CYCLIC ALGEBRAS AND CONSTRUCTION OF SOME GALOIS MODULES

JÁN MINÁČ*†, ANDREW SCHULTZ, AND JOHN SWALLOW

Abstract. Let p be a prime and suppose that K/F is a cyclic extension of degree p^n with group G. Let J be the $\mathbb{F}_pG$-module $K^\times/K^{\times p}$ of pth-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 $0 \le i < n$. We show that for all primes p and all $0 \le i < n$, there exists a field extension K/F with a summand of dimension p^i+1.

Let p be a prime and K/F a cyclic extension of fields of degree p^n with Galois group G. Let $K^\times$ be the multiplicative group of nonzero elements of K and $J = J(K/F) := K^\times/K^{\times p}$ be the group of pth-power classes of K. We see that J is naturally an $\mathbb{F}_pG$-module. In our previous paper [MSS] we established the decomposition of J into indecomposables, as follows.

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

Theorem. [MSS, Theorems 1, 2, and 3] *Suppose*

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

then

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

where each Y_i is a free $\mathbb{F}_pG_i$-module.

Date: October 30, 2004.

*Research supported in part by the Natural Sciences and Engineering Research Council of Canada, as well as by the special Dean of Science Fund and a Distinguished Research Professorship during 2004–2005 at the University of Western Ontario.

†Supported by the Mathematical Sciences Research Institute, Berkeley.

Otherwise, let

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

Then

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

where 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 that the decomposition is unique. (See the well-known result of Azumaya [AF, p. 144].)

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 $\xi_p \in N_{K/K_s}(K_s^\times)$ for all $s \in \{0, 1, \ldots, n\}$ if $m = -\infty$ and $\xi_p \in N_{K/K_s}(K^\times)$ for all $s \in \{m+1, \ldots, n\}$ if $m > -\infty$.

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

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

does there exist a cyclic extension K/F with $\xi_p \in F^\times$ such that the exceptional summand X has dimension d?

It turns out that we may answer this question in the affirmative using a construction of cyclic division algebras due to Brauer-Rowen. We remark that in [MS] the full realization problem, realizing all possible isomorphism classes for the $\mathbb{F}_p G$-module $J(K/F)$, has been solved in the case $n = 1$ and $\xi_p \in F^\times$.

1. Strategy and Main Theorem

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

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

In two later sections we will examine the relations between $m(K/F)$ and the index of a certain cyclotomic cyclic algebra A defined over F. In particular, we show by example that while these two invariants of K/F are closely related, they are not same.

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

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

is a central simple algebra such that

$$B = \bigoplus_{0\le j<r} u^j E,$$

where $u^{-1}du = d^\tau$ for all $d \in E$ and $u^r = b$. Thus B is an F-algebra of dimension r^2 over F. We say that $\deg B := r$. If $B \cong M_s(D)$, the matrix algebra containing matrices of size $s \times s$ over some division algebra D, then we set $\mathrm{ind}\, B = \sqrt{\dim_F D}$. We denote the order of $[B]$ in the Brauer group $\mathrm{Br}(F)$ by $\exp B$. Finally, we observe the following important connection:

$$[B] = 0 \text{ in } \mathrm{Br}(F) \quad \Leftrightarrow \quad b \in N_{E/F}(E^\times).$$

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

$$A := (K/F, \sigma, \xi_p), \quad \text{where } G = \langle\sigma\rangle.$$

(Recall that we assume $\xi_p \in F$ for our extensions K/F.)

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

First suppose $t \ge 0$. Set $q = p^{n-t}$ and let $K = \mathbb{Q}(\xi_q)(\mu_1, \dots, \mu_{p^n})$, where ξ_q is a primitive qth root of unity and the μ_i 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 $1 \le i \le n$, $K_i = K^{\langle\sigma^{p^i}\rangle}$. Then K/F is a cyclic extension of degree p^n satisfying $\mathbb{Q}(\xi_p) \subset F$, and $G = \langle\sigma\rangle = \mathrm{Gal}(K/F)$. Denote by $\bar\sigma$ the restriction of σ to the subfield K_{t+1}.

Let $A = (K/F, \sigma, \xi_p)$. Now A is Brauer-equivalent to the cyclic algebra $R = (K_{t+1}/F, \bar{\sigma}, \xi_q)$ by [P, Corollary 15.1b]. On the other hand, the construction of Brauer-Rowen provides that R is a division algebra of degree p^{t+1} and of 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

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

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

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

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

Suppose $m = m(K/F) < t$. Then $[A \otimes_F K_{m+1}] = 0 \in \mathrm{Br}(K_{m+1})$, whence K_{m+1}/F splits A. But then $p^{t+1} = \operatorname{ind} A \leq [K_{m+1} : F] < p^{t+1}$, a contradiction. Hence $m(K/F) = t$.

Now suppose that $t = -\infty$. Let F be a number field containing ξ_p. Then the extension F^c/F obtained by adjoining all pth-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 $G = \mathrm{Gal}(K/F)$ 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 $m = -\infty$. □

Remark 1. Observe that 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 $G = \mathrm{Gal}(K/F)$ as $\langle\sigma\rangle$ with $\sigma(\sqrt[p]{X}) = \xi_p\sqrt[p]{X}$. Then the cyclic algebra $A = (K/F, \sigma, \xi_p)$ is a symbol algebra $A = \left(\frac{X, \xi_p}{F, \xi_p}\right)$. (See, for instance, [P, p. 284].) Furthermore,

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

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]) that $[(E/F, \tau, X)] \neq 0$. Hence A is not split, and $m = 0$ as required.

The $m(K/F) = -\infty$ case follows as in the end of the proof of the theorem. Consider the tower

$$\mathbb{Q}(\xi_p) \subset \mathbb{Q}(\xi_{p^2}) \subset \mathbb{Q}(\xi_{p^3}).$$

By Albert's result, if $F = \mathbb{Q}(\xi_p)$ and $K = \mathbb{Q}(\xi_{p^2})$, we have $n = 1$ and $m(K/F) = -\infty$.

Remark 2. For extensions K/F of local fields one may then deduce that $m(K/F) \in \{-\infty, 0\}$, confirming [B], as follows. If $[A] = 0 \in \mathrm{Br}(F)$, then $m = -\infty$. Otherwise, since $\operatorname{ind} A = \exp A$ for local fields (see [P, Corollary 17.10b]), the local invariant $\operatorname{inv} A$ of A is s/p with $s \in \mathbb{N}, p \nmid s$. Because

$$\operatorname{inv} A \otimes_F E = [E : F] \operatorname{inv} A$$

(see [P, Proposition 17.10]), we obtain that $\operatorname{inv} A \otimes_F K_1 = 0$. Hence $[A \otimes_F K_1] = 0 \in \mathrm{Br}(K_1)$ and $m(K/F) = 0$, as desired.

2. The Invariants m and $\operatorname{ind} A$

The proof of the theorem turns on the fact that for the particular extension K/F we have $\operatorname{ind} A = p^{m+1}$. It is interesting to ask whether this equality holds generally.

We show in this section that the answer is negative. However, we have an inequality

$$\operatorname{ind} A \le p^{m+1},$$

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

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

for $m \neq -\infty$. Hence the inequality holds in the case $m \neq -\infty$. The statement also holds for $m = -\infty$, since A splits if and only if $m = -\infty$. 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 $\exp A = \operatorname{ind} A$. (See, for instance, [P, Theorem 18.6].) Therefore $\operatorname{ind} A$ is either 1 or p since the exponent of A divides p:

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

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 then

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

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

Let $\hat{K}_i$, $i = 1, 2$, 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 $\hat{K}_1 = \mathbb{Q}_2 \subset \hat{K}_2$.

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 obtain then that $m(K/F) = 1$.

3. When A is a Division Algebra

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

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

force the equality $\operatorname{ind} A = p^{m+1}$. In this section we show how a natural construction gives additional field extensions L_w/F_w with $\operatorname{ind} A = p^{m+1} = p^k$ for every $k < n$. More precisely:

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

Then

$$\operatorname{ind} A_i = p^{m(L_i/F_i)+1} = p^{n-i+1}, \quad i = 1, 2, \ldots, n.$$

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 $i \in \{1, 2, \ldots, n-1\}$, we have $[L_i : F_i] = p^n$, $\operatorname{ind} A_i = p^{n-i+1}$, 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 $\xi_{p^{i+1}} \in F_i'$, where F_i' is the subfield of L_i/F_i with $[L_i : F_i'] = p^i$. Without loss of generality we may assume that $\xi_{p^{i+1}}^{p^i} = \xi_p$. Then $\xi_p = N_{L_i/F_i'}(\xi_{p^{i+1}})$, and we obtain $m(L_i/F_i) \leq n - i - 1$, a contradiction.

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

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

Now let $\sigma_{i+1} \in \mathrm{Gal}(L_{i+1}/F_{i+1})$ 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 by [D, Lemma 7, p. 74] we see that

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

We therefore obtain from [P, Proposition 13.4v] that

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

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

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

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

Putting these last two equalities together with the equality of the second section, we reach the following chain:

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

We obtain $m(L_{i+1}/F_{i+1}) = n - (i+1)$ and $p^{m(L_{i+1}/F_{i+1})+1} = \operatorname{ind} A_{i+1}$, as desired. □

To include $m = -\infty$ 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 $m(L_{n+1}/F_{n+1}) = -\infty$.

4. Acknowledgement

We thank John Labute for his interest and for his valuable remarks related to this paper.

References

[A] A. Albert. On cyclic fields. *Trans. Amer. Math. Soc.* **37** (1935), no. 3, 454–462.

[AF] F. Anderson and K. Fuller. *Rings and categories of modules.* Graduate Texts in Mathematics 13. New York: Springer-Verlag, 1973.

[B] Z. Borevič. The multiplicative group of cyclic p-extensions of a local field. (Russian) *Trudy Mat. Inst. Steklov* **80** (1965), 16–29. English translation, *Proc. Steklov Inst. Math. No. 80 (1965): Algebraic number theory and representations*, edited by D. Faddeev, 15–30. Providence, RI: American Mathematical Society, 1968.

[Br] R. Brauer. Über den Index und Exponent von Divisionalgebren. *Tôhoku Math. Journal* **37** (1933), 77–87.

[D] P. Draxl. *Skew fields*. London Mathematical Society Lecture Notes Series 81. New York: Cambridge University Press, 1983.

[JLY] C. Jensen, A. Ledet, and N. Yui. *Generic polynomials: constructive aspects of the inverse Galois problem*. Mathematical Sciences Research Institute Publications 45. New York: Cambridge University Press, 2002.

[MS] J. Mináč and J. Swallow. Construction and classification of some Galois modules. Preprint arXiv:math.NT/0304203 (2003). http://arxiv.org/abs/math/0304203.

[MSS] J. Mináč, A. Schultz, and J. Swallow. Galois module structure of pth-power classes of cyclic extensions of degree p^n. Preprint arXiv:math.NT/0409532 (2004). http://arXiv.org/abs/math.NT/0409532.

[P] R. Pierce. *Associative algebras*. Graduate Texts in Mathematics 88. New York: Springer-Verlag, 1982.

[R] L. Rowen. *Ring theory*, vol. 2. Pure and Applied Mathematics 128. Boston: Academic Press, 1988.

[RT] L. Rowen and J.-P. Tignol. On the decomposition of cyclic algebras. *Israel J. Math.* **96** (1996), 553–578.

Department of Mathematics, Middlesex College, University of Western Ontario, London, Ontario N6A 5B7 CANADA

E-mail address: minac@uwo.ca

Department of Mathematics, Building 380, Stanford University, Stanford, California 94305-2125 USA

E-mail address: aschultz@stanford.edu

Department of Mathematics, Davidson College, Box 7046, Davidson, North Carolina 28035-7046 USA

E-mail address: joswallow@davidson.edu