GALOIS MODULE STRUCTURE OF GALOIS COHOMOLOGY

NICOLE LEMIRE⋆, JÁN MINÁČ∗†, AND JOHN SWALLOW‡

Abstract. Let F be a field containing a primitive pth root of unity, and let U be an open normal subgroup of index p of the absolute Galois group G_F of F. We determine the structure of the cohomology group $H^n(U, \mathsf{F}_p)$ as an $\mathsf{F}_p[G_F/U]$-module for all $n \in \mathsf{N}$. Previously this structure was known only for $n = 1$, and until recently the structure even of $H^1(U, \mathsf{F}_p)$ was determined only for F a local field, a case settled by Borevič and Faddeev in the 1960s.

Let F be a field containing a primitive pth root of unity ξ_p. Let G_F be the absolute Galois group of F, U an open normal subgroup of G_F of index p, and $G = G_F/U$. Let E be the fixed field of U in the separable closure F_{sep} of F. Fix $a \in F$ such that $E = F(\sqrt[p]{a})$, and let $\sigma \in G$ satisfy $\sqrt[p]{a}^{\sigma-1} = \xi_p$.

In the 1960s Z. I. Borevič and D. K. Faddeev classified the possible G-module structures of the first cohomology groups $H^1(U, \mathsf{F}_p)$ in the case F a local field [B]. Quite recently this result was extended for all fields F as above [MS]. For the study of Galois cohomology it is important to extend these results to all cohomology groups $H^n(U, \mathsf{F}_p)$, $n \in \mathsf{N}$, and a solution of this problem was out of reach until now.

Recently, based on earlier work of A. S. Merkurjev, M. Rost and A. A. Suslin, V. Voevodsky established the Bloch-Kato Conjecture [V1, V2], and it turns out that some of the main theorems in his proof are sufficient to determine the structure of all G-Galois modules $H^n(U, \mathsf{F}_p)$, using only simple arithmetical invariants attached to the field extension E/F. The theorems we use (quoted as Theorems 3 and 4 in section 1 below) had, in fact, been standard conjectures on Galois cohomology.

Date: October 29, 2004.

⋆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 National Security Agency grant MDA904-02-1-0061.

It is interesting to point out, however, that the case $n = 2$ could have already been settled some 20 years ago, thanks to the work of Merkurjev and Suslin [MeSu].

The main ingredient for our determination of the G-module structure of $H^n(U, \mathsf{F}_p)$ is Milnor K-theory. (See [Mi] and [FV, Chap. IX].) For $i \geq 0$, let K_iF denote the ith Milnor K-group of the field F, with standard generators denoted by $\{f_1, \dots, f_i\}$, $f_1, \dots, f_i \in F \setminus \{0\}$. For $\alpha \in K_iF$, we denote by $\bar{\alpha}$ the class of α modulo p, and we use the usual abbreviation k_nF for K_nF/pK_nF. We write $N_{E/F}$ for the norm map $K_nE \to K_nF$, and we use the same notation for the induced map modulo p. We denote by i_E the natural homomorphism in the reverse direction. We also apply the same notation $N_{E/F}$ and i_E for the corresponding homomorphisms between cohomology groups. The image of an element $\alpha \in K_iF$ in $H^i(G_F, \mathsf{F}_p)$ we also denote by α. Voevodsky's proof of the Bloch-Kato Conjecture establishes a G_F-isomorphism $H^n(U, \mathsf{F}_p) \cong k_nE$. We formulate our results in terms of Galois cohomology for intended applications, but we use Milnor K-theory in our proof.

We concentrate upon the case when F is a perfect field, and at the end of the paper we indicate how one may reduce the case of an imperfect field F to the case of characteristic 0.

Our decomposition depends on four arithmetic invariants Υ_1, Υ_2, y, z, which we define as follows. First, for an element $\bar{\alpha}$ of k_iF, let

$$\operatorname{ann}_{k_{n-1}F} \bar{\alpha} = \operatorname{ann}\left(k_{n-1}F \xrightarrow{\bar{\alpha}\cdot -} k_{n-1+i}F\right)$$

denote the annihilator of the product with $\bar{\alpha}$. When the domain of $\bar{\alpha}$ is clear, we omit the subscript on the map and write simply $\operatorname{ann} \bar{\alpha}$. Because we will often use the elements $\overline{\{a\}}$, $\overline{\{\xi_p\}}$, $\overline{\{a, a\}}$, and $\overline{\{a, \xi_p\}}$, we omit the bars for these elements. We also omit the bar in the element $\overline{\{\sqrt[p]{a}\}} \in k_nE$.

Fix $n \in \mathsf{N}$ and U an open normal subgroup of G_F of index p with fixed field E. Define invariants associated to E/F and n as follows:

$$\begin{aligned}
d &:= \dim_{\mathsf{F}_p}\ k_nF \ /\ N_{E/F}k_nE \\
e &:= \dim_{\mathsf{F}_p}\ N_{E/F}k_nE \\
\Upsilon_1 &:= \dim_{\mathsf{F}_p}\ \operatorname{ann}\{a, \xi_p\} \ /\ \operatorname{ann}\{a\} \\
\Upsilon_2 &:= \dim_{\mathsf{F}_p}\ k_{n-1}F \ /\ \operatorname{ann}\{a, \xi_p\}
\end{aligned}$$

$$y := \begin{cases} \dim_{\mathsf{F}_p} \ (N_{E/F}k_nE) \ / \ \{a\} \cdot k_{n-1}F, & p > 2 \\ \dim_{\mathsf{F}_2} \ (N_{E/F}k_nE) \ / \ \{a\} \cdot \operatorname{ann}_{k_{n-1}F}\{a,-1\}, & p = 2 \end{cases}$$

$$z := \begin{cases} \dim_{\mathsf{F}_p} \ (k_nF) \ / \ \left(\{\xi_p\} \cdot W + N_{E/F}k_nE\right), & p > 2 \\ \dim_{\mathsf{F}_2} \ (k_nF) \ / \ \left(\{a\} \cdot k_{n-1}F + N_{E/F}k_nE\right), & p = 2, \end{cases}$$

where W is a complement of $\operatorname{ann}\{a, \xi_p\}$ in $k_{n-1}F$. (In Lemma 1 we show that z is independent of the choice of W.)

Our main results are then the following.

Theorem 1. *If $p > 2$, F is perfect and $n \in \mathsf{N}$ then*

$$H^n(U, \mathsf{F}_p) \cong X_1 \oplus X_2 \oplus Y \oplus Z$$

where

(1) *X_1 is a trivial $\mathsf{F}_p[G]$-module of dimension Υ_1*
(2) *X_2 is a direct sum of Υ_2 cyclic $\mathsf{F}_p[G]$-modules of dimension 2*
(3) *Y is a free $\mathsf{F}_p[G]$-module of rank y*
(4) *Z is a trivial $\mathsf{F}_p[G]$-module of dimension z.*

Further we have

(5) $Y^G = i_E N_{E/F} H^n(U, \mathsf{F}_p)$
(6) $N_{E/F} \colon X_1 \oplus X_2 \to \{a\} \cdot H^{n-1}(G_F, \mathsf{F}_p)$ *is surjective*
(7) $\Upsilon_1 + \Upsilon_2 + y = e$
(8) $\Upsilon_2 + z = d$

Theorem 2. *If $p = 2$ and $n \in \mathsf{N}$ then*

$$H^n(U, \mathsf{F}_2) \cong X_1 \oplus Y \oplus Z$$

where

(1) *X_1 is a trivial $\mathsf{F}_2[G]$-module of dimension Υ_1*
(2) *Y is a free $\mathsf{F}_2[G]$-module of rank y.*
(3) *Z is a trivial $\mathsf{F}_2[G]$-module of dimension z.*

Further we have

(4) $Y^G = i_E N_{E/F} H^n(U, \mathsf{F}_2)$
(5) $N_{E/F} \colon X_1 \to \{a\} \cdot \operatorname{ann}\{a, -1\}$ *is an isomorphism*
(6) $\Upsilon_1 + y = e$
(7) $\Upsilon_2 + z = d$

Remark. As explained at the end of section 5, if $n \leq 2$ in Theorem 1, we may remove the hypothesis that F is perfect. The case $n = 1$ in the two theorems recovers the results of [MS].

1. Bloch-Kato and Milnor K-theory

Our proof relies on the following two results in Voevodsky's proof of the Bloch-Kato Conjecture. Because we apply Voevodsky's results in the case when the base field contains a primitive pth root of unity we shall formulate Voevodsky's results restricted to this case. The first is the Bloch-Kato Conjecture itself:

Theorem 3 ([V1, Def. 5.1] and [V2, Thm. 7.1])**.**

(1) *Let F be a field containing a primitive pth root of unity and $m \in \mathbb{N}$. Then the norm residue homomorphism*

$$k_m F \to H^m(G_F, \mu_p)$$

is an isomorphism.

(2) *For any cyclic extension E/F of degree p, the sequence*

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

is exact.

The second result establishes an exact sequence connecting $k_m F$ and $k_m E$ for consecutive m. (We translate the statement of the original result to K-theory using the previous theorem.) In the following result a is chosen to satisfy $E = F(\sqrt[p]{a})$.

Theorem 4 ([V1, Prop. 5.2])**.** *Let F be a field containing a primitive pth root of unity with no extensions of degree prime to p. Then for any cyclic extension E/F of degree p and $m \geq 1$, the sequence*

$$k_{m-1} E \xrightarrow{N_{E/F}} k_{m-1} F \xrightarrow{\{a\} \cdot -} k_m F \xrightarrow{i_E} k_m E$$

is exact.

Now if F is a perfect field, we observe that we may remove the hypothesis that the field F has no extensions of degree prime to p. It is precisely to ensure that the sequence above is exact that we require the hypothesis that F is perfect in Theorem 1. We give a proof of the following theorem in section 5.

Theorem 5 (Modification of Theorem 4)**.** *Let F be a field containing a primitive pth root of unity, and if $p > 2$ assume that F is perfect. Then for any cyclic extension E/F of degree p and $m \geq 1$ the sequence*

$$k_{m-1}E \xrightarrow{N_{E/F}} k_{m-1}F \xrightarrow{\{a\}\cdot -} k_mF \xrightarrow{i_E} k_mE$$

is exact.

2. Notation and Lemmas

For the remainder of the paper, except for section 6, we assume that F is perfect if $p > 2$. We fix $n \in \mathsf{N}$ and the cyclic extension $E = F(\sqrt[p]{a})$, and we write $k_{n-1}F = \operatorname{ann}\{a\} \oplus V \oplus W$, where $\operatorname{ann}\{a, \xi_p\} = \operatorname{ann}\{a\} \oplus V$. Observe that $\Upsilon_1 = \dim_{\mathsf{F}_p} V$ and $\Upsilon_2 = \dim_{\mathsf{F}_p} W$. We show that the invariant z is independent of the choice of W:

Lemma 1. *The invariant z is independent of the particular complement W of $\operatorname{ann}\{a, \xi_p\}$ in $k_{n-1}F$.*

Proof. This is obvious for $p = 2$, so assume that $p > 2$. Let W' be another F_p-subspace of $k_{n-1}F$ with $k_{n-1}F = \operatorname{ann}\{a, \xi_p\} \oplus W'$. Then we may choose bases $\{w_i\}_{i\in\mathcal{I}}$ and $\{w_i'\}_{i\in\mathcal{I}}$ of W and W', respectively, such that $w_i' = w_i + u_i$ for $u_i \in \operatorname{ann}\{a, \xi_p\}$. Then $\{\xi_p\}\cdot w_i' = \{\xi_p\}\cdot w_i + \{\xi_p\}\cdot u_i$, and $\{\xi_p\} \cdot u_i \in \operatorname{ann}\{a\}$. Because $\operatorname{ann}\{a\} = N_{E/F}k_nE$ by Theorem 5, we see that

$$\{\xi_p\} \cdot W + N_{E/F}k_nE = \{\xi_p\} \cdot W' + N_{E/F}k_nE$$

and therefore z does not depend on the choice of W.

We denote by $i_E\colon K_nF \to K_nE$ the map induced by the inclusion of F in E. In what follows we will frequently refer to the element $\sqrt[p]{a}$, and so we abbreviate it by A. We will also often use the observation that if $p = 2$ then $\{a, \xi_p\} = \{a, -1\} = \{a, a\} \in k_2F$, while if $p > 2$ then $\{a, a\} = 0 \in k_2F$. Finally, we will use the projection formula for taking the norms of standard generators of K_iF (see [FW, p. 81]).

Lemma 2. *We have the vector space isomorphism*

$$V \oplus W \xrightarrow{\{a\}\cdot -} \{a\} \cdot k_{n-1}F$$

and, if $p > 2$, the compositum of the maps $\{\xi_p\} \cdot -$ and i_E

$$W \xrightarrow{\{\xi_p\}\cdot -} \{\xi_p\} \cdot W \xrightarrow{i_E} i_E(\{\xi_p\} \cdot W)$$

is a vector space isomorphism as well.

Proof. The first isomorphism follows from the fact that $V \oplus W$ is a complement in $k_{n-1}F$ of the kernel of multiplication by $\{a\}$. For the second, assume $p > 2$. Suppose that $\bar{w} \in W$ and $\bar{\alpha} = \{\xi_p\} \cdot \bar{w} \in \ker i_E$. Then by Theorem 5, $\bar{\alpha} = \{a\} \cdot \bar{c}$ for $c \in K_{n-1}F$. Since $\{a, a\} = 0$ we see that $\{a\} \cdot \bar{\alpha} = 0$. But then $\bar{w} \in \operatorname{ann}\{a, \xi_p\}$ and so $\bar{w} = 0$.

For $\gamma \in K_nE$, let $l(\gamma)$ denote the dimension of the cyclic $\mathsf{F}_p[G]$-submodule $\langle\bar{\gamma}\rangle$ of k_nE generated by $\bar{\gamma}$. Then we have

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

We denote by N the map $(\sigma - 1)^{p-1}$ on k_nE. Because $(\sigma - 1)^{p-1} = 1 + \sigma + \cdots + \sigma^{p-1}$ in $\mathsf{F}_p[G]$, we may use $i_E N_{E/F}$ and N interchangeably on k_nE.

Lemma 3. *Suppose $p > 2$ and $\gamma \in K_nE$.*

(1) *If $3 \leq l(\gamma) \leq p$, then there exists $\alpha \in K_nE$ such that*
$$\langle N\bar{\alpha}\rangle = \langle\bar{\gamma}\rangle^G.$$
(2) *If $l(\gamma) = 2$ and*
$$\bar{\gamma} \notin \{A\} \cdot i_E(k_{n-1}F) + (k_nE)^G$$
then there exist $\alpha \in K_nE$ and $b \in K_{n-1}F$ such that
$$\langle N\bar{\alpha}\rangle = \langle\bar{\gamma} + \{A\} \cdot i_E(\bar{b})\rangle^G.$$

Proof. Let $l = l(\gamma)$ and suppose $3 \leq l \leq i \leq p$. We show by induction on i that there exists $\alpha_i \in K_nE$ 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 that 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 $i < p$, $i_E\bar{c} = 0$. By Theorem 5, $\bar{c} = \{a\} \cdot \bar{b}$ for $b \in K_{n-1}F$. Equivalently, $c = \{a\} \cdot b + pf$ for $f \in K_nF$. Then

$$N_{E/F}\big(\alpha_i - (\{A\} \cdot i_E(b) + i_E(f))\big) = 0.$$

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

$$(\sigma - 1)\omega = \alpha_i - (\{A\} \cdot i_E(b) + i_E(f)).$$

Then $(\sigma - 1)^2\omega = (\sigma - 1)\alpha_i - \{\xi_p\} \cdot i_E(b)$. Since $i \geq 3$, $\langle(\sigma - 1)^i\bar{\omega}\rangle = \langle\bar{\gamma}\rangle^G$ and we can set $\alpha_{i+1} = \omega$.

For the second part, suppose $l = 2 = i$. Proceeding in the same way as above, we see that for $\alpha_2 = \gamma$ we have $N_{E/F}\alpha_2 = \{a\} \cdot b + pf$ for $b \in K_{n-1}F$ and $f \in K_nF$. As before, there exists $\omega \in K_nE$ such that $(\sigma - 1)\omega = \alpha_2 - (\{A\} \cdot i_E(b) + i_E(f))$. Then

$$(\sigma - 1)^2\omega = (\sigma - 1)(\alpha_2 - \{A\} \cdot i_E(b)) = (\sigma - 1)(\gamma - \{A\} \cdot i_E(b)).$$

Observe that $\bar{\gamma} - \{A\} \cdot i_E(\bar{b}) \notin (k_nE)^G$ by hypothesis. Therefore $l(\gamma - \{A\} \cdot i_E(b)) = 2$ and we can set $\alpha_3 := \omega$. We may then continue by induction on i as above, concluding that there exists an element $\alpha = \alpha_p \in K_nE$ such that $\langle N\bar{\alpha}_p\rangle = \langle(\sigma - 1)^{p-1}\bar{\alpha}_p\rangle = \langle\bar{\gamma} - \{A\} \cdot i_E(\bar{b})\rangle^G$, as required.

In the following lemma we elongate the exact sequence of Theorem 5.

Lemma 4. *The following sequence is exact:*

$$0 \to \operatorname{ann}\{a\} \to k_{n-1}F \xrightarrow{\{a\}\cdot -} k_nF \xrightarrow{i_E} (k_nE)^G \xrightarrow{N_{E/F}} \{a\}\cdot\operatorname{ann}\{a, \xi_p\} \to 0.$$

Here the map $\operatorname{ann}\{a\} \to k_{n-1}F$ *is the natural inclusion.*

Proof. We show first that $N_{E/F}((k_nE)^G) \subset \{a\} \cdot \operatorname{ann}\{a, \xi_p\}$. Let $\bar{\alpha} \in (k_nE)^G$ and $\beta = N_{E/F}\alpha$. Since $i_E(N_{E/F}\bar{\alpha}) = (\sigma - 1)^{p-1}\bar{\alpha} = 0$ we have that $\bar{\beta} = N_{E/F}\bar{\alpha} = \{a\} \cdot \bar{b}$ for some $b \in K_{n-1}F$ by Theorem 5.

Suppose $p = 2$. Since $\bar{\beta}$ is in the image of $N_{E/F}$, we have by Theorem 5 that $\{a\} \cdot \bar{\beta} = \{a, a\} \cdot \bar{b} = 0$. Since $\{a, a\} = \{a, -1\}$, we have $\bar{b} \in \operatorname{ann}\{a, -1\}$.

Now suppose that $p > 2$. Write $\beta = \{a\} \cdot b + pf$ for some $f \in K_nF$. Then by the projection formula

$$N_{E/F}\big(\alpha - (\{A\} \cdot i_E(b) + i_E(f))\big) = 0.$$

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

$$(\sigma - 1)\omega = \alpha - (\{A\} \cdot i_E(b) - i_E(f)).$$

Then $(\sigma - 1)^2\bar{\omega} = \{\xi_p\} \cdot i_E(\bar{b})$.

If $(\sigma - 1)^2\bar{\omega} = 0$ then since by Theorem 5, $\ker i_E = \{a\} \cdot k_{n-1}F$,

$$\{\xi_p\} \cdot \bar{b} = \{a\} \cdot \bar{h}$$

for some $h \in K_{n-1}F$. Because $\{a, a\} = 0$, the right-hand side of the preceding equation is annihilated by $\{a\}$. Therefore $\bar{b} \in \operatorname{ann}\{a, \xi_p\}$.

If $(\sigma-1)^2\bar{\omega} \neq 0$ then $l(\omega)=3$ and Lemma 3 shows that

$$i_E(\{\xi_p\}\cdot\bar{b}) = cN\bar{\lambda} = i_E(N_{E/F}(\overline{c\lambda}))$$

for some $\lambda \in K_nE$ and $c \in \mathsf{Z}$. Since by Theorem 5, $\ker i_E = \{a\}\cdot k_{n-1}F$ we have

$$\{\xi_p\}\cdot\bar{b} = N_{E/F}(\overline{c\lambda}) + \{a\}\cdot\bar{h}$$

for some $h \in K_{n-1}F$. Now by Theorem 5 and the fact that $\{a,a\}=0$, the right-hand side of the preceding equation is annihilated by $\{a\}$. Then $\bar{b} \in \operatorname{ann}\{a,\xi_p\}$. Hence in all cases $N_{E/F}\bar{\alpha} \in \{a\}\cdot\operatorname{ann}\{a,\xi_p\}$.

Exactness at the first two terms is obvious, and exactness at the third term follows from Theorem 5.

For exactness at the fourth term, suppose

$$\bar{\gamma} \in (k_nE)^G \text{ and } N_{E/F}\bar{\gamma} = 0.$$

Then $N_{E/F}\gamma = pf$ for $f \in K_nF$. Let $\beta = \gamma - i_E(f)$. Then $N_{E/F}\beta = 0$ and by Theorem 3 there exists $\alpha \in K_nE$ such that $(\sigma-1)\alpha = \beta$. If $p=2$ then $\bar{\beta} = i_E(N_{E/F}\bar{\alpha}) \in i_Ek_nF$ and we are done. Thus assume $p>2$.

Now suppose $\bar{\alpha} \in \{A\}\cdot i_E(k_{n-1}F) + (k_nE)^G$. Then

$$\bar{\beta} = (\sigma-1)\bar{\alpha} \in \{\xi_p\}\cdot i_E(k_{n-1}F) \subset i_E(k_nF),$$

and hence $\bar{\gamma} = \bar{\beta} + i_E(\bar{f}) \in i_E(k_nF)$ as well. Otherwise $\bar{\alpha} \notin \{A\}\cdot i_E(k_{n-1}F) + (k_nE)^G$. Now if $(\sigma-1)\bar{\alpha} = \bar{\beta} = 0$ we are done as then $\bar{\gamma} = i_E(\bar{f})$. Hence assume $(\sigma-1)\bar{\alpha} \neq 0$. Then $l(\alpha)=2$ and by Lemma 3 we see that there exist $\delta \in K_nE, b \in K_{n-1}F$ and $c \in \mathsf{Z}$ such that

$$cN\bar{\delta} = (\sigma-1)(\bar{\alpha} + \{A\}\cdot i_E(\bar{b})) = \bar{\beta} + \{\xi_p\}\cdot i_E(\bar{b}).$$

Thus $\bar{\beta} = cN\bar{\delta} - \{\xi_p\}\cdot i_E(\bar{b}) \in i_E(k_nF)$ and exactness at the fourth term is established.

Finally we show the exactness at the fifth term. Since

$$\{a\}\cdot\operatorname{ann}\{a,\xi_p\} = \{a\}\cdot V$$

it is enough to show that each element $\{a\}\cdot\bar{v}$ where $\bar{v} \in V$ can be written as $N_{E/F}\bar{\alpha}$ for some $\bar{\alpha} \in (k_nE)^G$. Observe that $(\sigma-1)(\{A\}\cdot i_E\bar{v}) = \{\xi_p\}\cdot i_E(\bar{v})$. Also we have

$$N_{E/F}(\{A\}\cdot i_E(\bar{v})) = \begin{cases} \{a\}\cdot\bar{v} & \text{if } p>2 \\ \{-a\}\cdot\bar{v} & \text{if } p=2. \end{cases}$$

Therefore it is enough to show that there exists an element $\bar{\gamma} \in k_n E$ such that $(\sigma - 1)\bar{\gamma} = \{\xi_p\} \cdot i_E(\bar{v})$ and

$$N_{E/F}\bar{\gamma} = \begin{cases} 0 & \text{if } p > 2 \\ \{-1\} \cdot \bar{v} & \text{if } p = 2. \end{cases}$$

Indeed then we can set $\bar{\alpha} = \{A\} \cdot i_E(\bar{v}) - \bar{\gamma}$.

Because $\bar{v} \in \operatorname{ann}\{a, \xi_p\}$ we see that $\{\xi_p\} \cdot i_E(\bar{v}) \in \operatorname{ann}\{a\}$. By Theorem 5 there exists $\bar{\beta} \in k_n E$ such that

$$\{\xi_p\} \cdot \bar{v} = N_{E/F}\bar{\beta} \text{ and } i_E(N_{E/F}\bar{\beta}) = (\sigma - 1)^{p-1}\bar{\beta}.$$

Then setting $\bar{\gamma} = (\sigma - 1)^{p-2}\bar{\beta}$ we obtain our required element. The proof of our lemma has now been completed.

Finally, we need a general lemma about $\mathsf{F}_p[G]$-modules.

Lemma 5 (Exclusion Lemma)**.** *Let M_1 and M_2 be $\mathsf{F}_p[G]$-modules contained in a common $\mathsf{F}_p[G]$-module. Suppose that $M_1^G \cap M_2^G = \{0\}$. Then $M_1 + M_2 = M_1 \oplus M_2$.*

Proof. Let $M = M_1 \cap M_2$ and suppose that $m \in M \setminus \{0\}$. Let

$$\tilde{m} = (\sigma - 1)^{l(m)-1}(m) \neq 0.$$

Then $\tilde{m} \in M_1^G \cap M_2^G$, a contradiction. Hence $M_1 \cap M_2 = \{0\}$ and $M_1 + M_2 = M_1 \oplus M_2$.

3. Construction of Submodules

Proposition 1. *$k_n E$ contains a submodule X_1 such that*

- *X_1 is a trivial $\mathsf{F}_p[G]$-module of dimension Υ_1*
- *$X_1 \cap i_E k_n F = \{0\}$*
- *$N_{E/F}$ restricts to an isomorphism $X_1 \to \{a\} \cdot V$.*

Moreover, if $p > 2$, then $k_n E$ contains a submodule X_2, independent of X_1, such that

- *X_2 is a direct sum of Υ_2 cyclic submodules of dimension 2 and $\dim_{\mathsf{F}_p} X_2^G = \Upsilon_2$.*
- *$(X_1 + X_2) \cap i_E k_n F = (\sigma - 1)X_2 = X_2^G = i_E(\{\xi_p\} \cdot W)$*

- *We have an exact sequence*

$$0 \to \{\xi_p\} \cdot W \xrightarrow{i_E} X_1 + X_2 \xrightarrow{N_{E/F}} \{a\} \cdot k_{n-1}F \to 0$$

Proof. Let $\mathcal{I}$ be an F_p-basis for V. Let $\bar{v}$ be an arbitrary element of $\mathcal{I}$, and consider $\bar{\alpha} = \{A\} \cdot i_E\bar{v}$. Now $(\sigma - 1)\bar{\alpha} = i_E(\{\xi_p\} \cdot \bar{v})$.

Since $\bar{v} \in \operatorname{ann}\{a, \xi_p\}$ we see that $\{\xi_p\} \cdot \bar{v} \in \operatorname{ann}_{k_nF}\{a\}$. By Theorem 5

$$\{\xi_p\} \cdot \bar{v} = N_{E/F}\bar{\beta} \text{ and } i_E(N_{E/F}\bar{\beta}) = N\bar{\beta} = (\sigma - 1)^{p-1}\bar{\beta}$$

for some $\beta \in K_nE$. Set $\gamma = (\sigma - 1)^{p-2}\beta$ and $\bar{x}_v = \bar{\alpha} - \bar{\gamma} \in k_nE$.

If $p = 2$ then

$$N_{E/F}\bar{x}_v = \{-a\} \cdot \bar{v} - N_{E/F}\bar{\gamma} = \{-a\} \cdot \bar{v} - \{-1\} \cdot \bar{v} = \{a\} \cdot \bar{v}.$$

If $p > 2$, then observe that since γ is in the image of $\sigma - 1$ we have $\overline{N_{E/F}\gamma} = 0$. Then, by the projection formula

$$N_{E/F}\bar{x}_v = \{a\} \cdot \bar{v} - \overline{N_{E/F}\gamma} = \{a\} \cdot \bar{v}.$$

Now in either case, since $(\sigma - 1)^{p-1}\bar{\beta} = i_E(N_{E/F}\bar{\beta})$,

$$(\sigma - 1)\bar{x}_v = i_E(\{\xi_p\} \cdot \bar{v}) - (\sigma - 1)^{p-1}\bar{\beta} = i_E(\{\xi_p\} \cdot \bar{v}) - i_E(\{\xi_p\} \cdot \bar{v}) = 0.$$

Set

$$X_1 := \oplus_{\bar{v} \in \mathcal{I}}\langle \bar{x}_v \rangle.$$

We have shown that X_1 is a trivial $\mathsf{F}_p[G]$-module. Moreover, because $N_{E/F}\bar{x}_v = \{a\} \cdot \bar{v}$ and $\{a\} \cdot -$ is injective on V by Lemma 2,

$$N_{E/F}\big|_{X_1} : X_1 \to \{a\} \cdot V$$

takes a basis of X_1 to a basis of $\{a\} \cdot V$ and $\dim_{\mathsf{F}_p} X_1 = \dim_{\mathsf{F}_p} V = \Upsilon_1$. Finally, since $N_{E/F}$ is trivial on $i_E k_n F$, we have $X_1 \cap i_E k_n F = \{0\}$.

Now suppose that $p > 2$. Set

$$X_2 := (\{A\} \cdot i_E W) + i_E(\{\xi_p\} \cdot W).$$

Let $\bar{w} \in W$ and consider $\bar{x}_w = \{A\} \cdot i_E(\bar{w})$.

Since $(\sigma - 1)\bar{x}_w = i_E(\{\xi_p\} \cdot \bar{w})$ and $(\sigma - 1)(\{\xi_p\} \cdot \bar{w}) = 0$, we obtain $(\sigma - 1)X_2 = i_E(\{\xi_p\} \cdot W)$. Hence on $\{A\} \cdot i_E W$, $\sigma - 1$ acts as $i_E(\{\xi_p\} \cdot -)$, which by Lemma 2 is an isomorphism of vector spaces. Hence $\sigma - 1$ is an isomorphism as well. Moreover, if an arbitrary $\{A\} \cdot i_E(\bar{w}_1) + \{\xi_p\} \cdot i_E(\bar{w}_2) \in X_2$ lies in the kernel of $\sigma - 1$, $\bar{w}_1 = 0$. Hence $X_2^G = i_E(\{\xi_p\} \cdot$

W). Since we already observed that $X_1 \cap i_E k_n F = \{0\}$ we see that $X_2^G \cap X_1 = \{0\}$ and by Lemma 5 we conclude that $X_1 + X_2 = X_1 \oplus X_2$.

By the projection formula $N_{E/F}\bar{x}_w = \{a\} \cdot \bar{w}$ and by the definition of W, $\{a\} \cdot \bar{w} = 0$ implies $\bar{w} = 0$. Since $N_{E/F}(\{\xi_p\} \cdot i_E(\bar{w}_2)) = 0$ for all $\bar{w}_2 \in W$, we deduce that restricted to X_2, $N_{E/F}$ surjects X_2 onto $\{a\} \cdot W$ with kernel $i_E(\{\xi_p\} \cdot W)$. By Lemma 2, $\{a\} \cdot k_{n-1}F = \{a\} \cdot (V + W)$; hence on $X_1 \oplus X_2$, $N_{E/F}$ is a surjection onto $\{a\} \cdot k_{n-1}F$ with kernel $i_E(\{\xi_p\} \cdot W)$.

Finally observe that $N_{E/F} i_E k_n F = \{0\}$. Hence
$$(X_1 + X_2) \cap i_E k_n F \subset i_E(\{\xi_p\} \cdot W).$$
Since $i_E(\{\xi_p\} \cdot W) \subset i_E k_n F$, we have equality.

Now we have shown that $\sigma - 1$ is an isomorphism of vector spaces $\{A\} \cdot i_E W \to i_E(\{\xi_p\} \cdot W)$, and by Lemma 2, we have an isomorphism $W \to i_E(\{\xi_p\} \cdot W)$. Therefore X_2 is a direct sum of cyclic submodules $\langle \bar{x}_w \rangle$ of dimension 2, with $\bar{x}_w$ in one-to-one correspondence with basis elements of W. Hence the direct sum contains Υ_2 cyclic summands.

If $p = 2$, let $X = X_1$ be a submodule of $k_n E$ satisfying the conditions of the preceding proposition. If $p > 2$, let $X = X_1 + X_2$ for X_1, X_2 satisfying the conditions of the same.

Proposition 2. *$k_n E$ contains a submodule Y independent from X such that*

- *Y is a free $\mathsf{F}_p[G]$-module of rank*
$$y = \begin{cases} \dim_{\mathsf{F}_p}(N_{E/F} k_n E)/\{a\} \cdot k_{n-1}F, & p > 2 \\ \dim_{\mathsf{F}_2}(N_{E/F} k_n E)/\{a\} \cdot \mathrm{ann}_{k_{n-1}F}\{a, -1\}, & p = 2 \end{cases}$$
- $Y^G = i_E N_{E/F} k_n E$
- *if* $p > 2$, $\Upsilon_1 + \Upsilon_2 + y = e$
- *if* $p = 2$, $\Upsilon_1 + y = e$

Proof. Let $\mathcal{I}$ be a basis for the subspace $i_E(N_{E/F} k_n E)$. For each basis element $\bar{y} \in \mathcal{I}$, let $\alpha_y \in K_n E$ 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 $\mathsf{F}_p[G]$, 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
$$Y = \sum_{\bar{y} \in \mathcal{I}} \langle \bar{\alpha}_y \rangle.$$

By Lemma 5, $Y = \oplus_{\bar{y}\in\mathcal{I}}\langle\bar{\alpha}_y\rangle$ and so Y is a free $\mathsf{F}_p[G]$-module. Moreover,

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

Now the rank of Y is equal to the dimension of $i_E(N_{E/F}k_nE)$, or

$$\dim_{\mathsf{F}_p}(N_{E/F}k_nE)/\left((N_{E/F}k_nE)\cap\ker i_E\right).$$

Now by Theorem 5, $N_{E/F}(k_nE) = \operatorname{ann}\{a\}$, and by the same Theorem, $\ker i_E = \{a\}\cdot k_{n-1}F$. Hence

$$N_{E/F}(k_nE)\cap\ker i_E = \operatorname{ann}_{k_nF}\{a\}\cap\{a\}\cdot k_{n-1}F.$$

Suppose that $p=2$. Since $\{a,a\}=\{a,-1\}$ we deduce that

$$N_{E/F}(k_nE)\cap\ker i_E = \{a\}\cdot\operatorname{ann}\{a,-1\}.$$

The dimension of this subspace is equal to $\dim_{\mathsf{F}_p}\operatorname{ann}\{a,-1\}/\operatorname{ann}\{a\}$, or Υ_1.

Now suppose that $p>2$. Since $\{a,a\}=0$, $\{a\}\cdot k_{n-1}F\subset\operatorname{ann}\{a\}$ and we deduce that

$$N_{E/F}(k_nE)\cap\ker i_E = \{a\}\cdot k_{n-1}F,$$

which is of dimension $\dim_{\mathsf{F}_p}(k_{n-1}F)/\operatorname{ann}\{a\}$, or $\Upsilon_1+\Upsilon_2$.

As $e=\dim_{\mathsf{F}_p}N_{E/F}k_nE$, we deduce that if $p=2$ then $\Upsilon_1+\operatorname{rank}Y=e$ and if $p>2$, $\Upsilon_1+\Upsilon_2+\operatorname{rank}Y=e$.

Now we claim that Y is independent from X. Suppose $\bar{\beta}\in X^G\cap Y^G$. Now $Y^G=i_E(N_{E/F}k_nE)\subset i_E(k_nF)$, so $\bar{\beta}=i_E(\bar{\alpha})$ where $\bar{\alpha}=N_{E/F}\bar{\gamma}$ for $\gamma\in K_nE$. If $p=2$ then by Proposition 1, $i_E(k_nF)\cap X=\{0\}$, and so $X\cap Y=\{0\}$ by Lemma 5.

If $p>2$, Proposition 1 tells us that

$$i_E(k_nF)\cap X = X_2^G = \{\xi_p\}\cdot i_EW.$$

Hence $\bar{\beta}=\{\xi_p\}\cdot i_E(\bar{w})$ for $\bar{w}\in W$. Since $i_E(\{\xi_p\}\cdot\bar{w})=i_E(\bar{\alpha})$ and by Theorem 5, $\ker i_E=\{a\}\cdot k_{n-1}F$,

$$\{\xi_p\}\cdot\bar{w} = \bar{\alpha}+(\{a\}\cdot\bar{f}) \tag{1}$$

for $f\in K_{n-1}F$. Now because $\bar{\alpha}\in N_{E/F}k_nE$, by Theorem 5, $\{a\}\cdot\bar{\alpha}=0$. Moreover, $\{a,a\}=0$ since we have assumed that $p>2$. Hence the right-hand side of (1) is annihilated by multiplication by $\{a\}$. Therefore $\bar{w}\in\operatorname{ann}\{a,\xi_p\}$, and by the definition of W, $\bar{w}=0$. By Lemma 5, $X+Y=X\oplus Y$.

Now let X and Y be submodules satisfying the conditions of the preceding propositions.

Proposition 3. *k_nE contains a submodule Z independent from $X+Y$ such that*

- *Z is a trivial $\mathsf{F}_p[G]$-module of dimension*

$$z = \begin{cases} \dim_{\mathsf{F}_p}(k_nF)/(\{\xi_p\}\cdot W + N_{E/F}k_nE), & p>2 \\ \dim_{\mathsf{F}_2}(k_nF)/(\{a\}\cdot k_{n-1}F + N_{E/F}k_nE), & p=2 \end{cases}$$

- $(k_nE)^G = X^G + Y^G + Z$
- $\Upsilon_2 + z = d$

Proof. Let Z be a complement of $(X^G+Y^G)\cap i_E(k_nF)$ in $i_E(k_nF)$. By Lemma 5, $(X+Y)+Z = (X+Y)\oplus Z$.

Clearly $X^G+Y^G+Z \subset (k_nE)^G$. Now suppose $\bar\alpha \in (k_nE)^G$ and let $\beta = N_{E/F}\alpha$. By Lemma 4, $\bar\beta = \{a\}\cdot\bar b$ for some $\bar b \in \operatorname{ann}\{a,\xi_p\}$.

Let $\bar v \in V$ be the component of $\bar b$ in the decomposition $\operatorname{ann}\{a\}\oplus V$ of $\operatorname{ann}\{a,\xi_p\}$. By Proposition 1, there exists $\bar\gamma \in X_1 \subset X^G$ such that

$$N_{E/F}\bar\gamma = \{a\}\cdot\bar v = \{a\}\cdot\bar b = \bar\beta.$$

Then $N_{E/F}(\bar\alpha-\bar\gamma) = 0$. By Lemma 4, $\bar\alpha-\bar\gamma \in i_E(k_nF)$. But $i_E(k_nF) \subset X^G+Y^G+Z$. Hence $\bar\alpha \in X^G+Y^G+Z$ and we have shown that $(k_nE)^G = X^G+Y^G+Z$.

For the dimension of Z, assume first that $p>2$. By Theorem 5, $N_{E/F}k_nE = \operatorname{ann}_{k_nF}\{a\}$ and $\ker i_E = \{a\}\cdot k_{n-1}F$. Since $\{a,a\}=0$ we see that $\ker i_E \subset N_{E/F}k_nE$. Hence

$$d = \dim_{\mathsf{F}_p}\frac{k_nF}{N_{E/F}k_nE} = \dim_{\mathsf{F}_p}\frac{i_E(k_nF)}{i_E(N_{E/F}k_nE)} = \dim_{\mathsf{F}_p}\frac{i_E(k_nF)}{Y^G},$$

where in the last equation we use Proposition 2 to identify Y^G. By Propositions 1 and 2, $(X^G+Y^G)\cap i_E(k_nF) = X_2^G \oplus Y^G$. Hence $d = \dim_{\mathsf{F}_p}(X_2^G\oplus Y^G\oplus Z)/Y^G$. By Proposition 1, $\dim_{\mathsf{F}_p} X_2^G = \Upsilon_2$. Hence $\Upsilon_2 + \dim_{\mathsf{F}_p} Z = d$ for $p>2$. Also we see that

$$\dim_{\mathsf{F}_p} Z = \dim_{\mathsf{F}_p}\frac{i_E(k_nF)}{X_2^G\oplus Y^G} = \dim_{\mathsf{F}_p}\frac{k_nF}{\{\xi_p\}\cdot W + N_{E/F}k_nE} = z.$$

Now assume $p = 2$. By Propositions 1 and 2, $i_E(k_nF) \cap (X^G + Y^G) = Y^G$. Proceeding as in the last case,

$$\begin{aligned}\dim_{\mathsf{F}_2} Z = \dim_{\mathsf{F}_2} \frac{i_E(k_nF)}{Y^G} &= \dim_{\mathsf{F}_2} \frac{i_E(k_nF)}{i_E(N_{E/F}k_nE)} \\ &= \dim_{\mathsf{F}_2} \frac{k_nF}{N_{E/F}k_nE + \ker i_E} \\ &= \dim_{\mathsf{F}_2} \frac{k_nF}{N_{E/F}k_nE + \{a\} \cdot k_{n-1}F} = z,\end{aligned}$$

since $\ker i_E = \{a\} \cdot k_{n-1}F$, by Theorem 5.

We then consider the filtration

$$k_nF \supset \Big((\{a\} \cdot k_{n-1}F) + N_{E/F}k_nE\Big) \supset N_{E/F}k_nE.$$

The dimension of the quotient of the first and third modules is, by definition, d. By Theorem 5, $N_{E/F}k_nE = \operatorname{ann}_{k_nF}\{a\}$. Since $\{a, a\} = \{a, -1\}$ we see that

$$(\{a\} \cdot k_{n-1}F) \cap N_{E/F}k_nE = \{a\} \cdot V.$$

Hence

$$\dim_{\mathsf{F}_2} \frac{(\{a\} \cdot k_{n-1}F) + N_{E/F}k_nE}{N_{E/F}k_nE} = \dim_{\mathsf{F}_2} \frac{\{a\} \cdot k_{n-1}F}{\{a\} \cdot V} = \dim_{\mathsf{F}_2}\{a\} \cdot W.$$

By Lemma 2, $\dim_{\mathsf{F}_2}\{a\} \cdot W = \dim_{\mathsf{F}_2} W = \Upsilon_2$. Hence $\Upsilon_2 + \dim_{\mathsf{F}_2} Z = d$ for $p = 2$ as well.

4. Proofs of Theorems 1 and 2

Proof of Theorem 1. By Propositions 1, 2, and 3, there exist independent submodules $X = X_1 + X_2$, Y, and Z satisfying the conditions of the theorem. All that remains is to show that $k_nE = X + Y + Z$.

We proceed by induction on the length $l(\gamma)$ of the cyclic submodule $\langle\bar{\gamma}\rangle$ of k_nE generated by an arbitrary element $\bar{\gamma} \in k_nE$. If $l(\gamma) = 1$, then by Proposition 3, $\bar{\gamma} \in X^G + Y^G + Z$. Assume then that $\bar{\beta} \in X + Y + Z$ if $l(\beta) \leq i < p$ and that $l(\gamma) = i + 1$.

Suppose first that $l(\gamma) = 2$ and

$$\bar{\gamma} \in \{A\} \cdot i_E(k_{n-1}F) + (k_nE)^G.$$

Then $(\sigma - 1)\bar{\gamma} = i_E(\{\xi_p\} \cdot \bar{b})$ for some $b \in K_{n-1}F$. In the decomposition $\operatorname{ann}\{a, \xi_p\} \oplus W$ of $k_{n-1}F$, write $\bar{b} = \bar{f} + \bar{w}$. By Proposition 1 there exists

$\bar{\omega} \in X_2$ such that $(\sigma-1)\bar{\omega} = i_E(\{\xi_p\}\cdot\bar{w})$. We also have $\{\xi_p\}\cdot\bar{f} \in \operatorname{ann}\{a\}$ and therefore by Theorem 5 and Proposition 2 there exists $\bar{y} \in Y$ such that $i_E(\{\xi_p\}\cdot\bar{f}) = i_E(N_{E/F}(\bar{y}))$. Hence there exists $\overline{y'} \in Y$ such that $(\sigma-1)\bar{\gamma} = (\sigma-1)\bar{\omega} + (\sigma-1)\overline{y'}$. Hence $l(\gamma - \omega - y') \le 1$ and by the inductive hypothesis $\bar{\gamma} \in X + Y + Z$.

Now since by the preceding arguments $\{A\}\cdot i_E(k_{n-1}F) \subset X+Y+Z$, in order to show that an arbitrary $\bar{\gamma}$ with $l(\gamma) = 2$ lies in $X+Y+Z$ it is enough to show that $\bar{\gamma} + \{A\}\cdot i_E(\bar{b}) \in X+Y+Z$ for any $b \in K_{n-1}F$.

Suppose then that $l(\gamma) = 2$ and

$$\bar{\gamma} \notin \{A\}\cdot i_E(k_{n-1}F) + (k_nE)^G.$$

Then, by Lemma 3, there exist $b \in K_nF$ and $\alpha \in K_nE$ such that $\bar{\beta} = \bar{\gamma} + \{A\}\cdot i_E(\bar{b})$ satisfies $l(\bar{\beta}) \le 2$ and $\langle\bar{\beta}\rangle^G = \langle N\bar{\alpha}\rangle$. Hence $(\sigma-1)^{l(\beta)-1}\bar{\beta} = cN\bar{\alpha}$ for some $c \in \mathsf{Z}$. But $cN\bar{\alpha} = i_EN_{E/F}(\overline{c\alpha}) \in Y^G$, by Proposition 2. Hence there exists $\bar{\omega} \in Y$ such that $(\sigma-1)^{p-1}\bar{\omega} = cN\bar{\alpha}$. Now $\bar{\lambda} = (\sigma-1)^{p-l(\beta)}\bar{\omega} \in Y$ and $(\sigma-1)^{l(\beta)-1}(\bar{\beta}-\bar{\lambda}) = 0$. Hence $l(\beta-\lambda) < l(\gamma)$ and by the inductive hypothesis $\bar{\beta}$ and hence $\bar{\gamma}$ lie in $X+Y+Z$.

If $l(\gamma) \ge 3$ then the same argument works again. By Lemma 3 $\langle\bar{\gamma}\rangle^G = \langle N\bar{\alpha}\rangle$ and so $(\sigma-1)^{l(\gamma)-1}\bar{\gamma} = cN\bar{\alpha}$ for some $c \in \mathsf{Z}$. But $cN\bar{\alpha} = i_EN_{E/F}(c\bar{\alpha}) \in Y^G$, by Proposition 2. Hence there exists $\bar{\omega} \in Y$ such that $(\sigma-1)^{p-1}\bar{\omega} = cN\bar{\alpha}$. Now $\bar{\lambda} = (\sigma-1)^{p-l(\gamma)}\bar{\omega} \in Y$ and $(\sigma-1)^{l(\gamma)-1}(\bar{\gamma}-\bar{\lambda}) = 0$. Hence $l(\gamma-\lambda) < l(\gamma)$ and by the inductive hypothesis $\bar{\gamma} \in X+Y+Z$.

Proof of Theorem 2. By Propositions 1, 2, and 3, there exist independent submodules $X = X_1$, Y, and Z satisfying the conditions of the theorem. All that remains is to show that $k_nE = X+Y+Z$.

Let $\bar{\gamma} \in k_nE$ be arbitrary. If $l(\gamma) = 1$, then by Proposition 3, $\bar{\gamma} \in X^G + Y^G + Z$. Otherwise $(\sigma-1)\bar{\gamma} = (\sigma+1)\bar{\gamma} = i_EN_{E/F}\bar{\gamma} \in Y^G$, by Proposition 2. Hence there exists $\bar{\omega} \in Y$ such that $(\sigma-1)\bar{\omega} = (\sigma-1)\bar{\gamma}$. Therefore $l(\gamma-\omega) < 2$ and by the inductive hypothesis $\bar{\gamma} \in X+Y+Z$.

5. Proof of Theorem 5

For the case $p = 2$ we have the long exact sequence of Galois cohomology groups due to Arason [A, Satz 4.5]. Suppose then that $p > 2$

and F is perfect. Let S be any p-Sylow subgroup of $G_F = \mathrm{Gal}(F_{\mathrm{sep}}/F)$, and set L to be the fixed field of S. Because F is perfect, the separable closure F_{sep} is identical to the algebraic closure $\bar{F}$, and hence each finite extension of L has degree a power of p. In particular, all of the hypotheses of Theorem 4 are valid for the field L in place of F. Furthermore, $([L : F], p) = 1$. (Here we use basic properties of supernatural numbers and Sylow p-subgroups. See [Se, Chapter 1].) Therefore if $E = F(\sqrt[p]{a})$ is a cyclic extension of F of degree p, so is $EL = L(\sqrt[p]{a})$ over L. By Theorem 4 we see that the sequence

$$k_{m-1}EL \xrightarrow{N_{EL/L}} k_{m-1}L \xrightarrow{\{a\}\cdot -} k_mL \xrightarrow{i_{EL}} k_mEL$$

is exact for each $m \in \mathbb{N}$.

We claim that $i_L \colon k_mF \to k_mL$ is injective. Indeed, suppose that $i_L(\alpha) = 0$ for some $\alpha \in k_mF$. Then there exists a finite subextension M/F of L/F such that $i_M(\alpha) = 0$. Then

$$0 = N_{M/F}(i_M(\alpha)) = [M : F]\alpha,$$

(see [FV, p. 300]). Because $[M : F]$ is coprime with p, we see that $\alpha = 0$ and i_L is injective as asserted. Similarly we have that $i_{EL} \colon k_mE \to k_mEL$ is injective.

We then have the following commutative diagram:

$$\begin{array}{ccccccc}
k_{m-1}EL & \xrightarrow{N_{EL/L}} & k_{m-1}L & \xrightarrow{\{a\}\cdot -} & k_mL & \xrightarrow{i_{LE}} & k_mEL \\
\uparrow{\scriptstyle i_{EL}} & & \uparrow{\scriptstyle i_L} & & \uparrow{\scriptstyle i_L} & & \uparrow{\scriptstyle i_{EL}} \\
k_{m-1}E & \xrightarrow{N_{E/L}} & k_{m-1}F & \xrightarrow{\{a\}\cdot -} & k_mF & \xrightarrow{i_E} & k_mE
\end{array}$$

Because the vertical maps are injective, we see that the bottom row of the diagram is a complex: the composition of any two consecutive maps is the zero map. We now establish exactness at the second and third terms of the complex.

Let $\alpha \in k_{m-1}F$ such that $\{a\} \cdot \alpha = 0$. Then $\{a\} \cdot i_L(\alpha) = 0$ and therefore there exists an element $\beta \in k_{m-1}EL$ such that $N_{EL/L}(\beta) = i_L(\alpha)$. Let M/F be a finite extension such that β is defined over EM. Then $N_{EM/M}(\beta) = i_M(\alpha)$, and we have

$$N_{EM/F}(\beta) = N_{M/F}(N_{EM/M}(\beta)) = N_{M/F}(i_M(\alpha)) = [M : F]\alpha$$

and $N_{EM/F}(\beta) = N_{E/F}(N_{EM/E}(\beta))$. Thus

$$N_{E/F}(N_{EM/E}(\beta)) = [M : F]\alpha.$$

Because $([M:F],p)=1$ we see that $\alpha \in N_{E/F}(k_{m-1}E)$. Therefore we have established the exactness of our complex at $k_{m-1}F$.

Now assume that $\alpha \in k_mF$ such that $i_E(\alpha) = 0 \in k_mE$. Then arguing as above, we see that there exist a finite extension M/F and $\beta \in k_{m-1}M$ such that

$$\{a\} \cdot \beta = i_M(\alpha) \in k_mM.$$

Applying $N_{M/F}$ and using the projection formula we see that

$$\{a\} \cdot N_{M/F}(\beta) = N_{M/F}(i_M(\alpha)) = [M:F]\alpha.$$

Because $[M:F]$ is coprime with p, $\alpha \in \{a\} \cdot N_{M/F}(\gamma)$ for a suitable element $\gamma \in k_{m-1}M$. Hence we see that our complex is also exact at k_mF and the full complex is exact.

Remark. Assuming as usual that F contains a primitive root ξ_p, then if $m \leq 2$, no further assumption on F in Theorem 5 is necessary. For $m=1$ this claim follows from basic Kummer theory, and for $m=2$ see [Me, Prop. 5] and [Sr, Chap. 5, Lemma 8.4].

6. Reduction to the Case char $F = 0$

Suppose now that char $F = q > 0$ and $q \neq p$. We also assume that F is infinite, because if F is finite then $K_nF = 0$ for $n \geq 2$ and therefore this is a trivial case. (See [FV, Prop. IX.1.3].) Assume as before that F contains a primitive pth root of unity ξ_p and E/F is a cyclic extension of degree p. We shall show that there exists an explicitly defined cyclic extension J/L of degree p such that char $L = 0$, so that L is perfect, and k_nJ is naturally isomorphic with k_nE as a $G = \mathrm{Gal}(E/F) \cong \mathrm{Gal}(J/L)$ module.

Recall first that there exists a discrete valuation ring A of characteristic 0 such that its maximal ideal M is generated by q and $A/M \cong F$. (Such a ring is called a q-ring. See [Ma, p. 223].) By passing to a completion $\hat{A}$ of A with respect to M-adic topology and observing that $\hat{A}/\hat{M} \cong A/M \cong F$ and $\hat{M} = \hat{A}.q$ we see that we may and will assume that A is a complete local q-ring such that $A/M \cong F$.

It is known that a complete q-ring is uniquely determined up to its isomorphism by its residue field. (See [Ma, Cor., p. 225].) Observe further that a complete discrete valued field is henselian. (See [R, Thm. 5].)

Now following [FW, §IX.3] we have a natural construction

$$R = \varinjlim (A^{(1)} \subset A^{(2)} \subset A^{(3)} \subset \cdots), \text{ where}$$
$$A^{(1)} = A \text{ as above and } A^{(n+1)} := A^{(n)}[t]/(t^p - \pi_n),$$

where π_n is a uniformizer of $A^{(n)}$ for $n \geq 1$. As was noticed in [FW], this ring R is a henselian valuation ring of characteristic 0, with value group the underlying group of the ring $\mathsf{Z}[1/p]$.

For each $i \in \mathsf{N}$ let $L^{(i)}$ be the quotient field of $A^{(i)}$, and let L be the quotient field of R. Then from Lemma IX.3.5 in [FW], there is a natural isomorphism $k_nF \cong k_nL$ for each $n \in \mathsf{N}$.

Let T be the inertia subgroup of $G_{L^{(1)}}$. We have the natural isomorphism $G_{L^{(1)}}/T \xrightarrow{\mathsf{s}} G_F$. Let φ be the compositum of the natural surjections

$$G_{L^{(1)}} \to G_{L^{(1)}}/T \xrightarrow{\mathsf{s}} G_F \to \mathrm{Gal}(E/F),$$

and let $J^{(1)}$ be the fixed field of $\ker\varphi$. Then $\mathrm{Gal}(J^{(1)}/L^{(1)})$ is naturally isomorphic to $\mathrm{Gal}(E/F)$. (This is a special case of a more general construction about lifting certain Galois abelian extensions. See [K, Lemma 2.5].)

Thus we see that $J^{(1)}/L^{(1)}$ is a cyclic, purely inert extension of degree p. Because the tower

$$L^{(1)} \subset L^{(2)} \subset \cdots \subset L^{(n)} \subset \cdots$$

is a chain of totally ramified extensions $L^{(n+1)}/L^{(n)}$, we see that $J^{(1)} \cap L = L^{(1)}$. Set $J := J^{(1)}L$. Then J/L is a cyclic, purely inert extension of degree p.

Now set $J^{(i)} := J^{(1)}L^{(i)}$, and let $B^{(i)}$ be the unique valuation ring in $J^{(i)}$ such that $B^{(i)} \cap L^{(i)} = A^{(i)}$. ($B^{(i)}$ is unique because $A^{(i)}$ is henselian.) Then again following the proofs of Lemma IX.3.2 and Lemma IX.3.5 in [FW], we establish, in exactly the same way we proved that $k_nF \cong k_nL$, that $k_nE \cong k_nJ$ under a G-equivariant isomorphism. Our reduction is complete.

7. Acknowledgements

We are very grateful to M. Rost and to J.-P. Serre for correspondence concerning the Bloch-Kato conjecture. We are also very grateful to J.-P. Tignol for his kind and encouraging remarks concerning this paper.

References

[A] J. Kr. Arason. Cohomologische invarianten quadratischer Formen. *J. Algebra* **36** (1975), 448–491.

[B] Z. I. Borevič. 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*, edited by D. K. Faddeev, 15–30. Providence, RI: American Mathematical Society, 1968.

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

[FW] E. M. Friedlander and C. W. Weibel. An overview of algebraic K-theory. *Algebraic K-theory and its applications (Trieste, 1997)*, edited by H. Bass, A. O. Kuku, and C. Pedrini, 1–119. River Edge, NJ: World Sci. Publishing, 1999.

[K] J. Koenigsmann. Encoding valuations in absolute Galois groups. *Proceedings of the international conference and workshop on Valuation Theory (Saskatoon, 1999)*, edited by F.-V. Kuhlmann, S. Kuhlmann, and M. Marshall, 107–132. Fields Institute Communications 33. Providence, RI: American Mathematical Society, 2003.

[Ma] H. Matsumura. *Commutative ring theory*, 2nd ed. Cambridge Studies in Advanced Mathematics 8. Cambridge: Cambridge University Press, 1989.

[Me] A. S. Merkurjev. K_2 of fields and the Brauer group. *Applications of algebraic K-theory to algebraic geometry and number theory (Boulder, Colo., 1983)*, Part II, 529–546. Contemporary Mathematics 55. Providence, RI: American Mathematical Society, 1986.

[MeSu] A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982), no. 5, 1011–1046, 1135–1136. Translated as *Math. USSR-Izv.* **21** (1983), no. 2, 307–340.

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

[MS] J. Mináč and J. Swallow. Galois module structure of pth-power classes of extensions of degree p. *Israel J. Math.* **138** (2003), 29–42.

[R] P. Ribenboim. Equivalent forms of Hensel's lemma. *Exposition. Math.* **3** (1985), no. 1, 3–24.

[Se] J.-P. Serre. *Galois cohomology.* Berlin: Springer-Verlag, 1997. English translation, with revisions, of *Cohomologie Galoisienne*, Lecture Notes in Math. 5, Springer-Verlag, 1964.

[Sr] V. Srinivas. *Algebraic K-theory*, 2nd ed. Progress in Mathematics 90. Boston: Birkhäuser Boston, 1996.

[V1] V. Voevodsky. On 2-torsion in motivic cohomology. arXiv:math.AG /0107110. Available: http://arXiv.org/abs/math/0107110 (2001).

[V2] V. Voevodsky. On motivic cohomology with Z/l coefficients. K-theory preprint archive 639. Available: http://www.math.uiuc.edu/K-theory/0639/ (2003).

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

E-mail address: nlemire@uwo.ca

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

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