# UNIVERSAL COMPLETIONS OF CYCLIC AMALGAMS OF THE SAME TYPE

by

ATAPATTU CHAMILA KANCHANA ARACHCHILLE

A thesis submitted to

the University of Birmingham

for the Degree of Master of Philosophy

School of Mathematics and Statistics

University of Birmingham

Birmingham, United Kingdom

January, 2010

# Abstract


Automorphisms of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\times}$. If G is a finite abelian group, which is

isomorphic to direct product of m cyclic groups of order q where $q = p^n$ for some prime p. Then Aut(G) is isomorphic to the set of m×m matrices with determinant coprime to p, $GL_m(\mathbb{Z}_q)$. Also $|Aut(G)| = p^{(n-1)m^2}|GL_m(\mathbb{Z}_q)|$.

If $\alpha$ is an automorphism of $S_n$ and t is a transposition of $S_n$ for $n \neq 6$, then $\alpha(t)$ is a transposition. If $\alpha$ maps transposition to a transposition, then $\alpha$ is an inner automorphism. Then $Aut(S_n) \cong S_n$, $n \neq 6$. Furthermore, there exists an outer automorphism of $S_6$ and $Out(S_6) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$. Thus $|Out(S_6)| = 2$.

Coset enumeration is one of the basic methods for investigating finitely generated subgroups in finitely presented.. Information are gradually added to a coset, a relation , a subgroup tables and once they are filled in, all cosets have been enumerated, the algorithm terminates.

Goldschmidt's Lemma on the number of isomorphism classes of amalgams having fixed type, verify that there is one isomorphism class of amalgam of type $\mathcal{A} = (S_n, S_n, S_{n-1}, \phi_1, \phi_2)$, where $\phi_i$ is an identity map from $S_{n-1}$ to $S_n$ for i=1, 2 and $n \neq 2, 3, 6, 7$. When $n = 2,7$ we have two isomorphic class of amalgam of type $\mathcal{A}$.

Finally,
If $\mathcal{A}$ and $\mathcal{A}'$ are cyclic amalgams of the same type then there universal completions are isospectral.

# Acknowledgment

I would like to express my deep and sincere gratitude to my supervisor, Professor C.W. Parker. His wide knowledge and his logical way of thinking have been of great value for me. His understanding, encouraging and personal guidance have provided a good basis for the present thesis.

I warmly thank to Dr. Simon Goodwin for his detailed and constructive comments, and important support throughout this work.

I am also grateful to my mother and my husband for the inspiration and endless patience during this period.

The financial support of the Asian Development Bank and the Open University of Sri Lanka are gratefully acknowledged.

# Contents

# Introduction

In this thesis we shall prove that universal completions of two cyclic amalgams of the same type are isospectral. We approach to this theory by proving the bijection between the homomorphisms of universal completions of amalgams $\mathcal{A}$ and $\mathcal{A}^\gamma$ with $\mathrm{Sym}(n)$.

Automorphisms of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ which is proved under the Automorphism Groups in Chapter 2. If $G$ is a finite abelian group, which is isomorphic to direct product of $m$ cyclic groups of order $q$ where $q = p^n$ for some prime $p$. Then $\mathrm{Aut}(G)$ is isomorphic to the set of $m \times m$ matrices with determinant coprime to $p$, denoted by $GL_m(\mathbb{Z}_q)$. Also $\mid \mathrm{Aut}\ (G) \mid = p^{(n-1)m^2} \mid GL_m(\mathbb{Z}_q) \mid$.

If $\alpha$ is an automorphism of $S_n$ and $t$ is a transposition of $S_n$ for $n \neq 6$, then we show that $\alpha(t)$ is a transposition. Also, if $\alpha$ maps transposition to transposition, then $\alpha$ is an inner automorphism. Using these two results it will be shown that $\mathrm{Aut}(S_n) \cong S_n$,unless $n \neq 6$ under the section 2.3.3. Furthermore, using the Sylow's Theorem, we will prove that there exists an outer automorphism of $S_6$ and $\mathrm{Out}(S_6) = \dfrac{\mathrm{Aut}(S_6)}{\mathrm{Inn}(S_6)} \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}}$. Thus, $\mid \mathrm{Out}(S_6) \mid = 2$.

The set $F$ of equivalence classes of words is called **free group** on the set of symbols $S$, denoted by $F[S]$. In the Chapter 3 we will prove that the theorem:

*Let $G$ be a group generated by $T = \{a_i | i \in I\}$ and let $H$ be any group. Then there is at most one homomorphism $\phi : G \longrightarrow H$ such that $\phi(a_i) = h_i$ for any element $h_i \in H$ and $i \in I$. If $G$ is free on $T$, then there is exactly one such homomorphism.*

Coset enumeration, discuss in Chapter 4, is one of the basic methods for investigating finitely presented groups. Todd and Coxeter's algorithm for enumerating cosets of finitely generated subgroups in finitely presented groups is one of the famous methods

from combinatorial group theory for studying the subgroup problem. In 1936, J.A. Todd and H.S.M. Coxeter published a paper in which they described a technique for enumerating the cosets of a finite group given only a presentation for the group and the generators of the subgroup written in terms of the generators of the group.

It consists three types of tables: a coset table, a relation table, a subgroup table of the group. Informations are gradually added to these tables, and once they are filled in and all cosets have been enumerated and the algorithm terminates.

In Chapter 5 we will move to the Amalgams. An **amalgam** consists of a five-tuple $(A_1, A_2, B, \phi_1, \phi_2)$ where $A_1, A_2$ and $B$ are groups and $\phi_i : B \longrightarrow A_i$ for $i = 1, 2$, are monomorphisms. Let $\mathcal{A}_1 = (A_1, A_2, B, \phi_1, \phi_2)$ and $\mathcal{A}_2 = (\hat{A}_1, \hat{A}_2, \hat{B}, \varphi_1, \varphi_2)$ be amalgams. Then $\mathcal{A}_1$ and $\mathcal{A}_2$ have the **same type** provided there exists ismorphisms $\alpha_i : A_i \longrightarrow \hat{A}_i$ and $\gamma : B \longrightarrow \hat{B}$ such that $\mathrm{Im}(\phi_i\alpha_i) = \mathrm{Im}(\gamma\varphi_i)$ for $i = 1, 2$. Two amalgams of the same type are **isomorphic**, if $\phi_i\alpha_i = \gamma\varphi_i$ for $i = 1, 2$. A **completion** of $\mathcal{A}$ in a group $G$ is the triple $(\langle\psi_1(A_1), \psi_2(A_2)\rangle, \psi_1, \psi_2)$, where $\psi_i : A_i \longrightarrow G$ for $i = 1, 2$ such that $\phi_1\psi_1 = \phi_2\psi_2$. A completion of $\mathcal{A}$ is **faithful** if $\psi_1$ and $\psi_2$ are monomorphisms.

Goldschmidt's Lemma on the number of isomorphism classes of amalgams having fixed type is included in section 5.2. In order to give an example of how it works we verify that there is one isomorphic class of amalgam of type $\mathcal{A} = (S_n, S_n, S_{n-1}, \phi_1, \phi_2)$, where $\phi_i$ is an identity map from $S_{n-1}$ to $S_n$ for $i = 1, 2$ and $n \neq 2, 3, 6, 7$. When $n = 2$ and $n = 7$ we have two isomorphic class of amalgam of type $\mathcal{A}$.

Let $G$ be a group. Then the number of subgroups of $G$ of index $n$ is denoted by $a_n(G)$. Let $H$ be a group, then $G$ and $H$ are called **isospectral** if, and only if, $a_n(G) = a_n(H)$ for all natural numbers $n$. If $B$ is a cyclic group then $\mathcal{A}$ is a **cyclic amalgam**.

The main result of the thesis as follows:

*If $\mathcal{A}$ and $\mathcal{A}'$ are cyclic amalgams of the same type then their universal completions are isospectral.*

First we prove that for cyclic amalgam $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ there is a bijection between $\mathrm{Hom}(\mathcal{A}, \mathrm{Sym}(n))$ and $\mathrm{Hom}(\mathcal{A}^\gamma, \mathrm{Sym}(n))$ for all natural numbers $n$ and for all $\gamma \in \mathrm{Aut}(C)$. Furthermore, there is a bijection between $\mathrm{Hom}(G(\mathcal{A}), \mathrm{Sym}(n))$ and $\mathrm{Hom}(G(\mathcal{A}^\gamma), \mathrm{Sym}(n))$ for a group $G$.

# Chapter 1

# Preliminaries

## 1.1 Normalizer and Centralizer

**Definition 1.1.1.** The *centralizer* of an element $g$ of a group $G$ is the set of elements of $G$ which commute with $g$, that is $C_G(g) = \{x \in G \mid xg = gx\}$. Let $H$ be a subgroup of $G$. Then the centralizer of $H$ in $G$ is

$$C_G(H) = \{x \in G \mid xh = hx \text{ for all } h \in H\} = \cap_{h \in H} C_G(h).$$

**Definition 1.1.2.** The *normalizer* of a subgroup $H$ in a group $G$ is $N_G(H) = \{x \in G \mid xH = Hx\}$.

**Theorem 1.1.1.** *Let $H$ be a subgroup of a group $G$. Then $C_G(H)$ is a normal subgroup of $N_G(H)$.*

*Proof.* Since every element of $C_G(H)$ satisfies $Hg = gH$, $C_G(H)$ is a subgroup of $N_G(H)$. Let $n \in N_G(H)$ and $c \in C_G(H)$. Then we need to show that $n^{-1}cn \in C_G(H)$.

i.e. $(n^{-1}cn)^{-1}h(n^{-1}cn) = h$ for $h \in H$. So consider,

$$(n^{-1}cn)^{-1}h(n^{-1}cn) = (n^{-1}c^{-1}n)h(n^{-1}cn)$$

$$= n^{-1}c^{-1}(nh)n^{-1}cn.$$

Since $n \in N_G(H)$ and $h \in H$, $nhn^{-1} = h_1$ for some $h_1 \in H$. Then we have,

$$\begin{aligned}(n^{-1}c^{-1}n)h(n^{-1}cn) &= n^{-1}c^{-1}h_1cn = n^{-1}h_1n \\ &= n^{-1}nhn^{-1}n = h.\end{aligned}$$

Thus, $C_G(H)$ is a normal subgroup of $N_G(H)$. □

**Definition 1.1.3.** Let $G$ and $H$ be groups. Then a *homomorphism* of a group $G$ to $H$ is a mapping $\phi$ of $G$ to $H$ such that for all $x$ and $y$ in $G$, $\phi(xy) = \phi(x)\phi(y)$.

**Definition 1.1.4.** An *automorphism* of a group $G$ is a bijective homomorphism from $G$ to itself. The set of automorphisms is denoted by $\mathrm{Aut}(G) = \{\phi : G \longrightarrow G \mid \phi \text{ is an automorphism}\}$. $\mathrm{Aut}(G)$ forms a group under composition of functions.

**Example 1.1.1.** Consider the group $C_2 \times C_2 = \{(1,1),(1,x),(x,1),(x,x)\}$. $C_2 \times C_2$ is generated by $(1,x)$ and $(x,1)$. Since $(1,1)$ is the identity and so any automorphism is generated by the images of these generators. This gives six automorphisms:

$\varphi_1 : (x,1) \longmapsto (x,1)$
$\quad (1,x) \longmapsto (1,x)$

$\varphi_2 : (x,1) \longmapsto (x,1)$
$\quad (1,x) \longmapsto (x,x)$

$\varphi_3 : (x,1) \longmapsto (1,x)$
$\quad (1,x) \longmapsto (x,1)$

$\varphi_4 : (x,1) \longmapsto (1,x)$
$\quad (1,x) \longmapsto (x,x)$

$\varphi_5 : (x,1) \longmapsto (x,x)$
$\quad (1,x) \longmapsto (x,1)$

$\varphi_6 : (x,1) \longmapsto (x,x)$
$\quad (1,x) \longmapsto (1,x)$

It is clear that these six automorphisms are acting faithfully on the set $\{(1,x),(x,1),(x,x)\}$ and it follows that $\mathrm{Aut}(C_2 \times C_2) \cong \mathrm{Sym}(3)$.

**Lemma 1.1.1.** *For any fixed $g \in G$ define $\theta_g : G \longrightarrow G$ by $\theta_g(x) = x^g = g^{-1}xg$ for $x \in G$. Then $\theta_g \in Aut(G)$.*

*Proof.* For given $y \in G$, let $x = gyg^{-1}$. Then $\theta_g(x) = g^{-1}xg = g^{-1}(gyg^{-1})g = y$. So $\theta_g$ is onto. If $\theta_g(x) = \theta_g(y)$, then $g^{-1}xg = g^{-1}yg$, so by the cancellation laws in $G$, $x = y$. Hence $\theta_g$ is one-to-one. Now consider, for $xy \in G$,

$$\theta_g(xy) = g^{-1}(xy)g = g^{-1}(xgg^{-1}y)g = (g^{-1}xg)(g^{-1}yg) = \theta_g(x)\theta_g(y).$$

Hence, $\theta_g$ is a homomorphism. So $\theta_g$ is an automorphism of $G$. □

**Definition 1.1.5.** The set $\{\theta_g | g \in G\}$ is called the *inner automorphism group* of $G$ and is denoted by $\mathrm{Inn}(G)$.

**Lemma 1.1.2.** *$Inn(G)$ is a normal subgroup of $Aut(G)$.*

*Proof.* $\mathrm{Inn}(G)$ is non-empty since $\theta_1 \in \mathrm{Inn}(G)$. Take $\theta_a, \theta_b \in \mathrm{Inn}(G)$. Then

$$\theta_a(\theta_b(g)) = \theta_a(g^b) = (g^b)^a = g^{ba} = \theta_{ba}(g).$$

So $\theta_a\theta_b = \theta_{ba}$. Therefore $\theta_b\theta_{b^{-1}} = \theta_1$ and this implies that $(\theta_b)^{-1} = \theta_{b^{-1}}$. Hence

$$\theta_a(\theta_b)^{-1} = \theta_a\theta_{b^{-1}} = \theta_{b^{-1}a} \in \mathrm{Inn}(G)$$

as $b^{-1}a \in G$. Therefore $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Take any $\theta_a \in \mathrm{Inn}(G)$ and $\beta \in \mathrm{Aut}(G)$. Then for any $g \in G$,

$$\begin{aligned}(\theta_a)^\beta(g) &= \beta^{-1}(\theta_a)\beta(g) \\ &= \beta^{-1}[\beta(g)]^a \\ &= \beta^{-1}[a^{-1}\beta(g)a]\end{aligned}$$

$$
\begin{aligned}
&= \beta^{-1}(a^{-1})\beta^{-1}\beta(g)\beta^{-1}(a) \\
&= \beta^{(a^{-1})}g\beta^{-1}(a) \\
&= [\beta^{-1}(a)]^{-1}g\beta^{-1}(x) \\
&= g^{\beta^{-1}(a)} = \theta_{\beta^{-1}(a)}(g) \in \mathrm{Inn}(G)
\end{aligned}
$$

Hence $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. □

**Theorem 1.1.2.** *Let $H$ be a subgroup of a group of $G$. Then $\dfrac{N_G(H)}{C_G(H)}$ is isomorphic to a subgroup of $Aut(H)$.*

*Proof.* Let $\alpha_x \in \mathrm{Inn}(G)$ such that $\alpha_x : G \longrightarrow G$ by $g \longmapsto g^x$ for $x \in N_G(H)$.

*Claim:* $(\alpha_x \mid_H) \in \mathrm{Aut}(H)$.

*Proof.* Suppose that $\alpha_x(h_1) = \alpha_x(h_2)$ for $h_1, h_2 \in H$. This implies that ${h_1}^x = {h_2}^x$ and hence $h_1 = h_2$. Thus, $(\alpha_x \mid_H)$ is injective. For any $h \in H$, $h^{x^{-1}} \in H$ as $x^{-1} \in N_G(H)$ and $(\alpha_x \mid_H)h^{x^{-1}} = (h^{x^{-1}})^x = h$. This implies that $(\alpha_x \mid_H)$ is surjective. Hence $(\alpha_x \mid_H) \in \mathrm{Aut}(H)$.

Next define a map, $\theta : N_G(H) \longrightarrow \mathrm{Aut}(H)$ by $x \longmapsto (\alpha_{x^{-1}} \mid_H)$.

*Claim: $\theta$ is a homomorphism and* $\mathrm{Ker}\ \theta = C_G(H)$.

*Proof.* So consider

$$
\begin{aligned}
\theta(xy) &= (\alpha_{(xy)^{-1}} \mid_H) = (\alpha_{y^{-1}x^{-1}} \mid_H) \\
&= (\alpha_{x^{-1}}\alpha_{y^{-1}} \mid_H) = (\alpha_{x^{-1}} \mid_H)(\alpha_{y^{-1}} \mid_H) \\
&= \theta(x)\theta(y).
\end{aligned}
$$

Next

$$
\mathrm{Ker}\ \theta = \{g \in N_G(H) \mid \theta(g) = 1\} = \{g \in N_G(H) \mid (\alpha_{g^{-1}} \mid_H) = 1\}
$$

$$
\begin{aligned}
&= \{g \in N_G(H) \mid h^{g^{-1}} = h, \text{ for all } h \in H\} \\
&= \{g \in N_G(H) \mid h^g = h, \text{ for all } h \in H\} \\
&= \{g \in N_G(H) \mid g \in C_G(H)\} = C_G(H).
\end{aligned}
$$

Therefore by the first isomorphism theorem,

$$\frac{N_G(H)}{C_G(H)} \cong \text{ Im } \theta \leq \text{ Aut } (H).$$

□

**Theorem 1.1.3.** *Let $G$ be a group. Then* $\dfrac{G}{Z(G)} \cong Inn(G)$.

*Proof.* Define a map $\varphi : G \longrightarrow$ Inn $(G)$ by $\varphi(g) = \sigma_g$ where $\sigma_g$ is an inner automorphism of $G$. Let $g, h \in G$. For all $x \in G$ we have

$$
\begin{aligned}
\sigma_{gh}(x) &= (gh)^{-1}\sigma x(gh) \\
&= h^{-1}(g^{-1}xg)h \\
&= h^{-1}(\sigma_g(x))h \\
&= \sigma_h\sigma_g(x).
\end{aligned}
$$

Hence $\varphi(gh) = \sigma_{gh} = \sigma_g\sigma_h = \varphi(g)\varphi(h)$. So $\varphi$ is a homomorphism. If $\varphi \in$ Inn $(G)$, then by the definition of $\varphi, \sigma_g = \varphi(g)$ for some $g \in G$, hence $\varphi$ is surjective and Im $\varphi =$ Inn $(G)$. An element $g \in G$ is in Ker $\varphi$ if, and only if, $\varphi(g) = \sigma_g$ is the identity map on $G$, hence if, and only if, $x = \sigma_g(x) = g^{-1}xg$ for all $x \in G$. This holds if, and only if, $g \in Z(G)$. Hence, Ker $\varphi = Z(G)$ and, by the First Isomorphism Theorem, $\dfrac{G}{Z(G)} = \dfrac{G}{\text{Ker } \varphi} \cong$ Im $\varphi =$ Inn $(G)$. □

## 1.2 Some Symmetric Groups Results

**Definition 1.2.1.** *A permutation* of a finite set $X$ is a bijection $\sigma : X \longrightarrow X$.

**Definition 1.2.2.** The *symmetric group* on a set $X$ is a group of permutations on $X$, denoted by $\mathrm{Sym}(X)$ or $S_X$.

In particular, the symmetric group on the finite set $X = \{1, \ldots, n\}$ is written $S_n$.

**Definition 1.2.3.** An *even permutation* is a permutation that can be produced by an even number of exchanges (called transpositions).

**Definition 1.2.4.** The *alternating group* on a set $X$ is the group of even permutations on the set $X$, denoted by $\mathrm{Alt}(X)$ or $A_X$.

The set of even permutations of $S_n$ is the alternating group on $n$ symbols, denoted by $\mathrm{Alt}(n)$ or $A_n$.

**Theorem 1.2.1.** *If $\sigma$ is a permutation in $S_n$, then $\sigma$ can be expressed as a product of cycles.*

*Proof.* We proceed by induction. If $\sigma \in S_1$, then $\sigma = (1)$, the identity permutation, and hence, $\sigma$ is a cycle. Now assume that every permutation in $S_m$ can be expressed as a product of cycles. Let $\sigma$ be an element of $S_{m+1}$. If $(m+1)\sigma = m+1$, then $\sigma \in S_m$ and therefore $\sigma$ can be expressed as a product of cycles. If $(m+1)\sigma \neq m+1$, let $\rho = (m+1)\sigma^{-1}$, and let $\tau = (m+1\ \rho)\sigma$. Then

$$\begin{aligned} (m+1)\tau &= (m+1)[(m+1\ \rho)\sigma] = [(m+1)(m+1\ \rho)]\sigma \\ &= \rho\sigma = m+1. \end{aligned}$$

Therefore $\tau \in S_m$ and hence $\tau$ can be expressed as a product of cycles, say, $C_1, C_2, \ldots, C_l$. Since $\tau = C_1C_2 \ldots C_l$ and $\tau = (m+1\ \rho)\sigma$,

$$\begin{aligned} C_1C_2 \ldots C_l &= (m+1\ \rho)\sigma \\ (m+1\ \rho)C_1C_2 \ldots C_l &= (m+1\ \rho)(m+1\ \rho)\sigma = I\sigma = \sigma \end{aligned}$$

and therefore

$$(m+1\ \rho)C_1C_2 \ldots C_l = \sigma.$$

Thus, every element of $S_{m+1}$ can be expressed as a product of cycles. Then by the Mathematical induction the theorem follows. □

**Theorem 1.2.2.** *If $\sigma$ is a cycle in $S_n$ for $n \geq 2$, then $\sigma$ can be expressed as a product of transpositions of the form $(1\ m)$, where $m$ is a positive integer.*

*Proof.* If $\sigma = (1)$, then $\sigma = (1\ 2)(1\ 2)$. If $\sigma = (a\ b)$ then $\sigma = (1\ a)(1\ b)(1\ a)$. Thus, cycle $m$ of length 1 and 2 can be expressed. Assume the assertion is true for cycle $m$ of length $n$ and let $\sigma = (a_1\ a_2\ \ldots\ a_n\ a_{n+1})$. But $(a_1\ a_2\ \ldots\ a_n)(a_1\ a_{n+1})$. Since $(a_1\ a_2\ \ldots\ a_n)$ is of length $n$ and $(a_1\ a_{n+1})$ is of length 2, both can be expressed as a product of transpositions of the form $(1\ m)$ and hence, product can be so expressed. □

**Theorem 1.2.3.** *Every element of $S_n$ can be expressed as a product of transpositions of the form $(1\ m)$, where $m$ is a positive integer.*

*Proof.* The result follows from Theorems 1.2.1 and 1.2.2. □

**Theorem 1.2.4.** *Two permutations of $S_n$ are conjugate if, and only if, they have the same cycle type.*

*Proof.* If $\sigma$ and $\tau$ are conjugate permutations in $S_n$, then there exists a permutation $\rho$ such that $\sigma = \rho\tau\rho^{-1}$. Suppose $C = (x_1 \ \dots \ x_l)$ is a cycle of $\sigma$ of length $l$. Then

$$\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_l) = x_1.$$

Let $\rho(x_i) = y_i$ for each $i$. Then

$$\tau(y_i) = (\rho^{-1}\sigma\rho)(y_i) = (\sigma\rho)(x_i) = \rho(x_{i+1}) = y_{i+1}$$

in which the subscripts are to be evaluated modulo $l$. Thus every cycle of $\sigma$ of length $l$ corresponds to a cycle of $\tau$ of length $l$. So $\sigma$ and $\tau$ are of the same cycle type.

On the other hand, assume that $\sigma$ and $\tau$ are of the same cycle type, and let $C = (x_1 \ \dots \ x_l)$ be a cycle of $\sigma$. Then $\tau$ has a cycle of the form $C' = (y_1 \ \dots \ y_l)$. Define $\rho(x_i) = y_i$, over $C$ and similarly, over every other cycle of $\sigma$. This is possible because, $\rho$ is a bijection from $S_n$ to $S_n$, or a permutation of $S_n$. So we have,

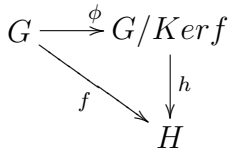
$$\rho\sigma(x_i) = \rho(x_{i+1}) = y_{i+1} = \tau(y_i) = \tau\rho(x_i).$$

So $\sigma$ and $\tau$ are conjugate. □

## 1.3 Commutative Diagram and Double Cosets

**Definition 1.3.1.** *A commutative diagram* is a diagram of objects and morphisms such that, when picking two objects, one can follow any directed path through the diagram and obtain the same result by composition.

**Example 1.3.1.** The first isomorphism theorem is a commutative triangle as follows:



The diagram commutes if and only if $f = h \circ \phi$.

**Definition 1.3.2.** Let $H$ and $K$ be subgroups of a group $G$. Then the set $HgK = \{hgk | h \in H, k \in K\}$ for some $g \in G$ is a $(H, K)$-*double coset*. Every $(H, K)$-double coset is a union of right cosets of $H$ and also a union of left cosets of $K$. The set of all $(H, K)$-double cosets of $G$ is denoted by $H \setminus G/K$.

**Example 1.3.2.** Consider the symmetric group $S_3$ with the subgroups $H = \langle(12)\rangle$ and $K = \langle(13)\rangle$ then the two $(H, K)$-double cosets are $\{1, (12), (13), (132)\}$ and $\{(23), (123)\}$.

**Theorem 1.3.1.** Let $G$ be finite group and $H$ and $K$ are subgroups of $G$. Then the number of double cosets of $G$ is

$$\mid H \setminus G/K \mid = \frac{\mid G \mid}{\mid H \mid\mid K \mid} \sum_{j=1}^{m} \frac{\mid C_j \cap H \mid\mid C_j \cap K \mid}{\mid C_j \mid}.$$

where $C_j$, $1 \leq j \leq m$ are the conjugacy classes of $G$.

*Proof.* Let $C_1, \ldots, C_m$ be the conjugacy classes of finite group $G$, and $H$ and $K$ be subgroups of $G$. Let $H \setminus G$ be the left coset of $H$. Then $K$ acts on $H \setminus G$ by right multiplication. So, $(Hg)k = Hgk$ for $g \in G$ and $k \in K$. The orbits of $K$ on $H \setminus G$ are the double cosets $HgK$ for $g \in G$. So

$$\begin{aligned} \mid H \setminus G/K \mid &= \text{number of orbits of } K \text{ on } H \setminus G \\ &= \frac{1}{\mid K \mid} \sum_{k \in K} \text{fix}_{\,H\setminus G}(k) \end{aligned}$$

where $\text{fix}_{\,H\setminus G}(k) = \mid \{Hg \mid Hgk = Hg\} \mid$.

Then $Hgk = Hg$ if, and only if, $gkg^{-1} \in H$. Also,

$$\mid \{g \in G \mid gkg^{-1} \in H\} \mid = \mid k^G \cap H \mid\mid C_G(k) \mid$$

where $k^G = \{x^{-1}kx \mid x \in G\}$ and

$$\mid \{Hg \in H \setminus G \mid gkg^{-1} \in H\} \mid \;=\; \frac{\mid k^G \cap H \mid\mid C_G(k) \mid}{\mid H \mid}.$$

thus, $\mid \text{fix}_{H\setminus G}(k) \mid = \dfrac{\mid k^G \cap H \mid\mid C_G(k) \mid}{\mid H \mid}$. If $k$ conjugates to $k'$, $k' = g^{-1}kg$ for some $g \in G$, then $\text{fix}_{H\setminus G}(k) = \text{fix}_{H\setminus G}(k')$. Hence,

$$\begin{aligned}
\frac{1}{\mid K \mid}\sum_{k\in K}\text{fix}_{H\setminus G}(k) &= \frac{1}{\mid K \mid}\sum_{j=1}^{m}\sum_{k\in C_j\cap K}\text{fix}_{H\setminus G}(k) \\
&= \frac{1}{\mid K \mid}\sum_{j=1}^{m}\mid C_j \cap K \mid \text{fix}_{H\setminus G}(k_j) \text{ where } k_j \in C_j \\
&= \frac{1}{\mid K \mid}\sum_{j=1}^{m}\frac{\mid C_j \cap K \mid\mid C_j \cap H \mid\mid C_G(k_j) \mid}{\mid H \mid} \\
&= \frac{\mid G \mid}{\mid H \mid\mid K \mid}\sum_{j=1}^{m}\frac{\mid C_j \cap K \mid\mid C_j \cap H \mid}{\mid C_j \mid} \text{ as } \mid C_G(k_j) \mid = \frac{\mid G \mid}{\mid C_j \mid}.
\end{aligned}$$

□

**Example 1.3.3.** Consider the group $S_3$ with the subgroups $H = \langle(1\ 2)\rangle$ and $K = \langle(1\ 3)\rangle$. Then the conjugacy classes of $S_3$ are $C_1 = 1, C_2 = \{(1\ 2), (2\ 3), (1\ 3)\}$ and $C_3 = \{(1\ 2\ 3), (1\ 3\ 2)\}$. Thus, the number of $(H, K)$ double cosets of $S_3$ is

$$\begin{aligned}
\mid H \setminus S_3/K \mid &= \frac{\mid S_3 \mid}{\mid H \mid\mid K \mid}\sum_{j=1}^{3}\frac{\mid C_j \cap H \mid\mid C_j \cap K \mid}{\mid C_j \mid} \\
&= \frac{6}{4}\Big\{1 + \frac{1}{3}\Big\} = 2.
\end{aligned}$$

# Chapter 2

# Automorphism Groups

## 2.1 Automorphism of $\mathbb{Z}/n\mathbb{Z}$

The factor ring $\mathbb{Z}/n\mathbb{Z}$ is called the ring of integers modulo $n$. We also denote $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}(n)$. For an integer $n > 1$, the units in the ring $\mathbb{Z}/n\mathbb{Z}$ consist of those residue classes mod $n\mathbb{Z}$ which are represented by integers $m \neq 0$ and coprime to $n$.

The multiplicative group of invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$ is denoted by $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

**Theorem 2.1.1.** *Let $G$ be a cyclic group of order $n$. For each $k \in \mathbb{Z}$ let $\phi_k : G \longrightarrow G$ be the endomorphism $x \longmapsto kx$ (writing $G$ additively). Then $k \longmapsto \phi_k$ induces a ring isomorphism $\mathbb{Z}/n\mathbb{Z} \cong End(G)$ and a group isomorphism $(\mathbb{Z}/n\mathbb{Z})^{\times} \cong Aut(G)$.*

*Proof.* The additive group structure on End($G$) is simply addition of mappings and the multiplication is composition of mappings. The fact that the $k \longmapsto \phi_k$ is a ring homomorphism is then a restatement of the formulas

$$1a = a$$

$$(k + k')a = ka + k'a \text{ and}$$

$$kk^{'}a \;\; = \;\; k(k^{'}a)$$

for $k, k^{'} \in \mathbb{Z}$ and $a \in G$. If $a$ is a generator of $G$, then $ka = 0$ if and only if, $k \equiv 0(\text{mod } n)$, so $\mathbb{Z}/n\mathbb{Z}$ is embedded in End$(G)$. On the other hand, let $\phi : G \longrightarrow G$ be an endomorphism. Again for a generator $a$ we have $\phi(a) = ka$ for some $k$, whence, $\phi = \phi_k$ since every $x \in G$ is of the form $ma$ for some $m \in \mathbb{Z}$, and

$$\phi(x) = \phi(ma) = m\phi(a) = mka = kma = kx.$$

This proves the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \text{End}(G)$.

Furthermore, if $k \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ then there exists $k^{'}$ such that $kk^{'} \equiv 1(\text{mod } n)$ so $\phi_k$ is an automorphism. Conversely, given any automorphism $\phi$ with inverse $\varphi$, we know from the first part of the proof that $\phi = \phi_k$ and $\varphi = \varphi_k$ for some $k, k^{'}$ and $\phi \circ \varphi = id$ means that $kk^{'} \equiv 1(\text{mod } n)$, so $kk^{'} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. This proves the isomorphism $(\mathbb{Z}/n\mathbb{Z})^{\times} \cong \text{Aut}(G)$, [15]. $\square$

## 2.2 Automorphisms of Abelian Groups

Let $G$ be a finite additive abelian group, which is isomorphic to a direct product of $m$ cyclic groups of order $q$ where $q = p^n$ for some prime $p$. Consider the ring endomorphism of $G$, End$(G)$. This is the of group homomorphisms from $G$ to itself with ring multiplication given by composition of maps and addition given naturally by $(\phi + \varphi)(g) = \phi(g) + \varphi(g)$ for endomorphisms $\phi$ and $\varphi$ and all $g \in G$, [12].

Consider $G$ as a direct sum of $m$ copies of the integers modulo $q$. Let $g \in G$. Then $g$ has the form $g = (\bar{g_1}, \bar{g_2}, \ldots, \bar{g_m})$ where $\bar{g_i}$ is an equivalence class of integers modulo $q$ and $g_i \in \mathbb{Z}$ is an integral representative. Let $\theta : \mathbb{Z}^m \longrightarrow G$ be a natural homomorphism defined

by $\theta(g_1, g_2, \ldots, g_m) \longmapsto (\bar{g_1}, \bar{g_2}, \ldots, \bar{g_m})$, where $\mathbb{Z}^m = \{(g_1, \ldots, g_m) \mid g_i \in \mathbb{Z} \text{ for all } i = 1, \ldots, m\}$.

**Lemma 2.2.1.** *Let $M_m(\mathbb{Z}) = \{(a_{ij})_{m\times m} \mid a_{ij} \in \mathbb{Z}\}$. Consider the map,*

$$\chi_q : M_m(\mathbb{Z}) \longrightarrow End(G) \text{ defined by}$$

$$A \longmapsto \chi_q(A),$$

*where $\chi_q(A) : (\bar{g_1}, \bar{g_2}, \ldots, \bar{g_m}) \longmapsto \theta((g_1, g_2, \ldots, g_m)A)$ and $\chi_q$ is a surjective ring homomorphism.*

*Proof.* We need to show that the map $\chi_q(A)$ is a well-defined endomorphism of group $G$. Suppose that $(g_1, \ldots, g_m)$ and $(h_1, \ldots, h_m)$ satisfy the condition $\theta(g_1, \ldots, g_m) = \theta(h_1, \ldots, h_m)$ for $g_i$ and $h_i$ from $G$ for all $i = 1, 2, \ldots, m$. Then $q \mid (g_i - h_i)$ for each $1 \leq i \leq m$. Therefore,

$$\begin{aligned}
\chi_q(A)(\bar{g_1}, \ldots, \bar{g_m}) - \chi_q(A)(\bar{h_1}, \ldots, \bar{h_m}) &= \theta((g_1, \ldots, g_m)A) - \theta((h_1, \ldots, h_m)A) \\
&= \theta\left(\sum_{i=1}^{m} g_i a_{i1}, \ldots, \sum_{i=1}^{m} g_i a_{im}\right) - \\
&\quad \theta\left(\sum_{i=1}^{m} h_i a_{i1}, \ldots, \sum_{i=1}^{m} h_i a_{im}\right) \\
&= \theta\left(\sum_{i=1}^{m} (g_i - h_i) a_{i1}, \ldots, \sum_{i=1}^{m} (g_i - h_i) a_{im}\right) \\
&= \left(\sum_{i=1}^{m} \theta\left((g_i - h_i) a_{i1}\right), \ldots, \sum_{i=1}^{m} \theta\left((g_i - h_i) a_{im}\right)\right) \\
&= 0_G, \text{ since } q \mid (g_i - h_i).
\end{aligned}$$

So that $\chi_q(A)$ is well-defined and, as $\theta$ is linear and matrix multiplication is distributive, $\chi_q(A)$ is a group homomorphism. Therefore, $\chi_q$ is a map into End$(G)$.

Next we need to show that $\chi_q$ is surjective. Let $\bar{x_i} := (0, \ldots, \bar{1}, \ldots, 0)$ be the element

whose non zero entry is a $\bar{1}$ in the $i^{\text{th}}$ component and zero everywhere else. Suppose that $\theta(x_i) = (\bar{g_1}, \ldots, \bar{g_m})$. Then consider the matrix $A = (a_{ij})$ where $a_{ij} = g_j$ for each $j \leq m$. Then we have $\chi_q(A) = \theta$ by doing this for each $i \leq m$. Thus, $\chi_q$ is surjective.

Also from the definition,

$$\begin{aligned} \chi_q(I) &= 1_{\text{End}(G)} \text{ and} \\ \chi_q(A+B) &= \chi_q(A) + \chi_q(B) \text{ for } A, B \in M_m(\mathbb{Z}). \end{aligned}$$

Furthermore, from the properties of matrix multiplication, $\chi_q(A)\chi_q(B) = \chi_q(AB)$. Thus $\chi_q$ is a surjective ring homomorphism. □

**Lemma 2.2.2.** *The kernel of $\chi_q$ is the set of matrices $A = (a_{ij}) \in M_m(\mathbb{Z})$ such that $q \mid a_{ij}$ for all $i, j$.*

*Proof.* Let $Y = \{(a_{ij})_{m\times m} \mid (a_{ij}) \in M_m(\mathbb{Z}) \text{ and } q \mid a_{ij} \text{ for all } i, j\}$. Take any element $y$ from $Y$ and let $x_i := (0, \ldots, \bar{1}, \ldots, 0)$ be defined as above. Then, $\chi_q(y)(x_i) = 0_G$. Since $G$ is generated by $x_i$'s, $Y \subseteq \text{Ker}\chi_q$. Since each $g \in G$ is a linear combination of the $x_i$, $\chi_q(A)(g) = 0$ for all $g \in G$. Therefore, $A \in \text{Ker}\chi_q$.

Conversely, suppose that $A = (a_{ij}) \in \text{Ker}\chi_q$. Thus, $\chi_q(A)(x_i) = 0_G$ for each $x_i$. Then each $a_{ij}$ is divisible by $q$. Therefore, $Y = \text{Ker}\chi_q$. □

**Definition 2.2.1.** Let $A = (a_{ij})$ be a matrix of order $n$. For each pair $(i, j)$ of indices, let $A'_{ij}$ be the matrix of order $(n-1)$ obtained by deleting the $i^{th}$ row and the $j^{th}$ column in the matrix $A$. The scalar

$$d_{ij} := (-1)^{i+j} \det(A'_{ij})$$

is called the $(i, j)$-*cofactor* of the matrix $A$, and the matrix Cof $(A) := d_{ij}$ is called the *cofactor matrix* of the matrix $A$.

We know that $\det(A) = \sum_{j=1}^{n} a_{ij}d_{ij}, 1 \leq i \leq n$ and $\det(A) = \sum_{i=1}^{n} a_{ij}d_{ij}, 1 \leq j \leq n$, are equivalent to $A(\mathrm{Cof}(A))^T = (\mathrm{Cof}(A))^T A = \det(A))I$. If the matrix is invertible $\mathrm{Cof}(A) = (det(A))A^{-T}$ with $A^{-T} = (A^{-1})^T$ and in this case $\mathrm{Cof}(A)^T$ is the only matrix $B$ that satisfies $AB = BA = (\det(A))I$.

**Lemma 2.2.3.** *$\chi_q(A) \in End(G)$ is an automorphism of $G$ if, and only if, $det(A)$ is prime to $p$.*

*Proof.* Suppose that $A$ is a $m \times m$ matrix which has determinant prime to $p$. Let $B$ be the cofactor matrix of $A$, which is the matrix satisfies $AB^T = \det(A)I$. Since, $\det(A)$ is prime to $p$, there exists $r \in \mathbb{Z}$ such that $r\det(A) \equiv 1(\mathrm{mod}\ q)$. Set $\chi_q(A^{-1}) := \chi_q(rB)$. Then we have

$$\begin{aligned} \chi_q(A).\chi_q(rB^T) &= \chi_q(rAB^T) \\ &= \chi_q(r\ \det(A)I) \\ &= 1_{\mathrm{End}(G)}. \end{aligned}$$

Therefore $\chi_A$ is an invertible endomorphism of $G$.

Conversely, suppose that $\chi_q(A)$ is an invertible endomorphism of $G$ for $A \in M_m(\mathbb{Z})$. Let $\chi_q(A^{-1}) = \chi_q(C)$ for some $C \in M_m(\mathbb{Z})$. Then

$$\begin{aligned} \chi_q(AC - I) &= \chi_q(AC) - \chi_q(I) \\ &= \chi_q(A)\chi_q(C) - 1_{\mathrm{End}(G)} \\ &= 0_{\mathrm{End}(G)}. \end{aligned}$$

Hence $AC - I \in \mathrm{Ker}(\chi)$. So every entries of $AC - I$ is divisible by $q$. Thus, the entries of $AC$ are equal to the entries of $I$ modulo $p$ by Lemma 2.2.2. Therefore,

$$1 \equiv \det(AC) \equiv \det(A)\det(C)(\mathrm{mod}\ p)$$

Hence $\det(A)$ is prime to $p$. $\square$

**Lemma 2.2.4.** *Let $GL_m(\mathbb{Z}_q)$ be the set of matrices with determinant prime to $p$. Then $GL_m(\mathbb{Z}_q) \cong Aut(G)$ has order $p^{(n-1)m^2} \mid GL_m(\mathbb{Z}_p) \mid$ .*

*Proof.* First we will show that the set $GL_m(\mathbb{Z}_q)$ is a group under matrix multiplication. The determinant is multiplicative; if $A$ and $B$ are matrices such that $\det(A) = a$ and $\det(B) = b$ with $a, b$ are prime to $p$, then $\det(AB)$ =$\det(A)\det(B) = ab$ which is prime to $p$. Hence closure property satisfies under multiplication. Assosiativity holds due to matrix multiplication. The identity element exists since the determinant of identity matrix is 1 and hence prime to $p$. Also $A \times id = id \times A = A$. Furthermore, each element has an inverse, since determinant is not zero.

Define a map

$$\Psi : GL_m(\mathbb{Z}_q) \longrightarrow \mathrm{Aut}(G)$$

by $\Psi((\bar{a_{ij}})) = \chi_q((a_{ij}))$ for each $(\bar{a_{ij}}) \in GL_m(\mathbb{Z}_q)$. Then we have $\Psi = \chi \mid_{GL_m(\mathbb{Z}_q)}$. As $\chi_q$ is a homomorphism, $\Psi$ is a well-defined homomorphism and the matrix $(a_{ij})$ is not in $\mathrm{Ker}(\chi_q)$. If $(\bar{a_{ij}}), (\bar{b_{ij}}) \in GL_m(\mathbb{Z}_q)$ with $\chi_q((a_{ij})) = \chi_q((b_{ij}))$, then $a_{ij} - b_{ij} \in \mathrm{Ker}(\chi_q)$ and hence $q \mid a_{ij} - b_{ij}$ for all $i, j$. Hence $(\bar{a_{ij}}) = (\bar{b_{ij}})$. Therefore, $\Psi$ is injective. Next, for any automorphism of $G$, there exists $(m_{ij}) \in M_n(\mathbb{Z})$ such that $(m_{ij})$ has determinant prime to $p$. Hence, $(\bar{m_{ij}}) \in GL_m(\mathbb{Z}_q)$ and so $\Psi$ is surjective.

Next consider the map

$$\Gamma : GL_m(\mathbb{Z}_q) \longrightarrow GL_m(\mathbb{Z}_p)$$

such that for each $A \in GL_m(\mathbb{Z}_q)$ we restrict the matrix entries modulo $p$. Then the determinant of $\Gamma(A)$ is non-zero modulo $p$, so $\Gamma(A)$ is an element of $GL_m(\mathbb{Z}_p)$. It is clear

that $\Gamma$ is a surjective homomorphism. Also,

$$\text{Ker}(\Gamma) = \{(a_{ij}) \mid a_{ii} \equiv 1(\text{mod } p) \text{ for all } i \text{ and } a_{ij} \equiv 0(\text{mod } p) \text{ for all } i \neq j\}.$$

Therefore there are $p^{n-1}$ choices for each entry since each $A$ is invertible as the determinant of $A$ is not equal zero.. Hence, $\mid \text{Ker}(\Gamma) \mid = p^{(n-1)m^2}$. Hence, $GL_m(\mathbb{Z}_q) \cong \text{Aut}(G)$ and has order $p^{(n-1)m^2} \mid GL_m(\mathbb{Z}_q) \mid$ . □

## 2.3 Automorphisms of $S_n$

In this section we will prove that if $n \neq 6$, then $\text{Aut}(S_n) \cong S_n$. In particular, when $n \neq 6$, every automorphism of $S_n$ is an inner automorphism. However, $\text{Aut}(S_6)$ is not isomorphic to $S_6$. In fact, $[\text{Aut}(S_6) : \text{Inn}(S_6)] = 2$ as we shall see in Theorem 2.3.3. We first present an example 2.3.1.

**Example 2.3.1.** Let us find $\text{Aut}(G)$ and $\text{Inn}(G)$ for $G = S_3$.

Let $S_3 = \{1, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ where $\rho_1 = (1\ 2\ 3), \rho_2 = (1\ 3\ 2), \mu_1 = (2\ 3), \mu_2 = (1\ 3)$ and $\mu_3 = (1\ 2)$. So $S_3 = \langle \rho_1, \mu_1 \rangle$. Therefore any element of $S_3$ is of the form ${\rho_1}^r {\mu_1}^s$ where $r = 0, 1, 2$ and $s = 0, 1$. Take any $\alpha \in \text{Aut}(G)$. Then

$$\alpha({\rho_1}^r {\mu_1}^s) = \alpha({\rho_1}^r)\alpha({\mu_1}^s) = (\alpha(\rho_1))^r(\alpha(\mu_1))^s.$$

Since $o(\rho_1) = 3$, $(\alpha(\rho_1))^3 = \alpha(\rho_1^3) = \alpha(1) = 1$. Hence $\alpha(\rho_1)$ is $\rho_1$ or ${\rho_1}^2 = \rho_2$. Similarly, $o(\mu_1) = 2$ and $\alpha(\mu_1) = \mu_1, \mu_2$ or $\mu_3$. Therefore $\alpha \in Aut(S_3)$ if $\alpha(1) = 1, \alpha(\rho_1) = {\rho_1}^r$ for $r = 1, 2$ and $\alpha(\mu_1) = {\rho_1}^r \mu_1$ for $r = 0, 1, 2$. So these are the only possibilities for $\alpha$. Therefore the order of $\text{Aut}(S_3)$ is at most 6. Since $\mid \text{Inn}(S_3) \mid = \mid S_3 \mid = 6$, we have $\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3$.

**Lemma 2.3.1.** *The number of elements of cycle shape* $2^k 1^{n-2k}$ *in* $S_n$ *is* $\dfrac{n!}{2^k k!(n-2k)!}$ *for* $1 \leq k \leq n/2$.

*Proof.* A product of $k$ disjoint transpositions in $S_n$ has the form, $(a_1\ b_1)\ldots(a_k\ b_k)$ with the $a_i, b_i$ distinct integers between 1 and $n$. A transposition can be done in $\binom{n}{2} = \dfrac{n(n-1)}{2}$ ways. Therefore, we have $\dfrac{n(n-1)}{2}$ choices for $(a_1\ \ b_1)$. And for $(a_2\ \ b_2)$ there are $\dfrac{(n-2)(n-3)}{2}$ choices, after $(a_1\ b_1)$ has been chosen. Proceeding this way, there are

$$\frac{n(n-1)}{2}.\frac{(n-2)(n-3)}{2}\cdot\cdot\cdot\cdot\cdot\frac{(n-2k-2)(n-2k-1)}{2} = \frac{n!}{2^k(n-2k)!}$$

choices for $k$ disjoint transpositions. To account for over counting, divide by $k!$ since there are $k$ transpositions. Hence, we have $\dfrac{n!}{2^k k!(n-2k)!}$. □

**Lemma 2.3.2.** *Let* $\alpha$ *be an automorphism of* $S_n$ *and let* $t$ *be a transposition of* $S_n$. *If* $n \neq 6$, *then* $\alpha(t)$ *is a transposition.*

*Proof.* Let $X = S_n$ and let $t \in X$ be a transposition. Suppose the lemma is false. Since the only elements of order 2 in $X$ are those whose disjoint cycle decomposition consists of disjoint transpositions, we may suppose that $\alpha$ takes a transposition to a product of $k$ disjoint transpositions where $1 \neq k \leq n/2$. That is $\alpha(t)$ is an element of cycle type $1^{n-2k}2^k$. Since $\alpha$ is an automorphism $|\ \alpha^X\ | = |\ \alpha(t)^X\ |$. The number of elements of the conjugacy class of the transposition is $\binom{n}{2} = \dfrac{n(n-1)}{2}$.

Therefore $|\ \alpha(t)^X\ | = \dfrac{n(n-1)}{2}$ and , as $\alpha(t)$ has cycle type $2^k 1^{n-2k}$ ,

$$|\ \alpha(t)^X\ | = \frac{n!}{2^k k!(n-2k)!},$$

by Lemma 2.3.1. Hence, we require

$$\frac{n!}{(n-2)!2!} = \frac{n!}{2^k k!(n-2k)!}.$$

Thus we have $2^k(n-2k)!k! = (n-2)!2!$ and therefore $2^{k-1}(n-2k)!k! = (n-2)!$. Divide both sides by $(n-2k)!(2k-2)!$ to get

$$\binom{n-2}{2k-2} = \frac{2^{k-1}k!}{(2k-2)!}. \tag{2.1}$$

Now consider the possible values of $k$. If $k = 1$, then $\alpha(t)$ is a transposition which is a contradiction. So start with $k = 2$. Then equation 2.1 says $\binom{n-2}{2} = 2$, which has no integer solution for $n$. If $k = 3$, then we get $\binom{n-2}{2} = 1$, which has the unique solution $n = 6$. But we have not allowed $n = 6$. Consider $k \geq 4$. we know that $2^{k-1} < 2^{2k-4}$ and hence, $\frac{2^{k-1}k!}{(2k-2)!} < \frac{2^{2k-4}k!}{(2k-2)!}$ as $k \geq 4$. Consider

$$\begin{aligned} \frac{(2k-2)!}{k!} &= (2k-2)(2k-3)...(k+1) \\ &> \underbrace{4.4...4}_{k-2 \text{ terms}} \\ &= 4^{k-2} = 2^{2k-4}. \end{aligned}$$

Hence,

$$\frac{2^{k-1}k!}{(2k-2)!} < \frac{2^{2k-4}k!}{(2k-2)!} < \frac{2^{2k-4}}{2^{2k-4}} = 1.$$

So that $\frac{2^{k-1}k!}{(2k-2)!} < 1$ for $k \geq 4$.

Therefore equation 2.1 has no integer solution for $n$. This proves that $\alpha(t)$ is a transposition, as claimed. □

**Lemma 2.3.3.** *Let $\phi \in \mathrm{Aut}(S_n)$. If $\phi$ maps transpositions to transpositions, then $\phi$ is an inner automorphism.*

*Proof.* Suppose that $\phi(1\ r) = (a_r\ b_r)$ for each $r$. Then $\phi((1\ 2)(1\ r)) = (a_2\ b_2)(a_r\ b_r)$. However, if $r \geq 3$, then $(1\ 2)(1\ r) = (1\ 2\ r)$ is an element of order 3. Thus either $a_r \in \{a_2, b_2\}$ or $b_r \in \{a_2, b_2\}$ but not both. We claim that for all $r$ either $a_r = a_2$ or

$a_r = b_2$ .

Suppose that there are $r \neq s$ with $a_r = a_2$ and $a_s = b_2$. Note that $(1\ r\ 2)(1\ s\ 2) = (1\ r)(2\ s)$ has order 2. Also,

$$\begin{aligned} \phi((1\ 2\ r)(1\ 2\ s)) &= (a_2\ b_2)(a_r\ b_r)(a_2\ b_2)(a_s\ b_s) \\ &= (a_2\ b_2)(a_2\ b_r)(a_2\ b_2)(b_2\ b_s) \\ &= (b_2\ b_r\ b_s) \end{aligned}$$

has order 3. This is a contradiction. Hence we have either $a_2 = a_r$ for all $r$ or $b_2 = b_r$ for all $r$. So we assume that $a_2 = a_r$ for all $r$. Then the other case is similar. We then have $\phi(1\ r) = (a_2\ b_r)$ for all $r \geq 3$. So that this shows, $b_r \neq b_s$ if $r \neq s$ since $\phi$ is injective.

Let $\sigma$ be a permutation such that $\sigma(1) = a_2$ and $\sigma(r) = b_r$ for all $r \geq 3$. This uniquely determines $\sigma$ as we have defined $\sigma$ on $n-1$ values. From the choice of $\sigma$ we can see that $\phi(1\ r) = (a_2\ b_r) = \sigma(1\ r)\sigma^{-1}$. Therefore $\phi$ is an inner automorphism. □

**Theorem 2.3.1.** *If $n \neq 6$, then $Aut(S_n) \cong S_n$.*

*Proof.* The result now follows from 2.3.2 and 2.3.3. □

**Lemma 2.3.4.** *If $H$ is a transitive subgroup of $S_6$ having order 120, then $H$ cannot contain a transposition.*

*Proof.* The transitive subgroup $H$ of order 120 contains an element $\sigma$ of order 5, which is a 5-cycle. We may suppose that $\sigma = (1\ 2\ 3\ 4\ 5)$. If $(i\ j) \in H$, then the transitivity of $H$ gives, $\tau \in H$ with $\tau(j) = 6$. Therefore $\tau(i\ j)\tau^{-1} = (k\ 6)$ for some $k \neq 6$. Conjugating $(k\ 6)$ by the powers of $\tau\sigma$ shows that $H$ contains $(1\ 6), (2\ 6), (3\ 6), (4\ 6), (5\ 6)$. However these transpositions generate all of $S_6$. □

**Theorem 2.3.2.** *There exists an outer automorphism of* $S_6$.

*Proof.* By the Sylow's Theorem, the Sylow 5-subgroup $P$ of $S_5$ has 6 conjugates. Let $\varphi : S_5 \longrightarrow S_6$ be the representation of $S_5$ on the conjugates of $P$.

Since $\mathrm{Ker}\varphi \subseteq N(P)$, the normalizer of $P$ which has index 6 in $S_6$, and hence is not one of the subgroups $A_5$ or $S_5$, we have $\varphi$ is one-one. Hence $H = \mathrm{Im}\varphi$ is a transitive subgroup of $S_6$ and $H \cong \mathrm{Sym}(5)$.

Next let $\phi : S_6 \longrightarrow S_6$ be the permutation representation on the cosets of $H$.

As above, $\phi$ is injective, hence onto and so $\phi \in \mathrm{Aut}(S_6)$. If $\phi \in \mathrm{Inn}(S_6)$, then $\phi((1\ 2))$ will be a transposition, that fixes four symbols. Thus, (1 2) will be contained in exactly four conjugates of $H$. But then $H$ contains a transposition which contradicts Lemma 2.3.4. Thus, $\phi$ is an outer automorphism. □

**Theorem 2.3.3.** $\dfrac{\mathrm{Aut}(S_6)}{\mathrm{Inn}(S_6)} \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

*Proof.* Two permutations lie in the same conjugacy class if and only if they have the same cycle structure. Therefore we have the following table of conjugacy classes of $S_6$.

Let $\mathcal{C} = \{C_1, \ldots, C_{11}\}$ be the set of conjugacy classes of $S_6$ and if $\phi \in \mathrm{Aut}(S_6)$, then $\phi \in S_{\mathcal{C}}$. If $\phi$ is an inner automorphism if, and only if $\phi(C_2) = C_2$ by Theorem 4.2. Therefore, $\phi$ is an outer automorphism if, and only if $\phi$ interchanges $C_2$ and $C_{10}$, since these are the only conjugacy classes having 15 elements. It follows that if $\phi$ and $\varphi$ are outer automorphisms. Then $\phi\varphi(C_2) = C_2$, hence $\phi\varphi$ is an inner automorphism, and $\dfrac{\mathrm{Aut}(S_6)}{\mathrm{Inn}(S_6)}$ has order at most 2. Combining this with Theorem 2.3.2 we have the claim.

| *Conjugacy classes* | *Cycle structure* | *Order* | *Parity* | *Number of such* |
|---|---|---|---|---|
| $C_1$ | (1) | 1 | *even* | 1 |
| $C_2$ | (1 2) | 2 | *odd* | 15 |
| $C_3$ | (1 2 3) | 3 | *even* | 40 |
| $C_4$ | (1 2 3 4) | 4 | *odd* | 90 |
| $C_5$ | (1 2 3 4 5) | 5 | *even* | 144 |
| $C_6$ | (1 2 3 4 5 6) | 6 | *odd* | 120 |
| $C_7$ | (1 2)(3 4) | 2 | *even* | 45 |
| $C_8$ | (1 2)(3 4 5) | 6 | *odd* | 120 |
| $C_9$ | (1 2)(3 4 5 6) | 4 | *even* | 90 |
| $C_{10}$ | (1 2)(3 4)(5 6) | 2 | *odd* | 15 |
| $C_{11}$ | (1 2 3)(4 5 6) | 3 | *even* | $\underline{40}$ |
| | | | | $720 = 6!$ |

□

# Chapter 3

# Free Groups

## 3.1 Words and Reduced Words

**Definition 3.1.1.** Let $S$ be an arbitrary set of symbols, say $S = \{x_1, x_2, \ldots\}$, which may be finite or infinite, and define a *word* to be a finite string of symbols from $S$, in which repetetion is allowed. For example, $x_1, x_1x_2, x_1x_1$ and $x_1x_1x_2x_1$ are words. Two words can be composed by juxtaposition:

$$x_1x_1, x_2x_1 \longmapsto x_1x_1x_2x_1.$$

Thus the set $W$ of all words has an associative law of composition. Also, the *empty word* can be introduced as an identity element. We will denote the empty word by 1.

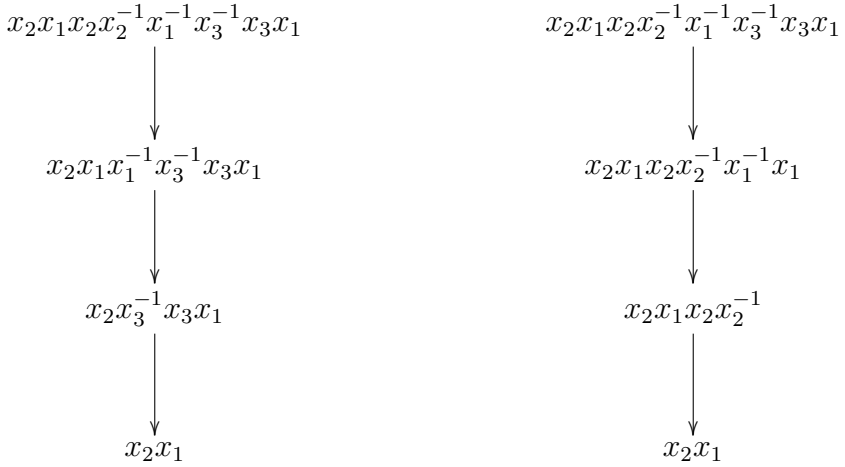
Let $S^{'}$ be the set consisting of the symbols in $S$ and also $x_i^{-1}$ for every $x_i \in S$:

$$S^{'} = \{x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots\}.$$

Let $W^{'}$ be the set of words made using the symbols $S^{'}$. If a word $w \in W^{'}$ looks like $\ldots xx^{-1} \ldots$ or $\ldots x^{-1}x \ldots$ for some $x \in S$, then we can cancel the two symbols $x, x^{-1}$ and

reduce the length of the word. The word is said to be *reduced* if no such cancellation can be made.

Now there is more than one way to proceed with cancellation. For instance, let $w = x_2x_1x_2x_2^{-1}x_1^{-1}x_3^{-1}x_3x_1$,




At the end we will obtained the same reduced word.

**Lemma 3.1.1.** *There is only one reduced form of a given word $w$.*

*Proof.* We will use the Mathematical Induction on the length of $w$. If $w$ is a reduced word then the assertion is true. If not, there should be some pair which can be canceled, say $w = \dots xx^{-1} \dots$ be a word for $x \in S'$. Suppose that $w'$ is reduced form of $w$. We know that $w'$ is obtained from $w$ by some steps of cancellation. The first case is that our pair $xx^{-1}$ is canceled at some step. Then we might rearrange the operations and cancel $xx^{-1}$ first. On the other hand, the pair $xx^{-1}$ cannot remain in $w'$ as $w'$ is a reduced word. Therefore at least one of the two symbols must be canceled at some time. If the pair itself is not canceled, then the first cancellation involving the pair must look like,

$$\dots x^{-1}xx^{-1} \dots \text{ or } \dots xx^{-1}x \dots .$$

Note that the word obtained by this cancellation is the same as that obtained by canceling the original pair $xx^{-1}$. Then we are back in the first case, and the lemma is proved. □

**Definition 3.1.2.** Two words $w$ and $w^{'}$ in $W^{'}$ are *equivalent* if they have the same reduced form, and we write $w \sim w^{'}$.

This is an equivalence relation.

**Lemma 3.1.2.** *The product of two equivalent words is equivalent.*

*Proof.* Let $w$ and $v$ be two words and equivalent to $w^{'}$ and $v^{'}$ respectively. Hence we need to show that $w \sim w^{'}$ and $v \sim v^{'}$, then $wv \sim w^{'}v^{'}$. to obtain the reduced word equivalent to the product $wv$, cancel the possible terms in $w$ and $v$,to reduce $w$ to $w_{\circ}$ and $v$ to $v_{\circ}$. Then $wv$ is reduced to $w_{\circ}v_{\circ}$. Next we continue canceling in $w_{\circ}v_{\circ}$ if possible. Since, $w \sim w^{'}$ and $v \sim v'$, the same process applied to $w^{'}v^{'}$. Therefore it gives the same reduced word. □

Lemma 3.1.2 says that multiplication of equivalence classes of words is well-defined law of composition.

**Lemma 3.1.3.** *Let $F$ denote the set of equivalence classes of words in $W^{'}$. Then $F$ is a group with the law of composition induced from $W^{'}$.*

*Proof.* It is clear that the multiplication is associative and 1 is an identity in $W^{'}$. We need to show that all the elements of $F$ are invertible. But we know that $w = x_1x_2 \dots x_n$ then the class of $x_n^{-1} \dots x_2^{-1}x_1^{-1}$ is the inverse of the class of $w$. □

## 3.2 Free Groups

**Definition 3.2.1.** The group $F$ of equivalence classes of words is called the *free group* on the set $S$, denoted by $F[S]$.

**Definition 3.2.2.** Let $G$ be a group and let $T \subseteq G$. Then the smallest subgroup of $G$ containing $T$ is the *subgroup generated by* $T$. We write $\langle T \rangle$ for subgroup generated by $T$. A group $G$ is *generated* by a set $T$, if $G$ has no proper subgroup containing $T$. That is $G = \langle T \rangle$. If there is a finite set that generates $G$, then $G$ is *finitely generated*.

**Theorem 3.2.1.** *Let $G$ be a group and $a_i \in G$ for $i \in I$. Let $H$ be a subgroup of $G$ generated by $T = \{a_i \mid i \in I\}$. Then $H$ has elements precisely those elements of $G$ that are finite products of integral powers of $a_i$, where powers of a fixed $a_i$ may occur several times in the product.*

*Proof.* Let $K$ be the set of all finite products of integral powers of the $a_i$. Clearly, $K \subseteq H$. The product of elements in $K$ is again in $K$. The identity element $e \in K$. For every element $k \in K, k^{-1} \in K$, since from the product giving $k$ a new product with the order of the $a_i$ reversed and the opposite sign on all exponents, we have $k^{-1}$, and $k^{-1} \in K$. Therefore $K$ is a subgroup of $G$ and since $H$ is the smallest subgroup containing $a_i$ for $i \in I, K = H$. □

To illustrate how we invert elements in the last but one sentence of the previous we have the following:

$$[(x_1)^2(x_2)^{-3}(x_3)^2]^{-1} = (x_3)^{-2}(x_2)^3(x_1)^{-2}.$$

**Theorem 3.2.2.** *Let $G$ be a group generated by $T = \{a_i | i \in I\}$ and let $H$ be any group. Then there is at most one homomorphism $\phi : G \longrightarrow H$ such that $\phi(a_i) = h_i$ for any element $h_i \in H$ and $i \in I$. If $G$ is free on $T$, then there is exactly one such homomorphism.*

*Proof.* Let $\phi$ be a homomorphism from $G$ to $H$ such that $\phi(a_i) = h_i$. Now for any $g \in G$ for some finite product of the generators $a_i$. Then we have

$$\phi(g) = \phi(\prod_j {a_{ij}}^{n_j}) = \prod_j \phi(a_{i_j}^{n_j}) = \prod_j h_{i_j}^{n_j}$$

as $\phi$ is a homomorphism. Therefore a homomorphism is completely determined by its values on elements of a generating set. Hence there is at most one homomorphism such that $\phi(a_i) = h_i$.

Let $G$ be a free group on the set $S$, that is, $G = F[S]$. Define a map

$$\varphi : G \longrightarrow H$$

by

$$\varphi(g) = \prod_j h_{i_j}^{n_j} \quad \text{for} \quad g = \prod_j a_{i_j}^{n_j}$$

Since $F[S]$ contains precisely reduced words, two different products in $F[S]$ are not equal. Therefore map $\varphi$ is well defined.

$$\varphi(gg^{'}) = (\prod_j h_{i_j}^{n_j})(\prod_k h_{ik}^{'m_k}) = \varphi(g)\varphi(g^{'})$$

for any elements $g$ and $g^{'}$ in $G$. Hence $\varphi$ is a homomorphism. □

# Chapter 4

# Coset Enumeration

## 4.1 Group Presentation

**Definition 4.1.1.** Let $S$ be a set and $F[S]$ be a free group. Let $R = \{r_i | i \in I\} \subseteq F[S]$. Let $N$ be the least normal subgroup containing the $r_i$. An isomorphism $\phi$ of $F[S]/N$ onto a group $G$ is a *presentation* of $G$. The sets $S$ and $\{r_i\}$ give a *group presentation.* The set $S$ is the set of *generators for the presentation* and each $r_i$ is a *relator.* An equation $r_i = 1$ is a *relation.* The notation $\langle S \mid R \rangle$ denote the group presentation in which the generators are elements from $S$ and the relators are from $R$. A *finite presentation* is one which both $S$ and $I$ are finite sets. .

**Example 4.1.1.** The presentation $\langle x, y \mid x^2 = 1, y^n = 1, (xy)^2 = 1 \rangle$ defines a group which is isomorphic to $D_{2n}$.

**Example 4.1.2.** A *Coxeter group* can be defined as a group with the presentation

$$\langle a_1, a_2, ..., a_n | (a_i a_j)^{m_{ij}} = 1 \rangle$$

where $a_i, i = 1, 2, ..., n$ is a relation and $m_{ij}$ is an integer for all $i, j = 1, 2, ..., n$. Also $m_{ij} = 1$ if $i = j$ and $m_{ij} \geq 2$ if $i \neq j$.

If $m_{ii} = 1$ then $(a_i)^2 = 1$ for all $i = 1, 2, ..., n$ and the generators are either involutions or trivial. Recall an involution is elements such that $(a_i)^2 = 1$. If $m_{ij} = 2$ then the generators $a_i$ and $a_j$ commute for all $i$, $j$ such that $i \neq j$. So $(a_i a_j)^2 = 1$. Let $a_i a_j = x$ then $x^2 = 1$.

## 4.2 Coset Enumeration

*Coset enumeration* is a method of counting the cosets of a subgroup $H$ of a group $G$ given in terms of a presentation. As a by-product, one can obtain a permutation representation for $G$ on the cosets of $H$. If $H$ has a known finite order, coset enumeration gives the order of $G$ as well.

The algorithm for the coset enumeration is the **Todd Coxeter algorithm** which we now describe.

**Todd Coxeter Algorithm**

Let $G$ be a group with a finite set $X = \{g_1, ..., g_n\}$ of generators. Let $R$ be a finite set of relators in these generators. Thus, $G$ is the quotient of the free group on $X$ by the normal closure of the subgroup, as we have seen in Section 4.1, generated by the elements in $R$. Elements of $R$ are words in the elements of $X \cup X^{-1}$. Suppose that $H$ is a subgroup of $G$ generated by $Y = \{h_1, ..., h_m\}$. The elements of $Y$ are also words in the elements of $X \cup X^{-1}$.

Todd coxeter enumeration is a method to enumerate all the different cosets of $H$ in

$G$. These cosets will be denoted by positive integers. The integer 1 represents $H$. The notation $n \cdot g$ is the image under $g$ of the coset represented to $n$. Todd Coxeter enumeration relies on the following three observations:

$\bullet 1 \cdot h = 1$, for all $h \in H$.

Since for all $h \in H$, $Hh = H$.

$\bullet j.r = j$, for all cosets $j$ and $r \in R$.

This follows as $r$ evaluates to 1 in $G$.

$\bullet i \cdot g = j \iff i = j \cdot g^{-1}$, for all cosets $i, j$ and all $g \in X$.

Assume that $i = Hm$ and $j = Hl$, then $i\cdot = Hmg = Hl$ if, and only if, $Hm = Hlg^{-1}$.

These three observations will be used to set up three types of tables:

- subgroup table
- relator table and
- coset table.

We will illustarte the process in the following example.

**Example 4.2.1.** $G^* = \langle x, y | x^2, y^2, (xy)^3 \rangle$ and subgroup $H^* = \langle x \rangle$. We start to construct a subgroup table for every generator $h = g_{j1}...g_{jl}$ of $H$, where $g_{ji}$ are the set of generators. This table consists of only one row of length $l + 1$ and starts and ends with the entry 1, that represents the coset $H$. In this example, there is only one subgroup table as $H^*x = H^*$.

| *subgroup* | $x$ |
|---|---|
| 1 | 1 |

Next we will construct relator tables for each relator $r = g_{i_1}...g_{i_k}$ with the generators $g_{i_j}$. These tables consist of $k + 1$ columns and the number of rows is determined during the

process. As with the subgroup table, each row starts and ends with the same integer. For this example, there are three relator tables: using the subgroup table, the first row of each of these is filled as follows:

| *relator* | $x$ | $x$ | $y$ | $y$ | $x$ | $y$ | $x$ | $y$ | $x$ | $y$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | 1 | 1 | 2 | 3 | 4 | 5 | 1 |

Where $H^*y = 2$, $H^*yx = 3$, $H^*yxy = 4$. Then add the other rows using

$2 \cdot y = H^*y^2 = H^* = 1$

$3 \cdot x = H^*yx^2 = H^*y = 2$

$3 \cdot y = H^*yxy = 4$

$4 \cdot x = H^*yxyx = 5$

$4 \cdot y = H^*yxy^2 = H^*yx = 3$

$5 \cdot x = H^*yxyx^2 = H^*yxy = 4$

$5 \cdot y = H^*yxyxy = H^*x = 1$

| *relator* | $x$ | $x$ | $y$ | $y$ | $x$ | $y$ | $x$ | $y$ | $x$ | $y$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | 1 | 1 | 2 | 3 | 4 | 5 | 1 |
| 2 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 1 | 1 | 2 |
| 3 | 2 | 3 | 4 | 3 | 2 | 1 | 1 | 2 | 3 | 3 |
| 4 | 5 | 4 | 3 | 4 | 5 | 1 | 1 | 2 | 3 | 4 |
| 5 | 4 | 5 | 1 | 5 | 4 | 3 | 2 | 1 | 1 | 5 |

Then the coset table for $G^*$ is

| *coset* | $x$ | $y$ |
|---|---|---|
| 1 | 1 | 2 |
| 2 | 3 | 1 |
| 3 | 2 | 4 |
| 4 | 5 | 3 |
| 5 | 4 | 1 |

If the information from the tables tells that $i \cdot g = j \cdot g$ for some generator $g$, but $i \neq j$, then two distinct integers $i$ and $j$ represent the same coset. This is called a *coincidence*. From the second relator table $2 \cdot y = 1$ and from the third relator table $5 \cdot y = 1$. This says that coset labeled 2 and 5 are equal. So replace 5 by 2 in the relator tables and remove the row starting with 5. Hence, the table now has four rows.

| *relator* | $x$ | $x$ | $y$ | $y$ | $x$ | $y$ | $x$ | $y$ | $x$ | $y$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | 1 | 1 | 2 | 3 | 4 | 2 | 1 |
| 2 | 3 | 2 | 1 | 2 | 3 | 4 | 2 | 1 | 1 | 2 |
| 3 | 2 | 3 | 4 | 3 | 2 | 1 | 1 | 2 | 3 | 3 |
| 4 | 2 | 4 | 3 | 4 | 2 | 1 | 1 | 2 | 3 | 4 |

Another coincidence is from the first relator table, $2 \cdot x = 3$ and $2 \cdot x = 4$. So we can replace 4 by 3. Then only three cosets remain. Furthermore the coset table is closed. The relator tables and coset table are

| *relator* | $x$ | $x$ | $y$ | $y$ | $x$ | $y$ | $x$ | $y$ | $x$ | $y$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 2 | 1 | 1 | 2 | 3 | 3 | 2 | 1 |
| 2 | 3 | 2 | 1 | 2 | 3 | 3 | 2 | 1 | 1 | 2 |
| 3 | 2 | 3 | 3 | 3 | 2 | 1 | 1 | 2 | 3 | 3 |

| *coset* | $x$ | $y$ |
|---|---|---|
| 1 | 1 | 2 |
| 2 | 3 | 1 |
| 3 | 2 | 3 |

So the group $H^* = \langle x \rangle$ has index 3 in $G^*$. Moreover, we can obtain a permutation representation of $G^*$ into $S_3$. Hence $x$ maps to (2 3) and $y$ maps to (1 2). So $G^* = \langle (1\ 2), (2\ 3) \rangle \cong S_3$ and $\mid G^* : H^* \mid = 3$. The group $G^*$ is of order 6, since $H^*$ is the order of 2.

We now demonstrate a more complicated example.

**Example 4.2.2.** *[6]* Consider the group

$$G = \langle x_1, x_2, x_3, x_4, x_5 | x_1x_2 = x_3, x_2x_3 = x_4, x_3x_4 = x_5, x_4x_5 = x_1, x_5x_1 = x_2 \rangle$$

and enumerate cosets of $\langle x_1 \rangle$. The subgroup table is

| *subgroup* | $x_1$ |
|---|---|
| 1 | 1 |

and relator tables are (after some work)

| *relator* | $x_1$ | $x_2$ | ${x_3}^{-1}$ | $x_2$ | $x_3$ | ${x_4}^{-1}$ | $x_3$ | $x_4$ | ${x_5}^{-1}$ | $x_4$ | $x_5$ | ${x_1}^{-1}$ | $x_5$ | $x_1$ | ${x_2}^{-1}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Therefore the group $G$ is generated by only one element and $G = \langle x_1 \rangle$. Hence $G$ is cyclic.

**Example 4.2.3.** Consider the group

$$\begin{aligned} G \;=\; & \langle x_1, x_2, x_3, x_4 | {x_1}^2 = {x_2}^2 = {x_3}^2 = {x_4}^2 = 1, [x_1, x_3] = [x_1, x_4] = [x_2, x_4] = 1, \\ & (x_1x_2)^3 = (x_2x_3)^3 = (x_3x_4)^3 = 1 \rangle \end{aligned}$$

and enumerate cosets with respect to the subgroups $H = \langle x_1, x_2 \rangle$. We know the elements of $H$ satisfy the relations $(x_1x_2)^3 = {x_1}^2 = {x_2}^2 = 1$. But as a subgroup of $G$ it may satisfy further relations. $K = \langle x_1, x_2, x_3 \rangle$ and the elements of $K$ satisfy relations ${x_1}^2 = {x_2}^2 = {x_3}^2 = [x_1, x_3] = (x_1x_2)^3 = (x_2x_3)^3 = 1$. Subgroup table for $H$, relator tables for subgroup $H$ in $K$ and coset table for $H$ are

| $Subgroup$ | $x_1$ | $x_2$ |
|---|---|---|
| 1 | 1 | 1 |

| $relator$ | $x_1$ | $x_1$ | $x_2$ | $x_2$ | $x_3$ | $x_3$ | $x_1$ | $x_3$ | $x_1$ | $x_3$ | $x_1$ | $x_2$ | $x_1$ | $x_2$ | $x_1$ | $x_2$ | $x_2$ | $x_3$ | $x_2$ | $x_3$ | $x_2$ | $x_3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 4 | 4 | 2 | 1 |
| 2 | 2 | 2 | 4 | 2 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 4 | 3 | 3 | 4 | 2 | 4 | 4 | 2 | 1 | 1 | 2 |
| 3 | 4 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 2 | 2 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 3 | 4 | 2 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 2 | 2 | 4 | 2 | 1 | 1 | 2 | 4 | 4 |

| $coset$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|
| 1 | 1 | 1 | 2 |
| 2 | 2 | 4 | 1 |
| 3 | 4 | 3 | 3 |
| 4 | 3 | 2 | 4 |

We deduce that $|K : H| = 4$. We also have $x_1 = (3\ 4), x_2 = (2\ 4)$ and $x_3 = (1\ 2)$. A group generated by three elements of order 2 subject only to relations $[x_1, x_3] = (x_1, x_2)^3 = (x_2, x_3)^3 = 1$ must be Sym(4). Thus $K = \text{Sym}(4)$. It follows that $|K| = 24$ and $|H| = 6$. So $H = \text{Sym}(3)$.

Next we will consider the relator tables for subgroup $K$ in $G$.

| *relator* | $x_1$ | $x_1$ | $x_2$ | $x_2$ | $x_3$ | $x_3$ | $x_4$ | $x_4$ | $x_1$ | $x_3$ | $x_1$ | $x_3$ | $x_1$ | $x_4$ | $x_1$ | $x_4$ | $x_2$ | $x_4$ | $x_2$ | $x_4$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 1 |
| 2 | 2 | 2 | 2 | 2 | 3 | 2 | 1 | 2 | 2 | 3 | 3 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 2 |
| 3 | 3 | 3 | 4 | 3 | 2 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 3 | 3 |
| 4 | 5 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 5 | 5 | 4 | 4 | 3 | 3 | 4 | 4 |
| 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 |

| $x_1$ | $x_2$ | $x_1$ | $x_2$ | $x_1$ | $x_2$ | $x_2$ | $x_3$ | $x_2$ | $x_3$ | $x_2$ | $x_3$ | $x_3$ | $x_4$ | $x_3$ | $x_4$ | $x_3$ | $x_4$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 3 | 3 | 2 | 1 |
| 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 4 | 4 | 3 | 2 | 3 | 3 | 2 | 1 | 1 | 2 |
| 3 | 4 | 5 | 5 | 4 | 3 | 4 | 4 | 3 | 2 | 2 | 3 | 2 | 1 | 1 | 2 | 3 | 3 |
| 5 | 5 | 4 | 3 | 3 | 4 | 3 | 2 | 2 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 4 | 3 | 3 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |

Coset table for $G$

| *coset* | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 2 |
| 2 | 2 | 2 | 3 | 1 |
| 3 | 3 | 4 | 2 | 3 |
| 4 | 5 | 3 | 4 | 4 |
| 5 | 4 | 5 | 5 | 5 |

From the coset table we can see that $|G : K| = 5$. Also we have $x_1 = (4\ 5), x_2 = (4\ 3\ 5), x_3 = (3\ 2\ 5), x_4 = (1\ 2)(3\ 4\ 5)$.

$$|G| = \frac{|G|}{|K|}.\frac{|K|}{|H|}.|G| = 5.4.6 = 120.$$

Hence as $|\ G\ | = |$ Sym(5) $|$ and $G$ acts faithfully on five points $G$ is the group Sym (5). Since the elements $(1\ 2)(2\ 3)\ldots(4\ 5)$ of Sym(5) satisfy the relations we get that $|\ G\ | \geq 120$.

# Chapter 5

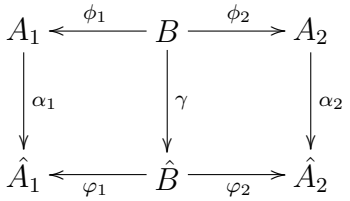
# Amalgams

## 5.1 Amalgams

**Definition 5.1.1.** Let $A, B$ and $C$ be groups, and $\phi_1 : C \longrightarrow A$ and $\phi_2 : C \longrightarrow B$ be monomorphisms. Then the five-tuple $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ is called an *amalgam*.

**Example 5.1.1.** Let $A_1 = \mathrm{Sym}(4), A_2 = \mathrm{Sym}(4)$ and $B = \mathrm{Dih}(8) = \langle (12)(34), (23) \rangle$. Define $\phi_1 : B \longrightarrow A_1$ and $\phi_2 : B \longrightarrow A_2$ by identity mappings. Then $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ is an amalgam, since $\phi_1$ and $\phi_2$ are monomorphisms.

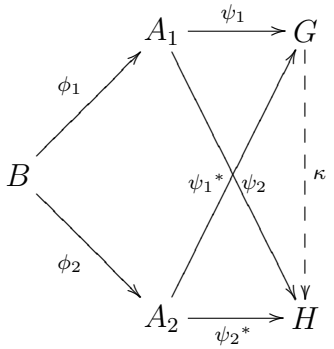
**Definition 5.1.2.** Let $\mathcal{A}_1 = (A_1, A_2, B, \phi_1, \phi_2)$ and $\mathcal{A}_2 = (\hat{A}_1, \hat{A}_2, \hat{B}, \varphi_1, \varphi_2)$ be amalgams. If there exist isomorphisms $\alpha_i : A_i \longrightarrow \hat{A}_i$ and $\gamma : B \longrightarrow \hat{B}$ for $i = 1, 2$, such that $\mathrm{Im}(\phi_i \alpha_i) = \mathrm{Im}(\gamma \varphi_i)$ then we say that $\mathcal{A}_1$ and $\mathcal{A}_2$ have same *type*. Two amalgams of the same type are *isomorphic*, if for $i = 1$ and 2, $\phi_i \alpha_i = \gamma \varphi_i$. This is equivalent to saying that the following diagram of groups commutes.




**Definition 5.1.3.** Let $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ be an amalgam. A *representation of* $\mathcal{A}$ *into* a group $G$ is a homomorphism $(\psi_1, \psi_2)$ where $\psi_i : A_i \longrightarrow G$ for $i = 1, 2$, such that $\phi_1\psi_1 = \phi_2\psi_2$. Then a *completion* of $\mathcal{A}$ in $G$ is the triple $(\langle \psi_1(A_1), \psi_2(A_2) \rangle, \psi_1, \psi_2)$.

**Definition 5.1.4.** A completion of $\mathcal{A}$ is *faithful* if $\psi_1$ and $\psi_2$ are monomorphisms.

**Definition 5.1.5.** A completion $(G, \psi_1, \psi_2)$ of $\mathcal{A}$ is called a *universal completion* of $\mathcal{A}$ if given any other completion $(H, {\psi_1}^*, {\psi_2}^*)$ there exists a unique homomorphism $\kappa : G \longrightarrow H$ which makes the following diagram commute.




**Definition 5.1.6.** Let $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ be an amalgam and let $N$ be the normal subgroup of the *free product* $A_1 * A_2$ generated by $\{\phi_1(b)\phi_2(b^{-1}) \mid b \in B\}$. The group $(A_1 * A_2)/N$, often denoted by $G(\mathcal{A})$, is the *free amalgamated product* of $A_1$ and $A_2$ over $B$.

**Lemma 5.1.1.** *Let* $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ *be an amalgam, and* $N$ *be a normal subgroup of the free product* $A_1 * A_2$ *generated by the set* $\{\phi_1(b)\phi_2(b^{-1}) | b \in B\}$. *Let*

$\theta_1 : A_1 \longrightarrow (A_1 * A_2)/N$ *be defined by* $\theta_1(x) = xN$, *for all* $x \in A_1$

*and*

$$\theta_1 : A_2 \longrightarrow (A_1 * A_2)/N \text{ be defined by } \theta_2(y) = yN, \text{ for all } y \in A_2.$$

*Then* $((A_1 * A_2)/N, \theta_1, \theta_2)$ *is a universal completion of* $\mathcal{A}$.

*Proof.* We have $\phi_1\theta_1 = \phi_2\theta_2$ as $\theta_1$ and $\theta_2$ are homomorphisms. Then the following diagram commutes.

$$\begin{array}{ccc} B & \xrightarrow{\phi_1} & A_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \theta_1} \\ A_2 & \xrightarrow[\theta_2]{} & (A_1 * A_2)/N \end{array}$$

Let $(H, \psi_1, \psi_2)$ be a completion of $\mathcal{A}$. Define $\kappa : A_1 * A_2 \longrightarrow H$ be the unique homomorphism such that $\kappa(x) = \psi_1(x)$ and $\kappa(y) = \psi_2(y)$ for all $x \in A_1$ and $y \in A_2$. Then

$$\kappa(\phi_1(b)\phi_2(b^{-1})) = \kappa(\phi_1(b))\kappa(\phi_2(b^{-1}))$$

$$= \psi_1(\phi_1(b))\psi_2(\phi_2(b^{-1})) = 1$$

for all $b \in B$. Next define $\kappa^{'} : (A_1 * A_2)/N \longrightarrow H$ by $\kappa^{'}(x^{'}N) = \kappa(x^{'})$ for all $x^{'} \in A_1 * A_2$. Then $\kappa^{'}$ is a homomorphism. Also $\kappa^{'}(\theta_1(x)) = \kappa^{'}(xN) = \kappa(x)$ for all $x \in A_1$, and $\kappa^{'}(\theta_2(y)) = \kappa^{'}(yN) = \kappa(y)$ for all $y \in A_2$,. Also, $\kappa(x) = \psi_1(x)$ and $\kappa(y) = \psi_2(y)$ for all $x \in A_1, y \in A_2$. This shows that the uniqueness of $\kappa^{'}$. □

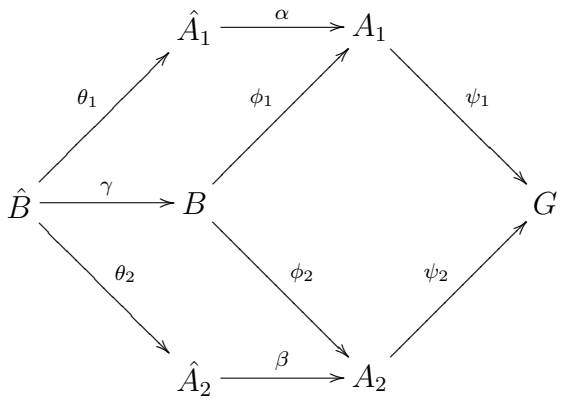
Note that the uniqueness of the homomorphism $\kappa$ in the Definition 5.1.5 and the existence of a universal completion for any amalgam, $\mathcal{A}$, by Lemma 5.1.1, imply that $G(\mathcal{A})$ is unique upto isomorphism, and that any other completion of $\mathcal{A}$ is a quotient of $G(\mathcal{A})$.

**Lemma 5.1.2.** *Isomorphic amalgams have the same groups as completions.*

*Proof.* Assume that $\mathcal{A}_1 = (A_1, A_1, B, \phi_1, \phi_2)$ and $\mathcal{A}_2 = (\hat{A}_1, \hat{A}_2, \hat{B}, \theta_1, \theta_2)$ are isomorphic amalgams by the triple of isomorphisms:

$$\alpha : \hat{A}_1 \longrightarrow A_1, \beta : \hat{A}_2 \longrightarrow A_2, \gamma : \hat{B} \longrightarrow B.$$

Let $(G, \psi_1, \psi_2)$ be a completion of $\mathcal{A}_1$. Then the following diagram commutes.




$$\theta_1\alpha\psi_1 = \gamma\phi_1\psi_1$$

$$= \gamma\phi_2\psi_2$$

$$= \theta_2\beta\psi_2.$$

Therefore $(G, \alpha\psi_1, \beta\psi_2)$ is a completion of $\mathcal{A}_2$. □

**Lemma 5.1.3.** *Let $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ and $\mathcal{A}' = ({A_1}', {A_2}', B', \phi_1', \phi_2')$ be amalgams with the same type, then there exists $\gamma \in Aut(B)$ such that $\mathcal{A}'$ is isomorphic to $\mathcal{A}^\gamma = (A_1, A_2, B, \phi_1, \gamma\phi_2)$.*

*Proof.* Suppose that $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ and $\mathcal{A}' = ({A_1}', {A_2}', B', \phi_1', \phi_2')$ are amalgams of the same type. Let $\tau_i : A_i \longrightarrow {A_i}'$ be an isomorphism such that $\mathrm{Im}(\phi_i\tau_i) = \mathrm{Im}({\phi_i}')$. Next define $\theta_i : B \longrightarrow B'$ by $\theta_i \longmapsto \theta_i\tau_i({\phi_i}')^{-1}$. Since $\phi_i$ and ${\phi_i}'$ are monomorphisms $\theta_i$

is an isomorphism.

Let $\rho : B \longrightarrow B^{'}$ be any isomorphism and define $\beta_i \in \mathrm{Aut}(B)$ as $\beta_i = \rho{\theta_i}^{-1}$ for $i = 1, 2$.

Note that

$$\begin{aligned} {\theta_i}^{-1} &= {\phi_i}^{'}(\tau_i)^{-1}{\phi_i}^{-1} \\ \beta_i\phi_i\tau_i &= \rho{\theta_i}^{-1}\phi_i\tau_i \\ &= \rho({\phi_i}^{'}{\tau_i}^{-1}\phi_i\tau_i) = \rho{\phi_i}^{'} \end{aligned}$$

for $i = 1, 2$.

Hence $\mathcal{A}^{'}$ and $(A_1, A_2, B, \beta_1\phi_1, \beta_2\phi_2)$ are isomorphic as the triple $(\tau_1, \rho, \tau_2)$. The amalgams $(A_1, A_2, B, \beta_1\phi_1, \beta_2\phi_2)$ and $(A_1, A_2, B, \phi_1, {\beta_1}^{-1}\beta_2\phi_2)$ are isomorphic as the triple of automorphisms $(1, \beta_i, 1)$. Therefore $({A_1}^{'}, {A_2}^{'}, B^{'}, \phi_1^{'}, \phi_2^{'})$ and $(A_1, A_2, B, \phi_1, {\beta_1}^{-1}\beta_2\phi_2)$ are isomorphic amalgams. So take $\gamma = \beta_1^{-1}\beta_2$. Hence $\gamma \in$ Aut $(B)$. □

**Theorem 5.1.1.** Let $H$ and $K$ be subgroups of a group $G$ such that $H \leq K$. Then $\dfrac{N_{\mathrm{Aut}(K)}(H)}{C_{\mathrm{Aut}(K)}(H)}$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

*Proof.* Define

$$\begin{aligned} \phi : N_{\mathrm{Aut}(K)}(H) &\longrightarrow \text{ Aut } (H) \\ \phi(\sigma) &= \sigma\mid_H \end{aligned}$$

where $\sigma$ is a map from $H$ to a subgroup of $K$. Then $\sigma \in \mathrm{Ker}\phi$ if, and only if $\sigma(h) = h$ for $h \in H$ if, and only if $\sigma \in C_{\mathrm{Aut}(K)}(H)$. So Ker $\phi = C_{\mathrm{Aut}(K)}(H)$. Then by the first isomorphism theorem,

$$\frac{N_{\mathrm{Aut}(K)}(H)}{C_{\mathrm{Aut}(K)}(H)} \cong \mathrm{Im}\phi \leq \mathrm{Aut}(H).$$

□

## 5.2 Goldschmidt's Lemma

**Definition 5.2.1.** Suppose that $H$ and $K$ are subgroups of a group $G$ such that $H \leq K$. Let $\sigma$ be an automorphism from $K$ to $K$. Then $\sigma$ is a map from $H$ to a subgroup of $K$ as $H$ is a subgroup of $K$. So $\sigma(H) = \{\sigma(h) \mid h \in H\}$ and then the normalizer of $H$ in the automorphism of $K$ is defined as

$$N_{\mathrm{Aut}(K)}(H) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(H) = H\}$$

and the centralizer of $H$ in the automorphism of $K$ is defined as

$$C_{\mathrm{Aut}(K)}(H) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(h) = h, \text{for all } h \in H\}.$$

Then Aut $(K, H) = N_{\mathrm{Aut}(K)}(H)/C_{\mathrm{Aut}(K)}(H)$ is a subgroup of $\mathrm{Aut}(H)$ by Theorem 5.1.1. If $L$ is also a subgroup of $K$ then a $(H, L)$- double coset is a subset $HxL$ of $K$ for some $x \in K$.

**Notation** Let $\mathcal{A}$ be an amalgam. Then for an amalgam $\mathcal{B}$ of the same type as $\mathcal{A}$ denote by $[\mathcal{B}]$ its isomorphism class.

**Theorem 5.2.1. [Goldschmidt's Lemma]** *Let $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ be an amalgam and define the following subgroup of $Aut(C)$.*

$$A^* = \{\phi_1 \alpha {\phi_1}^{-1} | \alpha \in Aut(A, \phi_1(C))\}$$

*and*

$$B^* = \{\phi_2 \beta {\phi_2}^{-1} | \beta \in Aut(B, \phi_2(C))\}.$$

*Then the isomorphism classes of amalgams of type $\mathcal{A}$ are in one-to-one correspondence with the $(A^*, B^*)$-double cosets in $Aut(C)$.*

*Proof.* Let $\mu \in \mathrm{Aut}(C)$ and define $\mathcal{A} = (A, B, C, \phi_1, \mu\phi_2)$. Consider the map

$$F : A^* \setminus \mathrm{Aut}(C)/B^* \longrightarrow \mathcal{C}(\mathcal{A})$$

$$A^*\mu B^* \longmapsto [\mathcal{A}_\mu]$$

where $A^* \setminus \mathrm{Aut}(C)/B^*$ denote the $(A^*, B^*)$-double cosets in $\mathrm{Aut}(C)$. First we will show that $F$ is well defined. Suppose that $A^*\mu B^* = A^*\delta B^*$.Then there exist $\alpha \in \mathrm{Aut}(A, \phi_1(C))$ and $\beta \in \mathrm{Aut}(B, \phi_2(C))$ such that

$$\mu = (\phi_1\alpha{\phi_1}^{-1})^{-1}\delta(\phi_2\beta{\phi_2}^{-1}).$$

Hence the amalgam $\mathcal{A}$ and $\mathcal{A}_\mu$ are isomorphic as the following diagram commutes.

$$\begin{array}{ccccccc}
A & \xleftarrow{\phi_1} & C & \xrightarrow{\mu} & C & \xrightarrow{\phi_2} & B \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \phi_1\alpha{\phi_1}^{-1}} & & \downarrow{\scriptstyle \phi_2\beta{\phi_2}^{-1}} & & \downarrow{\scriptstyle \beta} \\
A & \xleftarrow[\phi_1]{} & C & \xrightarrow[\mu]{} & C & \xrightarrow[\phi_2]{} & B
\end{array}$$

Therefore, $F(A\mu B) = F(A\delta B)$. Suppose that $[\mathcal{A}_\mu] = [\mathcal{A}_\delta]$. Then the triple of isomorphism $(\alpha, \gamma, \beta)$ makes the following diagram commute.

$$\begin{array}{ccccc}
A & \xleftarrow{\phi} & C & \xrightarrow{\mu\phi_2} & B \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} \\
A & \xleftarrow[\phi_1]{} & C & \xrightarrow{\gamma\phi_2} & B
\end{array}$$

Then,

$$\mu = \gamma\delta\phi_2\beta^{-1}{\phi_2}^{-1} = (\phi_1\alpha{\phi_1}^{-1})\delta(\phi_2\beta^{-1}{\phi_2}^{-1})$$

Thus, $A\mu B = A\delta B$ and so $F$ is one-to-one.

Suppose that $\mathcal{A}'$ is an amalgam of the same type of $\mathcal{A}$. Then by Lemma 3.3 $\mathcal{A}'$ is

isomorphic to $\mathcal{A}_\epsilon$, for some $\epsilon \in$ Aut $(C)$. So, $F(A\epsilon B) = [\mathcal{A}'] = [\mathcal{A}_\epsilon]$. This shows that $F$ is onto and hence, a bijection. $\square$

Goldschmidt's Lemma can be found in [11].

**Example 5.2.1.** Consider the amalgam $\mathcal{A} = (S_n, S_n, S_{n-1}, \phi_1, \phi_2)$ where, $\phi_i$ is an identity map from $S_{n-1}$ to $S_n$ for $i = 1, 2$ and $n$ is a positive integer. Then $\phi_i(S_{n-1}) = S_{n-1}$ and $\phi_i(C) = C$ for $i = 1, 2$. Hence,

$$\begin{aligned} \text{Aut}(S_n, \phi_1(C)) &= \text{Aut } (S_n, S_{n-1}) \\ &= \frac{N_{\text{Aut}(S_n)}(S_{n-1})}{C_{\text{Aut}(S_n)}(S_{n-1})} \end{aligned} \tag{5.1}$$

by the Theorem 5.1.1. Also the Theorem 2.3.1 says that $\text{Aut}(S_n) = S_n$ unless $n = 6$. Therefore,

$$\text{Aut}(S_n, S_{n-1}) = \frac{N_{S_n}(S_{n-1})}{C_{S_n}(S_{n-1})}$$

Next we need to show that $N_{S_n}(S_{n-1}) = S_{n-1}$. Clearly, $S_{n-1} \subseteq N_{S_n}(S_{n-1})$. To show that $N_{S_n}(S_{n-1}) \subseteq S_n$, let $\tau \in S_n \setminus S_{n-1}$. Then $n\tau = i \neq n$. Let $j \in \{1, ..., n\}$ such that $j \neq i$. Thus,

$$\begin{aligned} \tau^{-1}(ij)\tau &= (i\tau j\tau) \\ &= (nj\tau) \notin S_{n-1} \end{aligned}$$

as $n$ fixes in $S_{n-1}$. So $\tau \notin N_{S_n}(S_{n-1})$. This implies that $S_{n-1} \subseteq N_{S_n}(S_{n-1})$. We know that $C_{S_n}(S_{n-1}) \subseteq N_{S_n}(S_{n-1})$. Since $C_{S_n}(S_{n-1}) = C_{S_{n-1}}(S_{n-1})$,

$$C_{S_{n-1}}(S_{n-1}) = Z(S_{n-1}) = \{1\}, n \geq 4.$$

So, $\text{Aut}(S_n, S_{n-1}) \cong S_{n-1} = \text{Sym}(1, ..., n-1)$. Also, $\text{Aut}(S_{n-1}) = S_{n-1}$ for $n \neq 2, 3, 6, 7$.

Then $A^* = S_{n-1}, B^* = S_{n-1}$ and $\mathrm{Aut}(C) = \mathrm{Aut}(S_{n-1}) = S_{n-1}$.

Then the double cosets,

$$\begin{aligned} A^* \setminus \mathrm{Aut}(C)/B^* &= S_{n-1} \setminus S_{n-1}/S_{n-1} \\ &= \{S_{n-1}1S_{n-1}\}. \end{aligned}$$

Hence there is only one double coset. Therefore there is one isomorphic class of amalgam of type $\mathcal{A}$ when $n \neq 2, 3, 6, 7$.

Consider $n = 6$. Then by Theorem 2.3.3, Aut $(S_n) = 2 : S_n$. Hence $N_{\mathrm{Aut}(S_n)}(S_{n-1}) = S_{n-1}$ and $C_{\mathrm{Aut}(S_n)}(S_{n-1}) = \{1\}$. Then the equation 5.1 gives $\mathrm{Aut}(S_n, S_{n-1}) = S_{n-1}$. Then the double cosets,

$$\begin{aligned} A^* \setminus \mathrm{Aut}(C)/B^* &= S_{n-1} \setminus 2 : S_n/S_{n-1} \\ &= S_5 \setminus 2 : S_5/S_5 \\ &= \{S_5 1 S_5, S_5 x S_5\} \text{ for } x \notin S_5. \end{aligned}$$

If $n = 7$, $\mathrm{Aut}(S_{n-1}) = \mathrm{Aut}S_6 = 2 : S_6$ by Theorem 2.3.3. Then $A^* = S_6$ and $B^* = S_6$. Then the double cosets,

$$\begin{aligned} A^* \setminus \mathrm{Aut}(C)/B^* &= S_6 \setminus 2 : S_6/S_6 \\ &= \{S_6 1 S_6, S_6 x S_6\} \text{ for } x \notin S_6. \end{aligned}$$

Therefore there are two double cosets when $n = 7$ and $n = 6$. Hence we have two isomorphic class of amalgam of type $\mathcal{A}$ when $n = 7, 6$.

## 5.3 Isospectral Groups

**Definition 5.3.1.** Let $G$ be a group. Then the number of subgroups of $G$ of index $n$ is denoted by $a_n(G)$. Let $H$ be a group, then $G$ and $H$ are called *isospectral* if, and only if, $a_n(G) = a_n(H)$ for all natural numbers $n$.

**Definition 5.3.2.** Let $G$ be a group and suppose that $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ is an amalgam. Define

$$\mathrm{Hom}(\mathcal{A}, G) = \{\psi \mid \psi \text{ is a representation of } \mathcal{A} \text{ into } G\}.$$

Let $\theta \in \mathrm{Hom}(C, G)$, where $\mathrm{Hom}(C, G)$ is the set of homomorphisms from $C$ to $G$. Then we say that $(\varphi_1, \varphi_2) \in \mathrm{Hom}(\mathcal{A}, G)$ *extends* $\theta$ if $\theta = \phi_1\varphi_1 = \phi_2\varphi_2$ for $\varphi_1, \varphi_2 \in \mathrm{Hom}(\mathcal{A}, G)$. *Then*

$$\mathrm{Hom}_\theta(\mathcal{A}, G) = \{\psi \in \mathrm{Hom}(\mathcal{A}, G) \mid \psi \text{ extends } \theta\}.$$

**Lemma 5.3.1.** *Let $G = \langle x \rangle$ be a cyclic group of order $n$ Then for each divisor $m$ of $n$, there is a unique subgroup $G$ with order $m$. This subgroup is a cyclic group generated by $x^{n/m}$, and these are all the subgroups of $G$.*

*Proof.* Let $H$ be a subgroup of $G$, and let $k$ be the smallest positive integer such that $x^k \in H$. We claim that $x^l \in H$ if, and only if, $k$ divides $l$. If $l = kq$, the $x^l = (x^k)^q \in H$. Conversely, suppose that $x^l \in H$ and let $l = kq+r$, with $0 \leq r < k$. Then $x^r = x^{l-kq} \in H$, and so $r = 0$. In particular, $x^n = 1 \in H$, so $k$ divides $n$. Putting $m = n/k$, we can see that $H$ is generated by $x^{n/m}$, and that $H$ has $m$ elements $1 = x^0, x^k, x^{2k}, ..., x^{(m-1)k}$. □

**Lemma 5.3.2.** *If $H$ is a subgroup of a cyclic group $C$, and $\gamma \in Aut(C)$, then $\gamma(H) = H$.*

*Proof.* We can use the fact that a subgroup of a cyclic group is uniquely determined by

its order from the Lemma 5.3.1. Since $\gamma(H)$ and $H$ have the same number of elements, they must be the same. Hence, $\mid H \mid = \mid \gamma(H) \mid$. Therefore, $H = \gamma(H)$. □

**Lemma 5.3.3.** *Let $G = \mathrm{Sym}(n)$. Let $C$ be a cyclic group. Suppose that $\theta \in Hom(C, G)$. Then the generators for $\theta(C)$ in $G$ all have the same cycle type and so are conjugate in $G$.*

*Proof.* Let $C$ be a cycle of order $m$ and $x$ be a generator of $C$. Consider $\theta(x) \in G$. Then the order of $\theta(x)$ divides $m$. Write $l$ for the order of $\theta(x)$. Let $\theta(x)$ has a cycle shape $1^{a_1}2^{a_2}....$ Then the order of $\theta(x) = \mathrm{lcm}\{i \mid a_i \neq 0\} = l$. i.e. $\theta(x)^l = 1$. That means $\theta(x)^l = 1$. Write $\theta(x) = c_{1,1}c_{1.2}...c_{1,a_1}c_{2,1}c_{2,a_2}....$ Suppose $c_{i,j}$ as a cycle of length $i$.

$$1 = \theta(x)^l = c_{1,1}^l...c_{1,a_1}^l c_{2,1}^l...c_{2,a_2}^l...$$

where $c_{i,j}$ denote the conjugacy class. Hence, $c_{i,j}^l = 1$ for all $i, j$. Thus $i \mid l$ for all $i$ such that $a_i \neq 0$.

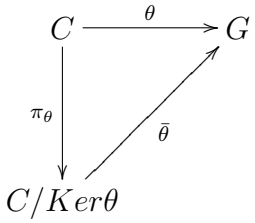
Now look at the cycle shape of $\theta(x)^k$.

$$\theta(x)^k = c_{1,1}^k...c_{1,a_1}^k c_{2,1}^k...c_{2,a_2}^k...$$

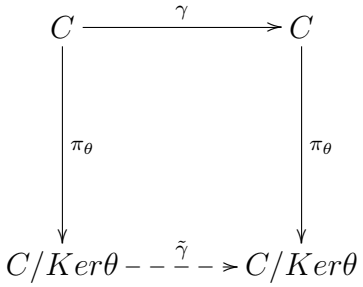
Let $i$ be such that $a_i \neq 0$. Consider $c_{i,1}^k$ is a cycle shape of length $i$. Thus, $\gcd(k, i) = 1$. Now $i \mid l$ since $l = \mathrm{lcm}\{i \mid a_i \neq 0\}$. So, if s divide $k$ and $i$ then $s$ divide $k$ and $l$, but $\gcd(l, k) = 1$. This implies that $s = 1$. Hence, $c_{i,1}^k$ is a cycle of length $i$. Therefore $\theta(x)^k$ has the same cycle shape as $\theta(x)$. □

Let $\theta \in \mathrm{Hom}(C, G)$. Let $\pi_\theta : C \longrightarrow C/\mathrm{Ker}\ \theta$ be a projection map and $\bar{\theta} : C/\mathrm{Ker}\ \theta \longrightarrow$

$\theta(C)$ be the unique homomorphism which makes the following diagram commutes.




Define $\tilde{\theta} : N_G(\theta(C)) \longrightarrow \text{Aut}(C/\text{ Ker } \theta)$ by $\tilde{\theta}(x) = \bar{\theta}c_x\bar{\theta}^{-1}$,where $c_x$ is the automorphism of $\theta(C)$ induced by conjugation by $x$. Next, take $\gamma \in \text{Aut}(C)$ such that $\gamma(\text{ Ker } \theta) =$ Ker $\theta$. Define $\tilde{\gamma}$ such that $\pi_\theta\tilde{\gamma}{\pi_\theta}^{-1} = \gamma$. Then we have the following commutative diagram




and hence $\tilde{\gamma} \in \text{Aut}(C/\text{Ker } \theta)$.

**Recall.** Let $\mathcal{A} = (A_1, A_2, B, \phi_1, \phi_2)$ be an amalgam. Then $\mathcal{A}^\gamma$ is defined as $(A_1, A_2, B, \phi_1, \gamma\phi_2)$, where $\gamma \in$ Aut $(B)$.

**Lemma 5.3.4.** *Let $\theta \in \text{Hom}(C, G)$ and $\gamma \in \text{Aut}(C)$ such that $\gamma(\text{ Ker } \theta) = \text{Ker } \theta$. If there exists $x \in N_G(\theta(C))$ such that $\tilde{\theta}(x) = \tilde{\gamma}^{-1}$ then there exists a bijection between $\text{Hom}_\theta(\mathcal{A}, G)$ and $\text{Hom}_\theta(\mathcal{A}^\gamma, G)$.*

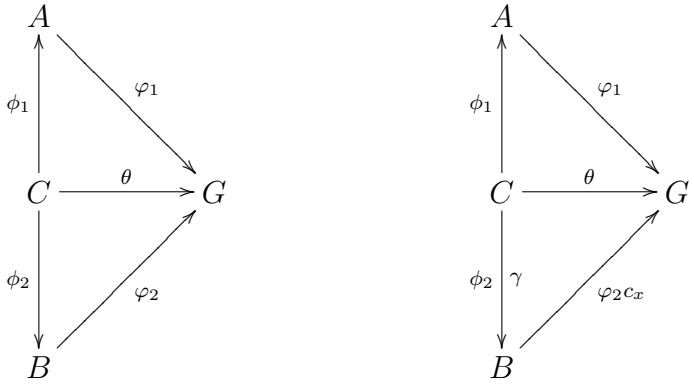
*Proof.* Define two maps:

$$\sigma_1 : \text{Hom}_\theta(\mathcal{A}, G) \longrightarrow \text{Hom}_\theta(\mathcal{A}^\gamma, G) \text{ by } (\varphi_1, \varphi_2) \longmapsto (\varphi_1, \varphi_2 c_x)$$

and

$$\sigma_2 : \text{Hom}_\theta(\mathcal{A}^\gamma, G) \longrightarrow \text{Hom}_\theta(\mathcal{A}, G) \text{ by } (\varphi_1, \varphi_2) \longmapsto (\varphi_1, \varphi_2 c_{x^{-1}}).$$

Then we have the following two commutative diagrams,




We need to show that these two maps are well defined. So, we will show that $(\varphi_1, \varphi_2 c_x) \in \mathrm{Hom}_\theta(\mathcal{A}^\gamma, G)$. Consider,

$$\begin{aligned}
\gamma\phi_2\varphi_2 c_x &= \gamma\theta c_x = \gamma\pi_\theta\bar{\theta}c_x = \gamma\pi_\theta\bar{\theta}c_x\bar{\theta}^{-1}\bar{\theta} \\
&= \gamma\pi_\theta\tilde{\theta}(x)\bar{\theta} = \gamma\pi_\theta\tilde{\gamma}^{-1}\bar{\theta}(\text{ as } \tilde{\theta}(x) = \tilde{\gamma}^{-1}) \\
&= \gamma\gamma^{-1}\pi_\theta\bar{\theta} \text{ as } \pi_\theta\tilde{\gamma} = \gamma\pi_\theta \\
&= \pi_\theta\bar{\theta} = \theta.
\end{aligned}$$

Hence, we infer that $\sigma_1$ is well defined. Similarly, we can show that $\sigma_2$ is well defined. □

**Definition 5.3.3.** Let $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ be an amalgam. Then we say that $\mathcal{A}$ is a *cyclic amalgam* if $C$ is a cyclic group

**Lemma 5.3.5.** *Let $\mathcal{A} = (A, B, C, \phi_1, \phi_2)$ be a cyclic amalgam. Then there is a bijection between $\mathrm{Hom}(\mathcal{A}, \mathrm{Sym}(n))$ and $\mathrm{Hom}(\mathcal{A}^\gamma, \mathrm{Sym}(n))$, for all natural numbers $n$ and for all $\gamma \in \mathrm{Aut}(C)$.*

*Proof.* Let $G = \mathrm{Sym}(n)$. Suppose that $\theta \in \mathrm{Hom}(C, G)$. Since $C$ is a cyclic group, $\gamma(\mathrm{Ker}\ \theta) = \mathrm{Ker}\ \theta$ by the Lemma 5.3.2. Also, the generators of $\theta(C)$ in $G$ have the same cycle type and they are conjugate in $G$ by the Lemma 5.3.3. Therefore the

map, $\tilde{\theta} : N_G(\theta(C)) \longrightarrow$ Aut $(C/\text{ Ker } \theta)$ is an isomorphism. Therefore, there exists $x \in N_G(\theta(C))$ such that $\tilde{\theta}(x) = \tilde{\gamma}^{-1}$, for all $\theta \in \text{Hom}(\mathcal{A}, G)$. Then by Lemma 5.3.4, there exists a bijection between $\text{Hom}_\theta(\mathcal{A}, G)$ and $\text{Hom}_\theta(\mathcal{A}^\gamma, G)$.

Let $\Theta \in$ Hom $(\mathcal{A}, G)$. Then $\Theta$ determines $\theta \in$ Hom $(C, G)$ such that $\Theta \in$ Hom $_\theta(C, G)$. Therefore

$$\text{Hom } (\mathcal{A}, G) \subseteq \bigcup_{\theta \in \text{Hom } (C,G)} \text{Hom } _\theta(\mathcal{A}, G).$$

It is easy to see that

$$\text{Hom } (\mathcal{A}, G) \supseteq \bigcup_{\theta \in \text{Hom } (C,G)} \text{Hom } _\theta(\mathcal{A}, G).$$

Thus, Hom $(\mathcal{A}, G)$ is a disjoint union of Hom $_\theta(\mathcal{A}, G)$.

$$\text{i.e. Hom } (\mathcal{A}, G) = \bigsqcup_{\theta \in \text{ Hom } (C,G)} \text{Hom } _\theta(\mathcal{A}, G).$$

Similarly, we can see that

$$\text{Hom } (\mathcal{A}^\gamma, G) = \bigsqcup_{\theta \in \text{ Hom } (C,G)} \text{Hom } _\theta(\mathcal{A}^\gamma, G).$$

Hence, there is a bijection between Hom $(\mathcal{A}, G)$ and Hom $(\mathcal{A}^\gamma, G)$. □

Let $G$ be a group and $H$ a subgroup of index $n$ in $G$. Then $G$ permutes the right cosets of $H$ by right multiplication. Let $H$ as 1 and remaining $n-1$ cosets with $2, ..., n$ in any order. Then we have a homomorphism $\kappa : G \longrightarrow \text{Sym } (n)$. It is clear that $\kappa(G)$ is transitive. Denote

$$t_n(G) =\mid \{\kappa : G \longrightarrow \text{Sym } (n) \mid \kappa(G) \text{ is transitive } \} \mid .$$

Then we have $a_n(G) = \dfrac{t_n(G)}{(n-1)!}$.

Denote $h_n(G) =\mid \text{Hom } (G, \text{Sym } (n)) \mid$ . Then $h_0 = 1$.

**Lemma 5.3.6.** *For a group $G$,*

$$h_n(G) = \sum_{m=1}^{n} \binom{n-1}{m-1} t_m(G) h_{n-m}(G).$$

*Proof.* Denote the number of representations of $G$ in Sym $(n)$ such that the orbit of 1 has length $m$, by $h_{n,m}(G)$. So we have $\binom{n-1}{m-1}$ ways to choose the orbit of 1 for given $m$. Also, $t_m(G)$ ways for $G$ to act on this orbit. Hence, there are $h_{n-m}(G)$ ways for $G$ to act on its complement in $\{1, ..., n\}$. Thus, we have

$$h_{n,m}(G) = \binom{n-1}{m-1} t_m(G) h_{n-m}(G).$$

Therefore, the number of homomorphisms from $G$ into Sym $(n)$ is,

$$\begin{aligned} h_n(G) &= \sum_{m=1}^{n} h_{n,m}(G) \\ &= \sum_{m=1}^{n} \binom{n-1}{m-1} t_m(G) h_{n-m}(G). \end{aligned}$$

□

**Lemma 5.3.7.** *Let $G$ be a group. Then*

$$a_n(G) = \frac{1}{(n-1)!} h_n(G) - \sum_{m=1}^{n-1} \frac{1}{(n-m)!} h_{n-m}(G) a_m(G).$$

*Proof.* Note that $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$. We have $t_n(G) = (n-1)! a_n(G)$.

Then

$$\begin{aligned} h_n(G) &= \sum_{m=1}^{n} \frac{(n-1)!}{(k-1)!(n-m)!} t_n(G) h_{n-m}(G) \\ &= \sum_{m=1}^{n} \frac{(n-1)!}{(m-1)!(n-m)!} (m-1)! a_m(G) h_{n-m}(G) \\ &= (n-1)! \sum_{m=1}^{n} \frac{1}{(n-m)!} a_m(G) h_{n-m}(G) \\ &= (n-1)! \left[ \sum_{m=1}^{n-1} \frac{1}{(n-m)!} a_m(G) h_{n-m}(G) + a_n h_0 \right]. \end{aligned}$$

as $h_0 = 1, a_n(G) = \frac{1}{(n-1)!}h_n(G) - \sum_{m=1}^{n-1} \frac{1}{(n-m)!}h_{n-m}(G)a_m(G)$. [8] □

**Corollary 5.3.1.** *For all natural numbers $n$ and all $\gamma \in Aut\,(C)$, there is a bijection between $Hom(G(\mathcal{A}), Sym(n))$ and $Hom(G(\mathcal{A}^\gamma), Sym(n))$.*

*Proof.* Since there is a bijection between $\mathrm{Hom}(\mathcal{A}, \mathrm{Sym}(n))$ and $\mathrm{Hom}(\mathcal{A}^\gamma, \mathrm{Sym}(n))$ by the Lemma 5.3.4 and also, $\mathrm{Hom}(G(\mathcal{A}), \mathrm{Sym}(n))$ is isomorphic to $\mathrm{Hom}(\mathcal{A}, \mathrm{Sym}(n))$ the result follows. □

**Theorem 5.3.1.** *If $\mathcal{A}$ and $\mathcal{A}'$ are cyclic amalgams of the same type, then their universal completions are isospectral.*

*Proof.* Assume that $\mathcal{A}$ and $\mathcal{A}'$ are cyclic amalgams of the same type. Then there exists $\gamma \in \mathrm{Aut}(C)$ such that $\mathcal{A}'$ and $\mathcal{A}^\gamma$ are isomorphic by Lemma 5.3.7. Then by Corollary 5.3.1, $h_n(G(\mathcal{A})) = h_n(G(\mathcal{A}'))$ for all $n$. Lemma 5.3.7 says that $a_1(G(\mathcal{A})) = 1 = a_1(G(\mathcal{A}^\gamma))$ . Now we want to prove by induction that $a_n(G(\mathcal{A})) = a_n(G(\mathcal{A}^\gamma))$ for all $n$. Suppose that $a_m(G((A)) = a_m(G(\mathcal{A}^\gamma))$ for all $m < n$. Then by Corollary 5.3.1, $h_n(G(\mathcal{A})) = h_n(G(\mathcal{A}^\gamma))$. Also, $h_{n-m}(G(\mathcal{A})) = h_{n-m}(G(\mathcal{A}^\gamma))$ for all $m$. Then by induction hypothesis, $a_m(G(\mathcal{A})) = a_m(G(\mathcal{A}^\gamma))$. Thus by Lemma 5.3.7 $G(\mathcal{A})$ and $G(\mathcal{A}^\gamma)$ are isospectral. □

# Bibliography


[1] Fraleigh, John B., *A First Course in Abstract Algebra*, Narosa Publishing House, New Delhi, Third edition, 1997.

[2] Rose, John S., *A course on group theory*, Dover Publications, Inc., New York, 1994.

[3] Ashbacher, M., *Finite Group Theory*, volume 10 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, second edition, 2000.

[4] Suzuki, Michio, *Group Theory I*, volume 247 ,Springer-Verlag, Berlin, 1982.

[5] Suzuki, Michio, *Group Theory II*, volume 248, Springer-Verlag, Berlin, 1982.

[6] Johnson, D. L., *Presentations Groups*, Cambridge University Press, Cambridge, 1976.

[7] Derek F. Holt, Bettina Eick, Eamonn A. O'Brien, *Handbook of Computational Group Theory*, Chapman and Hall/CRC press, London, 2005.

[8] Alexander Lubotzky, Dan Segal, *Subgroup Growth*, Basel, Switzerland, 2003.

[9] Roger C. Lyndon, Paul E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, New York, 1976.

[10] Christopher Parker, Peter Rowley, *Symplectic Amalgams*, Springer Monographs in Mathematics, Springer- Verlag London Ltd., 2002.

[11] David M. Goldschmidt, *Automorphisms of Trivalent Graphs, Ann. of Math.* (2); 111(2): 377-406, 1980.

[12] Christopher Hiller, Darren Rhea, *Automorphisms of Finite Abelian Groups*, unpublished.

[13] Derek J. S. Robinson, *A Course in the Theory of Groups*, A Graduate Texts in Mathematics, Springer-Verlag, New York, Second edition, 1996.

[14] C.W. Parker, *Amalagams and Isospectral Groups*, unpublished.

[15] Lecture Notes- Group Theory (University of Peradeniya, Sri Lanka), unpublished.