Spring 2021

About Automorphisms of Some Finite Groups

Sarah Emery
se851997@wcupa.edu

About Automorphisms of Some Finite Groups

A Thesis

Presented to the Faculty of the

Department of Mathematics

West Chester University

West Chester, Pennsylvania

In Partial Fulfillment of the Requirements for the

Degree of

Master of Arts

By

Sarah Emery

May 2021

Acknowledgements

First, I would like to thank my committee chairperson Dr. Shiv Gupta. Without him, I may not have discovered my love for group theory, and I certainly would not have completed this thesis. I owe thanks as well to my committee members Dr. Jeremy Brazas and Dr. Michael Fisher, both for their participation in the approval of my thesis, but also for their encouragement during my time at West Chester. I owe special thanks to Dr. Brazas for supporting and encouraging me more than anyone else at West Chester during my academic career. I also thank my classmate Sean Gould for his friendship and for many discussions about mathematics and all things related to our theses.

Some of my former mathematics professors at Delaware County Community College who encouraged me greatly include Dr. John Boncek and Dr. Sydney Kolpas and to them I owe a debt of gratitude.

I must also give thanks to my family and friends; especially my mother who supported me through every victory and loss during my years in school. She is my best friend and I think I never would have found a love of mathematics without her.

Finally, I want to thank Dr. Robert Styer at Villanova university. Before joining a local Math Olympiad group, led by Dr. Styer, fifteen years ago, math was just another boring school subject. That perspective changed as soon as I joined his group. Because of him I will never forget the cardinal rule when attacking a problem: “Be organized!”

Abstract

This thesis gives an introduction to some topics from group theory, with a focus on automorphism groups of finite groups. Chapter one introduces the basic definitions and properties of groups and subgroups. In chapter two, the different classifications of functions between groups are defined and some properties thereof are given. Here we define automorphisms which are the focus of the paper. Chapters three and four deal with permutation groups and Sylow theorems respectively, and are discussions of some important groups, subgroups, and theorems pertaining thereto. The topics of these chapters help with our discussion of automorphism groups in the final three chapters. Chapter five gives a discussion on the automorphism groups of finite groups of small order, and then some general results about the automorphism groups of cyclic groups. The last two chapters are dedicated to interesting case studies in the study of automorphism groups. Chapter six discusses an example of a group G which has an outer automorphism which preserves the conjugate classes of a group, and chapter seven gives the introduction and details to the theorem that S_6 is the only symmetric group having an outer automorphism.

Contents

Notation

$(G, *)$	A group G with binary operation $*$.
e	The identity element of a group.
g^{-1}	The inverse of an element g in a group.
$\langle S \rangle$	The group generated by the set S.
$\mathbb{Z}$	The set of integers.
$\lvert G \rvert$	The order of a group G. That is, the number of elements therein.
$\mathbb{N}$	The set of natural numbers 1, 2, 3, ...
$Order(g)$	The order of an element g. That is, the smallest number n such that $g^n = e$.
$a \equiv b \pmod{n}$	Equivalence modulo n. That is, $a \equiv b \pmod{p}$ is there exists some k such that $a = kn + b$.
$\mathbb{Z}_n$	The set $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ of integers modulo n. We usually just write $\{0, 1, 2, \ldots, n-1\}$ for simplicity. These group a group under addition modulo n.
$\gcd(a, b)$	The greatest common divisor of a and b.
$\mathbb{Z}_n^*$	The set $\{i \in \mathbb{Z}_n \mid \gcd(i, n) = 1\}$. This forms a group under multiplication modulo n.
D_{2n}	The dihedral group of order $2n$, or the group of symmetries of an n-sided polygon.
$[G : H]$	The index of a subgroup H in a group G, which is $\lvert G \rvert / \lvert H \rvert$.
C_n	The cyclic group of order n.
$Z(G)$	The center of a group G.
$C_G(g)$	The centralizer of an element $g \in G$.
C_i	The i^{th} conjugate class of a group.
$N \trianglelefteq G$	The subgroup N of G is normal in G.
Q_8	The quaternion group.
$G \times H$	The direct product of groups G and H.
$N_G(H)$	The normalizer of H in G.
G/N	The quotient set of cosets of N in G. If N is normal, it denotes the quotient group.
$\mathbb{C}^*$	The set of complex numbers excluding zero.
$[g, h]$	The commutator of g and h, which equals $g^{-1}h^{-1}gh$.
G'	The commutator subgroup of G, which is the subgroup generated by the commutators of G.
$G \cong H$	There exists an isomorphism between G and H, or G and H are isomorphic.
$Aut(G)$	The group of automorphisms of a grouop G.
$Inn(G)$	The group of inner automorphisms of a group G.
S_n	The symmetric group on n letters.
A_n	The alternating group on n letters, or the subgroup of S_n consisting only of even permutations.

$\boldsymbol{GL(n,q)}$	The general linear group of $n \times n$ matrices, with entries from the finite field of order q.
$\boldsymbol{GF(q)}$	The finite field, of order q, also known as the Galois Field of order q.
$\boldsymbol{\mathbb{F}_q}$	Alternate notation for $GF(q)$.
$\boldsymbol{GL(n,\mathbb{Z}_m)}$	The general linear group of $n \times n$ matrices, with entries from $\mathbb{Z}_m$.
$\boldsymbol{Sym(\Omega)}$	The symmetric group on Ω, or the group of permutations of the elements of Ω.

Chapter 1

Introduction

1.1 Groups

Definition 1.1. Let G be a set together with a binary operation $*$. Then $(G, *)$ is a *group* if the following hold:

1. For every $g, h, k \in G$, $g * (h * k) = (g * h) * k$. This property is known as the *associative* property.

2. There exists some $e \in G$ so that $g * e = g = e * g$, for all $g \in G$. We call this the *identity* in G and it is unique.

3. For every $g \in G$, there exists some $h \in G$ so that $g * h = e = h * g$, where e is the identity element from (2). We call this the *inverse* of g in G, and denote it by g^{-1}. This inverse is unique.

For the sake of simplicity, unless it is necessary to distinguish different binary operations, we shall write

$$g * h = gh$$

and refer generally to the operation of a group G as multiplication. Also, we will usually refer to the group as G instead of $(G, *)$ unless it is necessary to be specific.

Definition 1.2. Let G be a group such that $gh = hg$ for all $g, h \in G$. Then we say that the binary operation in G is *commutative*, and we refer to G as a commutative or an *abelian* group.

Definition 1.3. Let G be a group and S be a non-empty subset of G such that for $g \in G$, there exist some $s_1, s_2, \ldots, s_n \in S$ so that $g = s_1 s_2 \cdots s_n$. Then we say that the group G is *generated* by S. and write $G = \langle S \rangle$ or $G = \langle t_1, t_2, ..., t_k \rangle$, where $S = \{t_1, t_2, ..., t_k\}$.

We give several examples of groups.

Example 1.4. The set of integers, $\mathbb{Z}$, is a group under addition, defined the usual way, with identity 0, and for every $z \in \mathbb{Z}$, $-z$ is its inverse.

Notice that any positive integer z can be written as the sum of z $1s$. For example, $2 = 1 + 1$, $7 = 1+1+1+1+1+1+1$, etc. Further, any negative integers can be written similarly as the sum of $-1s$, the inverse of 1. When every element of a group can be written in terms of a single element, as we just saw, we say that the group is *generated* by that element. That is, $(\mathbb{Z}, +)$ is generated by 1, and we can write $\mathbb{Z} = \langle 1 \rangle$.

This group $\mathbb{Z}$ is an example of an infinite group, but we will mostly concern ourselves with finite groups in this paper.

Definition 1.5. Let G be a finite group with n elements. Then we say the *order* of G is n and write $|G| = n$.

Definition 1.6. Let G be a group with element $g \in G$. Suppose there exists a smallest $n \in \mathbb{N}$ such that $g^n = e$; that is, there is some smallest positive integer n such that g multiplied by itself n times yields the identity element e of G. Then, we say the *order* of g is n and write $\text{Order}(g) = n$.

Definition 1.7. Let G be a group such that there exists some $g \in G$ where for every $h \in G$, $h = g^n$ for some n. Then, we call G a *cyclic group* and write $G = \langle g \rangle$. Here, g is call the *generator* of G. We often denote a cyclic group of order n by C_n.

Example 1.8. Recall from number theory, that if $a, b, n \in \mathbb{Z}$ with $n > 1$, then we say $a \equiv b \pmod{n}$ if $a - b$ is divisible by n. The relation $\equiv$ is an equivalence relation and as such $\mathbb{Z}$ is partitioned into equivalence classes and we denote the resulting quotient set (set of equivalence classes) by $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

where $\overline{i}$ represents the equivalence class corresponding to i. For convenience we will simply write

$$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$$

with the understanding the we are referring to equivalence classes under the relation $\equiv$.

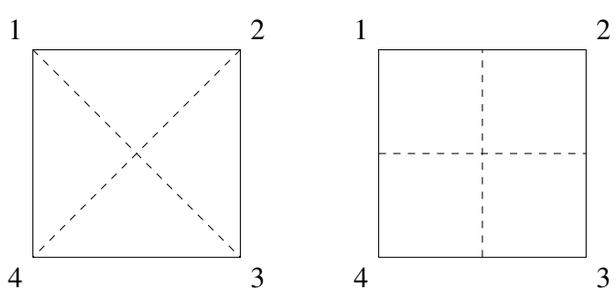
By $\mathbb{Z}_n^*$, we denote the subset of $\mathbb{Z}_n$ which consists of $i \in \mathbb{Z}$ such that $\gcd(i, n) = 1$. The cardinality of this set is $\phi(n)$ where ϕ is the Euler ϕ function. Under multiplication modulo n, this forms a group. For example:

$\mathbb{Z}_5^* = \{1, 2, 3, 4\} \pmod 5$	Cyclic group: C_4
$\mathbb{Z}_8^* = \{1, 3, 5, 7\} \pmod 8$	Klein-Four group: $C_2 \times C_2$ *
$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} \pmod 9$	Cyclic group: C_6

*Groups of this kind, namely non-cyclic order four groups are named Klein-Four after mathematician Felix Klein.

Example 1.9. Consider a square and the set of symmetries thereof; that is the functions one can perform on a square which will fix the overall square but not necessarily the individual vertices. These form a group under the binary operation of function composition. Function composition is associative, the identity element is the identity function, which fixes each vertex, and if we think of each symmetry as a permutation of the vertices, then each is a one-to-one and onto function and thus has an inverse with respect to the identity function.

Consider the square with vertices 1, 2, 3, and 4 listed clockwise. Let the major diagonal be that which runs from the top left to the bottom right of the square and the minor be the opposite. We've drawn the major and minor diagonals, as well as the vertical and horizontal lines of reflection as dashed lines in the following illustration.



We give a table of the elements. Vertical reflection refers to the swapping of vertices with those directly above or below them. Horizontal reflection refers to swapping vertices with those horizontally across from them.

Action	Vertex Permutation
Rotation by 0°	$1 \to 1;\ 2 \to 2;\ 3 \to 3;\ 4 \to 4$
Rotation by 90°	$1 \to 2;\ 2 \to 3;\ 3 \to 4;\ 4 \to 1$
Rotation by 180°	$1 \to 3;\ 2 \to 4;\ 3 \to 1;\ 4 \to 2$
Rotation by 270°	$1 \to 4;\ 2 \to 1;\ 3 \to 2;\ 4 \to 3$
Vertical Reflection	$1 \to 4;\ 2 \to 3;\ 3 \to 2;\ 4 \to 1$
Horizontal Reflection	$1 \to 2;\ 2 \to 1;\ 3 \to 4;\ 4 \to 3$
Major Diagonal Reflection	$1 \to 3;\ 2 \to 2;\ 3 \to 1;\ 4 \to 4$
Minor Diagonal Reflection	$1 \to 1;\ 2 \to 4;\ 3 \to 3;\ 4 \to 2$

Let a denote rotation by 90° and b denote vertical reflection. Any element of this group can be written in terms of these. For example, rotation by 180° is simply rotation by 90° performed twice. Thus we can denote this a^2. Further, rotation by 270° can be denoted a^3. Rotation by 90° followed by vertical reflection results in major diagonal reflection, so it may be denoted ab. Rotation by 180° followed by vertical reflection results in horizontal reflection, so it may be denoted a^2b. Finally, if rotation by 270° is followed by vertical reflection, the result is minor diagonal reflection, which may be denoted a^3b. Thus,

$$D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

Action	Denotation
Rotation by 0°	e
Rotation by 90°	a
Rotation by 180°	a^2
Rotation by 270°	a^3
Vertical Reflection	b
Horizontal Reflection	a^2b
Major Diagonal Reflection	ab
Minor Diagonal Reflection	a^3b

From the list of elements, it is clear that a and b generate this group, so we can say $D_8 = \langle a,\ b \rangle$. However, in this presentation, without noting what a and b represent in terms of the symmetries, it is not obvious how these elements relate. To fully describe this group using only the generators, it is necessary to note how ab and ba differ, since this group is non-abelian. In this particular case,

$ba = a^3b$. In order to fully describe this group, the last thing we must take note of is the orders of each generator. The order of a is 4 and the order of b is 2, and so with this, we can finally write a full description of the group.

$$D_8 = \langle a, b \,|\, a^4 = b^2 = e, ba = a^3b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

This is commonly called that *dihedral group* of order eight. Generally, the dihedral group of order $2n$ is the group of symmetries of a regular n-sided polygon. For example, the group of symmetries of the regular hexagon is D_{12}, the dihedral group of order twelve.

What we have just shown is a compact way of describing a group. We will describe groups this way whenever possible. This is commonly called the *presentation* of a group.

Definition 1.10. Let $(G, *)$ and $(H, \diamond)$ be groups. Then the set

$$G \times H = \{(g, h) \,|\, g \in G, h \in H\}$$

forms a group under the operation $\star$ defined:

$$(g_1, h_1) \star (g_2, h_2) \coloneqq (g_1 * g_2, h_1 \diamond h_2).$$

This group $(G \times H, \star)$ is called the *direct product* of G and H.

It is easily shown that the direct product forms a group under the defined operation. The following are properties of the direct product $G \times H$:

1. The identity element is (e_G, e_H) where e_G and e_H are the respective identities in G and H.
2. The order of an element (g, h) is the least common multiple of the orders of g and h.
3. The inverse of an element (g, h) is (g^{-1}, h^{-1})

Example 1.11. Consider the Klein-four group which we referred to in Example 1.8. This is denoted by $C_2 \times C_2$ because it is the direct product of C_2 with itself. Here, C_2 is the cyclic group (see Definition 1.7) of order two. Let $G = \{e_G, x\}$ and $H = \{e_H, y\}$ where e_G and e_H are the respective identities in G and H, and where x and y have order two. Consider the direct product

$$G \times H = \{(e_G, e_H), (x, e_H), (e_G, y,), (x, y)\}.$$

Every non-identity element has order two.

Because $G \cong C_2 \cong H$, we denote this group generally as $C_2 \times C_2$.

Usually, when we refer to direct products, we do not use the notation of ordered pairs used in the definition above. So, we usually enumerate the elements of the Klein-four group $C_2 \times C_2 = \{e, x, y, xy\}$.

1.2 Subgroups

Definition 1.12. Let G be a group and H be a subset of G such that H itself is a group under G's operation. Then we say H is a *subgroup* of G.

Proposition 1.13. *A non-empty subset H of a finite group G is a subgroup if and only if for $g, h \in H$, $gh \in H$.*

Proof. Suppose H is a subgroup of G and $g, h \in H$. Then, being a group, H must be closed under the operation of G and so $gh \in H$.

Now, suppose that for any $g, h \in H$, $gh \in H$. The associativity of the operation is unaffected. Let $g \in H$ have order n. Since H is closed under the binary operation of G, $g^n = e \in H$ contains an identity element. Further, $g^{n-1} = g^{-1} \in H$ by the same reasoning and so H is closed under taking inverses ◇

Note that the above only works in the case of finite groups. In the infinite case, one need require that gh^{-1} be in H be every $g, h \in H$ because in the infinite case one cannot count on any element having finite order, which was crucial to the proof.

Definition 1.14. Let G be a group, H be a subgroup of G, and $g \in G$. Then,

1. the set defined by $Hg = \{hg | h \in H\}$ is called a right coset of H in G, and
2. the set defined by $gH = \{gh | h \in H\}$ is called a left coset of H in G.

For all $g \in G$, $|Hg| = |H| = |gH|$.

Proposition 1.15. *Let H be a subgroup of a group G and $a, b \in G$. Then, $Ha = Hb$ if and only if $ab^{-1} \in H$.*

Proof. It can be easily checked that the relation $\sim$ where $a \sim b$ if $ab^{-1} \in H$ is an equivalence relation. The resulting equivalence classes are the right cosets of H in G. ◇

We can draw the conclusion from this result that cosets of subgroups are always disjoint or equal. Consider in the first part of the proof that if we simply supposed that $Ha \subseteq Hb$, that is, that some overlap between the cosets existed, then the implications would have still led to $ab^{-1} \in H$, which according to the second part of the proof implies that $Ha = Hb$. Therefore, if any overlap between cosets of some subgroup exists, then the cosets must be equal.

Theorem 1.16 (Lagrange's Theorem)**.** *Let G be a finite group with subgroup H. Then $|H|$ divides $|G|$.*

It follows directly from this that the order of every element of a group must divide the order of the group. This is because each element of G generates some subgroup thereof, which must have order dividing the order of the group.

Because the order of element must divide the order of the group, any group of prime order must be cyclic, as the only element of order one is the identity.

Definition 1.17. Let G be a finite group and H be a subgroup of G. We define the *index* of H in G as $[G : H] = \dfrac{|G|}{|H|}$.

Theorem 1.18. *Let G be a cyclic group with subgroup H. Then H is also cyclic.*

Proof. Let G be a cyclic group with subgroup H. Because G is cyclic, there exists some $g \in G$ such that $G = \langle g \rangle$; that is, for every $x \in G$, there exists some n such that $x = g^n$.

Assume that $H \neq \{e\}$. Then by the Well-Ordering Principle, there is some smallest non-zero power of g in H, say g^d. Let g^a be in H. By the Division Algorithm, we can write

$$a = qd + r, \quad 0 \leq r < d$$

so

$$g^a = (g^d)^q (g^r), \quad 0 \leq r < d.$$

Since H is a subgroup of G, it is closed under the operation in G and thus $((g^d)^q)^{-1}g^a = g^r \in H$, but d is the smallest non-zero power of g in H, so $r = 0$ and we have that

$$g^a = (g^d)^q.$$

Thus, every element in H is some power of g^d and H is cyclic. ◇

Theorem 1.19. *Let G be a cyclic group of order n and d be an integer which divides n. Then G has a unique subgroup of order d.*

Proof. Let $G = \langle g \rangle$ be a cyclic group of order n and d be a positive integer such that d divides n. Let $n = md$. Then $\text{Order}(g^m) = d$ and $H = \langle g^m \rangle$ is a subgroup of order d.

We show that H is the unique subgroup of order d. Let K be a subgroup of G of order d. Then $K = \langle g^k \rangle$ for some k. Then, $g^{kd} = g^n = e$, which means n divides kd and therefore $n \leq kd$. However, since K is order d, d is the smallest positive integer such that $kd \equiv 0 \pmod{n}$. Thus, $n \geq kd$. Therefore $kd = n = md$, which implies that $k = m$ and thus $H = K$. ◇

Theorem 1.20. *The group $\mathbb{Z}_p^*$ is cyclic where p is a prime.*

Proof. Recall that a polynomial of degree n over a field $\mathbb{F}$ has at most n roots in $\mathbb{F}$.

Let t be the least common multiple of the orders of the elements in $\mathbb{Z}_p^*$ and consider the polynomial $x^t - 1$ over $\mathbb{F}_p$. This polynomial can have no more than t roots in $\mathbb{F}_p$, but all elements of $\mathbb{Z}_p^*$ are roots of it, so $p - 1 \leq t$. Given that $\mathbb{Z}_p^*$ is abelian, it has an element of order t and so $t \mid p - 1$. Therefore $t = p - 1$ and $\mathbb{Z}_p^*$ has an element of order $p - 1$ meaning it is cyclic. ◇

Definition 1.21. Let G be a group and define

$$Z(G) = \{g \in G \mid gh = hg, \ \ \forall h \in G\}.$$

This is the set of elements of G which commute with every element in G, and is called the *center* of G.

It can be easily shown that $Z(G)$ is a subgroup of G.

Definition 1.22. Let G be a group with $g, h \in G$. If there exists some $k \in G$ such that $g = k^{-1}hk$, then we say that g and h are *conjugates* in G.

The relation $\sim$ defined so that $g \sim h$ whenever g and h are conjugates is an equivalence relation, where the resulting equivalence classes are called *conjugate classes*.

Example 1.23. Consider

$$D_{12} = \langle a, b \mid a^6 = b^2 = e, \ b^{-1}ab = a^{-1} \rangle = \{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5\},$$

the dihedral group of order 12. The conjugate classes of D_{12} are as follows:

Class	Representative	Elements	# Elements	Order
C_1	e	e	1	1
C_2	a	a, a^5	2	6
C_3	a^2	a^2, a^4	2	3
C_4	a^3	a^3	1	2
C_5	b	b, a^4b, a^2b	3	2
C_6	ab	ab, a^5b, a^3b	3	2

Definition 1.24. Let G be a group and $g \in G$. Define

$$C_G(g) = \{x \in G \mid gx = xg\}.$$

Then, we call $C_G(g)$ the *centralizer* of g in G.

The centralizer of any element $g \in G$ can be easily shown to be a subgroup of G.

Proposition 1.25. *Let G be a finite group and g be in G. The number of elements conjugate to g in G is equal to the index of $C_G(g)$.*

Proof. Let $g, a, b \in G$ such that $a^{-1}ga = b^{-1}gb$. Then,

$$\begin{aligned} a^{-1}ga = b^{-1}gb &\iff ba^{-1}gab^{-1} = g \\ &\iff (ab^{-1})^{-1}g(ab^{-1}) = g \\ &\iff ab^{-1} \in C_G(g) \\ &\iff C_G(g)a = C_G(g)b \quad \text{(by Proposition 1.15)} \end{aligned}$$

Thus, the number of elements conjugate to g is the number of right cosets of $C_G(g)$, which is the index of $C_G(g)$. ◇

Definition 1.26. Let G be a group and N be a subgroup of G such that $g^{-1}Ng = N$ for all $g \in G$. That is, for all $n \in N$, $g^{-1}ng \in N$ for all $g \in G$. Then N is a *normal subgroup* of G. We denote this $N \trianglelefteq G$.

The trivial subgroup $\{e\}$ is always normal, as is the center $Z(G)$ and the group itself G.

Theorem 1.27. *Any subgroup of index two is normal.*

Proof. Let H be a subgroup of G of index two. Then H has two right cosets H and Hx, and two left cosets H and xH. Given that

$$H \cup Hx = G = H \cup xH,$$

Hx must equal xH and so $H \trianglelefteq G$.

◇

Example 1.28. Consider again the group

$$D_8 = \langle a, b \,|\, a^4 = b^2 = e,\ b^{-1}ab = a^{-1} \rangle.$$

Earlier, we merely introduced this group in the context of the symmetries of a geometric object. Now we give a more detailed description of its subgroups and conjugate classes.
Recall the elements are as follows

$$\{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}.$$

A description of their inverses and order is given in the following table:

Element	Inverse	Order
e	e	1
a	a^3	4
a^2	a^2	2
a^3	a	4
b	b	2
ab	ab	2
a^2b	a^2b	2
a^3b	a^3b	2

Now we describe the conjugate classes of D_8. The last column in the table gives the orders of the elements of each the conjugate class.

Class	Representative	Centralizer	Elements	# Elements	Order
C_1	e	D_8	e	1	1
C_2	a	$\langle a \rangle$	a, a^3	2	4
C_3	a^2	D_8	a^2	1	2
C_4	b	$\langle a^2, b \rangle$	b, a^2b	2	2
C_5	ab	$\langle a^2, ab \rangle$	ab, a^3b	2	2

Finally, we give a table listing the subgroups of D_8.

Subgroup	Elements	Order	Type
D_8	e, a, a^2, a^3, b, ab, a^2b, a^3b	8	Dihedral
$\langle a \rangle$	e, a, a^2, a^3	4	Cyclic
$\langle a^2, b \rangle$	e, a^2, b, a^2b	4	Klein-Four
$\langle a^2, ab \rangle$	e, a^2, ab, a^3b	4	Klein-Four
$Z(D_8) = \langle a^2 \rangle$	e, a^2	2	
$\langle b \rangle$	e, b	2	
$\langle ab \rangle$	e, ab	2	
$\langle a^2b \rangle$	e, a^2b	2	
$\langle a^3b \rangle$	e, a^3b	2	
$\langle e \rangle$	e	1	

We've already said that center of a group is always normal, so we know that $\langle a^2 \rangle \trianglelefteq D_8$, but this group has several other normal subgroups.
Any subgroups of order four will be normal as they have index two in D_8. These groups are $\langle a \rangle$, $\langle a^2, b \rangle$, and $\langle a^2, ab \rangle$.

The previous example highlights two things about normal subgroups:

Proposition 1.29. *Let G be a group with a non-empty subset S such that $G = \langle S \rangle$. If H is a subgroup of G, and $s^{-1}Hs = H$ for all $s \in S$, then $H \trianglelefteq G$.*

Proof. Every element of G can be written in terms of elements of S. Therefore, if $g \in G$, then

$g = s_1 s_2 \cdots s_n$, and

$$\begin{aligned} g^{-1}Hg &= s_n^{-1} \cdots s_2^{-1} s_1^{-1} H s_1 s_2 \cdots s_n \\ &= s_n^{-1} \cdots s_2^{-1} \left(s_1^{-1} H s_1\right) s_2 \cdots s_n \\ &= s_n^{-1} \cdots s_2^{-1} H s_2 \cdots s_n \\ &= s_n^{-1} \cdots \left(s_2^{-1} H s_2\right) \cdots s_n \\ &= s_n^{-1} \cdots H \cdots s_n \\ &= \cdots \\ &= s_n^{-1} H s_n \\ &= H. \end{aligned}$$

◇

Proposition 1.30. *A subgroup K is normal in G if and only if it is the union of some conjugate classes of G.*

Proof. One implication holds because if $k \in K$, then $g^{-1}kg$ is in the conjugate class for k which is a subset of K and therefore $g^{-1}kg \in K$ for all $g \in G$. The other implication holds because if K were not the union of conjugate classes, then there would exist some $k \in K$ such that there would be a $g \in G$ where $g^{-1}kg \notin K$. Thus, K would not be normal. ◇

Proposition 1.30 implies that if a group G is abelian, then all subgroups are normal, since each element is in its own conjugate class. It is not true however that every subgroup being normal implies the group is abelian, as can be seen in the following example.

Example 1.31. Let $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$ with the following relations:

$$i^4 = j^4 = k^4 = 1 \qquad ij = k \qquad ik = j \qquad jk = i$$

$$i^2 = j^2 = k^2 = -1 \qquad ji = -k \qquad ki = -j \qquad kj = -i$$

The multiplication table for Q_8 is as follows:

	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	j	1	$-k$	$-j$
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	$-j$	$-i$	-1	j	i	1
$-i$	$-i$	i	1	$-k$	$-j$	-1	k	j
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	j	i	1	$-j$	$-i$	-1

Now we give the subgroups of Q_8.

Subgroup	Elements	Order	Type
Q_8	$1, -1, i, j, k, -i, -j, -k$	8	
$\langle i \rangle$	$1, i, -1, -i$	4	cyclic
$\langle j \rangle$	$1, j, -1, -j$	4	cyclic
$\langle k \rangle$	$1, k, -1, -k$	4	cyclic
$Z(Q_8) = \langle -1 \rangle$	$1, -1$	2	
$\langle 1 \rangle$	1	1	

Clearly $\langle -1 \rangle$ is a normal subgroup since it is the only order two subgroup of Q_8. The others are also normal because they are of index two.

Theorem 1.32. *Let G be a group and H be a subgroup of G. Then for $x \in G$, $x^{-1}Hx$, the conjugate of H by x, is a subgroup of G.*

Definition 1.33. Let G be a group and H be a subgroup of G. Define

$$N_G(H) = \{x \in G \mid Hx = xH\}.$$

Then, we call $N_G(H)$ the *normalizer* of H in G.

It can be easily shown that the normalizer of any subgroup is itself a subgroup of G. In fact, $N_G(H)$ is the largest subgroup of G which has H as a normal subgroup.

Proposition 1.34. *Let G be a group and H a subgroup of G. The number of subgroups conjugate to H is equal to the index of $N_G(H)$, the normalizer of H in G.*

Proof. This is proven by replacing g with H and $C_G(g)$ with $N_G(H)$ in the proof for Proposition 1.25. ◇

1.3 Quotient Groups

The right quotient set of a group G with respect to a subgroup H is the set of right cosets of H in G. This is the set of equivalence classes which arise from the equivalence relation $\sim$ where $a \sim b$ if $ab^{-1} \in H$, which implies that $Ha = Hb$. The left quotient set can be similarly defined as the equivalence classes which arise if $\sim$ is defined so that $a \sim b$ if $a^{-1}b \in H$. The quotient defined for right cosets is not, in general, equal to that which is defined in terms of left cosets. If, however, H is normal, these are equal and the single quotient set becomes a group with the following binary operation:

$$HaHb = Hab \quad \text{for } a, b \in G$$

To show this is well-defined let $Ha = Ha_0$ and $Hb = Hb_0$. We will show that $Hab = Ha_0b_0$. Let $x \in Hab$. Then $x = hab$ for some $h \in H$. Then, $x = ea(a^{-1}ha)b$. Because H is normal in G, $a^{-1}ha \in H$. Call $h_1 = e$ and $h_2 = a^{-1}ha$ so that $x = h_1ah_2b \in HaHb = Ha_0Hb_0$. Thus, $x = h_3a_0h_4b_0 = h_3(a_0h_4a_0^{-1})a_0b_0$. Because H is normal, $a_0h_4a_0^{-1} \in H$, so call $h_5 = a_0h_4a_0^{-1}$ and $h_6 = h_3h_5$. Then $x = h_6a_0b_0 \in Ha_0b_0$. Thus, $Hab = Ha_0b_0$ and the operation is well-defined.

Given that G's operation is associative,

$$(HaHb)Hc = HabHc$$

$$= Habc$$
$$= HaHbc$$
$$= Ha(HbHc).$$

The identity element is H, and for a coset Hg, its inverse is Hg^{-1}. We call this group a *quotient group* and denote it G/N.

Example 1.35. Let $\mathbb{C}^*$ be the set of complex numbers excluding 0. These form a group under multiplication with identity 1 and inverses given by the following: for $a+bi \in \mathbb{C}$, $(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$. Notice that because this group is abelian, every subgroup is normal. Recall that $|z|$ refers to z's distance from the origin in the complex plane. Consider $U = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$, the unit circle.
To show this is a subgroup, let z_1 and z_2 be in U. Then, $|z_1| = 1 = |z_2|$ and $|z_1 z_2| = |z_1||z_2|$ so $|z_1 z_2| = 1$.

Because U is a normal subgroup of $\mathbb{C}^*$, we can define the quotient group $\mathbb{C}^*/U$. To understand what elements of $\mathbb{C}^*/U$ look like, remember that U is the unit circle in the complex plane; that is, the circle of radius 1, whose center is at the origin. If we take another real number, say $r > 0$ and consider the coset $Ur \in \mathbb{C}^*/U$, what we are doing is multiplying each element in the circle by r, and thus creating a new circle of radius r. In fact, the same circle would be produced if we multiplied U by $-r$, ri, or $\frac{r\sqrt{2}}{2} + \frac{r\sqrt{2}}{2}i$, and infinitely more points on the complex plane whose magnitude is equal to r. Thus, the quotient group $\mathbb{C}^*/U$ can be thought of as the group of origin-centered circles in the complex plane, distinguished by their radius.
Consider the map $\phi : \mathbb{C}^*/U \to \mathbb{R}^+$ so that $\phi(Ur) = r$ for all $Ur \in \mathbb{C}^*/U$. This is clearly onto, as any real positive number r is mapped to by Ur, and it is one-to-one because if $r = s$, then the circles Ur and Us have the same radius and are thus equal. Thus this quotient group $\mathbb{C}^*/U$ is "like" the real numbers in a way we have yet to define. We will revisit this example in section 3.

Example 1.36. Consider $G = \langle x, y \,|\, x^5 = y^4 = e,\ y^{-1}xy = x^2 \rangle$, a group of order 20. We will show it has two normal subgroups; one of order 5 and one of order 10. First we give the elements of this group, along with their orders and inverses.

Element	Inverse	Order
e	e	1
x	x^4	5
x^2	x^3	5
x^3	x^2	5
x^4	x	5
y	y^3	4
xy	x^3y^3	4
x^2y	xy^3	4
x^3y	x^4y^3	4
x^4y	x^2y^3	4
y^2	y^2	2
xy^2	xy^2	2
x^2y^2	x^2y^2	2
x^3y^2	x^3y^2	2
x^4y^2	x^4y^2	2
y^3	y	4
xy^3	x^2y	4
x^2y^3	x^4y	4

x^3y^3	xy	4
x^4y^3	x^3y	4

The subgroups of G are as follows:

Subgroup	Elements	Order	Type
G	$e, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y, y^2, xy^2,$ $x^2y^2, x^3y^2, x^4y^2, y^3, xy^3, x^2y^3, x^3y^3, x^4y^3$	20	
$\langle x, y^2\rangle$	$e, x, x^2, x^3, x^4, y^2, xy^2, x^2y^2, x^3y^2, x^4y^2$	10	dihedral
$\langle x\rangle$	e, x, x^2, x^3, x^4	5	cyclic
$\langle y\rangle$	e, y, y^2, y^3	4	cyclic
$\langle xy\rangle$	e, xy, x^4y^2, x^3y^3	4	cyclic
$\langle x^2y\rangle$	e, x^2y, x^3y^2, xy^3	4	cyclic
$\langle x^3y\rangle$	e, x^3y, x^2y^2, x^4y^3	4	cyclic
$\langle x^4y\rangle$	e, x^4y, xy^2, x^2y^3	4	cyclic
$\langle y^2\rangle$	e, y^2	2	
$\langle xy^2\rangle$	e, xy^2	2	
$\langle x^2y^2\rangle$	e, x^2y^2	2	
$\langle x^3y^2\rangle$	e, x^3y^2	2	
$\langle x^4y^2\rangle$	e, x^4y^2	2	
$\langle e\rangle$	e	1	

Now, we describe the conjugate classes of G. Remember that each normal subgroup of a group is the union of one or more of its conjugate classes.

Class	Representative	Centralizer	Class Elements	Order
C_1	e	G	e	1
C_2	x	$\langle x\rangle$	x, x^2, x^4, x^3	5
C_3	y	$\langle y\rangle$	y, x^2y, x^4y, xy, x^3y	4
C_4	y^2	$\langle y\rangle$	$y^2, x^3y^2, xy^2, x^4y^2, x^2y^2$	2
C_5	y^3	$\langle y\rangle$	$y^3, x^4y^3, x^3y^3, x^2y^3, xy^3$	4

Notice that $C_1 \cup C_2 = \langle x\rangle$ and $C_1 \cup C_2 \cup C_4 = \langle x, y^2\rangle$. Let $H = \langle x\rangle$ and $K = \langle x, y^2\rangle$. These are normal subgroups in G and their respective quotient groups are

$$G/H = \{H, Hy, Hy^2, Hy^3\},$$

and

$$G/K = \{K, Ky\}.$$

Clearly, $G/H = \langle Hy\rangle$ and $G/K = \langle Ky\rangle$ are both cyclic groups.

We note that in the previous example, the group G has a subgroup $\langle y\rangle$, which is disjoint from its conjugates, and is its own normalizer in G. Groups which contain such subgroups are known in group theory as *Frobenius* groups. They are so called after the German mathematician Ferdinand Georg Frobenius.

Definition 1.37. Let G be a group. Let $[g, h]$ denote the following for all $g, h \in G$:

$$[g, h] = g^{-1}h^{-1}gh.$$

We call this the *commutator* of g and h in G. Collectively, they are referred to as the commutators of G.

Definition 1.38. Let G be a group and define G' to be the group generated by the commutators. We call this the *commutator subgroup* of G.

Notice that the commutator subgroup of a group G is the subgroup which is generated by its commutators, not simply that which consists only of its commutators. The set of commutators of a group do not necessarily form a subgroup. A counterexample which shows this can be found in [2] .

An observation which can be made about the commutator subgroup is that it is trivial if and only if the group G is abelian. The following is a theorem which can help compute the commutator subgroup of some group.

Theorem 1.39. *Let G be a group, H be a normal subgroup of G and G' be the commutator subgroup of G. Then, G/H is abelian if and only if $G' \subseteq H$.*

Proof. Suppose the H is a normal subgroup of G and G/H is abelian. Let $a, b \in G$. Then since G/H is abelian, $Hab = Hba$, and $Haba^{-1}b^{-1} = H$, which implies $aba^{-1}b^{-1} \in H$. Therefore, since an arbitrary commutator is in H, $G' \subseteq H$.
Suppose now that $G' \subseteq H$ and let $a, b \in G$. Then, $aba^{-1}b^{-1} \in H$ which implies $Hab = Hba$, and so G/H is abelian. ◇

Example 1.40. Consider the group $D_8 = \langle x, y \,|\, x^4 = y^2 = e,\ y^{-1}xy = x^{-1}\rangle$. The subgroup $\langle x^2\rangle$ is normal in D_8 as $y^{-1}x^2y = x^2$. Thus $G/\langle x^2\rangle$ is a quotient group of order 4, which means that it is abelian. Thus, $G' \subseteq \langle x^2\rangle$. Seeing as how D_8 is not abelian, $G' \neq \{e\}$. Therefore, $G' = \langle x^2\rangle = \{e, x^2\}$

Chapter 2

Homomorphisms, Isomorphisms, and Automorphisms of Groups

2.1 Homomorphisms and Isomorphisms

Definition 2.1. Let $(G, *)$ and $(H, \cdot)$ be groups. Then a map $\phi : G \to H$ such that $\phi(g * h) = \phi(g) \cdot \phi(h)$ for all $g, h \in G$ is called a *homomorphism*.

One way which we refer to this defining property of homomorphisms is to say that the map is *structure preserving*. This property extends to any finite product of elements. That is, if $\phi : G \to H$ is a homomorphism, then $\phi(g_1 g_2 ... g_k) = \phi(g_1)\phi(g_2)...\phi(g_k)$ for any $g_1, g_2, ..., g_k \in G$. In particular, $\phi(g^n) = \phi(g)^n$ for any $g \in G$ and $n \in \mathbb{N}$.

Definition 2.2. Let G and H be groups with identity elements e_G and e_H respectively, $\phi : G \to H$ be a homomorphism, and

$$K = \{g \in G \mid \phi(g) = e_H\}$$

be the group of elements in G which map to the identity in H. Then we call K to *kernel* of the homomorphism ϕ.

Theorem 2.3. *Let $\phi : G \to H$ be a homomorphism with kernel K. Then, $K \trianglelefteq G$.*

Proof. Let $\phi : G \to H$ be a homomorphism with kernel K, and let e_G and e_H be the respective identities of G and H. Then, let $g \in G$ and consider $g^{-1}Kg$. Let $k \in K$, so that $g^{-1}kg \in g^{-1}Kg$. Thus,

$$\begin{aligned} \phi(g^{-1}kg) &= \phi(g^{-1}) \underbrace{\phi(k)}_{=e_H} \phi(g) \\ &= \phi(g)^{-1}\phi(g) \\ &= e_H, \end{aligned}$$

and we have that $g^{-1}kg \in K$. Thus, $g^{-1}Kg = K$ by Theorem 1.15 and thus $K \trianglelefteq G$. ◇

Theorem 2.4. *If $\phi : G \to H$ is a homomorphism, then for $g \in G$, Order$(\phi(g))$ divides Order(g).*

Definition 2.5. Let $\phi : G \to H$ be a one-to-one and onto homomorphism. Then, ϕ is called an *isomorphism*, and we say that the groups G and H are *isomorphic* to each other, which we denote by $G \cong H$.

One consequence of two groups being isomorphic is that they will have equal orders. This follows from the fact that isomorphisms are one-to-one and onto. Thus, sometimes we can immediately see that two groups are not isomorphic, such as D_8 and D_{12}. Nothing beyond the observation that these groups have different orders is required to confirm that no isomorphism can exist

between them. The next consequence is that the image of an element under an isomorphism will have equal order to that elements.

Proposition 2.6. *Let G and H be groups and $\phi : G \to H$ be an isomorphism. Then for all $g \in G$, Order$(\phi(g))$ =Order(g).*

Proof. First, notice that since ϕ is one-to-one, the kernel of ϕ is trivial. In other words, no non-identity element in G maps to the identity in H.
Now, let g be in G and suppose that Order$(\phi(g)) = n$ and Order$(g) = m$. Then, $\phi(g^n) = \phi(g)^n = e_H$. Thus, because the kernel of ϕ is trivial, $g^n = e_G$. Since Order$(g) = m$, n must be some multiple of m. In particular, $n \geq m$. But then, $e_H = \phi(e_G) = \phi(g^m) = \phi(g)^m$ and so $\phi(g)^m = e_H$ so m must be some multiple of n. In particular, $m \geq n$. Therefore, $m = n$. ◇

It follows directly from this that two isomorphic groups will have the same number of elements of any given order.

Example 2.7. Recall $D_8 = \langle a, b \,|\, a^4 = b^2 = e,\ b^{-1}ab = a^{-1}\rangle$ and $Q_8 = \langle x, y \,|\, x^4 = y^4 = e,\ x^2 = y^2,\ y^{-1}xy = x^3\rangle$. These were discussed in Examples 1.28 and 1.31 respectively. While D_8 has five elements of order two, Q_8 has only one. Then, even though these groups have equal orders, we can say that they are non isomorphic because they do not have equal numbers of elements of a given order.

Theorem 2.8 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism. Then, if K is the kernel of ϕ,*

$$G/K \cong \phi(G).$$

Proof. Let $\sigma : G/K \to \phi(G)$ be defined so that for $g \in G$,

$$\sigma : Kg \longmapsto \phi(g).$$

This is a homomorphism as

$$\sigma(KgKh) = \sigma(Kgh) = \phi(gh) = \phi(g)\phi(h) = \sigma(Kg)\sigma(Kh).$$

It is onto because for every $h \in \phi(G)$, there is a $g \in G$ such that $\phi(g) = h$ and so $Kg \in G/K$ and $\sigma(Kg) = \phi(g) = h$.

Finally this function is one-to-one. Let $Kg, Kh \in G/K$ be such that $Kg \neq Kh$. Then, $gh^{-1} \notin K$ and so

$$\begin{aligned} & \phi(gh^{-1}) \neq e_H \\ \implies\ & \phi(g)\phi(h)^{-1} \neq e_H \\ \implies\ & \phi(g) \neq \phi(h). \end{aligned}$$

Thus, being a one-to-one and onto homomorphism, ϕ is an isomorphism and $G/K \cong \phi(G)$. ◇

Example 2.9. Recall Example 1.35 where we introduced the unit circle as a normal subgroup of the complex plane. Because $|z_1 z_2| = |z_1||z_2|$ in the complex plane, the map $\phi : \mathbb{C}^* \to \mathbb{R}^+$ defined so that $|z| \longmapsto z$, is a homomorphism. Then U, consisting of those $z \in \mathbb{C}^*$ such that $|z| = 1$ is the kernel of ϕ and by the previous theorem, $\mathbb{C}^*/U \cong \phi(\mathbb{C}^*) = \mathbb{R}^+$.

2.2 Automorphisms

Definition 2.10. Let G be a group and $\sigma : G \to G$ be an isomorphism. Then, σ is called an *automorphism* of G.

We give an example of an automorphism of a group.

Example 2.11. Consider the group $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. This group can be generated by the elements 2 and 11. In fact, it is the direct product $\langle 2 \rangle \times \langle 11 \rangle$ which is isomorphic to the group $C_4 \times C_2$. See Theorem 5.6 for a further discussion of the automorphisms of this group.
The orders of the elements of $\mathbb{Z}_{15}^*$ are given in the following table.

Element(s)	Order
1	1
2, 7, 8, 13	4
4, 11, 14	2

Let σ be the following mapping.

$$\begin{aligned} 1 &\longmapsto 1 & 2 &\longmapsto 7 \\ 4 &\longmapsto 4 & 7 &\longmapsto 2 \\ 8 &\longmapsto 13 & 11 &\longmapsto 11 \\ 13 &\longmapsto 8 & 14 &\longmapsto 14 \end{aligned}$$

Clearly this map is one-to-one and onto, so we only need to confirm that it is structure-preserving.

Element	Image under σ
$1 = 2^0$	$1 = 7^0$
$2 = 2^1$	$7 = 7^1$
$4 = 2^2$	$4 = 7^2$
$7 = 2 \cdot 11$	$2 = 7 \cdot 11$
$8 = 2^3$	$13 = 7^3$
$11 = 11^1$	$11 = 11^1$
$13 = 2^3 \cdot 11$	$8 = 7^3 \cdot 11$
$14 = 2^2 \cdot 11$	$14 = 7^2 \cdot 11$

In the left column, each element is written in terms of 2 and 11. The map σ sends 2 to 7 and 11 to itself. Because the image of each element can be written in terms of 7 and 11 with the same respective exponents, then this map is indeed structure-preserving and this is an automorphism of $\mathbb{Z}_{15}^*$.

Let $Aut(G)$ be the set of automorphisms of a group G. Then, with the binary operation of function composition, $Aut(G)$ is a group. Function composition is known to be associative, the identity is the identity map, and because each map σ is one-to-one and onto, it must have an inverse map σ^{-1} so that $\sigma \circ \sigma^{-1}$ and $\sigma^{-1} \circ \sigma$ both equal the identity.

Example 2.12. Consider the group $D_{10} = \langle x, y \,|\, x^5 = y^2 = e, y^{-1}xy = x^{-1} \rangle$. We said before that if we know how an automorphism maps the generating set of a group, we know how it maps the rest of the elements as well. So, in order to find out how many automorphisms there are, first we

consider how many ways there are of mapping the generating set $\{x, y\}$.
We know that an isomorphism maps elements to elements of the same order, so for our generator x, we can only map it to other order 5 elements. Likewise, we can only map y to other order 2 elements.

Element(s)	Order
e	1
x	5
x^2	5
x^3	5
x^4	5
y	2
xy	2
x^2y	2
x^3y	2
x^4y	2

Then, x may only be mapped to x, x^2, x^3, or x^4, and y may be mapped to y, xy, x^2y, x^3y, or x^4y. Any combination of these is a valid automorphism. To show this, we show that the structure of the relation $y^{-1}xy = x^{-1}$ is preserved no matter the configuration. Let ϕ be such that

$$\phi : x \longmapsto x^i, \qquad y \longmapsto x^j y.$$

Then,

$$\begin{aligned}\phi\left(y^{-1}xy\right) &= \left(x^j y\right)^{-1} x^i \left(x^j y\right) \\ &= y^{-1}x^{-j}x^i x^j y \\ &= y^{-1}x^i y \\ &= x^{-i} = \phi\left(x^{-1}\right)\end{aligned}$$

Then, there are $4 \times 5 = 20$ different ways of mapping x and y, and thus there are 20 automorphisms of D_{10}.
We can define the generators of the automorphism group by considering automorphisms which change one generator of D_{10} and leave the other invariant. Let σ and η be the following mappings:

$$\sigma : x \longmapsto x,\ y \longmapsto xy$$

$$\eta : x \longmapsto x^2,\ y \longmapsto y$$

It can be easily seen that σ is of order five, while η is of order four. Composing right to left, we consider the relationship between σ and η:

$$\begin{aligned}\eta^{-1}\sigma\eta(x) &= \eta^{-1}\sigma(x^2) \\ &= \eta^{-1}(x^2) \\ &= x\end{aligned}$$

$$\eta^{-1}\sigma\eta(y) = \eta^{-1}\sigma(y)$$

$$= \eta^{-1}(xy)$$
$$= x^3 y$$

This means that $\eta^{-1}\sigma\eta = a^3$, and so we can describe the automorphism group of D_{10} as

$$Aut(D_{10}) = \langle \sigma, \eta \,|\, \sigma^5 = \eta^4 = \varepsilon, \eta^{-1}\sigma\eta = \sigma^3 \rangle,$$

where ε is the identity mapping. Notice that $Aut(D_{10})$ is the same group we discussed in Example 1.36; it is often referred to as the Frobenius group of order 20 and denoted F_{20}.

In Chapter 5 we give numerous examples of automorphism groups.

Theorem 2.13. *Suppose G is a group and σ is an automorphism of G. If C is a conjugate class of G, then $\sigma(C)$ will be a conjugate class of G.*

Proof. Let $g, h \in G$ such that $g = x^{-1}hx$ for some $x \in G$. Suppose that σ is an automorphism of G and $\sigma(g) = g_0$, $\sigma(h) = h_0$, and $\sigma(x) = x_0$. Then,

$$\begin{aligned} x_0^{-1} g_0 x_0 &= \sigma(x)^{-1}\sigma(g)\sigma(x) \\ &= \sigma(x^{-1})\sigma(g)\sigma(x) \\ &= \sigma(x^{-1}gx) \\ &= \sigma(h) \\ &= h_0. \end{aligned}$$

Therefore, g_0 and h_0 are conjugate and automorphisms of G send conjugate classes to conjugate classes. Further, because σ is one-to-one, if C is a conjugate class of G, then $|C| = |\sigma(C)|$. ◇

Definition 2.14. Let G be a group with automorphism group $Aut(G)$. Let $\sigma \in Aut(G)$ such that for all $g \in G$, $\sigma(g) = x^{-1}gx$ for some fixed $x \in G$. Then σ is an *inner automorphism* of G. The set of inner automorphisms is denoted $Inn(G)$.

Definition 2.15. Let $\phi \in Aut(G)$ be such that ϕ is not inner. Then, ϕ is called an *outer automorphism* of G.

Theorem 2.16. *The set of inner automorphisms of a group G is a normal subgroup of the group of automorphisms of G.*

Proof. Note that we will be composing automorphisms from right to left.

First we prove that $Inn(G)$ is a subgroup of $Aut(G)$. Let α and β be in $Inn(G)$. Then there are fixed $a, b \in G$ so that $\alpha(g) = a^{-1}ga$ and $\beta(g) = b^{-1}gb$ for all $g \in G$. We can define the inverse of β as

$$\beta^{-1} : g \longmapsto bgb^{-1}$$

so that $\beta(\beta^{-1}(g)) = b^{-1}(bgb^{-1})b = g$. Thus we have the following:

$$\begin{aligned} \alpha(\beta^{-1}(g)) &= a^{-1}(bgb^{-1})a \\ &= (a^{-1}b)g(b^{-1}a) \\ &= (b^{-1}a)^{-1}g(b^{-1}a) \end{aligned}$$

Thus $\alpha\beta^{-1} \in Inn(G)$ and $Inn(G)$ is a subgroup of $Aut(G)$.
To show that it is normal, let $\sigma \in Aut(G)$ and $\phi \in Inn(G)$. Then,

$$\sigma^{-1}\phi\sigma : g \longmapsto \sigma^{-1}(\phi(\sigma(g)))$$

$$
\begin{aligned}
&= \sigma^1 \left(x^{-1} \sigma(g) x \right) \\
&= \sigma^{-1} \left(x^{-1} \right) \sigma^{-1}(\sigma(g)) \sigma^{-1}(x) \\
&= \left(\sigma^{-1}(x) \right)^{-1} g \, \sigma^{-1}(x)
\end{aligned}
$$

Then, $\sigma^{-1}\phi\sigma$ is defined by conjugation by $\sigma^{-1}(x) \in G$ which means that it is an inner automorphism. Thus,

$$\sigma^{-1} Inn(G) \sigma = Inn(G),$$

for any automorphism σ of G and $Inn(G) \trianglelefteq Aut(G)$. ◇

The quotient group $Aut(G)/Inn(G)$ is often denoted $Out(G)$. This is not to be confused with the set of outer automorphisms of a group, which itself does not constitute a group.

Theorem 2.17. *Let G be a group with center $Z(G)$. Then, $G/Z(G) \cong Inn(G)$.*

Proof. If we define a map $\phi : G \to Inn(G)$ wherein we send each $g \in G$ to the automorphism defined by conjugation by g, then $Z(G)$ is the kernel of ϕ and by Theorem 2.8, $G/Z(G) \cong \phi(G) = Inn(G)$. ◇

In particular, if $Z(G)$ is trivial, $G \cong G/Z(G) \cong Inn(G)$.

Chapter 3

Permutation Groups and Symmetric Groups

3.1 Introduction

Consider the sets $\Omega = \{1, 2, ..., n\}$ and S_n, the set of bijections from Ω to Ω. Under the operation of function composition, these form a group. Function composition is always associative, the identity element is the trivial map, which maps each $i \in \Omega$ to itself (we will usually denote this ε), and seeing as how the elements of S_n are bijections, each has an inverse. We call this the *symmetric group* on n letters, where "letters" refers to the elements of Ω.

We call the elements of S_n *permutations* because each bijection permutes the elements of Ω. The order of S_n is $n!$ because we can map the element 1 to any of the n elements, then 2 can be mapped to any of the remaining $n - 1$ elements, etc.

We have two common ways of denoting to elements of S_n. To illustrate, let $\sigma \in S_n$.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

This notation is easy to read, but takes up a bit of space. As such, it is more convenient to use what is called *cyclic* notation. For letters $a_1, a_2, ...a_k \in \Omega$, the *cycle* $(a_1, a_2, ..., a_k)$ refers to the permutation which sends a_1 to a_2, a_2 to a_3, and eventually a_{k-1} to a_k. Each permutation in S_n can be written uniquely as a disjoint product of these cycles, the sum of the lengths of which must equal n. Cycles of length k, we refer to as k-cycles. For example, the permutation $(1, 3, 2)$ in S_3, is a three-cycle which sends 1 to 3, 3 to 2, and 2 to 1. Using our other notation, we would write this as

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Another permutation in S_3 is $(1)(2, 3)$ which maps 1 to itself, 2 to 3, and 3 to 2. Note however, that if we know that 2 and 3 are mapped to each other, there is no other letter to which 1 can be mapped but itself. For this reason, we usually only write $(2, 3)$. Generally, for any n, we omit the one-cycles when writing elements of S_n in cyclic notation.

The binary operation in S_n is composition of functions, but we often refer to it as multiplication. We must decide then whether to multiply these elements from left to right, or right to left. The convention is composing functions is to compose from right to left, which is consistent with the usual way of writing a function f operating on an element x as $f(x)$, with the element written on the right of the function. However, when multiplying these permutations, we will multiply from

left to right, so that for permutations $\sigma, \phi \in S_n$:

$$\sigma\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ s_1 & s_2 & \cdots & s_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n \\ t_1 & t_2 & \cdots & t_n \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ t_{s_1} & t_{s_2} & \cdots & t_{s_n} \end{pmatrix}.$$

As an example for cycle multiplication, take $\alpha = (1,3,2,4)$ and $\beta = (1,4,3,2)$ in S_4. Then, $\alpha\beta = (1,2,3)(4) = (1,2,3)$; as 1 first goes to 3 in α, then 3 goes to 2 in β, which means that 1 will go to 2 in $\alpha\beta$; then 2 goes to 4 in α, then 4 goes to 3 in β, which means that 2 will go to 3 in $\alpha\beta$; then 3 goes to 2 in α, and 2 goes to 1 in β, which means that 3 will go to 1 in $\alpha\beta$; finally 4 goes to 1 in α, and then 1 goes to 4 in β so 4 is fixed by $\alpha\beta$.

Every permutation can be written as a product of disjoint cycles. For example, the permutation given by $(1,2,5,4,6)(1,2,4,3)(2,4,6,3)$ can be written as $(1,6,4,3)(2,5)$. This is unique up to the order of cycles. In the case of disjoint cycles, the order in which we write them does not matter because they commute.

The order of a cycle is equal to its length. This is because for a k-cycle $\sigma = (a_1, a_2, ...a_k)$, σ^ℓ would yield the following mapping:

$$\sigma^\ell : a_i \underset{\sigma}{\longmapsto} a_{i+1} \underset{\sigma}{\longmapsto} a_{i+2} \underset{\sigma}{\longmapsto} \cdots \underset{\sigma}{\longmapsto} a_{i+\ell} \pmod{k}.$$

Therefore, to fix each letter, one would need to perform σ some multiple of k times in order to cycle back around to the original letter.

If a permutation is expressed as the product of disjoint cycles, then its order will be the least common multiple of the lengths of each cycle. For example, consider a permutation ϕ which consists of a three and a two cycle. Then performing ϕ three times will fix each of the letters in the three-cycle, but not the two cycle, as it needs to be performed a multiple of two times in order to fix each letter. Therefore the smallest number which is divisible by three and two will fix each letter. This is the least common multiple, which in this case is six.

To make some of these ideas clearer, we will now give an example of a symmetric group on a relatively small set Ω.

Example 3.1. Let $\Omega = \{1,2,3,4\}$. We list the elements of S_4, organized by order and cycle type in the following table.

Element(s)	Order	Cycle Type
ε	1	1^4
$(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)$	2	$1^2 \cdot 2^1$
$(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$	2	2^2
$(1,2,3),(1,2,4),(1,3,2),(1,3,4),$ $(1,4,2),(1,4,3),(2,3,4),(2,4,3)$	3	$1^1 \cdot 3^1$
$(1,2,3,4),(1,2,4,3),(1,3,2,4),$ $(1,3,4,2),(1,4,2,3),(1,4,3,2)$	4	4^1

Sometimes we will refer to the *partition type* of a permutation. This refers to the number of letters in each cycle when said permutation is written in terms of disjoint cycles. For example, $(1,3,4)(2,5) \in S_5$ is of the type 3 + 2 because it consists of a three-cycle and a transposition. In

general if a permutation $\sigma \in S_n$ is the disjoint product

$$\sigma = (a_{11}, a_{12}, \ldots, a_{1k_1})(a_{21}, a_{22}, \ldots, a_{2k_2}) \cdots (a_{m1}, a_{m2}, \ldots, a_{mk_m}),$$

then σ is the type $k_1 + k_2 + \cdots + k_m$. Note that some of these k_is may be equal to one.
Suppose that we have a permutation η of the type

$$\underbrace{k_1 + \cdots + k_1}_{r_1 \text{ times}} + \underbrace{k_2 + \cdots + k_2}_{r_2 \text{ times}} + \cdots + \underbrace{k_\ell + \cdots + k_\ell}_{r_\ell \text{ times}}.$$

Instead of writing out the above, we will sometimes abbreviate this notation by writing that η is of the type $k_1^{r_1} \cdot k_2^{r_2} \cdots k_\ell^{r_\ell}$.

Theorem 3.2 (Cayley's Theorem)**.** *Let G be a group of order n. Then G is isomorphic to some subgroup of S_n.*

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. For every $g \in G$, let σ_g represent the following function from G to itself:

$$\sigma_g : g_i \longmapsto g_i g, \qquad g_i \in G, 1 \leq i \leq n.$$

This is known as the right regular representation of G. As a permutation of G, σ_g belongs to $Sym(G)$, the group of permutations on the elements of G.

Let $\phi : G \to Sym(G)$ be the following function:

$$\phi : g \longmapsto \sigma_g.$$

Recall that the operation in $Sym(G)$ is function composition, which we perform from left to right. Let $\sigma_g, \sigma_h \in Sym(G)$. Then,

$$\sigma_g = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 g & g_2 g & \cdots & g_n g \end{pmatrix}$$
$$\sigma_h = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 h & g_2 h & \cdots & g_n h \end{pmatrix}$$
$$\sigma_g \sigma_h = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 gh & g_2 gh & \cdots & g_n gh \end{pmatrix}.$$

We have that ϕ is a homomorphism as $\phi(gh) = \sigma_{gh}$ which sends $g_i \in G$ to $g_i gh = (g_i g)h = (\sigma_g(g_i))h = \sigma_g \sigma_h(g_i)$. Thus, $\sigma_{gh} = \sigma_g \sigma_h$ and so $\phi(gh) = \phi(g)\phi(h)$.

The kernel of ϕ is the trivial subgroup $\{e\}$ in G and by the First Isomorphism Theorem, $G/\{e\} \cong \phi(G)$, so $G \cong \phi(G)$, which is a subgroup of $Sym(G)$ as σ_g and σ_h being member of $Sym(G)$ implies $\sigma_g \sigma_h = \sigma_{gh}$ and $gh \in G$, so $\sigma_g \sigma_h \in \phi(G)$. ◇

Now we illustrate Cayley's Theorem in the following example.

Example 3.3. Consider D_{10}, the dihedral group of order ten, given by

$$D_{10} = \langle a, b \,|\, a^5 = b^2 = e,\ b^{-1}ab = a^{-1} \rangle = \{e, a, a^2, a^3, a^4, b, ab, a^2 b, a^3 b, a^4 b\}.$$

With each element of $g \in D_{10}$, we will associate the permutation σ_g, which sends each element of D_{10} to that element multiplied by g on the right. If we identify the elements of D_{10} as numbers:

$$e \longmapsto 1, \qquad\qquad b \longmapsto 6,$$

$$a \longmapsto 2, \qquad ab \longmapsto 7,$$
$$a^2 \longmapsto 3, \qquad a^2b \longmapsto 8,$$
$$a^3 \longmapsto 4, \qquad a^3b \longmapsto 9,$$
$$a^4 \longmapsto 5, \qquad a^4 \longmapsto 10,$$

then we can write the permutations σ_a and σ_b as follows:

$$\sigma_a = \begin{pmatrix} e & a & a^2 & a^3 & a^4 & b & ab & a^2b & a^3b & a^4b \\ a & a^2 & a^3 & a^4 & e & a^4b & b & ab & a^2b & a^3b \end{pmatrix} = (1,2,3,4,5)(6,10,9,8,7)$$
$$\sigma_b = \begin{pmatrix} e & a & a^2 & a^3 & a^4 & b & ab & a^2b & a^3b & a^4b \\ b & ab & a^2b & a^3b & a^4b & e & a & a^2 & a^3 & a^4 \end{pmatrix} = (1,6)(2,7)(3,8)(4,9)(5,10)$$

We give a table with each element of D_{10} and its associated permutation.

σ_e :	(e)	(1)
σ_a :	$(e, a, a^2, a^3, a^4)(b, a^4b, a^3b, a^2b, ab)$	$(1,2,3,4,5)(6,10,9,8,7)$
σ_{a^2} :	$(e, a^2, a^4, a, a^3)(b, a^3b, ab, a^4b, a^2b)$	$(1,3,5,2,4)(6,9,7,10,8)$
σ_{a^3} :	$(e, a^3, a, a^4, a^2)(b, a^2b, a^4b, ab, a^3b)$	$(1,4,2,5,3)(6,8,10,7,9)$
σ_{a^4} :	$(e, a^4, a^3, a^2, a)(b, ab, a^2b, a^3b, a^4b)$	$(1,5,4,3,2)(6,7,8,9,10)$
σ_b :	$(e,b)(a,ab)(a^2,a^2b)(a^3,a^3b)(a^4,a^4b)$	$(1,6)(2,7)(3,8)(4,9)(5,10)$
σ_{ab} :	$(e,ab)(a,a^2b)(a^2,a^3b)(a^3,a^4b)(a^4,b)$	$(1,7)(2,8)(3,9)(4,10)(5,6)$
σ_{a^2b} :	$(e,a^2b)(a,a^3b)(a^2,a^4b)(a^3,b)(a^4,ab)$	$(1,8)(2,9)(3,10)(4,6)(5,7)$
σ_{a^3b}	$(e,a^3b)(a,a^4b)(a^2,b)(a^3,ab)(a^4,a^2b)$	$(1,9)(2,10)(3,6)(4,7)(5,8)$
σ_{a^4b} :	$(e,a^4b)(a,b)(a^2,ab)(a^3,a^2b)(a^4,a^3b)$	$(1,10)(2,6)(3,7)(4,8)(5,9)$

Then, $D_{10} \cong \langle (1,2,3,4,5)(6,10,9,8,7),\ (1,6)(2,7)(3,8)(4,9)(5,10) \rangle$, which is a subgroup of S_{10}.

Definition 3.4. Let S_n be the symmetric group on n letters and $\tau \in S_n$ which fixes all elements in Ω except for two, which it interchanges. Then we call τ a *transposition*.

A few examples of transpositions in S_7 would be $(1,2)$, $(2,6)$, $(3,7)$, etc. In the group S_7, there are twenty-one transpositions. Because transpositions fix all but two elements which are mapped to each other, the number of transpositions in S_n for any n is equal to $\binom{n}{2}$.

Theorem 3.5. *Any cycle can be written as the product of transpositions.*

Proof. Let $(a_1, a_2, ..., a_k) \in S_n$ be a k-cycle. Then,

$$(a_1, a_2, ..., a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_{k-1})(a_1, a_k).$$

$\diamond$

For example, take $(2,4,5,3,6) \in S_6$. This can be written $(2,4)(2,5)(2,3)(2,6)$. This product is not unique; there may be many ways of expressing a cycle as a product of transpositions.

Theorem 3.6. *The symmetric group on* $\{1,2,...,n\}$ *is generated by its transpositions. In fact, it can generated by the* $n-1$ *transpositions* $(1,2)$*,* $(1,3)$*, ...,* $(1,n)$*.*

Proof. Let $\sigma \in S_n$. We know that any permutation can be written in terms of disjoint cycle, so let $\sigma = \eta_1\eta_2 \cdots \eta_k$ where each η_i is disjoint from the others.

By Theorem 3.5, each of these η_is can be written as a product of transpositions.Observe that for any transposition (a, b) we can write $(a, b) = (1, a)(1, b)(1, a)$, so any transposition can be written in terms of the $n - 1$ transpositions $(1, 2)$, $(1, 3)$, $\ldots$, $(1, n)$. Thus, any permutation can be written in terms of these and we have that these transpositions generate the whole group.

$\diamond$

Definition 3.7. Let G be a subgroup of S_n and suppose that for any $i, j \in \{1, 2, \ldots, n\}$, there exists some $\sigma \in G$ such that $\sigma(i) = j$. Then, G is called a *transitive* subgroup of S_n.

3.2 Parity of a Permutation and Alternating Groups

We've shown that any permutation may be written as a product of transpositions. This product may not be unique though. For example, the permutation $(1, 3, 4, 5, 2)$ in S_5 can be expressed as

$$(1, 3, 4, 5, 2) = (1, 3)(1, 4)(1, 5)(1, 2),$$

but $(1, 4)$ may be written $(1, 4) = (1, 2)(2, 4)(1, 2)$ so we can also write $(1, 3, 4, 5, 2)$ as

$$(1, 3, 4, 5, 2) = (1, 3)(1, 2)(2, 4)(1, 2)(1, 5)(1, 2).$$

Notice that although these are different ways of expressing our permutation, the number of transpositions in each product is even. For any $\sigma \in S_n$, when it is expressed as the product of transpositions, the number of transpositions in that product is always odd or always even. If a permutation always has an even number of transpositions when expressed as a product thereof, then we call it an *even permutation*. Similarly, a permutation which can only be expressed as a product of an odd number of transpositions is called an *odd permutation*. The nature of a permutation being either even or odd is referred to as its *parity*. In the following table we illustrate the possible parities of $\sigma\eta$ for $\sigma, \eta \in S_n$.

σ	η	$\sigma\eta$
Even	Even	Even
Even	Odd	Odd
Odd	Odd	Even

Theorem 3.8. *In a subgroup G of S_n, either all permutations are even or exactly half are even.*

Proof. First, because the identity is an even permutation, means that a G must contain at least one even permutation. If G contains an odd permutation however, we show that it must contain the exact same number of even permutations.

Let G be a subgroup of S_n such that $|G| = m$. Suppose G has $k \neq 0$ odd permutations. Then it have $m-k$ even permutations. Let A and B be the subsets of odd and even permutations respectively, so

$$A = \{a_1, a_2, ..., a_k\}, \qquad B = \{b_1, b_2, ..., b_{m-k}\}.$$

Let C and D be the following subsets of G

$$C = a_1A = \{a_1a_1,\ a_1a_2,\ ...,\ a_1a_k\}, \qquad D = a_1B = \{a_1b_1,\ a_1b_2,\ ...,\ a_1b_{m-k}\}.$$

The set C, whose cardinality is equal to that of A consists entirely of even permutations and thus must be a subset of B. Therefore, $|A| \leq |B|$. Similarly, D, whose cardinality is equal to that of B consists of odd permutations and is thus a subset of A. Therefore $|B| \leq |A|$. Then we have $|A| = |B|$

and so if G contains an odd permutation, exactly half of its permutations must be even. ◇

Theorem 3.9. *The set of all even permutations in S_n is a subgroup of S_n. It is called the alternating group on n letters and is denoted A_n. Its order is half that of S_n.*

Proof. Any two even permutations multiplied yield an even permutation, and the identity is an even permutation so A_n indeed constitutes a subgroup of S_n. By the previous theorem, the order of A_n is half that of S_n. That is, $|A_n| = |S_n|/2$. ◇

Example 3.10. The alternating group on four letters A_4 consists of the following twelve elements:

$$\begin{array}{cccc} (1), & (1,2)(3,4), & (1,3)(2,4), & (1,4)(2,3), \\ (1,2,3), & (1,2,4), & (1,3,2), & (1,3,4), \\ (1,4,2), & (1,4,3), & (2,3,4), & (2,4,3). \end{array}$$

Chapter 4

Sylow Theorems

Theorem 4.1. *Let G be a finite group with normal subgroups H and K. If $|H \cap K| = 1$, then $HK \cong H \times K$.*

Proof. It can be easily shown that HK is a subgroup of G is $HK = KH$. Because these are both normal, this is a given. Further, we have that $HK \trianglelefteq G$.

Because $|H \cap K| = 1$, for all $h \in H$ and $k \in K$, $|\langle h \rangle \cap \langle k \rangle| = 1$ and so the map $(h, k) \longmapsto hk$ is one-to-one and onto. Further notice that because H and K only intersect at the identity and are normal, that for $h \in H$ and $k \in K$, $h^{-1}k^{-1}hk \in H \cap K$ and thus $h^{-1}k^{-1}hk = e$, which implies that elements of H and K commute with each other.

Thus the map is also a homomorphism:

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2) \longmapsto h_1h_2k_1k_2 = (h_1k_1)(h_2k_2).$$

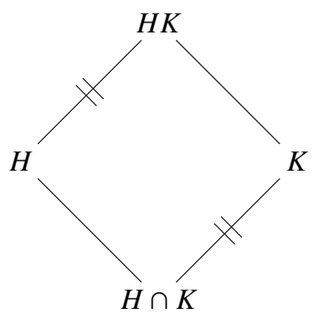
Therefore, $HK \cong H \times K$.

◇

Lemma 4.2. *Let G be a finite group with subgroups H and K. Then*

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

Proof. Consider the diagram:



The set HK can be written as the disjoint union

$$HK = Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n \quad \text{(disjoint)}$$

where $k_i \in K$, $1 \leq i \leq n$. Then $|HK| = |H|n$. Our goal now is to show that $n = \dfrac{|K|}{|H \cap K|}$. Let $\sim$ be a relation in K so that $g_1 \sim g_2$ if $g_1g_2^{-1} \in H$. Because $g_1, g_2 \in K$, then $g_1g_2^{-1} \in H \cap K$. Then, the number of resulting equivalence classes of K is exactly the number of right cosets of $H \cap K$ in K,

which is $\frac{|K|}{|H \cap K|}$. That is

$$K = (H \cap K)k_1 \cup (H \cap K)k_2 \cup \cdots \cup (H \cap K)k_n \quad \text{(disjoint)}.$$

Thus,

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

◇

Theorem 4.3 (Cauchy's Theorem)**.** *Let G be a finite abelian group and p be a prime such that p divides $|G|$. Then, G has an element of order p.*

Proof. We shall prove this by induction on the order of G. Clearly, the theorem holds for all groups of prime order. Now, assume that the theorem holds for all groups with order less than $|G|$.

Let H be a proper subgroup of G of largest order. There are two cases:

1. The first case is where H has order divisible by p. In this case, by our induction hypothesis, H contains an element of order p and thus so does G.

2. The other case is where the order of H is not divisible by p. Then, let $x \in G - H$, and $K = \langle x \rangle$.

   Because G is abelian, the subgroups H and K are normal, so HK is a subgroup of G. Further, because H is a subgroup of the largest order, $HK = G$. Then, $|G| = \frac{|H||K|}{|H \cap K|}$ and since $|G|$ is divisible by p and $|H|$ is not, this implies that $|K|$ is divisible by p. By the induction hypothesis then, K contains an element of order p, and thus so does G.

◇

Theorem 4.4 (Sylow's Theorem)**.** *Let G be a group such that $|G| = p^n t$ where p does not divide t. Then, G has a subgroup of order p^n.*

Proof. We prove this by induction on the order of G, so assume that the theorem holds for groups whose order is less than $|G|$.

Let C_i for $1 \leq i \leq k$ be the conjugate classes of G each with representative $x_i \in C_i$. The number of elements in each class is equal to the centralizer of an element in the class. So,

$$|C_i| = \frac{|G|}{C_G(x_i)},$$

for $1 \leq i \leq k$. We also have that

$$|G| = |C_1| + |C_2| + \cdots + |C_k|,$$

where C_1 is the class containing the identity, so $|C_i| = 1$. Regarding the number of elements of the other classes, we have the following two cases:

1. The first case is that for some i where $1 < i \leq k$, either $|C_i| > 1$, and is not divisible by p. As $|G| = |C_G(x_i)| \cdot |C_i|$, we have that $|C_G(x_i)|$ is divisible by p^n. By our induction hypothesis, $C_G(x_i)$ has a subgroup of order p^n, and thus so does G.

2. The other case is that for all $i \neq 1$, $i \leq k$, $|C_i| = 1$ or $|C_i|$ is divisible by p. Because $|C_1| = 1$, at least $p - 1$ other classes must also contain only one element because otherwise the sum

$$|C_1| + |C_2| + \cdots + |C_k|$$

would not be divisible by p, which it must be since it equals $|G| = p^n t$. Thus, there are some multiple of p classes which contain only one element. Any element which is alone in a conjugate class is in the center of the group $Z(G)$, so $|Z(G)|$ is divisible by p. By Theorem 4.3, $Z(G)$, being abelian, has an element z of order p. Thus $H = \langle z \rangle$ is a normal subgroup of G. Then G/H is a group of order $p^{n-1}t$. By our induction hypothesis, G/H has a subgroup P/H of order p^{n-1}. Then $|P| = p^n$. Therefore G has a subgroup of order p^n.

$\diamond$

Definition 4.5. Let G be a group with $|G| = p^n t$ where p does not divide t. Then, a subgroup of G of order p^n is called a *Sylow p-subgroup* of G.

Lemma 4.6. *Let G be a group with subgroups H and K. Then, there exists $\{x_1, x_2, ..., x_r\} \subset G$ such that*

$$G = Hx_1K \cup Hx_2K \cup \cdots \cup Hx_rK \quad \textit{(disjoint).}$$

Further,

$$|G| = \sum_{i=1}^{r} \frac{|H||K|}{|(x_i^{-1}Hx_i) \cap K|}.$$

Proof. Define the relation $\sim$ on G so that for $x, y \in G$, $x \sim y$ if there exists $a \in H$ and $b \in K$ so that $x = ayb$. It is easy to show that this is an equivalence relation.

The equivalence classes are exactly the sets HxK for each x and these partition the group G into disjoint sets Hx_iK. Thus,

$$G = Hx_1K \cup Hx_2K \cup \cdots \cup Hx_rK \quad \text{(disjoint)}$$

where $x_1, x_2, ..., x_r$ all lie in separate equivalence classes.

Recall that for any subgroup H, $x^{-1}Hx$ is also a subgroup for any $x \in G$. Further recall the statement from Lemma 4.2. Then,

$$|HxK| = \left|\left(x^{-1}HxK\right)\right| = \frac{|x^{-1}Hx||K|}{|(x^{-1}Hx) \cap K|} = \frac{|H||K|}{|(x^{-1}Hx) \cap K|}.$$

Thus,

$$|G| = \sum_{i=1}^{r} |Hx_iK| = \sum_{i=1}^{r} \frac{|H||K|}{|(x_i^{-1}Hx_i) \cap K|}.$$

$\diamond$

Theorem 4.7. *Let G be a group such that $|G| = p^n t$ where p does not divide t. If P and Q are any two Sylow p-subgroups of G, then there exists some $g \in G$ such that $P = g^{-1}Qg$.*

Proof. By the previous lemma, we can find $x_1, x_2, ..., x_r \in G$ such that

$$G = Px_1Q \cup Px_2Q \cup \cdots \cup Px_rQ \quad \text{(disjoint)}.$$

Let $d_i = |(x_i^{-1}Px_i) \cap Q|$ for $1 \leq i \leq r$. The orders of P and Q are both p^n so d_i must be some power of p since their intersection is a subgroup of each of them. Thus $d_i = p^{m_i}$ for some $0 \leq m_i \leq n$ for $1 \leq i \leq r$. Then,

$$|G| = p^n t = \sum_{i=1}^{r} \frac{|P||Q|}{|(x_i^{-1}Px_i) \cap Q|} = \sum_{i=1}^{r} \frac{p^{2n}}{d_i} = \sum_{i=1}^{r} \frac{p^{2n}}{p^{m_i}}$$

$$\implies p^n t = \sum_{i=1}^{r} \frac{p^{2n}}{p^{m_i}}$$

$$\implies t = \sum_{i=1}^{r} \frac{p^n}{p^{m_i}}$$

If each $m_i < n$, then t is the sum of powers of p, meaning that p divides t, which we've assumed not to be true. Thus, there must be some j, $1 \leq j \leq r$, such that $m_j = n$, so that $\frac{p^n}{p^{m_j}} = 1$. Then, $|x_j^{-1} P x_j \cap Q| = p^n$ which implies that $x_j^{-1} P x_j = Q$ ◇

Corollary 4.8. *The subgroup P is the unique Sylow p-subgroup of G if and only if P is normal in G.*

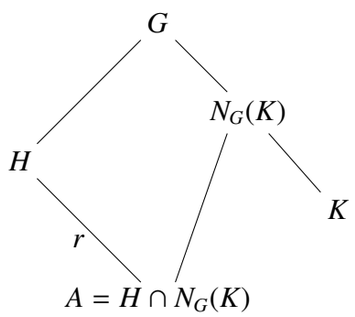
Proof. If P is the only Sylow p-subgroup of G, then for any $g \in G$, $g^{-1}Pg = P$ since otherwise, $g^{-1}Pg = Q$, another Sylow p-subgroup. Therefore $P \trianglelefteq G$.

If, on the other hand, P is normal in G, $g^{-1}Pg = P$ for $g \in G$ and therefore there can be no other Sylow p-subgroup Q because that would imply that there exists some $g \in G$ for which $g^{-1}Pg \neq P$. ◇

Lemma 4.9. *Let G be a group with subgroups H and K. The number of disjoint conjugates of K by elements in H is equal to $\frac{|H|}{|N_G(K) \cap H|}$.*

Proof. First notice that because $N_G(K)$ and H are both subgroups of G, so is $N_G(K) \cap H$. Further, it is a subgroup of H. Call $N_G(K) \cap H = A$. Then, we can write H as

$$H = Ah_1 \cup Ah_2 \cup \cdots \cup Ah_r \quad \text{(disjoint)}.$$



Let $\{h^{-1}Kh \,|\, h \in H\}$ be the set of conjugates of K by elements in H. We will show that there are r conjugates by showing a one-to-one and onto function exists between $\{h^{-1}Kh \,|\, h \in H\}$ and the set of right cosets of A.

Define f so that $h^{-1}Kh \longmapsto Ah$. This is clearly onto as any element $h \in H$ gives us a coset Ah and a conjugate $h^{-1}Kh$. To show it is one-to-one, assume $g^{-1}Kg \neq h^{-1}Kh$. Then, we have

$$\begin{aligned} & g^{-1}Kg \neq h^{-1}Kh \\ \implies & hg^{-1}Kgh^{-1} \neq K \\ \implies & gh^{-1} \notin K \\ \implies & Kg \neq Kh \end{aligned}$$

Thus, f is one-to-one and onto and the number of conjugates of K by elements in H is equal to the number of right cosets of $A = N_G(K) \cap H$ by elements in H, which is $\frac{|H|}{|N_G(K) \cap H|}$. ◇

Theorem 4.10. *The number of Sylow p-subgroups of G is n_p where n_p divides $|G|$ and $n_p \equiv 1 \pmod{p}$.*

Proof. Let $\Omega = \{P_1, P_2, ..., P_{n_p}\}$ be the set of Sylow p-subgroups of G. These are all conjugate to each other by Theorem 4.7. Consider the relation $\sim$ where $P_i \sim P_j$ if there exists some $g \in P_1$ such that $g^{-1}P_i g = P_j$. This is an equivalence relation, so the set Ω is partitioned into disjoint classes $\Delta_i = \{g^{-1}P_i g, \mid g \in N_G(P_1)\}$. Then,

$$\Omega = \Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_k \quad \text{(disjoint)},$$

and

$$|\Omega| = \sum_{i=1}^{k} |\Delta_i|.$$

There is only one element in Δ_1 and that is P_1. For any P_i, $i > 1$, the equivalence class containing P_i will have $\dfrac{|P_1|}{|N_G(P_i) \cap P_1|}$ elements by the previous lemma. We note that each $N_G(P_i) \cap P_1$ cannot have the same number of elements as P_1 for $i > 1$. This is because P_i is distinct from P_1 for all $i > 1$, and so if $|N_G(P_i) \cap P_1| = |P_1|$, then it follows that $P_1 P_i$ is a subgroup of order greater than p^n, which is not possible. Then, $\dfrac{|P_1|}{|N_G(P_i) \cap P_1|} = p^{m_i}$ for $1 \leq m_i \leq n$. Thus, each Δ_i has some power of p elements except for Δ_1 which has only one. Therefore

$$n_p = |\Omega| \equiv 1 \pmod{p}.$$

$\diamond$

Theorem 4.11. *Let G be an abelian group where $|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. Let P_i be the Sylow p_i-subgroup for each prime factor p_i, $1 \leq i \leq k$, of n. Then*

$$G \cong P_1 \times P_2 \times \cdots \times P_k$$

Proof. Because G is abelian, each P_i is normal. Because each pair of Sylow p_i-subgroups has relatively prime order, each pair has a trivial intersection.

By Theorem 4.1, $P_1 P_2$ is a normal subgroup of G isomorphic to $P_1 \times P_2$. Then $(P_1 P_2)P_3$ is a normal subgroup of G isomorphic to $(P_1 \times P_2) \times P_3$. Proceed inductively to conclude that $P_1 P_2 \cdots P_k$ is a normal subgroup of G isomorphic to $P_1 \times P_2 \times \cdots \times P_k$. Because the orders of all the Sylow subgroups multiply to yield the order of G,

$$G = P_1 P_2 \cdots P_k \cong P_1 \times P_2 \times \cdots \times P_k.$$

$\diamond$

Chapter 5

Automorphisms of Some Finite Groups

In this chapter, we shall describe the automorphism groups of some finite groups, as well as describe the automorphism groups of finite cyclic groups generally. We give a table of the groups we consider along with their automorphism groups. In one case, we refer to F_{20}, which denotes the Frobenius group of order 20, which we described in Example 2.12. Throughout, we refer to the cyclic group of order n as C_n. By $GL(n, q)$, we mean the general linear group of $n \times n$ matrices over $GF(q)$, which is the group of non-singular $n \times n$ matrices with entries from the finite field, of order q.

Order	Group	Automorphism Group
4	C_4	C_2
4	$C_2 \times C_2$	S_3
6	C_6	C_2
6	S_3	S_3
8	C_8	$C_2 \times C_2$
8	$C_4 \times C_2$	D_8
8	$C_2 \times C_2 \times C_2$	$GL(3, 2)$
8	D_8	D_8
8	Q_8	S_4
9	C_9	C_6
9	$C_3 \times C_3$	$GL(2, 3)$
10	C_{10}	C_4
10	D_{10}	F_{20}
12	A_4	S_4
24	S_4	S_4
60	A_5	S_5
120	S_5	S_5
p	C_p	C_{p-1}
p^n, $p > 2$	C_{p^n}	$C_{p^{n-1}(p-1)}$
2^n	C_{2^n}	$C_{2^{n-2}} \times C_2$

5.1 Order Four Groups

Theorem 5.1. *The automorphism group Aut*(C_4) *is isomorphic to* C_2.

Proof. Let C_4 be the cyclic group generated by x, so

$$C_4 = \langle x \rangle = \{e, x, x^2, x^3\}.$$

The image of an element under an automorphism must be the same order as the element, so x which is of order four, can only be mapped to x or x^3, meaning there are exactly two automorphisms possible. Thus $Aut(C_4) \cong C_2$. ◇

Theorem 5.2. *The automorphism group $Aut(C_2 \times C_2)$ is isomorphic to S_3.*

Proof. The group $C_2 \times C_2 = \{e, x, y, xy\}$ consists of three elements of order two, along with the identity, where multiplying two order two elements yields the third. This means that any one-to-one mapping from $\{x, y, xy\}$ to itself will be an automorphism. Therefore, any automorphism is a permutation of these three elements, and so $Aut(C_2 \times C_2) \cong S_3$. ◇

5.2 Order Six Groups

Theorem 5.3. *The automorphism group $Aut(S_3)$ is isomorphic to S_3.*

Proof. First, we give a presentation of S_3 which will make defining automorphisms easier. Let $x = (1, 2, 3)$ and $y = (1, 2)$. Then we have that $y^{-1}xy = (1, 3, 2) = x^{-1}$. Thus,

$$S_3 = \langle x, y \,|\, x^3 = y^2 = e,\ y^{-1}xy = x^{-1} \rangle \cong D_6.$$

Because x and y generate this group, we will define our automorphisms in terms of these. Being of order three x can only go to x or x^2, and being order two y can only go to y, xy, or x^2y. Any order three and order two elements will generate the group so any combination of these mapping yields a valid automorphism.

Let σ and η be that following maps:

$$\sigma : x \longmapsto x, \qquad y \longmapsto xy,$$

$$\eta : x \longmapsto x^2, \qquad y \longmapsto y.$$

Then,

$$\sigma^3 : x \longmapsto x, \qquad y \longmapsto y,$$

$$\eta^2 : x \longmapsto x, \qquad y \longmapsto y.$$

And finally,

$$\begin{aligned} \eta^{-1}\sigma\eta(x) &= \eta^{-1}\sigma(x^2) \\ &= \eta^{-1}(x^2) \\ &= x = \sigma^{-1}(x), \end{aligned}$$

$$\begin{aligned} \eta^{-1}\sigma\eta(y) &= \eta^{-1}\sigma(y) \\ &= \eta^{-1}(xy) \\ &= x^2y = \sigma^{-1}(y). \end{aligned}$$

Thus, $Aut(S_3) = \langle \sigma, \eta \,|\, \sigma^3 = \eta^2 = e,\ \eta^{-1}\sigma\eta = \sigma^{-1} \rangle \cong S_3$. ◇

Theorem 5.4. *The automorphism group $Aut(C_6)$ is isomorphic to C_2.*

Proof. The group C_6 has only two elements of order 6 and thus its automorphism group is order two, meaning $Aut(C_6) \cong C_2$. ◇

5.3 Order Eight Groups

Theorem 5.5. *The automorphism group $Aut(C_8)$ is isomorphic to $C_2 \times C_2$.*

Proof. The group C_8 has four elements of order eight and thus its automorphism group can be either C_4 or $C_2 \times C_2$. Those elements are x, x^3, x^5, and x^7. Because $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, all automorphisms of C_8 have order two.

Thus, $Aut(C_8) \cong C_2 \times C_2$. ◇

Theorem 5.6. *The automorphism group $Aut(C_4 \times C_2)$ is isomorphic to D_8.*

Proof. In Example 2.11, we discussed the group $\mathbb{Z}_{15}^*$ which is isomorphic to $C_4 \times C_2$. Here, we describe its automorphism group.

The group $C_4 \times C_2 = \langle x, y \,|\, x^4 = y^2 = e,\ xy = yx \rangle$ is generated by any of its order four elements x, x^3, xy, and x^3y and either y and x^2y. Thus, there are eight possible mappings for x and y. Let σ and η be the following maps:

$$\sigma : x \longmapsto xy, \qquad y \longmapsto x^2y,$$

$$\eta : x \longmapsto xy, \qquad y \longmapsto y.$$

Then,

$$\sigma^4 : x \longmapsto x, \qquad y \longmapsto y,$$

$$\eta^2 : x \longmapsto x, \qquad y \longmapsto y.$$

And,

$$\begin{aligned} \eta^{-1}\sigma\eta(x) &= \eta^{-1}\sigma(xy) \\ &= \eta^{-1}(x^3) \\ &= x^3y = \sigma^{-1}(x), \end{aligned}$$

$$\begin{aligned} \eta^{-1}\sigma\eta(y) &= \eta^{-1}\sigma(y) \\ &= \eta^{-1}(x^2y) \\ &= x^2y = \sigma^{-1}(x). \end{aligned}$$

Thus, $Aut(C_4 \times C_2) = \langle \sigma, \eta \,|\, \sigma^4 = \eta^2 = e,\ \eta^{-1}\sigma\eta = \sigma^{-1} \rangle \cong D_8$. ◇

Theorem 5.7. *The automorphism group $Aut(C_2 \times C_2 \times C_2)$ is isomorphic to $GL(3,2)$, the group of non-singular 3×3 matrices with entries from $GF(2)$.*

Proof. Let $G = C_2 \times C_2 \times C_2$. Every non-identity element in G is order two, so any two elements along with a third which is not their product will generate this group. Thus, there are $7 \times 6 \times 4$ possible automorphisms of G, and $|Aut(G)| = 168$. Let $G = \langle x, y, z \rangle$. Then, let automorphisms α and β be defined as follows:

$$\alpha : x \longmapsto x^{a_{11}}y^{a_{21}}z^{a_{31}}, \qquad y \longmapsto y^{a_{12}}y^{a_{22}}z^{a_{32}}, \qquad z \longmapsto z^{a_{13}}y^{a_{23}}z^{a_{33}}$$

$$\beta : x \longmapsto x^{b_{11}}y^{b_{21}}z^{b_{31}}, \qquad y \longmapsto y^{b_{12}}y^{b_{22}}z^{b_{32}}, \qquad z \longmapsto z^{b_{13}}y^{b_{32}}z^{b_{33}},$$

where a^{ij}, $b^{kl} \in \{0, 1\}$. Consider the group $GL(3,2)$ of non-singular 3×3 matrices whose entries come from $GF(2) = \{0, 1\}$. Let $\phi : Aut(G) \to GL(3,2)$ be defined so that each automorphism is mapped to a matrix whose entries correspond to the exponents of x, y, and z. This is a valid function as no automorphism takes x, y, or z to the identity, and no one of x, y, or z can be mapped

to the product of the images of the other two, which ensures that the image of every automorphism under ϕ is non-singular. This map is clearly one-to-one and thus onto because the two groups have equal orders. Then, ϕ maps α and β thus:

$$\phi : \alpha \longmapsto A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \quad \beta \longmapsto B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Now we compute the images of x, y, and z under $\alpha\beta$, where $\alpha\beta$ denotes first performing β and then α:

$$\begin{aligned} \alpha\beta(x) &= \alpha(x^{b_{11}} y^{b_{21}} z^{b_{31}}) \\ &= \alpha(x)^{b_{11}} \alpha(y)^{b_{21}} \alpha(z)^{b_{31}} \\ &= (x^{a_{11}} y^{a_{21}} z^{a_{31}})^{b_{11}} (y^{a_{12}} y^{a_{22}} z^{a_{32}})^{b_{21}} (z^{a_{13}} y^{a_{23}} z^{a_{33}})^{b_{31}} \\ &= x^{a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31}} y^{a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31}} z^{a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31}} \end{aligned}$$

$$\begin{aligned} \alpha\beta(y) &= \alpha(x^{b_{12}} y^{b_{22}} z^{b_{32}}) \\ &= \alpha(x)^{b_{12}} \alpha(y)^{b_{22}} \alpha(z)^{b_{32}} \\ &= (x^{a_{11}} y^{a_{21}} z^{a_{31}})^{b_{12}} (y^{a_{12}} y^{a_{22}} z^{a_{32}})^{b_{22}} (z^{a_{13}} y^{a_{23}} z^{a_{33}})^{b_{31}} \\ &= x^{a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32}} y^{a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32}} z^{a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32}} \end{aligned}$$

$$\begin{aligned} \alpha\beta(z) &= \alpha(x^{b_{13}} y^{b_{23}} z^{b_{33}}) \\ &= \alpha(x)^{b_{13}} \alpha(y)^{b_{23}} \alpha(z)^{b_{33}} \\ &= (x^{a_{11}} y^{a_{21}} z^{a_{31}})^{b_{13}} (y^{a_{12}} y^{a_{22}} z^{a_{32}})^{b_{23}} (z^{a_{13}} y^{a_{23}} z^{a_{33}})^{b_{33}} \\ &= x^{a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33}} y^{a_{21}b_{13}+a_{22}b_{23}+a_{23}b_{33}} z^{a_{31}b_{13}+a_{32}b_{23}+a_{33}b_{33}} \end{aligned}$$

The image of $\alpha\beta$ under ϕ would then be a matrix with the first column having the exponents of x, y, and z in $\alpha\beta(x)$, like so:

$$\begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{bmatrix}$$

Notice that this matches AB. Thus, ϕ maps $\alpha\beta$ to $AB = \phi(\alpha)\phi(\beta)$ and thus is a homomorphism.

Thus, $Aut(G) = Aut(C_2 \times C_2 \times C_2) \cong GL(3, 2)$. ◇

Remark: Here, we are essentially regarding $C_2 \times C_2 \times C_2$ as a three-dimensional vector space over $GF(2)$, where our automorphisms correspond to linear transformations, which are 3×3 non-singular matrices, of which the group $GL(3, 2)$ consists.

Theorem 5.8. *The automorphism group $Aut(D_8)$ is isomorphic to D_8.*

Proof. The group D_8 has two elements of order four, namely x and x^3, and five elements of order two, x^2, y, xy, x^2y, and x^3y. Any order two elements except x^2 and any order four element generate this group, so x has two possible images under an automorphism and y has four. Thus, there are

eight automorphisms. Let σ and η be the following automorphisms:

$$\sigma : x \longmapsto x, \qquad y \longmapsto xy,$$

$$\eta : x \longmapsto x^3, \qquad y \longmapsto y.$$

Then,

$$\sigma^4 : x \longmapsto x, \qquad y \longmapsto y,$$

$$\eta^2 : x \longmapsto x, \qquad y \longmapsto y,$$

and

$$\begin{aligned} \eta^{-1}\sigma\eta(x) &= \eta^{-1}\sigma(x^3) \\ &= \eta^{-1}(x^3) \\ &= x = \sigma^{-1}(x), \end{aligned}$$

$$\begin{aligned} \eta^{-1}\sigma\eta(y) &= \eta^{-1}\sigma(y) \\ &= \eta^{-1}(xy) \\ &= x^3y = \sigma^{-1}(x). \end{aligned}$$

Thus, $Aut(D_8) = \langle \sigma, \eta \,|\, \sigma^4 = \eta^2 = e,\ \eta^{-1}\sigma\eta = \sigma^{-1} \rangle \cong D_8$. ◇

Theorem 5.9. *The automorphism group $Aut(Q_8)$ is isomorphic to S_4.*

Proof. Consider the quaternion group:

$$Q_8 = \langle x, y \,|\, x^4 = y^4 = e,\ x^2 = y^2,\ y^{-1}xy = x^3 \rangle = \{e,\ x,\ x^2,\ x^3,\ y,\ xy,\ x^2y,\ x^3y\}.$$

This group has only one element of order two, namely x^2, and it has six elements of order four. The element of order two is the square of each of these order four elements. Therefore, we have three subgroups of order four in this group. Denote these:

$$H_1 = \langle x \rangle = \{e, x, x^2, x^3\}, \quad H_2 = \langle y \rangle = \{e, y, x^2, x^2y\}, \quad H_3 = \langle xy \rangle = \{e, xy, x^2, x^3y\}.$$

Observe that the group can be generated by any two of its order four elements if they are not inverses of each other. There are twelve possible generating sets:

$$\begin{array}{cccccc} \{x, y\}, & \{x, xy\}, & \{x, x^2y\}, & \{x, x^3y\}, & \{x^3, y\}, & \{x^3, xy\} \\ \{x^3, x^2y\}, & \{x^3, x^3y\}, & \{y, xy\}, & \{y, x^3y\}, & \{x^2y, xy\}, & \{x^2y, x^3y\}. \end{array}$$

The image of just one of these sets under an automorphism will define the images of the rest, so consider the set $\{x, y\}$. There are twelve sets it may be mapped to, and two ways it can be mapped to each. Therefore there are a total of twenty-four possible automorphisms. In other words $|Aut(Q_8)| = 24$.

Now, from each of our cyclic subgroups H_1, H_2, and H_3 above, choose one order four representative and put these into a set. The different combinations result in eight possible subsets:

$$\begin{array}{cccc} \{x, y, xy\}, & \{x, y, x^3y\} & \{x, x^2y, xy\}, & \{x, x^2y, x^3y\}, \\ \{x^3, y, xy\}, & \{x^3, y, x^3y\} & \{x^3, x^2y, xy\}, & \{x^3, x^2y, x^3y\}. \end{array}$$

For convenience, define $i = x$, $j = y$, and $k = xy$. Then, the subsets we've define above are

$$\begin{array}{llll} \{i, j, k\}, & \{i, j, k^{-1}\} & \{i, j^{-1}, k\}, & \{i, j^{-1}, k^{-1}\}, \\ \{i^{-1}, j, k\}, & \{i^{-1}, j, k^{-1}\} & \{i^{-1}, j^{-1}, k\}, & \{i^{-1}, j^{-1}, k^{-1}\}. \end{array}$$

An automorphism must map an element to one of the same order and since we can generate our group from two elements, we need only be concerned with where these go. Then, if i, for example, can go to any of the six order four elements, j then can go only to four because it cannot go to the inverse of i's image. Because k is the product of i and j, its image is determined from those of i and j. Therefore, an automorphism will map each of the three element sets above to one of the eight, and the inverses of that set will be mapped to the inverses of the image set. If we group our three element sets like so:

$$\begin{array}{ll} \Delta_1 = \{\{i, j, k\}, \{i^{-1}, j^{-1}, k^{-1}\}\}, & \Delta_2 = \{\{i, j, k^{-1}\}, \{i^{-1}, j^{-1}, k\}\}, \\ \Delta_3 = \{\{i, j^{-1}, k\}, \{i^{-1}, j, k^{-1}\}\}, & \Delta_4 = \{\{i, j^{-1}, k^{-1}\}, \{i^{-1}, j, k\}\}, \end{array}$$

it is clear that an automorphism of Q_8 will permute the Δ_is. In fact, any permutation of these yields a valid automorphism because it maps generating sets to generating sets and such a map would be structure-preserving, one-to-one, and onto. Therefore the automorphism group of Q_8 is the group of permutations on four symbols.Thus, $Aut(Q_8) \cong S_4$.

◇

5.4 Order Nine Groups

Theorem 5.10. *The automorphism group $Aut(C_9)$ is isomorphic to C_6.*

Proof. The group $C_9 = \langle x \rangle$ has six elements of order nine and thus six automorphisms. If we let σ map x to x^2, then

$$\sigma : x \longmapsto x^2,$$

$$\sigma^2 : x \longmapsto x^4,$$

$$\sigma^3 : x \longmapsto x^8,$$

$$\sigma^4 : x \longmapsto x^7,$$

$$\sigma^5 : x \longmapsto x^5,$$

$$\sigma^6 : x \longmapsto x.$$

Because σ is order six, the same as the number of automorphisms, the group $Aut(C_9) \cong C_6$. ◇

Theorem 5.11. *The automorphism group $Aut(C_3 \times C_3)$ is isomorphic to $GL(2, 3)$.*

Proof. Let $G = C_3 \times C_3$. Every non-identity element in G is order three, so any two elements will generate this group as long as they are not inverses. Thus, there are 8×6 possible generating sets and thus 48 automorphisms of G, so $|Aut(G)| = 48$. Let $G = \langle x, y \rangle$. Then an automorphism of G will map x and y as follows:

$$\sigma : x \longmapsto x^{a_{11}} y^{a_{21}}, \qquad y \longmapsto y^{a_{12}} y^{a_{22}}.$$

Consider the group $GL(3, 2)$ of non-singular 3×3 matrices whose entries come from $GF(3) =$

$\{0, 1, 2\}$. Let $\phi : Aut(G) \to GL(2, 3)$ be defined as follows:

$$\phi : \sigma \longmapsto \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

This is a valid function as no automorphism takes x or y to the identity, and no automorphism will take x to the inverse of the image of y, which ensures that the image of every automorphism under ϕ is non-singular. This map is clearly one-to-one and thus onto because the two groups have equal orders. To show it is a homomorphism, let automorphisms σ and η be defined as follows:

$$\sigma : x \longmapsto x^{a_{11}} y^{a_{21}}, \quad y \longmapsto y^{a_{12}} y^{a_{22}},$$

$$\eta : x \longmapsto x^{b_{11}} y^{b_{21}}, \quad y \longmapsto y^{b_{12}} y^{b_{22}},$$

where a_{ij} and $b_{k\ell}$ are in $GF(3)$ for all i, j, k, ℓ. Then, ϕ maps σ and η thus:

$$\phi : \sigma \longmapsto A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad \eta \longmapsto B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

No we compute the images of x and y under $\sigma\eta$ where we're composing from right to left:

$$\begin{aligned} \sigma\eta(x) &= \sigma(x^{b_{11}} y^{b_{21}}) \\ &= \sigma(x)^{b_{11}} \sigma(y)^{b_{21}} \\ &= (x^{a_{11}} y^{a_{21}})^{b_{11}} (x^{a_{12}} y^{a_{22}})^{b_{21}} \\ &= x^{a_{11}b_{11} + a_{12}b_{21}} y^{a_{21}b_{11} + a_{22}b_{21}} \end{aligned}$$

$$\begin{aligned} \sigma\eta(y) &= \sigma(x^{b_{12}} y^{b_{22}}) \\ &= \sigma(x)^{b_{12}} \sigma(y)^{b_{22}} \\ &= (x^{a_{11}} y^{a_{21}})^{b_{12}} (x^{a_{12}} y^{a_{22}})^{b_{22}} \\ &= x^{a_{11}b_{12} + a_{12}b_{22}} y^{a_{21}b_{12} + a_{22}b_{22}} \end{aligned}$$

The image of $\sigma\eta$ under ϕ would then be a matrix with the first column having the exponents of x and y in $\sigma\eta(x)$ and the second column having the exponents of x and y in $\sigma\eta(y)$, like so:

$$\begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}$$

Notice that this is equal to AB. Thus, ϕ maps $\sigma\eta$ to $AB = \phi(\sigma)\phi(\eta)$ and thus is a homomorphism.

Thus, $G = C_3 \times C_3 \cong GL(2, 3)$. ◇

5.5 Order Ten Groups

Theorem 5.12. *The automorphism group $Aut(C_{10})$ is isomorphic to C_4.*

Proof. The group $C_{10} = \langle x \rangle$ has four elements of order ten and thus ten automorphisms. If we let σ map x to x^3, then

$$\sigma : x \longmapsto x^3,$$

$$\sigma^2 : x \longmapsto x^9,$$

$$\sigma^3 : x \longmapsto x^7,$$

$$\sigma^4 : x \longmapsto x.$$

Because σ is order four, the same as the number of automorphisms, the group $Aut(C_{10}) \cong C_4$. ◇

Theorem 5.13. *The automorphism group $Aut(D_{10})$ is isomorphic to F_{20}, the Frobenius group of order 20.*

Proof. See Example 2.12 in Chapter 2. ◇

5.6 S_4 and S_5

Theorem 5.14. *The automorphism group $Aut(S_4)$ is isomorphic to S_4.*

Proof. The center $Z(S_4)$ is trivial, so $S_4/Z(S_4) \cong S_4$ and by Theorem 2.17, we have that $Inn(S_4) \cong S_4$. Thus, it suffices to show that there are no more than 24 automorphisms of S_4.

Consider the set $S = \{(1,2,3),(1,4)\}$ consisting of a three-cycle and transposition which share only one letter. This generates a subgroup, whose order will be divisible by 4 and 3. Then, the order is divisible by 12, but $\langle S \rangle$ cannot be the alternating group A_4 as $(1,4)$ is an odd permutation. Thus, S generates the whole group S_4.

Consider the conjugate classes of S_4:

Conjugate Class	Permutation Type	Number of Elements
C_1	1 + 1 + 1 + 1	1
C_2	2 + 1 + 1	6
C_3	2 + 2	3
C_4	3 + 1	8
C_5	4	6

The only two classes whose elements have equal order are C_2 and C_3, but the number of elements in each class is different so these cannot be mapped to each other by an automorphism. Thus, each permutation type is mapped to another of the same type. Thus, our generating set S may only be mapped to another set containing a three-cycle and a transposition which only share one letter. For any three-cycle (a,b,c) in S_4, there are three transpositions which share only one letter with (a,b,c). These are (a,d), (b,d), and (c,d). Thus, since there are eight three-cycles in S_4, there are a total of 24 three-cycle, transposition pairs such that the cycles share only one letter. Thus, S has only 24 possible images under an automorphism.

Thus $|Aut(S_4)| \leq 24$, but $|Inn(S_4)| = 24$, so $Aut(S_4) = Inn(S_4)$. Thus, because $Inn(S_4) \cong S_4$, $Aut(S_4) \cong S_4$.

◇

Theorem 5.15. *The automorphism group $Aut(S_5)$ is isomorphic to S_5.*

Proof. The center $Z(S_5)$ is trivial, so $S_5/Z(S_5) \cong S_5$ and by Theorem 2.17, we have that $Inn(S_5) \cong S_5$. Thus, it suffices to show that there are no more than 120 automorphisms of S_5.

Consider the set $S = \{(1,2,3,4),(1,5)\}$ consisting of a four-cycle and transposition which share only one letter. This generates a subgroup, whose order will be divisible by 5 and 4. The order is also divisible by six as $(1,2,3,4)^2(1,5) = (1,3,5)(2,4)$. Then, the order is divisible by 60, but $\langle S \rangle$

cannot be the alternating group A_5 as $(1,5)$ is an odd permutation. Thus, S generates the whole group S_5.

Consider the conjugate classes of S_5:

Conjugate Class	Permutation Type	Number of Elements
C_1	1 + 1 + 1 + 1 + 1	1
C_2	1 + 1 + 1 + 2	10
C_3	2 + 2 + 1	15
C_4	3 + 1 + 1	20
C_5	4 + 1	30
C_6	3 + 28	20
C_7	5	24

The only two classes whose elements have equal order are C_2 and C_3, but the number of elements in each class is different so these cannot be mapped to each other by an automorphism. Thus, each permutation type is mapped to another of the same type. Thus, our generating set S may only be mapped to another set containing a four-cycle and a transposition which only share one letter. For any four-cycle (a,b,c,d) in S_5, there are four transpositions which share only one letter with (a,b,c,d). These are (a,e), (b,e), (c,e), and (d,e). Thus, since there are thirty four-cycles in S_5, there are a total of 120 four-cycle, transposition pairs such that the cycles share only one letter. Thus, S has only 120 possible images under an automorphism.

Thus $|Aut(S_5)| \leq 120$, but $|Inn(S_5)| = 120$, so $Aut(S_5) = Inn(S_5)$. Thus, because $Inn(S_5) \cong S_5$, $Aut(S_5) \cong S_5$. ◇

5.7 Cyclic Groups

Theorem 5.16. *The automorphism group $Aut(C_n)$ is isomorphic to $\mathbb{Z}_n^*$ for all n.*

Proof. Let $C_n = \langle x \rangle$ be a cyclic group of order n. This group is generated by x which has order n. An automorphism of C_n may only map x to those elements of equal order. These are any power of x which is relatively prime to n. That is for $\sigma \in Aut(C_n)$,

$$\sigma_i : x \longmapsto x^i, \quad \gcd(i,n) = 1.$$

Then, $|Aut(C_n)| = |\mathbb{Z}_n^*|$. Let $\phi : Aut(C_n) \to \mathbb{Z}_n^*$ be the following map:

$$\phi : \sigma_i \longmapsto i \in \mathbb{Z}_n^*, \text{ where } \sigma_i : x \longmapsto x^i.$$

This is clearly one-to-one, and thus onto given that the groups have equal order. It is also a homomorphism as $\sigma_i \circ \sigma_j$ maps x to x^{ij} and so ϕ maps $\sigma_i \circ \sigma_j$ to $ij = \phi(\sigma_i)\phi(\sigma_j)$.

Thus, $Aut(C_n) \cong \mathbb{Z}_n^*$. ◇

Corollary 5.17. *The group of automorphisms of a group of prime order p is isomorphic to the cyclic group of order $p-1$.*

Proof. This follows from the previous theorem and Theorem 1.20 which says that $\mathbb{Z}_p^*$ is cyclic where p is a prime. ◇

Theorem 5.18. *If H and K are group with* $\gcd(|H|, |K|) = 1$*, then*

$$Aut(H \times K) \cong Aut(H) \times Aut(K)$$

Proof. Let H and K be groups such that $\gcd(|H|, |K|) = 1$. Then, let σ_H, σ_K, and σ denote automorphisms of H, K, and $H \times K$ respectively. Let

$$\phi : Aut(H) \times Aut(K) \to Aut(H \times K)$$

be defined so that

$$\phi : (\sigma_H, \sigma_H) \longmapsto \sigma, \text{ where } \sigma(h, k) = (\sigma_H(h), \sigma_K(k)).$$

This map is clearly a one-to-one homomorphism as any automorphisms $\sigma_H \in Aut(H)$ and $\sigma_K \in Aut(K)$ together form an automorphism $\sigma = (\sigma_H, \sigma_K) \in Aut(H \times K)$. If we let η be in $Aut(H \times K)$ and let $\eta|_H$ and $\eta|_K$ denote the restrictions of η to the subsets (H, e_K) and (e_H, K) respectively, then these can be thought of as automorphisms of H and K. Let $\eta_H \in Aut(H)$ be such that $(\eta_H(h), e_K) = \eta|_H(h, e_K)$. Define $\eta_K \in Aut(K)$ similarly with respect to $\eta|_K$. Then,

$$\phi : (\eta_H, \eta_K) \longmapsto \eta.$$

Therefore our mapping is also onto and is thus an isomorphism.

◇

Corollary 5.19. *Let G be an abelian group of order n where $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ where p_1, p_2, ..., p_k are distinct primes. Let P_1, P_2, ..., P_k be the Sylow p-subgroups associated with each prime factor. Then,*

$$Aut(G) \cong Aut(P_1) \times Aut(P_2) \times \cdots \times Aut(P_k)$$

Proof. This is a direct result of the previous theorem together with Theorem 4.11. ◇

Lemma 5.20. *Let p be an odd prime and $k \geq 1$. Then, if x is an integer such that $x \equiv 1 \pmod{p^k}$ but $x \not\equiv 1 \pmod{p^{k+1}}$, then*

$$x^p \equiv 1 \pmod{p^{k+1}} \text{ and } x^p \not\equiv 1 \pmod{p^{k+2}}.$$

The same result holds if $p = 2$ and $k \geq 2$.

Proof. Let $x = 1 + tp^k$ where p does not divide t. Then $x \equiv \pmod{p^k}$ and $x \not\equiv \pmod{p^{k+1}}$. Then,

$$\begin{aligned} x^p &= (1 + tp^k)^p \\ &= 1 + \binom{p}{1} tp^k + \binom{p}{2} (tp^k)^2 + \cdots + \binom{p}{p-1} (tp^k)^{p-1} + (tp^k)^p \\ &\equiv 1 \pmod{p^{k+1}}. \end{aligned}$$

All terms in the above expansion are divisible by p^{k+2} except for the first two, so $x^p \equiv 1 + \binom{p}{1} tp^k \pmod{p^{k+2}}$. Because p does not divide t, p^{k+2} does not divide $\binom{p}{1} tp^k$, so $x^p \not\equiv 1 \pmod{p^{k+2}}$.
If $p = 2$ and $k \geq 2$, then we can write $x = 1 + t2^k$ so then $x^2 = 1 + t2^{k+1} + t^2 2^{2k}$. Thus $x \equiv 1 \pmod{2^k}$ and $x \not\equiv 1 \pmod{2^{k+1}}$. We restrict k to being greater than 2 as $3 \equiv 1 \pmod{2}$ and $3 \not\equiv 1 \pmod{2^2}$, but $3^2 \equiv 1 \pmod{2^3}$. ◇

Theorem 5.21. *Let $p > 2$ be a prime. Then, $Aut(C_{p^n}) \cong C_{p^{n-1}(p-1)}$.*

Proof. We've shown before that for any m, $Aut(C_m) \cong \mathbb{Z}_m^*$, so what we need to show here is that $\mathbb{Z}_{p^n}^*$ is cyclic.

Let p be an odd prime and $n > 1$. Let $\phi : \mathbb{Z}_{p^n}^* \to \mathbb{Z}_p^*$ be defined so that $x \longmapsto x \pmod{p}$. This is clearly an onto homomorphism. As such, for each $x \in \mathbb{Z}_{p^n}^*$, Order($\phi(x)$) will divide Order(x). Because we know $\mathbb{Z}_p^*$ to be cyclic of order $p-1$, there is some element y in $\mathbb{Z}_p^*$ which has order $p-1$. Let $x \in \mathbb{Z}_{p^n}^*$ so that $\phi(x) = y$. Then, the order of x will be some $m = k(p-1)$ and so Order(x^k) $= p-1$.

Now, let $z = p+1$. Then, $z \equiv 1 \pmod{p}$ and $z \not\equiv 1 \pmod{p^2}$. By applying the previous lemma repeatedly, we can conclude that $z^{p^{n-1}} \equiv 1 \pmod{p^n}$ and $z^{p^{n-2}} \not\equiv 1 \pmod{p^n}$, so Order($z$) $= p^{n-1}$. Because $\mathbb{Z}_{p^n}^*$ is abelian, and $\gcd(p^{n-1}, p-1) = 1$, Order($x^k z$) $= p^{n-1}(p-1)$, which is the order of the group. Therefore $\mathbb{Z}_{p^n}^* \cong C_{p^{n-1}(p-1)}$.

◇

Theorem 5.22. *Let $n \geq 3$. Then, $Aut(C_{2^n}) \cong C_{2^{n-2}} \times C_2$.*

Proof. Similar to the last proof, because we know $Aut(C_{2^n}) \cong \mathbb{Z}_{2^n}$, we need to show that $\mathbb{Z}_{2^n} \cong C_{2^{n-2}} \times C_2$ for $n > 2$.

We shall show that for any $n > 2$, $\mathbb{Z}_{2^n}$ can be generated by 5 and -1. Notice that $5 \equiv 1 \pmod{2^2}$ and $5 \not\equiv 1 \pmod{2^3}$, so by our lemma, $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ and $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$, so 5 has order 2^{n-2}. Because for any k, $5^k \equiv 1 \pmod{4}$ and $-1 \equiv 3 \pmod{4}$, $-1 \notin \langle 5 \rangle$. Therefore $\langle 5 \rangle \times \langle -1 \rangle$ is a subgroup of $\mathbb{Z}_{2^n}$ which has order $2^{n-2} \times 2$, which is the order of the group. Therefore

$$\mathbb{Z}_{2^n} \cong \langle 5 \rangle \times \langle -1 \rangle \cong C_{2^{n-2}} \times C_2.$$

◇

Theorem 5.23. *Let C_n be a cyclic group of order n for some $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ where p_1, p_2, ..., p_k are distinct primes. Then,*

$$Aut(C_n) \cong Aut(C_{p_1^{m_1}}) \times Aut(C_{p_2^{m_2}}) \times \cdots \times Aut(C_{p_k^{m_k}}).$$

Proof. Because C_n is an abelian group of order n, by Corollary 5.19 we have

$$Aut(C_n) = Aut(P_1) \times Aut(P_2) \times \cdots \times Aut(P_k)$$

where P_i, $1 \leq i \leq k$, is the Sylow p_i subgroup of C_n. Because C_n is cyclic, each of its Sylow subgroups is cyclic, by Theorem 1.18. Thus,

$$Aut(C_n) \cong Aut(C_{p_1^{m_1}}) \times Aut(C_{p_2^{m_2}}) \times \cdots \times Aut(C_{p_k^{m_k}}).$$

◇

Chapter 6

A Class-Preserving Outer Automorphism

It is clear that inner automorphisms will preserve the conjugate classes of a group. That is, each conjugate class remains invariant under an inner automorphism. The question naturally arises if there exist outer automorphisms which do the same. This has been answered in the affirmative by Burnside [1], who gave an example of a group of order 729, which has a class-preserving outer automorphism.

In this chapter, we give a description of an example of a group having a class-preserving outer automorphism; that is, an automorphism which fixes each conjugate class, but which is not inner. This example is due to G.E. Wall, [9], who cites William Burnside with the original construction of such groups. This example is also discussed by Huppert [5, p. 22] but without much detail.

6.1 A Subgroup G of $GL(2, \mathbb{Z}_8)$ of Order 32

Consider $GL(2, \mathbb{Z}_8)$, the group of invertible 2×2 matrices with entries from the commutative ring $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. This group has order 1536. If the following matrix A is in $GL(2, \mathbb{Z}_8)$,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then $ad - bc$ must be equivalent to 1, 3, 5, or 7 in $\mathbb{Z}_8$. Thus, if ad is even, bc must be even and vice versa. Thus there are $2 \times 48 \times 16$ different choices for a, b, c, and d so that A is invertible.

This group has a subgroup of order 32 for which we will define an outer automorphism which preserves its conjugate classes. Let G be the subgroup of $GL(2, \mathbb{Z}_8)$ consisting elements of the form

$$\begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix}$$

where $x \in \mathbb{Z}_8$ and $y \in \{1, 3, 5, 7\}$, the group of units in $\mathbb{Z}_8$. Clearly, G has order 32. Let A, B, and C be the following:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 5 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 \\ 0 & 7 \end{bmatrix}$$

Then,

$$G = \langle A, B, C \rangle = \{A^i B^j C^k, \ 0 \leq i \leq 7, \ 0 \leq \ j, k \leq 1\}.$$

We show that this is a group under matrix multiplication where each entry is reduced modulo 8. As $G \subset GL(2, \mathbb{Z}_8)$, we need only show it is closed under the operation of matrix multiplication mod 8. To show this, let $a, b, c, d \in \mathbb{Z}_8$ where $b, d \in \{1, 3, 5, 7\}$ so that we have the following elements in G:

$$X = \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix}$$

Then,

$$XY = \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix}\begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} 1 & a+bc \\ 0 & bd \end{bmatrix}$$

Because $\mathbb{Z}_8$ is itself closed under multiplication and addition modulo 8, $a+bc \in \mathbb{Z}_8$ and further, $bd \in \{1,3,5,7\}$, so $XY \in G$.
The generators A, B, and C, of G satisfy the following relations:

$$A^8 = B^8 = C^2 = I, \quad A^4 = B^4, \quad A^6 = B^2, \quad B^{-1}AB = A^5,$$

$$C^{-1}AC = A^7, \quad C^{-1}BC = A^2B, \quad B^{-1}CB = A^2C.$$

We will work with a permutation representation of this group and show the class-preserving outer automorphism in the next section.

6.2 Permutation Representation of G

To find a permutation representation of this group, we find an appropriate subgroup and determine the representation of G on the set of its right cosets.

Choose the subgroup H to be the Klein-Four subgroup:

$$H = \{I,\ A^7B,\ A^3C,\ A^6BC\}.$$

Then, H has eight right cosets, which are

$$\begin{aligned} HI &= \{\{I,\ A^7B,\ A^3C,\ A^6BC\} & HA &= \{A, A^4B, A^2C, ABC\} \\ HA^2 &= \{A^2, AB, AC, A^4BC\} & HA^3 &= \{A^3, A^6B, C, A^7BC\} \\ HA^4 &= \{A^4, A^3, A^7C, A^2BC\} & HA^5 &= \{A^5, B, A^6C, A^5BC\} \\ HA^6 &= \{A^6, A^5B, A^5C, BC\} & HA^7 &= \{A^7, A^2B, A^4C, A^3BC\} \end{aligned}$$

Then, we identify each coset with the numbers 1 through 8 as follows:

$$\begin{aligned} 1 &\longmapsto HI &&= \{\{I,\ A^7B,\ A^3C,\ A^6BC\} \\ 2 &\longmapsto HA &&= \{A, A^4B, A^2C, ABC\} \\ 3 &\longmapsto HA^2 &&= \{A^2, AB, AC, A^4BC\} \\ 4 &\longmapsto HA^3 &&= \{A^3, A^6B, C, A^7BC\} \\ 5 &\longmapsto HA^4 &&= \{A^4, A^3, A^7C, A^2BC\} \\ 6 &\longmapsto HA^5 &&= \{A^5, B, A^6C, A^5BC\} \\ 7 &\longmapsto HA^6 &&= \{A^6, A^5B, A^5C, BC\} \\ 8 &\longmapsto HA^7 &&= \{A^7, A^2B, A^4C, A^3BC\} \end{aligned}$$

Because our aim is to construct a permutation group isomorphic to G, we need only find the permutations associated with our generators A, B, and C. We find these via the right representation:

$$A \longrightarrow \begin{pmatrix} HI & HA & HA^2 & HA^3 & HA^4 & HA^5 & HA^6 & HA^7 \\ HA & HA^2 & HA^3 & HA^4 & HA^5 & HA^6 & HA^7 & HI \end{pmatrix}$$

$$\longrightarrow (1,2,3,4,5,6,7,8)$$

$$B \longrightarrow \begin{pmatrix} HI & HA & HA^2 & HA^3 & HA^4 & HA^5 & HA^6 & HA^7 \\ HB & HAB & HA^2B & HA^3B & HA^4B & HA^5B & HA^6B & HA^7B \end{pmatrix}$$
$$\longrightarrow (1,6,7,4,5,2,3,8)$$

$$C \longrightarrow \begin{pmatrix} HI & HA & HA^2 & HA^3 & HA^4 & HA^5 & HA^6 & HA^7 \\ HC & HAC & HA^2C & HA^3C & HA^4C & HA^5C & HA^6C & HA^7C \end{pmatrix}$$
$$\longrightarrow (1,4)(2,3)(5,8)(6,7)$$

Then, let a, b, and c be these permutations in S_8.

$$a = (1,2,3,4,5,6,7,8),\ b = (1,6,7,4,5,2,3,8),\ c = (1,8)(2,7)(3,6)(4,5)$$

Then, $\langle a, b, c\rangle$ is isomorphic to G as a, b, and c satisfy the following relations:

$$a^8 = b^8 = c^2 = \varepsilon,\quad a^4 = b^4,\quad a^6 = b^2,\quad b^{-1}ab = a^5,$$
$$c^{-1}ac = a^7,\quad c^{-1}bc = a^2b,\quad b^{-1}cb = a^2c.$$

Note that the above relations still hold if we replace b with b^5.

- The center of the group is $Z(G) = \langle a^4\rangle = \{\epsilon, a^4\}$. This can be seen from the following:

$$ba^4 = a^{5\cdot4}b = a^4b \implies a^4 \in C_G(b)$$

$$ca^4 = a^{7\cdot4}c = a^4c \implies a^4 \in C_G(c)$$

$$ca^2 = a^{7\cdot2}c = a^6c \implies a^2 \notin C_G(c)$$

$$cb = a^2bc \implies c \notin C_G(b) \text{ and } b \notin C_G(c)$$

  Thus, as a^4 is common to the centralizers of b and c, but a^2 is not in the centralizer of c, the only common element in the centralizers of the three generators is a^4.

- The commutator subgroup is $G' = \langle a^2\rangle = \{\epsilon, a^2, a^4, a^6\}$. To show this is the case, let $H = \langle a^2\rangle = \{\epsilon, a^2, a^4, a^6\}$. Then $G/H = \langle Ha, Hb, Hc\rangle$ and all we need show is that these generator elements commute. Observe the following:

$$\begin{aligned} & ba = a^5b \\ \implies & a^6ba = ab \\ \implies & ba \in Hab \\ \implies & Hba = Hab \end{aligned}$$

$$\begin{aligned} & ca = a^7c \\ \implies & a^2ca = ac \\ \implies & ca \in Hac \\ \implies & cb = a^2bc \\ \implies & cb \in Hbc \\ \implies & Hcb = Hbc \end{aligned}$$

Thus, Ha, Hb, and Hc commute and we have that G/H is abelian. By Lemma 1.39, we have that $G' \subseteq H$. Since $b^{-1}c^{-1}bc = b^{-1}a^2b = a^2$, $a^2 \in G'$ and $G' = H = \langle a^2 \rangle$. Thus,

$$G = H\epsilon \cup Ha \cup Hb \cup Hab \cup Hc \cup Hac \cup Hbc \cup Habc$$

6.3 A Class-Preserving Outer Automorphism of G

Now, we describe an automorphism of G which preserves its conjugate classes. First, the following table gives the conjugate classes of G.

Class	Class Rep.	Centralizer	Class Elements	# Elements	Order
C_1	ϵ	G	ϵ	1	1
C_2	a^4	G	a^4	1	2
C_3	a^2	$\langle a, b \rangle$	a^2, a^6	2	4
C_4	a	$\langle a \rangle$	a, a^3, a^5, a^7	4	8
C_5	b	$\langle a^2, b \rangle$	b, a^2b, a^4b, a^6b	4	8
C_6	ab	$\langle ab \rangle \times \langle a^2 \rangle$	ab, a^5b	2	4
C_7	a^3b	$\langle a^3b \rangle \times \langle a^2 \rangle \times \langle bc \rangle$	a^3b, a^7b	2	2
C_8	c	$\langle ab \rangle \times \langle c \rangle$	c, a^2c, a^4c, a^6c	4	2
C_9	ac	$\langle ac \rangle \times \langle a^4 \rangle \times \langle bc \rangle$	ac, a^3c, a^5c, a^7c	4	2
C_{10}	bc	$\langle bc \rangle \times \langle a^4 \rangle \times \langle a^3b \rangle$	bc, a^2bc, a^4bc, a^6bc	4	2
C_{11}	abc	$\langle abc \rangle \times \langle a^4 \rangle \times \langle c \rangle$	abc, a^3bc, a^5bc, a^7bc	4	4

Let σ be the following automorphism:

$$\sigma: \quad a \longrightarrow a, \quad c \longrightarrow c, \quad b \longrightarrow b^5 = a^4b$$

We claim this is an outer automorphism. Because $\{a, b^5 = a^4b, c\}$ is an alternative generating set of G and the restriction of σ to a, b, and c is one-to-one, onto, and structure-preserving, this constitutes an automorphism of G. It is an outer automorphism because if it were not, then there would be some $g \in G$ such that σ is the inner automorphism induced by g. Given that σ fixes a and c, $g \in C_G(a) \cap C_G(c)$. However, $C_G(a) \cap C_G(c) = Z(G) = \{\epsilon, a^4\}$, and so σ would be the trivial automorphism. Therefore, σ must be an outer automorphism.

From the class table above, it can be clearly seen that this mapping preserves the conjugate classes of G. As an illustration, the following table gives the explicit mappings of five of the classes, with respect to the order of elements listed. The classes only containing elements in terms of a and c will clearly be preserved as our map fixes them. As such, we only give classes C_5, C_6, C_7, C_{10}, and

C_{11}, which contain elements in terms of b.

Class	Representative	Elements as Listed Above	Respective Mappings
C_5	b	b, a^2b, a^4b, a^6b	a^4b, a^6b, b, a^2b
C_6	ab	ab, a^5b	a^5b, ab
C_7	a^3b	a^3b, a^7b	a^7b, a^3b
C_{10}	bc	bc, a^2bc, a^4bc, a^6bc	a^4bc, a^6bc, bc, a^2bc
C_{11}	abc	abc, a^3bc, a^5bc, a^7bc	a^5bc, a^7bc, abc, a^3bc

Chapter 7

Outer Automorphisms of S_6

This chapter will be devoted to the automorphism groups of symmetric groups, giving particular focus to S_6, the only symmetric group which has an outer automorphism. First we will discuss the automorphisms of symmetric groups S_n for $n \neq 6$ and some properties thereof, culminating in the well-known theorem that for $n \neq 2, 6$, $S_n \cong Aut(S_n)$. Then, we will begin our construction of the outer automorphism of S_6.

Note: Throughout, we will multiply permutations from left to right. Although this is not always the convention, because of how we write permutations, we prefer this over the alternative.

7.1 Automorphisms of the Symmetric Groups

Irving Segal [8] proved that $S_n \cong Aut(S_n)$, $n \neq 2, 6$, in a one-page paper in 1940, and it is his proof which inspires our proof. However, concise as his is, we seek to put forth a modified proof. We begin with a lemma.

Lemma 7.1. *Let S_n be the symmetric group on n letters. Then the number of permutations in S_n of the type $1^{r_1} \cdot 2^{r_2} \cdots n^{r_n}$ is given by*

$$\frac{n!}{1^{r_1} \cdot r_1! \cdot 2^{r_2} \cdot r_2! \cdot 3^{r_3} \cdot r_3! \cdots n^{r_n} \cdot r_n!}.$$

The proof of the following theorem will use this lemma in a combinatorial argument as to why automorphisms must map transpositions to transpositions except in the special case of $n = 6$.

Theorem 7.2. *Let $n > 1$ and $n \neq 6$. If $\sigma \in Aut(S_n)$ and $x \in S_n$ is a transposition, then then $\sigma(x)$ is a transposition.*

Proof. Because σ is an automorphism, $\sigma(x)$ must be of order two. Thus we can write

$$\sigma(x) = \tau_1 \tau_2 \cdots \tau_k$$

for some $k \geq 1$, where τ_i are *disjoint* transpositions. Thus, x is of the type $2^1 \cdot 1^{n-2}$ and $\sigma(x)$ is of the type $2^k \cdot 1^{n-2k}$.

By Lemma 2.13 we know that given a conjugate class C_i of S_n, $\sigma(C_i)$ will be a conjugate class as well. Further, C_i and $\sigma(C_i)$ must have the same number of elements. In S_n, conjugate classes are made up of elements of the same type. That is, the transpositions are in a unique conjugate class, as are the 3-cycles, etc. Let C and C' be the conjugate classes of x and $\sigma(x)$ respectively. These two must have the same number of elements in them and given that conjugate classes in S_n are made up of elements of the same permutation type, we make use of Lemma 7.1 and have the

following equation:

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

which simplifies to

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

We will show that apart from $n = 6$ and $k = 3$, no positive integer values for n and k make the above equation hold. First, we will rewrite the above equation in the following way:

$$\frac{n(n-1)}{2} = \frac{n!}{(n-2k)!\cdot 2^k\cdot k!} \tag{7.1}$$

$$\implies \quad \frac{n(n-1)}{2} = \frac{1}{2^k\cdot k!}n(n-1)\cdots(n-2k+1) \tag{7.2}$$

$$\implies \quad \frac{1}{2} = \frac{1}{2^k\cdot k!}(n-2)(n-3)\cdots(n-2k+1) \tag{7.3}$$

$$\implies \quad 2^{k-1}k! = (n-2)(n-3)\cdots(n-2k+1) \tag{7.4}$$

First, we show that $k \neq 2$. Letting $k = 2$ in (7.4), we have $4 = 2\cdot 2! = (n-2)(n-3) = n^2 - 5n + 6$. However, there is no integer solution to $4 = n^2 - 5n + 6$.
We now show by induction that $k \geq 4$ is impossible. First note that as k is the number of disjoint transpositions in the cycle-decomposition of $\sigma(x)$, $n \geq 2k$. Then,

$$2^{k-1}k! = (n-2)(n-3)\cdots(n-2k+1) \geq (2k-2)(2k-3)\cdots(1) = (2k-2)! \tag{7.5}$$

We show that (7.5) does not hold when $k = 4$. The right sides gives us $(2(4)-2)! = 6! = 720$ while the left yields $4!\cdot 2^{4-1} = 24\cdot 8 = 192$ and so for $k = 4$, $2^{k-1}k! < (2k-2)!$.
To show that $k > 4$ is also impossible, suppose k is such that $2^{k-1}k! < (2k-2)!$ and consider $k+1$.

$$\begin{aligned}[2(k+1)-2]! = (2k)! &= (2k)(2k-1)\cdot(2k-2)! \\ &> 2k(2k-1)k!2^{k-1} \\ &= k(2k-1)k!2^k \\ &> (k+1)k!2^k = (k+1)!2^k\end{aligned}$$

Thus, $2^{k-1}k! < (2k-2)!$ for all $k \geq 4$.
The only k which we have not excluded is $k = 3$ which we've previously stated will work for $n = 6$ as can be seen by substituting 3 for k in the right side of (7.4):

$$\begin{aligned}(n-2)(n-3)\cdots(n-2(3)+1) = (n-2)(n-3)(n-4)(n-5) &= 3!\cdot 2^{3-1} \\ &= 6\cdot 4 = 24\end{aligned}$$

If $1 < n < 6$, then $(n-2)(n-3)(n-4)(n-5) \leq 0$ and if $n > 6$, then $(n-2)(n-3)(n-4)(n-5) > 4! = 24$. Therefore, for $n > 1$ $n \neq 6$, $\sigma(x)$ is a transposition. ◇

Lemma 7.3. *Let $n \geq 4$, and A_i, $1 \leq i \leq n-1$ be distinct sets of two elements such that $|A_i \cap A_j| = 1$ for all $i \neq j$. Then,*

$$\left|\bigcap_{i=1}^{n} A_i\right| = 1$$

Proof. Let $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$. Arbitrarily define $A_1 = \{a, b\}$. Let $\mathcal{X} \subseteq \mathcal{A}$ be such that for all $A_i \in \mathcal{X}$, $A_1 \cap A_i = \{a\}$, and $\mathcal{Y} \subseteq \mathcal{A}$ be such that for all $A_j \in \mathcal{Y}$, $A_1 \cap A_j = \{b\}$. We will show that

one of these subsets must be empty. Clearly we have that $\mathcal{A} = \mathcal{X} \cup \mathcal{Y} \cup \{a, b\}$ and $\mathcal{X} \cap \mathcal{Y} = \emptyset$.

There are at least four sets in $\mathcal{A}$, so let A_i, A_j, and A_k be in $\mathcal{A}$. At least two of these must be in either $\mathcal{X}$ or $\mathcal{Y}$. Without loss of generality, let A_i and A_j be in $\mathcal{X}$. We will show that A_k must be in $\mathcal{X}$ also.
We have $A_1 \cap A_i = A_1 \cap A_j = \{a\}$ so let $A_i = \{a, c\}$ and $A_j = \{a, d\}$. The set A_k must overlap A_1, A_i, and A_j in exactly one letter, so if it does not contain a, it must contain b, c, and d, which is impossible since it is a two-point set. Therefore $A_k \in \mathcal{X}$. For the same reason, any other set in $\mathcal{A}$ must be in $\mathcal{X}$ as not containing the letter a while still overlapping each other set in exactly one letter would require the set to have more than two elements. Therefore $\mathcal{Y} = \emptyset$ and $\left|\bigcap_{i=1}^{n} A_i\right| = 1$.

◇

Theorem 7.4. *Let $\sigma \in Aut(S_n)$ such that, for all transpositions $x \in S_n$, $\sigma(x)$ is a transposition. Then, σ is an inner automorphism.*

Proof. We know already from Chapter 5 that $Aut(S_3) \cong S_3$, $Aut(S_4) \cong S_4$, and $Aut(S_5) \cong S_5$. Further, these groups, having trivial centers, are isomorphic to their inner automorphism groups. Thus, we know already that for $n = 3, 4, 5$, all automorphisms are inner automorphisms. The same is obviously true for S_2 whose only automorphism is the trivial one.

Then, let $n > 4$ and $A = \{(1, 2), (1, 3), ..., (1, n)\}$. This set generates the group; that is, $S_n = \langle A \rangle$. Then an automorphism σ which sends transpositions to transpositions will send A to another set of transpositions who generate the group.

Because for any $a, b \in \{2, 3, ..., n\}$, $(1, a)(1, b) = (1, a, b)$, we have that any two of the elements of A yield a three-cycle when multiplied. Thus, $\sigma((1, a))$ and $\sigma((1, b))$ must also yield an order three element when multiplied. This is only possible if $\sigma((1, a))$ and $\sigma((1, b))$ overlap in one letter.

Thus, we have that $\sigma(A)$ consists of $n - 1$ transpositions, each pair of which overlaps in exactly one letter. Lemma 7.3 gives us that all of the transpositions in $\sigma(A)$ must overlap in exactly one letter. Therefore, we have that σ maps the elements of A thus:

$$\begin{aligned} \sigma : (1, 2) &\longmapsto (a_1, a_2) \\ (1, 3) &\longmapsto (a_1, a_3) \\ &\cdots \\ (1, n) &\longmapsto (a_1, a_n) \end{aligned}$$

Let $\eta \in S_n$ be defined

$$\eta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}.$$

Then, $\sigma(x) = \eta^{-1} x \eta$ for $x \in S_n$, and $\sigma \in Inn(S_n)$. (Note that we are multiplying permutations from left to right.) ◇

Corollary 7.5. *The group of automorphisms of the symmetric group S_n is isomorphic to S_n for all $n \neq 2, 6$.*

Proof. For $n > 2$, the symmetric group S_n has a trivial center, so $S_n \cong S_n/Z(S_n)$. By Theorem 2.17, $S_n/Z(S_n) \cong Inn(S_n)$, so $S_n \cong Inn(S_n)$ for all $n > 2$. By Theorem 7.2, all automorphisms of S_n map transpositions to transpositions for $n \neq 6$. By Theorem 7.4, all automorphisms which map transpositions to transpositions are inner automorphisms. Therefore, for $n \neq 6$, $Inn(S_n) = Aut(S_n)$. Therefore, $S_n \cong Aut(S_n)$. ◇

7.2 The Automorphisms of S_6

In the previous section we discussed how the automorphism group of the symmetric group on n letters is isomorphic to the symmetric group on n letters when $n \neq 2, 6$. The case of $n = 2$ is trivial. Now, we discuss the automorphisms of the symmetric group on six letters. Unlike the other symmetric groups, the automorphism group of S_6 contains outer automorphisms.

Recall that in Theorem 7.2 we gave a combinatorial argument for why automorphisms of the symmetric groups other than S_6 had to send transpositions to transpositions. Our discussion of the automorphisms of S_6 will show how there is an automorphism thereof which does not send transpositions to transpositions and therefore is not inner. Much of this discussion is inspired by Janusz and Rotman [6].

First, we prove some things about some subgroups of S_6 which will be helpful later on.

7.2.1 Subgroups of S_6

Lemma 7.6. *The only normal subgroups of S_6 are $\{\varepsilon\}$, A_6, and S_6.*

Proof. The subgroups $\{\varepsilon\}$, A_6, and S_6 are obviously normal. We will show that no other normal subgroup is possible. Consider the conjugate classes of S_6:

Class	Order	Partition Type	Number of Elements
C_1	1	1 + 1 + 1 + 1 + 1 + 1	1
C_2	2	2 + 1 + 1 + 1 + 1	15
C_3	2	2 + 2 + 1 + 1	45
C_4	2	2 + 2 + 2	15
C_5	3	3 + 1 + 1 + 1	40
C_6	3	3 + 3	40
C_7	4	4 + 1 + 1	90
C_8	4	4 + 2	90
C_9	5	5 + 1	144
C_{10}	6	3 + 2	120
C_{11}	6	6	120

Any normal subgroup of S_6 will be the union of some conjugate classes thereof, always including C_1. The divisors of 720 are:

1	2	3	4	5
6	8	9	10	12
15	16	18	20	24
30	36	40	45	48
60	72	80	90	120
144	180	240	360	720

Notice that because the smallest non-trivial conjugate class has 15 elements, any union of them must be of order greater than 15. $C_1 \cup C_2$ and $C_1 \cup C_4$ each have 16 elements which divides 720, but these are not subgroups. After that, any union of conjugate classes will have number of elements equivalent to $0 \pmod{10}$, $1 \pmod{10}$, $5 \pmod{10}$, or $6 \pmod{10}$. The union that has number of elements equivalent to $0 \pmod{10}$ and is divisible by 720 is the union which results in A_6. Other than that, 720 has no divisors greater than 16 which end in a 1, 5, or a 6 aside from 36 and 45 and it is easy to see that no union of conjugate classes which includes C_1 can have 36 or 45 elements.

Thus S_6 can have no other normal subgroups besides $\{\varepsilon\}$, A_6, and S_6. ◇

Lemma 7.7. *The alternating group on six letters has no non-trivial proper normal subgroups.*

Proof. Consider the conjugate classes of A_6:

Class	Order	Partition Type	Number of Elements
C_1	1	1 + 1 + 1 + 1 + 1 + 1	1
C_2	2	2 + 2 + 1 + 1	45
C_3	3	3 + 1 + 1 + 1	40
C_4	3	3 + 3	40
C_5	4	4 + 2	90
C_6	5	5 + 1	72
C_7	5	5 + 1	72

A normal subgroup must be some union of conjugate classes, but it can be easily seen, by process similar to that of the proof of the previous lemma, that no union of these classes will have order divisible by 360, except for C_1 and $\bigcup_{i=1}^{7} C_i$. ◇

Remark: These proofs can be somewhat simplified by the observation that a proper normal subgroup of A_6 or S_6 is transitive.

Theorem 7.8. *The subgroup H of S_6, which has order* 120 *must equal its own normalizer.*

Proof. Let k be the number of conjugates of H in S_6. Then $k \leq 6$. We will show that $k = 6$.
Let $\{H = H_1, H_2, \ldots, H_k\}$ be the set of conjugates of H in S_6. Let $\rho : S_6 \to Sym(H_1, H_2, \ldots, H_k)$ be defined so that

$$x \longmapsto \begin{pmatrix} H_1 & H_2 & \cdots & H_k \\ x^{-1}H_1x & x^{-1}H_2x & \cdots & x^{-1}H_kx \end{pmatrix}.$$

The kernel $\ker\rho$ is equal to the intersection of the normalizers of the H_is, so $\ker\rho = \bigcap_{i=1}^{k} N_{S_6}(H_i)$. Further $\ker\rho$ is a normal subgroup of S_6. The only normal subgroups of S_6 are $\{\varepsilon\}$, A_6, and S_6 itself.

- If $\ker\rho = \{\varepsilon\}$ then by the First Isomorphism Theorem, $S_6/\ker\rho \cong S_6 \cong \rho(S_6)$.Then S_6 is isomorphic to a subgroup of $Sym(H_1, H_1, \ldots, H_k)$. This is only possible is $k = 6$.
- If $\ker\rho = A_6$, then for some i, $1 \leq i \leq k$, $N_{S_6}(H_i) = A_6$, which means that H_i is a normal subgroup of A_6. This is not possible by the previous lemma.
- If $\ker\rho = S_6$, then each H_i is normal and so there is only one H_i, namely H_1. This is impossible as S_6 has no order 120 normal subgroups.

Thus, the only option is that $k = 6$ and so $N_{S_6}(H)$ is of index six, and thus of order 120, and thus is equal to H. ◇

7.2.2 Transitive Representation of S_5 on Six Letters

Let $G = S_5$ be the symmetric group on five letters. The group G has six Sylow 5-subgroups, which we'll denote P_i for $1 \leq i \leq 6$. Then let $\Omega = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Let these subgroups be:

$$
\begin{aligned}
P_1 &= \langle\,(1,2,3,4,5)\,\rangle &&= \{\epsilon,\ (1,2,3,4,5),\ (1,3,5,2,4),\ (1,4,2,5,3),\ (1,5,4,3,2)\}\\
P_2 &= \langle\,(1,2,3,5,4)\,\rangle &&= \{\epsilon,\ (1,2,3,5,4),\ (1,3,4,2,5),\ (1,5,2,4,3),\ (1,4,5,3,2)\}\\
P_3 &= \langle\,(1,2,4,3,5)\,\rangle &&= \{\epsilon,\ (1,2,4,3,5),\ (1,4,5,2,3),\ (1,3,2,5,4),\ (1,5,3,4,2)\}\\
P_4 &= \langle\,(1,2,4,5,3)\,\rangle &&= \{\epsilon,\ (1,2,4,5,3),\ (1,4,3,2,5),\ (1,5,2,3,4),\ (1,3,5,4,2)\}\\
P_5 &= \langle\,(1,2,5,3,4)\,\rangle &&= \{\epsilon,\ (1,2,5,3,4),\ (1,5,4,2,3),\ (1,3,2,4,5),\ (1,4,3,5,2)\}\\
P_6 &= \langle\,(1,2,5,4,3)\,\rangle &&= \{\epsilon,\ (1,2,5,4,3),\ (1,5,3,2,4),\ (1,4,2,3,5),\ (1,3,4,5,2)\}
\end{aligned}
$$

Define the map $\sigma : G \to Sym(\Omega)$ such that

$$
x \longrightarrow \begin{pmatrix} P_i \\ x^{-1}P_ix \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 \\ x^{-1}P_1x & x^{-1}P_2x & x^{-1}P_3x & x^{-1}P_4x & x^{-1}P_5x & x^{-1}P_6x \end{pmatrix}
$$

This yields a transitive subgroup of $Sym(\Omega)$ as $\sigma((1,2)(3,4,5)) = (P_1, P_2, P_5, P_6, P_4, P_3)$.

Because there are six conjugates, each P_i has an order 20 normalizer and these contain no transpositions. For example, $N_G(P_1) = \langle(1,2,3,4,5), (2,3,5,4)\rangle$. Observe then that σ cannot send a transposition to a transposition. This is because in order to yield a permutation of the P_is which only transposes two of them, the elements being operated on by σ would necessarily normalize the other four. Thus, for a transposition $x \in S_5$, $\sigma(x)$ must be the disjoint product of three transpositions as this is the only order two option which fixes no P_i.

7.2.3 Outer Automorphisms of S_6

If we identify each permutation of the P_is with their index, this map σ yields a transitive subgroup of S_6 of order 120 which is isomorphic to S_5. Call this subgroup H.

In S_6, H is its own normalizer and has six conjugates, by Theorem 7.8. Call these $H = H_1$, H_2, H_3, H_4, H_5, and H_6. Consider the mapping $\phi : S_6 \longrightarrow Sym(H_1, H_2, H_3, H_4, H_5, H_6)$ given by

$$
g \longmapsto \begin{pmatrix} H_i \\ g^{-1}H_ig \end{pmatrix} = \begin{pmatrix} H_1 & H_2 & H_3 & H_4 & H_5 & H_6 \\ g^{-1}H_1g & g^{-1}H_2g & g^{-1}H_3g & g^{-1}H_4g & g^{-1}H_5g & g^{-1}H_6g \end{pmatrix}
$$

The mapping ϕ is clearly a homomorphism. In the proof of Theorem 7.8 we showed that $\bigcap_{i=1}^{6} N_{S_6}(H_i)$ is trivial. Therefore ϕ must be one-to-one, and hence onto, as $Sym(H_1, H_2, H_3, H_4, H_5, H_6)$ has order equal to S_6. Thus ϕ is an isomorphism and can be thought of as an automorphism of S_6 if we identify each H_i with its subscript.

To show that $\phi \notin Inn(S_6)$, consider a transposition $x \in S_6$. If $\phi(x)$ were a transposition, then $x \in N_{S_6}(H_i)$ for some i. Each H_i is its own normalizer however, and so $x \in H_i$. This cannot be the case however because in the previous section we showed that the image of S_5 in $Sym(P_1, P_2, P_3, P_4, P_5, P_6)$ contained no transpositions. Because H is that image, it contains no transpositions and therefore none of its conjugates do either. Thus, ϕ does not send transpositions to transpositions and thus cannot be an inner automorphism.

Theorem 7.9. *The index of $Inn(S_6)$ in $Aut(S_6)$ is two.*

Proof. Consider the conjugate classes of S_6:

Class	Order	Partition Type	Number of Elements
C_1	1	1 + 1 + 1 + 1 + 1 + 1	1
C_2	2	2 + 1 + 1 + 1 + 1	15

C_3	2	2 + 2 + 1 + 1	45
C_4	2	2 + 2 + 2	15
C_5	3	3 + 1 + 1 + 1	40
C_6	3	3 + 3	40
C_7	4	4 + 1 + 1	90
C_8	4	4 + 2	90
C_9	5	5 + 1	144
C_{10}	6	3 + 2	120
C_{11}	6	6	120

The quotient group $Aut(S_6)/Inn(S_6)$ consists of cosets of $Inn(S_6)$. If we let $\sigma, \eta \in Aut(S_6) - Inn(S_6)$ be outer automorphisms, then σ and η send elements from C_2 to C_4 and vice versa. This means that $\sigma\eta$ preserves these classes. Thus $\sigma\eta \in Inn(S_6)$. Then, if $Inn(S_6)\sigma$ and $Inn(S_6)\eta$ are in $Aut(S_6)/Inn(S_6)$, then they are inverses. Also, σ^2 preserves the classes so the coset $Inn(S_6)\sigma$ is of order two and is therefore its own inverse. So, $Inn(S_6)\sigma = Inn(S_6)\eta$ and so there is only only non-identity element of $Aut(S_6)/Inn(S_6)$. Therefore, $|Aut(S_6)/Inn(S_6)| = 2$. $\diamond$

Bibliography

[1] W. Burnside, *On the outer automorphisms of a group*, Proc. Lond. Math. Soc. **11** (1913), no.2, 40-42.

[2] Phyllis Joan Cassidy, *Products of commutators are not always commutators: an example*, The Amer. Math. Month. **86** (1979), no. 9, 772.

[3] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, 2004.

[4] Gail Gallitano and Shiv Gupta. *Topics in number theory*. Kendall Hunt Publishing Company, 2018.

[5] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, 1983.

[6] Gerald Janusz and Joseph Rotman, *Outer automorphisms of S_6*, The Amer. Math. Month. **89** (1982), no. 6, 407-410.

[7] Walter Ledermann. *Introduction to the theory of finite groups*. Oliver & Boyd, 1957.

[8] Irving E. Segal, *The automorphisms of the symmetric group*, Bull. Amer. Math. Soc. **46** (1940), no. 6, 565.

[9] G. E. Wall, *Finite groups with class-preserving outer automorphisms*, Jour. Lond. Math. Soc. **S1-22** (1947), no. 4, 315-320.