2014

Local Conjugations of Groups and Applications to Number Fields

Bir B. Kafle
Louisiana State University and Agricultural and Mechanical College, kaflebb@gmail.com

LOCAL CONJUGATION OF GROUPS AND APPLICATIONS TO NUMBER FIELDS

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
Bir B. Kafle
M.S., Western Illinois University, 2009
August 2014

Acknowledgments

First and foremost, I would like to thank my advisor Professor Robert Perlis for all of his support, guidance and for everything he has taught me over these past five years, from mathematics, grammar and punctuation to life events. Without his endless patience, this work would not have been possible.

Many thanks to my committee members Professors William Adkins, Charles Delzell, Mark Davidson, Richard Litherland, Jorge Morales and Thomas Ricks. I can not thank Professor James Oxley enough for providing continuous feedback which helped me to grow as a teacher.

Many thanks to Alex and Nik in the Mathematics Department, LSU for helping me out in hardwares and softwares. I would also like to thank my wonderful friends that I have made here at LSU.

Finally and most importantly, I would like to thank my wife Dibya for her love, support and understanding, and my children Diya and Aaron, the loves of my life. They are my source of inspiration every day.

Table of Contents

Abstract

This dissertation studies pairs of subgroups H, H' of a finite group G together with a bijective map $\varphi : H \longrightarrow H'$ that is a *local conjugation*, meaning that each element h in H is conjugate in G to its image $\varphi(h)$. The map φ is *not* required to take products to products.

The motivation for studying such pairs comes from a paper of F. Gassmann in 1926, in which he formulated an equivalent but different-sounding condition now known as *Gassmann's condition*. There are now at least ten equivalent reformulations of Gassmann's condition, of which local conjugation is perhaps the most elementary; see Lemma (4.2.1).

The utility of studying local conjugation is that it raises natural questions. For example, if we do *additionally require* that the map φ preserve products (that is, if it is required that φ be an isomorphism as well as a local conjugation), does it follow that φ is a global conjugation? An example showing the answer is *no* is given in this dissertation.

Many applications of local conjugacy have been discovered. In number theory, the groups H, H', G appear as Galois groups of field extensions of the field of algebraic number field k, and H, H' are locally conjugate in G if and only if the fixed fields K, K' of H, H' have identical Dedekind zeta functions. In 1985, Sunada looked at H, H', G as groups of deck isometrices of coverings of Riemann surfaces and showed that when H, H' are locally conjugate but not conjugate in G then the corresponding Riemann surfaces are isospectral but non-isometric [25]. And more recently, locally conjugate subgroups of a finite group G have been used to produce pairs of nonisomorphic graphs with identical Ihara zeta functions.

All of this motivated the study of local conjugacy in this dissertation. Among other things, yet another reformulation, called *cycle number equivalence*, was discovered, which gives as a corollary a new proof of a theorem of Stuart and Perlis [24].

Chapter 1
Introduction

After the German mathematician and ETH Zürich chair Adolf Hurwitz died in 1919, several notebooks of his unpublished work were found. One notebook concerned Kronecker's suggestion to try to characterize an arbitrary algebraic number field K by the manner in which prime numbers split when lifted to the ring of algebraic integers in K. In an article [8] published in 1926, the ETH Zürich student Fritz Gassmann reformulated Hurwitz's initial attempts to the following condition. Let G be a group and let H, H' be subgroups of G such that each conjugacy class c of G intersects H and H' in the same number of elements, that is,

$$|c \cap H| = |c \cap H'| \tag{1.0.1}$$

for any conjugacy class c in G. Today condition (1.0.1) is called *Gassmann's condition,* and we say subgroups $H, H' \leq G$ satisfying it are *Gassmann equivalent* in G. Gassmann's condition can be reformulated in many ways. Perhaps the simplest is the following, due to Sheng Chen [5] in 1992:

$$\text{There is a set bijection } \varphi : H \longrightarrow H' \text{ with } \varphi(h) \text{ conjugate in } G \text{ to } h \tag{1.0.2}$$

for every $h \in H$. When H and H' satisfy (1.0.2), we say that H and H' are *bijectively locally conjugate* (bloc for short) in G and the map φ is called a *bijective local conjugation* (which we also shorten to "φ is bloc" when the context is clear). We use the notation $H \sim_G H$ to indicate H and H' are bloc in G.

We start by proving the equivalence of (1.0.1) and (1.0.2) and proving that if φ exists then φ extends to a bloc on the parent group G. We also draw some elementary conclusions.

Lemma 1.0.1. *Let H and H' be two subgroups of a finite group G. Then the following statements are equivalent.*

1. *H and H' are Gassmann equivalent in G.*

2. *H and H' are bloc in G.*

3. *There exists a bloc $\bar{\varphi} : G \longrightarrow G$ such that $\bar{\varphi}(H) = H'$.*

Proof. Let $c_1, c_2, \ldots, c_t$ denote the conjugacy classes in G. Then c_i is disjoint from c_j when $i \neq j$ $(i, j = 1, 2, \cdots, t)$ and $G = \bigcup_{i=1}^{t} c_i$.

(1) $\Rightarrow$ (2) The set of intersections $\{c_i \cap H\}$ partitions H and the set $\{c_i \cap H'\}$ partitions H', $i = 1, 2, \ldots, t$. But $|c_i \cap H| = |c_i \cap H'|$ by Gassmann equivalence. For $i = 1, 2, \cdots, t$, choose any bijection from $c_i \cap H$ to $c_i \cap H'$. These then assemble into a bijection $\varphi : H \longrightarrow H'$. For any $h \in H$, h^G is one of the conjugacy class in G, say $h^G = c_i$ for some i. So, $\varphi(h)$ is in $c_i \cap H' \subset c_i = h^G$. Hence $\varphi(h)$ is conjugate in G to h. Therefore φ is a bloc in G from H to H'.

(2) $\Rightarrow$ (3) Fix a bijective local conjugationφ from H to H'. Let i be an index with $c_i \cap H \neq \phi$. Take any $h \in c_i \cap H$. Then $\varphi(h) \in H'$ and $\varphi(h)$, being G-conjugate to h, also lies in $h^G = c_i$. So, $\varphi(h) \in c_i \cap H'$. This holds for all $h \in c_i \cap H$. Hence $\varphi(c_i \cap H) \subseteq c_i \cap H'$. This holds for any $i = 1, 2, \cdots, t$. Thus $|H| = \sum_{i=1}^{t} |c_i \cap H| = \sum_{i=1}^{t} |\varphi(c_i \cap H)| \leq \sum_{i=1}^{t} |c_i \cap H'| = |H'|$. But $|H| = |H'|$ since φ is a bijection, hence $\varphi(c_i \cap H) = c_i \cap H'$, $(i = 1, 2, \cdots, t)$.

For any conjugacy class c_i in G and put $\varphi_i = \varphi|_{c_i \cap H}$. Write $c_i = (c_i \setminus H) \cup (c_i \cap H)$ and also $c_i = (c_i \setminus H') \cup (c_i \cap H')$. We have $|c_i \setminus H| = |c_i \setminus H'|$. Choose any bijection $\psi_i : c_i \setminus H \longrightarrow c_i \setminus H'$. For $g \in G$, then $g \in c_i$ for some unique i. Now define a map

$$\bar{\varphi}(g) = \begin{cases} \varphi_i(g) \text{ if } g \in c_i \cap H, \\ \psi_i(g) \text{ if } g \in c_i \setminus H. \end{cases}$$

Then $\bar{\varphi}$ is a bloc in G taking H to H'.

(3) $\Rightarrow$ (1) Fix a conjugacy class c_i in G. We have $c_i \cap H \subseteq H$, which implies that $\bar{\varphi}(c_i \cap H) \subseteq \bar{\varphi}(H) = H'$. Also $c_i \cap H \subseteq c_i$, so $\bar{\varphi}(c_i \cap H) \subseteq \bar{\varphi}(c_i) \subseteq c_i$, since for all x in c_i, we have $\bar{\varphi}(x) \in x^G = c_i$. Therefore, $\bar{\varphi}(c_i \cap H) \subseteq c_i \cap H'$ and then $|c_i \cap H| \leq |c_i \cap H'|$. So $|H| = \sum_i |c_i \cap H| \leq \sum_i |c_i \cap H'| = |H'|$. But the bloc $\bar{\varphi}$ maps from H to H', so $|H| = |H'|$. Thus $|c_i \cap H| = |c_i \cap H'|$ showing that H and H' are Gassmann equivalent in G. □

Following two corollaries are the immediate consequences of Lemma (1.0.1).

Corollary 1.0.2. *If H and H' are Gassmann equivalent in G, then $|H| = |H'|$ and hence $[G : H] = [G : H']$.*

Corollary 1.0.3. *1. If $\varphi : H \longrightarrow H'$ is a bloc in G, then $h^G = \varphi(h)^G$ for all $h \in H$.*

2. If $\bar{\varphi} : G \longrightarrow G$ is a bloc, then

(a) $\bar{\varphi}(N) = N$ for all $N \trianglelefteq G$,

(b) $\bar{\varphi}(c^G) = \bar{\varphi}(c)^G$ for all $c \in G$.

Another consequence of H, H' being bloc in G is the following lemma.

Lemma 1.0.4. *Let H, H' be bloc in G, and let M any normal subgroup of G. Then $H \cap M$ and $H' \cap M$ are bloc in G.*

Proof. Let $\varphi : H \longrightarrow H'$ be a bloc in G. The restriction of φ to $H \cap M$ is a bloc in G from $H \cap M$ to $H' \cap M$. □

Lemma (1.0.4) leads us to the following open problem.

Open Problem. Let H, H' be bloc in G, and M be any normal subgroup in G. Are the subgroups HM and $H'M$ bloc in G?

Theorem 1.6(a), Chapter 3 in [10] purports to answer this question in the affirmative, but there is a mistake in the proof. In Chapter 2, several different additional assumptions are given and it is shown that any of these additional assumptions give an affirmative answer to the open problem.

Chapter 3 relates bijective local conjugacy to a concept called *same order type*. The relevant definitions can be found the chapter.

In Chapter 4, a new concept called *same cycle number* is introduced and used it to give a new characterization of H, H' being bloc in G.

Chapter 5 relates bloc equivalence to number theory. Let K and K' be algebraic number fields and let N be a normal extension of $\mathbb{Q}$ containing K, K'. Set $G = Gal(N/\mathbb{Q})$, $H = Gal(N/K)$ and $H' = Gal(N/K')$. In 1977, Perlis proved that H, H' are bloc in G if and only if K and K' have identical Dedekind zeta functions. This allows us to translate some results about pairs of bloc subgroups of a finite group to number fields. In particular, the results on same cycle length sequence in Chapter 4 give a new proof of a theorem of Stuart and Perlis (see [24]).

There are other applications of bloc equivalent pairs of subgroups, which we do not discuss in this dissertation other than to point to some of the literature. In differential geometry, bloc equivalence can be used to construct isospectral but non-isomorphic Riemannian manifolds (see [3], [5], [25]). In graph theory, bloc equivalence can be used to construct non-isomorphic graphs with identical Ihara zeta functions (see [23]).

Chapter 2
Local Conjugation in Groups

In this chapter, we discuss various properties of locally conjugate subgroups of a group. Throughout, H and H' will denote subgroups of a finite group G.

2.1 Locally Conjugate Subgroups

Recall that

1. H and H' are said to be *Gassmann equivalent* in G if

$$|c \cap H| = |c \cap H'|$$

for any conjugacy class c in G. It is clear from the definition that if H and H' are conjugate in G, then they are Gassmann equivalent in G.

2. H and H' are said to be *locally conjugate* in G if there exists a map $\varphi\colon H \to H'$ such that for any $h \in H$, then h and $\varphi(h)$ are conjugate in G. If such a map φ is bijective, we say H and H' are bijectively locally conjugate (bloc for short) in G. We use the notation $H \sim_G H$ to indicate that H and H' are bloc in G

If $H \sim_G H'$, then H and H' are not necessarily conjugate in G, see Example (2.3.1). Following two lemmas show that under some additional conditions, bloc subgroups are conjugate in the parent group G.

Lemma 2.1.1. *If $H \sim_G H'$ and H is cyclic, then H and H' are conjugate.*

Proof. Assume $H = \langle h \rangle \sim_G H'$. There is a bloc $\varphi : H \longrightarrow H'$ in G such that $\varphi(h) = ghg^{-1}$ for some $g \in G$. Let $ghg^{-1} = h'$ for some $h' \in H'$. So $\langle h' \rangle \subseteq H'$. Further $(h')^i = (ghg^{-1})^i = gh^ig^{-1}$ for all $i = 1, 2, \cdots, |H|$. But also $|H'| = |\langle h \rangle| = |\langle ghg^{-1} \rangle| = |\langle h' \rangle|$. Therefore $H' = \langle h' \rangle$. Because H and H' have conjugate generators, the groups themselves are conjugate. This proves the lemma. □

Lemma 2.1.2. *If $H \sim_G H'$ and $H \trianglelefteq G$, then $H = H'$.*

Proof. By definition, there is a bloc $\nu : H' \longrightarrow H$ in G such that for any $h' \in H'$, $\nu(h') = g^{-1}h'g \in H$ for some $g \in G$, so $h' \in gHg^{-1} = H$, since H is normal in G. Hence, $H' \subseteq H$. Also by Corollary (1.0.2), $|H| = |H'|$. Hence $H = H'$. □

Proposition 2.1.3. *Let H and H' be bloc subgroups in G. Then*

1. $\cap_{g \in G} H^g = \cap_{g \in G} H'^g$.

2. $\cup_{g \in G} H^g = \cup_{g \in G} H'^g$.

Proof. Fix a bloc $\varphi : H \longrightarrow H'$ in G.

1. Set $N = \cap_{g \in G} H^g$ and $N' = \cap_{g \in G} H'^g$. Since N is the largest normal subgroup of G contained in H, it follows that $\varphi(N) \subseteq \varphi(H) = H'$. For $x \in N$, $\varphi(x) = \gamma x \gamma^{-1} \in N$ for some $\gamma \in G$. This shows that $\varphi(N) \subseteq N$ and so $\varphi(N) = N$, since φ is bijective. Thus $N = \varphi(N) \subseteq \varphi(H) = H'$ which implies that $N \subseteq N'$, since N' is the largest normal subgroup of G contained in H'. By symmetry, it follows that $N = N'$.

2. Let $x \in \cup_{g \in G} H^g$. So $x \in H^g$ for some $g \in G$ and therefore $x^g \in H$ for some $g \in G$. Also $\varphi(x^g) = \gamma x^g \gamma^{-1} = x^{g\gamma}$ in H'. Hence $x \in H'^{\delta}$ for $\delta = (g\gamma)^{-1} \in G$ and $x \in \cup_{\delta \in G} H'^{\delta}$. The result follows by symmetry.

□

For bloc subgroups H, H' of G and $M \trianglelefteq G$ we do not know whether HM and $H'M$ are bloc in G. Propositions [(2.1.4), (2.1.5)] and Corollaries [(2.1.6), (2.1.12)] give partial results giving an affirmative answer.

Proposition 2.1.4. *Let $H \sim_G H'$ and $M \trianglelefteq G$. Then each of the following holds.*

1. *If G/M is abelian, then $HM = H'M$.*

2. *$\cup_{g\in G}(HM)^g = \cup_{g\in G}(H'M)^g$. (These are subsets of G.)*

Proof. By definition, there is a bloc $\varphi : H \longrightarrow H'$ in G, so for any h in H, $\varphi(h) = ghg^{-1}$ in H' for some g in G.

1. Fix $h' \in H'$ and write $h' = \varphi(h)$ for some $h \in H$. Then

$$\begin{aligned} h'M &= \varphi(h)M \\ &= ghg^{-1}M \\ &= hM, \text{ since } G/M \text{ is abelian.} \end{aligned}$$

   So for all $h' \in H'$, there exists $h \in H$ such that $h'M = hM \subseteq HM$. This holds for all $h' \in H'$. So $H'M \subseteq HM$. But

$$|H'M| = \frac{|H'| \cdot |M|}{|H' \cap M|} = \frac{|H| \cdot |M|}{|H \cap M|} = |HM|,$$

   since $H \cap M \sim_G H' \cap M$ by Lemma (1.0.4). Therefore $HM = H'M$.

2. Fix $h' \in H'$ and write $h' = \varphi(h)$ for some $h \in H$. Then

$$\begin{aligned} h'M = \varphi(h)M = \gamma h\gamma^{-1}M \text{ for some } \gamma \in G \\ = \gamma h\gamma^{-1}M\gamma\gamma^{-1} \\ = \gamma hM\gamma^{-1} \subseteq \gamma HM\gamma^{-1} \subseteq (HM)^\gamma \subseteq \cup_{g\in G}(HM)^g. \end{aligned}$$

This holds for any $h' \in H'$, so $H'M \subseteq \cup_{g\in G}(HM)^g$. For any $t \in G$,

$$(H'M)^t \subseteq \cup_{g\in G}(HM)^g$$

which implies that $\cup_{t\in G}(H'M)^t \subseteq \cup_{g\in G}(HM)^g$. Equality follows by symmetry.

This proves the proposition. □

Proposition 2.1.5. *Let $\varphi : H \longrightarrow H'$ be a bloc in G and $M \trianglelefteq G$. Suppose $h_1, h_2, \cdots, h_t$ in H represent HM/M and $\varphi(h_1), \varphi(h_2), \cdots, \varphi(h_t)$ in H' represent $H'M/M$. Then each of the following holds.*

1. *HM/M and $H'M/M$ are bloc subgroups in G/M.*
2. *HM and $H'M$ are bloc subgroups in G.*

Proof. 1. Every element in HM/M can be written uniquely as the form $h_i m$, for some $i \in \{1, 2, \cdots, t\}$. Therefore

$$HM/M = \{h_i M, i = 1, 2, \cdots, t\}, \text{ and}$$
$$H'M/M = \{\varphi(h_i)M, i = 1, 2, \cdots, t\}.$$

Define a map $\tilde{\varphi} : HM/M \longrightarrow H'M/M$ by

$$\begin{aligned}\tilde{\varphi}(h_i M) &= \varphi(h_i)M, \text{ for all } i = 1, 2, \cdots, t \\ &= g_i h_i g_i^{-1} M \text{ for some } g_i \in G \\ &= g_i h_i M g_i^{-1} \text{ [because we can write } M = g_i M g_i^{-1}]\end{aligned}$$

This shows that the element h_iM in HM/M and the element $\tilde{\varphi}(h_iM)$ in $H'M/M$ are conjugate in G/M. The map $\tilde{\varphi}$ is clearly an injective. By proposition (2.1.4), we have $|H \cap M| = |H' \cap M|$. Thus $|HM/M| = |H'M/M|$, which implies that $\tilde{\varphi}$ is bijective and is a bloc in G/M.

2. For each i, write $\varphi(h_i) = \gamma_i h_i \gamma_i^{-1}$ for some choice of $\gamma_i \in G$. We write

$$\begin{aligned} HM &= \cup_{i=1}^{t} h_i M, \text{ and} \\ H'M &= \cup_{i=1}^{t} \varphi(h_i) M \\ &= \cup_{i=1}^{t} \gamma_i h_i \gamma_i^{-1} M \end{aligned}$$

Define a map $\bar{\varphi} : HM \longrightarrow H'M$ as follows.

For $hm_0 \in HM (h \in H, m_0 \in M)$ and $h_i m_1 \in M (h_i \in H, m_1 \in M)$ with $hm_0 = h_i m_1$, define

$$\begin{aligned} \bar{\varphi}(hm_0) = \bar{\varphi}(h_i m_1) &= \gamma_i h_i m_1 \gamma_i^{-1} \\ &= \gamma_i h_i \gamma_i^{-1} \gamma_i m_1 \gamma_i^{-1} \\ &= \varphi(h_i) m \in H'M. \end{aligned}$$

So $\bar{\varphi}$ is a local conjugation. But $\bar{\varphi}$ is also a bijection. Hence $\bar{\varphi} : HM \longrightarrow H'M$ is a bloc in G.

This proves the proposition. □

Corollary 2.1.6. *Let $H \sim_G H'$ and $M \trianglelefteq G$. If $H \cap M = H' \cap M = \{e\}$, then $HM \sim_G H'M$.*

Proof. Let $\varphi : H \longrightarrow H'$ be a bloc in G. Let $H = \{h_1, h_2, \cdots, h_t\}$. These elements represent $H = H/(H \cap M) = HM/M$. And $H' = \{\varphi(h_1), \varphi(h_2), \cdots, \varphi(h_t)\}$ represents $H'M/M$. Therefore $HM \sim_G H'M$, by Proposition (2.1.5). □

In Lemma (1.0.4), we showed that $H \sim_G H'$ and $M \trianglelefteq G$ imply $H \cap M \sim_G H' \cap M$. By assuming that M is in the center of G, we obtain a stronger conclusion.

Corollary 2.1.7. *Let $H \sim_G H'$ and $M \leq Z(G)$, where $Z(G)$ is the center of G. Then $H \cap M = H' \cap M$.*

Proof. Let $\varphi : H \longrightarrow H'$ be a bloc in G.

Let $a \in H \cap M$, so $\varphi(a) \in H'$. Also for some $\gamma \in G$, $\varphi(a) = \gamma a \gamma^{-1} = \gamma\gamma^{-1}a = a \in M$. So $\varphi(a) = a \in H \cap M$. Thus $H \cap M \subseteq H' \cap M$ and also $|H \cap M| = |H' \cap M|$. So $H \cap M = H' \cap M$. □

Definition 2.1.8. The fixed point character of G on G/H is the function

$$\chi_{G/H}(g) = |\{\gamma H \mid g\gamma H = \gamma H\}|,$$

giving the number of cosets in G/H fixed by elements $g \in G$.

Lemma 2.1.9. *For any $g \in G$*

$$\chi_{G/H}(g) = \frac{|C_G(g)|}{|H|} \, |g^G \cap H|,$$

where $C_G(g)$ is the centralizer of g in G.

Proof. By definition

$$\begin{aligned} \chi_{G/H}(g) &= |\{\gamma H \,|\, g\gamma H = \gamma H\}| \\ &= |\{\gamma H \,|\, \gamma^{-1} g \gamma H = H\}| \\ &= |\{\gamma H \,|\, \gamma^{-1} g \gamma \in H\}| \\ &= \frac{1}{|H|} \, |\{\gamma \in G \,|\, \gamma^{-1} g \gamma \in H\}|. \end{aligned}$$

But $|\{\gamma \in G \,|\, \gamma^{-1} g \gamma \in H\}| = |C_G(g)| \cdot |g^G \cap H|$. □

Let $g_1, g_2, \cdots, g_n$ represent G/H. Then $\mathbb{Q}[G/H]$ is an n-dimensional $\mathbb{Q}$-vector space with basis $g_1H, g_2H, \cdots, g_nH$. The representation ρ of G on $\mathbb{Q}[G/H]$ defined by $\rho(g)(g_iH) = g_jH$ where $gg_iH = g_jH$ is called the "representation of G induced by the trivial representation of H". The character of ρ is trace(ρ), that is, for all $g \in G$:

$$\begin{aligned} \text{trace } (\rho(g)) &= \text{number of cosets } g_iH \text{ with } gg_iH = g_iH \\ &= \chi_{G/H}(g). \end{aligned}$$

Proposition 2.1.10. *The following statements are equivalent.*

1. *H, H' are Gassmann equivalent in G.*
2. *$\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules.*
3. *$\chi_{G/H} = \chi_{G/H'}$.*

Proof. (1) $\Rightarrow$ (3) Suppose $|g^G \cap H| = |g^G \cap H'|$ for all $g \in G$. By Corollary (1.0.2), we have $|H| = |H'|$. Then the equality of $\chi_{G/H}$ and $\chi_{G/H'}$ follows by Lemma (2.1.9).

(3) $\Rightarrow$ (1) Suppose $\chi_{G/H} = \chi_{G/H'}$. By taking $g = id$ in Lemma (2.1.9), $\chi_{G/H}(id)$ $= |G|/|H|$ and $\chi_{G/H'}(id) = |G|/|H'|$, so $|H| = |H'|$. Then $|g^G \cap H| = |g^G \cap H'|$ follows from Lemma (2.1.9).

(2) $\Rightarrow$ (3) Let ρ and ρ' be the representations of G corresponding to the $\mathbb{Q}[G]$-modules $\mathbb{Q}[G/H]$ and $\mathbb{Q}[G/H']$ respectively. But $\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules, by definition, there exists a rational $n \times n$ matrix $M \in GL_n(\mathbb{Q})$ satisfying

$$\rho'(g) = M\rho(g)M^{-1}$$

for every $g \in G$. Taking the traces to both sides, gives

$$\text{trace}(\rho'(g)) = \text{trace}(M\rho(g)M^{-1}) \tag{2.1.1}$$

for all $g \in G$. But trace$(M\rho(g)M^{-1})$ = trace $\rho(g)$. Therefore, (2.1.1) gives us

$$\chi_{G/H}(g) = \chi_{G/H'}(g)$$

for all $g \in G$.

(3) $\Rightarrow$ (2) This is standard result in representation theory. Over a field of characteristic 0, any representation of a finite group is determined up to isomorphism by its character.

This proves the proposition. $\square$

Proposition 2.1.11. *Let $M \trianglelefteq G$ and $M \subseteq H \cap H'$. The following statements are equivalent.*

1. *H and H' are Gassmann equivalent in G.*

2. *H/M and H'/M are Gassmann equivalent in G/M.*

Proof. The group G acts on G/H with fixed point character $\chi_{G/H}$ given by

$$\chi_{G/H}(g) = |\{\gamma H | g\gamma H = \gamma H\}|.$$

We have $H/M \leq G/M$. Denote $\mathcal{G} = G/M$ and $\mathcal{H} = H/M$. Now $\mathcal{G}$ acts on $\mathcal{G}/\mathcal{H}$ with fixed point character $\chi_{\mathcal{G}/\mathcal{H}}$: for any

$$\begin{aligned}
\chi_{\mathcal{G}/\mathcal{H}}(gM) &= |\{\gamma M\mathcal{H} \,|\, gM(\gamma M\mathcal{H}) = \gamma M\mathcal{H}\}| \\
&= |\{\gamma M\{hM\}_{h\in H} \,|\, gM\gamma M\{hM\}_{h\in H} = \gamma M\{hM\}_{h\in H}\}| \\
&= |\{\gamma MHM \,|\, g\gamma HM = \gamma HM|\} \\
&= \{\gamma H \,|\, g\gamma H = \gamma H\} = \chi_{G/H}(g).
\end{aligned}$$

Similarly, $\chi_{\mathcal{G}/\mathcal{H}'}(g) = \chi_{G/H'}(g)$. Hence $\chi_{G/H} = \chi_{G/H'} \Leftrightarrow \chi_{\mathcal{G}/\mathcal{H}} = \chi_{\mathcal{G}/\mathcal{H}'}$. Therefore by Proposition (2.1.10), the proposition follows. $\square$

Corollary 2.1.12. *If $H \sim_G H'$ and if $M \trianglelefteq G$, then the following statements are equivalent.*

1. $HM \sim_G H'M$.

2. $HM/M \sim_{G/M} H'M/M$.

Proof. Put $L = HM$ and $L' = H'M$. Then $M \subseteq L \cap L'$. The corollary follows by Proposition (2.1.11) with L replacing H and L' replacing H'. □

Now we take the direct product on the bloc subgroups of a finite group G to construct new such pairs.

Lemma 2.1.13. *Let $G = K \times L$, the direct product of the groups K and L. If $H, H' \leq K$ with $H \sim_G H'$, then $H \sim_K H'$.*

Proof. Since $H \sim_G H'$, there exists a bloc $\varphi : H \longrightarrow H'$ in G, so for any $h \in H$;

$$\begin{aligned} \varphi(h) &= (k,l)(h,e)(k,l)^{-1} \\ &= (khk^{-1}, e) \in H' \end{aligned}$$

for some $(k,l) \in G$. Hence $\varphi(h) = khk^{-1} \in H'$ for all $h \in H$ and for some $k \in K$. So φ bloc in K. Therefore $H \sim_K H'$. □

Proposition 2.1.14. *Let $H, M \leq G$ and $H', M' \leq G'$. Then*

1. *If $H \sim_G M$ and $H' \sim_{G'} M'$, then $H \times H' \sim_{G \times G'} M \times M'$.*

2. *If $|H| = |M|$, then the converse of statement* (1) *also holds.*

Proof. We use the fixed point characters to prove the first result and the bloc φ to prove the second one.

1. Fix an element $(g, g') \in G \times G'$. We have

$$\begin{aligned}\chi_{G\times G'/H\times H'}(g,g') &= |\{(\gamma H,\gamma' H') \,|\, (g,g')(\gamma H,\gamma' H') = (\gamma H,\gamma' H')\}| \\ &= |\{(\gamma H,\gamma' H') \,|\, (g\gamma H, g'\gamma' H') = (\gamma H,\gamma' H')\}| \\ &= |\{(\gamma H,\gamma' H') \,|\, g\gamma H = \gamma H \text{ and } g'\gamma' H' = \gamma' H'\}| \\ &= \chi_{G/H}(g)\cdot\chi_{G'/H'}(g')\end{aligned}$$

Similarly $\chi_{G\times G'/H\times H'}(g,g') = \chi_{G/M}(g)\cdot\chi_{G'/M'}(g')$. By Proposition (2.1.10), $\chi_{G/H} = \chi_{G/M}$ and $\chi_{G'/H'} = \chi_{G'/M'}$. Therefore $\chi_{G\times G'/H\times H'} = \chi_{G\times G'/M\times M'}$.

2. Since $H\times H' \sim_{G\times G'} M\times M'$, there is a bloc $\varphi : H\times H' \longrightarrow M\times M'$ in $G\times G'$. So

$$\begin{aligned}\varphi((h,h')) &= (g,g')(h,h')(g,g')^{-1} \\ &= (ghg^{-1}, g'h'g'^{-1})\end{aligned}$$

for all $(h,h') \in H\times H'$ and for some $(g,g') \in G\times G'$. Take $h' = e$. Then $\varphi((h,e)) = (ghg^{-1},e)$. Hence φ induces a well-defined map $\bar{\varphi} : H \longrightarrow M$ given by $h \longmapsto ghg^{-1}$ for all $h \in H$.

Suppose $\bar{\varphi}(h_1) = \bar{\varphi}(h_2)$ for $h_1, h_2 \in H$. This implies that $h_1 = h_2$, so $\bar{\varphi}$ is an injective map. Also $|H| = |M|$ insures that $\bar{\varphi}$ is bijective. Hence $\bar{\varphi}$ is a G-bloc and therefore $H \sim_G M$.

Since $H\times H' \sim_{\bar{G}} M\times M'$ and $|H| = |M|$, it follows that $|H'| = |M'|$. Taking $g = e$ in the map φ, there is an induced map $\varphi' : H' \longrightarrow M'$, defined by $\varphi'(h') = g'h'g'^{-1}$ for all $h' \in H'$ and it is also a bloc in G. Hence $H' \sim_{G'} M'$.

□

2.2 Double Cosets and Equal Coset Types

We begin with the following small remark.

Remark 2.2.1. Let G be a group and H and C be subgroups of G. We consider the equivalence relation in G defined by

$$\sigma \sim \tau \iff \tau = h\sigma c \text{ for some } h \in H, \quad \text{and some } c \in C.$$

For $\sigma \in G$, the equivalence class

$$H\sigma C = \{h\sigma c \mid h \in H,\ c \in C\}$$

is called a double coset of G mod (H, C) and the set of all the double cosets is denoted by $H \setminus G/C$.

The double coset $H\sigma C$ has order

$$|H\sigma C| = \frac{|H|\,|C|}{|H \cap \sigma C \sigma^{-1}|}\,, \tag{2.2.1}$$

so σ varies, different double cosets can have different order. The group G decomposes as the disjoint union $G = \bigcup_{i=1}^{m} H\sigma_i C$ with $\{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ being representatives of double cosets.

Definition 2.2.2. The coset type of G modulo (H, C) is defined as the integer tupel $T = (t_1, t_2, \ldots, t_m)$, where t_i's are given by $|H\sigma_i C| = |H|\,t_i$ with the double cosets listed in non-decreasing order.

Proposition 2.2.3. *Let $H, H', C \leq G$. If*

$$\textit{coset type } [G \textit{ mod } (H, C)] = \textit{coset type } [G \textit{ mod } (H', C)],$$

then $|H| = |H'|$.

Proof. Let $(t_1, t_2, \ldots, t_m)$ be the common coset type of G mod (H, C), and G mod (H', C). We can write G as $G = \bigcup_{i=1}^{m} H\sigma_i C$ and $G = \bigcup_{i=1}^{m} H'\sigma_i C$, the disjoint union of double cosets. So

$$|G| = \sum_{i=1}^{m} |H\sigma_i C| = \sum_{i=1}^{m} |H'\sigma_i C|.$$

Hence,

$$|H| \sum_{i=1}^{m} t_i = |H'| \sum_{i=1}^{m} t_i.$$

Therefore $|H| = |H'|$. □

The following Lemma is proved by Perlis [15] p. 344.

Lemma 2.2.4. *Two subgroups H and H' of a group G are Gassmann equivalent if and only if the cosets types of G mod (H, C) and G mod (H, C) coincide for every cyclic subgroup C of G.*

Proof. cf. [15] Either condition, equal coset types or Gassmann equivalence, implies $|H| = |H'|$ [by Corollary (1.0.2) and by Proposition (2.2.3)].

Let C be a cyclic subgroup of G generated by $c \in G$.

For each $i = 1, 2, \cdots, n$, let l_i be the cardinality of the set $\{g \in G$ such that $|HgC|$ $= |H| \cdot i\}$. Since each double coset HgC of order $|H| \cdot i$ has exactly $|H| \cdot i$ elements. So $l_i = |\{$ cosets HgC of order $|H| \cdot i\}| \cdot |H| \cdot i$

Note that knowing $(t_1, t_2, \cdots, t_m)$ is equivalent to knowing $(l_1, l_2, \cdots, l_n)$. For example, if the coset type is $(1, 1, 1, 2, 5)$ then the tuple of l_i's is $(3, 1, 0, 0, 1)$ and each sequence defines the other.

Fix i. Then we have

$$\sum_{d|i} l_d = |\{g \in G \text{ such that } |HgC| \text{ divides } |H| \cdot i\}|$$

$$= |\{g \in G \text{ such that } \frac{|H||gCg^{-1}|}{|H \cap gCg^{-1}|} \text{ divides } |H| \cdot i\}|$$
$$= |\{g \in G \text{ such that } \left|\frac{gCg^{-1}}{H \cap gCg^{-1}}\right| \text{ divides } \cdot i\}|.$$

If $g \in G$ is an element counted in this sum, then the order of $\frac{gCg^{-1}}{H \cap gCg^{-1}}$ divides i. So $(gcg^{-1})^i \in H \cap g\langle c\rangle g^{-1}$ which implies that $gcg^{-1} \in H$. Conversely, if $g \in G$ satisfies $gc^ig^{-1} \in H$ then $\left|\frac{gCg^{-1}}{H \cap gCg^{-1}}\right|$ divides i. So

$$\sum_{d/i} l_d = |\{g \in G \text{ such that } gc^ig^{-1} \in H\}|$$
$$= |(c^i)^G \cap H| \cdot |\text{ stabilizer of } c^i|.$$

Call the last quantity k_i. Let μ be the Möbius function. By the Möbius inversion formula $l_i = \sum_{d/i} \mu(i/d) \cdot k_d$. Similarly, replacing H with H' gives l'_i in terms of k'_i, for d/i.

The sets of numbers $\{k_i\}$ and $\{l_i\}$ determine each other. For any cyclic subgroup C of G the coset types of G mod (H, C) and G mod (H', C) are equal if and only if $l_i = l'_i$ for all i if and only if $k_i = k'_i$ for all i if and only if $|(c^i)^G \cap H| = |(c^i)^G \cap H'|$ for all i, which defines Gassmann equivalence of H and H' in G. □

2.3 Multiplicative Bloc

In this section, we give an example of a multiplicative bloc φ (i.e. an isomorphism) from H to H' that is not a global conjugation in G.

Example 2.3.1. Let $\mathbb{Z}/8\mathbb{Z}$ be the additive group of integers modulo 8 and $(\mathbb{Z}/8\mathbb{Z})^*$ be the multiplicative group of units modulo 8. Consider the group

$$G = (\mathbb{Z}/8\mathbb{Z})^* \ltimes \mathbb{Z}/8\mathbb{Z} = \{(h, k) |\, h = 1, 3, 5, 7; k = 0, 1, 2, \ldots, 7\}$$

of order 32 with the operation defined by

$$(x, y)(h, k) = (xh, hy + k)$$

integers modulo 8. The identity element of G is $(1, 0)$ and for all $(h, k) \in G$, $(h, k)^{-1} = (h, -hk)$ as

$$(h, k)(h, -hk) = (h^2, hk - hk) = (1, 0) \text{ and}$$
$$(h, -hk)(h, k) = (h^2, -h^2k + k) = (1, 0).$$

Let

$$H = \{(1, 0), (3, 0), (5, 0), (7, 0)\}, \text{ and}$$
$$H' = \{(1, 0), (3, 4), (5, 4), (7, 0)\}.$$

These are two subgroups of G of index 8. Now define a map $\varphi : H \longrightarrow H'$ by

$$(1, 0) \longmapsto (1, 0)$$
$$(3, 0) \longmapsto (3, 4) = (1, 2)(3, 0)(1, 2)^{-1}$$
$$(5, 0) \longmapsto (3, 4) = (1, 7)(5, 0)(1, 7)^{-1}$$
$$(7, 0) \longmapsto (7, 0).$$

Clearly, φ is bijective, and φ is a bloc between H and H'. One can check that φ is also a group isomorphism from H to H'.

Suppose φ is a global conjugation by (x, y). Then for (h, k) in H,

$$\begin{aligned}\varphi(h, k) = (x, y)(h, k)(x, y)^{-1} &= (x, y)(h, k)(x, -xy) \\ &= (x, y)(hx, xk - xy) \\ &= (h, hxy + xk - xy).\end{aligned}$$

Thus the conjugation fixes the first factor h of any element (h, k), so we must have $\varphi(3, 0) = (3, 0)^{(x,y)} = (3, 4)$ and $\varphi(7, 0) = (7, 0)^{(x,y)} = (7, 0)$. But $(3, 0)^{(x,y)} = (3, 2xy)$ and $(7, 0)^{(x,y)} = (7, 6xy)$. Therefore $(3, 4) = (3, 2xy)$ and $(7, 0) = (7, 6xy)$

which imply $2xy \equiv 4(\text{mod } 8)$ and $6xy \equiv 0(\text{mod } 8)$ giving $6xy \equiv 12 \equiv 4 \equiv 0(\text{mod } 8)$, which is a contradiction. Hence φ is not a global conjugation in G.

Chapter 3
Local Conjugation and Same Order Type

In this chapter, we collect some results on local conjugation and prove that for any natural number m there exists a finite group G with $m+1$ subgroups that are pairwise non-conjugate and pairwise bloc in G.

3.1 Same Order Type Groups

Let G be a finite group. For each natural number j, define

$$G(j) = \{g \in G \text{ such that } |g| = j\}.$$

Definition 3.1.1. Two finite groups G and G' are said have the same order type if

$$|G(j)| = |G'(j)|$$

for any natural number j.

In such a case, we use the notation $G \sim_{ord} G'$. If $G \sim_{ord} G'$ then $|G| = |G'|$.

Lemma 3.1.2. *If $H \sim_G H'$, then H, H' have the same order type.*

Proof. Fix a bloc $\varphi : H \longrightarrow H'$ in G. Then for each $j \in \mathbb{N}$, the map φ induces a bijection

$$H(j) \longrightarrow H'(j).$$

Hence

$$|H(j)| = |H'(j)|.$$

□

The following example shows that the converse of the Lemma (3.1.2) is not true in general.

Example 3.1.3. Let $G = S_6$, symmetric group of degree 6. Let $H = \langle (12)(345) \rangle$ and $H' = \langle (123456) \rangle$ be two subgroups of G, both cyclic of order 6. These two subgroups have

- 1 element of order 1
- 1 element of order 2
- 2 elements of order 3 and
- 2 elements of order 6.

Therefore H and H' have the same order type. However, they are not locally conjugate in G because H has a generator with one fixed point and no generator of H' has any fixed points.

If two groups G and G' are isomorphic, then $G \sim_{ord} G'$. But the converse is not true, see Example (3.1.4). While assuming G and G' are abelian, the story is different, see Proposition (3.1.5) below.

Example 3.1.4. Consider the elementary abelian group $G = (\mathbb{Z}/3\mathbb{Z})^3$ and the Heisenberg group

$$G' = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{F}_3 \right\}$$

over the finite field $\mathbb{F}_3$. Both G and G' have the same order 27 and both have

$\circ$ 1 element of order 1 and

$\circ$ 26 elements of order 3

which means $G \sim_{ord} H$. However, G is not isomorphic to G' since G is abelian and G' is non-abelian.

Proposition 3.1.5. *If two finite abelian groups G and G' have the same order type, then they are isomorphic.*

Proof. Let G and G' be finite abelian groups having the same order type. So they have the same order.

Let $|G| = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ where $p_1, p_2, \cdots, p_t$ represent distinct prime numbers. Then G can be written as the direct product of its Sylow p_i-subgroups, say G_{p_i}:

$$G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_t}$$

such that $|G_{p_i}| = p_i^{e_i}$ for all $i = 1, 2, \cdots, t$. Similarly for G', we write

$$G' \cong G'_{p_1} \times G'_{p_2} \times \cdots \times G'_{p_t}.$$

Now it is enough to work on the groups G_{p_i} and G'_{p_i}. So we assume that G and G' are finite abelian p-groups of the same order type. The group G decomposes as

$$G \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_u}}, \quad n_1 \leq \cdots \leq n_u$$

with u direct summands, where each C_p is a cyclic group of p-power order. Similarly for G'

$$G' \cong C'_{p^{m_1}} \times C'_{p^{m_2}} \times \cdots \times C'_{p^{m_v}} \quad m_1 \leq \cdots \leq m_v$$

with v direct summands.

The number of elements of order p in G is $|G(p)| = p^u - 1$ and in G' is $|G'(p)| = p^v - 1$. But $|G(p)| = |G'(p)|$. Therefore $u = v$. If $n_u \neq m_u$ with $n_u > m_u$, then

G has elements of order p^{n_u} while G' does not. So $C_{p^{n_u}} = C'_{p^{n_v}} (= C,$ say). We proceed by induction on u. If $u = 1$, then $G \cong G'$. Assume that the result is true for all $k < u$

Write $H = C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_{u-1}}}$ and $H' = C'_{p^{n_1}} \times C'_{p^{n_2}} \times \cdots \times C'_{p^{n_{v-1}}}$. So $G \cong H \times C$ and $G' \cong H' \times C$. Suppose H, H' do not have the same order type. Then there exists a smallest $k \geq 1$ such that $|H(p^k)| \neq |H'(p^k)|$. Write $|H(p^k)| = f_k$ and $|H'(p^k)| = f'_k$. So $|G(p^k)| = f_k \cdot \sum_{i=0}^{k} |C(p^i)| + \sum_{i=0}^{k-1} f_i \cdot |C(p^k)|$ and similarly for $|G'(p^k)|$. But this leads that $|G(p^k)| \neq |G'(p^k)|$, which is a contradiction. Therefore H, H' must have the same order type. By induction hypothesis $H \cong H'$. Therefore $H \times C \cong H' \times C$. □

Fix $n \in \mathbb{N}$. Let S_n be the symmetric group of degree n. Any permutation $\sigma \in S_n$ can be written as a product of disjoint cycles.

Definition 3.1.6. Let $\sigma \in S_n$ be the product of t disjoint cycles of lengths $\lambda_1, \lambda_2, \cdots, \lambda_t$ with $1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_t$. Note that cycles of length 1 are included here. The sequence $(\lambda_1, \lambda_2, \ldots, \lambda_t)$ is called the *cycle type* of σ, or the *cycle length sequence* of σ.

Example 3.1.7. Let $\sigma \in S_6$ and $\sigma = (1)(34)(256)$. Then σ has cycle type $(1, 2, 3)$.

Remark 3.1.8. Note that any two permutations in S_n are conjugate if and only if they have the same cycle length sequence.

3.2 Constructing Groups with Pairwise Non-Conjugate Bloc Subgroups

Let H and H' be any two non-isomorphic groups not assumed to be bloc in any group. Assume that they are of the same order type and hence have the same order, say t. Each group H, H' can be embedded in the symmetric group S_t via its

regular representation. Since H and H' are not isomorphic, they are not conjugate in S_t.

Lemma 3.2.1. *[15] Two elements $h, k \in H \cup H'$ of same order j are conjugate in S_t.*

Proof. Assume that $h \in H$. As an element of S_t, h acts on H by multiplying its elements on the left. By the embedding H into S_t, h is the product of $\frac{t}{j}$ disjoint cycles where $|h| = j$. The same holds for k by the similar argument. Therefore h and k have the same cycle length sequence and hence, conjugate in S_t. □

Theorem 3.2.2. *Let H and H' be two non-isomorphic groups having the same the order t. Identify H and H' as subgroups of the symmetric group S_t by their regular representations. Then the following two statements are equivalent.*

1. *$H \sim_{S_t} H'$.*

2. *H and H' are of the same order type.*

Proof. (1) $\Rightarrow$ (2). Let I be the set of elements of G of order i. Then I is the disjoint union of conjugacy calsses in G : $I = \bigcup_{g \in T_i} g^G$, where T_i is the set set of representatives of conjugates of g of order i. Thus

$$|I \cap H| = \sum_{g \in T_i} |g^g \cap H| = \sum_{g \in T_i} |g^g \cap H'| = |I \cap H'|$$

(2) $\Rightarrow$ (1). Suppose H and H' have the same order type. Then H, H' can be embedded into the symmetric group S_t via its regular representation, where $|H| = |H'| = t$. We can define a bijection $\varphi : H \longrightarrow H'$ which preserves order, that is $|h| = |h'|$ where $h' = \varphi(h)$ for $h \in H$. By Lemma (3.2.1), φ is a bloc in S_t and hence $H \sim_{S_t} H'$. □

We now let p be an odd prime.

Theorem 3.2.3. *A nonabelian group G of order p^3 is isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$.*

Proof. See [7]. Example: (Groups of order p^3, p an odd prime) p. 183. □

As suggested by Perlis [15] p. 352, we consider an elementary abelian group $H = (\mathbb{Z}/p\mathbb{Z})^3$ and a nonabelian group $H' = \mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$ both of order p^3.

The group H' has the presentation

$$\langle x, y, z | x^p = y^p = z^p = 1, yz = zy, xyx^{-1} = yz, xzx^{-1} = z \rangle.$$

One computes that $Z(H') = \langle z \rangle$.

We consider H and H' as subgroups of the symmetric group S_{p^3} by their regular representations.

Lemma 3.2.4. *Let the groups H and H' be as above, then $H \sim_{S_{p^3}} H'$.*

Proof. Both H and H' have the same order p^3 and have

- 1 element of order 1 and
- $p^3 - 1$ elements of order p.

Hence H and H' have the same order type. Therefore by Lemma (3.2.2), we have $H \sim_{S_{p^3}} H'$. □

Theorem 3.2.5. *For every natural number m, there exists a finite group G with $m+1$ pairwise non-conjugate subgroups $H_0, H_1, \ldots, H_m$ such that $H_i \sim_G H_j$ for all $i, j = 0, 1, \ldots, m$.*

Proof. Let p be an odd prime number. Consider the following two groups as in Lemma (3.2.4), both of order p^3 :

- an abelian group $H = (\mathbb{Z}/p\mathbb{Z})^3$ and
- a non-abelian group $H' = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$.

Fix a natural number m. Now we construct the following groups

$$H_i = \underbrace{H \times H \times \cdots \times H}_{i \text{ times}} \times \underbrace{H' \times H' \times \cdots \times H'}_{m-i \text{ times}}$$

for all $i = 0, 1, \ldots, m$. Each H_i has

- 1 element of order 1 and
- $p^{3m} - 1$ elements of order p.

Hence these groups are of the same order type. Also $|H_i| = p^{3m}$ for all $i = 0, 1, \ldots, m$ and each H_i can be embedded into the symmetric group $S_{p^{3m}}$ by its regular representation.

We now assert that H_i is not isomorphic to H_j, for all $i \neq j$. We look at the centers of the groups H_i, for all $i = 0, 1, \ldots, m$. We have

$$Z(H_i) = \underbrace{Z(H) \times Z(H) \times \cdots \times Z(H)}_{i \text{ times}} \times \underbrace{Z(H') \times Z(H') \times \cdots \times Z(H')}_{m-i \text{ times}}.$$

The group H is abelian, so $Z(H) = H$ and $|Z(H)| = p^3$. And that $|Z(H')| = p$. Therefore

$$\begin{aligned} |Z(H_i)| &= p^{3i}.p^{m-i} \\ &= p^{m+2i} \end{aligned}$$

for $i = 0, 1, \ldots, m$ and hence $Z(H_i) \neq Z(H_j)$ for any $i \neq j$. This shows that these groups are pairwise non-isomorphic and hence pairwise non-conjugate in $S_{p^{3m}}$. However, by Lemma (3.2.2), $H_i \sim_{S_{p^{3m}}} H_j$ for all $i, j = 0, 1, \ldots, m$. □

3.3 Blocs and Nilpotency

Lemma 3.3.1. *Let $\varphi : H \longrightarrow H'$ be a bloc in G. For a fixed prime number p, let P be a p-Sylow subgroup of H. If $P \trianglelefteq H$, then $\varphi(P) \trianglelefteq H'$.*

Proof. Being normal in H, the subgroup P contains all elements of p-power order in H. Let $|P| = p^e$, for some positive integer e. Since φ preserves the number of elements of given order in H and H' [Lemma (3.1.2)], the number of elements of p-power order in H' is p^e. Let P' be a p-Sylow subgroup of H'. Also $\varphi(P) \subseteq H'$, consisting of p^e elements each of p-power order. Therefore $P' \subseteq \varphi(P)$, and hence $P' = \varphi(P)$. This proves $\varphi(P)$ is subgroup of H'.

Now if P' is not normal in H', then there would be a distinct p-Sylow subgroup P'' in H'. Pick $x \in P'' \setminus P'$, then x has p-power order. So $x \in \varphi(P) = P'$, a contradiction. □

Proposition 3.3.2. *Let $H \sim_G H'$ and H be a nilpotent group. Then H' is also a nilpotent group.*

Proof. Let $p_1, p_2, \cdots, p_t$ be the distinct prime factors of the order of H, say $|H| = p_1^{e_1} \cdot p_2^{e_2} \cdots p_t^{e_t}$. So the number of elements of order p_i-power in H is $p_i^{e_i}$. Let P_i be a p_i-Sylow subgroup of H for all $i = 1, 2, \cdots, t$. Since H is nilpotent, it must be the direct product of all Sylow subgroups: $H \cong P_1 \times P_2 \times \cdots \times P_t$. Moreover, $P_i \trianglelefteq H$.

Since H and H' are bloc subgroups, there exists a bloc $\varphi : H \longrightarrow H'$ in G under which the number of elements of given order in H and H' is preserved [Lemma (3.1.2)]. Therefore the number of elements of order p_i-power in H' has to be $p_i^{e_i}$. This means $|H'| = p_1^{e_1} \cdot p_2^{e_2} \cdots p_t^{e_t}$. Let P' be a p_i-Sylow subgroup of H'. By Proposition (3.3.2), we have $P_i' = \varphi(P_i)$ and also $P_i' \trianglelefteq H'$. Hence we proved that each p_i-Sylow subgroup P_i' of H' is a normal subgroup. Thus H' is also nilpotent. □

In Proposition (3.3.2), however, H and H' do not necessarily have the same nilpotency class. Suppose that the nilpotency class of H is 1, which means H is abelian. But the local conjugation does not force H' to be abelian. Hence the nilpotency class of H' has to be greater than 1.

On the other hand if two subgroups $H, H' \leq G$ are both nilpotent and have the same nilpotency class, then one can ask whether H and H' are locally conjugate. The answer again is no! We can take a simple example. Consider two groups

$$H = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \text{ and } H' = \mathbb{Z}/p^2\mathbb{Z}$$

both of order p^2, where p is a prime number. Both of these groups are nilpotent with the same nilpotency class 1. However, they are not locally conjugate. Since they do not have the same order type.

Let π be any set of prime numbers. A finite group is called a π-group if all the primes that divide its order lie in π. A subgroup H of G is called a *Hall π-subgroup* if it is a π-group and its index $[G : H]$ is not divisible by any primes from π.

Theorem 3.3.3. *c.f. [17] Let the finite group G possess a nilpotent Hall π-subgroup H. Then every π-subgroup of G is contained in a conjugate of H. In particular all Hall π-subgroups of G are conjugate.*

Proof. See [17] §9.1 pp. 259. □

Theorem 3.3.4. *Suppose $H \sim_G H'$ and H is a nilpotent Hall π-subgroup of G. Then H and H' are conjugate in G.*

Proof. By Proposition (3.3.2), H' is nilpotent. But H' is also a Hall π-subgroup. The rest of the proof follows from the theorem above. □

Chapter 4

A Different Approach to Locally Conjugate Groups

In this chapter, we provide an alternative approach to bloc equivalence.

4.1 Yet Another Characterization of Bloc Equivalence

Fix $n \in \mathbb{N}$. Let σ be a permutation in S_n which is the product of t disjoint cycles of lengths $\lambda_1, \lambda_2, \cdots, \lambda_t$ with $1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_t$, each $\lambda_i = \lambda_i(\sigma)$. We include 1-cycles in σ. Recall from Chapter 3 that the sequence $(\lambda_1, \lambda_2, \ldots, \lambda_t)$ is called the *cycle length sequence* of σ, also called the cycle type of σ. Now consider the tuple $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ where $\gamma_i = \gamma_i(\sigma)$ denotes the number of cycles of length i in the canonical factorization of σ. We call $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ the *cycle number sequence* of σ.

Example 4.1.1. Let $n = 8$ and let $\sigma = (13)(27)(456)(8) \in S_8$. Then σ has the cycle length sequence $(1, 2, 2, 3)$ and the cycle number sequence $(1, 2, 1, 0, 0, 0, 0, 0)$.

The following result is trivial but we state as a proposition for later reference.

Proposition 4.1.2. *For any $\sigma \in S_n$, the cycle type $(\lambda_1, \lambda_2, \ldots, \lambda_t)$ of σ determines the cycle number sequence $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ and vice versa.*

Note that $\sum_{i=1}^{t} \lambda_i = n$, since every element in $\{1, 2, \ldots, n\}$ appears in exactly one cycle of σ. Also, $\sum_{i=1}^{n} \gamma_i(\sigma) = t$, the total number of cycles in σ. We write $\Gamma(\sigma)$ for t, the total number of cycles in σ.

Remark 4.1.3.

1. Fix positive integers k, j. When σ is raised to the k^{th} power, for each j-cycle in σ gives rise to a product of certain number, d, of cycles of the same lengths in σ^k. Namely, for $d = \gcd(k, j)$, each j-cycle in σ gives rise to d cycles each of length $\frac{j}{d}$ in σ^k.

2. Fix k and let j runs over the divisors of k. Then $d = \gcd(k, j) = j$. So $\frac{j}{d} = 1$ and the number of 1-cycles of σ^k is given by the following formula

$$\gamma_1(\sigma^k) = \sum_{j \mid k} j.\gamma_j(\sigma).$$

3. The total number of cycles in σ^k is

$$\Gamma(\sigma^k) = \gcd(k, 1) \cdot \gamma_1(\sigma) + \gcd(k, 2) \cdot \gamma_2(\sigma) + \cdots + \gcd(k, n) \cdot \gamma_n(\sigma).$$

Lemma 4.1.4. *For any $\sigma, \tau \in S_n$, the following statements are equivalent.*

1. *σ and τ are conjugate in S_n.*

2. *$\Gamma(\sigma^k) = \Gamma(\tau^k)$, for all $k \in \mathbb{N}$.*

3. *$\gamma_i(\sigma) = \gamma_i(\tau)$, for $i = 1, 2, \ldots, n$.*

Proof. [R. Litherland].

(1) $\Rightarrow$ (2). Fix $k \in \mathbb{N}$. Suppose σ, τ are conjugate in S_n. So σ^k, τ^k are also conjugate in S_n. This implies that $\gamma_i(\sigma^k) = \gamma_i(\tau^k)$ for all $i = 1, 2, \ldots, n$. Therefore,

$$\sum_{i=1}^{n} \gamma_i(\sigma^k) = \sum_{i=1}^{n} \gamma_i(\tau^k).$$

(2) $\Rightarrow$ (3). Let

$$M = \begin{pmatrix} (1,1) & (2,1) & \dots & (k,1) & \dots & (n,1) \\ (1,2) & (2,2) & \dots & (k,2) & \dots & (n,2) \\ \vdots & \vdots & & \vdots & & \vdots \\ (1,n) & (2,n) & \dots & (k,n) & \dots & (n,n) \end{pmatrix}$$

where (i,j) denotes for $\gcd(i,j)$. By Smith [22], $\det(M) = \prod_{k=1}^{n} \varphi(k)$ $(\neq 0)$, where $\varphi(k)$ is Euler's phi function applied to k. By Remark (4.1.3), we can write

$$(\Gamma(\sigma), \Gamma(\sigma^2), \dots, \Gamma(\sigma^n)) = (\gamma_1(\sigma), \gamma_2(\sigma), \dots, \gamma_n(\sigma))M.$$

Therefore,

$$\begin{aligned} (\gamma_1(\sigma), \gamma_2(\sigma), \dots, \gamma_n(\sigma)) &= (\Gamma(\sigma), \Gamma(\sigma^2), \dots, \Gamma(\sigma^n))M^{-1} \\ &= (\Gamma(\tau), \Gamma(\tau^2), \dots, \Gamma(\tau^n))M^{-1}, \text{ by assumption} \\ &= (\gamma_1(\tau), \gamma_2(\tau), \dots, \gamma_n(\tau)). \end{aligned}$$

Hence $\gamma_i(\sigma) = \gamma_i(\tau)$ for all $i = 1, 2, \dots, n$.

(3) $\Rightarrow$ (1) Since each of σ and τ has the same number of cycles of any given length $i \in \{1, 2, \dots n\}$ in its canonical factorization, the rest follows by Proposition (4.1.2). $\square$

Let H be a subgroup of index n in a finite group G. To each element $g \in G$, let π_g be the permutation on G/H given by left multiplication by g. We fix a counting of G/H and consider $\pi_g \in S_n$. Then

$$\Gamma(\pi_g) = \text{number of cycles in the factorization of } \pi_g \text{ in } S_n.$$

Similarly, π'_g is the permutation coming from g in G acting on G/H'.

Definition 4.1.5. Two subgroups H, H' in a finite group G are said to be *cycle number equivalence* in G if every g in G has $\Gamma(\pi_g) = \Gamma(\pi'_g)$.

Lemma 4.1.6. *The following statements are equivalent.*

1. *H and H' are bloc in G.*

2. *$\Gamma(\pi_g) = \Gamma(\pi'_g)$ for all $g \in G$.*

3. *π_g and π'_g have the same cycle length sequence for all $g \in G$.*

4. *$(G : H) = (G : H') = n$ and π_g, π'_g are conjugate in S_n, for all $g \in G$.*

Proof. Any of the above conditions implies $(G : H) = (G : H')$. We call this common index n.

(1) $\Rightarrow$ (4) We have $\chi_{G/H}(g) = \gamma_1(\pi_g)$ for all $g \in G$. By Remark (4.1.3),

$$\chi_{G/H}(g^k) = \sum_{j \mid k} j.\gamma_j(\pi_g) \text{ for all } g \in G \text{ and } k = 1, 2, \ldots, n.$$

But for all k, we have

$$\begin{aligned} \chi_{G/H}(g^k) &= \chi_{G/H'}(g^k) \\ &= \sum_{j \mid k} j.\gamma_j(\pi'_g). \end{aligned}$$

Successively choosing $k = 1, 2, \ldots, n$, we have the equality

$$\gamma_j(\pi_g) = \gamma_j(\pi'_g).$$

for all j. By Proposition (4.1.4), π_g and π'_g are conjugate in S_n for all $g \in G$.

(4) $\Rightarrow$ (3) Follows from Remark (3.1.8).

(3) $\Rightarrow$ (2) Follows from Proposition (4.1.2).

(2) $\Rightarrow$ (1) Suppose $\Gamma(\pi_g) = \Gamma(\pi'_g)$ for all $g \in G$. Fix $\alpha \in G$. Then $\Gamma(\pi_{\alpha^k}) = \Gamma(\pi'_{\alpha^k})$. But $\pi_{\alpha^k} = (\pi_\alpha)^k$, so

$$\Gamma(\pi_\alpha^k) = \Gamma(\pi_\alpha'^k) \text{ for } k = 1, 2, \ldots, n.$$

Then by Lemma (4.1.4), $\gamma_i(\pi_\alpha) = \gamma_i(\pi'_\alpha)$, for $i = 1, 2, \ldots, n$. In particular,

$$\gamma_1(\pi_\alpha) = \gamma_1(\pi'_\alpha).$$

This means, $\chi_{G/H}(\alpha) = \chi_{G/H'}(\alpha)$ and hence H and H' are bloc in G. □

4.2 Collection of Reformulations of Bloc Equivalence

In this section, we collect all the equivalent reformulations of Bloc equivalence (1.0.1) described in this dissertation.

Lemma 4.2.1. *Let G be a finite group and H, H' be subgroups of G. The following statements are equivalent.*

1. *H, H' satisfy Gassmann's condition* (1.0.1) *in G.*
2. *H, H' are bloc subgroups in G.*
3. *There exists a bloc $\bar{\varphi} : G \longrightarrow G$ such that $\bar{\varphi}(H) = H'$.*
4. *$\mathbb{Q}[G/H] \cong \mathbb{Q}[G/H']$ as $\mathbb{Q}[G]$-modules.*
5. *$\chi_{G/H} = \chi_{G/H'}$.*
6. *coset type $[G \text{ mod } (H, C)]$ = coset type $[G \text{ mod } (H', C)]$ for any cyclic subgroup C of G.*
7. *$\Gamma(\pi_g) = \Gamma(\pi'_g)$ for all $g \in G$,*
8. *π_g and π'_g have the same cycle length sequence for all $g \in G$,*
9. *π_g and π'_g have the same cycle number sequence for all $g \in G$,*
10. *$(G : H) = (G : H') = n$ and π_g, π'_g are conjugate in S_n, for all $g \in G$.*

Chapter 5
Applications to Number Fields

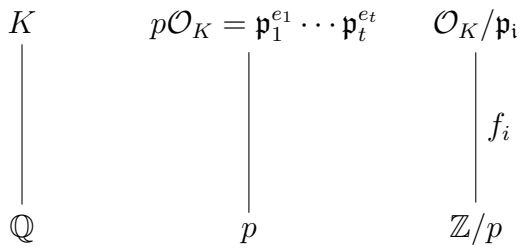
In this chapter, we apply some of the results we obtained in previous chapters to algebraic number fields. The main objective are:

1. to show that there is no finite upper bound to the number of pairwise non-isomorphic, arithmetically equivalent number fields.

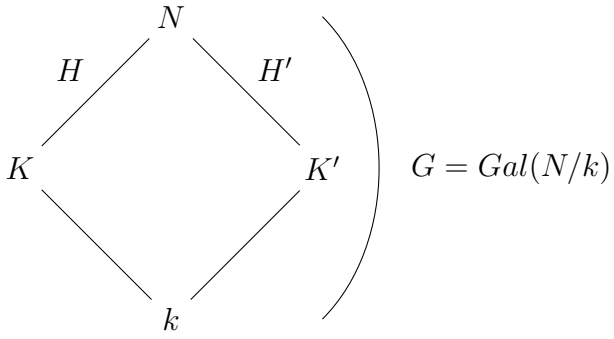
2. to give a new proof of the theorem of Stuart and Perlis: two number fields K and K' have identical Dedekind zeta functions if and only if almost every prime number p has the same number of prime ideal factors in K as in K'.

5.1 Arithmetically Equivalent Fields

One of the most interesting invariants associated to an algebraic number field K is its Dedekind zeta function $\zeta_K(s)$. If two number fields K and K' are isomorphic, then $\zeta_K(s) = \zeta_{K'}(s)$. However, there are examples of nonisomorphic number fields K, K' with identical zeta functions. The first such example was constructed by Gassmann [8] in 1926. In 1977 Perlis [15] discovered two infinite families of pairs of nonisomorphic number fields with identical zeta functions.



Throughout this chapter, K and K' will denote two finite extensions of a number field k and N/k denotes a finite Galois extension containing K, K' with Galois groups $G = Gal(N/k)$, $H = Gal(N/K)$ and $H' = Gal(N/K')$.



For any number field L, we denote by $\mathcal{O}_L$ the ring of integers and by $\mathcal{P}_L$ the set of non-zero prime ideals in $\mathcal{O}_L$. Let $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ be the decomposition of a prime ideal $\mathfrak{p}$ of k into prime ideals $\mathfrak{P}_i$ of K and let $f_i = (\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_k/\mathfrak{p})$ be the inertia degree of $\mathfrak{P}_i$ over $\mathfrak{p}$. Number the inertia degrees f_i so that $f_1 \leq \dots \leq f_g$.

Definition 5.1.1. 1. For $\mathfrak{p}$ in $\mathcal{O}_k$, the tuple $A_K(\mathfrak{p}) = (f_1, f_2, \dots, f_g)$ is called the *splitting type* of $\mathfrak{p}$ in K.

2. For any tuple $A = (f_1, f_2, \dots, f_g)$ of positive integers with $f_i \leq f_{i+1}$, define

$$\mathcal{P}_K(A) = \{\mathfrak{p} \in \mathcal{O}_k \,|\, \mathfrak{p} \text{ has splitting type } A \text{ in } K\}.$$

For many choices of A, the set $\mathcal{P}_K(A)$ could be empty.

If S and T are any two sets, the symbol $S \doteq T$ is used to indicate that S and T are equal up to a finite number of elements. In the case, when $k = \mathbb{Q}$, Perlis proved the following theorem which translates the analytic condition $\zeta_K(s) = \zeta_{K'}(s)$ into a group theory condition.

Theorem 5.1.2. *[15] The following statements are equivalent.*

1. $\zeta_K(s) = \zeta_{K'}(s)$.

2. $\mathcal{P}_K(A) = \mathcal{P}_{K'}(A)$ *for every tuple* A.

3. $\mathcal{P}_K(A) \doteq \mathcal{P}_{K'}(A)$ *for every tuple* A.

4. H *and* H' *are Gassmann equivalent in* G.

Proof. See [15] p. 345. □

The equivalence of (1) and (4) in this theorem, together with Proposition (1) show that $\zeta_K(s) = \zeta_{K'}(s)$ if and only if there exits a bloc $\varphi : H \longrightarrow H'$ in G.

Perlis [15] also proved that

Theorem 5.1.3. *If* $H \sim_G H'$ *and* $(G : H) \leq 6$*, then* H *is conjugate in* G *to* H.

His statement of this theorem refers to $\zeta_K(s) = \zeta_{K'}(s)$ but the proof only uses Gassmann's condition.

Definition 5.1.4. Two finite extensions K, K' of a number field k are said to be *arithmetically equivalent* over k if almost all prime ideals $\mathfrak{p}$ of k have the same splitting types in K and K', that is, for every tuple A:

$$\mathcal{P}_K(A) \doteq \mathcal{P}_{K'}(A).$$

We use the notation $K \approx_k K'$ to indicate that K, K' are arithmetically equivalent over k.

When the base field $\mathbb{Q}$ in Theorem (5.1.2) is replaced by a general number field k, the condition (1) is not sufficient for Gassmann's condition (4), see Example (5.1.8) below. In this case, Nagata [13] showed that (4) is equivalent to (1) if ζ_K is replaced by certain Artin L-functions. Alternatively, we can replace the zeta function of K by a family of so-called "partial zeta functions".

Definition 5.1.5. Let K/k be a finite extension of number fields. For any $\mathfrak{p} \in \mathcal{P}_k$, the partial zeta function of K over k is defined as

$$\zeta_{K,\mathfrak{p}}(s) = \prod_{\mathfrak{P} \mid \mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{P})^{-s}}$$

where the product runs over all primes $\mathfrak{P}$ of K lying above $\mathfrak{p}$.

The following theorem is proved in [10].

Theorem 5.1.6. *[10] Two finite extensions K and K' are arithmetically equivalent over k if and only if $\zeta_{K,\mathfrak{p}} = \zeta_{K',\mathfrak{p}}$, for all $\mathfrak{p} \in \mathcal{P}_k$.*

Theorem 5.1.7. *If $K \approx_k K'$ and K/k is a normal extension, then $K = K'$.*

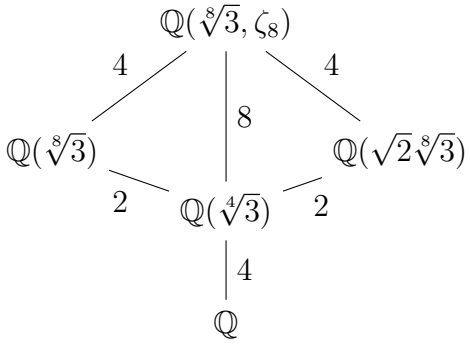
Proof. Let N/k be a common normal closure of K and K'. Set

$$G = Gal(N/k),\ H = Gal(N/K) \text{ and } H' = Gal(N/K').$$

Thus $H \sim_G H'$. Since K/k is normal, it follows that $H \trianglelefteq G$. By Lemma (2.1.2), $H = H'$ and hence $K = K'$. □

The following example shows that equality of zeta functions of two number fields does not always imply the Gassmann condition in Theorem (5.1.2) in case the base field is not $\mathbb{Q}$.

Example 5.1.8. Let $K = \mathbb{Q}(\sqrt[8]{3})$, $K' = \mathbb{Q}(\sqrt{2}\sqrt[8]{3})$ and $k = \mathbb{Q}(\sqrt[4]{3})$ be degree 8 extensions of $\mathbb{Q}$. Let $N = \mathbb{Q}(\sqrt[8]{3}, \zeta_8)$. Then N is a Galois extension of $\mathbb{Q}$ containing both K and K'.

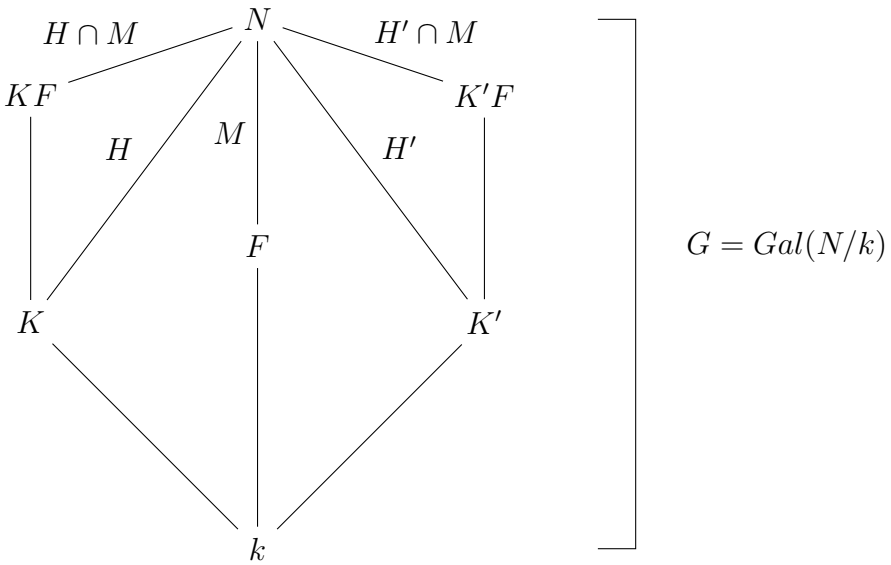


Denote $G = Gal(N/k)$, $H = Gal(N/K)$, $H' = Gal(N/K')$ and $\mathcal{G} = Gal(N/\mathbb{Q})$. Then $H, H' \leq G \leq \mathcal{G}$. By [6], number fields K and K' have the identical Dedekind zeta functions, so $H \sim_{\mathcal{G}} H'$.

Now H and H' have index 2 in G. If $H \sim_G H'$, then by (5.1.3), the subgroups H, H' are conjugate in G. Therefore K, K' are isomorphic quadratic extension over k. So they are normal over k. By Theorem (5.1.7), $K = K'$. But this is not true. Therefore H and H' do not satisfy Gassmann's condition in G.

Theorem 5.1.9. *[10] If $K \approx_k K'$ and F/k is a normal extension of number fields, then $KF \approx_k K'F$.*

Proof. Let N/k be a normal extension containing K, K' and F.



Set $G = Gal(N/k)$, $M = Gal(N/F)$, $H = Gal(N/K)$ and $H' = Gal(N/K')$ as shown in the following figure. So $M \trianglelefteq G$. Let KF be the fixed field of $H \cap M$ and $K'F$ be the fixed field of $H' \cap M$.

By proposition (1.0.4), $H \cap M$ and $H' \cap M$ are bloc in G. Hence $KF \approx_k K'F$.

□

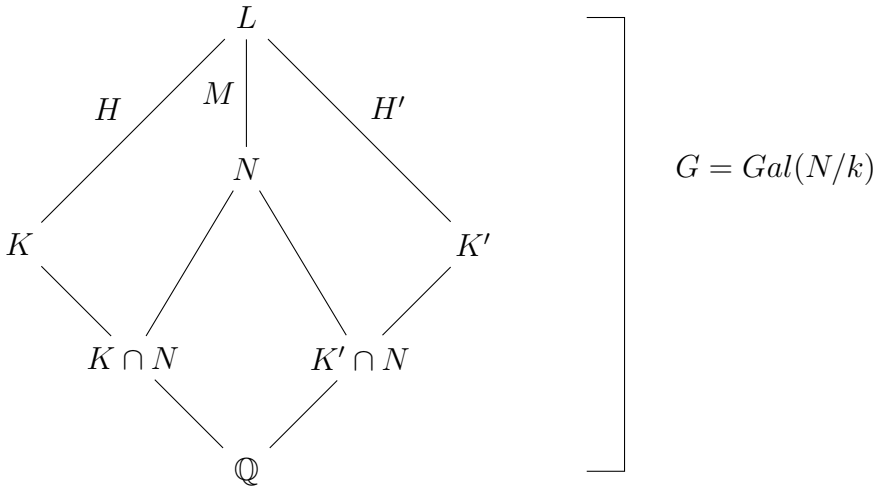
The following theorem is proved by Nagata [12] p. 362. The proof below comes from Proposition (2.1.4) of this dissertation.

Theorem 5.1.10. *Let $K \approx_k K'$ and N/k be an abelian extension of number fields. Then $K \cap N = K' \cap N$.*

Proof. Let L/k be the common normal closure of K and K' over k. Set

$$G = Gal(L/k),\ M = Gal(L/M),\ H = Gal(N/K) \text{ and } H' = Gal(N/K')$$

as shown in the above figure.



Then $Gal(L/K \cap N) = HM$ and $Gal(L/K' \cap N) = H'M$. In addition, G/M is abelian. By proposition (2.1.4), $HM = H'M$. Therefore, $K \cap N = K' \cap N$. □

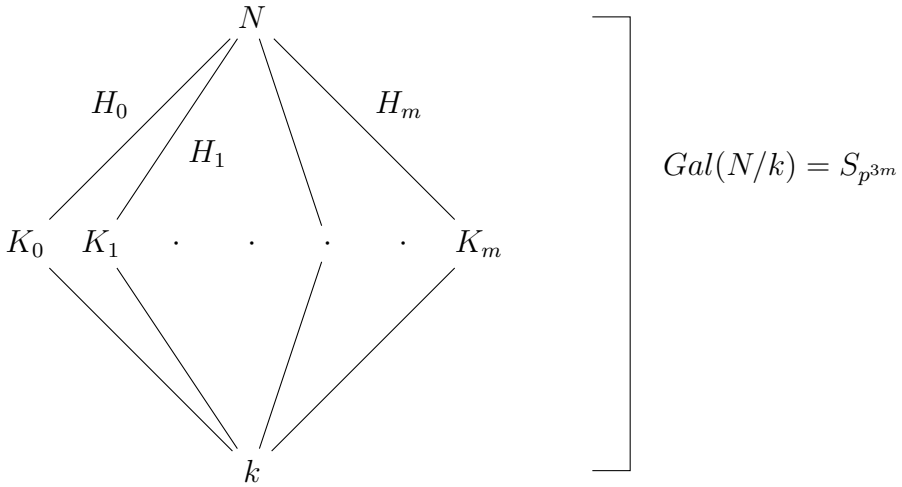
5.2 A Construction of Arithmetically Equivalent Fields

Following theorem shows that there is no upper bound to the number of pairwise non-isomorphic, arithmetically equivalent number fields. Most of the work for this result is already done in Theorem (3.2.5).

Theorem 5.2.1. *Fix a number field k. For every natural number m there exist $m+1$ arithmetically equivalent fields $K_0, K_1, \ldots, K_m$ over k such that K_i is not isomorphic to K_j for $i \neq j$ where $i, j = 0, 1, \ldots, m,$.*

Proof. Fix a natural number m. In Theorem (3.2.5), we constructed a finite group $G = S_{p^{3m}}$ with $m+1$ pairwise non-isomorphic, bloc subgroups $H_0, H_1, \ldots, H_m$.

We now turn our attention to the number fields. Let N/k be a Galois extension with $Gal(N/k) \cong S_{p^{3m}}$ and let $K_0, K_1, \ldots, K_m$ be the subfields of N corresponding to $H_0, H_1, \ldots, H_m$ respectively. Therefore, it follows by Theorem (5.1.2) that $K_i \approx_k K_j$ for all $i, j = 0, 1, \cdots, m$.



However, since the groups $H_0, H_1, \cdots, H_m$ are pairwise non-conjugate in $S_{p^{3m}}$, it follows that the fields $K_0, K_1, \cdots, K_m$ are pairwise non-isomorphic. □

5.3 A New Proof of the Stuart-Perlis Theorem

In this section, we give a new proof of the Theorem (5.3.1) below. This theorem appeared in a paper [24] by Stuart and Perlis in 1995 and comes here as a corollary of Lemma (4.1.6) in this dissertation.

Theorem 5.3.1. *[24] Let k be any number field and let K and K' be two finite extensions of k. The following statements are equivalent.*

1. *K, K' are arithmetically equivalent over k.*
2. *Almost every prime ideal $\mathfrak{p}$ of k has the same number of prime ideal factors in K and K'.*

The following theorem traces back to Weber and Dedekind. This gives the connection between decomposition of prime ideals in a field extension and group theory.

Theorem 5.3.2. *Let $K = k(\alpha)/k$ be a finite extension of number fields, N/k a Galois extension with $K \subset N$ and $G = Gal(N/k)$. For any prime ideal $\mathfrak{p}$ of k which is unramified in N the following statements are equivalent.*

1. *$\mathfrak{p}$ has splitting type $(f_1, f_2, \ldots, f_t)$ in K.*
2. *For any prime $\mathfrak{Q}/\mathfrak{p}$ of N, the Frobenius automorphism $\sigma_{\mathfrak{Q}}$ acting on the n conjugates of α has cycle length sequence $(f_1, f_2, \ldots, f_t)$.*

Proof. See Klingen [10] p. 11. □

Let N/k be a Galois extension of number fields containing both K and K'. Let $\mathfrak{p}$ be a prime ideal of k, unramified in N and let $\mathfrak{Q}$ some prime of N lying above $\mathfrak{p}$. Let $\sigma_{\mathfrak{Q}}$ be the Frobenius automorphism of $\mathfrak{Q}$.

Denote $G = Gal(N/k)$, $H = Gal(N/K)$ and $H' = Gal(N/K')$ as usual. Then G acts transitively on the conjugates of α in N and H is the G-stabilizer of α. So the G-action on the set of conjugates of α is the same as the action of G by left multiplication on the cosets G/H. Let $\pi_{\sigma_{\mathfrak{Q}}}$ be the permutation of G/H coming from the action of $\sigma_{\mathfrak{Q}}$ in G.

Let $(f_1, f_2, \ldots, f_t)$ be the splitting type of $\mathfrak{p}$ in K. It follows by Theorem (5.3.2) that $\pi_{\sigma_{\mathfrak{Q}}}$ has the cycle length sequence $(f_1, f_2, \ldots, f_t)$. Therefore, the total number of cycles in $\pi_{\sigma_{\mathfrak{Q}}}$ is t, the number of prime ideal factors of $\mathfrak{p}$ in K.

Proof of Theorem (5.3.1). (1) $\Rightarrow$ (2). Obvious.

(2) $\Rightarrow$ (1). By hypothesis, there is a finite subset S of $\mathcal{P}_k$, for which every prime in $\mathcal{P}_k \setminus S$ has the same number of prime ideal factors in K as in K'. If necessary, enlarge S to contain all primes of k that ramify in N. For each $\mathfrak{p}$ not in S, choose a prime $\mathfrak{Q}$ of N lying over $\mathfrak{p}$, and let $\sigma_{\mathfrak{Q}}$ denotes the Frobenius automorphism of $\mathfrak{Q}$ over $\mathfrak{p}$. It is given that

$$\Gamma(\pi_{\sigma_{\mathfrak{Q}}}) = \Gamma(\pi'_{\sigma_{\mathfrak{Q}}}) \text{ for all } \mathfrak{p} \in \mathcal{P}_k \setminus S.$$

Now take $\omega \in G$. By Chebotarev Density Theorem, there exists a prime $\mathfrak{p}$ in $\mathcal{P}_k \setminus S$ and a prime $\mathfrak{Q}$ of N lying over $\mathfrak{p}$ with $\sigma_{\mathfrak{Q}} = \omega$. So

$$\Gamma(\pi_\omega) = \Gamma(\pi'_\omega).$$

But ω is an arbitrary. So

$$\Gamma(\pi_\omega) = \Gamma(\pi'_\omega) \text{ for all } \omega \in G.$$

By Lemma (4.1.6), the subgroups H and H' are bloc in G. Therefore, $K \approx_k K'$ $\square$

References

[1] Adelmann, C., *The Decomposition of Primes in Torsion Point Fields*, Springer Lect. Notes Math. 1761 (2001)

[2] Adkins, W. and Weintraub, S., *Algebra: An Approach via Module Theory*, Springer - Verlang, New York, 1992.

[3] Buser, P., *Geometry and Spectra of Compact Riemann Surfaces*, Birkhäuser, Boston, 1992.

[4] Cassels, J. W. S. and Frohlich, A., editors *Algebraic Number Theory*, London Mathematical Society, London, 2010.

[5] Chen, S., *Constructing Isospectral but Non-isometric Riemann Manifolds*, Canad. Math. Bull. **35** (1992), 303–310.

[6] de Smit, B. and Perlis, R., *Zeta functions do not determine class numbers*, Bull. of the American Math. Soc. **31** (1994), 213 –215.

[7] Dummit, D. and Foote, R.*Abstract Algebra*, John Wiley and Sons,Inc. 2004.

[8] Gassmann, F., *Bemerkungen zu der Vorstehenden Arbeit von Hurwitz*, Math. Z. **25** (1926), 124–143.

[9] Johnson, W., *An LDU Factorization in Elementary Number Theory*, Math Magazine, **76** (2003), 392–394.

[10] Klingen, N., *Arithmetical Similarities*: *Prime Decomposition and Finite Group Theory*, Oxford University Press Inc., New York, 1998.

[11] Lang, S., *Algebraic Number Theory*, Springer - Verlag, New York, 1994.

[12] Nagata, K., *Artin's L-functions and Gassmann Equivalence*, Tokyo J. Math **9-2** (1986).

[13] Neukirch, J., *Class Field Theory*, Springer - Verlag, Berlin Heidelberg, 1986.

[14] Neukirch, J., *Algebraic Number Theory*, Springer - Verlang, Berlin Heidelberg, 1999.

[15] Perlis, R., *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 242–260.

[16] Perlis, R., *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 489–509.

[17] Robinson, D., *A Course in the Theory of Groups*, Springer - Verlag, New York, 1996.

[18] Schinzel, A., *On a theorem of Bauer and some of its applications*, Acta Arithmetica **XI** (1966), 333 - 344 .

[19] Scott, W. R., *Group Theory*, Dover Publications, Inc., New York, 1987.

[20] Serre, J. - P., *A Course in Arithmetic*, Springer - Verlag, New York (1973).

[21] Serre, J. - P., *Linear Representations of Finite Groups*, Springer - Verlag, New York (1977).

[22] Smith, H.J.S., *On the Value of a Certain Arithmetical Determinant*, Proc. London Math. Soc. **7** (1876), 208 - 212.

[23] Stark, H.M. and Terras, A.A., *Zeta functions of finite graphs and coverings, Part II*, Advances in Mathematics **154** (2000), 132–195.

[24] Stuart, D. and Perlis, R., *A new characterization of arithmetic equivalence*, J. Number Theory **53** (1995), 300–308.

[25] Sunada, T., *Riemannian coverings and isospectral manifolds*, Ann. of Math. **121**(1985), 169–186.

Vita

Bir B. Kafle was born in Dhankuta, Nepal. He finished his undergraduate studies in mathematics education at Tribhuvan University in 2000. He earned a Master of Science degree in mathematics from Western Illinois University in May 2009. In August 2009 he came to Louisiana State University to pursue graduate studies in mathematics. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2014.