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. We determine $k_m E$, the Milnor K-groups modulo p, as $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-modules for all $m \in \mathbb{N}$.

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, K]. In order to better understand Milnor K-theory, it is a natural problem to determine the Galois module structure of Milnor K-theory when the field is a Galois extension. 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 the remarkable fact that two results of Izhboldin are enough to determine precisely the Galois module structure of the Milnor groups $K_m E$ mod p when E is 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 $K_m E/pK_m E$ are all powers of p. Such a description represents a culmination of results of Bloch-Kato, Gabber, and Izhboldin, available since 1987, concerning the Galois module structure of Milnor K-groups mod p.

Date: October 29, 2004.

2000 *Mathematics Subject Classification.* 19D45, 12F10.

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

[⋆]Research supported in part by NSERC grant R3276A01.

[*]Research supported in part by NSERC grant R0370A01.

[†]Supported by the Mathematical Sciences Research Institute, Berkeley.

[‡]Research supported in part by NSA grant MDA904-02-1-0061.

The precise description of the $\mathbb{F}_p[\mathrm{Gal}(E/F)]$-module K_mE/pK_mE depends on a natural filtration of K_mF/pK_mF obtained from images of norm maps defined on Milnor K-groups mod p of intermediate fields of E/F. This description, together with the arguments in the proofs, reveals a flavor of abstract class field theory. In place of the axioms of class formations, we use Izhboldin's theorems below, together with some technical but relatively short consequences of Hilbert 90, which one might call "Hilbert 90 algebra."

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, [M] and [FV, IX.1].) If E/F is a Galois extension of fields, let $G = \mathrm{Gal}(E/F)$ denote the associated Galois group. We write $i_E\colon K_mF \to K_mE$ and $N_{E/F}\colon K_mE \to K_mF$ for the natural inclusion and 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.

Theorem 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.*

It is useful to observe that Theorem 1 generalizes to cyclic extensions of degree p^n. For $\alpha \in K_mE$ we write $\bar{\alpha}$ for the class of α in k_mE.

Theorem 2. *Suppose that E/F is cyclic of degree 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 Theorem 1 our statement is true for $n = 1$. Consider the tower $F \subset E_{n-1} \subset E$ where E/E_{n-1} is a cyclic extension of degree p. Set $H_{n-1} := \mathrm{Gal}(E/E_{n-1})$ and $G_{n-1} := \mathrm{Gal}(E_{n-1}/F)$. Assume by induction that $i_{E_{n-1}}\colon k_mF \to (k_mE_{n-1})^{G_{n-1}}$ is an isomorphism. From Theorem 1 we see that $i_{E_{n-1},E}\colon k_mE_{n-1} \to (k_mE)^{H_{n-1}}$ is an isomorphism. Hence $i_E\colon k_mF \to k_mE$ is injective.

Because $i_{F,E}(k_mF) \subset (k_mE)^G$ it is sufficient to show that each $\bar{\alpha} \in (k_mE)^G$ can be written as $i_{F,E}(\bar{f})$ for some $f \in K_mF$.

Since $\bar{\alpha} \in (k_mE)^G \subset (k_mE)^{H_{n-1}}$, by Theorem 1 we see that there exists $\bar{\gamma} \in k_mE_{n-1}$ such that $i_{E_{n-1},E}\bar{\gamma} = \bar{\alpha}$. Because $\bar{\alpha} \in (k_mE)^G$ we see also that $\bar{\gamma} \in (k_mE_{n-1})^{G_{n-1}}$ and therefore there exists $f \in K_mF$ such that $i_{F,E_{n-1}}(\bar{f}) = \bar{\gamma}$. Then $i_{F,E}(\bar{f}) = \bar{\alpha}$ as required. $\square$

Theorem 3 (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 sequence*

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

is exact.

Now suppose E/F is cyclic of degree p^n. For $i = 0, \ldots, n$, 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 4. *There exists an isomorphism of $\mathbb{F}_p[G]$-modules $k_mE \cong \oplus_{i=0}^n Y_i$, where*

- *Y_n is a free $\mathbb{F}_p[G]$-module of rank $\dim_{\mathbb{F}_p} N_{E/F}k_mE$,*
- *Y_i, $0 < i < n$, is a free $\mathbb{F}_p[G_i]$-module of rank*
$$\dim_{\mathbb{F}_p} N_{E_i/F}k_mE_i/N_{E_{i+1}/F}k_mE_{i+1}, \text{ and}$$
- *Y_0 is a trivial $\mathbb{F}_p[G]$-module of rank $\dim_{\mathbb{F}_p} k_mF/N_{E_1/F}k_mE_1$.*

Our proof of Theorem 4 proceeds by induction on n. At each stage we use the norm map images $N_{E_i/F}k_mE_i$, $i = 1, \ldots, n$, to construct the modules Y_i. The most interesting portion is the construction of Y_{n-1}. It is easy to show that the modules Y_i are all independent, and we then use Theorems 2 and 3 to show that the sum of the Y_i exhausts k_mE.

The case $n = 1$ is section 2, and in section 3 we present the inductive argument. This argument relies on an extension lemma, Lemma 6, 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 crucial step in our induction. Lemma 6, together with two more basic extension lemmas used in the proof of that lemma, are presented in section 1, along with technical results on $\mathbb{F}_p[G]$-modules.

This work uses some ideas previously developed in investigations of the structure of pth-power classes of field extensions of pth-power degree [MSS].

1. Notation and Lemmas

1.1. **$\mathbb{F}_p[G]$-modules.** For the reader's convenience, after introducing some notation, we recall in this section some basic elementary facts about $\mathbb{F}_p[G]$-modules.

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

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

As usual, if U is a free $\mathbb{F}_p[G]$-module with $U = \oplus_{i \in \mathcal{I}} \mathbb{F}_p[G]$, we say that U is a module of rank $|\mathcal{I}|$. Denote by N the operator $(\sigma - 1)^{p^n - 1}$ acting on module U.

Lemma 1 (Inclusion Lemma)**.** *Let U and V be $\mathbb{F}_p[G]$-modules contained in an $\mathbb{F}_p[G]$-module W. Suppose that $(U + V)^G \subset U$ and for each $w \in (U + V) \setminus (U + V)^G$ there exists $u \in U$ such that*

$$(\sigma - 1)^{l(w)-1}(w) = N(u).$$

Then $V \subset U$.

Proof. Let $\{T_i\}_{i=1}^s$ be the socle series of $U + V$: $T_1 = (U + V)^G$ and $T_{i+1}/T_i = ((U + V)/T_i)^G$, and let s be the least natural number such that $T_s = U + V$. Observe that since $(\sigma - 1)^{p^n} = 0$, we have $s \leq p^n$. We prove the lemma by induction on the socle series.

By hypothesis, $T_1 \subset U$. Assume now that $T_i \subset U$ for some $i < s$. Then for each $w \in T_{i+1} \setminus T_i$ we have $l(w) = i + 1$ and $(\sigma - 1)^{l(w)-1}(w) = N(u) = (\sigma - 1)^{p^n - 1}(u)$ for some $u \in U$. Therefore

$$(\sigma - 1)^{l(w)-1}\big(w - (\sigma - 1)^{p^n - l(w)}(u)\big) = 0.$$

Therefore $w - (\sigma - 1)^{p^n - l(w)}(u) \in T_i \subset U$. Hence $w \in U$ and $T_{i+1} \subset U$ as required. □

Lemma 2 (Exclusion Lemma)**.** *Let U and V be $\mathbb{F}_p[G]$-modules contained in an $\mathbb{F}_p[G]$-module W. Suppose that $U^G \cap V^G = \{0\}$. Then $U + V = U \oplus V$.*

Proof. Let $Z = U \cap V$ and suppose that $y \in Z \setminus \{0\}$. Let

$$z = (\sigma - 1)^{l(y)-1}(y) \neq 0.$$

Then $z \in U^G \cap V^G$, a contradiction. Hence $U \cap V = \{0\}$ and $U + V = U \oplus V$. □

The following lemma follows from the fact that each free $\mathbb{F}_p[G]$-module is injective. (See [C, Theorem 11.2].) We shall, however, provide a direct proof.

Lemma 3 (Free Complement Lemma)**.** *Let $V \subset U$ be free $\mathbb{F}_p[G]$-modules. Then there exists a free $\mathbb{F}_p[G]$-submodule $\tilde{V}$ of U such that $V \oplus \tilde{V} = U$.*

Proof. Let Z be a complement of V^G in U^G as $\mathbb{F}_p$-vector spaces, and let $\mathcal{Z}$ be an $\mathbb{F}_p$-base of Z. For each $z \in \mathcal{Z}$, there exists $u(z)$ such that $z = N(u(z))$. Let $M(z)$ be the $\mathbb{F}_p[G]$-submodule of W generated by $u(z)$. Then $M(z)$ is a free $\mathbb{F}_p[G]$-submodule. Moreover, its fixed submodule $M(z)^G$ is the $\mathbb{F}_p$-vector subspace generated by z. By the Exclusion Lemma, the set of modules $M(z)$, $z \in \mathcal{Z}$, is independent.

Set $\tilde{V} := \oplus_{z\in\mathcal{Z}} M(z)$. Then $\tilde{V}$ is a free $\mathbb{F}_p[G]$-submodule of U and $\tilde{V}^G = Z$. By the Exclusion Lemma $V + \tilde{V} = V \oplus \tilde{V}$ and $(V \oplus \tilde{V})^G = V^G \oplus \tilde{V}^G = U^G$.

Now let $u \in U$ be arbitrary and let M be the cyclic $\mathbb{F}_p[G]$-submodule of U generated by u. Then $(M+V+\tilde{V})^G \subset U^G \subset V+\tilde{V}$. Moreover, for any $m \in M+V+\tilde{V} \setminus (M+V+\tilde{V})^G$, $(\sigma-1)^{l(m)-1}(m) \in (M+V+\tilde{V})^G \subset U^G = (V+\tilde{V})^G = N(V+\tilde{V})$ by the freeness of V and $\tilde{V}$. By the Inclusion Lemma, then, $M \subset V + \tilde{V}$. Hence $U = V \oplus \tilde{V}$. □

1.2. **Milnor k-groups.**

Recall that if $\alpha \in K_mE$ we write $\bar{\alpha}$ 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 $\mathbb{F}_p[G]$-submodule $\langle\bar{\gamma}\rangle$ of k_mE generated by $\bar{\gamma}$. Because $(\sigma-1)^{p^n-1} = 1 + \sigma + \cdots + \sigma^{p^n-1}$ in $\mathbb{F}_p[G]$, we may use $i_E N_{E/F}$ and N interchangeably on k_mE.

Our proof of Theorem 4 depends on Lemma 6. This lemma, in turn, requires for its induction two basic extension lemmas, the first for the case $p > 2$, $n = 1$, and the second for the case $p = 2$, $n = 2$. (The case $p = 2$, $n = 1$ is clear.) It is in only these two basic lemmas that Theorem 3 is used in this paper.

Lemma 4. *Suppose E/F is a cyclic extension of degree $p > 2$ and $\gamma \in K_mE$ with $2 \le l(\gamma) \le p$. Then there exists $\alpha \in K_mE$ such that*

$$\langle N\bar{\alpha}\rangle = \langle\bar{\gamma}\rangle^G.$$

Proof. Let $l = l(\gamma)$ and suppose $2 \le l \le i \le p$. We show by induction on i that there exists $\alpha_i \in K_mE$ such that

$$\langle(\sigma-1)^{i-1}\bar{\alpha}_i\rangle = \langle\bar{\gamma}\rangle^G.$$

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 $i_E\bar{c} = N\bar{\alpha}_i = (\sigma - 1)^{p-1}\bar{\alpha}_i$ and $i < p$, we conclude that $i_E\bar{c} = 0$. By the injectivity of i_E from Theorem 1, $\bar{c} = 0$. Therefore there exists $f \in K_mF$ such that $c = pf$ in K_mF.

We calculate

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

By Theorem 3, there exists $\omega \in K_mE$ such that

$$(\sigma - 1)\omega = \alpha_i - i_E(f).$$

Hence $(\sigma - 1)^2\omega = (\sigma - 1)\alpha_i$. Since $i \geq 2$,

$$\langle(\sigma - 1)^i\bar{\omega}\rangle = \langle(\sigma - 1)^{i-1}\bar{\alpha}_i\rangle = \langle\bar{\gamma}\rangle^G$$

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

Lemma 5. *Suppose $p = 2$ and E/F is a cyclic extension of degree 4. Suppose $\gamma \in K_mE$ with $3 \leq l(\gamma) \leq 4$. Then there exists $\alpha \in K_mE$ such that*

$$\langle N\bar{\alpha}\rangle = \langle\bar{\gamma}\rangle^G.$$

Proof. The case $l(\gamma) = 4$ is clear. Assume then that $l(\gamma) = 3$, and set $\beta := (\sigma - 1)\gamma$. Then

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

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

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

$$i_E\bar{c} = i_E(\sigma + 1)\bar{b} = (\sigma^2 - 1)\bar{\gamma} = i_EN_{E/E_1}\bar{\gamma},$$

and since $l(\gamma) = 3$, $\langle\bar{\gamma}\rangle^G = \langle\bar{c}\rangle$. Now $N_{E/E_1}\gamma = c + 2e$ for some $e \in K_mE$, and $e_1 := 2e \in K_mE_1 \cap 2K_mE$. Then $i_E(\bar{e}_1) = 0 \in k_mE$, and by the injectivity of i_E from Theorem 1, $e_1 = 2g$ for some $g \in K_mE_1$. Hence

$$N_{E/E_1}\gamma = c + 2g, \quad g \in K_mE_1.$$

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

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

so that $N_{E/F}(\gamma-\delta)=0$. By Theorem 3 there exists an $\alpha\in K_mE$ with $(\sigma-1)\alpha=\gamma-\delta$. Then

$$\begin{aligned} i_E N_{E/F}\bar{\alpha} &= (\sigma-1)^3\bar{\alpha} = (\sigma-1)^2\overline{(\gamma-\delta)} = \\ & i_E\overline{N_{E/E_1}(\gamma-\delta)} = i_E\overline{(c+2g-2b-2g)} = \\ & i_E\bar{c} = (\sigma-1)^2\bar{\gamma}. \end{aligned}$$

Because $\langle(\sigma-1)^2\bar{\gamma}\rangle=\langle\bar{\gamma}\rangle^G$ our statement follows. □

Our full extension lemma is then

Lemma 6. *Suppose that E/F is a cyclic extension of degree p^n, $n\in\mathbb{N}$, and let $\bar{\gamma}\in k_mE\setminus k_mE_{n-1}$. Then there exists $\chi\in K_mE$ such that*

$$(\sigma-1)^{l(\gamma)-1}\bar{\gamma}=(\sigma-1)^{p^n-1}\bar{\chi}=i_EN_{E/F}\bar{\chi}.$$

Proof. We shall first prove our statement in the case $p>2$. If $n=1$ then our statement follows from Lemma 4.

Assume therefore that $n>1$. Let $H:=H_{n-1}$, and write $l_H(\gamma)$ for the dimension over $\mathbb{F}_p$ of the $\mathbb{F}_p[H]$-submodule of k_mE generated by $\bar{\gamma}$. From Theorem 1 we see that $l_H(\gamma)\geq 2$. Therefore Lemma 4 tells us that there exists an element $\alpha\in K_mE$ such that

$$(\sigma-1)^{p^n-p^{n-1}}\bar{\alpha}=\left(\sigma^{p^{n-1}}-1\right)^{p-1}\bar{\alpha}=\left(\sigma^{p^{n-1}}-1\right)^{l_H(\gamma)-1}\bar{\gamma}\neq 0.$$

Set $s:=l(\gamma)-p^{n-1}(l_H(\gamma)-1)$. Then

$$(\sigma-1)^{p^n-p^{n-1}+s-1}\bar{\alpha}=(\sigma-1)^{p^{n-1}(l_H(\gamma)-1)+s-1}\bar{\gamma}\neq 0.$$

Furthermore, this element belongs to $(k_mE)^G$. Set $\lambda:=(\sigma-1)^s\alpha$. Then

$$(\sigma-1)^{p^n-p^{n-1}-1}\bar{\lambda}=(\sigma-1)^{p^n-p^{n-1}+s-1}\bar{\alpha},$$

whence $l(\lambda)=p^n-p^{n-1}$.

Now we consider $l_H(\lambda)$. On one hand,

$$\left(\sigma^{p^{n-1}}-1\right)^{p-1}\bar{\lambda}=0,$$

and on the other,

$$(\sigma-1)^{p^{n-1}(p-2)}\bar{\lambda}=(\sigma-1)^{p^n-2p^{n-1}}\bar{\lambda}\neq 0.$$

We deduce that $l_H(\lambda)=p-1\geq 2$. Applying Lemma 4 again, there exists $\chi\in K_mE$ with

$$(\sigma-1)^{p^n-p^{n-1}}\bar{\chi}=(\sigma-1)^{p^n-2p^{n-1}}\bar{\lambda}.$$

In particular, $l(\chi) = l(\lambda) + p^{n-1} = p^n$.

Summarizing, we have obtained

$$i_E N_{E/F}\bar{\chi} = (\sigma-1)^{p^n-1}\bar{\chi} = (\sigma-1)^{p^n-p^{n-1}-1}\bar{\lambda} = (\sigma-1)^{p^n-p^{n-1}+s-1}\bar{\alpha}.$$

Because

$$(\sigma-1)^{p^n-p^{n-1}+s-1}\bar{\alpha} = (\sigma-1)^{p^{n-1}(l_H(\gamma)-1)+s-1}\bar{\gamma} = (\sigma-1)^{l(\gamma)-1}\bar{\gamma},$$

we have established our equality in the case $p > 2$.

Now we shall consider the case $p = 2$. The case $n = 1$ is trivial, and the case $n = 2$ is handled by Lemma 5. Assume therefore that $n \geq 3$. Let $H := \mathrm{Gal}(E/E_{n-2})$, and write $l_H(\gamma)$ for the dimension over $\mathbb{F}_2$ of the cyclic $\mathbb{F}_2[H]$-submodule of $k_m E$ generated by $\bar{\gamma}$.

Because $\bar{\gamma} \notin k_m E_{n-1}$, we have $l_H(\gamma) \geq 3$. From Lemma 5 we see that there exists $\alpha \in K_m E$ such that

$$\left(\sigma^{2^{n-2}}-1\right)^3 \bar{\alpha} = \left(\sigma^{2^{n-2}}-1\right)^{l_H(\gamma)-1} \bar{\gamma}.$$

Hence

$$(\sigma-1)^{2^n-2^{n-2}} \bar{\alpha} = (\sigma-1)^{2^{n-2}(l_H(\gamma)-1)} \bar{\gamma} \neq 0.$$

Let $s := l(\gamma) - 2^{n-2}(l_H(\gamma)-1)$. Then we have

$$(\sigma-1)^{2^n-2^{n-2}+s-1} \bar{\alpha} = (\sigma-1)^{2^{n-2}(l_H(\gamma)-1)+s-1} \bar{\gamma} \neq 0.$$

Furthermore, this element belongs to $(k_m E)^G$. Set $\lambda := (\sigma-1)^s\alpha$. Then

$$(\sigma-1)^{2^n-2^{n-2}-1}\bar{\lambda} = (\sigma-1)^{2^n-2^{n-2}+s-1}\bar{\alpha},$$

whence $l(\lambda) = 2^n - 2^{n-2}$.

Now we consider $l_H(\lambda)$. On one hand,

$$\left(\sigma^{2^{n-2}}-1\right)^3 \bar{\lambda} = (\sigma-1)^{2^n-2^{n-2}}\bar{\lambda} = 0,$$

and on the other,

$$\left(\sigma^{2^{n-2}}-1\right)^2 \bar{\lambda} \neq 0.$$

We deduce that $l_H(\lambda) = 3$. By Lemma 5 there exists $\chi \in K_m E$ with

$$\left(\sigma^{2^{n-2}}-1\right)^3 \bar{\chi} = \left(\sigma^{2^{n-2}}-1\right)^2 \bar{\lambda}.$$

Equivalently, $(\sigma-1)^{2^n-2^{n-2}}\bar{\chi} = (\sigma-1)^{2^{n-1}}\bar{\lambda}$, and therefore $l(\chi) = l(\lambda) + 2^{n-2} = 2^n$.

Summarizing, we have obtained

$$\begin{aligned} i_E N_{E/F}\bar{\chi} &= (\sigma-1)^{2^n-1}\bar{\chi} = (\sigma-1)^{2^n-2^{n-2}-1}\bar{\lambda} \\ &= (\sigma-1)^{2^n-2^{n-2}+s-1}\bar{\alpha} = (\sigma-1)^{l(\gamma)-1}\bar{\gamma} \end{aligned}$$

as required. □

Remark. Observe that since $\langle\bar{\gamma}\rangle^G$ is a one-dimensional $\mathbb{F}_p$-vector space and N is additive, the equality $\langle N\bar{\alpha}\rangle = \langle\bar{\gamma}\rangle^G$ holds if and only if any $\bar{\delta} \in \langle\bar{\gamma}\rangle^G \setminus \{0\}$ is expressible as $N\bar{\beta}$ for some $\bar{\beta} \in k_m E$.

Lemma 7 (Submodule-Subfield Lemma)**.** *Suppose E/F is a cyclic extension of degree p^n, and let U be a free $\mathbb{F}_p[G]$-submodule of $k_m E$. Then for each i in $\{0, 1, \ldots, n-1\}$ we have:*

$$U^{H_i} = (\sigma-1)^{p^n-p^i}U = U \cap i_E(N_{E/E_i}k_m E) = U \cap i_E(k_m E_i).$$

Proof. Suppose $\bar{\alpha} \in U^{H_i}$. Then $(\sigma^{p^i}-1)\bar{\alpha} = (\sigma-1)^{p^i}\bar{\alpha} = 0$, so $l(\alpha) \leq p^i$. Since U is free, $\bar{\alpha} = (\sigma-1)^{p^n-l(\alpha)}\bar{\beta}$ for some $\bar{\beta} \in U$. In particular,

$$\bar{\alpha} = (\sigma-1)^{p^n-p^i}(\sigma-1)^{p^i-l(\alpha)}\bar{\beta}.$$

Hence $U^{H_i} \subset (\sigma-1)^{p^n-p^i}U$. Now suppose $\bar{\alpha} = (\sigma-1)^{p^n-p^i}\bar{\gamma}$. Then since

$$(\sigma-1)^{p^n-p^i}\bar{\gamma} = i_E N_{E/E_i}\bar{\gamma},$$

we have $(\sigma-1)^{p^n-p^i}U \subset U \cap i_E(N_{E/E_i}k_m E) \subset U \cap i_E(k_m E_i)$.

Now suppose that $\bar{\alpha} \in U \cap i_E(k_m E_i)$. Then $\bar{\alpha} \in U^{H_i}$ and hence all of the inclusions are equalities. □

Remark. Alternatively one can derive the first equality in the lemma above, as follows. If U is a free $\mathbb{F}_p[G]$-module, then U is also a free $\mathbb{F}_p[H_i]$-module. But then $H^2(H_i, U) = \{0\}$. Hence $U^{H_i} = N_i(U) :=$ the image of the norm operator N_i. Thus $U^{H_i} = U^{(\sigma-1)^{p^n-p^i}}$ as required.

2. E/F Cyclic of Degree p

Proposition. *Theorem 4 holds for $n = 1$.*

Proof. We first construct submodules Y_0 and Y_1 of $k_m E$. Let $\mathcal{I}$ be an $\mathbb{F}_p$-basis for the subspace $i_E(N_{E/F}k_m E)$. For each basis element $\bar{y} \in \mathcal{I}$, let $\alpha_y \in K_m E$ satisfy $i_E(N_{E/F}\bar{\alpha}_y) = \bar{y}$. Then $\langle\bar{\alpha}_y\rangle$ is a cyclic submodule of dimension p, hence isomorphic to $\mathbb{F}_p[G]$, with

$$\langle\bar{\alpha}_y\rangle^G = (\sigma-1)^{p-1}\langle\bar{\alpha}_y\rangle = \langle N\bar{\alpha}_y\rangle = \langle\bar{y}\rangle.$$

Set $Y_1 := \sum_{\bar{y}\in\mathcal{I}}\langle\bar{\alpha}_y\rangle$. By the Exclusion Lemma, $Y_1 = \oplus_{\bar{y}\in\mathcal{I}}\langle\bar{\alpha}_y\rangle$ and so Y_1 is a free $\mathbb{F}_p[G]$-module. Moreover,

$$Y_1^G = (\sigma-1)^{p-1}Y_1 = NY_1 = \oplus_{\bar{y}\in\mathcal{I}}\langle\bar{y}\rangle = i_E(N_{E/F}k_mE).$$

The rank of Y_1 is equal to the dimension of $i_E(N_{E/F}k_mE)$, and by the injectivity of i_E from Theorem 1, we conclude

$$\operatorname{rank} Y_1 = \dim_{\mathbb{F}_p} N_{E/F}k_mE.$$

Now let Z be any $\mathbb{F}_p$-module complement of $N_{E/F}k_mE$ in k_mF, and set $Y_0 := i_EZ$. By the injectivity of i_E from Theorem 1, we obtain

$$\operatorname{rank} Y_0 = \dim_{\mathbb{F}_p} k_mF/N_{E/F}k_mE.$$

By the Exclusion Lemma, $Y_0 + Y_1 = Y_0 \oplus Y_1$. Moreover, $Y_0 + Y_1$ contains $(k_mE)^G$:

$$\begin{aligned}(k_mE)^G &= i_E(k_mF) = i_E((N_{E/F}k_mE)\oplus Z)\\ &= i_E(N_{E/F}k_mE)\oplus Y_0 = Y_1^G \oplus Y_0 \subset Y_0\oplus Y_1.\end{aligned}$$

If $p=2$, we already have enough to prove the proposition, as follows. Let $\bar{\gamma}\in k_mE$. If $(\sigma-1)\bar{\gamma}=0$ then $\bar{\gamma}\in(k_mE)^G\subset Y_0\oplus Y_1$ as above. Otherwise, observe that since $p=2$, the operator $\sigma-1$ is equivalent to $i_EN_{E/F}$ on k_mE. Let $\beta = i_EN_{E/F}\gamma$. Then $(\sigma-1)\bar{\gamma} = \bar{\beta}\in Y_1^G$. Since Y_1 is free there exists $\bar{\alpha}\in Y_1$ such that $(\sigma-1)\bar{\alpha}=\bar{\beta}$. Then $(\sigma-1)(\bar{\gamma}-\bar{\alpha})=0$, so $l(\gamma-\alpha)\le 1$ and $\bar{\gamma}-\bar{\alpha}\in(k_mE)^G\subset Y_1\oplus Y_0$. Since $\bar{\alpha}\in Y_1$, we conclude that $\bar{\gamma}\in Y_1\oplus Y_0$ as well. Hence $k_mE = Y_1\oplus Y_0$.

If $p>2$, we instead prove by induction on $l(\gamma)$ that each $\bar{\gamma}\in k_mE$ lies in $Y_1\oplus Y_0$, whence we will obtain the proposition. The case $l(\gamma)=1$ follows from $(k_mE)^G\subset Y_1\oplus Y_0$. Suppose now that for each $\bar{\beta}\in k_mE$ with $l(\beta)\le i<p$ we have $\bar{\beta}\in Y_1\oplus Y_0$, and assume that $l(\gamma)=i+1\ge 2$. By Lemma 4 there exists an $\alpha\in K_mE$ with

$$\langle N\bar{\alpha}\rangle = \langle\bar{\gamma}\rangle^G.$$

Hence $(\sigma-1)^i\bar{\gamma} = cN\bar{\alpha}$ for some $c\in\mathbb{Z}$. Now $cN\bar{\alpha} = i_EN_{E/F}(c\bar{\alpha})\in Y_1^G$. Since Y_1 is free, there exists $\bar{\omega}\in Y_1$ such that $(\sigma-1)^{p-1}\bar{\omega} = cN\bar{\alpha}$. Set $\bar{\lambda} = (\sigma-1)^{p-l(\gamma)}\bar{\omega}\in Y_1$, so that $(\sigma-1)^{l(\gamma)-1}(\bar{\gamma}-\bar{\lambda}) = 0$. Hence $l(\gamma-\lambda)<l(\gamma)$ and by induction $\bar{\gamma} = (\bar{\gamma}-\bar{\lambda})+\bar{\lambda}\in Y_1\oplus Y_0$. Thus again we conclude that $k_mE = Y_1\oplus Y_0$. □

3. Proof of Theorem 4

We proceed by induction. The case $n = 1$ is the preceding proposition. Assume then that Theorem 4 holds when degree of E/F is $\leq p^{n-1}$, and suppose that E/F is a cyclic extension of degree p^n with $n \geq 2$.

3.1. **Constructing the Y_i.**

Let $\mathcal{I}$ be an $\mathbb{F}_p$-basis for $i_E(N_{E/F}k_mE)$. For each basis element $\bar{y} \in \mathcal{I}$ construct a free $\mathbb{F}_p[G]$-module $\langle \bar{\alpha}_y \rangle$, such that $i_E N_{E/F}\bar{\alpha}_y = \bar{y}$. We see by the Exclusion Lemma that the modules $\langle \bar{\alpha}_y \rangle$, $\bar{y} \in \mathcal{I}$, are independent. Set $Y_n := \oplus_{y\in\mathcal{I}}\langle \bar{\alpha}_y \rangle$. Hence Y_n is a direct sum of cyclic $\mathbb{F}_p[G]$-modules of dimension p^n, and $Y_n^G = i_E(N_{E/F}k_mE)$. By the injectivity of i_E from Theorem 2,

$$\operatorname{rank}_{\mathbb{F}_p[G]} Y_n = \dim_{\mathbb{F}_p} Y_n^G = \dim_{\mathbb{F}_p} N_{E/F}k_mE.$$

By induction, we have a $\mathbb{F}_p[G_{n-1}]$-module decomposition

$$k_mE_{n-1} = \tilde{Y}_{n-1} \oplus \tilde{Y}_{n-2} \oplus \cdots \oplus \tilde{Y}_0$$

into direct sums $\tilde{Y}_i$ of cyclic $\mathbb{F}_p[G_{n-1}]$-modules of dimension p^i, $i = 0, 1, \ldots, n-1$. Let $\bar{\sigma}$ denote the image of σ under the natural projection $G \to G_{n-1}$. Because $i_{E_{n-1}}N_{E_{n-1}/F}$ acts on k_mE_{n-1} as $(\bar{\sigma}-1)^{p^{n-1}-1}$ and $i_{E_{n-1}}$ is injective, we see that $N_{E_{n-1}/F}$ annihilates the sum $\tilde{Y}_{n-2} \oplus \cdots \oplus \tilde{Y}_0$. Therefore

$$i_{E_{n-1}}(N_{E_{n-1}/F}k_mE_{n-1}) = \tilde{Y}_{n-1}^{G_{n-1}}.$$

Now consider k_mE as an $\mathbb{F}_p[H_{n-1}]$-module. By the injectivity of i_E from Theorem 1, the images of $\tilde{Y}_i$, $i = 0, \ldots, n-1$, under i_E are direct sums of cyclic modules of dimension p^i and are independent. Because the modules $\tilde{Y}_i$ are direct sums of cyclic $\mathbb{F}_p[G_{n-1}]$-modules, the images $i_E\tilde{Y}_i$ are direct sums of cyclic $\mathbb{F}_p[G]$-modules. Set $Y_i := i_E\tilde{Y}_i$ for $i < n-1$. Observe that $\operatorname{rank}_{\mathbb{F}_p[G_i]} Y_i = \operatorname{rank}_{\mathbb{F}_p[G_i]} \tilde{Y}_i$.

Set $W := Y_n^{H_{n-1}}$. By the Submodule-Subfield Lemma,

$$W = (\sigma - 1)^{p^n - p^{n-1}} Y_n = Y_n \cap i_E k_m E_{n-1}.$$

Since Y_n is a direct sum of cyclic $\mathbb{F}_p[G]$-modules of dimension p^n, W is a direct sum of cyclic modules of dimension p^{n-1} and hence is free as an $\mathbb{F}_p[G_{n-1}]$-module. Because $W \subset i_E k_m E_{n-1}$, we may consider the image

P of the projection map $\mathrm{pr}\colon W \to i_E\tilde{Y}_{n-1}$ from W to the summand $i_E\tilde{Y}_{n-1}$ in the decomposition

$$i_E k_m E_{n-1} = i_E\tilde{Y}_{n-1} \oplus Y_{n-2} \oplus \cdots \oplus Y_0.$$

Observe that $W \cong P$ as $\mathbb{F}_p[G_{n-1}]$-modules. Indeed, since W is a free $\mathbb{F}_p[G_{n-1}]$-module, each $w \in W \setminus \{0\}$ may be written as $(\bar{\sigma}-1)^s\tilde{w}$ for some $0 \le s \le p^{n-1}-1$ and $\tilde{w} \in W$ with $l(\tilde{w}) = p^{n-1}$. We have

$$(\bar{\sigma}-1)^{p^{n-1}-1}\,\mathrm{pr}(\tilde{w}) = (\bar{\sigma}-1)^{p^{n-1}-1}\tilde{w} \neq 0,$$

since all other components of $\tilde{w}$ are killed by $(\bar{\sigma}-1)^{p^{n-1}-1}$. (Since $n \ge 2$, $p^{n-1}-1 \ge p^{n-2}$.) Therefore $(\bar{\sigma}-1)^s\,\mathrm{pr}(\tilde{w}) = \mathrm{pr}(w) \neq 0$. We conclude that the kernel of the projection map is (0), as required.

Since $M^{G_{n-1}} = (\sigma-1)^{p^{n-1}-1}M$ for free $\mathbb{F}_p[G_{n-1}]$-modules, we have further obtained that $W^{G_{n-1}} = P^{G_{n-1}}$. Observe that

$$W^{G_{n-1}} = (\sigma-1)^{p^{n-1}-1}W \subset i_E(N_{E_{n-1}/F}k_m E_{n-1}) = (i_E\tilde{Y}_{n-1})^G.$$

By the Free Complement Lemma, there exists a free $\mathbb{F}_p[G_{n-1}]$-module complement Y_{n-1} in $i_E\tilde{Y}_{n-1}$ of P. Since $W = Y_n \cap i_E k_m E_{n-1}$, we obtain $Y_n^G = W^{G_{n-1}} = P^{G_{n-1}}$. By the Exclusion Lemma, $P^{G_{n-1}} \cap Y_{n-1}^{G_{n-1}} = \{0\}$ implies that $Y_{n-1}+Y_n = Y_{n-1}\oplus Y_n$. Then, since $P^G + Y_{n-1}^G = (i_E\tilde{Y}_{n-1})^G$, we obtain $(Y_{n-1}+Y_n)^G = (i_E\tilde{Y}_{n-1})^G$. By induction and the injectivity of i_E,

$$\mathrm{rank}_{\mathbb{F}_p[G_{n-1}]}\, i_E\tilde{Y}_{n-1} = \dim_{\mathbb{F}_p}(i_E\tilde{Y}_{n-1})^G = \dim_{\mathbb{F}_p} N_{E_{n-1}/F}k_m E_{n-1}.$$

Since $Y_{n-1}^G \oplus Y_n^G = (i_E\tilde{Y}_{n-1})^G$,

$$\mathrm{rank}_{\mathbb{F}_p[G_{n-1}]}\, Y_{n-1} = \dim_{\mathbb{F}_p} Y_{n-1}^G = \dim_{\mathbb{F}_p} N_{E_{n-1}/F}k_m E_{n-1}/N_{E/F}k_m E.$$

Finally, by the Exclusion Lemma, $Y_{n-1}+Y_n$ is independent from $Y_{n-2}+\cdots+Y_0$. Hence we have a submodule

$$Y = Y_n \oplus Y_{n-1} \oplus \cdots \oplus Y_0 \subset k_m E$$

with ranks satisfying the claims of Theorem 4.

3.2. **Showing $k_m E = \oplus Y_i$.**

We prove first that $Y^{H_{n-1}} = i_E k_m E_{n-1}$. Theorem 1 tells us that $Y^{H_{n-1}} \subset i_E k_m E_{n-1}$, and we have the decomposition $i_E k_m E_{n-1} = i_E\tilde{Y}_{n-1} \oplus Y_{n-2} \oplus \cdots \oplus Y_0$. Therefore it is sufficient to show that

$$i_E\tilde{Y}_{n-1} \subset Y^{H_{n-1}} = Y_n^{H_{n-1}} + Y_{n-1} + \cdots + Y_0.$$

Because $i_E\tilde{Y}_{n-1} = Y_{n-1} + P$ it is enough to show that

$$P \subset Y_n^{H_{n-1}} + Y_{n-1} + \cdots + Y_0 = W + Y_{n-1} + \cdots + Y_0.$$

But by the definition of the projection, $P \subset W + Y_{n-2} + \cdots + Y_0$. Hence $P \subset W + Y_{n-1} + \cdots + Y_0$, and we conclude that $Y_n^{H_{n-1}} = i_E k_m E_{n-1}$.

We adapt the proof of the Inclusion Lemma to show that $k_m E \subset Y$, by induction on the socle series V_i of $k_m E$. Our base case is $V_{p^{n-1}}$. Observe that $V_{p^{n-1}}$ is the kernel of $(\sigma - 1)^{p^{n-1}} = \sigma^{p^{n-1}} - 1$, which is $(k_m E)^{H_{n-1}}$. Hence $V_{p^{n-1}} \subset Y$.

For the inductive step, assume that $V_i \subset Y$ for all $i < t$ for some $p^{n-1} < t \leq p^n$, and let $\bar{\gamma} \in V_t \setminus V_{t-1}$. Hence $l(\gamma) = t$. Therefore $\bar{\gamma} \notin i_E k_m E_{n-1}$, and by Lemma 6 there exists $\chi \in K_m E$ such that

$$(\sigma - 1)^{t-1}\bar{\gamma} = i_E N_{E/F}\bar{\chi} \in Y_n^G.$$

Since Y_n is a free $\mathbb{F}_p[G]$-module, there exists $\bar{\nu} \in Y_n$ such that

$$i_E N_{E/F}\bar{\nu} = (\sigma - 1)^{p^n - 1}\bar{\nu} = (\sigma - 1)^{p^n - 1}\bar{\chi} = (\sigma - 1)^{t-1}\bar{\gamma}.$$

Set $\bar{\delta} := (\sigma - 1)^{p^n - t}\bar{\nu} \in Y_n \subset Y$. Then $(\sigma - 1)^{t-1}(\bar{\gamma} - \bar{\delta}) = 0$ and hence $l(\gamma - \delta) < t$. By induction $\bar{\gamma} - \bar{\delta} \in Y$, and since $\bar{\delta} \in Y$, we see that $\bar{\gamma} \in Y$ as well. □

Acknowledgment

We are very grateful to Andy Schultz, as some of his ideas, developed in [MSS], proved quite useful to us during the investigations leading to this paper.

References

[BK] S. Bloch and K. Kato. p-adic étale cohomology. *Inst. Hautes Études Sci. Publ. Math.* **63** (1986), 107–152.

[C] J. Carlson. *Modules and group algebras.* Lectures in Mathematics ETH Zürich. Basel: Birkhäuser Verlag, 1996.

[FV] I. Fesenko and S. Vostokov. *Local fields and their extensions*, 2nd ed. Translations of Mathematical Monographs 121. Providence, RI: American Mathematical Society, 2002.

[I1] O. Izhboldin. 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.

[I2] O. Izhboldin. On p-torsion in K_*^M for fields of characteristic p. *Algebraic K-theory.* Advances in Soviet Mathematics 4. Providence, RI: American Mathematical Society, 1991, 129–144.

[K] K. Kato. Symmetric bilinear forms, quadratic forms and Milnor K-theory in characteristic two. *Invent. Math.* **66** (1982), no. 3, 493–510.

[M] J. Milnor. Algebraic K-theory and quadratic forms. *Invent. Math.* **9** (1970), 318–344.

[MSS] J. Mináč, A. Schultz, and J. Swallow. Galois module structure of pth-power classes of cyclic extensions of degree p^n. Preprint, 2004.

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

E-mail address: gbhandar@uwo.ca

E-mail address: nlemire@uwo.ca

E-mail address: minac@uwo.ca

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

E-mail address: joswallow@davidson.edu