1996

Some Lifting Problems in Arithmetic Equivalence.

Nancy C. Colwell

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_disstheses

Recommended Citation

https://repository.lsu.edu/gradschool_disstheses/6237

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6” x 9” black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700  800/521-0600

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
SOME LIFTING PROBLEMS IN ARITHMETIC EQUIVALENCE

A Dissertation
Submitted to the Graduate Faculty of the Louisiana State University and Agricultural and Mechanical College in partial fulfillment of the requirements for the degree of Doctor of Philosophy
in
The Department of Mathematics

by
Nancy C. Colwell
B.A., University of California at San Diego, 1982
M.S., Louisiana State University, 1992
August, 1996
Acknowledgments

The author wishes to thank her advisor, Professor Robert Perlis, for his help and encouragement during the preparation of this dissertation.

The author also wishes to thank her family and friends, for their support. Special thanks go to Hamza Ahmad from Al-Yarmouk University for his technical advice.
Table of Contents

Acknowledgements ................................................................. ii

Abstract ................................................................................ iv

Chapter

1. Introduction and Background .................................................. 1
   1.1 Arithmetic equivalence and Gassman equivalence .......... 1
   1.2 Permutation representations ............................................ 5
   1.3 Iwasawa $\mathbb{Z}_p$-towers ................................................. 7

2. Relative Equivalence ........................................................... 9
   2.1 Relative arithmetic equivalence ........................................ 9
   2.2 Relative Gassmann equivalence ......................................... 10
   2.3 Exceptional divisors .......................................................... 12

3. The Two Main Theorems ....................................................... 14
   3.1 The theorem for representations of groups ....................... 14
   3.2 The theorem for arithmetically equivalent fields .............. 17

4. The Lifting Problem ............................................................ 20
   4.1 Notation and description of the matrices ......................... 21
   4.2 The matrix $M \otimes I$ ........................................................ 23
   4.3 Examples ..................................................................... 26

Bibliography ............................................................................. 32

Vita......................................................................................... 34
Abstract

The main theorem in this dissertation provides a partial answer to the following question: Given a $\mathbb{Z}_p$-extension $F_\infty/F$ and a finite extension $K/F$, where $F$ is a number field and $p$ a prime number, to what extent does the $K$-splitting behavior the prime ideals of $F$ determine the Iwasawa invariants of the $\mathbb{Z}_p$-extension $K \cdot F_\infty/K$.

The answer is that if two fields $K$ and $L$ are arithmetically equivalent over $F$, then $K \cdot F_\infty/K$ and $L \cdot F_\infty/L$ have exactly the same Iwasawa invariants for any $\mathbb{Z}_p$-extension $F_\infty/F$, so long as $p$ is not an exceptional divisor for $K$ and $L$ over $F$. The exceptional divisors are a subset of the primes dividing the degree $[N : K]$, where $N$ is the normal closure of $K$ over $F$. The definition is found in Chapter 2.

This theorem comes as a corollary of a theorem concerning representations of finite groups which has importance in its own right. Its statement is: If $H$, $H'$, and $B$ are subgroups of a finite group $G$, with $B$ normal in $G$, and if the $\mathbb{Z}_q[G]$-modules $\mathbb{Z}_q[G/H]$ and $\mathbb{Z}_q[G/H']$ are isomorphic, then the $\mathbb{Z}_q[G]$-modules $\mathbb{Z}_q[G/H \cap B]$ and $\mathbb{Z}_q[G/H' \cap B]$ are also isomorphic.

This result is not constructive. Given a specific $\mathbb{Z}_q[G]$-map $M$ between $\mathbb{Z}_q[G/H]$ and $\mathbb{Z}_q[G/H']$, it does not tell us how to obtain a $\mathbb{Z}_q[G]$-map between $\mathbb{Z}_q[G/H \cap B]$ and $\mathbb{Z}_q[G/H' \cap B]$ which will be an isomorphism whenever $M$ is. Chapter 4 deals with this question, with some partial results for certain choices of $G$, in particular for the case when $G/B$ is abelian and $HB = H'B$. 

iv
Chapter 1
Introduction and Background

This dissertation deals with a connection between two subjects, arithmetic equivalence and Iwasawa theory, which have developed independently. The first has developed over the past century and the second over the past twenty years. Theorem 4 in Chapter 3 establishes a relationship between the two. The purpose of this chapter is to pull together some of the historical background of these two subjects. It also includes the basic definitions and lemmas used in later chapters.

1.1 Arithmetic equivalence and Gassmann equivalence

In 1880 Kronecker developed the idea of characterizing finite algebraic extensions of a number field by the splitting behavior of the prime ideals of the base field. In 1926 F. Gassmann showed that non-isomorphic number fields can share the decomposition behavior of prime ideals of the base field. One definition of arithmetically equivalent number fields is as follows:

**Definition 1.1.** Let $K$ be a finite extension of $\mathbb{Q}$, $O_K$ its ring of integers, and $p$ a rational prime. Let

$$pO_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$$

be the factorization of $p$ into distinct prime ideals of $O_K$. Let $f_i = (O_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z})$ be the inertia degree of $\mathcal{P}_i/p$, numbered so that $f_1 \leq \cdots \leq f_g$. Two number fields $K$ and $L$ are said to be arithmetically equivalent whenever every rational prime has the same sequence $\{f_1, \ldots, f_g\}$ in $K$ as in $L$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Arithmetically equivalent fields $K$ and $L$ share many field invariants such as the degree $[K:Q] = [L:Q]$, discriminant, and normal closure over $Q$ (see [P1]). There are several other characterizations of arithmetic equivalence, which are presented in Proposition 1.5 below. For this we need the following notion of equivalence of subgroups introduced by Gassmann.

**Definition 1.2.** Let $H$ and $H'$ be subgroups of a finite group $G$. $H$ and $H'$ are *Gassmann equivalent* in $G$ provided

$$|g^G \cap H| = |g^G \cap H'|$$

for all $g$ in $G$, where $g^G$ denotes the conjugacy class of $g$ in $G$.

The following two lemmas on Gassmann equivalence are used in the proof of Proposition 1.5. The first, which is Lemma 2 in [C], gives a useful criterion for determining when two subgroups are Gassmann equivalent.

**Lemma 1.3.** Let $H$ and $H'$ be subgroups of a finite group $G$. $H$ and $H'$ are Gassmann equivalent in $G$ if and only if there exists a bijection $\psi : H \rightarrow H'$, with $\psi(h)$ conjugate to $h$ in $G$, for all $h$ in $H$.

**Proof.** Suppose $|g^G \cap H| = |g^G \cap H'|$ for all $g$ in $G$. For each $h$ in $H$, $|h^G \cap H| = |h^G \cap H'|$, so there is a bijection $\psi$ from $h^G \cap H$ to $h^G \cap H'$. If $b$ is in $h^G \cap H$, we have $\psi(b)$ is conjugate to $h$, and thus also conjugate to $b$. As the $h^G \cap H$ and $h^G \cap H'$ partition $H$ and $H'$, we have a bijection from all of $H$ to $H'$ with the desired property.

Conversely, suppose such a bijection exists, and suppose $g^G \cap H$ and $g^G \cap H'$ are not both empty. Let $h$ be in $g^G \cap H$. Then $\psi(h)$ is in $h^G \cap H'$, which is the same as $g^G \cap H'$ as $h$ is conjugate to $g$. Since $\psi$ is injective, this shows that $|g^G \cap H| \leq |g^G \cap H'|$. By symmetry we also have the opposite inequality, so $|g^G \cap H| = |g^G \cap H'|$. $\square$
Lemma 1.4. Let $J$ be a normal subgroup of $G$ contained in $H \cap H'$. Then $H$ and $H'$ are Gassmann equivalent in $G$ if and only if $H/J$ and $H'/J$ are Gassmann equivalent in $G/J$.

Proof. Suppose $H$ and $H'$ are Gassmann equivalent in $G$. By Lemma 1.3 there is a bijection $\psi : H \to H'$ with $\psi(h)$ conjugate in $G$ to $h$. Since $J$ is a normal subgroup, $\psi(J) = J$. Then the map $\bar{\psi} : H/J \to H'/J$ defined by $\bar{\psi}([h]) = [\psi(h)]$, where $[g]$ denotes the coset $gJ$, is a bijection with $\bar{\psi}([h])$ conjugate in $G/J$ to $[h]$, for all $[h]$ in $H/J$.

Conversely, suppose such a bijection $\bar{\psi}$ exists. For each coset of $H/J$, choose a fixed representative $h$. Write each element in $[h]$ as $ha$, for some $a$ in $J$. Since $\bar{\psi}([h])$ is conjugate to $[h]$ in $G/J$, there is some $u$ in $G$ such that $\bar{\psi}([h]) = [u][h][u]^{-1} = [uhu^{-1}]$. Necessarily $uhu^{-1}$ is in $H'$ as $\bar{\psi}([h])$ is in $H'/J$. Set $\psi(ha) = uha = (uhu^{-1})(ua^{-1})$. Since $ua^{-1}$ is in $J$, we have $\psi(ha)$ in $\bar{\psi}([h])$. Since the cosets partition $H$ and $H'$, and $\bar{\psi}$ is a bijection, $\psi$ is the desired bijection between $H$ and $H'$. □

Proposition 1.5. Let $K$ and $L$ be finite extensions of $Q$. The following are equivalent:

1. $K$ and $L$ are arithmetically equivalent.
2. $\zeta_K(s) = \zeta_L(s)$ for all complex numbers $s$, where $\zeta_K(s)$ is the Dedekind zeta function of a number field $K$.
3. Every rational prime has the same number of prime divisors in $K$ as in $L$.
4. There exists $N$, a finite normal extension of $Q$ containing $K$ and $L$, such that the Galois groups $Gal(N/K)$ and $Gal(N/L)$ are Gassmann equivalent in $Gal(N/Q)$.
5. The Galois groups $Gal(N/K)$ and $Gal(N/L)$ are Gassmann equivalent in $Gal(N/Q)$, for every finite normal extension $N/Q$ containing $K$ and $L$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
PROOF. For the equivalence of 1, 2, and 4, see [P1]. For the equivalence of 1 and 3, see [S-P]. That 5 implies 4 is trivial. To see that 4 implies 5, suppose there exists $N$ with $\text{Gal}(N/K)$ and $\text{Gal}(N/L)$ Gassmann equivalent in $\text{Gal}(N/Q)$, and let $N'$ be any other normal extension of $\mathbb{Q}$ containing both $K$ and $L$. Let $\bar{N}$ be a normal extension of $\mathbb{Q}$ containing both $N$ and $N'$. Now both $\text{Gal}(\bar{N}/N)$ and $\text{Gal}(\bar{N}/N')$ are normal subgroups of $\text{Gal}(\bar{N}/\mathbb{Q})$ contained in $\text{Gal}(\bar{N}/K) \cap \text{Gal}(\bar{N}/L)$. So by using Lemma 1.4, the Gassmann equivalence of $\text{Gal}(N/K)$ and $\text{Gal}(N/L)$ in $\text{Gal}(N/Q)$ (which the same as to $\text{Gal}(\bar{N}/\mathbb{Q})/\text{Gal}(\bar{N}/N)$) implies that $\text{Gal}(\bar{N}/K)$ and $\text{Gal}(\bar{N}/L)$ are Gassmann equivalent in $\text{Gal}(\bar{N}/\mathbb{Q})$, which in turn implies that $\text{Gal}(N'/K)$ and $\text{Gal}(N'/L)$ are Gassmann equivalent in $\text{Gal}(N'/\mathbb{Q})$.

The characterization of Gassmann equivalence in terms of permutation representations is discussed in the following section. We complete the background on Gassmann equivalence with a lemma of K. Uchida (see [U]). It is stated here in terms of Gassmann equivalence of subgroups rather than the arithmetic equivalence of field extensions.

**Lemma 1.6.** If $H$ and $H'$ are Gassmann equivalent in a finite group $G$, and if $B$ is a normal subgroup of $G$, then $H \cap B$ and $H' \cap B$ are also Gassmann equivalent in $G$.

**PROOF.** Since $B$ is normal in $G$, every conjugacy class $g^G$ is either contained completely in $B$ or is disjoint from $B$. If $g^G$ is disjoint from $B$, $|g^G \cap H \cap B| = |g^G \cap H' \cap B| = 0$. If $g^G$ is contained in $B$, $g^G \cap B = g^G$. So $|g^G \cap H \cap B| = |g^G \cap H|$ and $|g^G \cap H' \cap B| = |g^G \cap H'|$. So if $|g^G \cap H| = |g^G \cap H'|$, we also have $|g^G \cap H \cap B| = |g^G \cap H' \cap B|$.

□
1.2 Permutation representations

We wish to describe Gassmann equivalence in terms of linear representations. We start with some basic definitions. Throughout this section $R$ denotes an integral domain, and all groups are finite.

**Definition 1.7.** Let $G$ be a group. Let $V$ be a finite dimensional free $R$-module. A *linear representation* of $G$ on $V$ is a homomorphism $\rho$ from $G$ to $\text{Aut}(V)$, the group of automorphisms of $V$.

Concretely, for each $g$ in $G$, $\rho(g)$ is an $R$-module automorphism with $\rho(g_1g_2)(v) = \rho(g_1)(\rho(g_2)(v))$, $\rho(1_G)(v) = (v)$ (where $1_G$ is the identity element in $G$), for all $v$ in $V$. We also have $\rho(g^{-1}) = \rho(g)^{-1}$. The representation space $V$ is an $R[G]$-module, with scalar multiplication given by $gv = \rho(g)(v)$, which extends by linearity to all of $R[G]$. We also say that $\rho$ is a linear representation of $G$ over $R$.

**Definition 1.8.** Two representations $\rho$ and $\rho'$ from a group $G$ to $\text{Aut}(V)$ and $\text{Aut}(V')$ respectively, are *isomorphic* if $V$ and $V'$ are isomorphic as $R[G]$-modules. In other words, there exists an $R$-module isomorphism $\alpha : V \rightarrow V'$ such that $\alpha(\rho(g)(v)) = \rho'(g)\alpha(v)$ for all $g$ in $G$ and $v$ in $V$.

**Definition 1.9.** Let $\rho$ be a linear representation of a finite group $G$ over $R$. The *character* of the representation $\rho$ is the function $\chi_\rho : G \rightarrow R$ given by $\chi_\rho(g) = \text{trace}(\rho(g))$ for each $g \in G$.

**Proposition 1.10.** Two representations on vector spaces over a field of characteristic 0 with the same character are isomorphic.

**Proof.** See [S], proposition 3.3. □

A *permutation representation* of a group $G$ is a representation which arises in the following way. Let $S$ be a $G$-set, that is, a set on which $G$ acts. Consider
a free $R$-module $V$ with basis elements indexed by the elements of $S$. The elements of $G$ act on this module by permuting the basis elements, making it an $R[G]$-module, denoted $R[S]$. Specifically, $R[S] = \{ \sum_{s \in G} r_s s : r_s \in R \}$. The corresponding representation $\rho : G \rightarrow \text{Aut}(R[S])$ is given by $\rho(g)([s]) = [s']$, where $s' = g(s)$. If $\chi$ is the character of this representation, then for all $g$ in $G$, $\chi(g)$ is just the number of elements of $S$ which are fixed by $g$.

We are interested in a particular permutation representation of a group $G$ induced from a subgroup $H$ of $G$. $G$ acts on the set $G/H$ by permuting the cosets by left translation. The permutation representation of $G$ defined by this action is called the representation of $G$ induced by the trivial representation of $H$, and the corresponding $R[G]$-module will be denoted $R[G/H]$. The character $\chi$ of this representation is given by

$$\chi(g) = \frac{|C_G(g)| \cdot |g^G \cap H|}{|H|}$$

(1)

where $C_G(G)$ is the center of $g$ in $G$. (See [S], Theorem 12.) The Gassmann equivalence of two subgroups $H$ and $H'$ also implies $|H| = |H'|$. So by Proposition 1.10, equation (1) shows:

**Proposition 1.11.** Let $k$ be a field of characteristic $0$. Let $H$ and $H'$ be subgroups of a finite group $G$. $H$ and $H'$ are Gassmann equivalent in $G$ if and only if $k[G/H] \cong k[G/H']$ as $k[G]$-modules.

We are primarily interested in $R[G]$-modules when $R$ is either $\mathbb{Q}$, a finite field $\mathbb{F}_q$, where $q$ is a prime number, or the ring of $q$-adic integers $\mathbb{Z}_q$. If $R$ is not a field of characteristic $0$ (or of characteristic prime to the order of $G$), representations over $R$ are not in general determined up to isomorphism by their character. But in the cases $R = \mathbb{Z}_q$ and $R = \mathbb{F}_q$, the Krull-Schmidt-Azumaya Theorem says that $R[G]$-modules do have a structure which we can, in some way, determine.
THEOREM 1.12. (Krull-Schmidt-Azumaya) Let $R$ be a complete commutative noetherian local ring, and $A$ an $R$-algebra which is finitely generated as an $R$-module. Let $M$ be a finitely generated $A$-module.

Then $M$ is expressible as a finite direct sum of indecomposable submodules, and this expression is unique up to isomorphism and the order of the summands.

PROOF. For a proof, one reference is [C-R], Volume 1, Theorem 6.12. □

1.3 Iwasawa $\mathbb{Z}_p$-towers.

In 1959, K. Iwasawa established a formula giving the $p$-order of the class number of the $n$-th field in a $\mathbb{Z}_p$-extension of a number field $K$. In this section, some basic facts about Iwasawa theory and $\mathbb{Z}_p$-extensions are reviewed.

DEFINITION 1.13. Let $K$ be an algebraic number field, $p$ a prime number. A Galois extension $K_\infty/K$ is called a $\mathbb{Z}_p$-extension if its Galois group is isomorphic to the additive group $\mathbb{Z}_p$ of $p$-adic integers.

For every $\mathbb{Z}_p$-extension there is a unique tower of fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_\infty = \bigcup_{n=1}^{\infty} K_n$$

with $K_n/K$ a cyclic extension of degree $p^n$. These are the only fields between $K$ and $K_\infty$. (See e.g. [W1] section 13.1.)

Every number field $K$ has at least one $\mathbb{Z}_p$-extension called the cyclotomic $\mathbb{Z}_p$-extension of $K$. It is obtained as follows. For each $n$, consider the cyclotomic field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}}$ is a primitive $p^{n+1}$ root of unity. (If $p = 2$, take $\mathbb{Q}(\zeta_{2^{n+1}})$ instead.) By standard Galois theory, $\mathbb{Q}(\zeta_{p^{n+1}})$ has a unique subfield which is a cyclic extension of $\mathbb{Q}$ of degree $p^n$. Denote this field $Q_n$. Then

$$\mathbb{Q} \subset Q_1 \subset Q_2 \subset \cdots \subset Q_\infty = \bigcup_{n=1}^{\infty} Q_n$$

is a $\mathbb{Z}_p$-tower over $\mathbb{Q}$. Let $K$ be any finite extension of $\mathbb{Q}$. Then the compositum
\( K \cdot Q_\infty \) is a \( \mathbb{Z}_p \)-extension of \( K \). This is the cyclotomic \( \mathbb{Z}_p \)-extension of \( K \). (See [W1], section 7.3.)

Let \( K_n \) be the subfield with degree \( p^n \) over \( K \) in a given \( \mathbb{Z}_p \)-extension \( K_\infty /K \). Let \( A_n \) be the Hilbert \( p \)-class field of \( K_n \), so that the Galois group of \( A_n/K_n \) is isomorphic to \( Cl_p(K_n) \), the \( p \)-Sylow subgroup of the ideal class group of \( K_n \). Taking projective limits of these Galois groups produces the profinite group \( X_{K_\infty} = X(K_\infty/K) \). This \( X_{K_\infty} \) is a module over the ring of formal power-series \( \Lambda = \mathbb{Z}_p[[T]] \). Sometimes \( X_{K_\infty} \) is referred to as the Iwasawa module, and \( \Lambda \) as the Iwasawa algebra. By studying the structure of these \( \Lambda \)-modules, Iwasawa determined the behavior of the \( p \)-part of the class number of the field \( K_n \). His formula is:

**Theorem 1.14.** Let \( K \) be a number field, \( p \) a prime number, and

\[ K = K_0 \subset K_1 \subset \cdots \subset K_\infty \]

a \( \mathbb{Z}_p \)-tower. Let \( p^n \) be the exact power of \( p \) dividing the class number of \( K_n \). Then there exist integers \( \lambda, \mu, \nu \) and \( n_0 \) such that \( e_n = \lambda n + \mu p^n + \nu \) for all \( n \geq n_0 \).

**Proof.** See [I] or [W1], section 13.3. □

The integers \( \lambda, \mu, \) and \( \nu \) are called the Iwasawa invariants of the extension \( K_\infty/K \). In 1983, K. Komatsu established a connection between arithmetic equivalence and Iwasawa \( \mathbb{Z}_p \)-towers. Among other things, he showed:

**Theorem 1.15.** Let \( K \) and \( L \) be fields which are arithmetically equivalent over \( \mathbb{Q} \). Let \( N \) be the normal closure of \( K \) over \( \mathbb{Q} \), let \( p \) be any prime number not dividing the degree \( [N: \mathbb{Q}] \), and let \( K_\infty \) and \( L_\infty \) denote the cyclotomic \( \mathbb{Z}_p \)-extensions of \( K \) and \( L \). Then \( X_{K_\infty} \) and \( X_{L_\infty} \) are isomorphic \( \Lambda \)-modules.

**Proof.** The proof is in [K1]. □
Chapter 2
Relative Equivalence

In this chapter, the notions of arithmetic equivalence and Gassmann equivalence are both generalized. We also introduce an invariant of equivalent subgroups, and consequently of equivalent fields, the set of exceptional divisors. The definition and description of these divisors is found in Section 2.3, which also contains an important consequence of a prime not being exceptional.

2.1 Relative arithmetic equivalence

In Section 1.1, arithmetic equivalence was defined for finite extensions of $\mathbb{Q}$. We generalize this notion to arbitrary fields with the following definition:

**Definition 2.1.** Two finite, separable extensions $K$ and $L$ of a field $F$ are said to be *arithmetically equivalent over $F$* when $\text{Gal}(N/K)$ and $\text{Gal}(N/L)$ are Gassmann equivalent in $\text{Gal}(N/F)$, where $N$ is the normal closure over $F$ of the compositum $K \cdot L$.

Just as in Proposition 1.5, this definition is unaffected when the normal closure $N$ is replaced by any other normal extension of $F$ containing both $K$ and $L$.

If $F$ is a number field, parts 1, 3, 4, and 5 of Proposition 1.5 still hold when "rational prime" is replaced by "prime ideal of $F". We still have that arithmetic equivalence over $F$ implies $\zeta_K(s) = \zeta_L(s)$, but in general, not the converse.
2.2 Relative Gassmann equivalence

We know from Proposition 1.11 that two subgroups of a finite group $G$ are Gassmann equivalent in $G$ if and only if $\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules. However, we are interested in a stronger condition, $\mathbb{Z}_q[G/H] \cong \mathbb{Z}_q[G/H']$ as $\mathbb{Z}_q[G]$-modules. With this in mind, we make the following definition which generalizes the notion of Gassmann equivalence.

**Definition 2.2.** Let $R$ be an integral domain. Two subgroups $H$ and $H'$ of a finite group $G$ are said to be $R$-Gassmann equivalent in $G$ provided

$$R[G/H] \cong R[G/H']$$


By Proposition 1.11, $\mathbb{Q}$-Gassmann equivalence (or $k$-Gassmann equivalence, where $k$ is any field of characteristic 0) is the same as regular Gassmann equivalence as defined in Definition 1.2. We have an analogue to Lemma 1.4.

**Lemma 2.3.** Let $H$ and $H'$ be subgroups of a finite group $G$. Let $\mathcal{G}$ be a finite group with $\phi : \mathcal{G} \rightarrow G$ a surjective homomorphism. Let $\mathcal{H}$ and $\mathcal{H}'$ be the preimages of $H$ and $H'$ in $\mathcal{G}$. Then $H$ and $H'$ are $R$-Gassmann equivalent in $G$ if and only if $\mathcal{H}$ and $\mathcal{H}'$ are $R$-Gassmann equivalent in $\mathcal{G}$.

**Proof.** Note that the kernel of $\phi$ is a normal subgroup of $\mathcal{G}$ contained in both $\mathcal{H}$ and $\mathcal{H}'$. It follows that this kernel acts trivially by left translation on $\mathcal{G}/\mathcal{H}$. Elements of $\mathcal{G}$ act on $G/H$ via $\phi$, and elements of $G$ act on $\mathcal{G}/\mathcal{H}$ by taking any preimage under $\phi$. This is well defined, since for $g_1$ and $g_2$ in $\mathcal{G}$, $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2k$ for some $k$ in the kernel of $\phi$. So $g_1g\mathcal{H} = g_2kg\mathcal{H} = g_2(g^{-1}kg)\mathcal{H} = g_2g\mathcal{H}$, for all $g$ in $\mathcal{G}$. This allows us to identify $\mathcal{G}/\mathcal{H}$ and $G/H$ both as $\mathcal{G}$-sets as well as $G$-sets. We similarly identify $\mathcal{G}/\mathcal{H}'$ and $G/H'$ as both $\mathcal{G}$-sets and $G$-sets. From this, the Lemma follows. □
Lemma 2.4. For subgroups $H$ and $H'$ of a finite group $G$:

1. $H$ and $H'$ are $\mathbb{Z}_q$-Gassmann equivalent in $G$ if and only if they are $\mathbb{F}_q$-Gassmann equivalent in $G$, for every prime number $q$. (Here $\mathbb{F}_q \cong \mathbb{Z}/q\mathbb{Z}$ is the finite field with $q$ elements.)

2. If $H$ and $H'$ are $\mathbb{Z}_q$-Gassmann equivalent in $G$, for any prime number $q$, then they are also $\mathbb{Q}$-Gassmann equivalent.

3. If $H$ and $H'$ are $\mathbb{Q}$-Gassmann equivalent then they are also $\mathbb{Z}_q$-Gassmann equivalent for all but finitely many primes $q$.

Proof. $R[G/H]$ and $R[G/H']$ are isomorphic $R[G]$-modules if and only if $H$ and $H'$ have the same index, $n$, in $G$ and there is an $R$-module isomorphism between $R[G/H]$ and $R[G/H']$ which commutes with the action of $G$. By picking bases for $R[G/H]$ and $R[G/H']$, this isomorphism is given by an invertible $n$-by-$n$ matrix $M$ with coefficients in $R$. Suppose $M$ produces a $\mathbb{Z}_q[G]$-equivalence between $H$ and $H'$. Reducing the entries of $M$ mod $q$ then produces an $\mathbb{F}_q$-equivalence. Next, suppose $M$ produces a $\mathbb{F}_q$-equivalence. Let $S$ be a fixed set of representatives in $\mathbb{Z}$ for $\mathbb{F}_q$. Then the matrix $\tilde{M}$ obtained by replacing each entry in $M$ with its representative in $S$ will be a $\mathbb{Z}_q[G]$-homomorphism between $\mathbb{Z}_q[G/H]$ and $\mathbb{Z}_q[G/H']$. The determinant of $\tilde{M}$ is congruent modulo $q$ to the determinant of $M$, which is nonzero mod $q$, hence a unit of $\mathbb{Z}_q$. Thus, $\tilde{M}$ is the required $\mathbb{Z}_q$-equivalence. This proves 1. Moreover, $\tilde{M}$ is an integral matrix of non-zero determinant, commuting with the actions of $G$. This shows that $H$ and $H'$ are $\mathbb{Q}$-Gassmann equivalent, proving 2 as well.

For 3, let $M$ be a matrix giving a $\mathbb{Q}[G]$-module isomorphism. Multiplying $M$ by the least common multiple of the denominators of the rational entries of $M$ produces an integral matrix giving a $\mathbb{Z}_q[G]$-module homomorphism between
$\mathbb{Z}_q[G/H]$ and $\mathbb{Z}_q[G/H']$ for all $q$, which is an isomorphism whenever $q$ does not divide the determinant of $M$. This proves 3. □

2.3 Exceptional divisors

Let $H$ and $H'$ be subgroups of a finite group $G$. The set of exceptional divisors for the subgroups $H$ and $H'$ in $G$ is defined as follows:

**Definition 2.5.** Given two subgroups $H$ and $H'$ of a finite group $G$, an *exceptional divisor* is any prime number $q$ for which $\mathbb{Z}_q[G/H]$ and $\mathbb{Z}_q[G/H']$ fail to be isomorphic as $\mathbb{Z}_q[G]$-modules.

By Lemma 2.4, the set of exceptional divisors is finite if and only if $H$ and $H'$ are Gassmann equivalent in $G$; all prime numbers are exceptional otherwise.

For a more concrete description of this set for the case when $H$ and $H'$ are Gassmann equivalent in $G$, consider the set $\mathcal{M}$ of all $n \times n$ integral matrices, where $n = [G:H] = [G:H']$, giving a $\mathbb{Q}[G]$-isomorphism between $\mathbb{Q}[G/H]$ and $\mathbb{Q}[G/H']$, as in the proof of Lemma 2.4. Let $D$ be the greatest common divisor of the set $\{\det(M) : M \in \mathcal{M}\}$. Then the set of exceptional divisors for $H$ and $H'$ in $G$ is precisely the set of prime divisors of $D$, which is clearly finite.

**Proposition 2.6.** If $H$ and $H'$ are Gassmann equivalent, the set of exceptional divisors for $H$ and $H'$ is contained in the set of the prime divisors of $|H|$.

**Proof.** For a proof of this, examples in which the set of exceptional divisors is properly contained in the set of primes dividing $|H|$, as well as a more detailed description of the set $\mathcal{M}$, see [P2], section 2. □

When $G$ is the Galois group of a normal extension of fields $N/F$, and $K$ and $L$ are the fixed fields of $H$ and $H'$ respectively, then an exceptional divisor for $H$ and $H'$ in $G$ is also called an exceptional divisor for $K$ and $L$ over $F$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Using Lemma 2.3 and an argument identical to the one found in the proof of Proposition 1.5, the set of exceptional divisors for $K$ and $L$ over $F$ does not depend on the choice of overfield $N$, as long as $N$ is normal over $F$ and contains $K$ and $L$. By Lemma 2.4, the set of exceptional divisors for $K$ and $L$ over $F$ is finite if and only if $K$ and $L$ are arithmetically equivalent over $F$, and every prime is exceptional otherwise. Also, by Proposition 2.6, when $K$ and $L$ are arithmetically equivalent over $F$, the exceptional divisors are found among the prime numbers dividing $[N:K]$, where $N$ is the normal closure of $K$ over $F$.

The following result, essential for the theorem of section 3.2, is a restatement of Theorem 3 of [P2]. All of [P2] is stated and proved for the case when the base field $F$ is $\mathbb{Q}$; the statement and proof of Theorem 3 remains valid when $\mathbb{Q}$ is replaced by a number field $F$. For a more sophisticated point of view, see [R-S].

**Theorem 2.7.** If $q$ is a prime number that is not an exceptional divisor for arithmetically equivalent number fields $K$ and $L$ over $F$, then the $q$-Sylow subgroups of the ideal class groups of $K$ and $L$ are isomorphic:

$$\text{Cl}_K(q) \cong \text{Cl}_L(q).$$
Chapter 3
The Two Main Theorems

The second theorem discussed in this chapter, Theorem 3.4, generalizes Komatsu's result in two ways. First, by looking at arithmetic equivalence over base fields $F$ other than $\mathbb{Q}$, we can consider non-cyclotomic $\mathbb{Z}_p$-extensions; our results apply equally well in this richer context. Second, rather than excluding all the prime divisors of $[N:F]$, where $N$ denotes the normal closure of $K \cdot L$ over $F$, we only need to exclude the exceptional divisors. Theorem 3.4 is actually a corollary of Theorem 2.7 and Theorem 3.3 of this chapter, which is group-theoretic in nature. Theorem 3.3 is of interest in its own right as a result about subgroups which induce isomorphic permutation representations.

3.1 The theorem for representations of groups

The central theorem of this section generalizes Uchida's Lemma. It is used in the proof of the theorem in the next section, and is the key step which allows us to exclude only the exceptional divisors, rather than all of the divisors of $[N:F]$.

We need the following lemma which is a corollary of the Krull-Schmidt-Azumaya Theorem. The notation $\oplus^d L$ denotes the direct sum of $d$ copies of a module $L$.

**Lemma 3.1.** Let $L$ and $M$ be finitely generated $\mathbb{Z}_q[G]$-modules, where $G$ is a finite group. If $\oplus^d L \cong \oplus^d M$ for some positive integer $d$, then $L \cong M$.

**Proof.** When $G$ is finite, $\mathbb{Z}_q[G]$ satisfies the conditions for $A$ in Theorem 1.12. So we may write both $L$ and $M$ as a direct sum of indecomposable
submodules. Write $L \cong \bigoplus_{j=1}^r (\oplus^{l_j} L_j)$ and $M \cong \bigoplus_{k=1}^s (\oplus^{m_k} M_k)$, where each $l_j$ and $m_k$ are positive integers, and the $L_j$, respectively the $M_k$, are pairwise distinct indecomposable $\mathbb{Z}[G]$-modules. But we can also write the isomorphic modules $\bigoplus^d L \cong \bigoplus^d M$ uniquely as a direct sum of indecomposable submodules, say $\bigoplus_{i=1}^t (\oplus^{n_i} N_i)$, where the $N_i$ are also pairwise distinct. So we have

$$\bigoplus_{j=1}^r (\oplus^{l_j} L_j) \cong \bigoplus_{i=1}^t (\oplus^{n_i} N_i) \cong \bigoplus_{k=1}^s (\oplus^{m_k} M_k).$$

So, after reordering, we must have $r = s = t$, $L_i \cong N_i \cong M_i$, and $dl_i = n_i = dm_i$ for all $i$. Since this also means $l_i = m_i$ for all $i$, $L \cong M$. □

**Lemma 3.2.** Let $H$ and $B$ be subgroups of a finite group $G$, with $B$ normal in $G$. Let $R$ be an integral domain. Let $d$ denote the index of $HB$ in $G$. Then

$$R[G/H] \otimes R[G/B] \cong \bigoplus^d R[G/(H \cap B)]$$


**Proof.** Consider the $G$-set $G/H \times G/B$, on which $G$ acts componentwise by $g(g_1H, g_2B) = (gg_1H, gg_2B)$. Each $G$-orbit in this set contains an element of the form $(H, gB)$, since, if the orbit contains the arbitrary element $(g_1H, g_2B)$, it must also contain $g_i^{-1}(g_1H, g_2B) = (H, g_i^{-1}g_2B)$. The $G$-stabilizer of $(H, gB)$ is $H \cap gBg^{-1}$, which is $H \cap B$ since $B$ is normal in $G$. Thus, each orbit is isomorphic to a copy of $G/(H \cap B)$.

Now let $\{g_1, \ldots, g_d\}$ be a complete set of coset representatives for $G/HB$. We claim every orbit contains exactly one element of the form $(g_iH, B)$, for some $g_i$. To see this, suppose an orbit contains the element $(H, gB)$. Since the $g_i$ are a complete set of coset representatives, we can write $g^{-1}$ as $g_ihb$, for some $i$, with $h$ in $H$ and $b$ in $B$. Then the orbit also contains $g_ih(H, gB)$. But since $g_ih = g^{-1}b^{-1}$, $g_ih(H, gB) = (g_ihH, g^{-1}b^{-1}gB) = (g_iH, B)$. Now suppose $(g_iH, B)$ and $(g_jH, B)$ are in the same orbit. That means there is some $a$ in
$G$ with $a(g_iH, B) = (g_jH, B)$. Since $aB = B$, $a$ is in $B$. Also, $ag_iH = g_jH$; so $ag_i = g_jh$ for some $h$ in $H$. So $g_j^{-1}a = hg_i^{-1}$, and $g_j^{-1}g_i = h(g_j^{-1}a^{-1}g_i)$, so is in $HB$. Since the $g_i$ are representatives for the cosets of $HB$, this is impossible unless $i = j$. So there are exactly $d = [G : HB]$ orbits.

Therefore $R[G/H \times G/B] \cong \oplus^d R[G/(H \cap B)]$, as $R[G]$-modules. But we also have $R[G/H \times G/B] \cong R[G/H] \otimes R[G/B]$, the tensor product taken over $R$. The lemma follows. □

**Theorem 3.3.** Let $H$ and $H'$ be $\mathbb{Z}_q$-Gassmann equivalent subgroups of a finite group $G$, and let $B$ be a normal subgroup of $G$. Then $H \cap B$ and $H' \cap B$ are also $\mathbb{Z}_q$-Gassmann equivalent in $G$.

**Proof.** By Lemma 3.2

$$\mathbb{Z}_q[G/H] \otimes \mathbb{Z}_q[G/B] \cong \oplus^{[G:H_B]} \mathbb{Z}_q[G/(H \cap B)],$$  \hspace{1cm} (1)

and

$$\mathbb{Z}_q[G/H'] \otimes \mathbb{Z}_q[G/B] \cong \oplus^{[G:H'_B]} \mathbb{Z}_q[G/(H' \cap B)].$$  \hspace{1cm} (2)

The left sides of equations (1) and (2) are isomorphic as $\mathbb{Z}_q[G]$-modules since we have tensored the isomorphic $\mathbb{Z}_q[G]$-modules $\mathbb{Z}_q[G/H] \cong \mathbb{Z}_q[G/H']$ with the same module $\mathbb{Z}_q[G/B]$. Thus the right sides are isomorphic $\mathbb{Z}_q[G]$-modules.

By part 2 of Lemma 2.4, $H$ and $H'$ are $\mathbb{Q}$-Gassmann equivalent, so by Lemma 1.6, $H \cap B$ and $H' \cap B$ are $\mathbb{Q}$-Gassmann equivalent. Thus $H \cap B$ and $H' \cap B$ have the same index in $G$. It follows that subgroups $HB$ and $H'B$ also have the same index, $d$, in $G$. Therefore $\oplus^d \mathbb{Z}_q[G/(H \cap B)]$ is isomorphic to $\oplus^d \mathbb{Z}_q[G/(H' \cap B)]$.

Now $\mathbb{Z}_q[G/(H \cap B)]$ and $\mathbb{Z}_q[G/(H' \cap B)]$ are finitely-generated $\mathbb{Z}_q[G]$-modules. So we can apply Lemma 3.1 to conclude that $\mathbb{Z}_q[G/(H \cap B)]$ is isomorphic to $\mathbb{Z}_q[G/(H' \cap B)]$. □
3.2 The theorem for arithmetically equivalent fields

**Theorem 3.4.** Let $p$ be any prime number. Let $K$ and $L$ be number fields arithmetically equivalent over a number field $F$. Let $q$ be a non-exceptional divisor for $K$ and $L$ over $F$, possibly equal to $p$. Let $F_\infty/F$ be any $\mathbb{Z}_p$-extension. Finally, let $K_n$ (respectively $L_n$) denote the subfield of degree $p^n$ over $K$ (respectively $L$) in the $\mathbb{Z}_p$-extension $K \cdot F_\infty/K$ (respectively $L \cdot F_\infty/L$). Then the $q$-Sylow subgroups of the ideal class groups of $K_n$ and $L_n$ are isomorphic:

$$Cl_q(K_n) \cong Cl_q(L_n)$$

for $n \geq 0$.

**Proof.** Fix an index $n$. Then $K_n = K \cdot F_j$ for some index $j \geq n$. (In fact $j = n + e$, where $e$ is the index given by $K \cap F_\infty = F_e$. Since $Gal(K \cdot F_j/K) \cong Gal(F_j/K \cap F_j) = Gal(F_j/F_e)$, it follows that $K \cdot F_j$ is the unique subfield of $K \cdot F_\infty$ with degree $p^n$ over $K$.) Let $N$ be a normal extension of $F$ containing $K$, $L$, and $F_j$. Put $G = Gal(N/F)$, $H = Gal(N/K)$, $H' = Gal(N/L)$, and $B = Gal(N/F_j)$. By our hypothesis on the prime $q$ and Lemma 2.3, $H$ and $H'$ are $\mathbb{Z}_q$-Gassmann equivalent subgroups of $G$, and $B$ is a normal subgroup of $G$. By Theorem 3.3, the subgroups $H \cap B$ and $H' \cap B$ are $\mathbb{Z}_q$-Gassmann equivalent in $G$. Their fixed fields are $K_n$ and $L \cdot F_j$. Thus these fields have the same degree over $F$. Since $K$ and $L$ also have the same degree over $F$, it follows that $L \cdot F_j$ is the field $L_n$. So $K_n$ and $L_n$ are arithmetically equivalent over $F$, and $q$ is non-exceptional for $K_n$ and $L_n$ over $F$. The rest follows from Theorem 2.7. \hfill \Box

The special case $q = p$ is of special interest. Recall from Section 1.3 the Iwasawa modules $X_{K_\infty}$, the projective limit of the groups $Cl_p(K_n)$. Putting $p = q$ into Theorem 3.4 yields the following result:
COROLLARY 3.5. Let $p$ be a nonexceptional divisor for $K$ and $L$ over a number field $F$. Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension, put $K_\infty = K \cdot F_\infty$ and put $L_\infty = L \cdot F_\infty$. Then

1. the Iwasawa modules $X_{K_\infty}$ and $X_{L_\infty}$ are isomorphic $\Lambda$-modules, and

2. $K_\infty/K$ and $L_\infty/L$ have the same Iwasawa invariants.

PROOF. Since we have $Cl_p(K_n) = Cl_p(L_n)$ for all $n$, 1 is clear; only 2 remains to be proved. The $p$-parts of the ideal class numbers of $K_n$ and of $L_n$ agree, for all $n \geq 0$. Hence, writing Iwasawa's formula for consecutive large indices $n$ and $n + 1$ gives

$$\lambda_K(n + 1) + \mu_K p^{n+1} + \nu_K = \lambda_L(n + 1) + \mu_L p^{n+1} + \nu_L$$

and

$$\lambda_K(n) + \mu_K p^n + \nu_K = \lambda_L(n) + \mu_L p^n + \nu_L.$$ 

Then subtracting shows

$$\lambda_K + \mu_K p^n (p - 1) = \lambda_L + \mu_L p^n (p - 1).$$

Hence, $\lambda_K - \lambda_L = (\mu_L - \mu_K) (p - 1) p^n$ for all large $n$. Since the left side is constant and the right side depends on $n$, we conclude that $\mu_K = \mu_L$ and $\lambda_K = \lambda_L$, whence also $\nu_K = \nu_L$. □

We conclude the chapter with an example borrowed from [P2], pages 503-505.

EXAMPLE 3.6. Let $G$ be the simple group of order 168. Let $H$ and $H'$ represent the two conjugacy classes of subgroups of index 7 in $G$. These are known to be Gassmann equivalent, and the only exceptional divisor is the prime number 2. Embed $G$ as a Galois group $G \cong Gal(N/F)$ for some number field $F$, and let $K$ and $L$ be the fixed fields of $H$ and $H'$. Then 2 is the only
exceptional divisor for $K$ and $L$ over $F$, while the degree $[N:F]$ is divisible by 2, 3, and 7. We conclude that, for any $\mathbb{Z}_p$-extension $F_\infty/F$, the Iwasawa invariants of the composite towers $K\cdot F_\infty/K$ and of $L\cdot F_\infty/L$ agree, for $p$ odd. This holds in particular for the primes 3 and 7.
Chapter 4
The Lifting Problem

Throughout this chapter $G$ is a finite group. $H, H'$, and $B$ are subgroups of $G$ with $B$ normal in $G$.

Theorem 3.3 tells us that if $\mathbb{Z}_p[G/H]$ is isomorphic to $\mathbb{Z}_p[G/H']$ as $\mathbb{Z}_p[G]$-modules, then $\mathbb{Z}_p[G/(H \cap B)]$ is isomorphic to $\mathbb{Z}_p[G/(H' \cap B)]$ as $\mathbb{Z}_p[G]$-modules. This means, if there is a $\mathbb{Z}_p[G]$-isomorphism $M$ which takes $\mathbb{Z}_p[G/H]$ to $\mathbb{Z}_p[G/H']$, we know that there must be a $\mathbb{Z}_p[G]$-isomorphism $\tilde{M}$ which takes $\mathbb{Z}_p[G/(H \cap B)]$ to $\mathbb{Z}_p[G/(H' \cap B)]$. There is also a natural map $P$, from $\mathbb{Z}_p[G/(H \cap B)]$ to $\mathbb{Z}_p[G/H]$, which sends the element $gH \cap B$, in $\mathbb{Z}_p[G/(H \cap B)]$, to $gH$, in $\mathbb{Z}_p[G/H]$. The lifting problem is, given such an isomorphism $M$, can we come up with an isomorphism $\tilde{M}$ which makes the following diagram commute?

\[
\begin{array}{ccc}
\mathbb{Z}_p[G/H \cap B] & \xrightarrow{P} & \mathbb{Z}_p[G/H] \\
\tilde{M} & & \tilde{M}
\end{array}
\]

\[
\begin{array}{ccc}
\mathbb{Z}_p[G/H' \cap B] & \xrightarrow{P'} & \mathbb{Z}_p[G/H']
\end{array}
\]  

(1)

A natural choice would be $M \otimes I$ (where $I$ is the identity map), but this, in general, will not respect the actions of $G$. On the other hand, we could define the action of $\tilde{M}$ on the basis element $H \cap B$ to be the same as the action of $M \otimes I$, and simply define the action on the rest of $\mathbb{Z}_p[G/(H' \cap B)]$ in the only way possible to preserve the actions of $G$. But in this case, although $\tilde{M}$ must be a $\mathbb{Z}_p[G]$-homomorphism, it may not be an isomorphism. To see some examples, we first need to understand what is necessary for a map, given in terms of a matrix, to be a $\mathbb{Z}_p[G]$-homomorphism from $\mathbb{Z}_p[G/H]$ to $\mathbb{Z}_p[G/H']$. 

20
4.1 Notation and description of the matrices

Let $M$ be a $\mathbb{Q}[G]$-homomorphism between $\mathbb{Q}[G/H]$ and $\mathbb{Q}[G/H']$. If we pick bases for $\mathbb{Q}[G/H]$ and $\mathbb{Q}[G/H']$, $M$ is given by a matrix with rational coefficients. By multiplying by a common denominator, we can take $M$ to be an integral matrix. Such a matrix can be described more explicitly as follows.

Let $\{g_1, \ldots, g_m\}$ and $\{g'_1, \ldots, g'_m\}$ ($m = [G:H] = [G:H']$) be a complete set of coset representatives for $G/H$ and $G/H'$. The action of $G$ on the cosets of $H$ defines a homomorphism $\Pi : G \rightarrow S_m$ by sending the element $x$ of $G$ to the permutation $\Pi_x$, where $\Pi_x(i) = j$ when $xg_iH = g_jH$. Similarly we have $\Pi' : G \rightarrow S_m$ by $\Pi'_x(i) = k$ when $xg'_iH' = g'_kH'$. In order to have $xM(g_iH) = M(xg_iH)$, for $i = 1, \ldots, m$, and all $x$ in $G$, if $M = (m_{i,j})$ is the matrix of the map $M$ with respect to the bases $\{g_iH\}$ and $\{g'_jH'\}$, we must have:

$$m_{i,j} = m_{\Pi_x(i), \Pi'_x(j)}$$

(2)

for all $i$ and $j$, and all $x$ in $G$. If $M$ is to be an isomorphism, we must also have the determinant of $M$ not equal to zero. Furthermore, $M$ will also represent an isomorphism between $\mathbb{Z}_p[G/H]$ and $\mathbb{Z}_p[G/H']$ if and only if $p$ does not divide the determinant of $M$.

Now in order to better describe a matrix which will represent a $\mathbb{Q}[G]$-homomorphism between $\mathbb{Q}[G/(H \cap B)]$ and $\mathbb{Q}[G/(H' \cap B)]$, it will be useful to choose our coset representatives for $G/H$ and $G/H'$ in terms of representatives for $G/HB$ and $G/H'B$.

The following notation holds for the rest of this chapter.

Let $\{g_1, \ldots, g_d\}, \{g'_1, \ldots, g'_d\}, \{b_1, \ldots, b_n\}, \{b'_1, \ldots, b'_n\}; \{h_1, \ldots, h_r\}$, and $\{h'_1, \ldots, h'_r\}$, be a complete set of coset representatives for $G/HB$, $G/H'B$, $HB/H$, $H'B/H'$, $H/(H \cap B)$, and $H'/(H' \cap B)$ respectively. Here $d$ is the
index of $HB$ and also of $H'B$ in $G$; $n$ is the index of $H$ in $HB$ and of $H'$ in $H'B$; and $r$ is the index of $H \cap B$ in $H$ and of $H' \cap B$ in $H'$. Assume $g_1 = g'_1 = b_1 = b'_1 = h_1 = h'_1 = 1_G$, the identity element of $G$. Assume further that $b_i$ and $b'_i$ are in $B$ for all $i$.

A complete set of coset representatives for $G/H$ is $\{g_i b_j\}_{i,j=1}^{d n}$, and the action of $G$ described above can be thought of an action on the pair $(i,j)$. That is, $\Pi_x(i,j) = (k,l)$, where $x g_i b_j H = g_k b_l H$. $\Pi$ can then be described explicitly by $\Pi_x(i,j) = (\pi_x(i), \rho_{i,x}(j))$, where $\pi : G \rightarrow S_d$ is given by:

$$x g_i H B = g_{\pi_x(i)} H B, \quad x \in G$$

and $\rho_{i,x} = \rho(g_{\pi_x(i)}^{-1} x g_i)$, where $\rho : HB \rightarrow S_n$ is given by:

$$y b_j H = b_{\rho_x(j)} H, \quad y \in HB.$$ 

Define $\pi' : G \rightarrow S_d$ and $\rho' : H'B \rightarrow S_n$ analogously.

When the basis for $Q[G/H]$ is taken to be:

$$\{g_1 b_1 H, g_1 b_2 H, \ldots, g_1 b_n H, g_2 b_1 H, \ldots, g_2 b_n H, \ldots, g_d b_n H\},$$

and the basis for $Q[G/H']$ ordered similarly, the matrix $M$ may be thought of as a $d \times d$ matrix of $n \times n$ matrices. Let $m_{i,j}^{k,l}$ denote the coefficient in the $j^{th}$ row and $l^{th}$ column of the $n \times n$ matrix in the $i^{th}$ row and $k^{th}$ column of $M$. So now the equation (2) is the same as:

$$m_{i,j}^{k,l} = m_{\pi_x(i)}^{\pi_x(l)} \rho_{i,x}(j)$$

for all $i, j, k, l$ and all $x$ in $G$.

Now we want to describe all $dnr \times dnr$ matrices $\tilde{M}$ that can represent a $Q[G]$-homomorphism taking $Q[G/(H \cap B)]$ to $Q[G/(H' \cap B)]$. The set $\{g_i b_j h_k\}_{i,j,k=1}^{d n r}$ is a complete set of coset representatives for $G/(H \cap B)$. The action of $x$ in $G$
on a triple \((i, j, k)\) is given by \((i, j, k) \mapsto (\pi_x(i), \rho_{i,x}(j), \chi_{i,x}(k))\) where \(\pi_x\) and \(\rho_{i,x}\) are defined as above, and \(\chi_{i,x}\) is \(\chi(g_{\pi_x(i)}xg_i)\), where \(\chi : HB \rightarrow S_r\) is the map given by:

\[
yh_iB = h_{x(i)}B, \quad y \in HB.
\]

At first glance it may seem that \(\chi\) should depend on both \(i\) and \(j\). To see that it does not, first notice that \(H/(H \cap B) \cong HB/B\), so that the set \(\{h_1, \ldots, h_r\}\) is also a complete set of coset representatives for \(HB/B\). So \(\chi\) is a well-defined homomorphism into \(S_r\). Now let \(l\) be the index given by:

\[
xg_i b_j h_k H \cap B = g_{\pi_x(i)} b_{\rho_{i,x}(j)} h_l H \cap B.
\]

We need to see that \(l = \chi_{i,x}(k)\). Since \(h_l H \cap B = b_{\rho_{i,x}(j)} g_{\pi_x(i)} xg_i b_j h_k H \cap B\), this also means that \(h_l B = b_{\rho_{i,x}(j)} g_{\pi_x(i)} xg_i b_j h_k B\), and since \(B\) is normal in \(G\), \(b_{\rho_{i,x}(j)} g_{\pi_x(i)} xg_i b_j h_k B = g_{\pi_x(i)} xg_i h_k B\). So \(l = \chi_{i,x}(k)\) as claimed.

Again, define \(\chi' : H'B \rightarrow S_r\) analogously to describe the action of \(G\) on the cosets of \(H' \cap B\). With respect to the bases \(\{\{g_i b_j h_k H \cap B\}_{k=1}^r\}_{i=1}^d\) and \(\{\{g'_i b'_j h'_k H' \cap B\}_{k=1}^r\}_{i=1}^{d'}\), \(\widetilde{M}\) will be a "triple-indexed" matrix satisfying:

\[
\widetilde{m}_{i', j', k'}^{i, j, k} = \frac{\pi_{x(i')}(i') \rho_{i', x(j')}(j') \chi_{i', x(k')}(k')}{\pi_{x(i)}(i) \rho_{i, x(j)}(j) \chi_{i, x(k)}(k)}
\]

for all \(x\) in \(G\). Furthermore, in order for (1) to commute, we must also have:

\[
\sum_{k'=1}^r \widetilde{m}_{i, j, k'}^{i', j', k} = m_{i', j'}^{i, j}
\]

for all \(i, i', j, j', \) and \(k\).

### 4.2 The matrix \(M \otimes I\)

Let \(\mathcal{M}\) be the set of all integral \(nd \times nd\) matrices satisfying (3). Let \(\widetilde{\mathcal{M}}\) be the set of all integral \(ndr \times ndr\) matrices satisfying (4) and (5). Let \(\mathcal{M}_p = \{M \in \mathcal{M} : p \mid \det(M)\}\) and \(\widetilde{\mathcal{M}}_p = \{\widetilde{M} \in \widetilde{\mathcal{M}} : p \mid \det(\widetilde{M})\}\).
PROPOSITION 4.1. If $HB = G$, then $M \otimes I_{r \times r}$ is in $\tilde{\mathcal{M}}_p$ whenever $M$ is in $\mathcal{M}_p$.

PROOF. As $M \otimes I$ satisfies (5) and $\det(M \otimes I) = (\det M)^r$, we only need to verify that $M \otimes I$ is a $\mathbb{Q}[G]$-isomorphism whenever $M$ is. Now $G = HB$, then $G = H'B$ because $|HB| = |H'B|$. Then the proposition is immediate as $\mathbb{Q}[G/H \cap B] \cong \mathbb{Q}[G/H] \otimes \mathbb{Q}[G/B]$ and $\mathbb{Q}[G/H' \cap B] \cong \mathbb{Q}[G/H'] \otimes \mathbb{Q}[G/B]$ by Lemma 3.2. □

PROPOSITION 4.2. Let $M$ be in $\mathcal{M}$. If there exists any $r \times r$ invertible matrix $N$ such that $M \otimes N$ satisfies (4), then $M$ satisfies the condition:

$$m_i^{j'} j' \neq 0 \implies g_i^{-1} g_j^{-1} g_i \in B. \tag{6}$$

(Note, this is trivially satisfied when $G = HB$.)

PROOF. Suppose that (6) is not satisfied and there exists an invertible matrix $N$ such that $M \otimes N \in \tilde{\mathcal{M}}$. Since $M \otimes N$ satisfies (4), we must have:

$$m_i^{j'} j' \nu \kappa = m_{\pi_{x_x(i)} \rho_{\nu_x(j)}} n_{x_{x_x(k)}} \chi_{x_{x_x}(\kappa')}$$

for all $x$ in $G$. Since $M$ does not satisfy (6), there exist some indices $i$, $i'$, $j$ and $j'$ such that $g_i^{-1} g_j^{-1} g_i$ is not in $B$, and $m_i^{j'} j'$ is nonzero. Since $m_i^{j'} j'$ is the same as $m_{\pi_{x_x(i)} \rho_{\nu_x(j)}}$ already, we must have:

$$n_k \kappa' = n_{x_{x_x(k)}} \chi_{x_{x_x}(\kappa')} \tag{7}$$

for all $x$ in $G$. Taking $x = g_i^{-1}$, and noting that $\pi_{g_i^{-1}}(i') = 1$, we have $\chi_{g_i^{-1}g_i^{-1}} = \chi(g_i^{-1} g_j^{-1} g_i) = \chi(1)$, which is the identity. So $\chi_{g_i^{-1}g_i^{-1}}(k') = (k')$ for all $k' = 1, \ldots, r$. So from equation (7), $n_1 \kappa = n_{x_{x_x(1)}} \kappa'$ for all $k'$. But
\( \chi_{i,g_{i}^{-1}}(1) \neq 1 \) since \( g_{\pi_{i}^{-1}}^{-1}(i)g_{\pi_{i}^{-1}}^{-1}g_{i} \) is not in \( B \). This means the determinant of \( N \) is 0, contradicting the assumption that \( N \) is invertible. \( \square \)

In some circumstances, condition (6) is sufficient to show that \( M \otimes I \) is in \( \tilde{\mathcal{M}} \).

**Proposition 4.3.** Assume \( G/B \) is abelian, and \( HB = H'B \). If \( M \) is in \( \mathcal{M}_p \), and \( M \) satisfies (6), then \( M \otimes I_{r,r} \) is in \( \tilde{\mathcal{M}}_p \).

In the case \( G/B \) is cyclic, which is the case when \( G = \text{Gal}(N/F) \) and \( B = \text{Gal}(N/F_j) \), as in chapter 3, both assumptions, \( G/B \) abelian and \( HB = H'B \), are satisfied. We will examine this case further in the next section.

It is natural to ask if it is possible for any \( M \) in \( \mathcal{M} \) to satisfy condition (6). Under the hypothesis \( HB = H'B \), we may take \( g_{i}' = g_{i} \) for all \( i \), then \( g_{\pi_{i}^{-1}}^{-1}(i)g_{\pi_{i}^{-1}}^{-1}g_{i} = 1 \), so condition (6) is satisfied whenever \( M \) is block diagonal, that is, if \( m_{i,j}'' = 0 \) for all \( j \) and \( j' \) whenever \( i \neq i' \). Unfortunately, as we shall see from example 2, it may not be possible to have such a matrix in \( \mathcal{M} \). But condition (6) will be satisfied for all \( M \) if the coset representatives for \( G/HB \) form a group mod \( B \), in other words, if \( \{g_1B, \ldots, g_dB\} \) is a subgroup of \( G/B \).

In this case \( g_{\pi_{i}^{-1}}^{-1}(i)g_{\pi_{i}^{-1}}^{-1}g_{i} \) is in \( B \) for all \( i \) and \( i' \).

**Proof of Proposition 4.3.** Since \( HB = H'B \), we may take \( g_{i}' = g_{i} \) for all \( i \), and we may take \( h_k \equiv h_k' \) mod \( B \), for all \( k \), so that the permutations \( \pi \) and \( \pi' \) are the same, as well as the permutations \( \chi \) and \( \chi' \). (This is possible as \( H/H \cap B \cong HB/B = H'B/B \cong H'/H' \cap B \).) As noted in the proof of Proposition 4.1, we only need to establish that \( M \otimes I \) is a \( \mathbb{Q}[G] \)-isomorphism, in other words, satisfies equation (4). \( (M \otimes I)_{ij}^{ij'k'} = m_{ij}^{ij'k'} \delta_{k,k'} \), so we need to see that \( \delta_{k,k'} = \delta_{x_{i}(k),x_{i'}(k')} \) for all \( x \) in \( G \), whenever there is some \( j \) and \( j' \) such that \( m_{ij}^{ij'} \neq 0 \). This is satisfied if and only if \( \chi_{i,x}(k) = \chi_{i',x}(k) \). Under our
hypothesis, \( m_{ij}^{t'j'} \neq 0 \) implies that \( g_{\pi_{x}(i)}^{t'}g_{\pi_{x}(i)}^{-1}g_{t'j'}^{-1}g_{t'j'} \) is in \( B \). And since \( m_{\pi_{x}(i),\pi_{x}(j)}^{t'j'} = m_{ij}^{t'j'} \neq 0 \), we also have \( g_{\pi_{x}(i)}^{t'}g_{\pi_{x}(i)}^{-1}g_{\pi_{x}(i)}^{-1}g_{\pi_{x}(i)}^{-1} \) in \( B \). (That \( \pi_{\pi_{x}(t')}^{-1}(\pi_{x}(i)) \) is equal to \( \pi_{\pi_{x}(t')}^{-1}(\pi_{x}(i)) \) may be seen as follows: \( \pi_{\pi_{x}(t')}^{-1}(\pi_{x}(i)) = \pi_{\pi_{x}(t')}^{-1}(\pi_{x}(i)) \); and \( g_{\pi_{x}(t')}^{-1}xg_{t'H}B = (xg_{t'})^{-1}xg_{t'H}B = g_{t'}^{-1}g_{t'H}B. \)

So we have:

\[
g_{t'}^{-1}g_{t'H}B = g_{\pi_{x}(i)}^{-1}g_{t'}^{-1}g_{\pi_{x}(i)}B.
\]

Which, since \( G/B \) is abelian, can be rewritten as:

\[
g_{\pi_{x}(i)}^{-1}g_{t'H}B = g_{\pi_{x}(t')}^{-1}g_{t'H}B.
\]

Using the above, the definition of \( \chi_{x_{i,t}^{x_{i}}} \), and again the fact that \( G/B \) is abelian, we get:

\[
h_{x_{i,t}^{x_{i}}(k)}B = g_{\pi_{x}(i)}^{-1}xg_{t'h_{k}B} = g_{\pi_{x}(t')}^{-1}xg_{t'h_{k}B} = h_{x_{i,t}^{x_{i}}(k)}B.
\]

Which means precisely that \( \chi_{x_{i,t}^{x_{i}}}(k) = \chi_{x_{i,t}^{x_{i}}}(k) \).

4.3 Examples

**Example 1.** Suppose \( G/B \) is cyclic. In light of Propositions 4.2 and 4.3, we would like to see what is necessary for a matrix in \( M \) to satisfy condition (6).

Let \( gB \) be a generator for \( G/B \). This means \( g^{dr} \) is in \( B \) but \( g^{r} \) is not in \( B \) if \( k \) is less than \( dr \). As \( HB/B \) is a subgroup of \( G/B \) with order \( r \), \( g^{d}B \) is a generator for \( HB/B \). So \( g^{d} \) is in \( HB \) but \( g^{k} \) is not, if \( k \) is less than \( d \). Take \( g_{i} = g_{i}' = g^{i-1} \) for \( i = 1, \ldots, d \) as coset representatives for \( G/HB = G/H'B \).

We want to determine for which indices \( i \) and \( i' \) is \( g_{\pi_{x}(i)}^{-1}g_{t'}^{-1}g_{i} \) in \( B \). Since

\[
g_{t'}^{-1}g_{i}HB = g^{-i+1}g^{-i}HB = g^{-i'}HB = g^{d+i'\cdot HB},
\]

we get:

\[
g_{\pi_{x}(i)}^{-1}(t') = \begin{cases} g^{i'} & \text{if } i' \leq i \\ g^{d+i' - i} & \text{if } i' > i. \end{cases}
\]

This means:

\[
g_{\pi_{x}(i)}^{-1}(t')g_{t'}^{-1}g_{i} = \begin{cases} g^{i'-i}g^{-i'+1}g^{i-1} = 1 \in B & \text{if } i' \leq i \\ g^{-d+i'+i}g^{-i'+1}g^{i-1} = g^{d} \notin B & \text{if } i' > i. \end{cases}
\]
So to satisfy condition (6), we must have \( m_{ij}^{i'j'} = 0 \) whenever \( i' \) is greater than \( i \). But if \( i' \) is strictly less than \( i \), taking \( x = g^{d-i'} \), we have \( \pi_x(i') \) greater than \( \pi_x(i) \), so we must have \( m_{ij}^{i'j'} = 0 \) whenever \( i' \neq i \).

Proposition 4.2 tells us that \( M \otimes I \) will not be in \( \tilde{M} \) for many choices of \( M \) in \( \mathcal{M} \). Another natural choice for creating \( \tilde{M} \) from \( M \) is to define the first row of \( \tilde{M} \) to be the first row of \( M \otimes I \), and then define the other rows in the only way possible to ensure \( \tilde{M} \) satisfies equation (5). This will guarantee that \( \tilde{M} \) will be in \( \tilde{M} \), but it may not be in \( \tilde{M}_p \). Before turning to an example where this is the case, we need to see how to define \( \tilde{M} \) in this way.

Set \( (\tilde{M})_{1j}^{i'j'} = m_{1j}^{i'j'} \delta_{1,k} \). We must have:
\[
(\tilde{M})_{1j}^{i'j'} = (\tilde{M})_{11}^{i'j'} = (\tilde{M})_{11}^{i'j'} = m_{1j}^{i'j'} \delta_{1,k} \delta_{i',(g_{ki,h_{k}})}^{-1}((k')) \]

Set:
\[
(\tilde{M})_{1j}^{i'j'} = m_{1j}^{i'j'} \delta_{1,k} \delta_{i',(g_{ki,h_{k}})}^{-1}((k')) \tag{8}
\]

To check that this satisfies (5), we need:
\[
\chi_{i',(g_{ki,h_{k}})}^{-1}((k')) = \chi_{\pi_x(i'),G_{\pi_x(i)}h_{ki,x,(k)}}^{-1}((\chi^{-1}_{i',x}(k'))) \]

for all \( x \) in \( G \), and all \( k' \). From the definition of \( \chi' \), this means that we need to check that:
\[
g_{\pi_{x,-1}^{-1}(i')}^{-1}h_{ki}^{-1}g_{i}^{-1}g_{i'} \equiv (g_{\pi_{x,-1}^{-1}(i')}^{-1}h_{ki}^{-1}g_{\pi_x(i)}^{-1}(g_{\pi_x(i')}^{-1}xg_{i'}))g_{\pi_x(i')}^{-1}xg_{i'} \tag{9}
\]

mod \( B \), for all \( x \) in \( G \). Since \( g_{\pi_x(i')}^{-1}xH = (xg_{i})^{-1}xH = g_{i}^{-1}H \), the permutation \( \pi_{x,-1}^{-1} \) is equal to \( \pi_{i,-1}^{-1} \). Putting this into the right hand side of equation (9) we get:
\[
(g_{\pi_{x,-1}^{-1}(i')}^{-1}h_{ki}^{-1}g_{\pi_x(i)}^{-1}(g_{\pi_x(i')}^{-1}xg_{i'})) = g_{\pi_{x,-1}^{-1}(i')}^{-1}h_{ki}^{-1}g_{\pi_x(i)}^{-1}xg_{i'} \equiv
\]
mod \( B \), as desired.

To show that \( M \) being in \( \mathcal{M}_p \) does not guarantee \( \tilde{M} \) is in \( \mathcal{M}_p \), we take an example which comes from example 2 in [P2].

**Example 2.** Let \( c \) be a rational integer that is neither a square nor twice a square. Let \( \theta \) be a root of \( x^8 - c \) and \( \theta' \) a root of \( x^8 - 16c \). Let \( K = \mathbb{Q}(\theta) \) and \( K' = \mathbb{Q}(\theta') \). Then \( K \) and \( K' \) are arithmetically equivalent over \( \mathbb{Q} \) (see [P1], p. 351) The field \( \mathbb{Q}(\sqrt{c}) \) is contained in \( K \cap K' \). Choose any two rational numbers, \( b \) and \( d \) such that \( b^2 - 4cd^2 \) is in the same square class as \( c \), and let \( \beta = \sqrt{b + 2d\sqrt{c}} \). Let \( L = \mathbb{Q}(\beta) \). The field \( \mathbb{Q}(\sqrt{c}) \) is contained in \( L \). The conjugates of \( \beta \) are \( \beta' = \sqrt{b - 2d\sqrt{c}}, -\beta, \) and \( -\beta' \). Since \( \beta\beta' = \sqrt{b^2 - 4cd^2} \) is in \( \mathbb{Q}(\sqrt{c}) \), \( \beta' \) is in \( L \). So \( L \) is a normal extension of \( \mathbb{Q} \). The map which sends \( \beta \) to \( \beta' \) has order four, so \( L/\mathbb{Q} \) is cyclic of degree four.

Let \( N = \mathbb{Q}(\theta, \sqrt{2}, i, \beta) \). \( N \) is a normal extension of \( \mathbb{Q} \) which contains \( K, K' \), and \( L \). Let \( G \) be the Galois group of \( N/\mathbb{Q} \). \( G \) can be described as follows. Let \( \tau \) be the map which sends \( i \) to \( -i \) and fixes \( \theta, \sqrt{2}, \) and \( \beta \). Let \( \sigma \) be the map which sends \( \sqrt{2} \) to \( -\sqrt{2} \) and fixes \( \theta, i, \) and \( \beta \). Now if \( \gamma \) is any map which sends \( \theta \) to \( \zeta\theta \), where \( \zeta = \zeta_8 = \frac{1 + i}{\sqrt{2}} \) is a primitive eighth root of unity, we must have:

\[
\gamma(\beta^2) = \gamma(b + 2d\sqrt{c}) = \gamma(b + 2d\theta^4) = b + 2d(\zeta\theta)^4 = b - 2d\theta^4 = \beta'^2.
\]

So either \( \gamma(\beta) = \beta' \) or \( \gamma(\beta) = -\beta' \). Let \( \gamma \) be the map which sends \( \theta \) to \( \zeta\theta \) and \( \beta \) to \( \beta' \) and fixes \( \sqrt{2} \) and \( i \). Let \( \alpha \) be the map which sends \( \theta \) to \( \zeta\theta \) and \( \beta \) to \( -\beta' \) and fixes \( \sqrt{2} \) and \( i \). Then \( \alpha^2 = \gamma^2 \), but \( \alpha \neq \gamma \). \( G = \langle \alpha, \gamma, \sigma, \tau \rangle \), with the relations \( \gamma\sigma = \sigma\gamma^5, \gamma\tau = \tau\gamma^6\alpha, \alpha\sigma = \sigma\gamma^4\alpha, \alpha\tau = \tau\gamma^7, \) and \( \alpha^2 = \gamma^2 \). \( \sigma \) commutes with \( \tau \), and \( \gamma \) commutes with \( \alpha \). Also \( \alpha \) and \( \gamma \) have order 8; \( \sigma \) and \( \tau \) have order 2.
Let $H$ be the Galois group of $N/K$, $H'$ the Galois group of $N/K'$, and $B$ that of $N/L$. Then $H = \langle \sigma, \tau, \gamma^2 \alpha \rangle$; $H' = \langle \sigma \gamma^4, \tau, \gamma^7 \alpha \rangle$; and $B = \langle \sigma, \tau, \gamma \alpha \rangle$. Furthermore, $HB = H'B = \langle \sigma, \tau, \gamma^2, \gamma \alpha \rangle$; $H \cap B = \langle \sigma, \tau \rangle$; and $H' \cap B = \langle \sigma \gamma^4, \tau \rangle$. Coset representatives for $G/HB$ are $\{1, \gamma\}$; representatives for $HB/H$ and also for $HB/H'$ are $\{1, \gamma \alpha, \gamma^4 = (\gamma \alpha)^2, \gamma^5 \alpha = (\gamma \alpha)^3\}$; and representatives for $H/HB$, $H'/HB$ and $HB/B$ are $\{1, \gamma^7 \alpha\}$. We'd like to determine what a matrix $M$ in $M$ looks like. Let $M_{ii'}$ refer to the $4 \times 4$ matrix with coefficients $m_{ij}^{i'j}$. So that $M$ looks like:

$$
\begin{bmatrix}
M_{11} & M_{12} \\
M_{21} & M_{22}
\end{bmatrix}.
$$

Since $\pi_x(i) = \pi_x(i')$ if and only if $i = i'$, we can deal with the matrices $M_{ii}, i = 1, 2$, separately from $M_{ii'}, i \neq i'$.

We need to find $\pi_x, \rho_{i,x}$ and $\rho'_{i,x}$ for each $x$ in $G$ and $i = 1, 2$. There are 64 elements in $G$, but as $\gamma^7 \alpha$ is in $H \cap H'$ and $\gamma^7 \alpha$ commutes with everything in $G$, $\pi_x = \pi_{x\gamma^7 \alpha}$, $\rho_{i,x} = \rho_{i,x\gamma^7 \alpha}$, and $\rho'_{i,x} = \rho'_{i,x\gamma^7 \alpha}$, for each $x$ in $G$ and $i = 1, 2$.

For $x$ in $HB$:

$$
\pi_x(i) = i, \quad \rho_{1,x} = \rho(x), \quad \rho_{2,x} = \rho(\gamma^7 x \gamma).
$$

For $y$ in $\gamma HB$:

$$
\pi_y(i) = i + 1, \text{ mod } (2), \quad \rho_{1,y} = \rho(\gamma^7 y), \quad \rho_{2,y} = \rho(y \gamma).
$$

The relationships in (10) and (11) are equally valid for $\rho'$.

For $x$ in $HB$, $\rho(x)$ and $\rho'(x)$ are computed in the following table. All values are taken mod 4.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\rho_z(j)$</th>
<th>$\rho_z(j)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tau \gamma^{2t}, \tau \gamma^{2t-1} \alpha$</td>
<td>$2 - t - j$</td>
<td>$2 - t - j$</td>
</tr>
<tr>
<td>$\sigma \gamma^{2t}, \sigma \gamma^{2t-1} \alpha$</td>
<td>$t + j$</td>
<td>$2 + t + j$</td>
</tr>
<tr>
<td>$\gamma^{2t}, \gamma^{2t-1} \alpha$</td>
<td>$t + j$</td>
<td>$t + j$</td>
</tr>
<tr>
<td>$\sigma \tau \gamma^{2t}, \sigma \tau \gamma^{2t-1} \alpha$</td>
<td>$2 - t - j$</td>
<td>$- t - j$</td>
</tr>
</tbody>
</table>
From (10) we get \( m^i_1 j' = m^i_1 \rho(x)(j') \) for all \( x \) in \( HB \) and \( i = 1, 2 \). By taking \( x = \gamma \), and using (11), we get \( m^1_1 j' = m^2_1 \rho_1, \gamma(j') = m^2_2 j' \). So \( M_{11} = M_{22} \).

Taking \( x = \gamma^2 \), we see that \( m^1_1 j' = m^1_1 j'+1 \), and from \( x = \sigma \) we have \( m^1_1 j' = m^1_1 j'+2 \). These are the only relations we have for \( M_{11} \) and \( M_{22} \). So \( M_{11} = M_{22} \) looks like:

\[
\begin{bmatrix}
A & B & A & B \\
B & A & B & A \\
A & B & A & B \\
B & A & B & A \\
\end{bmatrix}
\]

Also from \( x = \gamma \), we get the relationship between \( M_{12} \) and \( M_{21} \) as \( m^1_1 j' = m^2_2 \rho_2, \gamma(j') = m^2_2 j'+1 \). Taking \( x = \gamma^2 \), we get \( m^2_1 j' = m^2_1 j'+1 \). And from \( x = \tau \) we have \( m^2_1 j = m^2_1 j^2 \) and \( m^2_2 j = m^2_2 j^2 \). So \( M_{12} \) looks like:

\[
\begin{bmatrix}
C & D & D & C \\
C & C & D & D \\
D & C & C & D \\
D & D & C & C \\
\end{bmatrix}
\]

and \( M_{21} \) is:

\[
\begin{bmatrix}
C & C & D & D \\
D & C & C & D \\
D & D & C & C \\
C & D & C & C \\
\end{bmatrix}
\]

The determinant of \( M \) is given by \( 64(A - B)^2(C - D)^4((A + B)^2 - (C + D)^2) \).

Notice that in this example, if we had \( m_{1_1 j'} = 0 \) whenever \( i \neq i' \), \( M \) would not be invertible.

Now we want to compute \( \widetilde{M} \) using equation (8). Notice that \( \delta_{1, x', (a_{k_1} a_{k_2})^{-1}(k')} \) is always independent of \( j \) and \( j' \). Furthermore, in this case we have \( h_k = h'_k \) for \( k = 1, 2 \), so \( \chi = \chi' \). This, plus the fact that \( G/B \) is abelian, gives us that \( \delta_{1, x', (a_{k_1} a_{k_2})^{-1}(k')} = \delta_{k, x', (a_{k_1} a_{k_2})^{-1}(k')} \). Let \( P_{i, j'} \) be the permutation matrix associated to \( x', \delta_{k_1}^{-1}; \) that is, \( P_{i, j'} = (\delta_{k, x', \delta_{k_1}^{-1}(k')}) \). From equation (8), \( \widetilde{M} \) looks like:

\[
\begin{bmatrix}
M_{11} \otimes P_{11} & M_{12} \otimes P_{12} \\
M_{21} \otimes P_{21} & M_{22} \otimes P_{22} \\
\end{bmatrix}
\]

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
In our case we have $g_1^{-1} = 1$ and $g_2^{-1} = \gamma^{-1}$. So $\chi_{1,1} = \chi(1)$, $\chi_{2,1} = \chi(\gamma^{-1}1\gamma)$, and $\chi_{2,7^{-1}} = \chi(1\gamma^{-1}1\gamma)$, making each of these the identity. While $\chi_{1,7^{-1}} = \chi(\gamma^{-1}1\gamma^{-1}1) = \chi(\gamma^{-2})$ is the transposition, as $\gamma^{-2} = \gamma^6$, which is not in $B$. So $P_{11} = P_{12} = P_{22} = I_{2 \times 2}$, and $P_{21}$ is the matrix:

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

The determinant of $\tilde{M}$ is $(\det M)64(A-B)^2(C-D)^2((A+B)^2 + (C+D)^2)$. For example, we can take $A = D = 1$, $B = 2$, $C = 3$, and $p = 5$. Then the determinant of $M$ is $2^{10}(-7)$, so $M$ is in $\mathcal{M}_5$, but the determinant of $\tilde{M}$ is $2^{14}(-7)^2$.

It is interesting to note that in this example the determinant of $\tilde{M}$ is nonzero whenever the determinant of $M$ is. So it is still an open question whether or not $M$ invertible as a $\mathbb{Q}$-isomorphism always implies $\tilde{M}$ is also invertible.
Bibliography


[P1] Perlis, R. : On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory 9, 342-360 (1977).


32


Vita

Nancy Colwell was born in Ithica, New York, on August 26, 1959. She graduated from high school in June 1977. She attended Reed College and the University of California at San Diego, where she received a bachelor of arts in communications and visual arts in December 1982. In August 1990, she began her graduate study at Louisiana State University, and is presently a candidate for the doctoral degree in mathematics at LSU, which she will receive on August 1, 1996.
DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Nancy C. Colwell

Major Field: Mathematics

Title of Dissertation: Some Lifting Problems in Arithmetic Equivalence

Approved:

Robert Perlis
Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

J. Hurelbrink
William C. Athearn
Peter Wolenski

Date of Examination:

April 30, 1996