The Galois Cohomology of Square-Classes of Units in Klein-Four Group Extensions of Characteristic Not Two:
A Thesis Submitted to the Department of Mathematics for Honors

Jason Ferguson
Duke University, Durham, NC
Submitted Wednesday, April 22, 2009
## Contents

Chapter 1. Introduction
   1. Acknowledgments 5
   2. Introduction and Statement of Results 5
   3. Brief Summary of the Proof 8

   1. The Exclusion Lemma and Related Results 13
   2. A Proof That Ten $F_2[G]$-Modules are Indecomposable 14
   3. Analysis of $F_2[G]$-Modules $M$ that Satisfy $\sum_{i=1}^{3} (\rho_i M \cap M^G) \subseteq \sum_{i \neq j} \rho_i M^{(\tau_j)}$ 19

Chapter 3. Review of Galois Cohomology
   1. Topological Groups 35
   2. Infinite Galois Theory 35
   3. Inverse Limits and Profinite Groups 37
   4. Cohomology of Profinite Groups 39
   5. Inflation, Conjugation, Restriction, Corestriction, and Cup-Product 45
   6. Direct Limits 53
   7. Shapiro’s Lemma 56
   8. Kummer Theory 58
   9. Central Simple Algebras, the Brauer Group, and Cyclic Algebras 60

Chapter 4. Decomposition of $E^\times/(E^\times)^2$
   1. A Decomposition of $H^1(G_F, V)$ 65
   2. Consequences of Shapiro’s Lemma 85
   3. Connections to Kummer Theory and Brauer Groups 87
   4. Construction of $X$ and $Y$ 90

Chapter 5. Final Remarks and Directions for Possible Further Research 99

Bibliography 101
CHAPTER 1

Introduction

1. Acknowledgments

I am very grateful to Prof. Chad Schoen for working with me in independent studies since the summer of 2007, to Prof. John Swallow for allowing me to work at Davidson College in the summer of 2008, and to Dr. Kraines for his encouragement. I was supported by a PRUV fellowship in the summer of 2007.

2. Introduction and Statement of Results

This report is an expository article that gathers and proves some of the results of a certain unpublished paper [CMS] co-authored by Prof. John Swallow of Davidson College. For this paper, I assume familiarity with abstract algebra at the level of MATH 251 and point-set topology at the level of MATH 205. I also assume the reader has had some experience with infinite Galois theory; cohomology of profinite groups; operations on the cohomology of profinite groups, including conjugation, inflation, corestriction, and cup-product; Kummer theory; and Brauer groups. However, all of these latter topics will be quickly reviewed within this report in Chapter 3.

The topic of [CMS] is as follows: Let \( p \) be a prime number and \( n \) a positive integer. Let \( E/F \) be a Galois extension of fields whose Galois group is isomorphic to \( \mathbb{Z}/p^n \mathbb{Z} \). Then, if we let \( F_q \) denote the field of \( q \) elements, the multiplicative abelian group \( E^x/(E^x)^p \) is a module over the group algebra \( F_p[\text{Gal}(E/F)] \). Elements of \( \text{Gal}(E/F) \) act as automorphisms on \( E^x/(E^x)^p \), and this makes \( E^x/(E^x)^p \) a \( \mathbb{Z}[\text{Gal}(E/F)] \)-module. For all \( \alpha \in E^x/(E^x)^p \), \( \alpha^p = 1 \), so this \( \mathbb{Z}[\text{Gal}(E/F)] \) structure induces an \( F_p[\text{Gal}(E/F)] \)-structure on \( E^x/(E^x)^p \).

It is then natural to try to write the module \( E^x/(E^x)^p \) as a direct sum of indecomposable modules over the group ring \( F_p[\text{Gal}(E/F)] \). [CMS] gives this decomposition in the case that \( p = 2 \) and \( n = 2 \). The remarkable thing about this decomposition is that there is a finite set \( S \) of isomorphism classes of indecomposable modules over \( F_2[\text{Gal}(E/F)] \) such that for any field extension \( E/F \), only modules in \( S \) can appear in the decomposition of \( E^x/(E^x)^2 \). Furthermore, in [CMS], the cardinality with which each element of \( S \) appears is given in terms of invariants of the field extension \( E/F \). In this report, we will decompose \( E^x/(E^x)^2 \) in the case that \( \text{char}(F) \neq 2 \).

The topic of [CMS] is a natural generalization of the papers [MS] and [MSS]. In [MS], \( E/F \) is any Galois extension of fields such that \( \text{Gal}(E/F) \cong \mathbb{Z}/p^n \mathbb{Z} \) for a prime \( p \), and the module \( E^x/(E^x)^p \) is decomposed over \( F_p[\text{Gal}(E/F)] \). In [MSS], \( E/F \) is any Galois extension of fields such that \( \text{Gal}(E/F) \cong \mathbb{Z}/p^n \mathbb{Z} \) for a prime \( p \) and positive integer \( n \), and the module \( E^x/(E^x)^p \) is decomposed over \( F_p[\text{Gal}(E/F)] \). In both [MS] and [MSS], it is found that there is a finite list of indecomposable \( F_p[\text{Gal}(E/F)] \)-modules that can appear as a direct summand in the direct-sum decomposition of \( E^x/(E^x)^p \).

In order to state what the module in \( S \) are, we first need to introduce notation to describe modules over \( F_2[\text{Gal}(E/F)] \). Let \( G \) denote \( \text{Gal}(E/F) \cong (\mathbb{Z}/2\mathbb{Z})^2 \), and denote the elements of \( G \) as \( 1, \tau_1, \tau_2, \) and \( \tau_3 \), where \( \tau_3 = \tau_1 \tau_2 \). Then we are trying to decompose \( E^x/(E^x)^2 \) over \( F_2[G] \). For \( i \in \{1, 2, 3\} \), let \( \rho_i = \tau_i - 1 \in F_2[G] \), so that \( \rho_3 = \rho_1 \rho_2 + \rho_1 + \rho_2 \). Then we have:

\[
F_2[G] = F_2[\tau_1, \tau_2]/(\tau_1^2 - 1, \tau_1^2 - 1) = F_2[\rho_1, \rho_2]/(\rho_1^2, \rho_2^2) .
\]
(For the rest of this proof, \( (r_i) \) will be used to denote the ideal generated by the elements \( r_i \), while \( \langle r_i \rangle \) will be used to denote either the subgroup generated by \( r_i \) or the subspace spanned by \( r_i \), according to context.)

Now, many \( \mathbb{F}_2[G] \) modules can be depicted as directed graphs where each arrow can only emanate from either the bottom-left or bottom-right of a vertex. An example of such a directed graph is shown below; it corresponds to \( \mathbb{F}_2[G] \) acting on itself by left multiplication:

The vertices of such a graph depict the elements in an \( \mathbb{F}_2 \) basis of the module: each vertex corresponds to a different basis element. In the previous directed graph, the correspondence is as follows:

In general, the arrows pointing down and to the left indicate the action of \( \rho_1 \) on this module: If there is an arrow from vertex \( V_1 \) to vertex \( V_2 \) and the arrow emanates from the bottom-left of \( V_1 \), then \( \rho_1 \) times the basis element corresponding to \( V_1 \) is the basis element corresponding to \( V_2 \); if a vertex \( V \) has no arrow emanating from the bottom-left, then \( \rho_1 \) annihilates the basis element corresponding to \( V \). Similarly, the arrows pointing down and to the right indicate the action of \( \rho_2 \) on this module: If there is an arrow from vertex \( V_1 \) to vertex \( V_2 \) and the arrow emanates from the bottom-right, then \( \rho_2 \) times the basis element corresponding to \( V_1 \) is the basis element corresponding to \( V_2 \); if a vertex \( V \) has no arrow emanating from it that points down and to the right, then \( \rho_2 \) annihilates the basis element corresponding to \( V \).

To illustrate more examples of depicting \( \mathbb{F}_2[G] \)-modules as directed graphs, we let \( \mathbb{F}_2 \) denote the trivial one-dimensional \( \mathbb{F}_2[G] \) module. Then the diagrams corresponding to \( \mathbb{F}_2 \), \( \mathbb{F}_2[G]/(\rho_1) \), \( \mathbb{F}_2[G]/(\rho_2) \), and \( \mathbb{F}_2[G]/(\rho_3) \) are, respectively:

Define the modules \( \Omega(1) \), \( \Omega(2) \), and \( \Omega(3) \) to be the \( \mathbb{F}_2[G] \)-modules that correspond to the following three directed graphs, respectively,

and define \( \Omega(-1) \), and \( \Omega(-2) \) to be the \( \mathbb{F}_2[G] \)-modules corresponding to the following two directed graphs, respectively.

We may now give the list of ten indecomposable \( \mathbb{F}_2[G] \)-modules that can appear as a direct summand in \( E^\times/(E^\times)^2 \). They are:

\[
\mathbb{F}_2[G] \quad \mathbb{F}_2[G]/(\rho_1) \quad \mathbb{F}_2[G]/(\rho_2) \quad \mathbb{F}_2[G]/(\rho_3) \quad \mathbb{F}_2 \quad \Omega(1) \quad \Omega(2) \quad \Omega(3) \quad \Omega(-1) \quad \Omega(-2).
\]
To state the cardinalities with which each module appears, we need a bit more notation. More specifically, since \( \text{char}(F) \neq 2 \), \( F \) must have a primitive square root of unity (i.e. \(-1\)). Thus, from Kummer theory, since \( \text{Gal}(E/F) \cong (\mathbb{Z}/2\mathbb{Z})^2 \), there are elements \( a_1, a_2 \in F^\times \) such that:

\[
E = F (\sqrt{a_1}, \sqrt{a_2}).
\]

For any element \( a \in F^\times \), we let \( \overline{a} \) denote the class of \( a \) in \( F^\times/(F^\times)^2 \). We let:

\[
\mathcal{A}' = \text{Span}_{F_2}(\overline{a_1}, \overline{a_2}) \subseteq F^\times/(F^\times)^2.
\]

For \( a, b \in F^\times \), we let \((a, b)\) denote a generalized quaternion algebra. More specifically, let \((a, b)\) denote the unique four-dimensional associative \( F \)-algebra with multiplicative identity 1, basis \( \{1, i, j, k\} \), and multiplication defined as \( k = ij = -ji, \ i^2 = a, \) and \( j^2 = b \). Then from elementary properties of the Brauer group, \((a, b)\) represents an element of \( 2\text{Br}(F) \), where \( \text{Br}(F) \) denotes the Brauer group of \( F \) and \( 2\text{Br}(F) \) denotes the 2-torsion part of \( \text{Br}(F) \). Note that if \( a'/a, b'/b \in F^\times/(F^\times)^2 \), then \((a', b') \cong (a, b)\) as \( F \)-algebras, so the object \((\overline{a}, \overline{b})\) is well-defined as an element of \( 2\text{Br}(F) \).

Next, let \( \mathcal{B}' \) denote:

\[
\text{Span}_{F_2}((\overline{a_1}, \overline{a_1}), (\overline{a_1}, \overline{a_2}), (\overline{a_2}, \overline{a_2})) \subseteq 2 \text{Br}(F),
\]

and let \((\overline{a}, \overline{b})\) denote the class of \((\overline{a}, \overline{b})\) in \( 2\text{Br}(F)/\mathcal{B}' \). Finally, note that if \( N_{E/F} : E \to F \) is the norm from the field extension \( E/F \), then we have that \( N_{E/F}( (E^\times)^2) \subseteq (F^\times)^2 \), so \( N_{E/F} \) descends to a well-defined function from \( E^\times/(E^\times)^2 \) to \( F^\times/(F^\times)^2 \).

Now we may state the cardinalities with which each of the ten modules appear:

**Theorem 1.1.** Keeping all of the notation of this section, we let \( u, v, \) and \( w \) be as follows:

\[
v = \dim_{F_2}(\mathcal{A}' \cap N_{E/F}( (E^\times)^2))
\]

\[
w = 3 - \dim_{F_2}(\mathcal{B}')
\]

Further, let \( u = 1 \) if there are elements \( a_1, a_2 \in E^\times \) such that \( \overline{a_1} = N_{E/F}(\overline{a_1}), \overline{a_2} = N_{E/F}(\overline{a_2}) \), and \( \rho_1 \overline{a_1} = \rho_2 \overline{a_2} \), and let \( u = 0 \), otherwise. Then \( 0 \leq w \leq 3, 0 \leq v \leq 2, u = 1 \) implies \( v = 2 \), and \( w = 3 \) implies \( v = 2 \).

Furthermore, as \( F_2[G] \)-modules,

\[
E^\times/(E^\times)^2 \cong \mathcal{X} \oplus \mathcal{Y},
\]

where:

\[
\mathcal{X} \cong \begin{cases} 
F_2^w & \text{if } v = 0 \\
\Omega(-1) & \text{if } v = 1 \\
\Omega(-1) \oplus \Omega(-1) & \text{if } v = 2 \text{ and } u = 0 \\
\Omega(-2) & \text{if } v = 2 \text{ and } u = 1 
\end{cases}
\]

and \( \mathcal{Y} \) is a direct sum of some cardinal number of each of the following eight indecomposable modules:

\[
\begin{align*}
F_2[G] & \quad F_2[G]/(\rho_1) & \quad F_2[G]/(\rho_2) & \quad F_2[G]/(\rho_3) & \quad F_2 & \quad \Omega(1) & \quad \Omega(2) & \quad \Omega(3).
\end{align*}
\]

Let \( e, e_1, e_2, e_3, l_1, l_2, l_3 \), and \( z \) be the cardinalities of the direct summands of the previous eight indecomposable modules. Then:

\[
e + v = \dim_{F_2} N_{E/F}(E^\times/(E^\times)^2)
\]

\[
e_1 = \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_1}, f) = 0 \right\}
\]

\[
e_2 = \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_2}, f) = 0 \right\}
\]

\[
e_3 = \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_1}a_2, f) = 0 \right\}
\]

\[
\begin{align*}
e_1 &= \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_1}, f) = 0 \right\} \\
e_2 &= \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_2}, f) = 0 \right\} \\
e_3 &= \dim_{F_2} \left\{ f \in E^\times/(E^\times)^2 | (\overline{a_1}a_2, f) = 0 \right\}
\end{align*}
\]
l_1 = \dim_{F_2} \{ f \in F^*/(F^*)^2 | (\bar{a_1}, f) = (\bar{a_2}, f) = 0 \}

l_2 + l_3 = \dim_{F_2} \{ f \in F^*/(F^*)^2 | (\bar{a_1}, f) = (\bar{a_2}, f) = 0 \}

l_2 + 2l_3 = \dim_{F_2} \{ f \in F^*/(F^*)^2 | (\bar{a_1}, f) \in (\bar{a_2}, F^*/(F^*)^2) \}

3. Brief Summary of the Proof

This section gives an overview of the decomposition of $E^*/(E^*)^2$, outlines what each of the major steps are, and gives the general strategy of the proof. This section is included because this proof is very long and technical, and many of the major steps of the proof require several sub-lemmas. There will be no proofs in this section.

We continue to use all of the notation introduced in the introduction, namely that $\text{Gal}(E/F) \cong G = \{1, \tau_1, \tau_2, \tau_3\}$ and $\rho_1 = \tau_1 - 1 \in \mathbb{F}_2[G]$. We also let $F^{\text{sep}}$ denote any separable closure of $F$ that contains $E$, $G_F$ denote $\text{Gal}(F^{\text{sep}}/F)$, and $G_E$ denote $\text{Gal}(F^{\text{sep}}/E)$.

Also, as was hinted at in the introduction, for any group $H$ and prime number $p$, $H$-modules with exponent $p$ (i.e. $H$-modules $M$ such that $p \cdot m = 0$ for all $m \in M$) are identical to $\mathbb{F}_p[H]$-modules. For this reason, we identify $\mathbb{F}_2[G]$-modules and $G$-modules with exponent 2 for the rest of the proof.

As was mentioned in the introduction, the proof is written entirely using the language of Galois cohomology. For this reason, the first step of the proof is to use Kummer theory to prove that $E^*/(E^*)^2$ is isomorphic to $H^1(G_E, \mathbb{F}_2)$, with trivial action of $G_F$ on $\mathbb{F}_2$, as groups and to determine that the induced $\mathbb{F}_2[G]$-module action on $H^1(G_E, \mathbb{F}_2)$ is conjugation. It is $H^1(G_E, \mathbb{F}_2)$ that will be decomposed and not $E^*/(E^*)^2$.

$H^1(G_E, \mathbb{F}_2)$ is decomposed by precisely specifying the submodules $\mathcal{X}$ and $\mathcal{Y}$ stated in Theorem 1.1, directly proving that $\mathcal{X}$ is of the isomorphism types stated in Theorem 1.1, proving that $\mathcal{Y}$ satisfies the following property:

$$\sum_{i=1}^{3} \left( \rho_i \mathcal{Y} \cap \mathcal{Y}^G \right) \subseteq \sum_{i \neq j} \rho_i \mathcal{Y}^{\tau_j},$$

and then showing that $\mathcal{X} + \mathcal{Y} = \mathcal{X} \oplus \mathcal{Y}$ and that $H^1(G_E, \mathbb{F}_2) = \mathcal{X} \oplus \mathcal{Y}$.

Next, it is shown that for any $\mathbb{F}_2[G]$-module $M$, $M$ satisfies

$$\sum_{i=1}^{3} \left( \rho_i M \cap M^G \right) \subseteq \sum_{i \neq j} \rho_i M^{\tau_j},$$

if and only if $M$ is a direct sum of some cardinality of the following eight indecomposable modules:

$$\mathbb{F}_2[G] \quad \mathbb{F}_2[G]/(\rho_1) \quad \mathbb{F}_2[G]/(\rho_2) \quad \mathbb{F}_2[G]/(\rho_3) \quad \mathbb{F}_2 \quad \Omega(1) \quad \Omega(2) \quad \Omega(3),$$

and that it is possible to give precise module-theoretic value for the cardinal number with which each module appears. The remarkable thing about the proof of this statement is that it is incredibly constructive. In the course of the proof, every copy of each of those eight modules is precisely identified within $M$.

The next question to consider is how one obtains $\mathcal{X}$ and $\mathcal{Y}$. First, one uses Shapiro’s lemma to construct an isomorphism between $H^1(G_E, \mathbb{F}_2)$ and $H^1(G_F, \mathbb{F}_2[G])$ and computes what the induced action of $\mathbb{F}_2[G]$ on $H^1(G_F, \mathbb{F}_2[G])$. The action of $G_F$ on $\mathbb{F}_2[G]$ is natural; in fact, any continuous $G$-module is automatically a continuous $G_F$-module. This follows from the fundamental theorem of infinite Galois theory: As $E$ is an intermediate field in the Galois extension $F^{\text{sep}}/F$ such that $E/F$ is Galois, we have that $G_E \leq G_F$ and that $G_F/G_E \cong G$ as topological groups; an isomorphism
from $G_F/G_E$ to $G$ is induced by the continuous, surjective homomorphism $\phi : \sigma \mapsto \sigma|_E$ for $\sigma \in G_F$. Therefore, for any continuous $G$-module $M$, $G_F$ acts continuously on $M$ acts via:

$$\sigma \cdot m = \phi(\sigma) \cdot m.$$ 

Establishing the isomorphism between $H^1(G_F, F_2)$ and $H^1(G_F, \mathbb{F}_2[G])$ is important for the following reason: Let $V$ denote the following subset of $\mathbb{F}_2[G]$:

$$V = \text{Span}_{\mathbb{F}_2} \langle \rho_1, \rho_2, \rho_1\rho_2 \rangle.$$ 

Then $V$ is both the nilradical and the maximal ideal of $\mathbb{F}_2[G]$, and also:

$$V^G = \text{Span}_{\mathbb{F}_2} \langle \rho_1\rho_2 \rangle.$$ 

It so happens that we have:

$$\mathbb{F}_2 \cong V^G \subseteq V \subseteq \mathbb{F}_2[G],$$

and the successive quotients satisfy: $\mathbb{F}_2[G]/V \cong \mathbb{F}_2$ and $V/V^G \cong \mathbb{F}_2^2$. Thus, we can write down the following two exact sequences of $\mathbb{F}_2[G]$ modules

$$0 \longrightarrow \mathbb{F}_2 \overset{\iota_1}{\longrightarrow} V \overset{\pi_1}{\longrightarrow} V/V^G \longrightarrow 0.$$ 

$$0 \longrightarrow V \overset{\iota_2}{\longrightarrow} \mathbb{F}_2[G] \overset{\pi_2}{\longrightarrow} \mathbb{F}_2 \longrightarrow 0$$

Because of these short exact sequences, one has the following two exact sequences taken from the long exact sequence of cohomology:

$$H^1(G_F, \mathbb{F}_2) \overset{\iota_1}{\longrightarrow} H^1(G_F, V) \overset{\pi_1}{\longrightarrow} H^1(G_F, V/V^G) \cong (V/V^G) \otimes_{\mathbb{F}_2} H^1(G_F, \mathbb{F}_2)$$

$$H^0(G_F, \mathbb{F}_2) \overset{\partial_2}{\longrightarrow} H^1(G_F, V) \overset{\iota_2}{\longrightarrow} H^1(G_F, \mathbb{F}_2[G]).$$

Every term in these two exact sequences can be made into an $\mathbb{F}_2[G]$-module, and these four homomorphisms can be proved to be $\mathbb{F}_2[G]$-module homomorphisms. The interplay of these four homomorphisms involving $H^1(G_F, V)$, and their relation with rest of their respective long exact sequences is used to decompose $H^1(G_F, V)$ into a direct sum of four submodules.

Then, we map this decomposition forward to $H^1(G_F, \mathbb{F}_2[G])$ via $\iota_2^*$, and then use the map of Shapiro’s lemma to bring the image of the decomposition into $H^1(G_E, \mathbb{F}_2)$. Within $H^1(G_E, \mathbb{F}_2)$, this information from Galois cohomology is overlayed with field-theoretic information from $E^\times/(E^\times)^2$. The submodule $X$ and $Y$ are described using this information.

With this kind of description of the proof it is difficult to see what the key original idea of the proof is. This key idea is to convert the common slot lemma for quaternion algebras into the language of cohomology and to use this restated result to prove that $\mathcal{Y}$ satisfies the property:

$$\sum_{i=1}^{3} (\rho_i \mathcal{Y} \cap \mathcal{Y}^{\rho_i}) \subseteq \sum_{i \neq j} \rho_i \mathcal{Y}^{(\rho_j)}.$$ 

The common slot lemma is the following property of quaternion algebras: For $a, b, c, d \in F$, if $(a, b) \cong (c, d)$ as $F$-algebras, then there is an $e \in F$ such that:

$$(a, b) \cong (a, e) \cong (c, e) \cong (c, d),$$

each as $F$-algebras.

Finally, we remark that although the proof ultimately aims to decompose $E^\times/(E^\times)^2$ as an $\mathbb{F}_2[G]$-module when $G = \text{Gal}(E/F) \cong (\mathbb{Z}/2\mathbb{Z})^2$ using the strategy mentioned before, many of the intermediate steps can be proved in a more general situation with little extra work.

More specifically, we let $p$ be an arbitrary prime number and $n$ denote a fixed natural number. We let $E/F$ be any Galois field extension whose Galois group $G$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. We let
$F^\text{sep}$ be any fixed separable closure of $F$ that contains $E$, and let $G_E$ and $G_F$ denote $\text{Gal}(F^\text{sep}/E)$ and $\text{Gal}(F^\text{sep}/F)$. Then we have that $\mathbb{F}_p[G]$ acts on $H^1(G_E, \mathbb{F}_p)$ by conjugation, and:

$$H^1(G_E, \mathbb{F}_p) \cong H^1(G_F, \mathbb{F}_p[G])$$

as abelian groups.

Now let $V$ denote the second socle layer of $\mathbb{F}_p[G]$. More explicitly, let:

$$G = \langle \tau_1, \ldots, \tau_n | \forall i,j \; \tau_i \tau_j = \tau_j \tau_i \rangle$$

so that:

$$\mathbb{F}_p[G] = \mathbb{F}_p[\tau_1, \ldots, \tau_n]/( \tau_1^n - 1, \ldots, \tau_n^n - 1) = \mathbb{F}_p[\rho_1, \ldots, \rho_n]/( \rho_1^n - 1, \ldots, \rho_n^n - 1),$$

where for each $1 \leq i \leq n$, $\rho_i = \tau_i - 1$. (We note that the notation here differs slightly from that used previously. Namely, when $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, $\tau_3$ denoted $\tau_1 \tau_2$, while if $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ for $n \geq 3$, $\tau_3$ is a generator of $G$ that cannot be expressed as powers of any of the other generators. However, this abuse of notation should not cause too much trouble.) For each $1 \leq i \leq n$, let:

$$b_i = \rho_1^{p-1} \cdots \rho_i^{p-1} \rho_i^{p-1} \rho_{i+1} \cdots \rho_{n-1} \in \mathbb{F}_p[G],$$

and let:

$$z = \rho_1^{p-1} \cdots \rho_n^{p-1} \in \mathbb{F}_p[G].$$

Then:

$$V = \langle b_1, \ldots, b_n, z \rangle \subseteq \mathbb{F}_p[G].$$

[We note that the notation here differs slightly from that used previously. Namely, when $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, $\tau_3$ denoted $\tau_1 \tau_2$, while if $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ for $n \geq 3$, $\tau_3$ is a generator of $G$ that cannot be expressed as powers of any of the other generators. However, this abuse of notation should not cause too much trouble, as we will always specify whether $G$ is an arbitrary group of the form $(\mathbb{Z}/p\mathbb{Z})^n$ or is $(\mathbb{Z}/2\mathbb{Z})^2$. Furthermore, when we mention the group algebra $\mathbb{F}_p[G]$, we assume that $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ for an arbitrary prime number $p$ and positive integer $n$. When we mention $\mathbb{F}_2[G]$, we assume that $G \cong (\mathbb{Z}/2\mathbb{Z})^n$.]

Next, we compute that:

$$V^G = \langle z \rangle \cong \mathbb{F}_p$$

and

$$V/V^G = \langle b_1, \ldots, b_n \rangle \cong \mathbb{F}_p^n$$

as $\mathbb{F}_p[G]$-modules, where $\mathbb{F}_p$ denotes the one-dimensional trivial $\mathbb{F}_p[G]$-module. Thus, we can write down the following two exact sequences of $\mathbb{F}_p[G]$ modules

$$0 \rightarrow \mathbb{F}_p \xrightarrow{\iota_1} V \xrightarrow{\pi_1} V/V^G \rightarrow 0,$$

$$0 \rightarrow V \xrightarrow{\iota_2} \mathbb{F}_2[G] \xrightarrow{\pi_2} \mathbb{F}_p[G]/V \rightarrow 0.$$

Because of these short exact sequences, one has the following two exact sequences taken from the long exact sequence of cohomology:

$$H^1(G_F, \mathbb{F}_p) \xrightarrow{\iota_1^*} H^1(G_F, V) \xrightarrow{\pi_1^*} H^1(G_F, V/V^G) \cong (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p).$$

Again, every term in these two exact sequences can be made into an $\mathbb{F}_p[G]$-module, and these four homomorphisms can be proved to be $\mathbb{F}_2[G]$-module homomorphisms, and these four homomorphisms can be used to decompose $H^1(G_F, V)$ into a direct sum of four submodules.

Furthermore, if $F$ contains $\omega$, a primitive $p$th root of unity, then we can use Kummer theory to obtain an $\mathbb{F}_p[G]$-module isomorphism from $E^\times/(E^\times)^p$ to $H^1(G_F, \mathbb{F}_p)$, and many of the lemmas relating field-theoretic information to the maps involved in the decomposition of $H^1(G_F, V)$ extend to this case, as well. In fact, it is fair to say that the only steps when it is necessary to assume that
$G \cong (\mathbb{Z}/2\mathbb{Z})^2$ are those steps directly related to identifying $\mathcal{X}$ and $\mathcal{Y}$. The exposition in this report is written according to this point of view.

Now we describe what is contained in the rest of the report. As the proofs of many of the module-theoretic lemmas are logically independent from the decomposition of $E^\times/(E^\times)^2$ and do not require any Galois cohomology, they have all been collected into Chapter 2. More specifically:

In Section 2.1 we prove the Exclusion Lemma. The Exclusion Lemma gives a simple condition to determine when the sum of a certain set of submodules of a given $\mathbb{F}_p[G]$-module is direct. The Exclusion Lemma will be used many times in the rest of the proof; in fact, the Exclusion Lemma is what will be used to prove that $\mathcal{X} + \mathcal{Y} = \mathcal{X} \oplus \mathcal{Y}$.

Section 2.2 is a logically independent section wherein we prove that the ten $\mathbb{F}_2[G]$-modules:

$$
\mathbb{F}_2[G] \mathbb{F}_2[G]/(\rho_1) \mathbb{F}_2[G]/(\rho_2) \mathbb{F}_2[G]/(\rho_3) \mathbb{F}_2 \Omega(1) \Omega(2) \Omega(3) \Omega(-1) \Omega(-2).
$$
defined before are well-defined and indecomposable.

Section 2.3 is a very long and logically independent section in which we prove that for $\mathbb{F}_2[G]$-modules $M$, $M$ satisfies

$$
\sum_{i=1}^{3} (\rho_i M \cap M^G) \subseteq \sum_{i \neq j} \rho_i M^{(\tau_j)},
$$
if and only if the indecomposable components of $M$ are among the eight modules:

$$
\mathbb{F}_2[G] \mathbb{F}_2[G]/(\rho_1) \mathbb{F}_2[G]/(\rho_2) \mathbb{F}_2[G]/(\rho_3) \mathbb{F}_2 \Omega(1) \Omega(2) \Omega(3),
$$
and determine ways to compute the cardinal number of times each of the eight modules appears within $M$.

Chapter 3 consists entirely of statements of background material from Galois cohomology and the cohomology of profinite groups. More specifically, they include results on topological groups, infinite Galois theory, the cohomology of profinite groups, operations on cohomology, Kummer theory, and properties of the Brauer group. This chapter is included to collect useful lemmas and standardize definitions and notation. Few proofs will be given in this chapter; in fact, proofs are included only if they are not explicitly found in the literature.

Chapter 4 consists of the actual decomposition of $E^\times/(E^\times)^2$.

In Section 4.1, we assume that $G \cong (\mathbb{Z}/p\mathbb{Z})^N$, and we decompose $H^1(G_F, V)$ using the maps from the long-exact sequence in the cohomology of profinite groups.

In Section 4.2, we consider the isomorphism $H^1(G_F, \mathbb{F}_p[G]) \rightarrow H^1(G_E, \mathbb{F}_p)$ of Shapiro’s lemma and determine how it interacts with some of the maps used to decompose $H^1(G_F, V)$.

In Section 4.3, we consider the isomorphism $E^\times/(E^\times)^p \rightarrow H^1(G_E, \mathbb{F}_p)$ of Kummer theory and the isomorphism of Brauer group $p\text{Br}(F)$ with $H^2(G_F, \mathbb{F}_p)$, and we examine how they interact with the maps used to decompose $H^1(G_F, V)$ and the map from Shapiro’s lemma.

In Section 4.4, we assume that $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, and we construct $\mathcal{X}$ and $\mathcal{Y}$, prove that $\mathcal{Y}$ satisfies:

$$
\sum_{i=1}^{3} (\rho_i \mathcal{Y} \cap \mathcal{Y}^G) \subseteq \sum_{i \neq j} \rho_i \mathcal{Y}^{(\tau_j)},
$$
and prove that $H^1(G_E, \mathbb{F}_2) = \mathcal{X} \oplus \mathcal{Y}$.

In Section 4.5, we combine the results from sections 2.2, 2.3, and 4.4 to finally complete the desired decomposition of $E^\times/(E^\times)^2$ into indecomposable modules and give the cardinal number of times each of the ten modules appear within $E^\times/(E^\times)^2$. 

11
CHAPTER 2


1. The Exclusion Lemma and Related Results

In this section we prove several general results about $p$-group representations over fields of characteristic $p$. One of these results, the so-called Exclusion Lemma, will be ubiquitous in the rest of the proof. These results are found in Section 1 of [CMS], on pages 9 and 10.

This first lemma is found in the first full paragraph on page 9 of [CMS]. However, in that paragraph it is only proved for $k = \mathbb{F}_p$, $H \cong (\mathbb{Z}/p\mathbb{Z})^m$, and finite $k$-dimensional modules $M$, and it is necessary to use this lemma when $M$ is infinite-dimensional. For a proof when $k$ is an arbitrary field of characteristic $p$, $H$ an arbitrary $p$-group, but $M$ a finite-dimensional $k[H]$-module, see Examples 5.1.1 and 5.1.2 on page 156 of [We].

**Lemma 2.1.** Fix a prime number $p$, a $p$-group $H$, and a finite field $k$ of characteristic $p$. Then for any nonzero $k[H]$-module $M$, $M^H \neq 0$.

**Proof 2.1.** We first prove this result assuming that $M$ is finite-dimensional over $k$. As a corollary of the orbit-stabilizer theorem, the size of the orbit of any element in any set acted on by a finite group divides the order of that group. In particular, for any $m \in M$, $|k[H]|m$ divides $|H|$, so $|k[H]|m$ must be a power of $p$. Furthermore, if $M$ has $k$-dimension $n$, then since $M$ is nonzero, $n \geq 1$ and $M$ has $p^n$ elements. Now, let $S \subseteq M$ be a set of representatives of the orbits of $M$ under the action of $H$. Then we have:

$$p^n = |M| = \sum_{s \in S} |k[H]|s.$$ 

Now, $|k[H]|s = 1$ if and only if $s \in M^H$. We already know that $0 \in M^H$, so that $|k[H]|0 = 1$ and thus $0 \in S$. If $M^H$ were to equal 0, then for any nonzero element $s \in S$ $|k[H]|s$ would be a power of $p$ greater than or equal to $p$. Therefore, reducing both sides of:

$$p^n = |M| = \sum_{s \in S} |k[H]|s,$$

modulo $p$ gives:

$$0 \cong |k[H]|0 = 1 \pmod{p},$$

a clear contradiction. Therefore, $M^H \neq 0$ when $M$ has finite dimension over $k$.

Now assume that $M$ is an arbitrary $k[H]$-module. As $M \neq 0$, there is a nonzero $m \in M$. Then consider the cyclic submodule $k[H]|m$ of $M$. As $k$ and $H$ are finite, so is $k[H]$, so $k[H]|m$ is also finite. $k[H]|m$ is also nonzero, as $1m = m \in k[H]|m$ is nonzero. Then $k[H]|m$ is a nonzero, finite-dimensional $k[H]$-module, so the previous paragraph applies, and we conclude that $(k[H]|m)^H \neq 0$. As $(k[H]|m)^H \subseteq M^H$, we conclude that $M^H \neq 0$, as well. QED

The following statement was used several times in in Section 2 of [CMS] and will be used several times in this proof, but it was never formally stated or proved in [CMS].

**Corollary 2.2.** Fix a prime number $p$, a $p$-group $H$, and a finite field $k$ of characteristic $p$. For any $k[H]$-module homomorphism $f : M \rightarrow N$, if $f$ is injective when restricted to $M^H$, then $f$ is injective on all of $M$.

**Proof 2.2.** $f$ restricted to $M^H$ being injective implies that $\ker(f)^H = 0$. Applying Lemma 2.1 to $\ker(f)$ gives that $\ker(f) = 0$ and thus that $f$ is injective, as desired. QED
The following lemma was stated and proved as Lemma 5 in [CMS]. This result gives a very useful criterion to determine whether the sum of certain $F_2[H]$-modules is direct, and it will be used in this way extensively throughout this paper.

**Proposition 2.3.** (Lemma 5 of [CMS]) **(Exclusion Lemma)** Fix a prime number $p$, a $p$-group $H$, and a finite field $k$ of characteristic $p$. Let $M$ be any $k[H]$-module and $\{N_i | i \in \mathcal{I}\}$ be any collection of $k[H]$-submodules of $M$. If:

$$\sum_{i \in \mathcal{I}} M_i^H = \bigoplus_{i \in \mathcal{I}} M_i^H,$$

then:

$$\sum_{i \in \mathcal{I}} M_i = \bigoplus_{i \in \mathcal{I}} M_i.$$

**Proof 2.3.** We first prove this statement in the case when $\mathcal{I}$ is finite; in this case we induct on the size of $\mathcal{I}$. The proposition is vacuously true when $\mathcal{I}$ is empty. Now assume that $\mathcal{I}$ is nonempty. Pick an arbitrary element $i \in \mathcal{I}$, and let $\mathcal{I}' = \mathcal{I} - \{i\}$. Assume for the inductive hypothesis that:

$$\sum_{i \in \mathcal{I}} M_i^H = \bigoplus_{i \in \mathcal{I}} M_i^H \quad \text{and} \quad \sum_{i \in \mathcal{I}} M_i = \bigoplus_{i \in \mathcal{I}} M_i.$$

Then by assumption, we have:

$$\left( M_i \cap \left( \bigoplus_{i \in \mathcal{I}} M_i \right) \right)^H = M_i^H \cap \left( \bigoplus_{i \in \mathcal{I}} M_i \right)^H = M_i^H \cap \left( \bigoplus_{i \in \mathcal{I}} M_i^H \right) = 0.$$

Applying Lemma 2.1 allows us to conclude that:

$$M_i \cap \left( \bigoplus_{i \in \mathcal{I}'} M_i \right) = 0,$$

so that the sum:

$$\sum_{i \in \mathcal{I}} M_i = M_i + \left( \bigoplus_{i \in \mathcal{I}'} M_i \right)$$

is direct, and the induction is complete.

Now assume that $\mathcal{I}$ is arbitrary. Let $\mathcal{J}$ be any finite subset of $\mathcal{I}$. Then $\sum_{i \in \mathcal{I}} M_i^H = \bigoplus_{i \in \mathcal{I}} M_i^H$ implies $\sum_{j \in \mathcal{J}} M_j^H = \bigoplus_{j \in \mathcal{J}} M_j^H$, and from the result of the previous paragraph, we have:

$$\sum_{j \in \mathcal{J}} M_j = \bigoplus_{j \in \mathcal{J}} M_j.$$

Since the previous equation is true for any finite subset of $\mathcal{I}$, we have that:

$$\sum_{i \in \mathcal{I}} M_i = \bigoplus_{i \in \mathcal{I}} M_i,$$

as desired. QED

**2. A Proof That Ten $F_2[G]$-Modules are Indecomposable**

Recall how the ten modules:

$$F_2[G] \quad F_2[G]/(y_1) \quad F_2[G]/(y_2) \quad F_2[G]/(y_3) \quad F_2 \quad \Omega(1) \quad \Omega(2) \quad \Omega(3) \quad \Omega(-1) \quad \Omega(-2).$$

were defined. Also recall that their respective associated directed graphs are as follows:

```
```

```
We now prove that each of these ten modules are indecomposable. Although stated several times in [CMS], this fact was never proved within [CMS] itself. The indecomposability of these ten modules follows easily from the following proposition, modified from examples 5.1.2 to 5.1.4 on pages 155-157 of [We].

**Proposition 2.4.** Fix a prime number \( p \) and a finite field \( k \) of characteristic \( p \). Then:

1. For any \( p \)-group \( H \), \( k[H] \) is indecomposable as a \( k[H] \)-module.

2. Let \( H = \langle a | a^p \rangle \cong \mathbb{Z}/p\mathbb{Z} \) and \( M = k^2 \). Turn \( M \) into a \( k[H] \)-module by having \( a \) act via the matrix \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \). Then \( M \) is indecomposable as a \( k[H] \)-module.

3. Let \( H = \langle a, b | a^p = b^p = 1, ab = ba \rangle \cong (\mathbb{Z}/p\mathbb{Z})^2 \), and for \( n \geq 0 \) let \( M_n \) denote the \( (2n + 1) \)-dimensional \( k \)-vector space with basis \( \{ x_0, \ldots, x_n, y_1, \ldots, y_n \} \). Turn \( M_n \) into a \( k[H] \) module by having \( a \) and \( b \) act in the following ways:

\[
\begin{align*}
  a \cdot x_i &= x_i \\
  a \cdot y_i &= x_i + y_i \\
  b \cdot x_i &= x_i \\
  b \cdot y_i &= x_i + y_{i-1}.
\end{align*}
\]

Then \( M_n \) is indecomposable as a \( k[H] \)-module.

**Proof 2.4.** We prove (1) by contradiction: If \( k[H] \) were decomposable, then there would be nonzero \( k[H] \)-submodules \( M_1 \) and \( M_2 \) of \( k[H] \) such that \( k[H] = M_1 \oplus M_2 \). But if this were the case, then from Lemma 2.1 we would have nonzero submodules \( M_1^H \) and \( M_2^H \) of \( M_1 \) and \( M_2 \), respectively. Thus, \( M_1^H \oplus M_2^H \) would be a trivial submodule of \( k[H] \) of dimension at least 2. But we will now compute directly that \( (k[H])^H \) is one-dimensional. To this end, suppose that \( v = \sum_{h \in H} a_h h \in k[H] \) is fixed by every element of \( H \). Then for each \( h_1 \in H \), we have that:

\[
h_1 \cdot v = \sum_{h \in H} a_h h_1 h = \sum_{h \in H} a_{h^{-1}h} h = v = \sum_{h \in H} a_h h
\]

Looking at the coefficients of 1 in this equality, we have that \( a_{h^{-1}1} = a_1 \). Thus, each coefficient of every term in the sum defining \( v \) is identical, so \( v \) is a scalar multiple of:

\[
\sum_{h \in H} h.
\]

Thus, the subspace of all vectors in \( k[H] \) on which \( k[H] \) acts trivially is contained in the one-dimensional subspace generated by \( \sum_{h \in H} h \). From Lemma 2.1, this subspace must be nonzero, so this subspace is all of \( \langle \sum_{h \in H} h \rangle \) and so is one-dimensional. Thus, from earlier remarks, we are finished with the proof of (1).

To prove (2), we first show that the given action really does make \( k^2 \) into a \( k[H] \)-module. To prove this, it suffices to prove that \( A^p = \text{Id} \), where

\[
A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.
\]

But in any characteristic,

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix},
\]

and in characteristic \( p \), the latter matrix is the identity. Next we prove that \( M \) is indecomposable. If \( M \) were not indecomposable, then \( M = M_1 \oplus M_2 \), where \( M_1 \) and \( M_2 \) are nonzero \( k[H] \)-submodules
of $M$. As $\dim_k M = 2$, we must have that $\dim_k M_1 = \dim_k M_2 = 1$. Now, a one-dimensional $k[H]$-submodule is necessarily generated by an eigenvector of $A$. But the only eigenvalue of this matrix is $1$, and so the eigenvectors of this matrix are precisely those elements of $k^2$ in the kernel of

$$
\begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}.
$$

The kernel of this matrix is the one-dimensional subspace of $k^2$ generated by $[1 \ 0]^T$. This means that $M_1 = M_2 = \text{Span}_k([1 \ 0]^T)$, and so $k^2 \neq M_1 \oplus M_2$. This is a contradiction, and so $M$ is indecomposable, as desired, so (2) is proved.

To prove (3), we first show that the given action makes $M_n$ into a $k[H]$-module. With respect to the ordered basis $(x_0, y_1, x_1, \ldots, y_n, x_n)$, the matrix representations of $a \cdot \_\_\_$ and $b \cdot \_\_\_$ are $B$ and $C$, respectively, where $B$ and $C$ have the following block-diagonal forms:

$$
B = \begin{bmatrix}
I & A^T & A^T & \cdots \\
0 & A^T & A^T & \cdots \\
0 & 0 & A^T & \cdots \\
0 & 0 & 0 & \cdots 
\end{bmatrix}
$$

and $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $I = [1 \ 0]$. We have from (2) that $A^p = \text{Id}$, and also $P = \text{Id}^p = \text{Id}$. Therefore, $B^p = C^p = \text{Id}$. Furthermore, we compute that:

$$
a \cdot (b \cdot x_i) = a \cdot x_i = x_i \quad \quad \quad b \cdot (a \cdot x_i) = b \cdot x_i = x_i
$$

$$
a \cdot (b \cdot y_i) = a \cdot (x_i + y_{i-1}) = x_i + x_i + y_{i-1} \quad \quad b \cdot (a \cdot y_i) = b \cdot (x_i + y_i) = x_i + x_i + y_{i-1}
$$

and thus $ab \cdot \_\_\_ = ba \cdot \_\_\_$. This is enough to prove that $M_n$ is a $k[H]$-module.

To prove that $M_n$ is indecomposable, we let $\alpha : M_n \to M_n$ and $\beta : M_n \to M_n$ be $(a - 1) \cdot \_\_\_$ and $\beta = (b - 1) \cdot \_\_\_$, respectively, where $a - 1, b - 1 \in k[H]$. Next, let $X = \text{Span}_k \langle x_0, \ldots, x_n \rangle$ and $Y = \text{Span}_k \langle y_1, \ldots, y_n \rangle$, so that $X$ and $Y$ are $k$-vector subspaces (NOT necessarily $k[H]$-submodules) of $M_n$ such that $M_n = X \oplus Y$, and let $\pi : M_n \to Y$ be orthogonal projection along this decomposition. In other words, we have:

$$
\alpha(x_i) = \beta(x_i) = \pi(x_i) = 0 \quad \quad \alpha(y_i) = x_i \quad \quad \beta(y_i) = x_{i-1} \quad \quad \pi(y_i) = y_i.
$$

We claim that for any nonzero $k[H]$-submodule $N$ of $M_n$:

$$
\dim_k N \geq 2 \left( \dim_k \pi(N) \right) + 1.
$$

Notice that to prove (3) it suffices to prove this claim: Suppose for a proof by contradiction that $M_n$ is not indecomposable. Then $M_n = N_1 \oplus N_2$ for some nonzero $k[H]$-submodules $N_1$ and $N_2$ of $M_n$. Then we would have:

$$
2n + 1 = \dim_k M_n = \dim_k N_1 + \dim_k N_2 \geq 2 \left( \dim_k \pi(N_1) + \dim_k \pi(N_2) \right) + 2
$$

$$
\geq 2 \dim_k (\pi(N_1) + \pi(N_2)) + 2 = 2 \dim_k (\pi(N_1 + N_2)) + 2
$$

$$
= 2 \dim_k (\pi(M_n)) + 2 = 2 \dim_k Y + 2 = 2n + 2,
$$

and this is a clear contradiction.

To prove the claim, we fix a nonzero $k[H]$-submodule $N$ of $M_n$. Let $r = \dim_k \pi(N)$. The claim is trivial if $r = 0$, so assume $r > 0$. Choose $r$ elements $n_1, \ldots, n_r$ of $N$ such that $\{\pi(n_1), \ldots, \pi(n_r)\}$ is a $k$-basis of $\pi(N)$. We claim that the set

$$
S = \{n_1, \ldots, n_r, \alpha(n_1), \ldots, \alpha(n_r)\}
$$

is a $k$-basis of $N$. Let $v \in N$, and let $\alpha_1, \ldots, \alpha_r$ be the unique $k$-linear combination of $\alpha(n_1), \ldots, \alpha(n_r)$ such that $v = \sum \alpha_i \alpha(n_i)$. Then $\sum \alpha_i \alpha(n_i) = v$, so $v = \sum \alpha_i \alpha(n_i)$. Therefore, $S$ is a $k$-basis of $N$. Therefore, $r \geq \dim_k \pi(N)$, so

$$
\dim_k N \geq \dim_k \pi(N) + 1.
$$

This is a contradiction, and so (3) is proved.
is a linearly independent subset of $N$ that does not span $N$. This immediately gives the desired claim that $\dim_k N \geq 2r + 1$. Because $N$ is a $k[H]$-submodule of $M$, $\alpha(N) \subseteq N$, so $S$ is a subset of $N$. Next, to prove that $S$ is linearly independent, suppose that $c_1, \ldots, c_r, d_1, \ldots, d_n \in k$ are such that:

$$c_1n_1 + \cdots + c_rn_r + d_1\alpha(n_1) + \cdots + d_r\alpha(n_r) = 0.$$

Applying $\pi$ to this equation and noting that $\pi \circ \alpha = 0$, we therefore have:

$$c_1\pi(n_1) + \cdots + c_r\pi(n_r) = 0,$$

and since $\{\pi(n_1), \ldots, \pi(n_r)\}$ is linearly independent, we have $c_1 = \cdots = c_r = 0$. Thus, we have:

$$d_1\alpha(n_1) + \cdots + d_r\alpha(n_r) = \alpha(d_1n_1 + \cdots + d_rn_r) = 0,$$

so $d_1n_1 + \cdots + d_rn_r \in \ker(\alpha) = \ker(\pi) = X$. Thus,

$$d_1\pi(n_1) + \cdots + d_r\pi(n_r) = \pi(d_1n_1 + \cdots + d_rn_r) = 0,$$

and again since $\{\pi(n_1), \ldots, \pi(n_r)\}$ is linearly independent, we have $d_1 = \cdots = d_r = 0$. Thus, $c_1 = \cdots = c_r = d_1 = \cdots = d_r = 0$, and $S$ is linearly independent.

Next, to prove that $S$ does not span $N$. To this end, let $j_0$ be the largest positive integer such that:

$$\{\pi(n_1), \ldots, \pi(n_r)\} \subseteq \operatorname{Span}_k \langle y_{j_0}, y_{j_0+1}, \ldots, y_{j-1}, y_r \rangle.$$

Such a positive integer $j_0$ exists, as $\operatorname{im}(\pi) = Y = \operatorname{Span}_k \langle y_1, \ldots, y_{r-1}, y_r \rangle$. Next, choose a positive integer $i_0$ such that:

$$\pi(n_{i_0}) \notin \operatorname{Span}_k \langle y_{j_0}, y_{j_0+1}, \ldots, y_{n-1}, y_n \rangle$$

and

$$\pi(n_{i_0}) \notin \operatorname{Span}_k \langle y_{j_0+1}, y_{j_0+2}, \ldots, y_{n-1}, y_n \rangle.$$

Such an $i_0$ exists by definition of $j_0$. We claim that $\beta(n_{i_0})$ is not in the span of $S$; proving this would show that $S$ does not span $N$, for $\beta(n_{i_0}) \notin N$.

To prove this final claim, we let the values $q_{ij} \in k$ be such that for all $1 \leq i \leq r$,

$$\pi(n_i) = \sum_{j=1}^n q_{ij} y_j.$$

The value $q_{ij}$ exist because $\operatorname{im}(\pi) = Y$. Then by construction of $i_0$ and $j_0$, we have that for all $1 \leq i \leq r$ and $1 \leq j < j_0$, $q_{ij} = 0$, and furthermore, $q_{i_0 j_0} \neq 0$. Since $\ker(\alpha) = \ker(\beta) = \ker(\pi) = X$, we also have that:

$$\alpha(n_i) = \sum_{j=1}^n q_{ij} x_j,$$

and

$$\beta(n_{i_0}) = \sum_{j=1}^n q_{i_0 j} x_{j-1}.$$

Thus, by construction, $\beta(n_{i_0})$ is not in the span of $\{\pi(n_1), \ldots, \pi(n_r)\}$, as the coefficient of $x_{j_0-1}$ in $\beta(n_{i_0})$ is nonzero, but the coefficient of $x_{j_0-1}$ is zero in $\pi(n_i)$ for all $1 \leq i \leq r$. Now, if $\beta(n_{i_0})$ were in the span of $S$, then there would be values $c_1, \ldots, c_r, d_1, \ldots, d_n \in k$ such that:

$$\beta(n_{i_0}) = c_1n_1 + \cdots + c_rn_r + d_1\alpha(n_1) + \cdots + d_r\alpha(n_r).$$

Applying $\pi$ to both sides and noting that $\pi \circ \alpha = \pi \circ \beta = 0$, we have that:

$$0 = c_1\pi(n_1) + \cdots + c_r\pi(n_r),$$

and from the linear independence of $\{\pi(n_1), \ldots, \pi(n_r)\}$ is linearly independent, we have $c_1 = \cdots = c_r = 0$. Thus, we have:

$$\beta(n_{i_0}) = d_1\alpha(n_1) + \cdots + d_r\alpha(n_r),$$

which contradicts the assumption that $\beta(n_{i_0}) \notin N$. Therefore, $S$ does not span $N$.\]
contradicting that $\beta(n_{i0})$ is not in the span of $\{\pi(n_1), \ldots, \pi(n_r)\}$. Thus, from earlier remarks, we have proved that
\[ \dim_k N \geq 2(\dim_k \pi(N)) + 1 \]
for any nonzero $k[H]$-submodule of $M_n$. From earlier remarks, we are finished with the proof of (3).
QED

**Proposition 2.5.** The ten $\mathbb{F}_2[G]$-modules:
\[ \mathbb{F}_2[G], \mathbb{F}_2[G]/(y_1), \mathbb{F}_2[G]/(y_2), \mathbb{F}_2[G]/(y_3), \mathbb{F}_2, \Omega(1), \Omega(2), \Omega(3), \Omega(-1), \Omega(-2). \]
are all indecomposable.

**Proof.** $\mathbb{F}_2$, as it has dimension 1, cannot be represented as a direct sum of two nonzero $\mathbb{F}_2[G]$-submodules of itself, so $\mathbb{F}_2$ is indecomposable.

Next, $\mathbb{F}_2[G]$ is indecomposable from part (1) of Proposition 2.4.

The action of $y_2$ on $\mathbb{F}_2[G]/(y_1)$; of $y_1$ on $\mathbb{F}_2[G]/(y_2)$; and of $y_1$ on $\mathbb{F}_2[G]/(y_3)$. all have the matrix representation $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$. Thus, the action of $\mathbb{F}_2[(\tau_2)]$ on $\mathbb{F}_2[G]/(y_1)$; of $\mathbb{F}_2[(\tau_1)]$ on $\mathbb{F}_2[G]/(y_2)$; and of $\mathbb{F}_2[(\tau_1)]$ on $\mathbb{F}_2[G]/(y_3)$ all are actions of $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z}]$ on two-dimensional $\mathbb{F}_2$-vector spaces such that the generator of $\mathbb{Z}/2\mathbb{Z}$ acts via the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$; in short a module of the type described in part (2) of Proposition 2.4.

Thus, if any of the $\mathbb{F}_2[G]$-modules $\mathbb{F}_2[G]/(y_1)$, $\mathbb{F}_2[G]/(y_2)$, and $\mathbb{F}_2[G]/(y_3)$ were not indecomposable, the nontrivial decomposition would induce a nontrivial decomposition of the module described in part (2) of Proposition 2.4, and this is impossible. Thus, $\mathbb{F}_2[G]/(y_1)$, $\mathbb{F}_2[G]/(y_2)$, and $\mathbb{F}_2[G]/(y_3)$ are all indecomposable.

Let $M_1$, $M_2$, and $M_3$ denote the modules of part (3) of Proposition 2.4, when $H = G$ and $k = \mathbb{F}_2$. Then their associated directed graphs are:

\[ \begin{array}{c}
\cdot \quad \cdot \quad \cdot \\
\cdot \quad \cdot \quad \cdot \\
\cdot \quad \cdot \quad \cdot
\end{array} \]

In other words, $M_1 \cong \Omega(-1)$ and $M_2 \cong \Omega(-2)$, so from part (3) of Proposition 2.4, $\Omega(-1)$ and $\Omega(-2)$ are indecomposable.

Next, the actions of left-multiplication by $a$ and $b$ in $M_1$, $M_2$, and $M_3$ have the following block-diagonal matrix representations with respect to the ordered bases $\{x_0, y_1, x_1\}$, $\{x_0, y_1, x_1, y_2, x_2\}$, and $\{x_0, y_1, x_1, y_2, x_2, y_3, x_3\}$:

For $M_1$:
\[ a \cdot A_1 = \begin{bmatrix} I \\ A^T \end{bmatrix}, \quad b \cdot B_1 = \begin{bmatrix} A \\ I \end{bmatrix} \]

For $M_2$:
\[ a \cdot A_2 = \begin{bmatrix} I \\ A^T \\ A^T \end{bmatrix}, \quad b \cdot B_2 = \begin{bmatrix} A \\ A \\ I \end{bmatrix} \]

For $M_3$:
\[ a \cdot A_3 = \begin{bmatrix} I \\ A^T \\ A^T \\ A^T \end{bmatrix}, \quad b \cdot B_3 = \begin{bmatrix} A \\ A \\ A \\ I \end{bmatrix} , \]

where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in M_2(\mathbb{F}_2)$ and $I = \begin{bmatrix} 1 \end{bmatrix} \in M_1(\mathbb{F}_2)$. Next, if we denote the basis elements of $\Omega(1)$, $\Omega(2)$, and $\Omega(3)$ as follows:

\[ \begin{array}{c}
\omega_1 \\
\omega_2 \\
\omega_3 \\
\omega_4 \\
\omega_5 \\
\omega_6 \\
\omega_7
\end{array} \]
then for each \( i \in \{1, 2, 3\} \), the actions of left-multiplication by \( \tau_1 \) and \( \tau_2 \) on \( \Omega(i) \) have the following block-diagonal matrix representations with respect to the ordered bases \( \{\omega_1, \ldots, \omega_{2^{i+1}}\} \)

\[
\begin{align*}
\Omega(1): & \quad \tau_1 \cdot A_1^T = \begin{bmatrix} I & \ast \\ \ast & A \end{bmatrix} \\
\Omega(2): & \quad A_2^T = \begin{bmatrix} I & \ast \\ \ast & A \end{bmatrix} \\
\Omega(3): & \quad A_3^T = \begin{bmatrix} I & \ast \\ \ast & A \end{bmatrix} \\
\end{align*}
\]

In other words, the matrix representation of multiplication by \( \rho_1 \) in \( \Omega(i) \) is the transpose of the matrix representation of multiplication by \( a \) in \( M_i \), and the matrix representation of multiplication by \( \rho_2 \) in \( \Omega(i) \) is the transpose of the matrix representation of multiplication by \( b \) in \( M_i \).

Now, assume for a proof by contradiction that for some \( i \in \{1, 2, 3\} \) that \( \Omega(i) \) were not indecomposable, so that there are submodules \( N_1 \) and \( N_2 \) of \( \Omega(i) \) of dimension \( n_1 > 0 \) and \( n_2 > 0 \) such that \( \Omega(i) \cong N_1 \oplus N_2 \). Then if \( \{v_1, \ldots, v_{n_1}\} \) and \( \{v_{n_1+1}, \ldots, v_{n_2}\} \), are \( \mathbb{F}_2 \)-bases for \( N_1 \) and \( N_2 \) and \( P \in GL_{2^{i+1}}(\mathbb{F}_2) \) is the change of basis matrix from the ordered basis \( \{\omega_1, \ldots, \omega_{2^{i+1}}\} \) to \( \{v_1, \ldots, v_{n_1}, v_{n_1+1}, \ldots, v_{n_2}\} \), then:

\[
PA_i^T P^{-1} \quad \text{and} \quad PB_i^T P^{-1}
\]

are both block-diagonal matrices of the form:

\[
\begin{bmatrix}
C_1 \\
C_2
\end{bmatrix},
\]

where \( C_1 \in M_{n_1}(\mathbb{F}_2) \) and \( C_2 \in M_{n_2}(\mathbb{F}_2) \). Taking transposes gives that:

\[
(P^T)^{-1} A_i P^T \quad \text{and} \quad (P^T)^{-1} B_i P^T
\]

are also block-diagonal matrices of this form. This is enough to imply that \( M_i \) is not indecomposable. This contradicts part (3) of Proposition 2.4, so \( \Omega(1), \Omega(2), \) and \( \Omega(3) \) are all indecomposable.

We have shown that all modules in Proposition refindec are indecomposable. QED

3. Analysis of \( \mathbb{F}_2[G] \)-Modules \( M \) that Satisfy \( \sum_{i=1}^{3} (\rho_i M \cap M^G) \subseteq \sum_{i \neq j} \rho_i M^{(\tau_j)} \)

The purpose of this section is to prove the following proposition, which will be used both when \( \text{char}(F) \neq 2 \) and when \( \text{char}(F) = 2 \).

**Proposition 2.6.** (Proposition 2 of [CMS].) Let \( M \) be an \( \mathbb{F}_2[G] \)-module. Then the following two statements are equivalent:

1. \( \sum_{i=1}^{3} (\rho_i M \cap M^G) \subseteq \sum_{i \neq j} \rho_i M^{(\tau_j)} \).
2. \( M \) is isomorphic to the direct sum of some cardinal number of copies of the eight indecomposable \( \mathbb{F}_2[G] \)-modules in the following set \( S \):

\[
S = \{ \mathbb{F}_2[G], \mathbb{F}_2[G]/(\rho_1), \mathbb{F}_2[G]/(\rho_2), \mathbb{F}_2[G]/(\rho_3), \Omega(1), \Omega(2), \Omega(3), \mathbb{F}_2 \}.
\]

Further, if either of the previous two statements hold, then the following two statements also hold:

3. \( \sum_{i=1}^{3} (\rho_i M \cap M^G) = \sum_{i \neq j} \rho_i M^{(\tau_j)} \).
Furthermore, left-multiplication by $x$ by $G$.

This is because, for example, $m$.

Similarly, if $m$.

Next, notice that:

Therefore, if $m$.

Therefore, for any $F$.

It is these conditions that we will use in the proof.

PROOF 2.6. For the proof of this statement, for any $x \in \mathbb{F}_2[G]$, we will denote left-multiplication by $x$ as $\rho_i$. In other words, “$x$” could mean either the element $x$ in $\mathbb{F}_2[G]$, or the linear transformation “left-multiplication by $x$.” Notice that for any $\mathbb{F}_2[G]$-module $M$ and $i \in \{1, 2, 3\}$, $M^{(\tau_i)} = \ker (\rho_i)$. Furthermore,

$$M^G = M^{(\tau_1)} \cap M^{(\tau_2)} = \ker (\rho_1) \cap \ker (\rho_2)$$

$$= M^{(\tau_1)} \cap M^{(\tau_3)} = \ker (\rho_1) \cap \ker (\rho_3)$$

This is because, for example, $\tau_1$ and $\tau_2$ generate $G$, so that if $m \in M$ is fixed by both $\tau_1$ and $\tau_2$, then it is fixed by all of $G$, and similarly for the other equalities.

Next, notice that for any $\mathbb{F}_2[G]$-module $M$, $\rho_2 M^{(\tau_1)} = \rho_3 M^{(\tau_1)}$, $\rho_1 M^{(\tau_2)} = \rho_3 M^{(\tau_2)}$, and $\rho_1 M^{(\tau_3)} = \rho_2 M^{(\tau_3)}$. This is because for $m \in M^{(\tau_1)}$, we have:

$$\rho_3 m = (\rho_1 \rho_2 + \rho_1 + \rho_2) m = \rho_2 \cdot \rho_1 m + \rho_1 m + \rho_2 m = 0 + 0 + \rho_2 m = \rho_2 m.$$

Similarly, if $m \in M^{(\tau_2)}$, we have:

$$\rho_3 m = (\rho_1 \rho_2 + \rho_1 + \rho_2) m = \rho_1 \cdot \rho_2 m + \rho_1 m + \rho_2 m = 0 + \rho_1 m + 0 = \rho_1 m.$$

Next, notice that:

$$\rho_1 \rho_3 + \rho_1 + \rho_3 = \rho_1 (\rho_1 \rho_2 + \rho_1 + \rho_2) + \rho_1 (\rho_1 \rho_2 + \rho_1 + \rho_2) = \rho_1 \rho_2 + \rho_1 + (\rho_1 \rho_2 + \rho_1 + \rho_2) = \rho_2.$$

Therefore, if $m \in M^{(\tau_3)}$, we have:

$$\rho_2 m = (\rho_1 \rho_3 + \rho_1 + \rho_3) m = \rho_1 \cdot \rho_3 m + \rho_1 m + \rho_3 m = 0 + \rho_1 m + 0 = \rho_1 m.$$

Therefore, for any $\mathbb{F}_2[G]$-module $M$,

$$\sum_{i \neq j} \rho_i M^{(\tau_j)} = \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_2)} + \rho_1 M^{(\tau_3)},$$

so that condition (1) is equivalent to:

$$\sum_{i=1}^3 (\rho_i M \cap M^G) \subseteq \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_2)} + \rho_1 M^{(\tau_3)}$$

and condition (3) is equivalent to:

$$\sum_{i=1}^3 (\rho_i M \cap M^G) = \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_2)} + \rho_1 M^{(\tau_3)}.$$

It is these conditions that we will use in the proof.
Finally, for the rest of the proof, we will denote the basis elements of the eight modules in $S$ as follows:

$$
\begin{array}{cccccccc}
& 1 & & 1 & & 1 & & 1 \\
\rho_1 & \rho_2 & \rho_1 \rho_2 & \rho_1 & \rho_2 & \rho_1 & \rho_2 & \\
\omega_1 & \omega_2 & \omega_3 & \omega_1 & \omega_2 & \omega_3 & \omega_5 & \\
\end{array}
$$

(2) $\Rightarrow$ (1),(3),(4): In order to prove this, it suffices to show that (3) and (4) hold when $M$ is one of the eight modules listed in $S$. To show that (3) holds when $M$ is one of the eight modules in $S$, we have the following table, where $\langle r_i \rangle$ denotes the span of $r_i$:

$$
\begin{array}{cccccccc}
M & F_2[G] & F_2[G]/(\rho_1) & F_2[G]/(\rho_2) & F_2[G]/(\rho_3) & \Omega(1) & \Omega(2) & \Omega(3) & F_2 \\
M^G & (\rho_1 \rho_2) & (\rho_1) & (\rho_1) & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 1 \\
\rho_1 M & (\rho_1 \rho_2, \rho_2) & (\rho_1) & (\rho_1) & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\rho_1 M \cap M^G & (\rho_1 \rho_2) & 0 & (\rho_1) & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\rho_1 M & (\rho_1 \rho_2, \rho_2) & (\rho_1) & 0 & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\rho_1 M \cap M^G & (\rho_1 \rho_2) & (\rho_2) & 0 & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\rho_1 M & (\rho_1 \rho_2, \rho_2) & (\rho_1) & (\rho_1) & (\rho_1) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\rho_1 M \cap M^G & (\rho_1 \rho_2) & (\rho_2) & (\rho_2) & (\rho_2) & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\Sigma_{i \neq j} \rho_1 M & (\rho_1 \rho_2) & (\rho_2) & (\rho_2) & 0 & (\omega_2) & (\omega_2) & (\omega_2) & 0 \\
\end{array}
$$

Thus, for all eight of the modules $M$ in $S$, we have that:

$$
\sum_{i=1}^{3} (\rho_i M \cap M^G) = \rho_2 M^{(r_1)} + \rho_1 M^{(r_2)} + \rho_1 M^{(r_3)} = \sum_{i \neq j} \rho_i M^{(r_j)},
$$

so each of the eight modules satisfies (3).

We now show that each of the modules in $S$ satisfies the equalities in (4), using the rows from the previous table:
Thus, we have shown all equalities in (4), and from earlier remarks we have proved that (2) implies (1), (3), and (4).

(1)⇒(2): The proof that statement (1) implies (2) is very long and complicated, and for this reason remarks about the proof in italics are peppered throughout the formal proof. However, no parts of the proof are counterintuitive. In fact, its heuristic is very simple. First, identify copies of the eight modules in $S$ within $M$ in a carefully controlled way, but without seeming to pay special attention to whether these copies span all of $M$. Then, prove that the copies of the eight modules previously identified indeed do span all of $M$ by choosing an arbitrary element $m$ of $M$ and directly showing that $m$ is contained in the span of the copies, based on how the modules were identified. What is remarkable about this proof is that even though the classification of all finite-dimensional indecomposable $\mathbb{F}_2[G]$-modules is known (see Theorem 4.3.3 of [Be] for a statement of the classification), this proof does not use it in any way.

As a first step, we find the ideals of $\mathbb{F}_2[G]$. Notice that

$$(\mathbb{F}_2[G])^\times = 1 + \langle \rho_1, \rho_2, \rho_1\rho_2 \rangle.$$ 

Thus, the ideals different from $\mathbb{F}_2[G]$ will be subspaces of $\langle \rho_1, \rho_2, \rho_1\rho_2 \rangle$. Next, notice that we have the following nonzero principal ideals:

$$(\rho_1) = (\rho_1 + \rho_1\rho_2) = \langle \rho_1, \rho_1\rho_2 \rangle$$

$$(\rho_2) = (\rho_2 + \rho_1\rho_2) = \langle \rho_2, \rho_1\rho_2 \rangle$$

$$(\rho_1\rho_2) = \langle \rho_1\rho_2 \rangle$$

$$(\rho_1 + \rho_2) = (\rho_1\rho_2 + \rho_1 + \rho_2) = \langle \rho_3 \rangle = \langle \rho_1 + \rho_2, \rho_1\rho_2 \rangle$$

All other ideals of $\mathbb{F}_2[G]$ other than (0) can be formed by adding some of these ideals together. However, the only ideals that result from this procedure are $\mathbb{F}_2[G]$ and:

$$V = (\rho_1, \rho_2) = \langle \rho_1, \rho_2, \rho_1\rho_2 \rangle.$$ 

Thus, $\mathbb{F}_2[G]$ has exactly seven ideals, namely:

$$(0) = 0$$

$$(\rho_1, \rho_2) = \langle \rho_1, \rho_2 \rangle$$

$$(\rho_1) = \langle \rho_1, \rho_1\rho_2 \rangle$$

$$(\rho_2) = \langle \rho_2, \rho_1\rho_2 \rangle$$

$$(\rho_3) = \langle \rho_1 + \rho_2, \rho_1\rho_2 \rangle$$

$$V = (\rho_1, \rho_2) = \langle \rho_1, \rho_2, \rho_1\rho_2 \rangle$$

$$(1) = \langle 1, \rho_1, \rho_2, \rho_1\rho_2 \rangle$$

The first of the eight modules in $S$ that we identify within $M$ is $\mathbb{F}_2[G]$. This is done by associating to each nonzero element of $\rho_1\rho_2 M$ a copy of $\mathbb{F}_2[G]$, then choosing a subset of these copies of $\mathbb{F}_2[G]$ in such a way that the Exclusion Lemma ensures that the sum of the copies of $\mathbb{F}_2[G]$ within $M$ is direct. This makes intuitive sense for the following reason: From the earlier tables, the only module $N \in S$ such that $\rho_1\rho_2 N$ is nonzero is $N = \mathbb{F}_2[G]$. Thus, if $M$ were the direct sum of copies of modules in $S$, then elements of $\rho_1\rho_2 M$ would correspond to copies of $\mathbb{F}_2[G]$.

Let $L = \rho_1\rho_2 M$. Since the map $\rho_1\rho_2 : M \rightarrow L$ is a surjective linear transformation, there is an $\mathbb{F}_2$-subspace $Y$ of $M$ such that $\rho_1\rho_2$ maps $Y$ isomorphically onto $L$. Let $f : L \rightarrow Y$ be the inverse of this isomorphism. Next, let $\ell \in L$ be nonzero. Then $\ell = \rho_1\rho_2 f(\ell)$. As $\ell \neq 0$, $\rho_1\rho_2 \notin \text{Ann}(f(\ell))$. Since $\text{Ann}(f(\ell))$ is an ideal of $\mathbb{F}_2[G]$ and the only ideal of $\mathbb{F}_2[G]$ that does not contain $\rho_1\rho_2$ is 0, we have that $\text{Ann}(f(\ell)) = 0$. Therefore:

$$f(\ell)\mathbb{F}_2[G] \cong \mathbb{F}_2[G]/\text{Ann}(f(\ell)) \cong \mathbb{F}_2[G]$$

and $(f(\ell)\mathbb{F}_2[G])^G = \rho_1\rho_2 f(\ell) = \ell$. Thus, to each nonzero element $\ell \in L$ we can find a submodule $E(\ell)$ of $M$, namely $F_2[G] f(\ell)$, that is isomorphic to $\mathbb{F}_2[G]$ and has $(E(\ell))^G = \langle \ell \rangle$. Let $\mathcal{L}$ be an $\mathbb{F}_2$-basis for $L$. Then we have:

$$\sum_{\ell \in \mathcal{L}} E(\ell)^G = \sum_{\ell \in \mathcal{L}} \langle \ell \rangle = \bigoplus_{\ell \in \mathcal{L}} \langle \ell \rangle,$$

so from the Exclusion Lemma we have that:

$$\sum_{\ell \in \mathcal{L}} E(\ell) = \bigoplus_{\ell \in \mathcal{L}} E(\ell).$$
The second module to be found is $\Omega(1)$. This is done by noting first that
\[\rho_1 \rho_2 M \subseteq \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)},\]
and associating to each element of $\rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$ a copy of $\Omega(1)$, then choosing a subset of these copies of $\Omega(1)$ in such a way that the Exclusion Lemma ensures that the sum of the copies of $\mathbb{F}_2[G]$ and $\Omega(1)$ within $M$ is direct.

Again, this makes intuitive sense: From the earlier tables, the only modules $N \in S$ such that $\rho_1 N^{(\tau_2)} \cap \rho_2 N^{(\tau_1)}$ is nonzero are $\mathbb{F}_2[G]$ and $\Omega(1)$. Furthermore, if $N = \mathbb{F}_2[G]$, then:
\[\rho_1 \rho_2 N \subseteq \rho_1 N^{(\tau_2)} \cap \rho_2 N^{(\tau_1)},\]
and $\mathbb{F}_2[G]$ contains $\Omega(1)$ as a submodule. Thus, if $M$ were the direct sum of copies of modules in $S$, then elements of $\rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$ would correspond to copies of $\Omega(1)$; furthermore, elements in a complement of $\rho_1 \rho_2 M$ in $\rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$ would correspond to copies of $\Omega(1)$ not contained within copies of $\mathbb{F}_2[G]$.

Let $Y_1 = \rho_2 Y$. The map $\rho_1 : Y_1 \to \rho_1 \rho_2 M = L$ is an isomorphism of $\mathbb{F}_2$-vector spaces. Let $v_1 : L \to Y_1$ be its inverse. Then since we have that $\ell = \rho_1 \rho_2 f(\ell)$ for all $\ell \in L$, applying $v_1$ gives:
\[v_1(\ell) = \rho_1 f(\ell)\]
Similarly, let $Y_2 = \rho_1 Y$, so that $\rho_2 : Y_2 \to L$ is an isomorphism; let $v_2 : L \to Y_2$ be its inverse, so that:
\[v_2(\ell) = \rho_2 f(\ell)\]
The isomorphisms $v_1$ and $v_2$ will be extended several times throughout the course of this proof; they will always be such that $\rho_1 \cdot v_1$ and $\rho_2 \cdot v_2$ are the identity on the domains of $v_1$ and $v_2$, respectively.

We have $L \subseteq \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$. This is because if $\ell \in L = \rho_1 \rho_2 M$, then $\ell = \rho_1 \rho_2 m$ for some $m \in M$. Then $\rho_2 \cdot \rho_2 m = \rho_2^2 m = 0m = 0$, so $\rho_2 m \in M^{(\tau_2)}$ and $\rho_1 \rho_2 m \in \rho_1 M^{(\tau_2)}$. Similarly, $\rho_1 m \in M^{(\tau_1)}$, so that $\rho_1 \rho_2 m = \rho_2 \rho_1 m \in \rho_2 M^{(\tau_1)}$. Thus, we let $T$ be a subspace complement of $L$ in $\rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$, so that:
\[L \oplus T = \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}\]
Since $\rho_1 : M^{(\tau_2)} \to \rho_1 M^{(\tau_2)}$ is surjective and $T \subseteq \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)} \subseteq \rho_1 M^{(\tau_2)}$, there is a subspace $W_1$ of $M^{(\tau_2)}$ that is mapped isomorphically onto $T$ by $\rho_1$. Extend $v_1$ to an isomorphism
\[v_1 : m_1 m_2 M \oplus T \to \rho_2 Y \oplus W_1 \subseteq M^{(\tau_2)},\]
where $v_1$ is defined on $T$ to be the inverse of $\rho_1 : W_1 \to T$. Similarly, there is a subspace $W_2$ of $M^{(\tau_1)}$ that is mapped isomorphically onto $T$ by $\rho_2$. Extend $v_2$ to an isomorphism
\[v_2 : m_1 m_2 M \oplus T \to \rho_2 Y \oplus W_1 \subseteq M^{(\tau_1)},\]
where $v_2$ is defined on $T$ to be the inverse of $\rho_2 : W_2 \to T$.

Now let $t \in \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$ be nonzero, and define $L_1(t)$ to be the following $\mathbb{F}_2$-vector space:
\[(t, v_1(t), v_2(t)).\]
We have:
\[\rho_1 \cdot v_1(t) = \rho_2 \cdot v_2(t) = t\text{ by definition of }v_1 \text{ and } v_2,\]
\[\rho_1 \cdot t = \rho_2 \cdot t = 0\text{ because }t \in \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)},\]
\[\rho_1 \cdot v_2(t) = 0\text{ because }v_2(t) \in M^{(\tau_2)},\text{ and}\]
\[\rho_2 \cdot v_1(t) = 0\text{ because }v_1(t) \in M^{(\tau_1)}\]
Thus, $L_1(t)$ is an $\mathbb{F}_2[G]$-submodule of $M$, and the linear transformation defined on basis vectors as $\omega_1 \mapsto v_2(t), \omega_2 \mapsto t, \omega_3 \mapsto v_1(t)$ is an $\mathbb{F}_2[G]$-module homomorphism of $\Omega(1)$ onto $L_1(t)$. Furthermore, as $\Omega(1)^G = \langle \omega_2 \rangle$ and $L_1(t)^G = \langle t \rangle$, this $\mathbb{F}_2[G]$-module homomorphism maps $\Omega(1)^G$ isomorphically onto $L_1(t)^G$. By Corollary 2.2, we that the $\mathbb{F}_2[G]$-module homomorphism is an isomorphism from $\Omega(1)$ to $L_1(t)$. Therefore, $L_1(t) \cong \Omega(1)$ as $\mathbb{F}_2[G]$-modules for any nonzero $t \in \rho_1 M^{(\tau_2)} \cap \rho_2 M^{(\tau_1)}$. 23
Therefore, if we let $T$ be an $F_2$-basis for $T$, then $T \cup L$ is a basis for $L + T = \rho_1 M^{(r_2)} \cap \rho_2 M^{(r_1)}$. Therefore, the sum:

$$\sum_{\ell \in \mathcal{L}} E(\ell)^G + \sum_{t \in T} L_1(t)^G$$

is direct, so by the Exclusion Lemma the following sum is also direct:

$$\sum_{\ell \in \mathcal{L}} E(\ell) + \sum_{t \in T} L_1(t).$$

Next, we identify copies of $\Omega(2)$ and $\Omega(3)$ in $M$. This process requires more machinery than in the previous cases. However, this machinery can be immediately used to identify copies of $F_2[G]/(\rho_1)$, $F_2[G]/(\rho_2)$, $F_2[G]/(\rho_2)$, and $F_2$ in $M$. After we build some of the machinery, we will state the strategy more clearly and explain why this method makes intuitive sense.

Let $A$ and $B$ be $F_2$-subspaces of $M$ such that:

$$A \oplus (\rho_1 M^{(r_2)} \cap \rho_2 M^{(r_1)}) = A \oplus L \oplus T = \rho_1 M^{(r_2)}$$

$$B \oplus (\rho_1 M^{(r_2)} \cap \rho_2 M^{(r_1)}) = B \oplus L \oplus T = \rho_2 M^{(r_1)}.$$ 

Note that $A + B = A \oplus B$; this is because $A \cap B \subseteq \rho_1 M^{(r_2)} \cap \rho_2 M^{(r_1)} = L \oplus T$. Next, let $C$ be an $F_2$-subspace of $M$ such that:

$$C \oplus (\rho_1 M^{(r_3)} \cap (\rho_1 M^{(r_2)} + \rho_2 M^{(r_1)})) z = C \oplus (\rho_1 M^{(r_3)} \cap (A \oplus B \oplus L \oplus T)) = \rho_1 M^{(r_3)}.$$ 

Note also that we have:

$$A \oplus B \oplus C \oplus L \oplus T = \rho_1 M^{(r_2)} + \rho_2 M^{(r_1)} + \rho_1 M^{(r_3)} = \sum_{i \neq j} \rho_i M^{(r_i)}.$$ 

Therefore, condition (1) implies that any element of:

$$\sum_{i=1}^{3} (\rho_i M \cap M^G)$$

can be written along the direct sum $A \oplus B \oplus C \oplus L \oplus T$.

Finally, notice that $\rho_1 M^{(r_2)}$, $\rho_2 M^{(r_1)}$, and $\rho_1 M^{(r_3)}$ are all subsets of $M^G$. For example, if $m \in M^{(r_2)}$ is arbitrary, so that $\rho_1 m \in \rho_1 M^{(r_2)}$ is arbitrary, then we have:

$$\rho_1 \cdot \rho_1 m = \rho_2^2 m = 0 = 0 \quad \rho_1 \cdot \rho_2 m = \rho_1 \rho_2 m = \rho_1 \cdot 0 = 0,$$

so that $\rho_1 m \in M^G$. Similarly, $\rho_2 M^{(r_1)} \subseteq M^{r_1} \cap M^{r_2} = M^G$ and elements of $\rho_1 M^{(r_3)} \subseteq M^{r_1} \cap M^{r_2} = M^G$. Because $\rho_1 M^{(r_2)}$, $\rho_2 M^{(r_1)}$, and $\rho_1 M^{(r_3)}$ are all subsets of $M^G$, it is possible to find an $F_2$-subspace $Z$ of $M$ such that:

$$Z \oplus (A \oplus B \oplus C \oplus L \oplus T) = Z \oplus (\rho_1 M^{(r_2)} + \rho_2 M^{(r_1)} + \rho_1 M^{(r_3)}) = M^G.$$ 

For any vector subspace $V$ of $M^G$ that is the sum of some combination of $A$, $B$, $C$, $L$, $T$, and $Z$, we let $\pi_V$ denote the projection map of $M^G$ onto $V$ corresponding to this direct sum. Finally, let $A' = A \cap \rho_2 M$.

The identification of $\Omega(2)$ and $\Omega(3)$ in $M$ is less straightforward than those of $F_2[G]$ and $\Omega(1)$. This is because elements of $A'$ could potentially be identified with copies of $\Omega(2)$, or $\Omega(3)$. These two cases are separated as follows. First, we choose an $F_2$ vector space $A_2$ that $\rho_2$ maps isomorphically onto $A'$. Then, $A_2$ is replaced by a vector space $P$ that still has the property that $\rho_2$ maps $P$ isomorphically onto $A'$, and has the additional property that $\rho_1 P \subseteq B + C$. on $M$. To determine if an element $a \in A'$ should be associated to $\Omega(2)$ or $\Omega(3)$, we first find an element $p \in P$ such that $\rho_2 p = a$, and then project $\rho_1 p$ onto $C$ via $\pi_C$. If the projection of $\rho_1 p$ onto $C$ is zero, then $\Omega(2)$ is associated to $a$. If the projection is nonzero, we associate $\Omega(3)$ to $a$.

This classification, though very convoluted, again makes intuitive sense. Of the eight modules in $S$, the only three modules $N$ for which a complement of $\rho_1 N^{(r_2)} \cap \rho_2 N^{(r_1)}$ in $\rho_1 N^{(r_2)}$ is nonzero,
namely \(F_2[G]/(\rho_2), \Omega(2), \) and \(\Omega(3).\) Furthermore, there are only two modules in \(S\) such that the intersection \(A'\) of this complement with \(\rho_2 M\) is nonzero, namely \(\Omega(2)\) and \(\Omega(3).\)

Now, if \(N = \Omega(2)\), then \(A'\) must be \(\langle \omega_4 \rangle\), \(B\) must be \(\langle \omega_2 \rangle\) and \(C = 0\). \(A_2\) can be any one-dimensional subspace generated by a single vector in the coset

\[
\omega_3 + \langle \omega_2, \omega_4, \omega_5 \rangle.
\]

\(P\) can be any one-dimensional subspace generated by a single vector in the coset

\[
\omega_3 + \langle \omega_2, \omega_4 \rangle.
\]

\(\rho_1\) times any such vector is \(\omega_2\), and applying \(\pi_C\) gives 0.

If instead \(N = \Omega(3)\), then \(A'\) must be \(\langle \omega_6 \rangle\), \(B\) must be \(\langle \omega_2 \rangle\) and \(C\) must be \(\langle \omega_2 + \omega_4 + \omega_6 \rangle\). \(A_2\) can be any one-dimensional subspace generated by a single vector in the coset

\[
\omega_3 + \langle \omega_2, \omega_4, \omega_5, \omega_6 \rangle.
\]

\(P\) can be any one-dimensional subspace generated by a single vector in the coset

\[
\omega_5 + \omega_7 + \langle \omega_2, \omega_4, \omega_6 \rangle.
\]

\(\rho_1\) times any such vector is

\[
\omega_4 + \omega_6 = \omega_2 + (\omega_2 + \omega_4 + \omega_6),
\]

and applying \(\pi_C\) gives \(\omega_2 + \omega_4 + \omega_6 \neq 0\).

Therefore, if \(M\) were the direct sum of modules in \(S\), then the procedure stated above would distinguish between copies of \(\Omega(2)\) and \(\Omega(3).\)

As \(\rho_1 : M^{(\tau_2)} \rightarrow \rho_1 M^{(\tau_2)}, \rho_2 : M^{(\tau_3)} \rightarrow \rho_1 M^{(\tau_3)},\) and \(\rho_1 : M^{(\tau_1)} \rightarrow \rho_2 M^{(\tau_1)}\) are all surjective and \(A \subseteq \rho_1 M^{(\tau_2)}, B \subseteq \rho_2 M^{(\tau_3)},\) and \(C \subseteq \rho_1 M^{(\tau_1)},\) there are \(F_2\)-subspaces \(\tilde{A} \subseteq M^{(\tau_2)}, \tilde{B} \subseteq M^{(\tau_3)},\) and \(\tilde{C} \subseteq M^{(\tau_1)}\) such that \(\rho_1 : \tilde{A} \rightarrow A, \rho_2 : \tilde{B} \rightarrow B,\) and \(\rho_1 : \tilde{C} \rightarrow C.\) Thus, we can extend \(v_1\) and \(v_2\) to be the following isomorphisms:

\[
v_1 : L \oplus T \oplus A \oplus C = \rho_1 M^{(\tau_2)} \oplus C \rightarrow Y_1 \oplus W_1 \oplus \tilde{A} \oplus \tilde{C}
\]

\[
v_2 : L \oplus T \oplus B = \rho_2 M^{(\tau_1)} \rightarrow Y_2 \oplus W_2 \oplus \tilde{B},
\]

where \(v_1\) is defined on \(A\) and \(C\) to be the inverse of \(\rho_1 : \tilde{A} \rightarrow A\) and \(\rho_1 : \tilde{C} \rightarrow C,\) respectively, and where \(v_2\) is defined on \(B\) to be the inverse of \(\rho_2 : \tilde{B} \rightarrow B.\)

Recall that \(A' = A \cap \rho_2 M.\) Let \(A_1 = v_1(A').\) Then \(\rho_1 \cdot A_1 \rightarrow A'\) and \(v_1 : A' \rightarrow A_1\) are mutually inverse vector space isomorphisms. As \(\rho_2 : M \rightarrow \rho_2 M\) is surjective and \(A' \subseteq \rho_2 M,\) there is a subspace \(A_2\) of \(M\) such that \(\rho_2 : A_2 \rightarrow A'\) is an isomorphism. (We cannot define \(A_2\) to be \(v_2(A'),\) as \(v_2\) is currently not defined on any of \(A\) and on \(A'\) in particular.) We claim that \(\rho_1 A_2 \subseteq M^G.\) This is because

\[
\rho_1 \cdot \rho_1 A_2 = \rho_1^2 A_2 = 0 A_2 = 0
\]

\[
\rho_2 \cdot \rho_1 A_2 = \rho_1 \cdot \rho_2 A_2 \subseteq \rho_1 \cdot A' \subseteq \rho_1 \cdot A \subseteq \rho_1 \cdot \rho_1 M^{(\tau_2)} = \rho_1^2 M^{(\tau_2)} = 0 M^{(\tau_2)} = 0.
\]

Because \(\rho_1 A_2 \subseteq M^G,\) the following vector space is well-defined:

\[
(1 - v_1 \pi_{A+L+T} \rho_1) A_2.
\]

Call this vector space \(P.\)

Because \(v_1(A + L + T) = \tilde{A} + Y_1 + W_1 \subseteq M^{(\tau_2)},\) we have that on \(A_2:\)

\[
\rho_2 (1 - v_1 \pi_{A+L+T} \rho_1) = \rho_2 - 0 = \rho_2.
\]

Therefore, \(\rho_2\) is an \(F_2\)-isomorphism from \(P\) to \(A'.\) Extend \(v_2\) to be the following isomorphism:

\[
v_2 : L \oplus T \oplus B \oplus A' = \rho_2 M^{(\tau_1)} \oplus A' \rightarrow Y_2 \oplus W_2 \oplus \tilde{B} \oplus P,
\]

where \(v_2\) is defined on \(A'\) to be the inverse of \(\rho_2 : P \rightarrow A'.\)
We now prove that $\rho_1 P \subseteq B + C$. First note that:

\[ \rho_1 \cdot \rho_1 P = \rho_2^2 P = 0A_2 = 0 \]
\[ \rho_2 \cdot \rho_1 P = \rho_1 \cdot \rho_2 P \subseteq \rho_1 \cdot A' \subseteq \rho_1 \cdot A \subseteq \rho_1 \cdot \rho_1 M^{(\tau_2)} = \rho_2^2 M^{(\tau_2)} = 0M^{(\tau_2)} = 0. \]

so that $\rho_1 P \subseteq M^G$. Thus, we have that $\rho_1 P \subseteq \rho_1 M \cap M^G$. By using condition (1), we have that:

$\rho_1 P \subseteq A \oplus B \oplus C \oplus L \oplus T.$

Thus, to show that $\rho_1 P \subseteq B + C$, it suffices to prove that $\pi_{A+L+T}\rho_1 P = 0$. But this is simple:

\[ \pi_{A+L+T}\rho_1 P = \pi_{A+L+T}\rho_1 (1 - v_3 \pi_{A+L+T}\rho_1)A_2 = (\pi_{A+L+T}\rho_1 - \pi_{A+L+T}\rho_1 v_1 \pi_{A+L+T}\rho_1)A_2 = (\pi_{A+L+T}\rho_1 - \pi_{A+L+T}\rho_1)A_2 = 0A_2 = 0. \]

We now define the maps $\beta : A' \to B$ and $\gamma : A' \to C$ as:

\[ \beta = \pi_B \rho_1 v_2 \quad \gamma = \pi_C \rho_1 v_2. \]

Because $\rho_1 v_2 A' = \rho_1 P \subseteq B \oplus C$, we have that $\rho_1 v_2 (a) = \beta(a) + \gamma(a)$ for all $a \in A'$.

We claim that $\beta$ is injective. To this end, suppose that $a \in A'$ is in $\ker(\beta)$, and let $c = \gamma(a) \in C$. Since $\beta(a) = 0$, we have $\gamma(a) = \rho_1 v_2(a)$. Let $x = v_2(a) + v_1(c)$. Then since:

\[ \rho_1 x = \rho_1 v_2(a) + \rho_1 v_1 c = c + c = 0, \]

we have $x \in M^{(\tau_1)}$, so that $\rho_2 x \in \rho_2 M^{(\tau_1)} = B \oplus L \oplus T$. Recalling that $v_1 C = \tilde{C} \subseteq M^{(\tau_3)}$ and that $\rho_1 m = \rho_2 m$ for all $m \in M^{(\tau_3)}$, we also have that:

\[ \rho_2 x = \rho_2 v_2(a) + \rho_2 v_1 c = a + \rho_1 v_1 c = a + c \in A \oplus C. \]

Since $\rho_1 x = a + c$ is in $A \oplus C$ and $B \oplus L \oplus T$, and $(A \oplus C) + (B \oplus L \oplus T) = (A \oplus C) \oplus (B \oplus L \oplus T)$, we have that $a + c = 0$, so that $a = c$. As $a \in A$ and $c \in C$ and $A + C = A \oplus C$, we have $a = 0$. Thus, $\ker(\beta) = 0$ and $\beta$ is injective.

Now we prove that if $a \in A'$ is nonzero and satisfies $\gamma(a) = 0$, then we can associate a copy of $\Omega(2)$ to $a$. For such an $a$, $\rho_1 v_2(a) = \beta(a)$, and since $\beta$ is injective, $\beta(a)$ is nonzero. Now let $b = \beta(a) \in B$ and:

\[ L_2(a) = \langle v_2(b), b, v_2(a), a, v_1(a) \rangle. \]

We have the following equations along with their justifications:

\[ \rho_1 \cdot v_2(b) = 0 \quad v_2 B = \tilde{B} \subseteq M^{(\tau_1)}, \]
\[ \rho_2 \cdot v_2(b) = b \quad v_2 \text{ is a right-inverse of } \rho_2, \]
\[ \rho_1 \cdot b = \rho_2 \cdot b = 0 \quad b \in B \subseteq M^G, \]
\[ \rho_1 \cdot v_2(a) = \beta(a) = b \quad \text{definition of } b, \]
\[ \rho_2 \cdot v_2(a) = a \quad v_2 \text{ is a right-inverse of } \rho_2, \]
\[ \rho_1 \cdot a = \rho_2 \cdot a = 0 \quad a \in A \subseteq M^G, \]
\[ \rho_1 \cdot v_1(a) = a \quad v_1 \text{ is a right-inverse of } \rho_1, \]
\[ \rho_2 \cdot v_1(a) = 0 \quad \rho_1 A = \tilde{A} \subseteq M^{(\tau_2)}. \]

Therefore, $L_2(a)$ is an $\mathbb{F}_2[G]$-submodule of $M$ and the $\mathbb{F}_2$-linear transformation from $\Omega(2)$ to $L_2(a)$ defined on basis vectors as:

\[ \omega_1 \mapsto v_2(b) \quad \omega_2 \mapsto b \quad \omega_3 \mapsto v_2(a) \quad \omega_4 \mapsto a \quad \omega_5 \mapsto v_1(a) \]

is a surjective homomorphism of $\mathbb{F}_2[G]$-modules. Furthermore, we have:

\[ \Omega(2)^G = \langle \omega_2, \omega_4 \rangle \quad \text{and} \quad L_2(a)^G = \langle a, b \rangle. \]

Also, since $a \in A, b \in B, a \neq 0, b \neq 0$, and $A + B = A \oplus B$, $a$ and $b$ are linearly independent. Therefore, the previous $\mathbb{F}_2[G]$-module homomorphism from $\Omega(2)$ to $L_2(a)$ maps $\Omega(2)^G$ isomorphically.
onto $L_2(a)^G$. By Corollary 2.2, we that the $\mathbb{F}_2[G]$-module homomorphism is an isomorphism from $\Omega(2)$ to $L_2(a)$. Therefore, $L_2(a) \cong \Omega(2)$ as $\mathbb{F}_2[G]$-modules for any nonzero $a \in \ker(\gamma)$.

Next we prove that if $a \in A'$ is nonzero and satisfies $\gamma(a) \neq 0$, then we can associate a copy of $\Omega(3)$ to $a$. Since $\beta$ is injective, $\beta(a)$ is nonzero. Let $b = \beta(a) \in B$ and $c = \gamma(a) \in C$, so that $\rho_1v_2(a) = b + c$. We define:

$$L_3(a) = \langle v_2(b), v_2(a) + v_2(b) + v_1(c), a + b + c, (v_1 + v_2)(a), a, v_1(a) \rangle.$$

We have the following equations, with the respective justifications:

- $\rho_1 \cdot v_2(b) = 0$
- $\rho_2 \cdot v_2(b) = b$
- $\rho_2 \cdot (v_2(a) + v_2(b) + v_1(c)) = \rho_1v_2(a) + 0 + c$
- $\rho_1 \cdot (a + b + c) = 0$
- $\rho_2 \cdot (a + b + c) = 0$
- $\rho_1 \cdot (v_1 + v_2)(a) = a + \rho_1v_2(a)$
- $\rho_2 \cdot (v_1 + v_2)(a) = \rho_2v_1(a) + a$
- $\rho_1 \cdot a = \rho_2 \cdot a = 0$
- $\rho_1 \cdot v_1(a) = a$
- $\rho_2 \cdot v_1(a) = 0$

Therefore, $L_3(a)$ is an $\mathbb{F}_2[G]$-submodule of $M$ and the $\mathbb{F}_2$-linear transformation from $\Omega(3)$ to $L_3(a)$ defined on basis vectors as:

- $\omega_1 \mapsto v_2(b)$
- $\omega_3 \mapsto v_2(a) + v_2(b) + v_1(c)$
- $\omega_5 \mapsto (v_1 + v_2)(a)$
- $\omega_7 \mapsto v_1(a)$
- $\omega_2 \mapsto b$
- $\omega_4 \mapsto a + b + c$
- $\omega_6 \mapsto a$

is a surjective homomorphism of $\mathbb{F}_2[G]$-modules. Furthermore, we have:

$$\Omega(3)^G = \langle \omega_2, \omega_4, \omega_6 \rangle \quad \text{and} \quad L_3(a)^G = \langle b, a + b + c, a \rangle.$$

Also, since $a \in A$, $b \in B$, $c \in C$, $a \neq 0$, $b \neq 0$, $c \neq 0$, and $A + B + C = A \oplus B \oplus C$, $a$, $b$, and $c$ are linearly independent. Therefore, the previous $\mathbb{F}_2[G]$-module homomorphism from $\Omega(3)$ to $L_3(a)$ maps $\Omega(3)^G$ isomorphically onto $L_3(a)^G$. By Corollary 2.2, we that the $\mathbb{F}_2[G]$-module homomorphism is an isomorphism from $\Omega(3)$ to $L_3(a)$. Therefore, $L_3(a) \cong \Omega(3)$ as $\mathbb{F}_2[G]$-modules for any nonzero $a \in A' - \ker(\gamma)$.

Now we find copies of $\mathbb{F}_2[G]/(\rho_1)$, $\mathbb{F}_2[G]/(\rho_2)$, $\mathbb{F}_2[G]/(\rho_3)$, and $\mathbb{F}_2$ in $M$. This can be done fairly quickly given the previous machinery. More specifically, we show that for any nonzero $a \in A$ we can associate a copy of $\mathbb{F}_2[G]/(\rho_1)$, for any nonzero $b \in B$ we can associate a copy of $\mathbb{F}_2[G]/(\rho_2)$, for any nonzero $c \in C$ we can associate a copy of $\mathbb{F}_2[G]/(\rho_3)$, and for any nonzero $z$ in $M$ we can associate a copy of $\mathbb{F}_2$. However, in order to apply the Exclusion Lemma properly, we only associate copies of
\[ F_2[G]/(\rho_2) \] to nonzero elements of \( A - A' \), copies of \( F_2[G]/(\rho_1) \) to nonzero elements of \( B - \beta(A') \), copies of \( F_2[G]/(\rho_3) \) to nonzero elements of \( C - \gamma(A') \), and copies of \( F_2 \) to nonzero elements of:

\[
M^G - (\rho_1 M^{(\tau_2)} + \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_3)}).
\]

These associations make intuitive sense: The only modules \( N \in S \) for which \( B \) is nonzero are \( F_2[G]/(\rho_2) \), \( \Omega(2) \), and \( \Omega(3) \), and the only module \( N \) for which \( B - \beta(A') \) is nonzero is \( F_2[G]/(\rho_1) \). Similarly, the only modules \( N \in S \) for which \( A \) is nonzero are \( F_2[G]/(\rho_1) \), \( \Omega(2) \), and \( \Omega(3) \), and the only module \( N \) for which \( A - A' \) is nonzero is \( F_2[G]/(\rho_2) \). The only modules \( N \in S \) for which \( C \) is nonzero are \( F_2[G]/(\rho_3) \) and \( \Omega(3) \), and the only module \( N \) for which \( C - \gamma(A') \) is nonzero is \( F_2[G]/(\rho_3) \). Finally, the only module in \( S \) for which

\[
M^G - (\rho_1 M^{(\tau_2)} + \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_3)})
\]

is nonzero is \( F_2 \). Therefore, if \( M \) were the direct sum of modules in \( S \), then this procedure would identify copies of \( F_2[G]/(\rho_1) \), \( F_2[G]/(\rho_2) \), \( F_2[G]/(\rho_3) \), and \( F_2 \) in \( M \).

Now we prove that if \( b \in B \) is nonzero, then we can associate a copy of \( F_2[G]/(\rho_1) \) to \( b \). More specifically, for such an \( b \), define

\[
E_1(b) = \langle v_2(b), b \rangle.
\]

We have the following equations along with their justifications:

\[
\begin{align*}
\rho_1 \cdot v_2(b) & = 0 & v_2 B = \tilde{B} \subseteq M^{(\tau_1)}, \\
\rho_2 \cdot v_2(b) & = b & v_2 \text{ is a right-inverse of } \rho_2, \text{ and} \\
\rho_1 \cdot b & = \rho_2 \cdot b = 0 & b \in B \subseteq M^G.
\end{align*}
\]

Therefore, \( E_1(b) \) is an \( F_2[G] \)-submodule of \( M \) and the \( F_2 \)-linear transformation from \( F_2[G]/(\rho_1) \) to \( E_1(b) \) defined on basis vectors as \( 1 \mapsto v_2(b) \) and \( \rho_2 \mapsto b \) is a surjective homomorphism of \( F_2[G] \)-modules. Furthermore, we have that \( F_2[G]/(\rho_1)^G = \langle \rho_2 \rangle \) and \( E_1(b)^G = \langle b \rangle \), so the previous \( F_2[G] \)-module homomorphism from \( F_2[G]/(\rho_1) \) to \( E_1(b) \) maps \( F_2[G]/(\rho_1)^G \) isomorphically onto \( E_1(b)^G \). By Corollary 2.2, we that the \( F_2[G] \)-module homomorphism is injective. Therefore, \( E_1(b) \cong F_2[G]/(\rho_1) \) as \( F_2[G] \)-modules for any nonzero \( b \in B \).

Now we prove that if \( a \in A \) is nonzero, then we can associate a copy of \( F_2[G]/(\rho_2) \) to \( a \). More specifically, for such an \( a \), define

\[
E_2(a) = \langle a, v_1(a) \rangle.
\]

We have the following equations along with their justifications:

\[
\begin{align*}
\rho_1 \cdot a & = \rho_2 \cdot a = 0 & a \in A \subseteq M^G, \\
\rho_1 \cdot v_1(a) & = a & v_1 \text{ is a right-inverse of } \rho_1, \text{ and} \\
\rho_2 \cdot v_1(a) & = 0 & v_1 A = \tilde{A} \subseteq M^{(\tau_2)}.
\end{align*}
\]

Therefore, \( E_2(a) \) is an \( F_2[G] \)-submodule of \( M \) and the \( F_2 \)-linear transformation from \( F_2[G]/(\rho_2) \) to \( E_1(a) \) defined on basis vectors as \( 1 \mapsto v_1(a) \) and \( \rho_2 \mapsto a \) is a surjective homomorphism of \( F_2[G] \)-modules. Furthermore, we have that \( F_2[G]/(\rho_2)^G = \langle \rho_2 \rangle \) and \( E_1(a)^G = \langle a \rangle \), so the previous \( F_2[G] \)-module homomorphism from \( F_2[G]/(\rho_2) \) to \( E_1(a) \) maps \( F_2[G]/(\rho_2)^G \) isomorphically onto \( E_1(a)^G \). By Corollary 2.2, we that the \( F_2[G] \)-module homomorphism is injective. Therefore, \( E_1(a) \cong F_2[G]/(\rho_2) \) as \( F_2[G] \)-modules for any nonzero \( a \in A \).

Next we prove that if \( c \in C \) is nonzero, then we can associate a copy of \( F_2[G]/(\rho_3) \) to \( c \). More specifically, for such an \( c \), define

\[
E_3(c) = \langle v_1(c), c \rangle.
\]
We have the following equations along with their justifications:

\[
\begin{align*}
\rho_1 \cdot v_1(c) &= c & v_1 \text{ is a right-inverse of } \rho_1, \\
\rho_2 \cdot v_1(c) &= \rho_1 \cdot v_1(c) = c & v_1C \subseteq M^{(\tau_3)} \text{ and } \rho_2m = \rho_1m \text{ for all } m \in M^{(\tau_3)}, \text{ and} \\
\rho_1 \cdot c &= \rho_2 \cdot c = 0 & c \in C \subseteq M^G.
\end{align*}
\]

Therefore, \(E_3(c)\) is an \(\mathbb{F}_2[G]\)-submodule of \(M\) and the \(\mathbb{F}_2\)-linear transformation from \(\mathbb{F}_2[G]/(\rho_3)\) to \(E_3(c)\) defined on basis vectors as \(1 \mapsto v_1(c)\) and \(\rho_1 \mapsto c\) is a surjective homomorphism of \(\mathbb{F}_2[G]\)-modules. Furthermore, we have that \(\mathbb{F}_2[G]/(\rho_3)^G = \langle \rho_1 \rangle\) and \(E_3(c)^G = \langle c \rangle\), so the previous \(\mathbb{F}_2[G]\)-module homomorphism from \(\mathbb{F}_2[G]/(\rho_3)\) to \(E_3(c)\) maps \(\mathbb{F}_2[G]/(\rho_3)^G\) isomorphically onto \(E_3(c)^G\). By Corollary 2.2, we that the \(\mathbb{F}_2[G]\)-module homomorphism is injective. Therefore, \(E_3(c) \cong \mathbb{F}_2[G]/(\rho_3)^G\) as \(\mathbb{F}_2[G]\)-modules for any nonzero \(c \in C\).

Now, if \(m \in M^G\), then:

\[
\rho_1 \cdot m = \rho_2 \cdot m = 0.
\]

Thus, if we let \(Z(m) = \langle z \rangle\), then \(Z(m)\) is an \(\mathbb{F}_2[G]\)-submodule of \(G\) isomorphic to \(\mathbb{F}_2\).

Now we let \(A_3\) denote \(\ker(\gamma)\), \(A_4\) denote an \(\mathbb{F}_2\)-complement of \(\ker(\gamma)\) in \(A^\prime\), and \(A_0\) be an \(\mathbb{F}_2\)-complement of \(A^\prime\) in \(A\), so that:

\[
A^\prime = A_3 \oplus A_4 \quad \text{and} \quad A = A_0 \oplus A^\prime = A_0 \oplus A_3 \oplus A_4.
\]

Now we let \(B_0\) be an \(\mathbb{F}_2\)-complement of \(\beta(A^\prime)\) in \(B\) and \(C_0\) be an \(\mathbb{F}_2\)-complement of \(\gamma(A^\prime)\) in \(C\), so that:

\[
B = B_0 \oplus \beta(A^\prime) \quad \text{and} \quad C = C_0 \oplus \gamma(A^\prime).
\]

However, \(\beta\) is injective, so \(\beta(A^\prime) = \beta(A_3) \oplus \beta(A_4)\). Furthermore, \(\gamma\) is identically 0 on \(A_3 = \ker(\gamma)\), and so is injective on \(A_4\). This implies that \(\gamma(A^\prime) = \gamma(A_4)\). Therefore,

\[
B = B_0 \oplus \beta(A_3) \oplus \beta(A_4) \quad \text{and} \quad C = C_0 \oplus \gamma(A_4).
\]

We also recall that \(Z\) is an \(\mathbb{F}_2\) complement of:

\[
\rho_1 M^{(\tau_2)} + \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_3)} = A \oplus B \oplus C \oplus L \oplus T
\]

in \(M^G\). Therefore, we have that:

\[
M^G = A \oplus B \oplus C \oplus L \oplus T \oplus Z = A_0 \oplus A_3 \oplus A_4 \oplus B_0 \oplus \beta(A_3) \oplus \beta(A_4) \oplus C_0 \oplus \gamma(A_4) \oplus L \oplus T \oplus Z.
\]

Next, let \(A_0, A_3, A_4, B_0, C_0,\) and \(Z\) be \(\mathbb{F}_2\)-bases for \(A_0, A_3, A_4, B_0, C_0,\) and \(Z\), respectively. We also recall that \(L\) and \(T\) are \(\mathbb{F}_2\)-bases of \(L\) and \(T\). Then because \(\beta\) is injective and \(\gamma\) is injective on \(A_4, \beta(A_3), \beta(A_4),\) and \(\gamma(A_4)\) are \(\mathbb{F}_2\)-bases of \(\beta(A_3), \beta(A_4),\) and \(\gamma(A_4)\), respectively. This implies that:

\[
A_0 \cup \{ a', \beta(a') | a' \in A_3 \} \cup \{ a, \beta(a), \gamma(a) | a \in A_4 \} \cup B_0 \cup C_0 \cup L \cup T \cup Z
\]

is an \(\mathbb{F}_2\)-basis for \(M^G\). Therefore:

\[
A_0 \cup \{ a', \beta(a') | a' \in A_3 \} \cup \{ a, \beta(a), a + \beta(a) + \gamma(a) | a \in A_4 \} \cup B_0 \cup C_0 \cup L \cup T \cup Z.
\]
is also an $\mathbb{F}_2$-basis for $M^G$. Therefore, since:
\[
E(\ell)^G = \langle \ell \rangle \quad \text{for all } \ell \in \mathcal{L},
\]
\[
E_1(b_0)^G = \langle b_0 \rangle \quad \text{for all } b_0 \in \mathcal{B}_0,
\]
\[
E_2(a_0)^G = \langle a_0 \rangle \quad \text{for all } a_0 \in \mathcal{A}_0,
\]
\[
E_3(c_0)^G = \langle c_0 \rangle \quad \text{for all } c_0 \in \mathcal{C}_0,
\]
\[
L_1(t)^G = \langle t \rangle \quad \text{for all } t \in \mathcal{T},
\]
\[
L_2(a_3)^G = \langle a_3, \beta(a_3) \rangle \quad \text{for all } a_3 \in \mathcal{A}_3,
\]
\[
L_3(a_4)^G = \langle a_4, \beta(a_4), a_4 + \beta(a_4) + \gamma(a_4) \rangle \quad \text{for all } a_4 \in \mathcal{A}_4,
\]
\[
Z(m)^G = \langle m \rangle \quad \text{for all } m \in \mathcal{Z},
\]
the sum:
\[
\sum_{\ell \in \mathcal{L}} E(\ell)^G + \sum_{b_0 \in \mathcal{B}_0} E_1(b_0)^G + \sum_{a_0 \in \mathcal{A}_0} E_2(a_0)^G + \sum_{c_0 \in \mathcal{C}_0} E_3(c_0)^G + \sum_{t \in \mathcal{T}} L_1(t)^G
\]
\[
+ \sum_{a_3 \in \mathcal{A}_3} L_2(a_3)^G + \sum_{a_4 \in \mathcal{A}_4} L_3(a_4)^G + \sum_{m \in \mathcal{Z}} Z(m)^G
\]
is direct. Therefore, from the Exclusion Lemma, the sum:
\[
\sum_{\ell \in \mathcal{L}} E(\ell) + \sum_{b_0 \in \mathcal{B}_0} E_1(b_0) + \sum_{a_0 \in \mathcal{A}_0} E_2(a_0) + \sum_{c_0 \in \mathcal{C}_0} E_3(c_0) + \sum_{t \in \mathcal{T}} L_1(t) + \sum_{a_3 \in \mathcal{A}_3} L_2(a_3) + \sum_{a_4 \in \mathcal{A}_4} L_3(a_4) + \sum_{m \in \mathcal{Z}} Z(m)
\]
is also direct. Let $\tilde{M}$ denote the previous sum.

The last step is to show that $M = \tilde{M}$. To do this, we choose an arbitrary element $m \in M$ and consider seven cases based on which of the seven ideals of $\mathbb{F}_2[G]$ $\text{Ann}_{\mathbb{F}_2[G]}(m)$ is. In each of the seven cases, we show that $m \in \tilde{M}$ by adding or subtracting known elements of $M$ until the result is clearly in $\tilde{M}$. In order to facilitate this procedure, we first prove that $M^G$, $Y$, the image of $v_1$, and the image of $v_2$ are all contained in $M$.

Note that because $\tilde{M}$ contains the following basis of $M^G$, it contains all of $M^G$:
\[
\mathcal{A}_0 \cup \{a', \beta(a')|a' \in \mathcal{A}_3\} \cup \{a, \beta(a), a + \beta(a) + \gamma(a)|a \in \mathcal{A}_4\} \cup \mathcal{B}_0 \cup \mathcal{C}_0 \cup \mathcal{L} \cup \mathcal{T} \cup \mathcal{Z}.
\]
Next, for any $\ell \in \mathcal{L}$, $f(\ell) \in E(\ell)$, so $f(\mathcal{L}) \subseteq \tilde{M}$. But since $f : L \to Y$ is an isomorphism, $f(\mathcal{L})$ is a basis for $Y$, so $Y \subseteq \tilde{M}$.

We prove that $\tilde{M}$ contains the image of $v_1$ in the same way. We first recall that the domain of $v_1$ is:
\[
A \oplus C \oplus L \oplus T = A_0 \oplus A_3 \oplus A_4 \oplus C_0 \oplus \gamma(A_4) \oplus L \oplus T.
\]
Since $v_1$ is an isomorphism, its image is therefore:
\[
v_1(A_0) \oplus v_1(A_3) \oplus v_1(A_4) \oplus v_1(C_0) \oplus v_1\gamma(A_4) \oplus v_1(L) \oplus v_1(T).
\]
Now, for $a \in \mathcal{A}_4$,
\[
v_1\gamma(a) = v_1(a) + (v_1 + v_2)(a) + (v_2(a) + v_2\beta(a) + v_1\gamma(a)) + v_2\beta(a) \in L_3(a),
\]
so that $v_1\gamma(\mathcal{A}_4) \subseteq \tilde{M}$. But $v_1\gamma(\mathcal{A}_4)$ is a basis for $v_1\gamma(\mathcal{A}_4)$, so $v_1\gamma(\mathcal{A}_4) \in \tilde{M}$. Similarly:

For $a \in \mathcal{A}_0$, $v_1(a) \in E_2(a)$, so that $v_1(A_0) \subseteq \tilde{M}$, thus $v_1(A_0) \subseteq \tilde{M}$.

For $a \in \mathcal{A}_3$, $v_1(a) \in L_2(a)$, so that $v_1(\mathcal{A}_3) \subseteq \tilde{M}$, thus $v_1(\mathcal{A}_3) \subseteq \tilde{M}$.

For $a \in \mathcal{A}_4$, $v_1(a) \in L_3(a)$, so that $v_1(A_4) \subseteq \tilde{M}$, thus $v_1(A_4) \subseteq \tilde{M}$.

For $c \in \mathcal{C}_0$, $v_1(c) \in E_3(c)$, so that $v_1(C_0) \subseteq \tilde{M}$, thus $v_1(C_0) \subseteq \tilde{M}$.

For $\ell \in \mathcal{L}$, $v_1(\ell) = p_2 f(\ell) \in E(\ell)$, so that $v_1(\mathcal{L}) \subseteq \tilde{M}$, thus $v_1(L) \subseteq \tilde{M}$.

For $t \in \mathcal{T}$, $v_1(t) = L_1(t)$, so that $v_1(T) \subseteq \tilde{M}$, thus $v_1(T) \subseteq \tilde{M}$. 

30
Therefore, the image of $v_1$ is in $\tilde{M}$.

Similarly, $\tilde{M}$ contains the image of $v_2$. The domain of $v_2$ is:

$$A' \oplus B \oplus L \oplus T = A_3 \oplus A_4 \oplus B_0 \oplus \beta(A_3) \oplus \beta(A_4) \oplus L \oplus T.$$  

Since $v_2$ is an isomorphism, its image is therefore:

$$v_2(A_3) \oplus v_2(A_4) \oplus v_2(B_0) \oplus v_2(\beta(A_3)) \oplus v_2(\beta(A_4)) \oplus v_2(L) \oplus v_2(T).$$

We have:

For $a \in A_3$, $v_2(a) \in L_2(a)$, so that $v_2(A_3) \subseteq \tilde{M}$, thus $v_2(A_3) \subseteq \tilde{M}$.

For $a \in A_3$, $v_2(\beta(a)) \subseteq L_2(a)$, so that $v_2(\beta(A_3)) \subseteq M$, thus $v_2(\beta(A_3)) \subseteq M$.

For $a \in A_4$, $v_2(a) = v_1(a) + v_2(a) \in L_3(a)$, so that $v_2(A_4) \subseteq \tilde{M}$, thus $v_2(A_4) \subseteq \tilde{M}$.

For $b \in B_0$, $v_2(b) \in E_1(b)$, so that $v_2(B_0) \subseteq \tilde{M}$, thus $v_2(B_0) \subseteq \tilde{M}$.

For $\ell \in L$, $v_2(\ell) = \rho_1 f(\ell) \in E(\ell)$, so that $v_2(L) \subseteq \tilde{M}$, thus $v_2(L) \subseteq \tilde{M}$.

For $t \in T$, $v_2(t) = L_1(t)$, so that $v_2(T) \subseteq \tilde{M}$, thus $v_2(T) \subseteq \tilde{M}$.

Therefore, the image of $v_2$ is in $\tilde{M}$.

Let $m \in M$ be arbitrary. Then $\text{Ann}_{F_2[G]}(m)$ is an ideal of $F_2[G]$, so there are seven possibilities for it, namely:

$$F_2[G] = (\rho_1 \cup \rho_2) \cup (\rho_1 \rho_2) \cup (\rho_3).$$

We examine each of these cases in turn, in this order.

**Case 1:** If $\text{Ann}_{F_2[G]}(m) = F_2[G]$, then $1m = 0$, so $m = 0 \in \tilde{M}$.

**Case 2:** If $\text{Ann}_{F_2[G]}(m) = (\rho_1 \cup \rho_2)$, then $m \in M^{G} \subseteq \tilde{M}$.

**Case 3:** If $\text{Ann}_{F_2[G]}(m) = (\rho_2)$, then $m \in M^{(\tau_2)}$ and $\rho_1 m \in \rho_1 M^{(\tau_2)} = A + L + T$. Then $\rho_1 m$ is in the domain of $v_1$, $v_1 \rho_1 m \in \tilde{M}$, and

$$v_1 \rho_1 m \in \tilde{A} + Y_1 + W_1 \subseteq M^{(\tau_2)}.$$  

Then we have:

$$\rho_1(m - v_1 \rho_1 m) = \rho_1 m - \rho_1 m = 0 \quad \text{and} \quad \rho_2(m - v_1 \rho_1 m) = 0 - 0 = 0.$$  

Thus, $m - v_1 \rho_1 m \in M^{G} \subseteq \tilde{M}$, so $m = (m - v_1 \rho_1 m) + v_1 \rho_1 m \in \tilde{M}$.

**Case 4:** If $\text{Ann}_{F_2[G]}(m) = (\rho_1)$, then $m \in M^{(\tau_1)}$ and $\rho_2 m \in \rho_2 M^{(\tau_1)} = B + L + T$. Then $\rho_2 m$ is in the domain of $v_2$, $v_2 \rho_2 m \in \tilde{M}$, and

$$v_2 \rho_2 m \in \tilde{B} + Y_2 + W_2 \subseteq M^{(\tau_1)}.$$  

Then we have:

$$\rho_1(m - v_2 \rho_2 m) = 0 - 0 = 0 \quad \text{and} \quad \rho_2(m - v_2 \rho_2 m) = \rho_2 m - \rho_2 m = 0.$$  

Thus, $m - v_2 \rho_2 m \in M^{G} \subseteq \tilde{M}$, so $m = (m - v_2 \rho_2 m) + v_2 \rho_2 m \in \tilde{M}$.

**Case 5:** Assume $\text{Ann}_{F_2[G]}(m) = (\rho_1 \rho_2)$. Then:

$$\rho_1 \rho_2 m = \rho_1 \rho_2 m = 0 \quad \text{and} \quad \rho_2 \rho_2 m = \rho_2^2 m = 0 m = 0.$$  

Thus, $\rho_2 m \in M^{G}$, so that:

$$\rho_2 m \in \rho_2 M \cap M^{G} \subseteq \sum_{i=1}^{3} (\rho_i \cap M^G) \subseteq \rho_2 M^{(\tau_1)} + \rho_1 M^{(\tau_2)} + \rho_1 M^{(\tau_3)} = A \oplus B \oplus C \oplus L \oplus T.$$  

Thus, there are $a \in A$, $b \in B$, $c \in C$, $\ell \in L$, and $t \in T$ so that:

$$\rho_1 m = a + b + c + \ell + t.$$
Notice that $c$ is in the domain of $v_1$ and $b + \ell + t$ is in the domain of $v_2$, so that $v_1(c)$ and $v_2(b + \ell + t)$ are well-defined elements of $\hat{M}$. Furthermore, as $v_1(c) \in \hat{C} \subseteq M^{(\tau_3)}$ and $\rho_1 v = \rho_2 v$ for all $v \in M^{(\tau_3)}$, we have that $\rho_2 v_1(c) = \rho_1 v_1(c) = c$. Thus, if we define:

$$x = m - v_1(c) - v_2(b + \ell + t),$$

then:

$$\rho_2 x = \rho_2 m - \rho_2 v_1(c) - \rho_2 v_2(b + \ell + t) = (a + b + c + \ell + t) - c - (b + \ell + t) = a.$$

Therefore, $a \in A \cap \rho_2 M$, which, we recall, was equal to $A'$. Also recall that $A'$ is in the domain of $v_2$, so that $v_2(a)$ is a well-defined element of $\hat{M}$. Further, if we let $x' = x - v_2(a)$, then:

$$\rho_2 x' = \rho_2 x - \rho_2 v_2(a) = a - a = 0.$$

Thus, $\rho_2 \in \text{Ann}_{F_2[G]}(x')$, and there are only three ideals of $F_2[G]$ that contain $\rho_2$, namely $F_2[G]$, $V$, and $(\rho_2)$. We therefore have, by appealing to Cases 1, 2, and 3, that $x' \in \hat{M}$, and therefore:

$$m = x + v_1(c) + v_2(b + \ell + t) = x' + v_2(a) + v_1(c) + v_2(b + \ell + t) \in \hat{M},$$

so we are done with this case.

**Case 6:** Assume $\text{Ann}_{F_2[G]}(m) = (\rho_3)$. Then $m \in M^{(\tau_3)}$, so that $\rho_1 m = \rho_2 m$

$$\rho_1 m \in \rho_1 M^{(\tau_3)} \subseteq A \oplus B \oplus C \oplus L \oplus T.$$

Thus, there are $a \in A$, $b \in B$, $c \in C$, $\ell \in L$, and $t \in T$ so that:

$$\rho_1 m = a + b + c + \ell + t.$$

We now split this case into three different subcases.

**Case 6a:** $a + \ell + t = b = 0$. Then $\rho_1 m = c$, $v_1(c) \in M^{(\tau_3)}$, and $\rho_1 v_1(c) = \rho_2 v_1(c) = c$. Thus, if $x = m - v_1(c)$, then:

$$\rho_1 x = \rho_1 m - \rho_1 v_1(c) = c - c = 0 \quad \rho_2 x = \rho_2 m - \rho_2 v_1(c) = \rho_1 m - \rho_1 v_1(c) = 0.$$

Thus, $x \in M^G \subseteq \hat{M}$, so $m = x + v_1(c) \in \hat{M}$.

**Case 6b:** $a + \ell + t \neq 0$ and $b = 0$. Then $\rho_1 m = \rho_2 m = (a + \ell + t) + c$, which is in the domain of $v_1$. Now, $v_1(a + \ell + t) \in M^{(\tau_3)}$. However, $v_1(c) \in M^{(\tau_3)}$, so that $\rho_1 v_1(c) = \rho_2 v_1(c) = c$. Thus, if $x = m - v_1(\rho_1 m)$, then:

$$\rho_1 x = \rho_1 m - \rho_1 v_1(\rho_1 m) = \rho_1 m - \rho_1 m = 0,$$

$$\rho_2 x = \rho_2 m - \rho_2 v_1(\rho_1 m) = \rho_2 m - \rho_2 v_1(a + \ell + t) - \rho_2 v_1(c) = (a + c + \ell + t) - 0 - c = a + \ell + t,$$

$$\rho_1 \rho_2 x = \rho_2 x = \rho_2 \cdot \rho_1 x = \rho_2 \cdot 0 = 0.$$

Since $a + \ell + t \neq 0$, $\rho_1 x \neq \rho_2 x$, so $(\rho_1 + \rho_2)x = (\rho_1 - \rho_2)x \neq 0$ and $\rho_1 + \rho_2 \notin \text{Ann}_{F_2[G]}(x)$. However, $\rho_1 \rho_2 \in \text{Ann}_{F_2[G]}(x)$. There are only three ideals of $F_2[G]$ that contain $\rho_1 \rho_2$ but do not contain $\rho_1 + \rho_2$, namely $(\rho_2)$, $(\rho_2)$, and $(\rho_1 \rho_2)$. We therefore have, by appealing to Cases 3, 4, and 5, that $x \in \hat{M}$ and therefore:

$$m = x + v_1(\rho_1 m) \in \hat{M},$$

so we are done with this case.

**Case 6c:** $b \neq 0$. Then $v_2(b) \in M^{(\tau_3)}$. Thus, if $x = m - v_2(b)$, then:

$$\rho_1 x = \rho_1 m - \rho_1 v_2(b) = (a + b + \ell + t) - 0 = a + b + c + \ell + t,$$

$$\rho_2 x = \rho_2 m - \rho_2 v_2(b) = (a + b + c + \ell + t) - b = a + c + \ell + t.$$
we have that $\rho_1\rho_2x = 0$, so $\rho_1\rho_2 \in \text{Ann}_{\mathbb{F}_2[G]}(x)$. There are only three ideals of $\mathbb{F}_2[G]$ that contain $\rho_1\rho_2$ but do not contain $\rho_1 + \rho_2$, namely $(\rho_2)$, $(\rho_3)$, and $(\rho_1\rho_2)$. We therefore have, by appealing to Cases 3, 4, and 5, that $x \in M$ and therefore:

$$m = x + v_2(b) \in \tilde{M},$$

so we are done with this case.

**Case 7**: Assume $\text{Ann}_{\mathbb{F}_2[G]}(m) = 0$. Then $\rho_1\rho_2m$ is a nonzero element of $L$, so there is some nonzero element $y \in Y$ (namely $f(m)$) such that $\rho_1\rho_2y = \rho_1\rho_2m$. Let $x = m - y$. Then:

$$\rho_1\rho_2x = \rho_1\rho_2m - \rho_1\rho_2y = 0,$$

so $\rho_1\rho_2 \in \text{Ann}_{\mathbb{F}_2[G]}(x)$. Thus, $\text{Ann}_{\mathbb{F}_2[G]}(x)$ is one of the six nonzero ideals of $\mathbb{F}_2[G]$, namely $\mathbb{F}_2[G]$, $(\rho_1, \rho_2)$, $(\rho_1)$, $(\rho_2)$, $(\rho_3)$, and $(\rho_1\rho_2)$. We therefore have, by appealing to Cases 1 through 6, that $x \in \tilde{M}$. As $y \in Y \subseteq \tilde{M}$, we therefore have:

$$m = x + y \in \tilde{M},$$

so we are done with this case.

In all seven cases, $m \in \tilde{M}$. As $m \in M$ was arbitrary, we conclude that $M = \tilde{M}$ and that $M$ is a direct sum of copies of the eight $\mathbb{F}_2[G]$-modules $\mathbb{F}_2[G]$, $\mathbb{F}_2[G]/(\rho_1)$, $\mathbb{F}_2[G]/(\rho_2)$, $\mathbb{F}_2[G]/(\rho_3)$, $\Omega(1)$, $\Omega(2)$, $\Omega(3)$, and $\mathbb{F}_2$. This is precisely statement (2), and we are finally done with the proof of Proposition 2.6. QED
CHAPTER 3

Review of Galois Cohomology

1. Topological Groups

This exposition is taken largely from Chapter IV of [Mc].

A topological group is a group $G$ with a topology such that the two maps $\_ \cdot \_ : G \times G \to G$ and $\_^{-1} : G \to G$ are both continuous. If $G_1$ and $G_2$ are topological groups, then a homomorphism of topological groups is a map $f : G_1 \to G_2$ that is both a group homomorphism and continuous map. An isomorphism of topological groups is a map $f : G_1 \to G_2$ that is both a group isomorphism and a homeomorphism. Under these definitions, the class of all topological groups and homomorphisms of topological groups is a category, and the isomorphisms of topological groups are the isomorphisms of this category.

For any topological group $G$ and fixed $g \in G$, the maps $g \cdot \_ : G \to G$ and $\_ \cdot g : G \to G$ are both homeomorphisms of $G$ onto itself. An open subgroup of a topological group is automatically closed.

Any abstract group can be made into a topological group by giving it the discrete topology; a topological group with the discrete topology is called a discrete group. Furthermore, if $G_1$ and $G_2$ are topological groups and $f : G_1 \to G_2$ is a homomorphism of abstract groups, then if $G_1$ is a discrete group, then $f$ is automatically continuous and therefore a homomorphism of topological groups.

Given any abstract group $G$, it can be made into a topological group by specifying a local base of the identity. More specifically, let $\mathcal{B} = \{ B_i : i \in \mathcal{I} \}$ be a set of subsets of $G$, each of which contains the identity $1$, such that $\bigcup_{i \in \mathcal{I}} B_i = G$ and for any $i_1, i_2 \in \mathcal{I}$, there is an $i_3 \in \mathcal{I}$ such that $B_{i_3} \subseteq B_{i_1} \cap B_{i_2}$. Then define a topology on $G$ by calling a subset of $G$ open if and only if it is a union of sets of the form $g_1 B g_2$ for $g_1, g_2 \in G$ and $B \in \mathcal{B}$. This topology is the coarsest topology on $G$ that makes $G$ into a topological group. It is called the topology generated by $\mathcal{B}$, and $\mathcal{B}$ is said to be a local base of the identity for this topology.

For any topological group $G$ and subgroup $H$ of $G$, $H$ is a topological group under the subspace topology, and under this topology the inclusion $H \hookrightarrow G$ is an injective homomorphism of topological groups.

For any topological group $G$ and closed normal subgroup $H$ of $G$, the quotient group $G/H$ is a topological group under the quotient topology, and furthermore the quotient map $G \to G/H$ is a surjective homomorphism of topological groups.

(First isomorphism theorem for topological groups.) For any homomorphism $f : G_1 \to G_2$ of topological groups, the induced group isomorphism $\tilde{f} : G_1/\ker(f) \to \im(f)$ is an isomorphism of topological groups (i.e. a homeomorphism) if and only if $f$ is an open mapping.

Finally, let $\{ G_i | i \in \mathcal{I} \}$ be any collection of topological groups. Then the direct product $\prod_{i \in \mathcal{I}} G_i$ is a topological group under the product topology.

2. Infinite Galois Theory

This exposition is taken largely from Section IV.1 of [Ne] and Sections V.3 and VI.1 of [La].

Let $K/k$ be any field extension. Then the Galois group Gal($K/k$) is defined to be the group of all automorphisms of $K$ that fix $k$ pointwise.

Now let $K/k$ be any field extension. An element $\alpha \in K$ is said to be algebraic over $k$ if there is a polynomial $f \in k[x]$ such that $f(\alpha) = 0$. The field extension $K/k$ is said to be algebraic if every element of $K$ is algebraic over $k$. An element $\alpha \in K$ is said to be separable over $k$ if it is algebraic
over \( k \) and its minimal polynomial \( f_\alpha \in k[x] \) has no repeated roots in its splitting field. The field extension \( K/k \) is said to be **separable** if every element of \( K \) is separable over \( k \). If \( K/k \) is algebraic, then the following four conditions on \( K/k \) are equivalent; if \( K/k \) satisfies any one of them, then \( K/k \) is said to be **normal**:

1. Let \( \overline{k} \) be any algebraic closure of \( k \) that contains \( K \). Then for any embedding \( \sigma : K \to \overline{k} \) such that \( \sigma|_k \) is the identity on \( k \), \( \sigma(K) = K \).
2. \( K \) is the splitting field of some set of polynomials in \( k[x] \).
3. If \( f \in k[x] \) is irreducible and has a root in \( K \), then \( f \) splits into linear factors in \( K \).
4. For any element of \( \alpha \in K \setminus k \), there is some \( \sigma \in \text{Gal}(K/k) \) such that \( \sigma(\alpha) \neq \alpha \).

Finally, \( K/k \) is said to be a **Galois** extension if it is algebraic, separable, and normal.

As an example of a Galois extension, let \( \overline{k} \) be any algebraic closure of \( k \), and let \( k^{\text{sep}} \subseteq \overline{k} \) be the set of all elements of \( \overline{k} \) that are separable over \( k \). Then \( k^{\text{sep}} \) is called a **separable closure** of \( k \), and \( k^{\text{sep}}/k \) is a Galois extension. Furthermore, if \( K/k \) is a separable extension, then we may choose an algebraic closure \( \overline{k} \) of \( k \) that contains \( K \), so \( k^{\text{sep}} \) can be chosen so that it contains \( K \), and in this case \( k^{\text{sep}} \) is a separable closure for \( K \), as well.

Galois groups of Galois extensions \( K/k \) have several nice properties. The first is that if \( L \) is any field such that \( k \subseteq L \subseteq K \), then \( K/L \) is automatically Galois. Second, they can be made into topological groups under a topology called the **Krull topology**. It is the topology generated by the following local base of the identity of \( \text{Gal}(K/k) \):

\[
\{ \text{Gal}(K/L) | k \subseteq L \subseteq K, [L : k] < \infty \}.
\]

Like all topological groups, any closed subgroup of \( \text{Gal}(K/k) \) is automatically open. However, the Krull topology has the property that closed subgroups of \( \text{Gal}(K/k) \) are open if and only if they are of finite index in \( \text{Gal}(K/k) \). Furthermore, if \( K/k \) is a finite Galois extension, then the Krull topology on \( \text{Gal}(K/k) \) is the discrete topology.

The introduction of the Krull topology makes it possible to state the following theorem:

**Theorem 3.1. (Fundamental Theorem of Infinite Galois Theory)** Let \( K/k \) be any Galois extension of fields. Let \( \mathcal{L} \) be the set of all fields \( L \) such that \( k \subseteq L \subseteq K \), and let \( \mathcal{H} \) be the set of all closed subgroups of \( \text{Gal}(K/k) \) under the Krull topology. Furthermore, let \( \mathcal{L}_0 \subseteq \mathcal{L} \) be the set of all fields \( L \) such that \( k \subseteq L \subseteq K \) and \( [L : k] < \infty \), and let \( \mathcal{H}_0 \subseteq \mathcal{H} \) be the set of all open subgroups of \( \text{Gal}(K/k) \) under the Krull topology. Finally, for any \( H \in \mathcal{H} \), let \( F(H) = K^H \), and for any \( L \in \mathcal{L} \), let \( G(L) \) be the group \( \text{Gal}(L/K) \). Then:

1. \( F \) and \( G \) are mutually inverse bijections between \( \mathcal{H} \) and \( \mathcal{L} \).
2. \( F \) and \( G \) are mutually inverse bijections between \( \mathcal{H}_0 \) and \( \mathcal{L}_0 \).
3. For \( L_1, L_2 \in \mathcal{L} \), \( L_1 \subseteq L_2 \) if and only if \( G(L_1) \supseteq G(L_2) \).
4. For \( H \in \mathcal{H} \), if \( H \) is finite, then \( K^H/k \) is a finite extension and \( [K^H : k] = |H| \).
5. For \( L \in \mathcal{L} \), \( L/k \) is Galois if and only if \( \text{Gal}(K/L) \subseteq \text{Gal}(K/k) \), and if either of these two conditions hold, then the map \( \phi : \text{Gal}(K/k) \to \text{Gal}(L/k) \) defined as \( \sigma \mapsto \sigma_L \) is a well-defined and surjective homomorphism of topological groups that induces the following isomorphism of profinite groups:

\[
\text{Gal}(L/k) \cong \text{Gal}(K/k)/\text{Gal}(L/K).
\]

**Proof.** (1) and (2) together form the statement of Theorem IV.1.2 of [Ne]. (3) is Corollary VI.1.5 of [La]. (4) is Theorem VI.1.8 of [La]. Theorem VI.1.10 of [La] essentially states all parts of (5) except that the surjective group homomorphism \( \phi : \sigma \mapsto \sigma_L \) is continuous and that the induced group isomorphism \( \tilde{\phi} : \text{Gal}(K/k)/\text{Gal}(L/K) \to \text{Gal}(L/k) \) is a homeomorphism. We now prove these statements.

Note that by the definition of the Krull topology and the fact that \( \phi \) is a surjective group homomorphism, to prove that \( \phi \) is continuous, it suffices to prove that the inverse image of an open set of the form \( \text{Gal}(L/L') \) under \( \phi \) is open in \( \text{Gal}(K/k) \), for any field \( L' \) such that \( k \subseteq L' \subseteq L \) and
[L' : k] < ∞. But for such a field L', φ⁻¹(Gal(L/L')) = Gal(K/L'), and by definition of the Krull topology, Gal(K/L') is open in Gal(K/k). Thus, φ is continuous.

By the first isomorphism theorem for topological groups, to prove that ˜φ is a homeomorphism, it suffices to show that φ is an open mapping. By the definition of the Krull topology, it suffices to show that the image of an open set of the form Gal(K/L) under φ is open in Gal(L/k), for any field L' such that k ⊆ L' ⊆ K and [L' : k] < ∞. But by what we have already proved of statement (5), φ(Gal(K/L')) = Gal(L/L'), and by definition of the Krull topology, Gal(K/L') is open in Gal(K/k). Thus, φ is open and ˜φ is a homeomorphism, as desired. QED

Notice that since the Krull topology on Gal(K/k) is the discrete topology if K/k is finite, the fundamental theorem of infinite Galois theory reduces to the standard fundamental theorem of Galois theory if K/k is finite.

3. Inverse Limits and Profinite Groups

This exposition is taken largely from Section IV.2 of [Ne].

Let I be a set with a preorder, i.e. a set with a reflexive and transitive relation ≤. Let \{G_i|i ∈ I\} be a collection of topological groups indexed by I. Suppose that for all i, j ∈ I with i ≤ j there is a homomorphism of topological groups f_{ij} : G_j → G_i such that f_{ii} = Id_{G_i} and for all i, j, k ∈ I with i ≤ j ≤ k, we have f_{ik} = f_{ij} ∘ f_{jk}. Then the collection (\{G_i|i ∈ I\}, \{f_{ij}|i, j ∈ I, i ≤ j\}) is called an inverse system of topological groups.

A topological group G and set of homomorphisms of topological groups \{π_i : G → G_i|i ∈ I\} is called an inverse limit or a projective limit of the inverse system (\{G_i|i ∈ I\}, \{f_{ij}|i, j ∈ I, i ≤ j\}) if:

1. For all i, j ∈ I with i ≤ j, π_i = f_{ij} ∘ π_j.
2. For any topological group G' and set of homomorphisms of topological groups \{π'_i : G' → G_i|i ∈ I\} such that for all i, j ∈ I with i ≤ j, π'_i = f_{ij} ∘ π'_j, there is a unique homomorphism of topological groups g : G' → G such that for all i ∈ I we have π_i ∘ g = π'_i, in other words there is a unique homomorphism of topological groups g : G' → G such that for all i, j ∈ I with i ≤ j the following diagram commutes:

```
   G'
   | π'_j
   v   |
   G  π'
   |   |
   v   |
G_j  f_{ij}  G_i
```

By this definition, inverse limits are unique up to isomorphism. In other words, if (G, \{π_i|i ∈ I\}) and (G', \{π'_i|i ∈ I\}) are both inverse limits of the inverse system (\{G_i|i ∈ I\}, \{f_{ij}|i, j ∈ I, i ≤ j\}), then there is an isomorphism g : G' → G of topological groups such that for all i ∈ I we have π_i ∘ g = π'_i.

Now let \( \{G_i|i ∈ I\}, \{f_{ij}|i, j ∈ I, i ≤ j\} \) and \( \{G_i|i ∈ I\}, \{f_{ij}|i, j ∈ I, i ≤ j\} \) be any two inverse systems of topological groups indexed by the same set I. A homomorphism of inverse systems of topological groups is any set \{h_i : G_i → G_i|i ∈ I\} of homomorphisms of topological groups such that for all i, j ∈ I with i ≤ j, the following square commutes:

```
   G_j  f_{ij}  G_i
   ↓   ↓    ↓    ↓
   G_j  f_{ij}  G_i
```

37
Now suppose that \{\hat{G}_i, \hat{f}_{ij}|i, j \in I, i \leq j\} has an inverse limit \(\hat{G}, \{\hat{\pi}_i|i \in I\}\) and \(\{G_i, f_{ij}|i, j \in I, i \leq j\}\) has an inverse limit \(\hat{G}, \{\hat{\pi}_i|i \in I\}\). Then there is a unique homomorphism \(h: \hat{G} \to G\) such that for all \(i \in I\), the following square commutes:

\[
\begin{array}{ccc}
\hat{G} & \xrightarrow{\hat{\pi}_i} & \hat{G}_i \\
\downarrow{h} & & \downarrow{h_i} \\
G & \xrightarrow{\pi_i} & G_i
\end{array}
\]

This is because if we define \(\pi'_i : \hat{G} \to G_i\) to be \(h_i \circ \hat{\pi}_i\) for each \(i \in I\), then for all \(i, j \in I\) we have \(\pi'_i = f_{ij} \circ \pi'_j\), and by condition (2) of inverse limit, there must be a there is a unique homomorphism of topological groups \(h : \hat{G} \to G\) such that for all \(i \in I\) we have \(\pi_i \circ h = \pi'_i\). This homomorphism \(h\) is called the homomorphism induced by the homomorphism \(\{h_i|i \in I\}\) of direct systems. Furthermore, if each \(h_i\) is an isomorphism, then \(h\) is also an isomorphism.

As should be clear, this definition of inverse system, inverse limit, homomorphism of inverse systems, and homomorphism of inverse limits induced by a homomorphism of inverse systems can be applied to any category, not just for topological groups. However, within this paper we will only use these constructions for topological groups.

It happens that any inverse system of topological groups has an inverse limit. More specifically, let \(\{\{G_i|i \in I\}, \{f_{ij}|i, j \in I, i \leq j\}\}\) be an inverse system of topological groups. Let \(G\) be the following subset of the product topological group \(\prod_{i \in I} G_i\):

\[
\left\{(g_i) \in \prod_{i \in I} G_i | \forall i, j \in I, i \leq j \Rightarrow f_{ij}(g_i) = g_i \right\}.
\]

Then \(G\) is a subgroup of \(\prod_{i \in I} G_i\). Next, for each \(i \in I\), let \(\pi_i : G \to G_i\) be projection onto the \(i\)th component. Then \((G, \{\pi_i|i \in I\})\) is an inverse limit of \(\{\{G_i|i \in I\}, \{f_{ij}|i, j \in I, i \leq j\}\}\). We will denote this inverse limit as \(\lim_{i \in I} G_i\), provided it is obvious what the set \(I\) and the maps \(f_{ij}\) are.

Furthermore, we have a simple description of the homomorphism \(h : \lim_{i \in I} \hat{G}_i \to \lim_{i \in I} G_i\) induced by the homomorphism \(\{h_i : \hat{G}_i \to G_i\}\) of inverse systems. Specifically, the element \((\hat{g}_i) \in \lim_{i \in I} \hat{G}_i\) is mapped to the element \((h_i(\hat{g}_i)) \in \lim_{i \in I} G_i\).

We say that a topological group \(G\) is a **profinite group** if it is the group of an inverse limit of some direct system of finite, discrete topological groups. A somewhat deep theorem says that a topological group is profinite if and only if Hausdorff, compact, and totally disconnected. Note that all finite discrete groups are automatically profinite groups. In any profinite group \(G\), a closed subgroup \(H\) is open if and only if \((G : H)\) is finite.

For any profinite group \(G\) and any closed normal subgroup \(H\), \(G/H\) is automatically a profinite group. More specifically, suppose that \((G, \{\pi_i : i \in I\})\) is an inverse limit of the inverse system \(\{\{G_i|i \in I\}, \{f_{ij}|i, j \in I, i \leq j\}\}\) of finite, discrete topological groups and \(H\) is a closed subgroup of \(G\). For \(i \in I\), let \(G'_i\) be the finite discrete group \(G_i/(G_i \cap H)\). For all \(i, j \in I\) with \(i \leq j\), let \(f_{ij}' : G'_j \to G'_i\) be the homomorphism induced from \(f_{ij}\). Then \(f_{ij}'\) is automatically a homomorphism of topological groups, and \(\{\{G'_i|i \in I\}, \{f_{ij}'|i, j \in I, i \leq j\}\}\) is an inverse system of finite, discrete topological groups. Next, for each \(i \in I\), let \(\pi_i' : G/H \to G'_i\) be the homomorphism induced from \(\pi_i : G \to G_i\). Then \(\pi_i'\) is a homomorphism of topological groups, and furthermore, \((G/H, \{\pi'_i : i \in I\})\) is an inverse limit of \(\{\{G'_i|i \in I\}, \{f_{ij}'|i, j \in I, i \leq j\}\}\).

Furthermore, the quotient map \(G \to G/H\) is the homomorphism induced by the homomorphism \(\{G_i \to G'_i|i \in I\}\) of inverse systems, where the map \(G_i \to G'_i\) is the quotient homomorphism.
Now let $G$ be any profinite group, let $I$ be the set of all open normal subgroups $N$ of $G$. Then $I$ can be made into a partially ordered set by declaring $N_1 \leq N_2$ if and only if $N_2 \subseteq N_1$. For each $N \in I$, let $G_N$ be $G/N$, and for $N_1, N_2 \in I$ with $N_1 \leq N_2$, let $f_{N_1,N_2} : G_{N_2} \to G_{N_1}$ be projection. Then each $G_N$ is a topological group under the quotient topology, and each $f_{N_1,N_2}$ is a homomorphism of topological groups. Furthermore,

\[
\{(G_N | N \in I), \{f_{N_1,N_2} | N_1, N_2 \in I, N_1 \leq N_2\}\}
\]
is an inverse system of topological groups. Also, for each $N \in I$, we let $\pi_N : G \to G_N$ be the quotient map. Then

\[
(G, \{\pi_N : N \in I\})
\]
is an inverse limit of $\{(G_N | N \in I), \{f_{N_1,N_2} | N_1, N_2 \in I, N_1 \leq N_2\}\}$. More briefly, we have that:

\[
G \cong \lim_{\rightarrow} G/N.
\]

One reason for the importance of profinite groups is that all Galois groups are profinite under the Krull topology. More specifically, let $K/k$ be any Galois extension. Let $I$ be the set of all fields $L$ such that $k \subseteq L \subseteq K$ and $L/k$ is finite and Galois, and make $I$ into a partially ordered set by declaring $L_1 \leq L_2$ if and only $L_2 \subseteq L_1$. Next, for each $L \in I$, let $G_L = \text{Gal}(L/k)$ with the Krull topology. For $L_1, L_2 \in I$ with $L_1 \leq L_2$, let $f_{L_1,L_2} : G_{L_1} \to G_{L_2}$ be restriction, i.e. $\sigma \mapsto \sigma|_{L_2}$. For $L \in I$, let $\pi_L : \text{Gal}(K/k) \to G_L$ also be restriction. Then

\[
\{(G_L | L \in I), \{f_{L_1,L_2} | L_1, L_2 \in I, L_1 \leq L_2\}\}
\]
is an inverse system of finite, discrete groups, and $(\text{Gal}(K/k), \{\pi_L | L \in I\})$ is an inverse limit of this inverse system. Briefly,

\[
\text{Gal}(K/k) \cong \lim_{\rightarrow} \text{Gal}(L/k).
\]

In fact, we see that this previous fact is a special case of the isomorphism $G \cong \lim_{\rightarrow} G/N$ once we recall the fundamental theorem of infinite Galois theory. More specifically, open normal subgroups of $\text{Gal}(K/k)$ can be represented uniquely in the form $\text{Gal}(K/L)$, where $L$ is a field such that $k \subseteq L \subseteq K$ and $L/k$ is a finite Galois extension. Furthermore, for such a field $L$, $\text{Gal}(K/k)/\text{Gal}(K/L) \cong \text{Gal}(L/k)$. Not only that, but we have that if $L_1 \leq L_2$ if and only if $\text{Gal}(K/L_1) \leq \text{Gal}(K/L_2)$ as normal subgroups of $\text{Gal}(K/k)$, and if either of these two facts are true, then the following diagram commutes:

\[
\begin{tikzcd}
\text{Gal}(K/k)/\text{Gal}(K/L_1) \ar{r}[swap]{\cong} \ar{d}[swap]{\text{proj}} & \text{Gal}(L_1/k) \ar{d}{\text{incl}} \\
\text{Gal}(K/k)/\text{Gal}(K/L_2) \ar{r}[swap]{\cong} & \text{Gal}(L_2/k).
\end{tikzcd}
\]

Thus, $\text{Gal}(K/k) \cong \lim_{\rightarrow} \text{Gal}(L/k)$ is a special case of $G \cong \lim_{\rightarrow} G/N$, as was claimed.

4. Cohomology of Profinite Groups

This exposition is taken largely from Section I.2 of [NSW].

Let $G$ be any abstract group. By a $G$-module we mean an abelian group $A$ with a function $\cdot : G \times A \to A$ such that for all $g, g_1, g_2 \in G$ and $a, a_1, a_2 \in A$:

\[
g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2 \quad (g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) \quad \text{and} \quad 1 \cdot a = a.
\]

Alternatively, a $G$-module is a group homomorphism $\rho : G \to \text{Aut}(A)$, where $\text{Aut}(A)$ is the group of all group automorphisms of $A$ under composition. These two definitions are equivalent, as if we have $\cdot : G \times A \to A$, then we may define $\rho$ as $g \mapsto g \cdot \_$. Alternatively, if we have the homomorphism $\rho$, then we may define $\cdot : G \times A \to A$, as $g \cdot a = (\rho(g))(a)$.

If $A$ is a $G$-module and $B$ is a subgroup of $A$, then $B$ is a $G$-submodule of $A$ if $g \cdot b \in B$ for all $g \in G$ and $b \in B$. Furthermore, suppose that $H$ is a normal subgroup of $G$ such that for all $h \in H$ and $a \in A$, $h \cdot a = a$. Then $H$ is contained in the kernel of the homomorphism $G \to \text{Aut}(A)$. Thus,
we may descend to a homomorphism $G/H \to \text{Aut}(A)$, so that we have that $A$ is a $G/H$-module under the action $g \cdot a = g \cdot a$.

Now let $G$ be any topological group. By a continuous $G$-module we mean an algebraic $G$-module with the additional property that $\cdot : G \times A \to A$ is continuous when $G$ is given the discrete topology. Alternatively, a continuous $G$-module is a continuous group homomorphism $G \to \text{Aut}(A)$, where $\text{Aut}(A)$ is the discrete group of all group automorphisms of $A$. As for the case when $G$ is an abstract group, these two definitions coincide. Furthermore, the definition of continuous $G$-submodule is the same, and if $H$ is a closed normal subgroup of $G$ such that $H$ acts trivially on $A$, $A$ is a continuous $G/H$-module under the action $g \cdot a = g \cdot a$.

If $A$ and $B$ are both continuous $G$-modules, then a homomorphism of continuous $G$-modules is a group homomorphism $f : A \to B$ that has the additional property that for all $g \in G$ and $a \in A$,

$$g \cdot f(a) = f(g \cdot a).$$

A $G$-module isomorphism is a $G$-module homomorphism that is also an isomorphism of groups. For any fixed topological group $G$, the set of all continuous $G$-modules and $G$-module homomorphisms is a category.

Now suppose that $A$ is a continuous $G$-module. For each $n \geq 0$, let $C^n(G, A)$ denote the set of all continuous maps from $G^n$ to $A$. In particular, since $G^0$ is the trivial group, $C^0(G, A)$ can be identified with $A$. Also define $C^n(G, A)$ to be the trivial group for all $n < 0$. Then for all $n \geq 0$, $C^n(G, A)$ is an abelian group under pointwise addition. To prove this fact, we note that since $A$ is a discrete group, a map $f : G^n \to A$ is continuous if and only if for each $a \in A$, $f^{-1}(\{a\})$ is open in $G^n$. Thus, for any $a \in A$ and functions $f_1, f_2 : G^n \to A$,

$$(f_1 + f_2)^{-1}(\{a\}) = \bigcup_{a \in A} (f_1^{-1}(\{a\}) \cap f_2^{-1}(\{a - a\})),$$

and the set on the right is open if $f_1$ and $f_2$ are continuous. $C^n(G, A)$ is called the group of inhomogeneous $n$-cochains of $G$ with coefficients in $A$.

Now for each $n \geq 0$, let $C^n(G, A)$ be the following subgroup of $C^{n+1}(G, A)$:

$$\{f \in C^{n+1}(G, A) | \forall g, g_0, \ldots, g_n \in G, f(gg_0, \ldots, gg_n) = g \cdot f(g_0, \ldots, g_n).$$

Also let $C^n(G, A)$ be the trivial group for all $n < 0$. $C^n(G, A)$ is called the group of homogeneous $n$-cochains of $G$ with coefficients in $A$.

An interesting and useful fact is that $C^n(G, A) \cong C^n(G, A)$, for all $n \in \mathbb{Z}$. This is obviously true for all $n < 0$. If $n \geq 0$, then let $F^n : C^n(G, A) \to C^n(G, A)$ be defined as $f \mapsto \tilde{f}$, where:

$$\tilde{f}(g_1, \ldots, g_n) = f(1, g_1, g_1g_2, \ldots, g_1 \cdot g_n).$$

In particular, if $f \in C^0(G, A)$, then $\tilde{f} = f(1) \in A = C^0(G, A)$. Let $G^n : C^n(G, A) \to C^n(G, A)$ be defined as $f \mapsto \tilde{f}$, where:

$$\tilde{f}(g_0, g_1, \ldots, g_n) = g_0 \cdot f(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{n-1}^{-1}g_n).$$

In particular, if $f \in C^0(G, A) = A$, then $\tilde{f}(g_0) = g_0 \cdot f$. Then it can be shown that $F$ and $G$ are well-defined and mutually inverse group homomorphisms.

For each $n \in \mathbb{Z}$, we define the map $\partial^n : C^n(G, A) \to C^{n+1}(G, A)$ as follows: If $n \leq -1$, then $\partial^n$ is the zero map. If $n \geq 0$, then for $f \in C^n(G, A)$, we let:

$$(\partial^n f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_n) + \left(\sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \right) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

In particular, if $f \in C^0(G, A) = A$, then

$$(\partial^1 f)(g_1) = g_1 \cdot f - f.$$

If $f \in C^1(G, A)$, then

$$(\partial^2 f)(g_1, g_2) = g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1).$$
In all cases, this is a well-defined homomorphism, called the coboundary homomorphism for inhomogeneous $n$-cochains.

Also, for each $n \in \mathbb{Z}$, we define the map $d^{n+1} : C^n(G, A) \to C^{n+1}(G, A)$ as follows: If $n \leq -1$, then $d^n$ is the zero map. If $n \geq 0$, then for $f \in C^n(G, A)$, we let:

$$(d^{n+1}f)(g_0, \ldots, g_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_{n+1}).$$

Then this is a well-defined homomorphism, called the coboundary homomorphism for homogeneous $n$-cochains.

For each $n \in \mathbb{Z}$, we make the definitions:

$$Z^n(G, A) = \ker(\partial^{n+1}) \quad B^n(G, A) = \operatorname{im}(\partial^n) \quad Z^n(G, A) = \ker(\partial^{n+1}) \quad B^n(G, A) = \operatorname{im}(\partial^n).$$

These four groups are the inhomogeneous $n$-cocycles, the inhomogeneous $n$-coboundaries, the homogeneous $n$-cocycles, and the homogeneous $n$-coboundaries of $G$ with coefficients in $A$, respectively. They have the properties that:

$$Z^n(G, A) \subseteq C^n(G, A) \quad B^n(G, A) \subseteq C^n(G, A) \quad Z^n(G, A) \subseteq C^n(G, A) \quad B^n(G, A) \subseteq C^n(G, A).$$

A routine computation shows that the following square commutes for each $n \in \mathbb{Z}$:

$$
\begin{CD}
C^n(G, A) @>{\partial^{n+1}}>> C^{n+1}(G, A) \\
\downarrow{F^n} @. \downarrow{F^{n+1}} \\
C^n(G, A) @>{\partial^{n+1}}>> C^{n+1}(G, A)
\end{CD}
$$

Therefore, $F^n$ maps $Z^n(G, A)$ isomorphically onto $Z^n(G, A)$ with inverse $G^n$, and $B^n(G, A)$ isomorphically onto $B^n(G, A)$ with inverse $G^n$.

Furthermore, another routine computation shows that $d^{n+1} \circ d^n = 0$ for all $n \in \mathbb{Z}$. Therefore, $B^n(G, A) \subseteq Z^n(G, A)$ for all $n \in \mathbb{Z}$, so it follows that $B^n(G, A) \subseteq Z^n(G, A)$ for all $n \in \mathbb{Z}$. Thus, we may make the following two definitions:

$$H^n(G, A) = Z^n(G, A)/B^n(G, A) \quad \mathcal{H}^n(G, A) = Z^n(G, A)/B^n(G, A).$$

These two groups are called the inhomogeneous and the homogeneous $n$-cohomology of $G$ with cohomology in $A$, respectively. Further, two cocycles that are in the same equivalence class in cohomology are said to be cohomologous. Because $F^n$ maps $Z^n(G, A)$ isomorphically onto $Z^n(G, A)$ and $B^n(G, A)$ isomorphically onto $B^n(G, A)$, we therefore have that $H^n(G, A) \cong \mathcal{H}^n(G, A)$.

Even though these two groups are isomorphic, we will use each group at different times, since each group has its own advantages and disadvantages. The functions in $C^n(G, A)$ take one fewer entry than do the functions in $C^n(G, A)$, so for small values of $n$ it is often easier to work with $H^n(G, A)$ rather than $\mathcal{H}^n(G, A)$. If $n$ is large, then this advantage nearly disappears, and the function $\partial^n$ becomes more complicated than the function $d^n$. Thus, for large values of $n$ it is often more convenient to work with $H^n(G, A)$.

Next, we give a few explicit expressions for functions in inhomogeneous cohomology. If $f \in C^0(G, A) = A$, then $(\partial^1 f)(g_1) = g_1 \cdot f - f$. Thus, $f \in Z^0(G, A)$ if and only if $g_1 \cdot f = f$ for all $g_1 \in G$, i.e. $f \in A^G$. Furthermore, since $C^{-1}(G, A) = \{0\}$, $B^0(G, A) = \{0\}$, so $H^0(G, A) \cong A^G$ as abelian groups.

If $f \in C^1(G, A)$, then $(\partial^2 f)(g_1, g_2) = g_1 \cdot f(g_2) - f(g_1 g_2) + f(g_1)$. Thus, $f \in Z^1(G, A)$ if and only if for all $g_1, g_2 \in G$, $f(g_1 g_2) = g_1 \cdot f(g_2) + f(g_1)$. This is called the 1-cocycle condition. From previous expressions, we have that $f \in B^1(G, A)$ if and only if there is an element $a \in A$ such that $f(g_1) = g_1 \cdot a - a$ for all $g_1 \in G$. This is the 1-coboundary condition.

Furthermore, suppose that the action of $G$ on $A$ is trivial, i.e. $g \cdot a = a$ for all $g \in G$ and $a \in A$. Then the 1-cocycle condition becomes $f(g_1 g_2) = f(g_2) + f(g_1)$. This previous expression in $f(g_1) + f(g_2)$, so $f \in Z^1(G, A)$ if and only if $f : G \to A$ is a homomorphism of topological groups,
\( \text{i.e. } Z^1(G, A) = \text{Hom}_{\text{cont}}(G, A). \) Next, the 1-coboundary condition becomes \( f(g_1) = a - a = 0 \) for all \( g_1 \in G \). Thus, \( B^1(G, A) = \{0\} \), so \( H^1(G, A) \cong Z^1(G, A) = \text{Hom}_{\text{cont}}(G, A) \), if the action of \( G \) on \( A \) is trivial.

Finally, if \( f \in C^2(G, A) \), then
\[
(\partial^3 f)(g_1, g_2, g_3) = g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2).
\]
Thus, \( f \in Z^2(G, A) \) if and only if for all \( g_1, g_2, g_3 \in G \),
\[
f(g_1, g_2) + f(g_1g_2, g_3) = f(g_2, g_3) + f(g_1, g_2g_3).
\]
This is called the 2-cocycle condition. From previous expressions, we have that \( f \in B^2(G, A) \) if and only if there is a function \( a \in C^1(G, A) \) such that
\[
f(g_1, g_2) = g_1 \cdot a(g_2) - a(g_1g_2) + a(g_1)
\]
for all \( g_1, g_2 \in G \). This is called the 2-coboundary condition.

Now, let \( f : A \to B \) be a homomorphism of continuous \( G \)-modules. Then \( f \) induces maps \( f^n : C^n(G, A) \to C^n(G, B) \) and \( f^n : C^n(G, A) \to C^n(G, B) \) as follows: \( f^n \) is the zero map if \( n \leq -1 \). If \( n \geq 0 \), then:
\[
f^n(a) = f \circ a
\]
for \( a \in C^n(G, A) \) and \( a \in C^n(G, A) \). \( f^n \) sends continuous functions to continuous functions; this is because \( A \) is discrete, so \( f : A \to B \) is continuous, and thus if \( a : G^n \to A \) is continuous, then \( f^n(a) = f \circ a \) is continuous. Also, \( f^n \) sends elements of \( C^n(G, A) \) to elements of \( C^n(G, A) \) for the following reason: Let \( g, g_0, \ldots, g_n \in G \) and \( a \in C^n(G, A) \) be arbitrary. Then:
\[
(f^n(a))(gg_0, \ldots, gg_n) = f \circ a(gg_0, \ldots, gg_n) = f(g \cdot a(g_0, \ldots, g_n)) = g \cdot f^n(a)(g_0, \ldots, g_n).
\]
The formulas for \( f^* \) for inhomogeneous and homogeneous cochains agree in the sense that the following square commutes:
\[
\begin{array}{ccc}
C^n(G, A) & \xrightarrow{f^n} & C^n(G, B) \\
\downarrow{F^n} & & \downarrow{F^n} \\
C^n(G, A) & \xrightarrow{f^n} & C^n(G, B).
\end{array}
\]
This is because for any \( a \in C^n(G, A) \),
\[
(f^n \circ F^n(a))(g_1, \ldots, g_n) = (f^n \circ \widetilde{a})(g_1, \ldots, g_n) = f \circ \widetilde{a}(g_1, g_1g_2, \ldots, g_1 \cdots g_n)
\]
\[
= f \circ a(g_1, \ldots, g_n) = f^n(a)(g_1, \ldots, g_n) = (F^n \circ f^n(a))(g_1, \ldots, g_n).
\]
Furthermore, \( f^n \) commutes with \( d^n \) in the sense that the following diagram commutes for each \( n \):
\[
\begin{array}{ccc}
C^{n-1}(G, A) & \xrightarrow{f^{n-1}} & C^{n-1}(G, B) \\
\downarrow{d^n} & & \downarrow{d^n} \\
C^n(G, A) & \xrightarrow{f^n} & C^n(G, B).
\end{array}
\]
This is obvious if \( n \leq -1 \). If \( n \geq 0 \), then the diagram commutes because for any \( a \in C^{n-1}(G, A) \),
\[
(f^n \circ d^n(a))(g_0, \ldots, g_n) = f \circ (d^n(a))(g_0, \ldots, g_n) = f \left( \sum_{i=0}^n (-1)^i a(g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) \right)
\]
\[
= \sum_{i=0}^n (-1)^i (f \circ a)(g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) = (d^n(f \circ a))(g_0, \ldots, g_n)
\]
\[
= (d^n \circ f^{n-1}(a))(g_0, \ldots, g_n).
\]
\[42\]
Because the previous diagram commutes, \( f^n \) maps \( \mathcal{Z}^n(G, A) \) into \( \mathcal{Z}^n(G, B) \) and \( \mathcal{B}^n(G, A) \) into \( \mathcal{B}^n(G, B) \). This means that \( f^n \) descends to a map on cohomology; i.e. from \( \mathcal{H}^n(G, A) \) to \( \mathcal{H}^n(G, B) \). Because \( f^n \) commutes with \( F^n \), \( f^n : C^n(G, A) \to C^n(G, B) \) descends to a map \( f^n : H^n(G, A) \to H^n(G, B) \).

In the sequel we will not be so detailed in our construction of maps on cohomology. We will simply state the formula for homogeneous and inhomogeneous \( n \)-cochains for \( n \geq 0 \), prove that the formulas for homogeneous and inhomogeneous cochains agree, and if need be, prove that the formulas on cochains commute with the coboundary map. The formula on \( n \)-cochains for \( n \leq -1 \) must be the zero map, and this is also enough to prove that the formulas descend to cohomology.

By a short exact sequence of continuous \( G \)-modules, we mean three continuous \( G \)-modules \( A \), \( B \), and \( C \) and \( G \)-module homomorphisms \( f : A \to B \) and \( g : B \to C \) such that the following sequence is exact:

\[
0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.
\]

For any exact sequence of \( G \)-modules, there is an associated **long exact sequence of cohomology** as follows: for each \( n \in \mathbb{Z} \) there are exact sequences of the following form:

\[
\cdots \longrightarrow H^{n-1}(G, C) \xrightarrow{\delta^n} H^n(G, A) \xrightarrow{f^n} H^n(G, B) \xrightarrow{g^n} H^n(G, C) \xrightarrow{\delta^{n+1}} H^{n+1}(G, A) \longrightarrow \cdots
\]

\[
\cdots \longrightarrow \mathcal{H}^{n-1}(G, C) \xrightarrow{\delta^n} \mathcal{H}^n(G, A) \xrightarrow{f^n} \mathcal{H}^n(G, B) \xrightarrow{g^n} \mathcal{H}^n(G, C) \xrightarrow{\delta^{n+1}} \mathcal{H}^{n+1}(G, A) \longrightarrow \cdots
\]

We now define the map \( \delta^{n+1} : H^n(G, C) \to H^{n+1}(G, A) \) and \( \delta^n : \mathcal{H}^n(G, C) \to \mathcal{H}^{n+1}(G, A) \), called the **connecting homomorphism**. If \( n \leq -1 \), then \( \delta^{n+1} \) is the zero map. If \( n \geq 0 \), then \( \delta^{n+1} : H^n(G, C) \to H^{n+1}(G, A) \) is defined as follows: For any \( c \in Z^n(G, C) \), there must be some \( b \in C^n(G, B) \) such that \( g^n(b) = c \). There must then be some \( a \in C^{n-1}(G, A) \) such that \( f^{n+1}(a) = \partial^n(b) \). Such an \( a \) must automatically be an element of \( Z^n(G, A) \). Then define \( \delta^{n+1}(\tau) = \pi \). There are many steps to check here, including the existence of such \( a \)'s and \( b \)'s, that the final cohomology class of \( a \) is independent of the specific choice of \( a \) and \( b \), and that \( \delta^{n+1} \) is a homomorphism. However, these are all routine. Furthermore, the check that this connecting homomorphism makes the long exact sequence in cohomology an exact sequence is also routine.

If \( n \geq 0 \), then \( \delta^{n+1} : \mathcal{H}^n(G, C) \to \mathcal{H}^{n+1}(G, A) \) is defined in exactly the same way: For any \( c \in \mathcal{Z}^n(G, C) \), choose a \( b \in C^n(G, B) \) such that \( g^n(b) = c \), then choose an \( a \in C^{n-1}(G, A) \) such that \( f^{n+1}(a) = d^n(b) \). \( a \) must be in \( Z^1(G, A) \); define \( \delta^{n+1}(\tau) = \pi \).

Furthermore, the formulas for \( \delta^n \) for homogeneous and inhomogeneous cochains agree in the sense that the following square commutes:

\[
\begin{array}{ccc}
\mathcal{H}^{n}(G, C) & \xrightarrow{\delta^n} & \mathcal{H}^{n}(G, A) \\
\mathcal{H}^{n-1}(G, C) & \xrightarrow{\delta^n} & \mathcal{H}^{n}(G, A) \\
\end{array}
\]

\[
\begin{array}{ccc}
F^{-1} & & F^n \\
\downarrow & & \downarrow \\
F^{-1} & & F^n \\
\end{array}
\]

This is because \( F^n \) commutes with both the coboundary maps \( d^n \) and \( \partial^n \) and the induced maps \( f^n \) and \( g^n \).

More specifically, let \( c \in \mathcal{Z}^{n-1}(G, C) \) be arbitrary. Let \( b \in C^{n-1}(G, B) \) be such that \( g^{n-1}(b) = c \), and let \( a \in C^n(G, A) \) be such that \( f^n(a) = d^n(b) \), so that \( \delta^n(\tau) = \pi \), and thus \( F^n \circ \delta^n(\tau) = F^n \circ \tau \). Now, \( F^{-1}(c) \) is an element of \( \mathcal{Z}^{n-1}(G, C) \). Notice that \( F^{-1}(b) \) is an element of \( \mathcal{Z}^{n-1}(G, B) \) such that \( g^{n-1}(F^{-1}(b)) = F^{-1}(c) \), since \( g^{n-1} \circ F^{-1} = F^{-1} \circ g^{n-1} \). Next, note that \( F^n(a) \) is an element of \( C^n(G, A) \) such that \( f^n(F^n(a)) = d^n(F^n(b)) \). This is because \( f^n \circ F^n = F^n \circ f^n \) and \( d^n \circ F^n = F^n \circ d^n \). Therefore, \( F^n(a) \) must be an element of \( Z^n(G, A) \), and therefore:

\[
\delta^n \left( F^{-1}(c) \right) = F^n(a)
\]
Therefore, we have:
\[ \delta^n \circ F^{n-1}(\overline{c}) = F^n(a) = F^n \circ \delta^n(\overline{c}), \]
and the previous diagram commutes, as desired.

In the sequel we will not explicitly prove that certain maps on cohomology commute with the connecting homomorphisms. We will only prove that the maps on cohomology in question commute with the coboundary homomorphism and the induced homomorphisms, and from that state that the map on cohomology commutes with the connecting homomorphism. The proof will be the same as in the previous paragraph.

Now, let \( \{A_i\}_{1 \leq i \leq m} \) be any finite collection of continuous \( G \)-modules. Then the direct sum \( \bigoplus_{i=1}^m A_i \) is a continuous \( G \)-module under the action:
\[ g \cdot (a_i) = (g \cdot a_i). \]
This map obviously makes \( \bigoplus_{i=1}^m A_i \) into an algebraic \( G \)-module. To prove that this action of \( G \) on \( \bigoplus_{i=1}^m A_i \) is continuous, we let \((a_i)_{i=1}^m \in \bigoplus_{i=1}^m A_i \) be arbitrary. For each \( 1 \leq i \leq m \), \( \cdots \cdot \cdot \cdot : G \times A_i \rightarrow A_i \) is continuous, so the inverse image of \( a_i \) under this map is an open set in \( G \times A_i \) and so can be written in the form:
\[ \bigcup_{j \in J_i} (G_{i,j} \times A_{i,j}) \]
for an index set \( J_i \) and open sets \( G_{i,j} \subseteq G \) and \( A_{i,j} \subseteq A_i \). Then the inverse image of \((a_i) \in \bigoplus_{i=1}^m A_i \) under the map \( \cdots \cdot \cdot \cdot : G \times \bigoplus_{i=1}^m A_i \rightarrow \bigoplus_{i=1}^m A_i \) is:
\[ \bigcup_{(i,j) \in \prod_{i=1}^m J_i} \left( \bigcap_{i=1}^m G_{i,j} \times \left( \prod_{i=1}^m A_{i,j} \right) \right), \]
which is open in \( G \times \bigoplus_{i=1}^m A_i \) by definition of the product topology.

Next, for \( n \geq 0 \) we define the homomorphism \( \theta^n : \bigoplus_{i=1}^m C^n(G, A_i) \rightarrow C^n(G, \bigoplus_{i=1}^m A_i) \) as:
\[ \theta^n ((a_1, \ldots, a_m)) (g_1, \ldots, g_n) = (a_1(g_1, \ldots, g_n), \ldots, a_m(g_1, \ldots, g_n)). \]
\( \theta^n \) is well-defined; it sends continuous maps to continuous maps. \( \theta^n \) is also an isomorphism; its inverse is \( a \mapsto (\pi^n_1(a), \ldots, \pi^n_m(a)) \). Furthermore, \( \theta^{n+1} \) maps \( \bigoplus_{i=1}^m C^n(G, A_i) \) isomorphically onto \( C^n(G, \bigoplus_{i=1}^m A_i) \). We therefore also define \( \theta^n : \bigoplus_{i=1}^m C^n(G, A_i) \rightarrow C^{n+1}(G, \bigoplus_{i=1}^m A_i) \) to be the restriction of \( \theta^{n+1} : \bigoplus_{i=1}^m C^n(G, A_i) \rightarrow C^{n+1}(G, \bigoplus_{i=1}^m A_i) \). A routine calculation shows that the following diagram commutes for each \( n \in \mathbb{Z} \):
\[
\begin{array}{ccc}
\bigoplus_{i=1}^m C^n(G, A_i) & \xrightarrow{\theta^n} & C^n(G, \bigoplus_{i=1}^m A_i) \\
\downarrow F^n \times \cdots \times F^n & & \downarrow F^n \\
\bigoplus_{i=1}^m C^n(G, A_i) & \xrightarrow{\theta^n} & C^n(G, \bigoplus_{i=1}^m A_i) .
\end{array}
\]
Therefore, the definitions of \( \theta^n \) on \( \bigoplus_{i=1}^m C^n(G, A_i) \) and on \( \bigoplus_{i=1}^m C^n(G, A_i) \) agree. Another routine computation shows that the following diagram commutes for each \( n \in \mathbb{Z} \):
\[
\begin{array}{ccc}
\bigoplus_{i=1}^m C^{n-1}(G, A_i) & \xrightarrow{\theta^{n-1}} & C^{n-1}(G, \bigoplus_{i=1}^m A_i) \\
\downarrow d^n \times \cdots \times d^n & & \downarrow d^n \\
\bigoplus_{i=1}^m C^{n-1}(G, A_i) & \xrightarrow{\theta^{n-1}} & C^{n-1}(G, \bigoplus_{i=1}^m A_i) .
\end{array}
\]
This means that \( \theta^n \) maps \( \bigoplus_{i=1}^m Z^n(G, A_i) \) isomorphically onto \( Z^n(G, \bigoplus_{i=1}^m A_i) \) and \( \bigoplus_{i=1}^m B^n(G, A_i) \) isomorphically onto \( B^n(G, \bigoplus_{i=1}^m A_i) \), so therefore \( \theta^n \) descends to an isomorphism:
\[
\bigoplus_{i=1}^m H^n(G, A_i) \rightarrow H^n \left( G, \bigoplus_{i=1}^m A_i \right) .
\]
Similarly, \( \theta^n : \bigoplus_{i=1}^n C^n (G, A_i) \to C^n (G, \bigoplus_{i=1}^n A_i) \) descends to an isomorphism:

\[
\bigoplus_{i=1}^m H^n (G, A_i) \to H^n \left( G, \bigoplus_{i=1}^m A_i \right).
\]

5. Inflation, Conjugation, Restriction, Corestriction, and Cup-Product

This exposition is taken largely from Sections I.4 and I.5 of [NSW]. However, most of the proofs were left to the reader, so many of them have been included here.

In this section we define the inflation, conjugation, restriction, and corestriction operations on cohomology. The first three operations are all special cases of a more general construction; we will define this construction now.

Suppose that we have two topological groups \( G_1 \) and \( G_2 \), a continuous \( G_1 \)-module \( A_1 \), a continuous \( G_2 \)-module \( A_2 \), a homomorphism \( \phi : G_2 \to G_1 \) of topological groups, and a group homomorphism \( f : A_1 \to A_2 \) such that for all \( a \in A_2 \) and \( a_1 \in A_1 \),

\[
f (\phi(g_2) \cdot a_1) = g_2 \cdot f(a_1).
\]

Then for each \( n \in \mathbb{Z} \) we have a map \( (f, \phi)^n : C^n (G_1, A_1) \to C^n (G_2, A_2) \); if \( n \geq 0 \), then \((f, \phi)^n\) is the map:

\[
a \mapsto f \circ a \circ (\phi \times \cdots \times \phi)
\]

\((f, \phi)^n\) sends continuous maps to continuous maps, as \( \phi \times \cdots \times \phi \), \( a \), and \( f \) are continuous maps. Furthermore, \((f, \phi)^{n+1}\) sends elements of \( C^n (G_1, A_1) \) to elements of \( C^n (G_2, A_2) \): If \( a \in C^n (G_1, A_1) \), then for any \( g, g_0, \ldots, g_n \in G_2 \),

\[
((f, \phi)^n(a)) (g g_0, \ldots, g g_n) = f \circ a (\phi(g) g_0, \ldots, \phi(g) g_n) = f \circ a (\phi(g) \phi(g_0), \ldots, \phi(g) \phi(g_n))
= f (\phi(g) \cdot a \phi(g_0), \ldots, \phi(g_n))) = g \cdot (f \circ a (\phi(g_0), \ldots, \phi(g_n)))
= g \cdot ((f, \phi)^n(a)) (g_0, \ldots, g_n).
\]

Therefore, we also define \((f, \phi)^n : C^n (G_1, A_1) \to C^n (G_2, A_2) \) to be the restriction of \((f, \phi)^{n+1} : C^n (G_1, A_1) \to C^n (G_2, A_2) \). Next, we have that the following diagram commutes for each \( n \in \mathbb{Z} \):

\[
\begin{array}{ccc}
C^n (G_1, A_1) & \xrightarrow{(f, \phi)^n} & C^n (G_2, A_2) \\
\downarrow \quad \quad \quad \quad F^n & & \quad \quad \quad \quad \quad F^n \\
C^n (G_1, A_1) & \xrightarrow{(f, \phi)^n} & C^n (G_2, A_2) \\
\end{array}
\]

To prove this for \( n \geq 0 \), we let \( a \in C^n (G_1, A_1) \) and \( g_1, \ldots, g_n \in G_2 \) be arbitrary. Then:

\[
((f, \phi)^n \circ F^n(a)) (g_1, \ldots, g_n) = (f \circ F^n(a)) (\phi(g_1), \ldots, \phi(g_n)) = f \circ \hat{a} (\phi(g_1), \ldots, \phi(g_n))
= f \circ a (1, \phi(g_1), \phi(g_1) \phi(g_2), \ldots, \phi(g_1) \cdots \phi(g_n))
= f \circ a (\phi(1), \phi(g_1), \phi(g_1 g_2), \ldots, \phi(g_1 \cdots g_n))
= ((f, \phi)^n(a)) (1, g_1, g_1 g_2, \ldots, g_1 \cdots g_n)
= ((f, \phi)^n(a)) (g_1, \ldots, g_n) = (F^n \circ (f, \phi)^n(a)) (g_1, \ldots, g_n).
\]

Therefore, the maps \((f, \phi)^n\) agree on homogeneous and inhomogeneous cohomology. Next, we have that for each \( n \in \mathbb{Z} \) the following diagram commutes:

\[
\begin{array}{ccc}
C^{n-1} (G_1, A_1) & \xrightarrow{(f, \phi)^{n-1}} & C^{n-1} (G_2, A_2) \\
\downarrow d^n & & \downarrow d^n \\
C^n (G_1, A_1) & \xrightarrow{(f, \phi)^n} & C^n (G_2, A_2) \\
\end{array}
\]

45
To prove this for \( n \geq 1 \), let \( a \in C^{n-1}(G_1, A_1) \) and \( g_0, \ldots, g_n \in G_2 \) be arbitrary. Then:

\[
((f, \phi)^n \circ d^n(a)) (g_0, \ldots, g_n) = (f \circ d^n(a)) (\phi(g_0), \ldots, \phi(g_n))
\]

\[
= f \left( \sum_{i=0}^{n} (-1)^i a (\phi(g_0), \ldots, \phi(g_{i-1}), \phi(g_{i+1}), \ldots, \phi(g_n)) \right)
\]

\[
= \sum_{i=0}^{n} (-1)^i \left( (f \circ a) (\phi(g_0), \ldots, \phi(g_{i-1}), \phi(g_{i+1}), \ldots, \phi(g_n)) \right)
\]

\[
= \sum_{i=0}^{n} (-1)^i \left( (f, \phi)^{n-1}(a) \right) (g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)
\]

\[
= (d^n \circ (f, \phi)^{n-1}(a)) (g_0, \ldots, g_n).
\]

This proves that \((f, \phi)^n\) descends to maps

\[
\mathcal{H}^n(G_1, A_1) \to \mathcal{H}^n(G_2, A_2)
\]

and

\[
H^n(G_1, A_1) \to H^n(G_2, A_2).
\]

Now, suppose in addition that we have a third topological group \( G_3 \), a continuous \( G_3\)-module \( A_3 \), a homomorphism \( \psi : G_3 \to G_2 \) of topological groups, and a group homomorphism \( f : A_2 \to A_3 \) such that for all \( g_3 \in G_3 \) and \( a_2 \in A_2 \),

\[
g(\psi(g_3) \cdot a_2) = g_3 \cdot g(a_2).
\]

Then \( \phi \circ \psi : G_3 \to G_1 \) is a homomorphism of topological groups and \( g \circ f : A_1 \to A_3 \) is a group homomorphism, and furthermore, for all \( g_3 \in G_3 \) and \( a_1 \in A_1 \):

\[
(g \circ f) (\phi \circ \psi)(g_3) \cdot a_1 = g(f(\phi(\psi(g_3))) \cdot a_1) = g(\psi(g_3) \cdot f(a_1)) = g_3 \cdot g(f(a_1))
\]

Thus, we may speak of the homomorphisms:

\[
(g, \psi)^n : C^n(G_2, A_2) \to C^n(G_3, A_3) \quad (g, \psi)^n : C^n(G_2, A_2) \to C^n(G_3, A_3)
\]

\[
(g \circ f, \phi \circ \psi)^n : C^n(G_1, A_1) \to C^n(G_3, A_3) \quad (g \circ f, \phi \circ \psi)^n : C^n(G_1, A_1) \to C^n(G_3, A_3).
\]

Note that for any \( n \geq 0 \) and \( a \in C^n(G_1, A_1) \) or \( a \in C^n(G_1, A_1) \),

\[
(g, \psi)^n \circ (f, \phi)^n(a) = (g, \psi)^n (f \circ a \circ (\phi \times \cdots \times \phi)) = (g \circ f \circ a \circ (\phi \times \cdots \times \phi) \circ (\psi \times \cdots \times \psi)
\]

\[
= (g \circ f) \circ a \circ ((\phi \circ \psi) \times \cdots \times (\phi \circ \psi)) = (g \circ f, \phi \circ \psi)^n(a).
\]

Thus, \((g, \psi)^n \circ (f, \phi)^n = (g \circ f, \phi \circ \psi)^n\) for all \( n \in \mathbb{Z} \) for both homogeneous and inhomogeneous cochains and cohomology.

As was said earlier, the inflation, conjugation, and restriction maps are special cases of the \((f, \phi)^n\) constructions mentioned earlier. To define inflation, we let \( G \) be any topological group and \( H \) any closed normal subgroup of \( G \). Let \( A \) be any continuous \( G \)-module. Then \( A^H \) is a continuous \( G \)-submodule of \( A \) on which \( H \) acts trivially. Thus, \( A^H \) is a \( G/H \) module. Let \( G_1 = G/H, G_2 = G, A_1 = A^H, A_2 = A, \phi : G_2 \to G_1 \) be the quotient map, and \( f : A_1 \to A_2 \) be inclusion. We have that for all \( g \in G_2 = G \) and \( a \in A_1 = A^H \) that:

\[
f(\phi(g_2) \cdot a_1) = \phi(g_2) \cdot a_1 = \overline{g_2} \cdot a_1 = g_2 \cdot a_1 = g_2 \cdot f(a_1).
\]

Then we let the map \( \text{infl}_G^{G/H} \), called inflation, be \((f, \phi)^n\) with any of the following domains and ranges:

\[
C^n(G/H, A^H) \to C^n(G, A) \quad C^n(G/H, A^H) \to C^n(G, A)
\]

\[
H^n(G/H, A^H) \to H^n(G, A) \quad \mathcal{H}^n(G/H, A^H) \to \mathcal{H}^n(G, A).
\]
For \( n \geq 0 \), it sends \( a \in C^n(G/H, A^H) \) to the map:
\[
(g_1, \ldots, g_n) \mapsto a(\overline{g_1}, \ldots, \overline{g_n})
\]
for \( g_1, \ldots, g_n \in G \).

To define **conjugation**, we let \( G \) be any topological group and \( H \) any closed subgroup of \( G \). Let \( A \) be any continuous \( G \)-module. Then \( A \) is automatically a \( H \)-module under the restriction of the action \( G \times A \to A \) to \( H \times A \). Let \( B \) be any \( H \)-submodule of \( A \). Fix any element \( g \in G \). Let \( G_1 = H, G_2 = gHg^{-1}, A_1 = B, A_2 = g \cdot B, \phi : G_2 \to G_1 \) be the map \( g' \mapsto g^{-1}g'g \), and \( f : A_1 \to A_2 \) be \( g \cdot \_ \). \( \phi \) is continuous, for the map \( g' \mapsto g^{-1}g'g \) is a continuous map from \( G \) to \( G \), and restricting the domain to \( gHg^{-1} \) and the range to \( H \) will still give a continuous map. Also, \( A_2 \) is a continuous \( G_2 \)-module under the restriction to \( G \times A \to A \) to \( G_2 \times A_2 \). To prove this, we let \( h \in H \) and \( b \in B \) be arbitrary, so that \( ghg^{-1} \in G_2 = gHg^{-1} \) and \( g \cdot b \in A_2 = g \cdot B \) arbitrary. Then:
\[
(ghg^{-1}) \cdot (g \cdot b) = (ghg^{-1}) \cdot b = (gh) \cdot b = g \cdot (h \cdot b).
\]
As \( h \cdot b \in B, g \cdot (h \cdot b) \in g \cdot B \), so \( A_2 \) is a continuous \( G_2 \)-module, as was claimed.

Next, for all \( ghg^{-1} \in G_2 = G \) (where \( h \in H \)) and \( b \in A_1 = B \) that:
\[
f(\phi(ghg^{-1}) \cdot b) = f((ghg^{-1}) \cdot g \cdot (h \cdot b)) = f(h \cdot b) = g \cdot (h \cdot b) = (gh) \cdot b = (ghg^{-1}) \cdot b
\]
\[
= (ghg^{-1}) \cdot (g \cdot b) = (ghg^{-1}) \cdot f(b).
\]
Then we define \( g^n \), called **conjugation by** \( g \), to be \((f, \phi)^n\) with any of the following domains and ranges:
\[
C^n(H, B) \to C^n(gHg^{-1}, g \cdot B) \quad C^n(H, B) \to C^n((gHg^{-1}, g \cdot B)
\]
\[
H^n(H, B) \to H^n(gHg^{-1}, g \cdot B) \quad \mathcal{H}^n(H, B) \to \mathcal{H}^n(gHg^{-1}, g \cdot B).
\]
For \( n \geq 0 \), \( g^n \) sends \( a \in C^n(H, B) \) to the map:
\[
(g_1, \ldots, g_n) \mapsto g \cdot a(g_1g, \ldots, g^{-1}gng).
\]
for \( g_1, \ldots, g_n \in gHg^{-1} \).

Note also that \( n \geq 0 \) and for \( g_1, g_2 \in G \), we have the three homomorphisms:
\[
(g_2)_n : C^n(H, B) \to C^n(g_2Hg_2^{-1}, g_2 \cdot B)
\]
\[
(g_1) : C^n(g_2Hg_2^{-1}, g_2 \cdot B) \to C^n((g_1g_2)Hg_1g_2, (g_1g_2) \cdot B) \to C^n((g_1, g_2)Hg_1g_2, (g_1, g_2) \cdot B)
\]
\[
(g_1g_2)_n : C^n(H, B) \to C^n((g_1g_2)Hg_1g_2, (g_1g_2) \cdot B)
\]
In this context, \((g_1g_2)^n = (g_1)_n \circ (g_2)_n \). This follows from the general fact that \((g, \psi)^n \circ (f, \phi)^n = (g \circ f, \phi \circ \psi)^n\).

To define **restriction**, we let \( G \) be any topological group and \( H \) any closed normal subgroup of \( G \). Let \( A \) be any continuous \( G \)-module. Then \( A \) is automatically a continuous \( H \)-module. Let \( G_1 = G, G_2 = H, A_1 = A, A_2 = A, \phi : G_2 \to G_1 \) be inclusion, and \( f : A_1 \to A_2 \) the identity map. We have that for all \( h \in G_2 = H \) and \( a \in A_1 = A \) that:
\[
f(\phi(h) \cdot a) = \phi(h) \cdot a = h \cdot a = h \cdot f(a).
\]
Thus we let the function \( \text{res}_H^n \), called “restriction,” be \((f, \phi)^n\) with any of the following domains and ranges:
\[
C^n(G, A) \to C^n(H, A) \quad C^n(G, A) \to C^n(H, A)
\]
\[
H^n(G, A) \to H^n(H, A) \quad \mathcal{H}^n(G, A) \to \mathcal{H}^n(H, A).
\]
For \( n \geq 0 \), restriction sends \( a \in C^n(G, A) \) to \( a|_{H^n} \).

Now we define **corestriction**. To this end, let \( G \) be any profinite group, \( A \) be any continuous \( G \)-module, and \( H \) any open subgroup of \( G \). Then \((G : H)\) is necessarily finite, say it is \( m \), and the right coset space \( H \backslash G = \{Hg|g \in G\} \) is finite. Choose a system \( x_1, \ldots, x_n \) of right coset representatives...
of $H$ in $G$. For any $g \in G$, let $\overline{g}$ denote the element of $\{x_1, \ldots, x_m\}$ that lies in the same right coset as $g$. Then for $n \geq 0$ define the corestriction map:

$$\text{cor}^H_G : C^n(H, A) \to C^n(G, A)$$

as:

$$(\text{cor})(g_0, \ldots, g_n) = \sum_{j=1}^m x_j^{-1} \cdot a \left( x_jg_0x_jy_0^{-1}, \ldots, x_jg_0x_jy_n^{-1} \right).$$

There are many things to check with this definition. First, we prove that for any $1 \leq j \leq m$ and $g \in G$ that $x_jg_0x_jg^{-1} \in H$. To this end, note that there is some $h \in H$ such that $x_jg = hx_jg$, so $x_jg_0x_jg^{-1} = hx_jg_0x_jg^{-1} = h \in H$, as was claimed.

Next we prove that for any $a \in C^n(H, A)$ and $g_0, \ldots, g_n \in G$ that the quantity:

$$\sum_{j=1}^m x_j^{-1} \cdot a \left( x_jg_0x_jy_0^{-1}, \ldots, x_jg_0x_jy_n^{-1} \right)$$

is independent of the choice of representatives $x_1, \ldots, x_n$ of $H \setminus G$. To this end, suppose that $y_1, \ldots, y_n$ is a different set of representatives of $H \setminus G$, so that for each $1 \leq j \leq n$ there is an element $h_j \in H$ such that $y_j = h_jx_j$. Then:

$$\sum_{j=1}^m y_j^{-1} \cdot a \left( y_jg_0y_jy_0^{-1}, \ldots, y_jg_0y_jy_n^{-1} \right) = \sum_{j=1}^m (h_jx_j)^{-1} \cdot a \left( (h_jx_j)g_0h_jx_jy_0^{-1}, \ldots, (h_jx_j)g_nh_jx_jy_n^{-1} \right)$$

$$= \sum_{j=1}^m (x_j^{-1}h_j^{-1}) \cdot a \left( h_jx_jg_0x_jy_0^{-1}, \ldots, h_jx_jg_0x_jy_n^{-1} \right)$$

$$= \sum_{j=1}^m (x_j^{-1}h_j^{-1}) \cdot \left( h_j \cdot a \left( x_jg_0x_jy_0^{-1}, \ldots, x_jg_0x_jy_n^{-1} \right) \right)$$

$$= \sum_{j=1}^m x_j^{-1} \cdot a \left( x_jg_0x_jy_0^{-1}, \ldots, x_jg_0x_jy_n^{-1} \right),$$

as was claimed. Therefore, $\text{cor}$ is a well-defined function.

Next we prove that $\text{cor}$ is continuous. Note that it suffices to prove that for each $1 \leq j \leq m$ that the function:

$$(g_0, \ldots, g_n) \mapsto x_j^{-1} \cdot a \left( x_jg_0x_jy_0^{-1}, \ldots, x_jg_0x_jy_n^{-1} \right)$$

is continuous. As $x_j^{-1} \cdot a : A \to A$ is continuous and $a$ is continuous, to prove this it suffices to show that the function $g \mapsto x_jg_0x_jg^{-1}$ from $G$ to $H$ is continuous. To this end, fix a $g' \in G$. Then the the function $g \mapsto x_jg$ is constant on the set $x_j^{-1}Hg'$. Thus, on the set $x_j^{-1}Hg'$, the function $g \mapsto x_jg_0x_jg^{-1}$ is of the form $g \mapsto g_1gg_2$ for some fixed $g_1, g_2 \in G$ and so is continuous on $x_j^{-1}Hg'$. Now the set:

$$\{x_j^{-1}Hg' : g' \in G\}$$

is a partition of $G$ into a finite number of open subsets. Thus, since $g \mapsto x_jg_0x_jg^{-1}$ is continuous on each element of this partition of $G$ into open sets, this function is continuous on all of $G$, and from earlier remarks $\text{cor}$ is continuous, as was claimed.

Now we prove that $\text{cor}$ is homogeneous. To this end, let $g, g_0, \ldots, g_n$ be arbitrary. Right-multiplication by $g$ permutes the right cosets $H \setminus G$. Thus, there is a permutation $\sigma_g \in S_m$ such that for all $1 \leq j \leq m$, $x_jg = x_{\sigma_g(j)}$. Therefore for each $1 \leq h \leq m$ there is an element $h_j \in H$ such that
\[ x_j g = h_j x_{\sigma(j)}. \] We can now compute that:

\[
\begin{align*}
(cora)(gg_0, \ldots, gg_n) &= \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j gg_0 x_j gg_0^{-1}, \ldots, x_j gg_n x_j gg_n^{-1} \right) \\
&= \sum_{j=1}^{m} x_j^{-1} \cdot a \left( h_j x_{\sigma(j)} g_0 h_j x_{\sigma(j)} g_0^{-1}, \ldots, h_j x_{\sigma(j)} g_n h_j x_{\sigma(j)} g_n^{-1} \right) \\
&= \sum_{j=1}^{m} \left( x_j^{-1} h_j \right) \cdot a \left( x_{\sigma(j)} g_0 x_{\sigma(j)} g_0^{-1}, \ldots, x_{\sigma(j)} g_n x_{\sigma(j)} g_n^{-1} \right) \\
&= \sum_{j=1}^{m} \left( g x_{\sigma(j)}^{-1} \right) \cdot a \left( x_{\sigma(j)} g_0 x_{\sigma(j)} g_0^{-1}, \ldots, x_{\sigma(j)} g_n x_{\sigma(j)} g_n^{-1} \right) \\
&= g \cdot \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j g_0 x_j g_n^{-1}, \ldots, x_j g_n x_j g_n^{-1} \right) = g \cdot (cor)(g_0, \ldots, g_n),
\end{align*}
\]

so that cora is homogeneous, as desired. Thus, cor is well-defined, and it is clearly a homomorphism.

Now we compute the analogous formula for inhomogeneous cochains. To this end, let \( a \in C^n(H,A) \) be arbitrary. Then the analogous formula will be:

\[
\begin{align*}
\widetilde{cor}a(g_1, \ldots, g_n) &= cora(1, g_1, g_1 g_2, \ldots, g_1 \cdots g_n) \\
&= \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j 1 x_j 1^{-1}, x_j g_1 x_j g_1^{-1}, x_j g_1 g_2 x_j g_1 g_2^{-1}, \ldots, x_j g_1 \cdots g_n x_j g_1 \cdots g_n^{-1} \right) \\
&= \sum_{j=1}^{m} (x_j^{-1} x_j 1 x_j 1^{-1}) \cdot a \left( \left( x_j 1 x_j 1^{-1}\right)^{-1} \left( x_j g_1 x_j g_1^{-1}\right), \left( x_j g_1 x_j g_1^{-1}\right)^{-1} \left( x_j g_1 g_2 x_j g_1 g_2^{-1}\right), \ldots, \left( x_j g_1 \cdots g_n x_j g_1 \cdots g_n^{-1}\right)^{-1} \left( x_j g_1 \cdots g_n x_j g_1 \cdots g_n^{-1}\right) \right) \\
&= \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j 1 x_j 1^{-1} x_j g_1 x_j g_1^{-1}, \ldots, x_j g_1 \cdots g_n x_j g_1 \cdots g_n^{-1} \right) \\
&= \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j g_1 x_j g_1^{-1}, \ldots, x_j g_1 \cdots g_n x_j g_1 \cdots g_n^{-1} \right).
\end{align*}
\]

Therefore, for \( n \geq 0 \) we define \( cor : C^n(H,A) \to C^n(G,A) \) according to the previous formula.

Next we prove that cor commutes with the coboundary map, more specifically that the following diagram commutes:

\[
\begin{array}{ccc}
C^{n-1}(H,A) & \xrightarrow{cor} & C^{n-1}(G,A) \\
\downarrow{d^n} & & \downarrow{d^n} \\
C^n(H,A) & \xrightarrow{cor} & C^n(G,A)
\end{array}
\]

49
To prove this for \( n \geq 1 \), we let \( a \in C^{n-1}(H, A) \) and \( g_0, \ldots, g_n \in G \) be arbitrary. Then:

\[
(\text{cor} \circ d^n(a))(g_0, \ldots, g_n) = \sum_{j=1}^{m} x_j^{-1} \cdot (d^n(a)) \left( x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1} \right)
\]

\[
= \sum_{j=1}^{m} \left( x_j^{-1} \cdot \sum_{i=0}^{n} (-1)^i a \left( x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_i x_j^{-1} g_i^{-1}, x_j g_{i+1} x_j^{-1} g_{i+1}^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1} \right) \right)
\]

\[
= \sum_{i=0}^{n} \left( (-1)^i \sum_{j=1}^{m} x_j^{-1} \cdot a \left( x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_i x_j^{-1} g_i^{-1}, x_j g_{i+1} x_j^{-1} g_{i+1}^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1} \right) \right)
\]

\[
= \sum_{i=0}^{n} (-1)^i \left( (\text{cor}a)(g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) \right) = (d^n \circ \text{cor})(g_0, \ldots, g_n),
\]

as desired. This allows us to conclude that cor descends to an operation on \( \mathcal{H}^n(G, A) \) and \( H^n(G, A) \).

Now we prove that inflation and corestriction are functorial.

More specifically, let \( G \) be any topological group and \( H \) any closed normal subgroup of \( G \). Let \( A \) and \( B \) be any continuous \( G \)-modules and \( f : A \to B \) be a homomorphism of continuous \( G \)-modules. Then \( A^H \) and \( B^H \) are both \( G/H \)-modules. Furthermore, \( f \) is a \( G/H \)-module homomorphism of \( A^H \) into \( B^H \). \( f \) carries \( A^H \) into \( B^H \) for the following reason: Let \( h \in H \) and \( a \in A^H \) be arbitrary. Then \( h \cdot f(a) = f(h \cdot a) = f(a) \). \( f \) is a \( G/H \)-module homomorphism, as for any \( a \in A^H \) and \( g \in G \), so that \( g \in G/H \) is arbitrary, we have:

\[
f(g \cdot a) = f(g \cdot a) = g \cdot f(a) = g \cdot f(a).
\]

Therefore, we may write down the following diagram:

\[
\begin{array}{ccc}
C^n(G/H, A^H) & \xrightarrow{\text{infl}} & C^n(G, A) \\
\downarrow f^n & & \downarrow f^n \\
C^n(G/H, B^H) & \xrightarrow{\text{infl}} & C^n(G, B).
\end{array}
\]

To say that inflation is functorial means that the previous diagram commutes. To prove this, we let \( a \in C^n(G/H, A^H) \) be arbitrary and fix arbitrary \( g_0, \ldots, g_n \in G \). Then:

\[
(\text{infl} \circ f^n(a))(g_0, \ldots, g_n) = (\text{infl} \circ f \circ a)(g_0, \ldots, g_n) = f \circ a(g_0, \ldots, g_n) = (f \circ \text{infl}(a))(g_0, \ldots, g_n) = (f^n \circ \text{infl}(a))(g_0, \ldots, g_n).
\]

Thus, inflation is functorial, as was claimed. Furthermore, since inflation and \( f^n \) both commute with the maps \( F^n \) and \( G^n \), the following diagram also commutes:

\[
\begin{array}{ccc}
C^n(G/H, A^H) & \xrightarrow{\text{infl}} & C^n(G, A) \\
\downarrow f^n & & \downarrow f^n \\
C^n(G/H, B^H) & \xrightarrow{\text{infl}} & C^n(G, B).
\end{array}
\]

Furthermore, the respective diagrams for homogeneous and inhomogeneous cohomology also commute.

Now let \( G \) be any profinite group and \( H \) any open normal subgroup of \( G \). Let \( A \) and \( B \) be any continuous \( G \)-modules and \( f : A \to B \) be a homomorphism of continuous \( G \)-modules. Then \( A \) and \( B \) are automatically continuous \( H \)-modules and \( f \) is automatically a homomorphism of continuous
$H$-modules. Therefore, we may form down the following diagram for each $n \in \mathbb{Z}$:

\[
\begin{array}{ccc}
\mathcal{C}^n (H, A) & \xrightarrow{\text{cor}} & \mathcal{C}^n (G, A) \\
\downarrow{f^n} & & \downarrow{f^n} \\
\mathcal{C}^n (H, B) & \xrightarrow{\text{cor}} & \mathcal{C}^n (G, B).
\end{array}
\]

To say that corestriction is functorial means that the previous diagram commutes. To prove this for $n \geq 0$, we let $a \in \mathcal{C}^n (H, A)$ be arbitrary and fix arbitrary $g_0, \ldots, g_n \in G$. Then:

\[
\begin{align*}
\left( \text{cor} \circ f^n (a) \right) (g_0, \ldots, g_n) &= \sum_{j=1}^{m} x_j^{-1} \cdot (f^n (a)) (x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1}) \\
&= \sum_{j=1}^{m} x_j^{-1} \cdot \left( (f \circ a) (x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1}) \right) \\
&= f \left( \sum_{j=1}^{m} x_j^{-1} \cdot a (x_j g_0 x_j^{-1} g_0^{-1}, \ldots, x_j g_n x_j^{-1} g_n^{-1}) \right) \\
&= \left( f \circ (\text{cor} a) \right) (g_0, \ldots, g_n) = \left( f^n \circ \text{cor} (a) \right) (g_0, \ldots, g_n).
\end{align*}
\]

Thus, corestriction is functorial, as was claimed. Furthermore, since corestriction and $f^n$ both commute with the maps $F^n$ and $G^n$, the respective diagrams for inhomogeneous cocycles and homogeneous and inhomogeneous cohomology also commute.

Next, we show that inflation and corestriction commutes with the connecting homomorphism.

More specifically, suppose that $G$ is any topological group and $H$ is any closed normal subgroup of $G$. Let $A$, $B$, and $C$ be any continuous $G$-modules such that there is the following short exact sequence of continuous $G$-modules:

\[
\begin{array}{ccc}
0 & \longrightarrow & A \\
\downarrow{f} & & \downarrow{g} \\
B & \longrightarrow & C \\
\downarrow{0} & & \downarrow{0} \\
0 & \longrightarrow & 0.
\end{array}
\]

Then $A^H$, $B^H$, and $C^H$ are automatically continuous $G/H$-modules, $f$ is automatically a $G/H$-module homomorphism of $A^H$ into $B^H$, and $g$ is automatically a $G/H$-module homomorphism of $B^H$ into $C^H$. It is not true in general that the sequence:

\[
\begin{array}{ccc}
0 & \longrightarrow & A^H \\
\downarrow{f} & & \downarrow{g} \\
B^H & \longrightarrow & C^H \\
\downarrow{0} & & \downarrow{0} \\
0 & \longrightarrow & 0.
\end{array}
\]

is an exact sequence of $G/H$-modules. However, if it is, then we can form the following diagram for each $n \in \mathbb{Z}$:

\[
\begin{array}{ccc}
\mathcal{H}^{n-1} (G/H, C^H) & \xrightarrow{\text{inf}} & \mathcal{H}^{n-1} (G, C) \\
\downarrow{\delta^n} & & \downarrow{\delta^n} \\
\mathcal{H}^n (G/H, A^H) & \xrightarrow{\text{inf}} & \mathcal{H}^n (G, A).
\end{array}
\]

This diagram commutes; this is an immediate consequence of the fact that inflation commutes with the coboundary homomorphism and is functorial. For similar reasons, the respective diagram for inhomogeneous cohomology also commutes.

Now suppose that $G$ is any profinite group and $H$ is open subgroup of $G$. Let $A$, $B$, and $C$ be any continuous $G$-modules such that there is the following short exact sequence of continuous $G$-modules:

\[
\begin{array}{ccc}
0 & \longrightarrow & A \\
\downarrow{f} & & \downarrow{g} \\
B & \longrightarrow & C \\
\downarrow{0} & & \downarrow{0} \\
0 & \longrightarrow & 0.
\end{array}
\]
Then the previous sequence is automatically a short exact sequence of continuous $H$-modules, so we can form the following diagram for each $n \in \mathbb{Z}$:

$$
\begin{array}{ccc}
\mathcal{H}^{n-1}(H, C) & \xrightarrow{\text{inf}} & \mathcal{H}^{n-1}(G, C) \\
\downarrow{\delta^n} & & \downarrow{\delta^n} \\
\mathcal{H}^n(H, A) & \xrightarrow{\text{inf}} & \mathcal{H}^n(G, A). \\
\end{array}
$$

This diagram commutes; this is an immediate consequence of the fact that corestriction commutes with the coboundary homomorphism and is functorial. For similar reasons, the respective diagram for inhomogeneous cohomology also commutes.

Let $G$ be a topological group and $A$ and $B$ be continuous $G$-modules. Then $A \otimes_Z B$ is automatically a continuous $G$-module under the action defined on pure tensors as:

$$
g \cdot (a \otimes b) = (g \cdot a) \otimes (g \cdot b)
$$

for $a \in A$, $b \in B$, and $g \in G$. Now we fix integer $p$ and $q$ and define a bilinear map

$$
_a \cup_b : C^p(G, A) \times C^q(G, B) \to C^{p+q}(G, A \otimes_Z B)
$$

to be 0 if either $p$ or $q$ is negative and as:

$$
(a \cup b)(g_0, \ldots, g_{p+q}) = a(g_0, \ldots, g_p) \otimes a(g_p, \ldots, g_{p+q})
$$

if $p$ and $q$ are both nonnegative. This is well-defined in the sense that $a \cup b$ is continuous and homogeneous if $a$ and $b$ are. We call the function $_a \cup_b$ the cup-product.

A straightforward computation shows that:

$$
d^{p+q+1}(a \cup b) = (d^{p+1}a) \cup b + (-1)^p(a \cup (d^q+1)b)
$$

for all $a \in C^p(G, A)$ and $C^q(G, B)$. This implies that if $a$ and $b$ are both cocycles, then $a \cup b$ is a cocycle, and also that if one of $a$ and $b$ is a coboundary while the other is a cocycle, then $a \cup b$ is a coboundary. This is enough to conclude that the cup-product descends to a bilinear map:

$$
_a \cup_b : \mathcal{H}^p(G, A) \times \mathcal{H}^q(G, B) \to \mathcal{H}^{p+q}(G, A \otimes_Z B)
$$

on cohomology.

Next we find what the analogous operation on inhomogeneous cochains is. To this end we let $a \in C^p(G, A)$ and $b \in C^p(G, B)$ be arbitrary. Then the analogous formula is:

$$
\begin{array}{c}
\tilde{a} \cup \tilde{b}(g_1, g_2, \ldots, g_{p+q}) = (\tilde{a} \cup \tilde{b})(1, g_1, g_1g_2, \ldots, g_1 \cdots g_{p+q}) \\
= \tilde{a}(1, g_1g_2, \ldots, g_1 \cdots g_p) \otimes \tilde{b}(g_1, \ldots, g_{p+1}) = (1 \cdot a \left(1^{-1}g_1, g_1^{-1}(g_1g_2), \ldots, (g_1 \cdots g_{p-1})^{-1}(g_1 \cdots g_p)\right) \otimes \\
\left((g_1 \cdots g_p) \cdot b((g_1 \cdots g_p)^{-1}(g_1 \cdots g_{p+1}), \ldots, (g_1 \cdots g_{p+q-1})^{-1}(g_1 \cdots g_{p+q}))\right) = a(g_1, \ldots, g_p) \otimes (g_1 \cdots g_p) \cdot b(g_{p+1}, \ldots, g_{p+q}).
\end{array}
$$

Therefore, the definition of cup-product we will use for inhomogeneous cochains is:

$$
(a \cup b)(g_1, g_2, \ldots, g_{p+q}) = a(g_1, \ldots, g_p) \otimes ((g_1 \cdots g_p) \cdot b(g_{p+1}, \ldots, g_{p+q})).
$$

Just as for homogeneous cochains, this operation also descends to cohomology.

Finally, we state one other result. Suppose that $a \in \mathcal{H}^p(G, A)$ and $b \in \mathcal{H}^q(G, A)$. Then $a \cup b = (-1)^{pq}(b \cup a)$ as elements of $\mathcal{H}^{p+q}(G, A \otimes_Z A)$. This is proved as part of Proposition 1.4.4 of [NSW].
6. Direct Limits

This exposition is taken largely from Section IV.2 of [Ne]. This exposition is also very similar to the exposition on inverse limits; conceptually speaking the setup of a direct system and a direct limit is precisely the setup of an inverse system and an inverse limit with every function going in the opposite direction.

Let $\mathcal{I}$ be a directed set, in other words a set with a reflexive and transitive relation $\leq$ with the additional property that for each $i, j \in \mathcal{I}$ there is a $k \in \mathcal{I}$ such that $i \leq k$ and $j \leq k$. Next, let $\{G_i|i \in \mathcal{I}\}$ be a collection of abstract (not necessarily topological!) groups indexed by $\mathcal{I}$. Suppose that for all $i, j \in \mathcal{I}$ with $i \leq j$ there is a group homomorphism $f_{ij} : G_i \to G_j$ such that $f_{ii} = \text{Id}_{G_i}$ and for all $i, j, k \in \mathcal{I}$ with $i \leq j \leq k$, we have $f_{ik} = f_{jk} \circ f_{ij}$. Then the collection $\{(G_i|i \in \mathcal{I}), \{f_{ij}|i, j \in \mathcal{I}, i \leq j\}\}$ is called a direct system of groups.

A group $G$ and set of group homomorphisms $\{\iota_i : G_i \to G|i \in \mathcal{I}\}$ is called a direct limit or an inductive limit of the direct system $\{(G_i|i \in \mathcal{I}), \{f_{ij}|i, j \in \mathcal{I}, i \leq j\}\}$ if:

1. For all $i, j \in \mathcal{I}$ with $i \leq j$, $\iota_i = \iota_j \circ f_{ij}$.
2. For any group $G'$ and set of group homomorphisms $\{\iota_i' : G_i \to G'|i \in \mathcal{I}\}$ such that for all $i, j \in \mathcal{I}$ with $i \leq j$, $\iota_i' = \iota_j' \circ f_{ij}$, there is a unique group homomorphism $g : G \to G'$ such that for all $i \in \mathcal{I}$ we have $g \circ \iota_i = \iota_i'$, in other words there is a unique group homomorphism $g : G \to G'$ such that for all $i, j \in \mathcal{I}$ with $i \leq j$ the following diagram commutes:

   \[ \begin{array}{ccc}
   G_i & \xrightarrow{f_{ij}} & G_j \\
   \iota_i \downarrow & & \iota_j \downarrow \\
   G & \xrightarrow{g} & G'.
   \end{array} \]

By this definition, direct limits are unique up to isomorphism. In other words, if $(G, \{\iota_i|i \in \mathcal{I}\})$ and $(G', \{\iota_i'|i \in \mathcal{I}\})$ are both direct limits of the direct system $\{(G_i,f_{ij}|i, j \in \mathcal{I}, i \leq j\}$, then there is an isomorphism $g : G \to G'$ of topological groups such that for all $i \in \mathcal{I}$ we have $g \circ \iota_i = \iota_i'$.

Now let $\left(\{\tilde{G}_i|i \in \mathcal{I}\}, \{\tilde{f}_{ij}|i, j \in \mathcal{I}, i \leq j\}\right)$ and $\left(\{G_i|i \in \mathcal{I}\}, \{f_{ij}|i, j \in \mathcal{I}, i \leq j\}\right)$ be any two direct systems of groups indexed by the same set $\mathcal{I}$. A homomorphism of direct systems of topological groups is any set $\{h_i : G_i \to \tilde{G}_i|i \in \mathcal{I}\}$ of homomorphisms of groups such that for all $i, j \in \mathcal{I}$ with $i \leq j$, the following square commutes:

\[ \begin{array}{ccc}
G_i & \xrightarrow{f_{ij}} & G_j \\
\tilde{h}_i \downarrow & & \tilde{h}_j \downarrow \\
\tilde{G}_i & \xrightarrow{\tilde{f}_{ij}} & \tilde{G}_j.
\end{array} \]

Now suppose that $\{\tilde{G}_i, \tilde{f}_{ij}|i, j \in \mathcal{I}, i \leq j\}$ has a direct limit $\left(\tilde{G}, \{\tilde{i}_i|i \in \mathcal{I}\}\right)$ and $\{G_i, f_{ij}|i, j \in \mathcal{I}, i \leq j\}$ has a direct limit $\left(\hat{G}, \{\hat{i}_i|i \in \mathcal{I}\}\right)$. Then there is a unique homomorphism $h : G \to \hat{G}$ such that for all $i \in \mathcal{I}$, the following square commutes:

\[ \begin{array}{ccc}
G & \xrightarrow{\hat{i}_i} & \hat{G}_i \\
\downarrow h & & \downarrow \hat{h}_i \\
\hat{G} & \xrightarrow{\hat{i}} & \hat{G}.
\end{array} \]
This is because if we define \( t'_i : G_i \to \tilde{G} \) to be \( \iota_i \circ h_i \) for each \( i \in \mathcal{I} \), then for all \( i, j \in \mathcal{I} \) we have \( t'_i = t'_j \circ f_{ij} \), and by condition (2) of direct limit, there must be a there is a unique homomorphism of topological groups \( h : G \to \tilde{G} \) such that for all \( i \in \mathcal{I} \) we have \( h \circ t_i = t'_i \). This homomorphism \( h \) is called the homomorphism induced by the homomorphism \( \{ h_i | i \in \mathcal{I} \} \) of direct systems. Furthermore, if each \( h_i \) is an isomorphism, then \( h \) is also an isomorphism.

As should be clear, this definition of direct system, direct limit, homomorphism of direct systems, and homomorphism of direct limits induced by a homomorphism of direct system can be applied to any category, not just for groups. However, within this paper we will only use these constructions for groups.

It happens that any direct system of groups has a direct limit. More specifically, let

\[
\{ G_i | i \in \mathcal{I} \}, \{ f_{ij} | i, j \in \mathcal{I}, i \leq j \}
\]

be a direct system of groups. Let \( \mathcal{C} \) be the disjoint union of the sets \( G_i \); i.e.:

\[
\mathcal{C} = \left\{ (g, i) \in \left( \bigcup_{i \in \mathcal{I}} G_i \right) \times \mathcal{I} | g \in G_i \right\}.
\]

We define the relation \( \sim \) on \( \mathcal{C} \) to be that \( (g_i, i) \sim (g_j, j) \) if and only if there is a \( k \in \mathcal{I} \) such that \( i \leq k, j \leq k \), and \( f_{ik}(g_i) = f_{jk}(g_j) \). It can be shown that \( \sim \) is an equivalence relation. Let \( G \) be the set of equivalence classes \( \mathcal{C}/\sim \) under this relation.

Next, define a binary operation on \( G \) as follows: Suppose that \( g_1, g_2 \in G \) are represented by \( (g_i, i) \) and \( (g_j, j) \), respectively. Let \( k \in \mathcal{I} \) be any element such that \( i \leq k \) and \( j \leq k \); such a \( k \) is guaranteed to exist because \( \mathcal{I} \) is a directed set. Then define \( a \cdot b \in G \) to be the class of \( (f_{ik}(g_i)f_{jk}(g_j), k) \) in \( G \). It can be shown that this operation is well-defined and makes \( G \) into a group. Next, for each \( i \in \mathcal{I} \) let \( \iota_i : G_i \to G \) be the function that sends \( g_i \) to the class of \( (g_i, i) \) in \( G \). It can be shown that \( \iota_i \) is a group homomorphism, and furthermore,

\[
(G, \{ \iota_i | i \in \mathcal{I} \})
\]

is a direct limit of

\[
\{ G_i | i \in \mathcal{I} \}, \{ f_{ij} | i, j \in \mathcal{I}, i \leq j \}.
\]

We will denote this direct limit as \( \lim_{\longrightarrow} G_i \), provided it is obvious what the set \( \mathcal{I} \) and the maps \( f_{ij} \) are.

Furthermore, we have a simple description of the homomorphism \( h : \lim_{\longrightarrow} G_i \to \lim_{\longrightarrow} \tilde{G}_i \) induced by the homomorphism \( \{ h_i : G_i \to \tilde{G}_i \} \) of directed systems. Specifically, the class of \( (g_i, i) \) in \( \lim_{\longrightarrow} G_i \) is mapped to the class of \( (h_i(g_i), i) \) in \( \lim_{\longrightarrow} \tilde{G}_i \). Of course, one needs to show that this map is well-defined and a homomorphism.

Although we will introduce other examples of directed systems later, we will give one example right now. This example is roughly the statement of Proposition 1.2.6 of [NSW]. Let \( G \) be a profinite group and \( A \) be any continuous \( G \)-module. Let \( \mathcal{I} \) be the set of all open normal subgroups of \( G \). For each \( N \in \mathcal{I} \), let \( G_N \) be the group \( H^n(G/N, A^N) \) arising from the statement of the inflation map. For \( N, K \in \mathcal{I} \), say that \( N \leq K \) if and only if \( K \subseteq N \). Then \( \mathcal{I} \) is a directed system: if \( N, K \in \mathcal{I} \), then \( N \cap K \in \mathcal{I} \) and \( N \leq N \cap K \) and \( K \leq N \cap K \). Next, for \( N, K \in \mathcal{I} \) with \( N \leq K \), let \( f_{NK} : G_N \to G_K \) be the homomorphism:

\[
(f, \phi)^n : H^n(G/N, A^N) \to H^n(G/K, A^K),
\]

where \( f : A^N \to A^K \) is inclusion and \( \phi : G/K \to G/N \) is projection. Then

\[
\{ G_N | N \in \mathcal{I} \}, \{ f_{NK} | N, K \in \mathcal{I}, N \leq K \}
\]

can be shown to be a direct system. Now, for each \( N \in \mathcal{I} \), let \( \iota_N : G_N \to H^n(G, A) \) be \( \inf_{G/N}^G \). Then \( (H^n(G, A), \{ \iota_N : N \in \mathcal{I} \}) \) is a direct limit of

\[
\{ G_N | N \in \mathcal{I} \}, \{ f_{NK} | N, K \in \mathcal{I}, N \leq K \}.
\]
More briefly, \[ \mathcal{H}^n(G, A) \cong \lim_{\to} \mathcal{H}^n(G/N, A^N). \]

In particular, since \( G/N \) is a finite group for each \( N \in \mathcal{I} \), \( \mathcal{H}^n(G, A) \) can always be written as a direct limit of cohomology of finite groups.

It can be proved in a similar way that:
\[ H^n(G, A) \cong \lim_{\to} H^n(G/N, A^N). \]

In fact, for each \( N \in \mathcal{I} \), we have an isomorphism \( F_N^n : \mathcal{H}^n(G/N, A^N) \to H^n(G/N, A^N) \). It can be shown that the isomorphisms \( \{ F_N^n \}_{N \in \mathcal{I}} \) are a homomorphism from the directed system
\[ (\{ \mathcal{H}^n(G/K, A^K) \}_{N \in \mathcal{I}}, \{ f_{NK} \}_{N \in \mathcal{I}, K \in \mathcal{I}, N \leq K}) \]
to the directed system
\[ (\{ H^n(G/K, A^K) \}_{N \in \mathcal{I}}, \{ f_{NK} \}_{N \in \mathcal{I}, K \in \mathcal{I}, N \leq K}) , \]
and that the induced isomorphism from \( \mathcal{H}^n(G, A) \) to \( H^n(G, A) \) is \( F^n \).

As a special case of the previous construction, we examine what happens when \( G \) is the Galois group of a Galois extension \( K/k \). By the fundamental theorem of infinite Galois theory, the open normal subgroups of \( G \) are in one-to-one correspondence with intermediate fields \( K/L/k \) such that \( L/k \) is a finite Galois extension. Thus in this case, we may take \( \mathcal{I} \) to be the set of all such intermediate fields \( L \), with the ordering that \( L_1 \leq L_2 \) if and only if \( L_1 \subseteq L_2 \). Note that \( L_1 \leq L_2 \) if and only if \( \text{Gal}(K/L_2) \subseteq \text{Gal}(K/L_1) \). Thus, we may take \( G_L \) to be
\[ \mathcal{H}^n(G/\text{Gal}(K/L), A^{\text{Gal}(K/L)}) \cong \mathcal{H}^n(\text{Gal}(L/k), A^{\text{Gal}(K/L)}), \]
\( \iota_L : G_L \to \mathcal{H}^n(G, A) \) to be inflation, and for \( L_1, L_2 \in \mathcal{I} \) with \( L_1 \leq L_2 \), we may take \( f_{L_1L_2} : G_{L_1} \to G_{L_2} \) to be the map:
\[ \mathcal{H}^n(G/\text{Gal}(K/L_1), A^{\text{Gal}(K/L_1)}) \to \mathcal{H}^n(G/\text{Gal}(K/L_2), A^{\text{Gal}(K/L_2)}). \]

Thus, \( (\mathcal{H}^n(G, A), \{ \iota_L : L \in \mathcal{I} \}) \) is a direct limit of
\[ (\{ G_L \}_{L \in \mathcal{I}}, \{ f_{L_1L_2} \}_{L_1, L_2 \in \mathcal{I}, L_1 \leq L_2}). \]

More briefly,
\[ \mathcal{H}^n(G, A) \cong \lim_{\to} \mathcal{H}^n(\text{Gal}(L/k), A^{\text{Gal}(K/L)}). \]

A similar statement holds for cohomology with inhomogeneous cochains.

It is true that each of the operations inflation, conjugation, restriction, corestriction, and cup-product for the cohomology of profinite groups are extensions of these respective operations on directed sets of cohomology of finite groups. As an example, we will precisely state what this means for the cup-product. Let \( G \) be a profinite group, \( A \) and \( B \) be continuous \( G \)-modules, and
\[ (\{ \mathcal{H}^{p+q}(G/N, (A \otimes_Z B)^N) \}_{N \in \mathcal{I}}, \{ f_{NK} \}_{N \in \mathcal{I}, K \in \mathcal{I}, N \leq K}) \]
the directed system given above. Then:
\[ (\{ \mathcal{H}^p(G/N, A^N) \times \mathcal{H}^q(G/N, B^N) \}_{N \in \mathcal{I}}, \{ f_{NK} \times f_{NK} \}_{N \in \mathcal{I}, K \in \mathcal{I}, N \leq K}) \]
is also a direct system, and for each \( N \in \mathcal{I} \), we have the composition:
\[ \mathcal{H}^p(G/N, A^N) \times \mathcal{H}^q(G/N, B^N) \to \mathcal{H}^{p+q}(G/N, A^N \otimes_Z B^N) \to \mathcal{H}^{p+q}(G/N, (A \otimes_Z B)^N). \]
of the cup-product, followed by the map induced by the inclusion \( A^N \otimes_Z B^N \to (A \otimes_Z B)^N \). Then the following diagram commutes:
\[
\begin{array}{ccc}
\mathcal{H}^p(G/N, A^N) \times \mathcal{H}^q(G/N, B^N) & \xrightarrow{i_i} & \mathcal{H}^{p+q}(G/N, (A \otimes_Z B)^N) \\
\downarrow h & & \downarrow h_i \\
\bar{G} & \xrightarrow{i_i} & \bar{G}_i.
\end{array}
\]
7. Shapiro’s Lemma

This exposition is taken largely from Section 1.6 of [NSW].

Shapiro’s lemma is a very useful result in the cohomology of profinite groups. To state it, we need some notation: Let \( G \) be any profinite group, \( H \) any closed subgroup of \( G \), and \( A \) any continuous \( G \)-module. We define \( \text{Ind}_{G}^{H}(A) \) to be the set of all continuous functions \( x : G \to A \) such that for all \( g \in G \) and \( h \in H \),

\[
x(hg) = h \cdot x(g).
\]

\( \text{Ind}_{G}^{H}(A) \) is a group under addition of functions. Furthermore, \( \text{Ind}_{G}^{H}(A) \) is a continuous \( G \)-module under the action:

\[
(g_{1} \cdot x)(g_{2}) = x(g_{2}g_{1})
\]

for \( x \in \text{Ind}_{G}^{H}(A) \) and \( g_{1}, g_{2} \in G \).

Let \( G/H \) denote the left coset space \( \{gH | g \in G \} \) of \( H \) in \( G \) with the quotient topology and \( \text{Map}_{\text{cont}}(G/H, A) \) denote the set of all continuous maps from \( G/H \) to \( A \). Then \( \text{Map}_{\text{cont}}(G/H, A) \) is a continuous \( G \)-module under the action,

\[
(g_{1} \cdot y)(g_{2}H) = g_{1} \cdot \left(y(g_{1}^{-1}g_{2}H)\right),
\]

and the map that sends \( x \in \text{Ind}_{G}^{H}(A) \) to the map \( y : gH \mapsto g \cdot (x(g^{-1})) \) is a well-defined isomorphism of \( G \)-modules from \( \text{Ind}_{G}^{H}(A) \) to \( \text{Map}_{\text{cont}}(G/H, A) \). The inverse of this isomorphism is the map that sends \( y \in \text{Map}_{\text{cont}}(G/H, A) \) to \( x : g \mapsto g \cdot y(g^{-1}H) \). Therefore,

\[
\text{Ind}_{G}^{H}(A) \cong \text{Map}_{\text{cont}}(G/H, A).
\]

There is a canonical projection \( \pi : \text{Ind}_{G}^{H}(A) \to A \) that sends \( x \) to \( x(1) \). The corresponding canonical projection \( \pi : \text{Map}_{\text{cont}}(G/H, A) \to A \), i.e. the function that makes the following diagram commute:

\[
\begin{array}{ccc}
\text{Ind}_{G}^{H}(A) & \xrightarrow{x \mapsto \tilde{\pi}} & \text{Map}_{\text{cont}}(G/H, A) \\
\pi \downarrow & & \pi \downarrow \\
A & & A
\end{array}
\]

is \( y \mapsto y(H) \).

Now we may state Shapiro’s lemma:

**Proposition 3.2. (Shapiro’s Lemma)** Let \( G \) be any profinite group, \( H \) be any closed subgroup of \( G \), and \( A \) be any continuous \( G \)-module. Then for each \( n \geq 0 \), there is a canonical isomorphism:

\[
\text{sh} : \mathcal{H}^{n}(G, \text{Ind}_{G}^{H}(A)) \to \mathcal{H}^{n}(H, A)
\]

induced by the map on cochains defined by sending \( a \in \mathcal{C}^{n}(G, \text{Ind}_{G}^{H}(A)) \) to the cochain:

\[
(\pi \circ a)|_{H^{n+1}}.
\]

The corresponding isomorphism:

\[
\text{sh} : \mathcal{H}^{n}(G, \text{Ind}_{G}^{H}(A)) \to \mathcal{H}^{n}(H, A)
\]

is the same: It is induced by the map on cochains that sends \( a \in \mathcal{C}^{n}(G, \text{Ind}_{G}^{H}(A)) \) to \( (\pi \circ a)|_{H^{n}} \).

**Proof 3.2.** Shapiro’s lemma for continuous cohomology with homogeneous cochains is stated and proved as Proposition 1.6.3 of [NSW]; the explicit isomorphism is given in the proof.

To find what the corresponding homomorphism is for inhomogeneous cochains, we let \( a \in \mathcal{C}^{n}(G, \text{Ind}_{G}^{H}(A)) \) be arbitrary. Then we compute:

\[
\tilde{\text{sh}}(h_{1}, \ldots, h_{n}) = \text{sh}(h_{1}, h_{1} h_{2}, \ldots, h_{1} \cdots h_{n}) = \pi \circ \tilde{a}(h_{1}, h_{1} h_{2}, \ldots, h_{1} \cdots h_{n})
\]

\[
= \pi \circ \left(1 \cdot a(1^{-1}h_{1}, h_{1}^{-1}(h_{1} h_{2}), \ldots, (h_{1} \cdots h_{n-1})^{-1}(h_{1} \cdots h_{n}))\right) = \pi \circ a(h_{1}, \ldots, h_{n}),
\]

as was claimed. QED
The corresponding isomorphisms:

\[ \text{sh} : H^n(G, \text{Map}_{\text{cont}}(G/H, A)) \rightarrow H^n(H, A) \]

and

\[ \text{sh} : H^n(G, \text{Map}_{\text{cont}}(G/H, A)) \rightarrow H^n(H, A) \]

are also induced by the maps on cochains that send \( a \in C^n(G, \text{Map}_{\text{cont}}(G/H, A)) \) to \( (\pi \circ a) |_{H^n} \), where in this case \( \pi \) is the projection from \( \text{Map}_{\text{cont}}(G/H, A) \) to \( A \).

There is one more proposition that will be useful later on. Let \( G \) be a profinite group and \( H \) an open subgroup of \( G \). Thus, the left coset space \( G/H = \{ gH | g \in G \} \) is finite. Define the map \( v : \text{Ind}_G^H(A) \rightarrow A \) as:

\[ x \mapsto \sum_{c \in G/H} \overline{c} \cdot x(\overline{c}^{-1}), \]

where \( \overline{c} \) is any representative of \( c \). This function is well-defined, for if \( \overline{d} \) is another representative of \( c \), then \( \overline{d} = \overline{c}h \) for some \( h \in H \), and

\[ \overline{d} \cdot x(\overline{d}^{-1}) = (\overline{c}h) \cdot x(h^{-1}\overline{c}^{-1}) = \overline{c} \cdot x(\overline{c}^{-1}). \]

One can prove that \( v \) is a \( G \)-module homomorphism. Then one has the following proposition:

**Proposition 3.3.** The following diagram is commutative, where \( \text{sh} \) denotes the isomorphism of Shapiro’s lemma.

\[
\begin{array}{ccc}
H^n(G, \text{Ind}_G^H(A)) & \xrightarrow{\text{sh}} & H^n(H, A) \\
\downarrow{\text{v}^n} & & \downarrow{\text{cor}} \\
H^n(G, A) & & \\
\end{array}
\]

A similar diagram holds for cohomology with homogeneous cochains.

**Proof 3.3.** This is stated and proved as part of Proposition 1.6.4 of [NSW].

The corresponding function \( v : \text{Map}_{\text{cont}}(G/H, A) \rightarrow A \) is:

\[ y \mapsto \sum_{c \in G/H} y(c). \]

This is because if \( y \in \text{Map}_{\text{cont}}(G/H, A) \) and \( x \in \text{Ind}_G^H(A) \) is \( x(g) = g \cdot y(g^{-1}H) \), then:

\[ v(x) = \sum_{c \in G/H} \overline{c} \cdot x(\overline{c}^{-1}) = \sum_{c \in G/H} (\overline{c} \overline{c}^{-1}) \cdot y(\overline{c}^{-1}H) = \sum_{c \in G/H} y(c). \]

Then the following diagram also commutes:

\[
\begin{array}{ccc}
H^n(G, \text{Map}_{\text{cont}}(G/H, A)) & \xrightarrow{\text{sh}} & H^n(H, A) \\
\downarrow{\text{v}^n} & & \downarrow{\text{cor}} \\
H^n(G, A) & & \\
\end{array}
\]

and similarly for homogeneous cocycles.
8. Kummer Theory

This exposition is taken largely from Section VI.2 of [NSW].

We return to the setting of Galois cohomology. Let $K/k$ be any Galois field extension, finite or otherwise. Then $\text{Gal}(K/k)$ is a profinite group that acts on the abelian group $K^\times$ by automorphisms and this action is continuous, so $K^\times$ is a continuous $\text{Gal}(K/k)$-module. Then we have the following theorem:

**Theorem 3.4. (Hilbert’s Theorem 90)** For any Galois extension $K/k$, $H^1(\text{Gal}(K/k), K^\times) \cong 0$.

**Proof.** This is stated and proved as Theorem 6.2.1 of [NSW].

Fix a positive integer $m$, and suppose that $\text{char}(k) \nmid m$, and that $k^{\text{sep}}$ is a separable closure of $k$. Then since $\text{char}(k) \nmid m$, $k^{\text{sep}}$ contains the group $\mu_m$ of $m$th roots of unity. Let $f : (k^{\text{sep}})^\times \to (k^{\text{sep}})^\times$ be $a \mapsto a^m$. Let $G$ denote $\text{Gal}(k^{\text{sep}}/k)$. Then the following is a short exact sequence of continuous $G$-modules:

$$1 \longrightarrow \mu_m \xrightarrow{\text{incl}} (k^{\text{sep}})^\times \xrightarrow{f} (k^{\text{sep}})^\times \longrightarrow 1,$$

and so from the long-exact sequence in cohomology we find that the following is an exact sequence:

$$H^0(G, (k^{\text{sep}})^\times) \xrightarrow{f^0} H^0(G, (k^{\text{sep}})^\times) \xrightarrow{\delta^1} H^1(G, \mu_m) \xrightarrow{\text{incl}} H^1(G, (k^{\text{sep}})^\times).$$

Recalling the isomorphism $H^0(G, A) \cong A^G$ for all profinite groups $G$ and $G$-modules $A$, and also Hilbert’s Theorem 90, we can rewrite the previous exact sequence as:

$$k^\times \xrightarrow{f} k^\times \xrightarrow{\delta^1} H^1(G, \mu_m) \xrightarrow{\text{incl}} 1.$$

This means that $\delta^1 : H^0(G, (k^{\text{sep}})^\times) \cong k^\times \to H^1(G, \mu_m)$ is surjective with kernel $f^0(H^0(G, (k^{\text{sep}})^\times)) = f(k^\times) = (k^\times)^m$. Therefore, $\delta^1$ induces an isomorphism:

$$\text{kum}_m : k^\times/(k^\times)^m \to H^1(G, \mu_m).$$

From the description of the connecting homomorphism $\delta^1$, we can give a precise description of $\text{kum}_m$: Suppose that $a \in k^\times$ is arbitrary. Pick an arbitrary $m$th root

$$\sqrt[a]{(k^{\text{sep}})} \in k^{\text{sep}} = C^0(\text{Gal}(k^{\text{sep}}, k), (k^{\text{sep}})^\times).$$

The coboundary map sends $\sqrt[a]{a}$ to the 1-cocycle:

$$\sigma \mapsto \sigma(\sqrt[a]{a}).$$

Though this cocycle is a priori one in $Z^1(\text{Gal}(k^{\text{sep}}, k), (k^{\text{sep}})^\times)$, we see that its range is $\mu_m$, so this cocycle is in $Z^1(\text{Gal}(k^{\text{sep}}, k), \mu_m)$. Therefore, $\text{kum}_m$ sends the class of $a$ in $k^\times/(k^\times)^m$ to the class of:

$$\sigma \mapsto \sigma(\sqrt[a]{a})$$

in $H^1(G, \mu_m)$. In particular, if $\mu_m \subseteq k^\times$, then $G$ acts trivially on $\mu_m$, so

$$H^1(G, \mu_m) \cong \text{Hom}_{\text{cont}}(G, \mu_m)$$

and we have an isomorphism of $k^\times/(k^\times)^m$ into $\text{Hom}_{\text{cont}}(G, \mu_m)$. The results of this and the previous paragraph are collectively called Kummer theory.

We now state two and prove two simple results:

**Proposition 3.5.** Let $K/k$ be any finite Galois extension of fields and let $k^{\text{sep}}$ be a separable closure of $k$ that contains $K$. Let $G = \text{Gal}(k^{\text{sep}}/k)$ and $H = \text{Gal}(k^{\text{sep}}/K)$. Then the corestriction map:

$$\text{cor}^H_G : H^0(H, (k^{\text{sep}})^\times) \to H^0(G, (k^{\text{sep}})^\times)$$

is precisely the field norm $N_{K/k} : K^\times \to k^\times$. 

58
**Proof 3.5.** $H$ is an open normal subgroup of $G$ by the fundamental theorem of infinite Galois theory, so the corestriction map is well-defined. Next, we have:

$$Z^0(H, (k_{\text{sep}})^\times) = ((k_{\text{sep}})^\times)^H = K^\times,$$

and $B^0(H, (k_{\text{sep}})^\times) \cong B^0(G, (k_{\text{sep}})^\times) \cong 0$. Furthermore, for $a \in K^\times = Z^0(H, (k_{\text{sep}})^\times)$,

$$\text{cor}^H_G(a) = \prod_{c \in H \setminus G} \overline{c}^{-1} \cdot a,$$

where $\overline{c}$ is a representative of $c$. However, since $H \trianglelefteq G$, $H \setminus G$ is the set of left cosets in the quotient group $G/H$, which from the fundamental theorem of Galois theory is isomorphic to $\text{Gal}(K/k)$. Furthermore, since the isomorphism $G/H \rightarrow \text{Gal}(K/k)$ is induced by the map $G \rightarrow \text{Gal}(K/k)$ given by $\sigma \mapsto \sigma|_K$, the previous quantity is:

$$\prod_{\sigma \in \text{Gal}(K/k)} \sigma^{-1}(a) = \prod_{\sigma \in \text{Gal}(K/k)} \sigma(a) = N_{K/k}(a),$$

as desired. QED

**Proposition 3.6.** Let $K/k$ be any finite Galois extension of fields and let $k_{\text{sep}}$ be a separable closure of $k$ that contains $K$. Fix a positive integer $m$ and assume that $\text{char}(k) \nmid m$, and let $\mu_m$ denote the group of $m$th roots of unity in $k_{\text{sep}}$. Let $G = \text{Gal}(k_{\text{sep}}/k)$ and $H = \text{Gal}(k_{\text{sep}}/K)$. Then the following diagram commutes:

$$\begin{array}{ccc}
K^\times / (K^\times)^m & \stackrel{\text{kum}_K}{\longrightarrow} & H^1(H, \mu_m) \\
\downarrow N_{K/k} & & \downarrow \text{cor}^H_G \\
k^\times / (k^\times)^m & \stackrel{\text{kum}_k}{\longrightarrow} & H^1(G, \mu_m),
\end{array}$$

where $N_{K/k}$ is descended from the norm map $N_{K/k} : K \rightarrow k$.

**Proof 3.6.** Recall the short exact sequence of $G$-modules in the construction of the map from Kummer theory:

$$1 \longrightarrow \mu_m \overset{\text{incl}}{\longrightarrow} (k_{\text{sep}})^\times \overset{f}{\longrightarrow} (k_{\text{sep}})^\times \longrightarrow 1.$$ 

Then since corestriction is functorial and commutes with connecting homomorphisms, the following diagram commutes and has exact rows:

$$\begin{array}{ccc}
H^0(H, (k_{\text{sep}})^\times) & \overset{f^0}{\longrightarrow} & H^0(H, (k_{\text{sep}})^\times) \\
\downarrow \text{cor}^H_G & & \downarrow \text{cor}^H_G \\
H^0(G, (k_{\text{sep}})^\times) & \overset{f^0}{\longrightarrow} & H^0(G, (k_{\text{sep}})^\times)
\end{array} \quad \delta^1 \quad \begin{array}{ccc}
H^1(H, \mu_m) & \longrightarrow & H^1(H, \mu_m) \\
\downarrow \text{cor}^H_G & & \downarrow \text{cor}^H_G \\
H^1(G, \mu_m) & \longrightarrow & H^1(G, \mu_m)
\end{array}$$

In view of the previous proposition, we can rewrite the previous diagram as:

$$\begin{array}{ccc}
K^\times & \overset{f}{\longrightarrow} & K^\times \\
\downarrow N_{K/k} & & \downarrow N_{K/k} \\
k^\times & \overset{f}{\longrightarrow} & k^\times
\end{array} \quad \delta^1 \quad \begin{array}{ccc}
H^1(H, \mu_m) & \longrightarrow & H^1(H, \mu_m) \\
\downarrow \text{cor}^H_G & & \downarrow \text{cor}^H_G \\
H^1(G, \mu_m) & \longrightarrow & H^1(G, \mu_m).
\end{array}$$

Since the previous diagram commutes, $N_{K/k}$ sends $f(K^\times) = (K^\times)^m$ into $f(k^\times) = (k^\times)^m$. Thus, recalling the definition of kum$_K$ and kum$_k$, we have the following commutative diagram:

$$\begin{array}{ccc}
K^\times / (K^\times)^m & \stackrel{\text{kum}_K}{\longrightarrow} & H^1(H, \mu_m) \\
\downarrow N_{K/k} & & \downarrow \text{cor}^H_G \\
k^\times / (k^\times)^m & \stackrel{\text{kum}_k}{\longrightarrow} & H^1(G, \mu_m),
\end{array}$$
9. Central Simple Algebras, the Brauer Group, and Cyclic Algebras

This exposition is taken mainly from Section VI.3 of [NSW] and Sections III.1 and III.3 of [Kn].

Let $k$ be a field. By a $k$-algebra, we mean a $k$-vector space $V$ with an associative, $k$-bilinear binary operation $-\cdot- : A \times A \to A$, such that this operation has an identity element. Any $k$-algebra is a ring under vector addition and the $k$-bilinear binary operation $-\cdot-$. By a $k$-division algebra we mean a $k$-algebra that when considered as a ring is a skew-field (i.e. a nonzero ring such that every nonzero element has a two-sided multiplicative inverse). A $k$-algebra homomorphism between two $k$-algebras $A$ and $B$ is a $k$-linear map $f : A \to B$ that is also a ring homomorphism when $A$ and $B$ are considered as rings. In particular, $f$ must send the identity of $A$ to the identity of $B$. A $k$-algebra isomorphism is a bijective $k$-algebra homomorphism. For each field $k$, the class of all $k$-algebras and all $k$-algebra homomorphisms is a category.

Note that for any $n \geq 0$, the ring of $n \times n$ matrices $M_n(k)$ is a $k$-algebra. $(M_0(k)$ is the zero ring.) More generally, if $D$ is any $k$-division algebra, then $M_n(D)$ is a $k$-algebra. For any field extension $K/k$, $K$ is a $k$-algebra. If $A$ and $B$ are both $k$-algebras, then $A \otimes_k B$ may be considered to be a $k$-algebra under the operation defined on pure tensors as:

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1a_2) \otimes (b_1b_2)$$

with multiplicative identity $1 \otimes 1$. Furthermore, if $K/k$ is any field extension and $A$ any $k$-algebra then $A \otimes_k K$ can be considered to be a $k$-algebra under extension of scalars. We say that $K$ splits $A$, or that $K$ is a splitting field of $A$, or that $A$ is split by $K$, if there is some $n \geq 0$ such that $A \otimes_k K \cong M_n(K)$ as $k$-algebras.

Note that for any $k$-algebra $A$ with identity 1, the set \{ $\alpha 1 | \alpha \in k$ \} is contained in the center of $A$. $A$ is called central if this is the entire center of $A$. $A$ is called simple if $A$ is simple as considered as a ring, i.e. the only two-sided ideals of the ring $A$ are 0 and $A$. A $k$-algebra $A$ is called central simple if it is nonzero, finite-dimensional, central, and simple. Note that for any finite-dimensional central division algebra $D$ and $n \geq 1$, $M_n(D)$ is a central simple algebra. We now have the following lemma:

**Lemma 3.7.** For any $k$-algebra $A$ and field extension $K/k$, $A$ is a central simple $k$-algebra if and only if $A \otimes_k K$ is a central simple $k$-algebra.

**Proof 3.7.** The $\Rightarrow$ direction of the proof can be found in paragraph 3 on p. 126 of [Kn]. For the $\Leftarrow$ direction, note that $\dim_k(A) = \dim_K(A \otimes_k K)$, so if $A \otimes_k K$ is finite-dimensional and nonzero, then $A$ is finite-dimensional and nonzero. Next, if $I$ is a two-sided ideal of $A$ that is neither 0 nor $A$, then the $k$-vector space $I \otimes_k K$ is a two-sided ideal of $A \otimes_k K$ that is neither 0 nor $A \otimes_k K$. Finally, if $c \in Z(A)$ is not of the form $\alpha 1$ for $\alpha \in k$, then the pure tensor $c \otimes 1$ is an element of $Z(A \otimes_k K)$ not of the form $\alpha (1 \otimes 1)$. This proves the lemma.

We now have the following characterization of central simple algebras:

**Proposition 3.8.** Let $A$ be a finite-dimensional nonzero $k$-algebra. Then the following statements are equivalent:

1. $A$ is central simple.
2. If $\overline{k}$ is an algebraic closure of $k$, then $A$ is split by $\overline{k}$.
3. There exists a finite-dimensional Galois extension $K/k$ such that $A$ is split by $K$.
4. There exists a finite-dimensional central $k$-division algebra $D$ and a positive integer $n$ such that $A \cong M_n(D)$ as $k$-algebras.

Furthermore, if any of the previous statements are true, then in item (4) $n$ is uniquely determined and $D$ is uniquely determined up to $k$-algebra isomorphism.
PROOF 3.8. The fact that (4) ⇒ (1) has already been stated. The fact that (1) ⇒ (4) and the uniqueness statements are well-known results and are collectively called Wedderburn’s theorem. It is stated and proved as Theorem 2.1.3 of [GS] and as Theorem 2.4 of [Kn]. The fact that (2) ⇒ (1) and (3) ⇒ (1) follow from the previous lemma and that $M_n(K)$ is a central simple $K$-algebra for all fields $K$. A proof that (1) ⇒ (2) is given in the proof of Theorem 2.2.1 of [GS]. The fact that (1) ⇒ (3) is stated and proved as part of Corollary 2.2.6 of [GS]. QED

The uniqueness statement in the previous proposition allows us to define an equivalence relation on central simple $k$-algebras as follows: Suppose that $A \cong M_n(D)$ and $B \cong M_n(D')$ are central simple $k$-algebras, where $D$ and $D'$ are finite-dimensional central division $k$-algebras. Then we say that $A$ and $B$ are Brauer equivalent if $D \cong D'$ as $k$-algebras. This can be shown to be well-defined and an equivalence relation. Then we have the following proposition:

PROPOSITION 3.9. If $A$ and $B$ are central simple $k$-algebras, then so is $A \otimes_k B$. Furthermore, this binary operation on the set of all central simple $k$-algebras descends to a well-defined binary operation on Brauer equivalence classes of central simple algebras. This binary operation makes the set of Brauer equivalence classes of central simple $k$-algebras into an abelian group. The identity of this group is class of $M_1(k)$, and the inverse of the class of $A$ is the class of $A^{\text{opp}}$, where $A^{\text{opp}}$ is the opposite algebra of $A$.

PROOF 3.9. The fact that the set of central simple algebras is closed under tensor products is stated and proved as Proposition 2.36(b) of [Kn]. The fact that this operation descends to one on Brauer equivalence classes is stated and proved as part of Proposition 3.2 of [Kn]. The fact that this operation is associative and commutative is a consequence of the associativity and commutativity of tensor products. Further, $M_1(k) \cong k$ as $k$-algebras, and for any $k$-algebra $A$, $A \otimes_k k \cong A$ as $k$-algebras. Therefore, $M_1(k)$ is an identity of this operation. The fact that the class of $A^{\text{opp}}$ is the inverse of the class of $A$ is equivalent to the fact that $A \otimes_k A^{\text{opp}} \cong M_n(k)$ for some positive integer $n$. This latter statement is stated and proved as Corollary 2.3.8 of [Kn]. QED

We define the Brauer group $\text{Br}(k)$ of $k$ to be the group indicated in the previous proposition. The operation of $\text{Br}(k)$ is usually written additively. Next, we have the following proposition:

PROPOSITION 3.10. Let $K/k$ be any field extension. The map from the set of central simple $k$-algebras to the set of central simple $K$-algebras given by:

$$A \mapsto A \otimes_k K$$

descends to a well-defined group homomorphism from $\text{Br}(k)$ to $\text{Br}(K)$. Furthermore, if $L/K/k$ is any tower of field extensions, then the associated group homomorphism $\text{Br}(k) \to \text{Br}(L)$ is the composition of the two group homomorphisms $\text{Br}(k) \to \text{Br}(K)$ and $\text{Br}(K) \to \text{Br}(L)$.

PROOF 3.10. The fact that the function $A \mapsto A \otimes_k K$ descends to a function on Brauer equivalence classes proved in the last paragraph on page 126 of [Kn]. The fact that this function is a group homomorphism is proved in the first full paragraph on page 127 of [Kn]. The statement about towers of field extensions is proved in the second full paragraph on page 127 of [Kn]. QED

For each field extension $K/k$, we define the group $\text{Br}(K/k)$ to be the kernel of the homomorphism $\text{Br}(k) \to \text{Br}(K)$ in the previous proposition. $\text{Br}(K/k)$ is called a relative Brauer group, and it consists of those classes in $\text{Br}(k)$ that can be represented by algebras that are split by $K$.

Fix a separable closure $k^{\text{sep}}$ of $K$, and let $\mathcal{I}$ denote the set of all intermediate fields $k^{\text{sep}}/K/k$ such that $K/k$ is a finite Galois extension. Then we have from Proposition 3.8(3) that:

$$\text{Br}(k) = \bigcup_{K \in \mathcal{I}} \text{Br}(K/k).$$

However, we can be more precise about this and write this as a direct limit. Make $\mathcal{I}$ into a directed set by saying that for $K, L \in \mathcal{I}$, $K \leq L$ if and only if $K \subseteq L$. For each $K \in \mathcal{I}$, let $G_K$ equal
$\text{Br}(K/k)$, and let $\iota_K : G_K \to \text{Br}(k)$ be inclusion. Next, for all $K, L \in \mathcal{I}$ with $K \leq L$, let $f_{KL} : G_K \to G_L$ be inclusion. $f_{KL}$ is well-defined because of the statement about compositions in the previous proposition. Then:

$$\left\{ \{G_K|K \in \mathcal{I}\}, \{f_{KL}|K, L \in \mathcal{I}, K \leq L\} \right\}$$

is a direct system and:

$$\left(\text{Br}(k), \{\iota_K|K \in \mathcal{I}\}\right)$$

is a direct limit of this system. Briefly,

$$\text{Br}(k) \cong \lim_{\rightarrow} \text{Br}(K/k).$$

To highlight the relevance of the previous observation, we need to define crossed product algebras. To this end, let $K/k$ be any finite Galois extension of fields, $G$ denote $\text{Gal}(K/k)$, $n$ denote $[K : k]$, and $a \in Z^2(G, K^\times)$ be any cocycle. Then let $A$ be the $n$-dimensional free $K$-vector space over $G$, i.e.:

$$A = \bigoplus_{g \in G} Ke_g,$$

and regard $A$ as an $n^2$-dimensional $k$-vector space. Define a binary operation on $A$ as follows: for $g_1, g_2 \in G$ and $\alpha_1, \alpha_2 \in K$, define:

$$(\alpha_1 e_{g_1}) \cdot (\alpha_2 e_{g_2}) = \alpha_1 g_1(\alpha_2) a(g_1, g_2)e_{g_1g_2}$$

and extend to all of $A$ by $Z$-linearity. It can be shown that this is a $k$-bilinear operation, that $a(1,1)^{-1}e_1$ is an identity of this operation, and that this operation is associative. All three of these facts are proved as part of Proposition 3.12 of [Kn]. Therefore, $A$ is a finite-dimensional $k$-algebra. We denote this $k$-algebra as $C(K, G, a)$ and call it the crossed product of $K$ and $G$ by $a$. We then have the following proposition:

**Proposition 3.11.** Let $K/k$ be any finite Galois extension, $G = \text{Gal}(K/k)$, and $a, a_1, a_2 \in Z^2(G, K^\times)$ be arbitrary. Then:

1. $C(K, G, a)$ is a central simple $k$-algebra split by $L$.
2. The cocycles $a_1$ and $a_2$ are cohomologous if and only if $C(K, G, a_1) \cong C(K, G, a_2)$ as $k$-algebras.
3. $C(K, G, a_1a_2)$ is Brauer equivalent to $C(K, G, a_1) \otimes_k C(K, G, a_2)$.
4. Every central simple $k$-algebra that is split by $K$ is Brauer equivalent to some crossed product algebra.

**Proof 3.11.** That $C(K, G, a)$ is central simple is proved as part of Proposition 3.12 of [Kn]. That $C(K, G, a)$ is split by $L$ follows from Theorem 3.3 and Proposition 3.12 of [Kn]. (2) is proved as part of Corollary 3.13 of [Kn]. (3) is proved as part of Theorem 3.14 of [Kn]. (4) is proved as Proposition 3.10 of [Kn]. QED

Thus, from the previous proposition, the map from $Z^2(\text{Gal}(K/k), K^\times)$ to central simple $k$-algebras split by $K$ defined as $a \mapsto C(K, \text{Gal}(K/k), a)$ descends to a well-defined isomorphism brau from $H^2(\text{Gal}(K/k), K^\times)$ to $\text{Br}(K/k)$.

Thus, we have two directed systems indexed by the same set $\mathcal{I}$ of intermediate fields $k^{sep}/K/k$ such that $K/k$ is finite and Galois. The first is:

$$\left\{ \{\text{Br}(K/k)|K \in \mathcal{I}\}, \{\text{incl} : \text{Br}(K/k) \to \text{Br}(L/k)|K, L \in \mathcal{I}, K \leq L\} \right\}$$

with direct limit

$$(\text{Br}(k), \{\text{incl} : \text{Br}(K/k) \to \text{Br}(k)|K \in \mathcal{I}\}).$$

The second is the example from the section on direct limits, namely:

$$\left\{ \{H^2(\text{Gal}(K/k), K^\times)|K \in \mathcal{I}\}, \{\text{incl} : H^2(\text{Gal}(K/k), K^\times) \to H^2(\text{Gal}(L/k), L^\times)|K, L \in \mathcal{I}, K \leq L\} \right\}$$

62
with direct limit:

\[
(H^2(\text{Gal}(k_{\text{sep}}/k), (k_{\text{sep}})^\times), \{\text{incl} : H^2(\text{Gal}(K/k), K^\times) \to H^2(\text{Gal}(k_{\text{sep}}/k), (k_{\text{sep}})^\times) | K \in \mathcal{I}\}).
\]

Furthermore, it can be shown that the collection of isomorphisms:

\[
\{\text{brau} : H^2(\text{Gal}(K/k), K^\times) \to \text{Br}(K/k) | K \in \mathcal{I}\}
\]

is a homomorphisms of directed systems, so there is an induced isomorphism:

\[
\text{brau} : H^2(\text{Gal}(k_{\text{sep}}/k), (k_{\text{sep}})^\times) \to \text{Br}(k).
\]

Now we have the following proposition:

**Proposition 3.12.** Fix a positive integer \( m \) and suppose that \( \text{char}(k) \nmid m \), so that \( k_{\text{sep}} \) contains a group \( \mu_m \) of \( m \)-th roots of unity, and let \( G = \text{Gal}(k_{\text{sep}}/k) \). Then the isomorphism \( \text{brau} : H^2(G, (k_{\text{sep}})^\times) \to \text{Br}(k) \) maps the elements of \( H^2(G, (k_{\text{sep}})^\times) \) that are represented by elements of \( Z^2(G, \mu_m) \) isomorphically onto \( m\text{Br}(k) \), the \( m \)-torsion part of \( \text{Br}(k) \), and \( m\text{Br}(k) \cong H^2(G, \mu_m) \).

**Proof 3.12.** As \( \text{brau} \) is an isomorphism, it must map the \( m \)-torsion part of \( H^2(G, (k_{\text{sep}})^\times) \) isomorphically onto the \( m \)-torsion part of \( \text{Br}(k) \). Therefore, we must find the \( m \)-torsion part of \( H^2(G, (k_{\text{sep}})^\times) \). To this end, we recall the short exact sequence of continuous \( G \)-modules:

\[
1 \longrightarrow \mu_m \xrightarrow{\text{incl}} (k_{\text{sep}})^\times \xrightarrow{f} (k_{\text{sep}})^\times \longrightarrow 1
\]

used to prove Kummer theory. We have from the long exact sequence in cohomology that the following sequence is exact:

\[
H^1(G, (k_{\text{sep}})^\times) \xrightarrow{\delta^2} H^2(G, \mu_m) \xrightarrow{\text{incl}^2} H^2(G, (k_{\text{sep}})^\times) \xrightarrow{f^2} H^2(G, (k_{\text{sep}})^\times).
\]

Now, the \( m \)-torsion part of \( H^2(G, (k_{\text{sep}})^\times) \) is precisely the kernel of \( f^2 \), which is the image of \( \text{incl}^2 \). \( \text{incl}^2 \) is descended from the inclusion map on cochains, so the \( m \)-torsion part of \( H^2(G, (k_{\text{sep}})^\times) \) are those cohomology classes that are represented by elements of \( Z^2(G, \mu_m) \). Furthermore, we have from Hilbert’s theorem 90 that \( H^1(G, (k_{\text{sep}})^\times) \) is trivial, so \( \text{incl}^2 \) is injective. Thus, \( H^2(G, \mu_m) \cong m\text{Br}(k) \), as desired. QED

Fix a positive integer \( m \), and suppose that \( \text{char}(k) \nmid m \) and that \( k \) contains a primitive \( m \)-th root of unity \( \omega \). For any two elements \( a, b \in k^\times \), we define the cyclic algebra \( (a, b)_\omega \) to be the \( m^2 \)-dimensional \( k \)-algebra with \( k \)-basis:

\[
\{x^iy^j | 0 \leq i < m, 0 \leq j < m\}
\]

and with multiplication defined by \( x^m = a, y^m = b, xy = \omega yx \). It is routine to show that \( (a, b)_\omega \) is a central simple \( k \)-algebra. Not only that, but if \( a/a', b/b' \in (k^\times)^m \), then \( (a, b)_\omega \cong (a', b')_\omega \) as \( k \)-algebras. Thus, for \( a, b \in k^\times/(k^\times)^m \), \( (a, b)_\omega \) is a well-defined element of \( \text{Br}(k) \).

Further, we have the following proposition:

**Proposition 3.13.** For a fixed positive integer \( m \), and field \( k \) with \( \text{char}(k) \nmid m \) that contains a primitive \( m \)-th root of unity \( \omega \), the following diagram commutes:

\[
\begin{array}{c}
k^\times/(k^\times)^m \times k^\times/(k^\times)^m \xrightarrow{\text{kum}_m \times \text{kum}_m} H^1(\text{Gal}(k_{\text{sep}}/k), \mu_m) \times H^1(\text{Gal}(k_{\text{sep}}/k), \mu_m) \\
\xrightarrow{\omega} \text{Br}(k) \xleftarrow{\text{brau}} H^2(\text{Gal}(k_{\text{sep}}/k)G, \mu_m).
\end{array}
\]

**Proof 3.13.** This is essentially the content of Proposition 4.7.1 of [GS]; this proposition is proved there.

Note that the cup-product on \( H^1(\text{Gal}(k_{\text{sep}}/k), \mu_m) \times H^1(\text{Gal}(k_{\text{sep}}/k), \mu_m) \) should a priori have as its range \( H^2(\text{Gal}(k_{\text{sep}}/k), \mu_m \otimes \mathbb{Z} \mu_m) \). However, \( \mu_m \otimes \mathbb{Z} \mu_m \cong \mu_m \) as abelian groups, and since \( \omega \in k \),
\( \mu_m \subseteq k \), so \( \text{Gal}(k^{\text{sep}}/k) \) acts trivially on \( \mu_m \) and \( \mu_m \otimes \mathbb{Z} \mu_m \), so \( \mu_m \otimes \mathbb{Z} \mu_m \cong \mu_m \) as \( G \)-modules, so the cup-product has the expected range. QED

Note that by the previous proposition, \((a, b)_\omega\) is actually an element of \( m\text{Br}(k) \). Furthermore, since the cup-product on \( H^1(\text{Gal}(k^{\text{sep}}/k), \mu_m) \times H^1(\text{Gal}(k^{\text{sep}}/k), \mu_m) \) is bilinear and anticommutative, we have that for all \( a, b, c \in k^\times/(k^\times)^m \),

\[
(a, bc)_\omega = (a, b)_\omega + (a, c)_\omega \\
(ab, c)_\omega = (a, c)_\omega + (b, c)_\omega \\
(a, b)_\omega = -(b, a)_\omega
\]
as elements of \( m\text{Br}(k) \). It can be proved that for any \( a, b, c \in k \), \((a, b)_\omega \cong (a, c)_\omega\) if and only if \( b/c \) is a norm arising from the field extension \( k(\sqrt[n]{a})/k \).

Finally, note that in the case \( m = 2 \), any field \( k \) with \( \text{char}(k) \nmid 2 \) will have a primitive \( m \)th root of \( 1 \), namely \(-1\), and that the cyclic algebras \((a, b)_\omega\) are precisely quaternion algebras.
CHAPTER 4

Decomposition of $E^\times/(E^\times)^2$

1. A Decomposition of $H^1(G_F, V)$

The purpose of this section is to decompose $H^1(G_F, V)$ as was stated in the introduction. These results will be proved in as much generality as possible. Therefore, for the time being, we assume that $E/F$ is a Galois extension of fields whose Galois group $G$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some prime number $p$ and positive integer $n$. We recall the notation from the introduction.

We assume that

$$G = \langle \tau_1, \ldots, \tau_n | \forall i, j, \tau_i^p = 1, \tau_i\tau_j = \tau_j\tau_i \rangle$$

so that:

$$\mathbb{F}_p[G] = \mathbb{F}_p[\tau_1, \ldots, \tau_n]/(\tau_1^p - 1, \ldots, \tau_n^p - 1) = \mathbb{F}_p[\rho_1, \ldots, \rho_n]/(\rho_1^p - 1, \ldots, \rho_n^p),$$

where for each $1 \leq i \leq n$, $\rho_i = \tau_i - 1$. For each $1 \leq i \leq n$, let:

$$b_i = \rho_i^{p-1} \cdot \rho_{i-1}^{p-2} \rho_{i+1}^{p-1} \cdots \rho_n^{p-1} \in \mathbb{F}_p[G],$$

and let:

$$z = \rho_1^{p-1} \cdots \rho_n^{p-1} \in \mathbb{F}_p[G].$$

Then we define

$$V = \langle b_1, \ldots, b_n, z \rangle \subseteq \mathbb{F}_p[G].$$

Note that an element $m$ of an $\mathbb{F}_p[G]$-module $M$ is fixed by $G$ if and only if $\rho_im = 0$ for all $1 \leq i \leq m$. Therefore, as an $\mathbb{F}_p$-vector space, the $\mathbb{F}_p[G]$-module $V^G$ is:

$$\langle z \rangle.$$

$V^G$ is clearly a trivial $\mathbb{F}_p[G]$-module, so it is isomorphic to $\mathbb{F}$ as an $\mathbb{F}_p[G]$-module.

$V/V^G$ is $\langle \overline{b}_1, \ldots, \overline{b}_n \rangle$ as an $\mathbb{F}_p$-vector space. Further, because

$$\rho_i\overline{b}_j = 0$$

in $V/V^G$, $V/V^G$ is a trivial $n$-dimensional $\mathbb{F}_p[G]$-module. Thus, we have the following two short exact sequences of $G$-modules:

$$0 \to \mathbb{F}_p \xrightarrow{\epsilon_1} V \xrightarrow{\pi_1} V/V^G \to 0.$$

$$0 \to V/V^G \xrightarrow{\pi_2} \mathbb{F}_p[G] \xrightarrow{\pi_2} \mathbb{F}_p[G]/V \to 0.$$

Therefore, we may speak of $H^n(G, \mathbb{F}_p), H^n(G, V/V^G), H^n(G, V), H^n(G, \mathbb{F}_p[G]),$ and $H^n(G, \mathbb{F}_p[G]/V)$.

Recall the notation from the introduction that $F^{\text{sep}}$ is a fixed separable closure of $F$ that contains $E$, that $G_F = \text{Gal}(F^{\text{sep}}/F)$ and $G_E = \text{Gal}(F^{\text{sep}}/E)$. From the fundamental theorem of infinite Galois theory we that that $G_E$ is an open normal subgroup of $G_F$ and that $G_F/G_E \cong G$ as topological groups. The isomorphism $G_F/G_E \cong G$ is induced by the surjective homomorphism of profinite groups $\phi : G_F \to G$ defined as $\sigma \mapsto \sigma_E$.

Next, recall from the overview that any continuous $G$-module $M$ can be made into a continuous $G_F$-module via the action:

$$\sigma \cdot m = \phi(\sigma) \cdot m.$$
for $\sigma \in G_F$ and $m \in M$. Furthermore, if $f : M \to N$ is a $G$-module homomorphism, then $f$ will also be a continuous $G_F$-module homomorphism under this action, as:

$$f(\sigma \cdot m) = f(\phi(\sigma)m) = \phi(\sigma)f(m) = \sigma \cdot f(m).$$

Therefore, the exact sequences:

$$0 \to \mathbb{F}_p \xrightarrow{\lambda_1} V \xrightarrow{\pi_1} V/V^G \to 0$$

$$0 \to V \xrightarrow{\iota_2} \mathbb{F}_p[G] \xrightarrow{\pi_2} \mathbb{F}_p[G]/V \to 0$$

are also exact sequences of $G_F$-modules. Therefore, we may speak of $H^n(G_F, \mathbb{F}_p)$, $H^n(G_F, V/V^G)$, $H^n(G_F, V)$, $H^n(G_F, \mathbb{F}_p[G])$, and $H^n(G_F, \mathbb{F}_p[G]/V)$.

Next, for any $G$-module $M$ and $n \geq 0$, $H^n(G, M)$ and $H^n(G_F, M)$ can both be made into $G$-modules under the action induced by the following action on cocycles: If $a \in C^n(G, M)$, then

$$(g \cdot a)(g_1, \ldots, g_n) = g \cdot (a(g_1, \ldots, g_n))$$

for $g, g_1, \ldots, g_n \in G$, and if $a' \in C^n(G_F, M)$, then

$$(g \cdot a')(\sigma_1, \ldots, \sigma_n) = g \cdot (a'(\sigma_1, \ldots, \sigma_n)).$$

for $g \in G$ and $\sigma_0, \ldots, \sigma_n \in G$. To prove that these actions are well-defined, we must prove that for all $a \in C^n(G, M)$, $a' \in C^n(G_F, M)$, and $g \in G$: (1) $g \cdot a$ and $g \cdot a'$ are continuous; (2) if $a$ and $a'$ are cocycles, then $g \cdot a$ and $g \cdot a'$ are cocycles; and (3) if $a$ and $a'$ are coboundaries, then $g \cdot a$ and $g \cdot a'$ are coboundaries.

To prove (1), as $M$ has the discrete topology, it suffices to show that for any $m \in M$, $(g \cdot a)^{-1}(\{m\})$ is open in $G$ and $(g \cdot a')^{-1}(\{m\})$ is open in $G_F$. But

$$(g \cdot a)^{-1}(\{m\}) = a^{-1}(\{g^{-1} \cdot m\})$$

and as $a$ and $a'$ are continuous, these two latter sets are open in $G_F$, so $g \cdot a$ and $g \cdot a'$ are continuous and we are finished with (1).

(2) and (3) are immediate consequences of the fact that the coboundary maps $\partial^n : C^{n-1}(G, M) \to C^n(G, M)$ and $\partial^n : C^{n-1}(G_F, M) \to C^n(G_F, M)$ are $G$-module homomorphisms. To prove this fact, we recall that $G$ is abelian and simply compute that:

$$(g \cdot (\partial^n a))(g_1, \ldots, g_n) = g \cdot ((\partial^n a)(g_1, \ldots, g_n))$$

$$= g \cdot \left( g_1 \cdot (a(g_2, \ldots, g_n)) + \sum_{i=1}^{n-1} (-1)^i a(g_1, \ldots, g_i, g_{i+1}, g_{i+2}, \ldots, g_n) + (-1)^n a(g_1, \ldots, g_{n-1}) \right)$$

$$= (gg_1) \cdot a(g_2, \ldots, g_n) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a(g_1, \ldots, g_i, g_{i+1}, g_{i+2}, \ldots, g_n)) + (-1)^n g \cdot (a(g_1, \ldots, g_{n-1}))$$

$$= (g_1 g) \cdot a(g_2, \ldots, g_n) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a(g_1, \ldots, g_i, g_{i+1}, g_{i+2}, \ldots, g_n)) + (-1)^n g \cdot (a(g_1, \ldots, g_{n-1}))$$

$$= g_1 \cdot (g \cdot a(g_2, \ldots, g_n)) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a(g_1, \ldots, g_i, g_{i+1}, g_{i+2}, \ldots, g_n)) + (-1)^n g \cdot (a(g_1, \ldots, g_{n-1}))$$

$$= g_1 \cdot ((g \cdot a)(g_2, \ldots, g_n)) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a(g_1, \ldots, g_i, g_{i+1}, g_{i+2}, \ldots, g_n)) + (-1)^n (g \cdot a)(g_1, \ldots, g_{n-1})$$

$$= (\partial^n (g \cdot a))(g_1, \ldots, g_n)$$
\[
(g \cdot (\partial^n a')) (\sigma_1, \ldots, \sigma_n) = g \cdot ((\partial^n a') (\sigma_1, \ldots, \sigma_n))
\]

\[
= g \cdot \left( \sigma_1 \cdot (a' (\sigma_2, \ldots, \sigma_n)) + \sum_{i=1}^{n-1} (-1)^i a' (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_n) + (-1)^n a' (\sigma_1, \ldots, \sigma_{n-1}) \right)
\]

\[
= g \cdot \left( \phi(\sigma_1) \cdot (a' (\sigma_2, \ldots, \sigma_n)) + \sum_{i=1}^{n-1} (-1)^i a' (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_n) + (-1)^n a' (\sigma_1, \ldots, \sigma_{n-1}) \right)
\]

\[
= (g \cdot \phi(\sigma_1)) \cdot a' (\sigma_2, \ldots, \sigma_n) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a' (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_n)) + (-1)^n g \cdot a' (\sigma_1, \ldots, \sigma_{n-1})
\]

\[
= \phi(\sigma_1) \cdot (g \cdot a' (\sigma_2, \ldots, \sigma_n)) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a' (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_n)) + (-1)^n g \cdot a' (\sigma_1, \ldots, \sigma_{n-1})
\]

\[
= \sigma_1 \cdot ((g \cdot a') (\sigma_2, \ldots, \sigma_n)) + \sum_{i=1}^{n-1} (-1)^i (g \cdot a') (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_n) + (-1)^n (g \cdot a') (\sigma_1, \ldots, \sigma_{n-1})
\]

\[
= (\partial^n (g \cdot a')) (\sigma_1, \ldots, \sigma_n)
\]

for all \( g, h_1, \ldots, h_n \in G, \sigma_1, \ldots, \sigma_n \in G_F, a \in C^{n-1}(G, M), \) and \( a' \in C^{n-1}(G_F, M). \) Thus, \( g \cdot (\partial^n a) = \partial^n (g \cdot a) \) and \( g \cdot (\partial^n (a')) = \partial^n (g \cdot a') \), so \( \partial^n \) and \( \partial^n \) are \( G \)-module homomorphisms, so from earlier remarks we have an action of \( G \) on \( H^n(G, M) \) and \( H^n(G_F, M) \) for any \( G \)-module \( M \).

Now we examine the relationship between the groups \( H^n(G, M) \) and \( H^n(G_F, M) \) for any \( G \)-module \( M \). More specifically, note that since \( G_E \) is a closed normal subgroup of \( G_F \), we may define an inflation map:

\[
\text{infl}^G_{G/F} : H^n(G_F, G_E, M^{G_E}) \to H^n(G_F, M).
\]

This is the map descended from the map on cochains that sends \( a \in C^n(G_F, G_E, M^{G_E}) \) to:

\[
(\sigma_1, \ldots, \sigma_n) \mapsto a(\overline{\sigma}_1, \ldots, \overline{\sigma}_n).
\]

However, since \( \phi(G_E) = 1 \), \( M^{G_E} = M \). Furthermore, \( G_F/G_E \cong G \). Thus, we may regard inflation as the map:

\[
\text{infl}^G : H^n(G, M) \to H^n(G_F, M)
\]

that is descended from the map descended on cochains that sends \( a \in C^n(G, M) \) to:

\[
(\sigma_1, \ldots, \sigma_n) \mapsto a(\phi(\sigma_1), \ldots, \phi(\sigma_n)).
\]

Furthermore, this inflation map is a \( G \)-module homomorphism, as for all \( a \in C^n(G, M), g \in G, \) and \( \sigma_1, \ldots, \sigma_n \in G_F, \)

\[
(g \cdot \text{infl}(a)) (\sigma_1, \ldots, \sigma_n) = g \cdot (\text{infl}(a) (\sigma_1, \ldots, \sigma_n)) = g \cdot a(\phi(\sigma_1), \ldots, \phi(\sigma_n))
\]

Next we show that the action of \( G \) on the cohomology of \( G \) and on the cohomology of \( G_F \) is functorial. More specifically, let \( A \) and \( B \) be any two \( G \)-modules and \( f : A \to B \) a \( G \)-module homomorphism. Then \( f \) is also a \( G_F \)-module homomorphism, and we have the induced homomorphisms:

\[
f^n : H^n(G, A) \to H^n(G, B)
\]

descended from the map on cocycles that sends \( a \in C^n(G, A) \) to \( f \circ a \) and

\[
f^n : H^n(G_F, A) \to H^n(G_F, B)
\]

descended from the map on cocycles that sends \( a' \in C^n(G_F, A) \) to \( f \circ a' \). We now show that \( f^n \) is a \( G \)-module homomorphism in both cases. To this end, let \( a \in C^n(G, A), a' \in C^n(G_F, A), \)
$g, g_1, \ldots, g_n \in G$, and $\sigma_1, \ldots, \sigma_n \in G_F$ be arbitrary. Then we have:

\[
(g \cdot f^n(a)) (g_1, \ldots, g_n) = g \cdot (f^n(a)) (g_1, \ldots, g_n) = f (g \cdot (g_1, \ldots, g_n)) = (f \circ (g \cdot a)) (g_1, \ldots, g_n) = (f^n(g \cdot a)) (g_1, \ldots, g_n)
\]

and

\[
(g \cdot f^n(a')) (\sigma_1, \ldots, \sigma_n) = g \cdot (f^n(a')) (\sigma_1, \ldots, \sigma_n) = f (g \cdot a' (\sigma_1, \ldots, \sigma_n)) = (f \circ (g \cdot a')) (\sigma_1, \ldots, \sigma_n) = (f^n(g \cdot a')) (\sigma_1, \ldots, \sigma_n)
\]

Because the action of $G$ on $H^n(G, M)$ and $H^n(G, G_F)$ is functorial and because it commutes with the coboundary map, the action of $G$ must also commute with the connecting homomorphism in the long exact sequence. Furthermore, if $0 \to A \to B \to C \to 0$ is any short exact sequence of $G$-modules, then this is also a short exact sequence of $G_F$-modules under the induced action. Then since $A^{G_E} = A$, $B^{G_E} = B$, and $C^{G_E} = C$, $0 \to A^{G_E} \to B^{G_E} \to C^{G_E} \to 0$

is a short exact sequence of $G_F/G_E$-modules. This is precisely the situation in which inflation commutes with the connecting homomorphism.

We are now in a position to construct the first large commutative diagram involved in the decomposition of $H^1(G_F, V)$:

**Proposition 4.1.** (Proposition 1 of [CMS]) We have following commutative diagram of $\mathbb{F}_p[G]$-modules with exact columns:

\[
\begin{array}{ccc}
H^0(G, V/V^G) & \xrightarrow{g^0} & H^0(G_F, V/V^G) \\
\downarrow \text{infl} & & \downarrow \text{infl} \\
H^1(G, \mathbb{F}_p) & \xrightarrow{g^0} & H^0(G_F, \mathbb{F}_p[G]/V) \\
\downarrow \pi_1 & & \downarrow \pi_1 \\
H^1(G_F, V) & \xrightarrow{\delta^1} & H^1(G_F, \mathbb{F}_p[G]/V) \\
\downarrow \pi_2 & & \downarrow \pi_2 \\
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \xrightarrow{\delta^2} & H^2(G_F, \mathbb{F}_p) \\
\end{array}
\]
where the columns are derived from the long exact sequence in cohomology, the rows are derived from inflation maps, and the actions of $F_p[G]$ on the cohomology groups are as they were explained earlier.

**Proof 4.1.** Using the long exact sequence in cohomology on the following two long exact sequences of $G$ and $G_F$-modules:

$$
0 \to F_p \overset{\iota_1}{\longrightarrow} V \overset{\pi_1}{\longrightarrow} V/V^G \to 0
$$

$$
0 \to V \overset{\iota_2}{\longrightarrow} F_p[G] \overset{\pi_2}{\longrightarrow} F_p \to 0
$$

gives the following commutative diagram of $G$-modules with exact columns:

All maps in this diagram are $G$-module homomorphisms because it has already been shown that inflation, functorial maps, and connecting homomorphisms are all $G$-module homomorphisms. The diagram is commutative because inflation, in this case, commutes with connecting homomorphisms.
Therefore, to complete the proof of this proposition, it suffices to do the following: (1) Prove that \( H^0(G, M) = H^0(G_F, M) \) for all \( G \)-modules \( M \). (2) Prove that the maps: the maps:
\[
\begin{align*}
H^0(G, V) &\to H^0(G, V/V^G) & H^0(G, V) &\to H^0(G_F, V/V^G) \\
H^0(G, \mathbb{F}_p[G]) &\to H^0(G, \mathbb{F}_p) & H^0(G_F, \mathbb{F}_p[G]) &\to H^0(G_F, \mathbb{F}_p)
\end{align*}
\]
in the long exact sequence in cohomology are the zero maps. (3) Prove that inflation is always the identity on 0-cohomology and always injective on 1-cohomology. (4) Prove that for all \( m \geq 0 \):
\[
H^m(G_F, V/V^G) \cong (V/V^G) \otimes_{\mathbb{F}_p} H^m(G, \mathbb{F}_p)
\]
as \( \mathbb{F}_p[G] \)-modules.

(1): Recall that for any profinite group \( H \) and \( H \)-module \( M \), \( Z^0(H, M) = M^H \) and \( B^0(H, M) = 0 \). Therefore, \( H^0(H, M) = M^H/\{0\} \). Thus:
\[
H^0(G, M) = M^{G_F}/\{0\} = \{m \in M| \phi(\sigma)m = m \text{ for all } \sigma \in G_F\}/\{0\}.
\]
Since \( \phi : G_F \to G \) is surjective, this last set is equal to:
\[
\{m \in M| gm = m \text{ for all } g \in G\}/\{0\} = M^G/\{0\} = H^0(G, M),
\]
and we are done with the proof of (1).

(2): The maps:
\[
\begin{align*}
V^G/\{0\} &\to H^0(G, V) \to H^0(G, V/V^G) = (V/V^G)^G/\{0\} \\
V^G/\{0\} &\to H^0(G_F, V) \to H^0(G_F, V/V^G) = (V/V^G)^G/\{0\} \\
(\mathbb{F}_p[G])^G/\{0\} &\to H^0(G, \mathbb{F}_p[G]) \to H^0(G, \mathbb{F}_p[G]/V) = (\mathbb{F}_p[G]/V)^G/\{0\} \\
(\mathbb{F}_p[G])^G/\{0\} &\to H^0(G_F, \mathbb{F}_p[G]) \to H^0(G_F, \mathbb{F}_p[G]/V) = (\mathbb{F}_p[G]/V)^G/\{0\}
\end{align*}
\]
are descended from restrictions of \( \pi_1, \pi_1, \pi_2, \) and \( \pi_2 \), respectively. Now, \( V^G = \langle z \rangle \), and \( \pi_1(z) = 0 \). Similarly, \( (\mathbb{F}_p[G])^G = \langle z \rangle \) and \( \pi_2(z) = 0 \). Therefore, the maps in question are the zero maps, as desired, and we are done with the proof of (2).

(3): We now prove that inflation from \( H^0(G, M) = M^G/\{0\} \) to \( H^0(G_F, M) = M^{G_F} = M^G/\{0\} \) is the identity. To this end, let \( m \in C^0(G, M) = M \) be arbitrary. Then \( \text{infl}_m \) is \( m \) by definition, so inflation is the identity map on cochains, so it is the identity on cohomology.

Injectivity of the inflation map from \( H^1(G, M) \to H^1(G_F, M) \) can be seen from the existence of a standard exact sequence, sometimes called the five-term exact sequence or the inflation-restriction-transgression sequence, of the following form:
\[
0 \to H^1(H/K, A^H) \xrightarrow{\text{infl}} H^1(H, A) \to H^1(K, A)^{K/H} \to H^2(H/K, A^H) \xrightarrow{\text{infl}} H^2(H, A)
\]
for any profinite group \( H \), closed normal subgroup \( K \) of \( H \), and any \( H \)-module \( A \). It is stated more precisely and proved as Proposition 3.3.14 of [GS] and as Proposition 1.6.6 of [NSW].

However, we will prove this fact directly, i.e. we prove that only elements of \( B^1(G, M) \) are sent to \( B^1(G_F, M) \) by infl. To this end, let \( a \in C^1(G, M) \) be such that \( \text{infl}_a \in B^1(G_F, M) \). Then by the 1-coboundary condition there is an element \( m \in M \) such that:
\[
a(\phi(\sigma)) = \text{infl}_a(\sigma) = \sigma \cdot m - m = \phi(\sigma)m - m
\]
for all \( \sigma \in G_F \). Fix a \( g \in G \) and let \( \bar{g} \) be in \( \phi^{-1}(\{g\}) \). Then:
\[
a(g) = a(\phi(\bar{g})) = \phi(\bar{g})m - m = gm - m.
\]
Thus, there is an \( m \in M \) such that for all \( g \in G \),
\[
a(g) = gm - m,
\]
and this is exactly what it means for \( a \) to be in \( B^1(G, M) \). Thus, (3) is proved.
(4): We have the following chain of group-isomorphisms from functoriality of homology and tensor products with respect to finite direct sums, the fact that an $F_p$-module is an abelian group with exponent $p$, and that $V/V^G \cong F_p^n$ as a $G$-module:

$$H^m(G,F,V/V^G) \cong H^m(G,F_p^n) \cong (H^m(G,F,F_p))^n \cong F_p \otimes_{F_p} H^m(G,F,F_p) \cong (V/V^G) \otimes_{F_p} H^m(G,F,F_p).$$

To state what the isomorphism is, we note that any $a' \in C^m(G,F,V/V^G)$ can be written in the form:

$$\sum_{i=1}^n c'_i \bar{b}_i$$

for $c'_1, \ldots, c'_n \in C^m(G,F,F_p)$. This is because for each $1 \leq i \leq n$, we let $p_i : V/V^G \to \langle \bar{b}_i \rangle$ be projections corresponding to the direct-sum decomposition $V/V^G = \langle \bar{b}_1 \rangle \oplus \cdots \oplus \langle \bar{b}_n \rangle$, then we may set $c'_i = p_i \circ a'$. Thus, the forward isomorphism $\kappa$ is the one induced by the following map from $C^m(G,F,V/V^G)$ to $(V/V^G) \otimes_{F_p} C^m(G,F,F_p)$:

$$\sum_{i=1}^n c'_i \bar{b}_i \mapsto \sum_{i=1}^n \bar{b}_i \otimes c'_i.$$

Its inverse is induced by the map from $(V/V^G) \otimes_{F_p} C^m(G,F,F_p)$ to $C^m(G,F,V/V^G)$ defined by sending the pure tensor $\bar{b}_i \otimes a'$ to the cochain $a' \bar{b}_i$ for each $1 \leq i \leq n$ and all $a' \in C^m(G,F,F_p)$.

Next, $(V/V^G) \otimes_{F_p} H^m(G,F,F_p)$ is naturally an $F_p[G]$-module under the action induced by the following action on pure tensors:

$$g \cdot (v \otimes a') = (g \cdot v) \otimes (g \cdot a') = v \otimes (g \cdot a')$$

for $g \in G$, $v \in V/V^G$, and $a' \in C^m(G,F,F_p)$. We now prove that the group isomorphism

$$\lambda : H^m(G,F,V/V^G) \cong (V/V^G) \otimes_{F_p} H^m(G,F,F_p)$$

written above is an isomorphism of $F_p[G]$-modules. But this is true because each of these two groups is a trivial $G$-modules, and we have proved all parts of (4).

We have proved (1) through (4), so by earlier remarks we are finished with the proof of Proposition 4.1. QED

Now that we are armed with this commutative diagram, we now prove a host of lemmas giving properties of the various homomorphisms in the commutative diagram. The eventual aim is to decompose $H^1(G,F,V)$ and map this decomposition into $H^1(G,F,F_p[G])$ via $\iota_2^*$, so most of these lemmas and computations are related to maps to and from these two groups. For this reason we define $R$ to be $\ker(\iota_2^*)$, and we have the first such lemma:

**Lemma 4.2.** (Corollary to Proposition 1 of [CMS]) Let $S$ be an $F_p[G]$-submodule of $H^1(G,F,V)$. Then

$$\iota_1^*(S) \subseteq \pi_1^*(R)$$

if and only if

$$\iota_2^*(S) \subseteq \iota_2^* \pi_1^*(H^1(G,F,F_p)).$$

**Proof 4.2.** $\Rightarrow$: Assume $\pi_1^*(S) \subseteq \pi_1^*(R)$. Let $s \in S$ be arbitrary. Then there is an $r \in R = \ker(\iota_2^*)$ such that $\pi_1^*(s) = \pi_1^*(r)$, so $s - r \in \ker(\iota_1^*) = \im(\iota_2^*)$. Thus, there is an $a' \in H^1(G,F,F_p)$ such that $s - r = \iota_1^*(a')$. Therefore,

$$\iota_2^*(s) = \iota_2^*(r + \iota_1^*(a')) = 0 + \iota_2^* \iota_1^*(a') \in \iota_2^* \pi_1^*(H^1(G,F,F_p)).$$

$\Leftarrow$: Assume $\iota_2^*(S) \subseteq \iota_2^* \pi_1^*(H^1(G,F,F_p))$. Let $s \in S$ be arbitrary. Then there is an $a' \in H^1(G,F,F_p)$ such that $\iota_2^*(s) = \iota_2^* \iota_1^*(a')$. Thus, $s - \iota_1^*(a') \in \ker(\iota_2^*) = R$. Let $r = s - \iota_1^*(a')$. Then:

$$\pi_1^*(s) = \pi_1^*(r + \iota_1^*(a')) = \pi_1^*(r) + 0 \in \pi_1^*(R).$$
QED

We now define:

$$\mathcal{A} = \text{im}(\delta^0).$$

While this definition may seem strange and unmotivated, \(\mathcal{A}\) has a natural interpretation in terms of fields. By Proposition 4.1,

$$\mathcal{A} = \inf(\delta^0(H^0(G, V/V^G))).$$

We use the standard definition of the connecting homomorphism to compute \(\delta^0\) of elements of \(H^0(G, V/V^G) = (V/V^G)^G/\{0\} = (V/V^G)/\{0\}\).

To this end, let \(1 \leq i \leq n\) be arbitrary, so that \(\overline{b}_i\) is an arbitrary basis element of \(Z^0(G, V/V^G) = (V/V^G)^G = V/V^G\). Note that \(b_i\) is an element of \(C^0(G, V) = V\) and \(\pi^*_i(b_i) = \pi_1(b_i) = \overline{b}_i\). Next, \(\partial^1(b_i)\) is the map:

$$g \mapsto g \cdot b_i - b_i = (g - 1)b_i$$

in \(Z^1(G, V)\), where \(g - 1\) is interpreted as an element of \(\mathbb{F}_p[G]\).

We claim that \(\partial^1(b_i)\) is a group homomorphism, i.e. for all \(g_1, g_2 \in G\):

$$(g_1 g_2 - 1)b_i = (g_1 - 1)b_i + (g_2 - 1)b_i.$$ 

Note that the previous condition is equivalent to:

$$(g_1 - 1)(g_2 - 1)b_i = 0$$

for all \(g_1, g_2 \in G\). To prove this fact, we note that for any \(g = \tau_1^{a_1} \cdots \tau_n^{a_n} \in G\), \(g - 1 \in \mathbb{F}_p[G]\) has zero as its constant term when written as a polynomial in \(\rho_1, \ldots, \rho_n\). This is because the constant term of \(g - 1\) is the value obtained when one substitutes \(\rho_1 = \cdots = \rho_n = 0\). But substituting \(\rho_1 = \cdots = \rho_n = 0\) causes \(\tau_1 = \cdots = \tau_n = 1\), so that the constant term of \(g - 1\) is \(1^{a_1} \cdots 1^{a_n} - 1 = 0\), as was claimed. Thus, for any \(g_2 \in G\), \((g_2 - 1)b_i\) will be a scalar multiple of \(z\), and multiplying such a scalar multiple of \(z\) by \((g_1 - 1)\) for any \(g_1 \in G\) will give 0. Thus,

$$(g_1 - 1)(g_2 - 1)b_i = 0$$

for all \(g_1, g_2 \in G\) and therefore \(\partial^1(b_i)\) is a group homomorphism, as was claimed.

Next, note that for any \(1 \leq j \leq n\),

$$(\partial^1(b_i))(\tau_j) = (\tau_j - 1)b_i = \rho_j b_i = \delta^0_{ij} z,$$

where \(\delta^0_{ij}\) is the Kronecker delta. Thus, if we let \(v_i\) be the element of the dual \(\mathbb{F}_p\)-vector space \(G^* = \text{Hom}_{\text{cont}}(G, \mathbb{F}_p) = Z^1(G, \mathbb{F}_p)\) that corresponds to \(\tau_i\) in the \(\mathbb{F}_p\)-basis \(\{\tau_1, \ldots, \tau_n\}\), then \(\partial^1(b_i) = v_i z\).

Furthermore, \(v_i^*(v_i) = \partial^1(b_i)\), so \(\delta^0\) sends the class of \(\overline{b}_i\) in \(H^0(G, V/V^G)\) to the class of \(\tau_i\) in \(H^1(G, \mathbb{F}_p)\).

Thus,

$$\delta^0(H^0(G, V/V^G)) = \langle v_1, \ldots, v_n \rangle \subseteq H^1(G, \mathbb{F}_p).$$

Thus, if for each \(1 \leq i \leq n\) we let \(v'_i = \inf(v_i) \in H^1(G_F, \mathbb{F}_p)\), we have that:

$$\mathcal{A} = \langle v'_1, \ldots, v'_n \rangle H^1(G_F, \mathbb{F}_p).$$

Furthermore, since \(\{v'_1, \ldots, v'_n\}\) is the image of the basis \(\{\overline{b}_1, \ldots, \overline{b}_n\}\) of \(H^0(G_F, V/V^G)\) under the injective mapping \(\inf \circ \delta^0\), \(\{v'_1, \ldots, v'_n\}\) is a basis of \(\mathcal{A}\).

**Lemma 4.3.** (Lemma 1 of [CMS]) \(\pi^*_1\) maps \(R\) injectively into \((V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A}\). Its precise image is:

$$\langle \overline{b}_i \otimes v'_j + \overline{b}_j \otimes v'_i \rangle_{1 \leq i < j \leq n}.$$ 

if \(p = 2\) and is:

$$\langle \overline{b}_i \otimes v'_j + \overline{b}_j \otimes v'_i \rangle_{1 \leq i < j \leq n} + \langle \overline{b}_i \otimes v'_i \rangle_{1 \leq i \leq n}$$

if \(p \geq 3\).
Proof 4.3. Because \( R = \ker(\iota_2) = \im(\delta^1) = \im(\infl \circ \delta^1) \), it suffices to directly compute the image of:

\[
\pi_i^* \circ \infl \circ \delta^1 : H^0(G, \mathbb{F}_p[G]/V) \to (V/VG) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p)
\]

and prove it is injective.

To this end, we have that \( H^0(G, \mathbb{F}_p[G]/V) = (\mathbb{F}_p[G]/V)^G/\{0\} \). Now, for each \( 1 \leq i < j \leq n \), let:

\[
c_{ij} = \rho_1^{p-1} \cdots \rho_{i-1}^{p-i} \rho_i \cdots \rho_{j-1}^{p-j} \rho_j \cdots \rho_n^{p-1} \in \mathbb{F}_p[G].
\]

Furthermore, if \( p \geq 3 \), then for each \( 1 \leq i \leq n \), let:

\[
d_i = \rho_1^{p-1} \cdots \rho_{i-1}^{p-i} \rho_i \cdots \rho_{n}^{p-n} \in \mathbb{F}_p[G],
\]

and otherwise let \( d_i = 0 \). We then have that:

\[
(\mathbb{F}_p[G]/V)^G = \langle \overline{c_{ij}} \rangle_{1 \leq i < j \leq n} \oplus \langle \overline{d_i} \rangle_{1 \leq i \leq n}.
\]

We now use the standard definition of the connecting homomorphism to compute \( \pi_i^* \circ \infl \circ \delta^1 \) of the class of \( \overline{c_{ij}} \) in \( H^0(G, \mathbb{F}_p[G]/V) \). Note that \( c_{ij} \in \mathbb{F}_p[G] = Z^0(G, \mathbb{F}_p[G]) \) is mapped to \( \overline{c_{ij}} \in (\mathbb{F}_p[G]/V)^G = Z^0(G, \mathbb{F}_p[G]/V) \). Next, \( \partial^i(c_{ij}) \) is the map:

\[
g \mapsto g \cdot c_{ij} - c_{ij} = (g - 1)c_{ij}
\]

in \( Z^0(G, \mathbb{F}_p[G]) \), where \( g - 1 \) is considered as an element of \( \mathbb{F}_p[G] \). Then:

\[
(\partial^1 c_{ij}) = \alpha_1 c_{ij} + \alpha_i b_i + \alpha_j b_j + \alpha_{ij} z,
\]

where \( \alpha_1, \alpha_i, \alpha_j, \alpha_{ij} \in C^1(G, \mathbb{F}_p) \) are the maps that send \( g \) to the coefficients of \( 1, \rho_i, \rho_j, \) and \( \rho_i \rho_j \), respectively, when \( g - 1 \) is written as a polynomial in \( \rho_1, \ldots, \rho_n \). Recall from earlier that \( \alpha_1 = 0 \). Then:

\[
(\partial^1 c_{ij}) = \alpha_j b_i + \alpha_i b_j + \alpha_{ij} z \in Z^0(G, V),
\]

so that \( \delta^1 \) sends the class of \( c_{ij} \) in \( H^0(G, \mathbb{F}_p[G]/V) \) to the class of:

\[
\alpha_j b_i + \alpha_i b_j + \alpha_{ij} z
\]

in \( H^1(G, V) \).

Next, \( \infl(\alpha_j b_i + \alpha_i b_j + \alpha_{ij} z) = \alpha_j' b_i + \alpha_i' b_j + \alpha_{ij}' z \in Z^1(G, F, V) \), where \( \alpha_j', \alpha_i', \alpha_{ij}' \in C^1(G, F, p) \) are the inflations of \( \alpha_j, \alpha_i, \) and \( \alpha_{ij} \), respectively. Finally, \( \pi^*_i \circ \infl \circ \delta^1(c_{ij}) \) is to find the function \( \alpha_i \) for each \( 1 \leq i \leq n \). But \( \alpha_i(g) = \frac{\partial}{\partial p_i}(g - 1) \) evaluated at \( \rho_1 = \ldots = \rho_n = 0 \). Now, \( \nabla^1 \equiv (\partial_1^{a_1} \cdots \partial_n^{a_n} - 1) = \frac{\partial}{\partial p_i}((\rho_1 + 1)^{a_1} \cdots (\rho_n + 1)^{a_n} - 1) \)

and evaluating this at \( \rho_1 = \ldots = \rho_j = 0 \) gives \( a_j \). Thus, \( \alpha_i(g) = a_i \), and thus \( \alpha_i = v_i \). Therefore, \( \pi^*_i \circ \infl \circ \delta^1 \) sends the class of \( \overline{c_{ij}} \) in \( H^1(G, \mathbb{F}_p[G]/V) \) to:

\[
\overline{\alpha_j b_i} + \overline{\alpha_i b_j} + \overline{\alpha_{ij} z} \in (V/VG) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p).
\]

Similarly, if \( p \geq 3 \), we compute \( \pi^*_i \circ \infl \circ \delta^1 \) of the class of \( \overline{d_i} \) in \( H^0(G, \mathbb{F}_p[G]/V) \). Note that \( d_i \in \mathbb{F}_p[G] = Z^0(G, \mathbb{F}_p[G]) \) is mapped to \( \overline{d_i} \in (\mathbb{F}_p[G]/V)^G = Z^0(G, \mathbb{F}_p[G]/V) \). Next, \( \partial^i(d_i) \) is the map:

\[
g \mapsto (g - 1)d_i = \alpha_1 d_i + \alpha_i b_i + \alpha_{ii} z = \alpha_i b_i + \alpha_{ii} z,
\]

73
where \( \alpha_i, \alpha_{ii} \in C^1(G, \mathbb{F}_p) \) are the maps that send \( g \) to the coefficients of \( \rho_i \) and \( \rho_i^2 \), respectively, when \( g - 1 \) is written as a polynomial in \( \rho_1, \ldots, \rho_n \). Thus, \( \delta^1 \) sends the class of \( d_i \) in \( H^0(G, \mathbb{F}_p[G]/V) \) to the class of:

\[
\alpha_i b_i + \alpha_{ii} z
\]
in \( H^1(G, V) \).

Next,

\[
\text{infl}(\alpha_i b_i + \alpha_{ii} z) = \alpha_i' b_i + \alpha_{ii}' z \in \mathbb{Z}^1(G, V),
\]

where \( \alpha_i', \alpha_{ii}' \in C^1(G, \mathbb{F}_p) \) are the inflations of \( \alpha_i \) and \( \alpha_{ii} \), respectively. Finally,

\[
\pi^*_i \circ \text{infl}(\alpha_i b_i + \alpha_{ii} z) = \overline{b_i} \otimes \alpha_i' \in (V/VG) \otimes_{\mathbb{F}_p} Z^1(G, \mathbb{F}_p).
\]

Therefore, \( \pi^*_i \circ \text{infl} \circ \delta^1 \) sends the class of \( d_i \) in \( H^1(G, \mathbb{F}_p[G]/V) \) to:

\[
\overline{b_i} \otimes \overline{\kappa_i} \in (V/VG) \otimes_{\mathbb{F}_p} H^1(G, \mathbb{F}_p).
\]

Therefore, the image of \( R \) under \( \pi^*_i \) is what the lemma says it is. Next, note that since \( \{v_1, \ldots, v_n\} \) is a basis for \( H^1(G, \mathbb{F}_p) \) and \( \text{infl} : H^1(G, \mathbb{F}_p) \rightarrow H^1(G, \mathbb{F}_p) \) is injective, \( \{\overline{v}_1, \ldots, \overline{v}_n\} \) is linearly independent over \( H^1(G, \mathbb{F}_p) \). Therefore, the sets:

\[
\{\overline{b_i} \otimes \overline{v}_j + \overline{b_j} \otimes \overline{v}_i | 1 \leq i < j \leq n\}
\]

and

\[
\{\overline{b_i} \otimes \overline{v}_j + \overline{b_j} \otimes \overline{v}_i | 1 \leq i < j \leq n\} \cup \{\overline{b_i} \otimes \overline{v}_i | 1 \leq i \leq n\}
\]

are linearly independent over \( (V/VG) \otimes_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) \). Thus, since \( \pi^*_i \circ \text{infl} \circ \delta^1 \) sends a basis of \( H^0(G, \mathbb{F}_p[G]/V) \) to a linearly independent set, \( \pi^*_i \circ \text{infl} \circ \delta^1 \) is injective, so \( \pi^*_i \) is injective on \( R \), as desired. QED

**Lemma 4.4.** (Lemma 2 of [CMS]) The following diagram is commutative:

\[
\begin{array}{ccc}
H^1(G, V) & \rightarrow & (V/VG) \otimes_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) \\
\pi^*_i & & \downarrow_{1 \otimes \iota^*_i} \\
& & (V/VG) \otimes_{\mathbb{F}_p} H^1(G, V).
\end{array}
\]

**Proof 4.4.** We will prove this at the level of cochains. To this end, let \( a' = c'_0 z + \sum_{j=1}^n c'_j b_j \) for \( c'_0, \ldots, c'_n \in C^1(G, \mathbb{F}_p) \). Then:

\[
\pi^*_i(a') = \sum_{j=1}^n \overline{b}_j \otimes c'_j,
\]

and applying \( 1 \otimes \iota^*_i \) to this gives:

\[
\sum_{j=1}^n \overline{b}_j \otimes \iota^*_i(c'_j) = \sum_{j=1}^n \overline{b}_j \otimes (c'_j z).
\]

On the other hand,

\[
\sum_{i=1}^n \overline{b}_i \otimes (\rho_i \cdot a') = \sum_{i=1}^n \overline{b}_i \otimes \left( \rho_i \cdot \left( c'_0 z + \sum_{j=1}^n c'_j b_j \right) \right) = \sum_{i=1}^n \overline{b}_i \otimes (c'_i z).
\]

Therefore, the diagram commutes, as desired. QED

**Lemma 4.5.** (Lemma 3 of [CMS]) \( \ker(\iota^*_2 \circ \iota^*_1) = \mathcal{A} \).

**Proof 4.5.** From Proposition 4.1, \( \ker(\iota^*_1) = \text{im}(\delta^0) = \mathcal{A} \). For this reason, if we prove that \( \iota^*_2 \) is injective on \( \text{im}(\iota^*_1) = \ker(\pi^*_1) \), we will be done. To this end, note that from Lemma 4.3, \( \pi^*_1 \) is injective on \( R = \ker(\iota^*_2) \). Therefore, \( \text{im}(\iota^*_1) \cap \ker(\iota^*_2) = \{0\} \), so \( \iota^*_2 \) is injective on \( \text{im}(\iota^*_1) \), as desired. QED
The rest of this section is devoted decomposing \( H^1(G_F, V) \) as was stated in the introduction. More specifically, we prove that for all \( \mathbb{F}_2[G] \)-submodules \( P, Q, \) and \( Q' \) of \( H^1(G_F, V) \) that can result from a certain construction,

\[
H^1(G_F, V) = P \oplus Q \oplus Q' \oplus R,
\]

\( R \) has already been defined; it is \( \ker(\iota_2^*) \). We now outline what sorts of modules \( P \) and \( Q \) may be.

As a starting point we find from Proposition 4.1 and Lemma 4.3 that:

\[
\pi_1^*(R) \subseteq \left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \cap \ker(\delta^2).
\]

Thus, we have the following filtration of the \( F \)-module \( \pi_1^*(R) \subseteq \left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \cap \ker(\delta^2) \). Note also that as \( \mathbb{F}_p \)-vector spaces \( T_P \) and \( T_Q \) and define the \( \mathbb{F}_p[G] \)-module \( T_R \) as follows:

\[
T_R = \pi_1^*(R)
\]

\[
T_Q \oplus T_R = \left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \cap \ker(\delta^2)
\]

\[
T_P \oplus T_Q \oplus T_R = \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \right) \cap \ker(\delta^2).
\]

Recalling that \( V/V^G \) and \( \mathbb{F}_p \) are both trivial \( \mathbb{F}_p[G] \)-modules, we have that \( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \) is a trivial module, as well. Therefore, \( T_P, T_Q, \) and \( T_R \) are automatically \( \mathbb{F}_p[G] \)-submodules of \( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \). Note also that as

\[
\dim_{\mathbb{F}_p} \left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) = \left( \dim_{\mathbb{F}_p} \left( V/V^G \right) \right) \left( \dim_{\mathbb{F}_p} A \right) = n \cdot n = n^2,
\]

\( T_Q \) and \( T_R \) are each finite-dimensional. In fact, their dimensions cannot sum to more than \( n^2 \).

As \( T_P \oplus T_Q \oplus T_R \subseteq \ker(\delta^2) = \im(\pi_1^*) \), we can pick \( \mathbb{F}_p \)-subspaces \( \tilde{P} \) and \( \tilde{Q} \) of \( H^1(G_F, V) \) such that \( \pi_1^* \) maps \( \tilde{P} \) and \( \tilde{Q} \) isomorphically onto \( T_P \) and \( T_Q \), respectively. Now let \( P \) and \( Q \) be the \( \mathbb{F}_p[G] \)-submodules of \( H^1(G_F, V) \) that are generated by \( \tilde{P} \) and \( \tilde{Q} \). Then because \( \rho_i \rho_j \) annihilates \( V \) and therefore \( H^1(G_F, V) \), for any \( 1 \leq i \leq j \leq n \), we have that:

\[
P = \tilde{P} + \sum_{i=1}^{n} \rho_i \tilde{P} \quad \text{and} \quad Q = \tilde{Q} + \sum_{i=1}^{n} \rho_i \tilde{Q}.
\]

Now that we have constructed \( P, Q, \) and \( R \), we can prove that they satisfy the following properties:

**Lemma 4.6.** (Lemma 7 of [CMS].) For any modules \( P, Q, \) and \( R \) as previously defined

1. \( Q \) and \( R \) are trivial \( \mathbb{F}_p[G] \)-modules.
2. \( P + Q + R = P \oplus Q \oplus R \).
3. \( \pi_1^*(P + Q + R) = \pi_1^*(P) \oplus \pi_1^*(Q) \oplus \pi_1^*(R) = \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \right) \cap \ker(\delta^2) \).
4. \( \pi_1^* \) maps \( Q \oplus R \) injectively into \( (V/V^G) \otimes_{\mathbb{F}_p} A \).
5. \( P^G = \sum_{i=1}^{n} \rho_i \cdot \tilde{P} = P \cap \ker(\pi_1^*) \subseteq \im(\iota_1^*) \).

**Proof.** 4.6. We will eventually prove every item listed in the statement of the lemma, but we will do this out of order. Namely, we will prove them in the order (1), (4), (3), (5), and finally (2).

(1): Let \( x \in Q + R \) be arbitrary. Then for some \( q_0, \ldots, q_n \in \tilde{Q} \) and \( r \in R \), we have:

\[
x = q_0 + \left( \sum_{i=1}^{n} \rho_i \cdot q_i \right) + r.
\]
Thus, as $\pi_1^*$ is a $G$-module homomorphism and $\pi_1^*$ maps $\hat{Q}$ and $\hat{R}$ into the trivial $\mathbb{F}_p[G]$-modules $T_Q$ and $T_R$, we have that:

$$\pi_1^*(x) = \pi_1^*(q_0) + \left( \sum_{i=1}^n \rho_i \cdot \pi_1^*(q_i) \right) + \pi_1^*(r) = \pi_1^*(q_0) + \left( \sum_{i=1}^n \pi_1^*(q_i) \right) + \pi_1^*(r) \subseteq T_Q \oplus T_R \subseteq (V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A}.$$ 

As $\ker(\iota_1^*) = \operatorname{im}(\delta^0) = \mathcal{A}$, we have that

$$(1 \otimes \iota_1^*) \circ \pi_1^*(x) = 0.$$ 

Then by using the commutative diagram from Lemma 4.4, we have that:

$$\sum_{i=1}^n \overline{b}_i \otimes (\rho_i \cdot x) \in (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p)$$

is also 0. As $\{\overline{b}_1, \ldots, \overline{b}_n\}$ is a basis for $V/V^G$, this means that $\rho_1 \cdot x = \cdots = \rho_n \cdot x = 0$. As $x \in Q + R$ was arbitrary, this means that

$$\rho_1 \cdot Q = \cdots = \rho_n \cdot Q = \rho_1 \cdot R = \cdots = \rho_n \cdot R = \{0\},$$

and this is precisely what it means for $Q$ and $R$ to be trivial $\mathbb{F}_p[G]$-modules, as desired.

(4): In order for statement (4) to be meaningful, we must first prove that $Q + R = Q \oplus R$. To this end, since $Q$ is a trivial module and $\hat{Q}$ is an $\mathbb{F}_p$-subspace of $Q$, we must have that $\rho_1 \hat{Q} = \cdots = \rho_n \hat{Q} = \{0\}$. Thus, $Q = \hat{Q}$, so that $\pi_1^*$ maps $Q$ isomorphically onto $T_Q$. By Lemma 1, $\pi_1^*$ is injective on $R$, so $\pi_1^*$ maps $R$ isomorphically onto $\pi_1^*(R) = T_R$. Thus, $\pi_1^*(Q \cap R) \subseteq T_Q \cap T_R = \{0\}$, and since $\pi_1^*$ is injective on $Q$, $Q \cap R = 0$. Thus, $Q + R = Q \oplus R$, and $\pi_1^*$ maps $Q \oplus R$ injectively into $T_Q \oplus T_R \subseteq (V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A}$, as desired.

(3): In order for statement (3) to be meaningful, we must prove that

$$\pi_1^*(P) + \pi_1^*(Q) + \pi_1^*(R) = \pi_1^*(P) \oplus \pi_1^*(Q) \oplus \pi_1^*(R).$$

To this end, since we already have that $\pi_1^*(Q) = T_Q$ and $\pi_1^*(R) = T_R$, we set about proving that $\pi_1^*(P) = \pi_1^*(\hat{P})$; as $\pi_1^*(\hat{P}) = T_P$ and $T_P + T_Q + T_R = T_P \oplus T_Q \oplus T_R$, this will give $\pi_1^*(P) + \pi_1^*(Q) + \pi_1^*(R) = \pi_1^*(P) \oplus \pi_1^*(Q) \oplus \pi_1^*(R)$.

To this end, we let $p \in \hat{P}$ be arbitrary. Then since $\pi_1^*$ is a $G$-module homomorphism and $\pi_1^*$ maps $\hat{P}$ into the trivial $\mathbb{F}_p[G]$-module $T_P$,

$$\pi_1^*(\rho_i \cdot p) = \rho_i \cdot \pi_1^*(p) = 0$$

for all $1 \leq i \leq n$. Thus,

$$\pi_1^*(P) = \pi_1^* \left( \hat{P} + \sum_{i=1}^n \rho_i \cdot \hat{P} \right) = \pi_1^*(\hat{P}) + \sum_{i=1}^n \{0\} = \pi_1^*(\hat{P}),$$

and from earlier remarks, we have shown that $\pi_1^*(P) + \pi_1^*(Q) + \pi_1^*(R) = \pi_1^*(P) \oplus \pi_1^*(Q) \oplus \pi_1^*(R)$, as is needed. Furthermore, as

$$\pi_1^*(P + Q + R) = \pi_1^*(P) + \pi_1^*(Q) + \pi_1^*(R)$$

and

$$\pi_1^*(P) \oplus \pi_1^*(Q) \oplus \pi_1^*(R) = T_P \oplus T_Q \oplus T_R = \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \right) \cap \ker(\delta^2),$$

this last equality proves all parts of (3).

(5): As $\ker(\pi_1^*) = \operatorname{im}(\iota_1^*)$ by the diagram of Proposition 4.1, the inclusion $P \cap \ker(\pi_1^*) \subseteq \operatorname{im}(\iota_1^*)$ is clear.

Because $P = \hat{P} + \sum_{i=1}^n \rho_i \cdot \hat{P}$, in order to show that $P^G = \sum_{i=1}^n \rho_i \cdot \hat{P}$, it suffices to show that $P^G \cap \hat{P} = \{0\}$ and $\sum_{i=1}^n \rho_i \cdot \hat{P} \subseteq P^G$. To this end, suppose that $p \in \hat{P}$ is nonzero. Then by definition
of \( \tilde{P} \), \( \pi_1^*(p) \) is a nonzero element of \( T_P \), so it does not lie in \( (V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A} \). Because the kernel of \( \operatorname{ker}(\iota_1) = \operatorname{im}(\delta^0) = \mathcal{A} \), the kernel of:

\[
1 \otimes \iota_1^* : (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \to (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, V)
\]

is \( (V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A} \). Therefore,

\[
((1 \otimes \iota_1) \circ \pi_1^*) (p) \neq 0.
\]

Then by using the commutative diagram from Lemma 4.4, we have that:

\[
\sum_{i=1}^n \tilde{b}_i \otimes (\rho_i \cdot p) \in (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p)
\]

is also nonzero. This means that at least one of \( \rho_1 \cdot p, \ldots, \rho_n \cdot p \) is nonzero, so that \( p \notin P^G \). This proves that \( P^G \cap \tilde{P} = \{0\} \).

Now suppose that \( p \in \tilde{P} \) is arbitrary. Then for any \( 1 \leq i \leq n, 1 \leq j \leq n, \rho_i \rho_j \) annihilates every element of \( V \), so \( \rho_i \rho_j \) also annihilates every element of \( H^1(G_F, V) \). In particular,

\[
(\rho_i \rho_j) \cdot p = \rho_i \cdot (\rho_j \cdot p) = 0.
\]

Therefore, \( \rho_1 \cdot p, \ldots, \rho_n \cdot p \in P^G \), so \( \sum_{i=1}^n (\rho_i \cdot \tilde{P}) \subseteq P^G \), and by earlier remarks we have proved that \( P^G = \sum_{i=1}^n \rho_i \cdot \tilde{P} \), as desired.

Similarly, in order to show that \( P \cap \ker(\pi_1) = \sum_{i=1}^n (\rho_i \cdot \tilde{P}) \), it suffices to show that \( P \cap \ker(\pi_1) = \{0\} \) and \( \sum_{i=1}^n (\rho_i \cdot \tilde{P}) \subseteq \ker(\pi_1) \). However, \( \pi_1^* \) is injective on \( \tilde{P} \) by definition of \( \tilde{P} \), so \( \tilde{P} \cap \ker(\pi_1) = \{0\} \). Furthermore, since \( \pi_1^* \) is a \( G \)-module homomorphism and \( \pi_1^* \) maps \( \tilde{P} \) into the trivial \( \mathbb{F}_p[G] \)-module \( T_P \), we have that for all \( 1 \leq i \leq n \):

\[
\pi_1^*(\rho_i \cdot \tilde{P}) \subseteq \rho_i \cdot \pi_1^*(\tilde{P}) = \rho_i \cdot T_P = \{0\}.
\]

Thus, \( \sum_{i=1}^n (\rho_i \cdot \tilde{P}) \subseteq \ker(\pi_1) \), and from earlier remarks we have proved all parts of (5).

(2): We intend to use the exclusion lemma to prove (2). To this end, suppose that \( x \in P^G \cap (Q+R) \) is arbitrary. Then from (5) and the fact that \( x \in P^G, \pi_1^*(x) = 0 \). However, since \( \pi_1^* \) is injective on \( Q+R \) by (4), this means that \( x = 0 \). Therefore, \( P^G \cap (Q+R) = \{0\} \), so \( P^G + (Q+R) = P^G \oplus (Q+R) \). But since \( Q \) and \( R \) are trivial modules, we have that \( Q + R = Q \oplus R = Q^G \oplus R^G \). Therefore, we have \( P^G + Q^G + R^G = P^G \oplus Q^G \oplus R^G \), and by the Exclusion Lemma we have \( P + Q + R = P \oplus Q \oplus R \), as desired.

We have proved (1) through (5), and so we are done with the proof of Lemma 4.6. QED

Next we construct \( Q' \). By Lemma 4.6(5), \( P^G \subseteq \operatorname{im}(\iota_1^*) = \iota_1^*(H^1(G_F, \mathbb{F}_p)) \). We may therefore pick an \( \mathbb{F}_p \)-subspace \( Q' \) of \( \operatorname{im}(\iota_1^*) \) such that:

\[
P^G \oplus Q' = \operatorname{im}(\iota_1^*)
\]

as \( \mathbb{F}_p \)-vector spaces. We now prove that \( Q' \) is a trivial \( \mathbb{F}_p[G] \)-module. To this end, let \( q \in Q' \) be arbitrary. Then \( q = \iota_1^*(x) \) for some \( x \in H^1(G_F, \mathbb{F}_p) \). Then as \( \iota_1^* \) is \( G \)-module homomorphism and \( H^1(G_F, \mathbb{F}_p) \) is a trivial \( \mathbb{F}_p[G] \)-module, for any \( 1 \leq i \leq n \) we have:

\[
\rho_i \cdot q = \rho_i \cdot \iota_1^*(x) = \iota_1^*(\rho_i \cdot x) = \iota_1^*(0) = 0.
\]

This shows \( Q' \) is a trivial \( \mathbb{F}_p[G] \)-module, so \( Q' \) is an \( \mathbb{F}_p[G] \)-submodule of \( \operatorname{im}(\iota_1^*) \subseteq H^1(G_F, V) \).

We have now constructed the submodules \( P, Q, Q', \) and \( R \). There is one last definition to make, namely we let

\[
\mathcal{B} = \delta^2 \left((V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A}\right) \subseteq H^2(G_F, \mathbb{F}_p).
\]

Later on we will see a more intuitive description of \( \mathcal{B} \). For the time being, though, we will state the desired decomposition.
**Proposition 4.7.** (Proposition 2 of [CMS].) For any modules $P$, $Q$, $Q'$, and $R$ as previously defined, we have that $H^1(G_F, V) = P \oplus Q \oplus Q' \oplus R$, and there is a commutative diagram of $G$-modules of the following form:

\[
\begin{array}{ccccccccc}
Q^c & \rightarrow & H^1(G_F, \mathbb{F}_p)/\mathcal{A} & \rightarrow & P^G \\
\downarrow \text{incl} & & \downarrow \pi_1 & & \downarrow \text{incl} \\
Q \oplus Q' \oplus R^c & \rightarrow & H^1(G_F, V) & \rightarrow & P \\
\downarrow \pi_1^* & & \downarrow \delta^2 & & \downarrow \text{proj} \\
(V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A} & \rightarrow & (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \rightarrow & (V/V^G) \otimes_{\mathbb{F}_p} (H^1(G_F, \mathbb{F}_p)/\mathcal{A}) \\
\downarrow \delta^2 & & \downarrow 1 \otimes \text{proj}_1 & & \downarrow \text{proj}_2 \\
\mathcal{B}^c & \rightarrow & H^2(G_F, \mathbb{F}_p) & \rightarrow & H^2(G_F, \mathbb{F}_p)/\mathcal{B}
\end{array}
\]

with exact columns and split-exact rows.

**Proof 4.7.** Using the diagram of Proposition 4.1, the injectivity of inclusions, standard facts about quotient modules, and the definition of $\mathcal{B}$, we can immediately obtain the following commutative diagram of $G$-modules with exact second column and third fourth row:

\[
\begin{array}{ccccccccc}
Q' & \rightarrow & H^1(G_F, \mathbb{F}_p)/\mathcal{A} & \rightarrow & P^G \\
\downarrow \text{incl} & & \downarrow \pi_1 & & \downarrow \text{incl} \\
Q \oplus Q' \oplus R^c & \rightarrow & H^1(G_F, V) & \rightarrow & P \\
\downarrow \pi_1^* & & \downarrow \delta^2 & & \downarrow \text{proj} \\
(V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A} & \rightarrow & (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \rightarrow & (V/V^G) \otimes_{\mathbb{F}_p} (H^1(G_F, \mathbb{F}_p)/\mathcal{A}) \\
\downarrow \delta^2 & & \downarrow 1 \otimes \text{proj}_1 & & \downarrow \text{proj}_2 \\
\mathcal{B}^c & \rightarrow & H^2(G_F, \mathbb{F}_p) & \rightarrow & H^2(G_F, \mathbb{F}_p)/\mathcal{B}
\end{array}
\]

To finish the proof, it therefore suffices to do the following:

1. Prove that $P + Q + Q' + R = P \oplus Q \oplus Q' \oplus R$ and that $H^1(G_F, V) = P + Q + Q' + R$. This will allow us to replace $Q + Q' + R$ with in $Q \oplus Q' \oplus R$ in the diagram, and complete the second row of the diagram and prove it is split-exact.  
2. Complete the second column with an appropriate injective $G$-module homomorphism that makes the second column exact at $H^1(G_F, V)$.  
3. Complete the first row with $G$-module homomorphisms that make the first row a short exact sequence.  
4. Prove that the now-complete top-left and top-right squares are commutative.  
5. Prove that the now-complete rows 1, 3, and 4 are split-exact.  
6. Complete the first column of the diagram to give an exact column and prove that the now-complete center-left square is commutative.  
7. Complete the third column of the diagram in such a way that the newly-completed right-center and bottom-right squares are commutative.  
8. Prove that given any ring $R$, $R$-modules $A_1$, $A_4$, $B_1$, $B_4$, $C_1$, $C_4$
of $R$-modules with exact rows, exact first column, and exact second column, the third column is also exact at $B_3$ and $C_3$.

(1): We will prove $P + Q + Q' + R = P \oplus Q \oplus Q' \oplus R$ using the exclusion lemma, so we assume
\[ x \in (Q')^G \cap (P^G + Q^G + R^G) = Q' \cap (P^G + Q + R) \]
is arbitrary, where the equality is because $Q'$, $Q$, and $R$ are trivial $G$-modules. Then let $x = p + q + r$, where $p \in P^G$, $q \in Q$, and $r \in R$. By definition, $P^G \oplus Q' = \ker(\pi_1^3)$, so we have:
\[ 0 = \pi_1^3(x) = 0 + \pi_1^3(q + r). \]

By Lemma 4.6(4), $\pi_1^3$ is injective on $Q \oplus R$, so we have $q + r = 0$, so that $x = p$. Then $x \in P^G \cap Q' = \{0\}$ since $P^G + Q' = P^G \oplus Q'$. Thus, we have shown that:
\[ (Q')^G \cap (P^G + Q^G + R^G) = (Q')^G \oplus (P^G + Q^G + R^G) = (Q')^G \oplus P^G \oplus Q^G + R^G, \]
and by the Exclusion Lemma, we have that $P + Q + Q' + R = P \oplus Q \oplus Q' \oplus R$.

Now we prove that $H^1(G_F, V) = P + Q + Q' + R$. As $P$, $Q$, $Q'$, and $R$ are submodules of $H^1(G_F, V)$ by construction, it suffices to show that $H^1(G_F, V) \subseteq P + Q + Q' + R$. To this end, let $x \in H^1(G_F, V)$ be arbitrary. Then by the diagram of Proposition 4.1, $\pi_1^3(x) \in \ker(\delta^2)$, so by Lemma 4.6(3),
\[ \pi_1^3(x) \in \left((V/V^G) \otimes_{F_p} H^1(G_F, F_p)\right) \cap \ker(\delta^2) = \pi_1^3(P + Q + R). \]

Thus, there is a $d \in P + Q + R$ such that $\pi_1^3(x) = \pi_1^3(d)$. Then $x - d \in \ker(\pi_1^3) = P^G \oplus Q'$. As $d \in P + Q + R$ and $x - d \in P^G + Q'$, we have that:
\[ x = (x - d) + d \in P + Q + Q' + R, \]
and from earlier remarks we have proved that $H^1(G_F, V) = P + Q + Q' + R$.

We have therefore shown that $H^1(G_F, V) = P \oplus Q \oplus Q' \oplus R$. Thus, if $\text{proj} : H^1(G_F, V) \rightarrow P$ is the projection onto $P$ corresponding to this direct sum and $\iota : P \rightarrow H^1(G_F, V)$ is inclusion, then:
\[ Q \oplus Q' \oplus R \xrightarrow{\text{incl}} H^1(G_F, V) \xrightarrow{\text{proj}} P \]
is a split short exact sequence of $G$-modules with splitting homomorphism $\iota : P \rightarrow H^1(G_F, V)$. This finishes the proof of (1).

(2): From Proposition 4.1, $\iota_1^4 : H^1(G_F, F_p) \rightarrow H^1(G_F, V)$ is a $G$-module homomorphism with kernel $\text{im}(\delta^0) = A$ and image $\ker(\pi_1^4)$. Thus, $\iota_1^4$ induces an injective $G$-module homomorphism:
\[ \iota_1^4 : H^1(G_F, F_p)/A \rightarrow H^1(G_F, V) \]
that maps $H^1(G_F, F_p)/A$ isomorphically onto $\text{im}(\iota_1^4) = \ker(\pi_1^4)$. Thus, we have completed the second column of the diagram to a short exact sequence of $G$-modules.

(3): $\iota_1^4$ maps $H^1(G_F, F_p)/A$ isomorphically onto $\text{im}(\iota_1^4) = \ker(\pi_1^4) = P^G \oplus Q'$. Thus,
\[ H^1(G_F, F_p)/A = \iota_1^{-1}(P^G) \oplus \iota_1^{-1}(Q'), \]
and \( \overline{\iota}_1^{-1} : P^G \oplus Q' \to H^1(G_F, \mathbb{F}_p)/A \) is a \( G \)-module isomorphism that maps \( P^G \) isomorphically onto \( \overline{\iota}_1^{-1}(P^G) \) and \( Q' \) isomorphically onto \( \overline{\iota}_1^{-1}(Q') \). Thus, we let

\[
p : H^1(G_F, \mathbb{F}_p)/A \to P^G
\]

be the unique \( \mathbb{F}_p \)-linear map that is \( \overline{\iota}_1 \) on \( \overline{\iota}_1^{-1}(P^G) \) and is 0 on \( \overline{\iota}_1^{-1}(Q') \). Then \( p \) is a \( G \)-linear transformation, so we have the following diagram of \( G \)-module homomorphisms:

\[
\begin{array}{ccc}
Q' & \xrightarrow{\overline{\iota}_1^{-1}} & H^1(G_F, \mathbb{F}_p)/A \\
\downarrow \text{incl} & & \downarrow \text{proj} \\
Q \oplus Q' \oplus R & \xrightarrow{\text{incl}} & H^1(G_F, V)
\end{array}
\]

As \( \overline{\iota}_1^{-1} \) is an isomorphism, it is certainly injective. As \( \overline{\iota}_1 \) is surjective, it will certainly map \( \overline{\iota}_1^{-1}(P^G) \subseteq H^1(G_F, \mathbb{F}_p)/A \) surjectively onto \( P^G \). Furthermore, the image of \( \overline{\iota}_1^{-1} : Q' \to H^1(G_F, \mathbb{F}_p)/A \) is \( \overline{\iota}_1^{-1}(Q') \) by definition, and this is precisely the kernel of \( p \) by definition. Therefore, the previous diagram of \( G \)-module homomorphisms is a short exact sequence, and we have completed the first row of the diagram to a short exact sequence of \( G \)-modules, as desired.

(4): Recall that we have completed the upper-left and upper-right squares of the commutative diagram as follows:

\[
\begin{array}{ccc}
Q' & \xrightarrow{\overline{\iota}_1^{-1}} & H^1(G_F, \mathbb{F}_p)/A \\
\downarrow \text{incl} & & \downarrow \text{proj} \\
Q \oplus Q' \oplus R & \xrightarrow{\text{incl}} & H^1(G_F, V)
\end{array}
\]

The left square is obviously commutative. Now we prove that the right square is commutative. To this end, recall that we have:

\[
H^1(G_F, \mathbb{F}_p)/A = \overline{\iota}_1^{-1}(P^G) \oplus \overline{\iota}_1^{-1}(Q').
\]

Thus, let \( p' \in \overline{\iota}_1^{-1}(P^G) \) and \( q' \in \overline{\iota}_1^{-1}(Q') \) be arbitrary, so that \( p' + q' \) is an arbitrary element of \( H^1(G_F, \mathbb{F}_p)/A \), \( \overline{\iota}_1^{-1}(p') \in P^G \) and \( \overline{\iota}_1^{-1}(q') \in Q' \). Then:

\[
\text{proj} \circ \overline{\iota}_1(p' + q') = \text{proj} (\overline{\iota}_1(p') + \overline{\iota}_1(q')) = \overline{\iota}_1(p') + 0 = q(p' + q') = \text{incl} \circ q(p' + q'),
\]

so that the right square commutes.

Thus, the top-left and top-right squares commute, as desired.

(5): Notice that every module in the first, third, and fourth rows of the diagram is a trivial \( \mathbb{F}_p[G] \)-module. This is because \( P^G, Q', V/V^G, H^1(G_F, \mathbb{F}_p), \) and \( H^2(G_F, \mathbb{F}_p) \) are all trivial, and every module in the first, third, and fourth is some combination of quotients and tensor products of these modules. Therefore, to prove (5) it suffices to show that any short exact sequence:

\[
0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,
\]

of trivial \( \mathbb{F}_p[G] \)-modules splits.

To this end, note that since \( g \) maps \( B \) surjectively onto \( C \), there is some \( \mathbb{F}_p \)-subspace \( S \) of \( B \) that \( g \) maps isomorphically onto \( C \). Let \( h : C \to S \) be an inverse of this isomorphism. As \( B \) is a trivial \( \mathbb{F}_p[G] \)-module, \( S \) is automatically a trivial \( \mathbb{F}_p[G] \)-submodule of \( B \), and since \( C \) is also trivial, \( h \) is a \( \mathbb{F}_p[G] \)-module homomorphism. Furthermore, by construction, \( h \) is a right-inverse to \( g \). Therefore, \( h \) is a splitting homomorphism for the short-exact sequence

\[
0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,
\]

and from earlier remarks, the first, third, and fourth rows of the diagram are all split-exact.

(6) The obvious way to complete the first column is to add the map:

\[
\pi_1^* : Q \oplus Q' \oplus R \to (V/V^G) \otimes_{\mathbb{F}_p} A.
\]
This map is well-defined, as \( Q' \subseteq \ker(\pi_1^*) \) and, by Lemma 4.6(4), \( \pi_1^* \) maps \( Q \oplus R \) injectively into \( (V/V^G) \otimes_{\mathbb{F}_p} A \).

To prove exactness at \( Q \oplus Q' \oplus R \), we note that \( Q' \subseteq \ker(\pi_1^*) \) and \( \pi_1^* \) being injective on \( Q \oplus R \) together imply that the kernel of the map:

\[
\pi_1^* : Q \oplus Q' \oplus R \to (V/V^G) \otimes_{\mathbb{F}_p} A
\]

is \( Q' \), which is precisely the image of \( Q' \) under inclusion into \( Q \oplus Q' \oplus R \).

To prove exactness at \( (V/V^G) \otimes_{\mathbb{F}_p} A \), we note that the kernel of:

\[
\delta^2 : (V/V^G) \otimes_{\mathbb{F}_p} A \to B
\]

is precisely:

\[
\left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \cap \ker(\delta^2) = T_Q \oplus T_R = \pi_1^*(Q) + \pi_1^*(R).
\]

Since \( Q' \subseteq \ker(\pi_1^*) \), this last module is precisely \( \pi_1^*(Q \oplus Q' \oplus R) \). Thus, the first column is an exact sequence of \( \mathbb{F}_p[G] \)-modules, as desired.

The center-left square has been completed to:

\[
\begin{array}{ccc}
Q \oplus Q' \oplus & R \xrightarrow{\text{incl}} & H^1(G,F,V) \\
\pi_1^* & \downarrow & \\
(V/V^G) \otimes_{\mathbb{F}_p} A \xrightarrow{1 \otimes \text{incl}} & (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p).
\end{array}
\]

Once we note that

\[
1 \otimes \text{incl} : (V/V^G) \otimes_{\mathbb{F}_p} A \to (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p)
\]

is inclusion, it is obvious that this square commutes, as desired.

(7) As \( P \subseteq H^1(G,F,V) \),

\[
(1 \otimes \text{proj}_1) \circ \pi_1^* : P \to (V/V^G) \otimes_{\mathbb{F}_p} \left( H^1(G,F,\mathbb{F}_p)/A \right)
\]

is a \( G \)-module homomorphism, and the square:

\[
\begin{array}{ccc}
H^1(G,F,V) \xrightarrow{\text{proj}} & P \\
\pi_1^* & \downarrow & \\
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \xrightarrow{1 \otimes \text{proj}_1} & (V/V^G) \otimes_{\mathbb{F}_p} \left( H^1(G,F,\mathbb{F}_p)/A \right)
\end{array}
\]

obviously commutes.

Next, since:

\[
\delta^2 : (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \to H^2(G,F,\mathbb{F}_p)
\]

is a \( G \)-module homomorphism and \( \delta^2 \) maps \( (V/V^G) \otimes_{\mathbb{F}_p} A \) surjectively onto \( B \), \( \delta^2 \) induces a \( G \)-module homomorphism:

\[
\overline{\delta}^2 : \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \right)/\left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \to H^2(G,F,\mathbb{F}_p)/B.
\]

\( \overline{\delta}^2 \) is the unique \( G \)-module homomorphism for which the following rectangle commutes:

\[
\begin{array}{ccc}
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \xrightarrow{\text{proj}_3} & \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \right)/\left( (V/V^G) \otimes_{\mathbb{F}_p} A \right) \\
\delta^2 & \downarrow & \pi_1^* \\
H^2(G,F,\mathbb{F}_p) \xrightarrow{\text{proj}_2} & H^2(G,F,\mathbb{F}_p)/B
\end{array}
\]

Next,

\[
(1 \otimes \text{proj}_2) : (V/V^G) \otimes_{\mathbb{F}_p} H^1(G,F,\mathbb{F}_p) \to (V/V^G) \otimes_{\mathbb{F}_p} \left( H^1(G,F,\mathbb{F}_p)/A \right)
\]
is a surjective $G$-module homomorphism and its kernel is $(V/V^G) \otimes_{\mathbb{F}_p} A$. It therefore induces a $G$-module isomorphism:

$$f : \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \right) / \left( (V/V^G) \otimes_{\mathbb{F}_p} \mathcal{A} \right) \to \left( (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) / \mathcal{A} \right).$$

$f$ is the unique $G$-module homomorphism for which the following triangle commutes:

$$\begin{array}{ccc}
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \xrightarrow{\delta^2} & (V/V^G) \otimes_{\mathbb{F}_p} (H^1(G_F, \mathbb{F}_p) / \mathcal{A}) \\
\downarrow & & \downarrow \\
H^2(G_F, \mathbb{F}_p) & \xrightarrow{\overline{\delta^2}} & H^2(G_F, \mathbb{F}_p) / \mathcal{B}.
\end{array}$$

Combining the two commutative diagrams along the map $\text{proj}_3$ gives the following commutative diagram of $G$-modules:

$$\begin{array}{ccc}
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \xrightarrow{\delta^2} & (V/V^G) \otimes_{\mathbb{F}_p} (H^1(G_F, \mathbb{F}_p) / \mathcal{A}) \\
\downarrow & & \downarrow \\
H^2(G_F, \mathbb{F}_p) & \xrightarrow{\overline{\delta^2}} & H^2(G_F, \mathbb{F}_p) / \mathcal{B}.
\end{array}$$

Replacing $f$ with $f^{-1}$ allows the previous diagram to be condensed to:

$$\begin{array}{ccc}
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) & \xrightarrow{\delta^2} & (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) / \mathcal{A} \\
\downarrow & & \downarrow \\
H^2(G_F, \mathbb{F}_p) & \xrightarrow{\overline{\delta^2} \circ f^{-1}} & H^2(G_F, \mathbb{F}_p) / \mathcal{B}.
\end{array}$$

We have been able to complete the third column of the diagram with $\mathbb{F}_p[G]$-module homomorphisms in such a way that the center-right and bottom-right squares of the diagram commute, as desired.

(8): In order to prove that the third column of the diagram is exact at $B_3$ and $C_3$, we must show that: $\text{im}(h_1) \subseteq \ker(h_2)$, $\ker(h_2) \subseteq \text{im}(h_1)$, $\text{im}(h_2) \subseteq \ker(h_3)$, and $\ker(h_3) \subseteq \text{im}(h_2)$.

Proof that $\text{im}(h_1) \subseteq \ker(h_2)$: For ease of understanding, this diagram illustrates the main steps:

We begin with an arbitrary element $b_3 \in \text{im}(h_1)$. Then there is an element $a_3 \in A_3$ such that $h_1(a_3) = b_3$. Because $\alpha_3$ is surjective, there is an $a_2 \in A_2$ such that $\alpha_2(a_2) = a_3$. Let $b_2 = g_1(a_2)$.
Then
\[ \beta_2(b_2) = \beta_2 \circ g_1(a_2) = h_1 \circ \alpha_2(a_2) = h_1(a_3) = b_3. \]
Since the second column is exact at \( B_2 \), \( g_2(b_2) = g_2 \circ g_1(a_2) = 0 \). Thus,
\[ h_2(b_3) = h_2 \circ \beta_2(b_2) = \gamma_2 \circ g_2(b_2) = \gamma_2(0) = 0, \]
so \( b_3 \in \ker(h_2) \) and \( \im(h_1) \subseteq \ker(h_2) \), as desired.

Proof that \( \ker(h_2) \subseteq \im(h_1) \): This diagram illustrates the main steps:

![Diagram](image)

We begin with an arbitrary element \( b_3 \in \ker(h_2) \), so that \( h_2(b_3) = 0 \). Since \( \beta_2 \) is surjective, there is a \( b_2 \in B_2 \) such that \( \beta_2(b_2) = b_3 \). Let \( c_2 = g_2(b_2) \). Then:
\[ \gamma_2(c_2) = \gamma_2 \circ g_2(b_2) = h_2 \circ \beta_2(b_2) = h_2(b_3) = 0. \]
Because the third row is exact at \( C_2 \), there is an element \( c_1 \in C_1 \) such that \( \gamma_1(c_1) = c_2 \). Because the second column is exact at \( C_2 \), \( g_3(c_2) = g_3 \circ g_2(b_2) = 0 \). Let \( d_1 = f_3(c_1) \). Then:
\[ \delta_1(d_1) = \delta_1 \circ f_3(c_1) = g_3 \circ \gamma_1(c_1) = g_3(c_2) = 0. \]
However, \( \delta_1 \) is injective, and this means that \( d_1 = 0 \).

Thus, since \( f_3(c_1) = d_1 = 0 \) and the first column is exact at \( C_1 \), there is an element \( b_1 \in B_1 \) such that \( f_2(b_1) = c_1 \). Now we consider the element \( \beta_1(b_1) \in B_2 \). As the second row is exact at \( B_2 \), we have that \( \beta_2(\beta_1(b_1)) = 0 \). Furthermore,
\[ g_2(\beta_1(b_1)) = \gamma_1 \circ f_2(b_1) = \gamma_1(c_1) = c_2. \]

Now we consider the element \( b_2 - \beta_1(b_1) \in B_2 \). We have that \( g_2(b_2 - \beta_1(b_1)) = c_2 - c_2 = 0 \). Since the second column is exact at \( B_2 \), we have that there is an element \( a_2 \in A_2 \) such that \( g_1(a_2) = b_2 - \beta_1(b_1) \). Let \( a_3 = \alpha_2(a_2) \). Then:
\[ h_1(a_3) = h_1 \circ \alpha_2(a_2) = \beta_2 \circ g_1(a_2) = \beta_2(b_2 - \beta_1(b_1)) = b_3 - 0 = b_3. \]
Thus, \( b_3 \in \im(h_1) \) and \( \ker(h_2) \subseteq \im(h_1) \), as desired.

Proof that \( \im(h_2) \subseteq \ker(h_3) \): This diagram illustrates the main steps:

![Diagram](image)

We begin with an arbitrary element \( c_3 \in \im(h_2) \). Then there is an element \( b_3 \in B_3 \) such that \( h_2(b_3) = c_3 \). Because \( \beta_2 \) is surjective, there is a \( b_2 \in B_2 \) such that \( \beta_2(b_2) = b_3 \). Let \( c_2 = g_2(b_2) \). Then
\[ \gamma_2(c_2) = \gamma_2 \circ g_2(b_2) = h_2 \circ \beta_2(b_2) = h_2(b_3) = c_3. \]
Since the second column is exact at $B_2$, $g_3(c_2) = g_3 \circ g_2(b_2) = 0$. Thus,

$$h_3(c_3) = h_3 \circ \gamma_2(c_2) = \delta_2 \circ g_3(c_2) = \delta_2(0) = 0,$$

so $c_3 \in \ker(h_3)$ and $\im(h_2) \subseteq \ker(h_3)$, as desired.

Proof that $\ker(h_3) \subseteq \im(h_2)$: This diagram illustrates the main steps:

$$\begin{array}{ccc}
c_1 & \xrightarrow{\gamma_2} & c_3 \\
\downarrow{g_3} & & \downarrow{h_3} \\
d_1 & \xrightarrow{\delta_1} & d_2
\end{array} \quad \begin{array}{ccc}
c_1 & \xrightarrow{\gamma_1} & c_2 \\
\downarrow{f_3} & & \downarrow{h_3} \\
d_1 & \xrightarrow{\delta_1} & d_2
\end{array} \quad \begin{array}{ccc}
c_1 & \xrightarrow{\gamma_1} & c_2 \\
\downarrow{f_3} & & \downarrow{g_3} \\
d_1 & \xrightarrow{\delta_1} & d_2
\end{array}$$

We begin with an arbitrary element $c_3 \in \ker(h_3)$, so that $h_3(c_3) = 0$. Since $\gamma_2$ is surjective, there is a $c_2 \in C_2$ such that $\gamma_2(c_2) = c_3$. Let $d_2 = g_3(c_2)$. Then:

$$\delta_2(d_2) = \delta_2 \circ g_3(c_2) = h_3 \circ \gamma_2(c_2) = h_3(c_3) = 0.$$

Because the fourth row is exact at $D_2$, there is an element $d_1 \in D_1$ such that $\delta_1(d_1) = d_2$. Because $f_3$ is surjective, there is an element $c_1 \in C_1$ such that $f_3(c_1) = d_1$. Now we consider the element $\gamma_1(c_1) \in C_2$. As the third row is exact at $C_2$, we have that $\gamma_2(\gamma_1(c_1)) = 0$. Furthermore,

$$g_3(\gamma_1(c_1)) = \delta_1 \circ f_3(c_1) = \delta_1(d_1) = d_2.$$

Now we consider the element $c_2 - \gamma_1(c_1) \in C_2$. We have that $g_3(c_2 - \gamma_1(c_1)) = d_2 - d_2 = 0$. Since the second column is exact at $C_2$, we have that there is an element $b_2 \in B_2$ such that $g_2(b_2) = c_2 - \gamma_1(c_1)$. Let $b_3 = \beta_2(b_2)$. Then:

$$h_3(b_3) = h_3 \circ \beta_2(b_2) = \gamma_2 \circ g_2(b_2) = \gamma_2(\gamma_2(c_2) - \gamma_1(c_1)) = c_3 - 0 = c_3.$$

Thus, $c_3 \in \im(h_2)$ and $\ker(h_3) \subseteq \im(h_2)$, as desired.

Thus, we have shown that $\im(h_1) \subseteq \ker(h_2)$, $\ker(h_2) \subseteq \im(h_1)$, $\im(h_2) \subseteq \ker(h_3)$, and $\ker(h_3) \subseteq \im(h_2)$, so by earlier remarks we are finished with the proof of (8), and therefore also with the proof of Proposition 4.7. QED

Let us summarize what we have done in this section: We let $T_P$ and $T_Q$ be any $\mathbb{F}_p$-vector subspaces of $(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p)$ such that:

$$T_Q \oplus T_R = (V/V^G) \otimes_{\mathbb{F}_p} A \cap \ker(\delta^2)$$

$$T_P \oplus T_Q \oplus T_R = (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) \cap \ker(\delta^2).$$

where $T_R = \pi^*_1(R)$. We let $\tilde{P}$ and $\tilde{Q}$ be any $\mathbb{F}_p$-vector subspaces of $H^1(G_F, V)$ that are mapped isomorphically onto $T_P$ and $T_Q$, respectively, by $\pi^*_2$. Then $\tilde{Q}$ is a trivial $\mathbb{F}_p[G]$-submodule of $H^1(G_F, V)$ that we call $Q$, while we let $P$ be the submodule of $H^1(G_F, V)$ that is generated by $\tilde{P}$. Then, we let $Q'$ be any $\mathbb{F}_p$-vector subspace of $H^1(G_F, V)$ such that:

$$P^G \oplus Q' = \im(\iota^*_1).$$

Then $Q'$ is automatically a trivial $\mathbb{F}_p[G]$-submodule of $H^1(G_F, V)$.

Notice that in this construction we have made five choices, namely $T_P, T_Q, \tilde{P}, \tilde{Q}$, and $Q'$. Even so, for any such choices $P, Q, Q'$, and $R$ automatically satisfy all facts in Lemma 4.6 and Proposition 4.7. The submodules $X$ and $Y$ of $H^1(G_F, \mathbb{F}_2[G])$ are constructed in part by making very controlled choices for these five subspaces and using the properties in Lemma 4.6 and Proposition 4.7.
2. Consequences of Shapiro’s Lemma

The starting point for this section is to note that $G$ acts on $H^1(G_F,F_p)$ by conjugation. More specifically, we already have that $F_p$ is a trivial $G_F$-module and that $G_E$ is a closed subgroup of $G_F$. Then for any $\sigma \in G_F$ and $m \geq 0$, we have the map:

$$\sigma_* : H^1(G_E,F_p) \to H^1(\sigma G_E \sigma^{-1}, \sigma \cdot F_p)$$

descended from the map on cochains that sends the cochain $a' \in C^m(G_E,F_p)$ to the cochain:

$$\eta \mapsto \sigma \cdot a(\sigma^{-1} \eta \sigma)$$

for $\eta \in \sigma G_E \sigma^{-1}$. But since $G_E$ is a normal subgroup of $G_F$ and $G_F$ acts trivially on $F_p$, $\sigma^*$ is a map from $H^1(G_E,F_p)$ to $H^1(G_E,F_p)$, and thus we have a group action:

$$G_F \times H^1(G_E,F_p) \to H^1(G_E,F_p)$$

defined as $\sigma \cdot a = \sigma_*(a)$.

We now claim that under this action $G_E$ acts trivially on $H^1(G_E,F_p)$. We prove this on the level of cocycles: Let $a \in Z^1(G_E,F_p)$ be arbitrary. Since the action of $G_E$ on $F_p$ is trivial, $Z^1(G_E,F_p) = \text{Hom}_\text{cont}(G_E,F_p)$, so for all $\eta, \eta' \in G_E$ we have:

$$(\eta_*(a))(\eta') = a(\eta^{-1} \eta' \eta) = -a(\eta) + a(\eta') + a(\eta) = a(\eta').$$

Thus, $G_E$ acts trivially on $H^1(G_E,F_p)$, so the conjugation action of $G_F$ on $H^1(G_E,F_p)$ descends to an action of $G$ on $H^1(G_E,F_p)$. This action can be defined as follows: for $a \in Z^1(G_E,F_p)$ and $g \in G$, let $\tilde{g} \in G_F$ be any element in $\phi^{-1}(\{g\})$. Then for all $\eta \in G_E$,

$$(g \cdot a)(\eta) = a(\tilde{g}^{-1} \eta \tilde{g}^{-1}).$$

Next, we recall the formulation of Shapiro’s lemma given in Chapter 3 as an isomorphism from $H^n(H,\text{Map}_\text{cont}(H/K,A))$ to $H^n(K,A)$ for all profinite groups $H$, $H$-modules $A$, and closed subgroups $K$ of $H$. We let $H = G_F$, $K = G_E$, and $A = F_p$. Since $G_F/G_E$ is a finite group isomorphic to $G$ as topological group, $G_F/G_E$ has the discrete topology, so all functions from $G_F/G_E$ to $F_p$ will be continuous. Thus, as abelian groups,

$$\text{Map}_\text{cont}(G_F/G_E,F_p) = \text{Map}(G_F/G_E,F_p) \cong F_p[G],$$

where an explicit isomorphism from $F_p[G]$ to $\text{Map}(G_F/G_E,F_p)$ is given by sending $\sum_{g \in G} \alpha g \in F_p[G]$ to the function:

$$\sigma G_E \mapsto \alpha_{\varphi(\sigma)}.$$ 

Thus, from Shapiro’s lemma, we have an explicit isomorphism:

$$\text{sh} : H^1(G_F,F_p[G]) \to H^1(G_E,F_p)$$

that is descended from the map on cocycles that sends $a \in Z^1(G_F,F_p[G])$ to:

$$(\pi \circ a)|_{G_E},$$

where $\pi : F_p[G] \to F_p$ is the map that sends $\sum_{g \in G} \alpha g \in F_p[G]$ to $\alpha_1 \in F_p$.

Now we can obtain the following two facts:

**Proposition 4.8.** The isomorphism

$$\text{sh} : H^1(G_F,F_p[G]) \to H^1(G_E,F_p)$$

is one of $G$-modules.

**Proof.** We prove this fact at the level of cocycles. $\text{sh}$ is a $G$-module isomorphism from $H^1(G_F,F_p[G])$ to $H^1(G_E,F_p)$, and we do this at the level of cocycles. To this end, let $g \in G$, $\eta \in G_E$, and $a \in Z^1(G_F,F_p[G])$ be arbitrary. Let $\tilde{g}$ be any lift of $g$ to $G_F$, and for each $x \in G$ let $c_x \in C^1(G_F,F_p)$ be such that:

$$a = \sum_{x \in G} c_x x.$$

85
Then we have:

$$(g \cdot \text{sh}(a))(\eta) = (\text{sha})(\tilde{g}^{-1}\eta\tilde{g}) = c_1(\tilde{g}^{-1}\eta\tilde{g})$$

and

$$\text{sh}(g \cdot a) = \text{sh} \left( \sum_{x \in G} c_x g x \right) = \text{sh} \left( \sum_{x \in G} c_{g^{-1} x} x \right) = c_{g^{-1} | G_E}.$$ 

Thus, we must prove that $c_{g^{-1}}(\eta) = c_1(\tilde{g}^{-1}\eta\tilde{g})$. To do this, we use the cocycle condition as follows. We first compute:

$$a(1) = a(1 \cdot 1) = 1 \cdot a(1) + a(1) = 2a(1),$$

so that $a(1) = 0$. Then:

$$0 = a(1) = a(\tilde{g}^{-1}\tilde{g}) = \tilde{g}^{-1} \cdot a(\tilde{g}) + a(\tilde{g}^{-1}) = \phi(\tilde{g}^{-1}) a(\tilde{g}) + a(\tilde{g}^{-1}) = \phi(\tilde{g})^{-1} a(\tilde{g}) + a(\tilde{g}^{-1})$$

$$= g^{-1} a(\tilde{g}) + a(\tilde{g}^{-1}).$$

Thus,

$$a(\tilde{g}^{-1}) = -g^{-1} a(\tilde{g}).$$

Now we compute:

$$a(\tilde{g}^{-1}\eta\tilde{g}) = \tilde{g}^{-1} \cdot a(\eta\tilde{g}) + a(\tilde{g}^{-1}) = \phi(\tilde{g}^{-1}) a(\eta\tilde{g}) - g^{-1} a(\tilde{g}) = g^{-1} (a(\eta\tilde{g}) - a(\tilde{g}))$$

$$= g^{-1} (\eta \cdot a(\tilde{g}) + a(\eta) - a(\tilde{g})) = g^{-1} (\phi(\eta)a(\tilde{g}) + a(\eta) - a(\tilde{g})) = g^{-1} (a(\tilde{g}) + a(\eta) - a(\tilde{g}))$$

$$= g^{-1} a(\eta).$$

Substituting $a = \sum_{x \in G} c_x x$ gives:

$$\sum_{x \in G} c_x (\tilde{g}^{-1}\eta\tilde{g}) x = g^{-1} \sum_{x \in G} c_x(\eta) x = \sum_{x \in G} c_x(\eta) g^{-1} x = \sum_{x \in G} c_x(\eta) x.$$

Comparing coefficients of 1 gives that $c_1(\tilde{g}^{-1}\eta\tilde{g}) = c_g(\eta)$, as desired. By earlier remarks, sh is a $G$-module isomorphism, and we have finished proving Proposition 4.8. QED

**PROPOSITION 4.9.** The homomorphism

$$\text{cor}_{G_E}^{G_F} : H^1(G_E, \mathbb{F}_p) \to H^1(G_F, \mathbb{F}_p)$$

is one of $G$-modules.

**PROOF 4.9.** We prove this at the level of cocycles: Let $g \in G$, $a \in Z^1(G_E, \mathbb{F}_p)$, and $\sigma \in G_F$ be arbitrary. Then let $\tilde{g}$ be any element of $\phi^{-1}({\{g\}})$, and let $x_1, \ldots, x_m$ be a set of representatives of the left coset space $G_F/G_E$. For each $\sigma' \in G_F$, let $\sigma'$ be the coset representative $x_i$ of $\sigma'$. Then recalling the definition of corestriction for inhomogeneous cochains, we have that:

$$\text{cor}(g \cdot a)(\sigma) = \sum_{j=1}^m x_j^{-1} \cdot ((g \cdot a)(x_j \sigma x_j^{-1} \sigma^{-1})) = \sum_{j=1}^m \phi(x_j^{-1}) \cdot (g \cdot a(x_j \sigma x_j^{-1} \sigma^{-1}))$$

$$= \sum_{j=1}^m (\phi(x_j^{-1})g) \cdot a(x_j \sigma x_j^{-1} \sigma^{-1}) = \sum_{j=1}^m (g \phi(x_j^{-1})) \cdot a(x_j \sigma x_j^{-1} \sigma^{-1})$$

$$= g \cdot \sum_{j=1}^m x_j^{-1} \cdot a(x_j \sigma x_j^{-1} \sigma^{-1}) = g \cdot (\text{cor}(a)(\sigma)) = (g \cdot \text{cor}(a))(\sigma)$$

and thus $\text{cor}_{G_E}^{G_F}$ is a $G$-module homomorphism. QED

As a corollary of Proposition 3.3, we obtain a lemma from [CMS]. This lemma describes the functions $b_1^*, \ldots, b_n^* : H^1(G_F, \mathbb{F}_p[G]) \to H^1(G_F, V)$ induced by the $G$-module homomorphisms

$$b_1 \cdot \ldots, b_n \cdot \cdot : \mathbb{F}_p[G] \to V.$$
LEMMA 4.10. (Lemma 4 of [CMS]) For each $1 \leq i \leq n$, the following diagram is commutative:

$$
\begin{array}{ccc}
H^1(G_F, \mathbb{F}_p[G]) & \xrightarrow{b_i} & H^1(G_F, \mathbb{F}_p) \\
\downarrow^{\text{sh}} & & \downarrow^{\pi_i} \\
H^1(G_E, \mathbb{F}_p) & \xrightarrow{a_i} & (V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p).
\end{array}
$$

PROOF 4.10. We will prove this at the level of cochains. To this end, let $a' \in C^1(G_F, \mathbb{F}_p[G])$ be arbitrary, let

$$M = \{ \rho_1^{a_1} \cdots \rho_n^{a_n} \in F_2[G] \mid \forall 1 \leq i \leq n, 0 \leq a_i \leq p-1 \}.$$

Next, let

$$a' = \sum_{m \in M} c'_m m,$$

where for each $m \in M$, $c'_m \in C^1(G_F, \mathbb{F}_p)$. Then:

$$\pi_i^* \circ b_i^*(a') = \pi_i^* \left( c'_i b_i + c'_{i+1} \right) = \overline{b_i} \otimes c'_i.$$

On the other hand, we have from Proposition 3.3 that $\text{cor}_{G_F} \circ \text{sh} = v^*$, where $v^*$ is induced by the homomorphism $v : \mathbb{F}_p[G] \cong \text{Map}_{\text{cont}}(G_F/G_E, \mathbb{F}_p) \to \mathbb{F}_p$ defined as:

$$\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g.$$

In other words, $v^*$ is obtained by substituting $\tau_1 = \cdots = \tau_n = 1$ into the expression $\sum_{g \in G} \alpha_g g$. But substituting $\tau_1 = \cdots = \tau_n = 1$ is equivalent to substituting $\rho_1 = \cdots = \rho_n = 0$, and thus:

$$v^*(a') = v^* \left( \sum_{m \in M} c'_m m \right) = c'_1.$$

Therefore:

$$\overline{b_i} \otimes (\text{cor}_{G_F} \circ \text{sh}(a')) = \overline{b_i} \otimes (v^*(a')) = \overline{b_i} \otimes c'_i,$$

so the diagram is commutative. All homomorphisms in each diagram have already been proved to be $G$-module homomorphisms. QED

3. Connections to Kummer Theory and Brauer Groups

Notice that in the previous two sections, there were no explicit facts about the field extension $E/F$ that were used other than it is Galois with $\text{Gal}(E/F) \cong (\mathbb{Z}/p\mathbb{Z})^n$. In fact, the previous analysis would have worked just as well if $G$ were any discrete group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$, $\phi : G_F \to G$ were any continuous, surjective homomorphism of profinite groups, and $G_E = \ker(\phi)$.

However, in this section we will start to use field theoretic information about $E/F$. Therefore, starting in this section we assume that $\text{char}(F) \neq p$ and that $F$ contains a primitive $p$th root of unity $\omega$. From standard Kummer theory, we can conclude that there are elements $a_1, \ldots, a_n \in F^\times$ such that:

$$E = F(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n})$$

and for each $1 \leq i \leq n$,

$$\sqrt[p]{a_i} \notin F(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_{i-1}}, \sqrt[p]{a_{i+1}}, \ldots, \sqrt[p]{a_n}).$$

Furthermore, we may take $\tau_i$ to be the unique automorphism of $E$ that fixes $F$ pointwise, fixes $\sqrt[p]{a_j}$ for $j \neq i$ and sends $\sqrt[p]{a_i}$ to $\omega \sqrt[p]{a_i}$. Next, let $\mu_p \subseteq (F^{\text{sep}})^\times$ be the group of proot of unity. Then $\mu_p = \langle \omega \rangle$, so $G_F$ and $G_E$ both fix $\mu_p$. Therefore, $\mu_p \cong F_p$ as $G_F$- and $G_E$-modules under the isomorphism $\omega \mapsto 1$. Thus the Kummer theory isomorphisms:

$$\text{kum}_E : E^\times/(E^\times)^p \cong H^1(G_E, \mu_m),$$
and

\[ \text{kum}_F : F^\times/(F^\times)^p \cong H^1(G_F, \mu_m) \]

may be considered as maps to \( H^1(G_E, \mathbb{F}_p) \) and \( H^1(G_F, \mathbb{F}_p) \), respectively. Next, we have the following fact:

**COROLLARY 4.11.** The group isomorphisms:

\[ \text{kum}_E : E^\times/(E^\times)^p \cong H^1(G_E, \mathbb{F}_p), \]

and

\[ \text{kum}_F : F^\times/(F^\times)^p \cong H^1(G_F, \mathbb{F}_p) \]

are isomorphisms of \( G \)-modules.

**PROOF 4.11.** Since elements of \( G \) fix all elements of \( F \), \( F^\times/(F^\times)^p \) and \( H^1(G_F, \mathbb{F}_p) \) are both trivial \( G \)-modules, so \( \text{kum}_F \) is a \( G \)-module homomorphism.

From Kummer theory, the isomorphism \( \text{kum}_E \) from \( E^\times/(E^\times)^p \) to \( H^1(G_E, \mu_p) \) is given by sending the class of \( a \in F^\times/(F^\times)^p \) to the class of \( \text{kum}_a \in Z^1(G_E, \mathbb{F}_p) \), where:

\[ \text{kum}_a(\eta) = \frac{\eta(\sqrt[p]{a})}{\sqrt[p]{a}} \]

and \( \sqrt[p]{a} \in F^{\text{sep}} \) is any element such that \((\sqrt[p]{a})^p = a\) and choosing a different \( p \)-th root of \( a \) yields a cohomologous cocycle. Now we prove that \( \text{kum} \) is an isomorphism of \( G \)-modules, so we let \( g \in G, \ a \in E^\times, \) and \( \eta \in G_E \) be arbitrary. Let \( \tilde{g} \in \phi^{-1}\{\{g\}\} \) be arbitrary. Then we compute:

\[ (g \cdot \text{kum}_a)(\eta) = \text{kum}_a (\tilde{g}^{-1} \eta \tilde{g}) = \frac{\tilde{g}^{-1} \eta \tilde{g} (\sqrt[p]{a})}{(\sqrt[p]{a})} = \tilde{g}^{-1} \left( \frac{\eta \tilde{g} (\sqrt[p]{a})}{\tilde{g} (\sqrt[p]{a})} \right). \]

As \((\tilde{g} (\sqrt[p]{a}))^p = \tilde{g} ((\sqrt[p]{a})^p) = \tilde{g}(a) = g(a)\), we have that \( \tilde{g}(\sqrt[p]{a}) \) is a \( p \)-th root of \( g(a) \). Thus, the previous quantity is:

\[ \tilde{g}^{-1} \left( \text{kum}_{g(a)}(\eta) \right) = \text{kum}_{g(a)}(\eta) = (\text{kum}(g(a)))(\eta), \]

where the first equality follows because \( \text{kum}_{g(a)}(\eta) \in \mu_p \subseteq F \), so this quantity will be fixed by \( \tilde{g}^{-1} \in G_F \). Thus, for all \( a \in E^\times, \ g \cdot \text{kum}(a) = \text{kum}(g \cdot a) \) and so \( \text{kum} \) is a homomorphism of \( G \)-modules. QED

Now, notice that we can apply the \( G \)-module homomorphism \( \text{kum}_F : F^\times/(F^\times)^p \rightarrow H^1(G_F, \mathbb{F}_p) \) to the elements \( \overline{a}_1, \ldots, \overline{a}_n \) of \( F^\times/(F^\times)^p \). To this end, let \( \sigma \in G \) be arbitrary, and suppose that \( \phi(\sigma) = \tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n} \). Then:

\[ \text{kum}_{a_i}(\sigma) = \frac{\sigma(\sqrt[p]{a_i})}{\sqrt[p]{a_i}} = \frac{\tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n}(\sqrt[p]{a_i})}{\sqrt[p]{a_i}} = \omega^{\alpha_i}, \]

so that \( \text{kum}_{f(a_i)} \), when considered as an element of \( H^1(G_F, \mathbb{F}_p) \), is \( \overline{\omega}_i \in \mathcal{A} \).

Thus, if we let

\[ \mathcal{A}' = (\overline{a}_1, \ldots, \overline{a}_n) \subseteq F^\times/(F^\times)^p, \]

then \( \text{kum}_F \) maps \( \mathcal{A}' \) isomorphically onto \( \mathcal{A} \), so that we now have a more natural interpretation of \( \mathcal{A} \).

Thus, in the following commutative diagram:

\[
\begin{array}{c}
H^0(G, V/V^G) \xrightarrow{\text{infl}} H^0(G_F, V/V^G) \\
\downarrow \phi^0 \downarrow \phi^0 \\
H^1(G, \mathbb{F}_p) \xrightarrow{\text{infl}} H^1(G_F, \mathbb{F}_p) \xrightarrow{\text{kum}} F^\times/(F^\times)^p
\end{array}
\]

88
we have for each $1 \leq i \leq n$ the following array of elements:

\[
\begin{array}{c}
\bar{b}_i \xrightarrow{\text{inf}} \bar{b}_i \\
\downarrow \delta^0 \\
\bar{t}_i \xrightarrow{\text{inf}} \bar{t}_i ^k \xrightarrow{\text{kum}} \bar{a}_i
\end{array}
\]

Next, in order to obtain a more natural interpretation of $\mathcal{B}$, we have the following interpretation of the homomorphism $\delta^2$:

**Lemma 4.12.** (Proposition 4 of [CMS]) $\delta^2$ has the following action on pure tensors of

\[
(V/V^G) \otimes_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p):
\]

for $x \in V/V^G \cong H^0(G_F, V/V^G)$ and $a \in H^1(G_F, \mathbb{F}_p)$,

\[
\delta^2(x \otimes a) = (\delta^0(x)) \cup a,
\]

provided we identity $\mathbb{F}_p$ with $\mathbb{F}_p \otimes \mathbb{Z} \mathbb{F}_p$ via the map $\alpha \mapsto (1 \otimes \alpha)$.

**Proof 4.12.** We will prove this result at the level of cocycles. Since $\delta^2$ is linear and the cup-product is bilinear, it suffices to prove this result for when $x$ ranges over an $\mathbb{F}_p$-basis of $V/V^G$. To this end, let $1 \leq i \leq n$ be arbitrary, let $a' \in Z^1(G_F, \mathbb{F}_p)$ be arbitrary, and let $\sigma_1, \sigma_2 \in G$ be arbitrary. Let $g = \phi(\sigma_1)$. Furthermore, we recall that the function that sends an element $g \in G$ to the coefficient of $\rho_i$ when $g$ is regarded as an element of $F_p[G]$ is written as a polynomial in $\rho_1, \ldots, \rho_n$ is $v_i$. Furthermore, the coefficient of 1 when $g \in G$ is written as a polynomial in $\rho_1, \ldots, \rho_n$ is always 1.

We compute $\delta^2$ of $\bar{b}_i \otimes a'$ in the standard way. Note that $a'b_i$ is an element of $C^1(G_F, V)$ that $\pi_2^*$ maps to $\bar{b}_i \otimes a'$. Next we compute $\partial^2(a'b_i)$:

\[
(\partial^2(a'b_i)) (\sigma_1, \sigma_2) = \sigma_1 \cdot ((a'b_i)(\sigma_2)) - (a'b_i)(\sigma_1\sigma_2) + (a'b_i)(\sigma_1)
\]

\[
= \phi(\sigma_1) \cdot (a'(\sigma_2)b_i) - (a'\sigma_1\sigma_2)b_i + (a'(\sigma_1))b_i
\]

\[
= g_i \cdot (a'(\sigma_2)b_i) - (a'(\sigma_1) + a'(\sigma_2))b_i + (a'(\sigma_1))b_i
\]

\[
= a'(\sigma_2)(b_i + v_i(g)z) - (a'(\sigma_1) + a'(\sigma_2))b_i + (a'(\sigma_1))b_i
\]

\[
= a'(\sigma_2)v_i(g)z = v_i'(\sigma_1)a'(\sigma_2)z
\]

The map $(\sigma_1, \sigma_2) \mapsto v'_i(\sigma_1)a'(\sigma_2)$ is therefore an element of $C^2(G_F, \mathbb{F}_p)$ that is sent to $\partial^2(a'b_i)$ by $\nu_2^*$. Thus, $\delta^2$ sends $\bar{b}_i \otimes a'$ to the class of:

\[
(\sigma_1, \sigma_2) \mapsto v'_i(\sigma_1)a'(\sigma_2)
\]

in $H^2(G_F, \mathbb{F}_2)$.

Next, we compute that:

\[
((\delta^0(\bar{b}_i)) \cup a') (\sigma_1, \sigma_2) = (v'_i \cup a')((\sigma_1, \sigma_2) = (v'_i(\sigma_1)) \otimes (\sigma_2 \cdot (a'(\sigma_2))) = (v'_i(\sigma_1)) \otimes (a'(\sigma_2))
\]

\[
= 1 \otimes (v'_i(\sigma_1)a'(\sigma_2)).
\]

Thus, after we identify $\mathbb{F}_p$ and $\mathbb{F}_p \otimes \mathbb{Z} \mathbb{F}_p$, $\delta^2(\bar{b}_i \otimes a') \in H^2(G_F, \mathbb{F}_2)$ is identical to $(\delta^0(\bar{b}_i)) \cup a' \in H^2(G_F, \mathbb{F}_2 \otimes \mathbb{Z} \mathbb{F}_2)$, as desired. QED

Therefore, $\mathcal{B} = \mathcal{A} \cup \mathcal{A}$. Now, let:

\[
\mathcal{B}' = \langle (a_i, a_j)_{1 \leq i \leq j \leq n} \rangle \subseteq_p \text{Br}(k).
\]

Then by Proposition 3.13, $\text{brau} : H^2(G_F, \mathbb{F}_p) \rightarrow_p \text{Br}(k)$ maps $\mathcal{B}$ isomorphically onto $\mathcal{B}'$. 89
4. Construction of $\mathcal{X}$ and $\mathcal{Y}$

Now we turn to proving results that specifically require $p = 2$ and $n = 2$; these will be used in the construction of $\mathcal{X}$ and $\mathcal{Y}$. For the rest of the proof, we will let $a_3 = a_1a_2$. The first of these results are on $\mathbb{F}_2[G]$-modules in general.

**Lemma 4.13.** Let $M$ be an $\mathbb{F}_2[G]$-module and $\tilde{M}$ an $\mathbb{F}_2$-subspace of $M$. Then $\tilde{M}$ is generated by $\tilde{M}$ as an $\mathbb{F}_2[G]$-module if and only if $M = \tilde{M} + VM$. If either of these two conditions hold, then $V\tilde{M} = VM$.

**Proof.** 4.13. Note that $M$ is generated by $\tilde{M}$ if and only if $M = \mathbb{F}_2[G]\tilde{M}$, and as $(1) + V$, $\mathbb{F}_2[G]\tilde{M} = \tilde{M} + VM$. Thus, $M$ is generated by $\tilde{M}$ if and only if $M = \tilde{M} + VM$.

If $M = \tilde{M} + VM$, then:

$$VM \subseteq V\tilde{M} + VV\tilde{M} \subseteq V\tilde{M}.$$  

As $V\tilde{M}$ is automatically a subset of $VM$, we have that $VM = V\tilde{M}$ if $M = \tilde{M} + V\tilde{M}$. This proves the lemma. QED

**Lemma 4.14.** (Lemma 6 of [CMS]) Let $M$ be an $\mathbb{F}_2[G]$-module and $\tilde{M}$ an $\mathbb{F}_2$-subspace of $M$ that generates $M$ as an $\mathbb{F}_2[G]$-module. Furthermore, assume that:

$$\rho_1\tilde{M} \cap \rho_1VM = \rho_2\tilde{M} \cap \rho_2V\tilde{M} = \tilde{M} \cap M^G = \{0\}.$$  

Then $M^G \subseteq VM$.

**Proof.** 4.14. Let $m \in M^G$ be arbitrary. Then by the previous lemma, there are elements $\bar{m}_1, \bar{m}_2 \in \tilde{M}$ and $v \in V$ such that:

$$m = \bar{m}_1 + vm\bar{m}_2.$$  

As $m \in M^G$, we have that $\rho_1m = \rho_2m = 0$. Thus, left-multiplying the previous equation by $\rho_1$ gives:

$$0 = \rho_1\bar{m}_1 + \rho_1vm\bar{m}_2.$$  

Since $\rho_1\tilde{M} \cap \rho_1VM = \{0\}$, we have that $\rho_1\bar{m}_1 = \rho_1vm\bar{m}_2 = 0$. Similarly,

$$\rho_2m = 0 = \rho_2\bar{m}_1 + \rho_2vm\bar{m}_2,$$

so $\rho_2\bar{m}_1 = 0$. Since $\rho_1\bar{m}_1 = \rho_2\bar{m}_2 = 0$, we have that $\bar{m}_2 \in M^G \cap \tilde{M} = \{0\}$. Thus, $m = vm\bar{m}_2 \in VM$. QED

We also have the following lemma concerning submodules of $H^1(G_E, \mathbb{F}_2)$.

**Lemma 4.15.** Let $M$ be an $\mathbb{F}_2[G]$-submodule of $H^1(G_E, \mathbb{F}_2)$ and $\tilde{M}$ an $\mathbb{F}_2$-subspace of $M$ that generates $M$ as an $\mathbb{F}_2[G]$-module. Let $\rho_1, \rho_2 : \mathbb{F}_2[G] \to V$ be the $G_F$-module homomorphisms left-multiplication by $\rho_1$ and $\rho_2$, respectively, and let $\rho_1^*, \rho_2^* : H^1(G_F, \mathbb{F}_2[G]) \to H^1(G_F, V)$ be the induced $G$-module homomorphisms on cohomology. Define $M_V$ to be:

$$\rho_1^*(\text{sh}^{-1}(M)) + \rho_2^*(\text{sh}^{-1}(M)) \subseteq H^1(G_F, V).$$
\textbf{Proof 4.15.} Consider the following two diagrams of $G$-modules:

\[
\begin{array}{ccc}
H^1(G,F_2) & \xrightarrow{\text{sh}^{-1}} & H^1(G,F_2) \\
\downarrow^{\rho^1} & & \downarrow^{\rho^1} \\
H^1(G,F_2[G]) & \xrightarrow{\text{sh}} & H^1(G,F_2[G])
\end{array}
\quad
\begin{array}{ccc}
H^1(G,F_2) & \xrightarrow{\text{sh}^{-1}} & H^1(G,F_2) \\
\downarrow^{\rho^2} & & \downarrow^{\rho^2} \\
H^1(G,F_2[G]) & \xrightarrow{\text{sh}} & H^1(G,F_2[G])
\end{array}
\]

They are both commutative, as for an element $\alpha' = c'_0 + c'_1\rho_1 + c'_2\rho_2 + c'_3\rho_1\rho_2 \in C^1(G,F_2[G])$ with $c'_0, c'_1, c'_2, c'_3 \in C^1(G,F_2)$:

\[
i_2^*(\rho_1^*(b)) = i_2^*(c'_0\rho_1 + 0\rho_2 + c'_2\rho_1\rho_2) = 0 \cdot 1 + c'_0\rho_1 + 0\rho_2 + c'_2\rho_1\rho_2 = \rho_1 \cdot b
\]

and similarly

\[
i_2^*(\rho_2^*(b)) = i_2^*(0\rho_1 + c'_0\rho_2 + c'_1\rho_1\rho_2) = 0 \cdot 1 + 0\rho_1 + c'_0\rho_2 + c'_1\rho_1\rho_2 = \rho_2 \cdot b.
\]

Therefore, since sh is a $G$-module isomorphism, we have that:

\[
VM = \rho_1M + \rho_2M + \rho_1\rho_2M = \rho_1M + \rho_2M = \rho_1\text{sh}(\text{sh}^{-1}(M)) + \rho_2\text{sh}(\text{sh}^{-1}(M))
\]

\[
= \text{sh}(\rho_1\text{sh}^{-1}(M)) + \text{sh}(\rho_2\text{sh}^{-1}(M)) = \text{sh}(\rho_1\text{sh}^{-1}(M) + \rho_2\text{sh}^{-1}(M))
\]

\[
= \text{sh}(i_2^*(\rho_1^*(\text{sh}^{-1}(M))) + i_2^*(\rho_2^*(\text{sh}^{-1}(M)))) = \text{sh}(i_2^*(\rho_1^*(\text{sh}^{-1}(M)) + \rho_2^*(\text{sh}^{-1}(M))))
\]

\[
= \text{sh}(i_2^*(\text{sh}^{-1}(M))).
\]

Thus, since $M^G \subseteq VM$, we have that $M^G \subseteq \text{sh}(i_2^*(M_V))$, and applying $\text{sh}^{-1}$ gives:

\[
\text{sh}^{-1}(M)^G = \text{sh}^{-1}(M^G) \subseteq i_2^*(M_V),
\]

as desired. QED

\textbf{Lemma 4.16. (Lemma 8 of \cite{CMS}.)} The following diagram is a commutative diagram of $G$-modules.

\[
\begin{array}{ccc}
H^1(G,F_2[G]) & \xrightarrow{\text{sh}} & H^1(G,F_2) \\
\downarrow^{\pi_2^*} & & \downarrow^{\text{cor}} \\
H^1(G,F_2) & \xrightarrow{\text{cor}} & H^n(G,F_2)
\end{array}
\]

\textbf{Proof 4.16.} Identify $\nu^*$ from Proposition 3.3 with $\pi_2^*$ to obtain the commutativity of the diagram. QED

We begin by defining three invariants $u, v, w$ of the field extension $E/F$. First,

\[
v = \dim F_2 \left( A \cap \kum(N_{E/F}(E^x/(E^x)^2)) \right)
\]

\[
w = 3 - \dim F_2(A \cup A).
\]

Next, let $u = 1$ if there are elements $e_1, e_2 \in E^x$ such that $N_{E/F}(e_1) = a_1 = a_2 \in F^x/(F^x)^2$, and $N_{E/F}(e_1)N_{E/F}(e_2) = (a_1)^2 \in (E^x)^2$. If there are no such elements, then let $u = 0$. 

91
We now explain some of the significance of these values. \( \dim_{F_2} A = 2 \), so \( 0 \leq v \leq 2 \). As the cup-product is anticommutative, \( A \cup A \) is spanned by \( \{ \overline{t}_1 \cup \overline{t}_1, \overline{t}_2 \cup \overline{t}_2 \} \), so \( 0 \leq w \leq 3 \). Also, since the following diagram commutes
\[
E^\times/(E^\times)^{2c} \xrightarrow{\kum} H^1(G_E, F_2) \xrightarrow{N_{E/F}} F^\times/(F^\times)^{2c} \xrightarrow{\cor} H^1(G_F, F_2),
\]
v is also equal to \( \dim_{F_2} (A \cap \cor (H^1(G_E, F_2))) \).

Next we interpret the value \( u \). Notice that if \( u = 1 \), then \( v \) automatically equals 2. We apply the map \( \kum : E^\times/(E^\times)^2 \to H^1(G_E, F_2) \) to \( N_{E/F(\sqrt{\pi})}(e_1)N_{E/F(\sqrt{\pi})}(e_2) \in (E^\times)^2 \) to obtain:
\[
\cor_{E/F(\sqrt{\pi})}(\kum(e_1)) + \cor_{E/F(\sqrt{\pi})}(\kum(e_2)) = 0,
\]
But by definition \( \cor_{E/F(\sqrt{\pi})}(a) = 1a + x_1a = x_1a - 1a = \rho_1a \), and similarly \( \cor_{E/F(\sqrt{\pi})}(a) = \rho_2a \).
Thus, the previous condition gives that: \( \rho_1\kum(e_1) + \rho_2\kum(e_2) = 0 \). Therefore, if \( u = 1 \), then there are elements \( e_1, e_2 \in H^1(G_E, F_2) \) such that \( \cor(e_1) = \overline{t}_1, \cor(e_2) = \overline{t}_2 \), and \( \rho_1e_1 = \rho_2e_2 \).

Now we recall the setup of Lemma 4.6 and Proposition 4.7. \( R = \ker(\pi^*_2) \), \( T_R = \pi^*_1(R) \), \( T_P \) and \( T_Q \) are any \( F_2 \)-subspaces of \( (V/V^G) \otimes_{F_2} H^1(G_F, F_2) \) such that:
\[
T_Q \oplus T_R = ((V/V^G) \otimes_{F_2} A) \cap \ker(\delta^2)
\]
\[
T_P \oplus T_Q \oplus T_R = ((V/V^G) \otimes_{F_2} H^1(G_F, F_2)) \cap \ker(\delta^2),
\]
\( \hat{P} \) and \( \hat{Q} \) are any \( F_2 \)-subspaces of \( H^1(G_F, V) \) such that \( \pi^*_1 \) maps \( \hat{P} \) and \( \hat{Q} \) isomorphically onto \( T_P \) and \( T_Q \) respectively, and \( P \) and \( Q \) are the \( F_2[G] \)-submodules of \( H^1(G_F, V) \) that are generated by \( \hat{P} \) and \( \hat{Q} \). Then \( T_R, T_P, \) and \( Q \) are automatically trivial \( F_2[G] \)-modules, and \( \hat{Q} \).

Since \( d^*_2 : (V/V^G) \otimes A \to B \) is a surjection by definition of \( B \), it has kernel \( ((V/V^G) \otimes_{F_2} A) \cap \ker(\delta^2) \) and the dimension of this kernel is:
\[
\dim_{F_2} ((V/V^G) \otimes_{F_2} A) - \dim_{F_2} (A \cup A) = 4 - \dim_{F_2} (A \cup A).\]

By Lemma 4.3, \( \dim_{F_2} T_R = \dim_{F_2} \pi^*_1(R) = 1 \), so:
\[
\dim_{F_2}(Q) = \dim_{F_2}(\hat{Q}) = \dim_{F_2}(T_Q) = \dim_{F_2}(((V/V^G) \otimes_{F_2} A) \cap \ker(\delta^2)) - \dim_{F_2}(T_R)
= 3 - \dim_{F_2} (A \cup A) = w.
\]

Furthermore, \( w = 3 \) implies \( v = 2 \). To prove this, we need the following lemma:

**Lemma 4.17.** Suppose there is a \( u_1 \in F(\sqrt{a_1})^\times \) and a \( u_2 \in F(\sqrt{a_2})^\times \) such that \( N_{F(\sqrt{\pi})/F(u_1)} = N_{F(\sqrt{\pi})/F(u_2)} \). Then there is a \( u \in E \) and an \( a \in F \) such that \( N_{E/F(\sqrt{\pi})}(u) = au_1 \) and \( N_{E/F(\sqrt{\pi})}(u) = au_2 \).

**Proof.** Lemma 4.17. This is proved as Lemma 2.14 of [Wa]. QED

Now, if \( w = 3 \), then \( \dim_{F_2} (A \cup A) = 0 \), so that \( A \cup A = 0 \). Switching to the language of Brauer groups, this means that:
\[
(\overline{a_1}, \overline{a_1}) = (\overline{a_1}, \overline{a_2}) = (\overline{a_2}, \overline{a_2}) = 0
\]
in \( \mathbb{2Br}(F) \). This implies that \( a_1 \) is a norm from both \( F(\sqrt{(a_1)})/F \) and \( F(\sqrt{a_2})/F \). By the lemma, there is a \( u \in E \) and an \( a \in F^\times \) such that:
\[
N_{E/F}(u) = N_{F(\sqrt{a_1})/F} \circ N_{E/F(\sqrt{a_1})}(u) = a^2 a_1,
\]
so that \( \overline{a_1} \in N_{E/F}(E^\times/(E^\times)^2) \). Similarly, \( \overline{a_2} \in N_{E/F}(E^\times/(E^\times)^2) \), and thus:
\[
v = \dim_{F_2} (A \cap \kum(N_{E/F}(E^\times/(E^\times)^2))) = 2.
\]

Now we have the following proposition:
PROPOSITION 4.18. (Proposition 5 of [CMS]) There is an $\mathbb{F}_2[G]$-submodule $\mathcal{X}$ of $H^1(G_E, \mathbb{F}_2)$ and a trivial $\mathbb{F}_2[G]$-submodule $Q \oplus Q'_\mathcal{X}$ of $H^1(G_E, V)$ such that:

1. $(Q \oplus Q'_\mathcal{X}) + R = (Q \oplus Q'_\mathcal{X}) \oplus R$.
2. The following is a short exact sequence:

$$0 \to Q \oplus Q'_\mathcal{X} \xrightarrow{\text{sho}_2^*} \mathcal{X} \xrightarrow{\text{cor}} A \cap \text{cor}(H^1(G_E, \mathbb{F}_2)) \to 0.$$

3. $\text{sho} \circ \iota_2^*$ maps $Q \oplus Q'_\mathcal{X}$ isomorphically onto $\mathcal{X}^G$.
4. The following is a short exact sequence:

$$0 \to Q'_\mathcal{X} \xrightarrow{\text{incl}} Q \oplus Q'_\mathcal{X} + R \xrightarrow{\pi^*_1} ((V/V^G) \otimes_{\mathbb{F}_2} A) \cap \ker(\delta^2) \to 0.$$

5. $Q'_\mathcal{X} = \{0\}$ unless $v = 2$ and $u = 0$, in which case $Q'_\mathcal{X} \cong \mathbb{F}_2$ as $G$-modules.
6. $$\iota_2^*(Q'_\mathcal{X}) \cap \sum_{i=1}^2 (\rho_i \cdot \text{sh}^{-1}(H^1(G_E, \mathbb{F}_2)) \cap \iota_2^*(H^1(G_E, \mathbb{F}_2))) = \{0\}.$$

(7)

$$\mathcal{X} \cong \begin{cases} \mathbb{F}_2^u & \text{if } v = 0 \\ \Omega(-1) & \text{if } v = 1 \\ \Omega(-1) \oplus \Omega(-1) & \text{if } v = 2 \text{ and } u = 0 \\ \Omega(-2) & \text{if } v = 2 \text{ and } u = 1 \end{cases}$$

as $\mathbb{F}_2[G]$-modules.

PROOF 4.18. We will proceed with this proof in cases, according to the value of $v$.

**Case 1:** $v = 0$. We define $Q'_\mathcal{X}$ to be $\{0\}$. Thus, $Q + Q'_\mathcal{X} = Q \oplus Q'_\mathcal{X}$ and $Q \oplus Q'_\mathcal{X}$ is trivial. By Lemma 4.6, we have that $Q + Q'_\mathcal{X} + R = Q + R = Q \oplus R = Q \oplus Q'_\mathcal{X} \oplus R$, so we have (1). Because $Q'_\mathcal{X} = \{0\}$, we have that so that we have (5) and (6). By Lemma 4.6(4), $\pi^*_1$ is injective on $Q \oplus R$. As $Q = Q$, $\pi^*_1$ maps $Q$ isomorphically onto $T_Q$, and also $\pi^*_1(R) = T_R$ by definition. Thus, $\pi^*_1$ maps $Q \oplus R$ isomorphically onto $T_Q \oplus T_R = ((V/V^G) \otimes_{\mathbb{F}_2} A) \cap \ker(\delta^2)$.

Since $Q'_\mathcal{X} = \{0\}$, this fact gives the exact sequence of (4).

Now we define $\mathcal{X}$ to be $\text{sho} \iota_2^*(Q)$. Since $Q \cap R = \{0\}$ and $R = \ker(\iota_2^*)$, $\text{sho} \circ \iota_2^*$ maps $Q$ isomorphically onto $\mathcal{X}$. Since $v = 0$, $A \cap \text{cor}(H^1(G_E, \mathbb{F}_2)) = \{0\}$, and since $Q'_\mathcal{X} = \{0\}$, we have (2). Because $\mathcal{X}$ is the image of a trivial $\mathbb{F}_2[G]$-module under a $G$-module homomorphism, $\mathcal{X}$ is a trivial $G$-module. Thus, $\mathcal{X}^G = \mathcal{X}$, and since $Q \oplus Q'_\mathcal{X} = Q$, we have (3). Finally, since $\dim_{\mathbb{F}_2}(Q) = w$ and $\text{sh} \circ \iota_2^* Q$ maps $Q$ isomorphically onto $\mathcal{X}$, $\dim_{\mathbb{F}_2}(\mathcal{X}) = w$, so $\mathcal{X} \cong \mathbb{F}_2^w$, thus obtaining (7). We have finished the proof of the proposition in this case.

**Case 2:** $v \in \{1, 2\}$. If $v = 1$, there is some $e \in H^1(G_E, \mathbb{F}_2)$ such that $\text{cor}(e) \in A \setminus \{0\}$. In this case, let $\mathcal{X}$ be the $\mathbb{F}_2$-vector space $\langle e \rangle$. If $v = 2$ and $u = 1$, then there are elements there are elements $e_1, e_2 \in H^1(G_E, \mathbb{F}_2)$ such that $\text{cor}(e_1) = \overline{e_1}$, $\text{cor}(e_2) = \overline{e_2}$, and $\rho_1 e_1 = \rho_2 e_2$. In this case, let $\mathcal{X}$ be the $\mathbb{F}_2$-vector space $\mathcal{X} = \langle e_1, e_2 \rangle$. If $v = 2$ and $u = 0$, then there are elements $e_1, e_2 \in H^1(G_E, \mathbb{F}_2)$ such that $\text{cor}(e_1) = \overline{e_1}$ and $\text{cor}(e_2) = \overline{e_2}$, and furthermore for any such choice of $e_1$ and $e_2$, we have $\rho_1 e_1 \neq \rho_2 e_2$. In this case, let $\mathcal{X}$ be the $\mathbb{F}_2$-vector space $\mathcal{X} = \langle e_1, e_2 \rangle$. Thus, in all cases, cor will map $\mathcal{X}$ isomorphically onto $A \cap \text{cor}(H^1(G_E, \mathbb{F}_2))$ as $\mathbb{F}_2$-vector spaces.

Regardless of whether $v = 1$ or $v = 2$, let $\mathcal{X}$ denote the $\mathbb{F}_2[G]$-submodule of $H^1(G_E, \mathbb{F}_2)$ generated by $\mathcal{X}$. We now claim that $\text{sh}^{-1}(X)^G \subseteq \iota_2^*(\mathcal{X})$, where $\mathcal{X}$ comes from the notation of Lemma 4.15. In fact, we use Lemmas 4.14 and 4.15 to prove this claim. To use Lemma 4.14, we need to prove
that \( \rho_1\tilde{X} \cap \rho_1V\tilde{X} = \rho_2\tilde{X} \cap \rho_2V\tilde{X} = \tilde{X} \cap X^G = \{0\} \). To this end, note that \( \rho_1V = \rho_2V = \langle \rho_1\rho_2 \rangle = (1 + x_1 + x_2 + x_1x_2) \). Thus:

\[
\rho_1V\tilde{X} = \rho_2V\tilde{X} = \rho_1\rho_2\tilde{X} = (1 + x_1 + x_2 + x_1x_2)\tilde{X} = \nu_2(\nu_1(\text{cor}(\tilde{X}))).
\]

By construction, \( \text{cor}(\tilde{X}) \subseteq \mathcal{A} = \ker(\nu_1) \), so therefore \( \rho_1V\tilde{X} = \rho_2V\tilde{X} = \{0, \} \), and thus:

\[
\rho_1\tilde{X} \cap \rho_1V\tilde{X} = \rho_2\tilde{X} \cap \rho_2V\tilde{X} = \{0\}.
\]

To prove that \( \tilde{X} \cap X^G = \{0\} \), we compute using Lemma 4.10 that for any nonzero \( z \in \tilde{X} \),

\[
\pi_1^* \circ \rho_1^*(z) = \overline{p_1} \otimes (\text{corsh}(z)), \quad \text{and}
\]

\[
\pi_1^* \circ \rho_2^*(z) = \overline{p_2} \otimes (\text{corsh}(z)).
\]

By Lemma 4.3 we have that \( \pi_1^*(R) = \langle \overline{p_1} \otimes \overline{v_2} + \overline{p_2} \otimes \overline{v_2} \rangle \). Therefore, \( \pi_1^* \circ \rho_1^*(z), \pi_1^* \circ \rho_2^*(z) \notin \pi_1^*(R), \) so \( \rho_1^*(z), \rho_2^*(z) \notin R = \ker(\nu_2) \). Thus, \( \rho_1z = \nu_2^* \circ \nu_1^*(z) \neq 0 \) and \( \rho_2z = \nu_2^* \circ \nu_2^*(z) \neq 0 \), so \( z \notin X^G \). As \( z \in \tilde{X} \) was an arbitrary nonzero element, we have that \( \tilde{X} \cap X^G = \{0\} \).

Thus, by Lemma 4.14, we have that \( X^G \subseteq V\tilde{X} \), and by Lemma 4.15, we have that \( \text{sh}^{-1}(X)^G \subseteq \nu_2^*(X_V) \), as desired.

**Case 2a:** \( v = 1 \). We let \( Q' \) be \( \{0\} \), so that we have (5) and (6). We now claim that \( X_V \) can fulfill the role of \( Q \) in Lemma 4.6. To this end, we have from the previous paragraph that:

\[
\pi_1^*(X_V) = (V/V^G) \otimes_{\pi_2} \text{cor}(e) \subseteq \left( (V/V^G) \otimes_{\pi_2} \mathcal{A} \right) \cap \ker(\delta^2),
\]

and since \( \pi_1^*(R) = \langle \overline{p_1} \otimes \overline{v_1} + \overline{p_2} \otimes \overline{v_2} \rangle \), we have that:

\[
\pi_1^*(X_V) \cap \pi_1^*(R) = \{0\}.
\]

This means that \( \pi_1^*(X_V) + \pi_1^*(R) = \pi_1^*(X_V) \oplus \pi_1^*(R) \) and therefore:

\[
\dim_{\pi_2} (\pi_1^*(X_V) + \pi_1^*(R)) = \dim_{\pi_2} (\pi_1^*(X_V)) + \dim_{\pi_2} (\pi_1^*(R)) = 2 + 1 = 3.
\]

Now, if \( \pi_1^*(X_V) + \pi_1^*(R) \) were not all of \( (V/V^G) \otimes_{\pi_2} \mathcal{A} \cap \ker(\delta^2) \), then since:

\[
\dim_{\pi_2} ((V/V^G) \otimes_{\pi_2} \mathcal{A}) = 2 \cdot 2 = 4,
\]

we must have that \( (V/V^G) \otimes_{\pi_2} \mathcal{A} \subseteq \ker(\delta^2) \). Then by the definition of \( w \), we would have that \( w = 3 \), and this is impossible, since \( v = 1 \). Therefore, \( \pi_1^*(X_V) \oplus \pi_1^*(R) \) is all of \( (V/V^G) \otimes_{\pi_2} \mathcal{A} \cap \ker(\delta^2) \).

Therefore, we may take \( T_Q \) to be \( \pi_1^*(X_V) \) and \( Q \) to be \( X_V \), as was claimed. By properties of \( Q \) and \( R, Q = Q \oplus Q'_X \) is trivial, and \( (Q \oplus Q'_X) \cap R = Q \oplus Q'_X \cap R \), so that we have (1). By properties of \( Q \) and \( R \), we have that \( \pi_1^* \) maps \( Q \oplus R \) isomorphically onto \( (V/V^G) \otimes_{\pi_2} \mathcal{A} \cap \ker(\delta^2) \), so that we have (4).

Next we prove (2). By definition,

\[
X = \tilde{X} + \rho_1\tilde{X} + \rho_2\tilde{X} + \rho_1\rho_2\tilde{X}.
\]

But, as was already shown, \( \rho_1\rho_2\tilde{X} = \{0\} \), and therefore:

\[
X = \tilde{X} + \rho_1\tilde{X} + \rho_2\tilde{X}.
\]

Now,

\[
\text{sh}(\nu_2^*(Q)) = \text{sh}(\nu_2^*(X_V)) = \text{sh} \left( \nu_2^* \left( \rho_1^*(\text{sh}^{-1}(X)) + \rho_2^*(\text{sh}^{-1}(X)) \right) \right) = \text{sh} \left( \rho_1\text{sh}^{-1}(X) + \rho_2(\text{sh}^{-1}(X)) \right) = \rho_1X + \rho_2X.
\]

Furthermore, \( \text{cor}(\rho_1 \cdot x) = \text{cor}(\rho_2 \cdot x) = 0 \), while \( \text{cor} \), by definition of \( \tilde{X} \), maps \( \tilde{X} \) isomorphically onto \( \mathcal{A} \cap H^1(G_F, F_2) \). We have therefore shown (2).

We now prove (3). We already have that \( X^G \subseteq V\tilde{X} = \rho_1\tilde{X} + \rho_2\tilde{X} \). Next, note that:

\[
\rho_1\rho_1\tilde{X} = \rho_2\rho_2\tilde{X} = 0\tilde{X} = \{0\}
\]

and it has already been shown that:

\[
\rho_1\rho_2\tilde{X} = \rho_2\rho_1\tilde{X} = \{0\}.
\]
Therefore, $\rho_1X + \rho_2X \subseteq X^G$, from which we conclude that $X^G = \rho_1X + \rho_2X = \iota_2^*(M_V) = \iota_2^*(Q)$. Furthermore, it was already shown that:

$$\pi_1^*(X_V) \cap \pi_1^*(R) = \{0\},$$

and, since $\pi_1^*$ is injective on $R$, this means that $X_V \cap R = \{0\}$. Since $R = \ker(\iota_2)$, we have that $\iota_2^*$ is injective on $X_V = Q$. Thus, $\iota_2^*$ maps $Q = Q \oplus Q'_X$ isomorphically onto $X^G$, as (3) says.

Finally, we note that $X = \hat{X} + \rho_1\hat{X} + \rho_2\hat{X} = \langle e, \rho_1e, \rho_2e \rangle$. It is clear that $X \cong \Omega(-1)$, thus proving (7).

Thus, we have shown all parts of 4.18 when $v = 1$ and this case is finished.

**Case 2b**: $v = 2$. We have that:

$$\langle \rho_1^* \circ \sh^{-1}(e_1), \rho_2^* \circ \sh^{-1}(e_1), \rho_1^* \circ \sh^{-1}(e_2), \rho_2^* \circ \sh^{-1}(e_2) \rangle \subseteq X_V.$$

Applying $\pi_1^*$ to this and using Lemma 4.10 gives that:

$$\pi_1^*(X_V) = (V/V^G) \otimes_{F_2} A,$$

and using Lemma 4.3 gives:

$$\pi_1^*(R) = \langle \pi_1^*(\rho_1^* \sh^{-1}(e_1) + \rho_2^* \sh^{-1}(e_2)) \rangle.$$

Let $S = \langle \rho_1^* \sh^{-1}(e_1) + \rho_2^* \sh^{-1}(e_2) \rangle \subseteq H^1(G_F, V)$, and let $Q$ be any $F_2$-vector space such that:

$$Q \oplus S = X_V.$$

Then by construction, $\pi_1^*(Q) \cap \pi_1^*(R) = \{0\}$, and since $\pi_1^*$ is injective on $R$, this means that $Q \cap R = \{0\}$. Therefore $\iota_2^*$ is injective on $Q$. By using Corollary 4.2, we have that $\iota_2^*(S) = \iota_2^*(H^1(G_F, F_2))$.

Now let $Q'_X \subseteq \iota_1^*(H^1(G_F, F_2))$ be any $F_2$-subspace such that $\iota_2^* Q'_X$ isomorphically onto $\iota_2^*(S)$. Then since $\iota_1^*(H^1(G_F, F_2))$ is a trivial $F_2[G]$-module, $Q'_X$ is automatically a trivial $F_2[G]$-module. Note that:

$$\iota_2^*(S) = \iota_2^* \langle \rho_1^* \sh^{-1}(e_1) + \rho_2^* \sh^{-1}(e_2) \rangle = \langle \iota_2^* \rho_1^* \sh^{-1}(e_1) + \iota_2^* \rho_2^* \sh^{-1}(e_2) \rangle = \langle \rho_1^* \sh^{-1}(e_1) + \rho_2^* \sh^{-1}(e_2) \rangle$$

Thus, if $u = 1$, then $\iota_2^*(S) = \{0\}$, so $Q'_X = \{0\}$, while if $u = 0$, then $\iota_2^*(S) \neq \{0\}$, so therefore $Q'_X \cong F_2$ as $F_2[G]$-modules. Therefore, we have proved (5).

Now, as $Q'_X \subseteq \iota_1^*(H^1(G_F, F_2))$, we have $\pi_1^*(Q'_X) = 0$, and we also have that $\pi_1^*$ is injective on $R$. This means that $Q'_X \cap R = \{0\}$. Therefore, as $Q \cap Q'_X = Q \cap R = Q'_X \cap R = \{0\}$, we that that $Q + Q'_X + R = Q \oplus Q'_X \oplus R$, so that we have (1).

As $R = \ker(\iota_2^*)$, we must have that $\iota_2^*$ is injective on $Q \oplus Q'_X$. We already have that $X^G \subseteq V X = \rho_1X + \rho_2X$. Next, note that:

$$\rho_1\rho_1X = \rho_2\rho_2X = 0X = \{0\}$$

and it has already been shown that:

$$\rho_1\rho_2X = \rho_2\rho_1X = \{0\}.$$

Thus, $\rho_1X + \rho_2X \subseteq X^G$, so therefore

$$X^G = \rho_1X + \rho_2X = \sh \rho_2^*(X_V) = \sh \rho_2^*(Q \oplus S) = \sh \rho_2^*(Q) + \sh \rho_2^*(S) = \sh \rho_2^*(Q) + \sh \rho_2^*(Q'_X) = \sh \rho_2^*(Q \oplus Q'_X),$$

and so we have (3).

Furthermore, since $\iota_2^*$ is a $G$-module homomorphism that maps $Q \oplus Q'_X$ isomorphically onto the trivial module $X^G$, we have that $Q \oplus Q'_X$ is trivial.

Next we show (2). As:

$$X = \hat{X} + \rho_1\hat{X} + \rho_2\hat{X} + \rho_1\rho_2\hat{X}.$$

But, as was already shown, $\rho_1\rho_2\hat{X} = \{0\}$, and therefore:

$$X = \hat{X} + \rho_1\hat{X} + \rho_2\hat{X}.$$
Now, as \( \text{im}(\iota_2^*) = \ker(\pi_1^*) \), we have that \( \text{im}(\text{sh} \circ \iota_2^*) = \ker(\pi_2^* \circ \text{sh}^{-1}) \), and by Lemma 4.16, this is \( \ker(\text{cor}) \). Therefore, \( \text{cor} \circ \text{sh} \circ \iota_2^*(Q \oplus Q'_x) = \{0\} \). As \( \text{cor} \) maps \( \mathcal{X} \) isomorphically onto \( \mathcal{A} \cap H^1(G_E, \mathbb{F}_2) \) by construction, and as

\[
\rho_1 \mathcal{X} + \rho_2 \mathcal{X} \subseteq \rho_1 \mathcal{X} + \rho_2 \mathcal{X} = \mathcal{X}^G = \text{sh} \circ \iota_2^*(Q \oplus Q'_x),
\]

we have the exact sequence of (2).

Now we show (4). \( \pi_1^*(R) = \pi_1^*(S) \) by construction, so

\[
\pi_1^*(Q + R) = \pi_1^*(Q) + \pi_1^*(R) = \pi_1^*(Q) + \pi_1^*(S) = \pi_1^*(\mathcal{X}_v) = (V/V^G) \otimes_{\mathbb{F}_2} \mathcal{A}.
\]

Furthermore, \( \pi_1^* \) is injective on both \( Q \) and \( R \), and \( \pi_1^*(Q) + \pi_1^*(R) = \pi_1^*(Q) \oplus \pi_1^*(R) \), so \( \pi_1^* \) maps \( Q + R \) isomorphically onto \( (V/V^G) \otimes_{\mathbb{F}_2} \mathcal{A} \). We have also already shown that \( \pi_1^*(-) = \{0\} \). This implies that we have the exact sequence of (4).

Given that we have (5), it suffices to prove (6) in the case that \( u = 0 \). Let \( y \) be the nonzero element of \( \iota_2^*(Q'_x) \), so that:

\[
y = \iota_2^*(\rho_1^* \text{sh}^{-1}(e_1) + \rho_2^* \text{sh}^{-1}(e_2)).
\]

Assume for a proof by contradiction that \( y = y_1 + y_2 \), where for \( i \in \{1, 2\} \),

\[
y_i \in \rho_i \cdot \text{sh}^{-1}(H^1(G_E, \mathbb{F}_2)) \cap \iota_2^* \circ \iota_1^* (H^1(G_F, \mathbb{F}_2)).
\]

Then there are elements \( z_1, z_2 \in H^2(G_E, \mathbb{F}_2) \) such that \( y_1 = \rho_1^* \text{sh}^{-1}(e_1) \) and \( y_2 = \rho_2^* \text{sh}^{-1}(e_2) \). Let \( y_1' = e_1 + z_1 \) and \( y_2' = e_2 + z_2 \). Then since \( \iota_2^* \rho_1^* = \rho_i \cdot \text{sh}^{-1} \) on \( H^1(G_E, \mathbb{F}_2[G]) \), we have:

\[
\begin{align*}
\rho_1^* \text{sh}^{-1}(y_1') &= \rho_1^* \text{sh}^{-1}(e_1) + \rho_1^* \text{sh}^{-1}(z_1) = \rho_1^* \text{sh}^{-1}(e_1) + y_1 + y_2 \\
&= \rho_1^* \text{sh}^{-1}(e_1) + \iota_2^* (\rho_2^* \text{sh}^{-1}(e_1) + \rho_2^* \text{sh}^{-1}(e_2)) + \rho_2^* \text{sh}^{-1}(z_2) = \iota_2^* \rho_2^* \text{sh}^{-1}(e_2) + \rho_2^* \text{sh}^{-1}(z_2) \\
&= \rho_2^* \text{sh}^{-1}(e_2) + \rho_2^* \text{sh}^{-1}(z_2).
\end{align*}
\]

Now note that for \( i \in \{1, 2\} \),

\[
\text{cor}_{E/F}(z_i) = \text{cor}_{E/\sqrt{\pi_t}F}(\text{cor}_{E/\sqrt{\pi_t}F}(z_i)) = \text{cor}_{E/F}(\sqrt{\pi_t})(y_i),
\]

and since \( y_i \in \iota_2^* \circ \iota_1^* (H^1(G_F, \mathbb{F}_2)) \),

\[
\text{cor}_{E/\sqrt{\pi_t}F}(y_i) = 2y_i = 0.
\]

Therefore,

\[
\text{cor}_{E/F}(y_i') = \text{cor}_{E/F}(e_i),
\]

and this implies \( u = 1 \), a contradiction. Therefore, (6) has been proved.

Finally, note that:

\[
\mathcal{X} = \langle \rho_1 e_2, e_2, \rho_2 e_2, \rho_1 e_1, e_1, \rho_2 e_1 \rangle
\]

if \( u = 0 \) and

\[
\mathcal{X} = \langle \rho_1 e_2, e_2, \rho_2 e_2, \rho_1 e_1, e_1, \rho_2 e_1 \rangle
\]

and it is routine to show that \( \mathcal{X} \cong \Omega(-1) \oplus \Omega(-1) \) in the first case and \( \Omega(-2) \) in the second, thus proving (7).

All parts of the proposition have been proved. QED

**Lemma 4.19. (Common Slot Lemma)** Let \( a, b, c, d \in F \) be such that: \( (a, b) \cong (c, d) \) as \( F \)-algebras. Then there is an \( e \in F \) such that:

\[
(a, b) \cong (a, e) \cong (c, e) \cong (c, d)
\]

as \( F \)-algebras.

**Proof of 4.19.** This is stated and proved as Lemma 7.6.8 of [GS]. An elementary proof of this fact is also outlined in Exercise I.6 of [GS]. QED
LEMMA 4.20. (Lemma 9 of [CMS]) Let $i$ and $j$ be any distinct elements of \{1, 2, 3\} and let $x \in F^\times/(F^\times)^2$ be such that:

\[
(a_i, x) \in (a_j, F^\times)
\]

in the group $2\text{Br}(F)/\mathcal{B}'$. Then:

\[
kum(x) \in \mathcal{A} + \sum_{\ell=1}^{3} \cor_{F(\sqrt{a_{\ell}})/F} (H^1(\text{Gal}(F^{\text{sep}}/F(\sqrt{a_{\ell}}), F_2))) .
\]

PROOF 4.20. We are given that there is a $y \in F^\times$ such that $(a_i, x) + (a_j, y) \in \mathcal{B}'$. Since $a_1a_2a_3 = 1$ in $F^\times/(F^\times)^2$,

\[
\mathcal{B}' = \{(a_i, a_i), (a_i, a_j), (a_j, a_j)\}.
\]

Thus, there are $d_1, d_2, d_3 \in \mathbb{Z}$ such that:

\[
0 = (a_i, x) + (a_j, y) + d_1(a_i, a_i) + d_2(a_i, a_j) + d_3(a_j, a_j) = (a_i, a_1^{d_1}a_2^{d_2}x) + (a_j, a_3^{d_3}y)
\]

in $\text{Br}(F)$. Thus, $(a_i, a_1^{d_1}a_2^{d_2}x) = (a_j, a_3^{d_3}y)$ and by the common slot lemma there is a $z \in F^\times$ such that:

\[
(a_i, a_1^{d_1}a_2^{d_2}x) = (a_i, z) = (a_j, z) = (a_j, a_3^{d_3}y)
\]

Then $(a_i, a_1^{d_1}a_2^{d_2}xz) = (a_i, a_j, z) = 0$, so

\[
da_1 \text{kum}(a_i) + d_2 \text{kum}(a_j) = \text{kum}(x) + \text{kum}(z) \in \cor_{F(\sqrt{a_{\ell}})/F} (H^1(\text{Gal}(F^{\text{sep}}/F(\sqrt{a_{\ell}}), F_2))) ,
\]

\[
\text{kum}(z) \in \cor_{F(\sqrt{a_{\ell}})/F} (H^1(\text{Gal}(F^{\text{sep}}/F(\sqrt{a_{\ell}}), F_2))) .
\]

Since $\text{kum}(a_i), \text{kum}(a_j) \in \mathcal{A}$, we therefore have:

\[
kum(x) \in \mathcal{A} + \sum_{\ell=1}^{3} \cor_{F(\sqrt{a_{\ell}})/F} (H^1(\text{Gal}(F^{\text{sep}}/F(\sqrt{a_{\ell}}), F_2))) ,
\]

as desired. QED

PROPOSITION 4.21. (Proposition 6 of [CMS]) Let $X$ and $Q \oplus Q'_X$ be as in Proposition 4.18. Then there is an $F_2[G]$-submodule $\mathcal{Y}$ of $H^1(G_E, F_2)$, together with an $F_2[G]$-submodule $W$ of $H^1(G_F, V)$ such that:

1. $W + (Q \oplus Q'_X \oplus R) = W \oplus Q \oplus Q'_X \oplus R$.
2. The following is an exact sequence:

\[
0 \longrightarrow W \overset{\text{sh} \circ \iota^*_2}{\longrightarrow} \mathcal{Y} \overset{\text{res} \circ \iota^*_2}{\longrightarrow} H^1(G_E, F_2) \longrightarrow 0.
\]

3. $\text{sh} \circ \iota^*_2$ maps $W^G$ isomorphically onto $\mathcal{Y}^G$.
4. $\pi^*_1$ maps $W \oplus Q \oplus R$ surjectively onto $((V/V^G) \otimes_{F_2} H^1(G_F, F_2)) \cap \ker(\delta^2)$.
5. $H^1(G_F, V) = W \oplus Q \oplus Q'_X \oplus R$.
6. $Q'_X \oplus W^G = \iota^*_2(H^1(G_F, F_2))$.
7. $\sum_{i=1}^{3} (y_i \mathcal{Y} \cap \mathcal{Y}^G) \subseteq \sum_{i \neq j} y_i \mathcal{Y}(x_j)$
8. $H^1(G_E, F_2) = \mathcal{X} \oplus \mathcal{Y}$.
Proof 4.21. Proof of (8) assuming the rest of the proposition: First we show that $X + Y = X \oplus Y$ by the Exclusion Lemma. To this end, note that $X^G = \iota_1^*(Q \oplus Q')$ and $Y_G = \iota_1^*(W^G)$. Furthermore, $Q \oplus Q'$ and $W^G$ are independent and $\iota_1^*$ is injective on both of these modules. Therefore, $X^G$ and $Y^G$ are independent, and therefore so are $X$ and $Y$.

By construction, $X + Y \subseteq H^1(G_E, F_2)$. Now let $w \in H^1(G_E, F_2)$ be arbitrary, and we will show that $w \in X + Y$. By (2) of this proposition, there is a $y \in Y$ such that:

$$\text{res}_{E/F} \text{cor}_{E/F}(w) = \text{res}_{E/F} \text{cor}_{E/F}(y).$$

Therefore, $\text{cor}_{E/F}(w - y) \in \ker(\text{res}_{E/F}) = \ker(\iota_2^* \iota_1^*) = A$, where the last equality is from Lemma 4.5. By Proposition 4.18(2), there is an element $x \in X$ such that:

$$\text{cor}_{E/F}(x) = \text{cor}_{E/F}(w - y).$$

Thus, $w - x - y \in \ker(\text{cor}_{E/F})$, which by Lemma 4.16 is $\text{sh}(\ker(\pi_2^*)) = \text{sh}(\iota_2^* (H^1(G_F, V)))$, which by (5) of this proposition is:

$$\text{sh}(\iota_2^* (W \oplus Q \oplus Q'^X)),$$

which by item (2) of this proposition and of Proposition 4.18 is contained in $X + Y$. Thus, $w - x - y \in X + Y$, so $w \in X + Y$ and $H^1(G_E, F_2) = X \oplus Y$, as desired.

The rest of the proof may be found in the original paper [CMS]. QED
Final Remarks and Directions for Possible Further Research

Item (8) of Proposition 4.21 shows that $H^1(G_E, \mathbb{F}_2) = \mathcal{X} \oplus \mathcal{Y}$. Item (7) of Proposition 4.18 shows that $\mathcal{X}$ is isomorphic to one of:

$$\Omega(-2) \quad \Omega(-1) \quad \Omega(-1) \oplus \Omega(-1) \quad \mathbb{F}_2^2 \quad \mathbb{F}_2 \quad 0.$$  

Item (7) of Proposition 4.21 and Proposition 2.6 show that $\mathcal{Y}$ is a direct sum of some cardinal number of the following modules.

$$\mathbb{F}_2[G] \quad \mathbb{F}_2[G]/(\rho_1) \quad \mathbb{F}_2[G]/(\rho_2) \quad \mathbb{F}_2[G]/(\rho_3) \quad \mathbb{F}_2 \quad \Omega(1) \quad \Omega(2) \quad \Omega(3).$$

Corollary 4.11 shows that $E^\times/(E^\times)^2 \cong H^1(G_E, \mathbb{F}_2)$, and 2.5 shows that the ten modules listed are indecomposable. We can therefore determine that there are only ten indecomposable modules that can appear in $E^\times/(E^\times)^2$, as well as what those ten modules are.

The original paper [CMS] contains a complete proof of Proposition 4.21, as well as computations which demonstrate how to find the cardinal number of times that of each of the eight indecomposable components of $\mathcal{Y}$ appear within $\mathcal{Y}$. The proofs are elementary, but also quite long.

[CMS] also contains similar decompositions in the case that char($F$) = 2. Much of the same machinery is used, except that Artin-Schreier theory is substituted for Kummer theory. However, the proof is a bit simpler because one can show that $H^2(G_F, \mathbb{F}_2)$ is trivial. One can show that $E^\times/(E^\times)^2$ itself satisfies the conditions of Proposition 2.6.

We have already mentioned the results of the papers [MS] and [MSS]. In these papers, the authors decompose $E^\times/(E^\times)^p$ in the event that Gal($E/F$) $\cong \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$, respectively.

Some time after discovering the results of [CMS], Professor John Swallow tried to perform a similar decomposition for when $F$ has characteristic not equal to 2 and $E$ is the field obtained by adjoining to $F$ all square roots of elements of $F$ contained in a fixed separable closure $F^{\text{sep}}$ of $F$. However, he said that this appeared to be fruitless so far.

Also, Markus Rost in [Ro] proves a version of the common slot lemma for cyclic algebras over fields that contain primitive cube roots of unity. Prof. Swallow has tried to use this version of the chain lemma as a tool to decompose $E^\times/(E^\times)^3$ in the event that Gal($E/F$) $\cong (\mathbb{Z}/3\mathbb{Z})^2$, but this has also been fruitless so far.
Bibliography


