

การกระทำโดยอัตตัตถฐานบนคู่ของกรุป



นายประพันธ์พงศ์ พงศ์ศรีเอี่ยม

สถาบันวิทยบริการ
วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2549

ISBN : 974-14-1817-5

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

ACTION BY AUTOMORPHISMS ON THE DUAL OF A GROUP



Mr. Prapanpong Pongsriiam

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics

Department of Mathematics
Faculty of Science

Chulalongkorn University


Academic Year 2006

ISBN : 974-14-1817-5


Copyright of Chulalongkorn University

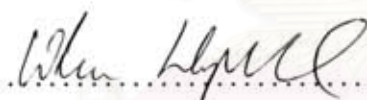
Thesis Title	Action by automorphisms on the dual of a group
By	Mr. Prapanpong Pongsriiam
Field of Study	Mathematics
Thesis Advisor	Assistant Professor Wicharn Lewkeeratiyutkul, Ph.D.
Thesis Co-advisor	Professor Roberto Conti, Ph.D.

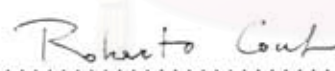
Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree



..... Dean of the Faculty of Science
(Professor Piamsak Menasveta, Ph.D.)

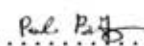
THESIS COMMITTEE


..... Chairman
(Assistant Professor Imchit Termwuttipong, Ph.D.)


..... Thesis Advisor
(Assistant Professor Wicharn Lewkeeratiyutkul, Ph.D.)

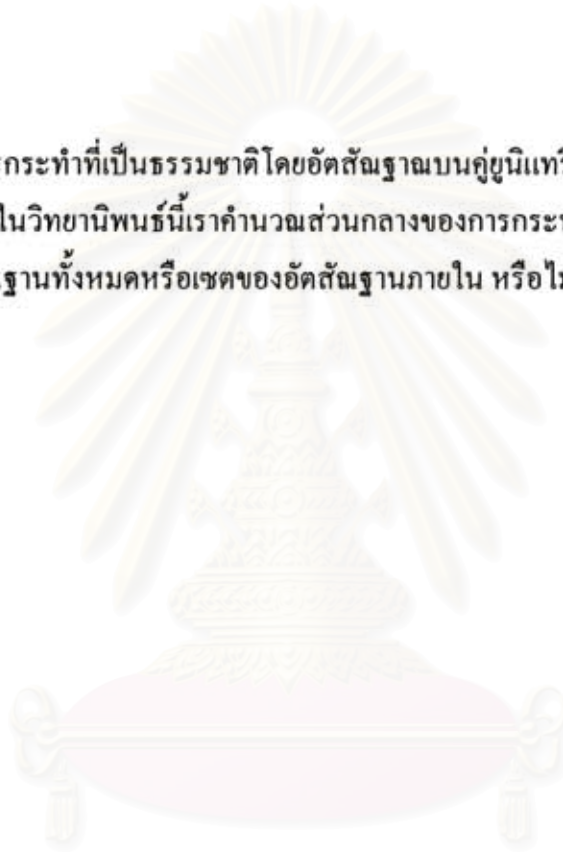

..... Thesis Co-advisor
(Professor Roberto Conti, Ph.D.)


..... Member
(Associate Professor Ajchara Harnchoowong, Ph.D.)


..... Member
(Paolo Bertozzini, Ph.D.)

ประพันธ์พงศ์ พงศ์ศรีเอี่ยม : การกระทำโดยอัตโนมัติบนคู่ของกลุ่ม (ACTION BY
 AUTOMORPHISMS ON THE DUAL OF A GROUP) อาจารย์ที่ปรึกษา: ผศ.ดร. วิชาญ
 ลีวเกียรติคุณ, อาจารย์ที่ปรึกษาร่วม : Professor Roberto Conti, 69 หน้า
 ISBN 947-14-1817-5

การศึกษาการกระทำที่เป็นธรรมชาติโดยอัตโนมัติบนคู่ของกลุ่มเป็นปัญหาที่น่าสนใจปัญหาหนึ่ง ในวิทยานิพนธ์นี้เรากำหนดส่วนกลางของการกระทำนี้และตัดสินใจว่ามันเท่ากับ เซตของอัตโนมัติทั้งหมดหรือเซตของอัตโนมัติภายใน หรือไม่ ในหลายกรณี



สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา ... คณิตศาสตร์ ...
 สาขาวิชา ... คณิตศาสตร์ ...
 ปีการศึกษา 2549

ลายมือชื่อนิสิต ...
 ลายมือชื่ออาจารย์ที่ปรึกษา ...
 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม ...

4772362823 : MAJOR MATHEMATICS

KEY WORDS : REPRESENTATION OF FINITE GROUP / AUTOMORPHISM / THE UNITARY DUAL OF A GROUP

PRAPANPONG PONGSRIIAM : ACTION BY AUTOMORPHISMS ON THE DUAL OF A GROUP. THESIS ADVISOR : ASSIST. PROF. WICHARN LEWKEERATIYUTKUL, Ph.D. THESIS CO-ADVISOR : PROF. ROBERTO CONTI, Ph.D., 69 pp. ISBN 974-14-1817-5

It is an interesting problem to study the natural action by automorphisms on the unitary dual of a group G . In this thesis, we compute the kernel of the action and determine whether it is equal to $\text{Inn } G$ or $\text{Aut } G$ in a number of cases.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Department : ...Mathematics...

Field of study : ...Mathematics...

Academic year :2006.....

Student's signature : *Prap Pongsriiam*

Advisor's signature : *Wicharn Lewkeeratiyutkul*

Co-advisor's signature : *Roberto Conti*

ACKNOWLEDGEMENTS

I wish to express my gratitude to many people who support me accomplish this thesis.

Foremost among these people are Assistant Professor Wicharn Lewkeeratiyutkul and Professor Roberto Conti, my thesis advisors. They take care of entire thesis manuscript and guide me how to prepare this thesis. They check both grammatical error and academic content. I am very impressed in these invaluable assistances and advices. Moreover, I would like to thank them for promoting far-sighted knowledge in mathematics. Above all academic support, they also suggest studying abroad preparation and give me the letters of recommendation which help me obtain teaching assistantship from Pennsylvania State University.

It is a pleasure to acknowledge Associate Professor Ajchara Harnchoowong who educated me a strong skill and knowledge in Algebra from many course works. This knowledge is an important background for conducting this thesis.

I also would like to thank Assistant Professor Imchit Termwuttipong, Assistant Professor Nattanard Triphop, and Professor Yupaporn Kemprasit. They taught me fundamental knowledge in conducting mathematics research when I was an undergraduate. This knowledge is very helpful for doing this thesis.

In addition, I would like to thank Dr. Paolo Bertozzini, the thesis committee's members from Thammasat University, for sacrificing his time in the thesis examination.

Special thanks for preparing this thesis go to Tammatada Khemaratchatakumthorn who teaches me using LATEX program and helps me type this thesis.

Last but not least, I am grateful to DPST who grant me the scholarship.

CONTENTS

	page
ABSTRACT IN THAI	iv
ABSTRACT IN ENGLISH	v
ACKNOWLEDGEMENTS	vi
CONTENTS	vii
CHAPTER	
I INTRODUCTION AND STATEMENT OF RESULTS	1
II REPRESENTATION OF FINITE GROUPS	4
III ACTION BY AUTOMORPHISMS ON THE DUAL OF A GROUP	10
IV DIHEDRAL GROUPS D_n	18
V SYMMETRIC GROUPS S_n	29
VI ALTERNATING GROUPS A_n	36
VII SEMIDIRECT PRODUCT $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$	49
REFERENCES	60
APPENDIX	61
VITA	69

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER I

Introduction and statement of results

A topological group is *complete* if it has a trivial center and every continuous automorphism is inner. In other words, a group G is complete if $Z(G) = \{1\}$ and $\text{Aut}(G) = \text{Inn}(G)$, where $\text{Aut}(G)$ and $\text{Inn}(G)$ denote the set of continuous automorphisms of G and the set of inner automorphisms of G , respectively. Finite complete groups have been extensively studied in the past, see e.g. Suzuki [14].

In [1], Burnside defined $\text{Aut}_{\widehat{G}}(G)$ and $\text{Aut}_C(G)$ to be the set of all automorphisms which preserve equivalence classes of irreducible representations of G , and the set of all automorphisms which preserve conjugacy classes of G , respectively. These definitions are first defined for finite groups, but carried over to more general settings. In general one has the inclusions, for every locally compact group G ,

$$\text{Inn}(G) \subseteq \text{Aut}_{\widehat{G}}(G) \subseteq \text{Aut}_C(G) \subseteq \text{Aut}(G). \quad (1.1)$$

In [2], Conti, D'Antoni, and Geatti show that $\text{Inn}(G) = \text{Aut}_{\widehat{G}}(G)$ for a certain class of connected Lie groups. From this result, one also recovers the fact that $\text{Inn}(G) = \text{Aut}_{\widehat{G}}(G)$ for every compact connected group G . Related work is also studied by Hertweck in [10]. He examined whether $\text{Inn}(G) = \text{Aut}_C(G)$ for certain classes of finite solvable groups whose Sylow subgroups are abelian. His work [10] has a connection with the isomorphism problem for integral group rings and with certain versions of the Zassenhaus's conjecture that group bases of $\mathbb{Z}G$ are rationally conjugate. He also mentioned in the introduction that Feit and Seitz, using the classification of finite simple groups, showed that $\text{Inn}(G) = \text{Aut}_c(G)$ for a finite simple group G ([4] Theorem c).

In this thesis, we investigate the relations among the sets in (1.1) for finite groups.

First, we show that, for any finite group G ,

$$\text{Inn}(G) \trianglelefteq \text{Aut}_{\widehat{G}}(G) = \text{Aut}_C(G) \trianglelefteq \text{Aut}(G). \quad (1.2)$$

After that, we study these relations for certain classes of finite groups, namely, dihedral groups, symmetric groups, and alternating groups. Then we obtain the result that all the group G from these families satisfy the equation

$$\text{Inn}(G) = \text{Aut}_{\widehat{G}}(G). \quad (1.3)$$

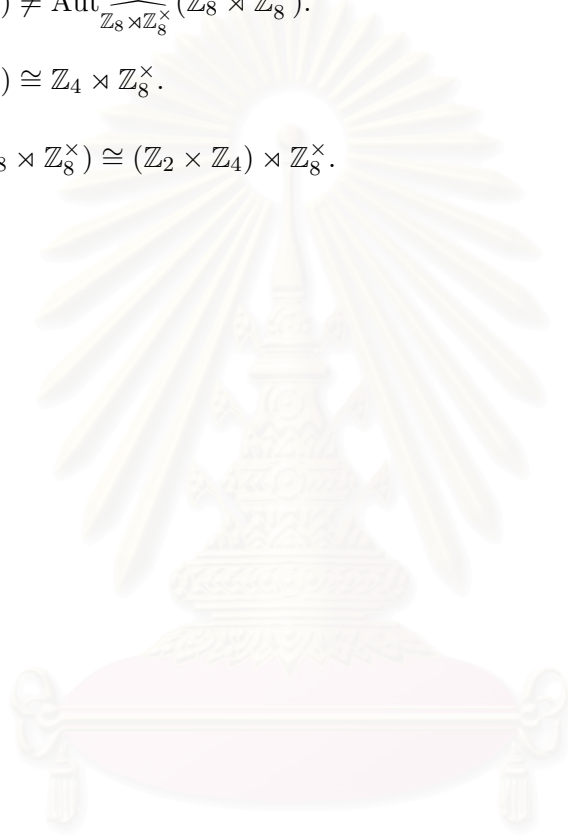
Therefore we also study $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$ which gives us an example of a group which does not satisfy (1.3).

This thesis is organized as follows. In Chapter 2, we introduce general terminologies, and review concepts of representation theory of finite groups. In Chapter 3, we define the action by automorphisms on the dual of a group and prove relation (1.2). In Chapter 4, 5, 6, and 7, we compute $\text{Inn}(G)$, $\text{Aut}_{\widehat{G}}(G)$, and $\text{Aut}(G)$ and determine whether $\text{Inn}(G) = \text{Aut}_{\widehat{G}}(G)$ or $\text{Aut}_{\widehat{G}}(G) = \text{Aut}(G)$ when G is a dihedral group, a symmetric group, an alternating group, and the semi direct product $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$, respectively.

The results of this work are summarized below:

1. $\text{Inn}(D_n) = \text{Aut}_{\widehat{D}_n}(D_n) \neq \text{Aut}(D_n)$ for every $n \geq 4$.
2. $\text{Inn}(D_3) = \text{Aut}_{\widehat{D}_3}(D_3) = \text{Aut}(D_3)$.
3. $\text{Inn}(D_n) \cong D_n$ if $n \geq 3$ and n is odd.
4. $\text{Inn}(D_n) \cong D_{\frac{n}{2}}$ if $n \geq 6$ and n is even.
5. $\text{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
6. $\text{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ for every $n \geq 3$.
7. $\text{Inn}(S_n) = \text{Aut}_{\widehat{S}_n}(S_n) = \text{Aut}(S_n) \cong S_n$ for every $n \geq 3$, $n \neq 6$.
8. $\text{Inn}(S_6) = \text{Aut}_{\widehat{S}_6}(S_6) \neq \text{Aut}(S_6)$.
9. $\text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n) \neq \text{Aut}(A_n)$ for every $n \geq 4$.

10. $\text{Inn}(A_n) \cong A_n$ for every $n \geq 4$.
11. $\text{Aut}(A_n) \cong S_n$ for every $n \geq 4$, $n \neq 6$.
12. Every automorphism of A_n is the restriction of an inner automorphism of S_n for every $n \geq 4$, $n \neq 6$.
13. $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \neq \text{Aut}_{\widehat{\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times}}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$.
14. $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_8^\times$.
15. $\text{Aut}_{\widehat{\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times}}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_8^\times$.



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER II

Representations of finite groups

In this chapter, we will give basic terminology related to representation theory of finite groups. Throughout this thesis, \mathbb{C} is the set of all complex numbers, and unless stated otherwise, all vector spaces are over \mathbb{C} and finite dimensional, and all groups are finite

$$\begin{aligned}M_d(\mathbb{C}) &= \{[a_{ij}]_{d \times d} \mid a_{ij} \in \mathbb{C} \text{ for all } i, j \in \{1, 2, \dots, d\}\}, \\GL_d(\mathbb{C}) &= \{A \in M_d(\mathbb{C}) \mid A \text{ is invertible}\}, \\U_d(\mathbb{C}) &= \{A \in M_d(\mathbb{C}) \mid AA^* = A^*A = I\} \text{ where } A^* = (\overline{A})^t.\end{aligned}$$

We call $GL_d(\mathbb{C})$ the general linear group of degree d , and $U_d(\mathbb{C})$ the unitary group of degree d .

Definition 2.1. A **matrix representation** of a group G is a group homomorphism $X : G \rightarrow GL_d(\mathbb{C})$. The parameter d is called the **degree**, or **dimension**, of the representation and is denoted by $\deg X$.

For any vector space V , define

$$GL(V) = \{T : V \rightarrow V \mid T \text{ is an invertible linear operator}\}.$$

If $\dim V = d$, then $GL_d(\mathbb{C}) \cong GL(V)$ as groups. Therefore, we can also think of representations in this term. This is the idea of G -module.

Definition 2.2. Let V be a vector space and G be a group. We say that V is a **G-module** if there is a group homomorphism

$$\rho : G \rightarrow GL(V).$$

Equivalently, V is a G -module if there is a multiplication, gv , of elements of V by elements of G such that

1. $gv \in V$,
2. $g(cv + dw) = c(gv) + d(gw)$,
3. $(gh)v = g(hv)$, and
4. $1v = v$

for all $g, h \in G$; $v, w \in V$; and scalars $c, d \in \mathbb{C}$.

We will go back and forth between the notions of matrix representations and G -modules. Each of them has its own advantage. Matrix representation is more concrete, while G -module, as it is more abstract, can give us a cleaner proof.

Definition 2.3. Let V be a G -module. A **submodule** of V is a subspace W that is closed under the action of G , i.e.,

$$w \in W \Rightarrow gw \in W \text{ for all } g \in G.$$

We also say that W is a **G -invariant** subspace. Equivalently, W is a subset of V that is a G -module in its own right. We write $W \leq V$ if W is a submodule of V .

Next, we introduce irreducible representations that will be the building blocks of all the others.

Definition 2.4. A nonzero G -module V is **reducible** if it contains a nontrivial submodule W . Otherwise, V is said to be **irreducible**. Equivalently, V is reducible if it has a basis \mathcal{B} in which every $g \in G$ is assigned a block matrix of the form

$$X(g) = \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}$$

where the $A(g)$ are square matrices, all of the same size, for each $g \in G$, and 0 is a non-empty matrix of zeros.

If V is reducible, then the corresponding representations are said to be reducible.

If V is irreducible, then so do the corresponding representations.

Theorem 2.5 (Maschke's Theorem ([13], p.16)). Let G be a finite group and let V be a nonzero G -module. Then

$$V = W^{(1)} \oplus W^{(2)} \oplus \dots \oplus W^{(k)},$$

where each $W^{(i)}$ is an irreducible G -submodule of V .

Corollary 2.6 ([13], p.17). Let G be a finite group and let X be a matrix representation of G of dimension $d > 0$. Then there is a fixed matrix T such that every matrix $X(g)$, $g \in G$, has the form

$$TX(g)T^{-1} = \begin{pmatrix} X^{(1)}(g) & 0 & \dots & 0 \\ 0 & X^{(2)}(g) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & X^{(k)}(g) \end{pmatrix},$$

where each $X^{(i)}$ is an irreducible matrix representation of G .

Definition 2.7. A representation is **completely reducible** if it can be written as a direct sum of irreducibles.

Note from this definition, Maschke's theorem could be restated as follows : Every representation of a finite group having positive dimension is completely reducible.

Next, we give a concept of isomorphism between G -modules.

Definition 2.8. Let V and W be G -modules.

Then a **G-homomorphism** (or simply a homomorphism) from V into W is a linear transformation $\phi : V \rightarrow W$ such that

$$\phi(gv) = g\phi(v)$$

for all $g \in G$ and $v \in V$.

A **G-isomorphism** is a G -homomorphism $\phi : V \rightarrow W$ that is bijective. In this case, we say that V and W are **G-isomorphic**, or **G-equivalent**, written $V \cong W$. Otherwise we say that V and W are G -inequivalent.

We also have the equivalence between matrix representations in the next definition.

Definition 2.9. Matrix representations X and Y of a group G are **equivalent** if there is an invertible matrix T such that

$$Y(g) = TX(g)T^{-1} \quad \text{for all } g \in G.$$

We write $X \cong Y$ if X and Y are equivalent.

Theorem 2.10 (Schur's Lemma, [13], p.22). Let V and W be two irreducible G -modules. If $\phi : V \rightarrow W$ is a G -homomorphism, then either

(i) ϕ is a G -isomorphism, or

(ii) ϕ is the zero map.

Corollary 2.11 ([13], p.22). Let X and Y be two irreducible matrix representations of G . If T is any matrix such that $TX(g) = Y(g)T$ for all $g \in G$, then either

(i) T is invertible, or

(ii) T is the zero matrix.

Corollary 2.12 ([13], p.23). Let X be an irreducible matrix representation of G over the field of complex numbers. Then the only matrices T that commute with $X(g)$ for all $g \in G$ are those of the form $T = cI$ i.e., scalar multiples of the identity matrix.

Next, we introduce the notion of characters and their inner product which is a powerful tool. Much of the information contained in a representation can be obtained from its character.

Definition 2.13. Let X be a matrix representation. Then the **character of X** is the function $\chi : G \rightarrow \mathbb{C}$ defined by

$$\chi(g) = \text{tr } X(g),$$

where tr denotes the trace of a matrix.

If V is a G -module, then its character is the character of a matrix representation X corresponding to V .

The terminology used for representations will be applied without change to the corresponding characters. For example, if X has character χ , we say that χ is irreducible whenever X is, etc.

Proposition 2.14 ([13], p.31). *Let X be a matrix representation of a group G of degree d with character χ . Then*

$$(i) \quad \chi(1) = d,$$

$$(ii) \quad \chi(hgh^{-1}) = \chi(g) \quad \forall g, h \in G,$$

(iii) *If Y is a representation of G with character ψ , then*

$$X \cong Y \rightarrow \chi(g) = \psi(g) \quad \text{for all } g \in G.$$

In fact, the converse of (iii) in proposition 2.14 is also true (see Corolary 2.18). This can be proved after we have the notion of inner product of characters.

We can think of a character χ of a group $G = \{g_1, \dots, g_n\}$ as a row vector of complex numbers :

$$\chi = (\chi(g_1), \chi(g_2), \dots, \chi(g_n)) \in \mathbb{C}^n.$$

We have the usual inner product in \mathbb{C}^n given by

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = a_1 \bar{b}_1 + a_2 \bar{b}_2 + \dots + a_n \bar{b}_n.$$

Therefore, we may define an inner product of χ and ψ by

$$\chi \cdot \psi = \sum_{g \in G} \chi(g) \overline{\psi(g)}.$$

Nevertheless, for normality (see [13], p.34), we divide this formula by $|G|$. This leads to the definition of character inner product.

Definition 2.15 ([13], p.34). Let χ and ψ be any two functions from a group G to the complex numbers \mathbb{C} . The **inner product of χ and ψ** is

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)}.$$

Proposition 2.16 ([13], p.34). Let χ and ψ be characters. Then

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \psi(g^{-1}).$$

Theorem 2.17 (Character Relations of the First Kind, ([13], p.35)). Let χ and ψ be irreducible characters of a group G . Then

$$\langle \chi, \psi \rangle = \delta_{\chi, \psi} = \begin{cases} 1 & \text{if } \chi = \psi, \\ 0 & \text{if } \chi \neq \psi. \end{cases}$$

Corollary 2.18 ([13], p.37). Let X be a matrix representation of G with character χ . Then

- (i) X is irreducible if and only if $\langle \chi, \chi \rangle = 1$.
- (ii) Let Y be another matrix representation of G with character ψ . Then $X \cong Y$ if and only if $\chi = \psi$.

Theorem 2.19 (Character Relations of the Second Kind, ([13], p.42)). Let K, L be conjugacy classes of G . Then

$$\sum_{\chi} \chi_K \overline{\chi_L} = \frac{|G|}{|K|} \delta_{K, L},$$

where the sum is taken over all irreducible characters of G .

CHAPTER III

Action by automorphisms on the dual of a group

In this chapter we define the action by automorphisms on the dual of a group. Then we give some results which will be used later.

3.1 Group automorphisms

In this section, we recall elementary definitions and theorems in group theory. Their proofs can be found in any standard text such as [3], [6], [9], and [11].

Definition 3.1. *Let G be a group.*

- (i) *A function $f : G \rightarrow G$ is called an **automorphism** of G if f is a bijective homomorphism. The set of all automorphisms of G is denoted by $\text{Aut}(G)$.*
- (ii) *Let $x \in G$, and $\phi_x : G \rightarrow G$ by $g \mapsto xgx^{-1}$. Then ϕ_x is an automorphism of G , called the **inner automorphism induced from x** . The set of all inner automorphisms of G is denoted by $\text{Inn}(G)$. Thus*

$$\text{Inn}(G) = \{\phi_x \mid x \in G\}.$$

*Since $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$, we can define a quotient group which is called the **outer automorphisms group** of G , by*

$$\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G).$$

- (iii) *Let $g, h \in G$. We say that g and h are **conjugate** if there exists $k \in G$ such that $g = khk^{-1}$. Then conjugation is an equivalence relation. The set of all conjugates of g is called the **conjugacy class** of g , and is denoted by K_g . Thus $K_g = \{hgh^{-1} \mid h \in G\}$.*

(iv) The **center** of G , denoted by $Z(G)$, is defined by

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}.$$

Theorem 3.2. *Let G be a group. Then*

- (i) $\text{Aut}(G)$ is a group under composition,
- (ii) $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$,
- (iii) The map $f : G \rightarrow \text{Inn}(G)$ defined by $f(g) = \phi_g$, is an epimorphism whose kernel is $Z(G)$,
- (iv) $Z(G) \trianglelefteq G$ and $G/Z(G) \cong \text{Inn}(G)$,
- (v) $\forall g, h \in G, \phi_g = \phi_h \leftrightarrow g^{-1}h \in Z(G)$,
- (vi) G is abelian $\leftrightarrow Z(G) = G$,
- (vii) G is abelian $\leftrightarrow \text{Inn}(G) = \{\text{id}_G\} \leftrightarrow \forall g \in G, K_g = \{g\}$.

3.2 The dual of a group

Since every representation of a finite group G can be written as a direct sum of irreducibles, it is useful to find the collection \mathcal{A} of all inequivalent irreducible representations of G . Suppose we can find such \mathcal{A} . Then every representation is equivalent to a direct sum of elements in \mathcal{A} . The collection \mathcal{A} is called the dual of G . We give a precise definition of the dual of a group as follows.

Definition 3.3. *Let G be a finite group. The **dual of G** , denoted by \widehat{G} , is defined to be the set of all equivalence classes of irreducible representations of G . That is*

$$\widehat{G} = \{[X]_{\cong} \mid X \text{ is an irreducible representation of } G\},$$

where \cong is the equivalence of representations defined in Definition 2.9.

Remark 3.4. *The dual of a group may not be a group. If G is abelian, then its dual will be a group. In fact, \widehat{G} is a group isomorphic to G if G is a finite abelian group (see [5], p.90). Perhaps, there is no natural condition on G so that the dual of G becomes a group.*

It may seem that there are infinitely many inequivalent irreducible representations, and \widehat{G} contains infinitely many elements. However, \widehat{G} is a finite set, as implied by the following theorem.

Theorem 3.5 ([13], p.40). *Let G be a finite group and suppose*

$$\mathbb{C}[G] \cong \bigoplus_i m_i V^{(i)}$$

where the $V^{(i)}$ form a complete list of pairwise inequivalent irreducible G -modules. Then

- (i) $m_i = \dim V^{(i)}$,
- (ii) $\sum_i (\dim V^{(i)})^2 = |G|$, and
- (iii) the number of $V^{(i)}$ equals the number of conjugacy classes of G .

Theorem 3.5 implies that for a finite group G

- (i) $|\widehat{G}| =$ the number of conjugacy classes of G , and
- (ii) $|G| = \sum_{[X] \in \widehat{G}} (\deg X)^2$.

3.3 Action by automorphisms on the dual of a group

We will give an action of $\text{Aut}(G)$ on \widehat{G} . This action will give us the definition of $\text{Aut}_{\widehat{G}}(G)$ on which our work will emphasize. In this section, unless stated otherwise, χ will be a character of some representation. If there are more than one representations in the context, such as X and Y , we denote their characters by χ_X and χ_Y , respectively.

Lemma 3.6. *Let $\phi \in \text{Aut}(G)$, and $X : G \rightarrow GL_d(\mathbb{C})$ a representation. Let χ be the character of X . Then the following statements hold.*

- (i) $X \circ \phi$ is a representation.
- (ii) $\deg(X \circ \phi) = \deg X$.
- (iii) $\chi_{X \circ \phi} = \chi \circ \phi$ where $\chi_{X \circ \phi}$ are characters of $X \circ \phi$.
- (iv) If $X \circ \phi \cong X$, then $\chi \circ \phi = \chi$.
- (v) If X is irreducible, then $X \circ \phi$ is irreducible.

Proof. (i) Since $\phi : G \rightarrow G$ and $X : G \rightarrow GL_d(\mathbb{C})$, $X \circ \phi : G \rightarrow GL_d(\mathbb{C})$. Next, we prove that $X \circ \phi$ is a group homomorphism. Let $g, h \in G$. Then

$$\begin{aligned} (X \circ \phi)(gh) &= X(\phi(gh)) = X(\phi(g)\phi(h)) \\ &= X(\phi(g))X(\phi(h)) \\ &= (X \circ \phi)(g)(X \circ \phi)(h). \end{aligned}$$

Therefore $X \circ \phi$ is a representation. This proves (i) and (ii).

For (iii),

$$\begin{aligned} \chi_{X \circ \phi}(g) &= \text{tr}(X \circ \phi)(g) = \text{tr} X(\phi(g)) \\ &= \chi(\phi(g)) \\ &= (\chi \circ \phi)(g) \quad \text{for all } g \in G. \end{aligned}$$

This shows $\chi_{X \circ \phi} = \chi \circ \phi$.

(iv) follows immediately from (iii) and Corollary 2.18.

To prove (v), we will use Corollary 2.18(i). Assume that X is irreducible. Then $\langle \chi, \chi \rangle = 1$. From (iii) the character of $X \circ \phi$ is $\chi \circ \phi$, so we would like to show that $\langle \chi \circ \phi, \chi \circ \phi \rangle = 1$.

$$\begin{aligned}
\langle \chi \circ \phi, \chi \circ \phi \rangle &= \frac{1}{|G|} \sum_{g \in G} (\chi \circ \phi)(g) (\chi \circ \phi)(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi(\phi(g)) \chi(\phi(g)^{-1}) \\
&= \frac{1}{|G|} \sum_{h \in G} \chi(h) \chi(h^{-1}) \quad \text{since } \phi \text{ is bijective.} \\
&= \langle \chi, \chi \rangle = 1.
\end{aligned}$$

Therefore $X \circ \phi$ is irreducible. □

Theorem 3.7. Let G be a finite group. Define $\cdot : \text{Aut}(G) \times \widehat{G} \rightarrow \widehat{G}$ by

$$\phi \cdot [X] = [X \circ \phi] \quad \text{for } \phi \in \text{Aut}(G) \text{ and } [X] \in \widehat{G}.$$

Then this function is a group action.

Proof. From Lemma 3.6, we have $[X \circ \phi] \in \widehat{G}$ for every $\phi \in \text{Aut}(G)$ and $[X] \in \widehat{G}$. Next, let $\phi \in \text{Aut}(G)$, and $[X], [Y] \in \widehat{G}$ be such that $[X] = [Y]$. Then $X \cong Y$, and

$$\chi_{X \circ \phi} = \chi_X \circ \phi = \chi_Y \circ \phi = \chi_{Y \circ \phi}.$$

Therefore $X \circ \phi \cong Y \circ \phi$. Hence

$$\phi[X] = [X \circ \phi] = [Y \circ \phi] = \phi[Y].$$

This shows that the action is well-defined. Next, for $\phi, \psi \in \text{Aut}(G)$ and $[X] \in \widehat{G}$,

$$(\phi \circ \psi)[X] = [X \circ (\phi \circ \psi)] = [(X \circ \phi) \circ \psi] = \psi[X \circ \phi] = \psi(\phi[X])$$

and $1[X] = [X \circ 1] = [X]$. This proves the theorem. □

Theorem 3.8. *Let G be a finite group, $\phi \in \text{Aut}(G)$. Then ϕ maps a conjugacy class of G onto a conjugacy class of G .*

Proof. Let $g \in G$ and K_g the conjugacy class of g . Then

$$\begin{aligned}\phi(K_g) &= \phi\{hgh^{-1} \mid h \in G\} \\ &= \{\phi(h)\phi(g)\phi(h)^{-1} \mid h \in G\} \\ &= \{l\phi(g)l^{-1} \mid l \in G\} \\ &= K_{\phi(g)}.\end{aligned}$$

This shows that ϕ maps the conjugacy class of g onto the conjugacy class of $\phi(g)$. \square

The action in Theorem 3.7 gives us the next definition.

Definition 3.9. *Let G be a finite group.*

(i) *If $\phi \in \text{Aut}(G)$ and $\phi(K) = K$ for every conjugacy class K of G , then ϕ is said to **preserve conjugacy classes** of G .*

Denote by $\text{Aut}_C(G)$ the set of all automorphisms which preserve conjugacy classes of G .

(ii) *If $\phi \in \text{Aut}(G)$ and is in the kernel of the action defined in Theorem 3.7, then ϕ is said to **preserve equivalence classes of irreducible representation** of G .*

Denote by $\text{Aut}_{\widehat{G}}(G)$ the kernel of the action in Theorem 3.7. Thus

$$\begin{aligned}\text{Aut}_{\widehat{G}}(G) &= \{\phi \in \text{Aut}(G) \mid \phi[X] = [X] \text{ for every } [X] \in \widehat{G}\} \\ &= \{\phi \in \text{Aut}(G) \mid X \circ \phi \cong X \text{ for every } [X] \in \widehat{G}\}.\end{aligned}$$

Since every inner automorphism maps an element $g \in G$ to its conjugate, and $\text{Aut}_{\widehat{G}}(G)$ is defined as the kernel of the action, we have the following corollary.

Corollary 3.10. *Let G be a finite group. Then*

$$(i) \text{ Inn}(G) \subseteq \text{Aut}_C(G),$$

$$(ii) \text{ Aut}_{\widehat{G}}(G) \trianglelefteq \text{Aut}(G).$$

Note We will show later that $\text{Aut}_C(G) = \text{Aut}_{\widehat{G}}(G)$ for any finite group G . Thus we will have $\text{Inn}(G) \trianglelefteq \text{Aut}_{\widehat{G}}(G) = \text{Aut}_C(G) \trianglelefteq \text{Aut}(G)$ for every finite group G .

Theorem 3.11. *Let G be a finite group, and $g, h \in G$. Then g and h are conjugate if and only if $\chi(g) = \chi(h)$ for every irreducible character χ of G .*

Proof. By Proposition 2.14, it suffice to prove only the converse. Suppose that $\chi(g) = \chi(h)$ for every irreducible character χ of G but g and h are not conjugate. Let $K = K_g, L = K_h$. By Theorem 2.19, we have

$$\begin{aligned} 0 &= \sum_x \chi_K \bar{\chi}_L = \sum_x \chi(g) \overline{\chi(h)} \\ &= \sum_x \chi(g) \overline{\chi(g)} \\ &= \sum_x |\chi(g)|^2 \end{aligned}$$

where the sum is taken over all irreducible characters. Therefore $\chi(g) = 0$ for every irreducible character. Applying Theorem 2.19 again, we have

$$\begin{aligned} 0 &= \sum_x \chi(g) \overline{\chi(g)} = \sum_x \chi_K \bar{\chi}_K \\ &= \frac{|G|}{|K|} \neq 0, \quad \text{which is a contradiction.} \end{aligned}$$

Therefore, the theorem is proved. □

Theorem 3.12. *Let G be a finite group. Then $\text{Aut}_{\widehat{G}}(G) = \text{Aut}_C(G)$.*

Proof. Let $\phi \in \text{Aut}(G)$. We denote by $\text{Irr}(G)$ the set of irreducible characters of G . Thus $[X] \in \widehat{G} \leftrightarrow \chi_X \in \text{Irr}(G)$.

$$\begin{aligned}
\phi \in \text{Aut}_{\widehat{G}}(G) &\leftrightarrow \forall [X] \in \widehat{G}, X \circ \phi \cong X \\
&\leftrightarrow \forall \chi \in \text{Irr}(G) \chi \circ \phi = \chi \\
&\leftrightarrow \forall \chi \in \text{Irr}(G) \forall g \in G \chi(\phi(g)) = \chi(g) \\
&\leftrightarrow \forall g \in G \forall \chi \in \text{Irr}(G) \chi(\phi(g)) = \chi(g) \\
&\leftrightarrow \forall g \in G, g \text{ and } \phi(g) \text{ are conjugate} \\
&\leftrightarrow \phi \text{ preserves conjugacy classes of } G.
\end{aligned}$$

□

Corollary 3.13. *For every finite group G ,*

$$\text{Inn}(G) \trianglelefteq \text{Aut}_{\widehat{G}}(G) = \text{Aut}_C(G) \trianglelefteq \text{Aut}(G).$$

Proof. It follows immediately from Corollary 3.10 and Theorem 3.12

□

Proposition 3.14. *Let G be a finite abelian group. Then*

$$\text{Inn}(G) = \text{Aut}_C(G) = \text{Aut}_{\widehat{G}}(G) = \{\text{id}_G\}.$$

Proof. Since $K_g = \{hgh^{-1} \mid h \in G\} = \{g\}$ for every $g \in G$, the automorphism which preserves conjugacy classes of G is necessarily the identity map, so we have

$$\text{Aut}_{\widehat{G}}(G) = \text{Aut}_C(G) \subseteq \{\text{id}_G\} \subseteq \text{Inn}(G) \subseteq \text{Aut}_C(G).$$

This proves the proposition.

□

สภานักศึกษา
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER IV

Dihedral groups D_n

4.1 Definition and notation

Let D_n ($n \geq 3$) be the dihedral group of order $2n$ defined by

$$D_n = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle.$$

Elementary properties of the dihedral group can be found in [3], [6], [9], and [11]. Denote by $\text{Hom}(D_n)$ the set of all homomorphisms from D_n into D_n . In this chapter, we determine whether $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Inn}(D_n)$ or $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Aut}(D_n)$. To do this, we directly calculate all conjugacy classes of D_n , all inner automorphisms of D_n , and all automorphisms of D_n . Since D_n is generated by r and s , every $\phi \in \text{Hom}(D_n)$ is completely determined by $\phi(r)$ and $\phi(s)$.

If $\phi \in \text{Hom}(D_n)$ and $\phi(r) = a$ and $\phi(s) = b$, we denote ϕ by the diagram

$$(r \mapsto a, s \mapsto b).$$

Also, recall that we denote the conjugacy class of an element g in a group G by $K_g = \{hgh^{-1} \mid h \in G\}$, and denote by ϕ_g the inner automorphism induced from g .

4.2 Conjugacy classes in D_n

Recall that

$$\begin{aligned} D_n &= \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle \\ &= \{s^i r^j \mid 0 \leq i \leq 1, 0 \leq j \leq n-1\} \\ &= \{r^j \mid 0 \leq j \leq n-1\} \cup \{sr^j \mid 0 \leq j \leq n-1\}. \end{aligned}$$

Let $i \in \{0, 1, \dots, n-1\}$,

$$\begin{aligned}
K_{r^i} &= \{x r^i x^{-1} \mid x \in D_n\} \\
&= \{r^j r^i r^{-j} \mid 0 \leq j \leq n-1\} \cup \{s r^j r^i r^{-j} s^{-1} \mid 0 \leq j \leq n-1\} \\
&= \{r^i\} \cup \{r^{-i}\} \\
&= \{r^i, r^{n-i}\} \\
K_{s r^i} &= \{r^j s r^i r^{-j} \mid 0 \leq j \leq n-1\} \cup \{s r^j s r^i r^{-j} s^{-1} \mid 0 \leq j \leq n-1\} \\
&= \{s r^{i-2j} \mid 0 \leq j \leq n-1\} \cup \{s r^{2j-i} \mid 0 \leq j \leq n-1\}.
\end{aligned}$$

Case 1: n is even.

$$\begin{aligned}
K_1 &= \{1\}, \\
K_r &= \{r, r^{n-1}\}, \\
K_{r^2} &= \{r^2, r^{n-2}\}, \\
&\vdots \\
K_{r^{\frac{n}{2}-1}} &= \{r^{\frac{n}{2}-1}, r^{\frac{n}{2}+1}\}, \\
K_{r^{\frac{n}{2}}} &= \{r^{\frac{n}{2}}\}, \\
K_s &= \{s r^{-2j} \mid 0 \leq j \leq n-1\} \cup \{s r^{2j} \mid 0 \leq j \leq n-1\} \\
&= \{s r^m \mid m \text{ is even and } 0 \leq m \leq n-1\}, \\
K_{s r} &= \{s r^{1-2j} \mid 0 \leq j \leq n-1\} \cup \{s r^{2j-1} \mid 0 \leq j \leq n-1\} \\
&= \{s r^m \mid m \text{ is odd and } 0 \leq m \leq n-1\}.
\end{aligned}$$

In this case the number of conjugacy classes in D_n is $\frac{n+6}{2}$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case 2: n is odd.

$$\begin{aligned}
K_1 &= \{1\}, \\
K_r &= \{r, r^{n-1}\}, \\
K_{r^2} &= \{r^2, r^{n-2}\}, \\
&\vdots \\
K_{r^{\frac{n-1}{2}}} &= \{r^{\frac{n-1}{2}}, r^{\frac{n+1}{2}}\}, \\
K_s &= \{sr^{-2j} \mid 0 \leq j \leq n-1\} \cup \{sr^{2j} \mid 0 \leq j \leq n-1\} \\
&= \{sr^{n-2j} \mid 0 \leq j \leq n-1\} \cup \{sr^{2j} \mid 0 \leq j \leq n-1\} \\
&\supseteq \{sr^{n-m} \mid m \text{ is even and } 0 \leq m \leq n-1\} \\
&\quad \cup \{sr^m \mid m \text{ is even and } 0 \leq m \leq n-1\} \\
&= \{sr^m \mid 0 \leq m \leq n-1\}.
\end{aligned}$$

Therefore $K_s = \{sr^m \mid 0 \leq m \leq n-1\}$.

In this case the number of conjugacy classes in D_n is $\frac{n+3}{2}$.

4.3 $\text{Inn}(D_n)$ $D_n = \{r^i \mid 0 \leq i \leq n-1\} \cup \{sr^i \mid 0 \leq i \leq n-1\}$
 $= \{r^i \mid 1 \leq i \leq n\} \cup \{sr^i \mid 1 \leq i \leq n\}.$

Then

$$\begin{aligned}
\text{Inn}(D_n) &= \{\phi_h \mid h \in D_n\} \\
&= \{\phi_{r^i} \mid 1 \leq i \leq n\} \cup \{\phi_{sr^i} \mid 1 \leq i \leq n\}.
\end{aligned}$$

For each $1 \leq i \leq n$, we have

$$\begin{aligned}
\phi_{r^i}(r) &= r^i r r^{-i} = r, \\
\phi_{r^i}(s) &= r^i s r^{-i} = s r^{-2i} = s r^{n-2i}, \\
\phi_{sr^i}(r) &= s r^i r r^{-i} s = s r s = r^{-1} = r^{n-1}, \\
\phi_{sr^i}(s) &= s r^i s r^{-i} s = r^{-2i} s = s r^{2i}.
\end{aligned}$$

Then

$$\begin{aligned}\text{Inn}(D_n) &= \{(r \mapsto r, s \mapsto sr^{-2i}) \mid 1 \leq i \leq n\} \\ &\cup \{(r \mapsto r^{n-1}, s \mapsto sr^{2i}) \mid 1 \leq i \leq n\}.\end{aligned}$$

Case 1 : n is odd.

$$\begin{aligned}\{r^{2i} \mid 1 \leq i \leq n\} &= \{r^{2i} \mid 1 \leq i \leq \frac{n-1}{2}\} \cup \{r^{2i} \mid \frac{n+1}{2} \leq i \leq n\} \\ &= \{r^m \mid m \text{ is even and } 2 \leq m \leq n-1\} \\ &\quad \cup \{r^m \mid m \text{ is even and } n+1 \leq m \leq 2n\} \\ &= \{r^m \mid m \text{ is even and } 1 \leq m \leq n\} \\ &\quad \cup \{r^{m-n} \mid m \text{ is even and } n+1 \leq m \leq 2n\} \\ &= \{r^m \mid m \text{ is even and } 1 \leq m \leq n\} \\ &\quad \cup \{r^i \mid i \text{ is odd and } 1 \leq i \leq n\} \\ &= \{r^m \mid 1 \leq m \leq n\}.\end{aligned}$$

Similarly $\{r^{-2i} \mid 1 \leq i \leq n\} = \{r^m \mid 1 \leq m \leq n\}$.

Thus

$$\begin{aligned}\text{Inn}(D_n) &= \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n\} \\ &\quad \cup \{(r \mapsto r^{n-1}, s \mapsto sr^m) \mid 1 \leq m \leq n\},\end{aligned}$$

$$\text{and } |\text{Inn}(D_n)| = 2n.$$

Case 2 : n is even. Similar to case 1, we have

$$\begin{aligned}\{r^{2i} \mid 1 \leq i \leq n\} &= \{r^m \mid 1 \leq m \leq n \text{ and } m \text{ is even}\} \\ &= \{r^{-2i} \mid 1 \leq i \leq n\}.\end{aligned}$$

Therefore

$$\begin{aligned} \text{Inn}(D_n) &= \{(r \mapsto r, s \mapsto sr^m) \mid m \text{ is even and } 1 \leq m \leq n\} \\ &\quad \cup \{(r \mapsto r^{n-1}, s \mapsto sr^m) \mid m \text{ is even and } 1 \leq m \leq n\} \end{aligned}$$

$$\text{and } |\text{Inn}(D_n)| = n.$$

4.4 $\text{Aut}_{\hat{D}_n}(D_n)$

We will use the result obtained in Section 4.2 to calculate $\text{Aut}_{\hat{D}_n}(D_n)$. First, assume that n is odd.

$$\begin{aligned} \phi \in \text{Aut}_{\hat{D}_n}(D_n) &\rightarrow \phi \text{ preserves conjugacy classes of } D_n \\ &\rightarrow (\phi(r) = r \text{ or } \phi(r) = r^{n-1}) \text{ and } (\phi(s) = sr^m \text{ for some } 1 \leq m \leq n) \\ &\rightarrow \phi \in \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n\} \\ &\quad \cup \{(r \mapsto r^{n-1}, s \mapsto sr^m) \mid 1 \leq m \leq n\}. \end{aligned}$$

Hence

$$\begin{aligned} \text{Aut}_{\hat{D}_n}(D_n) &\subseteq \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n\} \\ &\quad \cup \{(r \mapsto r^{n-1}, s \mapsto sr^m) \mid 1 \leq m \leq n\}. \end{aligned} \tag{4.1}$$

Similarly, if n is even,

$$\begin{aligned} \text{Aut}_{\hat{D}_n}(D_n) &\subseteq \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n \text{ and } m \text{ is even}\} \\ &\quad \cup \{(r \mapsto r^{n-1}, s \mapsto sr^m) \mid 1 \leq m \leq n \text{ and } m \text{ is even}\}. \end{aligned} \tag{4.2}$$

If we compare (4.1), (4.2) and the results in Section 4.3, we obtain the next theorem.

Theorem 4.1. $\text{Aut}_{\hat{D}_n}(D_n) = \text{Inn}(D_n)$ for every $n \geq 3$.

Proof. Use the fact that $\text{Inn}(G) \subseteq \text{Aut}_{\hat{G}}(G)$ for any finite group G and compare (4.1), (4.2) above to $\text{Inn}(D_n)$. \square

Theorem 4.2. $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Aut}(D_n) \leftrightarrow n = 3.$

Proof. (\leftarrow) Let $n = 3$ and $\phi \in \text{Aut}(D_n)$. Then $D_n = D_3 = \{1, r, r^2, s, sr, sr^2\}$. Since $|r| = |r^2| = 3$, and $|s| = |sr| = |sr^2| = 2$, we have $\phi(r) \in \{r, r^2\}$ and $\phi(s) \in \{s, sr, sr^2\}$. Then

$$\begin{aligned} \phi &\in \{(r \mapsto r, s \mapsto sr^m) \mid 0 \leq m \leq 2\} \cup \{(r \mapsto r^2, s \mapsto sr^m) \mid 0 \leq m \leq 2\} \\ &= \text{Inn}(D_n). \end{aligned}$$

Therefore $\phi \in \text{Inn}(D_n)$. This shows that

$$\text{Aut}(D_n) \subseteq \text{Inn}(D_n).$$

Hence $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Aut}(D_n)$.

(\rightarrow) Assume that $n \neq 3$. If n is odd, $(r \mapsto r^2, s \mapsto s)$ is an automorphism of D_n which does not belong to $\text{Aut}_{\widehat{D}_n}(D_n)$. If n is even, $(r \mapsto r, s \mapsto sr)$ is an automorphism of D_n which is not in $\text{Aut}_{\widehat{D}_n}(D_n)$. This shows that $\text{Aut}_{\widehat{D}_n}(D_n) \neq \text{Aut}(D_n)$. \square

Corollary 4.3. $\text{Inn}(D_n) = \text{Aut}(D_n) \leftrightarrow n = 3.$

Proof. It follows directly from Theorem 4.1 and Theorem 4.2. \square

4.5 $\text{Aut}(D_n)$

Although we already knew whether $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Inn}(D_n)$ and $\text{Aut}_{\widehat{D}_n}(D_n) = \text{Aut}(D_n)$, we are still interested in calculating $\text{Aut}(D_n)$.

Theorem 4.4. $\text{Aut}(D_n) = \{(r \mapsto r^i, s \mapsto sr^j) \mid 1 \leq i \leq n, \gcd(i, n) = 1, \text{ and } 1 \leq j \leq n\}$.

Proof. (\subseteq) Let $\phi \in \text{Aut}(D_n)$. Since $|r| = n \geq 3$ and $|sr^j| = 2$ for all j , we have $\phi(r) \neq sr^j$ for all j . Let $\phi(r) = r^i$ for some $i \in \{1, 2, \dots, n\}$. Since $\phi \in \text{Aut}(D_n)$, $n = |r| = |\phi(r)| = |r^i| = \frac{n}{\gcd(n, i)}$. Hence $\gcd(n, i) = 1$. It follows that

$$\phi(\langle r \rangle) = \langle \phi(r) \rangle = \langle r^i \rangle = \langle r \rangle \quad (4.3)$$

Since ϕ is 1-1, $\phi(s) \notin \langle r \rangle$. Therefore $\phi(s) = sr^j$ for some $1 \leq j \leq n$. This shows that $\phi \in \{(r \mapsto r^i, s \mapsto sr^j) \mid 1 \leq i \leq n, \gcd(i, n) = 1, \text{ and } 1 \leq j \leq n\}$.

(\supseteq) Let $\phi : D_n \rightarrow D_n$ be a homomorphism such that

$$\begin{aligned} \phi(r) &= r^i \text{ for some } 1 \leq i \leq n \text{ and } \gcd(i, n) = 1, \text{ and} \\ \phi(s) &= sr^j \text{ for some } 1 \leq j \leq n. \end{aligned}$$

Similar to (4.3) above, $\phi(\langle r \rangle) = \langle r \rangle$ and

$$\phi(s \langle r \rangle) = \phi(s)\phi(\langle r \rangle) = \phi(s) \langle r \rangle = sr^j \langle r \rangle = s \langle r \rangle.$$

This shows that ϕ is surjective. Since D_n is finite, ϕ is bijective. Therefore $\phi \in \text{Aut}(D_n)$. \square

Corollary 4.5. $|\text{Aut}(D_n)| = n\phi(n)$, where

$$\phi(n) = |\{m \in \mathbb{N} \mid 1 \leq m \leq n, \text{ and } \gcd(m, n) = 1\}|$$

is the Euler's phi Function.

Corollary 4.6. $|\text{Out}(D_n)| = \begin{cases} \frac{\phi(n)}{2} & \text{if } n \text{ is odd,} \\ \phi(n) & \text{if } n \text{ is even.} \end{cases}$

We will find some concrete groups to which $\text{Inn}(D_n)$, $\text{Aut}_{\widehat{D}_n}(D_n)$, and $\text{Aut}(D_n)$ are isomorphic. Since $\text{Inn}(D_n) = \text{Aut}_{\widehat{D}_n}(D_n)$, our work reduce to finding only the abstract groups for $\text{Inn}(D_n)$ and $\text{Aut}(D_n)$. To find a group to which $\text{Aut}(D_n)$ is isomorphic, we will use the notion of semidirect product of groups.

Theorem 4.7. (i) $\text{Inn}(D_n) \cong D_n$ if n is odd and $n \geq 3$.

(ii) $\text{Inn}(D_n) \cong D_{\frac{n}{2}}$ if n is even and $n \geq 6$.

(iii) $\text{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Assume that $n \geq 3$ and n is odd. Consider the map

$$D_n \rightarrow \text{Inn}(D_n), x \mapsto \phi_x.$$

This map is an epimorphism (Theorem 3.2(iii)). In addition, (see Section 4.3)

$$|D_n| = 2n = |\text{Inn}(D_n)|.$$

Thus the map is an isomorphism, and $\text{Inn}(D_n) \cong D_n$.

Next, assume that n is even and $n \geq 6$. Recall that

$$\begin{aligned} \text{Inn}(D_n) = & \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n, \text{ and } m \text{ is even}\} \\ & \cup \{(r \mapsto r^{-1}, s \mapsto sr^m) \mid 1 \leq m \leq n, \text{ and } m \text{ is even}\}. \end{aligned}$$

Let $a = (r \mapsto r, s \mapsto sr^2)$, and $b = (r \mapsto r^{-1}, s \mapsto s) \in \text{Inn}(D_n)$. Claim

(i) $a^{\frac{n}{2}} = 1 = b^2$,

(ii) $ba = a^{-1}b$,

(iii) $\text{Inn}(D_n) = \langle a, b \rangle$.

(i) and (ii) can be proved by direct calculation. In fact, $a^l = (r \mapsto r, s \mapsto sr^{2l})$ for every $1 \leq l \leq \frac{n}{2}$. Furthermore, $ba^l = (r \mapsto r^{-1}, s \mapsto sr^{-2l})$ for every $1 \leq l \leq \frac{n}{2}$. Thus

$$\begin{aligned} \text{Inn}(D_n) &= \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n, \text{ and } m \text{ is even}\} \\ &\quad \cup \{(r \mapsto r^{-1}, s \mapsto sr^m) \mid 1 \leq m \leq n, \text{ and } m \text{ is even}\} \\ &= \{a^l \mid 1 \leq l \leq \frac{n}{2}\} \cup \{ba^l \mid 1 \leq l \leq \frac{n}{2}\} \\ &\subseteq \langle a, b \rangle. \end{aligned}$$

This shows that $\text{Inn}(D_n) = \langle a, b \rangle$.

Now, recall that $D_{\frac{n}{2}} = \langle r, s \mid r^{\frac{n}{2}} = 1 = s^2, sr = r^{-1}s \rangle$. From (i) and (ii), we can see that a and b satisfy the relation in the presentation of $D_{\frac{n}{2}}$ if we replace r by a and s by b . Thus there is a unique homomorphism $\phi : D_{\frac{n}{2}} \rightarrow \text{Inn}(D_n)$ mapping r to a and s to b . From (iii), a and b generate $\text{Inn}(D_n)$, so we have ϕ is surjective. In addition, $|D_{\frac{n}{2}}| = n = |\text{Inn}(D_n)|$ (see Section 3.3). Hence ϕ is also injective. Therefore ϕ is an isomorphism, and $\text{Inn}(D_n) \cong D_{\frac{n}{2}}$. This proves (ii). From Section 3.3, we see that $|\text{Inn}(D_4)| = 4$. It is the fact that, up to isomorphism, the groups of order 4 are \mathbb{Z}_4 and $\mathbb{Z}_2 \times \mathbb{Z}_2$. By direct calculation, we can see that every nonidentity element of $\text{Inn}(D_4)$ has order 2. Thus $\text{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. \square

Note if we define D_2 to be the group of $\{1, r, s, sr\}$ of order 4 with the relation $r^2 = s^2 = 1$ and $sr = r^{-1}s$. Then $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and the previous theorem becomes

$$\text{Inn}(D_n) \cong D_{\frac{n}{2}} \text{ if } n \geq 3 \text{ and } n \text{ is even,}$$

$$\text{Inn}(D_n) \cong D_n \text{ if } n \geq 3 \text{ and } n \text{ is odd.}$$

Next, we will prove that $\text{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$. We first give theorems which will be used in the proof.

Theorem 4.8 ([3], p.93). *If H and K are finite subgroups of a group, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Theorem 4.9 ([3], p.180). *Suppose G is a group with subgroups H and K such that*

$$(i) \ H \trianglelefteq G,$$

$$(ii) \ H \cap K = 1.$$

Let $\varphi : K \rightarrow \text{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H . Then $HK \cong H \rtimes K$.

In particular, if $G = HK$ with H and K satisfying (i) and (ii), then G is the semidirect product of H and K .

Theorem 4.10. $\text{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ for every $n \geq 3$.

Proof. First, recall that (see Section 4.5)

$$\text{Aut}(D_n) = \{(r \mapsto r^i, s \mapsto sr^m) \mid 1 \leq i \leq n, \gcd(i, n) = 1 \text{ and } 1 \leq m \leq n\}.$$

$$\text{Let } G = \text{Aut}(D_n), H = \{(r \mapsto r, s \mapsto sr^m) \mid 1 \leq m \leq n\}, \text{ and}$$

$$K = \{(r \mapsto r^i, s \mapsto s) \mid 1 \leq i \leq n \text{ and } \gcd(i, n) = 1\}.$$

Claim

$$(i) \ H \cong \mathbb{Z}_n, \text{ and } K \cong \mathbb{Z}_n^\times.$$

$$(ii) \ H \trianglelefteq G, \text{ and } K \leq G.$$

$$(iii) \ H \cap K = 1.$$

$$(iv) \ G = HK.$$

First, we prove (i). Let $\phi : \mathbb{Z}_n \rightarrow G$ be defined by $\phi(m) = (r \mapsto r, s \mapsto sr^m)$. If $m_1 = m_2$ in \mathbb{Z}_n , then there exists $k \in \mathbb{Z}$ such that $m_1 = nk + m_2$, and thus $r^{m_1} = r^{nk+m_2} = r^{m_2}$. This shows that ϕ is well-defined. Next, let $m_1, m_2 \in \mathbb{Z}_n$

$$\begin{aligned} \phi(m_1 + m_2) &= (r \mapsto r, s \mapsto sr^{m_1+m_2}) \\ &= (r \mapsto r, s \mapsto sr^{m_1})(r \mapsto r, s \mapsto sr^{m_2}) \\ &= \phi(m_1)\phi(m_2). \end{aligned}$$

Therefore ϕ is a homomorphism. It is easy to see that $\text{Im}(\phi) = H$, and $\ker \phi = \{0\}$. Then ϕ is an isomorphism. Hence $\mathbb{Z}_n \cong H$. Next, let $\psi : \mathbb{Z}_n^\times \rightarrow K$ be defined by $\psi(i) = (r \mapsto r^i, s \mapsto s)$. Using the same argument as ϕ , we obtain that $\mathbb{Z}_n^\times \cong K$.

Next, we prove (ii). From (i), we know that $\mathbb{Z}_n^\times \cong K$ and, so $\mathbb{Z}_n \cong H$ we obtain that $H \leq G$ and $K \leq G$. Now, let $p = (r \mapsto r^i, s \mapsto sr^m) \in G$ and $q = (r \mapsto r, s \mapsto sr^l) \in H$. Let

$$p^{-1} = (r \mapsto r^i, s \mapsto sr^m)^{-1} = (r \mapsto r^x, s \mapsto sr^y). \quad (4.4)$$

Then

$$\begin{aligned} pqp^{-1} &= (r \mapsto r^i, s \mapsto sr^m)(r \mapsto r, s \mapsto sr^l)(r \mapsto r^x, s \mapsto sr^y) \\ &= (r \mapsto r^i, s \mapsto sr^m)(r \mapsto r^x, s \mapsto sr^{y+l}) \\ &= (r \mapsto r^{ix}, s \mapsto sr^{m+iy+il}) \end{aligned} \quad (4.5)$$

From Equation (4.4), $p^{-1} = (r \mapsto r^x, s \mapsto sr)$, so $p^{-1}(r) = r^x$ and $p^{-1}(s) = sr$. Therefore

$$r^{ix} = (r^i)^x = (p(r))^x = p(r^x) = r.$$

Thus, from (4.5), we obtain $pqp^{-1} = (r \mapsto r, s \mapsto sr^{m+iy+il}) \in H$. This shows that $H \trianglelefteq G$. (iii) is obvious. For (iv), by Theorem 4.8, we obtain that

$$\begin{aligned} |HK| &= \frac{|H||K|}{|H \cap K|} = |\mathbb{Z}_n||\mathbb{Z}_n^\times| \\ &= n\phi(n) \\ &= |\text{Aut}(D_n)| \quad (\text{Corollary 4.5}). \end{aligned}$$

Since $HK \subseteq \text{Aut}(D_n)$ and $\text{Aut}(D_n)$ is a finite set, we have $\text{Aut}(D_n) = HK$. By Theorem 4.9,

$$\text{Aut}(D_n) = HK \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times.$$

□

CHAPTER V

Symmetric groups S_n

5.1 Definition and notation

Recall that S_n is the group of all bijections from $\{1, 2, \dots, n\}$ onto itself under the function composition. We multiply elements in S_n from right to left. Its elementary properties can be found in [3], [6], [9], and [11].

If $f : S_n \rightarrow S_n$ and $\sigma = (a_1 a_2 \dots a_l)$ is a cycle in S_n , then sometimes we will write $f(\sigma) = f(a_1 a_2 \dots a_l)$ rather than $f(\sigma) = f((a_1 a_2 \dots a_l))$. In addition, if $x \in \{1, 2, \dots, n\}$ is written as one of the non-fixed symbols in the cycle decomposition of σ , we will say that σ contains x as a symbol in its cycle notation, or simply σ contains x , or x is in σ .

For example, if $\sigma = (123)(56) \in S_7$, then σ contains 1, 2, 3, 5, and 6 but does not contain 4 and 7. Consider $S_1 = \{(1)\}$ and $S_2 = \{(1), (12)\}$. It is easy to see that $\text{Inn}(S_i) = \text{Aut}(S_i) = \{\text{id}\}$ for $i = 1, 2$ where id is the identity map. Hence

$$\text{Inn}(S_i) = \text{Aut}_{\widehat{S}_i}(S_i) = \text{Aut}(S_i) \quad \text{for } i = 1, 2.$$

In Section 5.2, we consider S_n when $n \geq 3$.

5.2 $\text{Inn}(S_n)$, $\text{Aut}_{\widehat{S}_n}(S_n)$, and $\text{Aut}(S_n)$

Definition 5.1 ([12], p.92). A group G is called **complete** if it has no center and no outer automorphism.

Theorem 5.2 ([12], p.92). S_n is complete when $n \geq 3$ and $n \neq 6$.

Corollary 5.3. For $n \geq 3$, $n \neq 6$,

$$\text{Inn}(S_n) = \text{Aut}_{\widehat{S}_n}(S_n) = \text{Aut}(S_n) \cong S_n.$$

Proof. From Theorem 5.2, we obtain $\text{Inn}(S_n) = \text{Aut}_{\widehat{S}_n}(S_n) = \text{Aut}(S_n)$. In addition, the map $S_n \rightarrow \text{Inn}(S_n)$, by $g \mapsto \phi_g$ is an isomorphism. Therefore, the corollary is proved. \square

Next, we will show that

$$\text{Aut}_{\widehat{S}_6}(S_6) = \text{Inn}(S_6).$$

Lemma 5.4. Let $\phi \in \text{Aut}(S_n)$. If ϕ maps transpositions to transpositions, then the following statements hold :

- (i) If transpositions $(x y)$ and $(m n)$ have a common symbol (for instance, $x = m$), then transpositions $\phi(x y)$ and $\phi(m n)$ have a common symbol.
- (ii) for each $a \in \{1, 2, \dots, n\}$ there exists a unique $a' \in \{1, 2, \dots, n\}$ such that $\phi(\{(a \alpha) \mid \alpha \in \{1, 2, \dots, n\} - \{a\}\}) = \{(a' \beta) \mid \beta \in \{1, 2, \dots, n\} - \{a'\}\}$

Proof. Let $a \in \{1, 2, \dots, n\}$, $\alpha_1, \alpha_2 \in \{1, 2, \dots, n\} - \{a\}$ and $\alpha_1 \neq \alpha_2$. Assume that $\phi(a \alpha_1) = (x_1 y_1)$, $\phi(a \alpha_2) = (x_2 y_2)$. If x_1, y_1, x_2, y_2 are all distinct, then

$$\begin{aligned} 2 &= |(x_1 y_1)(x_2 y_2)| = |\phi(a \alpha_1)\phi(a \alpha_2)| \\ &= |\phi((a \alpha_1)(a \alpha_2))| \\ &= |\phi(\alpha_2 \alpha_1 a)| \\ &= |(\alpha_2 \alpha_1 a)| = 3, \text{ a contradiction.} \end{aligned}$$

Therefore $x_1 = x_2$, $x_1 = y_2$, $y_1 = x_2$, or $y_1 = y_2$. Then we can write

$$\phi(a \alpha_1) = (a' \beta_1), \phi(a \alpha_2) = (a' \beta_2)$$

for some $a' \in \{1, 2, \dots, n\}$, $\beta_1, \beta_2 \in \{1, 2, \dots, n\} - \{a'\}$, $\beta_1 \neq \beta_2$. This proves (i).

Next, let $a \in \{1, 2, \dots, n\}$. Choose $\alpha_1, \alpha_2 \in \{1, 2, \dots, n\} - \{a\}$, and $\alpha_1 \neq \alpha_2$. Then by (i), there exist $a', \beta_1, \beta_2 \in \{1, 2, \dots, n\}$, a', β_1, β_2 are all distinct, and $\phi(a \alpha_1) = (a' \beta_1)$, $\phi(a \alpha_2) = (a' \beta_2)$.

Suppose there exists $\alpha \in \{1, 2, \dots, n\} - \{a, \alpha_1, \alpha_2\}$ such that

$$\phi(a \alpha) \text{ does not contain the symbol } a'. \quad (5.1)$$

Since $(a \alpha_1)$ and $(a \alpha)$ have a common symbol, by (i), $\phi(a \alpha_1)$ and $\phi(a \alpha)$ have a common symbol. Because $\phi(a \alpha_1) = (a' \beta_1)$, $\phi(a \alpha)$ contains either the symbol a' or β_1 . But from (5.1), we see that $\phi(a \alpha)$ contains β_1 . If we consider $\phi(a \alpha_2)$ and $\phi(a \alpha)$ with the same argument, we have $\phi(a \alpha)$ contains β_2 . Hence $\phi(a \alpha) = (\beta_1 \beta_2)$. Now

$$\begin{aligned} 4 &= |(\alpha \alpha_2 \alpha_1 a)| = |\phi(\alpha \alpha_2 \alpha_1 a)| \\ &= |\phi((a \alpha_1) (a \alpha_2) (a \alpha))| \\ &= |\phi(a \alpha_1) \phi(a \alpha_2) \phi(a \alpha)| \\ &= |(a' \beta_1)(a' \beta_2)(\beta_1 \beta_2)| \\ &= |(a' \beta_2)| = 2, \text{ a contradiction.} \end{aligned}$$

The contradiction arises from supposition (5.1). This implies that for every $\alpha \in \{1, 2, \dots, n\} - \{a, \alpha_1, \alpha_2\}$, $\phi(a \alpha)$ contains the symbol a' . Thus $\phi(\{(a \alpha) \mid \alpha \in \{1, 2, \dots, n\} - \{a\}\}) = \{(a' \beta) \mid \beta \in \{1, 2, \dots, n\} - \{a'\}\}$. The uniqueness of a' is obvious, so we have proved (ii). \square

Theorem 5.5. $\text{Aut}_{\widehat{S}_6}(S_6) = \text{Inn}(S_6)$.

Proof. Let $\phi \in \text{Aut}_{\widehat{S}_6}(S_6)$. Then ϕ maps transpositions to transpositions. From Lemma 5.4(ii), we can define $s : \{1, 2, \dots, 6\} \rightarrow \{1, 2, \dots, 6\}$ by $s(a) = a'$ where a and a' are as in Lemma 5.4(ii). Then s is 1-1 because ϕ is. Therefore s is bijective, that is $s \in S_6$.

Next, we prove that $\phi = \phi_s$, (the inner automorphism induced from s). Let (xy) be a transposition. Then by Lemma 5.4(ii),

$$\begin{aligned}
\phi(xy) &\in \phi\{(x\alpha) \mid \alpha \in \{1, 2, \dots, 6\} - \{x\}\} \\
&= \{(x'\beta) \mid \beta \in \{1, 2, \dots, 6\} - \{x'\}\}, \quad \text{where } x' = s(x) \\
&= \{(s(x)\beta) \mid \beta \in \{1, 2, \dots, 6\} - \{x'\}\}.
\end{aligned}$$

Thus $\phi(xy) = (s(x)\beta)$ for some $\beta \in \{1, 2, \dots, 6\} - \{x'\}$.

Similarly,

$$\phi(yx) = (s(y)\gamma) \text{ for some } \gamma \in \{1, 2, \dots, 6\} - \{s(y)\}.$$

Since $\phi(xy) = \phi(yx)$, $(s(x)\beta) = (s(y)\gamma)$. because $x \neq y$, we have $s(x) \neq s(y)$, and thus $s(x) = \gamma$. Hence $\phi(xy) = (s(x)s(y))$.

$$\phi_s(xy) = s(xy)s^{-1} = (s(x)s(y)).$$

Therefore $\phi(xy) = \phi_s(xy)$ for every transposition (xy) . Then $\phi = \phi_s$, and $\phi \in \text{Inn}(S_6)$. This proves that $\text{Aut}_{\widehat{S}_6}(S_6) = \text{Inn}(S_6)$. \square

To show that $\text{Aut}_{\widehat{S}_6}(S_6) \neq \text{Aut}(S_6)$, we will find an automorphism ϕ of S_6 which does not preserve conjugacy classes. Since $\text{Inn}(S_6) = \text{Aut}_{\widehat{S}_6}(S_6)$, every outer automorphism of S_6 does not preserve conjugacy classes. Therefore ϕ can be any outer automorphism of S_6 . One of the outer automorphisms of S_6 is given in [3].

Theorem 5.6 ([3], p.221). *The map*

$$(12) \rightarrow (12)(34)(56)$$

$$(23) \rightarrow (14)(25)(36)$$

$$(34) \rightarrow (13)(24)(56)$$

$$(45) \rightarrow (12)(36)(45)$$

$$(56) \rightarrow (14)(23)(56)$$

extends to an automorphism of S_6 .

In the remaining part of this chapter, unless stated otherwise, ϕ is the automorphism in Theorem 5.6. We can see that ϕ does not preserve conjugacy classes of S_6 , so $\phi \in \text{Aut}(S_6) - \text{Aut}_{\widehat{S}_6}(S_6)$. Therefore, we obtain Theorem 5.7, and Corollary 5.8.

Theorem 5.7. $\text{Aut}_{\widehat{S}_6}(S_6) \neq \text{Aut}(S_6)$.

Corollary 5.8. *Let $n \in \mathbb{N}$.*

$$\text{If } n \neq 6, \text{ then } \text{Inn}(S_n) = \text{Aut}_{\widehat{S}_n}(S_n) = \text{Aut}(S_n).$$

$$\text{If } n = 6, \text{ then } \text{Inn}(S_6) = \text{Aut}_{\widehat{S}_6}(S_6) \neq \text{Aut}(S_6).$$

Proof. Combine Theorem 5.5, Theorem 5.7, and Corollary (5.3). □

Since $\phi \notin \text{Aut}_{\widehat{S}_6}(S_6)$. There exists an irreducible representation X of S_6 such that $X \circ \phi \not\cong X$. We will find such an X . The method of constructing irreducible representations of S_n (for $n \in \mathbb{N}$) can be found in [13]. After using the method, we obtain an irreducible representation X of S_6 such that $X \circ \phi \not\cong X$, which will be shown in the next example.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Examples 5.9. Let $X : S_6 \rightarrow GL_5(\mathbb{C})$ be irreducible representation of S_6 defined by

$$\begin{aligned}
 X(12) &= \begin{bmatrix} -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, & X(23) &= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \\
 X(34) &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, & X(45) &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \\
 X(56) &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.
 \end{aligned}$$

Let $Y = X \circ \phi : S_6 \rightarrow GL_5(\mathbb{C})$. Then Y is an irreducible representation of S_6 . We will show that $X \not\cong Y$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

$$\begin{aligned}
Y(12) &= X(\phi(12)) \\
&= X((12)(34)(56)) \\
&= X(12)X(34)X(56) \\
&= \begin{bmatrix} -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.
\end{aligned}$$

Then

$$\chi_X(12) = \text{tr } X(12) = 3$$

$$\chi_Y(12) = \text{tr } Y(12) = -1.$$

Therefore $\chi_X \neq \chi_Y$, which implies that $X \not\cong Y$. That is $X \circ \phi \not\cong X$.

CHAPTER VI

Alternating groups A_n

A_n is a normal subgroup of S_n consisting of all even permutations. In this chapter, we use the same terminology and notation as in the previous chapter.

If we consider $A_1 = A_2 = \{(1)\}$, and $A_3 \cong \mathbb{Z}_3$, then we have

$$\begin{aligned}\{\text{id}\} &= \text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n) = \text{Aut}(A_n) \quad \text{for } n = 1, 2 \quad \text{and} \\ \{\text{id}\} &= \text{Inn}(A_3) = \text{Aut}_{\widehat{A}_3}(A_3) \neq \text{Aut}(A_3).\end{aligned}$$

In the remaining part, we will consider A_n when $n \geq 4$.

6.1 $\text{Inn}(A_n)$, $\text{Aut}_{\widehat{A}_n}(A_n)$, $\text{Inn}_{A_n}(S_n)$, and $\text{Aut}(A_n)$

In this section, we determine whether $\text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n)$ or $\text{Aut}_{\widehat{A}_n}(A_n) = \text{Aut}(A_n)$. To do this, we also define $\text{Inn}_{A_n}(S_n)$ to be the set of inner automorphisms of S_n restricted to A_n .

Theorem 6.1. *Let $n \geq 4$. Then*

- (i) $Z(A_n) = \{(1)\}$,
- (ii) $\text{Inn}(A_n) = \{\phi_x \mid x \in A_n\}$ and $\phi_x = \phi_y$ iff $x = y$,
- (iii) $|\text{Inn}(A_n)| = \frac{n!}{2}$.

Proof. Let $n \geq 5$. Since $Z(A_n) \trianglelefteq A_n$ and A_n is simple,

$$Z(A_n) = A_n \text{ or } Z(A_n) = \{(1)\}.$$

Because A_n is not abelian, $Z(A_n) \neq A_n$. Therefore $Z(A_n) = \{(1)\}$. Then $f : A_n \rightarrow \text{Inn}(A_n)$, $g \mapsto \phi_g$ is an isomorphism. This implies (ii) and (iii). For $n = 4$, we can compute directly to see that $Z(A_4) = \{(1)\}$, and then (ii) and (iii) follow. \square

Lemma 6.2. *Let G be a group, $H \trianglelefteq G$, and $g \in G$. Then $\phi_g|_H \in \text{Aut}(H)$.*

Proof. Since $H \trianglelefteq G$, $\phi_g(H) = gHg^{-1} = H$. Therefore $\phi_g : H \rightarrow H$ is surjective. Hence $\phi_g|_H \in \text{Aut}(H)$. \square

From this Lemma, we have

$$\{\phi_x|_{A_n} \mid x \in S_n\} \subseteq \text{Aut}(A_n).$$

This set will be used in the rest of this chapter, so we give it a notation.

Notation : $\text{Inn}_{A_n}(S_n) = \{\phi_x|_{A_n} \mid x \in S_n\}$.

Theorem 6.3. *Let $n \geq 4$. Then*

- (i) For each $x, y \in S_n$, $\phi_x|_{A_n} = \phi_y|_{A_n} \leftrightarrow x = y$,
- (ii) $|\text{Inn}_{A_n}(S_n)| = n!$,
- (iii) $\text{Inn}_{A_n}(S_n) \supseteq \text{Inn}(A_n)$.

Proof. (i) Let $x, y \in S_n$.

$$\begin{aligned} \phi_x|_{A_n} = \phi_y|_{A_n} &\leftrightarrow \forall g \in A_n, \phi_x(g) = \phi_y(g) \\ &\leftrightarrow \forall g \in A_n, x g x^{-1} = y g y^{-1} \\ &\leftrightarrow \forall g \in A_n, y^{-1} x g = g y^{-1} x \\ &\leftrightarrow y^{-1} x \in Z(A_n) = \{(1)\} \quad (\text{by Theorem 6.1(i)}) \\ &\leftrightarrow y^{-1} x = (1) \\ &\leftrightarrow x = y. \end{aligned}$$

(ii) is an immediate consequence of (i).

For (iii),

$$\begin{aligned}\text{Inn}_{A_n}(S_n) &= \{\phi_x|_{A_n} \mid x \in S_n\} \\ &\supseteq \{\phi_x|_{A_n} \mid x \in A_n\} \\ &= \text{Inn}(A_n).\end{aligned}$$

□

Theorem 6.4. $\text{Inn}(A_n) \trianglelefteq \text{Inn}_{A_n}(S_n) \leq \text{Aut}(A_n)$ for every $n \geq 4$.

Proof. We know that $\text{Inn}_{A_n}(S_n) \subseteq \text{Aut}(A_n)$. Next let $x, y \in S_n$. Since $\phi_x(A_n) = A_n$ and $\phi_y(A_n) = A_n$, we have

$$\phi_x|_{A_n}(\phi_y|_{A_n})^{-1} = \phi_x|_{A_n}\phi_y^{-1}|_{A_n} = \phi_x\phi_y^{-1}|_{A_n} = \phi_{xy^{-1}}|_{A_n} \in \text{Inn}_{A_n}(S_n).$$

This shows $\text{Inn}(S_n)|_{A_n} \leq \text{Aut}(A_n)$. Since $\text{Inn}(A_n) \trianglelefteq \text{Aut}(A_n)$ and $\text{Inn}(A_n) \subseteq \text{Inn}_{A_n}(S_n)$, we also have $\text{Inn}(A_n) \trianglelefteq \text{Inn}_{A_n}(S_n)$. □

Theorem 6.5. (i) $\text{Inn}(A_4) = \text{Aut}_{\hat{A}_4}(A_4)$.

(ii) $\text{Aut}_{\hat{A}_4}(A_4) \trianglelefteq \text{Inn}_{A_4}(S_4)$.

Proof. First, we prove (i) by directly compute all conjugacy classes of A_4 .

$A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (132), (142), (143), (243)\}$. All conjugacy classes of A_4 are

$$\begin{aligned}K_{(1)} &= \{(1)\}, \\ K_{(12)(34)} &= \{(12)(34), (13)(24), (14)(23)\}, \\ K_{(123)} &= \{(123), (134), (142), (243)\}, \quad \text{and} \\ K_{(132)} &= \{(132), (143), (124), (234)\}.\end{aligned}$$

Claim $A_4 = \langle (123), (134) \rangle$. Since $(123)(134) = (234)$, and $(134)(123) = (124)$, we obtain that $(123), (134), (234)$, and $(124) \in \langle (123), (134) \rangle$. Then their inverses

(132) , (143) , (243) , and (142) are also in $\langle(123), (134)\rangle$. Hence $\langle(123), (134)\rangle$ contains all 3-cycles. Since 3-cycles generate A_4 , we obtain that $A_4 = \langle(123), (134)\rangle$. Thus every $\phi \in \text{Aut}(A_4)$ is completely determined by $\phi(123)$ and $\phi(134)$. Let $\phi \in \text{Aut}_{\widehat{A}_4}(A_4)$. There are at most 4 choices for $\phi(123)$ and at most 3 choices for $\phi(134)$. By Theorem 6.1(iii)

$$|\text{Aut}_{\widehat{A}_4}(A_4)| \leq 4 \cdot 3 = 12 = \frac{4!}{2} = |\text{Inn}(A_4)|.$$

Since $\text{Inn}(A_4) \subseteq \text{Aut}_{\widehat{A}_4}(A_4)$, $\text{Inn}(A_4) = \text{Aut}_{\widehat{A}_4}(A_4)$. This proves (i).

For (ii), since $\text{Inn}(A_4) \trianglelefteq \text{Inn}_{A_4}(S_4)$ and $\text{Aut}_{A_4}(S_4) = \text{Inn}(A_4)$, we have $\text{Aut}_{\widehat{A}_4}(A_4) \trianglelefteq \text{Inn}_{A_4}(S_4)$. \square

We will use the following propositions to prove Theorem 6.6. Nevertheless, the proofs of these propositions are routine, and we defer them to the appendix.

Proposition A.3. *Let $n \geq 5$ and $\phi \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles. If (xyz) and (abc) have two common symbols, then $\phi(xyz)$ and $\phi(abc)$ have two common symbols. Furthermore, after rotation the two common symbols of $\phi(xyz)$ and $\phi(abc)$ are in the corresponding positions of the common symbols in (xyz) and (abc) , respectively. More precisely,*

- (i) *For distinct $a, b, c, d \in \{1, 2, \dots, n\}$, $\phi(abc)$ and $\phi(abd)$ have two common symbols, and after rotation, we can write*

$$\phi(abc) = (a' b' c') \text{ and } \phi(abd) = (a' b' d').$$

where a', b', c', d' are all distinct.

- (ii) *For distinct $m, n, p, q \in \{1, 2, \dots, n\}$, $\phi(mnp)$ and $\phi(mqn)$ have two common symbols, and after rotation we can write*

$$\phi(mnp) = (m' n' p') \text{ and } \phi(mqn) = (m' q' n')$$

where m', n', p', q' are all distinct.

Proposition A.4. Let $n \geq 5$ and $\phi \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles. Then for every $a \in \{1, 2, \dots, n\}$ there exists a unique $a' \in \{1, 2, \dots, n\}$, such that

$$\begin{aligned} \phi\{(a m r) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} \\ = \{(a' x y) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}. \end{aligned}$$

Theorem 6.6. Let $n \geq 5$, and $\phi \in \text{Aut}(A_n)$. If ϕ maps 3-cycles to 3-cycles, then $\phi \in \text{Inn}_{A_n}(S_n)$.

Proof. Assume that ϕ map 3-cycles to 3-cycles. By Proposition A.4, for each a in $\{1, 2, \dots, n\}$, there exists a unique a' in $\{1, 2, \dots, n\}$ such that

$$\begin{aligned} \phi\{(a m r) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} \\ = \{(a' x y) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}. \end{aligned}$$

Define $x : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ by $x(a) = a'$ where a and a' are as above. Since ϕ is 1-1, x is 1-1. Because $\{1, 2, \dots, n\}$ is a finite set, x is bijective. That is $x \in S_n$. Claim that $\phi = \phi_x|_{A_n}$. To show this, let $(a b c)$ be a 3-cycle. We will apply Proposition A.4 to $\phi(a b c)$. Since $\phi(a b c) \in \phi\{(a m r) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} = \{(a' x y) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}$, where $a' = x(a)$, there are $x_1, y_1 \in \{1, 2, \dots, n\} - \{a'\}$, $x_1 \neq y_1$, such that

$$\phi(a b c) = (a' x_1 y_1) = (x(a) x_1 y_1).$$

Apply Proposition A.4 again, we have

$$\begin{aligned} \phi(a b c) &= \phi(b c a) \\ &\in \{(b m r) \mid m, r \in \{1, 2, \dots, n\} - \{b\}, m \neq r\} \\ &= \{(b' x y) \mid x, y \in \{1, 2, \dots, n\} - \{b'\}, x \neq y\}, \text{ where } b' = x(b). \end{aligned}$$

Then there are $x_2, y_2 \in \{1, 2, \dots, n\} - \{b'\}$, $x_2 \neq y_2$, and

$$\phi(bca) = (b'x_2y_2) = (x(b)x_2y_2).$$

Similarly, there are $x_3, y_3 \in \{1, 2, \dots, n\} - \{c'\}$, $x_3 \neq y_3$, and

$$\phi(cab) = (c'x_3y_3) = (x(c)x_3y_3).$$

Since $\phi(abc) = \phi(bca) = \phi(cab)$, we have

$$\phi(abc) = (x(a)x_1y_1) = (x(b)x_2y_2) = (x(c)x_3y_3).$$

Therefore $\phi(abc)$ contains $x(a)$, $x(b)$ and $x(c)$ as symbols in its cycle notation. Since $x(a)$, $x(b)$ and $x(c)$ are all distinct, and $\phi(abc)$ is a 3-cycles, we conclude that

$$\phi(abc) = (x(a)x(b)x(c)) \text{ or } (x(a)x(c)x(b)). \quad (6.1)$$

Suppose for a contradiction that

$$\phi(abc) = (x(a)x(c)x(b)). \quad (6.2)$$

Choose $d \in \{1, 2, \dots, n\} - \{a, b, c\}$. Using the same argument as $\phi(abc)$, we will have

$$\phi(abd) = (x(a)x(b)x(d)) \text{ or } (x(a)x(d)x(b)). \quad (6.3)$$

By Proposition A.3, $\phi(abc)$ and $\phi(abd)$ have two common symbols, and after rotations we can write $\phi(abc)$ and $\phi(abd)$ so that the common symbols lie in the first and second position. From (6.2) and (6.3), we can see that the common symbols of $\phi(abc)$ and $\phi(abd)$ are $x(a)$ and $x(b)$. Now, write

$$\phi(abc) = (x(b)x(a)x(c))$$

$$\phi(abd) = (x(b)x(d)x(a)) \text{ or } (x(b)x(a)x(d)).$$

Therefore

$$\phi(abd) = (x(b)x(a)x(d)). \quad (6.4)$$

Apply Proposition A.4 to $\phi(adc)$, we conclude that $\phi(adc)$ contains $x(a)$ as a symbol in its cycle notation. On the other hand, we obtain that

$$\begin{aligned} \phi(adc) &= \phi((abc)(adb)) \\ &= \phi(abc)\phi(adb) \\ &= \phi(abc)\phi(abd)^{-1} \\ &= \phi(abc)(\phi(abd))^{-1} \\ &= (x(a)x(c)x(b))(x(a)x(d)x(b))^{-1} \quad (\text{from (6.2) and (6.4)}) \\ &= (x(a)x(c)x(b))(x(a)x(b)x(d)) \\ &= (x(b)x(d)x(c)). \end{aligned}$$

This contradicts the fact that $\phi(adc)$ contains $x(a)$. This implies $\phi(abc) \neq (x(a)x(c)x(b))$.

From (6.1), we conclude that $\phi(abc) = (x(a)x(b)x(c))$. Now

$$\phi_x(abc) = x(abc)x^{-1} = (x(a)x(b)x(c)) = \phi(abc).$$

Since (abc) is arbitrary, ϕ and $\phi_x|_{A_n}$ are equal at every 3-cycle. Since 3-cycles generate A_n , we conclude that $\phi = \phi_x|_{A_n}$, and $\phi \in \text{Inn}_{A_n}(S_n)$. \square

Corollary 6.7. $\text{Aut}_{\widehat{A}_n}(A_n) \leq \text{Inn}_{A_n}(S_n)$ for every $n \geq 5$.

Proof. It suffices to prove $\text{Aut}_{\widehat{A}_n}(A_n) \subseteq \text{Inn}_{A_n}(S_n)$ since $\text{Inn}_{A_n}(S_n) \leq \text{Aut}(A_n)$ and $\text{Aut}_{\widehat{A}_n}(A_n) \leq \text{Aut}(A_n)$. Let $\phi \in \text{Aut}_{\widehat{A}_n}(A_n)$. Then ϕ preserves conjugacy classes of A_n . In particular, ϕ maps 3-cycles to 3-cycles. Apply the previous theorem, we obtain that $\phi \in \text{Inn}_{A_n}(S_n)$. This shows $\text{Aut}_{\widehat{A}_n}(A_n) \subseteq \text{Inn}_{A_n}(S_n)$. \square

Corollary 6.8. $\text{Inn}(A_n) \leq \text{Aut}_{\widehat{A}_n}(A_n) \leq \text{Inn}_{A_n}(S_n) \leq \text{Aut}(A_n)$ for every $n \geq 4$.

Proof. Combine Theorem 6.4, 6.5, and Corollary 6.7. \square

The next theorem appears in Exercise 2.12 of [13].

Theorem 6.9 ([13], p.89). *Let G be a group and let $H \leq G$ have index two. Then the following hold.*

(i) $H \trianglelefteq G$.

(ii) *Every conjugacy class of G having nonempty intersection with H becomes a conjugacy class of H or splits into two conjugacy classes of H having equal size. Furthermore, the conjugacy class K of G does not split in H if and only if some $k \in K$ commutes with some $g \notin H$.*

(iii) *Let χ be an irreducible character of G . Then $\chi|_H$ is irreducible or is the sum of two inequivalent irreducibles. Furthermore, $\chi|_H$ is irreducible if and only if $\chi(g) \neq 0$ for some $g \notin H$.*

Let A_n denote the alternating subgroup of S_n and consider $\pi \in S_n$ having cycle type $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_l)$ (see [13], p.2). Then

(iv) $\pi \in A_n$ if and only if $n - l$ is even.

(v) *The conjugacy classes of S_n that split in A_n are those where all parts of λ are odd and distinct.*

Theorem 6.10. $\text{Aut}_{\widehat{A}_n}(A_n) \subsetneq \text{Inn}_{A_n}(S_n)$ for every $n \geq 4$.

Proof. Let $n \geq 4$. We divide into 2 cases.

Case 1 : n is odd. Let $\alpha = (12 \dots n)$ be an n -cycle in S_n . Since n is odd, $\alpha \in A_n$. Also, the cycle type of α is $\lambda = (n)$. By Theorem 6.9(v), the conjugacy class of α in S_n split in A_n . That is there exists an n -cycle β in A_n such that α and β are conjugate in S_n but are not conjugate in A_n . Therefore there is a $\sigma \in S_n - A_n$ such that $\alpha = \sigma\beta\sigma^{-1} = \phi_\sigma(\beta)$. Then $\phi_\sigma \in \text{Inn}_{A_n}(S_n) - \text{Aut}_{\widehat{A}_n}(A_n)$. Therefore $\text{Aut}_{\widehat{A}_n}(A_n) \subsetneq \text{Inn}_{A_n}(S_n)$.

Case 2 : n is even. Let $\alpha = (12 \dots n - 1)$ and follow the same method as case 1, we will obtain $\sigma \in S_n - A_n$ such that $\phi_\sigma \in \text{Inn}_{A_n}(S_n) - \text{Aut}_{\widehat{A}_n}(A_n)$. Therefore $\text{Aut}_{\widehat{A}_n}(A_n) \subsetneq \text{Inn}_{A_n}(S_n)$. \square

Theorem 6.11. $\text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n)$ for every $n \geq 4$.

Proof. Let $n \geq 5$, $H = \text{Inn}(A_n)$, $K = \text{Aut}_{\widehat{A}_n}(A_n)$, and $G = \text{Inn}_{A_n}(S_n)$. Then by Corollary 6.8, we have

$$H \trianglelefteq K \trianglelefteq G.$$

By the Third Isomorphism Theorem, $\frac{G/H}{K/H} \cong G/K$. Then $|G/K||K/H| = |G/H| = \frac{|G|}{|H|} = \frac{n!}{\frac{n!}{2}} = 2$. Therefore $1 \leq |G/K| \leq 2$. From Theorem 6.10, $K \neq G$, so $|G/K| \neq 1$. Thus $|G/K| = 2$. Hence $|K/H| = 1$. Then $|K| = |H|$. Since $H \subseteq K$ and K is finite, $H = K$. That is $\text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n)$. \square

Corollary 6.12. $\text{Inn}(A_n) = \text{Aut}_{\widehat{A}_n}(A_n) \neq \text{Aut}(A_n)$ for every $n \geq 4$.

Proof. Combine Theorems 6.4, 6.10, and 6.11. \square

6.2 $\text{Aut}(A_n)$

In this section, we will give a relation between $\text{Aut}(A_n)$ and $\text{Inn}_{A_n}(S_n)$ which is stronger than that given in Theorem 6.4. In addition, we find a concrete group to which $\text{Aut}(A_n)$ is isomorphic. First, we give two lemmas about inequalities which are proved by induction.

Lemma 6.13. $\forall k \geq 3, (3k - 3)! > 6^{k-1}k!$.

Proof. We will prove by induction.

For $k = 3$, we have $(3k - 3)! = 6! = 6 \times 120 > 6 \times 36 = 6^{3-1}3! = 6^{k-1}k!$.

Assume that $k \geq 3$ and $(3k - 3)! > 6^{k-1}k!$. Then we obtain that

$$\begin{aligned} (3(k+1) - 3)! &= (3k)! \\ &= (3k)(3k-1)(3k-2)(3k-3)! \\ &> (3k)(3k-1)(3k-2)6^{k-1}k! \\ &> (3k)(3k-1)(6)6^{k-1}k! \\ &> (k+1)6^k k! \\ &= 6^{(k+1)-1}(k+1)!. \end{aligned}$$

Therefore $(3k - 3)! > 6^{k-1}k!$ for every $k \geq 3$. \square

Lemma 6.14. $\forall n \geq 7, \forall k \in \mathbb{N}, 2 \leq k \leq \frac{n}{3} \rightarrow (n - 3)! > 6^{k-1}k!(n - 3k)!$.

Proof. We will prove this statement by induction on n .

Let $n = 7$. The only $k \in \mathbb{N}$ such that $2 \leq k \leq \frac{7}{3}$ is $k = 2$. Then we have $(n - 3)! = 24$, $6^{k-1}k!(n - 3k)! = 12$, and $(n - 3)! > 6^{k-1}k!(n - 3k)!$. Let $n = 8$. Similar to the case $n = 7$, we will have $(n - 3)! > 6^{k-1}k!(n - 3k)!$. Next, assume that $n \geq 8$ and

$$\forall k \in \mathbb{N}, 2 \leq k \leq \frac{n}{3} \rightarrow (n - 3)! > 6^{k-1}k!(n - 3k)!.$$

Let $k \in \mathbb{N}$ be such that $2 \leq k \leq \frac{n+1}{3}$. We will divide into 2 cases :

case 1 : $6 \leq 3k \leq n$. Then

$$\begin{aligned} (n + 1 - 3)! &= (n - 2)! \\ &= (n - 2)(n - 3)! \\ &> (n - 2)6^{k-1}k!(n - 3k)! \quad (\text{by induction hypothesis}) \\ &> (n - 3k + 1)6^{k-1}k!(n - 3k)! \quad (n - 2 > n - 3k + 1) \\ &= 6^{k-1}k!(n + 1 - 3k)! \end{aligned}$$

case 2 : $3k = n + 1$. Then $6^{k-1}k!(n + 1 - 3k)! = 6^{k-1}k!$, and $(n + 1 - 3)! = (3k - 3)!$. Since $n \geq 8$, we have $k = \frac{n + 1}{3} \geq 3$. Thus by Lemma 6.13, we obtain $(3k - 3)! > 6^{k-1}k!$.

That is $(n + 1 - 3)! > 6^{k-1}k!(n + 1 - 3k)!$. \square

Corollary 6.15.

$$\forall n \geq 7, \forall k \in \mathbb{N}, 2 \leq k \leq \frac{n}{3} \rightarrow 2^{k-1}(n - 3)! > 6^{k-1}k!(n - 3k)!.$$

Lemma 6.16 ([3], p.33). *Let p be a prime number. Then an element has order p in S_n if and only if its cycle decomposition is a product of commuting p -cycles.*

Theorem 6.17. *Let $n \geq 4$, $n \neq 6$, and $\phi \in \text{Aut}(A_n)$. Then ϕ maps 3-cycles to 3-cycles.*

Proof. First, we consider in the case $n \in \{4, 5\}$. Let σ be a 3-cycle in A_n . Then $|\phi(\sigma)| = |\sigma| = 3$. Then, by Lemma 6.16, $\phi(\sigma)$ is the product of disjoint 3-cycles. Since $n \in \{4, 5\}$, there are no pair of disjoint 3-cycles. Hence $\phi(\sigma)$ is a 3-cycle. This shows that ϕ maps 3-cycles to 3-cycles. Now assume that $n \geq 7$. For each $k \in \mathbb{N}$ with $3k \leq n$, let C_k be the set of all even permutations in A_n which are the product of k 3-cycles. That is

$$C_k = \left\{ \sigma \in A_n \left| \begin{array}{l} \sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \cdots (a_{3k-2} a_{3k-1} a_{3k}) \text{ and} \\ a_1, \dots, a_{3k} \in \{1, 2, \dots, n\} \text{ are all distinct} \end{array} \right. \right\}.$$

By Theorem 6.9, C_k is a conjugacy class of A_n for every k . In particular, C_1 is the conjugacy class of 3-cycles. Let σ be a 3-cycle. Then $|\phi(\sigma)| = |\sigma| = 3$. By Lemma 6.16, $\phi(\sigma)$ is a product of disjoint 3-cycles. That is $\phi(\sigma) \in C_k$ for some $k \in \mathbb{N}$. This implies that $\phi(C_1) = C_k$ for some $k \in \mathbb{N}$. We claim that $\phi(C_1) = C_1$. Suppose that there exists $2 \leq k \leq \frac{n}{3}$ such that $\phi(C_1) = C_k$. Since ϕ is bijective, $|C_1| = |C_k|$. Therefore

$$\begin{aligned} \frac{2n!}{3!(n-3)!} &= 2 \binom{n}{3} = |C_1| = |C_k| \\ &= \frac{2^k}{k!} \binom{n}{3} \binom{n-3}{3} \cdots \binom{n-3(k-1)}{3} \\ &= \frac{2^k}{k!} \frac{n!}{3!(n-3)! 3!(n-6)! \cdots 3!(n-3k)!} \\ &= \frac{2^k}{k!} \frac{n!}{(3!)^k (n-3k)!} \end{aligned}$$

This implies $2^{k-1}(n-3)! = 6^{k-1}k!(n-3k)!$ which contradicts Corollary 6.15. Hence $\phi(C_1) = C_1$. That is ϕ maps 3-cycles to 3-cycles. \square

Corollary 6.18. *Let $n \geq 4$ and $n \neq 6$. Then*

(i) $\text{Aut}(A_n) = \text{Inn}_{A_n}(S_n),$

(ii) $|\text{Aut}(A_n)| = n!,$

(iii) $|\text{Out}(A_n)| = 2.$

Proof. First assume that $n \geq 5$ and $n \neq 6$. Then we obtain that (i) follows from Theorems 6.4, 6.6 and 6.17. (ii) follows from (i), and Theorem 6.3(ii). (iii) follows from (ii), and Theorem 6.1(iii).

Next, let $n = 4$. We will show that $\text{Aut}(A_4) = \text{Inn}_{A_4}(S_4)$.

Recall (see in the proof of Theorem 6.5) that $A_4 = \langle (123), (134) \rangle$ and the conjugacy class

$$K_{(123)} = \{(123), (134), (142), (243)\} \text{ together with}$$

$$K_{(132)} = \{(132), (143), (124), (234)\} \text{ contains all 3-cycles in } A_4.$$

Let $\phi \in \text{Aut}(A_4)$. Since $A_4 = \langle (123), (134) \rangle$, ϕ is completely determined by $\phi(123)$ and $\phi(134)$. Also, by Theorem 6.17, ϕ maps 3-cycles to 3-cycles. Therefore $\phi(123) \in K_{(123)} \cup K_{(132)}$. In addition, by Theorem 3.8,

$$\text{if } \phi(123) \in K_{(123)}, \text{ then } \phi(134) \in K_{(123)} \text{ and}$$

$$\text{if } \phi(123) \in K_{(132)}, \text{ then } \phi(134) \in K_{(132)}.$$

Thus there are at most 8 choices for the $\phi(123)$ and after $\phi(123)$ is known, there are at most 3 choices for $\phi(134)$. This implies that

$$|\text{Aut}(A_4)| \leq 8 \cdot 3 = 24 = 4! = \text{Inn}_{A_4}(S_4).$$

From Theorem 6.4, $\text{Inn}_{A_4}(S_4) \leq \text{Aut}(A_4)$, so we obtain that

$$\text{Aut}(A_4) = \text{Inn}_{A_4}(S_4).$$

This proves (i). (ii) follows from (i), and Theorem 6.3(ii). (iii) follows from (ii), and Theorem 6.1(iii).

□

Theorem 6.19. (i) $\text{Inn}_{A_n}(S_n) \cong S_n$ for every $n \geq 3$.

(ii) $\text{Aut}(A_n) \cong S_n$ for every $n \geq 4$, $n \neq 6$.

Proof. Let $f : \text{Inn}(S_n) \rightarrow \text{Inn}_{A_n}(S_n)$ be defined by $f(\phi_x) = \phi_x|_{A_n}$. Let $\phi_x, \phi_y \in \text{Inn}(S_n)$. Then

$$f(\phi_x\phi_y) = f(\phi_{xy}) = \phi_{xy}|_{A_n} = (\phi_x\phi_y)|_{A_n} = (\phi_x|_{A_n})(\phi_y|_{A_n}) = f(\phi_x)f(\phi_y).$$

Therefore f is a homomorphism.

$$\begin{aligned} f(\phi_x) = f(\phi_y) &\rightarrow \phi_x|_{A_n} = \phi_y|_{A_n} \\ &\rightarrow x = y \\ &\rightarrow \phi_x = \phi_y. \end{aligned}$$

Hence f is 1-1. Thus f is an isomorphism. Hence $\text{Inn}_{A_n}(S_n) \cong \text{Inn}(S_n)$. Since $\text{Inn}(S_n) \cong S_n$, we obtain that $\text{Inn}_{A_n}(S_n) \cong S_n$. This proves (i). For $n \geq 4$, $n \neq 6$, we obtain from (i) and Corollary 6.18(i) that

$$\text{Aut}(A_n) = \text{Inn}_{A_n}(S_n) \cong S_n.$$

□

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER VII

Semidirect product $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$

7.1 Definition and notation

Recall from Theorem 4.10 that $\text{Aut}(D_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$. It is easy to see that

$$(r \mapsto r^i, s \mapsto s)(r \mapsto r, s \mapsto sr^m)(r \mapsto r^i, s \mapsto s)^{-1} = (r \mapsto r, s \mapsto sr^{im}).$$

This shows that the action of \mathbb{Z}_n^\times on \mathbb{Z}_n in the semidirect product is given by

$$i \cdot m = im \quad \text{for } i \in \mathbb{Z}_n^\times, m \in \mathbb{Z}_n. \quad (7.1)$$

This action corresponds to an isomorphism ϕ from \mathbb{Z}_n^\times to $\text{Aut}(\mathbb{Z}_n)$ given by

$$\phi(a)(x) = ax \quad \text{for all } a \in \mathbb{Z}_n^\times, x \in \mathbb{Z}_n \text{ ([3], p.135)}.$$

In addition, from this action, we have the formula for the multiplication in $\mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ as follows : for all $(m, i), (l, j) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$

$$(m, i)(l, j) = (m + il, ij). \quad (7.2)$$

In this chapter, we compute $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$, and $\text{Aut}_{\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ and show that they are not equal. That is there is an automorphism which preserves conjugacy classes of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$ but is not an inner automorphism of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$. First, we give two lemmas which will be used in the calculation.

Lemma 7.1. *Let $H = \langle A \rangle$ and $K = \langle B \rangle$ be finite groups generated by $A \subseteq H$, and $B \subseteq K$, respectively. Then $H \rtimes K$ is generated by $\{(a, 1) \mid a \in A\} \cup \{(1, b) \mid b \in B\}$. In*

particular, if $K = \mathbb{Z}_n^\times = \langle b_1, b_2, \dots, b_l \rangle$, and $H = \mathbb{Z}_n = \langle 1 \rangle$, then

$$H \rtimes K = \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times = \langle (1, 1), (0, b_1), (0, b_2), \dots, (0, b_l) \rangle.$$

Proof. Let $(h, k) \in H \rtimes K$. Then $(h, k) = (h, 1)(1, k)$. Since $H = \langle A \rangle$ and $h \in H$, there exist $a_1, a_2, \dots, a_m \in A$ such that $h = a_1^{l_1} a_2^{l_2} \dots a_m^{l_m}$, where $l_1, \dots, l_m \in \{1, -1\}$. Similarly, there are $b_1, \dots, b_k \in B$ and $n_1, \dots, n_k \in \{1, -1\}$ such that $k = b_1^{n_1} b_2^{n_2} \dots b_k^{n_k}$. Then

$$(h, k) = (h, 1)(1, k) = (a_1^{l_1}, 1) \dots (a_m^{l_m}, 1)(1, b_1^{n_1})(1, b_2^{n_2}) \dots (1, b_k^{n_k}).$$

This shows that $H \rtimes K$ is generated by $\{(a, 1) \mid a \in A\} \cup \{(1, b) \mid b \in B\}$. \square

Assume that $\mathbb{Z}_n^\times = \langle b_1, \dots, b_l \rangle$. From Lemma 7.1, we have that every endomorphism ϕ of $\mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$ is completely determined by $\phi(1, 1), \phi(0, b_1), \dots, \phi(0, b_l)$. Like the notation used in Chapter IV, if $\phi \in \text{Hom}(\mathbb{Z}_n \rtimes \mathbb{Z}_n^\times)$ mapping $(1, 1), (0, b_1), \dots$, and $(0, b_l)$ to $(m_0, i_0), (m_1, i_1), \dots$, and (m_l, i_l) , respectively, we will denote ϕ by the diagram

$$((1, 1) \mapsto (m_0, i_0), (0, b_1) \mapsto (m_1, i_1), \dots, (0, b_l) \mapsto (m_l, i_l))$$

Lemma 7.2. *Let $(m, i) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$. Then*

$$(l, j)(m, i)(l, j)^{-1} = (l + jm - il, i)$$

for all $(l, j) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$.

Proof. Let $(l, j) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$. Then

$$\begin{aligned} (l, j)(m, i)(l, j)^{-1} &= (l, j)(m, i)(j^{-1} \cdot l^{-1}, j^{-1}) \\ &= (l, j)(m, i)(-j^{-1}l, j^{-1}) \\ &= (l, j)(m - ij^{-1}l, ij^{-1}) \\ &= (l + jm - il, i). \end{aligned}$$

\square

We will use the formula in Lemma 7.2 to calculate $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ and conjugacy classes of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$.

7.2 All conjugacy classes of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$

From Lemma 7.2, for each $(m, i) \in \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$, we have

$$K_{(m,i)} = \{(l + jm - il, i) \mid l \in \mathbb{Z}_8, j \in \mathbb{Z}_8^\times\}.$$

We compute directly by this formula all conjugacy classes of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$ and the results are shown as follows.

$$K_{(0,1)} = \{(0, 1)\}$$

$$K_{(0,3)} = \{(0, 3), (2, 3), (4, 3), (6, 3)\}$$

$$K_{(0,5)} = \{(0, 5), (4, 5)\}$$

$$K_{(0,7)} = \{(0, 7), (2, 7), (4, 7), (6, 7)\}$$

$$K_{(1,1)} = \{(1, 1), (3, 1), (5, 1), (7, 1)\}$$

$$K_{(1,3)} = \{(1, 3), (3, 3), (5, 3), (7, 3)\}$$

$$K_{(1,5)} = \{(1, 5), (3, 5), (5, 5), (7, 5)\}$$

$$K_{(1,7)} = \{(1, 7), (3, 7), (5, 7), (7, 7)\}$$

$$K_{(2,1)} = \{(2, 1), (6, 1)\}$$

$$K_{(2,5)} = \{(2, 5), (6, 5)\}$$

$$K_{(4,1)} = \{(4, 1)\}$$

7.3 Inn($\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$)

Since $\mathbb{Z}_8 = \langle 1 \rangle$ and $\mathbb{Z}_8^\times = \langle 3, 5 \rangle$, by Lemma 7.1, we obtain that

$$\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times = \langle (1, 1), (0, 3), (0, 5) \rangle$$

and every $\phi \in \text{Hom}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ is completely determined by $\phi(1, 1)$, $\phi(0, 3)$, and $\phi(0, 5)$. As mentioned before, we use the same notation as in Chapter IV. Thus we denote ϕ by the diagram

$$((1, 1) \mapsto (m_1, i_1), (0, 3) \mapsto (m_2, i_2), (0, 5) \mapsto (m_3, i_3))$$

when $\phi \in \text{Hom}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ mapping $(1, 1)$, $(0, 3)$, and $(0, 5)$ to (m_1, i_1) , (m_2, i_2) , and (m_3, i_3) , respectively. Let $(m, i) \in \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$. The values of $\phi_{(m, i)}$ at $(1, 1)$, $(0, 3)$, and $(0, 5)$ are shown below.

$$\begin{aligned} (1, 1) &\rightarrow (m, i)(1, 1)(m, i)^{-1} = (m + i - m, 1) = (i, 1) \\ (0, 3) &\rightarrow (m, i)(0, 3)(m, i)^{-1} = (m + 0 - 3m, 3) = (-2m, 3) \\ (0, 5) &\rightarrow (m, i)(0, 5)(m, i)^{-1} = (m + 0 - 5m, 5) = (-4m, 5) \end{aligned} \quad (7.3)$$

Therefore

$$\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) = \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (-2m, 3), (0, 5) \mapsto (-4m, 5)) \mid m \in \mathbb{Z}_8, i \in \mathbb{Z}_8^\times\}.$$

It is easy to see that $\{(-2m, -4m) \mid m \in \mathbb{Z}_8\} = \{(0, 0), (6, 4), (4, 0), (2, 4)\}$. Hence

$$\begin{aligned} \text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) &= \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (0, 3), (0, 5) \mapsto (0, 5)) \mid i \in \{1, 3, 5, 7\}\} \\ &\cup \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (6, 3), (0, 5) \mapsto (4, 5)) \mid i \in \{1, 3, 5, 7\}\} \\ &\cup \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (4, 3), (0, 5) \mapsto (0, 5)) \mid i \in \{1, 3, 5, 7\}\} \\ &\cup \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (2, 3), (0, 5) \mapsto (4, 5)) \mid i \in \{1, 3, 5, 7\}\} \end{aligned}$$

and $|\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)| = 16$.

7.4 $\text{Aut}_{\widehat{\mathbb{Z}_8 \times \mathbb{Z}_8^\times}}(\mathbb{Z}_8 \times \mathbb{Z}_8^\times)$

In this section, we calculate the set of all automorphisms preserving conjugacy classes of $\mathbb{Z}_8 \times \mathbb{Z}_8^\times$. To do this, we first find a presentation of $\mathbb{Z}_8 \times \mathbb{Z}_8^\times$.

Proposition 7.3 ([7], p.71). *Let R be a set of relations between elements of a set X . Let G be a group and $\varphi : X \rightarrow G$ be a mapping such that every relation $u = v$ in R holds in G (via φ). There is a unique homomorphism $\psi : \langle X; R \rangle \rightarrow G$ such that $\psi(x) = \varphi(x)$ for every $x \in X$. If G is generated by $\varphi(X)$, then ψ is surjective.*

Theorem 7.4. $\mathbb{Z}_8 \times \mathbb{Z}_8^\times \cong \langle a, b, c \mid a^8 = b^2 = c^2 = 1, bab = a^3, cac = a^5, bc = cb \rangle$.

Proof. Let $H = \langle a, b, c \mid a^8 = b^2 = c^2 = 1, bab = a^3, cac = a^5, bc = cb \rangle$. Since a, b , and c have finite orders, every element of G is a finite product of a, b , and c . Since $b^2 = c^2 = 1$, we have $b = b^{-1}$ and $c = c^{-1}$. From $bab = a^3$, and $cac = a^5$, we obtain that $ba = a^3b^{-1} = a^3b$, and $ca = a^5c^{-1} = a^5c$. This implies that the product of a, b , and c can be written so that all of a appear before b and c . In addition, since $bc = cb$, the products of a, b , and c can be written in the form $a^k b^i c^j$. Since $a^8 = b^2 = c^2 = 1$, we can assume that $0 \leq k \leq 7, 0 \leq i \leq 1, 0 \leq j \leq 1$. Hence H has at most 32 elements, $1, a, a^2, \dots, a^7, b, ab, \dots, a^7b, c, ac, a^2c, \dots, a^7c, bc, abc, \dots, a^7bc$.

Next, let $x = (1, 1), y = (0, 3), z = (0, 5) \in \mathbb{Z}_8 \times \mathbb{Z}_8^\times$. Let $\varphi : \{a, b, c\} \rightarrow \mathbb{Z}_8 \times \mathbb{Z}_8^\times$ be defined by $a \mapsto x, b \mapsto y, c \mapsto z$. It is easy to see that x, y , and z satisfy the relation in the presentation of H when a, b , and c are replaced by x, y , and z , respectively. In addition, we know that x, y , and z generate $\mathbb{Z}_8 \times \mathbb{Z}_8^\times$. Therefore, by Proposition 7.3, there exists an epimorphism $\psi : H \rightarrow \mathbb{Z}_8 \times \mathbb{Z}_8^\times$ mapping a to x, b to y , and c to z . Thus

$$|H| \leq 32 = |\mathbb{Z}_8||\mathbb{Z}_8^\times| = |\mathbb{Z}_8 \times \mathbb{Z}_8^\times| \leq |H|.$$

Hence $|H| = 32$ and ϕ is an isomorphism. \square

Corollary 7.5. *Let $a = (1, 1), b = (0, 3), c = (0, 5) \in \mathbb{Z}_8 \times \mathbb{Z}_8^\times$. Then*

$$\mathbb{Z}_8 \times \mathbb{Z}_8^\times = \langle a, b, c \mid a^8 = b^2 = c^2 = 1, bab = a^3, cac = a^5, bc = cb \rangle.$$

Lemma 7.6. *The map $(1, 1) \rightarrow (1, 1)$, $(0, 3) \rightarrow (2, 3)$, $(0, 5) \rightarrow (0, 5)$ extends to a unique automorphism of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$.*

Proof. We use the presentation of $\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$ in the previous Corollary. It can be checked directly that $(1, 1)$, $(2, 3)$, and $(0, 5)$ satisfy the relation in the presentation. Then, by Proposition 7.3, the map extends to a unique homomorphism $\phi : \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times \rightarrow \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$. Since $(1, 1)^6(2, 3) = (6, 1)(2, 3) = (0, 3)$, we obtain that $(0, 3) \in \langle (1, 1), (2, 3), (0, 5) \rangle$ and that $\langle (1, 1), (2, 3), (0, 5) \rangle = \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$. Therefore ϕ is onto and thus an isomorphism. \square

Theorem 7.7. *Let $G = \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times$. Then*

$$(i) \text{ Aut}_{\widehat{G}}(G) = \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (m, 3), (0, 5) \mapsto (l, 5)) \mid i \in \{1, 3, 5, 7\}, \\ m \in \{0, 2, 4, 6\}, l \in \{0, 4\}\}.$$

$$(ii) \text{ } |\text{Aut}_{\widehat{G}}(G)| = 32.$$

$$(iii) \text{ Aut}_{\widehat{G}}(G) \neq \text{Inn}(G).$$

Proof. Let $H = \{((1, 1) \mapsto (i, 1), (0, 3) \mapsto (m, 3), (0, 5) \mapsto (l, 5)) \mid i \in \{1, 3, 5, 7\}, m \in \{0, 2, 4, 6\}, l \in \{0, 4\}\}$. First we show that $\text{Aut}_{\widehat{G}}(G) \subseteq H$. Let $\phi \in \text{Aut}_{\widehat{G}}(G)$. Then ϕ preserves conjugacy classes of G . From the calculation in Section 7.2, we have

$$\phi_{(1,1)} \in K_{(1,1)} = \{(1, 1), (3, 1), (5, 1), (7, 1)\},$$

$$\phi_{(0,3)} \in K_{(0,3)} = \{(0, 3), (2, 3), (4, 3), (6, 3)\},$$

$$\phi_{(0,5)} \in K_{(0,5)} = \{(0, 5), (4, 5)\}.$$

This shows that $\phi \in H$, and $\text{Aut}_{\widehat{G}}(G) \subseteq H$. It is easy to see that $|H| = 32$. Therefore $|\text{Aut}_{\widehat{G}}(G)| \leq 32$. Since $\text{Inn}(G) \trianglelefteq \text{Aut}_{\widehat{G}}(G)$ and $|\text{Inn}(G)| = 16$, we have 16 divide $|\text{Aut}_{\widehat{G}}(G)|$. Then the possible order of $\text{Aut}_{\widehat{G}}(G)$ is 16 or 32. To show that $\text{Aut}_{\widehat{G}}(G) = H$, it suffices to find an automorphism of G preserving conjugacy class of G but not inner. Let ϕ be an automorphism given in Lemma 7.6. From the calculation of $\text{Inn}(G)$ in Section 7.3, we can see that ϕ is not inner. Next, we show that ϕ preserves conjugacy classes

of G . Let $m \in \{0, 1, \dots, 7\}$. Then

$$\begin{aligned}
\phi(m, 1) &= \phi(1, 1)^m = (1, 1)^m = (m, 1), \\
\phi(m, 3) &= \phi((m, 1)(0, 3)) = (m, 1)(2, 3) = (m+2, 3) \\
\phi(m, 5) &= \phi((m, 1)(0, 5)) = (m, 1)(0, 5) = (m, 5) \\
\phi(m, 7) &= \phi((m, 1)(0, 7)) = \phi((m, 1)(0, 3)(0, 5)) \\
&= (m, 1)(2, 3)(0, 5) = (m, 1)(2, 7) = (m+2, 7) \\
(m+2, 3) &= (3, 1)(m, 3)(3, 1)^{-1} \\
(m+2, 7) &= (1, 1)(m, 7)(1, 1)^{-1}.
\end{aligned}$$

This implies that ϕ preserves conjugacy classes of G . Hence $|\text{Aut}_{\widehat{G}}(G)| > 16$. Thus $|\text{Aut}_{\widehat{G}}(G)| = 32$. This prove (ii) and (iii). Since $\text{Aut}_{\widehat{G}}(G) \subseteq H$ and $|H| = 32$, we obtain that $\text{Aut}_{\widehat{G}}(G) = H$, which is (i). \square

Next, we find groups to which $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ and $\text{Aut}_{\widehat{\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times}}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$ are isomorphic.

Theorem 7.8. $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_8^\times$.

Proof. We will apply Theorem 4.9, to prove this theorem. Recall that

$$\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) = \{\phi_{(m,i)} \mid (m,i) \in \mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times\}.$$

Let $H = \langle \phi_{(1,1)} \rangle$, and $K = \langle \phi_{(0,3)}, \phi_{(0,5)} \rangle$. Since $(\phi_{(1,1)})^l = \phi_{(1,1)^l} = \phi_{(l,1)}$, we obtain that $H = \{\phi_{(l,1)} \mid l \in \mathbb{Z}_8\}$. Also, we can see that $\phi_{(4,1)}$ fixes $(1,1)$, $(0,3)$, and $(0,5)$, and thus it is the identity map. Then

$$|\phi_{(1,1)}| = 4 \quad \text{and} \quad H = \langle \phi_{(1,1)} \rangle \cong \mathbb{Z}_4. \quad (7.4)$$

Next, consider the group K . Since $\phi_{(0,3)}\phi_{(0,5)} = \phi_{(0,5)}\phi_{(0,3)} = \phi_{(0,7)}$ and $|\phi_{(0,3)}| = |\phi_{(0,5)}| = 2$, we obtain that

$$\begin{aligned}
K &= \{(\phi_{(0,3)})^l(\phi_{(0,5)})^k \mid l, k \in \{1, 2\}\} \\
&= \{\phi_{(0,3)}, \phi_{(0,5)}, \phi_{(0,7)}, \text{id}\}.
\end{aligned}$$

It is the fact that a group of order 4 which is not cyclic is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. From this, we can see that

$$K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_8^\times. \quad (7.5)$$

Next, we will show that $H \leq \text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$. Let $\phi_{(m,i)} \in \text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)$. Then

$$\begin{aligned} \phi_{(m,i)}\phi_{(l,1)}(\phi_{(m,i)})^{-1} &= \phi_{(m,i)(l,1)(m,i)^{-1}} \\ &= \phi_{(m+il-m,1)} \\ &= \phi_{(il,1)} \in H, \quad \text{for all } l \in \mathbb{Z}_8. \end{aligned}$$

Hence

$$H \leq \text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times). \quad (7.6)$$

From (7.4), and (7.5), we know that

$$\begin{aligned} H &= \{\phi_{(1,1)}, \phi_{(2,1)}, \phi_{(3,1)}, \phi_{(4,1)}\} \\ K &= \{\phi_{(0,3)}, \phi_{(0,5)}, \phi_{(0,7)}, \text{id}\}. \end{aligned}$$

We can see that any nonidentity map in H maps $(1, 1)$ to $(1, 1)$, while any nonidentity map in K maps $(1, 1)$ to $(3, 1)$, $(5, 1)$ or $(7, 1)$. Hence

$$H \cap K = \{\text{id}\}. \quad (7.7)$$

Also,

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{4 \times 4}{1} = 16 = |\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times)|.$$

Therefore

$$\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) = HK. \quad (7.8)$$

From (7.4) to (7.8), we obtain that $\text{Inn}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_8^\times$. \square

Next, we will show that $\text{Aut}_{\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times}(\mathbb{Z}_8 \rtimes \mathbb{Z}_8^\times) \cong (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_8^\times$. To show this, we will apply the next theorem in the proof.

Theorem 7.9 ([3]). Suppose G is a group such that

$$(1) H \triangleleft G \text{ and } K \triangleleft G$$

$$(2) H \cap K = 1.$$

Then $HK \cong H \times K$.

Theorem 7.10. $\text{Aut}_{\mathbb{Z}_8 \times \mathbb{Z}_8^\times}(\mathbb{Z}_8 \times \mathbb{Z}_8^\times) \cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times \mathbb{Z}_8^\times$.

Proof. Let $G = \mathbb{Z}_8 \times \mathbb{Z}_8^\times$, $K = \langle \phi_{(0,3)}, \phi_{(0,5)} \rangle$, and $H = \langle \phi_{(1,1)}, \phi \rangle$ where $\phi \in \text{Aut}_{\widehat{G}}(G)$ be defined by $\phi(1,1) = (1,1)$, $\phi(0,3) = (4,3)$, $\phi(0,5) = (0,5)$ (see Theorem 7.7(i)).

Consider the following diagram of mapping

$$\begin{array}{l} \phi_{(1,1)}\phi \quad (1,1) \xrightarrow{\phi} (1,1) \xrightarrow{\phi_{(1,1)}} (1,1) \\ \quad (0,3) \xrightarrow{\phi} (4,3) = (1,1)^4(0,3) \xrightarrow{\phi_{(1,1)}} (1,1)^4(6,3) = (10,3) = (2,3) \\ \quad (0,5) \xrightarrow{\phi} (0,5) \xrightarrow{\phi_{(1,1)}} (4,5) \\ \phi\phi_{(1,1)} \quad (1,1) \xrightarrow{\phi_{(1,1)}} (1,1) \xrightarrow{\phi} (1,1) \\ \quad (0,3) \xrightarrow{\phi_{(1,1)}} (6,3) = (1,1)^6(0,3) \xrightarrow{\phi} (1,1)^6(4,3) = (10,3) = (2,3) \\ \quad (0,5) \xrightarrow{\phi_{(1,1)}} (4,5) = (1,1)^4(0,5) \xrightarrow{\phi} (1,1)^4(0,5) = (4,5). \end{array}$$

Hence $\phi\phi_{(1,1)} = \phi_{(1,1)}\phi$. Also, $|\phi| = 2$ and $|\phi_{(1,1)}| = 4$. Then

$$H = \{(\phi_{(1,1)})^l \phi^k \mid l \in \{1, 2, 3, 4\}, k \in \{1, 2\}\}.$$

Let $H_1 = \langle \phi_{(1,1)} \rangle$, and $H_2 = \langle \phi \rangle$. Then $H_1 \cong \mathbb{Z}_4$, and $H_2 \cong \mathbb{Z}_2$, and $H_1 \cap H_2 = \{\text{id}\}$.

Therefore

$$|H_1 H_2| = \frac{|H_1| |H_2|}{|H_1 \cap H_2|} = \frac{4 \times 2}{1} = 8 \geq |H| \geq |H_1 H_2|.$$

Hence $H = H_1 H_2$. Since $\phi_{(1,1)}$ and ϕ commute, we obtain that $H_1 \triangleleft H$, and $H_2 \triangleleft H$. By Theorem 7.9, we obtain that

$$H = H_1 H_2 \cong H_1 \times H_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_2. \quad (7.9)$$

From the proof of Theorem 7.8, we know that

$$K \cong \mathbb{Z}_8^\times, \quad (7.10)$$

and $\{\phi_{(1,1)}, \phi_{(2,1)}, \phi_{(3,1)}, \phi_{(4,1)}\} \cap K = \{\text{id}\}$. Since $\phi_{(1,1)}\phi$, $\phi_{(2,1)}\phi$, $\phi_{(3,1)}\phi$ and $\phi_{(4,1)}\phi$ are all outer automorphism, we can see that

$$H \cap K = \{\phi_{(a,1)}\phi^k \mid k \in \{1, 2\}, a \in \{1, 2, 3, 4\}\} \cap K = \{\text{id}\}. \quad (7.11)$$

Therefore $|KH| = |HK| = |H||K| = 8 \times 4 = 32 = |G|$, and thus

$$G = HK = KH. \quad (7.12)$$

Next, we will show that $H \trianglelefteq G$. Let $g \in G$. Then there exist $k \in K$ and $h \in H$ such that $g = kh$. Let $h_0 \in H$. Then $gh_0g^{-1} = kh_0h^{-1}k^{-1} = kh_0k^{-1}$ (since H is abelian). From this, we can see that

$$H \triangleleft G \leftrightarrow \forall k \in K \forall h \in H, khk^{-1} \in H.$$

Let $a \in \{1, 3, 5, 7\}$ and $b \in \{1, 2, 3, 4\}$,

$$\begin{aligned} \phi_{(0,a)}\phi_{(b,1)}(\phi_{(0,a)})^{-1} &= \phi_{(0,a)}\phi_{(b,1)}\phi_{(0,a)} \\ &= \phi_{(0,a)(b,1)(0,a)} \\ &= \phi_{(ab,a^2)} \\ &= \phi_{(ab,1)} \in H. \end{aligned}$$

Next, we will show that $\phi_{(0,a)}\phi_{(b,1)}(\phi_{(0,a)})^{-1} \in H$. Consider the following diagram of mapping

$$\begin{aligned}
\phi_{(0,a)}\phi & (1, 1) \xrightarrow{\phi} (1, 1) \xrightarrow{\phi_{(0,a)}} (a, 1) \\
(0, 3) & \xrightarrow{\phi} (4, 3) = (1, 1)^4(0, 3) \xrightarrow{\phi_{(0,a)}} (a, 1)^4(0, 3) \\
& = (4a, 1)(0, 3) = (4a, 3) = (4, 3) \\
(0, 5) & \xrightarrow{\phi} (0, 5) \xrightarrow{\phi_{(0,a)}} (0, 5)
\end{aligned}$$

$$\begin{aligned}
\phi\phi_{(0,a)} & (1, 1) \xrightarrow{\phi_{(0,a)}} (a, 1) = (1, 1)^a \xrightarrow{\phi} (1, 1)^a = (a, 1) \\
(0, 3) & \xrightarrow{\phi_{(0,a)}} (0, 3) \xrightarrow{\phi} (4, 3) \\
(0, 5) & \xrightarrow{\phi_{(0,a)}} (0, 5) \xrightarrow{\phi} (0, 5).
\end{aligned}$$

We can see that $\phi\phi_{(0,a)} = \phi_{(0,a)}\phi$. Therefore

$$\begin{aligned}
\phi_{(0,a)}\phi & \rightarrow \phi_{(b,1)}\phi_{(0,a)^{-1}} = \phi(\phi_{(0,a)}\phi_{(b,1)}(\phi_{(0,a)})^{-1}) \\
& \in \phi H = H.
\end{aligned}$$

Thus

$$H \trianglelefteq G. \tag{7.13}$$

From (7.9) to (7.13), we obtain that $G \cong H \times K$. That is

$$\text{Aut}_{\mathbb{Z}_8 \times \mathbb{Z}_8^\times}(\mathbb{Z}_8 \times \mathbb{Z}_8^\times) \cong (\mathbb{Z}_2 \times \mathbb{Z}_4) \times \mathbb{Z}_8^\times.$$

□

REFERENCES

- [1] W. Burnside , *The theory of groups of finite order*, second Edition, Dover, New York 1995.
- [2] R. Conti, C. D'Antoni, and L. Geatti, *Group automorphisms preserving equivalence classes of unitary representations*, Forum Math. 16(2004), 483-503.
- [3] D.S. Dummit, and R.M. Foote, *Abstract Algebra*, Third Edition, John Wiley&Sons, Inc., 2004.
- [4] W. Feit and G.M. Seitz, *On the finite rational groups and related topics*, Illinois J. Math. 33, NO. 1 (1998), 103-131.
- [5] G.B. Folland, *A Course in Abstract Harmonic Analysis*, CRC Press, Inc., 1995.
- [6] J.B. Fraleigh, *A First Course in Abstract Algebra*, Fifth Edition, Addison-Wesley Publishing Company, 1994.
- [7] P.A. Grillet, *Algebra*, John Wiley&Sons, Inc., 1999.
- [8] M. Hamermesh, *Group Theory and Its Application to Physical Problems*, Addison-Wesley Publishing Company, 1962.
- [9] I.N. Herstein, *Topics in Algebra*, Second Edition, Xerox College Publishing, 1975.
- [10] M. Hertweck, *Class-Preserving Automorphisms of Finite Groups*, J. Algebra 241, 1-26(2001).
- [11] T.W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
- [12] A.G. Kurosh, *The Theory of Groups*, Translated from the Russian and edited by K.A. Hirsch, Volumn one.
- [13] B.E. Sagan, *The symmetric Group, Representations, Combinatorial Algorithms, and Symmetric Functions*, Second Edition, Springer-Verlag, 2001.
- [14] M. Suzuki, *Group Theory I*, Grundlehrender Mathematischen Wissenschaften 247, Springer, 1980.

Appendix I

Automorphism of A_n which maps 3-cycles to 3-cycles

Since we will use the argument about the order of elements, we first give the following Lemma here.

Lemma A.1. *Let (abc) and (xyz) be distinct 3-cycles in S_n .*

(i) *If (abc) and (xyz) have no common symbol, then $|(abc)(xyz)| = 3$.*

(ii) *If (abc) and (xyz) have one common symbol, then $|(abc)(xyz)| = 5$.*

(iii) *If (abc) and (xyz) have two common symbols, then $|(abc)(xyz)| = 2$ or 3 .*

More precisely, $|(abc)(abd)| = 2$, and $|(abc)(adb)| = |(acb)(abd)| = 3$

(iv) *If (abc) and (xyz) have 3 common symbol, then (abc) is the inverse of (xyz) , so $|(abc)(xyz)| = |(1)| = 1$.*

Proof. The proof is straightforward. It is just a direct calculation. □

Lemma A.2. *Let $n \geq 5$ and $\phi \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles. If 3-cycles (xyz) and (abc) have one common symbol, then $\phi(xyz)$ and $\phi(abc)$ have one common symbol.*

More precisely, for distinct $a, b_1, b_2, c_1, c_2 \in \{1, 2, \dots, n\}$, there exists a unique $a' \in \{1, 2, \dots, n\}$ such that $\phi(ab_1b_2) = (a'd_1d_2)$ and $\phi(ac_1c_2) = (a'e_1e_2)$ where a', d_1, d_2, e_1, e_2 are all distinct.

Proof. Let $a, b_1, b_2, c_1, c_2 \in \{1, 2, \dots, n\}$ be all distinct. Assume that

$$\phi(ab_1b_2) = (xyz) \text{ and}$$

$$\phi(ac_1c_2) = (mpq).$$

Then

$$\begin{aligned}
|(x y z) (m p q)| &= |\phi(a b_1 b_2) \phi(a c_1 c_2)| \\
&= |\phi((a b_1 b_2) (a c_1 c_2))| \\
&= |(a b_1 b_2) (a c_1 c_2)| \\
&= 5.
\end{aligned}$$

Therefore, by Lemma A.1, $(x y z)$, $(m p q)$ have one common symbol. After rotation and renaming, we may assume that $x = m = a'$, for some $a' \in \{1, 2, \dots, n\}$, and $\phi(a b_1 b_2) = (a' y z)$, and $\phi(a c_1 c_2) = (a' p q)$. The uniqueness of a' is obvious. \square

Proposition A.3. *Let $n \geq 5$ and $\phi \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles. If $(x y z)$ and $(a b c)$ have two common symbols, then $\phi(x y z)$ and $\phi(a b c)$ have two common symbols. Furthermore, after rotation the two common symbols of $\phi(x y z)$ and $\phi(a b c)$ are in the corresponding positions of the common symbols in $(x y z)$ and $(a b c)$, respectively. More precisely,*

- (i) *For distinct $a, b, c, d \in \{1, 2, \dots, n\}$, $\phi(a b c)$ and $\phi(a b d)$ have two common symbols, and after rotation, we can write*

$$\phi(a b c) = (a' b' c') \text{ and } \phi(a b d) = (a' b' d').$$

where a', b', c', d' are all distinct.

- (ii) *For distinct $m, n, p, q \in \{1, 2, \dots, n\}$, $\phi(m n p)$ and $\phi(m q n)$ have two common symbols, and after rotation we can write*

$$\phi(m n p) = (m' n' p') \text{ and } \phi(m q n) = (m' q' n')$$

where m', n', p', q' are all distinct.

Note If $(a b c)$ and $(x y z)$ are 3-cycles in A_n which have two common symbols, then there are 2 cases to be considered :

Case (1) We can rotate the 3-cycles (abc) and (xyz) so that their common symbols lie in the same position, for instance

$$(abc) = (132), (xyz) = (215).$$

Then $(abc) = (213), (xyz) = (215)$, the symbols 1 and 2 in (abc) and (xyz) are in the same position.

Case (2) We cannot rotate the 3-cycles (abc) and (xyz) so that their common symbols lie in the same position. For instance

$$(abc) = (132) \text{ and } (xyz) = (512).$$

Then

$$\begin{aligned} (abc) &= (132) = (321) = (213), \\ (xyz) &= (512) = (125) = (251). \end{aligned}$$

We can see that if 1 in (abc) and (xyz) lies in the same position, then 2 in them lies in the different position.

Proof. First, we will prove (i). Let $a, b, c, d \in \{1, 2, \dots, n\}$ be all distinct. Let consider the order of the product of 3-cycles $\phi(abc)$ and $\phi(abd)$

$$\begin{aligned} |\phi(abc)\phi(abd)| &= |\phi((abc)(abd))| \\ &= |(abc)(abd)| = 2. \end{aligned}$$

By Lemma A.1, we have $\phi(abc)$ and $\phi(abd)$ have two common symbols and after rotation, the common symbols lie in the first and second position of $\phi(abc)$ and $\phi(abd)$. Let a', b' be the common symbols which lie in the first and second position, respectively. Then we can write

$$\phi(abc) = (a'b'c') \text{ and } \phi(abd) = (a'b'd')$$

where a', b', c' and d' are all distinct. Next, we will prove (ii). Let $m, n, p, q \in \{1, 2, \dots, n\}$

be all distinct. Let $\phi(mnp) = (abc)$ and $\phi(mqn) = (xyz)$. Suppose that (abc) and (xyz) have no common symbol. Then

$$\begin{aligned}\phi(mqp) &= \phi((mnp)(mqn)) \\ &= \phi(mnp)\phi(mqn) \\ &= (abc)(xyz), \text{ which contradicts } \phi \text{ maps 3-cycles to 3-cycles.}\end{aligned}$$

Therefore (abc) and (xyz) have at least one common symbol. Now using the same argument about the order as in (i) we will have a proof of (ii). \square

Proposition A.4. *Let $n \geq 5$ and $\phi \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles. Then for each $a \in \{1, 2, \dots, n\}$ there exists a unique such that $a' \in \{1, 2, \dots, n\}$,*

$$\begin{aligned}\phi\{(amr) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} \\ = \{(a'xy) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}.\end{aligned}$$

Proof. Let $a \in \{1, 2, \dots, n\}$. Choose $m_1, r_1, m_2, r_2 \in \{1, 2, \dots, n\} - \{a\}$ which are all distinct. This can be done, since $n \geq 5$. From Lemma A.2, there exists $a' \in \{1, 2, \dots, n\}$ such that

$$\phi(am_1r_1) = (a'm_3r_3), \phi(am_2r_2) = (a'm_4r_4)$$

where a', m_3, r_3, m_4, r_4 are all distinct.

Suppose for a contradiction that there exists a 3-cycle (amr) such that

$$\phi(amr) \text{ does not contain } a' \text{ as a symbol in its cycle rotation.} \quad (\text{A.1})$$

Consider (amr) and (am_1r_1) . The number of common symbols in (amr) and (am_1r_1) is 1 or 2. Similarly for (amr) and (am_2r_2) . From Lemma A.2 and Proposition A.3, $\phi(amr)$ and $\phi(am_1r_1)$ have at least one common symbol. Also, $\phi(amr)$ and $\phi(am_2r_2)$ have at least one common symbol.

We denote by $[\phi(amr), \phi(am_i r_i)]$ the number of common symbols of $\phi(amr)$ and $\phi(am_i r_i)$ for $i = 1, 2$.

There are 4 cases to be considered :

Case 1 : $[\phi(a m r), \phi(a m_i r_i)] = 1$ for $i \in \{1, 2\}$

Case 2 : $[\phi(a m r), \phi(a m_i r_i)] = 2$ for $i \in \{1, 2\}$

Case 3 : $[\phi(a m r), \phi(a m_1 r_1)] = 1$ and $[\phi(a m r), \phi(a m_2 r_2)] = 2$

Case 4 : $[\phi(a m r), \phi(a m_1 r_1)] = 2$ and $[\phi(a m r), \phi(a m_2 r_2)] = 1$

We will show that all cases do not occur.

Case 1 : Let $\phi(a m r) = (x y z)$ where x, y, z are all distinct. For $i \in \{1, 2\}$, $\phi(a m r)$ and $\phi(a m_i r_i)$ have one common symbol, so we have $(a m r)$ and $(a m_i r_i)$ have one common symbol, that is a . Therefore $a, m_1, r_1, m_2, r_2, m, r$ are all distinct. Then

$$\begin{aligned}
 7 &= |(a m_2 r_2 m_1 r_1 m r)| = |\phi(a m_2 r_2 m_1 r_1 m r)| \\
 &= |\phi((a m r)(a m_1 r_1)(a m_2 r_2))| \\
 &= |\phi(a m r)\phi(a m_1 r_1)\phi(a m_2 r_2)| \\
 &= |(x y z)(a' m_3 r_3)(a' m_4 r_4)| \\
 &= |(x y z)(a' m_4 r_4 m_3 r_3)| \tag{A.2}
 \end{aligned}$$

Since $\phi(a m r)$ and $\phi(a m_1 r_1)$ have one common symbol, and $\phi(a m r)$ does not contain a' , we have $\phi(a m r)$ contains either m_3 or r_3 . Similarly, $\phi(a m r)$ contains m_4 or r_4 .

Hence there are 4 cases to be considered :

case 1.1 : $\phi(a m r)$ contains m_3 and m_4 .

case 1.2 : $\phi(a m r)$ contains r_3 and m_4 .

case 1.3 : $\phi(a m r)$ contains r_3 and r_4 .

case 1.4 : $\phi(a m r)$ contains m_3 and r_4 .

All cases will contradict Equation A.2. In fact, in the first three cases, we obtain that $|(x y z)(a' m_4 r_4 m_3 r_3)| = 4$ or 3 , and in the last case, we have

$$|(x y z)(a' m_4 r_4 m_3 r_3)| = 5 \text{ or } 4.$$

Therefore case 1 does not occur.

Case 2 : Since $\phi(amr)$ does not contain a' , $\phi(amr)$ contains m_3, r_3, m_4 and r_4 . This cannot happen because $\phi(amr)$ is a 3-cycle and m_3, r_3, m_4, r_4 are all distinct.

Case 3 : We have $\phi(amr)$ contains m_4 and r_4 and contains either m_3 or r_3 . Then $\phi(amr) = (m_4 r_4 m_3), (m_4 m_3 r_4), (m_4 r_4 r_3)$ or $(m_4 r_3 r_4)$.

Case 3.1 : $\phi(amr) = (m_4 r_4 m_3)$. Then

$$\phi^{-1}(m_4 r_4 m_3) = (amr), \quad (\text{A.3})$$

$$\phi^{-1}(a' m_3 r_3) = (am_1 r_1), \quad (\text{A.4})$$

$$\phi^{-1}(a' m_4 r_4) = (am_2 r_2). \quad (\text{A.5})$$

Note that $\phi^{-1} \in \text{Aut}(A_n)$ which maps 3-cycles to 3-cycles, so we can apply Lemma A.2 and Proposition A.3 for ϕ^{-1} . Consider (A.3) and (A.4). Since $(amr) = \phi^{-1}(m_4 r_4 m_3)$, $(am_1 r_1) = \phi^{-1}(a' m_3 r_3)$, and $(m_4 r_4 m_3)$ and $(a' m_3 r_3)$ have one common symbol, we conclude that (amr) and $(am_1 r_1)$ have one common symbol. We see that the symbol a is the common symbol of (amr) and $(am_1 r_1)$. Therefore a, m, r, m_1, r_1 are all distinct. From (A.3) and (A.5)

$$(amr) = \phi^{-1}(m_4 r_4 m_3)$$

$$(am_2 r_2) = \phi^{-1}(a' m_4 r_4) = \phi^{-1}(m_4 r_4 a').$$

Apply Proposition A.3, we have $(m = m_2 \text{ and } r \neq r_2)$ or

$(r = r_2 \text{ and } m \neq m_2)$

$$5 = |(a' r_4 m_4 m_3 r_3)| \quad (\text{A.6})$$

$$= |(m_4 r_4 m_3)(a' m_3 r_3)(a' m_4 r_4)| \quad (\text{A.7})$$

$$= |\phi(a m r)\phi(a m_1 r_1)\phi(a m_2 r_2)|$$

$$= |\phi((a m r)(a m_1 r_1)(a m_2 r_2))|$$

$$= \begin{cases} |\phi(a m r)(a m_1 r_1)(a m_2 r_2)| & \text{if } m = m_2 \text{ and } r \neq r_2 \\ |\phi(a m r)(a m_1 r_1)(a m_2 r)| & \text{if } r = r_2 \text{ and } m \neq m_2 \end{cases}$$

$$= \begin{cases} |\phi(a r)(m_1 r_1 m r_2)| & \text{if } m = m_2 \text{ and } r \neq r_2 \\ |\phi(a m_2)(m_1 r_1 m r)| & \text{if } r = r_2 \text{ and } m \neq m_2 \end{cases}$$

$$= 4, \quad \text{a contradiction.}$$

Case 3.2 : $\phi(a m r) = (m_4 m_3 r_4)$.

We use the same process as in case 3.1. Apply Lemma A.2, we have a, m, r, m_1, r_1 are all distinct. Apply Proposition A.3, we have

$(m = r_2 \text{ and } r \neq m_2)$ or $(r = m_2 \text{ and } m \neq r_2)$. Then we have

$$(a' m_4 r_3) = (a' m_3 r_3)(a' m_4 r_4)(m_4 m_3 r_4) \quad (\text{A.8})$$

$$= \phi(a m_1 r_1)\phi(a m_2 r_2)\phi(a m r)$$

$$= \phi((a m_1 r_1)(a m_2 r_2)(a m r))$$

$$= \begin{cases} \phi((a m_1 r_1)(a m_2 m)(a m r)) & \text{if } m = r_2, r \neq m_2 \\ \phi((a m_1 r_1)(a r r_2)(a m r)) & \text{if } r = m_2, m \neq r_2 \end{cases}$$

$$= \begin{cases} \phi((a m_1 r_1)(m_2 m r)) & \text{if } m = r_2, r \neq m_2 \\ \phi(a m r_2 m_1 r_1) & \text{if } r = m_2, m \neq r_2 \end{cases}$$

Then $\phi^{-1}(a' m_4 r_3)$ is a 5-cycle or product of two 3-cycles. This contradicts the fact that ϕ^{-1} maps 3-cycles to 3-cycles.

Case 3.3 : $\phi(amr) = (m_4 r_4 r_3)$.

Use the same process as case 3.1. The proof is different from case 3.1 at equation (A.6) and (A.7). Just replace $(a' r_4 m_4 m_3 r_3)$ by $(a' r_4 m_3 m_4 r_3)$ in (A.6) and $(m_4 r_4 m_3)$ by $(m_4 r_4 r_3)$ in (A.7) we will have the proof of case 3.3.

Case 3.4 : $\phi(amr) = (m_4 r_3 r_4)$.

Using the same process as case 3.2. The proof is different from case 3.2 at equation (A.8). Just replace $(a' m_4 r_3)$ by $(a' m_4)(m_3 r_3)$, and $(m_4 m_3 r_4)$ by $(m_4 r_3 r_4)$ in (A.8), then taking the order of the elements we have a contradiction.

Case 4 : This can be proved similarly to case 3.

All cases lead to a contradiction. This result from supposition (A.1). Hence

$$\begin{aligned} \phi\{(amr) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} \\ \subseteq \{(a'xy) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}. \end{aligned}$$

Since ϕ is 1-1, $\phi\{(amr) \mid m, r \in \{1, 2, \dots, n\} - \{a\}, m \neq r\} = \{(a'xy) \mid x, y \in \{1, 2, \dots, n\} - \{a'\}, x \neq y\}$. The uniqueness of a' is obvious. Therefore, Proposition A.4 is proved. \square

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

VITA

Name : Mr. Prapanpong Pongsriiam
Date of Birth : November 13, 1980
Place of Birth : Chiangmai, Thailand
Previous Studies : B.Sc.(Mathematics), Chulalongkorn University, 2003.
Scholarship : The Development and promotion of Science and
Technology Talented Project (DPST).



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย