MATH 3021
Algebra I
Group Theory

Paul Skoufranis

December 15, 2025

Preface:

These are the first edition of these lecture notes for MATH 3021 (Algebra I). Consequently, there may be several typographical errors, missing exposition on necessary background, or unclear explanations. If you come across any typos, errors, omissions, or unclear explanations, please feel free to contact me so that I may continually improve these notes.

Contents

Motivation for this Course

In MATH 2022 students were introduced to the notion of an abstract vector space, specifically sets together with operations of vector addition and scalar multiplication that have certain relations. Soon after, the focus was shifted away from this abstractification to specific examples of vector spaces such as $\mathbb{R}^n$, $\mathbb{C}^n$, polynomials, matrices, and functions. However, studying abstract vector spaces has merit as it produces results that can be applied to all examples without the need to verify the results for each specific example. The mathematical disciple that studies the general and specific properties of sets equipped with operations is known as Algebra.

In this first course in Abstract Algebra, we will focus on sets equipped with the simplest of operations: multiplication. Like with vector spaces, we want to study objects where the multiplication has certain nice properties, such as associativity, identity elements, and inverses. This leads us quickly to the notion of a group.

By studying groups, students will be introduces to the ideas, structures, and thought processes of the mathematical discipline of Algebra. After examining the basic structures, properties, and examples of groups, we will investigate other algebra constructs that apply for other algebraic structures, such as subgroups, homomorphisms, and quotients. We will also examine how groups can act on other objects and develop some powerful theory that help us answer the question "How many groups with n elements are there?"

Chapter 1

Groups: An Introduction

In this chapter, we will introduce the algebraic structure of a group. Specifically, groups are sets together with a multiplication that is associative, has an identity element, and has inverses. We will show some very elementary properties shared by all groups. More importantly, we will provide a plethora of examples of groups to show that developing group theory can be applied to a wide variety of situations.

1.1 Groups

In order to define the notion of a group, it first is necessary to formalize what we mean by a "multiplication" operation. At a basic level, multiplication is an operation that takes two elements of a set and produces a new element in the set. This is mathematically formalized as follows.

Definition 1.1.1. Let S be a set. A *binary operation on* S is a function $* : S \times S \to S$; that is, for every $a, b \in S$ there is an element $a * b \in S$.

Of course, we are familiarly with many binary operations.

Example 1.1.2. The operations $+$, $-$, and $\times$ are binary operations on the integers $\mathbb{Z}$.

Of course, there are operations that are not binary operations.

Example 1.1.3. The operation $\div$ is not a binary operation on $\mathbb{Z}$ since the division of two integers needs not be an integer.

Example 1.1.4. The operation $\div$ is not a binary operation on the real numbers $\mathbb{R}$ since $1 \div 0$ is not a real number.

Note the above example fails simply because of one element. If we remove this element, we do obtain a binary operation. Thus it is important to know specifically what set we are working with when contemplating if an operation is a binary operation.

Example 1.1.5. The operation $\div$ is a binary operation on $\mathbb{R} \setminus \{0\}$.

With our notion of a binary operation, we can introduce the main (and really only) object of study in this course: groups. Specifically, a group is a set and a 'nice' binary operation on the set that resembles multiplication.

Definition 1.1.6. A *group* is a pair $(G, *)$ where G is a set and $*$ is a binary operation on G such that:

(i) (Associativity) for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$,

(ii) (Identity) there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$, and

(iii) (Inverses) for all $a \in G$ there exists a $b \in G$ such that $a * b = b * a = e$.

The element e in (ii) is known as the *identity element of* G. We will always use e to denote the identity element of a group.

For $a \in G$, the element b in (iii) is known as the *inverse of* a *in* G and will be denoted a^{-1}.

Remark 1.1.7. Note in Definition 1.1.6 that for $(G, *)$ to be a group, we require that $*$ is a binary operation. Thus we must have that G is *closed under* $*$; that is, if $a, b \in G$ then $a * b \in G$. This is analogous to how vector spaces (and subspaces of vector spaces) must be closed under vector addition and scalar multiplication.

Remark 1.1.8. Note in Definition 1.1.6 that we used the terms **the** identity element and **the** inverse. A priori, it is not clear based on the definition of a group that a group can only have one identity element and each element of a group has exactly one inverse. The proofs of these facts will be presented in Section 1.3 once we have provided some examples of groups. Consequently, we will reserve the character e for the identity element of a group throughout these notes.

1.2 A Microscopic Selection of Groups

Before we begin to examine common properties shared by groups and resolve the use of the word 'the' for 'the identity element' and 'the inverse', we desire some examples of groups. However, it is not possible to describe all possible groups; there are just too many. In fact, it is conjectured that the number of groups that have been written down by mathematicians is a minuscule portion of all the groups in existence!

1.2.1 Simple Examples of Groups

We begin with some simple examples of groups. As our motivation for a group came from multiplication on a set, let us examine multiplication on our common number systems and see if we have a group.

Example 1.2.1. The pair $(\mathbb{Z}, \times)$ is not a group. Even through $(\mathbb{Z}, \times)$ is associative and has identity element 1, $(\mathbb{Z}, \times)$ does not have inverses. Indeed, note that $2 \in \mathbb{Z}$ but there is no element $b \in \mathbb{Z}$ such that $2 \times b = 1 = b \times 2$.

Example 1.2.2. The pair $(\mathbb{Q} \setminus \{0\}, \times)$ is a group. Indeed multiplication is clearly associative. Moreover, the identity element is 1 since

$$a \times 1 = 1 \times a = a$$

for all $a \in \mathbb{Q} \setminus \{0\}$. Finally, for $a \in \mathbb{Q} \setminus \{0\}$, $\frac{1}{a}$ is the inverse of a since

$$a \times \frac{1}{a} = \frac{1}{a} \times a = 1.$$

Example 1.2.3. Note that $(\mathbb{R} \setminus \{0\}, \times)$ and $(\mathbb{C} \setminus \{0\}, \times)$ are groups by the same argument as Example 1.2.2.

Although we intended that groups are sets together with a 'multiplication', it turns out that the some of the simplest examples a groups comes where the 'multiplication' doesn't look much like multiplication.

Example 1.2.4. The pair $(\mathbb{Z}, +)$ is a group. Indeed addition is clearly associative. Moreover, the identity element is 0 since

$$a + 0 = 0 + a = a$$

for all $a \in \mathbb{Z}$. Finally, for $a \in \mathbb{Z}$, $-a$ is the inverse of a since

$$a + (-a) = (-a) + a = 0.$$

Remark 1.2.5. By Example 1.2.4, we have see in the group $(\mathbb{Z}, +)$ that $a^{-1} = -a$ for all $a \in \mathbb{Z}$. In particular, $2^{-1} = -2$ in this context, not $\frac{1}{2}$ as one might expect. Thus, in this course, one must always think of a^{-1} as the group inverse of a, even when $\frac{1}{a}$ makes sense.

Example 1.2.6. Note that $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all groups by the same argument as Example 1.2.4.

In fact, it is often easier to see how addition produces groups than it is to see that multiplication produces groups. To emphasize how we can tell an object is not a group, consider the following example.

Example 1.2.7. The pair $(\mathbb{Z}, -)$ is not a group for many reasons. First, $(\mathbb{Z}, -)$ is not associative. To see this, we need only exhibit one counterexample. Indeed note if $a = 1$, $b = 2$, and $c = 3$, then $a, b, c \in \mathbb{Z}$ but

$$(a - b) - c = (1 - 2) - 3 = (-1) - 3 = -4$$

whereas

$$a - (b - c) = 1 - (2 - 3) = 1 - 1 = 0.$$

Thus $-$ is not associative.

Moreover, $(\mathbb{Z}, -)$ does not have an identity element. To see this, suppose for the sake of a contradiction that $e \in \mathbb{Z}$ were an identity element. Then

$$a - e = a = e - a$$

for all $a \in \mathbb{Z}$. Since $1 \in \mathbb{Z}$, we can take $a = 1$ in the previous equation to get

$$1 - e = 1 \qquad \text{and} \qquad 1 = e - 1.$$

The first equation implies $e = 0$ whereas the second equation implies $e = 2$. Since $0 \neq 2$, we obtain a contradiction. Hence $(\mathbb{Z}, -)$ has no identity element.

Since $(\mathbb{Z}, -)$ has no identity element, note it does not make sense to even consider inverses in Definition 1.1.6.

1.2.2 Integers Modulo n

Our next examples of groups come directly from MATH 1200. Specifically, there are many important examples of groups that can be obtained by considering the integers modulo n. Although we will reintroduce the basics of the integers modulo n here, a mode in-depth reminder can be found in Appendix Section A.4 and Appendix Section A.5.

Definition 1.2.8. Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, it is said that n *divides* a, denoted $n|a$, if there exists a $b \in \mathbb{Z}$ such that $nb = a$.

Definition 1.2.9. Let $n \in \mathbb{N}$. Two integers $a, b \in \mathbb{Z}$ are said to be *equivalent modulo* n, denoted $a \equiv b \mod n$, if $n|(b - a)$.

Recall for $n \in \mathbb{N}$ that "equivalence modulo n" is an equivalence relation and, for $a \in \mathbb{Z}$, the equivalence class of a, denoted $[a]$, is

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \mod n\}.$$

These equivalence classes partition $\mathbb{Z}$ into disjoint sets.

Definition 1.2.10. Let $n \in \mathbb{N}$. The *integers modulo* n, denoted $\mathbb{Z}_n$, is the set

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n - 1]\}.$$

Remark 1.2.11. Recall by standard properties of divides, if $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$ are such that

$$a \equiv c \mod n \qquad \text{and} \qquad b \equiv d \mod n,$$

then

$$a + b \equiv c + d \mod n \qquad \text{and} \qquad ab \equiv cd \mod n.$$

Therefore, the binary operations $+, \times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \times [b] = [ab]$$

for all $a, b \in \mathbb{Z}$ are well-defined operations.

Like the integers, the following demonstrates that the integers modulo n form a group when equipped with addition.

Example 1.2.12. Let $n \in \mathbb{N}$. The pair $(\mathbb{Z}_n, +)$ is a group. To see that $(\mathbb{Z}_n, +)$ is associative, note for all $a, b, c \in \mathbb{Z}$ that

$$\begin{aligned} ([a] + [b]) + [c] &= [a + b] + [c] \\ &= [(a + b) + c] \\ &= [a + (b + c)] \\ &= [a] + [b + c] \\ &= [a] + ([b] + [c]). \end{aligned}$$

The identity element is $[0]$ since

$$[a] + [0] = [0] + [a] = [a]$$

for all $a \in \mathbb{Z}$. Moreover, for $a \in \mathbb{Z}$, $[-a]$ is the inverse of $[a]$ since

$$[a] + [-a] = [-a] + [a] = [0].$$

Remark 1.2.13. Note the fact that $(\mathbb{Z}_n, +)$ is a group seems to follow because $(\mathbb{Z}, +)$ is a group. This will be explored further in Section 2.7.

If we want to consider $\mathbb{Z}_n$ as a group with respect to multiplication, we of course have to remove the zero element since the zero element cannot have an inverse. Is this enough? Unfortunately no.

Example 1.2.14. The pair $(\mathbb{Z}_6 \setminus \{[0]\}, \times)$ is not a group. Indeed, notice that $[2], [3] \in \mathbb{Z}_6 \setminus \{[0]\}$ yet

$$[2] \times [3] = [6] = [0] \notin \mathbb{Z}_6 \setminus \{[0]\}$$

so $\times$ is not a binary operation on $\mathbb{Z}_6 \setminus \{[0]\}$.

However, for specific values of n, we do indeed have $(\mathbb{Z}_n \setminus \{[0]\}, \times)$ is a group! Note this differs greatly from the integers as the integers are not a group with respect to multiplication as demonstrated in Example 1.2.1.

Example 1.2.15. Let p be a prime number. The pair $(\mathbb{Z}_p \setminus \{[0]\}, \times)$ is a group. To see that $(\mathbb{Z}_p \setminus \{[0]\}, \times)$ is closed under multiplication, assume $[a] \neq [0]$ and $[b] \neq 0$. Thus $a, b \not\equiv 0 \mod p$ so p does not divide a nor b and thus is not part of the prime decomposition of a and b. Hence p is not part of the prime decomposition of ab so $ab \not\equiv 0 \mod p$ so $[a] \times [b] \neq 0$. Thus $\times$ is a binary operation on $\mathbb{Z}_p \setminus \{[0]\}$.

To see that $(\mathbb{Z}_p \setminus \{[0]\}, \times)$ is associative, note for all $a, b, c \in \mathbb{Z}$ that

$$\begin{aligned}([a] \times [b]) \times [c] &= [ab] \times [c] \\ &= [(ab)c] \\ &= [a(bc)] \\ &= [a] \times [bc] \\ &= [a] \times ([b] \times [c]).\end{aligned}$$

The identity element is [1] since

$$[a] \times [1] = [1] \times [a] = [a]$$

for all $a \in \mathbb{Z}$.

Finally, to see that $(\mathbb{Z}_p \setminus \{[0]\}, \times)$ has inverses, let $[a] \in \mathbb{Z}_p \setminus \{[0]\}$ be arbitrary. Since $[a] \neq [0]$, we know that $a \not\equiv 0 \mod p$. Therefore $\gcd(a, p) = 1$. Hence, by the Euclidean Algorithm (Theorem A.6.8), there exists $s, t \in \mathbb{Z}$ such that $as + pt = 1$. Therefore

$$1 \equiv as + pt \equiv as + 0(t) \equiv as \mod p$$

so

$$[a] \times [s] = [s] \times [a] = [1].$$

Note that $[s] \neq [0]$ for otherwise $[a] \times [s] = [0] \neq [1]$. Hence $[s] \in \mathbb{Z}_p \setminus \{[0]\}$ so $[s]$ is the inverse of $[a]$ in $\mathbb{Z}_p \setminus \{[0]\}$.

Building on Example 1.2.15, we can resolve the issue from Example 1.2.14 by removing the correct set of elements.

Example 1.2.16. Let $n \in \mathbb{N}$ and let

$$\mathbb{Z}_n^\times = \{[a] \mid a \in \mathbb{Z} \text{ and } \gcd(a, n) = 1\}.$$

The pair $(\mathbb{Z}_n^\times, \times)$ is a group. To see that $\times$ is a binary operation on $\mathbb{Z}_n^\times$, let $a, b \in \mathbb{Z}$ be such that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. Therefore, every prime that divides n does not divide a and does not divide b. Hence no prime that divides n divides ab (since if p is prime and $p|(ab)$ then $p|a$ or $p|b$; this was

proved in MATH 1200 to prove the Fundamental Theorem of Arithmetic) so $\gcd(ab, n) = 1$. Hence $[a] \times [b] = [ab] \in \mathbb{Z}_n^\times$. Thus $\times$ is a binary operation on $\mathbb{Z}_n^\times$.

To see that $(\mathbb{Z}_n^\times, \times)$ is associative, note for all $a, b, c \in \mathbb{Z}$ that

$$\begin{aligned}([a] \times [b]) \times [c] &= [ab] \times [c] \\ &= [(ab)c] \\ &= [a(bc)] \\ &= [a] \times [bc] \\ &= [a] \times ([b] \times [c]).\end{aligned}$$

The identity element is $[1]$ since

$$[a] \times [1] = [1] \times [a] = [a]$$

for all $a \in \mathbb{Z}$.

Finally, to see that $(\mathbb{Z}_n^\times, \times)$ has inverses, let $a \in \mathbb{Z}$ be such that $\gcd(a, n) = 1$. By the Extended Euclidean Algorithm, there exists $s, t \in \mathbb{Z}$ such that $as + nt = 1$. Therefore $\gcd(s, n) = 1$ (since if $p|s$ and $p|n$ then $p|(as + nt)$ so $p|1$ and thus $p = \pm 1$), and

$$1 \equiv as + nt \equiv as + 0(t) \equiv as \mod n$$

so

$$[a] \times [s] = [s] \times [a] = [1].$$

Hence $[s] \in \mathbb{Z}_n^\times$ and $[s]$ is the inverse of $[a]$ in $\mathbb{Z}_n^\times$.

Note the groups in this subsection are very different from those from the previous section. Specifically, the groups in this subsection have a finite number of elements whereas the groups from the previous subsection all have an infinite number of elements. As this is an important distinction, we encapsulate this with the following definition.

Definition 1.2.17. A group $(G, *)$ is said to be *finite* if G contains a finite number of elements. The number of elements of G is called the *order of* G and is denoted $|G|$.

A group $(G, *)$ that is not finite is said to be *infinite* and is said to have infinite order, denoted $|G| = \infty$.

Remark 1.2.18. In general, for a finite set X, we will use $|X|$ to denote the number of elements in X.

Remark 1.2.19. All groups in the previous subsection are easily seen to be infinite groups. Note the groups $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_p \setminus \{[0]\})$ in this section are finite groups with $|\mathbb{Z}_n| = n$ whereas $|\mathbb{Z}_p \setminus \{[0]\}| = p - 1$.

The number of elements in $(\mathbb{Z}_n^\times, \times)$ is an interesting mathematical object in number theory.

Definition 1.2.20. The function $\varphi : \mathbb{N} \to \mathbb{N}$ defined by $\varphi(1) = 1$ and

$$\varphi(n) = |\mathbb{Z}_n^\times| = |\{m \in \{1, \ldots, n\} \mid \gcd(m, n) = 1\}|$$

for all $n \geq 2$ is called the *Euler totient function*.

Note $\varphi(p) = p - 1$ for all prime numbers p. We will leave the study of the Euler totient function for MATH 3141, but we will obtain an interesting property directly from group theory in Corollary 2.5.5.

Remark 1.2.21. Similar to how in MATH 2022 one quickly restricted to finite dimensional vector spaces, we will often restrict our attention to finite groups. Much of our theory will hold for all groups, but perhaps some of the most interesting results in this course are specifically for finite groups.

1.2.3 Matrix Groups

More examples of groups can be obtained by considering matrices. For $n \in \mathbb{N}$, we will use M_n to denote all $n \times n$ matrices with real entries. Unsurprisingly, matrices equipped with addition forms a group.

Example 1.2.22. The pair $(M_n, +)$ is a group where $+$ denotes matrix addition. Indeed, matrix addition is associative, the identity element is the zero matrix, denoted 0_n, and for $A \in M_n$, $-A$ (the matrix where every entry in A is multiplied by -1) is the inverse of A.

How about matrix multiplication when we remove the zero element? For $A, B \in M_n$, let $A \times B$ denote matrix multiplication from MATH 1021.

Example 1.2.23. The pair $(M_n \setminus \{0_n\}, \times)$ is not a group when $n \geq 2$. Indeed, if $E_{1,n}$ is the $n \times n$ matrix with a 1 in the $(1, n)$-entry and 0s in every other entry, then

$$E_{1,n} \times E_{1,n} = 0_n$$

so $\times$ is not a binary operation on $M_n \setminus \{0_n\}$.

The above should not be surprising since we expect the identity element I_n to be the identity element with respect to multiplication, and and if $A \in M_n$ is a matrix, MATH 1021 studied when there exists a matrix $B \in M_n$ such that $A \times B = B \times A = I_n$. Recall $A \in M_n$ is invertible under matrix multiplication if and only if $\det(A) \neq 0$. Let GL_n denote all invertible $n \times n$ matrices.

Example 1.2.24. The pair $(GL_n, \times)$ is a group. To see this, first note that GL_n is closed under matrix multiplication since if A and B are invertible $n \times n$ matrices, then $A \times B$ is invertible with inverse $B^{-1} \times A^{-1}$. Moreover, recall matrix multiplication is associative. Moreover the identity matrix, denoted I_n, is an element of GL_n and is the identity element. Finally, if $A \in GL_n$, then the matrix inverse of A, denoted A^{-1}, is an element of GL_n and is the inverse of A in $(GL_n, \times)$. Hence $(GL_n, \times)$ is a group.

Definition 1.2.25. For $n \in \mathbb{N}$, the pair $(GL_n, \times)$ is call the *general linear group*.

Note that $(GL_n, \times)$ is very different from the groups we had previously constructed. Indeed note for all previous groups $(G, *)$ that we considered, if $a, b \in G$ then $a * b = b * a$. However, for $A, B \in GL_n$, it need not be true that $A \times B = B \times A$. This is an important property of groups that we should consider and thus we make the following definition.

Definition 1.2.26. A group $(G, *)$ is said to be *abelian* (or *commutative*) if $a * b = b * a$ for all $a, b \in G$. A group $(G, *)$ that is not abelian is said to be a *non-abelian group*.

Remark 1.2.27. All groups in the previous subsection are easily seen to be abelian groups. Note $(GL_n, \times)$ is an infinite non-abelian groups.

1.2.4 The Quaternion Group

Based on the previous section, it is natural to ask whether there is a finite non-abelian group. In this section, we will produce one example of a finite non-abelian group using an extension of a group we can construct using the complex numbers.

Example 1.2.28. Let $G = \{1, -1, i, -i\}$ where i is the complex number such that $i^2 = -1$. Then $(G, \times)$ is a group where $\times$ denotes the multiplication of complex numbers. Indeed, consider the following multiplication table:

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	-1

Note this multiplication table shows that G is closed under $\times$. It is clear $(G, \times)$ is associative since the multiplication on the complex numbers is associative. Moreover it is clear that 1 is the identity element of $(G, \times)$ and every element has an inverse. Thus, to show that $(G, \times)$ is a group, it remains only to show that $(G, \times)$ is associative. It is not difficult to see that G is abelian. Hence $(G, \times)$ is a finite abelian group with $|G| = 4$.

By adding some more elements to Example 1.2.28 and defining multiplication in a certain way, we can construct a very interesting group.

Example 1.2.29. Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Consider the following multiplication table for a binary operation $\times$ on Q_8 subject to the rules

$$\begin{array}{lll} i \times i = -1 & j \times j = -1 & k \times k = -1 \\ i \times j = k & j \times i = -k & j \times k = i \\ k \times j = -i & k \times i = j & i \times k = -j \end{array}$$

and minuses work as one would expect:

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$	$\boldsymbol{j}$	$\boldsymbol{-j}$	$\boldsymbol{k}$	$\boldsymbol{-k}$
$\mathbf{1}$	1	-1	i	$-i$	j	$-j$	k	$-k$
$\mathbf{-1}$	-1	1	$-i$	i	$-j$	j	$-k$	k
$\boldsymbol{i}$	i	$-i$	-1	1	k	$-k$	$-j$	j
$\boldsymbol{-i}$	$-i$	i	1	-1	$-k$	k	j	$-j$
$\boldsymbol{j}$	j	$-j$	$-k$	k	-1	1	i	$-i$
$\boldsymbol{-j}$	$-j$	j	k	$-k$	1	-1	$-i$	i
$\boldsymbol{k}$	k	$-k$	j	$-j$	$-i$	i	-1	1
$\boldsymbol{-k}$	$-k$	k	$-j$	j	i	$-i$	1	-1

It is clear that 1 is the identity element of $(Q_8, \times)$ and every element has an inverse. Thus, to show that $(Q_8, \times)$ is a group, it remains only to show that $(Q_8, \times)$ is associative. Since to show

$$(a \times b) \times c = a \times (b \times c)$$

for all $a, b, c \in G$ requires 8 options for each of a, b, and c, and thus $8^3 = 512$ computations, we leave the details as an exercise. Alternatively, we will see a better way for checking that $(Q_8, \times)$ is a group in Section 1.5.

It is not difficult to see that $(Q_8, \times)$ is a finite non-abelian group (since, for example, $i \times j \neq j \times i$) with $|Q_8| = 8$.

1.2.5 Symmetric Groups

There are many more finite non-abelian groups that we can construct. One of the most important examples comes from looking at composition of invertible functions on finite sets. Thus we require some function theory introduced in MATH 1200. Although we will reintroduce some of the basics here, a mode in-depth reminder can be found in Appendix Section A.2.

Recall a function $f : X \to Y$ is bijective if and only if f is one-to-one and onto if and only if f has an inverse under composition $f^{-1} : Y \to X$.

Example 1.2.30. Let X be a non-empty set and let

$$G = \{f : X \to X \mid f \text{ is bijective}\}.$$

Then $(G, \circ)$ is a group where $\circ$ denotes the composition of functions.

To see this, first note that the composition of bijective functions produces bijective functions and composition of functions is associative with

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x) = (f \circ (g \circ h))(x)$$

for all $x \in X$ and $f, g, h \in G$. Thus

$$(f \circ g) \circ h = f \circ (g \circ h)$$

for all $f, g, h \in G$. Moreover, the identity map $\mathrm{id} : X \to X$ defined by $\mathrm{id}(x) = x$ for all $x \in X$ is clearly the identity element. Finally, for $f \in G$, the group inverse of f is the inverse f^{-1} of f under composition since

$$\left(f^{-1} \circ f\right)(x) = f^{-1}(f(x)) = x = f\left(f^{-1}(x)\right) = \left(f \circ f^{-1}\right)(x)$$

so $f^{-1} \circ f = \mathrm{id} = f \circ f^{-1}$.

One of the most important examples of groups follows from Example 1.2.30 for specific sets X.

Definition 1.2.31. Let $n \in \mathbb{N}$ and let

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \sigma \text{ is bijective}\}.$$

The group $(S_n, \circ)$ is called the *symmetric group of degree n* (or the *permutation group of degree n*).

Remark 1.2.32. Elements of $(S_n, \circ)$ are called *permutations* as if $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is in S_n then $\sigma(1), \sigma(2), \ldots, \sigma(n)$ is a reordering (or permutation) of the numbers $1, \ldots, n$. Thus it is more natural to call $(S_n, \circ)$ the permutation group of degree n. Unfortunately, it is far more common in the mathematics literature to call $(S_n, \circ)$ the symmetric group of degree n so we will stick with this terminology.

Example 1.2.33. The group (S_2, σ) has two elements $\{\sigma_1, \sigma_2\}$ where the value of $\sigma_k(m)$ is as follows:

k	$\sigma_k(1)$	$\sigma_k(2)$
1	1	2
2	2	1

Note $\sigma_1 = \mathrm{id}$ and $\sigma_2 \circ \sigma_2 = \mathrm{id}$. Clearly (S_2, σ) is abelian.

Example 1.2.34. The group (S_3, σ) has six elements $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ where the value of $\sigma_k(m)$ is as follows:

k	$\sigma_k(1)$	$\sigma_k(2)$	$\sigma_k(3)$
1	1	2	3
2	1	3	2
3	2	1	3
4	2	3	1
5	3	1	2
6	3	2	1

Note $\sigma_1 = \text{id}$. However, since

$$(\sigma_2 \circ \sigma_3)(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3$$

whereas

$$(\sigma_3 \circ \sigma_2)(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$$

we see that $\sigma_3 \circ \sigma_2 \neq \sigma_2 \circ \sigma_3$. Hence $(S_3, \circ)$ is not abelian.

Remark 1.2.35. By a similar argument to that used in Example 1.2.34, it is not difficult to see that $(S_n, \circ)$ is not abelian for all $n \geq 3$.

Remark 1.2.36. Given a permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, it is more natural to write σ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

For example, the permutation σ_5 from Example 1.2.34 is written as

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

to represent that σ_5 sends 1 to 3, 2 to 1, and 3 to 2.

Using this notation, it is easy to determine the order of $(S_n, \circ)$. Indeed, note there are n options for the value of $\sigma(1)$, after which there are $n-1$ options for the value of $\sigma(2)$, after which there are $n-2$ options for the value of $\sigma(3)$, and so on. Hence $|S_n| = n!$.

Remark 1.2.37. The above notation is also very useful when it comes to group operations. First, note that the identity element is always easily identified as

$$\text{id} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Next, composition of group elements is easily read off this notation. For example, in $(S_5, \circ)$, let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \qquad \text{and} \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}.$$

How can we write $\sigma \circ \gamma$ in this notation? That is,

$$\sigma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ ? & ? & ? & ? & ? \end{pmatrix}?$$

First we would want to determine $(\sigma \circ \gamma)(1) = \sigma(\gamma(1))$. Thus we can read off the notation for γ that $\gamma(1) = 2$, and then we can read off the notation for σ that $\sigma(2) = 1$:

$$\sigma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & ? & ? & ? & ? \end{pmatrix}.$$

By repeating this procedure, we see that

$$\sigma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

Finally, inverses of group elements can be easily obtained via this notation. For example, again consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}.$$

Since $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 5$, $\sigma(4) = 2$, and $\sigma(5) = 4$ and since we know that σ^{-1} undoes what σ does, we know that $1 = \sigma^{-1}(3)$, $2 = \sigma^{-1}(1)$, $3 = \sigma^{-1}(5)$, $4 = \sigma^{-1}(2)$, and $5 = \sigma^{-1}(4)$. This can be obtained via the notation for σ by flipping the two rows, and then reordering the columns in the correct order:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 1 & 5 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \sigma^{-1}.$$

However, there is a more compact and convenient way to write elements of $(S_n, \circ)$. This method is obtained by examining certain special elements of S_n.

Definition 1.2.38. Let $n \in \mathbb{N}$. An element $\sigma \in S_n$ is said to be a *cycle* if there exists an $m \in \mathbb{N}$ and distinct elements $a_1, a_2, \ldots, a_m \in \{1, \ldots, m\}$ such that

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ \vdots &\quad \vdots \\ \sigma(a_{m-1}) &= a_m \\ \sigma(a_m) &= a_1, \end{aligned}$$

and $\sigma(b) = b$ for all $b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_m\}$. We denote this cycle by

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}.$$

Such a cycle is called a *cycle of length* m or an *m-cycle*.

Example 1.2.39. In S_5, the element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

is not cycle. To see this, note that no element of $\{1, 2, 3, 4, 5\}$ is fixed by σ. Thus, if σ were a cycle, we would need to be able to order $\{1, 2, 3, 4, 5\}$ as $\{a_1, a_2, a_3, a_4, a_5\}$ such that $\sigma(a_k) = a_{k+1}$ for $k = 1, 2, 3, 4$ and $\sigma(a_5) = a_1$. However, since $\sigma(1) = 3$ and $\sigma(3) = 1$, we see that there is no way to do this.

Note this shows that not every element of S_n needs to be a cycle.

Example 1.2.40. In S_5, the element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

is a 5-cycle. Indeed note that $\sigma(1) = 3$, $\sigma(3) = 5$, $\sigma(5) = 4$, $\sigma(4) = 2$, and $\sigma(2) = 1$. Hence

$$\sigma = \begin{pmatrix} 1 & 3 & 5 & 4 & 2 \end{pmatrix}.$$

Example 1.2.41. In S_5, the element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

is a 3-cycle. Indeed note that $\sigma(1) = 4$, $\sigma(4) = 3$, and $\sigma(3) = 1$, whereas $\sigma(k) = k$ for all $k \notin \{1, 3, 4\}$. Hence

$$\sigma = \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}.$$

Example 1.2.42. In S_6, the element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}$$

is not cycle. To see this, note that the only element of $\{1, 2, 3, 4, 5, 6\}$ that is fixed by σ is 5. Thus, if σ were a cycle, we would need to be able to order $\{1, 2, 3, 4, 6\}$ as $\{a_1, a_2, a_3, a_4, a_5\}$ such that $\sigma(a_k) = a_{k+1}$ for $k = 1, 2, 3, 4$ and $\sigma(a_5) = a_1$. However, since $\sigma(1) = 4$ and $\sigma(4) = 1$, we see that there is no way to do this.

Note this shows that not every element of S_n needs to be a cycle.

Remark 1.2.43. Note due to the 'cyclic' nature of cycles, there need not be a unique way of writing a cycle. For example, note in S_5 that

$$\begin{pmatrix}1 & 4 & 3\end{pmatrix}, \quad \begin{pmatrix}4 & 3 & 1\end{pmatrix}, \quad \text{and} \quad \begin{pmatrix}3 & 1 & 4\end{pmatrix}$$

all represent the permutation that fixes both 2 and 5 and sends $1 \to 4 \to 3 \to 1 \to 4 \to 3 \to \cdots$. However, note that

$$\begin{pmatrix}1 & 3 & 4\end{pmatrix}$$

is a different cycle since it sends 1 to 3, not 4.

Remark 1.2.44. Recall from Example 1.2.39 that in S_5, the element

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 1 & 2 & 4\end{pmatrix}$$

is not cycle. However, if we consider the cycles $\tau = \begin{pmatrix}1 & 3\end{pmatrix}$ and $\gamma = \begin{pmatrix}2 & 5 & 4\end{pmatrix}$, then

$$\begin{aligned}\tau \circ \gamma &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 1 & 4 & 5\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 5 & 3 & 2 & 4\end{pmatrix}\\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 5 & 1 & 2 & 4\end{pmatrix}.\end{aligned}$$

Hence σ is the product of cycles.

Note the above shows that the product of cycles need not be a cycle. However, this non-cycle element of S_5 is a product of cycles. Thus it is natural to ask, "Is every element of $(S_n, \circ)$ is a product of cycles?"

It turns out that the answer to this question is yes thereby letting us describe all elements of $(S_n, \circ)$ using products of cycles. In fact, we can show that we can take the cycles in the product to have a specific property, which we define as follows.

Definition 1.2.45. Let $n \in \mathbb{N}$. Two cycles

$$\begin{pmatrix}a_1 & a_2 & \cdots & a_m\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}b_1 & b_2 & \cdots & b_\ell\end{pmatrix}$$

in S_n are said to be *disjoint* if $a_i \neq b_j$ for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, \ell\}$.

In particular, our goal is to prove the following:

Theorem 1.2.46. *Every element of S_n can be written as a product of disjoint cycles.*

The reason we like disjoint cycles is that the they commute even though $(S_n, \circ)$ is a non-abelian group.

Lemma 1.2.47. *Let $n \in \mathbb{N}$ and let*

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} b_1 & b_2 & \cdots & b_\ell \end{pmatrix}$$

be two cycles in S_n. If σ and τ are disjoint, then $\sigma \circ \tau = \tau \circ \sigma$.

Proof. Since σ and τ are disjoint, $a_i \neq b_j$ for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, \ell\}$. Note this implies that $\sigma(b_j) = b_j$ for all $j \in \{1, \ldots, \ell\}$, $\tau(a_i) = a_i$ for all $i \in \{1, \ldots, m\}$, $n \geq m + k$, and there exists

$$c_1, \ldots, c_{n-m-\ell} \in \{1, \ldots, \ell\}$$

such that

$$\{a_1, \ldots, a_m, b_1, \ldots, b_\ell, c_1, \ldots, c_{n-m-\ell}\} = \{1, \ldots, n\}.$$

Note since $c_k \neq a_i$ and $c_k \neq b_j$ for all i, j, k, we have that $\sigma(c_k) = c_k$ and $\tau(c_k) = c_k$ for all $k \in \{1, \ldots, n-m-\ell\}$. Moreover, to show that $\sigma \circ \tau = \tau \circ \sigma$, it suffices to show that

$$\sigma(\tau(a_i)) = \tau(\sigma(a_i))$$

for all $i \in \{1, \ldots, m\}$, that

$$\sigma(\tau(b_j)) = \tau(\sigma(b_j))$$

for all $j \in \{1, \ldots, \ell\}$, and that

$$\sigma(\tau(c_k)) = \tau(\sigma(c_k))$$

for all $k \in \{1, \ldots, n - m - \ell\}$. However, notice for all $i \in \{1, \ldots, m\}$ that

$$\sigma(\tau(a_i)) = \sigma(a_i) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(a_i))$$

(where $a_{m+1} = a_1$), for all $j \in \{1, \ldots, \ell\}$ that

$$\sigma(\tau(b_j)) = \sigma(b_{j+1}) = b_{j+1} = \tau(b_j) = \tau(\sigma(b_j))$$

(where $b_{\ell+1} = b_1$), and for all $k \in \{1, \ldots, n - m - \ell\}$ that

$$\sigma(\tau(c_k)) = \sigma(c_k) = c_k = \tau(c_k) = \tau(\sigma(c_k))$$

as desired. ∎

Before we attempt to prove Theorem 1.2.46, let us first write down a specific, complicated permutation, and see if we can write it as a product of cycles. This example will provide a roadmap to the proof,

Example 1.2.48. In S_{12} consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 1 & 3 & 11 & 10 & 4 & 2 & 8 & 12 & 5 & 9 & 6 \end{pmatrix}.$$

If we start with 1 and see what repeated applications of σ does, we see that σ sends $1 \to 7 \to 2 \to 1$. Thus we expect

$$\begin{pmatrix} 1 & 7 & 2 \end{pmatrix}$$

to be part of the decomposition of σ into disjoint cycles. Next, we see that 2 was already the previous cycle, so we can move on. Subsequently, we see that 3 is fixed by σ so we can either use the cycle $\begin{pmatrix} 3 \end{pmatrix}$, or we can ignore 3 as any product of disjoint cycles that do not contain 3 will automatically fix the number 3. We arrive at the number 4 and see that σ sends $4 \to 11 \to 9 \to 12 \to 6 \to 4$. Thus we expect

$$\begin{pmatrix} 4 & 11 & 9 & 12 & 6 \end{pmatrix}$$

to be part of the decomposition of σ into disjoint cycles. Finally, we see that the only numbers we have not considered are 5, 8, and 10 where σ fixes 8 and sends $5 \to 10 \to 5$. So we expect

$$\begin{pmatrix} 1 & 7 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 \end{pmatrix} \circ \begin{pmatrix} 4 & 11 & 9 & 12 & 6 \end{pmatrix} \circ \begin{pmatrix} 5 & 10 \end{pmatrix} \circ \begin{pmatrix} 8 \end{pmatrix}$$

to be part of the decomposition of σ into disjoint cycles. One can easily check that this product of cycles is in fact σ since it sends each element of $\{1, \ldots, 12\}$ to the correct element.

As a matter of notation, we remove all 1-cycles as they are just the identity element of S_n. Moreover, to make notation easier, we omit all of the $\circ$'s. Hence we simply write

$$\sigma = \begin{pmatrix} 1 & 7 & 2 \end{pmatrix} \begin{pmatrix} 4 & 11 & 9 & 12 & 6 \end{pmatrix} \begin{pmatrix} 5 & 10 \end{pmatrix}.$$

Again, note that this decomposition is not unique as

i) we can cycle the entries in any cycle as in Remark 1.2.43, and

ii) we can write the disjoint cycles in any order since they commute by Lemma 1.2.47.

Remark 1.2.49. Example 1.2.48 implies that there is a simple algorithm to write any permutation $\sigma \in S_n$ as a product of disjoint cycles:

(1) Take 1 and apply σ over and over again until we reach the number 1.

(2) Write down the cycle that Step (1) produces.

(3) Look at the first number $k \in \{1, \ldots, n\}$ that is not in any previously produced cycle and repeat Steps (1) and (2) with k replacing 1.

(4) Once all numbers in $\{1, \ldots, n\}$ are in some cycle, then σ is the product of the cycles produced.

There are a few technical aspects of this algorithm that we will need to ensure do not produce a problem; namely:

(I) How do we know for all permutations $\sigma \in S_n$ and $k \in \{1, \ldots, n\}$ that eventually $\sigma^m(k) = k$ for some $m \in \mathbb{N}$ (where σ^m is σ composed with itself m times)?

(II) How do we know that $\sigma \in S_n$ and $k \in \{1, \ldots, n\}$ that if $m \in \mathbb{N}$ is the smallest natural number such that $\sigma^m(k) = k$, then k, $\sigma(k)$, $\sigma^2(k)$, …, $\sigma^{m-1}(k)$ are distinct?

(III) How do we know that cycles produced in Step (3) are disjoint?

(IV) How do we know that the product of the cycles is the permutation?

If we can resolve all of these possible issues, then the algorithm give us a decomposition of σ into a product of disjoint cycles thereby completing the proof.

Proof of Theorem 1.2.46. Let $n \in \mathbb{N}$ and let $\sigma \in S_n$. First, we claim that if $k \in \{1, \ldots, n\}$ then there exists an $m \in \mathbb{N}$ such that $\sigma^m(k) = k$. To see this, consider the numbers

$$k, \sigma(k), \sigma^2(k), \sigma^3(k), \ldots.$$

Since each of these infinite number expressions is in $\{1, \ldots, n\}$ and since $\{1, \ldots, n\}$ has a finite number of elements, two of these numbers must be the same. Thus there exists an $\ell, p \in \mathbb{N}$ such that $\ell < p$ and

$$\sigma^\ell(k) = \sigma^p(k).$$

By composing with σ^{-1} on the left exactly ℓ-times, this implies that

$$k = \sigma^{p-\ell}(k).$$

Since $p - \ell \in \mathbb{N}$, the claim is complete (note this resolves (I) from Remark 1.2.49).

Next, for $k \in \{1, \ldots, n\}$, let $m_k \in \mathbb{N}$ be the smallest natural number such that $\sigma^{m_k}(k) = k$. We claim that

$$k, \sigma(k), \sigma^2(k), \ldots, \sigma^{m_k-1}(k)$$

are distinct elements of $\{1,\dots,n\}$. To see this, suppose for the sake of a contradiction that there are $\ell, p \in \{0,1,\dots,m_k-1\}$ such that $\ell < p$ and

$$\sigma^{\ell}(k) = \sigma^{p}(k).$$

By composing with σ^{-1} on the left exactly ℓ-times, this implies that

$$k = \sigma^{p-\ell}(k).$$

However, since $\ell, p \in \{0,1,\dots,m_k-1\}$, we have that $p-\ell \in \mathbb{N}$ is such that $p-\ell < m_k$. Since this contradicts the fact that m_k is the smallest natural number such that $\sigma^{m_k}(k) = k$, we have our contradiction. Hence

$$k, \sigma(k), \sigma^2(k), \dots, \sigma^{m_k-1}(k)$$

are distinct elements of $\{1,\dots,n\}$ (note this resolves (II) from Remark 1.2.49).

Now, assume $q \in \{1,\dots,n\}$ is such that

$$q \notin \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{m_k-1}(k)\}.$$

By repeating the above with q in place of k, there exists a smallest natural number $m_q \in \mathbb{N}$ such that $\sigma^{m_q}(q) = q$ and

$$q, \sigma(q), \sigma^2(q), \dots, \sigma^{m_q-1}(q)$$

are distinct elements of $\{1,\dots,n\}$. We claim that

$$k, \sigma(k), \sigma^2(k), \dots, \sigma^{m_k-1}(k), q, \sigma(q), \sigma^2(q), \dots, \sigma^{m_q-1}(q)$$

are distinct elements of $\{1,\dots,n\}$. To see this, suppose for the sake of contradiction that there exists $p, \ell \in \mathbb{N}$ such that

$$\sigma^{p}(k) = \sigma^{\ell}(q).$$

By composition with σ on the left exactly $(m_q - \ell)$-times, this implies that

$$\sigma^{p+m_q-\ell}(k) = \sigma^{m_q}(q) = q.$$

Let $m \in \{0,\dots,m_k-1\}$ be such that $m \equiv p + m_q - \ell \mod m_k$. Thus, since $p + m_q - \ell > 0$, there exists a $d \in \mathbb{N}$ such that $p + m_q - \ell = m + dm_k$. Therefore, since $\sigma^{m_k}(k) = k$, we see that

$$q = \sigma^{p+m_q-\ell}(k) = (\sigma^{m} \circ (\sigma^{m_k})^{d})(k) = \sigma^{m}(k),$$

which contradicts our first assumption on q. Hence the result follows (note this resolves (III) from Remark 1.2.49).

Finally, since (I), (II), and (III) from Remark 1.2.49, we can apply steps (1), (2), and (3) of the algorithm to obtain a collection of disjoint cycles containing every number from $\{1,\dots,n\}$. Since every number r from $\{1,\dots,n\}$ is contained in exactly one cycle and since the cycle containing r sends r to $\sigma(r)$, it must be the case that the product of cycles is σ thereby completing the proof. ∎

Example 1.2.50. Multiplication of permutations using the cycle decomposition is no more difficult that using our earlier notation. Indeed, in σ_7 consider the permutations

$$\sigma = \begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix}.$$

Note

$$\begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix}$$

is NOT a decomposition of $\sigma \circ \tau$ into a product of disjoint cycles since the cycles in this product are not disjoint.

To write $\sigma \circ \tau$ as a product of disjoint cycles, we need only apply the algorithm from Remark 1.2.49 by reading what the cycles do to elements from right to left (after all, the right-most cycle is the first that is applied under composition).

To begin, let us see what this product does to 1. Note the right-most cycle does not modify 1, then the next cycle sends 1 to 3, and the last two cycles don't modify 3. Thus far we have

$$\begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix} = (1 \quad 3.$$

Next, we see what the product of cycles does to 3. Note the right-most cycle doesn't affect 3, then the next cycle sends 3 to 1, the next cycle doesn't modify 1, and the last cycle sends 1 to 4. Thus we have

$$\begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix} = (1 \quad 3 \quad 4.$$

Next, we see what the product of cycles does to 5. Note the right-most cycle sends 4 to 7, then the next two cycles don't modify 7, and the last cycle sends 7 to 1. Thus we have have completed our first cycle in the product:

$$\begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \end{pmatrix} (?.$$

Continuing this process, we obtain that

$$\begin{pmatrix} 1 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & 6 & 7 \end{pmatrix}$$

(Note 5 does to 2 and then goes back to 5 in the product).

To understand how we can compute the inverse of a disjoint product of cycles, we first must understand how we can compute the inverse of a cycle.

Remark 1.2.51. It is much easier to find the inverse of a cycle using the cycle notation that it is using our old notation. Indeed, if $\sigma \in S_n$ is the cycle

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$$

then we claim that

$$\sigma^{-1} = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 \end{pmatrix}.$$

Indeed, this immediately follows since

$$\begin{array}{rcl} \sigma(a_1) = a_2 & \longrightarrow & a_1 = \sigma^{-1}(a_2) \\ \sigma(a_2) = a_3 & \longrightarrow & a_2 = \sigma^{-1}(a_3) \\ \vdots \quad \vdots & & \vdots \quad \vdots \\ \sigma(a_{m-1}) = a_m & \longrightarrow & a_{m-1} = \sigma^{-1}(a_m) \\ \sigma(a_m) = a_1 & \longrightarrow & a_m = \sigma^{-1}(a_1), \end{array}$$

and $\sigma(b) = b$ and thus $b = \sigma^{-1}(b)$ for all $b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_m\}$.

Remark 1.2.52. Computing inverses of cycle using the decomposition of permutation into disjoint cycles is then easy. We claim that to take the inverse of a permutation decomposed into a product of disjoint cycles, we need only take the inverse of each cycle and reverse the order. For example, in σ_7 consider the permutation

$$\sigma = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 6 & 4 & 7 & 5 \end{pmatrix}.$$

It is not difficult to see that

$$\sigma^{-1} = \begin{pmatrix} 5 & 7 & 4 & 6 & 2 \end{pmatrix} \begin{pmatrix} 3 & 1 \end{pmatrix}.$$

To prove the general claim, we could just apply Remark 1.2.51 provided we know the inverse of a product is the product of the inverses in the reverse order. This is is a fact that does not just hold in S_n, but holds for any group! Thus, instead of just proving this fact for S_n, it is time we proved some facts about all groups.

1.3 Elementary Properties of Groups

Now that we have a (minuscule) collection of groups, it is time to develop the most elementary proprieties shared by all groups. All results obtained in this section are proved using the most basic of algebraic operations and techniques, and generalize results for invertible matrices seen in MATH 1021. To begin, we resolve the 'the' issue from Definition 1.1.6 by showing that every group has exactly one identity element.

Proposition 1.3.1. *Let $(G, *)$ be a group. If $a \in G$ is such that $a * b = b * a = b$ for all $b \in G$, then $a = e$. That is, a group has exactly one identity element.*

Proof. Assume $a \in G$ is such that $a*b = b*a = b$ for all $b \in G$. In particular, by taking $b = e$, we obtain that $e * a = e$. However, by the properties of the identity element, we know that $e * a = a$. Hence

$$e = e * a = a$$

as desired. ∎

Similarly, we can show that the 'the inverse' in Definition 1.1.6 was grammatically correct.

Proposition 1.3.2. *Let $(G, *)$ be a group and let $a \in G$. If $b, c \in G$ are such that $a * b = b * a = e$ and $a * c = c * a = e$, then $b = c$. That is, every group element has a unique inverse. In particular, $e^{-1} = e$.*

Proof. Let $a \in G$. Assume $b, c \in G$ are such that $a * b = b * a = e$ and $a * c = c * a = e$. Then

$$\begin{aligned} b &= b * e && \text{(identity element)} \\ &= b * (a * c) && (e = a * c) \\ &= (b * a) * c && \text{(associativity)} \\ &= e * c && (b * a = e) \\ &= c && \text{(identity element)} \end{aligned}$$

as desired. Moreover, since $e * e = e$ by the properties of the identity element, we obtain that $e^{-1} = e$. ∎

Using Proposition 1.3.2, we can demonstrate that in any group the inverse of the inverse is what one would expect.

Corollary 1.3.3. *Let $(G, *)$ be a group. If $a \in G$, then $\left(a^{-1}\right)^{-1} = a$.*

Proof. Let $a \in G$. Due to the existence of inverses, $a^{-1} \in G$ has the property that $a * a^{-1} = e = a^{-1} * a$. Therefore, since Proposition 1.3.2 implies every element has a unique inverse, a must be the inverse of a^{-1}; that is, $\left(a^{-1}\right)^{-1} = a$. ∎

Moreover, inverses of products behave just like they do for invertible matrices. Note this completes the description of inverses of elements of $(S_n, \circ)$ using the cycle decomposition in Remark 1.2.52.

Corollary 1.3.4. *Let $(G, *)$ be a group. If $a, b \in G$, then $(a*b)^{-1} = b^{-1} * a^{-1}$.*

Proof. Let $a, b \in G$. Thus $b^{-1} * a^{-1} \in G$. To apply Proposition 1.3.2, notice that

$$\begin{aligned}
\left(b^{-1} * a^{-1}\right) * (a * b) &= b^{-1} * \left(a^{-1} * (a * b)\right) && \text{(associativity)} \\
&= b^{-1} * \left((a^{-1} * a) * b\right) && \text{(associativity)} \\
&= b^{-1} * (e * b) && \text{(inverses)} \\
&= b^{-1} * b && \text{(identity)} \\
&= e && \text{(inverses).}
\end{aligned}$$

By a similar computation, $(a * b) * (b^{-1} * a^{-1}) = e$. Hence Proposition 1.3.2 implies that $b^{-1} * a^{-1} = (a * b)^{-1}$. ∎

Remark 1.3.5. By the associativity properties of groups and by similar arguments to those used in Corollary 1.3.4, one can just remove brackets when multiplying multiple elements of groups. For example, instead of

$$(a * (b * c)) * (d * f),$$

we will just write

$$a * b * c * d * f.$$

Using inverses (and noting that multiplication is not commutative so orders matter), we can solve equations involving group elements.

Corollary 1.3.6. *Let $(G, *)$ be a group and let $a, b \in G$. The equations $a * x = b$ and $y * a = b$ have exactly one solution in G, namely $x = a^{-1} * b$ and $y = b * a^{-1}$.*

Proof. Let $a, b \in G$. To see that the equation $a * x = b$ has a solution in G, we note that $a^{-1} * b$ is a well-defined element of G such that

$$\begin{aligned}
a * (a^{-1} * b) &= a * a^{-1} * b \\
&= e * b && \text{(inverse)} \\
&= b && \text{(identity).}
\end{aligned}$$

Hence $a^{-1} * b$ is a solution to $a * x = b$ in G.

To see that $a^{-1} * b$ is the only solution to $a * x = b$ in G, assume $x \in G$ is such that $a * x = b$. Thus

$$\begin{aligned}
a^{-1} * b &= a^{-1} * (a * x) && (b = a * x) \\
&= a^{-1} * a * x \\
&= e * x && \text{(inverse)} \\
&= x && \text{(identity).}
\end{aligned}$$

Hence $a^{-1} * b$ is the unique solution to $a * x = b$ in G.

The proof that $b * a^{-1}$ is the unique solution to $y * a = b$ in G is similar. ∎

Again using inverses, we can 'cancel off' a variable if it appears (correctly position) on both sides of an equation.

Corollary 1.3.7. *Let $(G, *)$ be a group and let $a \in G$. If $x, y \in G$ are such that $a * x = a * y$, then $x = y$. Similarly, if $x, y \in G$ are such that $x * a = y * a$, then $x = y$.*

Proof. Let $a \in G$. Assume $x, y \in G$ are such that $a * x = a * y$. Then

$$\begin{aligned} x &= e * x && \text{(identity)} \\ &= a^{-1} * a * x && \text{(inverse)} \\ &= a^{-1} * (a * x) \\ &= a^{-1} * (a * y) && (a * x = a * y) \\ &= a^{-1} * a * y \\ &= e * y && \text{(inverse)} \\ &= y && \text{(identity)} \end{aligned}$$

as desired.

The proof that $x = y$ under the assumption $x * a = y * a$ is similar. ∎

Remark 1.3.8. It is important to note that in a non-abelian group $(G, *)$, if $a * x = y * a$, it may not be the case that $x = y$. Indeed in $(Q_8, \times)$, note that $i \times j = k = (-j) \times i$, but $j \neq -j$. Thus the order of the terms in an equation matter if one wants to cancel off a term.

Finally, it turns out that if we know $(G, *)$ is a group and we are searching for the inverse of an element, we only need to check that multiplication on one side produces the identity. Note this is the same result for matrices seen in MATH 1021.

Corollary 1.3.9. *Let $(G, *)$ be a group and let $x, y \in G$. If $y * x = e$, then $x = y^{-1}$ and $y = x^{-1}$.*

Proof. Since $y * x = e$, Corollary 1.3.6 with $a = y$ and $b = e$ implies that $x = a^{-1} * b = y^{-1} * e = y^{-1}$. Similarly, since $y * x = e$, Corollary 1.3.6 with $a = x$ and $b = e$ implies that $y = b * a^{-1} = e * x^{-1} = x^{-1}$ as desired. ∎

1.4 Product Groups

Now that we know the elementary properties shared by all groups, it is time to... construct more groups. In particular, we will demonstrate that if we have two groups then there is a way to construct a new group that 'contains' both groups.

Definition 1.4.1. Let $(G, *)$ and $(H, \star)$ be groups. The *(direct) product of G and H* is the pair $(G \times H, \cdot)$ where

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

is the Cartesian product of G and H, and $\cdot : (G \times H) \times (G \times H) \to G \times H$ is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Of course, we should verify that the product group is indeed a group.

Theorem 1.4.2. *If $(G, *)$ and $(H, \star)$ are groups, then $(G \times H, \cdot)$ as in Definition 1.4.1 is a group.*

Proof. First note that $\cdot$ as defined in Definition 1.4.1 is a well-defined binary operation since $g_1 * g_2 \in G$ and $h_1 \star h_2 \in H$ for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

To see that $\cdot$ is associative, notice for all $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$ that

$$\begin{aligned}
&((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) \\
&= (g_1 * g_2, h_1 \star h_2) \cdot (g_3, h_3) \\
&= ((g_1 * g_2) * g_3, (h_1 \star h_2) \star h_3) \\
&= (g_1 * (g_2 * g_3), h_1 \star (h_2 \star h_3)) && \text{since } * \text{ and } \star \text{ are associative} \\
&= (g_1, h_1) \cdot (g_2 * g_3, h_2 \star h_3) \\
&= (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)).
\end{aligned}$$

Hence $\cdot$ is associative.

To see that $(G \times H, \cdot)$ has an identity element, let $e_G \in G$ and $e_H \in H$ be the identity elements of G and H respectively. Note $e = (e_G, e_H) \in G \times H$ by definition. We claim that e is the identity element of $(G \times H, \cdot)$. To see this, let $(g, h) \in G \times H$ be arbitrary. Then

$$(g, h) \cdot e = (g * e_G, h * e_H) = (g, h) = (e_G * g, e_H * h) = e \cdot (g, h).$$

Therefore, since $(g, h) \in G \times H$ was arbitrary, e is the identity element of $(G \times H, \cdot)$.

Finally, to see that $(G \times H, \cdot)$ has inverses, let $(g, h) \in G \times H$ be arbitrary. Let $g^{-1} \in G$ be the inverse of g in $(G, *)$ and let $h^{-1} \in H$ be the inverse of h in $(H, \star)$. Then $(g^{-1}, h^{-1}) \in G \times H$ and

$$\begin{aligned}
(g, h) \cdot (g^{-1}, h^{-1}) &= (g * g^{-1}, h \star h^{-1}) \\
&= (e_G, e_H) \\
&= (g^{-1} * g, h^{-1} \star h) \\
&= (g^{-1}, h^{-1}) \cdot (g, h).
\end{aligned}$$

Hence (g^{-1}, h^{-1}) is the inverse of (g, h) in $(G \times H, \cdot)$. Therefore, since $(g, h) \in G \times H$ was arbitrary, $(G \times H, \cdot)$ has inverses and thus is a group. ∎

Remark 1.4.3. Given two groups $(G, *)$ and $(H, \star)$, it is easy to see that $|G \times H| = |G||H|$ (where $|G||H| = \infty$ whenever $|G| = \infty$ or $|H| = \infty$), and that $G \times H$ is abelian if and only if G and H are abelian.

By considering product groups, we obtain more examples of groups. In particular, our first example is very similar to an example from MATH 1021.

Example 1.4.4. Consider the group $(\mathbb{R}, +)$ and the product group $\mathbb{R} \times \mathbb{R}$. Note

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$$

and the product operation on $\mathbb{R} \times \mathbb{R}$ is

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

This is the same vector space addition defined on $\mathbb{R}^2$ in MATH 1021. Thus $\mathbb{R}^2$ is a group with respect to vector addition.

Product groups can also be used to construct a group of order 4 that will be a significant example moving forward.

Example 1.4.5. Consider the group $(\mathbb{Z}_2, +)$ and the product group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is an abelian group with four elements:

$$e = ([0], [0]) \qquad a = ([1], [0])$$
$$b = ([0], [1]) \qquad c = ([1], [1]).$$

Since $[1] + [1] = [0]$ in $\mathbb{Z}_2$, we can easily obtain the following multiplication table:

$\cdot$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	e	c	b
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	b	a	e

The group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ is called the *Klein four group*.

If one stares at the multiplication tables of the Klein four group and of $(\mathbb{Z}_4, +)$, one will notice differences. More on this later.

Remark 1.4.6. Although our two illuminating examples of product groups given above are both for a product of a group and itself, one can always for $G \times H$ for two different groups G and H. For example, the product of the groups $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_3, +)$ is a abelian group with 6 elements.

Of course, we need not stop at only allowing two groups in a product

Definition 1.4.7. Let $n \in \mathbb{N}$ and let $(G_1, *_1)$, ..., $(G_n, *_n)$ be groups. The *(direct) product of* $G_1, \ldots, G_n$ is the pair $(G_1 \times G_2 \times \cdots \times G_n, \cdot)$ where

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_N\}$$

is the Cartesian product of $G_1, \ldots, G_n$, *and*

$$\cdot : (G_1 \times G_2 \times \cdots \times G_n) \times (G_1 \times G_2 \times \cdots \times G_n) \to G_1 \times G_2 \times \cdots \times G_n$$

is defined by

$$(g_1, g_2, \ldots, g_n) \cdot (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n)$$

for all $(g_1, g_2, \ldots, g_n), (h_1, h_2, \ldots, h_n) \in G_1 \times G_2 \times \cdots \times G_n$.

Remark 1.4.8. By repeating the proof of Theorem 1.4.2 by replacing pairs with n-tuples, it is not difficult to see that $(G_1 \times G_2 \times \cdots G_n, \cdot)$ is a group. Moreover, if e_k is the identity element of G_k for all $k \in \{1, \ldots, n\}$, then the identity element of $(G_1 \times G_2 \times \cdots G_n, \cdot)$ is

$$e = (e_1, e_2, \ldots, e_n)$$

and if $(g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \cdots \times G_n$, then

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}).$$

1.5 Subgroups

Recall from our motivation for product groups that the product group $(G \times H, \cdot)$ of $(G, *)$ and $(H, \star)$ was supposed to be a group that contains both $(G, *)$ and $(H, \star)$. So what exactly do we mean by 'contains' in this context?

This leads us back to an concept from MATH 2022, namely subspaces. Recall that a subspace of a vector space V is a smaller vector space inside of V with respect to the same operations of vector addition and scalar multiplication. We can study a similar concept for groups, which we define as follows.

Definition 1.5.1 (PMath Definition of a Subgroup). Let $(G, *)$ be a group. A subset $H \subseteq G$ is said to be a *subgroup of* G, denoted $H \leq G$, if H is a group with respect to the binary operation $*$.

Remark 1.5.2. Note Definition 1.5.1 may seem foreign based students' thoughts of what a subspace is either due to how their instructor in MATH 2022 defined a subspace, or due to the natural inclination of students to forget the actual definition and memorize how one checks they have a subspace: contains the zero vector and is closed under vector addition and scalar multiplication. However, Definition 1.5.1 is the correct way to think of what a subspace is and will be of use in this course. That is not to say that there isn't another way to verify that one has a subgroup similar to how one verifies they have a subspace. :)

Remark 1.5.3. Let $(G, *)$ be a group and let $H \subseteq G$. Since $(G, *)$ is a group, we know that $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$. However, since $H \subseteq G$, we automatically have $(a * b) * c = a * (b * c)$ for all $a, b, c \in H$. Thus one benefit for considering subgroups is that one need not check the associativity property for $(H, *)$ as one already knew associativity for $(G, *)$.

Remark 1.5.4. Let $(G, *)$ be a group and let $H \leq G$. By "H is a group with respect to the binary operation $*$", we mean that if we restrict the domain of $* : G \times G \to G$ to $H * H$, then $*$ is binary operation on H meaning $* : H \times H \to H$. Thus, for H to be a subgroup of H, we require that $a * b \in H$ for all $a, b \in H$; that is, H is closed under the operation $*$.

Remark 1.5.5. Let $(G, *)$ be a group and let $H \leq G$. Since groups have an identity element, H must have an identity element and thus H is non-empty.

Let e_G be the identity element of G and let e_H be the identity element of H. Must it be the case that $e_H = e_G$?

Since e_H is the identity element of H, we know that $e_H * e_H = e_H$ by the group properties of H. However, since e_G is the identity element of G and since $e_H \in H \subseteq G$, we know that $e_H = e_H * e_G$ by the group properties of G. Hence

$$e_H * e_H = e_H * e_G$$

in G. However, since G is a group and has cancellation by Corollary 1.3.7, we obtain that $e_H = e_G$. Thus the identity element of a subgroup must be the identity element of the group.

Remark 1.5.6. Let $(G, *)$ be a group, let $H \leq G$, and let $a \in H$. Since both $(G, *)$ and $(H, *)$ are groups, a has an inverse in both H and G. Note the inverse of a in H is also an inverse of a in G since H and G share the same identity element by Remark 1.5.5. Therefore, since inverses in $(G, *)$ are unique by Proposition 1.3.2, the inverse of a in H must agree with the inverse of a in G.

Using the above, we arrive at another definition of what a subgroup is that is analogous to the three property 'definition' of a subspace of a vector space.

Definition 1.5.7 (Practical Definition of a Subgroup). Let $(G, *)$ be a group. A subset $H \subseteq G$ is said to be a *subgroup of* G, denoted $H \leq G$, if

(i) (contains identity) $e \in H$,

(ii) (closed under products) $a * b \in H$ for all $a, b \in H$, and

(iii) (closed under inverses) $a^{-1} \in H$ for all $a \in H$.

Remark 1.5.8. It follows immediately from Remark 1.5.4, Remark 1.5.5, and Remark 1.5.6 that if H satisfies Definition 1.5.1, then H satisfies Definition 1.5.7. Conversely, if a subset H of a group $(G, *)$ has the three properties listed in Definition 1.5.7, then $(H, *)$ is a group as

- $*$ is a binary operation on H since H is closed under products,
- $*$ is associative on H since $*$ is associative on G,
- H has an identity elements since $e \in H$, and
- every element in H has an inverse since H is closed under inverses,

and thus H satisfies Definition 1.5.1.

The benefit of Definition 1.5.1 over Definition 1.5.7 often occurs when trying to prove certain results such as the following.

Corollary 1.5.9. *Let $(G, *)$ be a group. If $H \leq G$ and $K \leq H$, then $K \leq G$.*

Proof. Note, by Definition 1.5.1, $H \leq G$ implies $(H, *)$ is a group, and thus $K \leq H$ implies $(K, *)$ is a group. Therefore $K \leq G$. ∎

Of course Definition 1.5.7 can also be easier to use depending on the context. For example, Definition 1.5.7 it much easier to apply compared to Definition 1.5.1 to show the following.

Corollary 1.5.10. *Let $(G, *)$ be a group and let $\{H_i\}_{i \in I}$ be a non-empty collection of subgroups of $(G, *)$. Then $\bigcap_{i \in I} H_i \leq G$.*

Proof. To see that $\bigcap_{i \in I} H_i \leq G$, we need only verify the three properties from Definition 1.5.7.

First, to see that $\bigcap_{i \in I} H_i$ contains the identity, note since $H_i \leq G$ for all $i \in I$ that $e \in H_i$ for all $i \in I$. Hence $e \in \bigcap_{i \in I} H_i$ as desired.

Next, to see that $\bigcap_{i \in I} H_i$ is closed under products, let $a, b \in \bigcap_{i \in I} H_i$ be arbitrary. Thus $a, b \in H_i$ for all $i \in I$. Therefore, since $H_i \leq G$ for all $i \in I$, we obtain that $a * b \in H_i$ for all $i \in I$ and thus $a * b \in \bigcap_{i \in I} H_i$.

Finally, to see that $\bigcap_{i \in I} H_i$ is closed under inverses, let $b \in \bigcap_{i \in I} H_i$ be arbitrary. Therefore, since $H_i \leq G$ for all $i \in I$, we obtain that $b^{-1} \in H_i$ for all $i \in I$ and thus $b^{-1} \in \bigcap_{i \in I} H_i$.

Therefore, since we have verified the three properties from Definition 1.5.7, $\bigcap_{i \in I} H_i \leq G$ as desired. ∎

In fact, Definition 1.5.7 can be further simplified to the following.

Theorem 1.5.11 (Subgroup Criterion). *Let $(G, *)$ be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*

- *$H \neq \emptyset$ and*

- $a * b^{-1} \in H$ *for all* $a, b \in H$.

Proof. First, assume $H \leq G$. Thus $e \in H$ by Definition 1.5.7 so H is non-empty. Moreover, if $a, b \in H$, then $b^{-1} \in H$ as H is closed under inverses and thus $a * b^{-1} \in H$ as H is closed under products. Hence one direction of the proof is complete.

Conversely, assume $H \neq \emptyset$ and $a * b^{-1} \in H$ for all $a, b \in H$. To see that $H \leq G$, we need only verify the three properties from Definition 1.5.7.

First, to see that H contains the identity, note since $H \neq \emptyset$ that there exists an element $a \in H$. Therefore, $e = a * a^{-1} \in H$ by the assumptions of this direction (i.e. with $b = a$).

Next, to see that H is closed under inverses, let $b \in H$ be arbitrary. Therefore, since $e \in H$, we have that $b^{-1} = e * b^{-1} \in H$ by the assumptions of this direction (i.e. with $a = e$).

Finally, to see that H is closed under products, let $a, b \in H$ be arbitrary. Then $b^{-1} \in H$ as we have already demonstrated that H is closed under inverses. Therefore

$$a * b = a * (b^{-1})^{-1} \in H$$

by Corollary 1.3.3 and the assumptions of this direction (i.e. with b^{-1} in place of b).

Therefore, since we have verified the three properties from Definition 1.5.7, $H \leq G$ as desired. ∎

1.6 A Microscopic Selection of Subgroups

Using Definition 1.5.7, we can construct many examples of subgroups of the groups constructed in Section 1.2 and thus many more examples of groups.

1.6.1 Silly Subgroups

It turns out that there are always some subgroups of every group and these groups are a little silly.

Example 1.6.1. Let $(G, *)$ be a group. Then $(G, *)$ is a subgroup of $(G, *)$. Indeed $G \subseteq G$ and all three properties from Definition 1.5.7 are trivially satisfied.

As often we don't want to consider a group as a subgroup of itself, we will use the following terminology.

Definition 1.6.2. A subgroup H of a group $(G, *)$ is said to be a *proper subgroup*, denoted $H < G$, if $H \leq G$ and $H \neq G$.

There is one more silly subgroup we should mention.

Example 1.6.3. Let $(G, *)$ be a group. Let $H = \{e\}$. Then $H \leq G$. Indeed, clearly $e \in H$, $e * e = e \in H$, and $e^{-1} = e \in H$. Thus H satisfies all three properties from Definition 1.5.7 and thus is a subgroup of G.

As we often want to exclude this singleton subgroup, we can make use of the following terminology.

Definition 1.6.4. A subgroup H of a group $(G, *)$ is said to be a *non-trivial subgroup* if $H \leq G$, $H \neq \{e\}$, and $H \neq G$.

1.6.2 Subgroups of Standard Number Systems

Now that we have the silly subgroups out of the way, we can look at more interesting subgroups. We begin with our groups obtain via addition and multiplication on our common number systems.

Example 1.6.5. In the group $(\mathbb{R}, +)$, we claim that $\mathbb{Q}$ is a subgroup of $(\mathbb{R}, +)$. To see this, first note that 0 is the identity element of $(\mathbb{R}, +)$ and $0 \in \mathbb{Q}$ since 0 is rational.

Next, to see that $\mathbb{Q}$ is closed under products (i.e. the group operation, which is addition in this setting), let $a, b \in \mathbb{Q}$ be arbitrary. Then $a + b \in \mathbb{Q}$ since the sum of rational numbers is rational. Hence $\mathbb{Q}$ is closed under the group products.

Finally, to see that $\mathbb{Q}$ is closed under inverses, let $a \in \mathbb{Q}$ be arbitrary. Then, in $(\mathbb{R}, +)$,

$$a^{-1} = -a.$$

Therefore, since $-a \in \mathbb{Q}$, we obtain that $a^{-1} \in \mathbb{Q}$. Hence $\mathbb{Q}$ is closed under inverses. Thus $\mathbb{Q}$ is a subgroup of $(\mathbb{R}, +)$ by Definition 1.5.7.

Example 1.6.6. Let $n \in \mathbb{N}$. In the group $(\mathbb{Z}, +)$, consider the set

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

We claim that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. To see this, first note that 0 is the identity element of $(\mathbb{Z}, +)$ and $0 \in n\mathbb{Z}$ since $0 = n(0)$ (i.e. take $k = 0$).

Next, to see that $n\mathbb{Z}$ is closed under products (i.e. the group operation, which is addition in this setting), let $a, b \in n\mathbb{Z}$ be arbitrary. Since $a, b \in n\mathbb{Z}$, there exists $m, k \in \mathbb{Z}$ such that $a = nm$ and $b = nk$. Then

$$a + b = nm + nk = n(m + k).$$

Therefore, since $m + k \in \mathbb{Z}$, we obtain that $a + b \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is closed under the group products.

Finally, to see that $n\mathbb{Z}$ is closed under inverses, let $a \in n\mathbb{Z}$ be arbitrary. Since $a \in n\mathbb{Z}$, there exists a $k \in \mathbb{Z}$ such that $a = nk$. Then, in $(\mathbb{Z}, +)$,

$$a^{-1} = -a = -nk = n(-k).$$

Therefore, since $-k \in \mathbb{Z}$, we obtain that $a^{-1} \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is closed under inverses. Thus $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ by Definition 1.5.7.

Example 1.6.7. In the group $(\mathbb{R} \setminus \{0\}, \times)$, $\mathbb{Q} \setminus \{0\}$ is a subgroup. Indeed both $\mathbb{R} \setminus \{0\}$ and $\mathbb{Q} \setminus \{0\}$ are groups with respect to $\times$ by Example 1.2.2 and Example 1.2.3. Hence $\mathbb{Q} \setminus \{0\}$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$.

Similarly, both $\mathbb{R} \setminus \{0\}$ and $\mathbb{Q} \setminus \{0\}$ are subgroups of $(\mathbb{C} \setminus \{0\}, \times)$.

For a more exotic subgroup, we consider the following.

Example 1.6.8. In the group $(\mathbb{C} \setminus \{0\}, \times)$, consider the set

$$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$$

(note $\mathbb{T}$ stands for 'torus'). We claim that $\mathbb{T}$ is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$. To see this, first note that $\mathbb{T} \subseteq \mathbb{C} \setminus \{0\}$. Moreover, note that 1 is the identity element of $(\mathbb{C} \setminus \{0\}, \times)$ and $1 \in \mathbb{T}$ since $|1| = 1$.

Next, to see that $\mathbb{T}$ is closed under products, let $z, w \in \mathbb{T}$ be arbitrary. Since $z, w \in \mathbb{T}$, we know that $|z| = 1$ and $|w| = 1$. Thus

$$|z \times w| = |z||w| = 1(1) = 1.$$

Therefore $z \times w \in \mathbb{T}$. Hence $\mathbb{T}$ is closed under the group products.

Finally, to see that $\mathbb{T}$ is closed under inverses, let $z \in \mathbb{T}$ be arbitrary. Since $z \in \mathbb{T}$, we know that $|z| = 1$. Then, in $(\mathbb{C} \setminus \{0\}, \times)$,

$$z^{-1} = \frac{1}{z} \qquad \text{and} \qquad \left|\frac{1}{z}\right| = \frac{1}{|z|} = \frac{1}{1} = 1.$$

Therefore $z^{-1} \in \mathbb{T}$. Hence $\mathbb{T}$ is closed under inverses. Thus $\mathbb{T}$ is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$ by Definition 1.5.7.

Example 1.6.9. In the group $(\mathbb{C} \setminus \{0\}, \times)$, consider the set

$$H = \{1, -1, i, -i\}.$$

We claim that H is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$. To see this, recall the multiplication table from Example 1.2.28:

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	-1

From this table, we see that H is contains 1, which is the identity element of $(\mathbb{C} \setminus \{0\}, \times)$, is closed under products, and is closed under inverses. Thus H is a subgroup of $(\mathbb{C} \setminus \{0\}, \times)$. Similarly, H is a subgroup of $(\mathbb{T}, \times)$ with $\mathbb{T}$ as defined in Example 1.6.8.

1.6.3 Subgroups of Matrix Groups Systems

By considering subgroups of $(GL_n, \times)$, we can obtain groups consisting of matrices that have applications and significant throughout mathematics. We begin with the following.

Example 1.6.10. Let $n \in \mathbb{N}$. In the group $(GL_n, \times)$, consider the set

$$SL_n = \{A \in GL_n \mid \det(A) = 1\}.$$

We claim that SL_n is a subgroup of $(GL_n, \times)$. To see this, first note I_n is the identity element of $(GL_n, \times)$ and $I_n \in SL_n$ since $\det(I_n) = 1$.

Next, to see that SL_n is closed under products, let $A, B \in SL_n$ be arbitrary. Since $A, B \in SL_n$, we know that $\det(A) = 1$ and $\det(B) = 1$. Thus

$$\det(A \times B) = \det(A)\det(B) = 1(1) = 1.$$

Therefore $A \times B \in SL_n$. Hence SL_n is closed under the group products.

Finally, to see that SL_n is closed under inverses, let $A \in SL_n$ be arbitrary. Since $A \in SL_n$, we know that $\det(A) = 1$. Then, in $(GL_n, \times)$, A^{-1} is the matrix inverse of A and

$$1 = \det(I_n) = \det(A \times A^{-1}) = \det(A)\det(A^{-1}) = 1(\det(A^{-1}) = \det(A^{-1}).$$

Therefore $A^{-1} \in SL_n$. Hence SL_n is closed under inverses. Thus SL_n is a subgroup of $(GL_n, \times)$ by Definition 1.5.7.

Definition 1.6.11. For $n \in \mathbb{N}$, the pair $(SL_n, \times)$ from Example 1.6.10 is called the *special linear group*.

We can take the special linear group one step further by restricting the entries allowed in the matrices.

Example 1.6.12. Let $n \in \mathbb{N}$. In the group $(SL_n, \times)$, consider the set

$$SL_n(\mathbb{Z}) = \{[a_{i,j}] \in SL_n \mid a_{i,j} \in \mathbb{Z} \text{ for all } i, j \in \{1, \ldots, n\}\}.$$

We claim that $SL_n(\mathbb{Z})$ is a subgroup of $(SL_n, \times)$. To see this, first note I_n is the identity element of $(SL_n, \times)$ and $I_n \in SL_n(\mathbb{Z})$ since every entry of I_n is an integer.

Next, to see that $SL_n(\mathbb{Z})$ is closed under products, let $A, B \in SL_n(\mathbb{Z})$ be arbitrary. Since $A, B \in SL_n(\mathbb{Z})$, we know that the entries of A and B are integers. Thus the entries of $A \times B$ are also integers. Therefore $A \times B \in SL_n(\mathbb{Z})$. Hence $SL_n(\mathbb{Z})$ is closed under the group products.

Finally, to see that $SL_n(\mathbb{Z})$ is closed under inverses, let $A \in SL_n(\mathbb{Z})$ be arbitrary. Since $A \in SL_n(\mathbb{Z})$, we know that $\det(A) = 1$ and the entries of A are all integers. Then, in $(SL_n, \times)$, A^{-1} is the matrix inverse of A and the entries of A^{-1} must also be integers since A^{-1} will be the classical adjoint of A (see MATH 2022). Therefore $A^{-1} \in SL_n(\mathbb{Z})$. Hence $SL_n(\mathbb{Z})$ is closed under inverses. Thus $SL_n(\mathbb{Z})$ is a subgroup of $(SL_n, \times)$ by Definition 1.5.7.

More important matrix groups can be constructed using the notion of orthogonality and inner products.

Example 1.6.13. Let $n \in \mathbb{N}$. In the group $(GL_n, \times)$, consider the set

$$O(n) = \{Q \in GL_n \mid Q^{-1} = Q^t\}$$

(where, for a matrix A, A^t is the transpose of A). We claim that $O(n)$ is a subgroup of $(GL_n, \times)$. To see this, first note I_n is the identity element of $(GL_n, \times)$ and $I_n \in O(n)$ since $I_n^{-1} = I_n = I_n^t$.

Next, to see that $O(n)$ is closed under products, let $A, B \in O(n)$ be arbitrary. Since $A, B \in O(n)$, we know that $A^{-1} = A^t$ and $B^{-1} = B^t$. Thus

$$(A \times B)^{-1} = B^{-1} \times A^{-1} = B^t \times A^t = (A \times B)^t.$$

Therefore $A \times B \in O(n)$. Hence $O(n)$ is closed under the group products.

Finally, to see that $O(n)$ is closed under inverses, let $A \in O(n)$ be arbitrary. Since $A \in O(n)$, we know that $A^{-1} = A^t$. Then, in $(GL_n, \times)$, A^{-1} is the matrix inverse of A and

$$(A^{-1})^{-1} = A = (A^t)^t = (A^{-1})^t.$$

Therefore $A^{-1} \in O(n)$. Hence $O(n)$ is closed under inverses. Thus $O(n)$ is a subgroup of $(GL_n, \times)$ by Definition 1.5.7.

Definition 1.6.14. For $n \in \mathbb{N}$, the pair $(O(n), \times)$ from Example 1.6.13 is called the *orthogonal group*.

In fact, one of our more complicated previous groups $(Q_8, \times)$ can be realized as a subgroup of GL_n as the following example demonstrates. In particular, recall that it was difficult to show that $(Q_8 \times)$ was a group in Example 1.2.29 since it required us to check up to $8^3 = 512$ cases in order to show that the multiplication is associated. Therefore, by realizing $(Q_8, \times)$ as a subgroup of GL_4, we automatically obtain that the multiplication is associative without the need to do 512 computations. This is one of the powers of subgroups!

Example 1.6.15. In $(GL_4, \times)$, let

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \qquad D = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

and let $H = \{A, -A, B, -B, C, -C, D, -D\}$. One can check the following multiplication table for H:

$\times$	$\boldsymbol{A}$	$\boldsymbol{-A}$	$\boldsymbol{B}$	$\boldsymbol{-B}$	$\boldsymbol{C}$	$\boldsymbol{-C}$	$\boldsymbol{D}$	$\boldsymbol{-D}$
$\boldsymbol{A}$	A	$-A$	B	$-B$	C	$-C$	D	$-D$
$\boldsymbol{-A}$	$-A$	A	$-B$	B	$-C$	C	$-D$	D
$\boldsymbol{B}$	B	$-B$	$-A$	A	D	$-D$	$-C$	C
$\boldsymbol{-B}$	$-B$	B	A	$-A$	$-D$	D	C	$-C$
$\boldsymbol{C}$	C	$-C$	$-D$	D	$-A$	A	B	$-B$
$\boldsymbol{-C}$	$-C$	C	D	$-D$	A	$-A$	$-B$	B
$\boldsymbol{D}$	D	$-D$	C	$-C$	$-B$	B	$-A$	A
$\boldsymbol{-D}$	$-D$	D	$-C$	C	B	$-B$	A	$-A$

From this table, we see that H is contains I_4, which is the identity element of $(GL_4, \times)$, is closed under products, and is closed under inverses. Thus H is a subgroup of $(GL_4, \times)$.

Note that H is has the same multiplication table as the Quaternions as presented in Example 1.2.29 with $A \leftrightarrow 1$, $B \leftrightarrow i$, $C \leftrightarrow j$, and $D \leftrightarrow k$. Thus this proves $(Q_8, \times)$ is a group without verifying the associativity property and shows that $(Q_8, \times)$ can be viewed as a subgroup of $(GL_4, \times)$.

Remark 1.6.16. Note there is a much easier way to write Q_8 as matrices provided we allow complex entries. Indeed one can view $(Q_8, \times)$ as a subgroup of the 2×2 matrices with complex entries where

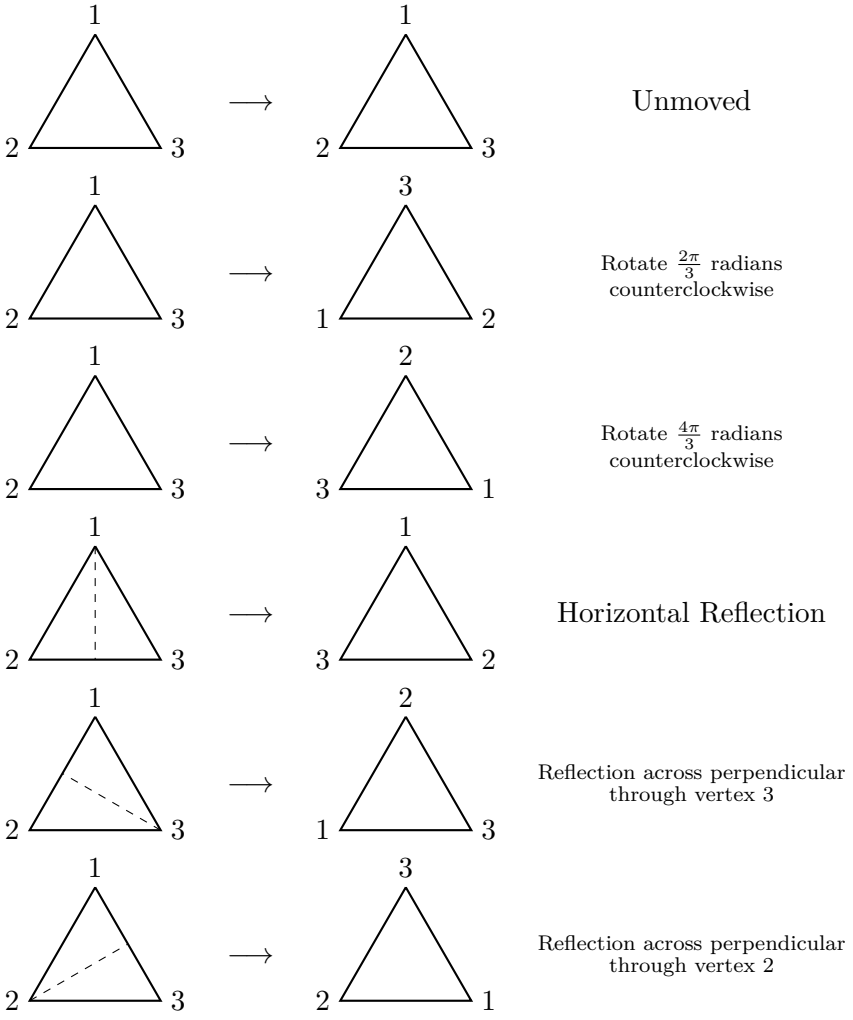
$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$
$$C = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad D = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

In this course, we will stick with matrices with real entries as all group theory examples involving complex matrices can be given using real matrices.

1.6.4 Dihedral Groups

By considering the geometry of a regular n-gon, we can construct some exotic subgroups of $(S_n, \circ)$. Instead of trying to construct all these groups at once, we will begin with the $n = 3$ and $n = 4$ cases to motivate the general case.

Example 1.6.17. Consider an equilateral triangle and all of the symmetries of the triangle; that is, all ways we can move the triangle that cause it to end up in the exact same spot. There are 6 such symmetries that we can visualize as follows where we have numbered the vertices just to emphasize the way in which we moved the triangle:



Note each of these symmetries corresponds to a unique permutation in S_3 on the labelling of the vertices of the triangle. Since $|S_3| = 3! = 6$ and since there are 6 symmetries, we have recognized all the elements of S_3 via symmetries on a equilateral triangle.

However, there is another way to present these symmetries. First we can let ρ be the rotation by $\frac{2\pi}{3}$ radians counter-clockwise; that is

$$\rho = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

(this is because 1 is going to the second spot on the triangle, 2 is going to the third spot on the triangle, and 3 is going to the first spot on the triangle). It is then not difficult to see that

$$\rho^2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$$

is the rotation by $\frac{4\pi}{3}$ radians counter-clockwise, and ρ^3 is the rotation by $\frac{6\pi}{3}$ radians counter-clockwise and thus $\rho^3 = e$. Next let τ be the horizontal

reflection; that is

$$\tau = \begin{pmatrix} 2 & 3 \end{pmatrix}.$$

It is not difficult to see that the reflection across the perpendicular through the vertex 3 can be realized by applying the horizontal reflection followed by a rotation by $\frac{2\pi}{3}$ radians counter-clockwise (i.e. $\rho \circ \tau$) and the reflection across the perpendicular through the vertex 2 can be realized by applying the horizontal reflection followed by a rotation by $\frac{4\pi}{3}$ radians counter-clockwise (i.e. $\rho^2 \circ \tau$). Thus we can write

$$S_3 = \{e, \rho, \rho^2, \tau, \rho \circ \tau, \rho^2 \circ \tau\}.$$

Using this way of presenting S_3, we must ask how do we multiply group elements in this form? We already know that $\rho^3 = e$ so we know how to multiple elements of the form ρ^k. For example ,

$$\rho^2 \circ \rho^2 = \rho^4 = \rho \circ (\rho^3) = \rho \circ e = \rho.$$

Next we note that $\tau^2 = e$ since if we apply the horizontal reflection twice we end up back where we started. Finally, it is not difficult to see via geometric operations that $\tau \circ \rho$ is the same as the reflection across the perpendicular through the vertex 2; that is,

$$\tau \circ \rho = \rho^2 \circ \tau = \rho^{-1} \circ \tau.$$

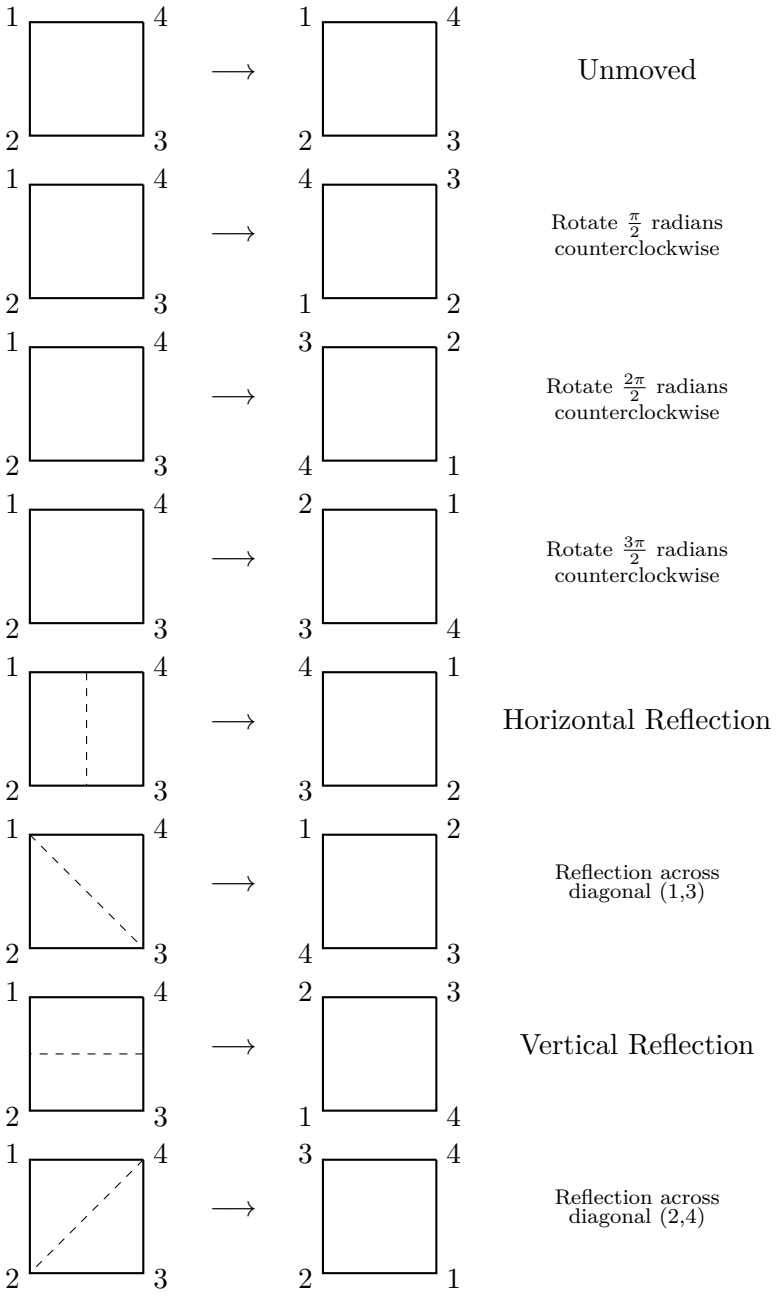
Using these rules, we can easily multiply all elements in the above presentation of S_3. For example,

$$\begin{aligned} \tau \circ (\rho^2 \circ \tau) &= (\tau \circ \rho) \circ (\rho \circ \tau) \\ &= (\rho^2 \circ \tau) \circ (\rho \circ \tau) \\ &= \rho^2 \circ (\tau \circ \rho) \circ \tau \\ &= \rho^2 \circ (\rho^2 \circ \tau) \circ \tau \\ &= \rho^4 \circ \tau^2 \\ &= \rho \circ e = \rho. \end{aligned}$$

In particular, we have the following multiplication table for S_3 in this presentation:

$\circ$	$\boldsymbol{e}$	$\boldsymbol{\rho}$	$\boldsymbol{\rho^2}$	$\boldsymbol{\tau}$	$\boldsymbol{\rho \circ \tau}$	$\boldsymbol{\rho^2 \circ \tau}$
$\boldsymbol{e}$	e	ρ	ρ^2	τ	$\rho \circ \tau$	$\rho^2 \circ \tau$
$\boldsymbol{\rho}$	ρ	ρ^2	e	$\rho \circ \tau$	$\rho^2 \circ \tau$	τ
$\boldsymbol{\rho^2}$	ρ^2	e	ρ^3	$\rho^2 \circ \tau$	τ	$\rho \circ \tau$
$\boldsymbol{\tau}$	τ	$\rho^2 \circ \tau$	$\rho \circ \tau$	e	ρ^2	ρ
$\boldsymbol{\rho \circ \tau}$	$\rho \circ \tau$	τ	$\rho^2 \circ \tau$	ρ	e	ρ^2
$\boldsymbol{\rho^2 \circ \tau}$	$\rho^2 \circ \tau$	$\rho \circ \tau$	τ	ρ^2	ρ	e

Example 1.6.18. Consider an square and all of the symmetries of the square; that is, all ways we can move the square that cause it to end up in the exact same spot. There are 8 such symmetries that we can visualize as follows where we have numbered the vertices just to emphasize the way in which we moved the square:



Note each of these symmetries corresponds to a unique permutation in S_4 by labelling the vertices of the square. However, since $|S_4| = 4! = 24$ whereas

there are only 8 symmetries, not all permutations in S_4 are symmetries of the square. Since it is easy to see that the composition of symmetries is a symmetry, since the identity permutation is a symmetry, and since all symmetries are reversible and thus invertible, the collection of symmetries on the square is a subgroup of S_4 which we will denoted by D_4.

Note there is a way to present these symmetries. First we can let ρ be the rotation by $\frac{\pi}{2}$ radians counter-clockwise; that is

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

(this is because 1 is going to the second spot on the square, 2 is going to the third spot on the square, 3 is going to the fourth spot on the square, and 4 is going to the first spot on the square). It is then not difficult to see that

$$\rho^2 = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

is the rotation by $\frac{2\pi}{2}$ radians counter-clockwise,

$$\rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

is the rotation by $\frac{3\pi}{2}$ radians counter-clockwise, and ρ^4 is the rotation by $\frac{4\pi}{2}$ radians counter-clockwise and thus $\rho^4 = e$. Next let τ be the horizontal reflection; that is

$$\tau = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}.$$

It is not difficult to see that the reflection across the diagonal $(1, 3)$ can be realized by applying the horizontal reflection followed by a rotation by $\frac{\pi}{2}$ radians counter-clockwise (i.e. $\rho \circ \tau$), the vertical reflection can be realized by applying the horizontal reflection followed by a rotation by $\frac{2\pi}{2}$ radians counter-clockwise (i.e. $\rho^2 \circ \tau$), and the reflection across the diagonal $(2, 4)$ can be realized by applying the horizontal reflection followed by a rotation by $\frac{3\pi}{2}$ radians counter-clockwise (i.e. $\rho^3 \circ \tau$). Thus we can write

$$D_4 = \{e, \rho, \rho^2, \rho^3, \tau, \rho \circ \tau, \rho^2 \circ \tau, \rho^3 \circ \tau\}.$$

Using this way of presenting D_4, we must ask how do we multiply group elements in this form? We already know that $\rho^4 = e$ so we know how to multiple elements of the form ρ^k. Next we note that $\tau^2 = e$ since if we do a horizontal reflection twice we end up back where we started. Finally, it is not difficult to see via geometric operations that $\tau \circ \rho$ is the same as the reflection across the diagonal $(2, 4)$; that is

$$\tau \circ \rho = \rho^3 \circ \tau = \rho^{-1} \circ \tau.$$

Using these rules, we can easily multiply all elements in the above presentation of D_4. In particular, we have the following multiplication table for D_4 in this presentation:

$\circ$	$\boldsymbol{e}$	$\boldsymbol{\rho}$	$\boldsymbol{\rho^2}$	$\boldsymbol{\rho^3}$	$\boldsymbol{\tau}$	$\boldsymbol{\rho \circ \tau}$	$\boldsymbol{\rho^2 \circ \tau}$	$\boldsymbol{\rho^3 \circ \tau}$
$\boldsymbol{e}$	e	ρ	ρ^2	ρ^3	τ	$\rho \circ \tau$	$\rho^2 \circ \tau$	$\rho^3 \circ \tau$
$\boldsymbol{\rho}$	ρ	ρ^2	ρ^3	e	$\rho \circ \tau$	$\rho^2 \circ \tau$	$\rho^3 \circ \tau$	τ
$\boldsymbol{\rho^2}$	ρ^2	ρ^3	e	ρ	$\rho^2 \circ \tau$	$\rho^3 \circ \tau$	τ	$\rho \circ \tau$
$\boldsymbol{\rho^3}$	ρ^3	e	ρ	ρ^2	$\rho^3 \circ \tau$	τ	$\rho \circ \tau$	$\rho^2 \circ \tau$
$\boldsymbol{\tau}$	τ	$\rho^3 \circ \tau$	$\rho^2 \circ \tau$	$\rho \circ \tau$	e	ρ^3	ρ^2	ρ
$\boldsymbol{\rho \circ \tau}$	$\rho \circ \tau$	τ	$\rho^3 \circ \tau$	$\rho^2 \circ \tau$	ρ	e	ρ^3	ρ^2
$\boldsymbol{\rho^2 \circ \tau}$	$\rho^2 \circ \tau$	$\rho \circ \tau$	τ	$\rho^3 \circ \tau$	ρ^2	ρ	e	ρ^3
$\boldsymbol{\rho^3 \circ \tau}$	$\rho^3 \circ \tau$	$\rho^2 \circ \tau$	$\rho \circ \tau$	τ	ρ^3	ρ^2	ρ	e

Generalizing the above, we obtain the following exotic subgroups of $(S_n, \circ)$.

Definition 1.6.19. For $n \geq 3$, the n^{th} *dihedral group*, denoted D_n, is the subgroup of S_n consisting of all symmetries on a regular n-gon.

Remark 1.6.20. For $n \geq 3$, one can present the dihedral group D_n as

$$D_n = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \rho \circ \tau, \ldots, \rho^{n-1} \circ \tau\}$$

where ρ is the rotation counter-clockwise by $\frac{2\pi}{n}$ radians and τ is any reflection. Moreover, the multiplication table for D_n is completely determined via $\rho^n = e$, $\rho^k \neq e$ for all $k \in \{1, \ldots, n-1\}$, $\tau^2 = e$, $\tau \neq e$, and

$$\tau \circ \rho = \rho^{n-1} \circ \tau = \rho^{-1} \circ \tau.$$

Since $|D_n| = 2n$, we see that D_n is a proper subgroup of S_n when $n \geq 4$.

Remark 1.6.21. One must be careful in the mathematics literature as sometimes the n^{th} dihedral group is denoted D_n (with the n denoting the regular n-gon the symmetries are acting on), and sometimes the n^{th} dihedral group is denoted D_{2n} (with the $2n$ denoting the number of elements in the dihedral group). Obviously we will stick with the notation we have defined.

1.6.5 Alternating Groups

There is another collection of subgroups of $(S_n, \circ)$ that by constructing will introduce us to some fascinating ideas. The construction of these subgroups is precipitated by the following type of permutation.

Definition 1.6.22. Let $n \in \mathbb{N}$. A permutation $\sigma \in S_n$ is said to be a *transposition* if σ is a 2-cycle.

Why have two names for the same thing?

Remark 1.6.23. A 2-cycle is called a transposition since for all $i, j \in \{1, \ldots, n\}$ with $i \neq j$, the 2-cycle

$$\begin{pmatrix} i & j \end{pmatrix}$$

is the permutation that interchanges i and j (i.e. sends i to j and j to i) and leaves all other elements fixed. Note that

$$\begin{pmatrix} i & j \end{pmatrix}^{-1} = \begin{pmatrix} i & j \end{pmatrix}$$

so every transposition is its own inverse.

Not only is every permutation a product of disjoint cycles, we also have that every permutation is the product of transpositions. The cost of reducing from cycles of any length to 2-cycles is that we may not have that the cycles are disjoint.

Theorem 1.6.24. *Let $n \in \mathbb{N}$ be such that $n \geq 2$. Every element in S_n is the product of 2-cycles.*

Proof. Since Theorem 1.2.46 showed that every element in S_n is a (disjoint) product of cycles, it suffices to show that every cycle can be written as a product of 2-cycles. Thus, let $\sigma \in S_n$ be an m-cycle for $m \geq 1$. To see that σ is a product of 2-cycles, we will proceed by induction on m.

Base Case: $m = 1$. In this case σ is a 1-cycle and thus $\sigma = e$. Since

$$e = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix},$$

we obtain that σ is a product of 2-cycles.

Base Case: $m = 2$. In this case σ is a 2-cycle and thus is a product of one 2-cycle.

Inductive Step. Assume that every m-cycle is a product of 2-cycles and let σ be an $(m+1)$-cycle. Thus we can write

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_m & a_{m+1} \end{pmatrix}$$

for some distinct integers $a_1, a_2, \ldots, a_m, a_{m+1}$. It is not difficult to check that

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix} \begin{pmatrix} a_m & a_{m+1} \end{pmatrix}.$$

Therefore, since

$$\begin{pmatrix} a_m & a_{m+1} \end{pmatrix}$$

is a 2-cycle, and since

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$$

is an m-cycle and thus a product of 2-cycles by the inductive hypothesis, we obtain that σ is a product of 2-cycles. Hence the inductive step is complete.

Therefore, by the Principle of Mathematical Induction, the proof is complete. ∎

In order to write a permutation as a product of 2-cycles, we need only apply the algorithm that is implicit in the proof of Theorem 1.6.24.

Example 1.6.25. In S_8, consider the permutation

$$\sigma = \begin{pmatrix} 1 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 & 8 & 4 \end{pmatrix}.$$

To write σ as a product of transpositions, we simply apply the argument in the inductive step from the proof of Theorem 1.6.24 to each cycle in σ. Indeed

$$\sigma = \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 \end{pmatrix} \begin{pmatrix} 7 & 8 \end{pmatrix} \begin{pmatrix} 8 & 4 \end{pmatrix}.$$

Using the idea that every permutation is a product of transpositions, we can describe various types of permutations.

Definition 1.6.26. A permutation $\sigma \in S_n$ is said to be *even* if σ can be written as the product of an even number of transpositions. Similarly, a permutation $\sigma \in S_n$ is said to be *odd* if σ can be written as the product of an odd number of transpositions.

Example 1.6.27. Since Example 1.6.25 showed that the permutation

$$\sigma = \begin{pmatrix} 1 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 & 8 & 4 \end{pmatrix}$$

can be written as

$$\sigma = \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7 \end{pmatrix} \begin{pmatrix} 7 & 8 \end{pmatrix} \begin{pmatrix} 8 & 4 \end{pmatrix},$$

we see that σ is an odd permutation.

Like with even and odd natural numbers, products of even and odd permutations follow the same rules for the results being even or odd. In fact, consider the following.

Remark 1.6.28. Assume σ is an even permutation so that we can write

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2k}$$

where $\tau_1, \ldots, \tau_{2k}$ are transpositions. Since $\tau_j^{-1} = \tau_j$ for all $1 \leq j \leq 2k$, we obtain that

$$\sigma^{-1} = \tau_{2k}^{-1} \circ \cdots \circ \tau_2^{-1} \circ \tau_1^{-1}.$$

Hence σ^{-1} is even.

Since the product of two even permutations is even and since

$$e = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$$

(when $n \geq 2$) so the identity element is even, the collection of even permutations forms a subgroup of the symmetric group by Definition 1.5.7. These subgroups are the focus of this subsection and thus they deserve a name.

Definition 1.6.29. Let $n \in \mathbb{N}$ be such that $n \geq 2$. The n^{th} *Alternating Group*, denoted A_n, is the subgroup of S_n consisting of the even permutations.

Remark 1.6.30. One would expect that the set of odd permutations does not form a subgroup of the symmetric group since it is easy to see that the product of two odd permutations is even and the identity element is even. However, note that it is not clear that a permutation cannot be both even and odd since there are many ways one can write a permutation as a product of transpositions. This will be our next goal: showing that a permutation cannot be both even and odd. In the process, we will also compute the order of A_n.

In order to do this, we require some more technology. To do so, we are moving a bit away from groups momentarily, but it is necessary to do so.

Definition 1.6.31. Let $n \in \mathbb{N}$ and let $\sigma \in S_n$. The *Vandermonde polynomial of* σ is the polynomial in the n variables $x_1, \ldots, x_n$ defined by $V_{n,\sigma} = \prod_{1 \leq i < j \leq n}(x_{\sigma(j)} - x_{\sigma(i)})$.

To clarify the notion of a Vandermonde polynomial of a permutation, we exhibit the following example.

Example 1.6.32. In S_3, there are $|S_3| = 6$ Vandermonde polynomials, namely:

$$\begin{aligned}
V_{3,e} &= (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) \\
V_{3,(1\ 2)} &= (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) \\
V_{3,(1\ 3)} &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\
V_{3,(2\ 3)} &= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) \\
V_{3,(1\ 2\ 3)} &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3), \text{ and} \\
V_{3,(1\ 3\ 2)} &= (x_1 - x_3)(x_1 - x_2)(x_3 - x_2)
\end{aligned}$$

Note that all of these polynomials are a product of $x_2 - x_1$, $x_3 - x_1$, and $x_3 - x_2$, or their negatives. In particular,

$$\begin{aligned}
V_{3,(1\ 2)} &= -V_{3,e} \\
V_{3,(1\ 3)} &= -V_{3,e} \\
V_{3,(2\ 3)} &= -V_{3,e} \\
V_{3,(1\ 2\ 3)} &= V_{3,e}, \text{ and} \\
V_{3,(1\ 3\ 2)} &= V_{3,e}.
\end{aligned}$$

Remark 1.6.33. Note for any $n \in \mathbb{N}$ and any $\sigma \in S_n$ that $V_{n,\sigma}$ and $V_{n,e}$ will either be equal or be negatives of each other. Thus

$$\frac{V_{n,\sigma}}{V_{n,e}} = \pm 1$$

(where we do not concern ourselves with the fact that dividing by $V_{n,e}$ doesn't make sense for certain values of $x_1, \ldots, x_n$). As this quantity is important, we provide it a name.

Definition 1.6.34. Let $n \in \mathbb{N}$ and let $\sigma \in S_n$. The *sign of* σ, denoted $\operatorname{sgn}(\sigma)$, is

$$\operatorname{sgn}(\sigma) = \frac{V_{n,\sigma}}{V_{n,e}} \in \{1, -1\}.$$

In order to show that a permutation cannot be both even and odd, and to compute the order of A_n, we require some properties of the sign of a permutation. We begin with the following.

Lemma 1.6.35. *If σ is a transposition, then* $\operatorname{sgn}(\sigma) = -1$.

Proof. Since σ is a transposition, there exists $1 \leq l < k \leq n$ such that

$$\sigma = \begin{pmatrix} k & l \end{pmatrix}.$$

Recall

$$\operatorname{sgn}(\sigma) = \frac{V_{n,\sigma}}{V_{n,e}} = \prod_{1 \leq i < j \leq n} \frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i}.$$

Hence, to compute $\operatorname{sgn}(\sigma)$, we need only analyze the terms in the above product. We divide the terms in the product into a few cases.

Case 1: $i, j \notin \{k, l\}$. In this case, we have the term

$$\frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i} = \frac{x_j - x_i}{x_j - x_i} = 1.$$

Case 2: $\{i, j\} = \{k, l\}$. In this case, since $l < k$ and $i < j$, we have $i = l$ and $j = k$. Thus we have the terms

$$\frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i} = \frac{x_{\sigma(k)} - x_{\sigma(l)}}{x_k - x_l} = \frac{x_l - x_k}{x_k - x_l} = -1.$$

In all other cases, we have one of i or j is k or l and the other is some element of $\{1, \ldots, n\} \setminus \{k, l\}$. We pair up the terms in the product based on the element of $\{1, \ldots, n\} \setminus \{k, l\}$.

Case 3: $(i, j) = (m, l)$ with $(i, j) = (m, k)$ for $1 \leq m < l$. In this case, we have the terms

$$\frac{x_{\sigma(k)} - x_{\sigma(m)}}{x_k - x_m} \cdot \frac{x_{\sigma(l)} - x_{\sigma(m)}}{x_l - x_m} = \frac{x_l - x_m}{x_k - x_m} \cdot \frac{x_k - x_m}{x_l - x_m} = 1.$$

Case 4: $(i, j) = (l, m)$ with $(i, j) = (k, m)$ for $k < m \leq n$. In this case, we have the terms

$$\frac{x_{\sigma(m)} - x_{\sigma(k)}}{x_m - x_k} \cdot \frac{x_{\sigma(m)} - x_{\sigma(l)}}{x_m - x_l} = \frac{x_m - x_l}{x_m - x_k} \cdot \frac{x_m - x_k}{x_m - x_l} = 1.$$

Case 5: $(i,j) = (l,m)$ with $(i,j) = (m,k)$ for $l < m < k$. In this case, we have the terms

$$\frac{x_{\sigma(k)} - x_{\sigma(m)}}{x_k - x_m} \cdot \frac{x_{\sigma(m)} - x_{\sigma(l)}}{x_m - x_l} = \frac{x_l - x_m}{x_k - x_m} \cdot \frac{x_m - x_k}{x_m - x_l} = 1.$$

Hence, we can write $\operatorname{sgn}(\sigma)$ as a product of 1s times a single -1 and thus $\operatorname{sgn}(\sigma) = -1$ as desired. ∎

Lemma 1.6.36. *Let $n \in \mathbb{N}$ and let $\sigma, \tau \in S_n$. Then*

$$\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

Proof. Note that

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \frac{V_{n,\sigma\circ\tau}}{V_{n,e}} \\
&= \frac{\prod_{1\le i<j\le n}(x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))})}{\prod_{1\le i<j\le n}(x_j - x_i)} \\
&= \frac{\prod_{1\le i<j\le n}(x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))})}{\prod_{1\le i<j\le n}(x_{\tau(j)} - x_{\tau(i)})} \frac{\prod_{1\le i<j\le n}(x_{\tau(j)} - x_{\tau(i)})}{\prod_{1\le i<j\le n}(x_j - x_i)} \\
&= \frac{\prod_{1\le i<j\le n}(x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))})}{\prod_{1\le i<j\le n}(x_{\tau(j)} - x_{\tau(i)})} \operatorname{sgn}(\tau).
\end{aligned}$$

Thus, it suffices to prove that

$$\frac{\prod_{1\le i<j\le n}(x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))})}{\prod_{1\le i<j\le n}(x_{\tau(j)} - x_{\tau(i)})} = \frac{\prod_{1\le l<k\le n}(x_{\sigma(k)} - x_{\sigma(l)})}{\prod_{1\le l<k\le n}(x_k - x_l)}.$$

Since $\tau : \{1,\dots,n\} \to \{1,\dots,n\}$ is a bijection, for all $1 \le i < j \le n$ it follows that $\tau(i), \tau(j) \in \{1,\dots,n\}$ are such that $\tau(i) < \tau(j)$ or $\tau(j) < \tau(i)$, and for all $k, l \in \{1,\dots,n\}$ with $l < k$ there exists a unique $1 \le i < j \le n$ such that $\{\tau(i), \tau(j)\} = \{k, l\}$. Moreover, if $\tau(i) = l$ and $\tau(j) = k$, then

$$\frac{x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))}}{x_{\tau(j)} - x_{\tau(i)}} = \frac{x_{\sigma(k)} - x_{\sigma(l)}}{x_k - x_l},$$

and otherwise if $\tau(i) = k$ and $\tau(j) = l$, then

$$\frac{x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))}}{x_{\tau(j)} - x_{\tau(i)}} = \frac{x_{\sigma(l)} - x_{\sigma(k)}}{x_l - x_k} = \frac{x_{\sigma(k)} - x_{\sigma(l)}}{x_k - x_l}.$$

Hence we see that

$$\frac{\prod_{1\le i<j\le n}(x_{\sigma(\tau(j))} - x_{\sigma(\tau(i))})}{\prod_{1\le i<j\le n}(x_{\tau(j)} - x_{\tau(i)})} = \frac{\prod_{1\le l<k\le n}(x_{\sigma(k)} - x_{\sigma(l)})}{\prod_{1\le l<k\le n}(x_k - x_l)}$$

thereby completing the proof. ∎

Using the above two results related to $\text{sgn}(\sigma)$, we have our proof that a permutation cannot be both even and odd, and we have the order of A_n.

Theorem 1.6.37. *Let $n \in \mathbb{N}$ and let $\sigma \in S_n$. Then*

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}.$$

Hence σ cannot be both even and odd. Moreover $|A_n| = \frac{n!}{2}$ for all $n \geq 2$.

Proof. To begin, assume $\sigma \in S_n$ is even. Hence we can write

$$\sigma = \tau_1 \circ \cdots \circ \tau_{2k}$$

where τ_i are all transpositions, and $k \in \mathbb{N}$. By Lemma 1.6.35 and Lemma 1.6.36, we have that

$$\text{sgn}(\sigma) = \sigma(\tau_1) \cdots \sigma(\tau_{2k}) = (-1)^{2k} = 1$$

as desired.

Similarly, if σ is odd, we see that $\text{sgn}(\sigma)$ will be an odd power of -1 and thus $\text{sgn}(\sigma) = -1$ as desired. Therefore, since for an arbitrary $\sigma \in S_n$ we know $\text{sgn}(\sigma)$ cannot be both 1 and -1 simultaneously, σ cannot be both even and odd.

To see that $|A_n| = \frac{n!}{2}$ when $n \geq 2$, let $O_n = S_n \setminus A_n$ be the set of odd permutations. Note we have shown that $S_n = A_n \cup O_n$ and $A_n \cap O_n = \emptyset$. Hence

$$n! = |S_n| = |A_n| + |O_n|.$$

Note if $\sigma \in A_n$ then

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma \in O_n$$

since

$$\text{sgn}\left(\begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma\right) = \text{sgn}\left(\begin{pmatrix} 1 & 2 \end{pmatrix}\right) \text{sgn}\,(\sigma) = (-1)(1) = -1.$$

Hence we can define $f : A_n \to O_n$ by

$$f(\sigma) = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma$$

for all $\sigma \in A_n$. Similarly, if $\sigma \in O_n$ then

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma \in A_n$$

since

$$\text{sgn}\left(\begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma\right) = \text{sgn}\left(\begin{pmatrix} 1 & 2 \end{pmatrix}\right) \text{sgn}\,(\sigma) = (-1)(-1) = 1.$$

Hence we can define $g : O_n \to A_n$ by

$$g(\sigma) = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma$$

for all $\sigma \in O_n$.

Note that

$$g(f(\sigma)) = g\left(\begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma\right) = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \sigma = \sigma$$

for all $\sigma \in A_n$, and similarly $f(g(\sigma)) = \sigma$ for all $\sigma \in O_n$. Hence f is a bijection from A_n to O_n. Thus A_n and O_n have the same number of elements. Therefore, we have that

$$n! = |S_n| = |A_n| + |O_n| = 2|A_n|.$$

Hence $|A_n| = \frac{n!}{2}$ as desired. ∎

To complete this subsection, let us examine what elements are in A_n.

Example 1.6.38. Let $n \in \mathbb{N}$. Since for three distinct numbers $a, b, c \in \{1, \ldots, n\}$ we have that

$$\begin{pmatrix} a & b & c \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} b & c \end{pmatrix},$$

we see that every 3-cycle is in A_n.

Example 1.6.39. Since every 3-cycle is in A_4, we see that

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}$$

are distinct element of A_4. Moreover, since $e \in A_4$, since

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}$$

are all distinct elements of A_4 that do not agree with any of the 3-cycles, we have written down 12 distinct elements of A_4. Therefore, since $|A_4| = \frac{4!}{2} = 12$, we have written a complete list of elements of A_4.

Remark 1.6.40. Permutations and the sign of a permutation are important concepts in mathematics that appear in many contexts. For example, if $n \in \mathbb{N}$ and $A = [a_{i,j}] \in M_n$, one can show that

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)}.$$

This is known as the *permutation expansion of the determinant* and is quite useful in linear algebra.

1.6.6 Subgroups of Product Groups

To conclude our (microscopic) collection of subgroups, we will examine the subgroups of product groups and show what we mean by $(G \times H, \cdot)$ is a group that contains $(G, *)$ and $(H, \star)$.

Proposition 1.6.41. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. Let H_1 and H_2 be subgroups of G_1 and G_2 respectively. Then $H_1 \times H_2$ is a subgroup of the product group $G_1 \times G_2$.*

Proof. To see that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$, we will verify the three properties required by Definition 1.5.7.

To begin, recall if $e_1 \in G_1$ and $e_2 \in G_2$ are the identity elements, then the identity element of $G_1 \times G_2$ is (e_1, e_2). Since $H_1 \leq G_1$ and $H_2 \leq G_2$, we know that $e_1 \in H_1$ and $e_2 \in H_2$ so

$$(e_1, e_2) \in H_1 \times H_2.$$

Hence $H_1 \times H_2$ contains the identity element of $G_1 \times G_2$.

Next, to see that $H_1 \times H_2$ is closed under products, let $(a_1, b_1), (a_2, b_2) \in H_1 \times H_2$ be arbitrary. Since $a_1, a_2 \in H_1$ and since H_1 is closed under products, we know that $a_1 *_1 a_2 \in H_1$. Similarly $b_1, b_2 \in H_2$ and since H_2 is closed under products, we know that $b_1 *_2 b_2 \in H_2$. Hence

$$(a_1, b_1) * (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2) \in H_1 \times H_2.$$

Thus $H_1 \times H_2$ is closed under products.

Finally, to see that $H_1 \times H_2$ is closed under inverses, let $(a, b) \in H_1 \times H_2$ be arbitrary. Recall that the inverse of (a, b) in $G_1 \times G_2$ is (a^{-1}, b^{-1}) where a^{-1} is the inverse of a in G_1 and b^{-1} is the inverse of b in G_2. Since $a \in H_1$ and since H_1 is closed under inverses, we know that $a^{-1} \in H_1$. Similarly, since $b \in H_2$ and since H_2 is closed under inverses, we know that $b^{-1} \in H_2$. Hence

$$(a^{-1}, b^{-1}) \in H_1 \times H_2.$$

Thus $H_1 \times H_2$ is closed under inverses. Hence $H_1 \times H_2 \leq G_1 \times G_2$ by Definition 1.5.7. ∎

Remark 1.6.42. Let $(G, *)$ and $(H, \star)$ be groups. Since $G \leq G$ and $\{e_H\} \leq H$, we see that $G \times \{e_H\}$ is a subgroup of $(G \times H, \cdot)$. Note that

$$G \times \{e_H\} = \{(a, e_H) \mid a \in G\}$$

is effectively $(G, *)$ in disguise. Similarly, since $\{e_G\} \leq G$ and $H \leq G$, we see that

$$\{e_G\} \times H = \{(e_G, b) \mid b \in H\}$$

is a subgroup of $(G \times H, \cdot)$ that is effectively H. Thus $(G \times H, \cdot)$ is group that 'contains' both $(G, *)$ and $(H, \star)$.

Example 1.6.43. Note that not every subgroup of a product group $(G_1 \times G_2, \cdot)$ is of the form $H_1 \times H_2$. To see this, consider the Klein 4-group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ and let

$$H = \{([0],[0]),([1],[1])\}.$$

We claim that H is a subgroup of $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$. To see this, note that $([0],[0]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ so H contains the identity element. Moreover

$$\begin{aligned}
([0],[0]) \cdot ([0],[0]) &= ([0],[0]) \\
([0],[0]) \cdot ([1],[1]) &= ([0]+[1],[0]+[1]) = ([1],[1]) \\
([1],[1]) \cdot ([0],[0]) &= ([1]+[0],[1]+[0]) = ([1],[1]) \\
([1],[1]) \cdot ([1],[1]) &= ([1]+[1],[1]+[1]) = ([0],[0])
\end{aligned}$$

so $\mathbb{Z}_2 \times \mathbb{Z}_2$ is closed under products and inverses as $([0],[0])^{-1} = ([0],[0])$ and $([1],[1])^{-1} = ([1],[1])$. Hence H is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

However, H is not of the form $H_1 \times H_2$. To see this, suppose for the sake of a contradiction that $H = H_1 \times H_2$ where H_1 and H_2 are subgroups of $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$. Note $2 = |H_1 \times H_2| = |H_1||H_2|$. Therefore $|H_1| = 2$ and $|H_2| = 1$ or $|H_1| = 1$ and $|H_2| = 2$. However, since $H_1, H_2 \subseteq \mathbb{Z}_2$ and since $\mathbb{Z}_2$ has two elements, either $H_1 = \{e\}$ and $H_2 = \mathbb{Z}_2$, or $H_1 = \mathbb{Z}_2$ and $H_2 = \{e\}$. This means

$$H_1 \times H_2 = \{([0],[0]),([0],[1])\} \quad \text{or} \quad H_1 \times H_2 = \{([0],[0]),([1],[0])\},$$

neither of which is H thereby yielding a contradiction. Hence H is not of the form $H_1 \times H_2$.

1.7 Cyclic Groups

To complete this chapter, we desire to look at some specific types of groups and subgroups that are useful in a wide variety of situations in this course. Moreover, by developing this theory, we will obtain a further understanding of how multiplication affects group elements.

1.7.1 Definitions

To begin, we desire to generalize some technology that was used in the proof of Theorem 1.2.46 when examining the symmetric groups.

Definition 1.7.1. Let $(G, *)$ be a group and let $a \in G$. For $n \in \mathbb{N}$, we define the n^{th} *power of* a, denoted a^n, to be the product of a with itself n times; that is $a^n = a * a * \cdots * a$ where a occurs n times. Similarly, for $n \in \mathbb{N}$, we define the *negative* n^{th} *power of* a, denoted a^{-n}, to be the product of a^{-1} with itself n times. Finally, we denote $a^0 = e$.

Remark 1.7.2. Again, it is important to remember that in groups like $(\mathbb{Z}, +)$ where the group operation is addition, a^n actually means that we should add a to itself n times, not multiply since addition is the group operation. In fact, sometimes when dealing with such groups, mathematicians use na instead of a^n. However, we will avoid this in order to keep consistent notation.

Remark 1.7.3. For any group $(G, *)$, for any $a \in G$, and for any $n, m \in \mathbb{Z}$, it is not difficult to verify that $a^{m+n} = a^m * a^n$. Indeed, if $m, n \geq 0$ or $n, m \leq 0$, this follows trivially from the definition. In the cases that $m \leq 0 \leq n$ and $n \leq 0 \leq m$, the equation will follow as $a^{-1} * a = e = a * a^{-1}$.

Moreover, since

$$a^{-n} * a^n = a^{-n+n} = a^0 = e = a^n * a^{-n},$$

we see that $(a^n)^{-1} = a^{-n}$. Hence for all $m, n \in \mathbb{Z}$, we have when $n \geq 0$ that

$$(a^m)^n = a^m * a^m * \cdots * a^m = a^{m+m+\cdots+m} = a^{mn}$$

(where there are n copes of a^m and n copies of m), and we have when $n < 0$ that

$$\begin{aligned}(a^m)^n &= (a^m)^{-1} * (a^m)^{-1} * \cdots * (a^m)^{-1} \\ &= a^{-m} * a^{-m} * \cdots * a^{-m} \\ &= a^{(-m)+(-m)+\cdots+(-m)} \\ &= a^{mn}\end{aligned}$$

(where there are $|n|$ copes of $(a^m)^{-1}$ and $|n|$ copies of $-m$). Hence our usual rules for exponentiating real numbers hold in any group $(G, *)$.

Using the powers of group elements, we can construct examples of subgroups of a very specific form.

Definition 1.7.4. Let $(G, *)$ be a group and let $a \in G$. The *cyclic subgroup generated by* a, denoted $\langle a \rangle$, is the subgroup

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Of course, we should check that the cyclic subgroup generated by a is actually a subgroup. Moreover, it turns out that $\langle a \rangle$ has some other properties.

Theorem 1.7.5. *Let $(G, *)$ be a group and let $a \in G$. The cyclic subgroup generated by a is an abelian subgroup of G. Moreover, $\langle a \rangle$ is the smallest (under inclusion) subgroup of G containing a.*

Proof. To see that $\langle a \rangle$, first note that $e = a^0 \in \langle a \rangle$. Hence $\langle a \rangle$ contains the identity element.

To see that $\langle a \rangle$ is closed under products, let $b, c \in \langle a \rangle$ be arbitrary. Thus there exists $n, m \in \mathbb{Z}$ such that $b = a^m$ and $c = a^n$. Hence

$$b * c = a^m * a^n = a^{m+n} \in \langle a \rangle.$$

Thus $\langle a \rangle$ is closed under products.

Finally, to see that $\langle a \rangle$ is closed under inverses, let $b \in \langle a \rangle$ be arbitrary. Thus there exists an $n \in \mathbb{Z}$ such that $b = a^n$. Hence $b^{-1} = a^{-n} \in \langle a \rangle$. Therefore $\langle a \rangle$ is closed under inverses. Hence $\langle a \rangle$ is a group by Definition 1.5.7.

To see that $\langle a \rangle$ is abelian, note for all $n, m \in \mathbb{Z}$ that

$$a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m.$$

Hence $\langle a \rangle$ is abelian.

To see that $\langle a \rangle$ is the smallest (under inclusion) subgroup of G containing a, let $H \leq G$ be such that $a \in H$. We claim that $\langle a \rangle \subseteq H$. To see this, note $a^0 = e \in H$ since H is a subgroup of G. Moreover, since $a \in H$ and since H is closed under products, we see that $a^n \in H$ for all $n \in \mathbb{N}$. Finally, since $a \in H$ and since H is closed under inverses, we see that $a^{-1} \in H$. Therefore, since H is closed under products, we obtain that $a^{-n} \in H$ for all $n \in \mathbb{N}$. Hence $\langle a \rangle \subseteq H$ as desired. ∎

Before we explicitly write down some examples of cyclic subgroups, we introduce some terminology that will be used throughout the course.

Definition 1.7.6. Let $(G, *)$ be a group and let $a \in G$. The *order of* a is $|a| = |\langle a \rangle|$.

We will see just how important of a tool the order of a group element is later in the course.

Definition 1.7.7. A group $(G, *)$ is said to be a *cyclic group* if there exists an element $a \in G$ such that $G = \langle a \rangle$. Any element $a \in G$ such that $G = \langle a \rangle$ is called a *generator of* G.

Remark 1.7.8. Since for any group $(G, *)$ and any element $a \in G$ we know that $\langle a \rangle$ is abelian, a group can only be cyclic if it is abelian. We will see examples of abelian groups that are not cyclic shortly.

1.7.2 Examples

In this subsection, we will examine some examples of cyclic subgroups and the order of elements of a group. For our first example, we begin with the most obvious but most boring cyclic subgroup.

Example 1.7.9. In any group $(G, *)$, it is elementary to see that $\langle e \rangle = \{e\}$ since $e^n = e$ for all $n \in \mathbb{N}$ and $e^{-1} = e$. Hence $|e| = 1$.

For something a little more illuminating, consider the following examples.

Example 1.7.10. In $(\mathbb{R} \setminus \{0\}, \times)$, we see that

$$\begin{aligned}\langle 2 \rangle &= \{2^n \mid n \in \mathbb{Z}\} \\ &= \left\{1, 2, \frac{1}{2}, 4, \frac{1}{4}, 8, \frac{1}{8}, \ldots\right\}.\end{aligned}$$

Thus $|2| = \infty$.

Unsurprisingly, some of the groups (respectively subgroups) we previously saw are cyclic groups (respectively subgroups).

Example 1.7.11. In $(\mathbb{Z}, +)$ it is elementary to see that $\langle 1 \rangle = \mathbb{Z}$. Hence $|1| = \infty$ and $(\mathbb{Z}, +)$ is a cyclic group.

Example 1.7.12. In $(\mathbb{Z}, +)$ it is elementary to see for all $n \in \mathbb{Z}$ that $\langle n \rangle = n\mathbb{Z}$. Hence $|n| = \infty$ for all $n \in \mathbb{Z}$ and all the subgroups $n\mathbb{Z}$ in $(\mathbb{Z}, +)$ are cyclic subgroups.

Example 1.7.13. In $(\mathbb{Z}_n, +)$ it is elementary to see that $\langle [1] \rangle = \mathbb{Z}_n$. Hence $|[1]| = n$ and $(\mathbb{Z}_n, +)$ is cyclic.

The following example shows that not every element of $\mathbb{Z}_n$ is a cyclic generator of $(\mathbb{Z}_n, +)$.

Example 1.7.14. In $(\mathbb{Z}_6, +)$, since

$$\begin{aligned}4 + 4 &\equiv 2 \mod 6, \\ 4 + 2 &\equiv 0 \mod 6, \text{ and} \\ 4 + 0 &\equiv 4 \mod 6,\end{aligned}$$

it is not difficult to see that

$$[4]^n = \begin{cases}[0] & \text{if } n \equiv 0 \mod 3 \\ [4] & \text{if } n \equiv 1 \mod 3 \\ [2] & \text{if } n \equiv 2 \mod 3\end{cases}.$$

Hence $\langle 4 \rangle = \{[0], [2], [4]\}$ so $|4| = 3$. Similarly, it is not difficult to see that $\langle [2] \rangle = \{[0], [2], [4]\} = \langle [4] \rangle$. Note $[4]^{-1} = [2]$.

Remark 1.7.15. In any group $(G, *)$, it is not difficult to see that $\langle a^{-1} \rangle = \langle a \rangle$ by the definition of a^n for $n \in \mathbb{Z}$ and the fact that $(a^{-1})^{-1} = a$. Hence $|a^{-1}| = |a|$ for any $a \in G$.

Example 1.7.16. It is possible for a cyclic group to have multiple generators that are not related by inverses. For example, consider $(\mathbb{Z}_5, +)$. Recall $\langle [1] \rangle = \mathbb{Z}_5$. However, since

$$\begin{aligned} 2+2 &= 4 \mod 5, \\ 2+4 &= 1 \mod 5, \\ 2+1 &= 3 \mod 5, \text{ and} \\ 2+3 &= 0 \mod 5, \end{aligned}$$

we see that $\langle [2] \rangle = \mathbb{Z}_5$ so $\langle [2] \rangle = \langle [1] \rangle$ even though $[2] \neq [1]^{-1}$ in $(\mathbb{Z}_5, +)$. Note $|[2]| = 5$.

For a few more examples, we can consider the complex numbers. Note that the following along with the fact that $i^4 = 1$ motivates the results on the order of group elements in the next subsection.

Example 1.7.17. In $(\mathbb{T}, \times)$, since $i^{-1} = -i$, we can verify that

$$i^n = \begin{cases} 1 & \text{if } n \equiv 0 \mod 4 \\ i & \text{if } n \equiv 1 \mod 4 \\ -1 & \text{if } n \equiv 2 \mod 4 \\ -i & \text{if } n \equiv 3 \mod 4 \end{cases}.$$

Hence $\langle i \rangle = \{1, -1, i, -i\}$ is a cyclic group with respect $\times$ and $|i| = 4$.

Example 1.7.18. More generally, in $(\mathbb{T}, \times)$, for $n \in \mathbb{N}$, since

$$\left(e^{\frac{2\pi}{n}i}\right)^{-1} = e^{\frac{2\pi(n-1)}{n}i},$$

it is not difficult to verify that

$$\left\langle e^{\frac{2\pi}{n}i} \right\rangle = \left\{ e^{\frac{2\pi k}{n}i} \;\middle|\; k \in \{0, 1, \ldots, n-1\} \right\}.$$

Hence $\left| e^{\frac{2\pi}{n}i} \right| = n$.

To complete this subsection, we note there is a simple example of an abelian group that is not cyclic.

Example 1.7.19. The Klein four group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ is an example of an abelian group that is not cyclic. Indeed, it is not difficult to verify that

$$\begin{aligned} \langle ([0],[0]) \rangle &= \{([0],[0])\}, \\ \langle ([1],[0]) \rangle &= \{([0],[0]), ([1],[0])\}, \\ \langle ([0],[1]) \rangle &= \{([0],[0]), ([0],[1])\}, \text{ and} \\ \langle ([1],[1]) \rangle &= \{([0],[0]), ([1],[1])\}. \end{aligned}$$

Hence $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Moreover, every non-identity element of $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ has order 2. This is in stark difference to $(\mathbb{Z}_4, +)$ which is cyclic and has two elements of order 4, namely [1] and [3].

Note the above example shows that $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ must be different groups since one is cyclic and the other is not. This raises the question, "How can we tell if two groups are actually the same?" More importantly, "What does it mean for two groups to be the same?"

1.7.3 Properties

Before we begin to answer these questions, it is extremely helpful to develop some theory about how the order of group elements behave and how to compute the order of a group element. We begin with the following.

Proposition 1.7.20. *Let $(G, *)$ be a group and let $a \in G$ be such that $|a| = \infty$. If $n \in \mathbb{Z}$, then $a^n = e$ if and only if $n = 0$. Consequently, if $m, n \in \mathbb{Z}$ and $a^n = a^m$, then $n = m$.*

Proof. Clearly if $n = 0$ then $a^n = e$ by definition. To see the other direct, suppose for the sake of a contradiction that $n \in \mathbb{Z} \setminus \{0\}$ is such that $a^n = e$. Since

$$a^{-n} = (a^n)^{-1} = e^{-1} = e,$$

we see that if $k = |n|$ then $k > 0$ and $a^k = e$.

Let $m \in \mathbb{Z}$ be arbitrary. By the Division Algorithm (Theorem A.4.6), we can write $m = qk + r$ where $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, k-1\}$. Therefore

$$a^m = a^{qk+r} = (a^k)^q * a^r = e^q * a^r = e * a^r = a^r.$$

Hence

$$\langle a \rangle = \left\{ e, a, a^2, \ldots, a^{k-1} \right\}.$$

Therefore $|a| \leq k$ which contradicts the fact that $|a| = \infty$. Hence if $n \in \mathbb{Z}$, then $a^n = e$ then $n = 0$.

To see the second claim, assume $m, n \in \mathbb{Z}$ are such that $a^n = a^m$. Therefore

$$a^{n-m} = a^n * a^{-m} = a^n * (a^m)^{-1} = a^n * (a^n)^{-1} = e.$$

Therefore, by the first part of the proof, $n - m = 0$ so $n = m$ as desired. ∎

By similar arguments, we can obtain an analogous result for group elements of finite order.

Proposition 1.7.21. *Let $(G, *)$ be a group and let $a \in G$ be such that $|a| = n$. Then $a^n = e$ and $e, a, a^2, \ldots, a^{n-1}$ are distinct elements of G. Hence*

$$\langle a \rangle = \left\{ e, a, a^2, \ldots, a^{n-1} \right\}.$$

Proof. Since

$$a^0, a^1, \ldots, a^n \in \langle a \rangle$$

and since $n = |a| = |\langle a \rangle|$, there must exists $k, m \in \{0, 1, \ldots, n\}$ such that $k < m$ and $a^k = a^m$. Hence

$$a^{m-k} = a^m * a^{-k} = a^m * (a^k)^{-1} = a^m * (a^m)^{-1} = e.$$

By the same argument as used in the proof of Proposition 1.7.20, this implies that

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{m-k-1}\}.$$

This implies that $|a| \leq m - k$. However, since $k, m \in \{0, 1, \ldots, n\}$ are such that $k < m$, the only possible way that $m - k \geq |a| = n$ is that $m = n$ and $k = 0$. Thus $a^n = e$, $a^m \neq a^k$ if $m, k \in \{0, 1, \ldots, n-1\}$, and

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

as desired. ∎

Expanding on this, we can determine what powers of a group element of finite order are equal.

Corollary 1.7.22. *Let $(G, *)$ be a group and let $a \in G$ be such that $|a| = n \in \mathbb{N}$. For all $k \in \mathbb{Z}$, $a^k = e$ if and only if $n|k$. Consequently, for $m, k \in \mathbb{Z}$, $a^k = a^m$ if and only if $k \equiv m \mod n$.*

Proof. First, assume $k \in \mathbb{Z}$ is such that $n|k$. Therefore, there exists an $m \in \mathbb{Z}$ such that $mn = k$. Hence

$$a^k = a^{mn} = (a^n)^m = e^m = e$$

as desired.

Conversely, assume $k \in \mathbb{Z}$ is such that $a^k = e$. By the Division Algorithm (Theorem A.4.6), we can write $k = mn + r$ where $m \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. However, notice that

$$e = a^k = a^{mn+r} = (a^n)^m * a^r = e^m * a^r = e * a^r = a^r.$$

However, since $r \in \{0, 1, \ldots, n-1\}$ and $a^r = e$, Proposition 1.7.21 implies that $r = 0$. Hence $n|k$ as desired.

Finally, notice for $m, n \in \mathbb{Z}$ that $a^k = a^m$ if and only if $a^{k-m} = e$ if and only if $n|(k-m)$ if and only if $k \equiv m \mod n$ as desired. ∎

Using Corollary 1.7.22, we obtain another description of what the order of a group element actually is that is consistent with all examples in the previous subsection.

Corollary 1.7.23. *Let $(G, *)$ be a group and let $a \in G$ be such that $|a| < \infty$. The order of a is the least positive natural number n such that $a^n = e$.*

Proof. If $k \in \mathbb{N}$ and $n = |a|$, then Corollary 1.7.22 implies that $a^k = e$ if and only if $n|k$. Hence the order of a is the least positive natural number n such that $a^n = e$. ∎

Moreover, using Corollary 1.7.23, we can compute the order of some new group elements.

Proposition 1.7.24. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. If $(a, b) \in G_1 \times G_2$, then*

$$|(a, b)| = \text{lcm}(|a|, |b|);$$

that is, the order of (a, b) is the least common multiple of the orders of a and of b.

Proof. Let $e_1 \in G_1$ and $e_2 \in G_2$ be the identity element of $(G_1, *_1)$ and $(G_2, *_2)$. Note that

$$(a, b)^n = (e_1, e_2)$$

if and only if $a^n = e_1$ and $b^n = e_2$. Since Corollary 1.7.22 implies $a^n = e_1$ if and only if $|a|$ divides n and $b^n = e_2$ if and only if $|b|$ divides n, we see that $(a, b)^n = (e_1, e_2)$ if and only if n is a multiple of $|a|$ and $|b|$. Hence Corollary 1.7.23 implies that $|(a, b)| = \text{lcm}(|a|, |b|)$. ∎

Example 1.7.25. Let $n \in \mathbb{N}$ and consider the m-cycle

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix} \in S_n.$$

We claim that $|\sigma| = m$. To see this, note for $k \in \{1, 2, \ldots, m-1\}$ that $\sigma^k(a_m) = a_{m-k}$. Hence $\sigma^k(a_m) \neq a_m$ for all $k \in \{1, 2, \ldots, m-1\}$ and

$$\sigma^m(a_m) = \sigma(\sigma^{m-1}(a_m)) = \sigma(a_1) = a_m.$$

Hence m is the first least natural number such that $\sigma^m(a_m) = a_m$. Hence $|\sigma| \geq m$. Moreover, it is elementary to show that $\sigma^m(a_k) = a_k$ for all $k \in \{1, \ldots, m\}$ by similar arguments (i.e. for a_k we apply σ exactly $k-1$ times to get to a_1, apply σ again to get to a_m, and then apply σ another $m-k$ times to get back to a_k). Hence $\sigma^m = e$ so $|\sigma| = m$ as claimed.

Expanding on this, we can compute the order of any element of $(S_n, \circ)$ based on its cycle decomposition.

Proposition 1.7.26. *For $n \in \mathbb{N}$, if $\sigma \in S_n$ and*

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_m$$

is a decomposition of σ into a product of disjoint cycles, then the order of σ is the least common multiple of the orders of the σ_k for $k \in \{1, \ldots, m\}$.

Proof. Since Lemma 1.2.47 demonstrated that disjoint cycles commute with each other, we see that

$$\sigma^n = \sigma_1^n \circ \sigma_2^n \circ \cdots \circ \sigma_m^n$$

for all $n \in \mathbb{N}$. Moreover, since $\sigma_1, \sigma_2, \ldots, \sigma_m$ are disjoint, we can see that

$$\sigma_1^n \circ \sigma_2^n \circ \cdots \circ \sigma_m^n = e$$

if and only if $\sigma_k^n = e$ for all $k \in \{1, \ldots, n\}$ (i.e. if j appears in the cycle σ_k, it does not appear in σ_ℓ for any $\ell \neq j$ and thus $\sigma^n(j) = \sigma_k^n(j)$ so $\sigma^n(j) = j$ if and only if $\sigma_k^n(j) = j$). Hence, by the same argument used in the proof of Proposition 1.7.24, it follows that the order of σ is the least common multiple of the orders of the σ_k for $k \in \{1, \ldots, m\}$. ∎

Remark 1.7.27. Given a group $(G, *)$ and elements $a, b \in G$, it need not be true that $|a * b| = \text{lcm}(|a|, |b|)$ even when $a * b = b * a$. To see this, consider the group $(\mathbb{Z}_4, +)$ and let $a = b = [1]$. Then $|a| = |b| = 4$. However $a + b = [2]$ and $|[2]| = 2$ since $[2]^2 = [2] + [2] = [4] = [0]$.

To conclude this chapter, we can easily describe all of the subgroups of cyclic groups.

Proposition 1.7.28. *Let $(G, *)$ be a cyclic group. Every subgroup of G is cyclic.*

Proof. Let $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$ so H is cyclic. Hence we can assume that $H \neq \{e\}$.

Since $(G, *)$ is a cyclic group, there exists an $a \in G$ such that $G = \langle a \rangle$. Since $H \subseteq G$, since $H \neq \{e\}$, and since $G = \langle a \rangle$, there exists an $m \in \mathbb{Z} \setminus \{0\}$ such that $a^m \in H$. Moreover, since $H \leq G$ so $a^{-m} = (a^m)^{-1} \in H$, there exists a $k \in \mathbb{N}$ such that $a^k \in H$.

Let

$$n = \min\{k \in \mathbb{N} \mid a^k \in H\}.$$

We claim that $H = \langle a^n \rangle$. To see this, recall from Theorem 1.7.5 that $\langle a^n \rangle$ is the smallest subgroup of $(G, *)$ that contains a^n. Therefore, since $a^n \in H$ and $H \leq G$, we have that $\langle a^n \rangle \subseteq H$.

To see the other inclusion, suppose for the sake of a contradiction that $H \not\subseteq \langle a^n \rangle$. Hence, since $H \subseteq G$ and $G = \langle a \rangle$, there exists an $\ell \in \mathbb{Z}$ such that $a^\ell \in H \setminus \langle a^n \rangle$. Since $a^{nm} = (a^n)^m \in \langle a^n \rangle$ for all $m \in \mathbb{Z}$, it follows that $\ell \neq nm$ for all $m \in \mathbb{Z}$. Hence ℓ is not a multiple of n and thus

$$1 \leq r = \gcd(\ell, n) < n.$$

By the Euclidean Algorithm (Theorem A.6.8), there exists $s, t \in \mathbb{Z}$ such that $s\ell + tn = r$. Therefore, since $H \leq G$ and since $a^n, a^\ell \in H$, we have that

$$a^r = a^{s\ell + tn} = (a^\ell)^s * (a^n)^t \in H.$$

However, since $r < n$, this contradicts the definition of n. Hence we have our contradiction so $H = \langle a^n \rangle$. Therefore H is cyclic as desired. ∎

Corollary 1.7.29. *The subgroups of* $(\mathbb{Z}, +)$ *are* $n\mathbb{Z}$ *for* $n \in \mathbb{N} \cup \{0\}$.

Proof. Since $(\mathbb{Z}, +)$ is cyclic by Example 1.7.11, Proposition 1.7.28 implies that every subgroup of $(\mathbb{Z}, +)$ is cyclic. Hence we just need to compute the cyclic subgroups of $(\mathbb{Z}, +)$.

Note $\langle n \rangle = n\mathbb{Z}$ for all $n \in \mathbb{N} \cup \{0\}$. Moreover, if $n \in \mathbb{N}$ then $\langle n \rangle = \langle -n \rangle = (-n)\mathbb{Z}$. Hence the cyclic subgroups of $(\mathbb{Z}, +)$ are $n\mathbb{Z}$ for $n \in \mathbb{N} \cup \{0\}$ ∎

Chapter 2

Groups: Basic Theory

When developing examples of groups in the previous section, we saw that even though $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ are both groups with 4 elements, they must be different groups since one is cyclic and the other is not. On the other side, we saw that $(Q_8, \times)$ could be constructed in two different ways: one involving a generalization of the complex numbers (Example 1.2.29), and one involving invertible matrices (Example 1.6.15). This raises the questions, "How can we tell if two groups are really the same group in disguise?" More interesting, "Given a natural number n, how many 'distinct' groups of order n are there?"

This chapter will being to answer these questions. In particular, we will develop the notion of what it means for two groups to be the 'same', produce several methods for determining whether or not two groups are the 'same', and determine the number of 'distinct' groups of order n there are for various values in n. In doing so, students are introduced to several algebraic concepts that are used in future courses and throughout the mathematical discipline of Algebra.

2.1 Group Homomorphisms

To begin our study, we will be taking a page out of linear algebra. When dealing with abstract vector spaces, to determine when two vector spaces are the 'same', one first looks at the concept of linear maps. Linear maps are the morphisms between vector spaces; that is, the maps that preserve the vector space structure. This is a common theme in Algebra; if given an algebraic structure, the morphisms are the maps that preserve that structure. In group theory, the algebraic structure we want to preserve is the multiplication. Consequently, we make the following definition.

Definition 2.1.1. Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. A *homomorphism*

from G_1 *to* G_2 is a map $\varphi : G_1 \to G_2$ such that

$$\varphi(g *_1 h) = \varphi(g) *_2 \varphi(h)$$

for all $g, h \in G_1$.

To begin, it is helpful to have some examples of homomorphisms. Since there are a plethora of groups, there are even more examples of homomorphisms. Consequently, we present just a few useful examples.

Example 2.1.2. Let $(G, *)$ be a group and let $a \in G$. Define $\varphi : \mathbb{Z} \to G$ by

$$\varphi(n) = a^n$$

for all $n \in \mathbb{Z}$. We claim that φ is a homomorphism from $(\mathbb{Z}, +)$ to $(G, *)$. To see this, note for all $n, m \in \mathbb{Z}$ that

$$\varphi(n + m) = a^{n+m} = a^n * a^m = \varphi(n) * \varphi(m).$$

Hence φ is a homomorphism by definition.

Example 2.1.3. Define $\varphi : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ by

$$\varphi(x) = e^x$$

for all $x \in \mathbb{R}$. We claim that φ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}\setminus\{0\}, \times)$. To see this, note for all $x, y \in \mathbb{R}$ that

$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x) \times \varphi(y).$$

Hence φ is a homomorphism by definition.

Example 2.1.4. Define $\varphi : \mathbb{R} \to \mathbb{T}$ by

$$\varphi(x) = e^{ix}$$

for all $x \in \mathbb{R}$. We claim that φ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{T}, \times)$. To see this, note for all $x, y \in \mathbb{R}$ that

$$\varphi(x + y) = e^{i(x+y)} = e^{ix} e^{iy} = \varphi(x) \times \varphi(y).$$

Hence φ is a homomorphism by definition.

Example 2.1.5. Let $n \in \mathbb{N}$. Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ by

$$\varphi(k) = [k]$$

for all $k \in \mathbb{Z}$ (recall $[k]$ is the equivalence class of k in $\mathbb{Z}_n$; thus $\varphi(k) = k \mod n$). We claim that φ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$. To see this, note for all $m, k \in \mathbb{Z}$ that

$$\varphi(m + k) = [m + k] = [m] + [k] = \varphi(m) + \varphi(k)$$

Hence φ is a homomorphism by definition.

Note in all of the above examples, one really should verify that $\varphi(a) \in G_2$ for all $a \in G_1$ to ensure that $\varphi : G_1 \to G_2$ is well-defined; that is, it doesn't make sense to define a function from G_1 to G_2 unless every element of G_1 maps to an element of G_2. Moreover, if elements of G_1 can be represented in multiple ways, it is necessary to make sure that the definition of φ does depend on how we represent the elements of G_1. The best example of this is the following.

Example 2.1.6. Let $n \in \mathbb{N}$. Define $\varphi : \mathbb{Z}_n \to \langle e^{\frac{2\pi}{n}i} \rangle$ by

$$\varphi([k]) = e^{\frac{2\pi k}{n}i}$$

for all $k \in \mathbb{Z}$. Note we must check that φ is well-defined as there are multiple ways to write the same element of $\mathbb{Z}_n$; that is, if $k_1, k_2 \in \mathbb{Z}$ are such that $[k_1] = [k_2]$, we better make sure that

$$\varphi([k_1]) = e^{\frac{2\pi k_1}{n}i} \stackrel{?}{=} e^{\frac{2\pi k_2}{n}i} = \varphi([k_2])$$

for otherwise we have defined $\varphi([k_1])$ in two different ways and functions are not allowed to take two different values at the same point!

To see that φ is well-defined, let $k_1, k_2 \in \mathbb{Z}$ be such that $[k_1] = [k_2]$. Hence $k_1 \equiv k_2 \mod n$ so there exists an $m \in \mathbb{Z}$ such that $k_1 = k_2 + mn$. Thus

$$\begin{aligned} e^{\frac{2\pi k_1}{n}i} &= e^{\frac{2\pi(k_2+mn)}{n}i} \\ &= e^{\frac{2\pi k_2}{n}i} e^{\frac{2\pi mn}{n}i} \\ &= e^{\frac{2\pi k_2}{n}i} e^{2\pi mi} \\ &= e^{\frac{2\pi k_2}{n}i} 1 \\ &= e^{\frac{2\pi k_2}{n}i}. \end{aligned}$$

Therefore, since $k_1, k_2 \in \mathbb{Z}$ with $[k_1] = [k_2]$ were arbitrary, φ is well-defined.

We claim that φ is a homomorphism from $(\mathbb{Z}_n, +)$ to $\langle e^{\frac{2\pi}{n}i} \rangle$. To see this, note for all $m, k \in \mathbb{Z}$ that

$$\varphi([m] + [k]) = \varphi([m + k]) = e^{\frac{2\pi(m+k)}{n}i} = e^{\frac{2\pi m}{n}i} e^{\frac{2\pi k}{n}i} = \varphi([m]) \times \varphi([k]).$$

Hence φ is a homomorphism by definition.

Remark 2.1.7. Note when proving φ is a homomorphism in Example 2.1.6 that we made extensive use of the fact that φ was well-defined; that is, it did not matter which representative of the equivalence class we used. If instead we try to avoid the well-defined issue by setting $\varphi([k]) = e^{\frac{2\pi k}{n}i}$ for $k \in \{0, 1, \ldots, n-1\}$, then whenever we needed to apply φ, we would first

need to reduce to one of these equivalence class. Thus, when computing $\varphi([m+k])$, even when $m, k \in \{0, 1, \ldots, n-1\}$, we would not have know that $m+k \in \{0, 1, \ldots, n-1\}$ and we would need to reduce $m+k$ modulo n. This may have required case work and, at the bare minimum, would require the same computation that we used to show that our definition of φ was well-defined.

It turns we made use of a homomorphism in Subsection 1.6.5 to check properties of the Alternating groups.

Example 2.1.8. Let $n \in \mathbb{N}$. Define $\varphi : S_n \to \{\pm 1\}$ by

$$\varphi(\sigma) = \text{sgn}(\sigma)$$

for all $\sigma \in S_n$. We claim that φ is a homomorphism from $(S_n, \circ)$ to $(\pm 1, \times)$. To see this, note by Lemma 1.6.36 for all $\sigma, \tau \in S_n$ we have that

$$\varphi(\sigma \circ \tau) = \text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = \varphi(\sigma)\varphi(\tau).$$

Hence φ is a homomorphism by definition.

There are also plenty of homomorphisms related to matrix algebras.

Example 2.1.9. Let $n \in \mathbb{N}$. Define $\varphi : GL_n \to \mathbb{R} \setminus \{0\}$ by

$$\varphi(A) = \det(A)$$

for all $A \in GL_n$. We claim that φ is a homomorphism from $(GL_n, \times)$ to $(\mathbb{R} \setminus \{0\}, \times)$. To see this, note for all $A, B \in GL_n$ that

$$\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B).$$

Hence φ is a homomorphism by definition.

Example 2.1.10. Let $n \in \mathbb{N}$ and let $V \in GL_n$. Define $\varphi : GL_n \to GL_n$ by

$$\varphi(A) = V^{-1}AV$$

for all $A \in GL_n$. Note that φ does indeed map into GL_n since the inverse and product of elements of GL_n are elements of GL_n since $(GL_n, \times)$ is a group. (This step was to ensure that φ as listed had the correct co-domain; we didn't do this in the previous examples as it was 'obvious').

We claim that φ is a homomorphism from $(GL_n, \times)$ to $(GL_n, \times)$. To see this, note for all $A, B \in GL_n$ that

$$\varphi(AB) = V^{-1}ABV = V^{-1}AVV^{-1}BV = (V^{-1}AV)(V^{-1}BV) = \varphi(A)\varphi(B).$$

Hence φ is a homomorphism by definition.

Now that we have a few examples of homomorphisms, let us analyze the common properties of homomorphisms and how group elements and subgroups behave under homomorphisms. Also, recall for a function $f : X \to Y$ and a subset $B \subseteq Y$, $f^{-1}(B)$ denotes the preimage of B under f; that is, the set $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. This DOES NOT mean f is invertible as a function.

Theorem 2.1.11. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and let $\varphi : G_1 \to G_2$ be a homomorphism.*

(I) If e is the identity element of G_1, then $\varphi(e)$ is the identity element of G_2.

(II) If $a \in G_1$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(III) If $a \in G_1$ and $n \in \mathbb{N}$, then $\varphi(a^n) = \varphi(a)^n$.

(IV) If $a \in G_1$, then $|\varphi(a)|$ divides $|a|$.

(V) If $H_1 \leq G_1$, then

$$\varphi(H_1) = \{\varphi(h) \mid h \in H_1\}$$

is a subgroup of G_2.

(VI) If $H_2 \leq G_2$, then

$$\varphi^{-1}(H_2) = \{h \in G_1 \mid \varphi(h) \in H_2\}$$

is a subgroup of G_1.

Proof. Let e_2 denote the identity element of $(G_2, *)$.

To see that (I) is true, note since $(G_1, *_1)$ is a group and φ is a homomorphism that

$$\varphi(e) = \varphi(e *_1 e) = \varphi(e) *_2 \varphi(e).$$

Hence, by Corollary 1.3.6, we obtain that

$$\varphi(e) = \varphi(e)^{-1} *_2 \varphi(e) = e_2$$

as desired.

To see that (II) is true, let $a \in G_1$ be arbitrary. Then

$$\varphi(a^{-1}) *_2 \varphi(a) = \varphi(a^{-1} *_1 a) = \varphi(e) = e_2.$$

Hence Corollary 1.3.9 implies that $\varphi(a^{-1}) = \varphi(a)^{-1}$.

To see that (III) is true, we appeal to the Principle of Mathematical Induction. Clearly the base case $n = 1$ holds. To see that the result holds for $n \geq 2$, suppose the result holds for $n - 1$. Therefore

$$\varphi(a^n) = \varphi(a^{n-1} *_1 a) = \varphi(a^{n-1}) *_2 \varphi(a) = \varphi(a)^{n-1} *_2 \varphi(a) = \varphi(a)^n$$

as desired. Hence (III) follows by the Principle of Mathematical Induction.

To see that (IV) is true, let $a \in G_1$ and let $n = |a|$. Then $a^n = e$ so

$$\varphi(a)^n = \varphi(a^n) = \varphi(e) = e_2$$

by (III) and (I). Hence, Corollary 1.7.22 implies that $|\varphi(a)|$ divides $|a|$.

To see that (V) is true, let $H_1 \leq G_1$. To see that $\varphi(H_1) \leq G_2$, note $e_2 = \varphi(e) \in H_1$ by (I). Hence $\varphi(H_1)$ contains the identity of $(G_2, *_2)$.

To see that $\varphi(H_1)$ is closed under products, let $x, y \in \varphi(H_1)$ be arbitrary. Therefore there exists $a, b \in H_1$ such that $x = \varphi(a)$ and $y = \varphi(b)$. However, since $a *_1 b \in H_1$ as $H_1 \leq G_1$, we see that

$$x *_2 y = \varphi(a) *_2 \varphi(b) = \varphi(a *_1 b) \in \varphi(H_1).$$

Therefore, since $x, y \in \varphi(H_1)$ were arbitrary, $\varphi(H_1)$ is closed under products.

Finally, to see that $\varphi(H_1)$ is closed under inverses, let $x \in \varphi(H_1)$. Therefore there exists an $a \in H_1$ such that $x = \varphi(a)$. However, since $H_1 \leq G_1$, $a^{-1} \in H_1$ so

$$x^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H_1)$$

by (II). Therefore, since $x \in \varphi(H_1)$ was arbitrary, $\varphi(H_1)$ is closed under inverses. Hence $\varphi(H_1) \leq G_2$.

Finally, to see that (VI) is true, let $H_2 \leq G_2$. To see that $\varphi^{-1}(H_2) \leq G_1$ note that $e_2 \in H_2$ and $\varphi(e) = e_2$ so $e \in \varphi^{-1}(H_2)$. Hence $\varphi^{-1}(H_2)$ contains the identity of $(G_1, *_1)$.

To see that $\varphi^{-1}(H_2)$ is closed under products, let $a, b \in \varphi^{-1}(H_2)$ be arbitrary. Hence $\varphi(a), \varphi(b) \in H_2$. Since $H_2 \leq G_2$ so H_2 is closed under products, we obtain that

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b) \in H_2.$$

Hence $a *_1 b \in \varphi^{-1}(H_2)$ by definition. Therefore, since $a, b \in \varphi^{-1}(H_2)$ were arbitrary, $\varphi^{-1}(H_2)$ is closed under products.

Finally, to see that $\varphi^{-1}(H_2)$ is closed under inverses, let $a \in \varphi^{-1}(H_2)$. Hence $\varphi(a) \in H_2$. Since $H_2 \leq G_2$ so H_2 is closed under inverses, we obtain that

$$\varphi(a^{-1}) = \varphi(a)^{-1} \in H_2$$

by (II). Hence $a^{-1} \in \varphi^{-1}(H_2)$ by definition. Therefore, since $a \in \varphi^{-1}(H_2)$ was arbitrary, $\varphi^{-1}(H_2)$ is closed under inverses. Hence $\varphi^{-1}(H_2) \leq G_1$. ∎

Recall that there are special subspaces related to a linear map. These concepts have immediate generalizations to groups and homomorphisms.

Definition 2.1.12. Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and let $\varphi : G_1 \to G_2$ be a homomorphism. The *image of* φ is

$$\text{Im}(\varphi) = \varphi(G_1) = \{\varphi(g) \mid g \in G_1\}$$

and the *kernel of* φ is

$$\ker(\varphi) = \{g \in G_1 \mid \varphi(g) = e\}$$

where e is the identity element of G_2.

Similar to how the image and kernel of a linear map are subspaces, the image and kernel of a homomorphism are subgroups as the following result demonstrates.

Corollary 2.1.13. *Let* $(G_1, *_1)$ *and* $(G_2, *_2)$ *be groups. If* $\varphi : G_1 \to G_2$ *is a homomorphism, then* $\text{Im}(\varphi) \leq G_2$ *and* $\ker(\varphi) \leq G_1$.

Proof. Since $G_1 \leq G_1$, we obtain that $\text{Im}(\varphi) = \varphi(G_1)$ is a subgroup of $(G_2, *)$ by Theorem 2.1.11 part (V). Moreover, since

$$\ker(\varphi) = \varphi^{-1}(\{e\})$$

and since $\{e\} \leq G_2$, we obtain that $\ker(\varphi) \leq G_1$ by Theorem 2.1.11 part (VI). ∎

Let us quickly look at the image and kernel of most of the homomorphisms we looked at earlier.

Example 2.1.14. For the homomorphism $\varphi : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ defined by

$$\varphi(x) = e^x$$

for all $x \in \mathbb{R}$, we see that

$$\text{Im}(\varphi) = \{x \in \mathbb{R} \mid x > 0\} \qquad \text{and} \qquad \ker(\varphi) = \{0\}.$$

Example 2.1.15. For the homomorphism $\varphi : \mathbb{R} \to \mathbb{T}$ defined by

$$\varphi(x) = e^{ix}$$

for all $x \in \mathbb{R}$, we see that

$$\text{Im}(\varphi) = \mathbb{T} \qquad \text{and} \qquad \ker(\varphi) = \{2\pi n \mid n \in \mathbb{Z}\}.$$

Example 2.1.16. Let $n \in \mathbb{N}$. For the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by

$$\varphi(k) = [k]$$

for all $k \in \mathbb{Z}$, we see that

$$\text{Im}(\varphi) = \mathbb{Z}_n \qquad \text{and} \qquad \ker(\varphi) = n\mathbb{Z}.$$

Example 2.1.17. Let $n \in \mathbb{N}$. For the homomorphism $\varphi : \mathbb{Z}_n \to \langle e^{\frac{2\pi}{n}i} \rangle$ defined by

$$\varphi([k]) = e^{\frac{2\pi k}{n}i}$$

for all $k \in \mathbb{Z}$, we see that

$$\text{Im}(\varphi) = \langle e^{\frac{2\pi}{n}i} \rangle \qquad \text{and} \qquad \ker(\varphi) = \{[0]\}.$$

Example 2.1.18. Let $n \in \mathbb{N}$. For the homomorphism $\varphi : S_n \to \{\pm 1\}$ defined by

$$\varphi(\sigma) = \text{sgn}(\sigma)$$

for all $\sigma \in S_n$, we see that

$$\text{Im}(\varphi) = \{\pm 1\} \qquad \text{and} \qquad \ker(\varphi) = A_n.$$

Example 2.1.19. Let $n \in \mathbb{N}$. For the homomorphism $\varphi : GL_n \to \mathbb{R} \setminus \{0\}$ defined by

$$\varphi(A) = \det(A)$$

for all $A \in GL_n$, we see that

$$\text{Im}(\varphi) = \mathbb{R} \setminus \{0\} \qquad \text{and} \qquad \ker(\varphi) = SL_n.$$

Example 2.1.20. Let $n \in \mathbb{N}$ and let $V \in GL_n$. For the homomorphism $\varphi : GL_n \to GL_n$ defined by

$$\varphi(A) = V^{-1}AV$$

for all $A \in GL_n$, we claim that

$$\text{Im}(\varphi) = GL_n \qquad \text{and} \qquad \ker(\varphi) = \{I_n\}.$$

To see this, define $\psi : GL_n \to GL_n$ by

$$\psi(A) = VAV^{-1}$$

for all $A \in GL_n$. Note that

$$\psi(\varphi(A)) = \psi(V^{-1}AV) = V(V^{-1}AV)V^{-1} = A$$

and

$$\varphi(\psi(A)) = \varphi(VAV^{-1}) = V^{-1}(VAV^{-1})V = A$$

for all $A \in GL_n$. Thus $\psi = \varphi^{-1}$ as functions so φ is a bijective homomorphism. The fact that $\text{Im}(\varphi) = GL_n$ and $\ker(\varphi) = \{I_n\}$ then follows from our next result, Proposition 2.2.2.

2.2 Isomorphisms

Note in Example 2.1.20 that the homomorphism constructed was bijective and thus invertible as a function. As with linear maps, there is a special name given to homomorphisms that are invertible as they are incredibly useful in the theory of groups.

Definition 2.2.1. Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. A homomorphism $\varphi : G_1 \to G_2$ is said to be an *isomorphism* if φ is bijective.

Similar to linear maps, there is a useful way to verify that a homomorphism is injective.

Proposition 2.2.2. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. A homomorphism $\varphi : G_1 \to G_2$ is an isomorphism if and only if $\mathrm{Im}(\varphi) = G_2$ and $\ker(\varphi) = \{e\}$.*

Proof. Let e_1 and e_2 denote the identity elements of G_1 and G_2 respectively.

Assume φ is an isomorphism. Hence φ is bijective and thus surjective and injective. Since φ is surjective, we obtain that $\mathrm{Im}(\varphi) = G_2$. Since Theorem 2.1.11 implies that $\varphi(e_1) = e_2$ and since φ is injective, we obtain that $\varphi(a) = e_2$ if and only if $a = e_1$ so $\ker(\varphi) = \{e_1\}$.

Conversely, assume $\mathrm{Im}(\varphi) = G_2$ and $\ker(\varphi) = \{e\}$. Since $\mathrm{Im}(\varphi) = G_2$, φ is clearly surjective. To see that φ is injective, let $a, b \in G_1$ be such that $\varphi(a) = \varphi(b)$. Hence Theorem 2.1.11 implies that

$$\varphi(a^{-1} *_1 b) = \varphi(a^{-1}) *_2 \varphi(b) = \varphi(a)^{-1} *_2 \varphi(b) = e_2.$$

Therefore $a^{-1} * b \in \ker(\varphi)$. Hence, since $\ker(\varphi) = \{e\}$, we obtain that $a^{-1} * b = e$ and thus $b = a$. Therefore, since $a, b \in G_1$ were arbitrary, φ is injective. Hence φ is bijective and thus an isomorphism. ∎

We have already seen some examples of homomorphisms that are isomorphisms.

Example 2.2.3. Let $n \in \mathbb{N}$ and let $V \in GL_n$. By Example 2.1.20 the homomorphism $\varphi : GL_n \to GL_n$ defined by

$$\varphi(A) = V^{-1}AV$$

for all $A \in GL_n$ is invertible and thus an isomorphism.

Example 2.2.4. Let $n \in \mathbb{N}$. By Example 2.1.6 and Proposition 2.2.2, the homomorphism $\varphi : \mathbb{Z}_n \to \langle e^{\frac{2\pi}{n}i} \rangle$ defined by

$$\varphi\left([k]\right) = e^{\frac{2\pi k}{n}i}$$

for all $k \in \mathbb{Z}$ is an isomorphism.

All other examples from the previous section are not isomorphisms as we demonstrated that either the image is not all of the codomain, or the kernel contains elements that are not the identity.

It turns out that isomorphisms behave well with respect to operations on functions. In particular, consider the following.

Proposition 2.2.5. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and let $\varphi : G_1 \to G_2$ be an isomorphism. Then $\varphi^{-1} : G_2 \to G_1$ is an isomorphism*

Proof. Assume $\varphi : G_1 \to G_2$ is an isomorphism. Thus φ is an invertible function with $\varphi^{-1} : G_2 \to G_1$ being bijective. Thus, to complete the proof, it suffices to show that φ^{-1} is a homomorphism.

To see that φ^{-1} is a homomorphism, let $a, b \in G_2$ be arbitrary. Let $c = \varphi^{-1}(a) \in G_1$ and $d = \varphi^{-1}(b) \in G_1$. Thus $\varphi(c) = a$ and $\varphi(d) = b$. Since φ is a homomorphism, we obtain that

$$\varphi(c *_1 d) = \varphi(c) *_2 \varphi(d) = a *_2 b$$

and thus

$$\varphi^{-1}(a *_2 b) = c *_1 d = \varphi^{-1}(a) *_2 \varphi^{-1}(b).$$

Therefore, since $a, b \in G_2$ were arbitrary, φ^{-1} is a homomorphism. ∎

Moreover, composition of isomorphisms is an isomorphism as the following general result for homomorphisms holds.

Proposition 2.2.6. *Let $(G_1, *_1)$, $(G_2, *_2)$, and $(G_3, *_3)$ be groups and let $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be homomorphisms. Then $\psi \circ \varphi : G_1 \to G_3$ is a homomorphism.*

Proof. To see that $\psi \circ \varphi$ is a homomorphism, let $a, b \in G_1$ be arbitrary. Therefore, since φ and ψ are homomorphism, we obtain that

$$\begin{aligned}(\psi \circ \varphi)(a *_1 b) &= \psi(\varphi(a *_1 b)) \\ &= \psi(\varphi(a) *_2 \varphi(b)) \\ &= \psi(\varphi(a)) *_3 \psi(\varphi(b)) \\ &= (\psi \circ \varphi)(a) *_3 (\psi \circ \varphi)(b).\end{aligned}$$

Therefore, since $a, b \in G_1$ were arbitrary, $\psi \circ \varphi$ is a homomorphism. ∎

Corollary 2.2.7. *Let $(G_1, *_1)$, $(G_2, *_2)$, and $(G_3, *_3)$ be groups and let $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be isomorphisms. Then $\psi \circ \varphi : G_1 \to G_3$ is an isomorphism*

Proof. Since the composition of bijective functions is bijective and since the composition of homomorphisms is a homomorphism by Proposition 2.2.6, the composition of isomorphisms is an isomorphism. ∎

There is a special collection of isomorphisms that will be useful in Section 5.4. This collection consists of the isomorphisms whose domain and codomain agree.

Definition 2.2.8. Let $(G, *)$ be a group. An *automorphism on* G is an isomorphism from G to itself. The set of all automorphisms on G is denoted $\text{Aut}(G)$.

Of course, we have already seen one example.

Example 2.2.9. Let $n \in \mathbb{N}$ and let $V \in GL_n$. By Example 2.2.3 the homomorphism $\varphi : GL_n \to GL_n$ defined by

$$\varphi(A) = V^{-1}AV$$

for all $A \in GL_n$ is an isomorphism and thus an automorphism.

Luckily every group has at least one automorphisms on every group.

Example 2.2.10. Let $(G, *)$ be a group. The identity map $\text{id} : G \to G$ defined by $\text{id}(a) = a$ for all $a \in G$ is clearly an automorphism.

Using the above, we immediately obtain a new way to construct groups.

Theorem 2.2.11. *Let* $(G, *)$ *be a group. Then* $(\text{Aut}(G), \circ)$ *is a group.*

Proof. First note that since the composition of automorphisms is an automorphism by Corollary 2.2.7, $\circ$ is a binary operation on $\text{Aut}(G)$. Moreover, since composition of functions is associativity, $\circ$ is associative on $\text{Aut}(G)$. Moreover, clearly id is the identity element and $\text{Aut}(G)$ is closed under inverses by Proposition 2.2.5. Hence $(\text{Aut}(G), \circ)$ is a group. ∎

In general, computing $\text{Aut}(G)$ for a group $(G, *)$ can be a difficult task. However, we will compute $\text{Aut}(G)$ for some groups $(G, *)$ much later in Section 5.4 where knowing $\text{Aut}(G)$ for some specific groups $(G, *)$ will be useful.

For now, note $(\text{Aut}(G), \circ)$ is a group for every group $(G, *)$, we can construct some very odd groups. In particular, we can consider the group $\text{Aut}(S_6)$ (which as twice the number of elements of S_6), then the group $\text{Aut}(\text{Aut}(S_6))$, then the group $\text{Aut}(\text{Aut}(\text{Aut}(S_6)))$, and so on to get some very peculiar groups.

2.3 Isomorphic Groups

Now that we have the notion of isomorphisms, we can discuss what it means for two groups to be the 'same'. After all, if $(G_1, *_1)$ and $(G_2, *_2)$ are groups that are the 'same', then they should have the same elements up

to relabelling the elements and should have the same multiplication table. Since an isomorphism $\varphi : G_1 \to G_2$ relabels the elements of G_1 to elements of G_2 in a bijective way and since isomorphism preserve multiplication, we have a simple way to determine and describe when two groups are the same!

Definition 2.3.1. Two groups $(G_1, *_1)$ and $(G_2, *_2)$ are said to be *isomorphic*, denoted $(G_1, *_1) \cong (G_2, *_2)$, if there exists an isomorphism $\varphi : G_1 \to G_2$.

For "isomorphic groups" to be a good mathematical notion of 'the same' or, more specifically, 'equal' groups, it should satisfy the properties of the generalization of 'equals' in mathematics; that is, it should be an equivalence relation.

Proposition 2.3.2. *The relation $\cong$ on a set of groups defined by $(G_1, *_1) \cong (G_2, *_2)$ if and only if G_1 and G_2 are isomorphic is an equivalence relation.*

Proof. To verify that $\cong$ is an equivalence relation, we must verify that $\cong$ is reflexive, symmetric, and transitive.

To see that $\cong$ is reflexive, let $(G, *)$ be a group. Since the identity map $\mathrm{id} : G \to G$ is an isomorphism, $(G, *) \cong (G, *)$. Thus $\cong$ is reflexive.

To see that $\cong$ is symmetric, let $(G_1, *_1)$ and $(G_2, *_2)$ be groups such that $(G_1, *_1) \cong (G_2, *_2)$. Therefore there exists an isomorphism $\varphi : G_1 \to G_2$. Hence, by Proposition 2.2.5, $\varphi^{-1} : G_2 \to G_1$ is an isomorphism so $(G_2, *_2) \cong (G_1, *_1)$. Thus $\cong$ is symmetric.

To see that $\cong$ is transitive, let $(G_1, *_1)$, $(G_2, *_2)$, and $(G_3, *_3)$ be groups such that $(G_1, *_1) \cong (G_2, *_2)$ and $(G_2, *_2) \cong (G_3, *_3)$. Therefore there exists isomorphisms $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$. Hence, by Corollary 2.2.7, $\psi \circ \varphi : G_1 \to G_3$ is an isomorphism so $(G_1, *_1) \cong (G_3, *_3)$. Thus $\cong$ is transitive.

Therefore, since $\cong$ is reflexive, symmetric, and transitive, $\cong$ is an equivalence relation. ∎

It turns out that many of the groups we have seen before are isomorphic to other groups we have seen before.

Example 2.3.3. Let $n \in \mathbb{N}$ and consider $(\mathbb{Z}_n, +)$. By Example 2.2.4 we have that $(\langle e^{\frac{2\pi}{n} i}, \times)\rangle \cong (\mathbb{Z}_n, +)$. In particular, $(\langle i \rangle, \times) \cong (\mathbb{Z}_4, +)$.

Example 2.3.4. The groups $(\mathbb{R}^2, +) = (\mathbb{R}, +) \times (\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are isomorphic. Indeed define $\varphi : \mathbb{R}^2 \to \mathbb{C}$ by

$$\varphi((a, b)) = a + bi$$

for all $(a, b) \in \mathbb{R}^2$. Clearly φ is bijective and since

$$\begin{aligned} \varphi((a, b) + (c, d)) &= \varphi((a + c, b + d)) \\ &= (a + c) + (b + d)i \\ &= (a + bi) + (c + di) \\ &= \varphi((a, b)) + \varphi((c, d)) \end{aligned}$$

for all $(a, b), (c, d) \in \mathbb{R}^2$, φ is a homomorphism by definition. Thus φ is an isomorphism so $(\mathbb{R}^2, +) \cong (\mathbb{C}, +)$

Example 2.3.5. Recall the map $\varphi : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ defined by

$$\varphi(x) = e^x$$

for all $x \in \mathbb{R}$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R} \setminus \{0\}, \times)$. Let

$$\mathbb{R}^+ = \text{Im}(\varphi) = \{y \in \mathbb{R} \mid y > 0\}.$$

Note $\mathbb{R}^+$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$ by Theorem 2.1.11. Since $\ker(\varphi) = \{0\}$, if we change the codomain of φ to be $\mathbb{R}^+$, then φ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$ so $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$.

Generalizing the above, we have the following.

Corollary 2.3.6. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and $\varphi : G_1 \to G_2$ be an injective homomorphism. Then $(G_1, *_1) \cong (\text{Im}(\varphi), *_2)$.*

We will explore how we can generalize the above to homomorphisms with non-trivial kernel in Section 2.8. For now, let us examine how product groups can be isomorphic. In particular, the following shows that if we change the order of elements in a product group, then the groups are still isomorphic.

Example 2.3.7. Let $(G_1, *_1)$ and $(G_2, *_2)$ be group. Define $\varphi : G_1 \times G_2 \to G_2 \times G_1$ by

$$\varphi((a, b)) = (b, a)$$

for all $a \in G_1$ and $b \in G_2$. Note φ is clearly bijective. To see that φ is a homomorphism, note for all $a_1, a_2 \in G_1$ and $b_1, b_2 \in G_2$ that

$$\begin{aligned}
\varphi((a_1, b_1) \cdot (a_2, b_2)) &= \varphi(a_1 *_1 a_2, b_1 *_2 b_2) \\
&= (b_1 *_2 b_2, a_1 *_1 a_2) \\
&= (b_1, a_1) \cdot (b_2, a_2) \\
&= \varphi((a_1, b_1)) \cdot \varphi((a_2, b_2)).
\end{aligned}$$

Therefore, since $a_1, a_2 \in G_1$ and $b_1, b_2 \in G_2$ were arbitrary, φ is a homomorphism by definition. Thus φ is an isomorphism so $(G_1 \times G_2, \cdot) \cong (G_2 \times G_1, \cdot)$.

Moreover, the above shows that iterated products of product groups produce isomorphic groups. In particular, we can construct the product of n groups from Definition 1.4.7 via taking the product of two groups from Definition 1.4.1 multiple times and the results will be isomorphic.

Example 2.3.8. Let $(G_1, *_1)$, $(G_2, *_2)$, and $(G_3, *_3)$ be group. Define $\varphi : (G_1 \times G_2) \times G_3 \to G_1 \times (G_2 \times G_3)$ by

$$\varphi(((a, b), c)) = (a, (b, c))$$

for all $a \in G_1$, $b \in G_2$, and $c \in G_3$. Note φ is clearly bijective. To see that φ is a homomorphism, note for all $a_1, a_2 \in G_1$, $b_1, b_2 \in G_2$, and $c_1, c_2 \in G_3$ that

$$\begin{aligned}
\varphi(((a_1, b_1), c_1) \cdot ((a_2, b_2), c_2)) &= \varphi(((a_1, b_1) \cdot (a_2, b_2), c_1 *_3 c_2)) \\
&= \varphi(((a_1 *_1 a_2, b_1 *_2 b_2), c_1 *_3 c_3)) \\
&= (a_1 *_1 a_2, (b_1 *_2 b_2, c_1 *_3 c_3)) \\
&= (a_1 *_1 a_2, (b_1, c_1) \cdot (b_2, c_2)) \\
&= (a_1, (b_1, c_1)) \cdot (a_2, (b_2, c_2)) \\
&= \varphi(((a_1, b_1), c_1)) \cdot \varphi(((a_2, b_2), c_2)).
\end{aligned}$$

Therefore, since $a_1, a_2 \in G_1$, $b_1, b_2 \in G_2$, and $c_1, c_2 \in G_3$ were arbitrary, φ is a homomorphism by definition. Thus φ is an isomorphism so

$$((G_1 \times G_2) \times G_3, \cdot) \cong (G_1 \times (G_2 \times G_3), \cdot).$$

Finally, isomorphic groups are preserved under taking products as the following result demonstrates.

Lemma 2.3.9. *Let $(G_1, *_1)$, $(G_2, *_2)$, $(G_3, *_3)$, and $(G_4, *_4)$ be group. If $(G_1, *_1) \cong (G_3, *_3)$, and $(G_2, *_2) \cong (G_4, *_4)$, then $(G_1 \times G_2, \cdot) \cong (G_3 \times G_4, \cdot)$.*

Proof. Since $(G_1, *_1) \cong (G_3, *_3)$ there exists an isomorphism $\varphi_1 : G_1 \to G_3$. Similarly, since $(G_2, *_2) \cong (G_4, *_4)$ there exists an isomorphism $\varphi_2 : G_2 \to G_4$.

Define $\varphi : G_1 \times G_2 \to G_3 \times G_4$ by

$$\varphi((a, b)) = (\varphi_1(a), \varphi_2(b))$$

for all $a \in G_1$ and $b \in G_2$. We claim that φ is a homomorphism. To see this, note for all $a, c \in G_1$ and $b, d \in G_2$ that

$$\begin{aligned}
\varphi((a, b) * (c, d)) &= \varphi((a *_1 c, b *_2 d)) \\
&= (\varphi_1(a *_1 c), \varphi_2(b *_2 d)) \\
&= (\varphi_1(a) *_3 \varphi_1(c), \varphi_2(b) *_4 \varphi_2(d)) \\
&= (\varphi_1(a), \varphi_2(b)) * (\varphi_1(c), \varphi_2(d)) \\
&= \varphi((a, b)) * \varphi((c, d)).
\end{aligned}$$

Hence φ is a group homomorphism.

Since φ_1 and φ_2 are bijective, it is elementary to verify that φ is bijective. Hence φ is an isomorphism so $(G_1 \times G_2, \cdot) \cong (G_3 \times G_4, \cdot)$ as desired. ∎

Using the concept of isomorphic groups, we can start reducing the number of groups we have by classifying all groups that are isomorphic to a fixed group. In particular, up to isomorphisms, there is only one cyclic group of every order as the following two results demonstrate.

Proposition 2.3.10. *Let $(G, *)$ be a cyclic group of infinite order. Then $(G, *) \cong (\mathbb{Z}, +)$.*

Proof. Since $(G, *)$ be a cyclic group of infinite order, there exists an $a \in G$ such that $G = \langle a \rangle$ and $|a| = \infty$. To see that $(G, *) \cong (\mathbb{Z}, +)$, define $\varphi : \mathbb{Z} \to G$ by

$$\varphi(n) = a^n$$

for all $n \in \mathbb{Z}$. Thus φ is a homomorphism from Example 2.1.2. Clearly $\text{Im}(\varphi) = \langle a \rangle = G$. Moreover, since $|a| = \infty$, we obtain that $\ker(\varphi) = \{0\}$ by Proposition 1.7.20. Hence φ is an isomorphism by Proposition 2.2.2 so $(G, *) \cong (\mathbb{Z}, +)$. ∎

Proposition 2.3.11. *Let $n \in \mathbb{N}$ and let $(G, *)$ be a cyclic group of order n. Then $(G, *) \cong (\mathbb{Z}_n, +)$.*

Proof. Since $(G, *)$ be a cyclic group of order n, there exists an $a \in G$ such that $G = \langle a \rangle$ and $|a| = n$. To see that $(G, *) \cong (\mathbb{Z}_n, +)$, define $\varphi : \mathbb{Z}_n \to G$ by

$$\varphi([k]) = a^k$$

for all $k \in \mathbb{Z}$. To see that φ is well-defined, let $k_1, k_2 \in \mathbb{Z}$ be such that $[k_1] = [k_2]$. Hence $k_1 \equiv k_2 \mod n$ so

$$\varphi([k_1]) = a^{k_1} = a^{k_2} = \varphi([k_2])$$

by Corollary 1.7.22. Therefore, since $k_1, k_2 \in \mathbb{Z}$ with $[k_1] = [k_2]$ were arbitrary, φ is well-defined.

We claim that φ is a homomorphism from $(\mathbb{Z}_n, +)$ to $(G, *)$. To see this, note for all $m, k \in \mathbb{Z}$ that

$$\varphi([m] + [k]) = \varphi([m + k]) = a^{m+k} = a^m * a^k = \varphi([m]) * \varphi([k]).$$

Hence φ is a homomorphism by definition.

Clearly $\text{Im}(\varphi) = \langle a \rangle = G$. We claim that $\ker(\varphi) = \{[0]\}$. To see this, assume $k \in \mathbb{Z}$ is such that $\varphi([k]) = e$. Thus $a^k = e$ so $n|k$ by Corollary 1.7.22. Hence $[k] = [0]$ so $\ker(\varphi) = \{[0]\}$ as desired. Hence φ is an isomorphism by Proposition 2.2.2 so $(G, *) \cong (\mathbb{Z}_n, +)$. ∎

Moreover, we can start to consider how many groups there are of order n up to isomorphisms. As there is one group of order 1, namely $\{e\}$, let's begin with groups of order 2.

Example 2.3.12. Let $(G, *)$ be a group of order 2. Thus $G = \{e, a\}$ where e is the identity element and $a \neq e$. Thus we automatically have

$$e * e = e, \quad a * e = a, \quad \text{and} \quad e * a = a.$$

We claim that $a * a = e$. To see this, suppose for the sake of a contradiction that $a * e = e$. Since $e^{-1} = e$ in any group by Proposition 1.3.2, we have that

$$e = e * e = e * e^{-1} = (a * e) * e^{-1} = a * (e * e^{-1}) = a * e = a$$

thereby contradicting the fact that $a \neq e$. Hence $a * a = e$. Thus $\langle a \rangle = G$ so $(G, *)$ is a cyclic group of order 2 and thus isomorphic to $(\mathbb{Z}_2, +)$ by Proposition 2.3.11.

To begin to determine how many groups there are of order n up to isomorphisms, it is useful to note all of the group properties that are preserved under isomorphisms. This is done in the following result.

Theorem 2.3.13. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and let $\varphi : G_1 \to G_2$ be an isomorphism. Then*

(I) G_1 and G_2 have the same number of elements,

(II) if $a \in G_1$, then $|\varphi(a)| = |a|$,

(III) G_1 has k elements of order n if and only if G_2 has k elements of order n,

(IV) G_1 is cyclic if and only if G_2 is cyclic,

(V) G_1 is abelian if and only if G_2 is abelian, and

(VI) G_1 has k (cyclic and/or abelian) subgroups of order n if and only if G_2 has k (cyclic and/or abelian) subgroups of order n.

Proof. To see that (I) is true, note since $\varphi : G_1 \to G_2$ is an isomorphism, φ is a bijection. Hence G_1 and G_2 have the same number of elements.

To see that (II) is true, let $a \in G_1$ be arbitrary and let $b = \varphi(a) \in G_2$. By part (IV) of Theorem 2.1.11, the order of b divides the order of a. However, since $\varphi^{-1} : G_2 \to G_1$ is a homomorphism and $\varphi^{-1}(b) = a$, part (IV) of Theorem 2.1.11 also implies that the order of a divides the order of b. Hence $|\varphi(a)| = |b| = |a|$ as desired.

Note (III) immediately follows from (II) as φ is bijective.

To see that (IV) is true, first assume that $(G_1, *_1)$ is cyclic. Hence there exists an $a \in G_1$ such that $G_1 = \langle a \rangle$. Therefore, since φ is an isomorphism,

$$\begin{aligned} G_2 &= \mathrm{Im}(\varphi) \\ &= \{\varphi(g) \mid g \in G_1 = \langle a \rangle\} \\ &= \{\varphi(a^n) \mid n \in \mathbb{Z}\} \\ &= \{\varphi(a)^n \mid n \in \mathbb{Z}\} \\ &= \langle \varphi(a) \rangle. \end{aligned}$$

Hence $(G_2, *_2)$ is cyclic. The fact that $(G_1, *_1)$ is cyclic when $(G_2, *_2)$ is cyclic then follows by the same argument with φ replaced with φ^{-1}. Hence (IV) is true.

To see that (V) is true, first assume that $(G_1, *_1)$ is abelian. To see that $(G_2, *_2)$ is abelian, let $a, b \in G_2$ be arbitrary. Then

$$\begin{aligned} a *_2 b &= \varphi(\varphi^{-1}(a *_2 b)) \\ &= \varphi(\varphi^{-1}(a) *_1 \varphi^{-1}(b)) \\ &= \varphi(\varphi^{-1}(b) *_1 \varphi^{-1}(a)) && \text{since } *_1 \text{ is commutative} \\ &= \varphi(\varphi^{-1}(b *_2 a)) \\ &= b *_2 a. \end{aligned}$$

Therefore, since $a, b \in G_2$ were arbitrary, $(G_2, *_2)$ is abelian. The fact that $(G_1, *_1)$ is abelian when $(G_2, *_2)$ is abelian follows by similar arguments. Hence (V) is true.

Finally, to see that (VI) is true, assume $H_1 \subseteq G_1$. Since φ is an isomorphism, parts (V) and (VI) of Theorem 2.1.11 imply that $H_1 \leq G_1$ if and only if $\varphi(H_1) \leq G_2$. Hence φ induces a bijection between the subgroups of $(G_1, *_1)$ and $(G_2, *_2)$. Moreover, when $H_1 \leq G_1$, φ produces an isomorphism from H_1 to $\varphi(H_1)$ by restricting the domain from G_1 to H_1. Therefore, since the number of elements, being cyclic, and being abelian are preserved under isomorphisms, φ induces a bijection between the subgroups of $(G_1, *_1)$ and $(G_2, *_2)$ with any combination of these properties. Thus (VI) follows. ∎

Theorem 2.3.13 can often be used to quickly show that two groups are not isomorphic either by looking at different orders, whether the groups are abelian or cyclic, orders of group elements, and/or subgroups of the groups. Here are a couple of quick examples.

Example 2.3.14. The groups $(D_3, \circ)$ and $(\mathbb{Z}_6, +)$ both have six elements, but $(D_3, \circ) \ncong (\mathbb{Z}_6, +)$ since $(D_3, \circ)$ is not abelian whereas $(\mathbb{Z}_6, +)$ is abelian.

Example 2.3.15. Although $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ are both groups of order 4, $(\mathbb{Z}_4, +) \ncong (\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$. To see this, note $(\mathbb{Z}_4, +)$ has two elements of order 4 (namely [1] and [3]) whereas $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ has no elements of order 4. Hence Theorem 2.3.13 implies that $(\mathbb{Z}_4, +) \ncong (\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$.

2.4 Cosets

To possibly determine whether two groups are isomorphic or not, Theorem 2.3.13 implies we should look at the orders of group elements and how many elements there are of each order. This raises the question, "Given an arbitrary group, what information can be obtained about the orders of group elements? In particular, what orders can occur?" Not only will this information help us

to determine whether two groups are isomorphic or not, it will be a powerful tool for us to future develop group theory.

To begin to answer these questions, we will consider an object that is motivated by the construction of $(\mathbb{Z}_n, +)$. Recall $(\mathbb{Z}_n, +)$ is constructed via the modulo n equivalence relation and the equivalence classes

$$[k] = \{m \in \mathbb{Z} \mid m \equiv k \mod n\}$$

for all $k \in \mathbb{Z}$. Note that

$$[0] = \{m \in \mathbb{Z} \mid m \equiv 0 \mod n\} = n\mathbb{Z}$$

is a subgroup of $(\mathbb{Z}, +)$ by Corollary 1.7.29. Moreover, note for all $k \in \mathbb{Z}$ that

$$\begin{aligned}[k] &= \{m \mid m \in \mathbb{Z}, m - k \equiv 0 \mod n\} \\ &= \{k + l \mid l \equiv 0 \mod n\} \\ &= \{k + l \mid l \in [0]\},\end{aligned}$$

that is, $[k]$ is obtained by adding k to each element of $[0]$ (often written as $k + [0] = k + n\mathbb{Z}$).

It turns out that the above can be extended by replacing $(\mathbb{Z}, +)$ with any group $(G, *)$ and replacing $n\mathbb{Z} \leq \mathbb{Z}$ with any subgroup $H \leq G$. To see this, we begin with the following.

Proposition 2.4.1. *Let $(G, *)$ be a group and let $H \leq G$. Consider the relation $\sim$ on G defined as follows: for $a, b \in G$, $a \sim b$ if and only if $a^{-1} * b \in H$. Then*

(I) $\sim$ is an equivalence relation, and

(II) for $a \in G$, the equivalence class of a with respect to $\sim$ is

$$[a] = \{a * h \mid h \in H\}.$$

Proof. To verify that $\sim$ is an equivalence relation, we must verify that $\sim$ is reflexive, symmetric, and transitive.

To see that $\sim$ is reflexive, let $a \in G$ be arbitrary. Since $a^{-1} * a = e \in H$ as $H \leq G$, we obtain that $a \sim a$ by definition. Thus $\sim$ is reflexive.

To see that $\sim$ is symmetric, let $a, b \in G$ be such that $a \sim b$. Hence $a^{-1} * b \in H$ by definition. However, since $H \leq G$, we obtain that

$$b * a^{-1} = (a * b^{-1})^{-1} \in H.$$

Therefore $b \sim a$ by definition. Thus $\sim$ is symmetric.

To see that $\sim$ is transitive, let $a, b, c \in G$ be such that $a \sim b$ and $b \sim c$. Hence $a^{-1} * b \in H$ and $b^{-1} * c \in H$. Therefore, since $H \leq G$, we obtain that

$$a^{-1} * c = (a^{-1} * b) * (b^{-1} * c) \in H.$$

Thus $\sim$ is transitive.

Therefore, since $\sim$ is reflexive, symmetric, and transitive, $\sim$ is an equivalence relation.

Finally, for $a \in G$, note that

$$\begin{aligned}
[a] &= \{b \in G \mid a \sim b\} \\
&= \{b \in G \mid a^{-1} * b \in H\} \\
&= \{b \in G \mid \text{there exists an } h \in H \text{ such that } a^{-1} * b = h\} \\
&= \{b \in G \mid \text{there exists an } h \in H \text{ such that } b = a * h\} \\
&= \{a * h \mid h \in H\}
\end{aligned}$$

as desired. ∎

Since not every group is abelian, there is another equivalence relation we could have considered in Proposition 2.4.1; namely $a \sim b$ if and only if $b * a^{-1} \in H$. This produces a different equivalence relation and potentially different equivalence classes. To prove that this is an equivalence relation and to compute the equivalence classes is nearly identical to the proof of Proposition 2.4.1. However, as both sets of equivalence classes are useful (with the ones from Proposition 2.4.1 being more useful), it is a good idea to given them a name.

Definition 2.4.2. Let $(G, *)$ be a group, let $H \leq G$, and let $a \in G$. The *left coset of H by a*, denoted aH, is the set

$$aH = \{a * h \mid h \in H\}.$$

Similarly, the *right coset of H by a*, denoted Ha, is the set

$$Ha = \{h * a \mid h \in H\}.$$

Unsurprisingly, the motivating example gives us our first examples of cosets.

Example 2.4.3. Let $n \in \mathbb{N}$. In $(\mathbb{Z}, +)$, let $H = n\mathbb{Z}$ so that $H \leq \mathbb{Z}$. For $a, b \in \mathbb{Z}$, note that $a^{-1} * b = b * a^{-1} \in H$ if and only if $b - a \in n\mathbb{Z}$ if and only if $n|(b-a)$. Thus the equivalence relation from Proposition 2.4.1 is 'equivalence modulo n' and produces the same cosets used to define $\mathbb{Z}_n$: $[0] = 0 + n\mathbb{Z}$, $[1] = 1 + n\mathbb{Z}$, ..., $[n-1] = (n-1) + n\mathbb{Z}$.

For a non-abelian example, consider the following.

Example 2.4.4. In $(D_3, \circ)$, let $H = \langle \tau \rangle = \{e, \tau\}$. We can verify that

$$\begin{aligned}
eH &= \{e, \tau\} & \rho H &= \{\rho, \rho \circ \tau\} \\
\rho^2 H &= \{\rho^2, \rho^2 \circ \tau\} & \tau H &= \{e, \tau\} \\
(\rho \circ \tau)H &= \{\rho, \rho \circ \tau\} & (\rho^2 \circ \tau)H &= \{\rho^2, \rho^2 \circ \tau\}
\end{aligned}$$

whereas

$$\begin{aligned} He &= \{e, \tau\} & H\rho &= \{\rho, \rho^2 \circ \tau\} \\ H\rho^2 &= \{\rho^2, \rho \circ \tau\} & H\tau &= \{e, \tau\} \\ H(\rho \circ \tau) &= \{\rho^2, \rho \circ \tau\} & H(\rho^2 \circ \tau) &= \{\rho, \rho^2 \circ \tau\}. \end{aligned}$$

Note for this specific group, left cosets of an element are often different from the right cosets of the same element.

Since cosets are equivalence classes of an equivalence relation, we immediately obtains some facts about cosets.

Corollary 2.4.5. *Let $(G, *)$ be a group, let $H \leq G$, and let $a, b \in G$. Then*

(I) $a \in aH$ *and* $a \in Ha$,

(II) $\bigcup_{c \in G} cH = \bigcup_{c \in G} Hc = G$,

(III) either $aH = bH$ *or* $aH \cap bH = \emptyset$, *and either* $Ha = Hb$ *or* $Ha \cap Hb = \emptyset$, *and*

(IV) $aH = bH$ *if and only if* $a^{-1} * b \in H$, *and* $Ha = Hb$ *if and only if* $b^{-1} * a \in H$.

Proof. This result follows immediately from facts about equivalence classes of equivalence relations (see Appendix A.3). However, we will provide a proof in the context of cosets (which is a rewriting of the general proof for this equivalence relation). We will only provide the proof for left cosets as the proof for right cosets is nearly identical.

Note since $H \leq G$ that $e \in G$ so $a = a * e \in aH$. Thus $a \in \bigcup_{c \in G} cH$ for all $a \in G$. Therefore, since $cH \subseteq G$ for all $c \in G$, we obtain that $\bigcup_{c \in G} cH = G$.

Next, to see that $aH = bH$ or $aH \cap bH = \emptyset$, assume $aH \cap bH \neq \emptyset$. Hence there exists a $c \in aH \cap bH$. Thus, with $\sim$ as in Proposition 2.4.1, $a \sim c$ and $b \sim c$. Therefore, since $\sim$ is an equivalence relation, we obtain that $a \sim b$. Therefore

$$aH = [a] = \{g \in G \mid a \sim g\} = \{g \in G \mid b \sim g\} = [b] = bH$$

as desired.

Finally, note if $a^{-1} * b \in H$ then $a \sim b$ so $aH = bH$ as above. Conversely, assume $aH = bH$. Since $a \in aH$, we obtain that $a \in bH$. Hence $a \in [b]$ so $b \sim a$. Thus $a \sim b$ so $a^{-1} * b \in H$ as desired. ∎

Cosets are essential tools in group theory. To see the power of cosets in the next section, we first need one basic fact about the number of elements in a coset. Note the following even holds when the sets have an infinite number of elements (see Example A.3.5).

Lemma 2.4.6. *Let $(G, *)$ be a group, let $H \leq G$, and let $a \in G$. Then $|aH| = |Ha| = |H|$.*

Proof. To see that $|aH| = |H|$, define $f : H \to aH$ by

$$f(h) = a * h$$

for all $h \in H$. Note that f does indeed map H into aH by the definition of aH. We claim that f is a bijection and thus $|aH| = |H|$. To see this, note f is clearly surjective by definition. Moreover, note that if $h_1, h_2 \in H$ are such that

$$a * h_1 = f(h_1) = f(h_2) = a * h_2$$

then by cancellation (Corollary 1.3.7) we obtain that $h_1 = h_2$. Hence f is a bijection so $|aH| = |H|$.

The proof that $|Ha| = |H|$ is similar. ∎

2.5 Lagrange's Theorem

With the theory of cosets in hand, we can prove our first major result of the course. Although innocent looking and simple to prove (being a simple application of results about equivalence relations), the utilization and importance of the following theory is impressive... most impressive.

Theorem 2.5.1 (Lagrange's Theorem). *Let $(G, *)$ be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$ and $\frac{|G|}{|H|}$ is the number of distinct left cosets (right cosets) of H.*

Proof. Since G is finite, Corollary 2.4.5 implies there exists an $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in G$ such that

$$G = \bigcup_{k=1}^{n} a_k H$$

and $a_i H \cap a_j H = \emptyset$ if $i \neq j$. Therefore

$$\begin{aligned} |G| &= \sum_{k=1}^{n} |a_k H| \\ &= \sum_{k=1}^{n} |H| && \text{by Lemma 2.4.6} \\ &= n|H|. \end{aligned}$$

Thus $|H|$ divides $|G|$ and $\frac{|G|}{|H|} = n$ is the number of distinct left cosets of H. The proof for right cosets is identical. ∎

Since the quantities occurring in Lagrange's Theorem (Theorem 2.5.1) will occur regularly, they are given a name and some notation.

Definition 2.5.2. Let $(G, *)$ be a group and let $H \leq G$. The *index of H in G* , denoted $[G : H]$, is the number of distinct left cosets of H in G. In particular, when G is finite,

$$[G : H] = \frac{|G|}{|H|}.$$

To begin to see the power of Lagrange's Theorem (Theorem 2.5.1), note the following immediate application of said result to obtain information about the order of group elements.

Corollary 2.5.3. *Let $(G, *)$ be a finite group and let $a \in G$. The order of a divides the order of G. Thus $a^{|G|} = e$.*

Proof. Recall $H = \langle a \rangle$ is a subgroup of G. Hence Theorem 2.5.1 implies that $|a| = |H|$ divides $|G|$. Thus Corollary 1.7.22 implies that $a^{|G|} = e$. ∎

As a specific example of Corollary 2.5.3, we obtain the following number theory result that should have been presented in MATH 1200.

Corollary 2.5.4 (Fermat's Little Theorem). *If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.*

Proof. Recall $(\mathbb{Z}_p \setminus \{[0]\}, \times)$ is a group with $p-1$ elements. To see the result, let $a \in \mathbb{Z}$ be arbitrary. If $a \equiv 0 \mod p$, then the result is trivially true. Otherwise, if $a \not\equiv 0 \mod p$ then $[a] \in \mathbb{Z}_p \setminus \{[0]\}$. Hence $[1] = [a]^{p-1} = [a^{p-1}]$ by Corollary 2.5.3. Thus $a^{p-1} \equiv 1 \mod p$ so the result holds by multiplying both sizes by a. ∎

In fact, with Corollary 2.5.3 and group theory, we can take Fermat's Little Theorem (Theorem 2.5.4) one step further to modding out by a non-prime number.

Corollary 2.5.5 (Euler's Theorem). *Let $n \geq 2$ and let $\varphi(n) = |\mathbb{Z}_n^\times|$ (see Definition 1.2.20). If $a \in \mathbb{Z}$ is such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} = 1 \mod n$.*

Proof. Recall $(\mathbb{Z}_n^\times, \times)$ is a group with $\varphi(n) = |\mathbb{Z}_n^\times|$ elements. If $a \in \mathbb{Z}$ is such that $\gcd(a, n) = 1$, then $[a] \in \mathbb{Z}_n^\times$ so $[1] = [a]^{\varphi(n)} = [a^{\varphi(n)}]$ by Corollary 2.5.3. Thus $a^{\varphi(n)} \equiv 1 \mod n$. ∎

Computing and utilizing $\varphi(n) = |\mathbb{Z}_n^\times|$ will be a focus of MATH 3141.

With Lagrange's Theorem (Theorem 2.5.1) and Corollary 2.5.3, we can return to studying the order of group elements and using these orders to determine whether or not two groups are isomorphic. In particular, the following lets us determine the number of groups of order n up to isomorphism for an infinite collection of n.

Corollary 2.5.6. *Let $(G, *)$ be a finite group. If $p = |G|$ is prime, then $G \cong (\mathbb{Z}_p, +)$.*

Proof. Since $|G| = p \geq 2$, there exists an $a \in G \setminus \{e\}$. By Corollary 2.5.3, $|a|$ divides p so $|a| \in \{1, p\}$. Since the only group element of order 1 is the identity element, it follows that $|a| = p$. Hence $\langle a \rangle$ has p elements. Since $\langle a \rangle \subseteq G$ and since both $\langle a \rangle$ and G have p elements, it follows that $G = \langle a \rangle$. Hence $(G, *)$ is a cyclic group of order p so $(G, *) \cong (\mathbb{Z}_p, +)$ by Proposition 2.3.11. ∎

With Corollary 2.5.6, we know up to isomorphism all of the groups of order 2, 3, 5, 7, and so on. Of course, we have a lot of gaps, the first of which are 4 and 6. Can we determine all groups of orders 4 and 6 up to isomorphism? Yes. Yes we can. First, we have already seen all groups of order 4.

Corollary 2.5.7. *Up to isomorphism, there are exactly two groups of order 4: $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$. (That is, these two groups are not isomorphic and every group of order 4 is isomorphic to one of these two groups.)*

Proof. By Example 2.3.15, we have that $(\mathbb{Z}_4, +) \ncong (\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$.

Let $(G, *)$ be such that $|G| = 4$. Thus we can write $G = \{e, a, b, c\}$ where e is the identity element of G and e, a, b, and c are all different elements of G. By Corollary 2.5.3, we know that $|a|, |b|$, and $|c|$ divide 4. Therefore, since a, b, and c are not the identity element, $|a|, |b|, |c| \in \{2, 4\}$.

If one of a, b, or c has order 4, then, as in the proof of Corollary 2.5.6, we obtain $(G, *)$ is a cyclic group of order 4 and thus isomorphic to $(\mathbb{Z}_4, +)$ by Proposition 2.3.11. Otherwise, $|a| = |b| = |c| = 2$. Hence $a^2 = b^2 = c^2 = e$ so $a^{-1} = a$, $b^{-1} = b$, and $c^{-1} = c$.

Consider $a * b \in G = \{e, a, b, c\}$. We claim that $a * b = c$. Indeed

- if $a * b = e$, then $b = a^{-1} = a$, which is impossible,
- if $a * b = a$ then cancellation implies $b = e$, which is impossible, and
- if $a * b = b$ then cancellation implies $a = e$, which is impossible.

Hence $a * b = c$. Similar arguments show $b * a = c$, $a * c = b$, $c * a = b$, $b * c = a$, and $c * b = a$. Hence $(G, *)$ has the same multiplication table as $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ and thus is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$. ∎

To determine all groups of order 6 up to isomorphism, we will actually prove the following which again determines the number of groups of order n up to isomorphism for an infinite collection of n.

Corollary 2.5.8. *Let $p \geq 3$ by prime. Up to isomorphism, there are exactly two groups of order $2p$: $(\mathbb{Z}_{2p}, +)$ and $(D_p, \circ)$. (That is, these two groups are not isomorphic and every group of order $2p$ is isomorphic to one of these two groups.)*

Proof. First note $(\mathbb{Z}_{2p}, +) \ncong (D_p, \circ)$ as $(\mathbb{Z}_{2p}, +)$ is abelian and $(D_p, \circ)$ is not abelian.

Let $(G, *)$ be such that $|G| = 2p$. By Corollary 2.5.3, if $a \in G$ then $|a|$ divides $|G| = 2p$ so $|a| \in \{1, 2, p, 2p\}$. If there exists an $a \in G$ such that $|a| = 2p$, then $\langle a \rangle = G$ so G is cyclic and thus $G \cong (\mathbb{Z}_{2p}, +)$ by Proposition 2.3.11. Hence, for the remainder of the proof, we can assume G contains no elements of order $2p$.

We claim that $(G, *)$ contains an element of order p. To see this, suppose for the sake of a contradiction that $(G, *)$ contains no elements of order p (and of order $2p$). Since $|G| = 2p \geq 6$, there exists $a, b \in G \setminus \{e\}$ such that $a \neq b$. Since G has no elements of order p and $2p$, it follows that $|a| = |b| = 2$. Thus $a^2 = e = b^2$ so $a^{-1} = a$ and $b^{-1} = b$.

Let $c = a * b$. Note

- if $a * b = e$, then $b = a^{-1} = a$, which is impossible,
- if $a * b = a$ then cancellation implies $b = e$, which is impossible, and
- if $a * b = b$ then cancellation implies $a = e$, which is impossible.

Hence $c \in G$ is a group element that is not e, a, or b. Thus $|c| = 2$ and $H = \{e, a, b, c\}$ contains exactly 4 elements.

Note that

$$a * b = c = c^{-1} = (a * b)^{-1} = b^{-1} * a^{-1} = b * a.$$

Hence a and b commute with each other and thus, along with the fact that $a^2 = b^2 = c^2 = e$, one can check that H is closed under multiplication since a and b commute (e.g. $c * a = (a * b) * a = a^2 * b = e * b = b$). Therefore, since H contains the identity and is closed under inverses, we obtain that H is a subgroup of $(G, *)$ with 4 elements. Thus Lagrange's Theorem (Theorem 2.5.1) implies that 4 divides $|G| = 2p$. However, this is impossible since p is prime and $p \geq 3$. Hence we have a contradiction. Therefore $(G, *)$ contains an element of order p.

Let $\rho \in G$ be such that $|G| = p$. Let $H = \langle \rho \rangle$ so $|H| = p$. By Lagrange's Theorem (Theorem 2.5.1), $(G, *)$ has $[G : H] = \frac{2p}{p} = 2$ right cosets. Let $\tau \in G$ be such that $H \neq H\tau$. Thus $G = H \cup H\tau$, $H \cap H\tau = \emptyset$,

$$H = \langle \rho \rangle = \{e, \rho, \ldots, \rho^{p-1}\}, \qquad \text{and} \qquad H\tau = \{\tau, \rho * \tau, \ldots, \rho^{p-1} * \tau\}.$$

We claim that if $b \in H\tau$, then $|b| = 2$. To see this, let $b \in H\tau$ be arbitrary. We claim that $b^2 \in H$. To see this, suppose for the sake of a contradiction that $b^2 \notin H$. Since $b \in H\tau$, we have $b \notin H$. Therefore, since Lagrange's Theorem (Theorem 2.5.1) implies that $(G, *)$ has two right cosets, it follows that $Hb \neq H$ and $G = H \cup Hb$. Since $b^2 \notin H$, it follows that $b^2 \in Hb$. Thus there exist an $h \in H$ such that $b^2 = h * b$ so cancellation implies that

$b = h \in H$. However, since $b \in H\tau$ and $H \cap H\tau = \emptyset$, this is a contradiction. Hence $b^2 \in H$.

To see that $|b| = 2$, suppose for the sake of a contradiction that $|b| \neq 2$. Since $b \in H\tau$ and $e \notin H\tau$, $b \neq e$ so $|b| \neq 1$. Therefore, since $(G, *)$ contains no elements of order $2p$, it follows that $|b| = p$. Since p is prime and $p \geq 3$, we can write $p = 2n + 1$ for some $n \in \mathbb{N}$. Since $b^2 \in H$, it follows that

$$b = e * b = b^p * b = b^{p+1} = b^{2n+2} = (b^2)^{n+1} \in H.$$

However, this contradicts the fact that $b \in H\tau$. Hence $|b| = 2$ for all $b \in H\tau$ as claimed.

The above shows that $|\rho| = p$ and $|\tau| = 2$ so $\rho^{p-1} = \rho^{-1}$ and $\tau^{-1} = \tau$. Moreover, $\rho^{-1} * \tau = \rho^{p-1} * \tau \in H\tau$ so $|\rho^{-1} * \tau| = 2$. Hence

$$\rho^{-1} * \tau * \rho^{-1} * \tau = e$$

so

$$\rho^{-1} * \tau = \tau^{-1} * (\rho^{-1})^{-1} = \tau * \rho.$$

Therefore, by Remark 1.6.20, $(G, *)$ has the same multiplication table as $(D_p, \circ)$ and thus is isomorphic to $(D_p, \circ)$. ∎

The natural number n for which we have yet to determine all groups of order n up to isomorphism is 8. We will do this in Section 5.3, but for now it is too challenging of a task for the theory we possess as it turns out that up to isomorphism there are 3 abelian and 2 non-abelian groups of order 8.

For now there is one more applications of Lagrange's Theorem (Theorem 2.5.1) that we should discuss: helping to determine all subgroups of a given group. This also can help us in our quest to determine whether two groups are isomorphic as Theorem 2.3.13 shows us that isomorphisms preserve the number of subgroups of each order. Therefore, we can demonstrate two groups are not isomorphic if they have a different number of subgroups of a given order.

Example 2.5.9. To compute all of the subgroups of $(D_5, \circ)$, recall $|D_5| = 10$. Therefore, if $H \leq D_5$, then $|H|$ divides 10 so $|H| \in \{1, 2, 5, 10\}$. Clearly if $|H| = 1$ then $H = \{e\}$ and if $|H| = 10$ then $H = D_5$. If $|H| = 2$ or $|H| = 5$, then the order of H is prime and thus H is cyclic by Corollary 2.5.6. Thus we simply need to compute all of the cyclic groups in $(D_5, \circ)$ by taking each of the 10 elements (excluding e) and computing the cyclic subgroup. Doing

so we obtain the following as the complete list of subgroups of $(D_5, \circ)$:

$$\begin{aligned}
\{e\} \\
\langle \tau \rangle &= \{e, \tau\} \\
\langle \rho \circ \tau \rangle &= \{e, \rho \circ \tau\} \\
\langle \rho^2 \circ \tau \rangle &= \{e, \rho^2 \circ \tau\} \\
\langle \rho^3 \circ \tau \rangle &= \{e, \rho^3 \circ \tau\} \\
\langle \rho^4 \circ \tau \rangle &= \{e, \rho^4 \circ \tau\} \\
\langle \rho \rangle &= \{e, \rho, \rho^2, \rho^3, \rho^4\} \\
D_5.
\end{aligned}$$

Finally, the following example shows that the converse of Lagrange's Theorem (Theorem 2.5.1) is not true; that is, if n divides $|G|$, then it need not be the case that there is a subgroup of $(G, *)$ of order n.

Example 2.5.10. Consider $A_4 \leq S_4$. Recall $|A_4| = \frac{4!}{2} = 12$ and, by Example 1.6.39, A_4 contains the following elements with the corresponding orders:

Element	**Order**
e	1
$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 2 & 4 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 4 & 2 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 3 & 4 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 4 & 3 \end{pmatrix}$	3
$\begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$	3
$\begin{pmatrix} 2 & 4 & 3 \end{pmatrix}$	3
$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$	2
$\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}$	2
$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}$	2

We claim that A_4 does not contain a subgroup of order 6. To see this, suppose for the sake of a contradiction that there exists a subgroup H of A_4 such that $|H| = 6$. Thus Corollary 2.5.8 implies that $H \cong (\mathbb{Z}_6, +)$ or $H \cong (D_3, \circ)$. However, since A_4 contains no elements of order 6, H cannot contain an element of order 6. Therefore, since $(\mathbb{Z}_6, +)$ has an element of order 6, $H \ncong (\mathbb{Z}_6, +)$. Hence, it must be the case that $H \cong (D_3, \circ)$. Since $(D_3, \circ)$ has exactly 3 elements of order 2 (namely τ, $\rho \circ \tau$, and $\rho^2 \circ \tau$), H must

contain 3 elements of order 2. Therefore, since A_4 only contains 3 elements of order 2, namely

$$a = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \quad b = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \quad \text{and} \quad c = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix},$$

it follows that $a, b, c \in H$. However, since $a^2 = b^2 = c^2 = e$ and $a \circ b = b \circ a = c$, it follows that $K = \{e, a, b, c\}$ is a subgroup of H of order 4. Hence Lagrange's Theorem (Theorem 2.5.1) implies that $4 = |K|$ divide $6 = |H|$, a clear contradiction. Hence A_4 has order 12 but has no subgroup of order 6.

2.6 Normal Subgroups

In general, the theory of abelian groups is much nicer due to the commutativity of elements (see Chapter 5). One additional nice property of abelian groups is that commutativity implies the left cosets always equal the right cosets; that is $aH = Ha$. Clearly for a non-abelian group, it need not be the case that $aH = Ha$ for every $a \in G$ and subgroup $H \leq G$ as Example 2.4.4. However, for some subgroups, this property does occur for all $a \in G$. As we will see, these types of subgroups are incredibly special. Thus they deserve a name.

Definition 2.6.1. Let $(G, *)$ be a group. A subgroup $H \leq G$ is said to be *normal*, denoted $H \lhd G$, if $aH = Ha$ for all $a \in G$.

Of course, we have some immediate examples.

Example 2.6.2. Let $(G, *)$ be an abelian group. Then every subgroup H of G is normal since $a * h = h * a$ for all $a \in G$ and $h \in H$.

Example 2.6.3. In $(D_3, \circ)$, the subgroup $H = \langle \rho \rangle$ is normal since

$$\begin{aligned}\rho^k H = H = H\rho^k \text{ for all } k \in \{0, 1, 2\}\\ (\rho^k \circ \tau)H = \{\tau, \rho \circ \tau, \rho^2 \circ \tau\} = H(\rho^k \circ \tau) \text{ for all } k \in \{0, 1, 2\}.\end{aligned}$$

However, the subgroup $\langle \tau \rangle$ is not normal since

$$\rho\langle \tau \rangle = \{\rho, \rho \circ \tau\} \quad \text{whereas} \quad \langle \tau \rangle \rho = \{\rho, \rho^2 \circ \tau\}.$$

More interesting, some of the subgroups we have previously studied are normal subgroups. In particular, the following is noteworthy.

Proposition 2.6.4. *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups and let $\varphi : G_1 \to G_2$ be a homomorphism. Then $\ker(\varphi) \lhd G_1$.*

Proof. Let $H = \ker(\varphi)$ and recall $H \leq G_1$ by Corollary 2.1.13. To see that $H \lhd G_1$, let $a \in G_1$ be arbitrary. We claim that $b \in aH$ if and only if

$\varphi(b) = \varphi(a)$. To see this, first assume $b \in aH$. Hence there exists an $h \in H$ such that $b = a *_1 h$. Therefore

$$\varphi(b) = \varphi(a *_1 h) = \varphi(a) *_2 \varphi(h) = \varphi(a) *_2 e_2 = \varphi(a)$$

as desired. Conversely, assume $\varphi(b) = \varphi(a)$. Thus

$$\varphi(a^{-1} *_1 b) = \varphi(a^{-1}) *_2 \varphi(b) = \varphi(a)^{-1} *_2 \varphi(b) = \varphi(b)^{-1} * \varphi(b) = e_2.$$

Hence $a^{-1} *_1 b \in \ker(\varphi) = H$ by the definition of the kernel so $b \in aH$ as desired.

By a similar argument, $b \in Ha$ if and only if $\varphi(b) = \varphi(a)$. Hence $b \in Ha$ if and only if $\varphi(b) = \varphi(a)$ if and only if $b \in aH$ so $aH = Ha$. Therefore, since $a \in G_1$ was arbitrary, $H \lhd G_1$. ∎

Proposition 2.6.4 is an excellent way to find normal subgroups of a given group.

Example 2.6.5. Let $n \in \mathbb{N}$ be such that $n \geq 2$. We claim that $A_n \lhd S_n$. To see this, recall $\text{sgn} : S_n \to \{\pm 1\}$ is a group homomorphism and

$$A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\} = \ker(\text{sgn}).$$

Hence $A_n \lhd S_n$ by Proposition 2.6.4.

Of course, there is another way to see that $A_n \lhd S_n$, namely by noting that there are not many left/right cosets (specifically $[S_n : A_n] = 2$) and using the following result.

Proposition 2.6.6. *Let $(G, *)$ be a group and $H \leq G$. If $[G : H] = 2$, then $H \lhd G$.*

Proof. Let $H \leq G$ be such that $[G : H] = 2$. By Lagrange's Theorem (Theorem 2.5.1), there are exactly two left cosets of H in G and exactly two right cosets of H in G.

To see that $H \lhd G$, let $a \in G$ be arbitrary. If $a \in H$ then $aH = H = Ha$ as desired. Assume $a \notin H$. By Corollary 2.4.5, we know that $aH \cap H = \emptyset$, $Ha \cap H = \emptyset$, and

$$H \cup aH = G = H \cup Ha.$$

It follows that $aH = Ha$. Therefore, since $a \in G$ was arbitrary, $H \lhd G$. ∎

Example 2.6.7. Let $n \in \mathbb{N}$ be such that $n \geq 2$. Since $A_n \leq S_n$ and $[S_n : A_n] = 2$, it follows that $A_n \lhd S_n$ by Proposition 2.6.6.

Example 2.6.8. Let $n \in \mathbb{N}$ be such that $n \geq 3$. Since $\langle \rho \rangle \leq D_n$ and $\frac{|D_n|}{|\rho|} = \frac{2n}{n} = 2$, it follows that $\langle \rho \rangle \lhd D_n$ by Proposition 2.6.6.

Of course, all of the above are ad hoc examples of how to check that a subgroup is normal. We desire something that lets us check that a subgroup is normal along the lines how Definition 1.5.7 lets us show a set is a subgroup. To develop such a theorem for normal subgroups, it is first useful to see a method to take a subgroup and produce another subgroup.

Lemma 2.6.9. *Let $(G, *)$ be a group and $H \leq G$. For all $a \in G$, let*

$$aHa^{-1} = \{a * h * a^{-1} \mid h \in H\}.$$

Then aHa^{-1} is a subgroup of $(G, *)$ with the same number of elements as H.

Proof. To see this, first note since $e \in H$ that

$$e = a * e * a^{-1} \in aHa^{-1}.$$

Thus aHa^{-1} contains the identity element.

Next, to see that aHa^{-1} is closed under products, let $b, c \in aHa^{-1}$ be arbitrary. Thus there exists $h, k \in H$ such that $b = a * h * a^{-1}$ and $c = a * k * a^{-1}$. Therefore, since $h * k \in H$ as $H \leq G$, it follows that

$$b * c = (a * h * a^{-1}) * (a * k * a^{-1}) = a * (h * k) * a^{-1} \in aHa^{-1}.$$

Hence aHa^{-1} is closed under the group products.

Finally, to see that aHa^{-1} is closed under inverses, let $b \in aHa^{-1}$ be arbitrary. Thus there exists an $h \in H$ such that $b = a * h * a^{-1}$. Therefore, since $h^{-1} \in H$ as $H \leq G$, it follows that

$$b^{-1} = (a * h * a^{-1}) = a * h^{-1} * a^{-1} \in aHa^{-1}.$$

Hence aHa^{-1} is closed under inverses. Thus $aHa^{-1} \leq G$ by Definition 1.5.7.

To see that aHa^{-1} has the same number of elements as H, define $f : H \to aHa^{-1}$ by

$$f(h) = a * h * a^{-1}$$

for all $h \in H$. Note that f does indeed map H into aHa^{-1} by the definition of aHa^{-1}. We claim that f is a bijection and thus $|aHa^{-1}| = |H|$. To see this, note f is clearly surjective by definition. Moreover, note that if $h_1, h_2 \in H$ are such that

$$a * h_1 * a^{-1} = f(h_1) = f(h_2) = a * h_2 * a^{-1}$$

then by cancellation on both sides (Corollary 1.3.7) we obtain that $h_1 = h_2$. Hence f is a bijection so $|aHa^{-1}| = |H|$. ∎

With the above in hand, we have the following method for testing when a subgroup is normal.

Theorem 2.6.10 (Normal Subgroup Test). *Let $(G, *)$ be a group and $H \leq G$. The following are equivalent:*

(I) $H \lhd G$.

(II) $aHa^{-1} \subseteq H$ *for all* $a \in G$.

(III) For all $a \in G$ *and* $h \in H$, $a * h * a^{-1} \in H$.

(IV) $aHa^{-1} = H$ *for all* $a \in G$.

Proof. It is elementary to see that (II) and (III) are equivalent, and clearly (IV) implies (II). To see that (II) implies (IV), assume (II) holds. To see that (IV) holds, let $a \in G$ be arbitrary. Hence $aHa^{-1} \subseteq H$ by (II). To see that $H \subseteq aHa^{-1}$, let $h \in H$ be arbitrary. Note since $a^{-1} \in G$, (II) implies that

$$a^{-1}Ha = (a^{-1})H(a^{-1})^{-1} \subseteq H.$$

Hence

$$a^{-1} * h * a \in a^{-1}Ha \subseteq H$$

so there exists a $h' \in H$ such that

$$a^{-1} * h * a = h'.$$

Hence Corollary 1.3.6 implies that $h = a * h' * a^{-1} \in aHa^{-1}$. Therefore, since $h \in H$ was arbitrary, $H \subseteq aHa^{-1}$. Hence $H = aHa^{-1}$ as desired.

Finally, we claim that (I) is equivalent to (IV). Indeed (I) holds if and only if $aH = Ha$ for all $a \in G$ if and only if $aHa^{-1} = H$ for all $a \in G$ (by the same arguments as above since multiplication on the left by a group element is a bijection) if and only if (IV) holds. Thus the proof is complete. ∎

Using the Normal Subgroup Test (Theorem 2.6.10), we have a third proof that $A_n \lhd S_n$.

Example 2.6.11. Let $n \in \mathbb{N}$ be such that $n \geq 2$. Let $\sigma \in S_n$ and let $\tau \in A_n$. Recall τ is even and consider

$$\tau' = \sigma \circ \tau \circ \sigma^{-1}.$$

Clearly τ' is even when σ is even being the product of three even permutations. Moreover, τ' is even when σ is odd as the product of two odd permutations and an even permutation is even. Hence

$$\sigma \circ \tau \circ \sigma^{-1} \in A_n$$

for all $\sigma \in S_n$ and $\tau \in A_n$. Hence $A_n \lhd S_n$ by the Normal Subgroup Test (Theorem 2.6.10).

Remark 2.6.12. Note the Normal Subgroup Test (Theorem 2.6.10) can be used to given another proof of Proposition 2.6.4. Indeed, to see that $\ker(\varphi) \lhd G_1$, let $h \in \ker(\varphi)$ and let $a \in G_1$ be arbitrary. Then

$$\varphi(a *_1 h *_1 a^{-1}) = \varphi(a) *_2 \varphi(h) *_2 \varphi(a^{-1}) = \varphi(a) *_2 e_2 *_2 \varphi(a)^{-1} = e_2$$

so $a *_1 h *_1 a^{-1} \in \ker(\varphi)$. Hence $\ker(\varphi) \lhd G_1$ as desired.

Of course the Normal Subgroup Test (Theorem 2.6.10) can be to check other subgroups are normal. We note the following examples.

Example 2.6.13. Let $H = \langle \rho^2 \rangle \leq D_4$. We claim that $H \lhd D_4$. To see this, first note that $H = \{e, \rho^2\}$. Hence, given $a \in D_4$ we have $aHa^{-1} \subseteq H$ if and only if $a \circ \rho^2 \circ a^{-1} = \rho^2$ if and only if $a \circ \rho^2 = \rho^2 \circ a$. Since

$$\rho^k \circ \rho^2 = \rho^{k+2} = \rho^2 \circ \rho^k$$

for all $k \in \{0, 1, 2, 3\}$, since

$$\tau \circ \rho^2 = \rho^{-1} \circ \tau \circ \rho = \rho^{-2} \circ \tau = \rho^2 \circ \tau,$$

and since every element of D_4 is a product of ρ^k and τ^m for some $k \in \{0, 1, 2, 3\}$ and $m \in \{0, 1\}$, it follows that $a \circ \rho^2 = \rho^2 \circ a$ for all $a \in D_4$. Hence $H \lhd D_4$ by the Normal Subgroup Test (Theorem 2.6.10).

Example 2.6.14. Let $n \in \mathbb{N}$. We claim that $SL_n \lhd GL_n$. To see this, note for all $A \in GL_n$ and $B \in SL_n$ that $\det(B) = 1$ so

$$\begin{aligned} \det(ABA^{-1}) &= \det(A)\det(B)\det(A^{-1}) \\ &= \det(A)\det(B)\det(A)^{-1} \\ &= \det(B) = 1 \end{aligned}$$

and thus $ABA^{-1} \in SL_n$. Hence by the Normal Subgroup Test (Theorem 2.6.10). Alternatively, SL_n is the kernel of the determinant map (see Example 2.1.19) and thus $SL_n \lhd GL_n$ by Proposition 2.6.4

Finally, there is one last property that can sometimes be used to imply a subgroup is normal.

Corollary 2.6.15. *Let $(G, *)$ be a group and $H \leq G$. If H is the only subgroup of G of order $|H|$, then $H \lhd G$.*

Proof. Let $H \leq G$ be such that H is the only subgroup of G of order $|H|$. To see that $H \lhd G$, let $a \in G$ be arbitrary. Since $aHa^{-1} \leq G$ by Lemma 2.6.9 with $|aHa^{-1}| = |H|$, it follows that $aHa^{-1} = H$. Therefore, since H was arbitrary, $H \lhd G$ by the Normal Subgroup Test (Theorem 2.6.10). ∎

2.7 Quotient Groups

Note the previous section did not discuss why normal subgroups are 'incredibly special'. The reason normal subgroups are important and powerful is that given a group $(G, *)$ and a normal subgroup $H \lhd G$, it is possible to form a special group based on G and H. This, in some way, allows one to decompose group into a normal subgroup and this special group. One can then repeat this process over and over again allowing one to study groups via studying groups with no non-trivial normal subgroups in addition to studying abelian groups. Groups that have no non-trivial normal subgroups are said to be *simple*.

This special group we want to form via $H \lhd G$ is constructed by 'modding G out by H'. In particular, this is how we constructed $(\mathbb{Z}_n, +)$ in MATH 1200: we take $(\mathbb{Z}, +)$ and the (normal) subgroup $n\mathbb{Z}$, and we obtain a group structure on the left cosets $\{k + n\mathbb{Z}\}$ using the 'multiplication' in $(\mathbb{Z}, +)$. In fact, this is why the proof that $(\mathbb{Z}_n, +)$ from Example 1.2.12 so closely resembled the proof that $(\mathbb{Z}, +)$ was a group!

To generalize the above so that we obtain a group by using $*$ on the left cosets via $aH * bH = (a * b)H$, we need to make sure that this multiplication is well-defined as, after all, every coset can be represented by more that one element. In particular, the following result shows that this multiplication on the left cosets is well-defined exactly when $H \lhd G$.

Lemma 2.7.1. *Let $(G, *)$ be a group and $H \leq G$. Then $H \lhd G$ if and only if whenever $a_1, a_2, b_1, b_2 \in G$ are such that $a_1H = a_2H$ and $b_1H = b_2H$, then $(a_1 * b_1)H = (a_2 * b_2)H$.*

Proof. Assume that $H \lhd G$ and that $a_1, a_2, b_1, b_2 \in G$ are such that $a_1H = a_2H$ and $b_1H = b_2H$. To see that $(a_1 * b_1)H = (a_2 * b_2)H$, it suffices by Corollary 2.4.5 to show that

$$b_2^{-1} * a_2^{-1} * a_1 * b_1 = (a_2 * b_2)^{-1} * (a_1 * b_1) \in H.$$

Since $a_1H = a_2H$ and $b_1H = b_2H$, we obtain by Corollary 2.4.5 that $a_2^{-1} * a_1 \in H$ and $b_2^{-1} * b_1 \in H$. Hence there exists $h_1, h_2 \in H$ such that $h_1 = a_2^{-1} * a_1$ and $h_2 = b_2^{-1} * b_1$. Moreover, since $H \lhd G$, we know that $b_1H = Hb_1$. Since

$$h_1 * b_1 \in Hb_1 = b_1H,$$

we obtain that there exists an $h_3 \in H$ such that $h_1 * b_1 = b_1 * h_3$. Therefore

$$\begin{aligned} b_2^{-1} * a_2^{-1} * a_1 * b_1 &= b_2^{-1} * h_1 * b_1 \\ &= b_2^{-1} * b_1 * h_3 \\ &= h_2 * h_3 \in H \end{aligned}$$

with the last equality following since $H \leq G$. Hence $(a_1 * b_1)H = (a_2 * b_2)H$ as desired.

Conversely, assume whenever $a_1, a_2, b_1, b_2 \in G$ are such that $a_1H = a_2H$ and $b_1H = b_2H$, then $(a_1 * b_1)H = (a_2 * b_2)H$. To see that $H \lhd G$, let $a \in G$ and $h \in H$ be arbitrary. Since $hH = eH$ by Corollary 2.4.5, by taking $a_1 = h$, $a_2 = e$, $b_1 = b_2 = a^{-1}$, we obtain that

$$(h * a^{-1})H = (e * a^{-1})H = a^{-1}H$$

and thus $(a * h * a^{-1})H = H$ by multiplying the above sets by a on the left. Hence $a * h * a^{-1} \in H$. Therefore, since $a \in G$ and $h \in H$ were arbitrary, $H \lhd G$ by the Normal Subgroup Test (Theorem 2.6.10). ∎

With Lemma 2.7.1 in hand, we can generalize $(\mathbb{Z}_n, +)$ to arbitrary groups by normal subgroups. Note this proof is identical to how we show $(\mathbb{Z}_n, +)$ is a group in Example 1.2.12.

Theorem 2.7.2. *Let $(G, *)$ be a group, let $H \lhd G$, and let*

$$G/H = \{aH \mid a \in G\}.$$

Then G/H is a group with respect to the operation $aH * bH = (a * b)H$ for all $a, b \in G$.

Proof. First note that the operation $* : (G/H) \times (G/H) \to G/H$ defined by

$$aH * bH = (a * b)H$$

for all $a, b \in G$ is a well-defined binary operation by Lemma 2.7.1. To see that $(G/H, *)$ is associative, note for all $a, b, c \in G$ that

$$\begin{aligned}
(aH * bH) * cH &= (a * b)H * cH \\
&= ((a * b) * c)H \\
&= (a * (b * c))H && \text{since } (G, *) \text{ is associative} \\
&= aH * (b * c)H \\
&= aH * (bH * cH)
\end{aligned}$$

Moreover, since

$$eH * aH = (e * a)H = aH = (a * e)H = aH * eH$$

for all $a \in G$, we see that eH is the identity element of G/H.

Finally, to see that $(G/H, *)$ has inverses, let $a \in G$ be arbitrary. Then $a^{-1}H \in G/H$ and, since

$$aH * a^{-1}H = (a * a^{-1})H = eH = (a^{-1} * a)H = a^{-1}H * aH,$$

we see that $a^{-1}H$ is the inverse of aH in $(G/H, *)$. Therefore, since $a \in G$ was arbitrary, $(G/H, *)$ has inverses. Hence $(G/H, *)$ is a group. ∎

Definition 2.7.3. Let $(G, *)$ be a group and let $H \lhd G$. The group

$$G/H = \{aH \mid a \in G\}$$

where $aH * bH = (a * b)H$ for all $a, b \in G$ is called the *quotient group of G by H*.

Of course, our first example of a quotient group is the one we are already familiar with.

Example 2.7.4. Consider the group $(\mathbb{Z}, +)$ and, for $n \in \mathbb{N}$, the subgroup $n\mathbb{Z}$. Since $(\mathbb{Z}, +)$ is abelian, we have that $n\mathbb{Z} \lhd \mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ is a group with elements $\{m + n\mathbb{Z} \mid m \in \mathbb{Z}\}$ where

$$(m + n\mathbb{Z}) + (k + n\mathbb{Z}) = (m + k) + n\mathbb{Z}.$$

In particular, since $m + n\mathbb{Z} = [m]$ modulo n, we see that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

For a more exotic quotient group, consider the following.

Example 2.7.5. Recall if $H = \langle \rho^2 \rangle = \{e, \rho^2\}$ in $(D_4, \circ)$, then $H \lhd D_4$ by Example 2.6.13. Note that

$$\begin{aligned} eH = \rho^2 H &= \{e, \rho^2\} \\ \rho H = \rho^3 H &= \{\rho, \rho^3\} \\ \tau H = (\rho^2 \circ \tau)H &= \{\tau, \rho^2 \circ \tau\} \\ (\rho \circ \tau)H = (\rho^3 \circ \tau)H &= \{\rho \circ \tau, \rho^3 \circ \tau\} \end{aligned}$$

are all of the left cosets of H. Thus

$$D_4/H = \{eH, \rho H, \tau H, (\rho \circ \tau)H\}.$$

Since D_4/H has four elements, D_4/H is isomorphic to either $(\mathbb{Z}_4, +)$ or $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ by Corollary 2.5.7. Since

$$\begin{aligned} (\rho H)^2 &= \rho^2 H = eH \\ (\tau H)^2 &= \tau^2 H = eH \\ ((\rho \circ \tau)H)^2 &= (\rho \circ \tau)^2 H = eH, \end{aligned}$$

we see that every non-identity element of $(D_4/H, *)$ has order 2. Therefore, since $(\mathbb{Z}_4, +)$ has an element of order 4, $(D_4/H, *)$ cannot be isomorphic to $(\mathbb{Z}_4, +)$ and thus $(D_4/H, *) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$.

Some more examples of quotient groups will be computed in the next section once more theory has been established. For now, some very nice properties of a group carry forward to every quotient group.

Proposition 2.7.6. *Let $(G, *)$ be a group and let $H \lhd G$.*

(I) If $a \in G$, then $|aH|$ is the least natural number n such that $a^n \in H$.

(II) The order of aH in G/H is less than the order of a in G.

(III) If $|a| < \infty$, $|aH|$ divides $|a|$.

(IV) $|G/H| = [G : H]$.

(V) If $(G, *)$ is abelian, $(G/H, *)$ is abelian.

(VI) If $(G, *)$ is cyclic, $(G/H, *)$ is cyclic.

Proof. To see that (I), (II), and (III) are true, let $a \in G$ be arbitrary. By Corollary 1.7.23, the order of $|aH|$ is the least natural number n such that $eH = (aH)^n = a^nH$. Since $a^nH = eH$ if and only if $a^n \in H$, (I) is true. Moreover, if $|a| = \infty$ then clearly (II) is true. Otherwise, if $|a| < \infty$ then $a^{|a|} = e$ so $(aH)^{|a|} = eH$. Therefore Corollary 1.7.22 implies $|aH|$ divides $|a|$. Hence (II) and (III) are true.

Since $|G/H|$ is the number of left cosets of H in $(G, *)$, (IV) follows.

To see that (V) is true, assume $(G, *)$ is abelian. To see that $(G/H, *)$ is abelian, let $a, b \in G$ be arbitrary. Therefore, since $(G, *)$ is abelian, we obtain that

$$aH * bH = (a * b)H = (b * a)H = bH * aH.$$

Hence, since $a, b \in G$ were arbitrary, $(G/H, *)$ is abelian.

Finally, to see that (VI) is true, assume $(G, *)$ is cyclic. Hence there exists an $a \in G$ such that $G = \langle a \rangle$. Therefore, for all $b \in G$ there exists an $n \in \mathbb{Z}$ such that $b = a^n$ so

$$bH = a^nH = (aH)^n \in \langle aH \rangle.$$

Thus $G/H = \langle aH \rangle$ so $(G/H, *)$ is cyclic. ∎

Remark 2.7.7. It is important to note that the converses of parts (V) and (VI) of Proposition 2.7.6 fail. Indeed, note in Example 2.7.5 that $\langle \rho^2 \rangle$ and $D_4/\langle \rho^2 \rangle$ are abelian groups whereas D_4 is not abelian.

Similarly, note for $n \geq 2$ that $A_n \lhd S_n$ by Example 2.6.5. However, since

$$|S_n/A_n| = [S_n : A_n] = 2,$$

we see that S_n/A_n has order 2. Hence $(S_n/A_n, *) \cong (\mathbb{Z}_2, +)$ by Example 2.3.12 so $(S_n/A_n, *)$ is abelian and cyclic even though $(S_n, \circ)$ is neither abelian nor cyclic.

Interesting, using the notion of quotient groups, we have another complete characterization of when a subgroup is normal. Indeed recall from Proposition 2.6.4 that the kernel of every homomorphism is a normal subgroup. The following is the converse that shows every normal subgroup occurs as the kernel of some homomorphism.

Theorem 2.7.8. *Let $(G, *)$ be a group and let $H \lhd G$. Define $q : G \to G/H$ by $q(a) = aH$ for all $a \in G$. Then q is a homomorphism with* $\ker(q) = H$.

Proof. To see that q is a homomorphism, note for all $a, b \in G$ that

$$q(a * b) = (a * b)H = aH * bH = q(a) * q(b).$$

Hence q is a homomorphism.

To see that $\ker(q) = H$, note $a \in \ker(q)$ if and only if $q(a) = eH$ if and only if $aH = eH$ if and only if $a \in H$. Hence $\ker(q) = H$ as desired. ∎

Since the homomorphisms in Theorem 2.7.8 take a group to one its quotient groups, the name of such maps is not a surprise.

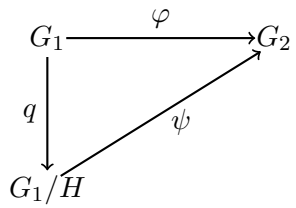
Definition 2.7.9. Let $(G, *)$ be a group and let $H \lhd G$. The homomorphism $q : G \to G/H$ from Theorem 2.7.8 defined by $q(a) = aH$ for all $a \in G$ is called the *quotient map*.

Corollary 2.7.10. *Let $(G, *)$ be a group and let $H \leq G$. Then $H \lhd G$ if and only if H is the kernel of some homomorphism with domain G.*

Proof. Proposition 2.6.4 implies that the kernel of every homomorphism is a normal subgroup. Theorem 2.7.8 shows that every normal subgroup occurs as the kernel of some homomorphism. ∎

The algebraic significant (and abstract definition) of the quotient map is that every group homomorphism with kernel containing $H \lhd G$ factors through the quotient group via the quotient map. This is formally stated as follows.

Theorem 2.7.11 (Universal Property of the Quotient Map). *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups, let $H \lhd G_1$, let $q : G_1 \to G_1/H$ be the quotient map, and let $\varphi : G_1 \to G_2$ be a homomorphism such that $H \subseteq \ker(\varphi)$. Then there exists a unique homomorphism $\psi : G_1/H \to G_2$ such that $\varphi = \psi \circ q$.*



That is, every homomorphism φ such that $H \subseteq \ker(\varphi)$ can be written as first applying the quotient map q and then applying a unique homomorphism from G_1/H to G_2.

Proof. We desire to define $\psi : G_1/H \to G_2$ by

$$\psi(aH) = \varphi(a)$$

for all $a \in G_1$. Since we are dealing with equivalence classes, to see that ψ is well-defined, let $a, b \in G_1$ be such that $aH = bH$. Hence $b^{-1} *_1 a \in H \subseteq \ker(\varphi)$. Therefore

$$e_2 = \varphi(b^{-1} *_1 a) = \varphi(b)^{-1} *_2 \varphi(a)$$

so

$$\psi(aH) = \varphi(a) = \varphi(b) = \psi(bH).$$

Hence ψ is well-defined.

We claim that $\psi : G_1/H \to G_2$ is a homomorphism such that $\varphi = \psi \circ q$. To see that ψ is a homomorphism, note for all $a, b \in G_1$ that

$$\psi(aH * bH) = \psi((a *_1 b)H) = \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b) = \psi(aH) *_2 \psi(bH).$$

Hence ψ is a homomorphism. Moreover, for all $a \in G_1$ note that

$$(\psi \circ q)(a) = \psi(q(a)) = \psi(aH) = \varphi(a).$$

Hence $\varphi = \psi \circ q$ as desired.

Finally, assume $\Psi : G_1/H \to G_2$ is a homomorphism such that $\varphi = \Psi \circ q$. Then for all $a \in G_1$ we have that

$$\Psi(aH) = \Psi(q(a)) = (\Psi \circ q)(a) = \varphi(a) = \psi(aH).$$

Hence $\Psi = \psi$ as desired. ∎

2.8 Isomorphism Theorems

Using the quotient map and its (defining) universal property from Theorem 2.7.11, we can prove what are known as the three Isomorphism Theorems for groups. Each of these isomorphism theorems enable us to show that groups are isomorphic if certain conditions are met. The First Isomorphism Theorem, which is the most and only Isomorphism Theorem that is important for future uses in this course, lets us take a homomorphism and produce isomorphic groups.

Theorem 2.8.1 (First Isomorphism Theorem). *Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups, let $\varphi : G_1 \to G_2$ be a homomorphism, and let $H = \ker(\varphi)$. Then $H \lhd G_1$ and $G_1/H \cong \mathrm{Im}(\varphi)$.*

Proof. Recall by Corollary 2.1.13 that $\text{Im}(\varphi) \leq G_2$. Moreover, by Proposition 2.6.4, $H = \ker(\varphi) \lhd G_1$. Hence the Universal Property of the Quotient Map (Theorem 2.7.11) implies that if $q : G_1 \to G_1/H$ is the quotient map, then there exists a unique homomorphism $\psi : G_1/H \to G_2$ such that $\varphi = \psi \circ q$. Moreover, since q is clearly surjective, we see that

$$\begin{aligned}\text{Im}(\psi) &= \{\psi(aH) \mid a \in G\} \\ &= \{\psi(q(a)) \mid a \in G\} \\ &= \{\varphi(a) \mid a \in G\} \\ &= \text{Im}(\varphi).\end{aligned}$$

Thus, we can view $\psi : G_1/H \to \text{Im}(\varphi)$ (i.e. change the co-domain to the image of φ).

We claim that ψ is an isomorphism from G_1/H to $\text{Im}(\varphi)$. To see this, note $\text{Im}(\psi) = \text{Im}(\varphi)$. To see that $\ker(\psi) = \{eH\}$, note $eH \in \ker(\psi)$ trivially. To see the other inclusion, assume $a \in G_1$ is such that $aH \in \ker(\psi)$. Hence

$$e_2 = \psi(aH) = \psi(q(a)) = \varphi(a).$$

Therefore $a \in \ker(\varphi) = H$ so $aH = eH$. Hence $\ker(\psi) = \{eH\}$ and $\text{Im}(\psi) = \text{Im}(\varphi)$ so ψ is an isomorphism from G_1/H to $\text{Im}(\varphi)$ by Proposition 2.2.2. ∎

Using the First Isomorphism Theorem (Theorem 2.8.1), we can now describe and compute some more quotient groups.

Example 2.8.2. Recall by Example 2.1.15 that if $\varphi : \mathbb{R} \to \mathbb{T}$ is defined by

$$\varphi(x) = e^{ix}$$

for all $x \in \mathbb{R}$, then φ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{T}, \times)$ such that

$$\text{Im}(\varphi) = \mathbb{T} \qquad \text{and} \qquad \ker(\varphi) = \{2\pi n \mid n \in \mathbb{Z}\}.$$

Therefore, the First Isomorphism Theorem (Theorem 2.8.1) implies that

$$(\mathbb{R}/(2\pi\mathbb{Z}), *) \cong (\mathbb{T}, \times).$$

Note that it is this isomorphism that lets us relate the real numbers modulo 2π with the circle and is fundamentally in the background of all trigonometric functions. Said isomorphism is also fundamental in MATH 3001.

Example 2.8.3. Let $n \in \mathbb{N}$. Recall from Example 2.1.19 that if $\varphi : GL_n \to \mathbb{R} \setminus \{0\}$ is defined by

$$\varphi(A) = \det(A)$$

for all $A \in GL_n$, then φ is a homomorphism from $(GL_n, \times)$ to $(\mathbb{R} \setminus \{0\}, \times)$ such that

$$\text{Im}(\varphi) = \mathbb{R} \setminus \{0\} \qquad \text{and} \qquad \ker(\varphi) = SL_n.$$

Therefore, the First Isomorphism Theorem (Theorem 2.8.1) implies that

$$GL_n/SL_n \cong (\mathbb{R} \setminus \{0\}, \times).$$

Example 2.8.4. Define $\varphi : \mathbb{C} \setminus \{0\} \to \mathbb{R}^+$ by

$$\varphi(z) = |z|$$

for all $z \in \mathbb{C} \setminus \{0\}$. We claim that φ is a homomorphism from $(\mathbb{C} \setminus \{0\}, \times)$ to $(\mathbb{R}^+, \times)$. To see this, note for all $z, w \in \mathbb{C} \setminus \{0\}$ that

$$\varphi(z \times w) = |z \times w| = |z||w| = \varphi(z) \times \varphi(w)$$

Hence φ is a homomorphism by definition. Since 1 is the identity of $\mathbb{R}^+$, we see that

$$\text{Im}(\varphi) = \mathbb{R}^+ \qquad \text{and} \qquad \ker(\varphi) = \mathbb{T}.$$

Therefore, the First Isomorphism Theorem (Theorem 2.8.1) implies that

$$(\mathbb{C} \setminus \{0\})/\mathbb{T} \cong (\mathbb{R}^+, \times).$$

For our Second Isomorphism Theorem (Theorem 2.8.7) we require the following which shows the product of two subgroups is a subgroup provided one of the subgroups is normal. It is not difficult to find examples where this fails when neither subgroup is normal.

Lemma 2.8.5. *Let $(G, *)$ be a group, let $H \lhd G$, and let $K \leq G$. Then*

$$KH = \{k * H \mid h \in H, k \in K\}$$

is a subgroup of G. Moreover $H \lhd KH$.

Proof. To see that KH is a subgroup of G, first note since $H \lhd G$ and $K \leq G$ that $e \in H$ and $e \in K$ so $e = e * e \in KH$.

Next, to see that KH is closed under products, let $a, b \in KH$ be arbitrary. Thus there exists $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that

$$a = k_1 * h_1 \qquad \text{and} \qquad b = k_2 * h_2.$$

Moreover, since $H \lhd G$, we have that $k_2 H = H k_2$. Therefore, since

$$h_1 * k_2 \in Hk_2 = k_2 H,$$

there exists an $h_3 \in H$ such that $h_1 * k_2 = k_2 * h_3$. Hence

$$\begin{aligned} a * b &= (k_1 * h_1) * (k_2 * h_2) \\ &= (k_1 * k_2) * (h_3 * h_2). \end{aligned}$$

Since $h_1, h_3 \in H$ and $k_1, k_2 \in K$, we obtain since $H \lhd G$ and $K \leq G$ that that $h_3 * h_2 \in H$ and $k_1 * k_2 \in K$ so $a * b \in KH$ as desired. Hence, since $a, b \in KH$ were arbitrary, KH is closed under products.

Finally, to see that KH is closed under inverses, let $a \in KH$ be arbitrary. Thus there exists $h \in H$ and $k \in K$ such that $a = k * h$. Moreover, since $H \lhd G$, we have that $k^{-1}H = Hk^{-1}$. Therefore, since $h^{-1} \in H$ as $H \lhd G$ so

$$h^{-1} * k^{-1} \in Hk^{-1} = k^{-1}H,$$

there exists an $h_3 \in H$ such that

$$h^{-1} * k^{-1} = k^{-1} * h_3.$$

Hence

$$a^{-1} = h^{-1} * k^{-1} = k^{-1} * h_3 \in KH$$

since $h_3 \in H$ and $k^{-1} \in K$ as $k \in K$ and $K \leq G$. Therefore, since $a \in KH$ was arbitrary, LH is closed under inverses. Thus KH is a subgroup of $(G, *)$ by Definition 1.5.7.

To see that $H \lhd KH$, first note that both H and KH are groups with respect to $*$ and that

$$H = \{e * h \mid h \in H\} \subseteq KH$$

since $e \in K$. Therefore $H \leq KH$ by Definition 1.5.1. Moreover, since $aHa^{-1} = H$ for all $a \in G$ by the Normal Subgroup Test (Theorem 2.6.10), we obtain that $aHa^{-1} = H$ for all $a \in KH$ since $KH \subseteq G$. Therefore, the Normal Subgroup Test (Theorem 2.6.10) implies that $H \lhd KH$. ∎

Remark 2.8.6. Let $(G, *)$ be a group, let $H \lhd G$, and let $K \leq G$. Since $kH = Hk$ for all $k \in K$ as $H \lhd G$, it follows that $HK = KH$. Thus the order of multiplication in Lemma 2.8.5 does not matter.

Theorem 2.8.7 (Second Isomorphism Theorem). *Let $(G, *)$ be a group, let $H \lhd G$, and let $K \leq G$. Then $H \cap K \lhd K$ and*

$$KH/H \cong K/(H \cap K).$$

Proof. Note $KH \leq G$ and $H \lhd KH$ by Lemma 2.8.5.

Define $\varphi : K \to KH$ by

$$\varphi(a) = a$$

for all $a \in K$. Note since $\varphi(a) = a = a * e \in KH$ for all $a \in K$ that the codomain of φ is correct. Moreover, we clearly see that φ is a homomorphism.

Let

$$q : KH \to KH/H$$

by the quotient map which exists since $H \lhd KH$. Let

$$\psi = \varphi \circ q : K \to KH/H.$$

Hence ψ is a group homomorphism by Proposition 2.2.6. Note $\psi(a) = aH$ for all $a \in K$.

Note $\text{Im}(\psi) \subseteq KH/H$. We claim that $\text{Im}(\psi) = KH/H$. To see this, let $b \in KH$ be arbitrary. Thus there exists a $k \in K$ and an $h \in H$ such that $b = k * h$. Hence

$$bH = kH = \psi(k)$$

Therefore, since $b \in KH$ was arbitrary, $\text{Im}(\psi) = KH/H$.

Next we claim that $\ker(\psi) = H \cap K$. To see this, let $a \in H \cap K$ be arbitrary. Hence $aH = eH$ so $\psi(a) = aH = eH$ and thus $a \in \ker(\psi)$. Therefore, since $a \in H \cap K$ was arbitrary, $H \cap K \subseteq \ker(\psi)$.

To see the other inclusion, let $a \in \ker(\psi)$. Since $\psi : K \to KH/H$, it follows that $a \in K$ by the definition of the kernel. Moreover, since $a \in \ker(\psi)$, we have that

$$eH = \psi(a) = aH$$

and thus $a \in H$. Hence $a \in H \cap K$. Therefore, since $a \in \ker(\psi)$ was arbitrary, $\ker(\psi) = H \cap K$.

Consequently, $H \cap K = \ker(\psi) \lhd K$ by Proposition 2.6.4 and

$$KH/H \cong K/(H \cap K)$$

by the First Isomorphism Theorem (Theorem 2.8.1). ∎

One use of the Second Isomorphism Theorem (Theorem 2.8.7) is the following example which is useful in Lie Theory, geometry, and representation theory.

Example 2.8.8. Let $GL_2(\mathbb{C})$ denote the set of all invertible 2×2 matrices with complex entries. Note $GL_2(\mathbb{C})$ together with matrix multiplication is a group by the same proof that GL_2 is a group (see Example 1.2.24).

Let $K = SL_2(\mathbb{C})$ denote the set of all elements of $GL_2(\mathbb{C})$ with determinant 1. By the same arguments as Example 2.6.14, we obtain that $H \lhd G$.

Let

$$H = \{\alpha I_2 \mid \alpha \in \mathbb{C} \setminus \{0\}\}.$$

It is elementary to verify that $H \leq G$. Moreover $H \lhd G$ since $A(\alpha I_2)A^{-1} = \alpha I_2 \in H$ for all $A \in GL_2(\mathbb{C})$ and $\alpha I_2 \in H$.

Note that

$$H \cap K = \{\alpha I_2 \mid \alpha \in \mathbb{C} \setminus \{0\}, \alpha^2 = \det(\alpha I_2) = 1\} = \{\pm I_2\}.$$

Moreover, $KH \subseteq GL_2$. We claim that $KH = GL_2(\mathbb{C})$. To see this, note if $A \in GL_2$ then $\det(A) \neq 0$,

$$B = \frac{1}{\sqrt{\det(A)}} A \in SL_2(\mathbb{C}),$$

$C = \sqrt{\det(A)} I_2 \in H$, and $A = BC \in KH$. Hence $GL_2(\mathbb{C}) = KH$.

Therefore, by the Second Isomorphism Theorem (Theorem 2.8.7), we obtain that

$$GL_2(\mathbb{C})/K = KH/H \cong K/(H \cap K) = SL_2(\mathbb{C})/\{\pm I_2\}.$$

The Second Isomorphism Theorem (Theorem 2.8.7) is also quite useful in the discussion of *solvable groups*; a concept that might be studied in MATH 4021. For now, another application of the theorem is the following, which actually also holds when H is not a normal subgroup of $(G, *)$, but we just present the case when H is normal as it trivially follows from the Second Isomorphism Theorem (Theorem 2.8.7).

Corollary 2.8.9 (Counting Principle). *Let $(G, *)$ be a group, let $H \lhd G$, and let $K \leq G$. If H and K are finite, then*

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

Proof. By the Second Isomorphism Theorem (Theorem 2.8.7),

$$|KH/H| = |K/(H \cap K)|.$$

By Proposition 2.7.6, it follows that

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

Hence the result follows. ∎

Finally, we arrive at the third and final of our Isomorphism Theorems.

Theorem 2.8.10 (Third Isomorphism Theorem). *Let $(G, *)$ be a group and let H and K be normal subgroups of G with $K \subseteq H$. Then $K \lhd H$, $H/K \lhd G/K$, and*

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

Proof. Since $K \leq G$ and $H \leq G$, we know that H and K are groups with respect to $*$. Therefore, since $K \subseteq H$, we obtain that $K \leq H$.

To see that $K \lhd H$, note since $K \lhd G$ that the Normal Subgroup Test (Theorem 2.6.10) implies that $aKa^{-1} = K$ for all $a \in G$. Hence $aKa^{-1} = K$ for all $a \in H$. Therefore $K \lhd H$ by the Normal Subgroup Test (Theorem 2.6.10).

We desire to define $\varphi : G/K \to G/H$ by

$$\varphi(aK) = aH$$

for all $a \in G$. However, since we are dealing with objects that can be represented multiple ways, we need to check that φ is well-defined. To see that φ is well-defined, let $a, b \in G$ be arbitrary elements such that $aK = bK$. Hence $b^{-1} * a \in K \subseteq H$ so $aH = bH$. Therefore

$$\varphi(aK) = aH = bH = \varphi(bK).$$

Hence, since a and b were arbitrary, φ is well-defined.

We claim that φ is a group homomorphism. To see this, let $a, b \in G$ be arbitrary. Then

$$\begin{aligned}\varphi(aK * bK) &= \varphi((a * b)K) \\ &= (a * b)H \\ &= aH * bH \\ &= \varphi(aK) * \varphi(bK).\end{aligned}$$

Therefore, since $a, b \in G$ were arbitrary, φ is a homomorphism.

Note $\text{Im}(\varphi) \subseteq G/H$. We claim that $\text{Im}(\varphi) = G/H$. To see this, let $a \in G$ be arbitrary. Then $aK \in G/K$ and

$$\varphi(aK) = aH.$$

Therefore, since $a \in G$ was arbitrary, $\text{Im}(\varphi) = G/H$.

Next we claim that

$$\ker(\varphi) = H/K = \{hK \mid h \in H\}.$$

To see this, let $h \in H$ be arbitrary. Hence $hH = eH$ so

$$\varphi(hK) = hH = eH$$

and thus $hK \in \ker(\varphi)$. Therefore, since $h \in H$ was arbitrary, $H/K \subseteq \ker(\varphi)$.

To see the other inclusion, let $aK \in \ker(\varphi)$ for some $a \in G$. Hence

$$aH = \varphi(aK) = eH.$$

Thus $a \in H$ so $aK \in H/K$. Therefore, since $aK \in \ker(\varphi)$ was arbitrary, $\ker(\varphi) = H/K$.

Consequently, $H/K = \ker(\varphi) \lhd G/H$ by Proposition 2.6.4 and

$$(G/K)/(H/K) \cong G/H$$

by the First Isomorphism Theorem (Theorem 2.8.1). ∎

Example 2.8.11. Let $n, m \in \mathbb{N}$ and consider the group $(\mathbb{Z}, +)$. Consider the subgroups $H = n\mathbb{Z}$ and $K = mn\mathbb{Z}$. Note $K \subseteq H$. Moreover H and K are normal subgroups of $(\mathbb{Z}, +)$ since all subgroups of abelian groups are normal. Therefore, the Third Isomorphism Theorem implies that

$$(\mathbb{Z}/(mn\mathbb{Z}))/(n\mathbb{Z}/(mn\mathbb{Z})) \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Chapter 3

Group: Actions

Throughout the previous chapter and our attempt to determine how many groups of order n there are up to isomorphism, we developed some quite interesting theory. Lagrange's Theorem (Theorem 2.5.1) was key, and through the cosets we need to prove the theorem, we also developed the idea of normal subgroups and quotient groups.

In this chapter, we will begin a similar study. We will define a concept related to groups that is interesting in its own right, but by studying this concept we will obtain unexpected results pertaining to the theory of finite groups and we will enable theory in Chapter 4 to help us answer the question "How many groups of order n are there up to isomorphism?"

As motivation for the main concept of this chapter, consider $(S_n, \circ)$. Recall if $\sigma \in S_n$, then $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. In particular, we can think of σ as a group element, and as an object that acts on the set $\{1, \ldots, n\}$. It is this later viewpoint that inspires the objects studied in this chapter. In particular, we will focus on the actions of groups on sets. Such actions will unveil important properties of the group and sets they act on. Moreover, such actions have applications in other areas of mathematics such as combinatorics and geometry. We endeavour to present at least one application of group theory to combinatorics in Section 3.4.

3.1 Group Actions

To begin we need to determine what we mean by a 'group acting on a set'. The idea is simple: the identity element of the group should act as the identity map on the set, and if we act by one group element and then another, it should be the same as acting by the product of the group elements. This is formalized as follows.

Definition 3.1.1. Let $(G, *)$ be a group and let X be a non-empty set. A *(left) group action of G on X* is a map $\cdot : G \times X \to X$ such that

(i) $e \cdot x = x$ for all $x \in X$, and

(ii) $a \cdot (b \cdot x) = (a * b) \cdot x$ for all $a, b \in G$ and $x \in X$.

When a group action of G on X exists, it is said that X is a *G-set* and that G *acts on* X. We denote "G acts on X" by $G \curvearrowright X$.

Remark 3.1.2. It is important to note that whenever one says 'X is a G-set', there is always an underlining group action of G on X which is denoted $\cdot$.

Of course, since there are so many groups, it should not be difficult to find examples of group actions. We begin with the 'silly' group action.

Example 3.1.3. Let $(G, *)$ be any group and let X be any set. Define the map $\cdot : G \times X \to X$ by

$$a \cdot x = x$$

for all $a \in G$ and $x \in X$. We claim that $\cdot$ is a group action. To see this, note

$$e \cdot x = x$$

for all $x \in X$ trivially. Moreover, for all $a, b \in G$ and $x \in X$ we see that

$$a \cdot (b \cdot x) = a \cdot x = x = (a * b) \cdot x.$$

Hence $\cdot$ is a group action. We call $\cdot$ the *trivial group action.*

Of course, our motivating idea for this chapter produces an example of a group action.

Example 3.1.4. Let $n \in \mathbb{N}$, let $X = \{1, \ldots, n\}$, and consider the group $(S_n, \circ)$. Define the map $\cdot : S_n \times X \to X$ by

$$\sigma \cdot x = \sigma(x)$$

for all $\sigma \in S_n$ and $x \in X$. We claim that $\cdot$ is a group action. To see this, note

$$e \cdot x = e(x) = x$$

for all $x \in X$. Moreover, for all $\sigma, \gamma \in S_n$ and $x \in X$ we see that

$$\sigma \cdot (\gamma \cdot x) = \sigma \cdot \gamma(x) = \sigma(\gamma(x)) = (\sigma \circ \gamma)(x) = (\sigma \circ \gamma) \cdot x.$$

Hence $\cdot$ is a group action.

Moreover, our construction of the dihedral groups implicitly made use of a group action.

Example 3.1.5. Let $n \in \mathbb{N}$, let X be the vertices of a regular n-gon, and consider the group $(D_n, \circ)$. Define the map $\cdot : D_n \times X \to X$ by

$$\sigma \cdot x = \sigma(x).$$

Then $\cdot$ is a group action by the same argument as Example 3.1.4.

Unsurprisingly, there are many group actions inspired by linear algebra.

Example 3.1.6. Let $X = \mathbb{R}^n$ and consider the group $(GL_n, \times)$. Define the map $\cdot : GL_n \times \mathbb{R}^n \to \mathbb{R}^n$ by

$$A \cdot \vec{x} = A\vec{x}$$

for all $A \in GL_n$ and $\vec{x} \in \mathbb{R}^n$ (where $A\vec{x}$ denotes matrix multiplication). We claim that $\cdot$ is a group action. To see this, note

$$I_n \cdot \vec{x} = I_n\vec{x} = \vec{x}$$

for all $\vec{x} \in \mathbb{R}^n$. Moreover, for all $A, B \in GL_n$ and $\vec{x} \in \mathbb{R}^b$ we see that

$$A \cdot (B \cdot \vec{x}) = A \cdot (B\vec{x}) = A(B\vec{x}) = (AB)\vec{x} = (A \times B) \cdot \vec{x}.$$

Hence $\cdot$ is a group action.

By modifying the above group action, we have a group action for every group of a similar vein.

Example 3.1.7. Let $(G, *)$ be a group and let $X = G$. Define the map $\cdot : G \times X \to X$ by

$$a \cdot x = a * x$$

for all $a \in G$ and $x \in X$. We claim that $\cdot$ is a group action. To see this, note $e \cdot x = e * x = x$ for all $x \in X$. Moreover, for all $a, b \in G$ and $x \in X$ we see that

$$a \cdot (b \cdot x) = a \cdot (b * x) = a * (b * x) = (a * b) * x = (a * b) \cdot x.$$

Hence $\cdot$ is a group action. We call $\cdot$ the *left group action*.

Going back to liner algebra, the notion of conjugation by a matrix is an example of a group action as the following example shows.

Example 3.1.8. Let $n \in \mathbb{N}$, let $X = M_n$, and consider the group $(GL_n, \times)$. Define the map $\cdot : GL_n \times M_n \to M_n$ by

$$V \cdot A = VAV^{-1}$$

for all $A \in M_n$ and $V \in GL_n$. We claim that $\cdot$ is a group action. To see this, note $I_n \cdot A = I_n A I_n^{-1} = A$ for all $A \in M_n$. Moreover, for all $V, W \in GL_n$ and $A \in M_n$ we see that

$$\begin{aligned} V \cdot (W \cdot A)) &= V \cdot (WAW^{-1}) \\ &= VWAW^{-1}V^{-1} \\ &= VWA(VW)^{-1} \\ &= VW \cdot A \\ &= (V \times W) \cdot A. \end{aligned}$$

Hence $\cdot$ is a group action.

Unsurprisingly, we can modify the above group action to obtain a very important group action for an arbitrary group.

Example 3.1.9. Let $(G, *)$ be a group and let $X = G$. Define the map $\cdot : G \times X \to X$ by

$$a \cdot x = a * x * a^{-1}$$

for all $a \in G$ and $x \in X$. We claim that $\cdot$ is a group action. To see this, note $e \cdot x = e * x * e^{-1} = x$ for all $x \in X$. Moreover, for all $a, b \in G$ and $x \in X$ we see that

$$\begin{aligned} a \cdot (b \cdot x) &= a \cdot (b * x * b^{-1}) \\ &= a * (b * x * b^{-1}) * a^{-1} \\ &= (a * b) * x * (a * b)^{-1} \\ &= (a * b) \cdot x. \end{aligned}$$

Hence $\cdot$ is a group action. We call $\cdot$ the *conjugation group action*. The element $a * b * a^{-1}$ is called the *conjugate of b by a*.

In particular, the group actions from Example 3.1.9 will be the focus of Section 3.5.

3.2 Cayley's Theorem

Before we start to apply group actions, it is best that we have a deeper understanding of what they actually are. In this section, we will see there is a deep connection between group actions of G on X and homomorphisms of G into the permutations on the set X that parallels our motivating example for group actions of $(S_n, \circ)$ acting on $\{1, \ldots, n\}$. This will lead us to the intriguing Cayley's Theorem (Theorem 3.2.5) that shows one can study all finite groups by studying just the symmetric groups.

To begin, for a fixed set X, let S_X denote the set of all permutations on the set X; that is,

$$S_X = \{f : X \to X \mid f \text{ is a bijection}\}.$$

By Example 1.2.30, $(S_X, \circ)$ is a group, which we also call a *symmetric group*. Recall if $X = \{1, \ldots, n\}$ then $S_X = S_n$.

Unfortunately we do not obtain any new groups by consider $(S_X, \circ)$ for an arbitrary set X as the following result shows.

Lemma 3.2.1. *Let X be a set with $|X| = n$. Then $(S_X, \circ) \cong (S_n, \circ)$.*

Proof. Since $|X| = n$, there exists a bijection $f : X \to \{1, \ldots, n\}$. Define $\varphi : S_n \to S_X$ by

$$\varphi(\sigma) = f^{-1} \circ \sigma \circ f$$

for all $\sigma \in S_n$. Note $\varphi(\sigma) : X \to X$ is a bijection for all $\sigma \in S_n$ since the composition of bijections is a bijection and since σ and f are bijections. Hence φ does indeed map into S_X.

We claim that φ is a homomorphism. Indeed note for all $\sigma, \gamma \in S_n$ that

$$\begin{aligned}\varphi(\sigma \circ \gamma) &= f^{-1} \circ (\sigma \circ \gamma) \circ f \\ &= f^{-1} \circ \sigma \circ f \circ f^{-1} \circ \gamma \circ f \\ &= \varphi(\sigma) \circ \varphi(\gamma).\end{aligned}$$

Hence φ is a homomorphism.

Similarly, define $\psi : S_X \to X_n$ by

$$\psi(g) = f \circ g \circ f^{-1}$$

for all $g \in S_X$. By the same arguments, ψ is a homomorphism. Therefore, since $\psi = \varphi^{-1}$, we obtain that φ and ψ are invertible and thus isomorphisms. Hence $(S_X, \circ) \cong (S_n, \circ)$. ∎

Given a homomorphism of a group $(G, *)$ into a permutation group S_X, we immediately obtain a new example of group actions similar to our motivating example of $(S_n, \circ)$ acting on $\{1, \ldots, n\}$ (which is the case $X = \{1, \ldots, n\}$, $G = S_n$, and $\varphi = \text{id}$ in the following).

Lemma 3.2.2. *Let $(G, *)$ be a group, let X be a set, and let $\varphi : G \to S_X$ be a group homomorphism. If $\cdot : G \times X \to X$ is defined by*

$$a \cdot x = \varphi(a)(x)$$

for all $a \in G$ and $x \in X$, then $\cdot$ is a group action of G on X.

Proof. To see that $\cdot$ is a group action of G on X, first note for all $x \in X$ that

$$e \cdot x = \varphi(e)(x) = \mathrm{id}(x) = x.$$

Moreover, for all $a, b \in G$ and $x \in X$, we see that

$$\begin{aligned} a \cdot (b \cdot x) &= a \cdot (\varphi(b)(x)) \\ &= \varphi(a)(\varphi(b)(x)) \\ &= (\varphi(a) \circ \varphi(b))(x) \\ &= \varphi(a * b)(x) \\ &= (a * b) \cdot x. \end{aligned}$$

Hence $\cdot$ is a group action. ∎

As a converse of Lemma 3.2.2, the following shows that every G-set X arises via the group action in Lemma 3.2.2 for some homomorphism $\varphi : G \to S_X$.

Lemma 3.2.3. *Let $(G, *)$ be a group and let X be a G-set. For each $a \in G$, the map $\tau_a : X \to X$ defined by $\tau_a(x) = a \cdot x$ is a permutation of X. Moreover, the map $\varphi : G \to S_X$ defined by $\varphi(a) = \tau_a$ for all $a \in G$ is a homomorphism.*

Proof. Fix $a \in G$. To see that τ_a is a bijection and thus an element of S_X, we claim that τ_a is invertible as a function. To see this, we claim that $\tau_{a^{-1}}$ is the inverse of τ_a. To see this, note for all $x \in X$ that

$$\tau_a(\tau_{a^{-1}}(x)) = \tau_a(a^{-1} \cdot x) = a \cdot (a^{-1} \cdot x) = (a * a^{-1}) \cdot x = e \cdot x = x$$

and

$$\tau_{a^{-1}}(\tau_a(x)) = \tau_{a^{-1}}(a \cdot x) = a^{-1} \cdot (a \cdot x) = (a^{-1} * a) \cdot x = e \cdot x = x.$$

Hence τ_a is invertible as a function so $\tau_a \in S_X$ as desired.

To see that φ is a homomorphism, let $a, b \in G$ be arbitrary. Then for all $x \in X$ we have that

$$\begin{aligned} \varphi(a * b)(x) &= \tau_{a*b}(x) \\ &= (a * b) \cdot x \\ &= a \cdot (b \cdot x) \\ &= \tau_a(b \cdot x) \\ &= \varphi(a)(b \cdot x) \\ &= \varphi(a)(\tau_b(x)) \\ &= \varphi(a)(\varphi(b)(x)) \\ &= (\varphi(a) \circ \varphi(b))(x). \end{aligned}$$

Therefore, since $x \in X$ was arbitrary, we obtain that $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ for all $a, b \in G$. Hence φ is a homomorphism. ∎

Remark 3.2.4. As discussed, it is not difficult to see that the operation of obtaining a group action of G on X from a homomorphism $\varphi : G \to S_X$ from Lemma 3.2.2 and the action of obtaining a homomorphism $\varphi : G \to S_X$ from a group action of G on X in Lemma 3.2.3 are inverses of each other. Hence there is a bijection between group actions of G on X and homomorphisms from G to S_X.

Using these ideas and a specific group action we have already seen, we come to another main result of this course.

Theorem 3.2.5 (Cayley's Theorem). *Every group is isomorphic to a subgroup of a symmetric group. Moreover, every group of order n is isomorphic to a subgroup of S_n.*

Proof. Let $(G, *)$ be a group. Let $X = G$ and let G act on X by left group action as in Example 3.1.7. By Lemma 3.2.3, if $\tau_a : X \to X$ is defined by

$$\tau_a(x) = a \cdot x = a * x$$

for all $a \in G$ and $x \in X$, and if $\varphi : G \to S_X$ is defined by $\varphi(a) = \tau_a$ for all $a \in G$, then φ is a homomorphism.

Recall $\{e\} \subseteq \ker(\varphi)$. We claim that $\ker(\varphi) = \{e\}$. To see this, assume $a \in \ker(\varphi)$. Hence $\varphi(a) = \mathrm{id}$ so $\tau_a(x) = x$ for all $x \in X$. Therefore $a * x = x$ for all $x \in X = G$. Thus $a * a = a$ so $a = e$ by cancellation. Hence $\ker(\varphi) = \{e\}$.

By the First Isomorphism Theorem (Theorem 2.8.1), we obtain that $G \cong \mathrm{Im}(\varphi)$. Therefore, since $\mathrm{Im}(\varphi) \leq S_X$, $(G, *)$ is isomorphic to a subgroup of a symmetric group.

Finally, if $|G| = n$ then $|X| = n$. By Lemma 3.2.1 there exists an isomorphism $\psi : S_X \to S_n$. Therefore $\psi \circ \varphi : G \to S_n$ is a homomorphism with kernel $\{e\}$. Hence the First Isomorphism Theorem (Theorem 2.8.1) implies that $G \cong \mathrm{Im}(\psi \circ \varphi)$. Therefore, since $\mathrm{Im}(\psi \circ \varphi) \leq S_n$, the result follows. ∎

By Cayley's Theorem (Theorem 3.2.5), in order to understand and construct all groups of order n, we just need to understand and construct all subgroups of $(S_n, \circ)$ of order n. However, since $|S_n| = n!$, and since $n!$ grows very quickly in n, this is easier said than done.

3.3 Kernels, Stabilizers, and Orbits

So far we have seen group actions are quite powerful as, for example, they let us prove Cayley's Theorem (Theorem 3.2.5). As such, for an arbitrary G-set X, it is likely useful for us to obtain more information about the relationships between elements of G and elements of X. This will be done in this section by

describing subsets of G and of X based on the group action. We begin with the following idea that occurred in the proof of Cayley's Theorem (Theorem 3.2.5).

Definition 3.3.1. Let $(G, *)$ be a group and let X be a G-set. The *kernel of* $G \curvearrowright X$, denoted $\ker(G \curvearrowright X)$, is the set

$$\ker(G \curvearrowright X) = \{a \in G \mid a \cdot x = x \text{ for all } x \in X\}.$$

An action is said to be *faithful* if $\ker(G \curvearrowright X) = \{e\}$.

Remark 3.3.2. Note $a \in$ if and only if $a \cdot x = x$ for all $x \in X$ if and only if the map τ_a from Lemma 3.2.3 is the identity map.

Example 3.3.3. Let $(G, *)$ be a group. Let $X = G$ and let G act on X by left group action as in Example 3.1.7. Note $a \in \ker(G \curvearrowright X)$ if and only if $a \cdot x = x$ for all $x \in X$ if and only if $a * b = b$ for all $b \in G$ if and only of $a = e$. Hence the left group action is faithful. In fact, in the proof of Cayley's Theorem (Theorem 3.2.5), we could have used any faithful group action of $(G, *)$ on itself.

However, for most applications, the kernel of a group action is too small of an object. For example, it is just $\{e\}$ for the left group action and thus we obtain no information about a group by examining the kernel of the left group action. We need some larger subsets of $(G, *)$. This can be accomplished by replacing the "for all $x \in X$" in the definition of the kernel with 'a fixed $x \in X$'. Such objects are formally defined as follows.

Definition 3.3.4. Let $(G, *)$ be a group, let X be a G-set, and let $x \in X$. The *stabilizer of* x, denoted G_x, is the set

$$G_x = \{a \in G \mid a \cdot x = x\}.$$

Note the stabilizer of x includes all the elements of $(G, *)$ that keep x 'stable' (i.e. unchanged).

Remark 3.3.5. For a group action $G \curvearrowright X$, it is not difficult to see based on the above definitions that

$$\ker(G \curvearrowright X) = \bigcap_{x \in X} G_x.$$

Stabilizers for the conjugation group action are very important and will be a main focus of Section 3.5. For now, let us look at some other group actions.

Example 3.3.6. Let $n \in \mathbb{N}$, let $X = \{1, \ldots, n\}$, and consider the group $(S_n, \circ)$ and the group action $S_n \curvearrowright X$ from Example 3.1.4; that is, $\sigma \cdot x = \sigma(x)$. Note that

$$G_n = \{\sigma \in S_n \mid \sigma(n) = n\}.$$

Thus G_n really looks like S_{n-1} with the additional assumption that elements of S_{n-1} map n to n. In this way, we can view $S_{n-1} = G_n \subseteq S_n$.

Example 3.3.7. Let $X = \{1, 2, 3, 4\}$ and consider the group D_4. With the elements of D_4 acting on X as they do in Example 1.6.18 (i.e. acting as permutations on X), we see that the only symmetries that fix the vertex 1 are the identity and the reflection across the diagonal $(1, 3)$. Therefore

$$G_1 = \{e, \rho \circ \tau\}.$$

Similarly, the only symmetries that fix the vertex 2 are the identity and the reflection across $(2, 4)$ so

$$G_2 = \{e, \rho^2 \circ \tau\}.$$

By similar arguments,

$$G_3 = \{e, \rho \circ \tau\} \quad \text{and} \quad G_4 = \{e, \rho^2 \circ \tau\}.$$

Hence

$$\ker(D_4 \curvearrowright X) = \{e\}.$$

Example 3.3.8. Let $X = \mathbb{R}^n$ and let $(GL_n, \times)$ act on X via matrix multiplication as in Example 3.1.6; that is $A \cdot \vec{x} = A\vec{x}$. Note for all $\vec{x} \in X$ that

$$G_x = \{A \in GL_n \mid \vec{x} \text{ is an eigenvector for } A \text{ with eigenvalue } 1\}.$$

Hence

$$\ker(G \curvearrowright X) = \{e\}.$$

Unsurprisingly based on the above examples, stabilizers are nice subset of $(G, *)$. In particular, we have the following.

Proposition 3.3.9. *Let $(G, *)$ be a group and let X be a G-set. For all $x \in X$, the stabilizer of x is a subgroup of $(G, *)$. Hence $\ker(G \curvearrowright X)$ is a subgroup of $(G, *)$.*

Proof. To see that $G_x \leq G$, we need only verify the three properties from Definition 1.5.7.

First, to see that $e \in G_x$, note since $e \cdot x = x$ by the definition of a group action (Definition 3.1.1), we obtain that $e \in G_x$.

Next, to see that G_x is closed under products, let $a, b \in G_x$ be arbitrary. Hence $a \cdot x = x$ and $b \cdot x = x$. Therefore, by the properties of a group action, we obtain that

$$(a * b) \cdot x = a \cdot (b \cdot x) = a \cdot x = x.$$

Hence $a * b \in G_X$ by definition. Therefore, since $a, b \in G_x$ were arbitrary, G_x is closed under products.

Finally, to see that G_x is closed under inverses, let $a \in G_x$ be arbitrary. Therefore $a \cdot x = x$. Thus, by the properties of a group action,

$$a^{-1} \cdot x = a^{-1} \cdot (a \cdot x) = (a^{-1} * a) \cdot x = e \cdot x = x.$$

Therefore, since $a \in G_x$ was arbitrary, G_x is closed under inverses.

Therefore, since we have verified the three properties from Definition 1.5.7, $G_X \leq G$ as desired.

Since $\ker(G \curvearrowright X) = \bigcap_{x \in X} G_x$ and since $G_x \leq G$ for all $x \in X$, it follows that $\ker(G \curvearrowright X)$ is a subgroup of $(G, *)$ by Corollary 1.5.10. ∎

On the other hand, instead of looking at a nice subset of $(G, *)$, we can look at a nice subset of X. In particular, given an element $x \in X$, it would be interesting to know all of the elements in X that can be obtained by applying the group action to x. We define this set as follows.

Definition 3.3.10. Let $(G, *)$ be a group, let X be a G-set, and let $x \in X$. The *orbit of* x, denoted $\mathcal{O}_x$, is the set

$$\mathcal{O}_x = \{y \in X \mid \text{there exists a } a \in G \text{ such that } a \cdot x = y\}.$$

For our motivating example of a group action, it is unsurprising that we can get from every element to every other element.

Example 3.3.11. Let $n \in \mathbb{N}$, let $X = \{1, \ldots, n\}$, and consider the group $(S_n, \circ)$ and the group action $S_n \curvearrowright X$ from Example 3.1.4; that is, $\sigma \cdot x = \sigma(x)$. Fix $x \in X$. To compute $\mathcal{O}_x \subseteq X$, note that for any $y \in X$ we have $\sigma = \begin{pmatrix} x & y \end{pmatrix} \in S_n$ is such that $\sigma \cdot x = \sigma(x) = y$. Hence $\mathcal{O}_x = X$ for all $x \in X$.

Example 3.3.12. Let $X = \{1, 2, 3, 4\}$ and consider the group D_4. With the elements of D_4 acting on X as they do in Example 1.6.18 (i.e. acting as permutations on X), we claim that $\mathcal{O}_1 = X$. Indeed note that

$$e \cdot 1 = 1, \quad \rho \cdot 1 = 4, \quad \rho^2 \cdot 1 = 3, \quad \text{and} \quad \rho^3 \cdot 1 = 2.$$

Hence $\mathcal{O}_1 = X$. By similar arguments $\mathcal{O}_2 = \mathcal{O}_3 = \mathcal{O}_4 = X$.

In the context of linear algebra, we start to see some different types of orbits.

Example 3.3.13. Let $X = \mathbb{R}^n$ and let $(GL_n, \times)$ act on X via matrix multiplication as in Example 3.1.6; that is $A \cdot \vec{x} = A\vec{x}$. Fix $\vec{x} \in X$. We divide the computation of $\mathcal{O}_{\vec{x}}$ into two cases.

If $\vec{x} = \vec{0}$, then $A \cdot \vec{x} = \vec{0}$ for all $A \in GL_n$ and thus

$$\mathcal{O}_0 = \left\{\vec{0}\right\}.$$

If $\vec{x} \neq \vec{0}$, we claim that $\mathcal{O}_{\vec{x}} = \mathbb{R}^n \setminus \{\vec{0}\}$. To see that $\vec{0} \notin \mathcal{O}_{\vec{x}}$, suppose for the sake of a contradiction that $\vec{0} \in \mathcal{O}_{\vec{x}}$. Hence, by the definition of the orbit, there exists an $A \in GL_n$ such that $\vec{0} = A \cdot \vec{x} = A\vec{x}$. Thus $\vec{x} \in \ker(A)$. However, since $A \in GL_n$, A is invertible and thus $\ker(A) = \{\vec{0}\}$. Thus $\vec{x} = \vec{0}$, which is a contradiction. Hence $\vec{0} \notin \mathcal{O}_{\vec{x}}$. Hence $\mathcal{O}_{\vec{x}} \subseteq \mathbb{R}^n \setminus \{\vec{0}\}$.

To see the other inclusion, let $\vec{y} \in \mathbb{R}^n \setminus \{\vec{0}\}$ be arbitrary. By extending $\{\vec{x}\}$ and $\{\vec{y}\}$ to bases for $\mathbb{R}^n$, there is a change of basis matrix $A \in M_n$ such that $A\vec{x} = \vec{y}$. Since A is a change of basis matrix, A is invertible so $A \in GL_n$. Therefore, since $A \cdot \vec{x} = \vec{y}$, we obtain that $\vec{y} \in \mathcal{O}_{\vec{x}}$. Therefore, since $\vec{y}$ was arbitrary, $\mathcal{O}_{\vec{x}} = \mathbb{R}^n \setminus \{\vec{0}\}$.

The following example begins to show us we can obtain some important structural information by looking at orbits.

Example 3.3.14. Let $X = \mathbb{R}^4$. Consider the group $(GL_4, \times)$ and the set

$$H = \{A_1 \oplus A_2 \mid A_1, A_2 \in GL_2\}$$

where

$$A_1 \oplus A_2 = \begin{bmatrix} A_1 & 0_2 \\ 0_2 & A_2 \end{bmatrix}$$

where 0_2 is the 2×2 zero matrix. Since $I_2 \oplus I_2 = I_4$, since

$$(A_1 \oplus A_2) \times (B_1 \oplus B_2) = A_1B_1 \oplus A_2B_2,$$

and since

$$(A_1 \oplus A_2)^{-1} = A_1^{-1} \oplus A_2^{-1},$$

we see that $H \leq GL_4$.

Let H act on $\mathbb{R}^4$ via matrix multiplication; that is $A \cdot \vec{x} = A\vec{x}$. Let

$$\vec{x} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \vec{z} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{and} \quad \vec{w} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Note for all $A_1 \oplus A_2 \in H$ that

$$(A_1 \oplus A_2) \cdot \vec{x} = A_1\vec{z} \oplus \vec{w}.$$

Thus the action of H on $\mathbb{R}^4$ always produces zeros in the third and fourth entries of the vector and can produce any vector of the form $A_1\vec{z}$ where $A_1 \in GL_2$ as entries in the first two entries. Hence, by Example 3.3.13, we see that

$$\mathcal{O}_{\vec{x}} = \left\{ \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} \middle| \, a, b \in \mathbb{R}, \text{ one of } a \text{ or } b \text{ is non-zero} \right\}.$$

With the notion of orbits in hand, it is natural to consider comparing the orbits of group elements. It turns out that doing so gives us an interesting (equivalence) relation between elements of X.

Proposition 3.3.15. *Let $(G, *)$ be a group and let X be a G-set. For $x, y \in X$, define $x \sim y$ if and only if $x \in \mathcal{O}_y$. Then $\sim$ is an equivalence relation on X.*

Proof. To verify that $\sim$ is an equivalence relation, we must verify that $\sim$ is reflexive, symmetric, and transitive.

To see that $\sim$ is reflexive, let $x \in X$. Since $e \cdot x = x$, we see that $x \in \mathcal{O}_x$. Hence $x \sim x$. Therefore $\sim$ is reflexive.

To see that $\sim$ is symmetric, let $x, y \in X$ be such that $x \sim y$. Thus $x \in \mathcal{O}_y$ so there exists an $a \in G$ such that $a \cdot y = x$. Note $a^{-1} \in G$ and

$$a^{-1} \cdot x = a^{-1} \cdot (a \cdot y) = (a^{-1} * a) \cdot y = e \cdot y = y$$

so $y \in \mathcal{O}_x$. Hence $y \sim x$ so $\sim$ is symmetric.

To see that $\sim$ is transitive, let $x, y, z \in X$ be such that $x \sim y$ and $y \sim z$. Thus $x \in \mathcal{O}_y$ and $y \in \mathcal{O}_z$ so there exists $a, b \in G$ such that $a \cdot y = x$ and $b \cdot z = y$. Therefore $a * b \in G$ and

$$(a * b) \cdot z = a \cdot (b \cdot z) = a \cdot y = x.$$

Hence $x \in \mathcal{O}_z$ so $x \sim z$. Therefore, since x, y, and z were arbitrary, $\sim$ is transitive.

Therefore, since $\sim$ is reflexive, symmetric, and transitive, $\sim$ is an equivalence relation. ∎

The equivalence relation from Proposition 3.3.15 is quite important in the context of group actions and thus is given a name. At least the name is easy to remember.

Definition 3.3.16. Let $(G, *)$ be a group and let X be a G-set. The equivalence relation from Proposition 3.3.15 is called the *orbit equivalence relation*.

The main reason stabilizers and orbits are both included in this section is that these two concepts are intimately related via the following result.

Theorem 3.3.17 (The Orbit-Stabilizer Relation). *Let $(G, *)$ be a group, let X be a G-set, and let $x \in X$. Then*

$$|\mathcal{O}_x| = [G : G_x].$$

Proof. To show that $|\mathcal{O}_x| = [G : G_x]$, it suffices to construct a bijection from $\mathcal{O}_x$ to the set of left cosets of G_x in G. Let $\mathcal{L} = \{aG_x \mid a \in G\}$. Recall

$$\mathcal{O}_x = \{a \cdot x \in X \mid a \in G\}.$$

Define $f : \mathcal{O}_x \to \mathcal{L}$ by

$$f(a \cdot x) = aG_x$$

for all $a \in G$. Note since we are defining f based on representations of elements of $\mathcal{O}_x$ and there may be multiple ways to write an element of $\mathcal{O}_x$ in this form, we need to verify that f is well-defined; that is, if $a, b \in G$ are such that $a \cdot x = b \cdot x$, then $aG_x = bG_x$. To see this, assume $a, b \in G$ are such that $a \cdot x = b \cdot x$. Therefore

$$(b^{-1} * a) \cdot x = b^{-1} \cdot (a \cdot x) = b^{-1} \cdot (b \cdot x) = (b^{-1} * b) \cdot x = e \cdot x = x.$$

Hence $b^{-1} * a \in G_x$ so $aG_x = bG_x$. Therefore f is well-defined.

To see that f is a bijection, first notice that f is clearly surjective since for any $a \in G$, we have $a \cdot x \in \mathcal{O}_x$ and

$$aG_x = f(a \cdot x).$$

To see that f is injective, assume $a, b \in G$ are such that $f(a \cdot x) = f(b \cdot x)$. Hence $aG_x = bG_x$ so $b^{-1} * a \in G_x$. Thus $(b^{-1} * a) \cdot x = x$ by the definition of G_x. Therefore

$$\begin{aligned} b \cdot x &= b \cdot ((b^{-1} * a) \cdot x) \\ &= b \cdot (b^{-1} \cdot (a \cdot x)) \\ &= (b * b^{-1}) \cdot (a \cdot x) \\ &= e \cdot (a \cdot x) \\ &= (e * a) \cdot x \\ &= a \cdot x. \end{aligned}$$

Thus $a \cdot x = b \cdot x$. Therefore, since $a, b \in G$ were arbitrary, f is injective.

Hence f is a bijection so $|\mathcal{O}_x| = [G : G_x]$ as desired. ∎

Although the Orbit-Stabilizer Relation (Theorem 3.3.17) makes it obvious, we present some examples that show it holds in specific contexts.

Example 3.3.18. Let $n \in \mathbb{N}$, let $X = \{1, \ldots, n\}$, and consider the group $(S_n, \circ)$ and the group action $S_n \curvearrowright X$ from Example 3.1.4; that is, $\sigma \cdot x = \sigma(x)$. Recall $\mathcal{O}_n = X$ so $|\mathcal{O}_n| = n$ whereas $|G_n| = |S_{n-1}| = (n-1)!$ so

$$[S_n : G_n] = \frac{n!}{(n-1)!} = n = |\mathcal{O}_n|.$$

Example 3.3.19. Let $X = \{1, 2, 3, 4\}$ and consider the group D_4. With the elements of D_4 acting on X as they do in Example 1.6.18 (i.e. acting as permutations on X), we recall that $\mathcal{O}_1 = X$ so $|\mathcal{O}_1| = 4$ whereas $|G_1| = 2$ so

$$[D_n : G_1] = \frac{8}{2} = 4 = |\mathcal{O}_1|.$$

It is important to note the Orbit-Stabilizer Relation (Theorem 3.3.17) implies the following.

Corollary 3.3.20. *Let $(G, *)$ be a finite group and let X be a G-set. For any $x \in X$, $|\mathcal{O}_x|$ divides $|G|$.*

Proof. By the Orbit-Stabilizer Relation (Theorem 3.3.17) and the fact that G is finite, we have that

$$|\mathcal{O}_x| = [G : G_x] = \frac{|G|}{|G_x|}$$

so $|G| = |\mathcal{O}_x||G_x|$. Therefore, since $|G|, |\mathcal{O}_x|, |G_x| \in \mathbb{N}$, it follows that $|\mathcal{O}_x|$ divides $|G|$. ∎

Finally, since the orbit equivalence relation is an equivalence relation on X, we immediately obtain the following equation that is most commonly used in the context of the conjugation group action in Section 3.5.

Corollary 3.3.21. *Let $(G, *)$ be a group and let X be a G-set. Assume X is a finite set, n is the number of distinct orbits of $G \curvearrowright X$, and let $x_1, \ldots, x_n \in X$ be one representative from each equivalence class of the orbit equivalence relation. Then*

$$|X| = \sum_{k=1}^{n} |\mathcal{O}_{x_k}| = \sum_{k=1}^{n} [G : G_{x_k}].$$

Proof. Since $\{x_1, \ldots, x_n\}$ consists of exactly one representative from each equivalence class of the orbit equivalence relation, and since equivalence classes from an equivalence relation partition the set on which they act, we obtain that

$$X = \bigcup_{k=1}^{n} \mathcal{O}_{x_k}.$$

Moreover, since distinct equivalence classes are pairwise disjoint, we obtain that

$$|X| = \sum_{k=1}^{n} |\mathcal{O}_{x_k}|.$$

Therefore, by the Orbit-Stabilizer Relation (Theorem 3.3.17), we obtain that

$$|X| = \sum_{k=1}^{n} [G : G_{x_k}]$$

as desired. ∎

3.4 Burnside's Lemma

There are some other sets that can be defined for a G-set X. In this section, we will look at one such example, prove Burnside's Lemma (Theorem 3.4.5) to obtain information about this set, and apply said theorem as an application of group actions to combinatorics.

We begin with the interesting set for a G-set. This set is formed by looking at all points in a G-set that remain invariant under the action of a fixed element of G.

Definition 3.4.1. Let $(G, *)$ be a group, let $a \in G$, and let X be a G-set. The *fixed point set of* a, denoted X_g, is the set

$$X_a = \{x \in X \mid a \cdot x = x\}.$$

Unsurprisingly, this notion and its name is based on our motivating example of a group action.

Example 3.4.2. Let $X = \{1, \ldots, 9\}$, and consider the group $(S_9, \circ)$ and the group action $S_n \curvearrowright X$ from Example 3.1.4; that is, $\sigma \cdot x = \sigma(x)$. Let

$$\sigma = \begin{pmatrix} 1 & 7 & 5 \end{pmatrix} \begin{pmatrix} 4 & 8 \end{pmatrix}.$$

Then

$$X_\sigma = \{2, 3, 6, 9\}.$$

Looking at the dihedral groups and $(GL_n, \times)$, we also see that fixed point sets are aptly named.

Example 3.4.3. Let $X = \{1, 2, 3, 4\}$ and consider the group D_4. With the elements of D_4 acting on X as they do in Example 1.6.18 (i.e. acting as permutations on X), we see that

$$\begin{aligned} X_e &= \{1, 2, 3, 4\} & X_\rho &= \emptyset \\ X_{\rho^2} &= \emptyset & X_{\rho^3} &= \emptyset \\ X_\tau &= \emptyset & X_{\rho\circ\tau} &= \{1, 3\} \\ X_{\rho^2\circ\tau} &= \emptyset & X_{\rho^3\circ\tau} &= \{2, 4\}. \end{aligned}$$

Example 3.4.4. Let $X = \mathbb{R}^n$ and let $(GL_n, \times)$ act on X via matrix multiplication as in Example 3.1.6; that is $A \cdot \vec{x} = A\vec{x}$. For $A \in GL_n$, note that

$$X_A = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{x}\};$$

that is, X_A is the eigenspace for A corresponding to the eigenvalue 1.

We now arrive at the main result of this section which relates the number of orbits to the number of elements in all fixed point sets.

Theorem 3.4.5 (Burnside's Lemma). *Let $(G, *)$ be a finite group acting on a finite set X. If N is the number of orbits of $G \curvearrowright X$, then*

$$N = \frac{1}{|G|} \sum_{a \in G} |X_a|.$$

Proof. Let

$$Y = \{(a, x) \mid a \in G, x \in X, a \cdot x = x\} \subseteq G \times X.$$

The proof of the result mostly boils down to computing $|Y|$ in two ways.

For our first way to compute $|Y|$, note that

$$Y = \{(a, x) \mid a \in G, x \in X_a\}.$$

Therefore, for each $a \in G$ there are $|X_a|$ elements in Y whose first entry is a so

$$|Y| = \sum_{a \in G} |X_a|.$$

For our second way to compute $|Y|$, note that

$$Y = \{(a, x) \mid x \in X, a \in G_x\}.$$

Therefore, for each $x \in X$ there are $|G_x|$ element in Y whose second entry is x so

$$|Y| = \sum_{x \in X} |G_x|.$$

Recall $[G : G_x] = \frac{|G|}{|G_x|}$. Moreover, by the Orbit-Stabilizer Relation (Theorem 3.3.17), we know that $[G : G_x] = |\mathcal{O}_x|$. Hence

$$|Y| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}.$$

Therefore, by equating with our first expression for $|Y|$, we obtain that

$$\frac{1}{|G|} \sum_{a \in G} |X_a| = \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}.$$

To complete the proof, it suffices to prove that

$$\sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = N,$$

where N is the number of orbits of $G \curvearrowright X$. Let $x_1, x_2, \ldots, x_N \in X$ be one representative from each orbit equivalence class. Therefore, since X is the disjoint union of $\mathcal{O}_{x_1}, \ldots \mathcal{O}_{x_N}$, we obtain that

$$\sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = \sum_{k=1}^{N} \sum_{x \in \mathcal{O}_{x_k}} \frac{1}{|\mathcal{O}_x|}.$$

However, if $x \in \mathcal{O}_{x_k}$ then $\mathcal{O}_x = \mathcal{O}_{x_k}$ by Proposition 3.3.15 so $|\mathcal{O}_x| = |\mathcal{O}_{x_k}|$. Therefore

$$\begin{aligned}\sum_{x\in X} \frac{1}{|\mathcal{O}_x|} &= \sum_{k=1}^{N} \sum_{x\in\mathcal{O}_{x_k}} \frac{1}{|\mathcal{O}_x|} \\ &= \sum_{k=1}^{N} \sum_{x\in\mathcal{O}_{x_k}} \frac{1}{|\mathcal{O}_{x_k}|} \\ &= \sum_{k=1}^{N} |\mathcal{O}_{x_k}| \frac{1}{|\mathcal{O}_{x_k}|} \\ &= \sum_{k=1}^{N} 1 = N\end{aligned}$$

thereby completing the proof. ∎

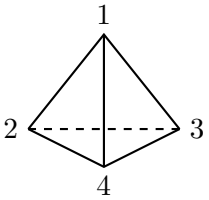
We quickly return to one of our previous examples to show how the computation in Burnside's Lemma (Theorem 3.4.5) works.

Example 3.4.6. Let $X = \{1, 2, 3, 4\}$ and consider the group D_4. With the elements of D_4 acting on X as they do in Example 1.6.18 (i.e. acting as permutations on X), recall from Example 3.3.12 that this group action has exactly one orbit. Moreover, by Example 3.4.3,

$$\frac{1}{|G|} \sum_{g\in G} |X_g| = \frac{1}{8}(4 + 0 + 0 + 0 + 0 + 2 + 0 + 2) = 1.$$

The significance of Burnside's Lemma (Theorem 3.4.5) is that it can be used to solve many problems in combinatorics (see MATH 4160). We present one here to show the importance and power of groups outside of Algebra.

Example 3.4.7. Consider a regular tetrahedron:



Assume we are given three colours in which to paint the four vertices of the tetrahedron. Up to symmetries (i.e. rotating the tetrahedron), how many uniquely coloured tetrahedron can we produce?

First, let us ignore the symmetries. As there are four vertices and three colours, there are $3^4 = 81$ possible ways we can colour the tetrahedron as

shown the diagram. Let X denote this set of coloured tetrahedron. Thus $|X| = 81$. However, there are elements of X that are equal with respect to some symmetry. How can we resolve this?

To resolve this, we must first ask, "What are the symmetries of the tetrahedron?" As the identity map is a symmetry, as the composition of two symmetries is a symmetry, and the inverse of a symmetry is a symmetry, the set of symmetries of the tetrahedron is a group. Moreover, since we can think of the symmetries of the tetrahedron as a symmetries of the tetrahedron on $\{1, 2, 3, 4\}$, the symmetries of the tetrahedron is a subgroup of S_4.

Note there are three types of symmetries of the tetrahedron: the identity symmetry, fixing one vertex and rotating the opposite face of the tetrahedron, and flipping across the line between the midpoints of two non-adjacent edges. Note the permutations of $\{1, 2, 3, 4\}$ corresponding to fixing one vertex and rotating the opposite face of the tetrahedron are

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}$$

and the permutations of $\{1, 2, 3, 4\}$ corresponding flipping across the line between the midpoints of two non-adjacent edges are

$$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}.$$

Hence the group of symmetries of the tetrahedron is A_4 by Example 1.6.39

Let A_4 act on the X as permutations. Note two elements of X are the same coloured tetrahedron up to symmetry exactly when they are in the same orbit under the action of A_4 on X. Hence the number of orbits of $A_4 \curvearrowright X$ is exactly the number of uniquely coloured tetrahedron we can produce up to symmetries. Thus we can use Burnside's Lemma (Theorem 3.4.5) to compute this number. To do this, we note that $|A_4| = 12$. Thus, we just need to compute $|X_\sigma|$ for all $\sigma \in A_4$.

Note X_e is the number of elements of X (i.e. coloured tetrahedron) that are fixed under the identity element. Since all elements of X are fixed under the action of the identity element e, we obtain that $|X_e| = |X| = 81$.

Next, let r be a symmetry consisting of fixing one vertex and rotating the opposite face of the tetrahedron. A coloured tetrahedron is fixed under r exactly when all three vertices of the triangle being rotated are the same. As there are 3 options for this colour and one option for the colour of the vertex being fixed, we see that $|X_r| = 3^2 = 9$. Note there are 8 such rotations thereby adding 8(81) to the sum in Burnside's Lemma (Theorem 3.4.5).

Finally, let f be a symmetry consisting of a flip across the line between the midpoints of two non-adjacent edges. A coloured tetrahedron is fixed under f exactly when vertices on each edge of the two non-adjacent edges being used in the flip are the same colour. As there are three options for the

colour of the vertices of each edge, we see that $|X_f| = 3^2 = 9$. Note there are 3 such flips thereby adding 3(81) to the sum in Burnside's Lemma (Theorem 3.4.5).

Therefore, Burnside's Lemma (Theorem 3.4.5) implies there are

$$N = \frac{1}{12}(81 + 8(81) + 3(81)) = 15$$

uniquely coloured tetrahedron up to symmetries.

3.5 Conjugacy Classes and Centralizers

Returning to the theory of groups, in this section we will focus on the conjugation group action from Example 3.1.9. It turns out that doing so will enable us to extend our understanding of groups by looking at a specific subgroup that can be defined in any group and obtain information that will enable us to determine, up to isomorphism, all groups of order p^2 for a prime number p.

As the conjugation group action is an group action, the kernel, stabilizers, and orbits all make sense. However, in the context of conjugation group action, these objects are (potentially confusingly) given new names.

Definition 3.5.1. Let $(G, *)$ be a group and let G act on itself by conjugation; that is, G is a G-set via the group action

$$a \cdot g = a * g * a^{-1}$$

for all $a, g \in G$. The *centre of* G, denoted $Z(G)$, is the set

$$\begin{aligned} Z(G) &= \ker(G \curvearrowright G) \\ &= \{a \in G \mid a \cdot g = g \text{ for all } g \in G\} \\ &= \{a \in G \mid a * g * a^{-1} = g \text{ for all } g \in G\} \\ &= \{a \in G \mid a * g = g * a \text{ for all } g \in G\}. \end{aligned}$$

That is, the centre of G is the set of all elements of G that commute with all elements of G.

For $a \in G$, the *centralizer of* g *in* G, denoted $C(a)$, is the set

$$\begin{aligned} C(a) &= G_a \\ &= \{b \in G \mid b \cdot a = a\} \\ &= \{b \in G \mid b * a * b^{-1} = a\} \\ &= \{b \in G \mid b * a = a * b\}. \end{aligned}$$

That is, the centralizer of a in G is the set of all elements in G that commute with a. Note that $a \in C(a)$ by taking $b = a$ in the above expression.

Finally, for $a \in G$, the *conjugacy class of a in G*, denoted $K(a)$, is the set

$$\begin{aligned} K(a) &= \mathcal{O}_a \\ &= \{b \in G \mid c \cdot a = b \text{ for some } c \in G\} \\ &= \{b \in G \mid c * a * c^{-1} = b \text{ for some } c \in G\} \\ &= \{c * a * c^{-1} \in G \mid c \in G\}. \end{aligned}$$

That is, the conjugacy class of a in G is the set of all conjugates of a in G. Note $a \in K(a)$ by taking $c = e$ in the above expression.

Remark 3.5.2. Since the centre, centralizer, and conjugacy classes are just examples of kernels, stabilizers, and orbits of from actions respectively, Section 3.3 implies that

- $Z(G) \leq G$ by Proposition 3.3.9,
- $C(a) \leq G$ for all $a \in G$ by Proposition 3.3.9,
- $Z(G) = \bigcap_{a \in G} C(a)$,
- $K(a)$ is the equivalence class of an equivalence relation on G (i.e. $a \sim b$ if and only if $a = g * b * g^{-1}$ for some $g \in G$) by Proposition 3.3.15, and
- $|K(g)| = [G : C(g)]$ so $|K(g)| = \frac{|G|}{|C(g)|}$ when G is finite by the Orbit-Stabilizer Relation (Theorem 3.3.17).

Before we look at examples of centres, centralizers, and stabilizers, it is important to note that the centre of a group has a particularly nice property beyond being a subgroup.

Proposition 3.5.3. *Let $(G, *)$ be a group. The centre $Z(G)$ is an abelian subgroup of $(G, *)$. Moreover $Z(G) \lhd G$.*

Proof. Recall $Z(G) \leq G$ by Proposition 3.3.9. To see that $Z(G)$ is abelian, let $a, b \in Z(G)$ be arbitrary. Since $a \in Z(G)$ and $b \in Z(G) \subseteq G$, we obtain by the definition of $Z(G)$ that $a * b = b * a$. Therefore, since $a, b \in Z(G)$ was arbitrary, $Z(G)$ is abelian.

To see that $Z(G) \lhd G$, note for all $a \in G$ and $b \in Z(G)$ that

$$a * b * a^{-1} = a * a^{-1} * b = e * b = b \in Z(G).$$

Therefore, by the Normal Subgroup Test (Theorem 2.6.10), we have that $Z(G) \lhd G$. ∎

The centre of a group is quite important. In particular, since $Z(G) \lhd G$, we can consider the quotient group $G/Z(G)$. Note that $Z(G)$ is abelian and it can be checked that $G/Z(G)$ has trivial centre; that is $Z(G/Z(G)) = \{e\}$.

This often means that one can understand groups by understanding abelian groups, understanding groups with trivial centre, and understand quotient groups. This idea is left for future courses (MATH 4021 perhaps).

For now, we focus on a few examples to illuminate what $Z(G)$, $C(a)$, and $K(a)$ look like.

Example 3.5.4. Consider $(GL_n, \times)$. We claim that

$$Z(GL_n) = \{\alpha I_n \mid \alpha \in \mathbb{R} \setminus \{0\}\}.$$

To see this, note if $\alpha \in \mathbb{R} \setminus \{0\}$ then

$$(\alpha I_n)A = A(\alpha I_n)$$

for all $A \in GL_n$. Hence

$$\{\alpha I_n \mid \alpha \in \mathbb{R} \setminus \{0\}\} \subseteq Z(GL_n).$$

To see the other inclusion, assume $A \in Z(GL_n)$. Write $A = [a_{i,j}]$ and let

$$B = \operatorname{diag}(1, 2, \ldots, n);$$

that is, B is the diagonal matrix with the entries $1, 2, \ldots, n$ along the diagonal. Then $B \in GL_n$. Thus, since $A \in Z(G)$, we have that

$$AB = BA.$$

Therefore

$$[a_{i,j}j] = [ia_{i,j}].$$

Hence $(i - j)a_{i,j} = 0$ for all $i, j \in \{1, \ldots, n\}$, so $a_{i,j} = 0$ whenever $i \neq j$. Therefore, A must be a diagonal matrix; that is,

$$A = \operatorname{diag}(a_{1,1}, a_{2,2}, \ldots, a_{n,n}).$$

Next, let

$$U = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix};$$

that is, U is the matrix with a 1 at $(i, i+1)$ for all $i \in \{1, 2, \ldots, n-1\}$ (i.e. each entry above the diagonal), a 1 at the $(n, 1)$ entry, and zeros everywhere else. Then U is an invertible matrix with $U^{-1} = U^T$. Thus $U \in GL_n$. Therefore, since $A \in Z(G)$, we obtain that

$$AU = UA.$$

Since

$$AU = \begin{bmatrix} 0 & a_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_{2,2} & 0 & \cdots & 0 \\ 0 & 0 & 0 & a_{3,3} & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{n-1,n-1} \\ a_{n,n} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

and

$$UA = \begin{bmatrix} 0 & a_{2,2} & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_{3,3} & 0 & \cdots & 0 \\ 0 & 0 & 0 & a_{4,4} & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{n,n} \\ a_{1,1} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Hence

$$a_{1,1} = a_{2,2} = \cdots = a_{n,n}$$

so $A = a_{1,1}I_n$. Therefore, since $A \in Z(GL_n)$ was arbitrary,

$$Z(GL_n) = \{\alpha I_n \mid \alpha \in \mathbb{R} \setminus \{0\}\}$$

as desired.

For an arbitrary $A \in GL_n$, it is more difficult to describe $C(A)$. However, note that

$$K(A) = \{VAV^{-1} \in| \ V \in GL_n\};$$

that is, $K(A)$ is the set of all $B \in GL_n$ that has the same Jordan Normal Form as A by MATH 2022.

Example 3.5.5. Consider $(D_4, \circ)$. By analyzing the multiplication table from Example 1.6.18, we see that

$$\begin{aligned} C(e) &= D_4 \\ C(\rho) &= \{e, \rho, \rho^2, \rho^3\} \\ C(\rho^2) &= D_4 \\ C(\rho^3) &= \{e, \rho, \rho^2, \rho^3\} \\ C(\tau) &= \{e, \rho^2, \tau, \rho^2 \circ \tau\} \\ C(\rho \circ \tau) &= \{e, \rho^2, \rho \circ \tau, \rho^3 \circ \tau\} \\ C(\rho^2 \circ \tau) &= \{e, \rho^2, \tau, \rho^2 \circ \tau\} \\ C(\rho^3 \circ \tau) &= \{e, \rho^2, \rho \circ \tau, \rho^3 \circ \tau\}. \end{aligned}$$

Therefore, since $Z(D_4)$ is the intersection of all of the centralizers, we see that

$$Z(D_4) = \{e, \rho^2\}.$$

Finally, by analyzing the multiplication table from Example 1.6.18 and recalling the conjugacy classes are the equivalence class of an equivalence relation on D_4 (i.e. $a \sim b$ if and only if $a = g * b * g^{-1}$ for some $g \in G$), we see that

$$\begin{aligned} K(e) &= \{e\} \\ K(\rho) = K(\rho^3) &= \{\rho, \rho^3\} \\ K(\rho^2) &= \{\rho^2\} \\ K(\tau) = K(\rho^2 \circ \tau) &= \{\tau, \rho^2 \circ \tau\} \\ K(\rho \circ \tau) = K(\rho^3 \circ \tau) &= \{\rho \circ \tau, \rho^3 \circ \tau\} \end{aligned}$$

We can quickly see the following occurs in all of the above examples.

Remark 3.5.6. Let $(G, *)$ be a group. As in the proof of Proposition 3.5.3, notice if $a \in Z(G)$ then

$$\begin{aligned} K(a) &= \{b * a * b^{-1} \mid b \in G\} \\ &= \{b * b^{-1} * a \mid b \in G\} \\ &= \{e * a \mid b \in G\} \\ &= \{a\}. \end{aligned}$$

Conversely, if $K(a) = \{a\}$, then $b * a * b^{-1} = a$ for all $b \in G$ so $b * a = a * b$ for all $b \in G$ so $a \in Z(G)$.

Using this remark along with Corollary 3.3.21, we obtain an important equation relating the number of elements of a group to the number of elements in the centre of the group and the indices of the non-trivial centralizers.

Theorem 3.5.7 (The Class Equation). *Let $(G, *)$ be a finite group. Let $a_1, \ldots, a_n$ be elements not in $Z(G)$ that form a complete set of representatives of the conjugacy classes that are not contained in $Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{k=1}^{n} [G : C(a_k)] = |Z(G)| + \sum_{k=1}^{n} \frac{|G|}{|C(a_k)|}.$$

Proof. Recall from Corollary 3.3.21 that if $(G, *)$ is a group, X is a finite G-set, m is the number of distinct orbits of $G \curvearrowright X$, and $x_1, \ldots, x_m$ is one representative from each equivalence class of the orbit equivalence relation, then

$$|X| = \sum_{j=1}^{m} |\mathcal{O}_{x_j}|.$$

Let G act on $X = G$ by conjugation. Therefore $|X| = |G|$. Recall for the conjugation group action that $\mathcal{O}_x = K(x)$. Therefore, if $x \in Z(G)$, we see that

$$|\mathcal{O}_x| = |K(x)| = |\{x\}| = 1$$

by Remark 3.5.6. Therefore, if $a_1, \ldots, a_n$ are elements not in $Z(G)$ that form a complete set of representatives of the conjugacy classes that are not contained in $Z(G)$, we see that

$$|G| = |Z(G)| + \sum_{k=1}^{n} |K(a_k)| = |Z(G)| + \sum_{k=1}^{n} [G : C(a_i)]$$

with the last equality following from Remark 3.5.2 (i.e. the Orbit-Stabilizer Relation (Theorem 3.3.17)). ∎

Before we demonstrate the importance of the Class Equation, we quickly verify it holds for one of our previous examples.

Example 3.5.8. Consider $(D_4, \circ)$. By Example 3.5.5, $Z(D_4) = \{e, \rho^2\}$, and ρ, τ, and $\rho \circ \tau$ is a complete set of representatives of the conjugacy classes that are not contained in $Z(D_4)$. Since

$$|C(\rho)| = |C(\tau)| = |C(\rho \circ \tau)| = 4,$$

we see that

$$|Z(D_4)| + \frac{|D_4|}{|C(\rho)|} + \frac{|D_4|}{|C(\tau)|} + \frac{|D_4|}{|C(\rho \circ \tau)|} = 2 + \frac{8}{4} + \frac{8}{4} + \frac{8}{4} = 8 = |D_4|$$

as expected by the Class Equation (Theorem 3.5.7).

To see the importance of the Class Equation (Theorem 3.5.7) to the theory of groups, we present the following two results. In particular, since we want to describe all groups of order p^2 up to isomorphism where p is a prime number, we first consider the following.

Theorem 3.5.9. *Let $(G, *)$ be a group such that $|G| = p^n$ where p is prime and $n \geq 1$. Then $Z(G) \neq \{e\}$.*

Proof. Suppose for the sake of a contradiction that $Z(G) = \{e\}$. Therefore, the Class Equation (Theorem 3.5.7) implies that

$$p^n = |G| = 1 + \sum_{k=1}^{m} [G : C(a_k)]$$

where $a_1, \ldots, a_m$ be elements not in $Z(G)$ that form a complete set of representatives of the conjugacy classes that are not contained in $Z(G)$.

Recall $C(a_k) \leq G$ for all $k = \{1, \ldots, m\}$. Therefore, since $|G| = p^n$ with p prime, Lagrange's Theorem (Theorem 2.5.1) implies that $|C(a_k)| \in \{1, p, p^2, \ldots, p^n\}$.

Since for each $k \in \{1, \ldots, m\}$ we know that $a_k \notin Z(G)$, there exists a $b_k \in G$ such that $b_k * a_k \neq a_k * b_k$ and thus $b_k \notin C(a_k)$. Thus $C(a_k) \neq G$ so,

since $|G| = p^n$, we have $|C(a_k)| \in \{1, p, p^2, \ldots, p^{n-1}\}$ for all $k \in \{1, \ldots, m\}$. Therefore p divides

$$[G : C(a_k)] = \frac{|G|}{|C(a_k)|}$$

for all $k \in \{1, \ldots, m\}$. Thus p divides p^n and p divides $\sum_{k=1}^{m}[G : C(a_k)]$ so the above equation implies that p divides 1 thereby contradicting the fact that p is prime. Hence $Z(G) \neq \{e\}$. ∎

Corollary 3.5.10. *Let $(G, *)$ be a group such that $|G| = p^2$ where p is prime. Then $(G, *)$ is abelian.*

Proof. Since $Z(G) \leq G$ and $|G| = p^2$ with p prime, Lagrange's Theorem (Theorem 2.5.1) implies that $|Z(G)| \in \{1, p, p^2\}$. Note $|Z(G)| \neq 1$ by Theorem 3.5.9.

Suppose for the sake of a contradiction that $|Z(G)| = p$. Since $|G| = p^2 > p = |Z(G)|$, there exists an $a \in G \setminus Z(G)$.

Consider $C(a)$. Since $C(a) \leq G$ and $|G| = p^2$ with p prime, Lagrange's Theorem (Theorem 2.5.1) implies that $|C(a)| \in \{1, p, p^2\}$. Note that $Z(G) \subseteq C(a)$ by the definitions of the centre and the centralizer. Therefore, since $a \in C(a)$ and $a \notin Z(G)$, it follows that $|C(a)| > |Z(G)|$. Hence, since $|Z(G)| = p$ and $|C(a)| \in \{1, p, p^2\}$, we obtain that $|C(a)| = p^2 = |G|$.

Since $|C(a)| = |G|$, we obtain that $C(a) = G$. However, the definition of the centralizer implies since $C(a) = G$ that every element of G commutes with a and thus $a \in Z(G)$ thereby contradicting the fact that $a \in G \setminus Z(G)$.

Hence $|Z(G)| = p^2 = |G|$. Therefore $Z(G) = G$ so G is abelian. ∎

In Chapter 5, we will develop a theory that determines all finite abelian groups up to isomorphism. Hence, in conjunction with Corollary 3.5.10, we will have determined all groups of order p^2 up to isomorphism for all prime numbers p.

3.6 Cauchy's Theorem

The Class Equation (Theorem 3.5.7) and its generalization for arbitrary group actions (Corollary 3.3.21) can be utilized further to obtain information about groups. To begin, recall Example 2.5.10 shows that $(A_4, \circ)$ has no subgroup of order 6 even though $|A_4| = 12$ and $6|12$. However, note that 6 is not prime. Therefore, since prime numbers are 'nicer', we can ask "If $(G, *)$ is a group and p divides $|G|$ for some prime p, does $(G, *)$ contain a subgroup of order p?" Since every group of order p is cyclic by Corollary 2.5.6, the above question is equivalent to "If $(G, *)$ is a group and p divides $|G|$ for some prime p, does $(G, *)$ contain an element of order p?" This is the content of the main result of this section, Cauchy's Theorem (Theorem 3.6.2).

To prove Cauchy's Theorem (Theorem 3.6.2), first recall that given a G-set X, Section 3.4 made use of looking at all elements of X that were fixed by a particular element of G. Instead of looking at each of these sets individually, we will look at the intersection of these sets. This is the parallel for X to how the intersection of all of the stabilizers of elements of G produces the kernel.

Definition 3.6.1. Let $(G, *)$ be a group and let X be a G-set. The *fixed point set of* $G \curvearrowright X$, denoted X^G, is the set

$$X^G = \{x \in X \mid a \cdot x = x \text{ for all } a \in G\}.$$

To prove Cauchy's Theorem (Theorem 3.6.2), we will look at a very specific group action, the generalization of the Class Equation for arbitrary group actions (Corollary 3.3.21), and the fixed point set.

Theorem 3.6.2 (Cauchy's Theorem). *Let $(G, *)$ be a finite group and let p be a prime number that divides $|G|$. There exists an $a \in G$ such that $|a| = p$.*

Proof. Let

$$X = \{(a_1, \ldots, a_p) \in G^p \mid a_1 * a_2 * \cdots * a_p = e\}.$$

We claim that $|X| = |G|^{p-1}$. Indeed note that

$$X = \{(a_1, \ldots, a_{p-1}, a_{p-1}^{-1} * \cdots * a_2^{-1} * a_1^{-1}) \mid a_1, a_2, \ldots, a_{p-1} \in G\}.$$

Therefore, since there are $|G|$ options for each value of a_1, a_2, ..., a_{p-1}, we see that $|X| = |G|^{p-1}$ so $|X|$ is divisible by p.

Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix} \in S_p.$$

Note if $(a_1, \ldots, a_p) \in G$ then

$$a_1 * a_2 * \cdots * a_p = e$$

so

$$a_2 * a_3 * \cdots * a_p = a_1^{-1}$$

and thus

$$a_2 * a_3 * \cdots * a_p * a_1 = e$$

implying that

$$(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, \ldots, a_{\sigma(p)}) = (a_2, a_3, \ldots, a_p, a_1) \in G.$$

Since the above holds for all $(a_1, \ldots, a_p) \in G$, we obtain that if $(a_1, \ldots, a_p) \in G$ then

$$(a_{\sigma^k(1)}, a_{\sigma^k(2)}, \ldots, a_{\sigma^k(p)}) \in G$$

for all $k \in \mathbb{N}$.

Define $\cdot : \mathbb{Z}_p \times X \to X$ by

$$[k] \cdot (a_1, a_2, \ldots, a_p) = (a_{\sigma^k(1)}, a_{\sigma^k(2)}, \ldots, a_{\sigma^k(p)}).$$

for all $(a_1, a_2, \ldots, a_p) \in X$. Note that $\cdot$ does indeed map into X by the above argument. Moreover $\cdot$ is well-defined since if $[k] = [m]$ in $\mathbb{Z}_p$ then $k \equiv m \mod p$ so $\sigma^k = \sigma^m$ as $|\sigma| = p$.

We claim that $\cdot$ is a group action on X. Indeed note that

$$[0] \cdot (a_1, a_2, \ldots, a_p) = (a_{\sigma^0(1)}, a_{\sigma^0(2)}, \ldots, a_{\sigma^0(p)}) = (a_1, a_2, \ldots, a_p).$$

Moreover, for all $[k], [m] \in \mathbb{Z}_p$ and $(a_1, a_2, \ldots, a_p) \in X$, we see that

$$\begin{aligned}
[k] \cdot ([m] \cdot (a_1, a_2, \ldots, a_p)) &= [k] \cdot (a_{\sigma^m(1)}, a_{\sigma^m(2)}, \ldots, a_{\sigma^m(p)}) \\
&= (a_{\sigma^k(\sigma^m(1))}, a_{\sigma^k(\sigma^m(2))}, \ldots, a_{\sigma^k(\sigma^m(p))}) \\
&= (a_{\sigma^{m+k}(1)}, a_{\sigma^{m+k}(2)}, \ldots, a_{\sigma^{m+k}(p)}) \\
&= [k+m] \cdot (a_1, a_2, \ldots, a_p) \\
&= ([k] + [m]) \cdot (a_1, a_2, \ldots, a_p).
\end{aligned}$$

Hence $\cdot$ is a group action on X.

By Corollary 3.3.21, we have if $x_1, \ldots, x_n \in X$ are one representative from each equivalence class of the orbit equivalence relation, then

$$|G|^{p-1} = |X| = \sum_{k=1}^{n} |\mathcal{O}_{x_k}|.$$

By Corollary 3.3.20, we have that $|\mathcal{O}_{x_k}|$ divides $|\mathbb{Z}_p|$ so $|\mathcal{O}_{x_k}| \in \{1, p\}$ for all $k \in \{1, \ldots, n\}$. Note if $|\mathcal{O}_{x_k}| = 1$, then $x_k \in X^{\mathbb{Z}_p}$. Hence

$$|G|^{p-1} = \left|X^{\mathbb{Z}_p}\right| + \ell p$$

where ℓ is the number of x_k such that $|\mathcal{O}_{x_k}| = p$.

Since p divides $|G|^{p-1}$, the above equation implies that p divides $\left|X^{\mathbb{Z}_p}\right|$. However, since $(e, e, \ldots, e) \in X^{\mathbb{Z}_p}$, $\left|X^{\mathbb{Z}_p}\right| \neq 0$. Therefore $\left|X^{\mathbb{Z}_p}\right| \geq p \geq 2$ so there exists an element $(b_1, b_2, \ldots, b_p) \in X^{\mathbb{Z}_p}$ such that

$$(b_1, b_2, \ldots, b_p) \neq (e, e, \ldots, e).$$

Since $(b_1, b_2, \ldots, b_p) \in X^{\mathbb{Z}_p}$, we have that

$$(b_1, b_2, \ldots, b_p) = [1] \cdot (b_1, b_2, \ldots, b_p) = (b_p, b_1, b_2, \ldots, b_{p-1}).$$

Hence $b_1 = b_2 = \cdots = b_p$. Moreover, since

$$(b_1, b_2, \ldots, b_p) \neq (e, e, \ldots, e),$$

we see that $b_1 \neq e$. Finally, since $(b_1, b_2, \ldots, b_p) \in X$, we obtain that

$$e = b_1 * b_2 * \cdots * b_p = b_1^p.$$

Therefore, since p is prime and $b_1 \neq e$, we obtain that $|b_1| = p$ by Corollary 1.7.22. ∎

Corollary 3.6.3. *If $(G, *)$ is a finite group and p is a prime number that divides $|G|$, then $(G, *)$ has a subgroup of order p.*

Proof. By Cauchy's Theorem (Theorem 3.6.2), there exists an $a \in G$ such that $|a| = p$. Hence $\langle a \rangle$ is a subgroup of G of order p. ∎

Chapter 4

Groups: Advanced Theory

Via our study of group actions in Chapter 3, we saw that if p is a prime that divides the order of a group $(G, *)$, then $(G, *)$ must have a subgroup of order p. Thus it is natural to ask "Are there conditions on $n \in \mathbb{N}$ so that if n divides $|G|$, then $(G, *)$ has a subgroup of order n?" We know by Example 2.5.10 that $(A_4, \circ)$ has no subgroup of order 6 even though $|A_4| = 12$ and $6|12$. Thus $n = 6$ is out. However, what goes wrong for 6?

It turns out that the problem with 6 is that it is the product of two primes and, if we focus on powers of prime numbers, something incredibly special happens. We have already seen examples of this in Theorem 3.5.9 and Corollary 3.5.10. By focusing on subgroups of order p^n for a prime number p, we will obtain some of the major and most powerful results of the course.

These results are known as the Sylow Theorems, of which there are three, will be our first focus of this chapter. The Sylow Theorems are powerful tools for understanding the subgroup structure of finite groups and thus determining whether a group has normal subgroups. After demonstrating the three Sylow Theorems and deriving some immediate applications, we will then be able to study the simple groups which were alluded to in Section 2.7.

4.1 Sylow's First Theorem

We begin with Sylow's First Theorem (Theorem 4.1.7). To do so, we will focus groups of order p^n for a prime number p and thus some names are in order.

Definition 4.1.1. Let p be a prime number. A group $(G, *)$ is said to be a *p-group* if $|G| = p^n$ for some $n \geq 1$.

Definition 4.1.2. Let p be a prime number and let $(G, *)$ be a finite group. A subgroup H of $(G, *)$ is said to be a *p-subgroup* if H is a p-group.

The ultimate goal of Sylow's First Theorem is to show there are p-subgroups of the largest possible order. Thus we make the following definition.

Definition 4.1.3. Let p be a prime number and let $(G, *)$ be a finite group such that $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$. A subgroup H of $(G, *)$ is said to be a *Sylow p-subgroup* if $|H| = p^n$.

For some of the examples we have studied in this course, it is not difficult to find Sylow p-subgroups.

Example 4.1.4. Recall that $|A_4| = 12 = 2^2(3)$. Thus any subgroup of $(A_4, \circ)$ of order 4 is a Sylow 2-subgroup and any subgroup of $(A_4, \circ)$ of order 3 is a Sylow 3-subgroup.

Note $(A_4, \circ)$ has three elements of order 2 and no elements of order 4 by Example 1.6.39. Therefore, since elements of a group of order 4 must have order 1, 2, or 4 by Lagrange's Theorem (Theorem 2.5.1), the only possible subgroup of $(A_4, \circ)$ of order 4 is

$$H = \left\{e, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\right\}.$$

Since H is a subgroup of $(A_4, \circ)$ (isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$), H is the only Sylow 2-subgroup of $(A_4, \circ)$.

Note $(A_4, \circ)$ has eight elements of order 3 by Example 1.6.39. Since any 3-subgroup is a cyclic group of order 3 by Corollary 2.5.6, the Sylow 3-subgroups are all cyclic subgroups of $(A_4, \circ)$ of order 3; namely

$$\left\langle \begin{pmatrix}1 & 2 & 3\end{pmatrix} \right\rangle, \left\langle \begin{pmatrix}1 & 2 & 4\end{pmatrix} \right\rangle, \left\langle \begin{pmatrix}1 & 3 & 4\end{pmatrix} \right\rangle, \left\langle \begin{pmatrix}2 & 3 & 4\end{pmatrix} \right\rangle.$$

Example 4.1.5. Recall that

$$D_6 = \left\{e, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \tau, \rho \circ \tau, \rho^2 \circ \tau, \rho^3 \circ \tau, \rho^4 \circ \tau, \rho^5 \circ \tau\right\}$$

where $|\rho| = 6$, $|\tau| = 2$, and $\tau \circ \rho = \rho^{-1} \circ \tau$. Thus $|D_6| = 12 = 2^2(3)$. Thus any subgroup of $(D_6, \circ)$ of order 4 is a Sylow 2-subgroup and any subgroup of $(D_6, \circ)$ of order 3 is a Sylow 3-subgroup.

Note that $(D_6, \circ)$ has 7 elements of order 2; namely

$$\rho^3, \tau, \rho \circ \tau, \rho^2 \circ \tau, \rho^3 \circ \tau, \rho^4 \circ \tau, \text{ and } \rho^5 \circ \tau.$$

Moreover, $(D_6, \circ)$ has no element of order 4. Therefore, since elements of a group of order 4 must have order 1, 2, or 4 by Lagrange's Theorem (Theorem 2.5.1), all subgroups of $(D_6, \circ)$ of order 4 must contain exact three of the seven elements of order 2 along with e. Since every group of order 4 is isomorphic to either $(\mathbb{Z}_4, +)$ or $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ by Corollary 2.5.7, every Sylow 2-subgroup of $(D_6, \circ)$ must be abelian. Note since $|\rho| = 6$ that

$$(\rho^k \circ \tau) \circ (\rho^m \circ \tau) = (\rho^m \circ \tau) \circ (\rho^k \circ \tau)$$

if and only if

$$\rho^{k-m} = \rho^{m-k}$$

if and only if

$$\rho^{2(k-m)} = e$$

if and only if $k \equiv m \mod 3$ by Corollary 1.7.23. Therefore any subgroup of $(D_6, \circ)$ of order 4 cannot contain elements from more than one of the following sets:

$$\{\tau, \rho^3 \circ \tau\}, \quad \{\rho \circ \tau, \rho^4 \circ \tau\}, \quad \text{and} \quad \{\rho^2 \circ \tau, \rho^5 \circ \tau\}.$$

Since a subgroup containing both elements from any one of the above sets must also contain ρ^3 as

$$(\rho^{k+3} \circ \tau) \circ (\rho^k \circ \tau)^{-1} = \rho^3,$$

we see that the possible subgroups of $(D_6, \circ)$ of order 4 are

$$\{e, \rho^3, \tau, \rho^3 \circ \tau\}, \quad \{e, \rho^3, \rho \circ \tau, \rho^4 \circ \tau\}, \quad \text{and} \quad \{e, \rho^3, \rho^2 \circ \tau, \rho^5 \circ \tau\}.$$

Since all of these can be verified to be groups of order 4 (isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$), there are exactly 3 Sylow 2-subgroups of $(D_6, \circ)$.

Note $(D_6, \circ)$ has two elements of order 3; namely ρ^2 and ρ^4. Since any 3-subgroup is a cyclic group of order 3 by Corollary 2.5.6, there is exactly one Sylow 3-subgroup of $(D_6, \circ)$; namely

$$\{e, \rho^2, \rho^4\}$$

Remark 4.1.6. Since $(A_4, \circ)$ and $(D_6, \circ)$ had different numbers of subgroups of order 4 (and of order 3), $(A_4, \circ)$ and $(D_6, \circ)$ cannot be isomorphic by Theorem 2.3.13.

The following Sylow Theorem solves the motivating question of this section. The proof will follow by induction, but is non-trivial. In particular, in the inductive step, after some reductions, we will need to consider the quotient group of $(G, *)$ by a subgroup N of $(G, *)$ of order p contained in $Z(G)$. Doing so will enable us to use the inductive hypothesis since G/N has order $\frac{|G|}{p}$.

Theorem 4.1.7 (Sylow's First Theorem). *Let p be a prime number and let $(G, *)$ be a finite group where $|G| = p^n m$ where $n, m \geq 1$ and $\gcd(m, p) = 1$. For all $1 \leq k \leq n$, $(G, *)$ has a subgroup of order p^k. Thus $(G, *)$ has a Sylow p-subgroup.*

Proof. For all $r \in \mathbb{N}$, let P_r be the mathematical statement that if $(G, *)$ is a group such that $|G| = r$ and $|G| = p^n m$ for some $n, m \geq 1$ and and $\gcd(m, p) = 1$, then $(G, *)$ has a subgroup of order p^k for every $1 \leq k \leq n$. We will proceed by strong induction on r. Note P_r is trivially true when r is not of the form $p^n m$ where $n, m \geq 1$ and $\gcd(m, p) = 1$. Thus $P_1, \ldots, P_{p-1}$ are trivially true.

Base Case: $|G| = p$. In this case, $(G, *) \cong (\mathbb{Z}_p, +)$ by Corollary 2.5.6. Hence the base case is complete as clearly $\mathbb{Z}_p$ is a subgroup of $(\mathbb{Z}_p, +)$ of order $p^1 = p$.

Inductive Step. Assume $(G, *)$ is a group of order $p^n m$ where $\gcd(m, p) = 1$ and that P_r is true for all $r < p^n m$. Fix $1 \leq k \leq n$.

For $a \in G$, recall $|K(a)| = 1$ if and only if $a \in Z(G)$. Let $a_1, \ldots, a_l \in G$ be a complete set of representatives of the conjugacy classes such that $|K(a_j)| \neq 1$. Hence $a_1, \ldots, a_l \notin Z(G)$. By the Class Equation (Theorem 3.5.7), we know that

$$|G| = |Z(G)| + \sum_{j=1}^{l} [G : C(a_j)] = |Z(G)| + \sum_{j=1}^{l} \frac{|G|}{|C(a_j)|}.$$

Since $a_j \notin Z(G)$ that a_j does not commute with all elements of $(G, *)$ so $C(a_j)$ is a proper subgroup of G for all $j \in \{1, \ldots, l\}$. Hence $|C(a_j)|$ divides $|G|$ and $|C(a_j)| < |G|$ for all $j \in \{1, \ldots, l\}$.

If p^k divides $|C(a_j)|$ for some $j \in \{1, \ldots, l\}$, then the induction hypothesis implies that $C(a_j)$ has a subgroup of order p^k and thus $(G, *)$ has a subgroup of order p^k by Corollary 1.5.9 thereby completing the inductive step. Therefore we can assume that p^k does not divide $|C(a_j)|$ for all $j \in \{1, \ldots, l\}$. This implies that p divides $[G : C(a_j)]$ for all $j \in \{1, \ldots, l\}$ so the Class Equation implies that p divides $|Z(G)|$. Therefore Cauchy's Theorem (Corollary 3.6.3) implies that there is a subgroup $N \leq Z(G)$ such that $|N| = p$.

By Corollary 1.5.9, $N \leq G$. Therefore, if $k = 1$ then the inductive step is complete. Hence we can assume that $k > 1$.

Recall $N \lhd G$ by Proposition 3.5.3. Hence $(G/N, *)$ is a group of order

$$|G/N| = [G : N] = \frac{|G|}{|N|} = \frac{p^n m}{p} = p^{n-1} m.$$

Since $1 \leq k - 1 \leq n - 1$, the Inductive Hypothesis implies that $(G/N, *)$ has a subgroup K of order p^{k-1}.

Let $q : G \to G/N$ be the quotient map and let

$$H = q^{-1}(K) = \{a \in G \mid aN \in K\}.$$

Note $H \leq G$ by Theorem 2.1.11. Since for all $a \in N$ we have $aN = eN \in K$, we see that $N \subseteq H$. Hence $N \leq H$ by Corollary 1.5.9. Moreover, since $N \lhd G$ so $aNa^{-1} = N$ for all $a \in G$, we have $aNa^{-1} = N$ for all $a \in H$ and thus $N \lhd H$ by the Normal Subgroup Test (Theorem 2.6.10). Finally, note that

$$H/N = \{hN \mid h \in H\} = \{hN \mid hN \in K\} = K.$$

Therefore

$$|H| = |H/N||N| = |K||N| = p^{k-1} p = p^k.$$

Hence $H \leq G$ and $|H| = p^k$. Thus the inductive step is complete.

Therefore, the statement is true by the Principle of Mathematical Induction. ∎

4.2 Sylow's Second Theorem

For our second Sylow Theorem, recall that if $(G, *)$ is a group, $H \leq G$, and $a \in G$, then $aHa^{-1} \leq G$ and $|aHa^{-1}| = |H|$ by Lemma 2.6.9. Therefore, conjugates of Sylow p-subgroups are Sylow p-subgroups. Thus, it is natural to ask, "What do the "conjugacy classes" of the Sylow p-subgroups look like?" This question will be answered by Sylow's Second Theorem (Theorem 4.2.3).

We begin with some examples. Of course, we only need to consider groups where there are multiple Sylow p-subgroups.

Example 4.2.1. Consider $(A_4, \circ)$. Recall by Example 4.1.4 are four Sylow 3-subgroups of A_4; namely

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 & 3 & 4 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \right\rangle.$$

Note

$$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle \left(\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \right)^{-1} = \left\langle \begin{pmatrix} 1 & 4 & 2 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \right\rangle$$
$$\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle \left(\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \right)^{-1} = \left\langle \begin{pmatrix} 1 & 3 & 4 \end{pmatrix} \right\rangle$$
$$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle \left(\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \right)^{-1} = \left\langle \begin{pmatrix} 2 & 4 & 3 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \right\rangle.$$

Hence all four Sylow 3-subgroups of A_4 are conjugate to one another.

Example 4.2.2. Consider $(D_6, \circ)$. Recall by Example 4.1.5 are three Sylow 2-subgroups of D_6; namely

$$\{e, \rho^3, \tau, \rho^3 \circ \tau\}, \quad \{e, \rho^3, \rho \circ \tau, \rho^4 \circ \tau\}, \quad \text{and} \quad \{e, \rho^3, \rho^2 \circ \tau, \rho^5 \circ \tau\}.$$

Note

$$\rho\{e, \rho^3, \tau, \rho^3 \circ \tau\}\rho^{-1} = \{e, \rho^3, \rho^2 \circ \tau, \rho^5 \circ \tau\}$$
$$\rho^2\{e, \rho^3, \tau, \rho^3 \circ \tau\}(\rho^2)^{-1} = \{e, \rho^3, \rho^4 \circ \tau, \rho \circ \tau\}.$$

Hence all three Sylow 2-subgroups of D_6 are conjugate to one another.

It turns out that this is no coincidence as our second Sylow Theorem is as follows.

Theorem 4.2.3 (Sylow's Second Theorem). *Let p be a prime number and let $(G, *)$ be a finite group where $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$. If H is a Sylow p-subgroup of $(G, *)$ and K is a p-subgroup of $(G, *)$, then*

there exists an $c \in G$ such that $K \subseteq cHc^{-1}$. Hence any p-subgroup of $(G, *)$ is contained in some Sylow p-subgroup of $(G, *)$.

Consequently, if H and K are both Sylow p-subgroup of $(G, *)$, then there exists an $a \in G$ such that $K = aHa^{-1}$.

To prove Sylow's Second Theorem (Theorem 4.2.3), we will make use of the following lemma that which be also be used to prove Sylow's Third Theorem (Theorem 4.3.1).

Lemma 4.2.4 (The Mod p Lemma). *Let p be a prime number, let $(G, *)$ be a p-group, and let X be a finite G-set. Then*

$$\left|X^G\right| \equiv |X| \mod p.$$

Proof. Let $x_1, \ldots, x_n \in X$ be one representative from each equivalence class of the orbit equivalence relation. By Corollary 3.3.21 we know that

$$|X| = \sum_{k=1}^{n} |\mathcal{O}_{x_k}|.$$

Note that $|\mathcal{O}_x| = 1$ if and only if $a \cdot x = x$ for all $a \in G$ if and only if $x \in X^G$. Therefore, if $y_1, \ldots, y_m \in X$ are the $x_1, \ldots, x_n$ that are not in X^G, we obtain that

$$|X| = \left|X^G\right| + \sum_{j=1}^{m} |\mathcal{O}_{y_j}|.$$

Moreover, by Corollary 3.3.20, we know that $|\mathcal{O}_{y_j}|$ divides $|G| = p^n$ for all $j \in \{1, \ldots, m\}$. Therefore, since $|\mathcal{O}_{y_j}| \neq 1$, we obtain that p divides $|\mathcal{O}_{y_j}|$ for all $j \in \{1, \ldots, m\}$. Hence

$$\left|X^G\right| \equiv \left|X^G\right| + \sum_{j=1}^{m} |\mathcal{O}_{y_j}| \equiv |X^G| + \sum_{j=1}^{m} 0 \equiv \left|X^G\right| \mod p$$

as desired. ∎

To prove Sylow's Second Theorem (Theorem 4.2.3), we will define an action on the p-subgroup K on the set of left cosets of the Sylow p-subgroup H (note we do not need H to be normal to consider the left cosets), and use the Mod p Lemma (Lemma 4.2.4) to obtain a fixed point. It is this fixed point that let's us conjugate K inside of H.

Proof of Sylow's Second Theorem (Theorem 4.2.3). Let K be a p-subgroup of $(G, *)$ and let H be a Sylow p-subgroup of $(G, *)$. Let X be the set of left cosets of H by G; that is

$$X = \{aH \mid a \in G\}.$$

Note since H is a Sylow p-subgroup of $(G, *)$ that

$$|X| = [G : H] = \frac{|G|}{|H|} = \frac{p^n m}{p^n} = m.$$

Hence $|X| \not\equiv 0 \mod p$.

Let $\cdot : K \times X \to X$ be defined by

$$k \cdot aH = (k * a)H$$

for all $k \in K$ and $a \in G$. Since elements of X are cosets and thus have multiple representations, we must verify that $\cdot$ is well-defined; that is, if $a, b \in G$ are such that $aH = bH$, then $(k * a)H = (k * b)H$ for all $k \in K$. To see this, let $a, b \in G$ be such that $aH = bH$ and let $k \in K$. Therefore $b^{-1} * a \in H$ so

$$(k * b)^{-1} * (k * a) = b^{-1} * k^{-1} * k * a = b^{-1} * a \in H.$$

Hence $(k * a)H = (k * b)H$. Therefore, since $a, b \in G$ and $k \in K$ were arbitrary, $\cdot$ is well-defined.

We claim that $\cdot$ is a group action of K on X. To see this, first note for all $aH \in X$ that

$$e \cdot aH = (e * a)H = aH.$$

Moreover, for all $k_1, k_2 \in K$ and $aH \in X$ we see that

$$\begin{aligned} k_1 \cdot (k_2 \cdot aH) &= k_1 \cdot (k_2 * a)H \\ &= (k_1 * (k_2 * a))H \\ &= ((k_1 * k_2) * a)H \\ &= (k_1 * k_2) \cdot aH. \end{aligned}$$

Therefore, $\cdot$ is a group action of K on X.

By the Mod p Lemma (Lemma 4.2.4), we obtain that

$$|X^K| \equiv |X| \not\equiv 0 \mod p.$$

Therefore, there exists a $c \in G$ such that $cH \in X^K$. Hence

$$(k * c)H = k \cdot cH = cH$$

for all $k \in K$. Therefore $c^{-1} * k * c \in H$ for all $k \in K$ so $c^{-1}Kc \subseteq H$. Hence $K \subseteq cHc^{-1}$ via a simple computation.

In the case that K is a Sylow p-group, we see by Lemma 2.6.9 that

$$|H| = |cHc^{-1}| = |K|.$$

Hence $K \subseteq cHc^{-1}$ implies that $K = cHc^{-1}$ as desired. ∎

One interesting corollary of Sylow's Second Theorem (Theorem 4.2.3) is that we can determine the number of Sylow p-subgroups of any abelian group.

Corollary 4.2.5. *Let p be a prime number and let $(G, *)$ be a finite group where $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$. If $(G, *)$ is abelian, $(G, *)$ has exactly one Sylow p-subgroup.*

Proof. By Sylow's First Theorem (Theorem 4.1.7), $(G, *)$ has at least one Sylow p-subgroup.

Assume H and K are Sylow p-subgroups of $(G, *)$. By Sylow's Second Theorem (Theorem 4.2.3) there exists an $a \in G$ such that $K = aHa^{-1}$. However, since $(G, *)$ is abelian, $aHa^{-1} = (a * a^{-1})H = H$. Hence $K = H$ so $(G, *)$ has exactly one Sylow p-subgroup. ∎

Remark 4.2.6. It is important to note that the converse of Corollary 4.2.5 is false; that is, there exists a non-abelian group $(G, *)$ such that for every prime p that divides $|G|$, $(G, *)$ has exactly one Sylow p-subgroup. Indeed note that $(D_8, \circ)$ is a group with order 16. Hence the only Sylow subgroup of D_8 is the Sylow 2-subgroup D_8. Clearly $(D_8, \circ)$ is not abelian.

4.3 Sylow's Third Theorem

Corollary 4.2.5 immediately raises the question "Given a group $(G, *)$, exactly how many Sylow p-subgroups does $(G, *)$ have?" Note Example 4.1.4 showed us that $(A_4, \circ)$ has one Sylow 2-subgroup and four Sylow 3-subgroups whereas Example 4.1.5 showed us that $(D_6, \circ)$ has three Sylow 2-subgroup and one Sylow 3-subgroups. Thus groups of order 12 can have different numbers of Sylow subgroups and there are options for how many Sylow p-subgroups there are. Therefore, a better question is, "If G is a group of order n, are there any constraints on the number of Sylow p-subgroups $(G, *)$ can have based on n?" A moments thought shows that this is an important question for determining the number of groups of order n up to isomorphism. In fact, this will be a main technique to determine all groups of order 8 and of order 12 up to isomorphism in Section 5.3 and Section 5.5 respectively.

The answer to the above question is Sylow's Third Theorem (Theorem 4.3.1) which is as follows.

Theorem 4.3.1 (Sylow's Third Theorem). *Let p be a prime number and let $(G, *)$ be a finite group where $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$. Let n_p be the number of Sylow p-subgroups of $(G, *)$. Then $n_p \equiv 1 \mod p$ and $n_p | m$.*

Before we delve into the proof of Sylow's Third Theorem (Theorem 4.3.1), we show how to apply said theorem in the context of groups of order 12.

Example 4.3.2. Let $(G, *)$ be a group of order 12. Since $12 = 2^2(3)$, Sylow's Third Theorem (Theorem 4.3.1) implies that $n_2 \equiv 1 \mod 2$, $n_2|3$, $n_3 \equiv 1 \mod 3$, and $n_3|4$.

Since $n_2|3$, we have that $n_2 \in \{1, 3\}$. Note both 1 and 3 are equivalent to 1 modulo 2. Hence $(G, *)$ either has one or three Sylow 2-subgroups.

Since $n_3|4$, we have that $n_3 \in \{1, 2, 4\}$. However, $2 \not\equiv 1 \mod 3$ whereas $4 \equiv 1 \equiv 1 \mod 3$. Hence $(G, *)$ either has one or four Sylow 2-subgroups.

Note $(\mathbb{Z}_{12}, +)$ is a group of order 12 with exactly one Sylow 2-subgroup and one Sylow 3-subgroup by Corollary 4.2.5. By Example 4.1.4, $(A_4, \circ)$ is a group of order 12 with exactly one Sylow 2-subgroup and four Sylow 3-subgroup. By Example 4.1.5, $(D_6, \circ)$ is a group of order 12 with exactly three Sylow 2-subgroup and one Sylow 3-subgroup.

Is there a group of order 12 with three Sylow 2-subgroups and four Sylow 3-subgroups? No! To see this, suppose for the sake of a contradiction that $(G, *)$ is a group of order 12 with 3 Sylow 2-subgroups and 4 Sylow 3-subgroups. Since every Sylow 3-subgroup of $(G, *)$ has three elements and thus is a cyclic group, there exists $a_1, a_2, a_3, a_4 \in G$ such that $|a_k| = 3$ for all k and $\langle a_k \rangle$ for $k = 1, 2, 3, 4$ are distinct subgroups of $(G, *)$. Note $|a_k| = 3$ implies $|a_k^2| = 3$ and $\langle a_k^2 \rangle = \langle a_k \rangle$. Therefore, since $\langle a_k \rangle \neq \langle a_j \rangle$ when $k \neq j$, we obtain that $\langle a_k \rangle \cap \langle a_j \rangle = \{e\}$. Therefore, $(G, *)$ contains at least 8 elements of order 3; namely $a_1, a_1^2, a_2, a_2^2, a_3, a_3^2, a_4, a_4^2$. Since $e \in G$ has order 1 and since G has 12 elements, there are at most 3 elements of even order in $(G, *)$. Since every element of a subgroup of $(G, *)$ order 4 must have an order in $\{1, 2, 4\}$, there is at most one subgroup of $(G, *)$ of order 4 consisting of e and the 3 elements of even order. Since this contradicts the assumption that $(G, *)$ has 3 Sylow 2-subgroup, we have our contradiction. Hence there is no group of order 12 with 3 Sylow 2-subgroups and 4 Sylow 3-subgroups.

In order to prove Sylow's Third Theorem (Theorem 4.3.1) we need a bit more group technology. In particular, we need the following notion that behaves a bit like the centralizers of elements of a group, but we replace the elements with subgroups.

Definition 4.3.3. Let $(G, *)$ be a group and let $H \leq G$. The *normalizer of H in G*, denoted $N(H)$, is the set

$$N(H) = \{a \in G \mid aH = Ha\} = \{a \in G \mid aHa^{-1} = H\}.$$

Like with the centre and centralizers, normalizers are subgroups with special properties.

Lemma 4.3.4. *Let $(G, *)$ be a group and let $H \leq G$. Then $N(H) \leq G$. Moreover $H \lhd N(H)$. Finally, if $K \leq G$ and $H \lhd K$, then $K \subseteq N(H)$; that is $N(H)$ is the largest subgroup of $(G, *)$ that contains H as a normal subgroup.*

Proof. To see that $N(H) \leq G$, first note that $eHe^{-1} = H$ so $e \in N(H)$ by definition.

Next, to see that $N(H)$ is closed under products, let $a, b \in N(H)$ be arbitrary. Since $a, b \in N(H)$, we know that $aHa^{-1} = H = bHb^{-1}$. Thus

$$(a * b)H(a * b)^{-1} = a(bHb^{-1})a^{-1} = aHa^{-1} = H.$$

Therefore $a, b \in N(H)$. Hence $N(H)$ is closed under group products.

Finally, to see that $N(H)$ is closed under inverses, let $a \in N(H)$ be arbitrary. Since $a \in N(H)$, we know that $aHa^{-1} = H$. Therefore

$$a^{-1}Ha = a^{-1}(aHa^{-1})a = H.$$

Therefore $a \in N(H)$. Hence $N(H)$ is closed under inverses. Thus $N(H) \leq G$ by Definition 1.5.7.

To see that $H \lhd N(H)$, first note for all $h \in H$ that $hHh^{-1} \subseteq H$ since $H \leq G$ and $|hHh^{-1}| = |H|$ by Lemma 2.6.9. Hence $hHh^{-1} = H$ for all $h \in H$ so $H \subseteq N(H)$. Therefore, since $(H, *)$ is a group, $H \leq N(H)$ by Definition 1.5.1. Moreover, note for all $a \in N(H)$ that $aHa^{-1} = H$. Hence $H \lhd N(H)$ by the Normal Subgroup Test (Theorem 2.6.10).

Finally, assume $K \leq G$ and $H \lhd K$. Therefore, by the Normal Subgroup Test (Theorem 2.6.10), $aHa^{-1} = H$ for all $a \in K$. Hence $K \subseteq N(H)$ by definition. ∎

To use normalizers to prove Sylow's Third Theorem (Theorem 4.3.1), we need some information about how normalizers behave with respect to Sylow p-subgroups. In particular, the following shows we can use normalizers to show Sylow p-subgroups are equal.

Lemma 4.3.5. *Let p be a prime number and let $(G, *)$ be a finite group where $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$. Let H and K be Sylow p-subgroups of $(G, *)$. Then $K \subseteq N(H)$ if and only if $K = H$.*

Proof. Assume $K = H$. Therefore, by Lemma 4.3.4, we have that

$$K = H \subseteq N(H)$$

as desired.

Conversely, assume $K \subseteq N(H)$. Since $K \leq G$ and $N(H) \leq G$, Definition 1.5.1 implies that $K \leq N(H)$. Since K is a Sylow p-subgroups of $(G, *)$ and thus has order p^n, Lagrange's Theorem (Theorem 2.5.1) implies that p^n divides $|N(H)|$. Moreover, since p^n divides $|N(H)|$, since $N(H) \leq G$, and since $|G| = p^n m$, Lagrange's Theorem (Theorem 2.5.1) implies that $|N(H)| = p^n k$ for some $k \in \mathbb{N}$.

Since $|K| = p^n$, since $|N(H)| = p^n k$, and since $K \leq N(H)$, K is a Sylow p-subgroup of $N(H)$. Similarly, since $H \leq N(H)$ by Lemma 4.3.4, since

$|N(H)| = p^n k$, and since $|H| = p^n$ as H is a Sylow p-subgroup of G, it follows that H is a Sylow p-subgroup of $N(H)$.

Since K and H are Sylow p-subgroups of $N(H)$, Sylow's Second Theorem (Theorem 2.8.7) implies that there exists an $a \in N(H)$ such that $K = aHa^{-1}$. However, since $a \in N(H)$, we have that $H = aHa^{-1} = K$ as desired. ∎

We are now prepared to prove Sylow's Third Theorem (Theorem 4.3.1). To do so, we will use two group actions on the set X of all Sylow p-subgroups of $(G, *)$. Each action will give us some information about the number of Sylow p-subgroups of $(G, *)$. In particular, information from the first action (conjugation of X by G) will follow from considering orbits and information from the second action (conjugation by a fixed Sylow p-subgroup) will follow from the Mod p Lemma (Lemma 4.2.4).

Proof of Sylow's Third Theorem (Theorem 4.3.1). Let

$$X = \{H \mid H \text{ is a Sylow } p\text{-subgroup of } (G, *)\}.$$

Note $|X| = n_p$. Moreover, by Sylow's First Theorem (Theorem 4.1.7), there exists a Sylow p-subgroup K of $(G, *)$. Hence $K \in X$ so $X \neq \emptyset$.

Let $\cdot : G \times X \to X$ be defined by

$$a \cdot H = aHa^{-1}$$

for all $a \in G$ and $H \in X$. Note if H is a Sylow p-subgroup of $(G, *)$ then aHa^{-1} Sylow p-subgroup of $(G, *)$ for all $a \in G$ so $\cdot$ does indeed map into X.

We claim that $\cdot$ is a group action of $(G, *)$ on X. To see this, note $e \cdot H = e * H * e^{-1} = H$ for all $H \in X$. Moreover, for all $a, b \in G$ and $H \in X$ we see that

$$\begin{aligned} a \cdot (b \cdot H) &= a \cdot (bHb^{-1}) \\ &= a(bHb^{-1})a^{-1} \\ &= (a * b)H(a * b)^{-1} \\ &= (a * b) \cdot H. \end{aligned}$$

Hence $\cdot$ is a group action.

By Sylow's Second Theorem (Theorem 4.2.3), any two Sylow p-subgroups of $(G, *)$ are conjugate to one another. Therefore, since $K \in X$, we obtain that then $\mathcal{O}_K = X$. Hence Corollary 3.3.20 implies that $n_p = |X|$ divides $|G| = p^n m$.

Let $\bullet : K \times X \to X$ be defined by

$$a \cdot H = aHa^{-1}$$

for all $a \in K$ and $H \in X$. By the same argument as above, $\bullet$ is a group action of $(K, *)$ on X.

Considered the fixed point set X^K of $K \curvearrowright X$. Note $H \in X^K$ if and only if $a \bullet H = H$ for all $a \in K$ if and only if $aHa^{-1} = H$ for all $a \in K$ if and only if $K \subseteq N(H)$ if and only if $K = H$ by Lemma 4.3.4. Therefore $X^K = \{K\}$. Therefore, since K is a p-group and X is a finite K-set, the Mod p Lemma (Lemma 4.2.4) implies that

$$n_p \equiv |X| \equiv \left|X^K\right| \equiv 1 \mod p.$$

Since $n_p \equiv 1 \mod p$, $n_p \not\equiv 0 \mod p$. Since p is prime, we obtain that $\gcd(n_p, p) = 1$. Therefore, since $n_p | p^n m$, we obtain that $n_p | m$. ∎

4.4 Applications of the Sylow Theorems

Although Sylow's Theorems will be greatly important and have applications in Chapter 5, we exhibit two results using Sylow's Theorems here. To begin, we prove the following that completely determines the number of groups of a specific order up to isomorphism. Note this can be seen to be an extension of Corollary 3.5.10 to a product of two primes, provided some additional conditions hold.

To demonstrate this result, we first require two lemmata that are quite useful for understanding the structure of an entire group based on two subgroups.

Lemma 4.4.1. *Let $(G, *)$ be a group, let $n, m \in \mathbb{N}$ be such that $\gcd(n, m) = 1$, and let $H, K \leq G$ be such that $|H| = n$ and $|K| = m$. Then $H \cap K = \{e\}$.*

Proof. Since H and K are subgroups of G, we know that $e \in H$ and $e \in K$ so $\{e\} \subseteq H \cap K$. To see the other inclusion, assume $a \in H \cap K$. Since $a \in H$, we know that $|a|$ divides $|H| = n$ by Lagrange's Theorem (Theorem 2.5.1). Similarly, since $a \in K$, we know that $|a|$ divides $|K| = m$ by Lagrange's Theorem (Theorem 2.5.1). Therefore, we have that $|a|$ is a common divisor of n and m so $1 \leq |a| \leq \gcd(n, m) = 1$. Hence $|a| = 1$ so $a^1 = e$ and thus $a = e$. Hence $H \cap K \subseteq \{e\}$ so $H \cap K = \{e\}$ as desired. ∎

Lemma 4.4.2. *Let $(G, *)$ be a group and let $H, K \lhd G$ be such that $H \cap K = \{e\}$. Then $a * b = b * a$ for all $a \in H$ and $b \in K$.*

Proof. Let $a \in H$ and $b \in K$ be arbitrary, and let

$$x = a * b * a^{-1} * b^{-1} \in G.$$

We claim that $x = e$, which will complete the proof since if $x = e$ then $a * b = b * a$ as desired.

To show that $x = e$, we note since $H \cap K = \{e\}$ that it suffices to show that $x \in H \cap K$. To see that $x \in H$, note that $a^{-1} \in H$ and $H \lhd G$ so

$$b * a^{-1} * b^{-1} \in bHb^{-1} = H$$

by the Normal Subgroup Test (Theorem 2.6.10). Therefore, since $H \leq G$ and thus is closed under multiplication, we obtain that

$$x = a * (b * a^{-1} * b^{-1}) \in H.$$

Similarly, to see that $x \in K$, note $b \in K$ and $K \lhd G$ so

$$a * b * a^{-1} \in aKa^{-1} = K$$

by the Normal Subgroup Test (Theorem 2.6.10). Therefore, since $K \leq G$ and thus is closed under multiplication, we obtain that

$$x = (a * b * a^{-1}) * b^{-1} \in K.$$

Hence $x \in H \cap K = \{e\}$ so $x = e$ as desired. ∎

Theorem 4.4.3. *Let $(G, *)$ be a group of order pq where p and q are odd primes with $p < q$. If p does not divide $q - 1$, then $(G, *)$ is cyclic and thus isomorphic to $(\mathbb{Z}_{pq}, +)$.*

Proof. We claim that $(G, *)$ has exactly one Sylow p-subgroup and one Sylow q-subgroup. To see this, let n_p and n_q denote the number of Sylow p-subgroups and Sylow q-subgroups respectively.

By Sylow's Third Theorem (Theorem 4.3.1), $n_p | q$ and $n_p \equiv 1 \mod p$. Since q is prime and $n_p | q$, we have that $n_p \in \{1, q\}$. Since p does not divide $q - 1$, we know that $q - 1 \not\equiv 0 \mod p$ and thus $q \not\equiv 1 \mod p$. Therefore, since $n_p \in \{1, q\}$, $n_p \equiv 1 \mod p$, and $q \not\equiv 1 \mod p$, we must have that $n_p = 1$. Hence $(G, *)$ has exactly one Sylow p-subgroup. Let H be the Sylow p-subgroup of $(G, *)$. Since aHa^{-1} is a Sylow p-subgroup for all $a \in G$, we must have $aHa^{-1} = H$ for all $a \in G$ so the Normal Subgroup Test (Theorem 2.6.10) implies that $H \lhd G$.

By Sylow's Third Theorem (Theorem 4.3.1), $n_q | p$ and $n_q \equiv 1 \mod q$. Since p is prime and $n_q | p$, we have that $n_q \in \{1, p\}$. However, since $1 < p < q$, we obtain that $p \not\equiv 1 \mod q$. Therefore, since $n_q \in \{1, p\}$, $n_q \equiv 1 \mod q$, and $p \not\equiv 1 \mod q$, we must have that $n_q = 1$. Hence $(G, *)$ has exactly one Sylow q-subgroup. Let K be the Sylow q-subgroup of $(G, *)$. Since aKa^{-1} is a Sylow q-subgroup for all $a \in G$, we must have $aKa^{-1} = K$ for all $a \in G$ so the Normal Subgroup Test (Theorem 2.6.10) implies that $K \lhd G$.

Since $|H| = p$ and $|K| = q$ where p and q are prime, Corollary 2.5.6 implies there are elements $a, b \in G$ such that

$$H = \langle a \rangle \qquad \text{and} \qquad K = \langle b \rangle$$

Moreover, since $\gcd(|H|, |K|) = 1$, Lemma 4.4.1 implies that $H \cap K = \{e\}$. Hence Lemma 4.4.2 implies that $a * b = b * a$.

Let $x = a * b \in G$. We claim that

$$G = \langle x \rangle.$$

To see this, first note since $a * b = b * a$ that

$$x^n = a^n * b^n$$

for all $n \in \mathbb{N}$. Therefore $x^n = e$ if and only if $a^n * b^n = e$ if and only if $a^n = b^{-n}$. Therefore, since $a^n \in H$, since $b^{-n} \in K$, and since $H \cap K = \{e\}$, we see that $x^n = e$ if and only $a^n = e$ and $b^n = e$ if and only if $p|n$ and $q|n$ if and only if $pq|n$ since p and q are distinct prime numbers. Thus $|x| = pq = |G|$ so $G = \langle x \rangle$. Hence $(G, *)$ is cyclic and thus isomorphic to $(\mathbb{Z}_{pq}, +)$ by Proposition 2.3.11. ∎

Example 4.4.4. Since $15 = 3(5)$ where 3 and 5 are odd primes such that $3 < 5$ and 3 does not divide $5 - 1 = 4$, Theorem 4.4.3 implies the only group of order 15 is $(\mathbb{Z}_{15}, +)$.

Remark 4.4.5. Unfortunately, Theorem 4.4.3 fails if the condition 'p does not divide $q - 1$' is removed. Indeed there are two groups of order 21, namely $(\mathbb{Z}_{21}, +)$ and ... another we cannot write down at this point. In particular, this group we cannot write down is a non-abelian group and is in fact the smallest non-abelian group of an odd order.

For another application, we prove a theorem from number theory that is often proved in MATH 1200 on the way to proving Fermat's Little Theorem (Theorem 2.5.4).

Theorem 4.4.6 (Wilson's Theorem). *If p is a prime number, then*

$$(p - 1)! \equiv -1 \mod p.$$

Proof. Consider the symmetric group $(S_p, \circ)$. Since

$$|S_p| = p! = pm$$

where $m = (p - 1)!$ is such that $\gcd(p, m) = 1$, every Sylow p-subgroup of S_p has exactly p elements.

We claim there are $(p - 2)!$ Sylow p-subgroups of $(S_p, *)$. To see this, first assume H is a Sylow p-subgroup of S_p. Since $|H| = p$, H must be cyclic by Corollary 2.5.6. Hence there exists a $\sigma \in S_p$ such that $H = \langle \sigma \rangle$. Since p is prime and $|\sigma| = p$, σ must be a p-cycle. Moreover, since p is prime, all of σ, σ^2, ..., σ^{p-1} are all p-cycles and thus have order p and be elements of H. Hence, any one of σ, σ^2, ..., σ^{p-1} generate H. Therefore each Sylow p-group is generated by and contains exactly $p - 1$ different p-cycles.

Note p-cycle in S_p contains all of the numbers $1, 2, \ldots, p$. Therefore, by putting the number 1 as the first entry in our cycle representation of elements of S_p, we see there are $(p-1)!$ ways we can complete the p-cycle (since the order of the numbers matters) and thus S_p has $(p-1)!$ p-cycles. Therefore, since there are exactly $p-1$ different p-cycles in each of the Sylow p-subgroups, we see that there are $(p-2)!$ Sylow p-subgroups of $(S_p, *)$.

By Sylow's Third Theorem (Theorem 4.3.1), we obtain that

$$(p-2)! \equiv 1 \mod p.$$

Hence

$$(p-1)! \equiv p-1 \equiv -1 \mod p$$

as desired. ∎

4.5 Simple Groups

With the three Sylow Theorems, we can discuss some essential types of groups. As discussed in Section 2.7, one reason normal subgroups are 'incredibly special' is that it allows one to decompose a group G into a normal subgroup H and the quotient group G/H. Thus the most complicated groups to understand are those of the following type.

Definition 4.5.1. A group $(G, *)$ is said to be *simple* if $(G, *)$ has no non-trivial normal subgroups.

As simple groups can be viewed as the building blocks of all other groups, the goal of this section is to obtain information about what finite groups are and can be simple. Unsurprisingly, the abelian case is quite easy.

Theorem 4.5.2. *Let $(G, *)$ be a finite abelian group. Then $(G, *)$ is simple if and only if $|G|$ is prime.*

Proof. First, assume $|G| = p$ is prime. By Corollary 2.5.6, $(G, *) \cong (\mathbb{Z}_p, +)$. Since every subgroup of a cyclic group is cyclic by Proposition 1.7.28 and since every non-identity element of $(\mathbb{Z}_p, +)$ cyclically generates $(\mathbb{Z}_p, +)$, we obtain that $(\mathbb{Z}_p, +)$ contains no non-trivial normal subgroups. Since subgroups are preserved under isomorphisms by Theorem 2.1.11, normal subgroups are preserved under isomorphism by an application of the Normal Subgroup Test (Theorem 2.6.10). Hence $(G, *)$ has no non-trivial normal subgroups and thus is simple.

Conversely, suppose G is a finite abelian group such that $|G|$ is not prime. Hence there exists a prime p such that p divides $|G|$ but $|G| \neq p$. By Cauchy's Theorem (Corollary 3.6.3), $(G, *)$ has a subgroup H such that $|H| = p$. Since $p < |G|$, we see that H is a non-trivial subgroup of $(G, *)$. Therefore, since $(G, *)$ is abelian so that every subgroup of $(G, *)$ is normal (Example 2.6.2), $(G, *)$ has a non-trivial normal subgroup and thus is not simple. ∎

With the above description of all simple finite abelian groups, we turn our attention to the non-abelian groups. Luckily, the three Sylow Theorems are of great aid in demonstrating certain groups cannot be simple. Indeed, consider the following.

Remark 4.5.3. Let p be a prime number and let $(G, *)$ be a group such that p divides $|G|$ If G is not a p-group and has one Sylow p-subgroup H then H is normal and $H \neq G$ (as G is not a p-group). Hence H is a non-trivial normal subgroup of $(G, *)$ and thus cannot be simple.

Using this idea, we can quickly demonstrate many non-abelian groups of small order cannot be simple. To do so, we proceed with a series of disjoint lemmata to cover a lot of different cases.

Lemma 4.5.4. *Let $(G, *)$ be a group of order pq where p and q are odd primes with $p < q$. Then $(G, *)$ is not simple.*

Proof. The proof of Theorem 4.4.3 shows that $n_q = 1$ under these conditions and thus $(G, *)$ has exactly one Sylow q-subgroup. Hence $(G, *)$ is not simple by Remark 4.5.3. ∎

Lemma 4.5.5. *Let $(G, *)$ be a group of order pqr where p, q, and r are primes such that $p < q < r$. Then $(G, *)$ is not simple.*

Proof. Let n_q and n_r be the number of Sylow q-subgroups and Sylow r-subgroups respectively. We claim that $n_q = 1$ or $n_r = 1$ thereby completing the proof by Remark 4.5.3.

By Sylow's Third Theorem (Theorem 4.3.1), we know that $n_q \equiv 1 \mod q$, $n_r \equiv 1 \mod r$, $n_q | pr$, and $n_r | pq$. Since p, q, and r are prime, $n_q | pr$ implies $n_q \in \{1, p, r, pr\}$, and $n_r | pq$ implies $n_r \in \{1, p, q, pq\}$. However, since $p < q < r$, p and q cannot be equivalent to 1 modulo r and thus $n_r \in \{1, pq\}$. Since the proof is complete if $n_r = 1$, we may assume without loss of generality that $n_r = pq$.

Since $|G| = pqr$ with $\gcd(pq, r) = 1$, we see that every Sylow r-subgroup of G has r elements. Hence $(G, *)$ has pq subgroups of order r. Since r is prime, every subgroup of order r must be cyclic by Corollary 2.5.6 and thus have $r-1$ elements of order r. Moreover, since any non-identity element of a cyclic group of order r also generates the subgroup (i.e. $\mathbb{Z}_r^\times = \mathbb{Z}_r \setminus \{[0]\}$), we obtain that the pq subgroups of G of order r can only have the identity element in common. Thus $(G, *)$ must contain exactly $pq(r-1) = pqr - pq = |G| - pq$ elements of order r. Hence $(G, *)$ contains exactly pq elements whose order is not r.

To see that $n_q = 1$, suppose for the sake of contradiction that $n_q \neq 1$. Since $n_q \in \{1, p, r, pr\}$, this implies $n_q \in \{p, r, pr\}$. However, since $n_q \equiv 1 \mod q$ and since $p < q$ so that $p \not\equiv 1 \mod q$, we obtain that $n_q \in \{r, pr\}$. Therefore $n_q \geq r$.

Since $|G| = pqr$ with $\gcd(pr, q) = 1$, an argument similar to the above one shows that $(G, *)$ must contain at least $n_q(q-1) \geq r(q-1)$ elements of order q. However, since $r > q > p$, we see that $r > q$ and $q - 1 \geq p$ so that $r(q-1) > pq$. Since is it impossible that $(G, *)$ contains exactly pq elements whose order is not r and contains more than pq elements of order q, we have our contradiction. Hence $n_q = 1$ in the case $n_r \neq 1$ thereby completing the proof. ∎

To demonstrate groups whose order is a power of a prime cannot be simple, we need only apply the following result with $m = 1$.

Lemma 4.5.6. *Let $(G, *)$ be a group such that $|G| = p^n m$ where p is a prime number, $n \geq 1$, $m > 1$, $\gcd(p, m) = 1$, and p^n does not divide $(m-1)!$. Then $(G, *)$ is not simple.*

Proof. Suppose for the sake of a contradiction that $(G, *)$ is simple. By Sylow's First Theorem (Theorem 4.1.7), there exists a Sylow p-subgroup H of G. Hence $|H| = p^n$ so $[G : H] = m$.

Let

$$X = \{aH \mid a \in G\}$$

and let $\cdot : G \times X \to X$ be defined by

$$a \cdot (bH) = (a * b)H$$

for all $a \in G$ and $bH \in X$. We claim that $\cdot$ is well-defined. Indeed if $bH, cH \in X$ are such that $bH = cH$, then $b^{-1} * c \in H$ so $(a * b)^{-1} * (a * c) = (b^{-1} * a^{-1}) * a * c = b^{-1} * c \in H$ and thus $(a * b)H = (a * c)H$. Thus $\cdot$ is well-defined.

We claim that $\cdot$ is a group action of $(G, *)$ on X. To see this, first note that $e \cdot (aH) = (e * a)H = aH$ for all $aH \in X$. Moreover, for all $aH \in X$ and $b, c \in G$, we see that

$$b \cdot (c \cdot (aH)) = b \cdot ((c * a)H) = (b * c * a)H = (b * c) \cdot aH.$$

Hence $\cdot$ is a group action of $(G, *)$ on X.

By Lemma 3.2.3, there is a homomorphism $\varphi : G \to S_X$ such that $\varphi(a)(bH) = a \cdot bH = (ab)H$ for all $a \in G$ and $bH \in X$. Since $(G, *)$ is simple and $\ker(\varphi) \lhd G$ by Proposition 2.6.4, it must be the case that $\ker(\varphi) = \{e\}$ or $\ker(\varphi) = G$. However, since $\varphi(a)(eH) = aH$ for all $a \in G$ and since $m > 1$ so there exists an $a \in G$ such that $aH \neq eH$, we see that $G \setminus H \notin \ker(\varphi)$ so it must be the case that $\ker(\varphi) = \{e\}$. Hence φ is an isomorphism from G to $\mathrm{Im}(\varphi)$. Therefore $|G| = |\mathrm{Im}(\varphi)|$.

Since $|\mathrm{Im}(\varphi)|$ divides $|S_X| = |X|! = m!$, we obtain that $|G|$ divides $m!$. Hence $p^n m$ divides $m!$ so it must be the case (by the Fundamental Theorem of Arithmetic) that p^n divides $(m-1)!$. However this contradicts our assumptions. Hence $(G, *)$ is not simple. ∎

To deal with some of the cases where the condition "p^n does not divide $(m-1)!$" fails in Lemma 4.5.6, we can consider the following.

Lemma 4.5.7. *Let $(G,*)$ be a group such that $|G| = p^2q$ where p and q are distinct prime numbers. Then $(G,*)$ is not simple.*

Proof. Let n_p and n_q be the number of Sylow p-subgroups and Sylow q-subgroups respectively. By Sylow's Third Theorem (Theorem 4.3.1), we know that $n_p \equiv 1 \mod p$, $n_q \equiv 1 \mod q$, $n_p|q$, and $n_q|p^2$. Note $n_p|q$ implies $n_p \in \{1, q\}$, and $n_q|p^2$ implies $n_q \in \{1, p, p^2\}$.

If $q < p$, then $q \not\equiv 1 \mod p$. Hence $n_p \neq q$. Thus the above implies $n_p = 1$. Hence $(G,*)$ is not simple by Remark 4.5.3.

If $p < q$, then $p \not\equiv 1 \mod q$. Hence $n_q \neq p$. Thus the above implies that $n_q \in \{1, p^2\}$. If $n_q = 1$, then $(G,*)$ is not simple by Remark 4.5.3. Thus we may assume without loss of generality that $n_q = p^2$.

Since every Sylow q-subgroup of G has q elements and since q is prime, every subgroup of order q must be cyclic and thus have $q-1$ elements of order q. Moreover, since any non-identity element of a cyclic group of order q also generates the subgroup (i.e. $\mathbb{Z}_q^\times = \mathbb{Z}_q \setminus \{[0]\}$), we obtain that the p^2 subgroups of G of order q can only have the identity element in common. Thus G must contain exactly $p^2(q-1) = p^2q - p^2 = |G| - p^2$ elements of order q. Hence G contains exactly p^2 elements whose order is not q.

Since every Sylow p-subgroup of G has order p^2 and since groups of order p^2 cannot contain elements of order q since $\gcd(p,q) = 1$, we obtain that any Sylow p-subgroup of G must contain all p^2 elements whose order is not q. Hence $(G,*)$ has a unique Sylow p-subgroup. Thus $(G,*)$ is not simple Remark 4.5.3. ∎

As our last step before analyzing which non-abelian groups of small order can be simple, we desire to get one specific case out of the way.

Lemma 4.5.8. *Let $(G,*)$ be a group such that $|G| = 72$. Then $(G,*)$ is not simple.*

Proof. Note $72 = 2^3(3^2)$. By Sylow's Third Theorem (Theorem 4.3.1), we know that $n_3 \equiv 1 \mod 3$ and $n_3|2^3$. Note the latter implies that $n_3 \in \{1, 2, 4, 8\}$. Since $n_3 \equiv 1 \mod 3$, we know that $n_3 \neq 2$ and $n_3 \neq 8$, so $n_3 \in \{1, 4\}$. If $n_3 = 1$ then G has a unique Sylow 3-group and thus G is not simple. Hence, without loss of generality, we may assume $n_3 = 4$.

As in the proof of Sylow's Third Theorem (Theorem 4.3.1), recall G acts on the set X of all four Sylow 3-subgroups by conjugation. Since there are 4 Sylow 3-groups, this group action induces a homomorphism $\varphi : G \to S_X$ such that $\varphi(a)(H) = a \cdot H = aHa^{-1}$ for all $H \in X$ and $a \in G$.

Since $|G| = 72$ and $|S_X| = 4! = 24$, $\ker(\varphi) \neq \{e\}$. Moreover, since every Sylow 3-subgroup is conjugate by Sylow's Second Theorem (Theorem 4.2.3), there exists an $H \in X$ and an $a \in G$ such that $aHa^{-1} \neq H$. Therefore

$\varphi(a) \neq \mathrm{id}_X$ so $a \notin \ker(\varphi)$. Hence $\ker(\varphi) \neq G$. Therefore $\ker(\varphi)$ is a non-trivial normal subgroup of G so $(G, *)$ is not simple. ∎

With all of the above results, the number of small orders for which there are non-abelian simple groups is strikingly very small.

Theorem 4.5.9. *If $(G, *)$ is a non-abelian simple group with $|G| < 100$, then $|G| = 60$.*

Proof. Assume $(G, *)$ is a non-abelian simple group with $|G| < 100$. Clearly $|G| \neq 1$.

Since Corollary 2.5.6 implies that for any prime p every group of order p must be cyclic and thus abelian, we know that

$$|G| \notin \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}.$$

Recall Corollary 2.5.8 implies for any prime $p \geq 3$ that the only groups of order $2p$ up to isomorphism are $(\mathbb{Z}_{2p}, +)$ or $(D_p, \circ)$. Note $(\mathbb{Z}_{2p}, +)$ is abelian. Moreover, since $\langle \rho \rangle$ has index 2 in $(D_p, \circ)$ and thus is normal, we see that $(D_p, \circ)$ is not simple. Hence

$$|G| \notin \{6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86, 94\}.$$

Since Theorem 3.5.9 implies for any prime p that a group order p^n has non-trivial centre and thus is either abelian or not simple, we obtain that

$$|G| \notin \{4, 8, 16, 32, 64, 9, 27, 81, 25, 49\}.$$

Since Lemma 4.5.4 implies that any group with order pq where p and q are distinct odd primes with $p < q$ is not simple, we obtain that

$$|G| \notin \{3(5), 3(7), 3(11), 3(13), 3(17), 3(19), 3(23), 3(29), 3(31), 5(7), 5(11), 5(13), 5(17), 5(19), 7(11), 7(13)\}.$$

Thus

$$|G| \notin \{15, 21, 33, 39, 51, 57, 69, 87, 93, 35, 55, 65, 85, 95, 77, 91\}.$$

Since Lemma 4.5.7 implies that any group with order p^2q where p and q are distinct primes is not simple, we obtain that

$$|G| \notin \{2^2(3), 2^2(5), 2^2(7), 2^2(11), 2^2(13), 2^2(17), 2^2(19), 2^2(23), 3^2(2), 3^2(5), 3^2(7), 3^2(11), 5^2(2), 5^2(3), 7^2(2)\}.$$

Thus

$$|G| \notin \{12, 20, 28, 44, 52, 68, 76, 92, 18, 45, 63, 99, 50, 75, 98\}.$$

Moreover Lemma 4.5.5 implies that any group with order pqr where p, q, and r are primes such that $p < q < r$ is not simple. Hence

$$|G| \notin \{2(3)(5), 2(3)(7), 2(3)(11), 2(3)(13), 2(5)(7)\}.$$

Thus

$$|G| \notin \{30, 42, 66, 78, 70\}.$$

Furthermore Lemma 4.5.6 imples that any group with order $p^n m$ where p is a prime number, $n \geq 1$, $m > 1$, $\gcd(p, m) = 1$, and p^n does not divide $(m-1)!$ is not simple. Hence

$$|G| \notin \{2^3(3), 2^4(3), 2^4(5), 2^5(3), 3^2(4), 3^3(2), 11(8)\}.$$

Thus

$$|G| \notin \{24, 48, 80, 96, 36, 54, 88\}.$$

Combining the above, we have shown that

$$|G| \in \{40, 56, 60, 72, 84, 90\}.$$

Hence, to complete the proof, we need to eliminate 5 of these possibilities. Note any group of order 72 is not simple by Lemma 4.5.8. Thus only 4 other possibilities remain.

Suppose for the sake of a contradiction that $|G| = 40$. Note $40 = 2^3(5)$. Hence Sylow's Third Theorem (Theorem 4.3.1) implies that $n_5 \equiv 1 \mod 5$ and $n_5 | 8$. The latter implies $n_5 \in \{1, 2, 4, 8\}$. Therefore, since the only element in $\{1, 2, 4, 8\}$ congruent to $1 \mod 5$ is 1, we obtain that $n_5 = 1$. Thus Remark 4.5.3 implies that $(G, *)$ is not simple. Hence we have a contradiction so $|G| \neq 40$.

Suppose for the sake of a contradiction that $|G| = 56$. Note that $56 = 2^3(7)$. Hence Sylow's Third Theorem (Theorem 4.3.1) implies that $n_7 \equiv 1 \mod 7$ and $n_7 | 2^3$. Note the latter implies that $n_7 \in \{1, 2, 4, 8\}$, which, combined with $n_7 \equiv 1 \mod 7$ implies that $n_7 \in \{1, 8\}$. Since $(G, *)$ is simple and thus cannot have a unique Sylow p-subgroup for any prime p by Remark 4.5.3, we must have that $n_2 = 7$ and $n_7 = 8$. Note any Sylow 7-subgroup has 7 elements and thus is cyclic by Corollary 2.5.6. Thus any Sylow 7-subgroup must have 6 elements of order 7. Moreover, since any non-identity element of a cyclic group of order 7 also cyclically generates the subgroup (i.e. $\mathbb{Z}_7^\times = \mathbb{Z}_7 \setminus \{[0]\}$), we obtain that the 8 subgroups of $(G, *)$ of order 7 can only have the identity element in common. Thus G must contain exactly $8(6) = 48$ elements of order 7. Hence $(G, *)$ contains exactly $56 - 48 = 8$ elements whose order is not 7. Thus, since every Sylow 2-subgroup of $(G, *)$ has $2^3 = 8$ elements, there can be at most one Sylow 2-subgroup which then implies $(G, *)$ is not simple by Remark 4.5.3. Hence we have a contradiction so $|G| \neq 56$.

Suppose for the sake of a contradiction that $|G| = 84$. Note that $84 = 2^2(3)(7)$. Hence Sylow's Third Theorem (Theorem 4.3.1) implies that $n_7 \equiv 1 \mod 7$ and $n_7 | 2^2(3)$. Note the latter implies that $n_7 \in \{1, 2, 3, 4, 6, 12\}$. Hence $n_7 \equiv 1 \mod 7$ implies that $n_7 = 1$. Thus Remark 4.5.3 implies that $(G, *)$ is not simple. Hence we have a contradiction so $|G| \neq 84$.

Finally, suppose for the sake of a contradiction that $|G| = 90$. This case will be ruled out by Lemma 4.6.7 after we have developed more theory in the next section.

Therefore, we have ruled out all possibilities other than 60. Hence if $(G, *)$ is a non-abelian simple group with $|G| < 100$, then $|G| = 60$. ∎

4.6 The Fifth Alternating Group

Note Section 4.5 could not rule out the possibility that a non-abelian group of order 60 was simple. Indeed note that $60 = 2^2(3)(5)$ so Sylow's Third Theorem (Theorem 4.3.1) implies that $n_2 \equiv 1 \mod 2$, $n_3 \equiv 1 \mod 3$, $n_5 \equiv 1 \mod 5$, $n_2 | 15$, $n_3 | 20$, and $n_5 | 12$. Note the latter implies that $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 2, 4, 5, 10, 20\}$, and $n_5 \in \{1, 2, 3, 4, 6, 12\}$. Even using the former, we can only reduce this down to $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 4, 10\}$, and $n_5 \in \{1, 6\}$. Thus a simple group of order 60 must have 6 Sylow 5-subgroups. Moreover, by similar arguments to those in Section 4.5, this group must have $4(6) = 24$ elements of order 5. This leaves plenty of elements to form multiple Sylow 2-subgroups and Sylow 3-subgroups. Thus, two natural questions are "Is there a simple group of order 60?' and, if so, "What are all the simple groups of order 60?"

Well, one special collection of groups we have looked at in this course are the Alternating groups. Recall $|A_5| = 60$. Thus, perhaps we should look deeper into $(A_5, \circ)$ and see if it is simple. We begin with the following which does show that $(A_5, \circ)$ has the correct number of elements of order 5 for there to be 6 Sylow 5-subgroups.

Lemma 4.6.1. *The group $(A_5, \circ)$ has one element of order 1, 15 elements of order 2, 20 elements of order 3, and 24 elements of order 5.*

Proof. Recall that $A_5 \leq S_5$. Since every element of S_5 is a product of disjoint cycles involving the numbers $\{1, 2, 3, 4, 5\}$, every element in S_5 is of exactly one of the following forms:

(1) the identity element,

(2) a 2-cycle,

(3) a 3-cycle,

(4) a 4-cycle,

(5) a 5-cycle,

(6) a product of two 2-cycles, or

(7) a product of a 2-cycle and a 3-cycle.

However, since A_5 contains precisely the even permutations, since elements of the forms (1), (3), (5), and (6) are even, and since elements of the forms (2), (4), and (7) are odd, A_5 consists of all elements of S_5 of the form (1), (3), (5), and (6). Note elements of the forms (1), (3), (5), and (6) have orders 1, 3, 5, and 2 respectively. Thus, if $n \in \mathbb{N}$ and $n \notin \{1, 2, 3, 5\}$, then A_5 has no elements of order n.

Since the identity element is the only group element of order 1, A_5 has one element of order 1.

Next let's count the number of elements of A_5 that have form (5), which will be equal to the number of elements of A_5 of order 5. Note to construct an element of S_5 that is a 5-cycle, we must use all of the elements of $\{1, 2, 3, 4, 5\}$ in the cycle. As we can cycle the elements of a cycle to make any one of the numbers appear first, we can always write the cycle as

$$\begin{pmatrix} 1 & x & y & z & w \end{pmatrix}$$

where x, y, z, w is some rearrangement of $2, 3, 4, 5$. Thus we have 4 options for x for which there are 3 options of y for which there are 2 options for z leaving one option for w. Thus there are $4! = 24$ elements of A_5 of order 5.

Now let's count the number of elements of A_5 that have the form (6), which will be equal to the number of elements of A_5 of order 2. Note to construct an element of S_5 that is the product of two 2-cycles, we must select 4 elements of $\{1, 2, 3, 4, 5\}$ to be the elements that occur in the two 2-cycles, which is equivalent to choosing one number to leave out. Thus there are 5 ways to do this. For the four distinct numbers x, y, z, w selected, there are 3 possible permutations

$$\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} z & w \end{pmatrix}, \qquad \begin{pmatrix} x & z \end{pmatrix}\begin{pmatrix} y & w \end{pmatrix}, \qquad \text{and} \qquad \begin{pmatrix} x & w \end{pmatrix}\begin{pmatrix} y & x \end{pmatrix}.$$

Thus there are $5(3) = 15$ elements of A_5 of order 2.

Finally, as every remaining element of A_5 has order 3, there are $60 - 1 - 24 - 15 = 20$ elements of A_5 of order 3. (This can also be computed as follows: for a 3-cycle, we need to chose three distinct elements from $\{1, 2, 3, 4, 5\}$ for which there are $\binom{5}{3} = 10$ options. For each of those three elements x, y, z, there are two 3-cycles: $\begin{pmatrix} x & y & x \end{pmatrix}$ and $\begin{pmatrix} x & z & y \end{pmatrix}$. Hence there are 20 elements of order 3 in A_5.) ∎

Since a careful analysis of Lemma 4.6.1 shows that $(A_5, \circ)$ does indeed have 6 Sylow 5-subgroups, we yet to have an argument that rules $(A_5, \circ)$ out

from being simple. One thing we could try is to look at the centre since the centre is always a normal subgroup of a group. However, the centre of $(A_5, \circ)$ is quite nice.

Lemma 4.6.2. *The centre of* $(A_5, \circ)$ *is* $\{e\}$.

Proof. Clearly $e \in Z(A_5)$ trivially. To see that $Z(A_5) = \{e\}$, we will brute-force check that every other elements of A_5 doesn't commute with some element of A_5. Recall that A_5 contains the following types of elements:

Case 1: 5-cycles. An arbitrary 5-cycle in A_5 has the form

$$\sigma = \begin{pmatrix} 1 & a & b & c & d \end{pmatrix}$$

where $\{a, b, c, d\} = \{2, 3, 4, 5\}$. Let

$$\tau = \begin{pmatrix} 1 & b & a & c & d \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & c \end{pmatrix}\begin{pmatrix} a & d \end{pmatrix} \qquad \text{and} \qquad \tau\sigma = \begin{pmatrix} 1 & c \end{pmatrix}\begin{pmatrix} b & d \end{pmatrix}.$$

Hence $\sigma\tau \neq \tau\sigma$ so $\sigma \notin Z(A_5)$.

Case 2: 3-cycles. An arbitrary 3-cycle in A_5 has the form

$$\sigma = \begin{pmatrix} a & b & c \end{pmatrix}$$

where $a, b, c \in \{1, 2, 3, 4, 5\}$ are distinct. Choose $d \in \{1, 2, 3, 4, 5\} \setminus \{a, b, c\}$ and let

$$\tau = \begin{pmatrix} a & b & d \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} a & c \end{pmatrix}\begin{pmatrix} b & d \end{pmatrix} \qquad \text{and} \qquad \tau\sigma = \begin{pmatrix} a & d \end{pmatrix}\begin{pmatrix} b & c \end{pmatrix}.$$

Hence $\sigma\tau \neq \tau\sigma$ so $\sigma \notin Z(A_5)$.

Case 3: products of disjoint 2-cycles. An arbitrary products of disjoint 2-cycles in A_5 has the form

$$\sigma = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$$

where $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$. Let

$$\tau = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & e \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} c & e & d \end{pmatrix} \qquad \text{and} \qquad \tau\sigma = \begin{pmatrix} c & d & e \end{pmatrix}.$$

Hence $\sigma\tau \neq \tau\sigma$ so $\sigma \notin Z(A_5)$.

Therefore, since we have covered all possible cases, $Z(A_5) = \{e\}$. ∎

It turns out that $(A_5, \circ)$ is, in fact, simple. To show this, we first need the following two results.

Lemma 4.6.3. *Let $(G, *)$ be a finite group and let $H \lhd G$. If $|H| = 2$, then $H \subseteq Z(G)$.*

Proof. Since $|H| = 2$, there exists an $a \in G \setminus \{e\}$ such that $H = \{e, a\}$. Since $H \lhd G$, we know by the Normal Subgroup Test (Theorem 2.6.10) that for all $b \in G$

$$\{e, a\} = H = bHb^{-1} = \{b * e * b^{-1}, b * a * b^{-1}\} = \{e, b * a * b^{-1}\}.$$

Thus we must have that $a = b * a * b^{-1}$ for all $b \in G$ so that $a * b = b * a$ for all $g \in G$. Hence $a \in Z(G)$. Since $e \in Z(G)$ trivially, we obtain that $H \subseteq Z(G)$. ∎

Lemma 4.6.4. *Let $(G, *)$ be a finite group and let $H \lhd G$. If $a \in G$ is such that $\gcd(|a|, |G/H|) = 1$, then $a \in H$.*

Proof. Recall that $|aH|$ divides $|a|$ by Proposition 2.7.6. Furthermore, since $aH \in G/H$, we know by Lagrange's Theorem (Theorem 2.5.1) that $|aH|$ divides $|G/H|$. Therefore $|aH|$ is a common divisor of $|a|$ and $|G/H|$. Hence $|aH| \leq \gcd(|a|, |G/H|) = 1$ so $|aH| = 1$. Therefore $aH = eH$ so $a \in H$ as desired. ∎

Theorem 4.6.5. *The group $(A_5, \circ)$ is simple.*

Proof. To see that $(A_5, \circ)$ is a simple group, assume that $H \lhd A_5$. Since $|A_5| = 60 = 4(3)(5)$, Lagrange's Theorem (Theorem 2.5.1) implies that $|H| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Our goal is to show that $|H| = 1$ or $|H| = 60$ thereby showing that the only normal subgroups of A_5 are the trivial subgroups. We will proceed by ruling out each other possibility systematically using the above results.

Case 1: $|H| = 2$. If $|H| = 2$, Lemma 4.6.3 implies that $H \subseteq Z(A_5)$. However, H has two elements and $Z(A_5)$ only contains the identity element by Lemma 4.6.2. Hence $|H| = 2$ is not possible.

Case 2: $|H| = 3$. If $|H| = 3$, then $|G/H| = 20$. Since $\gcd(3, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 3. By Lemma 4.6.1, this implies that H contains all 20 elements in A_5 of order 3. However, since H contains only 3 elements, it cannot contain all 20 elements. Hence $|H| = 3$ is not possible.

Case 3: $|H| = 4$. If $|H| = 4$, then $|G/H| = 15$. Since $\gcd(2, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 2. By Lemma 4.6.1, this implies that H contains all 15 elements in A_5 of order 2. However, since H contains only 4 elements, it cannot contain all 15 elements. Hence $|H| = 3$ is not possible.

Case 4: $|H| = 5$. If $|H| = 5$, then $|G/H| = 12$. Since $\gcd(5, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 5. By Lemma 4.6.1, this implies that H contains all 24 elements in A_5 of order 5. However, since H contains only 5 elements, it cannot contain all 24 elements. Hence $|H| = 5$ is not possible.

Case 5: $|H| = 6$. If $|H| = 6$, then $|G/H| = 10$. Since $\gcd(3, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 3. ByLemma 4.6.1, this implies that H contains all 20 elements in A_5 of order 3. However, since H contains only 6 elements, it cannot contain all 20 elements. Hence $|H| = 6$ is not possible.

Case 6: $|H| = 10$. If $|H| = 10$, then $|G/H| = 6$. Since $\gcd(5, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 5. By Lemma 4.6.1, this implies that H contains all 24 elements in A_5 of order 5. However, since H contains only 10 elements, it cannot contain all 24 elements. Hence $|H| = 10$ is not possible.

Case 7: $|H| = 12$. If $|H| = 12$, then $|G/H| = 5$. Since $\gcd(2, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 2. By Lemma 4.6.1, this implies that H contains all 15 elements in A_5 of order 2. However, since H contains only 12 elements, it cannot contain all 15 elements. Hence $|H| = 12$ is not possible.

Case 8: $|H| = 15$. If $|H| = 15$, then $|G/H| = 4$. Since $\gcd(5, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 5. By Lemma 4.6.1, this implies that H contains all 24 elements in A_5 of order 5. However, since H contains only 15 elements, it cannot contain all 24 elements. Hence $|H| = 15$ is not possible.

Case 9: $|H| = 20$. If $|H| = 20$, then $|G/H| = 3$. Since $\gcd(5, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 5. By Lemma 4.6.1, this implies that H contains all 24 elements in A_5 of order 5. However, since H contains only 20 elements, it cannot contain all 24 elements. Hence $|H| = 20$ is not possible.

Case 10: $|H| = 30$. If $|H| = 30$, then $|G/H| = 2$. Since $\gcd(3, |G/H|) = 1$ and $\gcd(5, |G/H|) = 1$, Lemma 4.6.4 implies that H must contain all elements in A_5 of order 3 and of order 5. By Lemma 4.6.1, this implies that H contains all 20 elements in A_5 of order 3 and all 24 elements in A_5 of order 5. However, since H contains only 30 elements, it cannot contain all $20+24 = 44$ elements. Hence $|H| = 30$ is not possible.

Therefore, since we have ruled out all other possibilities, $|H| = 1$ or $|H| = 60$. Hence A_5 is simple. ∎

In fact, Theorem 4.6.5 can be used to show that all larger alternating groups are simple. This follows by an induction argument coupled with understanding the action of $(S_n, \circ)$ on $\{1, \ldots, n\}$.

Theorem 4.6.6. *For all $n \geq 5$, the group $(A_n, \circ)$ is simple.*

Proof. Let P_n be the mathematical statement that $(A_n, \circ)$ is simple. We will use the Principle of Mathematical Induction to show that P_n is true for all $n \geq 5$.

Base Case: $n = 5$. Note that $(A_5, \circ)$ is simple by Theorem 4.6.5. Hence the base case is complete.

Inductive Step. Assume $n \geq 6$ is such that $(A_{n-1}, \circ)$ is simple. To see that $(A_n, \circ)$ is simple, suppose for the sake of a contradiction that $(A_n, \circ)$ is not simple. Hence there exists a non-trivial normal subgroup H of $(A_n, \circ)$.

We claim that if $\tau \in H \setminus \{e\}$, then $\tau(m) \neq m$ for all $m \in \{1, \ldots, n\}$. To see this, suppose for the sake of a contradiction that there exists a $\tau \in H \setminus \{e\}$ and a $m \in \{1, \ldots, n\}$ such that $\tau(m) = m$.

Recall that A_n acts on $\{1, 2, \ldots, n\}$ as even permutations. Note under this action that for $k \in \{1, \ldots, n\}$ we have G_k is all elements σ of A_n that leave k fixed (see Example 3.3.6) and is a subgroup of A_n. Since G_k consists of all even permutations that leave k fixed, we see that $G_k \cong A_{n-1}$ (i.e. just relabel $1, \ldots, k-1, k+1, \ldots, n$ as $1, \ldots, n-1$). Hence G_k is simple for all $1 \leq k \leq n$ by the induction hypothesis.

Since $\tau(m) = m$, we have that $\tau \in G_m$. However, since $H \lhd A_n$ and $G_m \leq A_n$, the Second Isomorphism Theorem (Theorem 2.8.7) implies that $H \cap G_m \lhd G_m$. However, since G_m is simple, $\tau \neq e$, and $\tau \in H \cap G_m$, we obtain that $H \cap G_m = G_m$. Therefore, it must be the case that $G_m \subseteq H$.

Since a simple (pun intended) computation shows that $\sigma G_m \sigma^{-1} = G_{\sigma(m)}$ for all $\sigma \in A_n$, we obtain that

$$G_{\sigma(m)} = \sigma G_m \sigma^{-1} \subseteq \sigma H \sigma^{-1} = H$$

by the Normal Subgroup Test (Theorem 2.6.10). However, since A_n for $n \geq 4$ is transitive (i.e. $\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} \in A_n$ for any $a, b, c, d \in \{1, \ldots, n\}$ distinct), we obtain that $G_k \subseteq H$ for all $k \in \{1, 2, \ldots, n\}$.

Since every permutation in A_n is even, Theorem 1.6.24 implies that every element of H is a product of an even number of transpositions. Since these transpositions can be paired up, and since the product of 2 transpositions always leaves at least one element of $\{1, \ldots, n\}$ fixed, every element of A_n is a product of elements from $\bigcup_{k=1}^{n} G_k$. Since $\bigcup_{k=1}^{n} G_k \subseteq H$, every element of A_n is a product of elements of H and thus an element of H since $H \leq A_n$. This implies that $H = A_n$ thereby contradicting that H is a non-trivial normal subgroup of $(A_n, \circ)$. Hence, it must be the case that $\tau(m) \neq m$ for all $m \in \{1, \ldots, n\}$ and $\tau \in H \setminus \{e\}$.

Let $\tau_1, \tau_2 \in H$ be such that $\tau_1 \neq \tau_2$. We claim that $\tau_1(m) \neq \tau_2(m)$ for all $m \in \{1, \ldots, m\}$. To see this, suppose for the sake of a contradiction that $\tau_1(m) = \tau_2(m)$ for some $m \in \{1, \ldots, n\}$. Since $\tau_1 \neq \tau_2$, we know that $\tau_1^{-1} \circ \tau_2 \neq e$. However $(\tau_1^{-1} \circ \tau_2)(m) = m$ thereby contradicting that which we proved above. Thus it must be the case that $\tau_1(m) \neq \tau_2(m)$ for all $m \in \{1, \ldots, m\}$ whenever $\tau_1, \tau_2 \in H$ are such that $\tau_1 \neq \tau_2$.

To obtain our final contradiction, we will show that H cannot contain any non-identity elements. To see this, assume $\tau_1 \in H \setminus \{e\}$. First, assume τ_1 is a product of disjoint transpositions (and thus we must have n being divisible by 4 in this case). Since $n \geq 6$, we can write

$$\tau_1 = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_3 & a_4 \end{pmatrix} \begin{pmatrix} a_5 & a_6 \end{pmatrix} \sigma$$

for some distinct $a_1, \ldots, a_6 \in \{1, \ldots, n\}$ and permutation σ on $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_6\}$. Let

$$\gamma = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_3 & a_5 \end{pmatrix}.$$

Thus $\gamma \in A_n$ and

$$\tau_2 = \gamma \tau_1 \gamma^{-1} \in \gamma H \gamma^{-1} = H$$

by the Normal Subgroup Test (Theorem 2.6.10). However

$$\tau_2 = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_3 & a_6 \end{pmatrix} \begin{pmatrix} a_4 & a_5 \end{pmatrix} \sigma$$

so that

$$\tau_2(a_1) = a_2 = \tau_1(a_1)$$

and $\tau_2 \neq \tau_1$ thereby contradicting what was demonstrated above. Hence τ_1 cannot be written as product of disjoint transpositions.

Therefore, it must be the case that τ_1 is a product of disjoint cycles with at least one cycle being of length 3. Thus we can write

$$\tau_1 = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_\ell \end{pmatrix} \sigma$$

for some distinct $a_1, a_2, a_3, \ldots, a_\ell \in \{1, \ldots, n\}$ and permutation σ on $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_\ell\}$. Since $n \geq 5$, there exists some $\gamma \in A_n$ such that $\gamma(a_1) = a_1$, $\gamma(a_2) = a_2$, but $\gamma(a_3) \neq a_3$. Let

$$\tau_2 = \gamma \tau_1 \gamma^{-1} \in \gamma H \gamma^{-1} = H$$

by the Normal Subgroup Test (Theorem 2.6.10). However

$$\tau_2 = \begin{pmatrix} a_1 & a_2 & \gamma(a_3) & \ldots \end{pmatrix} \sigma'$$

so that

$$\tau_2(a_1) = a_2 = \tau_1(a_1)$$

and $\tau_2 \neq \tau_1$ thereby contradicting what was demonstrated above.

Thus we have obtained a contradiction so $(A_n, \circ)$ has no non-trivial normal subgroup.

Therefore, by the Principle of Mathematical Induction, $(A_n, \circ)$ is simple for all $n \geq 5$. ∎

Using the fact that $(A_6, \circ)$ is simple, we can complete our omission from Theorem 4.5.9.

Lemma 4.6.7. *Let $(G, *)$ be a group such that $|G| = 90$. Then $(G, *)$ is not simple.*

Proof. Assume $(G, *)$ is a simple group of order 90. Note that $90 = 2(3)^2(5)$. Hence Sylow's Third Theorem (Theorem 4.3.1) implies that $n_5 \equiv 1 \mod 5$ and $n_5 | 2(3^2)$. Note the latter implies that $n_5 \in \{1, 2, 3, 6, 9, 18\}$. Hence $n_5 \equiv 1 \mod 5$ implies that $n_5 = 1$ or $n_5 = 6$. Since $(G, *)$ is not simple, we know that $n_5 \neq 1$ by Remark 4.5.3. Hence $n_5 = 6$.

As in the proof of Sylow's Third Theorem (Theorem 4.3.1), recall G acts on the set X of all six Sylow 5-subgroups by conjugation. By Lemma 3.2.3, this group action induces a homomorphism $\varphi : G \to S_X$ such that $\varphi(a)(H) = a \cdot H = aHa^{-1}$ for all $H \in X$ and $a \in G$. Since every Sylow 5-subgroup is conjugate by Sylow's Second Theorem (Theorem 4.2.3), there exists an $H \in X$ and an $a \in G$ such that $aHa^{-1} \neq H$. Therefore $\varphi(a) \neq \mathrm{id}_X$ so $a \notin \ker(\varphi)$. Hence $\ker(\varphi) \neq G$. Therefore, since $\ker(\varphi)$ is a normal subgroup of $(G, *)$ and since $(G, *)$ is simple, it must be the case that $\ker(\varphi) = \{e\}$. Hence $(G, *)$ is isomorphic to a subgroup of $S_X \cong S_6$. Therefore, without loss of generality, $G \leq S_6$.

Consider $A_6 \leq S_6$. Note every 5-cycle in S_6 is an element of A_6. Moreover, G must have an element of order 5 by Cauchy's Theorem (Theorem 3.6.2). Since the only elements of S_6 of order 5 are 5-cycles, G must have a 5-cycle and thus $G \cap A_6 \neq \{e\}$. Moreover $G \cap A_6 \lhd G$ by the Second Isomorphism Theorem (Theorem 2.8.7). However, since $G \cap A_6 \neq \{e\}$ and since $(G, *)$ is simple, it must be the case that $G \cap A_6 = G$. Thus $G \leq A_6$.

Note that $|A_6| = 360$ and $|G| = 90$. Hence $[A_6 : G] = 4$. Let $Y = \{aG \mid a \in A_6\}$ and let A_6 act on Y via left multiplication as in the proof of Lemma 4.5.6. By Lemma 3.2.3 there is a homomorphism $\psi : A_6 \to S_Y$ such that $\psi(a)(bG) = a \cdot bG = (ab)G$ for all $a \in A_6$ and $bG \in Y$. Since $(A_6, \circ)$ is simple by Theorem 4.6.6 and $\ker(\psi) \lhd A_6$, it must be the case that $\ker(\psi) = \{e\}$ or $\ker(\psi) = A_6$. However, since $\varphi(a)(eG) = aG$ for all $a \in A_6$, and since $G \neq A_6$ by the difference in the number of elements, we see that $\ker(\psi) \neq A_6$. Hence it must be the case that $\ker(\psi) = \{e\}$. However this means that $(A_6, \circ)$ is isomorphic to a subgroup of $(S_Y, \circ)$. However, $|S_Y| = 4! = 24$. Therefore, since 360 does not divide 24, we have a contradiction. Thus $|G| \neq 90$. ∎

Using Theorem 4.6.5 along with the results of Section 4.5, we actually can write down all finite, simple, non-abelian groups of order less than 100.

Theorem 4.6.8. *Let $(G, *)$ be a finite, simple, non-abelian group with $|G| < 100$. Then $(G, *) \cong (A_5, \circ)$.*

Proof. Let $(G, *)$ be a finite, simple, non-abelian group with $|G| < 100$. By Theorem 4.5.9, we know that $|G| = 60$. Thus $|G| = 2^2(3)(5)$. Hence Sylow's

Third Theorem (Theorem 4.3.1) implies that $n_5 \equiv 1 \mod 5$ and $n_5|12$. Note the latter implies that $n_5 \in \{1, 2, 3, 4, 6, 12\}$. Hence, since $n_5 \equiv 1 \mod 5$, we obtain that $n_5 \in \{1, 6\}$. Since Remark 4.5.3 implies that if $n_5 = 1$ then $(G, *)$ is not simple, we must have that $n_5 = 6$.

Let

$$X = \{H \leq G \mid H \text{ a Sylow 5-subgroup of } G\}.$$

Thus $|X| = 6$. Moreover, as in the proof of Sylow's Third Theorem (Theorem 4.3.1), G acts on X by conjugation. By Lemma 3.2.3, this action induces a homomorphism $\varphi_0 : G \to S_X$ such that $\varphi_0(a)(H) = aHa^{-1}$ for all $a \in G$ and $H \in X$.

Since $(G, *)$ is simple and $\ker(\varphi_0) \lhd G$ by Proposition 2.6.4, we know that $\ker(\varphi_0) = \{e\}$ or $\ker(\varphi_0) = G$. However, by Sylow's Second Theorem (Theorem 4.2.3), we know that the action of G on X is transitive so $\varphi_0(a) \neq id_X$ for some $a \in G$ and thus $\ker(\varphi_0) \neq G$. Hence $\ker(\varphi_0) = \{e\}$ so φ is injective. Thus $(G, *)$ is isomorphic to a subgroup of $(S_X, \circ)$. Therefore, since $S_X \cong S_6$, there exists an injective homomorphism $\varphi : G \to S_6$.

Recall the sign homomorphism $\text{sgn} : S_6 \to \{1, -1\}$ is a homomorphism with $\ker(\text{sgn}) = A_6$. Thus $\psi = \text{sgn} \circ \varphi : G \to \{1, -1\}$ is a homomorphism. Therefore since $(G, *)$ is simple and since $\ker(\psi) \lhd G$ by Proposition 2.6.4, we know that $\ker(\psi) = \{e\}$ or $\ker(\psi) = G$.

We claim that $\ker(\psi) = G$. To see this, suppose for the sake of contradiction that $\ker(\psi) = \{e\}$. Thus $\psi(a) = -1$ for all $a \in G \setminus \{e\}$. However, since $|G| = 60$, we can find two elements $a, b \in G \setminus \{e\}$ such that $a \neq b^{-1}$. Therefore $ab \in G \setminus \{e\}$ and thus

$$-1 = \psi(ab) = \psi(a)\psi(b) = (-1)(-1) = 1,$$

which is clearly a contradiction. Hence $\ker(\psi) = G$. Therefore $\varphi : G \to A_6$. Thus, since φ is injective, $(G, *)$ is isomorphic to a subgroup of $(A_6, \circ)$.

Let $K = \text{Im}(\varphi) \leq A_6$ and let

$$Y = \{aK \mid a \in A_6\}$$

be the left cosets of K in $(A_6, \circ)$. Since $|K| = |G| = 60$ and $|A_6| = 360$, we obtain that $|Y| = 6$.

Let $\cdot : G \times Y \to Y$ be defined by

$$a \cdot (bK) = (\varphi(a) * b)K$$

for all $a \in G$ and $bK \in Y$. We claim that $\cdot$ is well-defined. Indeed if $bK, cK \in Y$ are such that $bK = cK$, then $b^{-1} * c \in K$ so $(\varphi(a) * b)^{-1} * (\varphi(a) * c) = (b^{-1} * \varphi(a)^{-1}) * \varphi(a) * c = b^{-1} * \varphi(a^{-1} * a) * c = b^{-1} * c \in K$ and thus $(\varphi(a) * b)K = (\varphi(a) * c)K$. Thus $\cdot$ is well-defined.

We claim that $\cdot$ is a group action of $(G, *)$ on Y. To see this, first note that $e \cdot (aK) = (\varphi(e) * a)K = aK$ for all $aK \in X$. Moreover, for all $aK \in Y$ and $b, c \in G$, we see that

$$\begin{aligned} b \cdot (c \cdot (aK)) &= b \cdot ((\varphi(c) * a)K) \\ &= (\varphi(b) * \varphi(c) * a)K \\ &= (\varphi(b * c) * a)K \\ &= \varphi(b * c) \cdot aK. \end{aligned}$$

Hence $\cdot$ is a group action of $(G, *)$ on Y.

Note since $K = \text{Im}(\varphi)$ that $a \cdot eK = \varphi(a)K = eK$ for all $a \in G$. Hence G acts trivially on eK. Therefore, if $Y_0 = Y \setminus \{K\}$, then $a \cdot y \in Y_0$ for all $y \in Y_0$ and $a \in G$. Thus $\cdot : G \times Y_0 \to Y_0$ is a group action. By Lemma 3.2.3, there is a homomorphism $\Phi : G \to S_{Y_0}$ such that $\Phi(a)(bK) = a \cdot bK = (\varphi(a) * b)K$ for all $a \in G$ and $bK \in Y_0$. Moreover, since $(G, *)$ is simple and $\ker(\Phi) \lhd G$ by Proposition 2.6.4, we know that $\ker(\Phi) = \{e\}$ or $\ker(\Phi) = G$.

We claim that $\ker(\Phi) = \{e\}$. To see this, suppose for the sake of a contradiction that $\ker(\Phi) = G$. Hence $a \cdot bK = bK$ for all $a \in G$ and $b \in A_6$ so $(\varphi(a) * b)K = bK$ for all $a \in G$ and $b \in A_6$ and thus $b^{-1} * \varphi(a) * b \in K$ for all $a \in G$ and $b \in A_6$. Therefore $b^{-1}Kb = K$ for all $b \in A_6$ so that $K \lhd A_6$ by the Normal Subgroup Test (Theorem 2.6.10). However, since $|K| = 60$ and $(A_6, \circ)$ is normal by Theorem 4.6.6, we have a contradiction. Hence $\ker(\Phi) = \{e\}$.

Since $\ker(\Phi) = \{e\}$, we see that $\Phi : G \to S_{Y_0}$ is injective. Using the same arguments as above (i.e. $S_{Y_0} \cong S_5$ and by using the sign homomorphism and an identical argument), we obtain an injective homomorphism $\Psi : G \to A_{|Y_0|} = A_5$. However, since Ψ is injective and $|G| = 60 = |A_5|$, we must have that Ψ is bijective and thus an isomorphism. Hence $(G, *) \cong (A_5, \circ)$ as desired. ∎

It turns out that the next order for which there is a finite, simple, non-abelian group is 168.

Chapter 5

Groups: Finite Abelian

So far in the course, we have developed some deep and powerful results on the structure of finite groups. In particular, for some values of n, we have determined all groups of order n up to isomorphism. Specifically, for a prime number p, Corollary 2.5.6 showed that there is only one group of order p, Corollary 3.5.10 showed that every group of order p^2 is abelian, and Corollary 2.5.8 showed that there are only two groups of order $2p$. However, even going to order pq where p and q are odd prime numbers turned out to be a challenge as although we had Theorem 4.4.3, there was Remark 4.4.5. Moreover, we have see in the previous chapter that determining all of the simple groups can be quite the challenging task.

In this chapter, we will greatly simplify our discussion of groups by focus on the abelian groups. In particular, we will obtain something remarkable; a complete characterization of all of the finite abelian groups.

5.1 The Fundamental Theorem of Finite Abelian Groups

Throughout this chapter, we will always + as the group operation on $\mathbb{Z}_n$. By using the product of such groups, the following theorem extends Corollary 2.5.7 to completely describes all finite abelian groups of a given order and determines these groups up to isomorphism.

Theorem 5.1.1 (The Fundamental Theorem of Finite Abelian Groups). *Let $(G, *)$ be a finite abelian group such that $|G| \geq 2$. Then there exists an $\ell \in \mathbb{N}$, prime numbers $p_1, \ldots, p_\ell$, and $m_1, \ldots, m_\ell \in \mathbb{N}$ such that*

$$G \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{m_\ell}}.$$

Moreover, if $l \in \mathbb{N}$, $q_1, \ldots, q_l$ are prime numbers, and $k_1, \ldots, k_l \in \mathbb{N}$ are such that

$$\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{m_\ell}} \cong \mathbb{Z}_{q_1^{k_1}} \times \mathbb{Z}_{q_2^{k_2}} \times \cdots \times \mathbb{Z}_{q_l^{k_l}},$$

then $\ell = l$ and there exists a $\sigma \in S_\ell$ such that $q_j = p_{\sigma(j)}$ and $k_j = m_{\sigma(j)}$.

That is, if $(G, *)$ is a finite abelian group of order at least 2, then $(G, *)$ is isomorphic to a product of cyclic groups of prime-power orders and this product is unique up to reordering.

Remark 5.1.2. Note that the uniqueness portion of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1) (i.e. showing that if two different decompositions are isomorphic, then there is a rearrangement of one into another) is the best we can hope for since the reordering of the groups in the product always produces isomorphic groups by Example 2.3.7 and Example 2.3.8.

Remark 5.1.3. Note that

$$|\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{m_\ell}}| = p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell}.$$

Therefore, it is possible to determine all finite abelian groups of order n up to isomorphisms by looking at the prime decomposition of n and the number of ways it can arise in the above form.

To begin to describe all abelian groups produced by Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we first look at the p-groups.

Example 5.1.4. Let p be a prime number. By the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), up to isomorphism there is exactly one finite abelian group of order p; namely $\mathbb{Z}_p$. Recall there was only one group of order p by Corollary 2.5.6.

Example 5.1.5. Let p be a prime number. By the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), up to isomorphism there are exactly two finite abelian group of order p^2; namely $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. Note this generalizes Corollary 2.5.7 from $p = 2$ to any prime provided we only consider abelian groups.

Example 5.1.6. Let p be a prime number. By the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), up to isomorphism there are exactly three finite abelian group of order p^3; namely $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

Example 5.1.7. Let p be a prime number. By Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), up to isomorphism there are exactly five finite abelian group of order p^4; namely

$$\begin{aligned}
&\mathbb{Z}_{p^4} \\
&\mathbb{Z}_{p^3} \times \mathbb{Z}_p \\
&\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \\
&\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \\
&\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.
\end{aligned}$$

Remark 5.1.8. Let p be a prime number. By Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), the number of unique finite abelian groups of order p^n up to isomorphism is the number of ways to write

$$n = m_1 + m_2 + \cdots + m_k$$

where $k, m_1, \ldots, m_k \in \mathbb{N}$ and

$$m_1 \geq m_2 \geq \cdots \geq m_k.$$

Note computing the number of such ways to "partition" n is an interesting combinatorial problem.

To apply the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1) to an order n that is is not the power of a prime, we can see by the statement of the theorem that we just need to apply Remark 5.1.8 to each prime factor of n to write down all possible p-subgroups that can occur (this tells us all the possible $\mathbb{Z}_{p^m}$ that can occur), and then take the product over all prime divisors of n. To clarify this, consider the following example.

Example 5.1.9. How many abelian groups of order 720 are there up to isomorphism? Since $720 = 2^4 \cdot 3^2 \cdot 5$, by the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1) we can write a complete list of abelian groups of order 720 by looking at each prime-power in the prime decomposition of 720, determining all abelian groups of order p^n, and taking the product group of the resulting groups for each prime. Doing so, we find there are 10 unique abelian groups of order 720; namely:

$$\begin{aligned}
&\mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \times \mathbb{Z}_3 \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5
\end{aligned}$$

(that is, there were 5 abelian groups of order 2^4, 2 abelian groups of order 3^2, and 1 abelian group of order 5).

It turns out that the idea used in Example 5.1.9 is exactly how we will prove the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1):

first show we can decompose every abelian group as a product of abelian p-groups, and then we will decompose each abelian p-group into one of the desired form. The uniqueness portion of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1) will follow by analyzing the number of group elements of each order in each decomposition and showing that these numbers determine the decompositions up to reordering.

5.2 Proof of the Fundamental Theorem of Finite Abelian Groups

To follow the roadmap to the proof of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1) presented at the end of the last section, we first show that we can decompose every abelian group as a product of abelian p-groups. We do so using Sylow p-subgroups and the fact the group is abelian.

Lemma 5.2.1. *Let $(G, *)$ be a finite abelian group with order $q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l}$ where $l \in \mathbb{N}$, $q_1, \ldots, q_l$ are distinct prime numbers, and $k_1, \ldots, k_l \in \mathbb{N}$. There exists abelian subgroups $G_1, G_2, \ldots, G_l$ of $(G, *)$ such that $|G_j| = q_j^{k_j}$ for all $j \in \{1, \ldots, l\}$ and*

$$G \cong G_1 \times G_2 \times \cdots \times G_l.$$

Proof. By Sylow's First Theorem (Theorem 4.1.7), for each $j \in \{1, \ldots, l\}$ there exists a Sylow q_j-subgroup G_j of $(G, *)$. Since $|G| = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l}$ and $q_i \neq q_j$ when $i \neq j$, we obtain that $|G_j| = q_j^{k_j}$. Moreover, since $(G, *)$ is abelian, $(G_j, *)$ is abelian for all $j \in \{1, \ldots, l\}$.

Define $\varphi : G_1 \times G_2 \times \cdots \times G_l \to G$ by

$$\varphi((a_1, a_2, \ldots, a_l)) = a_1 * a_2 * \cdots * a_l$$

for all $(a_1, a_2, \ldots, a_l) \in G_1 \times G_2 \times \cdots \times G_l$. We claim that φ is a homomorphism. To see this, note since $(G, *)$ is abelian that for all

$$(a_1, a_2, \ldots, a_l), (b_1, b_2, \ldots, b_l) \in G_1 \times G_2 \times \cdots \times G_l$$

we have

$$\begin{aligned}
&\varphi((a_1, a_2, \ldots, a_l) * (b_1, b_2, \ldots, b_l)) \\
&= \varphi((a_1 * b_1, a_2 * b_2, \ldots, a_l * b_l)) \\
&= (a_1 * b_1) * (a_2 * b_2) * \cdots * (a_l * b_l) \\
&= (a_1 * a_2 * \cdots * a_l) * (b_1 * b_2 * \cdots * b_l) \\
&= \varphi((a_1, a_2, \ldots, a_l)) * \varphi((b_1, b_2, \ldots, b_l)).
\end{aligned}$$

Therefore φ is a homomorphism.

Recall $\{(e, e, \ldots, e)\} \subseteq \ker(\varphi)$. We claim that $\ker(\varphi) = \{(e, e, \cdots, e)\}$. To see this, assume $(a_1, a_2, \ldots, a_l) \in \ker(\varphi)$. Therefore

$$e = \varphi((a_1, a_2, \ldots, a_l)) = a_1 * a_2 * \cdots * a_l.$$

Let $r_1 = q_2^{k_2} \cdots q_l^{k_l}$. Since $(G, *)$ is abelian, we obtain that

$$e = e^{r_1} = (a_1 * a_2 * \cdots * a_l)^{r_1} = a_1^{r_1} * a_2^{r_1} * \cdots * a_l^{r_1}.$$

However, since $q_j^{k_j} | r_1$ whenever $j \in \{2, \ldots, l\}$ and since $a_j \in G_j$ with $|G_j| = q_j^{k_j}$, we obtain that

$$e = a_1^{r_1} * a_2^{r_1} * \cdots * a_l^{r_1} = a_1^{r_1} * e * \cdots * e = a_1^{r_1}$$

by Corollary 1.7.22. Therefore, since $a_1 \in G_1$, since $|G_1| = q_1^{k_1}$, and since $\gcd(r_1, q_1) = 1$, we obtain by Corollary 1.7.22 that $a_1^{r_1} = e$ implies $a_1 = e$. Thus

$$e = a_2 * \cdots * a_l.$$

By repeating the above argument with $r_2 = q_3^{k_3} \cdots q_l^{k_l}$, we obtain that $a_2 = e$. By a finite recursion, we obtain that $a_1 = a_2 = \cdots = a_l = e$. Hence $\ker(\varphi) = \{(e, e, \ldots, e)\}$.

By the First Isomorphism Theorem (Theorem 2.8.1), we obtain that

$$G_1 \times G_2 \times \cdots \times G_l \cong \mathrm{Im}(\varphi).$$

However $\mathrm{Im}(\varphi) \leq G$ and

$$|\mathrm{Im}(\varphi)| = |G_1 \times G_2 \times \cdots \times G_l| = \prod_{j=1}^{l} |G_j| = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l} = |G|.$$

Hence $\mathrm{Im}(\varphi) = G$ so

$$G_1 \times G_2 \times \cdots \times G_l \cong G$$

as desired. ∎

With Lemma 5.2.1, to complete the proof of the existence portion of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we just need to write every abelian p-group in the desired form. This is done recursively via the following lemma, which has the most technical and non-intuitive proof in the course.

Lemma 5.2.2. *Let p be a prime number and let $(G, *)$ be a finite abelian p-group. Let $a \in G$ be an element with maximal order among all elements in G. Then there exists a subgroup $H \leq G$ such that $\langle a \rangle \cap H = \{e\}$ and $G \cong \langle a \rangle \times H$.*

Proof. For each $n \in \mathbb{N}$, let P_n be the mathematical statement that if $(G, *)$ is an abelian group of order p^n and $a \in G$ is an element with the maximal order among all elements in G, then there exists a subgroup $H \leq G$ such that $\langle a \rangle \cap H = \{e\}$ and $G \cong \langle a \rangle \times H$. We will proceed by induction on n.

Base Case: $n = 1$. In this case $|G| = p$. Hence $(G, *)$ is cyclic by Corollary 2.5.6. Thus if $a \in G$ is an element with maximal order, we must have $|a| = p$ so $\langle a \rangle = G$. Let $H = \{e\}$ so that $H \leq G$ and $\langle a \rangle \cap H = \{e\}$. Define $\varphi : G \to \langle a \rangle \times \{e\}$ by

$$\varphi(g) = (g, e)$$

for all $g \in G$. It is elementary to verify that φ is an isomorphism and thus $G \cong \langle a \rangle \times H$.

Inductive Step. Assume that P_n is true. Let $(G, *)$ be an abelian group of order p^{n+1} and let $a \in G$ be an element with maximal order among all elements in G. Since $|G| = p^{n+1}$, Lagrange's Theorem (Theorem 2.5.1) implies that the order of every element of $(G, *)$ is a power of p. Hence $|a| = p^m$ for some $m \in \mathbb{N}$.

If $\langle a \rangle = G$, then we can repeat the proof of the base case with $H = \{e\}$ and obtain that $G \cong \langle a \rangle \times H$. Hence we can assume $G \setminus \langle a \rangle \neq \emptyset$.

Let $b \in G \setminus \langle a \rangle$ be an element with the smallest possible order among all elements of $G \setminus \langle a \rangle$. We claim that $|b| = p$. To see this, suppose for the sake of a contradiction that $|b| \neq p$. Since $e \in \langle a \rangle$, we know that $b \neq e$ so $|b| > p$. Moreover, since p^m is the largest possible order for an element of $(G, *)$, we know that $|b| \in \{p^2, p^3, \ldots, p^m\}$. Note

$$|b^p| = \frac{|b|}{p} < |b|$$

by Corollary 1.7.22. Since b was the element with the smallest possible order among all elements of $G \setminus \langle a \rangle$, $|b^p| < |b|$ implies that $b^p \in \langle a \rangle$. Hence there exist an $r \in \mathbb{N}$ such that $b^p = a^r$.

Since $|b| \in \{p^2, p^3, \ldots, p^m\}$ and $|b^p| = \frac{|b|}{p}$, we obtain that

$$|a^r| = |b^p| \leq \frac{p^m}{p} = p^{m-1}.$$

Note that if $\gcd(r, p) = 1$ then $|a^r| = |a| = p^m$ by Corollary 1.7.22 which is impossible since $|a^r| \leq p^{m-1}$. Therefore $\gcd(r, p) \neq 1$. Since p is prime, this implies that $r = ps$ for some $s \in \mathbb{N}$.

Let

$$c = a^{-s} * b \in G.$$

Since $b = a^s * c$, since $a^s \in \langle a \rangle$, and since $b \in G \setminus \langle a \rangle$, it follows that $c \notin \langle a \rangle$ so $c \in G \setminus \langle a \rangle$. However, notice since $(G, *)$ is abelian that

$$c^p = (a^{-s} * b)^p = a^{-sp} * b^p = a^{-r} * b^p = (a^r)^{-1} * b^p = (b^p)^{-1} * b^p = e.$$

Therefore, $c \in G \setminus \langle a \rangle$ and $|c| = p < |b|$. Since this contradicts the fact that $b \in G \setminus \langle a \rangle$ was an element with the smallest possible order among all elements of $G \setminus \langle a \rangle$, we have a contradiction. Hence $|b| = p$ as claimed.

Next, we claim that $\langle a \rangle \cap \langle b \rangle = \{e\}$. Clearly $\{e\} \subseteq \langle a \rangle \cap \langle b \rangle$. To see the other inclusion, assume for the sake of a contradiction that there exists an $g \in \langle a \rangle \cap \langle b \rangle$ such that $g \neq e$. Therefore

$$g \in \langle b \rangle = \{e, b, b^2, \ldots, b^{p-1}\},$$

so $g = b^u$ for some $u \in \{1, \ldots, p-1\}$. Therefore $b^u \in \langle a \rangle$. However, since $\gcd(u, p) = 1$, by the Euclidean Algorithm there exists $t, v \in \mathbb{Z}$ such that $tu + pv = 1$. Therefore

$$b = b^1 = b^{tu+pv} = (b^u)^t * (b^p)^v = (b^u)^t * e^v = (b^u)^t = g^t \in \langle a \rangle.$$

Since this contradicts the fact that $b \in G \setminus \langle a \rangle$, we have a contradiction. Hence $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Let $B = \langle b \rangle$. Note that $B \lhd G$ since $(G, *)$ is abelian. Consider the quotient group G/B, which is abelian since $(G, *)$ is abelian (see Proposition 2.7.6). Hence

$$|G/B| = \frac{|G|}{|B|} = \frac{p^{n+1}}{p} = p^n.$$

By Proposition 2.7.6, we know that $|cB| \leq |c| \leq p^m$ for all $c \in G$.

We claim that the order of aB in G/B is p^m. To see this, note if $t \in \mathbb{N}$, then $(aB)^t = B$ if and only if $a^t B = B$ if and only if $a^t \in B$ if and only if $a^t = e$ since $a^t \in \langle a \rangle$ and $\langle a \rangle \cap B = \{e\}$. Therefore Corollary 1.7.23 implies that $|aB| = |a| = p^m$.

Therefore $(G/B, *)$ is an abelian group of order p^n and aB is an element of G/B with the maximal order among all elements in G/B. Hence the inductive hypothesis implies there exists a subgroup $H_0 \leq G/B$ such that $\langle aB \rangle \cap H_0 = \{eB\}$ and $G/B \cong \langle aB \rangle \times H_0$.

Let $q : G \to G/B$ be the quotient map and let

$$H = q^{-1}(H_0)$$

which is a subgroup of $(G, *)$ by Theorem 2.1.11. Moreover, since $\varphi(q(B)) = \{e\} \in H_0$, we see that $B \subseteq H$. Therefore $B \leq H$ by Definition 1.5.1.

Define $\psi : H \to G/B$ by $\psi(h) = hB$ for all $h \in H$. It is elementary to check that ψ is a homomorphism, $\ker(\psi) = B$ (i.e. ψ is obtained by restricting the domain of q to H), and $\mathrm{Im}(\psi) = H_0$ (i.e. $H = q^{-1}(H_0)$). Therefore, by the First Isomorphism Theorem (Theorem 2.8.1), we obtain that $H_0 \cong H/B$. Hence $|H_0| = \frac{|H|}{|B|}$.

Note that

$$\begin{aligned} |G| &= |G/B||B| && \text{by Proposition 2.7.6} \\ &= |aB||H_0||B| && \text{since } G/B \cong \langle aB\rangle \times H_0 \\ &= p^m|H_0||B| && \text{since } |aB| = p^m \\ &= p^m|H| && \text{since } |H_0||B| = |H| \\ &= |a||H| && \text{since } |a| = p^m. \end{aligned}$$

We claim that $\langle a\rangle \cap H = \{e\}$. To see this, note that $\{e\} \subseteq \langle a\rangle \cap H$. To see the other inclusion, assume $x \in \langle a\rangle \cap H$. Since $x \in \langle a\rangle$ we see that $xB \in \langle aB\rangle$, and since $x \in H$ we see that

$$xB = q(x) \in q(H) = H_0.$$

Therefore $xB \in \langle aB\rangle \times H_0 = \{eB\}$. Thus $xB = eB$ so $x \in B$. Therefore $x \in \langle a\rangle \cap B = \{e\}$ so $x = e$ as desired. Hence $\langle a\rangle \cap H = \{e\}$.

Define $\varphi : \langle a\rangle \times H \to G$ by

$$\varphi((y, z)) = y * z$$

for all $y \in \langle a\rangle$ and $z \in H$. Since $(G, *)$ is abelian, we see that φ is a homomorphism by the same argument as used in Lemma 5.2.1. Moreover, note that $\varphi((y, z)) = e$ if and only if $y * z = e$ if and only if $z = y^{-1}$. However, if $y \in \langle a\rangle$, $z \in H$, and $z = y^{-1}$, then $z \in \langle a\rangle \cap H = \{e\}$ so $z = y = e$. Therefore $\ker(\varphi) = \{(e, e)\}$. Hence the First Isomorphism Theorem (Theorem 2.8.1) implies that

$$\langle a\rangle \times H \cong \mathrm{Im}(\varphi).$$

However, $\mathrm{Im}(\varphi) \leq G$ and

$$|\mathrm{Im}(\varphi)| = |\langle a\rangle \times H| = |\langle a\rangle||H| = |a||h| = |G|.$$

Hence $\mathrm{Im}(\varphi) = G$ so

$$\langle a\rangle \times H \cong G$$

as desired. Thus the inductive step is complete.

Therefore, by the Principle of Mathematical Induction, the proof is complete. ∎

By iterating applications of Lemma 5.2.2, we have the following.

Corollary 5.2.3. *Let p be a prime number and let $(G, *)$ be a finite abelian p-group. Then*

$$G \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_l}}$$

for some $l, k_1, \ldots, k_l \in \mathbb{N}$.

Proof. For each $n \in \mathbb{N}$, let P_n be the mathematical statement that if $(G, *)$ is an abelian group of order p^n then

$$G \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_l}}$$

for some $l, k_1, \ldots, k_l \in \mathbb{N}$. We will proceed by strong induction on n.

Base Case: $n = 1$. In this case $|G| = p$. Hence $G \cong \mathbb{Z}_p$ by Corollary 2.5.6. Thus the base case is complete.

Inductive Step. Assume that P_k is true for all $k \leq n$. Let $(G, *)$ be an abelian group of order p^{n+1}. Since for all $g \in G$ we have that $|g| \leq p^{n+1}$ by Lagrange's Theorem (Theorem 2.5.1), there exists an element $a \in G$ with maximal order among all elements in G. Therefore, since $|G| = p^{n+1}$, we have that $|a| = p^m$ for some $m \in \mathbb{N}$.

If $m = n + 1$, then $(G, *)$ is cyclic and $G \cong \mathbb{Z}_{p^{n+1}}$. Otherwise, $m \leq n$ and Lemma 5.2.2 implies there exists a subgroup $H \leq G$ such that $H \neq \{e\}$ and

$$G \cong \langle a \rangle \times H.$$

Since $|a| = p^m$, we have that $\langle a \rangle \cong \mathbb{Z}_{p^m}$ by Proposition 2.3.11. Moreover, since

$$p^{n+1} = |G| = |\langle a \rangle \times H| = |\langle a \rangle| \, |H| = p^m |H|,$$

we see that $|H| = p^{n+1-m}$. Thus, since $1 \leq m \leq n + 1$, the induction hypothesis implies that

$$H \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_l}}$$

for some $l, k_1, \ldots, k_l \in \mathbb{N}$. Hence, by Lemma 2.3.9,

$$G \cong \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_l}}$$

for some $l, k_1, \ldots, k_l \in \mathbb{N}$. Thus the inductive step is complete.

Therefore, by the Principle of Mathematical Induction, the proof is complete. ∎

Combining the above, we obtain the proof of the uniqueness portion of the Fundamental Theorem of Finite Abelian Groups.

Proof of the Uniqueness Portion of Theorem 5.1.1. Assume $(G, *)$ is a finite abelian group such that $|G| \geq 2$. Therefore

$$|G| = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l}$$

where $l \in \mathbb{N}$, $q_1, \ldots, q_l$ are distinct prime numbers, and $k_1, \ldots, k_l \in \mathbb{N}$. By Lemma 5.2.1, we know that

$$G \cong G_1 \times G_2 \times \cdots \times G_l$$

where $G_1, G_2, \ldots, G_l$ are abelian groups such that $|G_j| = q_j^{k_j}$ for all $j \in \{1, \ldots, l\}$. Moreover, for each $j \in \{1, \ldots, l\}$, Corollary 5.2.3 implies that

$$G_j \cong \mathbb{Z}_{q_j^{k_{j,1}}} \times \mathbb{Z}_{q_j^{k_{j,2}}} \times \cdots \times \mathbb{Z}_{q_j^{j,k_{j,l_j}}}$$

for some $l_j, k_{j,1}, \ldots, k_{j,l} \in \mathbb{N}$. Hence repeated use of Lemma 2.3.9 implies that

$$G \cong \mathbb{Z}_{q_1^{k_{1,1}}} \times \mathbb{Z}_{q_1^{k_{1,2}}} \times \cdots \times \mathbb{Z}_{q_l^{l,k_{l,l_l}}}$$

as desired. ∎

To prove the uniqueness portion of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we will analyzing the number of group elements of each order in each decomposition and show that these numbers determine the decompositions up to reordering. To begin, we need some notation.

Remark 5.2.4. For a group $(G, *)$ and $n \in \mathbb{N}$, let

$$N_n(G) = |\{a \in G \mid a^n = e\}|.$$

Note if $(G, *) \cong (H, \star)$ then $N_n(G) = N_n(H)$. Moreover, for all groups $(G_1, *_1)$ and $(G_2, *_2)$, note

$$N_n(G_1 \times G_2) = N_n(G_1)N_n(G_2)$$

since $(a, b)^n = (e_1, e_2)$ if and only if $a^n = e_1$ and $b^n = e_2$.

We can quickly obtain some information pertaining to the above quantities using our knowledge from MATH 1200.

Lemma 5.2.5. *Let $(G, *)$ be a cyclic group of order n and let $m \in \mathbb{N}$. Then $N_m(G) = \gcd(n, m)$.*

Proof. By Proposition 2.3.11, we know that $(G, *) \cong (\mathbb{Z}_n, +)$. Hence

$$N_m(G) = N_m(\mathbb{Z}_n).$$

Let $d = \gcd(m, n)$. By the Fundamental Theorem of Arithmetic (Theorem A.7.5), we can write $m = ds$ and $n = dt$ where $\gcd(s, t) = 1$.

For $[x] \in \mathbb{Z}_n$, note $[x]^m = e$ if and only if $mx \equiv 0 \mod n$ if and only if $n|(mx)$ if and only if $(dt)|(dsx)$ if and only if $t|sx$ if and only if $t|x$ since $\gcd(s, t) = 1$. However, there are exactly d values of x in $\{0, 1, 2, \ldots, n-\}$ such that $t|x$; namely 0, t, $2t$, …, $(d-1)t$ (as $dt = n$). Hence

$$N_m(G) = N_m(\mathbb{Z}_n) = d = \gcd(m, n)$$

as desired. ∎

Corollary 5.2.6. *Let p and q be prime numbers and let $j, k \in \mathbb{N}$. Then*

$$N_{p^j}\left(\mathbb{Z}_{q^k}\right) = \begin{cases} 1 & \text{if } p \neq q \\ p^{\min(k,j)} & \text{if } p = q \end{cases}.$$

Proof. By Lemma 5.2.5, we know that

$$N_{p_j}(\mathbb{Z}_{q^k}) = \gcd(p^j, q^k) = \begin{cases} 1 & \text{if } p \neq q \\ p^{\min(k,j)} & \text{if } p = q \end{cases}. \qquad \blacksquare$$

We are now ready to finish off the proof of the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1).

Proof of the Uniqueness Part of Theorem 5.1.1. Let $\ell, l \in \mathbb{N}$, let $p_1, \ldots, p_\ell$ and $q_1, \ldots, q_l$ be prime numbers, and let $m_1, \ldots, m_\ell, k_1, \ldots, k_l \in \mathbb{N}$. Assume if

$$G = \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{m_\ell}}$$
$$G' = \mathbb{Z}_{q_1^{k_1}} \times \mathbb{Z}_{q_2^{k_2}} \times \cdots \times \mathbb{Z}_{q_l^{k_l}},$$

then

$$G \cong G'.$$

Thus $|G| = |G'|$. Therefore, since

$$p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell} = |G| = |G'| = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l},$$

by the Fundamental Theorem of Arithmetic (Theorem A.7.5) we have that

$$\{p_1, \ldots, p_\ell\} = \{q_1, \ldots, q_l\}.$$

For a prime p in the above set and a $r \in \mathbb{N}$, let

$$n_p(r) = |\{i \mid 1 \leq i \leq \ell, p_i^{m_i} = p^r\}$$
$$n'_p(r) = |\{j \mid 1 \leq j \leq l, q_j^{k_j} = p^r\}.$$

To complete the proof, it suffices to prove that $n_p(r) = n'_p(r)$ for all prime p and $r \in \mathbb{N}$.

Fix a prime p and let

$$X_p = \{i \mid 1 \leq i \leq \ell, p_i = p\}$$
$$X'_p = \{j \mid 1 \leq j \leq l, q_j = p\}.$$

For $r \in \mathbb{N}$, let

$$x_p(r) = |\{i \in X_p \mid m_i \geq r\}|$$
$$x'_p(r) = |\{j \in X'_p \mid k_i \geq r\}|.$$

Note by construction that

$$x_p(r) - x_p(r+1) = n_p(r) \qquad \text{and} \qquad x'_p(r) - x'_p(r+1) = n'_p(r).$$

Therefore, to show that $n_p(r) = n'_p(r)$ for all $r \in \mathbb{N}$, it suffices to show that $x_p(r) = x'_p(r)$ for all $r \in \mathbb{N}$.

For $r \in \mathbb{N}$, let P_r be the mathematical statement that $x_p(r) = x'_p(r)$. We will proceed by strong induction (we really only a finite recursion is necessary).

Base Case: $r = 1$. Since

$$N_p\left(\mathbb{Z}_{p_i^{m_i}}\right) = \begin{cases} 1 & \text{if } p_i \neq p \\ p & \text{if } p_i = p \end{cases} \qquad \text{and} \qquad N_p\left(\mathbb{Z}_{q_j^{k_j}}\right) = \begin{cases} 1 & \text{if } q_j \neq p \\ p & \text{if } q_j = p \end{cases},$$

we obtain by Remark 5.2.4 that

$$p^{x_p(1)} = N_p(G) = N_p(G') = p^{x'_p(1)}.$$

Therefore $x_p(1) = x'_p(1)$.

Inductive Step. Assume P_t is true for all $t \leq r$; that is, $x_p(t) = x'_p(t)$ for all $t \leq r$. To see that P_{r+1} is true, note that

$$N_{p^{r+1}}\left(\mathbb{Z}_{p_i^{m_i}}\right) = \begin{cases} 1 & \text{if } p_i \neq p \\ p^{\min(m_i, r+1)} & \text{if } p_i = p \end{cases}$$

$$N_{p^{r+1}}\left(\mathbb{Z}_{q_j^{k_j}}\right) = \begin{cases} 1 & \text{if } q_j \neq p \\ p^{\min(k_j, r+1)} & \text{if } q_j = p \end{cases}.$$

Note if $i \in X_p$ then the the number of $t \leq r+1$ such that $t \leq m_i$ is exactly $\min(m_i, r+1)$. Therefore

$$N_{p^{r+1}}(G) = p^{x_p(1)+\cdots+x_p(r)+x_p(r+1)}$$

since the occurrence of $\mathbb{Z}_{p_i^{m_i}}$ in G multiplies $N_{p^{r+1}}(G)$ by $p^{\min(m_i, r+1)}$, adds 1 to the value of $x_p(t)$ for $t \leq m_i$, and adds 0 to the value of $x_p(t)$ for $t > m_i$. Similarly

$$N_{p^{r+1}}(G') = p^{x'_p(1)+\cdots+x'_p(r)+x'_p(r+1)}.$$

Therefore, since $x_p(t) = x'_p(t)$ for all $t \leq r$ and since

$$p^{x_p(1)+\cdots+x_p(r)+x_p(r+1)} = N_{p^{r+1}}(G) = N_{p^{r+1}}(G') = p^{x'_p(1)+\cdots+x'_p(r)+x'_p(r+1)},$$

we obtain that $x_p(r+1) = x'_p(r+1)$. Thus the inductive step is complete.

Therefore, by the Principle of Mathematical Induction, the proof is complete. ∎

5.3 Groups of Small Order

By the results of demonstrated in this course, we can determine how many groups of order n there are up to isomorphism for many different values of n. First, by the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we can easily determine all abelian groups of order n. Note all other groups of order n must be non-abelian and thus not isomorphic to the abelian groups.

Recall by Corollary 2.5.6 that if n is prime, then every group is cyclic and thus abelian. Hence if n is prime, we have completely determine all groups of order n up to isomorphism. Similarly, if $n = p^2$ where p is a prime number, then Corollary 3.5.10 implies all groups of order n are abelian and thus are characterized by the Fundamental Theorem of Finite Abelian Groups.

By Corollary 2.5.8, we know that if $n = 2p$ where p is prime, then there are exactly two groups of order n; namely $(\mathbb{Z}_{2p}, +)$ (which must be $\mathbb{Z}_2 \times \mathbb{Z}_p$ by the Fundamental Theorem of Finite Abelian Groups), and $(D_p, \circ)$. Finally, Theorem 4.4.3 completely determines all groups of order $n = pq$ up to isomorphism where p and q are primes provided $p < q$ and p does not divide $q - 1$.

Using the above results, we have the following table of groups. We have checked off every order where we have proved a complete list of groups of that order.

Order	Number	Abelian	Non-Abelian	Proved
1	1	$\{e\}$		✓
2	1	$\mathbb{Z}_2$		✓
3	1	$\mathbb{Z}_3$		✓
4	2	$\mathbb{Z}_{2^2}$, $\mathbb{Z}_2 \times \mathbb{Z}_2$		✓
5	1	$\mathbb{Z}_5$		✓
6	2	$\mathbb{Z}_2 \times \mathbb{Z}_3$	D_3	✓
7	1	$\mathbb{Z}_7$		✓
8	5	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$,	D_4, Q_8	×
9	2	$\mathbb{Z}_{3^2}$, $\mathbb{Z}_3 \times \mathbb{Z}_3$		✓
10	2	$\mathbb{Z}_2 \times \mathbb{Z}_5$	D_5	✓
11	1	$\mathbb{Z}_{11}$		✓
12	5	$\mathbb{Z}_{2^2} \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	D_6, A_4, ??	×
13	1	$\mathbb{Z}_{13}$		✓
14	2	$\mathbb{Z}_2 \times \mathbb{Z}_7$	D_7	✓
15	1	$\mathbb{Z}_3 \times \mathbb{Z}_5$		✓
16	14	5 (Example 5.1.7)	D_8, ???	×
17	1	$\mathbb{Z}_{17}$		✓
18	5	$\mathbb{Z}_2 \times \mathbb{Z}_{3^2}$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	D_9, $S_3 \times \mathbb{Z}_3$, ??	×
19	1	$\mathbb{Z}_{19}$		✓
20	5	$\mathbb{Z}_{2^2} \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$	D_{10}, ??, ??	×

Note that the first value of n for which we have not proved that we have a complete set of groups of order n up to isomorphism is $n = 8$. We can quickly rectify this situation with some ad hoc arguments.

Theorem 5.3.1. *Up to isomorphism, there are exactly five groups of order 8:* $(\mathbb{Z}_{2^3}, +)$, $(\mathbb{Z}_{2^2} \times \mathbb{Z}_2, \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$, $(D_4, \circ)$, *and* $(Q_8, \times)$.

Proof. By the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we know that the three abelian groups of order 8 are $(\mathbb{Z}_{2^3}, +)$, $(\mathbb{Z}_{2^2} \times \mathbb{Z}_2, \cdot)$, and $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$.

Clearly $(D_4, \circ)$, and $(Q_8, \times)$ are non-abelian groups of order 8 and thus not isomorphic to any of the above abelain groups. We claim that $(D_4, \circ)$ and $(Q_8, \times)$ are not isomorphic. To see this, note $(Q_8, \times)$ has exactly one element of order 2 (namely -1) whereas $(D_4, \circ)$ has at least two elements of order 2, namely (ρ^2 and τ). Hence $(D_4, \circ)$ and $(Q_8, \times)$ are not isomorphic. Hence, to complete the proof, it suffices to prove that every non-abelian group is isomorphic to either $(D_4, \circ)$ or $(Q_8, \times)$.

Assume $(G, *)$ is a non-abelian group of order 8. By Lagrange's Theorem (Theorem 2.5.1), if $a \in G$ then $|a|$ divides 8 so $|a| \in \{1, 2, 4, 8\}$.

We claim that $(G, *)$ does not have an element of order 8. To see this, suppose for the sake of contradiction that $(G, *)$ has an element $a \in G$ such that $|a| = 8$. Therefore, since $|a| = 8 = |G|$, G is cyclic and thus isomorphic

to $(\mathbb{Z}_8, +)$ by Proposition 2.3.11. Since this implies that $(G, *)$ is abelian, we obtain a contradiction. Hence $(G, *)$ does not have an element of order 8. Thus every element of $(G, *)$ has order 1, 2, or 4.

We claim that $(G, *)$ must have an element of order 4. To see this, suppose for the sake of a contradiction that $(G, *)$ does not have an element of order 4. Therefore $(G, *)$ has one element of order 1 (namely e), and 7 elements of order 2. Therefore, for all $a, b \in G$, we have that

$$\begin{aligned} a * b &= a * e * b \\ &= a * (a * b)^2 * b \\ &= a^2 * b * a * b^2 \\ &= e * b * a * e \\ &= b * a. \end{aligned}$$

Hence $(G, *)$ is abelian, which is a contradiction. Therefore $(G, *)$ has an element of order 4.

Let $c \in G$ be such that $|c| = 4$. Let $H = \langle c \rangle$. Since $|G| = 8 = 2(4) = 2|H|$ so $[G : H] = 2$, Proposition 2.6.6 implies that $H \lhd G$.

Choose $d \in G \setminus H$. Therefore, since the right cosets partition G and since $Hd \neq H$ as $d \notin H$, we obtain that $G = H \cup Hd$. Moreover, since H is normal,

$$d * c * d^{-1} \in dHd^{-1} = H.$$

Since

$$e = (d * c * d^{-1})^n = d * c^n * d^{-1}$$

if and only if $c^n = e$, we see that

$$|d * c * d^{-1}| = |c| = 4.$$

However, since H is a cyclic group of order 4 with c as a generator, we know the only elements of H with order 4 are c and c^3 (i.e. $c^4 = e$ and c^2 has order 2). Thus $d * c * d^{-1} = c$ or $d * c * d^{-1} = c^3$.

We claim that $d * c * d^{-1} = c^3$. To see this, suppose for the sake of contradiction that $d * c * d^{-1} = c$. Then $d * c = c * d$. However, since

$$G = H \cup Hd = \{e, c, c^2, c^3, d, c * d, c^2 * d, c^3 * d\},$$

and since d and c commute, we see that $(G, *)$ is abelian. Since this contradicts the fact that $(G, *)$ is not abelian, we have a contradiction. Therefore $d * c * d^{-1} = c^3$ so

$$d * c = c^3 * d.$$

Recall $|d| \in \{2, 4\}$.

If $|d| = 2$, one can verify that the conditions $d * c = c^3 * d$, $|c| = 4$, and $|d| = 2$ implies that $(G, *)$ has the same multiplication table as $(D_4, \circ)$ with $c \leftrightarrow \rho$ and $d \leftrightarrow \tau$. Thus $(G, *) \cong (D_4, \circ)$ when $|d| = 2$.

When $|d| = 4$, consider d^2. We know that $|d^2| = 2$. Since $|e| = 1$, $|c| = 4$, $|c^3| = 4$, and $|d| = 4$, we know that

$$d^2 \in \{c^2, c * d, c^2 * d, c^3 * d\}.$$

If $d^2 = c^k * d$ for some $k \in \{1, 2, 3\}$, then $d = c^k$ for some $k \in \{1, 2, 3\}$ thereby contradicting the fact that $d \in G \setminus H$. Hence $d^2 = c^2$. Thus $d^3 = c^2 * d$.

Since the conditions $|c| = 4$, $d * c = c^3 * d$, and $d^2 = c^2$ along with

$$G = H \cup Hd = \{e, c, c^2, c^3, d, c * d, c^2 * d, c^3 * d\}$$

completely determine the multiplication table of $(G, *)$, we see that $(G, *)$ has the same multiplication table as $(Q_4, \times)$ with $c \leftrightarrow i$ and $d \leftrightarrow j$ (so $c^2 = -1$, $c^3 = -i$, $c * d = k$, $c^2 * d = -j$, and $c^3 * d = d * c = -k$). Thus $(G, *) \cong (Q_8, \times)$ when $|d| = 4$ thereby completing the proof. ∎

5.4 Semidirect Products

We see that our next gap in the values of n for which we have not proved that we have a complete set of groups of order n up to isomorphism is $n = 12$. However, as indicated in the table, there is a group of order 12 that we have yet to identify. Thus, this section will be devoted to a method for constructing a plethora of non-abelian groups. The main construction is as follows.

Proposition 5.4.1. *Let $(H, *)$ and $(K, \star)$ be groups and let $\alpha : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $G = H \times K$ and define $\cdot : G \times G \to G$ by*

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 * (\alpha(k_1))(h_2), k_1 \star k_2).$$

for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $(G, \cdot)$ is a group.

Proof. For simplicity, for $k \in K$ we will write α_k in place of $\alpha(k)$. Therefore, for all $k \in K$, $\alpha_k \in \mathrm{Aut}(H)$. Moreover, since α is a homomorphism, if e_K is the identity element of K, we have $\alpha_{e_K} = \mathrm{id}_H$. Finally, since α is a homomorphism, we have

$$\alpha_{k_1 \star k_2} = \alpha_{k_1} \circ \alpha_{k_2}$$

for all $k_1, k_2 \in K$.

To begin, note that $\cdot$ is a binary operation on G since

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 * \alpha_k(h_2), k_1 \star k_2) \in G$$

for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

To see that $(G, \cdot)$ is associative, note for all $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$ that

$$\begin{aligned}
&((h_1, k_1) \cdot (h_2, k_2)) \cdot (h_3, k_3) \\
&= (h_1 * \alpha_{k_1}(h_2), k_1 \star k_2) \cdot (h_3, k_3) \\
&= ((h_1 * \alpha_{k_1}(h_2)) * \alpha_{k_1 \star k_2}(h_3), (k_1 \star k_2) \star k_3) \\
&= (h_1 * (\alpha_{k_1}(h_2) * \alpha_{k_1 \star k_2}(h_3)), k_1 \star (k_2 \star k_3)) \\
&= (h_1 * (\alpha_{k_1}(h_2) * (\alpha_{k_1} \circ \alpha_{k_2})(h_3)), k_1 \star (k_2 \star k_3)) \\
&= (h_1 * (\alpha_{k_1}(h_2) * \alpha_{k_1}(\alpha_{k_2}(h_3))), k_1 \star (k_2 \star k_3)) \\
&= (h_1 * (\alpha_{k_1}(h_2 * \alpha_{k_2})(h_3)), k_1 \star (k_2 \star k_3)) \\
&= (h_1, k_1) \cdot (h_2 * \alpha_{k_2}(h_3), k_2 \star k_3) \\
&= (h_1, k_1) \cdot ((h_2, k_2) \cdot (h_3, k_3)).
\end{aligned}$$

Hence $(G, \cdot)$ is associative.

We claim that the identity element of $(G, \cdot)$ is (e_H, e_K) where e_H is the identity element of $(H, *)$ and e_K is the identity element of $(K, \star)$. To see this, note for all $h \in H$ and $k \in K$ that

$$\begin{aligned}
(h, k) \cdot (e_H, e_K) &= (h * \alpha_k(e_H), k \star e_K) \\
&= (h * e_H, k \star e_K) \\
&= (h, k)
\end{aligned}$$

and

$$\begin{aligned}
(e_H, e_K) \cdot (h, k) &= (e_h * \alpha_{e_K}(h), e_K \star K) \\
&= (e_H * \mathrm{id}_H(h), e_K \star k) \\
&= (e_H * h, e_K \star k) \\
&= (h, k).
\end{aligned}$$

Hence (e_H, e_K) is the identity element of $(G, \cdot)$.

Finally, to see that $(G, \cdot)$ has inverses, let $(h, k) \in G$ be arbitrary. Therefore $k \in K$ so there exists an element $k^{-1} \in K$ such that $k \star k^{-1} = k^{-1} \star k = e$. Note $\alpha_{k^{-1}}(h) \in H$ so there exists an $a \in H$ such that

$$a * \alpha_{k^{-1}}(h) = \alpha_{k^{-1}}(h) * a = e_H;$$

that is, $a = (\alpha_{k^{-1}}(h))^{-1}$ in H. Since $\alpha_{k^{-1}} \in \mathrm{Aut}(H)$, we know that

$$a = (\alpha_{k^{-1}}(h))^{-1} = \alpha_{k^{-1}}(h^{-1}).$$

We claim that (a, k^{-1}) is the inverse of (h, k) in $(G, \cdot)$. To see this, first note that

$$(a, k^{-1}) \cdot (h, k) = (a * \alpha_{k^{-1}}(h), k^{-1} \star k) = (e_H, e_K).$$

Moreover

$$\begin{aligned}(h,k)\cdot(a,k^{-1}) &= (h*\alpha_k(a), k\star k^{-1})\\ &= (h*\alpha_k(\alpha_{k^{-1}}(h^{-1})), k\star k^{-1})\\ &= (h*(\alpha_k\circ\alpha_{k^{-1}})(h^{-1}), k\star k^{-1})\\ &= (h*\alpha_{k\star k^{-1}}(h^{-1}), k\star k^{-1})\\ &= (h*\alpha_{e_K}(h^{-1}), k\star k^{-1})\\ &= (h*\mathrm{id}_H(h^{-1}), k\star k^{-1})\\ &= (h*h^{-1}, k\star k^{-1})\\ &= (e_H, e_K).\end{aligned}$$

Hence (a,k^{-1}) is the inverse of (h,k) in $(G,\cdot)$. Therefore, since $(h,k)\in G$ was arbitrary, $(G,\cdot)$ is a group. ∎

Of course, it is worthwhile to give the above group construction a name.

Definition 5.4.2. Let $(H,*)$ and $(K,\star)$ be groups and let $\alpha: K\to \mathrm{Aut}(H)$ be a homomorphism. The group $(H\times K,\cdot)$ from Proposition 5.4.1 is called the *semidirect product of H by K with respect to α* and is denoted $H\rtimes_\alpha K$.

Remark 5.4.3. When discussing $H\rtimes_\alpha K$, we will continue to use α_k for $\alpha(k)$ as was done in the proof of Proposition 5.4.1.

Remark 5.4.4. Note that if $\alpha_k=\mathrm{id}_H$ for all $k\in K$, then $H\rtimes_\alpha K$ is just the group product $H\times K$. Hence we have generalized the construction in Section 1.4.

Remark 5.4.5. Note that if $\alpha_k\neq\mathrm{id}_H$ for some $k\in K$, then there exists an $h\in H$ such that $\alpha_k(h)\neq h$. Therefore, in $H\rtimes_\alpha K$,

$$(e_H,k)\cdot(h,e_H)=(\alpha_k(h),k)\neq(h,k)=(h,e_H)\cdot(e_H,k).$$

Thus $H\rtimes_\alpha K$ will be a non-abelian group if $\alpha_k\neq\mathrm{id}_H$ for some $k\in K$.

For an example of a semidirect product group, we will construct a group of order 12.

Example 5.4.6. Let $(H,*)=(\mathbb{Z}_3,+)$, let $a\in H$ be a generator of H, and let $\varphi\in\mathrm{Aut}(\mathbb{Z}_3)$. Thus $\varphi(a)$ must be an element of order 3. Therefore, since a and a^2 are the elements of H of order 3, there are two options: $\varphi(a)=a$ or $\varphi(a)=a^2$.

If $\varphi(a)=a$, then $\varphi=\mathrm{id}_H$. Otherwise, if $\varphi(a)=a^2$, then $\varphi(a^2)=(a^2)^2=a$. One can check that $\psi(e)=e$, $\psi(a)=a^2$, and $\psi(a^2)=a$ is a automorphism of H (i.e. $\psi([x])=[x^2]$ is an automorphism of $(\mathbb{Z}_3,+)$). Note that $\psi^2=\mathrm{id}_H$.

Let $(K, \star) = (\mathbb{Z}_4, +)$ and let $b \in K$ be a generator of K. Define $\alpha : K \to \text{Aut}(\mathbb{Z}_3)$ by

$$\alpha_e = \text{id}_H, \quad \alpha_b = \psi, \quad \alpha_{b^2} = \text{id}_H, \quad \text{and} \quad \alpha_{b^3} = \psi.$$

It is elementary to see that α is a homomorphism since $b^4 = e$ and $\psi^2 = \text{id}_H$.

Consider the semidirect product group $G = H \rtimes_\alpha K$. Note by construction $|G| = 12$.

We claim that $(G, \cdot)$ is not abelian. To see this, note that $\alpha_b \neq id_H$ so $(G, \cdot)$ is not abelian by Remark 5.4.5.

Notice that

$$(a, b)^2 = (a * \alpha_b(a), b \star b) = (a * a^2, b^2) = (a^3, b^2) = (e_H, b^2).$$

Since $|b| = 4$ so $b^2 \neq e_K$, we see that $|(a, b)| \neq 2$. However, since

$$(a, b)^4 = (e_H, b^2)^2 = (e_H * \alpha_{b^2}(e_H), b^2 \star b^2) = (e_H * e_H, b^4) = (e_H, e_K),$$

we see that $|(a, b)|$ must divide 4 by Corollary 1.7.23. Since $|(a, b)| \neq 1$ and $|(a, b)| \neq 2$, we obtain that $|(a, b)| = 4$.

Note $(A_4, \circ)$ has zero elements of order 4 by Example 1.6.39. Moreover, since in $(D_6, \circ)$, $(\rho^n \circ \tau)^2 = e$ for all $n \in \{0, 1, 2, 3, 4, 5\}$ and $|\rho| = 6$, we see that $(D_6, \circ)$ has no elements of order 4. Therefore $H \rtimes_\alpha K$ is a non-abelian group that is not isomorphic to any other group of order 12 that we had previously discovered!

Before showing that the above is our last missing group of order 12, we will provide a method for demonstrating that a group is a semidirect product group. To begin, we first need a bit of information about the subgroup structure of semidirect products.

Remark 5.4.7. In the semidirect product $H \rtimes_\alpha K$, let

$$H_0 = \{(h, e_K) \mid h \in H\}$$
$$K_0 = \{(e_H, k) \mid k \in K\}.$$

It is elementary to verify that $H_0, K_0 \leq H \rtimes_\alpha K$ are such that $H_0 \cong H$ and $K_0 \cong K$. Moreover clearly $H_0 \cap K_0 = \{e\}$ and

$$G = \{h_0 \cdot k_0 \mid h_0 \in H_0, k_0 \in K_0\}.$$

Finally, notice for all $h, a \in H$ and $b \in K$ that

$$\begin{aligned}(a, b) \cdot (h, e_K) \cdot (a, b)^{-1} &= (a * \alpha_k(h) * a^{-1}, b \star b^{-1}) \\ &= (a * \alpha_k(h) * a^{-1}, e_K) \in H_0.\end{aligned}$$

Therefore, by the Normal Subgroup Test (Theorem 2.6.10), we obtain $H_0 \lhd H \rtimes_\alpha K$.

If fact, the necessary conditions demonstrated in Remark 5.4.7 for semidirect products are actually sufficient as the following result shows.

Theorem 5.4.8. *Let $(G, *)$ be a group. Assume $K \leq G$, $H \lhd G$, $H \cap K = \{e\}$, and*

$$G = \{h * k \mid h \in H, k \in K\}.$$

Then $G \cong H \rtimes_\alpha K$ for some homomorphism $\alpha : K \to \mathrm{Aut}(H)$.

Proof. Since $H \lhd G$, by the Normal Subgroup Test (Theorem 2.6.10), $aHa^{-1} = H$ for all $a \in G$. Thus, if for $a \in K$ we define $\alpha_a : H \to H$ by

$$\alpha_a(b) = a * b * a^{-1}$$

for all $b \in H$, α_a does indeed map into H and thus is well-defined.

We claim that $\alpha_a \in \mathrm{Aut}(H)$ for all $a \in K$. To see that α_a is a homomorphism, note for all $b_1, b_2 \in H$ that

$$\begin{aligned}
\alpha_a(b_1 * b_2) &= a * (b_1 * b_2) * a^{-1} \\
&= a * (b_1 * e * b_2) * a^{-1} \\
&= a * (b_1 * (a^{-1} * a) * b_2) * a^{-1} \\
&= (a * b_1 * a^{-1}) * (a * b_2 * a^{-1}) \\
&= \alpha_a(b_1) * \alpha_a(b_2).
\end{aligned}$$

Hence i_a is a homomorphism. Therefore, to show that $\alpha_a \in \mathrm{Aut}(H)$, it suffices to show that α_a is bijective.

To see that α_a is a bijective, it suffices to show that α_a is invertible. Note since $a^{-1} \in K$ that $\alpha_{a^{-1}}$ is well-defined and $\alpha_{a^{-1}} : H \to H$. Moreover, for all $b \in H$,

$$\begin{aligned}
(\alpha_a \circ \alpha_{a^{-1}})(b) &= \alpha_a(\alpha_{a^{-1}}(b)) \\
&= \alpha_a(a^{-1} * b * (a^{-1})^{-1}) \\
&= a * (a^{-1} * b * (a^{-1})^{-1}) * a^{-1} \\
&= (a * a^{-1}) * b * (a * a^{-1}) \\
&= e * b * e = b.
\end{aligned}$$

Hence $\alpha_a \circ \alpha_{a^{-1}} = \mathrm{id}_H$. Similarly (or by replacing a with a^{-1} in the previous expression that does work for all $a \in G$), we obtain that $\alpha_{a^{-1}} \circ \alpha_a = \mathrm{id}_H$. Hence α_a is invertible and thus an isomorphism. Thus $\alpha_a \in \mathrm{Aut}(H)$ for all $a \in K$.

Define $\alpha : K \to \mathrm{Aut}(H)$ by

$$\alpha(a) = \alpha_a$$

for all $a \in K$. We claim that α is a homomorphism. To see this, notice for all $a, b \in K$ and for all $c \in H$ that

$$\begin{aligned}
\alpha(a*b)(c) &= \alpha_{a*b}(c) \\
&= (a*b)*c*(a*b)^{-1} \\
&= a*b*c*b^{-1}*a^{-1} \\
&= a*(b*c*b^{-1})*a^{-1} \\
&= \alpha_a(b*c*b^{-1}) \\
&= \alpha_a(\alpha_b(c)) \\
&= (\alpha_a \circ \alpha_b)(c) \\
&= (\alpha(a) \circ \alpha(b))(c).
\end{aligned}$$

Therefore, since the above holds for all $c \in H$, we see that $\alpha(a*b) = \alpha(a) \circ \alpha(b)$ for all $a, b \in K$. Hence α is a homomorphism. Thus $H \rtimes_\alpha K$ exists.

To see that $G \cong H \rtimes_\alpha K$, define $\Phi : H \rtimes_\alpha K \to G$ by

$$\Phi((h,k)) = h*k$$

for all $(h,k) \in H \rtimes_\alpha K$. We claim that Φ is an isomorphism. To see that Φ is a homomorphism, note for all $(h_k, k_1), (h_2, k_2) \in H \rtimes_\alpha K$ that

$$\begin{aligned}
\Phi((h_k,k_1)\cdot(h_2,k_2)) &= \Phi((h_1 * \alpha_{k_1}(h_2), k_1*k_2)) \\
&= h_1 * \alpha_{k_1}(h_2) * k_1 * k_2 \\
&= h_1 * (k_1 * h_2 * k_1^{-1}) * k_1 * k_2 \\
&= h_1 * k_1 * h_2 * k_2 \\
&= \Phi((h_k,k_1)) * \Phi((h_2,k_2)).
\end{aligned}$$

Therefore Φ is a homomorphism.

Note since

$$G = \{h*k \mid h \in H, k \in K\} = \{\Phi((h,k)) \mid (h,k) \in H \rtimes_\alpha K\} = \mathrm{Im}(\Phi),$$

we obtain that Φ is surjective. Finally, if $(h,k) \in \ker(\Phi)$, then $e = \Phi((h,k)) = h*k$ so $h = k^{-1}$. Therefore $h \in H$ and $h = k^{-1} = K$ so $h \in H \cap K = \{e\}$. Hence $h = e$ so $k = e$. Thus $\ker(\Phi) = \{(e,e)\}$. Hence Φ is injective so Φ is an isomorphism. Hence $G \cong H \rtimes_\alpha K$ as desired. ∎

5.5 Groups of Order 12

Finally, it is time to show that the group from Example 5.4.6 is the only group of order 12 that we were missing. This will be demonstrated by showing every group of order 12 is a semidirect product. Thus, before we get to the proof, we need some results about the automorphism of certain groups.

Theorem 5.5.1. *For a natural number $n \geq 2$, $(\mathrm{Aut}(\mathbb{Z}_n), \circ) \cong (\mathbb{Z}_n^\times, \times)$.*

Proof. For each $k \in \mathbb{Z}_n^\times$, define $\varphi_{[k]} : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\varphi_{[k]}([a]) = [a][k] = [ak]$. Since multiplication in $\mathbb{Z}_n$ is well-defined, $\varphi_{[k]}$ is a well-defined function.

We claim that $\varphi_{[k]} \in \mathrm{Aut}(\mathbb{Z}_n)$ for all $[k] \in \mathbb{Z}_n^\times$. To see this, we first show that $\varphi_{[k]}$ is a homomorphism. Indeed, notice for all $[a], [b] \in \mathbb{Z}_n$ that

$$\varphi_{[k]}([a]+[b]) = \varphi_{[k]}([a+b]) = [k][a+b] = [k][a]+[k][b] = \varphi_{[k]}([a])+\varphi_{[k]}([b]).$$

Thus $\varphi_{[k]}$ is a group homomorphism.

To show that $\varphi_{[k]}$ is invertible and thus an automorphism on $(\mathbb{Z}_n, +)$, first notice that $\varphi_{[1]} = \mathrm{id}$ by definition. Moreover, for all $[k], [m] \in \mathbb{Z}_n^\times$ that

$$\varphi_{[k]}(\varphi_{[m]}([a])) = \varphi_{[k]}([m][a]) = [k][m][a] = [km][a] = \varphi_{[km]}([a])$$

for all $[a] \in \mathbb{Z}_n$. Hence $\varphi_{[k]} \circ \varphi_{[m]} = \varphi_{[km]}$. Therefore, since $[k]$ is invertible in $(\mathbb{Z}_n^\times, \times)$, there exists an $[s] \in \mathbb{Z}_n^\times$ such that $[ks] = [k][s] = [s][k] = [1]$. Therefore

$$\varphi_{[k]} \circ \varphi_{[s]} = \varphi_{[s]} \circ \varphi_{[k]} = \varphi_{[ks]} = \varphi_{[1]} = \mathrm{id}.$$

Hence $\varphi_{[k]}$ is invertible with $\varphi_{[k]}^{-1} = \varphi_{[s]}$. Hence $\varphi_{[k]}$ is an automorphism on $(\mathbb{Z}_n, +)$.

Next, let $\psi \in \mathrm{Aut}(\mathbb{Z}_n)$ be arbitrary. We claim that $\psi = \varphi_{[k]}$ for some $[k] \in \mathbb{Z}_n^\times$. To see this, let $[k] = \psi([1])$. Since $|[k]| = |\psi([1])| = |[1]| = n \neq 1$, we see that $[k] \neq [0]$ in $(\mathbb{Z}_n, +)$. Next, notice for all $a \in \{0, 1, \ldots, n-1\}$ that

$$\begin{aligned}
\psi([a]) &= \psi([1] + [1] + \cdots + [1]) \\
&= \psi([1]) + \psi([1]) + \cdots + \psi([1]) \\
&= [a]\psi([1]) \\
&= [a][k].
\end{aligned}$$

Therefore, since $\psi \in \mathrm{Aut}(\mathbb{Z}_n)$ and thus is bijective, there exists an $[s] \in \mathbb{Z}_n$ such that $\psi([s]) = [1]$. Thus $[k][s] = [s][k] = [1]$. As seen earlier in the course, this implies $\gcd(k, n) = 1$ and $[k] \in \mathbb{Z}_n^\times$. Hence $\psi = \varphi_{[k]}$. Therefore

$$\mathrm{Aut}(\mathbb{Z}_p) = \{\varphi_{[k]} \mid [k] \in \mathbb{Z}_n^\times\}.$$

We claim that $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $(\mathbb{Z}_n^\times, \times)$. To see this, define $\Phi : \mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n)$ by

$$\Phi([k]) = \varphi_{[k]}$$

for all $[k] \in \mathbb{Z}_n^\times$. Note Φ is well-defined as $\varphi_{[k]}$ is defined for each element of $\mathbb{Z}_n^\times$. We claim that Φ is a homomorphism. Indeed for all $[k], [m] \in \mathbb{Z}_n^\times$ we have that

$$\Phi([m][k]) = \Phi([mk]) = \varphi_{[mk]} = \varphi_{[m][k]} = \varphi_{[m]} \circ \varphi_{[k]} = \Phi([m]) \circ \Phi([k]).$$

Hence Φ is a homomorphism.

Note that Φ is onto since $\text{Aut}(\mathbb{Z}_n) = \{\varphi_{[k]} \mid [k] \in \mathbb{Z}_n^\times\}$. To see that Φ is one-to-one, note $\varphi_{[k]} = \text{id}$ if and only if $[a][k] = [a]$ for all $[a] \in \mathbb{Z}_n$ if and only if $[k] = [1]$, which is the identity element of $(\mathbb{Z}_n^\times, \times)$. Hence Φ is an isomorphism from $(\mathbb{Z}_n^\times, \times)$ to $\text{Aut}(\mathbb{Z}_n)$ thereby completing the proof. ∎

Theorem 5.5.2. *Up to isomorphism, there are exactly five groups of order 12: $(\mathbb{Z}_{2^2} \times \mathbb{Z}_3, +)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \cdot)$, $(D_6, \circ)$, $(A_4, \circ)$, and $\mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$ where α is as in Example 5.4.6.*

Proof. By the Fundamental Theorem of Finite Abelian Groups (Theorem 5.1.1), we know that the two abelian groups of order 12 are $(\mathbb{Z}_{2^2} \times \mathbb{Z}_3, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \cdot)$. By Remark 4.1.6, $(D_6, \circ)$ and $(A_4, \circ)$ are non-abelian groups that are not isomorphic. Moreover, by Example 5.4.6, $\mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$ is a non-abelian group that is not isomorphic to $(D_6, \circ)$ nor $(A_4, \circ)$. Therefore, up to isomorphism, there are at least five groups of order 12.

Assume $(G, *)$ is a group of order $12 = 2^2(3)$. The proof is complete provided $(G, *)$ is isomorphic to one of the above five non-isomorphic groups.

Let H be a Sylow 2-subgroup of $(G, *)$ and let K be a Sylow 3-subgroup of $(G, *)$. Note $|H| = 4$ so $H \cong \mathbb{Z}_4$ or $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by Corollary 2.5.7, and $|K| = 3$ so $K \cong \mathbb{Z}_3$. Note $H \cap K = \{e\}$ by Lemma 4.4.1.

Let n_2 denote the number of Sylow 2-subgroups of $(G, *)$ and let n_3 denote the number of Sylow 3-subgroups of $(G, *)$. By Example 4.3.2 we know that $n_2 \in \{1, 3\}$, $n_3 \in \{1, 4\}$, and there are no groups of order 12 with $n_2 = 3$ and $n_3 = 4$. We will divide the discussion based on the values of n_2 and n_3.

Case 1: $n_2 = 1$. In this case, H is the unique Sylow 2-subgroup of $(G, *)$ and thus $H \lhd G$. Since $K \cong \mathbb{Z}_3$, there exists an element $b \in K$ such that $|b| = 3$ and $K = \{e, b, b^2\}$. We claim that if

$$X = \{h * b^m \mid h \in H, m \in \{0, 1, 2\}\}$$

then $G = X$. To see this, first note that $X \subseteq G$. Therefore, since $|X| \leq 3|H| = |G|$, to see that $X = G$ it suffices to prove that $|X| = 3|H|$; that is, different pairs (h, m) produce different elements of $(G, *)$. To see this, assume $h_1, h_2 \in H$ and $m_1, m_2 \in \{0, 1, 2\}$ are such that

$$h_1 * b^{m_1} = h_2 * b^{m_2}.$$

Hence $h_2^{-1} * h_1 = b^{m_2 - m_1}$ so $h_2^{-1} * h_1 = b^{m_2 - m_1} \in H \cap K = \{e\}$. Therefore $h_2^{-1} * h_1 = e$ and $b^{m_2 - m_1} = e$ so $h_1 = h_2$ and $b^{m_1} = b^{m_2}$. Hence $|X| = 3|H|$ so $X = G$.

Note Theorem 5.4.8 implies that $G \cong H \rtimes_\alpha K$ for some homomorphism $\alpha : H \to \text{Aut}(H)$. Hence, to determine all groups of order 12 with $n_2 = 1$, it suffices to determine all semidirect products of a group of order 4 by a group

of order 3. Since $H \cong \mathbb{Z}_4$ or $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we divide the discussion into two subcases.

Case 1a: $H \cong \mathbb{Z}_4$. In this case, $H = \langle c \rangle$ where $|c| = 4$. Since $|\mathbb{Z}_4^\times| = 2$, we see by Theorem 5.5.1, $\mathrm{Aut}(H) = \{id_H, \psi_0\}$ where

$$\psi_0(e) = e, \quad \psi_0(c) = c^3, \quad \psi_0(c^2) = c^2, \quad \text{and} \quad \psi_0(c^3) = c.$$

Note $\psi_0^2 = \mathrm{id}_H$.

Consider $\alpha_b \in \mathrm{Aut}(H) = \{\mathrm{id}_H, \psi_0\}$. Since $\alpha_b^3 = \alpha_{b^3} = \alpha_e = \mathrm{id}_H$, we know that α_b must have order 1 or order 3. Since ψ_0 has order 2, $\alpha_b \neq \psi_0$. Hence $\alpha_b = \mathrm{id}_H$. Thus

$$b * h = \alpha_b(h) * b = h * b$$

for all $h \in H$. Therefore, since b generates K, we obtain that $(G, *)$ is abelian and thus already described. In particular, $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ in this subcase (that is, $\mathbb{Z}_4 \rtimes_{\mathrm{id}} \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_3$).

Case 1b: $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. In this case

$$H = \{e, c, d, c * d\}$$

where $c^2 = e$, $d^2 = e$, and $c*d = d*c$. Assume $\psi \in \mathrm{Aut}(H)$. Thus $\psi : H \to H$ is an isomorphism so $\ker(\psi) = \{e\}$. Therefore $\psi(c) \neq e$, $\psi(d) \neq e$, and $\psi(c * d) \neq e$. Moreover $\{\psi(c), \psi(d), \psi(c * d)\}$ must be $\{c, d, c * d\}$ so there are 6 options for the triple $(\psi(c), \psi(d), \psi(c * d))$; namely

$$\begin{aligned}
\psi_0 &= (c, d, c * d) \\
\psi_1 &= (c, c * d, d) \\
\psi_2 &= (d, c, c * d) \\
\psi_3 &= (d, c * d, c) \\
\psi_4 &= (c * d, c, d) \\
\psi_5 &= (c * d, d, c).
\end{aligned}$$

It is possible to verify that all ψ_k are indeed elements of $\mathrm{Aut}(H)$ via a multiplication table argument. Hence $\mathrm{Aut}(H)$ is a group of order 6 (and, as it is easily seen to be non-abelian, $\mathrm{Aut}(H) \cong D_3$). Note $\psi_0 = \mathrm{id}_H$, $\psi_1^2 = \mathrm{id}_H$, $\psi_2^2 = \mathrm{id}_H$, $\psi_3^3 = \mathrm{id}_H$, $\psi_4^3 = \mathrm{id}_H$, and $\psi_5^2 = \mathrm{id}_H$.

Consider $\alpha_b \in \mathrm{Aut}(H)$. Since $\alpha_b^3 = \alpha_{b^3} = \alpha_e = \mathrm{id}_H$, we know that α_b must have order 1 or order 3. If α_b has order 1, then $\alpha_b = \mathrm{id}_H$ so that

$$b * h = \alpha_b(h) * b = h * b$$

for all $h \in H$. Therefore $H \rtimes_\alpha K = H \times K$ for this α so $G \cong H \times K = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$.

Otherwise α_b has order 3 so $\alpha_b = \psi_3$ or $\alpha_b = \psi_4$. When $\alpha_b = \psi_3$, we see that

$$b * c = d * b, \quad b * d = (c * d) * b, \quad \text{and} \quad b * (c * d) = c * b.$$

These product relations along with $c^2 = e$, $d^2 = e$, $c * d = d * c$, and $|b| = 3$ and the description that

$$G = \{h * b^m \mid h \in H, m \in \{0, 1, 2\}\}$$

completely determine the multiplication table of $(G, *)$. One can verify that $(G, *) \cong (A_4, \circ)$ where

$$\begin{aligned} b &= \begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \\ c &= \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \\ d &= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \\ c * d &= \begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \end{aligned}$$

Similarly, when $\alpha_b = \psi_4$, we see that

$$b * c = (c * d) * b, \quad b * d = c * b, \quad \text{and} \quad b * d = c * b.$$

These product relations along with $c^2 = e$, $d^2 = e$, $c * d = d * c$, and $|b| = 3$ and the description that

$$G = \{h * b^m \mid h \in H, m \in \{0, 1, 2\}\}$$

completely determine the multiplication table of $(G, *)$. One can verify that $(G, *) \cong (A_4, \circ)$ where

$$\begin{aligned} b &= \begin{pmatrix} 2 & 4 & 3 \end{pmatrix} \\ c &= \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \\ d &= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \\ c * d &= \begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \end{aligned}$$

Thus this subcase is complete.

Hence Case 1 is complete.

Case 2: $n_3 = 1$. In this case, K is the unique Sylow 3-subgroup of $(G, *)$ so $K \lhd G$.

Since $K \cong \mathbb{Z}_3$, there exists an element $b \in K$ such that $|b| = 3$ and $K = \{e, b, b^2\}$. We claim that

$$G = \{b^m * h \mid h \in H, m \in \{0, 1, 2\}\}.$$

Indeed, since $H \cap K = \{e\}$ by Lemma 4.4.1, the proof follows from the same argument as used earlier in the proof. Therefore, Theorem 5.4.8 implies that $G \cong K \rtimes_\alpha H$ for some homomorphism $\alpha : H \to \text{Aut}(K)$. Therefore, to determine all groups of order 12 with $n_3 = 1$, it suffices to determine all semidirect products of a group of order 3 by a group of order 4.

Since $|\mathbb{Z}_3^\times| = 2$, we see by Theorem 5.5.1, $\text{Aut}(K) = \{id_K, \varphi_0\}$ where

$$\varphi_0(e) = e, \quad \varphi_0(b) = b^2, \quad \text{and} \quad \varphi_0(b^2) = b.$$

Note $\varphi_0^2 = \text{id}_K$.

Since $H \cong \mathbb{Z}_4$ of $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we divide the discussion into two subcases.

Case 2a: $H \cong \mathbb{Z}_4$. In this case, $H = \langle c \rangle$ where $|c| = 4$. Note $\alpha_c \in \{\text{id}_K, \varphi_0\}$.

If $\alpha_c = \text{id}_K$, then $\alpha_{c^n} = \text{id}_K$ for all $n \in \mathbb{N}$. Thus

$$h * k = \alpha_h(k) * h = k * h$$

for all $h \in H$ and $k \in K$. Therefore we obtain that $(G, *)$ is abelian and thus already described. In particular, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_4$ in this subcase (that is, $\mathbb{Z}_3 \rtimes_{\text{id}} \mathbb{Z}_4 = \mathbb{Z}_3 \times \mathbb{Z}_4$).

Otherwise, if $\alpha_c = \varphi_0$, then $\alpha_{c^2} = \text{id}_K$ and $\alpha_{c^3} = \varphi_0$. Therefore $G \cong \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_4$ where α is as in Example 5.4.6.

Hence this subcase is complete.

Case 1b: $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. In this case

$$H = \{e, c, d, c * d\}$$

where $c^2 = e$, $d^2 = e$, and $c * d = d * c$. Note $\alpha_c, \alpha_d \in \{\text{id}_K, \varphi_0\}$ and the value of $\alpha_{c*d} = \alpha_c \circ \alpha_d$ is determined by the values of α_c and α_d.

If $\alpha_c = \alpha_d = \text{id}_K$, then $\alpha_{c*d} = \text{id}_k$. Therefore

$$h * k = \alpha_h(k) * h = k * h$$

for all $h \in H$ and $k \in K$. Therefore we obtain that $(G, *)$ is abelian and thus already described. In particular, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ in this subcase .

If $\alpha_c = \varphi_0$ and $\alpha_d = \text{id}_K$, then

$$c * b = \alpha_c(b) * c = \varphi_0(b) * c = b^2 * c$$

and

$$d * b = \alpha_d(b) * d = b * d.$$

We claim that $(G, *) \cong (D_6, \circ)$. To show this, we will show that if $\rho = b*d$ and $\tau = c$, then $|\rho| = 6$, $|\tau| = 2$, and $\rho * \tau * \rho = \tau$. This suffices since these facts completely determine the multiplication table of $(D_6, \circ)$. Note $\tau = c$ implies $|\tau| = 2$.

Since b and d commute, we know that $(b*d)^n = b^n * d^n$. Therefore, since $d^n \in H$, $b^n \in K$, and $H \cap K = \{e\}$, we see that $(b*d)^n = e$ if and only if $b^n = e$ and $d^n = e$. Therefore, since $|b| = 3$ and $|d| = 2$, we see that $(b*d)^n = e$ if and only if n is a multiple of 6. Hence $|b*d| = 6$. Note this computations also shows that $b^n, d^n \in \langle\rho\rangle$ so

$$\{\rho^n * \tau^m \mid n \in \{0,1,2,3,4,5\}, m \in \{0,1\}\} = G.$$

Finally, note that

$$\begin{aligned}\rho*\tau*\rho &= (b*d)*c*(b*d)\\ &= b*d*b^2*c*d\\ &= b^3*d*c*d\\ &= e*d*c*d\\ &= d*c*d\\ &= d^2*c\\ &= c = \tau\end{aligned}$$

as desired. Hence $(G,*) \cong (D_6,\circ)$ when $\alpha_c = \varphi_0$ and $\alpha_d = \mathrm{id}_K$.

In the case that $\alpha_d = \varphi_0$ and $\alpha_c = \mathrm{id}_K$, one can just interchange c and d in the above to obtain that $(G,*) \cong (D_6,\circ)$. Similarly, if $\alpha_c = \varphi_0$ and $\alpha_d = \varphi_0$, one can just interchange d and $c*d$ in the above to obtain that $(G,*) \cong (D_6,\circ)$.

Hence this subcase and thus this case is complete.

As we have covered all possible cases, the proof is complete. ∎

We see that our next gap in the values of n for which we have not proved that we have a complete set of groups of order n up to isomorphism is $n = 16$. However, there are just too many groups of order 16 compared to the time remaining in the course. As the next gap is $n = 18$, we can quickly construct the missing group.

Example 5.5.3. Let $(H,*) = (\mathbb{Z}_3 \times \mathbb{Z}_3, \cdot)$. Note since $(\mathbb{Z}_3,+)$ is abelian, if we define $\psi : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3$ by

$$\psi((a,b)) = (a^{-1}, b^{-1})$$

for all $a, b \in \mathbb{Z}_3$, then $\psi \in \mathrm{Aut}(H)$. Note $\psi^2 = \mathrm{id}_H$.

Let $(K,\star) = (\mathbb{Z}_2,+)$ and let $b \in K$ be a generator of K. Define $\alpha : K \to \mathrm{Aut}(H)$ by

$$\alpha_e = \mathrm{id}_H, \quad \text{and} \quad \alpha_b = \psi.$$

It is elementary to see that α is a homomorphism since $b^4 = e$ and $\psi^2 = \mathrm{id}_H$.

Hence $H \rtimes_\alpha K$ is a group of order 18. One can verify that $H \rtimes_\alpha K$ is the group of order 18 missing on the list and can prove that all groups of order 18 have been found by using an argument similar to that used in Theorem 5.5.2.

Appendix A

MATH 1200 Background

In this appendix chapter, we will quickly review the basic background material from MATH 1200 that students should be familiar with when entering this course. Of course, this appendix chapter is not comprehensive and not a replacement for taking MATH 1200. In particular, note the following omits all discussion of proof technique as we expect students in third year be familiar with all proof techniques including direct, contradiction, cases, example/counterexample, and induction.

A.1 Sets

All mathematics must contain some notation in order for one to adequately describe the objects of study. As such, we begin by developing the notation surrounding one of the most basic objects in mathematics.

Heuristic Definition. A *set* is a collection of distinct objects.

To utilize sets, we must first develop notation to adequately describe sets and symbols to adequately describe operations on sets. First we begin with how to write an explicit set.

Notation A.1.1. There are two notations commonly used to describe a set: namely

$$\{\text{objects}\}$$

and

$$\{\text{objects} \mid \text{conditions on the objects}\}.$$

The following are some examples of how one can use set notation to describe a set.

Example A.1.2. The set of natural numbers, denoted $\mathbb{N}$, is the set

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

Example A.1.3. The set of integers, denoted $\mathbb{Z}$, is the set

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}.$$

Example A.1.4. The set of rational numbers, denoted $\mathbb{Q}$, is the set

$$\mathbb{Q} = \left\{ \frac{a}{b} \,\middle|\, a, b \text{ are integers with } b \neq 0 \right\}.$$

Example A.1.5. The set of real numbers, denoted $\mathbb{R}$, is far more complicated to define (see MATH 2001).

Example A.1.6. The set of complex numbers, denoted $\mathbb{C}$, is the set

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

where i is a special symbol (with $i^2 = -1$ once one defines multiplication on $\mathbb{C}$).

Considering the above, it is useful to have some terminology and notation to determine when an object is in a given set.

Definition A.1.7. Given a set X and an object x, it is said that x is an *element of* X, denoted $x \in X$, if x is one of the objects that make up X. We use $x \notin X$ to denote when x is not an element of X.

Example A.1.8. It is clear based on the above definitions that $\frac{1}{2} \in \mathbb{Q}$ yet $\frac{1}{2} \notin \mathbb{Z}$. Similarly $0 \in \mathbb{Z}$ but $0 \notin \mathbb{N}$.

It is also useful to have terminology and notation to describe when one set contains another.

Definition A.1.9. Given two sets A and B, it is said that B is a *subset of* A, denoted $B \subseteq A$, if whenever $b \in B$ then $b \in A$. We use $B \nsubseteq A$ to denote B is not a subset of A.

Example A.1.10. It is clear based on the above definitions that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q} \nsubseteq \mathbb{Z}$, and $\mathbb{Z} \nsubseteq \mathbb{N}$.

There is one special set that is a subset of every set and is quite useful to describe.

Definition A.1.11. The *empty set*, denoted $\emptyset$, is the set with no elements.

Remark A.1.12. If A is any set, then it is vacuously true that if $x \in \emptyset$ then $x \in A$ since there are no objects x so that $x \in \emptyset$. Hence $\emptyset \subseteq A$ for all sets A.

Of course, the notion of when two sets are equal should be obvious.

Definition A.1.13. Two sets A and B are said to be *equal*, denoted $A = B$, if A and B have precisely the same elements.

Remark A.1.14. If one is trying to prove two sets A and B are equal, one needs to demonstrate that $x \in A$ if and only if $x \in B$. If we divide this bi-conditional statement into its two components, we need to prove "if $x \in A$ then $x \in B$" and "if $x \in B$ then $x \in A$". Theses conditional statements are asking us to prove $A \subseteq B$ and $B \subseteq A$. Hence $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

When trying to prove two sets are equal, keep the above in mind as these ideas are the most common techniques to show that two sets are equal.

Now that the basics of sets have been established, we can start to construct new, larger sets from other sets. The following is a generalization of something students have seen in high school.

Definition A.1.15. Given an $n \in \mathbb{N}$ and sets $A_1, A_2, \ldots, A_n$, the *Cartesian Product of* $A_1, A_2, \ldots, A_n$ is the set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_k \in A_k \text{ for all } k \in \{1, 2, \ldots, n\}\}.$$

Remark A.1.16. The most common Cartesian Product students have seen and are familiar with is $\mathbb{R}^n$ (where $\mathbb{R}$ denotes the set of real numbers). Indeed $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ where we have taken the Cartesian Product of n copies of $\mathbb{R}$. For example

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$$

and

$$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

More generally,

$$\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$$

is one of the main objects of study in MATH 1021.

Instead of combining sets in pairs or, more generally, n-tuples, there is another common way to combine sets.

Definition A.1.17. Let I be a non-empty set and for each $\alpha \in I$, let A_α be a set. The *union of* $\{A_\alpha \mid \alpha \in I\}$, denoted $\bigcup_{\alpha \in I} A_\alpha$, is the set

$$\bigcup_{\alpha \in I} A_\alpha = \{x \mid x \in A_\alpha \text{ for some } \alpha \in I\}.$$

Example A.1.18. For two examples, if A denotes the set of all odd natural numbers and B denotes the set of all even natural numbers, then $\mathbb{N} = A \cup B$. Furthermore

$$\mathbb{N} = \bigcup_{n=1}^{\infty} \{2n - 1, 2n\}.$$

Instead of taking the set that contains all of the elements of a collection of sets, we can take the set of elements that are common to each set.

Definition A.1.19. Let I be a non-empty set and for each $\alpha \in I$, let A_α be a set. The *intersection of* $\{A_\alpha \mid \alpha \in I\}$, denoted $\bigcap_{\alpha\in I} A_\alpha$, is the set

$$\bigcap_{\alpha\in I} A_\alpha = \{x \mid x \in A_\alpha \text{ for all } \alpha \in I\}.$$

Example A.1.20. For example, $\{1\} = \bigcap_{n=1}^{\infty}\{1, n, n+1, \ldots\}$ as the number 1 is the only element of each set.

Furthermore, it is possible to 'take away' one set from another.

Definition A.1.21. Given two sets A and B, the *set difference of A by B*, denoted $A \setminus B$, is the set

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$$

To summarize the above set operations, consider the following example.

Example A.1.22. If $X = \{1, 2, 3\}$ and $Y = \{2, 4, 6\}$, then

$$X \cup Y = \{1, 2, 3, 4, 6\}, \quad X \cap Y = \{2\}, \quad \text{and} \quad X \setminus Y = \{1, 3\}.$$

Remark A.1.23. Often in mathematics one has a set X such that all other sets under consideration are subsets of X. Consequently, given a subset Y of X, the set difference $X \setminus Y$ will be called the *complement* of Y (in X) and will be denoted Y^c for convenience.

It turns out that the operation of taking the complement of a set turns unions into complements and vice versa as the following result shows.

Theorem A.1.24 (De Morgan's Laws). *Let X and I be non-empty sets and for each $\alpha \in I$ let X_α be a subset of X. Then*

$$\left(\bigcup_{\alpha\in I} X_\alpha\right)^c = \bigcap_{\alpha\in I} X_\alpha^c \qquad \textit{and} \qquad \left(\bigcap_{\alpha\in I} X_\alpha\right)^c = \bigcup_{\alpha\in I} X_\alpha^c.$$

Proof. Notice that

$$\begin{aligned} x \in \left(\bigcup_{\alpha\in I} X_\alpha\right)^c &\text{ if and only if } x \notin \bigcup_{\alpha\in I} X_\alpha \\ &\text{if and only if } x \notin X_\alpha \text{ for all } \alpha \in I \\ &\text{if and only if } x \in X_i^c \text{ for all } \alpha \in I \\ &\text{if and only if } x \in \bigcap_{\alpha\in I} X_\alpha^c \end{aligned}$$

which completes the proof of the first equation.

It is possible to repeat the same proof technique to show that the other equation holds. Alternatively, it is possible to use the first result to prove the second. To do this, we must first claim that that if $Y \subseteq X$ and $Z = Y^c$, then $Z^c = Y$; that is, the complement of the complement is the original set. Indeed notice $x \in Z^c$ if and only if $x \notin Z$ if and only if $x \notin Y^c$ if and only if $x \in Y$. Hence $Z^c = Y$.

To prove the second equality using the first, for each $\alpha \in I$ let $Y_\alpha = X_\alpha^c$. By applying the first equation using the Y_α's instead of the X_α's, we obtain that

$$\left(\bigcup_{\alpha\in I} Y_\alpha\right)^c = \bigcap_{\alpha\in I} Y_\alpha^c.$$

Since $Y_\alpha = X_\alpha^c$ so $Y_\alpha^c = X_\alpha$ for all $\alpha \in I$, we have that

$$\left(\bigcup_{\alpha\in I} Y_\alpha^c\right)^c = \bigcap_{\alpha\in I} Y_\alpha.$$

Hence

$$\bigcup_{\alpha\in I} Y_\alpha^c = \left(\bigcap_{\alpha\in I} Y_\alpha\right)^c$$

by taking the complement of both sides. ∎

Sets will play an important role in mathematics. However, one important question that has not been addressed is, "What exactly is a set?" This questions must be asked as we have not provided a rigorous definition of a set. This leads to some interesting questions, such as, "Does the collection of all sets form a set?"

To consider these questions, let us assume that there is a set of all sets; that is the set

$$Z = \{X \mid X \text{ is a set}\}$$

makes sense. Note Z has the interesting property that $Z \in Z$. Since Z is a set, we would think that

$$Y = \{X \mid X \text{ is a set and } X \notin X\}$$

is a valid subset of Z and thus a set. Considering Y, there are two disjoint possibilities: either $Y \in Y$ or $Y \notin Y$.

If it were the case that $Y \in Y$, then the definition of Y implies $Y \notin Y$ which is a contradiction since we cannot have both $Y \in Y$ and $Y \notin Y$. Thus, as $Y \in Y$ must be false, then it must be the case that $Y \notin Y$.

However, $Y \notin Y$ implies by the definition of Y that $Y \in Y$. Again this is a contradiction since we cannot have both $Y \notin Y$ and $Y \in Y$. Therefore, if Y is a set, we would have reached a logical inconsistency in mathematics.

The above argument is known as Russell's Paradox and demonstrates that there cannot be a set of all sets. Russell's Paradox illustrates the necessity of a rigorous definition of a set. However, said definition takes us beyond the study of this class.

A.2 Functions

With our knowledge of sets, we turn next to the morphisms between sets: functions. In order to formally define what a function is and for future use in the next section, we begin with the following more general object.

Definition A.2.1. Let X and Y be sets. A *relation from X to Y* is any subset R of $X \times Y$. For $x \in X$ and $y \in Y$, we write xRy if $(x, y) \in R$ and we write $x \not R y$ if $(x, y) \notin R$. In the case that $Y = X$, we say that R is a relation on X.

For a natural example of a relation and to see where the notation xRy comes from, consider the following.

Example A.2.2. For example

$$R = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$$

is a relation on $\mathbb{R}$ that we normally denote as $\leq$. Consequently, one sees that the notation 'xRy' for '$(x, y) \in R$' makes sense for this relation since $x \leq y$ exactly when $(x, y) \in R$.

The most formal definition of a function is that functions are specific types of relations.

Definition A.2.3. Let X and Y be sets. A *function f from X to Y* is a relation from X to Y such that if $x \in X$ then there exists a unique $y \in Y$ such that $(x, y) \in f$. We write $f : X \to Y$ to denote that f is a function from X to Y and for $x \in X$ we write $f(x)$ for the unique $y \in Y$ such that $(x, y) \in f$. The set X is called the *domain* of f and the set Y is called the *codomain* of f.

Functions go far beyond what one considers in calculus. For example, consider the following.

Example A.2.4. Let $(a_n)_{n \geq 1}$ be a sequence of real numbers. Define $f : \mathbb{N} \to \mathbb{R}$ by $f(n) = a_n$ for all $n \in \mathbb{N}$. Then f is a function with domain $\mathbb{N}$ and range $\mathbb{R}$.

Remark A.2.5. Given $f : X \to Y$, it is important to remember that f is the function whereas $f(x)$ is not the function; $f(x)$ is the value of the function f at the point $x \in X$ and thus $f(x)$ is a single element of Y.

As functions are really subsets of a Cartesian Product and we have a notion for when two sets are equal, we have a notion for when two functions are equal.

Definition A.2.6. Let $f : X \to Y$ and let $g : A \to B$. We say that f *equals* g, denoted $f = g$, if

- $X = A$, and
- $f(x) = g(x)$ for all $x \in X$.

That is, two functions are equal if they have the same domain and the same value on each element of the domain.

There are many ways to construct new functions from other functions depending on the circumstances. The following is one common and useful way to construct new functions.

Definition A.2.7. Let X, Y, and Z be sets and let $f : X \to Y$ and let $g : Y \to Z$. The *composition of f and g* is the function $g \circ f : X \to Z$ such that

$$(g \circ f)(x) = g(f(x))$$

for all $x \in X$.

Example A.2.8. Consider the functions $g : \mathbb{R} \to \mathbb{R}$ and $f : [0, \infty) \to \mathbb{R}$ defined by $g(x) = x^2 + 2x - 1$ for all $x \in \mathbb{R}$ and $f(x) = \sqrt{x} + 1$ for all $x \in [0, \infty)$. The function $g \circ f : [0, \infty) \to \mathbb{R}$ is well-defined. Moreover, for all $x \in [0, \infty)$, we have that

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(\sqrt{x} + 1) \\ &= (\sqrt{x} + 1)^2 + 2(\sqrt{x} + 1) - 1 \\ &= x + 4\sqrt{x} - 1\end{aligned}$$

for all $x \in [0, \infty)$.

There are many properties and information one may want to describe about a function. We begin with the following.

Definition A.2.9. Let $f : X \to Y$ and let $Z \subseteq X$. The *image of Z under f*, denoted $f(Z)$, is the set

$$f(Z) = \{f(z) \mid z \in Z\} \subseteq Y.$$

The *range* (or *image*) *of f* is the set

$$\text{Range}(f) = f(X) = \{f(x) \mid x \in X\}.$$

Example A.2.10. Let $f : [0, \infty) \to \mathbb{R}$ be defined by $f(x) = \sqrt{x} + 1$ for all $x \in [0, \infty)$. Assuming a knowledge of calculus, we can show that $\text{Range}(f) = [1, \infty)$. Furthermore $f([4, 9]) = [3, 4]$.

Definition A.2.11. A function $f : X \to Y$ is said to be *surjective* (or *onto*) if $f(X) = Y$; that is, for all $y \in Y$ there exists an $x \in X$ such that $f(x) = y$.

Example A.2.12. Clearly the function $f : [0, \infty) \to \mathbb{R}$ defined by $f(x) = \sqrt{x} + 1$ for all $x \in [0, \infty)$ is not surjective since $\text{Range}(f) = [1, \infty) \neq \mathbb{R}$.

However, the function $g : [0, \infty) \to [1, \infty)$ defined by $g(x) = \sqrt{x} + 1$ for all $x \in [0, \infty)$ is surjective since $\text{Range}(g) = [1, \infty)$. Thus the notion of when a function is surjective or not is really a consideration of what one is thinking of for the codomain of the function. We can always decrease the codomain of a function to be equal to its range thereby making the function surjective.

One way to think of a surjective function is that it is a function that obtains all possible outputs. There is another property one might want to consider of a function: when does the function yield unique outputs given distinct inputs.

Definition A.2.13. A function $f : X \to Y$ is said to be *injective* (or *one-to-one*) if for all $x_1, x_2 \in X$ with $x_1 \neq x_2$, we have that $f(x_1) \neq f(x_2)$.

Remark A.2.14. Note by taking the contrapositive of the definition of an injective function, we immediately see that a function $f : X \to Y$ is injective if whenever $x_1, x_2 \in X$ are such that $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Example A.2.15. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 2x + 1 = (x-1)^2$ for all $x \in \mathbb{R}$ is not injective since $0 \neq 2$ yet $f(0) = (0-1)^2 = (-1)^2 = 1$ and $f(2) = (2-1)^2 = 1^2 = 1 = f(0)$.

However, it is possible using calculus to show that the function $g : [1, \infty) \to \mathbb{R}$ defined by $g(x) = (x-1)^2$ for all $x \in [1, \infty)$ is injective. Thus the notion of when a function is injective or not depends on the domain of the function.

Of course, we can combine the notions of injective and surjective.

Definition A.2.16. A function $f : X \to Y$ is said to be *bijective* if f is injective and surjective.

Example A.2.17. The function $f : [0, \infty) \to [1, \infty)$ defined by $f(x) = \sqrt{x}+1$ for all $x \in [0, \infty)$ has already been seen to be surjective. As it is possible using calculus to show that f is injective, we obtain that f is a bijective function.

Similarly, the function $g : [1, \infty) \to [0, \infty)$ defined by $g(x) = (x-1)^2$ for all $x \in [1, \infty)$ has already be seen to be injective with the given domain. With the codomain written, it is possible using calculus to show that g is surjective. Hence g is a bijective function.

With f and g as in the above example, notice for all $x \in [0, \infty)$ that

$$g(f(x)) = g\left(\sqrt{x}+1\right) = \left(\left(\sqrt{x}+1\right)-1\right)^2 = \sqrt{x}^2 = x$$

and for all $y \in [1, \infty)$ that

$$f(g(y)) = f\left((y-1)^2\right) = \sqrt{(y-1)^2}+1 = (y-1)+1 = y.$$

Thus perhaps there is a connection between bijective functions and the following type of function.

Definition A.2.18. A function $f : X \to Y$ is said to be *invertible* if there exists a function $g : Y \to X$ such that

- $(g \circ f)(x) = g(f(x)) = x$ for all $x \in X$, and
- $(f \circ g)(y) = f(g(y)) = y$ for all $y \in Y$.

The function g is called an *inverse of* f.

Remark A.2.19. Note the two conditions required for f to be an invertible function make this a 'two-sided inverse'. This is similar to how wants to be able to multiple the inverse of a matrix A on either side of A and still get the identity.

Notice in Definition A.2.18 that we called g 'a' inverse of f and not 'the' inverse of f. This is because, for all we know, it might be possible that f has multiple inverses. The following shows this is not the case.

Lemma A.2.20. *Let $f : X \to Y$ be invertible. If g_1 and g_2 are inverse of f, then $g_1 = g_2$.*

Proof. Assume g_1 and g_2 are both inverses of f. Then for all $y \in Y$, we see by the defining properties of an inverse that

$$\begin{aligned} g_1(y) &= (g_2 \circ f)(g_1(y)) \\ &= g_2(f(g_1(y)) \\ &= g_2((f \circ g_1)(y)) \\ &= g_2(y). \end{aligned}$$

Hence $g_1 = g_2$ as desired. ∎

As Lemma A.2.20 demonstrates that there can be at most one inverse of an invertible function, we desire some notation to denote this function.

Notation A.2.21. If $f : X \to Y$ is an invertible function, the inverse of f is denoted by f^{-1}.

To culminate our exploration of bijective and invertible functions, we prove the following.

Theorem A.2.22. *Let $f : X \to Y$. Then f is invertible if and only if f is bijective.*

Proof. First, assume f is invertible. Thus f^{-1} exists. To see that f is bijective, we must show that f is injective and surjective.

$\underline{f \text{ is injective.}}$ To see that f is injective, let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$. Then

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2$$

where the middle equality follows since $f(x_1) = f(x_2)$. Therefore f is injective by definition.

$\underline{f \text{ is surjective.}}$ To see that f is surjective, let $y \in Y$ be arbitrary. Let $x = g(y) \in X$. Then

$$f(x) = f(g(y)) = y.$$

Hence $y \in f(X)$. Therefore, since $y \in Y$ was arbitrary, $f(X) = Y$. Hence f is surjective by definition.

Since f is injective and surjective, f is bijective as desired.

To see the converse direction, assume $f : X \to Y$ is bijective. To show that f is invertible, we must construct an inverse of f. To do this, let $y \in Y$ be arbitrary. Since f is surjective, we know that there exists an $x_1 \in X$ such that $f(x_1) = y$. Moreover, since f is injective, we know that if $x_2 \in X$ such that $f(x_2) = y$, then $f(x_2) = f(x_1)$ so that $x_2 = x_1$. Hence, for each $y \in Y$ there exists a unique element of x, which we will denoted by x_y, such that $f(x_y) = y$.

Consider the function $g : Y \to X$ defined by $g(y) = x_y$ for. Note g is well-defined by the above paragraph. We claim that g is an inverse of f. To see this, first note for all $y \in Y$ that

$$f(g(y)) = f(x_y) = y$$

as desired. To see that $g(f(x)) = x$ for all $x \in X$, let $x \in X$ be arbitrary. Since $f(x) = y$, we have that $x = x_y$ by the definition of x_y being the unique element of X that f sends to y. Hence

$$g(f(x)) = g(y) = x_y = x$$

as desired. Thus g is the inverse of f thereby completing the proof. ∎

To complete our introduction to functions, there is one more set based on functions we desire to study.

Definition A.2.23. Given $f : X \to Y$ and a subset $Z \subseteq Y$, the *preimage of Z under f* (or *inverse image*), denoted $f^{-1}(Z)$, is the set

$$f^{-1}(Z) = \{x \in X \mid f(x) \in Z\}.$$

Example A.2.24. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. Then

$$\begin{aligned} f^{-1}(\{1\}) &= \{1, -1\} \\ f^{-1}([4, \infty)) &= (-\infty, -2] \cup [2, \infty) \\ f^{-1}((-\infty, 0)) &= \emptyset. \end{aligned}$$

Remark A.2.25. It is important to note that although the notation $f^{-1}(Z)$ is used for the preimage of a set Z under f, the preimage of a set has nothing to do with invertibility and one does not need a function to be invertible to consider the preimage.

However, when $f : X \to Y$ is invertible and $Z \subseteq Y$, then, because f is bijective, it is possible to show that the preimage of Z under f is the equal to the image of Z under f^{-1}. To see this, assume $f : X \to Y$ is invertible and let $Z \subseteq Y$. As we normally use $f^{-1}(Z)$ to denote both sets we are interested in, let

$$\begin{aligned} A &= \{x \in X \mid f(x) \in Z\} && \text{(i.e. the preimage of } Z \text{ under } f) \\ B &= \{f^{-1}(z) \mid z \in Z\} && \text{(i.e. the image of } Z \text{ under } f^{-1}). \end{aligned}$$

To see that $A = B$, we will show that $A \subseteq B$ and $B \subseteq A$.

To see that $A \subseteq B$, let $a \in A$ be arbitrary. By the definition of A, this implies $f(a) \in Z$. Therefore, by the definition of B, $f^{-1}(f(a)) \in B$. Since $a = f^{-1}(f(a))$, we obtain that $a \in B$. Therefore, since $a \in A$ was arbitrary, $A \subseteq B$.

To see that $B \subseteq A$, let $b \in B$ be arbitrary. By the definition of B, there exists a $z \in Z$ such that $f^{-1}(z) = b$. Hence

$$f(b) = f(f^{-1}(z)) = z \in Z.$$

Therefore $b \in A$ by the definition of A. Hence, as $b \in B$ was arbitrary, $B \subseteq A$.

Hence $A = B$ so, when f is invertible, the preimage of Z under f is the equal to the image of Z under f^{-1}.

To prove some results in this course, it is helpful to know how the preimage of sets behave under unions and intersections.

Proposition A.2.26. *Let $f : X \to Y$, let I be a non-empty set, and for each $\alpha \in I$ let $Z_\alpha \subseteq Y$. Then*

$$f^{-1}\left(\bigcup_{\alpha \in I} Z_\alpha\right) = \bigcup_{\alpha \in I} f^{-1}\left(Z_\alpha\right) \qquad \text{and} \qquad f^{-1}\left(\bigcap_{\alpha \in I} Z_\alpha\right) = \bigcap_{\alpha \in I} f^{-1}\left(Z_\alpha\right).$$

Proof. The proof of this result is very similar to the proof of De Morgan's Laws.

Notice that

$$\begin{aligned} x \in f^{-1}\left(\bigcup_{\alpha\in I} Z_\alpha\right) &\text{ if and only if } f(x) \in \bigcup_{\alpha\in I} Z_\alpha \\ &\text{if and only if } f(x) \in Z_\alpha \text{ for at least one } \alpha \in I \\ &\text{if and only if } x \in f^{-1}(Z_\alpha) \text{ for at least one } \alpha \in I \\ &\text{if and only if } x \in \bigcup_{\alpha\in I} f^{-1}\left(Z_\alpha\right) \end{aligned}$$

which completes the proof of the first equation.

Similarly, notice that

$$\begin{aligned} x \in f^{-1}\left(\bigcap_{\alpha\in I} Z_\alpha\right) &\text{ if and only if } f(x) \in \bigcap_{\alpha\in I} Z_\alpha \\ &\text{if and only if } f(x) \in Z_\alpha \text{ for all } \alpha \in I \\ &\text{if and only if } x \in f^{-1}(Z_\alpha) \text{ for all } \alpha \in I \\ &\text{if and only if } x \in \bigcap_{\alpha\in I} f^{-1}\left(Z_\alpha\right) \end{aligned}$$

which completes the proof of the second equation. ∎

A.3 Equivalence Relations

Functions, although the most prevalent type of relation, are not the only special type of relation that is useful in in this course. Specifically, this section will focus on another type of relation that mimics the basic properties of equality.

Definition A.3.1. A relation R on a set X is said to be an *equivalence relation* if R has the following three properties:

- (*reflexive*) xRx for all $x \in X$.
- (*symmetric*) If $x, y \in X$ are such that xRy, then yRx.
- (*transitive*) If $x, y, z \in X$ are such that xRy and yRz, then xRz.

Remark A.3.2. It is common in mathematics to denote an equivalence relation by $\sim$.

Example A.3.3. Let $R = \{(x, y) \in \mathbb{R}^2 \mid x = y\}$. We claim that R is an equivalence relation. To see this, we must show that the three properties of an equivalence relation hold.

Reflexivity. To see that R is reflexive, let $x \in \mathbb{R}$ be arbitrary. Since $x = x$, we have by the definition of R that xRx. Hence, since $x \in \mathbb{R}$ was arbitrary, R is reflexive.

Symmetry. To see that R is symmetric, let $x, y \in \mathbb{R}$ be such that xRy. Thus the definition of R implies that $x = y$. Hence $y = x$ so that yRx. Therefore, since $x, y \in \mathbb{R}$ were arbitrary, R is symmetric.

Transitivity. To see that R is transitive, let $x, y, z \in \mathbb{R}$ be such that xRy and yRz. Therefore $x = y$ and $y = z$ by definition. Hence $x = z$ so xRz. Therefore, since $x, y, z \in \mathbb{R}$ were arbitrary, R is transitive.

Therefore, since R is reflexive, symmetric, and transitive, R is an equivalence relation.

Example A.3.4. Let $R = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$. To determine whether R is an equivalence relation, we will examine whether the three properties of an equivalence relation hold. If all three hold, then R is an equivalence relation. However, if at least one property fails, then R is not an equivalence relation.

Reflexivity. We claim that R is reflexive. To see this, let $x \in \mathbb{R}$ be arbitrary. Since $x \leq x$, we have that xRx. Therefore, since $x \in \mathbb{R}$ was arbitrary, R is reflexive.

Symmetry. We claim that R is not symmetric. To see this, note that $2R3$ since $2 \leq 3$, but $3 \not R 2$ since $2 \not\leq 3$. Hence R is not symmetric.

Transitivity. We claim that R is transitive. To see this, let $x, y, z \in \mathbb{R}$ be such that xRy and yRz. Therefore $x \leq y$ and $y \leq z$ by definition. Hence $x \leq z$ so xRz. Therefore, since $x, y, z \in \mathbb{R}$ were arbitrary, R is transitive.

Since R is not symmetric, R is not an equivalence relation.

Example A.3.5. Let Z be a set whose elements are sets (not the 'collection' of all sets). Define a relation $\sim$ on Z by $A \sim B$ if and only if there exists a bijective function from A to B. We claim that $\sim$ is an equivalence relation on Z. To see this, we must show that the three properties of an equivalence relation hold.

Reflexivity. To see that $\sim$ is reflexive, let $A \in Z$ be arbitrary. Since the (identity) map $f : A \to A$ defined by $f(a) = a$ for all $a \in A$ is a bijection, we have by the definition of $\sim$ that $A \sim A$. Hence, since $A \in Z$ was arbitrary, $\sim$ is reflexive.

Symmetry. To see that $\sim$ is symmetric, let $A, B \in Z$ be such that $A \sim B$. Thus the definition of $\sim$ implies that there is a bijective function $f : A \to B$. Hence $f^{-1} : B \to A$ is a bijection so $B \sim A$. Therefore, since $A, B \in Z$ were arbitrary, $\sim$ is symmetric.

Transitivity. To see that $\sim$ is transitive, let $A, B, C \in Z$ be such that $A \sim B$ and $B \sim C$. Therefore there exists bijections $f : A \to B$ and $g : B \to C$ by definition. Hence $g \circ f : A \to C$ is a bijection so $A \sim C$. Therefore, since $A, B, C \in Z$ were arbitrary, $\sim$ is transitive.

Therefore, since $\sim$ is reflexive, symmetric, and transitive, R is an equivalence relation.

In this context, for $A, B \in Z$, it is said that A and B have the same *cardinality* if $A \sim B$.

Equivalence relations will be used quite regularly in this course. For now, we turn to trying to think of equivalence relations as a form of equality. Of course there can exist objects that are equivalent with respect to an equivalence relation that are not equal. However, if we combine all elements that are equivalence to a given element, we get sets that are quite useful. These sets are some form of 'modding out by the equivalence relation' to construct objects that are equal based on the equivalence relation. To begin, let's be formal about these sets of equivalent elements.

Definition A.3.6. Let $\sim$ be an equivalence relation on a set X. For each $a \in X$, the *equivalence class of a with respect to $\sim$* is

$$[a] = \{x \in X \mid x \sim a\}.$$

Example A.3.7. Consider the cardinality equivalence relation from Example A.3.5. For a set A, we see that $[A]$ is the set of all sets $B \in Z$ such that there is a bijection from A to B. In particular, if A is a finite set, $[A]$ consists of all sets with the same number of elements as A.

To show that elements being equivalent under an equivalence relation relates to equality of the equivalence classes, we prove the following.

Lemma A.3.8. *Let $\sim$ be an equivalence relation on a set X and let $a, b \in X$. Then $a \sim b$ if and only if $[a] = [b]$.*

Proof. To begin, assume that $a \sim b$. To show that $[a] = [b]$, we will show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

To see that $[a] \subseteq [b]$, let $x \in [a]$ be arbitrary. Hence $x \sim a$ by the definition of an equivalence class. Since equivalence relations are transitive, $x \sim a$ and $a \sim b$ implies that $x \sim b$. Hence $x \in [b]$ by the definition of an equivalence class. Therefore, since $x \in [a]$ was arbitrary, $[a] \subseteq [b]$.

To see that $[b] \subseteq [a]$, note since equivalence relations are symmetric that $a \sim b$ implies $b \sim a$. Therefore by interchanging a and b in the previous paragraph, we obtain that $[b] \subseteq [a]$. Hence $[a] = [b]$ as desired.

To see the converse direction, assume $[a] = [b]$. Since equivalence relations are reflexive, we know that $a \sim a$ so $a \in [a]$ by the definition of an equivalence class. Therefore $a \in [a] = [b]$. Since $a \in [b]$, the definition of an equivalence class implies that $a \sim b$ as desired. ∎

The main benefit of considering equivalence classes is that they provide a partition of the entire space into sets of equivalent elements. The following result formalize this.

Proposition A.3.9. *Let $\sim$ be an equivalence relation on a set X and let*

$$\mathcal{C} = \{[a] \mid a \in X\}.$$

Then

a) for all $A \in \mathcal{C}$, $A \neq \emptyset$,

b) for all $x \in X$ there exists an $A \in \mathcal{C}$ such that $x \in A$, and

c) if $A, B \in \mathcal{C}$ and $A \neq B$, then $A \cap B = \emptyset$.

Proof. a) Let $A \in \mathcal{C}$ be arbitrary. By the definition of $\mathcal{C}$, $A = [a]$ for some $a \in X$. Since equivalence relations are reflexive, we know that $a \sim a$ so $a \in [a] = A$ by the definition of an equivalence class. Since $a \in A$, $A \neq \emptyset$. Therefore, since $A \in \mathcal{C}$ was arbitrary, the result holds.

b) Let $x \in X$ be arbitrary. Let $A = [x]$ so that $A \in \mathcal{C}$. Since equivalence relations are reflexive, we know that $x \sim x$ so $x \in [x] = A$ by the definition of an equivalence class. Therefore, since $x \in X$ was arbitrary, the result follows.

c) Let $A, B \in \mathcal{C}$ be such that $A \neq B$. Since $A, B \in \mathcal{C}$, the definition of $\mathcal{C}$ implies that there exists $a, b \in X$ such that $A = [a]$ and $B = [b]$.

Suppose for the sake of a contradiction that $A \cap B \neq \emptyset$. Hence there exists an $x \in X$ such that $x \in A \cap B$. Thus $x \in A = [a]$ and $x \in B = [b]$. Since $x \in [a]$ and $x \in [b]$, we have by the definition of an equivalence class that $x \sim a$ and $x \sim b$. Since equivalence relations are symmetric, $x \sim a$ implies $a \sim b$. Therefore, since equivalence relations are transitive and since $a \sim x$ and $x \sim b$, we obtain that $a \sim b$. Hence Lemma A.3.8 implies that $A = [a] = [b] = B$. Hence we have a contradiction to the fact that $A \neq B$ so $A \cap B \neq \emptyset$ as desired. ∎

A.4 Divides

One important collection of equivalence relations and equivalence classes in this course are derived from number theory and the idea of when one integer divides another.

Definition A.4.1. Given $n, m \in \mathbb{Z}$ with $n \neq 0$, it is said that n *divides* m, denoted $n|m$, if there exists a $k \in \mathbb{Z}$ such that $nk = m$.

Example A.4.2. Note that $12|132$ since $11 \in \mathbb{Z}$ and $11(12) = 132$. However, 12 does not divide 5 since for any integer $k \in \mathbb{Z}$, we see that $12k \leq 0 < 5$ when $k \leq 0$ and $12k \geq 12 > 5$ when $k \geq 1$.

Of course, there are some special numbers that can be defined based on divides.

Definition A.4.3. A natural number p is said to be *prime* if $p \neq 1$ and if $n \in \mathbb{N}$ and $n|p$, then $n = 1$ or $n = p$.

It is not too difficult verify numbers such as 2, 3, 5, 7, 11, and so on are primes. However, it is an incredibly difficult problem to find large prime numbers and verify whether or not a natural number is prime.

Luckily, the notion of divides behaves well with respect to the operations on the integers.

Proposition A.4.4. *For all $a, b, c, d, e \in \mathbb{Z}$ with $a \neq 0$, if $a|b$ and $a|c$, then $a|(bd + ce)$.*

Proof. Since $a|b$ and $a|c$, there exists $m, k \in \mathbb{Z}$ such that $am = b$ and $ak = c$. Note that

$$bd + ce = (am)d + (ak)e = a(md + ke).$$

Therefore, since $md + ke \in \mathbb{Z}$, we obtain that $a|(bd + ce)$ by the definition of divides. ∎

As seen earlier, it can be a difficult task to determine whether one natural number divides another. The following immediately rules out large numbers dividing small numbers.

Lemma A.4.5. *If $a, b \in \mathbb{Z} \setminus \{0\}$ are such that $a|b$, then $|a| \leq |b|$.*

Proof. Assume $a, b \in \mathbb{Z} \setminus \{0\}$ are such that $a|b$. Hence there exists a $k \in \mathbb{Z}$ such that $b = ak$. Note if $k = 0$ then $b = 0$ which contradicts the fact that $b \in \mathbb{Z} \setminus \{0\}$. Hence $k \neq 0$. Therefore $|k| \geq 1$ so

$$|b| = |a||k| \geq |a|1 = |a|$$

as desired. ∎

Of course, we know from elementary school that if we divide one natural number by another, then there can be a remainder. This is formalized via the following.

Theorem A.4.6 (Division Algorithm). *If $n, b \in \mathbb{Z}$ are integers such that $b > 0$, then there exists unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $n = qb + r$.*

Proof. To see the existence of q and r, let q be the greatest number in $\mathbb{Z}$ such that $bq \leq n$ (note the existence of such a q relies on fact that $|n|b > n$ and the Well Ordering Principle, which is logically equivalent to the Principle of Mathematical Induction). Since $q + 1 > q$, the choice of q as the greatest number such that $bq \leq n$ implies that

$$bq \leq n < b(q + 1) = bq + b.$$

Let $r = n - bq \in \mathbb{Z}$. Note $n = bq + r$. Moreover, since $bq \leq n$, we have that $r = n - bq \geq 0$. Finally, since $n < bq + b$, we have that $r = n - bq < b$. Hence $q, r \in \mathbb{Z}$ are such that $0 \leq r < b$ and $n = qb + r$.

To see the uniqueness of q and r, assume $q_0, r_0 \in \mathbb{Z}$ are such that $0 \leq r_0 < b$ and $n = q_0 b + r_0$. Therefore

$$qb + r = q_0 b + r_0$$

so

$$b(q - q_0) = r_0 - r.$$

Since $q - q_0 \in \mathbb{Z}$, this implies $b|(r_0 - r)$. However

$$-b < 0 - r \leq r_0 - r \leq r_0 - 0 < b.$$

Hence $|r_0 - r| < b$. Since $b|(r_0 - r)$ and since $|r_0 - r| < b$, Lemma A.4.5 implies that $r_0 - r = 0$ so $r_0 = r$. Hence $b(q - q_0) = 0$. Thus, since $b > 0$, we obtain that $q - q_0 = 0$ so $q = q_0$. Hence the values of q and r are unique. ∎

A.5 Modular Arithmetic

One important use of the notion of divides in this course will follow from a specific equivalence relation.

Theorem A.5.1. *Let $n \in \mathbb{N}$. Define the relation $\sim$ on $\mathbb{Z}$ by $m \sim k$ if and only if $n|(m - k)$. Then $\sim$ is an equivalence relation on $\mathbb{Z}$.*

Proof. To see that $\sim$ is an equivalence relation, we must show that the three properties of an equivalence relation hold.

Reflexivity. To see that $\sim$ is reflexive, let $m \in \mathbb{Z}$ be arbitrary. Since $m - m = 0$, since $0 \in \mathbb{Z}$, and since $0n = 0 = m - m$, we obtain that $n|(m - m)$ by definition. Thus $m \sim m$. Hence, since $m \in \mathbb{Z}$ was arbitrary, $\sim$ is reflexive.

Symmetry. To see that $\sim$ is symmetric, let $m, k \in \mathbb{Z}$ be such that $m \sim k$. Thus the definition of $\sim$ implies that $n|(m - k)$. Therefore Proposition A.4.4 implies that $n|(-(m - k))$ so $n|(k - m)$. Hence $k \sim m$. Therefore, since $m, k \in \mathbb{Z}$ were arbitrary, $\sim$ is symmetric.

Transitivity. To see that $\sim$ is transitive, let $m, k, l \in \mathbb{Z}$ be such that $m \sim k$ and $k \sim l$. Thus $n|(m - k)$ and $n|(k - l)$. Since

$$(m - k) + (k - l) = m - l,$$

we obtain by Proposition A.4.4 that $n|(m - l)$. Hence $m \sim l$. Therefore, since $m, k, l \in \mathbb{Z}$ were arbitrary, $\sim$ is transitive.

Therefore, since $\sim$ is reflexive, symmetric, and transitive, R is an equivalence relation. ∎

As the above equivalence relation is incredibly important, it deserves a name.

Definition A.5.2. Let $n \in \mathbb{N}$ and let $m, k \in \mathbb{Z}$. It is said that m and k are said to be *equivalent modulo* n, denoted $m \equiv k \mod n$, if and only if $n|(m-k)$.

The equivalence classes of the modulo n equivalence relation are easily obtained via the Division Algorithm (Theorem A.4.6).

Theorem A.5.3. *Let $n \in \mathbb{N}$ and for $k \in \mathbb{Z}$, let $[k]$ denote the equivalence class of k modulo n. For all $m \in \mathbb{Z}$, m is in one of the following equivalence classes:*

$$[0], \quad [1], \quad \ldots \quad [n-1].$$

Moreover no two of these equivalence classes are the same.

Proof. Let $m \in \mathbb{Z}$ be arbitrary. By the Division Algorithm (Theorem A.4.6), there exists $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < n$. Hence $nq = m - r$ so $n|(m-r)$. Thus $m \equiv r \mod n$ so $m \in [r]$. Therefore, since $0 \leq r < n$, we see that m is in one of the desired equivalence classes.

To see that no two of these equivalence classes are the same, assume $m, k \in \{0, 1, \ldots, n-1\}$ are such that $[m] = [k]$. Thus $m \equiv k \mod n$ so $n|(m-k)$. However, since $m, k \in \{0, 1, \ldots, n-1\}$, we see that

$$-(n-1) \leq 0 - k \leq m - k \leq m - 0 \leq n - 1.$$

Thus $|m-k| \leq n-1 < n$ and $n|(m-k)$. Hence Lemma A.4.5 implies that $m - k = 0$ so $m = k$. Hence no two of these equivalence classes are the same. ∎

The set of equivalence classes modulo n forms an important mathematical object.

Definition A.5.4. For $n \in \mathbb{N}$, the set of equivalence classes of 'modulo n' equivalence relation

$$\{[0], [1], \ldots, [n-1]\}$$

is called the *integers modulo* n and is denoted $\mathbb{Z}_n$.

Remark A.5.5. The importance of the integers modulo n comes from the arithmetic we can perform on them and its connection to computer science and cryptography. We want to define binary operations $+, \times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by setting

$$[m] + [k] = [m + k] \quad \text{and} \quad [m] \times [k] = [mk]$$

However, there is a potential problem: if $m_1, m_2, k_1, k_2 \in \mathbb{Z}$, if $[m_1] = [m_2]$, and if $[k_1] = [k_2]$, is it necessarily true that $[m_1 + k_1] = [m_2 + k_2]$ and $[m_1 k_1] = [m_2 k_2]$?

Lemma A.5.6. *Let $n \in \mathbb{N}$ and let $m_1, m_2, k_1, k_2 \in \mathbb{Z}$ be such that $[m_1] = [m_2]$ and $[k_1] = [k_2]$. Then $[m_1 + k_1] = [m_2 + k_2]$ and $[m_1 k_1] = [m_2 k_2]$.*

Proof. Assume $[m_1] = [m_2]$ and $[k_1] = [k_2]$. Hence $m_1 \equiv m_2 \mod n$ and $k_1 \equiv k_2 \mod n$ so $n|(m_1 - m_2)$ and $n|(k_1 - k_2)$. Therefore, Proposition A.4.4 implies that

$$n|((m_1 - m_2) + (k_1 - k_2))$$

so

$$n|((m_1 + k_1) - (m_2 + k_2))$$

and thus $m_1 + k_1 \equiv m_2 + k_2 \mod n$. Hence $[m_1 + k_1] = [m_2 + k_2]$ as desired.

To see that $[m_1 k_1] = [m_2 k_2]$, note that

$$\begin{aligned} m_1 k_1 - m_2 k_2 &= m_1 k_1 - 0 - m_2 k_2 \\ &= m_1 k_1 - (m_1 k_2 - m_1 k_2) - m_2 k_2 \\ &= (m_1 k_1 - m_1 k_2) + (m_1 k_2 - m_2 k_2) \\ &= m_1(k_1 - k_2) + k_2(m_1 - m_2). \end{aligned}$$

Therefore, since $n|(m_1 - m_2)$ and $n|(k_1 - k_2)$, Proposition A.4.4 implies that

$$n|(m_1(k_1 - k_2) + k_2(m_1 - m_2)).$$

Hence $n|(m_1 k_1 - m_2 k_2)$ so $m_1 k_1 \equiv m_2 k_2 \mod n$. Thus $[m_1 k_1] = [m_2 k_2]$ completing the proof. ∎

It turns out that the integers modulo n have all of the same algebraic properties that the integers do. In particular, one can verify the following holds by performing the corresponding computations in $\mathbb{Z}$.

Theorem A.5.7. *Let $n \in \mathbb{N}$. Working modulo n, the following are true:*

1 (Commutativity)

a $[a] + [b] = [b] + [a]$ *for all* $a, b \in \mathbb{Z}$.

b $[a][b] = [b][a]$ *for all* $a, b \in \mathbb{Z}$.

2 (Associativity)

a $([a] + [b]) + [c] = [a] + ([b] + [c])$ *for all* $a, b, c \in \mathbb{Z}$.

b $([a][b])[c] = [a]([b][c])$ *for all* $a, b, c \in \mathbb{Z}$.

3 (Distributivity)

- $[a]([b] + [c]) = ([a][b]) + ([a][c])$ *for all* $a, b, c \in \mathbb{Z}$.

4 (Units)

a $[0] + [a] = [a]$ *for all* $a \in \mathbb{Z}$.

b $[1][a] = [a]$ *for all* $a \in \mathbb{Z}$.

A.6 Basic Number Theory

In addition to the integers modulo n be imperative in this course, we will also require some basic number theory from MATH 1200. In particular, we need a good understanding of the following objects.

Definition A.6.1. Let $m, n \in \mathbb{N}$. A $d \in \mathbb{N}$ is said to be a *common divisor of m and n* if $d|m$ and $d|n$.

Example A.6.2. It is not difficult to see that the common divisors of 120 and 150 are 1, 2, 3, 5, 6, 10, 15, and 30.

What we are actually interested in is the largest such divisor.

Definition A.6.3. Let $m, n \in \mathbb{N}$. A $d \in \mathbb{N}$ is said to be the *greatest common divisor of m and n*, denoted $\gcd(m, n)$, if d is a common divisor of m and n and whenever $c \in \mathbb{N}$ is a common divisor of m and n, then $c \leq d$.

Example A.6.4. Based on the above list of common divisors of 120 and 150, we see that $\gcd(120, 150) = 30$.

Remark A.6.5. It is important to note that:

- for any $m, n \in \mathbb{N}$, 1 is always a common divisor of m and n, and
- for any $m, n \in \mathbb{N}$, if d is a common divisor of m and n then $d \leq \min(m, n)$.

These facts together imply that $\gcd(m, n)$ always exists as there is always a common divisor and there cannot be arbitrarily large common divisors.

Although it was easy to compute $\gcd(120, 150) = 30$, for larger numbers it is far more challenging. It turns out that there is an algorithm that we can use to compute the greatest common divisor of two numbers. Moreover, this algorithm has an important extension that is incredibly useful in many discussion in this course. To prove said algorithm, we require two lemmata.

Lemma A.6.6. *Let $a, b \in \mathbb{N}$. If $b|a$, then $\gcd(a, b) = b$.*

Proof. Assume $b|a$. Since $b(1) = b$, we see that $b|b$. Hence b is a common divisor of a and b so $\gcd(a, b) \geq b$. However, since any divisor of b is at most b and since $\gcd(a, b)$ is a divisor of b, we obtain that $\gcd(a, b) \leq b$. Hence $\gcd(a, b) = b$ as desired. ∎

Lemma A.6.7. *If $a, b, q, r \in \mathbb{N}$ are such that $a = qb + r$, then $\gcd(a, b) = \gcd(r, b)$.*

Proof. Assume that $a = qb + r$. Let $d = \gcd(a, b)$ and let $d_0 = \gcd(r, b)$. Since $d = \gcd(a, b)$, we know that $d|a$ and $d|b$. Therefore, since $r = a - qb$, since $d|a$, and since $d|b$, Proposition A.4.4 implies that $d|r$. Hence $d|r$ and $d|b$ so d is a common divisor of r and b. Thus $d \leq \gcd(r, b) = d_0$.

To see the other inequality, since $d_0 = \gcd(r, b)$, we know that $d|r$ and $d|b$. Therefore, since $a = bq + r$, since $d_0|r$, and since $d_0|b$, Proposition A.4.4 implies that $d_0|a$. Hence $d_0|a$ and $d_0|b$ so d_0 is a common divisor of a and b. Thus $d_0 \leq \gcd(a, b) = d$. Therefore $d = d_0$ completing the proof. ∎

With the above lemmata in hand, we can prove the desired algorithm.

Theorem A.6.8 (The Euclidean Algorithm). *Let $a, b \in \mathbb{N}$ be such that $a > b$. Consider the following algorithm:*

(I) Let $r_1 = a$.

(II) Let $r_2 = b$.

(III) For $n \geq 2$, if $r_1 > r_2 > \cdots > r_n > 0$, define r_{n+1} to be the remainder when we divide r_{n-1} by r_n.

We know step III will always produce r_{n+1} with $0 \leq r_{n+1} < r_n$ by the Division Algorithm. Thus this algorithm is well-defined.

Then:

(1) This algorithm terminates as there will exists an $m \in \mathbb{N}$ such that $r_{m+1} = 0$ and $r_m \neq 0$.

(2) For the m in (1), $r_m = \gcd(a, b)$.

(3) There exists $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$.

Proof. First, since $0 \leq r_{n+1} < r_n$ at each step, the algorithm must terminate in at most $r_1 + 1 = a + 1$ steps. Hence there exists an $m \in \mathbb{N}$ such that $r_{m+1} = 0$ and $r_m \neq 0$. Thus (1) is true.

To see that (2) is true, note by Lemma A.6.7 that

$$\gcd(r_k, r_{k+1}) = \gcd(r_{k+1}, r_{k+2})$$

for all $1 \leq k \leq m - 2$. Thus

$$\gcd(a, b) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{m-1}, r_m).$$

Moreover, since $r_{m+1} = 0$, we have that $r_m|r_{m-1}$ so $\gcd(r_m, r_{m-1}) = r_m$ by Lemma A.6.6. Hence

$$\gcd(a, b) = \gcd(r_{m-1}, r_m) = r_m$$

as desired. Thus (2) is true.

Finally, to see that (3) is true, we will apply a recursive argument. Recall that r_m was obtained as the remainder when r_{m-2} was divided by r_{m-1}. Hence there exists a $q_m \in \mathbb{N}$ such that

$$r_{m-2} = q_m r_{m-1} + r_m.$$

Thus

$$\gcd(a, b) = r_m = r_{m-2} - q_m r_{m-1}.$$

Therefore, there exists $t_{m-1}, s_{m-2} \in \mathbb{Z}$ such that

$$\gcd(a, b) = s_{m-2} r_{m-2} + t_{m-1} r_{m-1}.$$

To apply recursion, assume $2 \leq k \leq m-2$ and $s_k, t_{k+1} \in \mathbb{Z}$ are such that

$$\gcd(a, b) = s_k r_k + t_{k+1} r_{k+1}.$$

Since r_{k+1} was obtained as the remainder when r_{k-1} was divided by r_k, there exists a $q_k \in \mathbb{N}$ such that

$$r_{k-1} = q_k r_k + r_{k+1}.$$

Hence

$$r_{k+1} = r_{k-1} - q_k r_k.$$

Therefore

$$\begin{aligned} \gcd(a, b) &= s_k r_k + t_{k+1} r_{k+1} \\ &= s_k r_k + t_{k+1}(r_{k-1} - q_k r_k) \\ &= t_{k+1} r_{k-1} + (s_k - q_k t_{k+1}) r_k. \end{aligned}$$

Thus, with $s_{k-1} = t_{k+1} \in \mathbb{Z}$ and $t_k = s_k - q_k t_{k+1}$, we see that

$$\gcd(a, b) = s_{k-1} r_{k-1} + t_k r_k.$$

By repeating this argument at most k times, we obtain that

$$\gcd(a, b) = s_1 r_1 + t_2 r_2 = s_1 a + t_2 b$$

for some $s_1, t_2 \in \mathbb{Z}$ as desired. ∎

One important corollary of the Euclidean Algorithm (Theorem A.6.8) in this course is the following.

Corollary A.6.9. *Let $m, n \in \mathbb{N}$. In $\mathbb{Z}_n$, $[m]$ has a multiplicative inverse if and only if* $\gcd(m, n) = 1$.

Proof. First, assume $[m]$ has a multiplicative inverse in $\mathbb{Z}_n$. Hence there exists a $k \in \mathbb{Z}$ such that

$$[1] = [m][k] = [mk].$$

Therefore $mk \equiv 1 \mod n$ so $n|(mk-1)$. Hence there exists an $a \in \mathbb{Z}$ such that $mk - 1 = na$. Thus

$$mk - na = 1.$$

Let $d = \gcd(m, n)$. Since $d|m$ and $d|n$, we obtain that $d|(mk - na)$ by Proposition A.4.4. Therefore $d|1$ so Lemma A.4.5 implies that $|d| \leq 1$. Since $d \in \mathbb{N}$, this implies that $d = 1$ as desired.

Conversely, assume that $\gcd(m, n) = 1$. By the Euclidean Algorithm (Theorem A.6.8), there exists a $s, t \in \mathbb{Z}$ such that

$$ms + nt = 1.$$

Therefore

$$1 \equiv ms + nt \equiv ms + 0t \equiv ms \mod n,$$

so $[1] = [ms] = [m][s]$. Hence $[m]$ has a multiplicative inverse in $\mathbb{Z}_n$. ∎

A.7 The Fundamental Theorem of Arithmetic

To complete our review of MATH 1200, we will prove the Fundamental Theorem of Arithmetic (Theorem A.7.5) thereby showing that every natural number greater than 1 has a unique factorization into a product of primes. To do so, we begin with some notation and results that are also of use in this course.

Definition A.7.1. Two natural numbers a and b are said to be *coprime* if $\gcd(a, b) = 1$.

Lemma A.7.2. *Let $a, b, c \in \mathbb{N}$. If a and b are coprime and $a|bc$, then $a|c$.*

Proof. Assume a and b are coprime and $a|bc$. Since a and b are coprime so $\gcd(a, b) = 1$, the Euclidean Algorithm (Theorem A.6.8), there exists a $s, t \in \mathbb{Z}$ such that

$$as + bt = 1.$$

Therefore

$$c = c(1) = c(as + bt) = a(cs) + (bc)t.$$

Since $a|a$ and since $a|bc$, Proposition A.4.4 implies that $a|(a(cs) + (bc)t)$. Hence $a|c$ as desired. ∎

Lemma A.7.3. *Let p be a prime number. If $a, b \in \mathbb{N}$ and $p|ab$, then $p|a$ or $p|b$.*

Proof. Assume p is a prime number, $a, b \in \mathbb{N}$, and $p|ab$. To see that $p|a$ or $p|b$, assume that $p \nmid a$. Therefore, since p is prime and only has 1 and p as divisors, and since $p \nmid a$, we see that $\gcd(a, p) = 1$. Thus, since $\gcd(a, p) = 1$ and since $p|ab$, Lemma A.7.2 implies that $p|b$ as desired. ∎

Lemma A.7.4. *Let p be a prime number. For all $n \in \mathbb{N}$, if $a_1, \ldots, a_n \in \mathbb{N}$ and $p|(a_1 a_2 \cdots a_n)$, then $p|a_k$ for some $k \in \{1, 2, \ldots, n\}$.*

Proof. For each $n \in \mathbb{N}$, let P_n be the mathematical statement that if $a_1, \ldots, a_n \in \mathbb{N}$ and $p|(a_1 a_2 \cdots a_n)$, then $p|a_k$ for some $k \in \{1, 2, \ldots, n\}$. To prove that P_n is true for all $n \in \mathbb{N}$, we will use induction.

Base Case: $n = 1$. In this case $p|a_1$ thereby showing that P_1 is true.

Inductive Step. Assume that P_n is true. To see that P_{n+1} is true, let $a_1, \ldots, a_n, a_{n+1} \in \mathbb{N}$ be such that $p|(a_1 a_2 \cdots a_n a_{n+1})$. Hence

$$p|(a_1 a_2 \cdots a_n)a_{n+1}.$$

Therefore Lemma A.7.3 implies that $p|(a_1 a_2 \cdots a_n)$ or $p|a_{n+1}$. Note by the Induction Hypothesis that $p|(a_1 a_2 \cdots a_n)$ implies that $p|a_k$ for some $k \in \{1, 2, \ldots, n\}$. Hence we have that $p|a_k$ for some $k \in \{1, 2, \ldots, n, n+1\}$ thereby completing the inductive step.

Therefore, by the Principle of Mathematical Induction, the result is true. ∎

Theorem A.7.5 (The Fundamental Theorem of Arithmetic). *If $n \in \mathbb{N}$ and $n \geq 2$, there exists a unique list of distinct prime numbers $p_1, p_2, \ldots p_k$ and unique powers $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ such that*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Proof. We begin by showing each natural number greater than 1 is a product of primes.

For each $n \in \mathbb{N}$ with $n \geq 2$, let P_n be the mathematical statement that n is prime or a product of prime numbers. To prove that P_n is true for all $n \geq 2$, we will use strong induction.

Base Case: $n = 2$. Since 2 is a prime number, P_2 is true.

Inductive Step. Assume that P_k is true for all $2 \leq k < n$. To see that n is prime or a product of primes, we consider two cases. First, if n is prime, then clearly n is prime or a product of primes. Otherwise n is a composite number. Hence there exists $2 \leq m, k < n$ such that $n = mk$. By the inductive hypothesis m is prime or a product of primes, and k is prime or a product of primes. Therefore, since $n = mk$, we see that n is a product of primes. Hence P_n is true.

Therefore, by the Principle of Strong Induction, P_n is true for all $n \geq 2$. Hence

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

for some distinct prime numbers $p_1, p_2, \dots p_k$ and powers $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$.

To see the uniqueness of the above decomposition of n into a product of primes, assume

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$$

for some distinct prime numbers $q_1, q_2, \dots q_l$ and powers $\beta_1, \beta_2, \dots, \beta_l \in \mathbb{N}$. First, we claim that $\{p_1, \dots, p_k\} = \{q_1, \dots, q_l\}$ and thus $k = l$. To see this, suppose for the sake of a contradiction that $\{p_1, \dots, p_k\} \neq \{q_1, \dots, q_l\}$. Hence there exists a $p_j \notin \{q_1, \dots, q_l\}$ or a $q_i \notin \{p_1, \dots, p_k\}$.

First assume there is a $p_j \notin \{q_1, \dots, q_l\}$. Note $p_j | n$ since $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hence

$$p_j | q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}.$$

However, Lemma A.7.4 implies that $p_j | q_i$ for some i. Therefore, since p_j and q_i are prime, we obtain that $p_j = q_i$ thereby contradicting the fact that $p_j \notin \{q_1, \dots, q_l\}$. Since the case where there is a $q_i \notin \{p_1, \dots, p_k\}$ is similar, we have a contradiction. Hence $\{p_1, \dots, p_k\} = \{q_1, \dots, q_l\}$ and thus $k = l$.

By rearranging $q_1, \dots, q_k$ to be in the same order as $p_1, \dots, p_k$, we can assume without loss of generality that

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

and it remains to prove that $\beta_j = \alpha_j$ for all j. To see that $\beta_1 = \alpha_1$, suppose for the sake of a contradiction that $\beta_1 \neq \alpha_1$. We divide the discussion into two cases.

First, assume $\alpha_1 > \beta_1$. Since

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

this implies that

$$p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_2^{\beta_2} \cdots p_k^{\beta_k}.$$

Hence, since $\alpha_1 - \beta_1 > 0$, this implies that $p_1 | p_2^{\beta_2} \cdots p_k^{\beta_k}$. Thus either we have $p_1 | 1$ (i.e. $k = 1$) thereby contradicting the fact that p_1 is prime, or Lemma A.7.4 implies that $p_1 | p_j$ for some $j \in \{2, ldots, k\}$. However, since p_1 and p_j are prime numbers, this implies that $p_j = p_1$ thereby contradicting the fact that $p_1, p_2, \dots p_k$ are distinct prime numbers. Thus $\alpha_1 > \beta_1$ is impossible. Since the proof in the case that $\alpha_1 < \beta_1$ is similar, we obtain a contradiction. Hence $\beta_1 = \alpha_1$. As a similar argument shows that $\beta_j = \alpha_j$ for all j, the proof is complete. ∎

Index