+914 pp.
- [MS1] J. Mináč and J. Swallow, *Galois module structure of p th-power classes of extensions of degree p* , Israel J. Math. **138** (2003), 29–42.
- [MS2] J. Mináč and J. Swallow, *Galois embedding problems with cyclic quotient of order p* , Israel J. Math. **145** (2005), 93–112.
- [MS3] J. Mináč and J. Swallow, *Galois modules appearing as p th-power classes of units of extensions of degree p* , Math. Z. **250** (2005), no. 4, 907–914.
- [MSS1] J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of p th-power classes of cyclic extensions of degree p^n* , Proc. London Math. Soc. (3) **92** (2006), no. 2, 307–341.
- [MSS2] J. Mináč, A. Schultz, and J. Swallow, *Automatic realizations of Galois groups with cyclic quotient of order p^n* , J. Théor. Nombres Bordeaux **20** (2008), no. 2, 419–430.
- [NP] J. Neukirch and R. Perlis, *Fields with local class field theory*, J. Algebra **42** (1976), no. 2, 531–536.
- [P] R.S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, 88, Studies in the History of Modern Science, 9, Springer-Verlag, New York-Berlin, 1982, xii+436 pp.
- [R] L.H. Rowen, *Ring theory*, vol. II, Pure and Applied Mathematics, 128, Academic Press Inc., Boston, MA, 1988, xiv+462 pp.
- [RT] L.H. Rowen and J.-P. Tignol, *On the decomposition of cyclic algebras*, Israel J. Math. **96** (1996), part B, 553–578.

A. SCHULTZ, DEPT. OF MATH., WELLESLEY C., 106 CENTRAL STREET, WELLESLEY, MA 02481
USA

andrew.c.schultz@gmail.com

J. SWALLOW, DEPT. OF MATH., DAVIDSON C., BOX 7046, DAVIDSON, NORTH CAROLINA 28035-
7046 USA

joswallow@davidson.edu