New York Journal of Mathematics

New York J. Math. **14** (2008) 215–224.

Galois module structure of Milnor K-theory in characteristic p

Ganesh Bhandari, Nicole Lemire, Ján Mináč and John Swallow

Abstract. Let E be a cyclic extension of degree p^n of a field F of characteristic p. Using arithmetic invariants of E/F we determine k_mE, the Milnor K-groups K_mE modulo p, as $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-modules for all $m \in \mathbb{N}$. In particular, we show that each indecomposable summand of k_mE has $\mathbb{F}_p$-dimension a power of p. That all powers p^i, $i = 0, 1, \ldots, n$, occur for suitable examples is shown in a subsequent paper, Mináč, Schultz and Swallow, 2008, where additionally the main result of this paper becomes an essential induction step in the determination of K_mE/p^sK_mE as $(\mathbb{Z}/p^s\mathbb{Z})[\mathrm{Gal}(E/F)]$-modules for all $m, s \in \mathbb{N}$.

Contents

In the 1960s (see [Bo]) Z. I. Borevič and D. K. Faddeev classified possible $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-modules k_1E where E is a cyclic extension of degree p^n of a local field F. In [MS] it was shown that if $n = 1$, the local field F can be replaced by any field containing a primitive pth-root of unity. In [MSS1] this

Received March 9, 2008; revised June 6, 2008.

Mathematics Subject Classification. 19D45, 12F10.

Key words and phrases. Milnor K-groups modulo p, cyclic extensions, Galois modules.

The second author's research was supported in part by NSERC grant R3276A01.

The third author's research was supported in part by NSERC grant R0370A01, and by a Distinguished Research Professorship at the University of Western Ontario.

The fourth author's research was supported in part by NSA grant MDA904-02-1-0061 and by NSF grant DMS-0600122.

ISSN 1076-9803/08

classification was extended to all base fields F and all cyclic extensions E of degree p^n. In [LMS] the classification of all $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-modules k_mE, $m \in \mathbb{N}$ was obtained, provided E is a cyclic extension of degree p and F contains a primitive pth-root of unity. In [BLMS] results from [LMS] were used to obtain a restriction on possible absolute Galois pro-p groups. Thus, only when $m = 1$ has the case of characteristic p been considered ([MSS1]). However, the case of characteristic p is important not only for its intrinsic value, but also because this case arises naturally in considering the residue fields of valuations on fields of characteristic 0.

Bloch, Gabber, and Kato established an isomorphism between, on one hand, Milnor K-theory modulo p in characteristic p and, on the other, the kernel of the Artin–Schreier operator defined on the exterior algebra on Kähler differentials [BK].

Two significant papers by Izhboldin consider Milnor K-theory in characteristic p and, using the previous work of Bloch, Gabber, and Kato, ascertain its important Galois module properties [I1, I2].

In this paper we establish that two results of Izhboldin are enough to determine precisely the Galois module structure of the Milnor groups K_mE mod p when E is a cyclic extension of pth-power degree of a field F of characteristic p. The result is simple and useful: these modules are direct sums of trivial modules and modules free over some quotient of the Galois group. Equivalently, the dimensions over $\mathbb{F}_p$ of the indecomposable $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-modules occurring as direct summands of K_mE/pK_mE are all powers of p. In [MSS2] it is shown that in fact each indecomposable summand of dimension p^i, $i = 0, 1, \ldots, n$, occurs in suitable examples.

Our decomposition of the $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-module k_mE into indecomposables in Theorem 2 is not canonical, although the ranks of the summands which are free over the various quotients of $\mathrm{Gal}(E/F)$ are invariants of the $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-module k_mE. Still, our results do have a canonical formulation, stemming from Lemma 4, which is in fact equivalent to Theorem 2. In particular, the filtration of $(k_mE)^{\mathrm{Gal}(E/F)} \simeq k_mF$, induced by the images of successive powers of the maximal ideal of $\mathbb{F}_p[\mathrm{Gal}(E/F)]$, is determined by the images of the norm maps $k_mE_i \to k_mF$, where E_i runs through the intermediate fields between E and F. It is possible that one could use the results in [J] to obtain alternative proofs, but we preferred instead a more self-contained short derivation.

In [MSS2] our main result is used as a critical first induction step to determine K_mE/p^sK_mE as a $(\mathbb{Z}/p^s\mathbb{Z})[\mathrm{Gal}(E/F)]$-module for all $m, s \in \mathbb{N}$. The classification problem of $\mathbb{Z}/p^s\mathbb{Z}[G]$-modules for cyclic G is nontrivial and in fact still not complete, despite some important results when, for instance, the module is free over $\mathbb{Z}/p^s\mathbb{Z}$ (see [T] and the references contained therein). However one can describe the $(\mathbb{Z}/p^s\mathbb{Z})[\mathrm{Gal}(E/F)]$-module K_mE/p^sK_mE completely and simply.

We assume in what follows that all fields have characteristic p and that m is a fixed natural number. For a field F, let K_mF denote the mth Milnor K-group of F and $k_mF = K_mF/pK_mF$ (see, for instance, [Ma] and [Mi, IX.1]). If E/F is a Galois extension of fields, let $G = \mathrm{Gal}(E/F)$ denote the associated Galois group. When G is a cyclic group we write $G = \langle\sigma\rangle$, with a suitable fixed generator σ. For the sake of simplicity we write ρ instead of $\sigma - 1$. We write $i_E\colon K_mF \to K_mE$ and $N_{E/F}\colon K_mE \to K_mF$ for the natural map induced by the inclusion and the norm maps, and we use the same notation for the induced maps modulo p between k_mF and k_mE. In order to avoid possible confusion, in a few instances we write $i_{F,E}$ instead of i_E.

Izhboldin's results are as follows.

Lemma 1 ([I2, Lemma 2.3])**.** *Suppose E/F is cyclic of degree p. Then $i_E\colon k_mF \to (k_mE)^G$ is an isomorphism.*

Theorem 1 (Hilbert 90 for Milnor K-theory: [I1, Corollary of Proposition 5], [I2, Theorem D])**.** *Suppose E/F is cyclic of pth-power degree. Then the following sequence is exact:*

$$K_mE \xrightarrow{1-\sigma} K_mE \xrightarrow{N_{E/F}} K_mF.$$

Observe that Lemma 1 can be used to prove the following stronger variant:

Lemma 1′. *Suppose E/F is a Galois extension such that G has order p^n, $n \in \mathbb{N}$. Then $i_E\colon k_mF \to (k_mE)^G$ is an isomorphism.*

Proof. We use induction on n. By Lemma 1 our statement is true for $n = 1$. Assume therefore that $n > 1$. Let H be a central subgroup of G of order p and D be its fixed field. Then D/F is a Galois extension of degree p^{n-1}. Let $L = \mathrm{Gal}(D/F)$. By induction $i_D : k_mF \to (k_mD)^L$ is an isomorphism. By Lemma 1 we see that $i_{D,E} : k_mD \to (k_mE)^G$ is an isomorphism. Hence $i_E : k_mF \to (k_mE)^G$ is injective.

Let $\alpha \in (k_mE)^G$. Since $(k_mE)^G \subseteq (k_mE)^H$, by Lemma 1 there exists $\gamma \in k_mD$ such that $i_{D,E}\gamma = \alpha$. Because $\alpha \in (k_mE)^G$ and $i_{D,E}$ is injective we see that $\gamma \in (k_mD)^L$. Hence by our induction hypothesis there exists $\delta \in k_mF$ such that $i_{F,D}\delta = \gamma$. Thus $i_E\delta = \alpha$ and we see that $i_E : k_mF \to (k_mE)^G$ is an isomorphism, as required. □

Now suppose E/F is cyclic of degree p^n. For $i = 0, 1, \ldots, n$, let E_i/F be the subextension of degree p^i of E/F, $H_i = \mathrm{Gal}(E/E_i)$, and $G_i = \mathrm{Gal}(E_i/F)$. Our main result is the following

Theorem 2. *There exists an isomorphism of $\mathbb{F}_pG$-modules $k_mE \simeq \oplus_{i=0}^n Y_i$, where*

- *Y_n is a free $\mathbb{F}_pG$-module of rank $\dim_{\mathbb{F}_p} N_{E/F}k_mE$, and*
- *Y_i, $0 \le i < n$, is a free $\mathbb{F}_pG_i$-module of rank*

$$\dim_{\mathbb{F}_p} N_{E_i/F}k_mE_i/N_{E_{i+1}/F}k_mE_{i+1}.$$

Remark 1. Observe that Y_0 is a trivial $\mathbb{F}_pG$-module of dimension over $\mathbb{F}_p$ equal to $\dim_{\mathbb{F}_p} k_mF/N_{E_1/F}k_mE_1$. Moreover, the statements about the ranks of the Y_i are immediate consequences of the fact that k_mE is a direct sum of indecomposable $\mathbb{F}_pG$-modules whose dimensions over $\mathbb{F}_p$ are all powers of p — which is the main point of the theorem (see Section 2, proof of the Reduction to Lemma 4).

Our proof of Theorem 2 relies on a filtration lemma, Lemma 4, which shows that certain elements in k_mE are expressible as norms. That the various norm groups $N_{E_i/F}k_mE_i$ contain enough elements is, in fact, the key to this lemma. In Section 1 we present technical results on $\mathbb{F}_pG$-modules. In Section 2 we state Lemma 4, prove that Theorem 2 is a corollary to Lemma 4, and prove basic lemmas in preparation for its proof. This proof is finally presented in Section 3, and in Section 4 we present an alternative proof for some cases of Theorem 2.

1. $\mathbb{F}_pG$-modules

For the reader's convenience, after introducing some notation, we recall in this section some basic elementary facts about $\mathbb{F}_pG$-modules (see [C] and [L]).

Let G be a cyclic group of order p^n with generator σ. We denote $\sigma - 1$ as ρ. For an $\mathbb{F}_pG$-module U, let U^G denote the submodule of U fixed by G. For an arbitrary element $u \in U$, we say that the length $l(u)$ is the dimension over $\mathbb{F}_p$ of the $\mathbb{F}_pG$-submodule $\langle u \rangle$ of U generated by u. Then we have

$$\rho^{l(u)-1}\langle u \rangle = \langle u \rangle^G \neq \{0\} \quad \text{and} \quad \rho^{l(u)}\langle u \rangle = \{0\}.$$

If we want to stress the dependence of length $l(u)$ on G, we write $l_G(u)$. As usual, if U is a free $\mathbb{F}_pG$-module with $U = \oplus_{i\in\mathcal{I}}\mathbb{F}_pG$, we say that U is a module of rank $|\mathcal{I}|$. Denote by N the operator ρ^{p^n-1} acting on module U. For each $k = 0, 1, \ldots, n$, let H_k be the subgroup of G of order p^{n-k}. Observe that if $G = \mathrm{Gal}(E/F)$ then this definition coincides with the previous definition $H_k = \mathrm{Gal}(E/E_k)$.

We use the following general lemma about $\mathbb{F}_pG$-modules. The simple proof of this lemma is omitted.

Lemma 2 (Exclusion Lemma)**.** *Let M_i, $i \in \mathcal{I}$, be a family of $\mathbb{F}_pG$-modules contained in a common $\mathbb{F}_pG$-module N. Suppose that the $\mathbb{F}_p$-vector subspace R of N generated by all M_i^G has the form $R = \oplus_{i\in\mathcal{I}}M_i^G$. Then the $\mathbb{F}_pG$-module M generated by M_i, $i \in \mathcal{I}$, has the form $M = \oplus_{i\in\mathcal{I}}M_i$.*

We also use the following result about the restriction of a cyclic $\mathbb{F}_pG$-module to a subgroup.

Lemma 3 (Restriction Lemma)**.** *Let Y be a cyclic $\mathbb{F}_pG$-module of length l generated by γ. Then $l_{H_k}(\gamma)$ is the unique integer such that*

$$l = (l_{H_k}(\gamma) - 1)p^k + r$$

for some unique integer $1 \leq r \leq p^k$. *Moreover,*

$$Y \simeq V^r_{l_{H_k}(\gamma)} \oplus V^{p^k-r}_{l_{H_k}(\gamma)-1}$$

where V_i *is a cyclic* $\mathbb{F}_pH_k$*-module of length* i.

Proof. The formula for l_{H_k} follows immediately from the definition of length. Since $\{\rho^i\gamma \mid 0 \leq i \leq l-1\}$ is an $\mathbb{F}_p$-basis for $Y = \mathbb{F}_pG\gamma$, then

$$\mathbb{F}_pG\gamma\big|_{H_k} \;=\; \oplus_{i=0}^{p^k-1}\mathbb{F}_pH_k\rho^i\gamma \;\simeq\; V^r_{l_{H_k}(\gamma)} \oplus V^{p^k-r}_{l_{H_k}(\gamma)-1}$$

since $l_{H_k}(\rho^j\gamma) = l_{H_k}(\gamma)$ if $0 \leq j < r$ and $l_{H_k}(\rho^j\gamma) = l_{H_k}(\gamma) - 1$ if $r \leq j \leq p^k - 1$. □

Finally, we need a general structure proposition about $\mathbb{F}_pG$-modules that shows that the structure of an $\mathbb{F}_pG$-module X can be determined from the natural filtration on X^G obtained by taking the intersection of X^G with the images of X under the successive powers of the augmentation ideal of $\mathbb{F}_pG$. The proposition below is proved for cyclic p-groups as [LMS, Proposition 2]. The generalization to cyclic groups of order p^n is automatic.

Proposition 1. *Let* X *be an* $\mathbb{F}_pG$*-module. Set* $L_{p^n} = \rho^{p^n-1}X$ *and for* $1 \leq i < p^n$, *suppose that* L_i *is an* $\mathbb{F}_p$*-complement of* $\rho^iX \cap X^G$ *in* $\rho^{i-1}X \cap X^G$.

Then there exist $\mathbb{F}_pG$*-modules* X_i, $i = 1, 2, \ldots, p^n$, *such that:*

1. $X = \bigoplus_{i=1}^{p^n} X_i$.
2. $X_i^G = L_i$ *for* $i = 1, 2, \ldots, p^n$.
3. *Each* X_i *is a direct sum of* $\dim_{\mathbb{F}_p}(L_i)$ *cyclic* $\mathbb{F}_pG$*-modules of length* i.
4. *For each* $i = 1, 2, \ldots, p^n$, *there exists an* $\mathbb{F}_p$*-submodule* Y_i *of* X_i *with* $\dim_{\mathbb{F}_p}(Y_i) = \dim_{\mathbb{F}_p}(L_i)$ *such that* $(\mathbb{F}_pG)Y_i = X_i$.

Remark 2. The uniqueness of the form of the decomposition of X into a direct sum of cyclic summands is quite easy to see. Indeed, if $X = \oplus_{i=1}^{p^n} X_i$, where X_i is a direct sum of cyclic modules of length i, indexed by a set $\mathcal{N}_i$, then we have

$$\operatorname{card}\mathcal{N}_i = \dim_{\mathbb{F}_p}(\rho^{i-1}X \cap X^G)/(\rho^iX \cap X^G).$$

The uniqueness of the decomposition of X into a direct sum is also a special case of the Krull–Schmidt–Azumaya Theorem (see [AF, Theorem 12.6]).

2. Milnor k-groups

If $\alpha \in K_mE$ we write $\overline{\alpha}$ for the class of α in k_mE. For $\gamma \in K_mE$, let $l(\gamma)$ denote the dimension over $\mathbb{F}_p$ of the $\mathbb{F}_pG$-submodule $\langle\overline{\gamma}\rangle$ of k_mE generated by $\overline{\gamma}$. Recall that $i_EN_{E/F}$ acts on k_mE as $1 + \sigma + \cdots + \sigma^{p^n-1}$ (see [FV, Chapter 1, (3.8) Theorem 1]). Because $\rho^{p^n-1} = 1 + \sigma + \cdots + \sigma^{p^n-1}$ in $\mathbb{F}_pG$, we may use $i_EN_{E/F}$ and N interchangeably on k_mE.

We will prove the following key lemma by induction on n.

Lemma 4. *Let $1 \le j \le p^n$ and let $0 \le i \le n$ be minimal such that $j \le p^i$. Then*

$$\rho^{j-1} k_m E \cap (k_m E)^G = i_E N_{E_i/F} k_m E_i.$$

Remark 3. (1) First note that Lemma 1′ proves this result for $j = 1$, and note also that for $j = p^n$, the result holds by definition.

(2) That the right-hand side of the equality is contained in the left-hand side follows from the fact that $i_{E_i} N_{E_i/F}$ is identical to ρ^{p^i-1} on $k_m E_i$ and also on the image under the injection $i_{E_i,E}$ into $k_m E$. To show inclusion in the opposite direction, it is enough to show that for each cyclic extension E/F of pth-power degree p^n, $\rho^{j-1} k_m E \cap (k_m E)^G \subseteq i_E N_{E/F} k_m E$ for all j with $p^{n-1} < j < p^n$, as follows.

Assume that the statement is true. Let j satisfy $1 \le j \le p^n$ and suppose that i is the smallest nonnegative integer such that $j \le p^i$. Applying the statement for E_i/F case, together with the observation above that the $j = p^i$ case for E_i/F holds by definition, and using the injectivity of Lemma 1′, we conclude that

$$\begin{aligned}\rho^{j-1}(i_{E_i,E}(k_m E_i)) \cap i_{E_i,E}(k_m E_i)^G &\subseteq i_{E_i,E}(i_{E_i}(N_{E_i/F} k_m E_i)) \\ &= i_E(N_{E_i/F}(k_m E_i)).\end{aligned}$$

Therefore it is enough to observe that

$$\rho^{j-1} k_m E \cap (k_m E)^G = \rho^{j-1}(i_{E_i,E}(k_m E_i)) \cap i_{E_i,E}(k_m E_i)^G,$$

and to do this it is enough to prove that

$$\rho^{j-1} k_m E \cap (k_m E)^G \subseteq \rho^{j-1}(i_{E_i,E}(k_m E_i)) \cap i_{E_i,E}(k_m E_i)^G,$$

as the inclusion in the opposite direction is obvious. Let $\alpha = \rho^{j-1}\gamma \in (k_m E)^G$ where $\gamma \in k_m E$. Then $\rho^{p^i}\gamma = 0$ and so $\sigma^{p^i}\gamma = \gamma$. Therefore by Lemma 1′ we see that $\gamma \in i_{E_i,E} k_m E_i$, as was required.

The foregoing thus establishes a reduction step for use in the proof of Lemma 4.

Before proving this lemma, we show:

Reduction to Lemma 4. *Theorem 2 holds for cyclic extensions of degree p^n for which Lemma 4 holds.*

Proof. We apply Proposition 1 to $k_m E$. Set $L_{p^n} = i_E N_{E/F} k_m E$, and for $0 \le i < n$, define L_{p^i} as an $\mathbb{F}_p$-complement of $i_E N_{E_{i+1}/F} k_m E_{i+1}$ in $i_E N_{E_i/F} k_m E_i$. We also set $L_k = \{0\}$ for each $k \in \{1, \dots, p^n\}$ which is not a power of p. Note that $(k_m E)^G = i_E k_m F$ by Lemma 1′. Then, Lemma 4 shows that the $\mathbb{F}_p$-modules L_j, $j = 1, \dots, p^n$, satisfy the conditions of the proposition. By the proposition, we have a decomposition of $k_m E$ into a direct sum of $\mathbb{F}_p G$-modules

$$k_m E = \oplus_{i=0}^n Y_i,$$

where $Y_i^G = L_{p^i}$ and Y_i is a direct sum of

$$\begin{aligned}\dim_{\mathbb{F}_p} L_{p^i} &= \dim_{\mathbb{F}_p} i_E N_{E_i/F} k_m E_i / i_E N_{E_{i+1}/F} k_m E_{i+1} \\ &= \dim_{\mathbb{F}_p} N_{E_i/F} k_m E_i / N_{E_{i+1}/F} k_m E_{i+1}\end{aligned}$$

cyclic $\mathbb{F}_p G$-modules of length p^i, using Lemma 1 for the last equality. Equivalently, $Y_i \simeq \oplus_{T_i} \mathbb{F}_p(G/H_i)$, where the cardinal number of T_i is $\dim_{\mathbb{F}_p} L_{p^i}$, and therefore Y_i is a free $\mathbb{F}_p G_i$-module of the same rank. $\square$

We now prove several lemmas as partial results toward the proof of Lemma 4. Note it is only in these lemmas, and in the alternative proof in Section 4, that Theorem 1 is used in this paper.

Lemma 5. *Lemma* 4 *holds for all cyclic extensions E/F of degree p.*

Proof. Let $G = \mathrm{Gal}(E/F)$. By Remark 3, it suffices to show the left-to-right inclusion. Let $\gamma \in K_m E$ such that $0 \neq \rho^{l-1}\overline{\gamma} \in \rho^{l-1} k_m E \cap (k_m E)^G$ where $1 < l \leq p$. Then $l(\gamma) = l$. We show by induction on i, $l \leq i \leq p$, that there exists $\alpha_i \in K_m E$ such that

$$\langle \rho^{i-1} \overline{\alpha}_i \rangle = \langle \overline{\gamma} \rangle^G.$$

Then setting $\alpha := \alpha_p$, the proof will be complete. If $i = l$ then $\alpha_i = \gamma$ suffices. Assume now that $l \leq i < p$ and our statement is true for i.

Set $c := N_{E/F}\alpha_i$. Since $i_E \bar{c} = N\overline{\alpha}_i = \rho^{p-1}\overline{\alpha}_i$ and $i < p$, we conclude that $i_E \bar{c} = 0$. By the injectivity of i_E from Lemma 1, $\bar{c} = 0$. Therefore there exists $f \in K_m F$ such that $c = pf$ in $K_m F$.

We calculate

$$N_{E/F}(\alpha_i - i_E(f)) = c - pf = 0.$$

By Theorem 1, there exists $\omega \in K_m E$ such that $\rho\omega = \alpha_i - i_E(f)$. Hence $\rho^2\omega = \rho\alpha_i$. Since $i \geq 2$,

$$\langle \rho^i \overline{\omega} \rangle = \langle \rho^{i-1} \overline{\alpha}_i \rangle = \langle \overline{\gamma} \rangle^G$$

and we can set $\alpha_{i+1} = \omega$. $\square$

Lemma 6. *Lemma* 4 *holds for all cyclic extensions E/F of degree* 4.

Proof. If $j = 1$ then our statement is a special case of Lemma $1'$.

Assume now that $j = 2$. As we observed in Remark 3, $i_E N_{E_1/F} k_m E_1 \subseteq \rho k_m E \cap (k_m E)^G$. In order to show the inclusion in the opposite direction, let $\gamma \in k_m E$ such that $\rho\gamma \in (k_m E)^G$. Then $\rho^2\gamma = 0$ and $\sigma^2\gamma = \gamma$. Thus Lemma 1 implies $\gamma = i_{E_1,E}\delta$, where $\delta \in k_m E_1$. Hence

$$\begin{aligned}\rho\gamma &= i_{E_1,E}\rho\delta \\ &= i_{E_1,E}\, i_{F,E_1} N_{E_1/F}\delta \\ &= i_E N_{E_1/F}\delta.\end{aligned}$$

Hence we have the desired inclusion $\rho k_m E \cap (k_m E)^G \subseteq i_E N_{E_1/F} k_m E_1$.

Now suppose that $j = 3$, and let $\gamma \in K_mE$ such that $0 \neq \rho^2\overline{\gamma} \in \rho^2 k_mE \cap (k_mE)^G$. Recall that for $\gamma \in K_mE$, we let $l(\gamma)$ denote the $\mathbb{F}_p$-dimension of the $\mathbb{F}_pG$-submodule $\langle\overline{\gamma}\rangle$ of k_mE generated by $\overline{\gamma}$. Then $l(\gamma) = 3$, and set $\beta := \rho\gamma$. We have

$$(\sigma^2 - 1)\overline{\beta} = \rho^3\overline{\gamma} = 0.$$

By Lemma 1 applied to E/E_1, $\overline{\beta} \in i_{E_1,E}(k_mE_1)$. Let $b \in K_mE_1$ such that $i_{E_1,E}\bar{b} = \overline{\beta}$.

Set $c := N_{E_1/F}b$. Then

$$i_{F,E}\bar{c} = i_{E_1,E}(\sigma + 1)\bar{b} = (\sigma^2 - 1)\overline{\gamma} = i_{E_1,E}N_{E/E_1}\overline{\gamma},$$

and since $l(\gamma) = 3$, $\langle\overline{\gamma}\rangle^G = \langle i_{F,E}\bar{c}\rangle$. By Lemma 1 we see that $i_{F,E_1}\bar{c} = N_{E/E_1}\overline{\gamma}$ and therefore $N_{E/E_1}\gamma = i_{F,E_1}c + 2g$ for some $g \in K_mE_1$.

Now $N_{E/F}\gamma = N_{E_1/F}(i_{F,E_1}c + 2g) = 2c + 2N_{E_1/F}g$. Set $\delta := b + g$. We calculate

$$N_{E/F}i_{E_1,E}\delta = 2c + 2N_{E_1/F}g,$$

so that $N_{E/F}(\gamma - i_{E_1,E}\delta) = 0$. By Theorem 1 there exists an $\alpha \in K_mE$ with $\rho\alpha = \gamma - i_{E_1,E}\delta$. Then observing that $\rho^2(\overline{i_{E_1,E}\delta}) = 0$ as $\delta \in K_mE_1$ we see that

$$i_{F,E}N_{E/F}\overline{\alpha} = \rho^3\overline{\alpha} = \rho^2\overline{(\gamma - i_{E_1,E}\delta)} = \rho^2\overline{\gamma},$$

as required. □

3. Proof of Lemma 4

We prove Lemma 4 and hence, using the Reduction to Lemma 4, Theorem 2. We do so by induction on n, using Lemmas 5 and 6 as base cases and assuming the result for cyclic extensions of degree p^{n-1}. Observe that Lemmas 5 and 6 and the Reduction to Lemma 4 give us that Theorem 2 holds for degree p and, if $p = 2$, then for degree 4 as well. By Remark 3, it suffices to prove that

$$\rho^{j-1}k_mE \cap (k_mE)^G \subseteq i_E N_{E/F} k_mE$$

for all $p^{n-1} < j < p^n$.

Assume that $k_mE = \oplus_{\gamma\in\Gamma}\mathbb{F}_pG\gamma$ is a decomposition of k_mE into cyclic $\mathbb{F}_pG$-modules given by Proposition 1. As we observed in Remark 2, this decomposition is unique in the sense that the multiplicity of the cyclic summands of given dimension of k_mE are determined by k_mE.

First assume that $p > 2$. We know by Lemma 5 and by Reduction to Lemma 4 that $k_mE|_{H_{n-1}}$ is a direct sum of trivial and free $\mathbb{F}_pH_{n-1}$-modules. Let $\gamma \in k_mE$ satisfy $p^{n-1} < l(\gamma) < p^n$. We want to show that $\rho^{l(\gamma)-1}\gamma \in \rho^{p^{n-1}}k_mE = i_Ek_mE$. Without loss of generality we may assume that γ generates a cyclic $\mathbb{F}_pG$-summand of k_mE. If $l(\gamma) < p^n$, then by Lemma 3, $\mathbb{F}_pG\gamma|_{H_{n-1}}$ contributes direct summands which are not free or trivial, a contradiction. Hence a cyclic generator γ with length greater than p^{n-1} must have length p^n.

Now assume $p = 2$. Suppose that $\gamma \in \Gamma$ satisfies $2^{n-1} < l(\gamma) < 2^n$. By Lemma 6 and the Reduction to Lemma 4, $k_m E|_{H_{n-2}}$ is a direct sum of cyclic $\mathbb{F}_2 H_{n-2}$-modules of lengths 1, 2, and 4, and $\mathbb{F}_2 G\gamma$ is a cyclic summand of $k_m E$. By Lemma 3, we know that $\mathbb{F}_2 G\gamma|_{H_{n-2}}$ contributes cyclic $\mathbb{F}_2 H_{n-2}$-summands of length 3, a contradiction. Hence a cyclic generator $\gamma \in \Gamma$ of length greater than 2^{n-1} must have length 2^n.

In both cases, we have shown for $p^{n-1} < j < p^n$ that

$$\rho^{j-1} k_m E \cap (k_m E)^G = i_E N_{E/F} k_m E,$$

as desired. $\square$

4. Alternative proof

The following simple alternate proof of Theorem 2 for cyclic extensions of prime degree was found by the referee, whom we thank for allowing us to reproduce it here. Observe that using this argument we obtain a simpler proof of Theorem 2 for cyclic extensions of degree p^n for $p > 2$. The case $p = 2$ remains the hardest, as one sees by examining the proof of Lemma 6.

Let E/F be a cyclic extension of degree $p > 2$, and write $k_m E = \oplus_{i=1}^{p} X_i$, where each X_i is a direct sum of cyclic $\mathbb{F}_p G$-modules of length i. We show that $X_i = \{0\}$ for all $i \in \{2, \ldots, p-1\}$. Suppose that it is not true: there exists a cyclic summand $\langle \overline{\gamma} \rangle$, $\gamma \in K_m E$, of length i, $2 \le i \le p-1$. Then $N(\overline{\gamma}) = 0$ and there exists $f \in K_m F$ such that $N_{E/F}\gamma = pf$. From Theorem 1 it follows that $\gamma = \rho w + f$ for some $w \in K_m E$. Hence $\overline{\gamma} = \rho \overline{w} + \overline{f}$. Passing to the projection of $k_m E$ onto $\langle \overline{\gamma} \rangle$ we see that $\langle \overline{\gamma} \rangle$ embeds into a cyclic module of length $i + 1$ — a contradiction.

Acknowledgments. We are very grateful to A. Schultz as some of his ideas, developed in [MSS1], proved quite useful to us during the investigations leading to this paper. We also wish to thank M. Rost and J.-P. Serre for their comments after a lecture delivered in Nottingham by the third author in September 2005. These comments led to the improvement of our exposition. Finally, we would like to thank the referee for such a careful reading of our article, resulting in valuable suggestions for improving our text and simplifications of some proofs.

References

[AF] Anderson, Frank W.; Fuller, Kent R. Rings and categories of modules. Graduate Texts in Mathematics, 13. *Springer-Verlag, New York*, 1974. MR0417223 (54 #5281), Zbl 0301.16001.

[BLMS] Benson, Dave; Lemire, Nicole; Mináč, Ján; Swallow, John. Detecting pro-p groups that are not absolute Galois groups. *J. Reine Angew. Math.* **613** (2007) 175–191. MR2377134.

[BK] Bloch, Spencer; Kato, Kazuya. p-adic étale cohomology. *Inst. Hautes Études Sci. Publ. Math.* **63** (1986) 107–152. MR0849653 (87k:14018), Zbl 0613.14017.

[Bo] Borevič, Z. I. The multiplicative group of cyclic p-extensions of a local field. *Trudy Mat. Inst. Steklov* **80** (1965), 16–29. Translated as *Proc. Steklov Inst. Math.* No. 80 (1965): Algebraic number theory and representations, D. K. Faddeev, ed., Providence, RI: American Mathematical Society (1968), 15–30. MR0205976 (34 #5801), Zbl 0174.08801.

[C] CARLSON, JON F. Modules and group algebras. Notes by Ruedi Suter. Lectures in Mathematics ETH Zürich. *Birkhäuser Verlag, Basel*, 1996. MR1393196 (97c:20013), Zbl 0883.20006.

[FV] *Fesenko, I. B.; Vostokov, S. V.* Local fields and their extensions. With a foreword by I. R. Shafarevich. Second edition. Translations of Mathematical Monographs 121. Providence, RI: American Mathematical Society, 2002. MR1915966 (2003c:11150), Zbl 0781.11042.

[I1] IZHBOLDIN, O. T. On the torsion subgroup of Milnor K-groups. *Dokl. Akad. Nauk SSSR* **294** (1987), no. 1, 30–33. Translated as *Soviet Math. Dokl.* **35**, no. 3, 493–495. MR0895480 (88m:11048), Zbl 0655.18009.

[I2] IZHBOLDIN, O. T. On p-torsion in K_*^M for fields of characteristic p. *Algebraic K-theory.* Advances in Soviet Mathematics, 4. *American Mathematical Society, Providence, RI*, 1991, 129–144. MR1124629 (92f:11165), Zbl 0746.19002.

[J] JAKOVLEV, A. V. Homological determination of p-adic representations of rings with basis of powers. *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970) 1000–1014. Translated as *Math. USSR–Izvestiya* **4** (1970), no. 5, 1001–1016. MR0282945 (44 #179).

[L] LAM, T. Y. Lectures on modules and rings. Graduate Texts in Mathematics, 189. *Springer-Verlag, New York*, 1999. MR1653294 (99i:16001), Zbl 0911.16001.

[LMS] LEMIRE, NICOLE; MINÁČ, JÁN; SWALLOW, JOHN. Galois module structure of Galois cohomology and partial Euler-Poincaré characteristics. *J. Reine Angew. Math.* **613** (2007) 147–163. MR2377133.

[Ma] MAGURN, BRUCE A. An algebraic introduction to K-theory. Encyclopedia of Mathematics and its Applications, 87. *Cambridge University Press, Cambridge*, 2002. MR1906572 (2003g:19001), Zbl 1002.19001.

[Mi] MILNOR, JOHN. Algebraic K-theory and quadratic forms. *Invent. Math.* **9** (1970) 318–344. MR0260844 (41 #5465), Zbl 0199.55501.

[MS] MINÁČ, JÁN; SWALLOW, JOHN. Galois module structure of pth-power classes of extensions of degree p. *Israel J. Math.* **138** (2003), 29–42. MR2031948 (2004m:12008), Zbl 1040.12006.

[MSS1] MINÁČ, JÁN; SCHULTZ, ANDREW; SWALLOW, JOHN. Galois module structure of pth-power classes of cyclic extensions of degree p^n. *Proc. London Math. Soc.* **92** (2006), no. 2, 307–341. MR2205719 (2006j:12006).

[MSS2] MINÁČ, JÁN; SCHULTZ, ANDREW; SWALLOW, JOHN. Galois module structure of Milnor K-theory mod p^s in characteristic p. *New York J. Math.* **14** (2008) 225–233.

[T] THÉVENAZ, JACQUES. Representations of finite groups in characteristic p^r. *J. Algebra* **72** (1981) 478–500. MR0641337 (83m:20019), Zbl 0482.20005.

DEPARTMENT OF MATHEMATICS, PHYSICS AND ENGINEERING, MOUNT ROYAL COLLEGE, 4825 MOUNT ROYAL GATE SW, CALGARY, ALBERTA T3E 6K6, CANADA
gbhandari@mtroyal.ca

DEPARTMENT OF MATHEMATICS, MIDDLESEX COLLEGE, UNIVERSITY OF WESTERN ONTARIO, LONDON, ONTARIO N6A 5B7, CANADA
nlemire@uwo.ca minac@uwo.ca

DEPARTMENT OF MATHEMATICS, DAVIDSON COLLEGE, BOX 7046, DAVIDSON, NORTH CAROLINA 28035-7046, USA
joswallow@davidson.edu

This paper is available via http://nyjm.albany.edu/j/2008/14-9.html.