GALOIS MODULE STRUCTURE OF GALOIS COHOMOLOGY

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Andrew Schultz
May 2007

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Ravi Vakil) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Daniel Bump)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Gunnar Carlsson)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Ján Mináč)

Abstract

The cohomology groups associated to the absolute Galois group of a field E encode a great deal of information about E, with the groups $H^m(G_E, \mu_p)$ being of classical interest. These groups are linked to the reduced Milnor K-groups $K_mE/pK_mE = k_mE$ by the Bloch-Kato conjecture. Using this conjecture when E/F is a Galois extension of fields with $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for some odd prime p, and additionally assuming $\xi_p \in E$, we study the groups $H^m(G_E, \mu_p)$ as modules over the group ring $\mathbb{F}_p[\mathrm{Gal}(E/F)]$. When E/F embeds in an extension E'/F with $\mathrm{Gal}(E'/F) \simeq \mathbb{Z}/p^{n+1}\mathbb{Z}$, we are able to give a highly stratified decomposition of $H^m(G_E, \mu_p)$. This allows us to give a decomposition of the cohomology groups of a p-adic extension of fields. In general we are able to give a coarse decomposition of $H^m(G_E, \mu_p)$, showing that many indecomposable types do not appear in $H^m(G_E, \mu_p)$. With an additional assumption about the norm map $N^n_{n-1} : k_mE_n \to k_mE_{n-1}$, we strengthen this coarse decomposition to a highly stratified one.

Acknowledgment

I am indebted to my advisor Ravi Vakil for his constant direction and encouragement, both in the development of this thesis and my development as a mathematician. Ján Mináč and John Swallow have been instrumental in every phase of my mathematical career, and their continued support has helped carry me through my time at Stanford. I cannot thank them enough. I look forward to completing this project and others with their help and with the help of Nicole Lemire.

I am also grateful to Gunnar Carlsson and Daniel Bump for sitting on both my area exam and thesis defense committees. I would like to say thanks to Daniel Krashen and Max Lieblich for helpful discussions on topics that didn't quite make it into my thesis.

Finally, I would like to thank my friends and family for helping preserve my sanity over the last five years.

Contents

Chapter 1

Galois Modules

1.1 Motivation

When a group G acts on an object X, there is typically an induced action of G on invariants associated to X. This action often provides insight into the objects parametrized by these invariants. We give a classical example here.

Let E be a field, and denote a separable algebraic closure of E by $\bar{E}$. We will also assume a primitive pth root of unity ξ_p is in E (so that, in particular, $\mathrm{char}(E) \neq p$). We have an exact sequence of $G_E = \mathrm{Gal}(\bar{E}/E)$-modules

$$1 \to \mu_p \to \bar{E}^\times \xrightarrow{p} \bar{E}^\times \to 1$$

which group cohomology converts into a long exact sequence, including the 4-term sequence

$$H^0(G_E, \bar{E}^\times) \xrightarrow{p} H^0(G_E, \bar{E}^\times) \to H^1(G_E, \mu_p) \to H^1(G_E, \bar{E}^\times).$$

By definition $H^0(G_E, \bar{E}^\times) = (\bar{E}^\times)^{G_E}$ (the submodule of $\bar{E}^\times$ fixed by G_E), which is $E^\times$ by Galois theory. Since $\xi_p \in E$, the action of G_E on μ_p is trivial, and so $H^1(G_E, \mu_p) = \mathrm{Hom}(G_E, \mu_p)$. Using $\mu_p \simeq \mathbb{Z}/p\mathbb{Z}$ and the properties of the absolute Galois group of E, we know that $\mathrm{Hom}(G_E, \mu_p)$ classifies extensions of L/E that

satisfy $\mathrm{Gal}(L/E) \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. Finally, the cohomological version of Hilbert's Theorem 90 gives $H^1(G_E, \bar{E}^\times) = \{1\}$. Hence the exact sequence above becomes

$$E^\times/E^{\times p} \simeq \left\{ \begin{array}{c} \text{extensions } L \text{ of } E \text{ with} \\ \mathrm{Gal}(L/E) \hookrightarrow \mathbb{Z}/p\mathbb{Z} \end{array} \right\}.$$

One can chase the connecting homomorphism and find that the extension of E corresponding to a power class represented by $\gamma \in E^\times$ is given by $E(\sqrt[p]{\gamma})$. This correspondence is known as Kummer Theory.

To strengthen bijections such as this, one often attempts to put a more refined structure on either side of the correspondence. The game is to then interpret how this additional structure on one side is manifested on the other.

For instance, the collection $E^\times/E^{\times p}$ is obviously an $\mathbb{F}_p$-vector space, and in fact we have a correspondence

$$\left\{ \mathbb{F}_p\text{-subspaces of } E^\times/E^{\times p} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{elementary } p\text{-abelian} \\ \text{extensions of } E \end{array} \right\},$$

where an elementary p-abelian extension of E is a Galois field extension L/E with $\mathrm{Gal}(L/E) \simeq \oplus^k \mathbb{Z}/p\mathbb{Z}$ for some k.

We now ask the following question: suppose that E is itself an extension of a field F, with $\mathrm{Gal}(E/F) = G$. Then $E^\times/E^{\times p}$ becomes a module over the group ring $\mathbb{F}_p[G]$. How is this additional structure translated into a property of the corresponding field extension L? The answer is the following

Proposition 1.1. *There is a correspondence*

$$\left\{ \begin{array}{c} \mathbb{F}_p[G]\text{-}\textit{submodules} \\ \textit{of } E^\times/E^{\times p} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{elementary } p\textit{-abelian extensions } L/E \\ \textit{which are also Galois over } F \end{array} \right\}.$$

In particular cases, one can say more. Toward this end, we restrict ourselves to the case $G = \mathrm{Gal}(E/F) = \mathbb{Z}/p^n\mathbb{Z}$ and also fix a generator $\sigma \in G$. We write E_i for the intermediate field of E/F which is degree p^i over F, and write G_i for the group $\mathrm{Gal}(E_i/F)$.

Definition 1.2. For $\gamma \in E^\times/E^{\times p}$, if either $N_{E/F}\gamma \in F^{\times p}$ or $N_{E/F}\gamma \notin E^{\times p}$, then we say γ is of *trivial index*. If $N_{E/F}\gamma \in E^{\times p} \setminus F^{\times p}$, then we say γ is of *non-trivial index*.

One can show that the triviality (or non-triviality) of a generator for a cyclic submodule M is invariant (i.e., if one generator for M is trivial index then all generators for M are trivial index).

With this (admittedly mysterious) notion of index, we have the following result of Waterhouse:

Proposition 1.3 ([15]). *Suppose that $G = Gal(E/F) = \mathbb{Z}/p^n\mathbb{Z}$, and let M be a cyclic $\mathbb{F}_p[G]$-submodule of $E^\times/E^{\times p}$. Let L be the extension of E corresponding to M. Then $Gal(L/F)$ can be computed knowing only $\dim_{\mathbb{F}_p} M$ and the index of a generator of M. If a generator for M is trivial index, then $Gal(L/F) = M \rtimes G$.*

Suppose that an $\mathbb{F}_p[G]$-module M can be written as a direct sum of $\mathbb{F}_p[G]$-submodules, say $M = M_1 \oplus M_2$. If L, L_1 and L_2 are the corresponding field extensions of E, then one can show $\mathrm{Gal}(L/F) = \mathrm{Gal}(L_1/F) \times \mathrm{Gal}(L_2/F)$. Since every $\mathbb{F}_p[G]$-submodule can be written as a direct sum of cyclic submodules (Theorem 2.9), the previous proposition implies we can determine the Galois group of a field extension corresponding to an arbitrary $\mathbb{F}_p[G]$-submodule M.

With this result in mind, it is natural to ask for the $\mathbb{F}_p[G]$-structure of $E^\times/E^{\times p}$. One would especially like this decomposition to keep track of the index of elements in $E^\times/E^{\times p}$, or possibly even contain in some obvious way a maximal trivial index submodule (that is, a submodule T whose elements are all trivial index, and so that any other module S properly containing T contains an element of non-trivial index). We shall describe such a result in the next section.

1.2 $H^1(G_E, \mu_p)$ as a Galois Module

The investigation of the $\mathbb{F}_p[G]$-module structure of $E^\times/E^{\times p}$ was started by Faddeev in [3], where F was assumed to be a local field of finite degree over $\mathbb{Q}_p$. More recently Mináč and Swallow calculated in [11] the module structure whenever $G = \mathbb{Z}/p\mathbb{Z}$ (i.e., when $n = 1$). The question was resolved for general p-power cyclic extensions E/F

by Mináč, Swallow and the author in [10]. Even in this general case, $E^\times/E^{\times p}$ has a highly stratified module structure, with all but one summand 'free' (i.e., isomorphic to $\mathbb{F}_p[\mathrm{Gal}(E_i/F)]$ for some i).

We state the decomposition in the case $p > 2$ and $\xi_p \in E$, although analogous results without these restrictions exist.

Theorem 1.4 ([10, Theorem 2]). *Let E/F be an extension of fields such that $Gal(E/F) simeq \mathbb{Z}/p^n\mathbb{Z}$, where $p > 2$ is prime and $\xi_p \in E$. Then as an $\mathbb{F}_p[G]$-module*

$$E^\times/E^{\times p} \simeq X \oplus \bigoplus_{i=0}^{n} Y_i,$$

where

- *X is cyclic of dimension $p^{i(E/F)} + 1$ for some $i(E/F) \in \{-\infty, 0, \cdots, n-1\}$, and*
- *for each i, $Y_i \subseteq E_i/E^{\times p}$ is a direct sum of free $\mathbb{F}_p[Gal(E_i/F)]$-modules.*

Moreover, the submodule $(\sigma - 1)X \oplus \bigoplus_{i=0}^{n} Y_i$ is a maximal trivial index submodule.

Given Kummer theory and Waterhouse's result, it is not surprising that this theorem contains a great deal of information about certain embedding problems involving E/F. For instance, the isomorphism class of the exceptional summand (i.e., X) is determined by an invariant $i(E/F) \in \{-\infty, 0, \cdots, n-1\}$ which can be defined as follows: if E/F embeds in a cyclic extension E'/F which is Galois with group $\mathbb{Z}/p^{n+1}\mathbb{Z}$, then $i(E/F) = -\infty$; otherwise, if j is chosen as small as possible so that E/E_j embeds in a cyclic extension E'/E_j which is Galois with group $\mathbb{Z}/p^{n-j+1}\mathbb{Z}$, then $i(E/F) = j - 1$. Since $\xi_p \in E$ we know that E embeds in a cyclic extension (here we're using the assumption that $p > 2$), and hence $i(E/F) \leq n - 1$ as stated. This characterization of $i(E/F)$ (and several others) are found in [10].

There are other connections with embedding results. Note that the last statement of Theorem 1.4 gives

Corollary 1.5. *A maximal trivial index submodule is a direct sum of 'free' submodules (i.e., submodules free over appropriate quotients $\mathbb{F}_p[G_i]$ of $\mathbb{F}_p[G]$).*

This result is used in the joint work of Mináč, Swallow and the author [8] as follows. Suppose that there exists a trivial-index, cyclic submodule M which is dimension $p^i + 1$. Then the corollary above gives the existence of some trivial-index submodule N of dimension p^{i+1}. In terms of Galois groups à la Waterhouse, this translates to an automatic realization result: if there exists some field extension L of E with $\mathrm{Gal}(L/F) \simeq \mathbb{F}_p[G]/(\sigma - 1)^{p^i+1} \rtimes \mathrm{Gal}(E/F)$ then there exists a field extension L' of E with

$$\mathrm{Gal}(L'/E) \simeq \mathbb{F}_p[G]/(\sigma - 1)^{p^{i+1}} \rtimes \mathrm{Gal}(E/F) \simeq \mathbb{F}_p[G_{i+1}] \rtimes \mathrm{Gal}(E/F).$$

One could also use this result to give specific obstructions to certain embedding problems, and just such an analysis was carried out in the case $n = 1$ by Mináč and Swallow [12].

1.3 Generalizations

One can attempt to generalize the results above in a number of ways. Again fixing an extension E/F with $\mathrm{Gal}(E/F) = \mathbb{Z}/p^n\mathbb{Z}$, one natural problem is to determine the $\mathbb{Z}/p^s\mathbb{Z}[G]$-module structure of $E^\times/E^{\times p^s}$. This question adds a new challenge because the isomorphism classes of indecomposable $\mathbb{Z}/p^s\mathbb{Z}[G]$-modules are more complex than those for $\mathbb{F}_p[G]$-modules: the former is of infinite representation type, while the latter is of finite representation type. In characteristic p one finds that all summands of $E^\times/E^{\times p^s}$ are 'free,' as shown by Mináč, Swallow and the author [9]. Preliminary work of these authors suggests that there will be more exotic summands in the decomposition of $E^\times/E^{\times p^s}$ when $\mathrm{char}(E) \neq p$.

One might also attempt to allow for more general Galois groups, perhaps moving away from cyclic groups of the form $\mathbb{Z}/p^n\mathbb{Z}$ to elementary p-abelian groups or even abelian p-groups. The group rings $\mathbb{F}_p[\oplus^k\mathbb{Z}/p\mathbb{Z}]$ are of infinite representation type when $k > 1$, and so studying these modules will be difficult. This project was initiated by Chemotti, Mináč and Swallow in [2], where they study the Galois module structure of $E^\times/E^{\times 2}$ when E/F is Galois with $\mathrm{Gal}(E/F) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. They show that

the module structure of $E^\times/E^{\times 2}$ contains only finitely many isomorphism classes of indecomposables.

Another direction of generalization was pursued in [7] by Lemire, Mináč, and Swallow, where they used the Bloch-Kato conjecture and recent work of Voevodsky to determine the module structure of $H^m(G_E, \mu_p)$ under the assumptions $\xi_p \in E$ and $\mathrm{Gal}(E/F) = \mathbb{Z}/p\mathbb{Z}$. In this case the only indecomposable types which appear in a decomposition are cyclic of dimension either 1, 2 or p, though — contrary to the results of [11] — the decomposition can have more than one 'exceptional' summand. These results have been used to study Sylow-p subgroups of absolute Galois groups of fields (see, for instance, [1] and [6]).

This thesis generalizes the investigation of $H^1(G_E, \mu_p)$ by studying the Galois module structure of $H^m(G_E, \mu_p)$ for extensions E/F with $\xi_p \in E$ and whose Galois group is a cyclic p-group, where p is an odd prime. Our approach mirrors that in [7]: we use the Bloch-Kato conjecture and several results of Voevodsky to inductively study the groups $H^m(G_E, \mu_p)$. The result requires studying maps induced by inclusion and norm maps for intermediate extensions within E/F, as well as understanding the subgroups of norms from these intermediate fields.

In Chapter 2 we give some basic facts about $\mathbb{F}_p[G]$-modules, including a full description of all indecomposable $\mathbb{F}_p[G]$-modules as well as a result which guarantees a unique decomposition of any $\mathbb{F}_p[G]$-module W into indecomposables. The basic module-theoretic language for the rest of the thesis is established in this chapter.

In Chapter 3 we begin the investigation of the groups $H^m(G_E, \mu_p)$ by introducing Milnor K-theory and its connection to our cohomology groups. Our main results are developed for the so-called reduced Milnor K-groups of E, which themselves are conjecturally isomorphic to our Galois cohomology groups via the Bloch-Kato conjecture. Hence after we develop our results for the reduced Milnor K-groups of E, we translate them back to the language of group cohomology for the reader's convenience. We state an exact sequence of Voevodsky that is the engine that drives our results. We also develop machinery for understanding $H^m(G_E, \mu_p)$ in our context,

particularly for determining those elements in

$$\operatorname{im}\left(N_{n-1}^{n} : k_m E_n \to k_m E_{n-1}\right) \cap \ker\left(\iota_{n-1}^{n} : k_m E_{n-1} \to k_m E_n\right),$$

and also for computing

$$k_m E_n^G \cap \iota_0^n(N_0^j(k_m E_j))$$

for $0 \leq j \leq n-1$. The conclusion of Chapter 3 gives the structure of $H^m(G_E, \mu_p)$ when $i(E/F) = -\infty$.

In Chapter 4 we use results from Chapter 3 to give the Galois module structure of the cohomology groups of a p-adic extension containing appropriate roots of unity. Again, results are developed in the language of K-theory and then translated back to Galois cohomology.

In the final chapter, we use the machinery developed in Chapter 3 and an additional assumption on the properties of the norm map $N_{n-1}^{n} : k_m E_n \to k_m E_{n-1}$ to give a decomposition of $H^m(G_E, \mu_p)$ when $i(E/F) \geq 0$; as always, it is first developed in the language of K-groups and then translated to Galois Cohomology via Bloch-Kato. In the case $i(E/F) = 0$ we show that this assumption on N_{n-1}^{n} holds.

Chapter 2

Properties of $\mathbb{F}_p[\mathbb{Z}/p^n\mathbb{Z}]$-modules

In order to prepare for the results which follow, we first remind the reader of some $\mathbb{F}_p[\mathbb{Z}/p^n\mathbb{Z}]$-module properties. Throughout this section we write $G = \mathbb{Z}/p^n\mathbb{Z}$ and denote by σ a fixed generator of G. Although we restrict ourselves to the case $p > 2$ in the sequel, we shall allow $p = 2$ in this section. We note that $\sigma - 1$ generates a maximal ideal of the commutative ring $\mathbb{F}_p[G]$, since the quotient of $\mathbb{F}_p[G]$ by this ideal is the field $\mathbb{F}_p$. Soon we will see that it is the only maximal ideal.

We start with the following polynomial identity, a result which will be important not only in showing that $\mathbb{F}_p[G]$ is a local ring, but also in understanding the norm operators which later play a key role in our results.

Lemma 2.1. *As elements of* $\mathbb{F}_p[G]$,

$$\sum_{i=0}^{p^n-1} \sigma^i = (\sigma - 1)^{p^n-1}.$$

Proof. The coefficient of σ^k in $(\sigma - 1)^{p^n-1}$ is $(-1)^{p^n-1-k}\begin{pmatrix} p^n - 1 \\ k \end{pmatrix}$. When $k = 0$ this coefficient is clearly $1 \mod p$ (in fact, if $p \neq 2$, it actually is 1). Now when $0 < k$ we have

$$\begin{pmatrix} p^n - 1 \\ k - 1 \end{pmatrix} + \begin{pmatrix} p^n - 1 \\ k \end{pmatrix} = \begin{pmatrix} p^n \\ k \end{pmatrix},$$

where the latter binomial coefficient is congruent to 0 modulo p. Hence

$$\begin{pmatrix} p^n - 1 \\ k \end{pmatrix} \equiv - \begin{pmatrix} p^n - 1 \\ k - 1 \end{pmatrix} \mod p,$$

and by induction we have that $\begin{pmatrix} p^n - 1 \\ k \end{pmatrix}$ is congruent to $(-1)^k$. Hence we conclude

$$(-1)^{p^n-1-k} \begin{pmatrix} p^m - 1 \\ k \end{pmatrix} \equiv 1 \mod p$$

as desired. (Notice that this argument works when $p = 2$ since $1 \equiv -1$.) □

The element $\sum_{i=0}^{p^n-1} \sigma^i$ defines the norm operator for the field extension E/F, and our theorem says that one can calculate the norm (modulo p) with the operator $(\sigma - 1)^{p^n-1}$. The following corollary records a generalization of this result to an intermediate extension E_i/E_j. Note that we abuse notation by writing σ^{p^j} for a generator of $\mathrm{Gal}(E_i/E_j)$ instead of the more traditional $\bar{\sigma}^{p^j}$ (this particular abuse of notation will happen frequently).

Corollary 2.2. *As elements of* $\mathbb{F}_p[Gal(E_i/E_j)]$,

$$\sum_{k=0}^{p^{i-j}-1} \left(\sigma^{p^j}\right)^k = (\sigma^{p^j} - 1)^{p^{i-j}-1} = (\sigma - 1)^{p^i - p^j}.$$

Proof. The first equivalence holds by the previous lemma (after replacing G by $\mathrm{Gal}(E_i/E_j)$). For the second equivalence, notice that the coefficient of σ^k in $(\sigma - 1)^p$ is $(-1)^{p-k} \begin{pmatrix} p \\ k \end{pmatrix}$, which is zero modulo p whenever $k \neq 0$ or p. Hence we have $(\sigma - 1)^p = \sigma^p - 1$ in $\mathbb{F}_p[G]$. Repeating this argument j times gives the desired equivalence. □

Corollary 2.3. *The ideal*

$$ann((\sigma - 1)^{p^n-1}) := \{r \in \mathbb{F}_p[G] : (\sigma - 1)^{p^n-1} r = 0\}$$

is the ideal generated by $\sigma - 1$.

Proof. Since $(\sigma-1)^{p^n-1} \neq 0$ from the previous lemma, we know that the annihilating ideal is not all of $\mathbb{F}_p[G]$. However we can see that

$$(\sigma - 1)^{p^n} = (\sigma - 1)^{p^n-1}(\sigma - 1) = \left(\sum \sigma^i\right)(\sigma - 1) = 0, \tag{2.4}$$

and hence $\sigma - 1$ is in the annihilating ideal. Since $\sigma - 1$ generates a maximal ideal, we have the desired result. □

Lemma 2.5. $\mathbb{F}_p[G]$ *is a local ring with maximal ideal* $(\sigma - 1)$.

Proof. Suppose that I is an ideal and $\sigma - 1 \notin I$. Then we have $1 = (\sigma - 1)f + ig$ for some $f, g \in \mathbb{F}_p[G]$ and $i \in I$. Using the $\mathbb{F}_p$-basis $\{1, \sigma - 1, \cdots, (\sigma - 1)^{p^n-1}\}$ of $\mathbb{F}_p[G]$, we write $g = \sum_{j=0}^{p^n-1} c_j(\sigma - 1)^j$. We also note that $c_0 \neq 0$, since otherwise 1 is an element of the ideal generated by $\sigma - 1$. Multiplying this equation by $(\sigma - 1)^{p^n-1}$ and recalling Equation 2.4, we have

$$(\sigma - 1)^{p^n-1} = c_0(\sigma - 1)^{p^n-1}i,$$

and hence by the previous corollary we have $i = c_0^{-1} + (\sigma - 1)h$ for some $h \in \mathbb{F}_p[G]$. Since the non-units of $\mathbb{F}_p[G]$ form an ideal, the element $i = c_0^{-1} + (\sigma - 1)h \in I$ must be a unit in $\mathbb{F}_p[G]$. Therefore $I = \mathbb{F}_p[G]$, contrary to our hypothesis. □

Our next goal is to determine the isomorphism classes of indecomposable $\mathbb{F}_p[G]$-modules. As a start we show the following

Lemma 2.6. *For* $0 \leq i \leq p^n$, *a cyclic submodule* M *of dimension* i *over* $\mathbb{F}_p$ *is indecomposable and isomorphic to the* $\mathbb{F}_p[G]$*-module* $A_i := \mathbb{F}_p[G]/(\sigma - 1)^i$.

Proof. If M is a cyclic submodule generated by m, then we have a short exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \to \text{ann}(m) \to \mathbb{F}_p[G] \to M \to 0.$$

Since $\mathbb{F}_p[G]$ is local with maximal ideal $(\sigma - 1)$, any ideal of $\mathbb{F}_p[G]$ is isomorphic to $(\sigma - 1)^k$ for some $0 \leq k \leq p^n - 1$. In particular $\text{ann}(m) = (\sigma - 1)^k$ for some k.

It is easy to verify $\dim_{\mathbb{F}_p}\left(\mathbb{F}_p[G]/(\sigma-1)^k\right) = k$, and so we have $k = i$ since M is i dimensional. Hence $M \simeq A_i$ as an $\mathbb{F}_p[G]$-module by the map

$$\left(\sum_{j=0}^{p^n-1} a_j(\sigma-1)^j\right) m \mapsto \sum_{j=0}^{i-1} a_j(\bar{\sigma}-1)^j.$$

To see that this module is indecomposable, suppose we could write $M = M_1 \oplus M_2$, where both M_1 and M_2 are $\mathbb{F}_p[G]$-submodules of M. Let $m = m_1 \oplus m_2$. Since $(\sigma-1)^{i-1}m \neq 0$, without loss of generality we may assume $(\sigma-1)^{i-1}m_1 \neq 0$. Hence M_1 is a submodule of M with $\dim_{\mathbb{F}_p} M \leq \dim_{\mathbb{F}_p}\langle m_1\rangle \leq \dim_{\mathbb{F}_p} M_1 < \infty$. Since $\dim_{\mathbb{F}_p} M_1 + \dim_{\mathbb{F}_p} M_2 = \dim_{\mathbb{F}_p} M$ we have $\dim_{\mathbb{F}_p}(M_2) = 0$, and hence $M_2 = \{0\}$. □

It will be convenient for us to have a simple notation for this defining quality of a cyclic submodule.

Definition 2.7. If M is a cyclic $\mathbb{F}_p[G]$-module generated by an element m, we write

$$\ell_G(m) := \dim_{\mathbb{F}_p} M.$$

By the previous result, this is the same as

$$\ell_G(m) = \min\{i \geq 1 : (\sigma-1)^i m = 0\}.$$

When there is no risk of confusion we will frequently abbreviate this notation by writing $\ell(\gamma)$ for $\ell_G(\gamma)$. Since $(\sigma-1)^{p^n} = 0$ in $\mathbb{F}_p[G]$ (Equation (2.4)), we have $\ell_G(m) \leq p^n = |G|$ for any m.

Since we are ultimately interested in giving decompositions of $\mathbb{F}_p[G]$-modules, we show below that every $\mathbb{F}_p[G]$-module W can be written as a direct sum of indecomposable $\mathbb{F}_p[G]$-modules. Then we show that all expressions of W as a direct sum of indecomposables are equivalent, in the sense that if $\oplus_{\alpha\in\mathcal{A}} W_\alpha$ and $\oplus_{\beta\in\mathcal{B}} W_\beta$ are two decompositions of W into indecomposable submodules, then there is a bijection $j : \mathcal{A} \to \mathcal{B}$ and, for each $\alpha \in \mathcal{A}$, an $\mathbb{F}_p[G]$-isomorphism $W_\alpha \simeq W_{j(\alpha)}$. There is certainly

machinery already in the literature that gives us this result, but in our context the result is fairly elementary and illuminates a technique we use frequently in the sequel.

First is a result that allows us to easily check when two submodules have trivial intersection.

Lemma 2.8 (Exclusion Lemma). *Suppose U, V are $\mathbb{F}_p[G]$-submodules of an $\mathbb{F}_p[G]$-module W. Then $U \cap V \neq \{0\}$ if and only if $U^G \cap V^G \neq \{0\}$.*

Proof. That $U^G \cap V^G \neq \{0\}$ implies $U \cap V \neq \{0\}$ is trivial, so we show that $U \cap V \neq \{0\}$ implies $U^G \cap V^G \neq \{0\}$. Suppose that $w \in U \cap V$ for some $w \neq 0$. Since $\operatorname{ann}(w) = (\sigma - 1)^{\ell(w)}$, the element $(\sigma-1)^{\ell(w)-1}w$ is nontrivial and fixed by G. Since U and V are both $\mathbb{F}_p[G]$-submodules, we therefore have $(\sigma - 1)^{\ell(w)-1}w \in U^G \cap V^G$. □

Theorem 2.9. *If W is an $\mathbb{F}_p[G]$-module, then there exists an $\mathbb{F}_p[G]$-isomorphism*

$$W \simeq \bigoplus_{i=1}^{p^n} \oplus_{d_i} A_i,$$

where d_i is the codimension of $\operatorname{im}((\sigma-1)^i) \cap W^G$ within $\operatorname{im}((\sigma-1)^{i-1}) \cap W^G$.

Proof. For $1 \leq i \leq p^n$ we define V_i as the $\mathbb{F}_p$-subspace of elements in W^G which are in the image of $(\sigma-1)^{i-1}$, and for each i we choose an $\mathbb{F}_p$-basis $\mathcal{I}_i$ for a complement to V_{i+1} in V_i. Hence $d_i = |\mathcal{I}_i|$ is the codimension of $\operatorname{im}((\sigma-1)^i) \cap W^G$ within $\operatorname{im}((\sigma-1)^{i-1}) \cap W^G$. Our construction also implies that $\langle \mathcal{I}_i, \mathcal{I}_{i+1}, \cdots, \mathcal{I}_{p^n} \rangle = V_i$.

For each $x \in \mathcal{I}_i$, let $w_x \in W$ be chosen so that $(\sigma-1)^{i-1}w_x = x$. Since $\ell(w_x) = i$ we have $\langle w_x \rangle_{\mathbb{F}_p[G]} \simeq A_i$ as an $\mathbb{F}_p[G]$-module. We define $W_i = \sum_{x \in \mathcal{I}_i} \langle w_x \rangle_{\mathbb{F}_p[G]}$; to show that $W_i \simeq \oplus_{d_i} A_i$, it will be enough to show that $\sum_{x\in\mathcal{I}_i} \langle w_x \rangle_{\mathbb{F}_p[G]} = \oplus_{x\in\mathcal{I}_i} \langle w_x \rangle_{\mathbb{F}_p[G]}$. Now the Exclusion Lemma 2.8 implies that a non-trivial dependence among $\langle w_x \rangle_{\mathbb{F}_p[G]}$ must appear as a non-trivial dependence among $\langle w_x \rangle^G_{\mathbb{F}_p[G]} = \langle x \rangle_{\mathbb{F}_p}$. But the x are chosen to be independent, and so $W_i = \oplus_{x\in\mathcal{I}_i} \langle w_x \rangle_{\mathbb{F}_p[G]}$ as desired.

We now show that $\sum_i W_i = \oplus_i W_i$. Again, any dependence among the modules must appear as a dependence among the various W_i^G by the Exclusion Lemma 2.8. Recall that

$$W_i^G = \oplus_{x\in\mathcal{I}_i} \langle w_x \rangle^G_{\mathbb{F}_p[G]} = \oplus_{x\in\mathcal{I}_i} \langle x \rangle_{\mathbb{F}_p} = \langle \mathcal{I}_i \rangle,$$

and that $\langle \mathcal{I}_i \rangle$ is selected as a complement to $V_{i+1} = \langle \mathcal{I}_{i+1}, \cdots, \mathcal{I}_{p^n} \rangle = \langle W_{i+1}^G, \cdots, W_{p^n}^G \rangle$ in V_i. Hence W_i^G has trivial intersection with $\langle W_{i+1}^G, \cdots, W_{p^n}^G \rangle$, and so $\sum_{j \geq i} W_j = \oplus_{j \geq i} W_j$. Running this argument inductively gives $\sum_i W_i = \oplus_i W_i$.

Finally we argue that $\oplus_{i=1}^{p^n} W_i = W$. By construction we have $\{\mathcal{I}_1, \cdots, \mathcal{I}_{p^n}\}$ is an $\mathbb{F}_p$-basis for $W^G = V_1$. Since $W_i^G = \langle \mathcal{I}_i \rangle$ we have $V_1 = \oplus_{i=1}^{p^n} W_i^G$, and hence all elements of length 1 are contained in $\oplus_{i=1}^{p^n} W_i$.

Suppose, then, that $\oplus W_i$ contains all vectors of length at most $\ell - 1$, and let w be an element of length ℓ. Then we have $(\sigma - 1)^{\ell - 1} w \in V_\ell$, and hence by construction $(\sigma - 1)^{\ell - 1} w \in \oplus_{i \geq \ell} W_i^G$. We may therefore write

$$(\sigma - 1)^{\ell - 1} w = \sum_{i \geq \ell} \sum_{x \in \mathcal{I}_i} c_x x = \sum_{i \geq \ell} \sum_{x \in \mathcal{I}_i} c_x (\sigma - 1)^{i - 1} w_x.$$

Hence

$$(\sigma - 1)^{\ell - 1} \left(w - \sum_{i \geq \ell} \sum_{x \in \mathcal{I}_i} c_x (\sigma - 1)^{i - \ell} w_x \right) = 0,$$

and so $w - \sum_i \sum_x c_x (\sigma - 1)^{i - \ell} w_x$ is an element of length at most $\ell - 1$. Hence it is contained in $\oplus W_i$ by induction. Since each $w_x \in \oplus W_i$, we also have $w \in \oplus W_i$ as desired. □

Corollary 2.10. *Every indecomposable $\mathbb{F}_p[G]$-module is cyclic.*

Proof. Suppose W is not cyclic. We argue that

$$\dim_{\mathbb{F}_p} W^G > 1. \tag{2.11}$$

Once we have this inequality the previous theorem implies W is decomposable.

First, choose an element w_1 of maximal length in W. Since W is not cyclic we have $\langle w_1 \rangle_{\mathbb{F}_p[G]} \neq W$. Hence choose an element $w_2 \notin \langle w_1 \rangle_{\mathbb{F}_p[G]}$ which has minimal length among elements with this property. We claim that $\langle w_1 \rangle_{\mathbb{F}_p[G]}^G \cap \langle w_2 \rangle_{\mathbb{F}_p[G]}^G = \{0\}$, from which our desired inequality (2.11) follows.

If $\langle w_1 \rangle_{\mathbb{F}_p[G]}^G \cap \langle w_2 \rangle_{\mathbb{F}_p[G]}^G \neq \{0\}$ then for some $c \in \mathbb{F}_p^\times$ we have $(\sigma - 1)^{\ell(w_1) - 1} w_1 = c(\sigma - 1)^{\ell(w_2) - 1} w_2$. This implies that $(\sigma - 1)^{\ell(w_2) - 1} \left(c w_2 - (\sigma - 1)^{\ell(w_1) - \ell(w_2)} w_1 \right) = 0$.

But then $cw_2-(\sigma-1)^{\ell(w_1)-\ell(w_2)}w_1$ has length at most $\ell(w_2)-1$ and is outside $\langle w_1\rangle_{\mathbb{F}_p[G]}$, contradicting the minimality of w_2. □

Corollary 2.12. *Let $\oplus_{\alpha\in\mathcal{A}}W_\alpha$ be a decomposition of W into indecomposable $\mathbb{F}_p[G]$-modules. Then $\mathcal{A}$ is a disjoint union of subsets $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{p^n}$ where*

- *$|\mathcal{A}_i|$ is the codimension of $\mathrm{im}\,((\sigma-1)^i)\cap W^G$ within $\mathrm{im}\,((\sigma-1)^{i-1})\cap W^G$, and*
- *for each $\alpha\in\mathcal{A}_i$ there is an $\mathbb{F}_p[G]$-isomorphism $A_i\simeq W_\alpha$.*

Proof. The previous corollary gives that any indecomposable $\mathbb{F}_p[G]$-module is isomorphic to $A_i := \mathbb{F}_p[G]/(\sigma-1)^i$ for some $1\le i\le p^n$. Hence we define $\mathcal{A}_i$ to be the collection of $\alpha\in\mathcal{A}$ so that $W_\alpha\simeq A_i$ as $\mathbb{F}_p[G]$-modules. Our goal is therefore to show that $|\mathcal{A}_i|$ is the codimension of V_{i+1} in V_i.

Our result will follow if we can show

$$V_i = \oplus_{j\ge i}\oplus_{\alpha\in\mathcal{A}_j} W_\alpha^G,$$

since then we have $\dim_{\mathbb{F}_p} V_i = \sum_{j\ge i}|\mathcal{A}_j|$ for any i. For the "$\supseteq$" containment, note that $A_j^G\in \mathrm{im}\,((\sigma-1)^{j-1})\subseteq \mathrm{im}\,((\sigma-1)^{i-1})$ for any $j\ge i$, so $\oplus_{j\ge i}\oplus_{\alpha\in\mathcal{A}_j}W_\alpha^G\subseteq V_i$. For the reverse containment, note that $(\sigma-1)^{i-1}$ annihilates every module A_k for $k<i$. Hence $\mathrm{im}\,((\sigma-1)^{i-1})\cap\oplus_{k<i}\oplus_{\alpha\in\mathcal{A}_k}W_\alpha=\{0\}$. The independence of the various W_α allows us to conclude $V_i=\oplus_{j\ge i}\oplus_{\alpha\in\mathcal{A}_j}W_\alpha^G$ as desired. □

Chapter 3

Galois Cohomology for $\mathbb{Z}/p^n\mathbb{Z}$ Extensions

In this chapter we again consider a cyclic extension of fields E/F with Galois group $\mathbb{Z}/p^n\mathbb{Z}$, where $p > 2$ is a prime. We further require $\xi_p \in E$. Since $\mathrm{Gal}(E/F) = \mathbb{Z}/p^n\mathbb{Z}$, this is equivalent to the assumption that $\xi_p \in F$. Via the Bloch-Kato Conjecture, we shall investigate the structure of the cohomology groups $H^m(G_E, \mathbb{F}_p)$ as modules over $\mathbb{F}_p[\mathrm{Gal}(E/F)]$. In particular, results are stated as theorems about the reduced Milnor K-groups of E, then translated back to statements about Galois Cohomology via Bloch-Kato.

3.1 Notation and Preliminary Results

We shall use the following notation. The intermediate field of E/F of degree p^i over F is written E_i, and hence we shall frequently write E_n for E and E_0 for F. The group $\mathrm{Gal}(E/F)$ will be written G, and we write G_i for the groups $\mathrm{Gal}(E_i/F)$. We shall write H_i for the subgroup of G whose quotient is G_i, and so $H_i = \mathrm{Gal}(E/E_i)$. As in Chapter 2 we write σ for a generator of G, though we will often abuse notation and also write σ as a generator of G_i.

Kummer Theory tells us that $E_{i+1} = E_i(\sqrt[p]{a_i})$ for some $a_i \in E_i^\times$, and keeping careful control of when these elements appear as norms in $E^\times/E^{\times p}$ was important in

determining Theorem 1.4. It was also important that these elements themselves be compatible with the norm operators, and so it was shown ([10, Proposition 1]) that one may choose these elements with the following norm compatibility property:

$$N_{E_i/E_j} a_i = a_j \quad \text{for any } i \geq j. \tag{3.1}$$

It is also shown that, up to pth powers in $E_i^\times$, the a_i are fixed by the action of G_i:

$$a_i^\sigma = a_i k_i^p \tag{3.2}$$

for some $k_i \in E_i^\times$. Hence for $i > j$, each a_i is an element of minimal length in $E_i^\times$ whose norm to E_j is a_j.

We make a few comments regarding the submodule X from Theorem 1.4 (the so-called 'exceptional' submodule). A generator for this submodule is the power class of an element $\chi \in E^\times$ which attempts to play the role of what we might call a_n, in the sense that $N_{n-1}^n(\chi) = a_{n-1}$ à la the norm compatibility condition (3.1), and that the power class of χ has minimal length among all elements whose norm to E_{n-1} is a_{n-1}. The length of the power class of χ is precisely $p^{i(E/F)} + 1$, where we recall that $i(E/F)$ has an explicit interpretation in terms of embedding properties.

It is useful to note that for an intermediate extension E_i/F with $i < n$, the power class of a_i in $E_i^\times/E_i^{\times p}$ plays the role of χ for the extension E_i/F: we have $N_{i-1}^i(a_i) = a_{i-1}$ from our norm compatibility condition (3.1), and from Equation (3.2) we see that the length of the power class of a_i is $1 = p^{i(E_i/F)} + 1 = p^{-\infty} + 1$ as expected. This means that the submodule $\langle a_i E_i^{\times p} \rangle_{\mathbb{F}_p}$ can be chosen to be the exceptional summand of $E_i^\times/E_i^{\times p}$ in Theorem 1.4. These observations will be important both in running the induction we use to prove the main results and in determining the structure of Galois cohomology for p-adic extensions in the next chapter.

3.2 Milnor k-theory and Galois Cohomology

For a field L, the m-th Milnor K-group of L is defined as

$$K_m L := \left(\bigotimes_{i=1}^{m} L^\times \right) / I_m$$

where I_m is the subgroup of $\otimes_{i=1}^m L^\times$ generated by elements $a_1 \otimes \cdots \otimes a_m$ with $a_i + a_j = 1$ for some $i \neq j$. We denote the equivalence class of $a_1 \otimes \cdots \otimes a_m$ in $K_m L$ by $\{a_1, \cdots, a_m\}$ and use additive notation: $\{a_1 a_1', a_2, \cdots, a_m\} = \{a_1, \cdots, a_m\} + \{a_1', \cdots, a_m\}$. It is not difficult to see that the map $K_m L \times K_{m'} L \to K_{m+m'} L$ defined by

$$(\{a_1, \cdots, a_m\}, \{b_1, \cdots, b_{m'}\}) \mapsto \{a_1, \cdots, a_m, b_1, \cdots, b_{m'}\}$$

puts the structure of a graded ring on the Milnor K-groups. When G acts on elements of $L^\times$ we have an induced action on $K_m L$ by $\tau\{a_1, \cdots, a_m\} = \{\tau(a_1), \cdots, \tau(a_m)\}$; notice we write the action additively. The exception to this is the natural $\mathbb{Z}$-action which acts by $n\{a_1, \cdots, a_m\} = \{a_1^n, a_2, \cdots, a_m\} (= \{a_1, \cdots, a_i^n, \cdots, a_m\})$ by virtue of the tensor product.

Although Milnor K-groups encode a great deal of information about a field, we shall be interested only in the quotients of these groups by the ideal (p). These so-called reduced Milnor K-groups are written $k_m L := K_m L / p K_m L$, which we call k-groups. Notice that when $m = 1$ we have $k_1 L = L^\times / L^{\times p}$, and hence

$$k_1 L \xrightarrow{\sim} H^1(G_L, \mu_p).$$

One can then attempt to extend this map to higher k- and cohomology groups via the cup product in cohomology:

$$\{a_1, \cdots, a_m\} \mapsto (a_1) \cup \cdots \cup (a_m) \in H^m(G_L, \mu_p^{\otimes m}).$$

This does produce a morphism $k_m L \to H^m(G_L, \mu_p^{\otimes m})$ because cohomology satisfies the relation $(a_i) \cup (a_j) = 0$ whenever $a_i + a_j = 1$ (see, for instance, [13, Chp. VI]). In

our context (i.e., when $L = E_i$) it is important to note that this morphism respects the action of G_i on both groups.

That this induced map is an equivariant isomorphism for $m > 1$ is the Bloch-Kato conjecture. In certain cases the Bloch-Kato conjecture has already been verified. Merkurev and Suslin showed the conjecture is true for $m = 2$ and all p; Merkurev and Suslin, and independently Rost, have verified the conjecture in the case $p = 2$ and $m = 3, 4$. A huge step forward was Voevodsky's verification of the result for $p = 2$ and m arbitrary in 1996. Voevodsky, Suslin, and Rost have worked to extend Voevodsky's attack on $p = 2$ to settle the Bloch-Kato conjecture when p is an arbitrary prime, and at writing it seems that the final details for a proof of the conjecture have been presented by Chuck Weibel in a seminar at Rutgers (in the fall of 2006).

We assume the Bloch-Kato conjecture for all m and p in developing our results, and we state all results in the language of reduced Milnor K-groups. We translate these results back to Galois Cohomology for the reader's convenience.

In order to proceed we shall need properties of two classes of maps on k-groups associated to an extension of fields L/K. The first is the collection of maps $\iota_{L/K} : k_mK \to k_mL$ induced by the inclusion $K \hookrightarrow L$, and the second is the collection of norm homomorphisms $N_{L/K} : k_mL \to k_mK$. In our context (where we are interested in the extensions E_i/E_j for various $i \geq j$), we shall write ι_{E_i/E_j} as ι^i_j, and we shall write N_{E_i/E_j} as N^i_j. The history of the norm map is particularly interesting, and the reader is encouraged to consult [4, Chp. 9].

In addition to the exact sequence below, we shall use the fact that the morphism $\iota^i_j \circ N^i_j$ is given by the polynomial function $\sum_{k=0}^{p^{i-j}-1} \left(\sigma^{p^j}\right)^k$, which is equivalent (over $\mathbb{F}_p[G]$) to $(\sigma - 1)^{p^i - p^j} = (\sigma^{p^j} - 1)^{p^{i-j}-1}$ by Lemma 2.2.

We shall also use the so-called Projection formula, which allows one to compute the norm $N_{L/K}$ of an element $\{a_1, \cdots, a_m\}$ in terms of the 'usual' norm operator $N_{L/K} : L \to K$ when all but one of the terms in the symbol is in the field K. Specifically, for an extension L/K of fields, and for elements $l \in L$ and $k_1, \cdots, k_{m-1} \in K$, the Projection Formula [5, p. 81] is

$$N_{L/K}\{l, \iota_{L/K}(k_1), \cdots, \iota_{L/K}(k_{m-1})\} = \{N_{L/K}(l), k_1, \cdots, k_{m-1}\}. \tag{3.3}$$

We now give an exact sequence that drives much of the machinery we use. In his work on the Bloch-Kato conjecture [14], Voevodsky proves that for a field F with $\xi_p \in F$ and which has no extensions of degree prime to p, and for any $a \in F^\times \setminus F^{\times p}$, there is an exact sequence

$$k_{m-1}F(\sqrt[p]{a}) \xrightarrow{N_{F(\sqrt[p]{a})/F}} k_{m-1}F \xrightarrow{\{a\}\cdot -} k_m F \xrightarrow{\iota_{F(\sqrt[p]{a})/F}} k_m F(\sqrt[p]{a}) \ .$$

In [7] Lemire, Mináč and Swallow show that the assumption on extensions of degree prime to p can be dropped. Hence for our $a_i \in E_i^\times$ (which satisfy $E_{i+1} = E_i(\sqrt[p]{a_i})$) we have the exact sequences

$$k_{m-1}E_{i+1} \xrightarrow{N_i^{i+1}} k_{m-1}E_i \xrightarrow{\{a_i\}\cdot -} k_m E_i \xrightarrow{\iota_i^{i+1}} k_m E_{i+1} \ . \tag{3.4}$$

We cannot overstate the important role these exact sequences play in the development of our results.

3.3 Main Results

In the case of cyclic field extensions E/F of degree p, the structure of the module k_mE was determined in [7], where it was shown that the k_mE consists of indecomposables of dimensions 1 and p if $i(E/F) = -\infty$, or dimensions 1, 2 and p if $i(E/F) = 0$. In trying to extend this result to cyclic, prime-power extensions, we remark that the principle difficulty is in using the 'coarse' knowledge of the action of $\mathrm{Gal}(E_n/E_{n-1})$ to determine the 'refined' action of $\mathrm{Gal}(E_n/E_0)$, particularly with respect to the norm map N_{n-1}^n. Here and elsewhere we say that the action of $\mathrm{Gal}(E_n/E_{n-1})$ is coarse because it is given by the action of $(\sigma^{p^{n-1}} - 1) = (\sigma - 1)^{p^{n-1}}$, whereas the action of $\mathrm{Gal}(E/F)$ is more refined because it is given by the action of $(\sigma - 1)$.

One can still formulate results with only knowledge of this coarse action. As an example, the following theorem concerning the structure of k_mE as an $\mathbb{F}_p[G]$-module is developed using only an understanding of the operator $(\sigma^{p^{n-1}} - 1)$ from [7], and so we call it a coarse decomposition. It will be important in running our induction.

Theorem 3.5. *Let E/F be an extension of fields with $Gal(E/F) = \mathbb{Z}/p^n\mathbb{Z}$, where $\xi_p \in E$ and $p > 2$. Let $\chi \in E^\times$ be an element selected according to the paragraph following Equation (3.2). Then as an $\mathbb{F}_p[G]$-module, $k_mE = U \oplus V$, where U is a direct sum of cyclic $\mathbb{F}_p[G]$-submodules of dimension at most $2p^{n-1}$ and V is a a free $\mathbb{F}_p[G]$-submodule.*

Remark 3.6. Under the assumptions above and using the Bloch-Kato conjecture, this result says that

$$H^m(G_E, \mu_p) = U \oplus V$$

as an $\mathbb{F}_p[G]$-module, with U and V having the given module structures.

This theorem implies that as either p or n tends to infinity, the collection of isomorphism classes of indecomposable $\mathbb{F}_p[G]$-modules which can appear as summands in k_mE_n has zero density within the collection of all isomorphism classes of indecomposable $\mathbb{F}_p[G]$-modules. It does not, however, provide much information on the submodule U, as it does not use the additional structure of E as a $\mathbb{Z}/p^n\mathbb{Z}$ extension.

A remedy for this situation is available when $i(E/F) = -\infty$, as the following theorem shows. It is the main result of the chapter.

Theorem 3.7. *Let E/F be an extension of fields with $Gal(E/F) = \mathbb{Z}/p^n\mathbb{Z}$, where $\xi_p \in E$ and $p > 2$ is a prime. Assume additionally that $i(E/F) = -\infty$. Let $\chi \in E^\times$ be an element selected according to the paragraph following Equation (3.2). Then as $\mathbb{F}_p[G]$-modules,*

$$k_mE \simeq X_0 \oplus X_1 \oplus \cdots \oplus X_{n-1} \oplus Y_0 \oplus \cdots \oplus Y_n,$$

where

(i) each X_i and Y_i is a direct sum of cyclic submodules of dimension p^i, with $Y_i \subseteq \iota_i^n(k_mE_i)$ and each $X_i \subseteq \{\chi\} \cdot \iota_i^n(k_{m-1}E_i)$; and

(ii) for every $i \geq 0$, $\iota_0^n(N_0^i(k_mE_i)) = (Y_i \oplus \cdots \oplus Y_n)^G$.

Remark 3.8. Using the Bloch-Kato conjecture, this results says that

$$H^m(G_E, \mu_p) = X_1 \oplus \cdots \oplus X_{n-1} \oplus Y_0 \oplus \cdots \oplus Y_n$$

where the X_i and Y_i have the stated $\mathbb{F}_p[G]$-module structure. In this language condition (i) says $X_i \subseteq (\chi) \cup \mathrm{res}_i^n\left(H^{m-1}(G_{E_i}, \mu_p)\right)$ and (ii) says $\mathrm{res}_0^n\left(\mathrm{cor}_0^i\left(H^m(G_{E_i}, \mu_p)\right)\right) = (Y_i \oplus \cdots \oplus Y_n)^G$. Here res_j^i is the map induced on cohomology by the inclusion $E_j \hookrightarrow E_i$, and cor_j^i is induced by the norm map $N_{E_i/E_j} : E_j \to E_i$.

This result is important for a number of reasons. First, since $i(E_n/E_0) = -\infty$ whenever E_n/E_0 embeds in a cyclic extension E_{n+1}/E_0 with group $\mathbb{Z}/p^{n+1}\mathbb{Z}$, this result will give us the module structure of $k_m E_i$ for any $i \leq n-1$. If an inductive technique is to be used to resolve the general case (i.e., without regard of $i(E/F)$), this will certainly be important. Second, this result will allow us to give the module structure of $k_m E$ when E/F is an extension with group $\mathbb{Z}_p$, again because any finite intermediate extension E_n/F will have $i(E_n/F) = -\infty$.

This theorem has many of the features of Theorem 1.4. First, it restricts the possible isomorphism types that appear in the structure of $k_m E$. It also shows the important role norm subgroups play in the decomposition of these modules. In the case $i(E/F) = -\infty$, the main difference in this decomposition as compared to the structure of $E^\times/E^{\times p}$ from Theorem 1.4 is that that there are more 'exceptional summands' when considering higher cohomology. In this case, the exceptional summands are the submodules X_i.

We shall prove our result by a multiple induction, assuming the structure of $k_{m'} E_i$ is known for all $m' < m$ and $i < n$. We shall also need the 'coarse' decomposition of $k_{m-1} E_n$ provided by Theorem 3.5. Our base cases are given by the known structures of $k_1 E_n$ (Theorem 1.4) and of $k_m E_1$ ([7, Theorem 1]).

Our induction will rely on a submodule $\Gamma(m, n) \subseteq k_{m-1} E_{n-1}$ whose properties we detail in the next section. With this submodule in hand, we show in the subsequent section that elements in the kernel of the map N_{n-1}^n which are fixed by the subgroup H_i actually lie in the image of ι_i^n, and moreover that the fixed parts of such submodules are norms from larger-than-expected intermediate fields. To control those elements which lie outside of N_{n-1}^n we shall also need the module $\Gamma(m, n)$, and we address this problem in the case $i(E/F) = -\infty$ in Section 3.6 (and the case $i(E/F) > -\infty$ in Chapter 5). In the final section of this chapter we bring prove Theorem 3.7 using the developed machinery.

3.4 The Submodule $\Gamma(m,n) \subseteq k_{m-1}E_{n-1}$

We shall see that understanding $\ker(\iota_{n-1}^n)$ and its intersection with $\mathrm{im}(N_{n-1}^n)$ will be essential in developing our results. Exact Sequence (3.4) tells us that

$$\ker(\iota_{n-1}^n) = \{a_{n-1}\} \cdot k_{m-1}E_{n-1},$$

so in this section we describe the structure of this module. Although we shall later focus on the case $i(E/F) = -\infty$, the structure of $\{a_{n-1}\}\cdot k_{m-1}E_{n-1}$ will be determined here without condition on $i(E/F)$. We shall see that this module carries many of the important features of the $\mathbb{F}_p[G]$-module structure from [10], namely that it is 'free' as an $\mathbb{F}_p[G]$-module and stratified according to norm subgroups (Property 1 below).

To investigate $\{a_{n-1}\} \cdot k_{m-1}E_{n-1}$ we find a complement $\Gamma(m,n)$ of $N_{n-1}^n(k_{m-1}E_n)$ in $k_{m-1}E_{n-1}$ (Property 2 below). Since Exact Sequence (3.4) gives

$$N_{n-1}^n(k_{m-1}E_n) = \ker\left(k_{m-1}E_{n-1} \xrightarrow{\{a_{n-1}\cdot -\}} k_mE_{n-1} \right),$$

our submodule $\Gamma(m,n)$ will satisfy $\{a_{n-1}\} \cdot k_{m-1}E_{n-1} = \{a_{n-1}\} \cdot \Gamma(m,n)$ (Property 3 below). Finally, since $a_{n-1}^\sigma = a_{n-1}k^p$ for some $k \in E_{n-1}^\times$ (Equation (3.2)), we have $\Gamma(m,n) \simeq \{a_{n-1}\}\cdot\Gamma(m,n)$ (Property 4 below), and so we have an $\mathbb{F}_p[G]$-isomorphism

$$\Gamma(m,n) \simeq \{a_{n-1}\} \cdot k_{m-1}E_{n-1}$$

as desired.

These results are summarized in the following

Lemma 3.9. *There exists a submodule $\Gamma(m,n) \subset k_{m-1}E_{n-1}$ such that*

1. *$\Gamma(m,n) = \oplus_{i=0}^{n-1}\mathcal{Z}_i$ where each $\mathcal{Z}_i \subset \iota_i^{n-1}(k_{m-1}E_i)$ is a direct sum of free $\mathbb{F}_p[G_i]$ modules, and $\mathcal{Z}_i^G \subset \iota_0^{n-1}\left(N_0^i\left(k_{m-1}E_i\right)\right)$;*
2. *$\Gamma(m,n) \oplus N_{n-1}^n(k_{m-1}E_n) = k_{m-1}E_{n-1}$;*
3. *$\{a_{n-1}\} \cdot k_{m-1}E_{n-1} = \{a_{n-1}\} \cdot \Gamma(m,n)$; and*

4. as $\mathbb{F}_p[G]$-modules, $\Gamma(m,n) \simeq \{a_{n-1}\} \cdot \Gamma(m,n)$ under the map $\gamma \mapsto \{a_{n-1}\} \cdot \gamma$.

Notice that we have already verified Properties 3 and 4 using only Property 2. Hence in proving the result we need only prove that there exists a complement of $N_{n-1}^n(k_{m-1}E_n)$ which is 'free.'

To prove this result, we shall use induction. Once we settle the base case, we resolve the inductive step in several steps. We begin by analyzing elements in $\ker \iota_{n-1}^n \cap \iota_0^{n-1}(k_{m-1}E_0)$, a result which allows us to give a 'nice' decomposition of $k_{m-1}E_{n-1}$ (in particular, we show that $\ker \iota_{n-1}^n$ is a free submodule of $k_{m-1}E_{n-1}$, and is captured as a summand in our 'nice' decomposition). Then we show that $N_{n-1}^n(k_{m-1}E_n)$ is a free submodule of $k_{m-1}E_{n-1}$, and again a summand of our 'nice' decomposition. This allows us to find a complement $\Gamma(m,n)$ of $N_{n-1}^n(k_{m-1}E_n)$ within $k_{m-1}E_{n-1}$ as the remaining summands in our 'nice' decomposition.

We proceed with the proof. For the base case we must verify that there exists a submodule $\Gamma(1,n) \subseteq k_0E_{n-1} = \mathbb{F}_p$ which is a complement of $N_{n-1}^n(k_0E_{n-1}) = \{0\}$ and appropriately free. Naturally, $\Gamma(1,n) = \mathbb{F}_p$ will be our choice. Those who prefer a non-vacuous base case can rest assured that the arguments we give below can be adjusted to prove the existence of a submodule $\Gamma(2,n) \subset k_1E_{n-1}$ with the desired properties.

We now assume by induction the existence of a submodule $\Gamma(m-1,n) \subseteq k_{m-2}E_{n-1}$ which verifies the properties of Lemma 3.9.

Lemma 3.10. *For $\gamma \in \iota_0^{n-1}(k_{m-1}E_0)$ with $\iota_{n-1}^n(\gamma) = 0$, there exists $\alpha \in k_{m-1}E_{n-1}$ so that $\iota_0^{n-1}(N_0^{n-1}(\alpha)) = \gamma$ and $\iota_{n-1}^n(\alpha) = 0$.*

Proof. Since $\gamma \in \ker \iota_{n-1}^n$ we have $\gamma = \{a_{n-1}\} \cdot g$ for some $g \in k_{m-2}E_{n-1}$ by Exact Sequence (3.4). By induction we may take $g \in \Gamma(m-1,n)$ by Lemma 3.9(3). Since $\gamma \in (k_{m-1}E_{n-1})^{G_{n-1}}$, Lemma 3.9(4) gives $g \in \Gamma(m-1,n)^{G_{n-1}}$, and by Lemma 3.9(1) we have $g \in \iota_0^{n-1}(k_{m-2}E_0) \subseteq \iota_{n-2}^{n-1}(k_{m-2}E_{n-2})$. (Here we've used $n \geq 2$.)

Since $\gamma \in \iota_0^{n-1}(k_{m-1}E_0)$ we know $N_{n-2}^{n-1}\gamma = 0$, and because $g = \iota_{n-2}^{n-1}(\hat{g})$ for some $\hat{g} \in k_{m-2}E_{n-2}$ the Projection Formula (3.3) gives

$$0 = N_{n-2}^{n-1}(\gamma) = N_{n-2}^{n-1}(\{a_{n-1}\} \cdot g) = \{a_{n-2}\} \cdot \hat{g}.$$

This means $\hat{g} \in N_{n-2}^{n-1}(k_{m-2}E_{n-1})$ by Exact Sequence (3.4), and therefore $\hat{g}$ is in the image of $(\sigma-1)^{p^{n-1}-p^{n-2}}$. This shows g is the fixed part of a submodule of length at least $p^{n-1}-p^{n-2}+1 > p^{n-2}$. Since $\Gamma(m-1,n)$ is a direct sum of free $\mathbb{F}_p[G_i]$-submodules for $0 \leq i \leq n-1$ by induction, $g = \iota_0^{n-1}\left(N_0^{n-1}(\alpha')\right)$ for some $\alpha' \in k_{m-2}E_{n-1}$. Letting $\alpha = \{a_{n-1}\}\cdot\alpha'$ we have $\iota_{n-1}^n(\alpha) = 0$ and

$$\iota_0^{n-1}(N_0^{n-1}(\alpha)) = (\sigma-1)^{p^{n-1}-1}(\alpha) = (\sigma-1)^{p^{n-1}-1}(\{a_{n-1}\}\cdot\alpha')) = \{a_{n-1}\}\cdot g = \gamma$$

as desired. □

Lemma 3.11. *There exists a module decomposition*

$$k_{m-1}E_{n-1} = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-1}$$

satisfying the conditions of Theorem 3.7, and with the properties

- $\mathcal{X}_i \subseteq \{a_{n-1}\}\cdot k_{m-2}E_{n-1}$ *for each* i*, and*
- $\mathcal{Y}_{n-1} = \mathcal{K} \oplus \mathcal{N} \oplus \hat{\mathcal{Y}}_{n-1}$*, where each of these submodules is free over* $\mathbb{F}_p[G_{n-1}]$*, and so that*
  1. $\mathcal{K} \subseteq \ker \iota_{n-1}^n$ *and*
  2. $\mathcal{N} \subseteq N_{n-1}^n(k_{m-1}E_n)$.

Proof. We shall let our decomposition come from an 'arbitrary' decomposition $\mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-1}$ of $k_{m-1}E_{n-1}$ provided by induction, subject to a few conditions on $\mathcal{X}$ and $\mathcal{Y}$ we are free to impose.

First, since a_{n-1} plays the role of χ for the extension E_{n-1}/F, Theorem 3.7 tells us that $\mathcal{X}_i \subseteq \{a_{n-1}\}\cdot\iota_i^{n-1}(k_{m-1}E_i) \subseteq \{a_{n-1}\}\cdot k_{m-2}E_{n-1}$.

Second, Corollary 3.24 gives us a great deal of freedom in choosing the submodule $\mathcal{Y}_{n-1}$. Specifically we may choose any $\mathbb{F}_p$-basis $\mathcal{I}$ of $\iota_0^{n-1}(N_0^{n-1}(k_{m-1}E_{n-1}))$ and — for every $x \in \mathcal{I}$ — an element $\alpha_x \in k_{m-1}E_{n-1}$ so that $\iota_0^{n-1}(N_0^{n-1}(\alpha_x)) = x$. Then Corollary 3.24 says that $\mathcal{Y}_{n-1}$ can be taken to be $\oplus_{x\in\mathcal{I}}\langle\alpha_x\rangle_{\mathbb{F}_p[G_{n-1}]}$.

We choose our basis $\mathcal{I}$ as the disjoint union of $\mathcal{I}_K, \mathcal{I}_N$ and $\hat{\mathcal{I}}$, where

1. $\mathcal{I}_K$ is a basis for $\ker \iota_{n-1}^n \cap \iota_0^{n-1}(N_0^{n-1}(k_{m-1}E_{n-1}))$;

2. $\mathcal{I}_N$ is a basis for a complement to

$$\ker \iota_{n-1}^n \cap \iota_0^{n-1}(N_0^n(k_{m-1}E_n)) \quad \text{in} \quad \iota_0^{n-1}(N_0^n(k_{m-1}E_n));$$

3. and $\hat{\mathcal{I}}$ is a basis for a complement to $\langle \mathcal{I}_K, \mathcal{I}_N \rangle_{\mathbb{F}_p}$ in $\iota_0^{n-1}(N_0^{n-1}(k_{m-1}E_{n-1}))$.

Lemma 3.10 says that for every $x \in \mathcal{I}_K$ there exists α_x so that $\iota_0^{n-1}(N^{n-1}(\alpha_x)) = x$ and $\alpha_x \in \ker \iota_{n-1}^n$. Hence $\mathcal{K} := \oplus_{x \in \mathcal{I}_K} \langle \alpha_x \rangle_{\mathbb{F}_p[G_{n-1}]}$ will be a free submodule of $\mathcal{Y}_{n-1}$ which is contained in $\ker \iota_{n-1}^n$.

For each $x \in \mathcal{I}_N$, there exists $\beta \in k_{m-1}E_n$ so that $\iota_0^{n-1}(N_0^n(\beta)) = x$, and therefore $\iota_0^{n-1}(N_0^{n-1}(N_{n-1}^n(\beta))) = x$. Hence $\mathcal{N} := \oplus_{x \in \mathcal{I}_N} \langle N_{n-1}^n(\beta) \rangle_{\mathbb{F}_p[G_{n-1}]} \subseteq N_{n-1}^n(k_{m-1}E_n)$ is a free submodule of $\mathcal{Y}_{n-1}$, and independent from $\mathcal{K}$ because $\mathcal{K}^{G_{n-1}} \cap \mathcal{N}^{G_{n-1}} = \langle \mathcal{I}_K \rangle \cap \langle \mathcal{I}_N \rangle = \emptyset$ by construction.

For each $x \in \hat{\mathcal{I}}$ we choose arbitrary $\alpha_x \in k_{m-1}E_{n-1}$ so that $\iota_0^{n-1}(N_0^{n-1}(\alpha_x)) = x$, and we let $\hat{\mathcal{Y}}_{n-1} = \oplus_{x \in \hat{\mathcal{I}}} \langle \alpha_x \rangle_{\mathbb{F}_p[G_{n-1}]}$. By construction $\hat{\mathcal{Y}}_{n-1}^{G_{n-1}}$ is independent from $\langle \mathcal{N}^{G_{n-1}}, \mathcal{K}^{G_{n-1}} \rangle_{\mathbb{F}_p} = \langle \mathcal{I}_N, \mathcal{I}_K \rangle$, and so the Exclusion Lemma 2.8 gives $\mathcal{K} + \mathcal{N} + \hat{\mathcal{Y}}_{n-1} = \mathcal{K} \oplus \mathcal{N} \oplus \hat{\mathcal{Y}}_{n-1}$. □

We will show that the submodule $\Gamma(m,n)$ of Lemma 3.9 is $\mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-2} \oplus \hat{\mathcal{Y}}_{n-1}$. We proceed by determining a complement for $N_{n-1}^n(k_{m-1}E_n)$ in $k_{m-1}E_{n-1}$.

Lemma 3.12. *Using the notation above,*

$$\ker \left(k_{m-1}E_{n-1} \xrightarrow{\iota_{n-1}^n} k_{m-1}E_n \right) = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K}.$$

Proof. We have $\mathcal{X}_i \subseteq \{a_{n-1}\} \cdot k_{m-2}E_{n-1}$ by Lemma 3.11, and hence $\mathcal{X}_i \subseteq \ker \iota_{n-1}^n$ for each i by Exact Sequence (3.4). Lemma 3.11 also gives $\mathcal{K} \subseteq \ker \iota_{n-1}^n$. We complete the proof by showing that

$$\ker(\iota_{n-1}^n) \cap \left(\mathcal{Y}_0 \oplus \mathcal{Y}_{n-2} \oplus \mathcal{N} \oplus \hat{\mathcal{Y}}_{n-1} \right) = \emptyset.$$

To do this we show that the fixed submodule has trivial intersection with $\ker \iota_{n-1}^n$ (after which we can appeal to the Exclusion Lemma 2.8).

First, by construction we have

$$\ker \iota_{n-1}^n \cap \left(\mathcal{N} \oplus \hat{\mathcal{Y}}_{n-1}\right)^{G_{n-1}} = \ker \iota_{n-1}^n \cap \left(\langle \mathcal{I}_N, \hat{\mathcal{I}} \rangle_{\mathbb{F}_p}\right) = \emptyset.$$

So suppose

$$\gamma \in \ker \iota_{n-1}^n \cap \left(\mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-2}\right)^{G_{n-1}}.$$

Since $\left(\mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-2}\right)^{G_{n-1}} \subseteq \iota_0^{n-1}(k_{m-1}E_0)$, we may apply Lemma 3.10 to find an element $\alpha \in k_{m-1}E_{n-1}$ with $\gamma = \iota_0^{n-1}(N_0^{n-1}(k_{m-1}E_{n-1}))$. This implies $\gamma \in \mathcal{Y}_{n-1}$ by Theorem 3.7(ii), a contradiction. □

Lemma 3.13. *Using the notation above,*

$$N_{n-1}^n(k_{m-1}E_n) = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \oplus \mathcal{N}.$$

Proof. An element $\gamma \in \ker \iota_{n-1}^n$ takes the form $\gamma = \{a_{n-1}\} \cdot g$ by Exact Sequence (3.4), and so $N_{n-1}^n(\{\chi\} \cdot \iota_{n-1}^n(g)) = \{a_{n-1}\} \cdot g$ by the Projection Formula (3.3). This implies

$$\ker \iota_{n-1}^n = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \subseteq N_{n-1}^n(k_{m-1}E_n).$$

Of course $\mathcal{N}$ is constructed so that $\mathcal{N} \subseteq N_{n-1}^n(k_{m-1}E_n)$, and so we have

$$N_{n-1}^n(k_{m-1}E_n) \supseteq \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \oplus \mathcal{N}.$$

For the containment $N_{n-1}^n(k_{m-1}E_n) \subseteq \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \oplus \mathcal{N}$, we show that

$$N_{n-1}^n(k_{m-1}E_n)^{G_{n-1}} \subseteq \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \oplus \mathcal{N}$$

after which we can apply the Exclusion Lemma 2.8 to complete the proof.

Let γ be an element in $N_{n-1}^n(k_{m-1}E_n)^{G_{n-1}}$, say $\gamma = N_{n-1}^n(\alpha)$ for some $\alpha \in k_{m-1}E_n$. If $\iota_{n-1}^n(\gamma) = 0$ then $\gamma \in \ker \iota_{n-1}^n = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K}$, and we are done. Otherwise $\gamma \notin \ker \iota_{n-1}^n$, and so $\iota_{n-1}^n(\gamma) = \iota_{n-1}^n(N_{n-1}^n(\alpha)) \neq 0$. Since $\iota_{n-1}^n \circ N_{n-1}^n$ is represented

by the polynomial

$$\sigma^{p^{n-1}} + \cdots + \sigma^{p^{n-1}(p-1)} \equiv (\sigma - 1)^{p^n - p^{n-1}},$$

this implies that $\ell(\alpha) > p^n - p^{n-1} \geq 2p^{n-1}$. (Here we've used $p > 2$.) Now our coarse decomposition of $k_{m-1}E_n$ in Theorem 3.5 implies $\iota_{n-1}^n(\gamma)$ is the fixed part of a submodule of dimension p^n; i.e., $\iota_{n-1}^n(\gamma) = \iota_0^n(N_0^n(\beta))$ for some $\beta \in k_{m-1}E_n$.

This last equation is an equation within $k_{m-1}E_n$, and so we translate to an equation in $k_{m-1}E_{n-1}$. To do this, notice that as elements in $K_{m-1}E_n$ the previous equation becomes

$$\iota_{n-1}^n(\gamma) = \iota_0^n(N_0^n(\beta)) + f \quad \text{for some} \quad f \in pK_{m-1}E_n.$$

After solving the equation for f, we see that $f = \iota_{n-1}^n(\hat{f})$ for some $\hat{f} \in K_{m-1}E_n$. Furthermore, since f is 0 in $k_{m-1}E_n$, this implies $\hat{f} \in \ker \iota_{n-1}^n$. Hence we have

$$\gamma \in \iota_0^{n-1}(N_0^n(k_{m-1}E_n)) + \ker \iota_{n-1}^n.$$

Recall, however, that $\mathcal{N}^{G_{n-1}} = \langle \mathcal{I}_N \rangle_{\mathbb{F}_p}$ was chosen as a complement to $\ker \iota_{n-1}^n \cap \iota_0^{n-1}(N_0^n(k_{m-1}E_n)) \subseteq \langle \mathcal{I}_K \rangle_{\mathbb{F}_p}$ in $\iota_0^{n-1}(N_0^n(k_{m-1}E_n))$. Hence we have $\langle \mathcal{I}_K, \mathcal{I}_N \rangle_{\mathbb{F}_p} \supseteq \iota_0^{n-1}(N_0^n(k_{m-1}E_n))$, and so

$$\gamma \in \langle \mathcal{I}_K, \mathcal{I}_N \rangle_{\mathbb{F}_p} + \ker \iota_{n-1}^n \subseteq \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{K} \oplus \mathcal{N}.$$

□

Proof of Lemma 3.9. For each $0 \leq i < n-1$ define $\mathcal{Z}_i := \mathcal{Y}_i$, and define $\mathcal{Z}_{n-1} := \hat{\mathcal{Y}}_{n-1}$. We define $\Gamma(m,n) := \mathcal{Z}_0 \oplus \cdots \oplus \mathcal{Z}_{n-1}$. The previous lemmas show that $\Gamma(m,n)$ satisfies (1) and (2), and we have already verified that Properties (3) and (4) follow from (2). □

We record the following corollary, since it will be useful later.

Corollary 3.14. *If $g \in \Gamma(m,n)^{G_{n-1}}$ and $N_{n-2}^{n-1}(\{a_{n-1}\} \cdot g) = 0$, then for some $\alpha \in \Gamma(m,n)$ we have $g = \iota_0^{n-1}(N_0^{n-1}(\alpha))$.*

Proof. Since $\Gamma(m,n)^{G_{n-1}} \subseteq \iota_0^{n-1}(k_{m-1}E_0)$, it follows that $g = \iota_{n-2}^{n-1}(\hat{g})$ for some $\hat{g}$ in $k_{m-1}E_{n-2}$. (Here we have used $n \geq 2$.) Hence $N_{n-2}^{n-1}(\{a_{n-1}\} \cdot g) = \{a_{n-2}\} \cdot \hat{g}$ by the Projection Formula (3.3), which — by Exact Sequence (3.4) — is 0 only if $\hat{g} \in N_{n-2}^{n-1}(k_{m-1}E_{n-1})$, say $\hat{g} = N_{n-2}^{n-1}(\alpha')$. But then $\ell_{G_{n-1}}(\alpha') > p^{n-1} - p^{n-2} \geq p^{n-2}$, and since $\Gamma(m,n)$ is a direct sum of cyclic submodules of dimensions p^i for $0 \leq i \leq n-1$, we must have $\hat{g} \in \mathrm{im}(\sigma - 1)^{p^{n-1}-1}$. Hence $g \in \mathcal{Z}_{n-1}^{G_{n-1}}$. The result now follows from Lemma 3.9(1). □

3.5 Fixed Elements are Norms

The key result of this section is Corollary 3.20. This result uses Hilbert 90-like results and facts about abstract $\mathbb{F}_p[G]$-modules, though in our setting we need to be careful about the possible difference in length between the $\mathbb{F}_p[G_i]$-submodule generated by an element $\gamma \in k_m E_i$ and the $\mathbb{F}_p[G_n]$-submodule generated by $\iota_i^n(\gamma)$.

Towards this end, we give results for determining when an element lies in the submodule $\mathrm{im}(\iota_j^n)$ and — when it does — for controlling the $\mathbb{F}_p[G_j]$-lengths of representatives from $k_m E_j$ for this element.

Lemma 3.15. *If $N_{n-1}^n \gamma = 0$ and $\gamma \in (k_m E_n)^{H_{n-1}}$, then there exists $\hat{\gamma} \in k_m E_{n-1}$ such that $\iota_{n-1}^n(\hat{\gamma}) = \gamma$ and $\ell_{G_{n-1}}(\hat{\gamma}) = \ell_G(\gamma)$. Additionally, if $\ell_G(\gamma) \leq p^{n-1} - p^{n-2}$ we may insist $N_{n-2}^{n-1}\hat{\gamma} = 0$.*

Proof. We know that $\gamma = \iota_{n-1}^n \hat{\gamma}$ for some $\hat{\gamma} \in k_m E_{n-1}$ by Theorem 1 and Remarks 1 and 2 (page 6) of [7]. We now argue that $\hat{\gamma}$ may be taken so that $\ell_{G_{n-1}}(\hat{\gamma}) = \ell_G(\gamma)$. We cannot have $\ell_{G_{n-1}}(\hat{\gamma}) < \ell_G(\gamma)$, since if $(\sigma - 1)^x \hat{\gamma} = 0 \in k_m E_{n-1}$ then

$$(\sigma - 1)^x \gamma = (\sigma - 1)^x \iota_{n-1}^n(\hat{\gamma}) = \iota_{n-1}^n\left((\sigma - 1)^x(\hat{\gamma})\right) = 0.$$

So suppose that $\ell := \ell_{G_{n-1}}(\hat{\gamma}) > \ell_G(\gamma)$. Our goal is to use Corollary 3.14 to adjust $\hat{\gamma}$ by an element $\{a_{n-1}\} \cdot \alpha \in k_m E_{n-1}$ in order to produce an element of smaller length whose image under inclusion is γ. For this we shall study $f := (\sigma - 1)^{\ell - 1}\hat{\gamma}$.

First, by induction we know $k_m E_{n-1} = \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-2} \oplus \mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-1}$, where by Theorem 3.7 we have $\mathcal{X}_i \subseteq \{a_{n-1}\} \cdot \iota_i^{n-1}(k_{m-1}E_i) \subseteq \ker \iota_{n-1}^n$. Hence we may take

$\hat{\gamma} \in \mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-1}$. Since $f := (\sigma-1)^{\ell-1}\hat{\gamma} \in (\mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_{n-1})^{G_{n-1}}$, Theorem 5.2(iii) gives $f \in \iota_0^{n-1}(k_m E_0)$. Since $n \geq 2$, we have

$$N_{n-2}^{n-1}(f) = 0. \tag{3.16}$$

On the other hand, Exact Sequence (3.4) and Lemma 3.9(3) give $f = \{a_{n-1}\} \cdot \iota_{n-1}^n(g)$ for some $g \in \Gamma(m,n)$. Lemma 3.9(4) gives $g \in \Gamma(m,n)^{G_{n-1}}$, so by Lemma 3.9(1) we have $g = \iota_0^{n-1}(\hat{g})$ for some $\hat{g} \in k_m E_0$. Using Equation 3.16, $n \geq 2$, and the Projection Formula (3.3), we have

$$0 = N_{n-2}^{n-1} f = N_{n-2}^{n-1}\left(\{a_{n-1}\} \cdot \iota_0^{n-1}(\hat{g})\right) = \{a_{n-2}\} \cdot \iota_0^{n-2}(\hat{g}).$$

Corollary 3.14 gives $g = \iota_0^{n-1}(N_0^{n-1}(\alpha))$ for some $\alpha \in \Gamma(m,n)$. Since $\{a_{n-1}\} \cdot \alpha$ satisfies $\ell_{G_{n-1}}(\{a_{n-1}\} \cdot \alpha) = p^{n-1}$ by Lemma 3.9(4), and since additionally $\iota_{n-1}^n(\{a_{n-1}\} \cdot \alpha) = 0$, we see that $\hat{\gamma}' := \hat{\gamma} - (\sigma-1)^{p^{n-1}-\ell_{G_{n-1}}(\hat{\gamma})}(\{a_{n-1}\} \cdot \alpha)$ satisfies $\iota_{n-1}^n(\hat{\gamma}') = \gamma$ and $\ell_{G_{n-1}}(\hat{\gamma}') < \ell_{G_{n-1}}(\hat{\gamma})$. Using induction, we continue this process until we have constructed an element $\hat{\gamma}$ so that $\iota_{n-1}^n(\hat{\gamma}) = \gamma$ and $\ell_{G_{n-1}}(\hat{\gamma}) = \ell_G(\gamma)$.

All we have left is to show that if $\ell_G(\gamma) \leq p^{n-1} - p^{n-2}$, then we may insist $N_{n-2}^{n-1}\hat{\gamma} = 0$. For this, since $\ell_{G_{n-1}}(\hat{\gamma}) \leq p^{n-1} - p^{n-2}$ we have $\iota_{n-2}^{n-1}(N_{n-2}^{n-1}(\hat{\gamma})) = 0$, so $N_{n-2}^{n-1}\hat{\gamma} = \{a_{n-2}\} \cdot g$ for some $g \in \Gamma(m, n-1) \subseteq k_{m-1}E_{n-2}$. We claim that $\hat{\gamma}' := \hat{\gamma} - \{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)$ has the desired properties: $\iota_{n-1}^n\hat{\gamma}' = \gamma$, $\ell_{G_{n-1}}(\hat{\gamma}') = \ell_G(\gamma)$, and $N_{n-2}^{n-1}\hat{\gamma}' = 0$.

To prove the claim, notice first that $\iota_{n-1}^n\left(\{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)\right) = 0$ by Exact Sequence (3.4), and hence $\iota_{n-1}^n(\hat{\gamma}') = \gamma$. It is also obvious that $N_{n-2}^{n-1}\left(\{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)\right) = \{a_{n-2}\} \cdot g$ by the Projection Formula (3.3) and $n \geq 2$, and hence $N_{n-2}^{n-1}(\hat{\gamma}') = 0$.

For the length condition, notice first that $\ell_{G_{n-1}}(\{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)) = \ell_{G_{n-2}}(g)$ by Lemma 3.9(4) applied to $\Gamma(m, n-1)$. Hence if $x < \ell_{G_{n-2}}(g)$, then

$$N_{n-1}^n\left((\sigma-1)^x(\hat{\gamma})\right) = (\sigma-1)^x\left(\{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)\right) \neq 0,$$

and in particular we have $(\sigma-1)^x\hat{\gamma} \neq 0$. This gives

$$\ell(\hat{\gamma}) \geq \ell_{G_{n-2}}(g) = \ell_{G_{n-1}}(\{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)),$$

and so $\hat{\gamma} - \{a_{n-1}\} \cdot \iota_{n-2}^{n-1}(g)$ satisfies $\ell_{G_{n-1}}(\hat{\gamma}) = \ell_G(\gamma)$ as desired. □

Lemma 3.17. *If $N_{n-1}^n\gamma = 0$ and $\gamma \in (k_mE_n)^{H_i}$, then there exists $\hat{\gamma} \in k_mE_i$ such that $\iota_i^n(\hat{\gamma}) = \gamma$ and $\ell_{G_i}(\hat{\gamma}) = \ell_G(\gamma)$. Additionally, if $\ell_G(\gamma) \leq p^i - p^{i-1}$ we may insist $N_{i-1}^i\hat{\gamma} = 0$.*

Proof. The base case of this result is the previous lemma.

For the inductive step, let $\gamma \in (k_mE_n)^{H_i}$ with $N_{n-1}^n\gamma = 0$, and suppose we have the result for $i+1$. Since $(k_mE_n)^{H_i} \subset (k_mE_n)^{H_{i+1}}$, there exists $\tilde{\gamma} \in k_mE_{i+1}$ such that $\iota_{i+1}^n\tilde{\gamma} = \gamma$ and $\ell_{G_{i+1}}(\tilde{\gamma}) = \ell_G(\gamma)$. Furthermore, since $\ell_G(\gamma) \leq p^i \leq p^{i+1} - p^i$ we may insist $N_{i+1,i}\tilde{\gamma} = 0$. Hence by induction there exists $\hat{\gamma} \in k_mE_i$ such that $\ell_{G_i}(\hat{\gamma}) = \ell_{G_{i+1}}(\tilde{\gamma})$, $\iota_i^{i+1}\hat{\gamma} = \tilde{\gamma}$, and so that if $\ell_{G_i}(\hat{\gamma}) \leq p^i - p^{i-1}$ then we may assume $N_{i-1}^i\hat{\gamma} = 0$. But then we also have $\ell_{G_i}(\hat{\gamma}) = \ell_G(\gamma)$ and $i_i^n\hat{\gamma} = \gamma$ as desired. □

We are now ready for the main theorem of the section. We shall state it in some generality and then restrict ourselves to a special case in the subsequent corollary.

Lemma 3.18. *For $\gamma \in k_mE_n$, if*

- *$N_{n-1}^n(\gamma) = 0$, and $\ell_{H_j}(\gamma) > p^{n-j-1}$;*
- *$i(E_n/E_j) = -\infty$ and $\ell_{H_j}(\gamma) > p^{n-j-1}$; or*
- *$\ell_{H_j}(\gamma) > 2p^{n-j-1}$,*

then $(\sigma^{p^j}-1)^{\ell_{H_j}(\gamma)-1}\gamma \in \iota_j^n(N_j^n(k_mE_n))$.

Proof. To prove the claim we proceed by induction on j. The base case is $j = n-1$ which follows from the decomposition provided by [7], together with the observation that there are no X summands of dimension 2 when $i(E_n/E_0) = -\infty$.

So suppose the result holds for $j+1$, and we show it also holds for j. For simplicity we let $\varepsilon = 1$ if either $i(E_n/E_0) = -\infty$ or $N_{n-1}^n(\gamma) = 0$, and let $\varepsilon = 2$

if both $N^n_{n-1}(\gamma) \neq 0$ and $i(E_n/E_0) \neq -\infty$. Since $\ell_{H_j}(\gamma) > \varepsilon p^{n-1-j}$, without loss we may assume $\ell_{H_j}(\gamma) = \varepsilon p^{n-1-j} + 1$. This means $(\sigma^{p^j} - 1)^{\varepsilon p^{n-1-j}+1}\gamma = 0$ and $(\sigma^{p^j} - 1)^{\varepsilon p^{n-1-j}}\gamma \neq 0$. This gives

$$(\sigma^{p^{j+1}} - 1)^{\varepsilon p^{n-1-j-1}+1}\gamma = (\sigma^{p^j} - 1)^{\varepsilon p^{n-j-1}+p}\gamma = 0 \qquad \text{and}$$
$$(\sigma^{p^{j+1}} - 1)^{\varepsilon p^{n-1-j-1}}\gamma = (\sigma^{p^j} - 1)^{\varepsilon p^{n-j-1}}\gamma \neq 0.$$

Hence we have $\ell_{H_{j+1}}(\gamma) = \varepsilon p^{n-1-j-1} + 1$, and so by induction it follows that

$$(\sigma^{p^{j+1}} - 1)^{\varepsilon p^{n-1-j-1}}\gamma = \iota^n_{j+1}(N^n_{j+1}(\alpha))$$

for some $\alpha \in k_m E_n$, or equivalently

$$(\sigma^{p^j} - 1)^{\varepsilon p^{n-1-j}}\gamma = (\sigma^{p^j} - 1)^{p^{n-j}-p}\alpha. \tag{3.19}$$

Unfortunately, α does not generate a submodule long enough to provide our desired equality. Instead of being length $p^{n-j} - 1$ we have $\ell_{H_j}(\alpha) = p^{n-j} - p + 1$:

$$(\sigma^{p^j} - 1)^{p^{n-j}-p}\alpha = (\sigma^{p^{j+1}} - 1)^{p^{n-j-1}-1}\alpha = \iota^n_j(N^n_j\alpha) = (\sigma^{p^j} - 1)^{\varepsilon p^{n-1-j}}\gamma \neq 0 \quad \text{and}$$
$$(\sigma^{p^j} - 1)^{p^{n-j}-p+1}\alpha = (\sigma^{p^j} - 1)(\sigma^{p^j} - 1)^{p^{n-j}-p}\alpha = (\sigma^{p^j} - 1)\iota^n_j(N^n_j(\alpha)) = 0.$$

We use induction to show that the H_{j+1}-fixed submodule of $(\sigma^{p^j} - 1)\alpha$ is generated by some $\iota^n_{j+1}(N^n_{j+1}(\beta))$, which will ultimately provide the desired result. With this goal in mind, we compute $\ell_{H_{j+1}}\Big((\sigma^{p^j} - 1)\alpha\Big) = p^{n-j-1} - 1$. First, we have

$$(\sigma^{p^{j+1}} - 1)^{p^{n-j-1}-2}(\sigma^{p^j} - 1)\alpha = (\sigma^{p^j} - 1)^{p^{n-j}-2p+1}\alpha \neq 0,$$

where the inequality follows from the fact that $\ell_{H_j}(\alpha) = p^{n-j} - p + 1 > p^{n-j} - 2p + 1$. We also have

$$(\sigma^{p^{j+1}} - 1)^{p^{n-j-1}-1}(\sigma^{p^j} - 1)\alpha = (\sigma^{p^j} - 1)^{p^{n-j}-p+1}\alpha = 0$$

(again using $\ell_{H_j}(\alpha) = p^{n-j} - p + 1$). Hence we have $\ell_{H_{j+1}}\left((\sigma^{p^j} - 1)\alpha\right) = p^{n-j-1} - 1$.

Now $p^{n-j-1} - 1 > 2p^{n-1-j-1}$ since $p > 2$, so by induction we have

$$(\sigma^{p^{j+1}} - 1)^{p^{n-j-1}-2}(\sigma^{p^j} - 1)\alpha = \iota_{j+1}^n(N_{j+1}^n(\beta)) = (\sigma^{p^{j+1}} - 1)^{p^{n-j-1}-1}\beta$$

for some $\beta \in k_m E_{j+1}$. Equivalently, this means

$$(\sigma^{p^j} - 1)^{p^{n-j}-2p}(\sigma^{p^j} - 1)\alpha = (\sigma^{p^j} - 1)^{p^{n-j}-p}\beta.$$

Hence, recalling Equation (3.19) for equality $\star$ below, we have the desired result:

$$\begin{aligned}
\iota_j^n(N_j^n(\beta)) &= (\sigma^{p^j} - 1)^{p^{n-j}-1}\beta \\
&= (\sigma^{p^j} - 1)^{p-1}(\sigma^{p^j} - 1)^{p^{n-j}-p}\beta \\
&= (\sigma^{p^j} - 1)^{p-1}(\sigma^{p^j} - 1)^{p^{n-j}-2p}(\sigma^{p^j} - 1)\alpha \\
&= (\sigma^{p^j} - 1)^{p^{n-j}-p}\alpha \\
&\overset{\star}{=} (\sigma^{p^j} - 1)^{\varepsilon p^{n-1-j}}\gamma.
\end{aligned}$$

□

Corollary 3.20. *For $\gamma \in k_m E_n$, let i be minimal such that $\gamma \in \iota_i^n(k_m E_i)$. If $N_{n-1}^n(\gamma) = 0$ and $\ell_G(\gamma) > p^{i-1}$, then $(\sigma - 1)^{\ell_G(\gamma)-1} \in \iota_0^n(N_0^i(k_m E_i(\gamma)))$.*

Note: When $i < n$, the condition $N_{n-1}^n(\gamma) = 0$ is trivial.

Proof. In the case $i = n$, the result follows by taking $j = 0$ in the previous lemma. For $i < n$, choose $\hat{\gamma} \in k_m E_i$ with $\iota_i^n(\hat{\gamma}) = \gamma$; by Lemma 3.17 we can (and do) insist $\ell_{G_i}(\hat{\gamma}) = \ell_G(\gamma)$. Then $\ell_{G_i}(\hat{\gamma}) > p^{i-1}$, and since $i(E_i/F) = -\infty$ the previous lemma (applied to the extension E_i/F) gives

$$(\sigma - 1)^{\ell_{G_i}(\hat{\gamma})-1}\hat{\gamma} \in \iota_0^i(N_0^i(k_m E_i))$$

(again by taking $j = 0$). Therefore

$$(\sigma-1)^{\ell_G(\gamma)-1}\gamma = \iota_i^n\left((\sigma-1)^{\ell_{G_i}(\hat{\gamma})-1}\hat{\gamma}\right) \subset \iota_i^n\left(\iota_0^i\left(N_0^i\left(k_m E_i\right)\right)\right)$$
$$\subset \iota_0^n(N_0^i(k_m E_i))$$

as desired. □

We are now ready to give a proof that the module structure of [7] can be used to give a 'coarse' understanding of the $\mathbb{F}_p[G]$-structure of $k_m E$.

Proof of Theorem 3.5. Using the notation and results from the proof of Theorem 2.9, we only need to verify that $V_{i+1} = V_{p^n}$ for every i satisfying $2p^{n-1} + 1 \leq i \leq p^n - 1$.

This means that we must show that for any $x \in \mathrm{im}(\sigma-1)^{i-1}$, we also have $x \in \mathrm{im}(\sigma-1)^{p^n-1}$. Choose an α_x with $(\sigma-1)^{i-1}\alpha_x = x$. Then $\ell_G(\alpha_x) = i$, and since $i > 2p^{n-1}$ we may apply Lemma 3.18 (with $j = 0$) to conclude that

$$x = (\sigma-1)^{i-1}\alpha_x = \iota_0^n(N_0^n(\alpha)) = (\sigma-1)^{p^n-1}\alpha$$

for some $\alpha \in k_m E$. But this means that $x \in V_{p^n}$ as desired.

□

3.6 The Exceptional Summand

In the previous section we saw that elements in $\ker N_{n-1}^n$ are particularly well-behaved: they have representatives from 'expected' intermediate fields, and their fixed submodules are generated by elements that lie in *a priori* unexpected norm subgroups (because within $\ker N_{n-1}^n$ we have $\mathrm{im}(\sigma-1)^{p^i+k} = \mathrm{im}(\sigma-1)^{p^{i+1}} = \mathrm{im}(\iota_0^n \circ N_0^i)$ for $k \geq 1$). We also saw that elements outside of $\ker N_{n-1}^n$ which are sufficiently long also share these characteristics. Hence we have left to understand those elements of small length which are outside $\ker N_{n-1}^n$, which in practice will mean that we need to have control over the elements in $\ker(\iota_{n-1}^n \circ N_{n-1}^n) \setminus \ker N_{n-1}^n$.

We make this notion more precise. Exact Sequence (3.4) gives $\ker \iota_{n-1}^n = \{a_{n-1}\} \cdot k_{m-1}E_n$, which by the results of Section 3.4 is the same as $\{a_{n-1}\} \cdot \Gamma(m,n)$. If

$\alpha \in \ker \iota^n_{n-1} \circ N^n_{n-1}$ is given, then $N^n_{n-1}(\alpha) = \{a_{n-1}\} \cdot \gamma$ for some $\gamma \in \Gamma(m,n)$. Our goal is to find an element $\mathfrak{g}$ so that $\ell(\mathfrak{g}) \leq \ell(\alpha)$ and $N^n_{n-1}(\mathfrak{g}) = \{a_{n-1}\} \cdot \gamma$. If we can do this, then the element $\alpha - \mathfrak{g}$ is trivial under the map N^n_{n-1} (so we are then free to use the results from the previous section) and does not increase in length (so that induction arguments are not disturbed). In the case that $i(E/F) = -\infty$, this is particularly easy to do.

Lemma 3.21. *Suppose $i(E/F) = -\infty$. Then*

$$X := \{\chi\} \cdot \iota^n_{n-1}(\Gamma(m,n)) \xrightarrow{N^n_{n-1}} \{a_{n-1}\} \cdot \Gamma(m,n)$$

is an isomorphism of $\mathbb{F}_p[G]$-modules. In particular, X is a direct sum of cyclic submodules of dimension p^i for $0 \leq i \leq n-1$.

Proof. The Projection Formula (3.3) ensures that $N^n_{n-1}(X) = \{a_{n-1}\} \cdot \Gamma(m,n)$, and the construction of $\Gamma(m,n)$ implies $N^n_{n-1}(\{\chi\} \cdot \iota^n_{n-1}(\gamma)) = \{a_{n-1}\} \cdot \gamma = 0$ only when $\gamma = 0$. Hence we have left to show that the isomorphism respects the $\mathbb{F}_p[G]$-action (where the $\mathbb{F}_p[G]$-action on $\{a_{n-1}\} \cdot \Gamma(m,n) \subseteq k_m E_{n-1}$ is given by reducing to the natural action of $\mathbb{F}_p[G_{n-1}]$). The multiplicative properties of N^n_{n-1} imply that we only need to verify that the action of σ is respected. For this, we recall that $i(E/F) = -\infty$ implies $\ell(\chi) = 1$, so that $\sigma\chi \equiv \chi$ in $E^\times/E^{\times p}$. Hence

$$\sigma\left(\{\chi\} \cdot \iota^n_{n-1}(\gamma)\right) = \{\sigma\chi\} \cdot \iota^n_{n-1}(\sigma(\gamma)) = \{\chi\} \cdot \iota^n_{n-1}(\sigma(\gamma)).$$

The Projection Formula (3.3) gives

$$N^n_{n-1}\left(\sigma\left(\{\chi\} \cdot \iota^n_{n-1}(\gamma)\right)\right) = N^n_{n-1}\left(\{\chi\} \cdot \iota^n_{n-1}(\sigma\gamma)\right) = \{a_{n-1}\} \cdot (\sigma\gamma).$$

□

Theorem 3.22. *Suppose $i(E/F) = -\infty$. If $N^n_{n-1}(\alpha) = \{a_{n-1}\} \cdot \gamma$ for $\gamma \in \Gamma(m,n)$, then $\ell(\alpha) \geq \ell_{G_{n-1}}(\gamma) = \ell(\{\chi\} \cdot \iota^n_{n-1}(\gamma))$.*

Proof. The equality is given by the previous theorem, so we only verify the inequality.

For this, suppose that $x < \ell_{G_{n-1}}(\gamma)$. Then by Lemma 3.9(4) we have

$$N_{n-1}^n\left((\sigma-1)^x\alpha\right) = (\sigma-1)^x\left(\{a_{n-1}\}\cdot\gamma\right) \neq 0,$$

and hence $(\sigma-1)^x\alpha \neq 0$. This gives the desired result. □

3.7 Proof of Theorem 3.7

Proof of Theorem 3.7. Let $X = \{\chi\}\cdot\iota_{n-1}^n(\Gamma(m,n))$. Then $X = X_0 \oplus \cdots \oplus X_{n-1}$ for $X_i = \{\chi\}\cdot\iota_{n-1}^n(\mathcal{Z}_i) \subseteq \{\chi\}\cdot\iota_i^n(k_mE_i)$. We now construct the submodules Y_i of the theorem.

To form Y_n, choose an $\mathbb{F}_p$-basis $\mathcal{I}_n$ of the space $\iota_0^n\left(N_0^n(k_mE_n)\right)$. For each $x \in \mathcal{I}_n$ there exists $\alpha_x \in k_mE_n$ with $x = \iota_0^n\left(N_0^n(\alpha_x)\right)$, and the $\mathbb{F}_p[G]$-submodule generated by α_x is free since $\ell_G(\alpha_x) = p^n$. We let $Y_n = \sum_{x\in\mathcal{I}_n}\langle\alpha_x\rangle_{\mathbb{F}_p[G]}$, and by the Exclusion Lemma 2.8 we see $Y_n = \bigoplus_{x\in\mathcal{I}_n}\langle\alpha_x\rangle_{\mathbb{F}_p[G]}$.

Now we define Y_i for $0 \leq i < n$. Select a complement of $\iota_0^n\left(N_0^{i+1}(k_mE_{i+1})\right)$ in $\iota_0^n\left(N_0^i(k_mE_i)\right)$, and let $\mathcal{I}_i$ be an $\mathbb{F}_p$-basis for this complement. For each $x \in \mathcal{I}_i$ there exists $\alpha_x \in k_mE_i$ with $x = \iota_0^n\left(N_0^i(\alpha_x)\right)$. The $\mathbb{F}_p[G]$-submodule generated by α_x is isomorphic to $\mathbb{F}_p[G_i]$ since $\ell_G(\alpha_x) = p^i$ and $\alpha_x \in k_mE_i$, and the Exclusion Lemma 2.8 shows $\sum_{x\in\mathcal{I}_i}\langle\alpha_x\rangle_{\mathbb{F}_p[G]} = \oplus_{x\in\mathcal{I}_i}\langle\alpha_x\rangle_{\mathbb{F}_p[G]}$. We define Y_i to be this submodule.

The submodules Y_i are independent from each other using an analogous argument: any dependence among these modules gives rise to a non-trivial dependence in Y_i^G, but there are no such dependencies by construction of the Y_i. Furthermore we have

$$(Y_i \oplus \cdots \oplus Y_n)^G = \iota_0^n(N_0^i(k_mE_i)). \tag{3.23}$$

This verifies the second condition of Theorem 3.7.

To show that X is independent from $\oplus Y_i$, again the Exclusion Lemma 2.8 implies that any non-trivial dependence between X and $\oplus Y_i$ must appear as a non-trivial dependence between X^G and $\oplus_i Y_i^G$. Now any (non-trivial) element in X has non-trivial image under N_{n-1}^n, whereas $\oplus_i Y_i^G \subseteq \iota_0^n(k_mE_0) \subseteq \ker N_{n-1}^n$. Hence $X + \oplus_i Y_i = X \oplus \oplus_i Y_i$.

For $J := X \oplus \oplus_i Y_i$, we now show $k_m E_n = J$ by induction on submodule length. We prove first that for any $\gamma \in k_m E_n$ with $\ell_G(\gamma) \leq p^n - p^{n-1}$ there exists $\gamma' \in k_m E_n$ with $N^n_{n-1}\gamma' = 0$, $\ell_G(\gamma') \leq \ell_G(\gamma)$, and such that $\gamma' \in J$ implies $\gamma \in J$. To see this, suppose $N^n_{n-1}\gamma \neq 0$ (since otherwise the result is trivial). Now $\iota^n_{n-1}(N^n_{n-1}(\gamma)) = 0$ since $\ell_G(\gamma) \leq p^n - p^{n-1}$, so that $N^n_{n-1}(\gamma) = \{a_{n-1}\} \cdot g$ for some $g \in k_{m-1}E_{n-1}$ by Exact Sequence (3.4); as usual, we take $g \in \Gamma(m, n)$ by Lemma 3.9(3). By construction $\{\chi\} \cdot \iota^n_{n-1}(g) \in X$, and this element satisfies $N^n_{n-1}(\{\chi\} \cdot \iota^n_{n-1}(g)) = \{a_{n-1}\} \cdot g$ by the Projection Formula (3.3) and has $\ell_G(\{\chi\} \cdot \iota^n_{n-1}(g)) \leq \ell_G(\gamma)$ by Lemma 3.22. Hence $\gamma' = \gamma - \{\chi\} \cdot \iota^n_{n-1}(g)$ has $N^n_{n-1}\gamma' = 0$ and $\ell_G(\gamma') \leq \ell_G(\gamma)$. Finally, since $\{\chi\} \cdot \iota^n_{n-1}(g) \in J$ by construction, we have $\gamma' \in J$ implies $\gamma \in J$ as desired. Hence for $\ell_G(\gamma) \leq p^n - p^{n-1}$, we shall assume that $N^n_{n-1}(\gamma) = 0$.

Now suppose $\ell_G(\gamma) = 1$. Since we assume $N^n_{n-1}(\gamma) = 0$, Lemma 3.17 gives $\gamma = \iota^n_0(f)$ for some $f \in k_m F$. Equation (3.23) with $i = 0$ gives $\gamma \in (Y_0 \oplus \cdots \oplus Y_n)^G \subseteq J$.

Suppose $\gamma \in k_m E$ with $\ell_G(\gamma) \leq p^n - p^{n-1}$, and assume J contains all elements of length at most $\ell_G(\gamma) - 1$. Choose i such that $p^{i-1} < \ell_G(\gamma) \leq p^i$. Lemma 3.17 gives $\gamma = \iota^n_i(\hat{\gamma})$ for some $\hat{\gamma} \in k_m E_i$, and by Corollary 3.20 we know $(\sigma - 1)^{\ell_G(\gamma)-1}\gamma \in \iota^n_0(N^i_0(k_m E_i))$. Equation (3.23) provides $\alpha \in J$ such that $(\sigma - 1)^{\ell_G(\gamma)-1}\gamma = (\sigma - 1)^{p^i-1}\alpha$. Hence we have $\ell_G\left(\gamma - (\sigma - 1)^{p^i - \ell_G(\gamma)}\alpha\right) \leq \ell_G(\gamma) - 1$ since

$$(\sigma - 1)^{\ell_G(\gamma)-1}\left(\gamma - (\sigma - 1)^{p^i - \ell_G(\gamma)}\alpha\right) = 0,$$

and by induction $\gamma - (\sigma - 1)^{p^i - \ell_G(\gamma)}\alpha \in J$. Since $\alpha \in J$ we have $\gamma \in J$ as desired.

Finally, suppose we have shown J contains all elements of length at most $\ell_G(\gamma) - 1$, where now $\ell_G(\gamma) > p^n - p^{n-1}$. Using Lemma 3.18 (since $p^n - p^{n-1} \geq 2p^{n-1}$; again $p > 2$ comes to the rescue) we know $(\sigma - 1)^{\ell_G(\gamma)-1}\gamma \in \iota^n_0(N^n_0(k_m E_n))$. Since $Y^G_n = \iota^n_0(N^n_0(k_m E_n))$, there exists $\alpha \in J$ with $\iota^n_0(N^n_0(\alpha)) = (\sigma - 1)^{\ell_G(\gamma)-1}\gamma$. Hence $\ell_G\left(\gamma - (\sigma - 1)^{p^n - \ell_G(\gamma)}\alpha\right) \leq \ell_G(\gamma) - 1$ since

$$(\sigma - 1)^{\ell_G(\gamma)-1}\left(\gamma - (\sigma - 1)^{p^n - \ell_G(\gamma)}\alpha\right) = 0,$$

and by induction $\gamma - (\sigma - 1)^{p^i - \ell_G(\gamma)}\alpha \in J$. Since $\alpha \in J$ we have $\gamma \in J$ as desired. $\square$

There is a great deal of control in the decomposition we have just constructed. The following corollary records the choices available in constructing the submodule Y_{n-1}, choices that are important in constructing the module $\Gamma(m,n)$.

Corollary 3.24. *Given any $\mathbb{F}_p$-basis $\mathcal{I}_n$ of $\iota_0^n(N_0^n(k_mE_n))$ and — for each $x \in \mathcal{I}_n$ — any choices $\alpha_x \in k_mE_n$ so that $\iota_0^n(N_0^n(\alpha_x)) = x$, there is a decomposition*

$$k_mE \simeq \mathcal{X}_0 \oplus \cdots \oplus \mathcal{X}_{n-1} \oplus \mathcal{Y}_0 \oplus \cdots \oplus \mathcal{Y}_n$$

per Theorem 5.2 so that $\mathcal{Y}_n = \oplus_{x\in\mathcal{I}_n}\langle\alpha_x\rangle_{\mathbb{F}_p[G]}$.

Chapter 4

Galois Cohomology for p-adic Extensions

In this chapter we give the module structure of $H^i(G_E, \mu_p)$ for a field extension E/F with $\mathrm{Gal}(E/F) = \mathbb{Z}_p$ and $\xi_p \in E$, where p is an odd prime. Again we develop our results in the language of reduced Milnor K-groups, then translate them to Galois Cohomology via the Bloch-Kato conjecture.

As in the last chapter, we write E_i for the intermediate field extension of E/F with $[E_i : F] = p^i$ and denote $\mathrm{Gal}(E_i/F)$ by G_i. We also write E_∞ for E and G_∞ for $\mathrm{Gal}(E/F)$. The groups G_i arise as quotients of G_∞ by its subgroups H_i; i.e., H_i is the subgroup of G_∞ so that $G_\infty/H_i = G_i$. Galois theory tells us $E_\infty^{H_i} = E_i$. Of course one has subgroups $H_i/H_n \subseteq G_n$ with $E_n^{H_i/H_n} = E_i$, and so $G_n/(H_i/H_n) = G_i$.

Also as before, there are elements $a_i \in E_i$ satisfying the norm compatibility property of Equation (3.1), and with $E_{i+1} = E_i(\sqrt[p]{a_i})$. For a fixed intermediate extension E_n/E_0, the element χ used in the previous chapter is now chosen to be the element a_n.

The main result of this section is

Theorem 4.1. *Suppose that $Gal(E/F) = \mathbb{Z}_p$, that $\xi_p \in E$, and that $p > 2$. Then as $\mathbb{F}_p[\mathbb{Z}_p]$-modules,*

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

where

- *each* $Y_i \subseteq \iota_i^\infty(k_m E_i)$ *is a direct sum of free* $\mathbb{F}_p[G_i]$*-modules; and*
- $(\oplus_{i=n}^\infty Y_i)^{G_\infty} = \iota_0^\infty(N_0^n(k_m E_n))$.

Remark 4.2. Translated into the language of Galois cohomology, this theorem says that

$$H^m(G_E, \mu_p) \simeq \oplus_{i=0}^\infty Y_i,$$

where now $Y_i \subseteq \mathrm{res}_i^\infty\left(H^m(G_{E_i}, \mu_p)\right)$, and that

$$(\oplus_{i=n}^\infty Y_i)^{G_\infty} = \mathrm{res}_0^\infty\left(\mathrm{cor}_0^n\left(H^m(G_{E_n}, \mu_p)\right)\right).$$

As we saw in the last chapter, res_j^i is the map induced on cohomology by the inclusion $E_j \hookrightarrow E_i$ and cor_j^i is the map induced by the norm $N_{E_i/E_j} : E_i \to E_j$.

Just as when E/F was a finite cyclic p-group, lengths of elements in $k_m E_\infty$ will be important. The length of an element $\gamma_\infty \in k_m E_\infty$ is defined as $\ell_{G_\infty}(\gamma_\infty) := \dim_{\mathbb{F}_p}\langle\gamma_\infty\rangle_{\mathbb{F}_p[G]}$. For an element $\gamma_n \in k_m E_n$ we know that $\ell_{G_n}(\gamma_n) := \dim_{\mathbb{F}_p}\langle\gamma_n\rangle_{\mathbb{F}_p[G_n]}$ is given as the minimal integer $\ell \geq 1$ so that

$$(\sigma - 1)^\ell(\gamma_n) = 0 \in k_m E_n$$

(where here σ denotes a generator of G_n).

The following lemma shows that for $\gamma \in k_m E_\infty$ we can choose a representative $\hat{\gamma} \in k_m E_i$ which has the correct length. By working with an element in $k_m E_i$ instead of $k_m E_\infty$, we can appeal to the results proved in the last chapter.

Lemma 4.3. *Every nonzero element* $\gamma \in k_m E_\infty^{H_i}$ *has a representative* $\hat{\gamma} \in k_m E_i$*. If* $\hat{\gamma}$ *is chosen with minimal length among all elements of* $k_m E_i$ *satisfying this property, then* $\ell_{G_i}(\hat{\gamma}) = \ell_{G_\infty}(\gamma)$.

Proof. An element $\gamma \in k_m E_\infty$ must have a representative $\gamma' \in k_m E_j$ for some j. We would like to argue that $\gamma' \in k_m E_j^{H_i/H_j}$. Now the action of $\mathrm{Gal}(E_\infty/E_i)$ is trivial on

γ, which means that for σ a generator of $\mathrm{Gal}(E_j/F)$ we have

$$\sigma^{p^i}(\gamma') = \gamma' + k \quad \text{for some} \quad k \in \ker \iota_j^\infty.$$

Since there is some n with $k \in \ker \iota_j^n$, we can include all elements and equations into $k_m E_n$ to show that $\iota_j^n(\gamma') \in k_m E_n^{H_i/H_n}$. Abusing notation slightly, we write γ' for a representative of γ from $k_m E_n^{H_i/H_n}$.

We now show the first part of the lemma, which claims that we can find a representative for γ from $k_m E_i$. We start by assuming $n > i$, since if $n \leq i$ there is nothing to prove. Since $\gamma' \in k_m E_n^{H_i/H_n}$ we have $\ell_{G_n}(\gamma') \leq p^i \leq p^{n-1}$. But since $p^{n-1} \leq p^n - p^{n-1}$, this implies $\iota_{n-1}^n(N_{n-1}^n(\gamma')) = 0$. If $N_{n-1}^n(\gamma') = 0$, then because $\gamma' \in k_m E_n^{H_i/H_n}$, Lemma 3.17 implies that $\gamma' = \iota_i^n(\bar{\gamma})$ for some $\bar{\gamma} \in k_m E_i$. Hence in this case, we have proven our claim.

Otherwise, we have $N_{n-1}^n(\gamma') = \{a_{n-1}\} \cdot g$ for some $g \in \Gamma(m,n)$. In this case $\{a_n\} \cdot \iota_{n-1}^n(g)$ has

$$N_{n-1}^n(\{a_n\} \cdot \iota_{n-1}^n(g)) = \{a_{n-1}\} \cdot g = N_{n-1}^n(\gamma')$$

by the Projection Formula (3.3). Additionally, $\ell_{G_n}(\{a_n\} \cdot \iota_{n-1}^n(g)) \leq \ell_{G_n}(\gamma')$ by Lemma 3.22, so that $\gamma' - \{a_n\} \cdot \iota_{n-1}^n(g) \in k_m E_n^{H_i/H_n}$. Then since $\gamma' - \{a_n\} \cdot \iota_{n-1}^n(g)$ has trivial norm to $k_m E_{n-1}$, Lemma 3.17 again shows there is an element $\bar{\gamma} \in k_m E_i$ so that

$$\iota_i^n(\bar{\gamma}) = \gamma' - \{a_n\} \cdot \iota_{n-1}^n(g).$$

Since $\iota_n^\infty\left(\gamma' - \{a_n\} \cdot \iota_{n-1}^n(g)\right) = \iota_n^\infty(\gamma')$, we have shown that γ has a representative from $k_m E_i$ in any case.

Now that we know there is some representative for γ from $k_m E_i$, we let $\hat{\gamma} \in k_m E_i$ be an element of minimal length so that $\iota_i^\infty(\hat{\gamma}) = \gamma$. We show that $\ell_{G_i}(\hat{\gamma}) = \ell_{G_\infty}(\gamma)$ by showing that $\ell_{G_i}(\hat{\gamma}) = \ell_{G_n}(\iota_i^n(\hat{\gamma}))$ for all $n \geq i$. We prove this result by induction, beginning with the case $n = i + 1$. We write σ for a generator of G_{i+1}.

First, if $x \geq \ell_{G_i}(\hat{\gamma})$ then we have

$$(\sigma - 1)^x \iota_i^{i+1}(\hat{\gamma}) = \iota_i^{i+1}((\sigma - 1)^x \hat{\gamma}) = 0,$$

and so $\ell_{G_i}(\hat{\gamma}) \geq \ell_{G_n}(\iota_i^n(\hat{\gamma}))$.

We now verify the opposite inequality by contradiction. Suppose that we have $\ell_{G_{i+1}}(\iota_i^{i+1}(\hat{\gamma})) < \ell_{G_i}(\hat{\gamma})$. This implies

$$(\sigma - 1)^{\ell_{G_i}(\hat{\gamma})-1}\hat{\gamma} \in \ker \iota_i^{i+1}.$$

Now if we let k be chosen so that $p^{k-1} < \ell_{G_i}(\hat{\gamma}) \leq p^k$, then since Theorem 3.7 shows that $k_m E_i$ is a direct sum of 'free' submodules, we must have $(\sigma-1)^{\ell_{G_i}(\hat{\gamma})-1}\hat{\gamma} \in \mathrm{im}(\sigma - 1)^{p^k-1}$. But Lemma 3.12 shows $\ker \iota_i^{i+1}$ is a direct sum of free $\mathbb{F}_p[G_j]$-submodules (for $0 \leq j \leq i$), so there must be some $\alpha \in \ker \iota_i^{i+1}$ with $\ell_{G_i}(\alpha) \geq p^k \geq \ell_{G_i}(\hat{\gamma})$ and $(\sigma-1)^{\ell_{G_i}(\hat{\gamma})-1}\hat{\gamma} = (\sigma-1)^{\ell_{G_i}(\alpha)-1}\alpha$. Hence we have $\hat{\gamma} - (\sigma-1)^{\ell_{G_i}(\alpha)-\ell_{G_i}(\hat{\gamma})}\alpha$ has length at most $\ell_{G_i}(\hat{\gamma}) - 1$, and

$$\iota_i^\infty\left(\hat{\gamma} - (\sigma-1)^{\ell_{G_i}(\alpha)-\ell_{G_i}(\hat{\gamma})}\alpha\right) = \iota_i^\infty(\hat{\gamma}) = \gamma.$$

This is a contradiction to the minimality of $\hat{\gamma}$, and hence we conclude $\ell_{G_{i+1}}(\hat{\gamma}) = \ell_{G_i}(\hat{\gamma})$.

For the inductive step, suppose $\ell_{G_n}(\iota_i^n(\hat{\gamma})) < \ell_{G_i}(\hat{\gamma})$, while

$$\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma})) = \ell_{G_i}(\hat{\gamma}). \tag{4.4}$$

This gives

$$(\sigma-1)^{\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma}))-1}\iota_i^{n-1}(\hat{\gamma}) \in \ker \iota_{n-1}^n.$$

Again, letting k be chosen so that $p^{k-1} < \ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma})) \leq p^k$, Theorem 3.7 shows that $(\sigma-1)^{\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma}))-1}\iota_i^{n-1}(\hat{\gamma}) \in \mathrm{im}(\sigma-1)^{p^k-1}$. Since Lemma 3.12 shows that $\ker \iota_{n-1}^n$ is a direct sum of 'free' submodules, there must be some $\alpha \in \ker \iota_{n-1}^n$ with

$\ell_{G_{n-1}}(\alpha) \geq p^k \geq \ell_{G_{n-1}}(\hat{\gamma})$ and

$$(\sigma-1)^{\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma}))-1}\iota_i^{n-1}(\hat{\gamma}) = (\sigma-1)^{\ell_{G_{n-1}}(\alpha)-1}\alpha.$$

Hence we have $\hat{\gamma} - (\sigma-1)^{\ell_{G_{n-1}}(\alpha)-\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma}))}\alpha$ has length at most $\ell_{G_{n-1}}(\hat{\gamma})-1$, and

$$\iota_{n-1}^{\infty}\left(\iota_i^{n-1}(\hat{\gamma}) - (\sigma-1)^{\ell_{G_{n-1}}(\alpha)-\ell_{G_{n-1}}(\iota_i^{n-1}(\hat{\gamma}))}\alpha\right) = \iota_i^{\infty}(\hat{\gamma}) = \gamma.$$

This contradicts Equation 4.4, and we conclude $\ell_{G_n}(\iota_i^n(\hat{\gamma})) = \ell_{G_i}(\hat{\gamma})$ for all $n \geq i$. □

Proof of Theorem 4.1. Let $\mathcal{I}_i$ be a basis for a complement of $\iota_0^{\infty}(N_0^{i+1}(k_mE_{i+1}))$ in $\iota_0^{\infty}(N_0^i(k_mE_i))$. For each $x \in \mathcal{I}_i$ choose $\alpha_x \in \iota_i^{\infty}(k_mE_i)$ with $\iota_0^{\infty}(N_0^i(\alpha_x))$. The Exclusion Lemma 2.8 shows that $\sum\langle\alpha_x\rangle_{\mathbb{F}_p[G_\infty]} = \oplus\langle\alpha_x\rangle_{\mathbb{F}_p[G_\infty]}$, and we denote this set by Y_i. Again, $\sum Y_i = \oplus Y_i$ since the Exclusion Lemma 2.8 implies any dependence would produce a nontrivial dependence in $Y_i^{G_\infty} = \langle\mathcal{I}_i\rangle_{\mathbb{F}_p}$, contrary to the construction of the $\mathcal{I}_i$.

That each Y_i is a direct sum of free $\mathbb{F}_p[G_i]$-modules is immediate. The fact that $(\oplus_{i=n}^{\infty}Y_i)^{G_\infty} = \iota_0^{\infty}(N_0^n(k_mE_n))$ comes from the construction of $Y_i^{G_\infty} = \langle\mathcal{I}_i\rangle$.

Since $\cup_n(k_mE_\infty)^{H_n} = k_mE_\infty$, we show by induction that for arbitrary n one has $(k_mE_\infty)^{H_n} \subseteq \oplus_{i=0}^{\infty}Y_i$. First, notice that $(k_mE_\infty)^{H_0} = \iota_0^{\infty}(k_mE_0)$ by Lemma 4.3. Since $\oplus_i\langle\mathcal{I}_i\rangle_{\mathbb{F}_p} = \iota_0^{\infty}(k_mE_0)$ by construction, we have $(k_mE_\infty)^{H_0} \subseteq \oplus_{i=0}^{\infty}Y_i$

Now suppose we have shown that all elements of $(k_mE_\infty)^{H_{n-1}}$ are in $\oplus_{i=0}^{\infty}Y_i$, and we will show that $(k_mE_\infty)^{H_n} \subseteq \oplus_{i=0}^{\infty}Y_i$. We prove this result by induction on the length of elements of $(k_mE_\infty)^{H_n}$. So let $\gamma \in (k_mE_\infty)^{H_n}$ be given, and let $\hat{\gamma} \in k_mE_n$ be a representative of γ as per Lemma 4.3. If $\ell_{G_n}(\hat{\gamma}) \leq p^{n-1}$, then $\hat{\gamma} \in k_mE_n^{H_{n-1}/H_n}$. Now if $X_0 \oplus \cdots \oplus X_{n-1} \oplus Y_0 \oplus \cdots \oplus Y_n$ is a decomposition of k_mE_n as per Theorem 3.7, then $\hat{\gamma} - \mathrm{proj}_X(\hat{\gamma})$ is an element which is also a preimage of γ, and $\ell_{G_n}(\hat{\gamma}) = \ell_{G_n}(\hat{\gamma} - \mathrm{proj}_X(\hat{\gamma}))$ by the minimality of $\hat{\gamma}$. But then

$$\hat{\gamma} - \mathrm{proj}_X(\hat{\gamma}) \in (Y_0 \oplus \cdots \oplus Y_n)^{H_{n-1}/H_n} \subseteq \iota_{n-1}^n(k_mE_{n-1}).$$

Hence $\gamma \in k_mE_\infty^{H_{n-1}}$, and by induction $\gamma \in \oplus_{i=0}^{\infty}Y_i$.

So we are left with the case $\ell_{G_n}(\hat{\gamma}) > p^{n-1}$. By Corollary 3.20 this implies that

$(\sigma-1)^{\ell_{G_n}(\hat{\gamma})-1}\hat{\gamma} \in \iota_0^n(N_0^n(k_mE_n))$, where here σ is a generator of G_n. So choose $c_x \in \mathbb{F}_p$ with

$$\iota_n^\infty\left((\sigma-1)^{\ell_{G_n}(\hat{\gamma})-1}\hat{\gamma}\right) = \sum_{i\geq n}\sum_{x\in\mathcal{I}_i} c_x x.$$

Let $\hat{\alpha}_x \in k_mE_i$ be a representative so that $\iota_i^\infty(\hat{\alpha}_x) = \alpha_x$, and we have

$$(\sigma-1)^{\ell_{G_n}(\hat{\gamma})-1}\hat{\gamma} \equiv (\sigma-1)^{p^n-1}\sum_{i\geq n}\sum_{x\in\mathcal{I}_i} N_n^i(c_x\hat{\alpha}_x) \mod \ker\iota_n^\infty.$$

Hence

$$\gamma' := \hat{\gamma} - (\sigma-1)^{p^n-\ell_{G_n}(\hat{\gamma})}\sum_{i\geq n}\sum_{x\in\mathcal{I}_i} N_n^i(c_x\hat{\alpha}_x) \in k_mE_n$$

is an element so that $(\sigma-1)^{\ell_{G_n}-1}\gamma' \in \ker\iota_n^\infty$. It follows that $\iota_n^\infty(\gamma')$ is an element of $k_mE_\infty^{H_n}$ with length at most $\ell_{G_\infty}(\gamma)-1$, and hence $\iota_n^\infty(\gamma') \in \oplus_{i\geq 0}Y_i$. Since $\alpha_x \in \oplus_{i\geq 0}Y_i$ by assumption, this implies $\gamma \in \oplus_{i\geq 0}Y_i$ as well. □

Chapter 5

The Case $i(E/F) > -\infty$

5.1 The Main Theorem

In this chapter we study the $\mathbb{F}_p[G]$-module structure of the Milnor k-groups $k_m E$ for a general field extension (i.e., without restriction on $i(E/F)$), but under the following

Assumption 5.1. *Suppose γ generates a summand of $\Gamma(m,n)$ and that $\mathfrak{g}$ has the smallest length among all elements whose image under N_{n-1}^n is $\{a_{n-1}\}\cdot\gamma$. Then $(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\mathfrak{g}$ has the smallest length among all elements whose image under N_{n-1}^n is $\{a_{n-1}\}\cdot(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\gamma$.*

In the course of proving the main theorem of this chapter, we show that this assumption is equivalent to a seemingly stronger statement where we drop the assumption that γ generates a summand of $\Gamma(m,n)$ (see Remark 5.28). We have stated the weaker version here since it is all we need to complete our result. We show that Assumption 5.1 holds when $i(E/F)=0$ in Corollary 5.11. We do not have evidence supporting this assumption for $i(E/F)>0$.

Our main result is the following generalization of Theorem 3.7.

Theorem 5.2. *Let E/F be an extension of fields with $Gal(E/F) = \mathbb{Z}/p^n\mathbb{Z}$ and*

$\xi_p \in E$, where $p > 2$ is a prime. Suppose Assumption 5.1 holds. Then as $\mathbb{F}_p[G]$-modules,

$$k_m E \simeq \bigoplus_{\substack{0 \le i \le n \\ j \in \{-\infty, 0, \cdots, n-1\}}} X_{i,j} \ \oplus Y_0 \oplus \cdots \oplus Y_n,$$

where

(i) each $X_{i,j}$ is a direct sum of cyclic submodules of dimension $p^i + p^j$ and $X_{i,j} = \emptyset$ when $i > i(E/F)$ and $j > -\infty$;

(ii) each $Y_i \subseteq \iota_i^n(k_m E_i)$ is a direct sum of free $\mathbb{F}_p[G_i]$-submodules; and

(iii) for every $j \le n$,

$$(Y_j \oplus \cdots \oplus Y_n \oplus \bigoplus_{\substack{i' \\ j' \ge j}} X_{i',j'})^G = \iota_0^n \left(N_0^j (k_m E_j) \right).$$

Remark 5.3. Using the Bloch-Kato conjecture, this result says that

$$H^m(G_E, \mu_p) \simeq \bigoplus_{\substack{0 \le i \le n \\ j \in \{-\infty, 0, \cdots, n-1\}}} X_{i,j} \ \oplus Y_0 \oplus \cdots \oplus Y_n.$$

Condition (ii) translates to $Y_i \subseteq \mathrm{res}_i^n \left(H^m(G_{E_i}, \mu_p) \right)$, and condition (iii) says

$$(Y_j \oplus \cdots \oplus Y_n \oplus \bigoplus_{\substack{i' \\ j' \ge j}} X_{i',j'})^G = \mathrm{res}_0^n \left(\mathrm{cor}_0^j \left(H^m(G_{E_j}, \mu_p) \right) \right).$$

As before, res_j^i is the map induced on cohomology by the inclusion $E_j \hookrightarrow E_i$ and cor_j^i is the map induced by the norm $N_{E_i/E_j} : E_i \to E_j$.

5.2 Minimal Preimages

As before, it is important to understand those elements which map to $\{a_{n-1}\} \cdot \gamma$ for $\gamma \in \Gamma(m, n)$. In this more general setting, however, one does not have a good

understanding of how the length of a preimage of an element $\{a_{n-1}\} \cdot \gamma$ under N_{n-1}^n compares to the length of a preimage of $\{a_{n-1}\} \cdot ((\sigma - 1)\gamma)$ under N_{n-1}^n. As such, it is difficult to construct a sufficiently 'small' exceptional submodule. This is the key complication in generalizing the results we have already determined for extensions with $i(E/F) = -\infty$ to extensions without condition on $i(E/F)$.

With this in mind, we make the following

Definition 5.4. For $\gamma \in \Gamma(m, n)$, a preimage of γ is an element $\mathfrak{h}$ satisfying

$$N_{n-1}^n(\mathfrak{h}) = \{a_{n-1}\} \cdot \gamma.$$

A minimal preimage of γ is a preimage $\mathfrak{g}$ of minimal length; i.e., if $\mathfrak{h}$ is a preimage for γ and $\mathfrak{g}$ is a minimal preimage, then $\ell_G(\mathfrak{g}) \leq \ell_G(\mathfrak{h})$.

In this section we shall explore some of the properties of minimal preimages. Our first result gives a naive lower bound on the length of a (minimal) preimage of an element $\gamma \in \Gamma(m, n)$.

Lemma 5.5. *If $\mathfrak{g} \in k_m E_n$ is a preimage for $\gamma \in \Gamma(m, n)$, then $\ell_G(\mathfrak{g}) \geq \ell_{G_{n-1}}(\gamma)$. In particular, if $\mathfrak{g}$ is a preimage of γ with $\ell_G(\mathfrak{g}) \leq \ell_{G_{n-1}}(\gamma)$, then $\mathfrak{g}$ is a minimal preimage.*

Proof. The second statement is a clear corollary of the first, so we just prove the first statement.

Let $x < \ell_{G_{n-1}}(\gamma)$, so that $(\sigma - 1)^x \gamma \neq 0$. Since

$$\Gamma(m, n) \cap \ker\left(k_{m-1}E_{n-1} \xrightarrow{\{a_{n-1}\}\cdot -} k_m E_{n-1} \right) = \{0\},$$

we have $\{a_{n-1}\} \cdot ((\sigma - 1)^x \gamma) \neq 0$. Since $a_{n-1}^\sigma = a_{n-1} k^p$ for some $k \in E_{n-1}^\times$ (Equation (3.2)), we have

$$\begin{aligned} (\sigma - 1)\left(\{a_{n-1}\} \cdot \gamma\right) &= \{a_{n-1}^\sigma\} \cdot \sigma(\gamma) - \{a_{n-1}\} \cdot \gamma \\ &= \{a_{n-1}\} \cdot \sigma(\gamma) - \{a_{n-1}\} \cdot \gamma = \{a_{n-1}\} \cdot (\sigma - 1)\gamma \end{aligned} \tag{5.6}$$

Hence

$$\begin{aligned} N_{n-1}^n((\sigma-1)^x\mathfrak{g}) &= (\sigma-1)^x N_{n-1}^n(\mathfrak{g}) = (\sigma-1)^x\{a_{n-1}\}\cdot\gamma \\ &= \{a_{n-1}\}\cdot((\sigma-1)^x\gamma) \neq 0. \end{aligned}$$

Therefore $(\sigma-1)^x\mathfrak{g} \neq 0$, and so $\ell_{G_{n-1}}(\gamma) \leq \ell_G(\mathfrak{g})$. □

Combined with Assumption 5.1, the next lemma gives us a useful tool for determining when an element is a minimal preimage.

Lemma 5.7. *If $\mathfrak{g}$ is a preimage of $\gamma \in \Gamma(m,n)$ which is not minimal, then $(\sigma-1)\mathfrak{g}$ is a preimage of $(\sigma-1)\gamma$ which is not minimal. Hence $(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\mathfrak{g}$ is a preimage of $(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\gamma$ which is not minimal.*

Proof. Let $\mathfrak{h}$ be a minimal preimage of γ. Then

$$\begin{aligned} N_{n-1}^n((\sigma-1)\mathfrak{g}) = (\sigma-1)N_{n-1}^n(\mathfrak{g}) &= (\sigma-1)\left(\{a_{n-1}\}\cdot(\gamma)\right) \\ &= (\sigma-1)N_{n-1}^n(\mathfrak{h}) = N_{n-1}^n((\sigma-1)\mathfrak{h}). \end{aligned}$$

In light of Equation (5.6) this shows $(\sigma-1)\mathfrak{g}$ and $(\sigma-1)\mathfrak{h}$ are preimages of $(\sigma-1)\gamma$. However, we have

$$\ell((\sigma-1)\mathfrak{g}) = \ell(\mathfrak{g}) - 1 > \ell(\mathfrak{h}) - 1 = \ell((\sigma-1)\mathfrak{h}),$$

and hence $(\sigma-1)\mathfrak{g}$ is not a minimal preimage.

The second statement is a clear corollary of the first. □

Now we show a way of constructing a minimal preimage for the sum of two elements, at least in some limited cases.

Lemma 5.8. *Suppose that $\mathfrak{g}_1$ is a minimal preimage of γ_1, that $\mathfrak{g}_2$ is a preimage of γ_2, and that $\ell(\mathfrak{g}_1) > \ell(\mathfrak{g}_2)$. Then $\mathfrak{g}_1 + \mathfrak{g}_2$ is a minimal preimage of $\gamma_1 + \gamma_2$.*

Proof. We have

$$N_{n-1}^n(\mathfrak{g}_1 + \mathfrak{g}_2) = N_{n-1}^n(\mathfrak{g}_1) + N_{n-1}^n(\mathfrak{g}_2) = \{a_{n-1}\}\cdot(\gamma_1 + \gamma_2),$$

and hence $\mathfrak{g}_1 + \mathfrak{g}_2$ is a preimage of $\gamma_1 + \gamma_2$. We also have $\ell(\mathfrak{g}_1 + \mathfrak{g}_2) = \ell(\mathfrak{g}_1)$ since $\ell(\mathfrak{g}_1) > \ell(\mathfrak{g}_2)$. Suppose for the sake of contradiction that there is a preimage $\mathfrak{g}$ of $\gamma_1 + \gamma_2$ so that $\ell(\mathfrak{g}) < \ell(\mathfrak{g}_1)$. Then $\ell(\mathfrak{g} - \mathfrak{g}_1) \leq \max\{\ell(\mathfrak{g}), \ell(\mathfrak{g}_2)\} < \ell(\mathfrak{g}_1)$. Since additionally we have

$$N_{n-1}^n(\mathfrak{g} - \mathfrak{g}_2) = N_{n-1}^n(\mathfrak{g}) - N_{n-1}^n(\mathfrak{g}_2) = \{a_{n-1}\} \cdot (\gamma_1 + \gamma_2) - \{a_{n-1}\} \cdot \gamma_2 = \{a_{n-1}\} \cdot \gamma_1,$$

we see that $\mathfrak{g} - \mathfrak{g}_2$ is a preimage of γ_1 with length strictly less than $\ell(\mathfrak{g}_1)$, contradicting the minimality of $\mathfrak{g}_1$. □

The next result shows that elements in $\Gamma(m,n)^{G_{n-1}}$ have minimal preimages whose lengths are highly restricted.

Lemma 5.9. *A minimal preimage $\mathfrak{g}$ of $\gamma \in \Gamma(m,n)^{G_{n-1}}$ has dimension $p^j + 1$ for some $j \in \{-\infty, 0, \cdots, i(E/F)\}$. When $j = -\infty$, $\mathfrak{g} \in k_m E_n \setminus \iota_{n-1}^n(k_m E_{n-1})$. When $j \geq 0$,*

$$(\sigma - 1)^{\ell_G(\mathfrak{g})-1}\mathfrak{g} \in \iota_0^n(N_0^j(k_m E_j)) \setminus \iota_0^n(N_0^{j+1}(k_m E_{j+1})).$$

Proof. We know $N_{n-1}^n(\{\chi\} \cdot \iota_{n-1}^n(\gamma)) = \{a_{n-1}\} \cdot \gamma$, and further $\ell_G(\{\chi\} \cdot \iota_{n-1}^n(\gamma)) \leq p^{i(E/F)} + 1$ since $\ell_G(\chi) = p^{i(E/F)} + 1$ and $\ell_G(\gamma) = 1$. Hence a minimal preimage of γ has dimension at most $p^{i(E/F)} + 1$.

Now suppose $\mathfrak{g}$ is a minimal preimage of γ and $\ell_G(\mathfrak{g}) = p^j + k \leq p^{j+1}$ for some $k \geq 2$. Since $i(E/F) \leq n-1$ we may assume $j < n-1$. Now $N_{n-1}^n((\sigma-1)\mathfrak{g}) = \{a_{n-1}\} \cdot (\sigma-1)\gamma = 0$, and so Lemma 3.17 gives $(\sigma-1)\mathfrak{g} \in \iota_{j+1}^n(k_m E_{j+1})$. Because $\ell_G((\sigma-1)\mathfrak{g}) = \ell_G(\mathfrak{g}) - 1 > p^j$, Corollary 3.20 shows there exists $\alpha \in k_m E_{j+1}$ so that

$$(\sigma-1)^{p^{j+1}-1}\alpha = \iota_0^n(N_0^{j+1}\alpha) = (\sigma-1)^{\ell_G(\mathfrak{g})-1}\mathfrak{g}.$$

Then $\mathfrak{g} - \iota_{j+1}^n\left((\sigma-1)^{p^{j+1}-\ell_G(\mathfrak{g})}\alpha\right)$ has length less than $\ell_G(\mathfrak{g})$, and since $j < n-1$ further satisfies

$$N_{n-1}^n\left(\mathfrak{g} - \iota_{j+1}^n((\sigma-1)^{p^{j+1}-p^j-1}\alpha)\right) = N_{n-1}^n\mathfrak{g} = \{a_{n-1}\} \cdot \gamma,$$

contradicting the minimality of $\mathfrak{g}$. Hence for some $j \in \{-\infty, 0, \cdots, i(E/F)\}$ we have

$\ell_G(\mathfrak{g}) = p^j + 1$.

Now we show the second part of the lemma. First, if $j = -\infty$ the statement that $\mathfrak{g} = (\sigma-1)^{p^{-\infty}}\mathfrak{g} \notin \iota^n_{n-1}(k_m E_{n-1})$ is obvious, because $N^n_{N-1}(\mathfrak{g}) = \{a_{n-1}\} \cdot \gamma \neq 0$ whereas $\iota^n_{n-1}(k_m E_{n-1}) \subseteq \ker N^n_{n-1}$. Hence we assume $j \geq 0$.

Since $N^n_{n-1}((\sigma-1)\mathfrak{g}) = 0$ and $\ell_G((\sigma-1)\mathfrak{g}) = p^j$ Lemma 3.17 tells us that $(\sigma-1)\mathfrak{g} \in \iota^n_j(k_m E_j)$, and so $(\sigma-1)^{p^j}\mathfrak{g} \in \iota^n_0(N^j_0(k_m E_j))$. If additionally $(\sigma-1)^{p^j}\mathfrak{g} \in \iota^n_0(N^{j+1}_0(k_m E_{j+1}))$ then there exists $\alpha \in k_m E_{j+1}$ with $\iota^n_0(N^{j+1}_0\alpha) = (\sigma-1)^{p^j}\mathfrak{g}$. We will now show that $\alpha' := (\sigma-1)^{p^{j+1}-p^j-1}\alpha$ satisfies

1. $N^n_{n-1}(\iota^n_{j+1}(\alpha')) = 0$,
2. $\ell_G(\alpha') = \ell_G(\mathfrak{g})$, and
3. $(\sigma-1)^{\ell_G(\alpha')-1}\alpha' = (\sigma-1)^{\ell_G(\mathfrak{g})-1}\mathfrak{g}$.

With these facts we can conclude that $\mathfrak{g} - \iota^n_{j+1}(\alpha')$ is a preimage of γ with length less than $\mathfrak{g}$, contrary to the minimality of $\mathfrak{g}$. Hence we can conclude

$$(\sigma-1)^{\ell_G(\mathfrak{g})-1}\mathfrak{g} = (\sigma-1)^{p^j}\mathfrak{g} \in \iota^n_0(N^j_0(k_m E_j)) \setminus \iota^n_0(N^{j+1}_0(k_m E_{j+1})).$$

Property 2 follows from the fact that

$$\ell_G(\alpha') = \ell_G((\sigma-1)^{p^{j+1}-p^j-1}\alpha) = \ell_G(\alpha) - p^{j+1} + p^j + 1 = p^j + 1,$$

and Property 3 follows because

$$(\sigma-1)^{p^j}\alpha' = (\sigma-1)^{p^{j+1}-1}\alpha = \iota^n_0(N^{j+1}_0(\alpha)) = (\sigma-1)^{p^j}\mathfrak{g}.$$

For Property 1, we have $N^n_{n-1}(\alpha') = 0$ if $j+1 \leq n-1$, since $N^n_{n-1}(\iota^n_i(k_m E_i)) = 0$ for $i \leq n-1$. When $j+1 = n$, we note that α' is in the image of $(\sigma-1)^{p^n-p^{n-1}-1}$, and that $p^n - p^{n-1} - 1 \geq p^{n-1}$. (Here we've used $p > 2$.) Hence $\alpha' \in \mathrm{im}(\sigma-1)^{p^{n-1}} \subseteq \ker N^n_{n-1}$ as desired. □

We now show how to construct minimal preimages for generators of $\Gamma(m,n)$ which are sufficiently long (compared to the element χ).

Lemma 5.10. *Suppose $\gamma \in \Gamma(m,n)$ has $\ell_{G_{n-1}}(\gamma) = p^i$ for some $i > i(E/F)$. Then $\{\chi\} \cdot \iota^n_{n-1}(\gamma)$ is a preimage of γ with length p^i, and hence is a minimal preimage.*

Proof. The Projection Formula (3.3) gives $N^n_{n-1}(\{\chi\} \cdot \iota^n_{n-1}(\gamma)) = \{a_{n-1}\} \cdot \gamma$. We will show that $\{\chi\} \cdot \iota^n_{n-1}(\gamma)$ has length at most p^i. Lemma 5.5 then implies the desired result.

Since χ has length $p^{i(E/F)} + 1 \leq p^i$ as an element of $H^1(G_E, \mu_p)$, we know that $\sigma^{p^i}(\chi) = \chi f^p$ for some $f \in E^\times$. We also know that $(\sigma - 1)^{p^i} \equiv (\sigma^{p^i} - 1)$ kills γ, so that $\sigma^{p^i}\gamma = \gamma$ in $k_m E_{n-1}$. Hence we have

$$\begin{aligned}(\sigma-1)^{p^i-1}\left(\{\chi\} \cdot \iota^n_{n-1}(\gamma)\right) &= \{\sigma^{p^i}(\chi)\} \cdot \sigma^{p^i}\left(\iota^n_{n-1}(\gamma)\right) - \{\chi\} \cdot \iota^n_{n-1}(\gamma) \\ &= \{\chi\} \cdot \iota^n_{n-1}(\gamma) - \{\chi\} \cdot \iota^n_{n-1}(\gamma) = 0.\end{aligned}$$

Therefore $\ell_G(\{\chi\} \cdot \iota^n_{n-1}(\gamma)) \leq p^i$. □

With this result, we can show Assumption 5.1 holds for $i(E/F) \leq 0$.

Corollary 5.11. *Suppose that $i(E/F) \leq 0$. If γ generates a summand of $\Gamma(m,n)$ and $\mathfrak{g}$ is a minimal preimage of γ, then $(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\mathfrak{g}$ is a minimal preimage of $(\sigma-1)^{\ell_{G_{n-1}}(\gamma)-1}\mathfrak{g}$.*

Proof. If $\gamma \in \Gamma(m,n)^{G_{n-1}}$ there is nothing to prove. Otherwise $\ell_{G_{n-1}}(\gamma) = p^i$ for some $i \geq 1$. By Lemma 5.10, γ has a minimal preimage $\{\chi\} \cdot \iota^n_{n-1}(\gamma)$ of dimension p^i. Hence $(\sigma-1)^{p^i-1}\{\chi\} \cdot \iota^n_{n-1}(\gamma)$ is a preimage of $(\sigma-1)^{p^i-1}\gamma$ of dimension 1, and so is minimal. □

There is one result in this section which is conspicuously missing. Given the importance of the operator $\sigma - 1$ in all of our computations, one naturally asks: if $\mathfrak{g}$ is a minimal preimage of γ, is $(\sigma-1)\mathfrak{g}$ a minimal preimage of $(\sigma-1)\gamma$? This question (and others like it) lead us to Assumption 5.1, and ultimately to the results we have been able to give.

5.3 The Exceptional Submodule

Having introduced minimal preimages, we are now ready to give the construction which will allow us to prove Theorem 5.2.

We know that $\Gamma(m,n)$ is a direct sum of cyclic submodules of dimensions p^i, $i \in \{0, \cdots, n-1\}$. We filter $\Gamma(m,n)^{G_{n-1}}$ into submodules

$$I_{i,j} := \left\{ \gamma \in \Gamma(m,n)^{G_{n-1}} : \begin{array}{l} \gamma \in \mathrm{im}(\sigma-1)^{p^i-1} \text{ and a minimal} \\ \text{preimage of } \gamma \text{ has length at most } p^j+1 \end{array} \right\},$$

where $i \in \{0, \cdots, n-1\}$ and $j \in \{-\infty, 0, \cdots, i(E/F)\}$. One can verify that

$$I_{i,j} \subseteq I_{i',j'} \quad \text{whenever} \quad i \geq i' \text{ and } j \leq j', \tag{5.12}$$

and that $I_{0,i(E/F)} = \Gamma(m,n)^{G_{n-1}}$ (this is Lemma 5.9). We order the pairs (i,j) by defining $(i',j') < (i,j)$ whenever either $j' < j$ or $j' = j$ and $i' > i$ (a modified lexicographical ordering).

Choose an $\mathbb{F}_p$-basis $\mathcal{I}_{n-1,-\infty}$ for $I_{n-1,-\infty}$, and inductively (using the lexicographical ordering) choose an $\mathbb{F}_p$-basis $\mathcal{I}_{i,j}$ for a complement to

$$\langle I_{i',j'} : (i',j') < (i,j) \rangle \cap \langle I_{i',j'} : (i',j') \leq (i,j) \rangle \quad \text{in} \quad \langle I_{i',j'} : (i',j') \leq (i,j) \rangle.$$

For each $x \in \mathcal{I}_{i,j}$ choose an element $\gamma_x \in \Gamma(m,n)$ so that $x = (\sigma-1)^{p^i-1}\gamma_x$, and then pick $\mathfrak{g}_x \in k_m E_n$ a minimal preimage of γ_x. Define $X_{i,j} = \sum_{x \in \mathcal{I}_{i,j}} \langle \mathfrak{g}_x \rangle$. The submodule X is defined to be $\sum_{i,j} X_{i,j}$.

Theorem 5.13. *Suppose Assumption 5.1 holds. Then the submodule $X = \sum_{i,j} X_{i,j}$ just constructed satisfies*

1. *$X = \oplus_{i,j} X_{i,j}$, where $0 \leq i \leq n-1$ and $j \in \{-\infty, 0, \cdots, i(E/F)\}$;*
2. *$X_{i,j}$ is a direct sum of cyclic submodules of dimension $p^i + p^j$;*
3. *for $i > i(E/F)$ and $j \neq -\infty$, $X_{i,j} = \emptyset$;*
4. *for every $\gamma \in \Gamma(m,n)$ there exists $\mathfrak{g} \in X$ which is a minimal preimage of γ;*

5. $X \cap \iota_0^n(N_0^j(k_m E_j)) = \oplus_{i'} \oplus_{j' \geq j} X^G_{i',j'}$.

The proof of this result is spread across several lemmas which follow. We need some results concerning the spaces $I_{i,j}$ and the collections $\mathcal{I}_{i,j}$. The first is an exercise in definitions, though it gives important information about elements in $\langle \mathcal{I}_{i,j} \rangle$.

Lemma 5.14. *Each nontrivial $x \in \langle \mathcal{I}_{i,j} \rangle$ is an element satisfying*

- *$x \in im(\sigma - 1)^{p^i - 1} \setminus im(\sigma - 1)^{p^i}$ and*
- *a minimal preimage of x has dimension exactly $p^j + 1$.*

Proof. For the first, we need only verify $x \notin \mathrm{im}(\sigma - 1)^{p^i}$, since an element of $\langle \mathcal{I}_{i,j} \rangle$ is an element of $I_{i,j}$, which by definition contains elements in the image of $(\sigma - 1)^{p^i - 1}$. Since $\Gamma(m,n)$ is a direct sum of cyclic submodules of dimension p^i, where $i \in \{-\infty, 0, \cdots, n-1\}$, then $x \in \Gamma(m,n)^{G_{n-1}} \cap \mathrm{im}(\sigma - 1)^{p^i}$ implies $x \in \mathrm{im}(\sigma - 1)^{p^{i+1}-1}$. Hence we have $x \in I_{i+1,j}$ contrary to the selection of $\langle \mathcal{I}_{i,j} \rangle$.

For the second, we need only verify that a minimal preimage does not have dimension less than $p^j + 1$, since an element of $\langle \mathcal{I}_{i,j} \rangle$ is an element of $I_{i,j}$, and hence has a minimal preimage of dimension at most $p^j + 1$. If a minimal preimage had dimension at most p^j, Lemma 5.9 implies that a minimal preimage of x has dimension at most $p^{j-1} + 1$. Hence we have $x \in I_{0,j-1}$, contrary to the selection of $\langle \mathcal{I}_{i,j} \rangle$. □

Lemma 5.15. *If $\gamma \in im\left((\sigma - 1)^{p^i - 1}\right) \cap \Gamma(m,n)^{G_{n-1}}$, then*

$$\gamma \in \sum_{\substack{i' \geq i \\ j' \in \{-\infty, \cdots, i(E/F)\}}} \langle \mathcal{I}_{i',j'} \rangle.$$

Proof. Every element of $\Gamma(m,n)^{G_{n-1}}$ can be written uniquely as a sum of elements from the various $\langle \mathcal{I}_{i,j} \rangle$ (where $0 \leq i \leq n-1$ and $j \in \{-\infty, \cdots, i(E/F)\}$), and for a particular (i,j) we write $\mathrm{proj}_{i,j}(x)$ to denote the projection of an element x onto the summand corresponding to $\langle \mathcal{I}_{i,j} \rangle$ in this decomposition. With this notation, our lemma says that an element $\gamma \in \mathrm{im}\left((\sigma - 1)^{p^i - 1}\right) \cap \Gamma(m,n)^{G_{n-1}}$ should have $\mathrm{proj}_{i',j'}(\gamma) = 0$ whenever $i' < i$. Our strategy will be as follows: assuming the

presence of some nonzero $\mathrm{proj}_{i',j'}(\gamma)$ with $i' < i$, we remove a certain component $g = \sum_{\tilde{i},\tilde{j}} \mathrm{proj}_{\tilde{i},\tilde{j}}(\gamma)$ from γ so that $\gamma - g \in I_{i,j}$, yet $\gamma - g$ contains a summand from some $\mathcal{I}_{i',j'}$ where $(i',j') > (i,j)$. This contradicts our construction of the $\mathcal{I}_{i',j'}$.

So suppose that $\mathrm{proj}_{i',j'}(\gamma) \neq 0$ for some $i' < i$, and choose (i',j') as large as possible with $i' < i$ and so that

$$\mathrm{proj}_{i',j'}(\gamma) \neq 0. \tag{5.16}$$

Hence for any $(\tilde{i},\tilde{j}) > (i',j')$ with $\mathrm{proj}_{\tilde{i},\tilde{j}}(x) \neq 0$ we have $\tilde{i} \geq i$, and therefore $\mathrm{proj}_{\tilde{i},\tilde{j}}(x) \in \mathrm{im}(\sigma - 1)^{p^i - 1}$. It follows that

$$g := \sum_{(\tilde{i},\tilde{j}) > (i',j')} \mathrm{proj}_{\tilde{i},\tilde{j}}(x) \in \mathrm{im}(\sigma - 1)^{p^i - 1},$$

and so $\gamma - g \in \mathrm{im}(\sigma - 1)^{p^i - 1}$. Notice that $\gamma - g$ is now expressable as a sum of elements from $\langle \mathcal{I}_{\hat{i},\hat{j}} \rangle$ with $(\hat{i},\hat{j}) \leq (i',j')$, and therefore can be written as a sum of elements whose minimal preimages have dimension $p^{j'} + 1$ (since $(\hat{i},\hat{j}) \leq (i',j')$ implies $\hat{j} \leq j'$). This shows that $\gamma - g$ also has a preimage of dimension $p^{j'} + 1$, and so — combined with our previous assertion that $\gamma - g \in \mathrm{im}(\sigma - 1)^{p^i - 1}$ — we have $\gamma - g \in I_{i,j'}$. Now $I_{i,j'}$ is spanned by $\mathcal{I}_{\tilde{i},\tilde{j}}$ for pairs $(\tilde{i},\tilde{j}) \leq (i,j')$ by construction, and since $(i',j') > (i,j')$ we therefore have

$$\mathrm{proj}_{i',j'}(\gamma - g) = 0.$$

But $\mathrm{proj}_{i',j'}(\gamma - g) = \mathrm{proj}_{i',j'}(\gamma)$ by the construction of g, and so $\mathrm{proj}_{i',j'}(\gamma) = 0$ contrary to Equation (5.16). □

With these lemmas in hand, we can begin to make progress towards proving Theorem 5.13. We begin by showing that each γ_x generates a summand of $\Gamma(m,n)$ so that we may use Assumption 5.1.

Lemma 5.17. $\sum\langle\gamma_x\rangle = \oplus\langle\gamma_x\rangle = \Gamma(m,n)$, *where the sum is taken over all indices* (i,j) *and elements* $x \in \mathcal{I}_{i,j}$.

Proof. The sum is direct because $\langle\gamma_x\rangle^{G_{n-1}} = \langle x\rangle$, and $\sum\langle x\rangle = \oplus\langle x\rangle$ by construction. We proceed to show the submodule spans $\Gamma(m,n)$. We know $\sum\langle x\rangle = \Gamma(m,n)^{G_{n-1}}$,

and hence $\sum\langle\gamma_x\rangle$ contains all elements of length 1. So suppose $\gamma \in \Gamma(m,n)$ has $\ell_{G_{n-1}}(\gamma) := \ell > 1$ and that $\sum\langle\gamma_x\rangle$ contains all elements of length at most $\ell - 1$. Since $\Gamma(m,n)$ is a direct sum of cyclic submodules of dimensions p^i, $0 \le i \le n-1$, the element $g = (\sigma-1)^{\ell-1}\gamma$ is in the image of $(\sigma-1)^{p^i-1}$ for some $p^i \ge \ell$. By the previous lemma, we can write $g = \sum c_x(\sigma-1)^{\ell_{G_{n-1}}(\gamma_x)-1}\gamma_x$ where the sum is over elements $x \in \mathcal{I}_{i',j'}$ with $i' \ge i$ and $j' \in \{-\infty, 0, \cdots, i(E/F)\}$; in particular the elements $(\sigma-1)^{\ell_{G_{n-1}}(\gamma_x)-\ell}\gamma_x$ exist since $\ell_{G_{n-1}}(\gamma_x) \ge p^i \ge \ell$. We have $\ell_{G_{n-1}}\left(\gamma - \sum c_x(\sigma-1)^{\ell_{G_{n-1}}(\gamma_x)-\ell}\gamma_x\right) < \ell$, and — since $\sum c_x(\sigma-1)^{\ell_{G_{n-1}}(\gamma_x)-\ell}\gamma_x$ is obviously in $\sum\langle\gamma_x\rangle$ — by induction we have $\gamma \in \sum\langle\gamma_x\rangle$. □

Corollary 5.18. *For each $x \in \mathcal{I}_{i,j}$, $(\sigma-1)^{p^i-1}\mathfrak{g}_x$ is a minimal preimage of x.*

Proof. By Lemma 5.17, γ_x is a summand of $\Gamma(m,n)$. Since $\mathfrak{g}_x$ is a minimal preimage of γ_x, Assumption 5.1 gives $(\sigma-1)^{p^i-1}\mathfrak{g}_x$ is a minimal preimage of $(\sigma-1)^{p^i-1}\gamma_x = x$. □

The proof of Theorem 5.13(3)

Corollary 5.19. *$\mathcal{I}_{i,j} = \emptyset$ if $i > i(E/F)$ and $j > -\infty$.*

Proof. Lemma 5.10 says that an element $\gamma \in \Gamma(m,n)$ of length p^i for $i > i(E/F)$ has minimal preimage of dimension p^i. Hence if x is the fixed part of such a submodule it must have a minimal preimage of dimension 1. □

The proof of Theorem 5.13(2)

Lemma 5.20. *If $x \in \mathcal{I}_{i,j}$, then $\langle\mathfrak{g}_x\rangle$ is a submodule of dimension $p^i + p^j$.*

Proof. By Corollary 5.18 we know $(\sigma-1)^{p^i-1}\mathfrak{g}_x$ is a minimal preimage of x. By Lemma 5.14 we have $\ell_G\left((\sigma-1)^{p^i-1}\mathfrak{g}_x\right) = p^j + 1$, and so $\ell(\mathfrak{g}_x) = p^i + p^j$. □

Lemma 5.21. *For fixed $0 \le i \le n-1$ and $j \in \{-\infty, 0, \cdots, n-1\}$,*

$$X_{i,j} = \oplus_{x \in \mathcal{I}_{i,j}}\langle\mathfrak{g}_x\rangle.$$

Proof. Suppose there is a non-trivial dependence among the $\mathfrak{g}_x$, and (without loss, via the Exclusion Lemma 2.8) we assume this dependence occurs in the fixed part of each submodule. By the previous lemma, our dependence can be written

$$\sum_x c_x(\sigma-1)^{p^i+p^j-1}\mathfrak{g}_x = 0.$$

Since $\sum c_x(\sigma-1)^{p^i-1}\mathfrak{g}_x$ is a preimage of $\sum c_x x$, this dependence shows that a minimal preimage of $\sum c_x x$ has dimension strictly less than p^j+1. This contradicts Lemma 5.14. □

The proof of Theorem 5.13(1)

Lemma 5.22. *Let $j \in \{-\infty, 0, \cdots, n-1\}$. Then*

- *when $j = -\infty$, $\left(\sum_i X_{i,j}^G\right) \cap \iota_{n-1}^n(k_m E_{n-1}) = \{0\}$; and*
- *when $j \geq 0$, $\left(\sum_i X_{i,j}^G\right) \cap \iota_0^n(N_0^{j+1}(k_m E_{j+1})) = \{0\}$.*

Proof. In either case, by Lemmas 5.20 and 5.21 we have

$$\sum_i X_{i,j}^G = \sum_i (\sigma-1)^{p^i+p^j-1} X_{ij}. \tag{5.23}$$

From this equation, we check the first statement by assuming there exists some $\alpha \in k_m E_{n-1}$ with

$$0 \neq \sum_i \sum_{x \in \mathcal{I}_{i,-\infty}} c_x(\sigma-1)^{p^i-1}\mathfrak{g}_x = \iota_{n-1}^n(\alpha).$$

Applying N_{n-1}^n to each side we have 0 on the right and $\{a_{n-1}\}\cdot(\sum c_x x)$ on the left. But $\{a_{n-1}\}\cdot(\sum c_x x) \neq 0$ since the $x \in \Gamma(m,n)$ are chosen to be independent, and so we have a contradiction.

Again using Equation (5.23), we check the second statement by assuming we can write

$$0 \neq \sum_i \sum_{x \in \mathcal{I}_{i,j}} c_x(\sigma-1)^{p^i+p^j-1}\mathfrak{g}_x = \iota_0^n(N_0^{j+1}(\alpha))$$

for some $\alpha \in k_m E_{j+1}$. Writing $\alpha' = (\sigma-1)^{p^{j+1}-p^j-1}\alpha$ we have $N^n_{n-1}(\alpha') = 0$; this is immediate when $j < n-1$ because $\iota^n_{n-1}(k_m E_{n-1}) \subseteq \ker N^n_{n-1}$, and is true when $j = n-1$ since then

$$\alpha' \in \operatorname{im}\left((\sigma-1)^{p^n-p^{n-1}-1}\right) \overset{\star}{\subseteq} \operatorname{im}\left((\sigma-1)^{p^{n-1}}\right) \subseteq \ker N^n_{n-1},$$

where containment $\star$ follows since $p > 2$. This implies that $\left(\sum c_x(\sigma-1)^{p^i-1}\mathfrak{g}_x\right) - \alpha'$ is a preimage of $\sum c_x x$.

We also have $(\sigma-1)^{p^j}\alpha' = \iota^n_0(N^{j+1}_0(\alpha))$, so that

$$(\sigma-1)^{p^j}\alpha' = (\sigma-1)^{p^j}\left(\sum_i \sum_{x\in\mathcal{I}_{i,j}} c_x(\sigma-1)^{p^i-1}\mathfrak{g}_x\right).$$

Hence $\ell_G\left(\left(\sum c_x(\sigma-1)^{p^i-1}\mathfrak{g}_x\right) - \alpha'\right) < p^j$, and so a minimal preimage of $\sum c_x x$ has dimension strictly less than p^j+1. By Lemma 5.9, $\sum c_x x$ must therefore have a minimal preimage of dimension at most $p^{j-1}+1$, and therefore lies in $I_{0,j-1}$. This contradicts the choice of the elements x, which were to sit in a complement of a submodule containing $I_{0,j-1}$. □

Lemma 5.24. *$X = \oplus_{i,j} X_{i,j}$.*

Proof. We proceed by induction on the index set (i,j). Suppose we have already shown $\sum_{(i,j)<(\tilde{i},\tilde{j})} X_{i,j} = \oplus X_{i,j}$. Now if we have a dependence

$$\sum_{(i,j)\le(\tilde{i},\tilde{j})} \sum_{x\in\mathcal{I}_{i,j}} c_x f_x(\sigma)\mathfrak{g}_x = 0,$$

then the Exclusion Lemma 2.8 allows us to assume this dependence occurs in the fixed submodule, so that we have

$$\sum_{i,j} \sum_{x\in\mathcal{I}_{i,j}} c_x(\sigma-1)^{p^i+p^j-1}\mathfrak{g}_x = 0.$$

We must have $c_x \neq 0$ for some $x \in \mathcal{I}_{\tilde{i},\tilde{j}}$ since the submodules $X_{i,j}$ are independent for

$(i,j) < (\tilde{i},\tilde{j})$.

Suppose first that there is a nontrivial coefficient c_x in this sum where $x \in \mathcal{I}_{\hat{i},\hat{j}}$ and $\hat{j} < \tilde{j}$. Choosing $\hat{j}$ to be the smallest index which shows up (nontrivially) in the dependence, we reorganize and find

$$\sum_i \sum_{x \in \mathcal{I}_{i,\hat{j}}} c_x (\sigma - 1)^{p^i - p^{\hat{j}} - 1} \mathfrak{g}_x = - \sum_{j > \hat{j}} \sum_i \sum_{x \in \mathcal{I}_{i,j}} c_x (\sigma - 1)^{p^i - p^j - 1} \mathfrak{g}_x.$$

We shall examine the left- and right-hand side of this equation to arrive at a contradiction; we shall consider the cases $\hat{j} = -\infty$ and $\hat{j} \geq 0$ separately.

In the case $\hat{j} = -\infty$, the left-hand side is a (nontrivial) element of $\sum_i X^G_{i,-\infty}$ (it is nontrivial since by induction we have already verified $\sum_i X_{i,\hat{j}} = \oplus_i X_{i,\hat{j}}$). The right-hand side, however, is an element of $\iota^n_{n-1}(k_m E_{n-1})$. This follows because a generator $\mathfrak{g}_x$ of $X_{i,j}$ has $(\sigma - 1)^{p^i} \mathfrak{g}_x \in \ker N^n_{n-1}$, and hence (since $j > -\infty$ and using Lemma 5.20) we have $(\sigma - 1)^{p^i + p^j - 1} \mathfrak{g}_x \in \ker N^n_{n-1} \cap (k_m E_n)^G$. But this submodule is contained in $\iota^n_0(k_m E_0) \subseteq \iota^n_{n-1}(k_m E_{n-1})$ by Lemma 3.17, as claimed. Hence we have

$$\sum_i X^G_{i,-\infty} \cap \iota^n_{n-1}(k_m E_{n-1}) \neq \{0\},$$

contradicting the first part of Lemma 5.22.

In the case $\hat{j} \geq 0$, the left-hand side is a (nontrivial) element of $\sum_i X^G_{i,\hat{j}}$. The right-hand side is an element of $\iota^n_0(N_0^{\hat{j}+1}(k_m E_{\hat{j}+1}))$ by Lemma 5.9 and the fact that $\iota^n_0(N_0^{\hat{j}+k}(k_m E_{\hat{j}+k})) \subset \iota^n_0(N_0^{\hat{j}+1}(k_m E_{\hat{j}+1}))$ for every $k \geq 1$. Hence we have

$$\sum_i X^G_{i,\hat{j}} \cap \iota^n_0(N_0^{\hat{j}+1}(k_m E_{\hat{j}+1})) \neq \{0\},$$

contradicting Lemma 5.22.

In either case we see that our dependence only involves elements $x \in \mathcal{I}_{i,j}$ where $j = \tilde{j}$, and so our dependence takes the form

$$\sum_i \sum_{x \in \mathcal{I}_{i,\tilde{j}}} c_x (\sigma - 1)^{p^i + p^{\tilde{j}} - 1} \mathfrak{g}_x = 0.$$

Since $(\sigma-1)^{p^i-1}\mathfrak{g}_x$ is a minimal preimage of x, this implies the element $\sum c_x x$ has a minimal preimage of dimension at most $p^{\tilde{j}}$. By Lemma 5.9, $\sum c_x x$ has a minimal preimage of dimension at most $p^{\tilde{j}-1}+1$, and hence $\sum c_x x$ must lie in $I_{0,\tilde{j}-1}$. But each $x \in \mathcal{I}_{i,\tilde{j}}$ is selected to lie in a complement of this submodule, and so we have a contradiction. □

The proof of Theorem 5.13(5)

Lemma 5.25. *For* $0 \le j \le n-1$,

$$X \cap \iota_0^n(N_0^j(k_m E_j)) = \oplus_{i'} \oplus_{j' \ge j} X^G_{i',j'}.$$

Proof. First we note that $\oplus_{i'} \oplus_{j' \ge j} X^G_{i',j'} = \sum_{i'} \sum_{j' \ge j} X^G_{i',j'}$ by Lemma 5.24. Lemma 5.9 gives the $\supseteq$ containment.

For the opposite containment, we show that for any $\hat{j} < j$ we have

$$\sum_i X^G_{i,\hat{j}} \cap \iota_0^n(N_0^j(k_m E_j)) = \{0\},$$

which by the Exclusion Lemma 2.8 gives $X_{i,\hat{j}} \cap \iota_0^n(N_0^j(k_m E_j)) = \{0\}$. Then the independence of the $X_{i,j}$ gives $\oplus_i \oplus_{\hat{j}<j} X_{i,\hat{j}} \cap \iota_0^n(N_0^j(k_m E_j)) = \emptyset$, which implies the desired result.

First, if $\hat{j} \ge 0$ then Lemma 5.22 gives

$$\{0\} = \sum_i X^G_{i,\hat{j}} \cap \iota_0^n(N_0^{\hat{j}+1}(k_m E_{\hat{j}+1})) \supseteq \sum_i X^G_{i,\hat{j}} \cap \iota_0^n(N_0^j(k_m E_j)).$$

For $\hat{j} = -\infty$, Lemma 5.22 gives

$$\{0\} = \sum_i X^G_{i,-\infty} \cap \iota_{n-1}^n(k_m E_{n-1}) \supseteq \sum_i X^G_{i,-\infty} \cap \iota_0^n(N_0^j(k_m E_j)).$$

□

The proof of Theorem 5.13(4)

Lemma 5.26. *Let $x_l \in \mathcal{I}_{i(l),j(l)}$ for $1 \le l \le r$, and let $c_l \in \mathbb{F}_p^\times$ and $1 \le e(l) \le p^{i(l)} - 1$. Suppose that there exists ℓ so that $\ell = \ell\left(c_l(\sigma-1)^{e(l)}\mathfrak{g}_{x_l}\right)$ for all $1 \le l \le r$. Then $\mathfrak{g} := \sum_l c_l(\sigma-1)^{e(l)}\mathfrak{g}_{x_l}$ is a minimal preimage of $\gamma := \sum_l c_l(\sigma-1)^{e(l)}\gamma_{x_l}$.*

Proof. Suppose this is not the case, and let $\mathfrak{h}$ be a minimal preimage of γ. Let $j = \min\{j(l)\}$, and (without loss) assume that $j(l) = j$ for $1 \le l \le s$, and that $j(l) > j$ for $l > s$. Hence for $l > s$ we have $\ell - p^j - 1 + e(l) = p^{i(l)} + p^{j(l)} - p^j - 1 \ge p^{i(l)}$, and so $\ell_{G_{n-1}}(\gamma_{x_l}) = p^{i(l)}$ gives $(\sigma-1)^{\ell-p^j-1+e(l)}\gamma_{x_l} = 0$.

We compute:

$$\begin{aligned} N_{n-1}^n\left((\sigma-1)^{\ell-p^j-1}\mathfrak{h}\right) &= (\sigma-1)^{\ell-p^j-1}\{a_{n-1}\}\cdot\left(\sum_{1\le l\le r} c_l(\sigma-1)^{e(l)}\gamma_{x_l}\right) \\ &= \{a_{n-1}\}\cdot\left(\sum_{1\le l\le r}(\sigma-1)^{\ell-p^j-1+e(l)}\gamma_{x_l}\right) \\ &= \{a_{n-1}\}\cdot\left(\sum_{1\le l\le s}(\sigma-1)^{\ell-p^j-1+e(l)}\gamma_{x_l}\right). \end{aligned}$$

This implies that $(\sigma-1)^{\ell-p^j-1}\mathfrak{h}$ is a preimage of $\sum_{1\le l\le s} c_l x_l \in \sum_{i=0}^{n-1}\langle\mathcal{I}_{i,j}\rangle$.

But now $\ell(\mathfrak{h}) < \ell$, and so we have $\ell\left((\sigma-1)^{\ell-p^j-1}\mathfrak{h}\right) = \ell(\mathfrak{h}) - (\ell - p^j - 1) < p^j + 1$. Since $\sum_{l=1}^s c_l x_l$ has a preimage of length less than p^j+1, Lemma 5.9 says that it has a preimage of length at most $p^{j-1}+1$, and so $\sum_{l=1}^s c_l x_l \in I_{0,j-1}$. This, however, contradicts the construction of the $\mathcal{I}_{i(l),j}$ $(1 \le l \le s)$. □

We are prepared to prove Theorem 5.13(4), though we state a more precise result. Lemma 5.17 implies that every element $\gamma \in \Gamma(m,n)$ can be written uniquely as an $\mathbb{F}_p$-linear combination of the elements $(\sigma-1)^e\gamma_x$, where x ranges through all elements of $\mathcal{I}_{i,j}$, i and j range through $\{0,\cdots,n-1\}$ and $\{-\infty,\cdots,i(E/F)\}$ (respectively), and $0 \le e \le p^i - 1$. The following lemma says that the 'obvious' preimage of γ in X is a minimal preimage.

Lemma 5.27. *Suppose that $\gamma \in \Gamma(m,n)$ takes the form*

$$\gamma = \sum_{i,j} \sum_{x \in \mathcal{I}_{i,j}} \sum_{e=0}^{p^i-1} c_{e,x}(\sigma-1)^e \gamma_x.$$

Then

$$\sum_{i,j} \sum_{x \in \mathcal{I}_{i,j}} \sum_{e=0}^{p^i-1} c_{e,x}(\sigma-1)^e \mathfrak{g}_x$$

is a minimal preimage for γ.

Proof. For a pair e, x, let $\ell_{e,x} := \ell\left(c_{e,x}(\sigma-1)^e \mathfrak{g}_x\right)$. Lemma 5.26 says that for fixed ℓ we have

$$\sum_{\ell_{e,x}=\ell} c_{e,x}(\sigma-1)^e \mathfrak{g}_x$$

is a minimal preimage of $\sum_{\ell_{e,x}=\ell} c_{e,x}(\sigma-1)^e \gamma_x$. Hence Lemma 5.8 says that

$$\sum_{\ell} \sum_{\ell_{e,x}=\ell} c_{e,x}(\sigma-1)^e \mathfrak{g}_x$$

is a minimal preimage of

$$\sum_{\ell} \sum_{\ell_{e,x}=\ell} c_{e,x}(\sigma-1)^e \gamma_x = \gamma.$$

□

Remark 5.28. The previous lemma doesn't just tell us that X contains a minimal preimage for every $\gamma \in \Gamma(m,n)$. In fact, the lemma tells us that our Assumption 5.1 is equivalent to the *a priori* stronger

Assumption 5.29. *For every $\gamma \in \Gamma(m,n)$, if $\mathfrak{g}$ is a minimal preimage of γ then $(\sigma-1)\mathfrak{g}$ is a minimal preimage of $(\sigma-1)\gamma$.*

5.4 Proof of Theorem 5.2

Let $X = \oplus_{i,j} X_{i,j}$ be defined as in the previous section, and we construct the submodules Y_i.

For $i = n$, let $\mathcal{I}_n$ be an $\mathbb{F}_p$-basis for $\iota_0^n(N_0^n(k_m E_n))$. For each $x \in \mathcal{I}_n$ choose an element $\alpha_x \in k_m E_n$ with $x = \iota_0^n(N_0^n(\alpha_x))$, and define $Y_n = \sum_{x \in \mathcal{I}_n} \langle \alpha_x \rangle_{\mathbb{F}_p[G]}$. The Exclusion Lemma 2.8 gives $\sum_{x \in \mathcal{I}_n} \langle \alpha_x \rangle_{\mathbb{F}_p[G]} = \oplus_{x \in \mathcal{I}_n} \langle \alpha_x \rangle_{\mathbb{F}_p[G]}$, and so Y_n is a direct sum of free $\mathbb{F}_p[G]$-modules.

For $i < n$, let $\mathcal{I}_i$ be an $\mathbb{F}_p$-basis for a complement of

$$\langle \iota_0^n(N_0^{i+1}(k_m E_{i+1})), X \cap \iota_0^n(N_0^i(k_m E_i)) \rangle_{\mathbb{F}_p}$$

within $\iota_0^n(N_0^i(k_m E_i))$. For each $x \in \mathcal{I}_i$ choose $\alpha_x \in k_m E_i$ with $\iota_0^n(N_0^i(\alpha_x)) = x$, and define $Y_i = \sum_{x \in \mathcal{I}_i} \langle \alpha_x \rangle_{\mathbb{F}_p[G]}$. This gives $Y_i \subseteq \iota_i^n(k_m E_i)$. As always, the Exclusion Lemma 2.8 ensures $Y_i = \oplus_{x \in \mathcal{I}_i} \langle \alpha_x \rangle_{\mathbb{F}_p[G]}$, and hence Y_i is a direct sum of free $\mathbb{F}_p[G_i]$-modules.

Our construction also implies

$$\iota_0^n(N_0^j(k_m E_j)) = \sum_{j' \geq j} Y_{j'}^G + \left(X \cap \iota_0^n(N_0^j(k_m E_j)) \right),$$

which by Theorem 5.13(5) gives

$$\iota_0^n(N_0^j(k_m E_j)) = \sum_{j' \geq j} Y_{j'}^G + \sum_i \sum_{j' \geq j} X_{i,j'}^G. \tag{5.30}$$

The submodule Y_n is independent from the submodule $\oplus_{i,j} X_{i,j}$ because $Y_n^G \subseteq \iota_0^n(N_0^n(k_m E_n))$, whereas $\oplus_{i,j} X_{i,j} \cap \iota_0^n(N_0^n(k_m E_n)) = \{0\}$ by Theorem 5.13(5). So assume $Y_{k+1} + \cdots + Y_n + \sum_{i,j} X_{i,j} = Y_{k+1} \oplus \cdots \oplus Y_n \oplus \oplus_{i,j} X_{i,j}$, and we show that Y_k is independent from this collection. For this we remark that $Y_k^G \subseteq \iota_0^n(N_0^k(k_m E_k))$ is chosen in a complement to the space spanned by $\iota_0^n(N_0^{k+1}(k_m E_{k+1})) \supseteq \oplus_{i \geq k+1} Y_i^G$ and $X \cap \iota_0^n(N_0^k(k_m E_k))$. The Exclusion Lemma 2.8 implies that Y_k is independent from

all of Y_i (for $i \geq k+1$) and $\oplus_{i,j} X_{i,j}$. Hence

$$Y_0 + \cdots + Y_n + \sum_{i,j} X_{i,j} = Y_0 \oplus \cdots \oplus Y_n \oplus \bigoplus_{i,j} X_{i,j} := J.$$

We only have to show that $k_m E_n = J$, which we do by induction on the length of elements. First, we claim that for any element with length at most $p^n - p^{n-1}$ there exists $\gamma' \in k_m E_n$ with $N^n_{n-1}(\gamma') = 0$, $\ell_G(\gamma') \leq \ell_G(\gamma)$, and so that $\gamma' \in J$ implies $\gamma \in J$. For this, suppose that $N^n_{n-1}(\gamma) \neq 0$, since otherwise there is nothing to do. Since $(\sigma-1)^{p^n - p^{n-1}} = \iota^n_0 \circ N^n_{n-1}$ annihilates γ, we have $N^n_{n-1}(\gamma) \in \ker \iota^n_{n-1}$. Hence we have $N^n_{n-1}(\gamma) = \{a_{n-1}\} \cdot g$ for some $g \in \Gamma(m,n)$. Theorem 5.13(4) says there exists $\mathfrak{g} \in X$ so that $\mathfrak{g}$ is a minimal preimage of g. Hence we have $\gamma' = \gamma - \mathfrak{g} \in \ker N^n_{n-1}$, and that $\ell(\gamma') \leq \ell(\gamma)$ by minimality of $\mathfrak{g}$. Finally, if $\gamma' \in J$, then because $\mathfrak{g} \in X \subseteq J$ we also have $\gamma \in J$. Hence if $\ell_G(\gamma) \leq p^n - p^{n-1}$, we can (and do) assume that $\gamma \in N^n_{n-1}$.

Let γ be an element of length 1. Then clearly $\ell_G(\gamma) \leq p^n - p^{n-1}$, so we can assume $N^n_{n-1}(\gamma) = 0$. Lemma 3.17 gives $\gamma \in \iota^n_0(k_m E_0)$, and hence Equation (5.30) gives $\gamma \in J$.

Suppose that $\ell(\gamma) = p^k + l$ for some $l \geq 2$. If $\ell_G(\gamma) \leq p^n - p^{n-1}$ then we can assume $\gamma \in \ker N^n_{n-1}$. Hence Corollary 3.20 gives $(\sigma-1)^{\ell(\gamma)-1}\gamma \in \iota^n_0(N^{k+1}_0(k_m E_{k+1}))$. By Equation (5.30) and the construction of the Y_i and $X_{i,j}$, we can find some $\alpha \in \bigoplus_{j' \geq k+1} Y_{j'} \oplus \bigoplus_i \bigoplus_{j' \geq k+1} X_{i,j'}$ with

$$(\sigma-1)^{\ell(\gamma)-1}\gamma = \iota^n_0(N^{k+1}_0(\alpha)) = (\sigma-1)^{p^{k+1}-1}\alpha.$$

Hence $\gamma - (\sigma-1)^{p^{k+1}-\ell(\gamma)}\alpha$ is an element of length at most $\ell(\gamma)-1$, and so is in J. But since $\alpha \in J$, so too is γ.

Finally, suppose that γ has $\ell(\gamma) > p^n - p^{n-1}$. Since $p > 2$ this gives $\ell(\gamma) > 2p^{n-1}$, and so Lemma 3.18 gives $(\sigma-1)^{\ell(\gamma)-1}\gamma \in \iota^n_0(N^n_0(k_m E_n))$. But Y^G_n is an $\mathbb{F}_p$-basis for $\iota^n_0(N^n_0(k_m E_n))$, so there exists some $\alpha \in Y_n$ with

$$(\sigma-1)^{\ell(\gamma)-1}\gamma = \iota^n_0(N^n_0(\alpha)) = (\sigma-1)^{p^n-1}(\alpha).$$

Therefore $\gamma - (\sigma-1)^{p^n-\ell(\gamma)}\alpha$ is an element of length at most $\ell(\gamma)-1$, and so by

induction is in J. Since $\alpha \in J$, we have $\gamma \in J$ also.

Bibliography

[1] D. Benson, N. Lemire, J. Mináč, and J. Swallow. Detecting pro-p-groups that are not absolute Galois groups. *J. Reine Angew. Math.* To appear.

[2] F. Chemotti, J. Mináč, and J. Swallow. Galois module structure for square classes of units in Klein 4-group extensions. In preparation.

[3] D.K. Faddeev. On the structure of the reduced multiplicative group of a cyclic extension of a local field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 24:145–152, 1960.

[4] I.B. Fesenko and S.V. Vostokov. *Local Fields and their extensions.* Translations of Math. Monographs 121. AMS, Providence, RI, 2nd edition, 2002.

[5] E. Friedlander and C. Weibel. An overview of algebraic K-theory. In H. Bass, A. Kuku, and C. Pedrini, editors, *Algebraic K-theory and its applications (Trieste, 1997).* River Edge, NJ, 1999.

[6] J. Labute, N. Lemire, J. Mináč, and J. Swallow. Demuškin groups, Galois modules, and the Elementary Type Conjecture. *J. of Alg.*, 304:1130–1146, 2006.

[7] N. Lemire, J. Mináč, and J. Swallow. Galois module structure of Galois cohomology and partial Euler-Poincaré characteristics. *J. Reine Angew. Math.* To appear.

[8] J. Mináč, A. Schultz, and J. Swallow. Automatic realizations of Galois groups with cyclic quotient of order p^n. In review.

[9] J. Mináč, A. Schultz, and J. Swallow. Galois module structure of Milnor k-theory mod p^s in characteristic p. Available at http://arxiv.org/pdf/math.NT/0602546.

[10] J. Mináč, A. Schultz, and J. Swallow. Galois module structure of pth-power classes of cyclic extensions of degree p^n. *Proc. London Math. Soc.*, 2(92):307–347, 2006.

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

[12] J. Mináč and J. Swallow. Galois embedding problems with cyclic quotient of order p. *Israel J. Math.*, 145:93, 2005.

[13] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer, New York, NY, 2000.

[14] V. Voevodsky. Motivic cohomology with $\mathbb{Z}/2$-coefficients. *Publ. Inst. Hautes Études Sci.*, (98):59–104, 2003.

[15] W. Waterhouse. The normal closures of certain Kummer extensions. *Canad. Math. Bull.*, 37(1):133–139, 1994.