Abstract Algebra
A Gentle Introduction

Volume I: Groups

Overwrite

2023
Version 0.1

[The] axioms for a group are short and natural, taking less than a line to write down and accounting for the natural notion of the symmetries of things. Yet somehow hidden behind these axioms is the monster simple group, a huge and extraordinary mathematical object, which appears to rely on numerous bizarre coincidences to exist. The axioms for groups give no obvious hint that anything like this exists.

— Richard Borcherds, 2009
([CB09])

Preface

Although algebra has a long history, it has undergone some quite striking changes in the past few decades. Abstract algebra is widely recognised as an essential element of higher mathematical education. The results and theorems that it showcases, however, are oft hard to grasp and understand without prerequisite knowledge or with a heavy background in mathematics. Most books on this subject are crafted for undergraduates at universities. They are not for a general mathematics enthusiast or one who seeks to understand more about the inner structure of algebra that many mathematicians encounter frequently.

It is thus the goal of this series of books to provide a step-by-step explanation of core results from abstract algebra; to demystify the core steps that many textbooks skip over when writing proofs. I aim to ensure that the results from such an essential field of study are as accessible, as approachable, and as understandable for as many people as possible.

Specifically, for this volume, we explore one of the most fundamental structures in abstract algebra: the group. As in most books, this book concentrates on abstract groups, and, in particular, on finite groups. This volume also discusses and explores some crucial results about the structure of groups in depth. The content covered in this volume should be more than enough for one to understand the fundamentals of group theory.

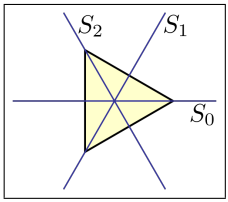
27 January, 2023

Contents

1 Introduction To Groups

1.1 The Study of Symmetry

A group is a *collection of symmetries of something*. A symmetry of something is a *mapping* from something to itself that *preserves structure*. This is, of course, not the formal definition of a group, but it gives an intuition of *why* mathematicians care about groups.

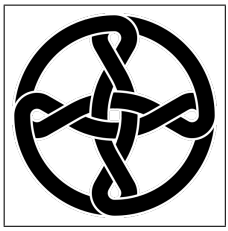


For example, one may consider the collection of symmetries of an equilateral triangle. What actions could one perform to make the triangle "look the same" as before applying the action? Well, we could do nothing. That action is called the *identity action*. We could also reflect the triangle about the line S_0 and observe that the triangle "looks the same as before". We may also reflect the triangle about the lines S_1 and S_2, and the triangle will still look the same as before. One may also consider rotating the triangle 120° or 240° about the centre in a clockwise manner (note that rotating the triangle 360° is the same as the identity action, so we do not count it here).

So, in total, we can count 6 distinct actions:

- 1 identity action
- 2 rotation actions
- 3 reflection actions

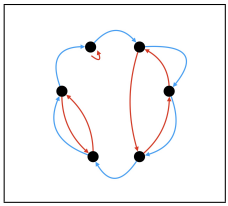
So we can say that the *group of symmetries of the triangle* has 6 actions (or elements) in total.



Another set of groups that we can consider is *groups of rotation*. For example, consider the image on the right. There are 4 actions that we can do to this image that makes it "look the same as before":

- Do nothing (the identity action).
- Rotate the circle 90° clockwise.
- Rotate the circle 180° clockwise.
- Rotate the circle 270° clockwise.

This image has **no** lines of symmetry. Due to the unique braiding on the knots, this image only has *rotational symmetry* and not *mirror* (or *reflective*) *symmetry*. Thus, this group has only 4 actions that are all rotations. One could say that this group is a *cyclic group* and that it has *order* 4 (we'll formally define what these terms mean in later chapters).



Let's look at a more technical example: consider a set of points in a pane. We can consider the *group of symmetries of a finite collection of points*. What are the symmetries of the points? Well, in this case, a *symmetry* is a way to move one of these points to another point whilst making it "look the same as before".

- One possible symmetry is given by the red arrows. In such a symmetry, we have a cycle of 3 points on the right, a cycle of 2 points on the left, and a point mapping to itself. Since the points "look the same as before", this is one valid symmetry.
- Another possible symmetry is given by the blue arrows. In this case, all points are shifted in a circle. Since the points "look the same as before", this is a valid symmetry.

One may notice that what each of the symmetries is doing is *permuting* the points around. In this case, this is exactly what each of the symme-

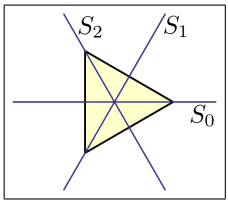
tries is doing: generating a possible permutation of points and ensuring that their locations stay the same. This is thus called the *symmetric group of degree 6*, and its group actions compose of *bijections from the set to itself.*

Exercise I.1.1. How many symmetries are there in the symmetric group of degree 6? In other words, what is the order of the group above? (*Hint: Consider the number of permutations in the group.*)

1.2 What Constitutes a Group?

Now that we have taken a look at some examples of groups, we now ask: what properties do all groups satisfy? What properties do all collections of symmetries satisfy?

These properties are known as the **axioms of groups**. We motivate the 'discovery' of such properties with examples.



Consider the group of symmetries of an equilateral triangle. One condition that the group of symmetries must satisfy is that performing group actions one after another should not make the underlying object "non-symmetric". We should not be able to apply group actions to other group actions until we obtain an action that results in the triangle being "non-symmetric". For example, we do not include rotating the triangle 90° clockwise about the line S_0 (into 3D space) as this immediately makes the triangle 'different to how it began'.

This property can be called the **axiom of closure** and can be written like this:

> A group $(G, *)$ is a set G together with a binary operation $*$ that ensures closure. That is, for any element a and b in the set G, we must ensure $a * b$ is in G.

(Of course, this is not the full definition, but we'll get into the other properties later.)

In the above example, the set G is the set of actions on the equilateral triangle that preserves symmetry. The binary operation $*$ is said to be the "followed by" operator. Thus:

> reflect about S_0 $*$ rotate the triangle 120° clockwise

means

> rotate the triangle 120° clockwise, *followed by* reflection about S_0

in standard English. In later chapters, such actions will be replaced with symbols. It should also be noted that we read actions **from right to left**, as seen in the example above.

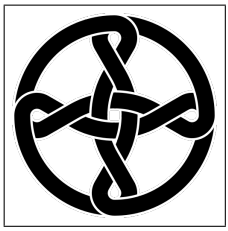
Another property that a group must have is the identity element. We emphasised this property numerous times in the above examples. This is called the **axiom of identity** and is phrased as follows:

> A group $(G, *)$ has an element e where for any element x in $(G, *)$, it satisfies $e * x = x * e = x$.

This means that the identity action should do nothing. Applying the action before or after another action should just perform the action.

We would also like, for every action, to have an action that *undoes* the previous action. For example, for rotation, we would like to *un-rotate* the rotation. This action is called the *inverse* of the action, and the **axiom of inverse** guarantees that every action in a group has an inverse:

> For every element x in the group $(G, *)$, there exists an action in the group, called the inverse of x and denoted by x^{-1}, such that $x * x^{-1} = x^{-1} * x = e$.



The last axiom is hard to discover naturally and hard to motivate, but is absolutely necessary for the definition of a group. Consider again this braided circle, and let's say we want to perform 3 rotations (say, r_1, r_2 and r_3) in that sequence. We would not want to differentiate between performing "r_1, then r_2 and r_3" (i.e., $r_1 * (r_2 * r_3)$), and between performing "r_1 then r_2, then r_3" (i.e. $(r_1 * r_2) * r_3$). We are only concerned about the *sequence* of the rotations. This is technically called the **axiom of associativity**:

> Let x, y, and z be elements in $(G, *)$. Then $(x * y) * z = x * (y * z)$.

So what is a group? A rigorous, careful, and mathematical definition of a group is as follows:

Definition I.1.2.1. *A group is a set G together with a operation on G, here denoted by $*$, satisfying the following conditions:*

1. ***Closure**: For all elements a and b in G, $a * b$ is also in G.*
2. ***Associativity**: For all elements a, b, and c in G, we have $a * (b * c) = (a * b) * c$.*
3. ***Identity**: There exists an element e in G such that for any element x in G we have $e * x = x * e = x$.*
4. ***Inverse**: For every element x in G, there exists an element x^{-1} in G such that $x * x^{-1} = x^{-1} * x = e$.*

Usually, for the brevity of notation, we will write $a * b$ as ab. We will look at more properties of groups in later chapters. We would usually suppress the operation $*$ when defining a group, so instead of saying that the group is $(G, *)$, we just say that the group is G.

1.3 Problems

Problem I.1.1. Determine whether the following are groups. If they are, prove it. If not, explain why they are not groups.

(a) $(\mathbb{Z}, +)$.

(b) $(\mathbb{Z} \setminus \{0\}, \times)$ where $\times$ denotes regular multiplication.

(c) $(\mathbb{R} \setminus \{0\}, \times)$ where $\times$ denotes regular multiplication.

(d) $(\{0\}, \times)$ where $\times$ denotes regular multiplication.

(e) $(\{1\}, +)$ where $+$ denotes regular addition.

(f) $(\{1\}, \times)$ where $\times$ denotes regular multiplication.

2 Basics of Groups

2.1 Basic Examples of Groups

Recall that a group has 4 axioms:

1. **Closure**: For all elements a and b in G, $a * b$ is also in G.
2. **Associativity**: For all elements a, b, and c in G, we have $a * (b * c) = (a * b) * c$.
3. **Identity**: There exists an element e in G such that for any element x in G we have $e * x = x * e = x$.
4. **Inverse**: For every element x in G, there exists an element x^{-1} in G such that $x * x^{-1} = x^{-1} * x = e$.

Recall also we write $a * b$ as ab, and say that the group $(G, *)$ is just G (suppressing the $*$).

Remark. If the group operation is additive, we write $a + b$ instead of ab.

Let's look at some examples of groups:

Example I.2.1.1. Let $\mathbb{Z}$ be the set of integers and let $+$ denote regular addition. Then $(\mathbb{Z}, +)$ forms a group:

1. **Closure**: For all integers a and b, we know $a + b$ is an integer.
2. **Associativity**: We know $a + (b + c) = (a + b) + c$.
3. **Identity**: The identity is 0, since $0 + x = x + 0 = x$.
4. **Inverse**: The inverse of integer x is $-x$, since $x + (-x) = (-x) + x = 0$.

An important thing to note about $(\mathbb{Z}, +)$ is that $+$ is *commutative*: $a + b = b + a$. A group with a commutative operation is called a **commutative group**. However, it is more often called an **abelian group**, named after Norwegian mathematician Niels Henrik Abel.

We now look at the notion of $\mathbb{Z}_n$.

Definition I.2.1.2. *The set* $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ *where* n *is a non-negative integer.*

Remark. Some sources (e.g. [Cla84], [Hum96]) define $\mathbb{Z}_n$ as a set of congruence classes modulo n, i.e. $\mathbb{Z}/n\mathbb{Z}$. We will show that these two definitions are equivalent in a future chapter.

Proposition I.2.1.3. *The set* $\mathbb{Z}_n$ *with the operation* $\oplus_n$ *such that* $a \oplus_n b = (a + b) \pmod{n}$ *forms a group.*

Proof. We prove this by showing the group axioms hold.

1. **Closure**: For a and b in $\mathbb{Z}_n$, $a \oplus_n b = (a+b) \pmod{n}$ is a integer between 0 and $n-1$. Thus $a \oplus b$ is inside $\mathbb{Z}_n$.
2. **Associativity**: For a, b, and c in $\mathbb{Z}_n$, since addition is associative, thus $a \oplus_n (b \oplus_n c) = (a+(b+c)) \pmod{n} = ((a+b)+c) \pmod{n} = (a \oplus_n b) \oplus_n c$.
3. **Identity**: The identity is 0 since for every x in $\mathbb{Z}_n$, $0 \oplus_n x = (0+x) \pmod{n} = (x+0) \pmod{n} = x \oplus_n 0 = x$.
4. **Inverse**: For inverses,
   - 0 is its own inverse since $0 \oplus_n 0 = 0$ which is the identity.
   - For any other integer x in $\mathbb{Z}_n$, the inverse is $n - x$. Since $1 \leq x \leq n-1$, thus $1 \leq n - x \leq n - 1$ so $n - x$ is indeed in $\mathbb{Z}_n$. Also, $x \oplus_n (n-x) = (x + (n-x)) \pmod{n} = n \pmod{n} = 0$ and $(n-x) \oplus_n x = ((n-x)+x) \pmod{n} = n \pmod{n} = 0$.

Since the four group axioms are satisfied, this is a group. □

One could use a **Cayley table** (or **group table**) to show that a structure is a group.

Example I.2.1.4. We show that $(\mathbb{Z}_6, \oplus_6)$ is a group. Note that:

$\oplus_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

1. For all x and y in $\mathbb{Z}_6$, $x \oplus_6 y$ is in $\mathbb{Z}_6$ from the above table.
2. For all x, y, and z in $\mathbb{Z}_6$, $x \oplus_6 (y \oplus_6 z) = (x \oplus_6 y) \oplus_6 z$ from the above table.
3. 0 is the identity since adding anything to it returns the original number.
4. Every row has an integer that when added gives 0.

Thus $(\mathbb{Z}_6, \oplus_6)$ is a group.

It should be noted that we use the convention of reading the **row before the column** in a group table. However, since this is an abelian group, the order does not matter. We will look at Cayley tables of non-abelian groups later.

Exercise I.2.1. Let $a \otimes_n b = (a \times b) \pmod{n}$. By using a group table, show that $(\mathbb{Z}_6, \otimes_6)$ does **not** form a group.

2.2 General Properties of Groups

Before we get into the general properties of groups, we introduce a useful notation for repeated application of $*$ on a single element a in the group G.

Definition I.2.2.1. *Let a be an element in G. Then*

$$a^n = \begin{cases} a * a * \cdots * a & \text{if } n > 0 \ (n \text{ copies of } a) \\ e & \text{if } n = 0 \\ a^{-1} * a^{-1} * \cdots * a^{-1} & \text{if } n < 0 \ (|n| \text{ copies of } a^{-1}) \end{cases}$$

Note that some laws of exponents apply to the above operation:

- $\left(a^{-1}\right)^m = (a^m)^{-1}$
- $a^{m+n} = a^m * a^n$
- $(a^m)^n = a^{mn}$

Proof of these properties are left as an exercise for the reader.

We are now ready to prove some properties of groups.

Proposition I.2.2.2. *The identity of a group G is unique.*

Proof. Suppose e_1 and e_2 are identities of the group G. Then, for all x in G, we have

$$e_1 x = x e_1 = x \text{ and } e_2 x = x e_2 = x,$$

since they are identities. Thus,

$$\begin{aligned} e_1 &= e_1 e_2 && \text{(since } e_2 \text{ is an identity, so } x e_2 = x) \\ &= e_2 && \text{(since } e_1 \text{ is an identity, so } x e_1 = x) \end{aligned}$$

Therefore $e_1 = e_2$, meaning that the identity is unique. □

Proposition I.2.2.3. $e^{-1} = e$

Proof. Clearly $e = ee^{-1}$ since $xx^{-1} = e$ for all elements x in G, including $x = e$. Also, $ee^{-1} = e^{-1}$ since e is the identity. Thus $e = e^{-1}$. □

Proposition I.2.2.4. *The inverse of an element x of a group G is unique.*

Proof. Suppose that a and b are inverses of x. Then we have

$$ax = xa = e \text{ and } bx = xb = e,$$

since a and b are inverses of x. Note that

$$\begin{aligned} a &= ae && \text{(since } e \text{ is the identity)} \\ &= a(xb) && \text{(since } b \text{ is an inverse, so } xb = e\text{)} \\ &= (ax)b && \text{(by associativity)} \\ &= eb && \text{(since } a \text{ is an inverse, so } ax = e\text{)} \\ &= b && \text{since } e \text{ is the identity)} \end{aligned}$$

Therefore $a = b$. Thus the inverse of x is unique. □

Proposition I.2.2.5 (Shoes and Socks)**.** *For all elements x and y in G, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Recall that if g^{-1} is the inverse of g then $gg^{-1} = g^{-1}g = e$. We will show that $(ab)(b^{-1}a^{-1}) = e$ and $(b^{-1}a^{-1})(ab) = e$.

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} && \text{(by associativity)} \\ &= a(e)a^{-1} && \text{(since } bb^{-1} = e\text{)} \\ &= aa^{-1} && \text{(since } e \text{ is the identity)} \\ &= e && \text{(since } aa^{-1} = e\text{)}, \end{aligned}$$

and,

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b && \text{(by associativity)}\\ &= b^{-1}(e)b && \text{(since } a^{-1}a = e\text{)}\\ &= b^{-1}b && \text{(since } e \text{ is the identity)}\\ &= e && \text{(since } b^{-1}b = e\text{).}\end{aligned}$$

Thus, $b^{-1}a^{-1}$ is the inverse of ab, so $(ab)^{-1} = b^{-1}a^{-1}$ □

Exercise I.2.2. Prove that for all x in G, $\left(x^{-1}\right)^{-1} = x$.

We now prove an important property of groups: the **cancellation law**.

Proposition I.2.2.6 (Cancellation Law)**.** *Let g, x, and y be elements in the group G. Then*

1. *if $gx = gy$ then $x = y$; and*
2. *if $xg = yg$ then $x = y$.*

Proof. We prove the two cases separately.

1. Suppose $gx = gy$. Then

$$\begin{aligned}g^{-1}(gx) &= g^{-1}(gy) && \text{(left multiply by } g^{-1}\text{)}\\ (g^{-1}g)x &= (g^{-1}g)y && \text{(by associativity)}\\ ex &= ey && \text{(since } g^{-1}g = e\text{)}\\ x &= y && \text{(since } e \text{ is the identity)}\end{aligned}$$

2. Suppose $xg = yg$. Then

$$\begin{aligned}(xg)g^{-1} &= (yg)g^{-1} && \text{(right multiply by } g^{-1}\text{)}\\ x(gg^{-1}) &= y(gg^{-1}) && \text{(by associativity)}\\ xe &= ye && \text{(since } gg^{-1} = e\text{)}\\ x &= y && \text{(since } e \text{ is the identity)}\end{aligned}$$

This completes the proof. □

2.3 Order of a Group and Order of an Element

We look at the notion of *order* with respect to groups and elements of a group.

Definition I.2.3.1. *Let G be a group. The order of a group, denoted by $|G|$, is the number of elements in the set G.*

If $|G| = n$ where n is finite, we say that G is a **finite group**. On the other hand, if $|G| = \infty$, then we say that G is an **infinite group**.

Example I.2.3.2. The group $(\mathbb{Z}_4, \oplus_4)$ has order 4 since it has 4 elements: 0, 1, 2, and 3.

Example I.2.3.3. The group $(\mathbb{R}, +)$ is an infinite group since $\mathbb{R}$ has an uncountably infinite number of elements.

Let's now look at the order of an element:

Definition I.2.3.4. *Let g be an element of the group G. Then the order of g, denoted by $|g|$, is the least positive integer n such that $g^n = e$.*

Note that if n is infinite, we say that the order of g is infinite.

Example I.2.3.5. Consider the group $(\mathbb{Z}_4, \oplus_4)$ and its 4 elements 0, 1, 2, and 3.

- The element 0 has order 1 since $0 = 0$ which is the identity. Thus $|0| = 1$ in $(\mathbb{Z}_4, \oplus_4)$.
- The element 1 has order 4 since $1 \oplus_4 1 \oplus_4 1 \oplus_4 1 = 0$ and no smaller n than 4 exists. Thus $|1| = 4$ in $(\mathbb{Z}_4, \oplus_4)$.
- The element 2 has order 2 since $2 \oplus_4 2 = 0$ and no smaller n than 2 exists. Thus $|2| = 2$ in $(\mathbb{Z}_4, \oplus_4)$.
- The element 3 has order 4 since $3 \oplus_4 3 \oplus_4 3 \oplus_4 3 = 0$ and no smaller n than 4 exists. Thus $|3| = 4$ in $(\mathbb{Z}_4, \oplus_4)$.

We note a few things about the order of elements in a group.

- The identity element always has order 1.
- A group in which every element has finite order is said to be **periodic**.
- A finite group is always periodic because all elements in a finite group has finite order.
- The order of any element in a group divides the order of the group.

The last point is actually a corollary of Lagrange's Theorem (**Theorem I.3.4.4**). We will look into the proof it in the next chapter.

Exercise I.2.3. Let i be a number such that $i^2 = -1$. Let $\mathcal{S} = \{1, -1, i, -i\}$.

(i) Find the identity of the group $(\mathcal{S}, \times)$ where $\times$ denotes regular multiplication.

(ii) Find the orders of the elements of the above group.

2.4 Cyclic Groups

Now that we have gotten some basic terminology and properties of groups out of the way, let's introduce a very simple type of group: the cyclic groups.

Suppose we have an element g belonging to a group G. Suppose that the entire set G is *generated* by g, that is, the set

$$G = \{g, g^2, g^3, g^4, \ldots, g^n\}$$

for some positive integer n. Then, we say that G is a **cyclic group of order** n and has a **generator** of g. Notationally, we write $G = \langle g \rangle$.

Example I.2.4.1. Let i be the imaginary unit, i.e. $i^2 = -1$. Let $\mathcal{S} = \{1, -1, i, -i\}$. Notice the group $(\mathcal{S}, \times)$ is completely generated by

the element i since

$$i^1 = i, i^2 = -1, i^3 = -i, \text{ and } i^4 = 1.$$

Thus, $\mathcal{S} = \{i, i^2, i^3, i^4\} = \langle i \rangle$.

Exercise I.2.4. Using the set $\mathcal{S}$ from the above example, find the other generator of the group $(\mathcal{S}, \times)$.

It should be noted that not every element in a cyclic group is a generator, and that a cyclic group may have more than 1 generator.

Cyclic groups may also be of **infinite order**. Such cyclic groups are called **cyclic groups of infinite order** or **infinite cyclic groups**.

Example I.2.4.2. The group $(\mathbb{Z}, +)$ is an infinite cyclic group with generators 1 and -1.

We now look at two results involving cyclic groups.

Proposition I.2.4.3. *Every cyclic group is abelian.*

Proof. Let G be the cyclic group with a generator g. Suppose x and y are elements in g. Thus, $x = g^m$ and $y = g^n$ for some integers m and n.

Thus, we have the following:

$$\begin{aligned} xy &= (g^m)(g^n) \\ &= g^m g^n \\ &= g^{m+n} \\ &= g^{n+m} && \text{(since + is commutative)} \\ &= g^n g^m \\ &= (g^n)(g^m) \\ &= yx \end{aligned}$$

so $xy = yx$. Therefore G is abelian. □

Theorem I.2.4.4. *A finite group G is cyclic if and only if there exists an element g in the group G with the same order as the group.*

Proof. We first prove the forward direction: suppose G is cyclic and $|G| = n$. Then there exists an element g in G such that

$$G = \langle g \rangle = \{g^k \mid 1 \leq k \leq n, k \in \mathbb{Z}\},$$

by definition (i.e. g is a generator of G). We just need to show $|g| = n$.

Suppose on the contrary there exists an integer $1 \leq m < n$ where $g^m = e$. Then $\langle g \rangle = \{g, g^2, \ldots, g^m\}$. Thus $|\langle g \rangle| = m < n = |G|$. But by the hypothesis of the forward direction, $G = \langle g \rangle$ so $n = |G| = |\langle g \rangle| = m$. This is a contradiction, i.e. there does **not** exist an integer $1 \leq m < n$ where $g^m = e$. Therefore $g^n = e$, i.e. $|g| = n$.

We now prove the reverse direction: suppose there exists an element g in G with order n. We claim that $g, g^2, \ldots, g^n$ are all distinct.

Suppose on the contrary that there exist integers i and j where $1 \leq i < j \leq n$ such that $g^i = g^j$. Then:

$$g^i = g^i g^{j-i} \implies g^{j-i} = e$$

by the cancellation law. Note that $1 \leq j - i < n$. Thus, since $g^{j-i} = e$, therefore $|g| = j - i < n$ which contradicts $|g| = n$.

Hence, $g, g^2, \ldots, g^n$ are all distinct. Therefore, $\langle g \rangle = \{g, g^2, \ldots, g^n\}$ contain distinct elements of G. But there are only n elements in G and $\langle g \rangle$ contains n distinct elements. Therefore, $G = \langle g \rangle$ which means that G is cyclic with generator g.

This completes the proof. □

There are more interesting properties of cyclic groups, but we will get to them when we develop more tools to explain and prove these properties.

2.5 Dihedral Groups

We motivate the definition of the dihedral groups by discussing the symmetries of an equilateral triangle.

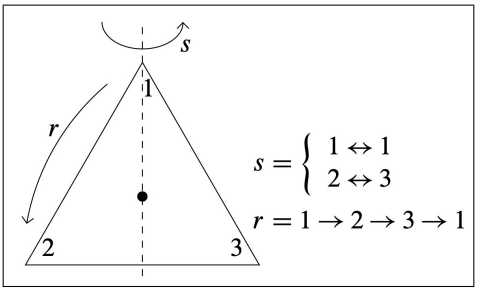


Figure 2.1: Symmetries of an Equilateral Triangle

Look at that equilateral triangle. What actions could we perform in order to maintain symmetry? Well, we could rotate the triangle in 120° anti-clockwise increments about the center of the triangle. We denote this action by the symbol r. Another thing we could do is reflect the triangle about the line going through one of the vertices and the center, like we discussed in Chapter 1. This action is denoted by s.

Now, suppose we define r to be the 120° anti-clockwise rotation about the center and s be the reflection of the triangle about the line going through vertex 1 and the center, like shown in the diagram. How do we obtain a 240° anti-clockwise rotation? Well, we apply two 120° anticlockwise rotations one after another. In other words, if $*$ means "action composition", then a 240° rotation would be represented by r^2. Note that r^3, which represents a 360° anti-clockwise rotation, is the same as doing nothing. Thus, $r^3 = e$. Similarly, applying the reflection s twice in a row (i.e., s^2) is the same as doing nothing. Thus, we have

$$r^3 = s^2 = e$$

for the case of an equilateral triangle.

There's another relationship governing r and s. Consider this: how do

we obtain a reflection about the line through vertex 3 and the center? Well, we apply r first, followed by s. This means that a reflection about the line through vertex 3 and the center is given by rs. Notice that this is the same thing as reflecting first and then applying r twice, i.e. sr^2. Thus, we have the second relationship:

$$rs = sr^2$$

for the case of an equilateral triangle.

The group of symmetries of an equilateral triangle is called the **dihedral group of order 6** and is denoted by D_3. In general, the **dihedral group of order** $2n$ is denoted by D_n and can be thought of as the symmetries of a regular polygon of n sides (a regular n-gon). For example, the symmetries of the square is given by the group D_4.

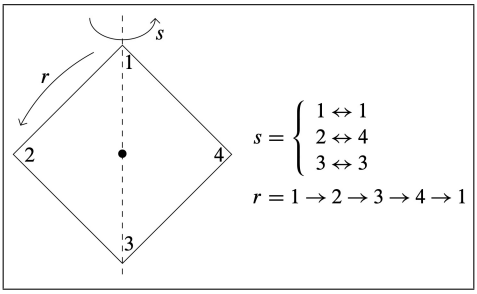


Figure 2.2: Symmetries of a Square

Thus, in general, the *set* D_n consists of the following elements.

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

with the relationship between r and s given by $r^n = s^2 = e$ and $rs = sr^{n-1}$.

Remark. Some authors (e.g. [Hum96]) will write the reflections of D_n with s leading the r, i.e. $s, sr, sr^2, sr^3, \ldots, sr^{n-1}$. However the underlying definition remains the same.

These relationships are succinctly given by the *presentation*

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

where r and s can be thought of as 'generators' and the conditions are given on the right side of the pipe (|).

Example I.2.5.1. We look at the group D_3 which has presentation

$$D_3 = \langle r, s \mid r^3 = s^2 = e, rs = sr^2 \rangle.$$

The Cayley table of the group is given below.

$*$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

It should be noted that we use the convention of reading the **row before the column**. So the action $rs * r^2$ (which is usually written as rsr^2) is given by the row of rs and the column of r^2, which is r^2s.

The *cannonical form* of an element in a dihedral group is of the form $r^m s^n$ where m and n are non-negative integers. So how do we find the canonical form of elements like sr or srs? We have this useful proposition to help:

Proposition I.2.5.2. *For the group D_n, we have $r^m s = sr^{n-m}$ for all integers $1 \leq m < n$.*

Proof. We prove this claim using induction on m.

When $m = 1$, $rs = sr^{n-1}$ is given by the definition of the group D_n.

Assume now that for some integer $1 \leq k < n$, we have $r^k s = sr^{n-k}$. We consider two cases.

- If $k = n - 1$, then $k + 1 = n$. Thus, $r^{k+1}s = r^n s = s$ since $r^n = e$. Note that $sr^{(k+1)-n} = sr^{n-n} = sr^0 = s$. Therefore $r^{k+1}s = sr^{(k+1)-n}$ for the case when $k = n - 1$.
- The other case is if $1 \leq k \leq n - 2$. Then we have:

$$\begin{aligned}
r^{k+1}s &= r^k(rs) \\
&= r^k(sr^{n-1}) && \text{(base case)} \\
&= (r^k s)r^{n-1} && \text{(associativity)} \\
&= (sr^{n-k})r^{n-1} && \text{(by Induction Hypothesis)} \\
&= sr^{2n-k-1} \\
&= sr^n r^{n-k-1} \\
&= sr^{n-(k+1)} && \text{(since } r^n = e\text{)}
\end{aligned}$$

Therefore this applies to the subsequent case of $k + 1$.

Hence $r^m s = sr^{n-m}$ for all integers $1 \leq m < n$. □

Exercise I.2.5. Simplify rsr^4sr^3 in the group D_6.

2.6 Problems

Problem I.2.1. Draw the Cayley table for D_4, the dihedral group of order 8, representing the symmetries of a square. By referring to the Cayley table,

(a) explain why D_4 is **not** abelian;

(b) simplify $r^3srsr^3sr^3sr^2$.

Problem I.2.2. Let G be a group. If every element in G is its own inverse, show that G is abelian.

Problem I.2.3. Let G be a group.

(a) Suppose $(gh)^2 = g^2h^2$ for all elements g and h in G. Prove that G is abelian.

(b) Suppose G is abelian. Prove that $(gh)^n = g^nh^n$ for all elements g and h in G and for all positive integers n.

Problem I.2.4. Prove that $(\mathbb{Z}_n, \oplus_n)$ is a cyclic group of order n. (It is given that $(\mathbb{Z}_n, \oplus_n)$ is a group.)

Problem I.2.5. The set $S = \mathbb{R}^2$, that is,

$$S = \{(x, y) \mid x, y \text{ are real numbers}\}.$$

The transformation $T : S \to S$ is defined by

$$T(x, y) = (-y, x + y).$$

Let the set $A = \{T^r \mid r \in \mathbb{Z} \text{ and } r \geq 1\}$. Show that A is a group under function composition $\circ$, and give the order of this group.

3 Subgroups

3.1 Definition and Examples

We look at the notion of a subgroup of a group.

Definition I.3.1.1. *Let G be a group with operation $*$. Let $H \subseteq G$. Then H is said to be a **subgroup** of G if:*

1. ***Closure**: For all x and y in H, $x * y$ is also in H.*
2. ***Identity**: The identity of the group G is in H.*
3. ***Inverse**: For all elements x in H, there exists an element x^{-1} in H such that $x * x^{-1} = x^{-1} * x = e$.*

Remark. Equivalently, H is a subgroup of G if $H \subseteq G$ and H is a group under the group operation of G.

We write $H \leq G$ if H is a subgroup of G.

Example I.3.1.2. Let's look at all possible subgroups of the group $(\mathbb{Z}, +)$. Suppose $H \leq G = (\mathbb{Z}, +)$. Suppose also that H is not the trivial subgroup containing only the identity in $(\mathbb{Z}, +)$, i.e. $H \neq \{0\}$.

Let n be the smallest *positive* integer in H. Let m be any *other* number in H. Then by the division algorithm, $m = nq + r$ where q and r are integers such that $0 \leq r < n$. Hence,

$$r = m + \underbrace{(-n) + (-n) + (-n) + \cdots + (-n)}_{q \text{ times}}$$

Note that m is in H, and $-n$ is also in H. Thus, $r = m + (-n) + \cdots + (-n)$ is also in H since H is closed under addition. But, $0 \leq r < n$ and n is the *smallest* positive integer in H. Thus, $r \not> 0$ which means

$r = 0$. Hence, $m = nq$, i.e. every element in H is a multiple of the smallest positive integer in H.

Hence,

$$H = \{nk \mid k \in \mathbb{Z}\},$$

which is often written as the group $n\mathbb{Z}$.

Exercise I.3.1. Let G be a group with operation $*$ and identity e. Prove that $\{e\} \leq G$.

We note that the group containing only the identity (i.e., $\{e\} \leq G$) is always present in every group. This is known as the **trivial subgroup**. We also note that the group itself is a subgroup of itself (that is, $G \leq G$). Any subgroup that are **not** these two groups is known as a **proper subgroup** of G, and we write $H < G$ if H is a proper subgroup of G.

3.2 Subgroup Test

To prove that a subset of a group is a subgroup using the axioms is too tedious. Wouldn't it be nice if we have a simple test to determine if a subset is a subgroup? Well, there is; it is called the **subgroup test**.

Proposition I.3.2.1 (Subgroup Test)**.** *Let G is a group and $H \subseteq G$ such that $H \neq \varnothing$ (i.e., H is not the empty set). Then $H \leq G$ if and only if for all x and y in H, then xy^{-1} is in H.*

Proof. We prove the forward direction first. Suppose $H \leq G$ and let x and y be elements in H. Since H is a subgroup of G, inverses exist. Thus y^{-1} is in H. Also, since H is a subgroup of G, thus H is closed under the group operation. Hence, xy^{-1} is in H. Therefore, if $H \leq G$ then for all x and y in H, xy^{-1} is in H.

We now prove the reverse direction. Suppose for all x and y in H, xy^{-1} is in H.

- Suppose h is an arbitrary element in H. Set $x = h$ and $y = h$. Then $xy^{-1} = hh^{-1} = e$ is in H. Thus the identity of G is present in H.
- Set $x = e$ and let $y = h$. Then $xy^{-1} = eh^{-1} = h^{-1}$ is in H. Hence every element in H has an inverse in H.
- Let a and b be elements in H. Then by above point, b^{-1} is in H. Set $x = a$ and $y = b^{-1}$. Then $xy^{-1} = a\left(b^{-1}\right)^{-1} = ab$ is in H. Hence H is closed under the group operation.

Therefore, if for all x and y in H, xy^{-1} is in H, then $H \leq G$.

This completes the proof of the subgroup test. □

Remark. We usually show the 'non-empty' and 'subset' requirement by checking if the identity of G is in H.

We look at some examples of the use of the subgroup test.

Example I.3.2.2. Let G be a group and $S \subseteq G$ where $S \neq \varnothing$. The **centralizer** of S in G is the set

$$\mathrm{C}_G(S) = \{g \in G \mid \text{for all } s \in S \text{ we have } gs = sg\}.$$

We claim that $\mathrm{C}_G(S)$ is a subgroup of G.

Proof. We show that for all elements x and y in $\mathrm{C}_G(S)$, xy^{-1} is also in the centralizer. Note that the condition $gs = sg$ is equivalent to the condition $sg^{-1} = g^{-1}s$.

Suppose x and y are in $\mathrm{C}_G(S)$. Let s be in S. Then

$$\begin{aligned}
(xy^{-1})s &= x(y^{-1}s) && \text{(associativity)} \\
&= x(sy^{-1}) && \text{(since } sg^{-1} = g^{-1}s\text{)} \\
&= (xs)y^{-1} && \text{(associativity)} \\
&= (sx)y^{-1} && \text{(since } gs = sg\text{)} \\
&= s(xy^{-1}) && \text{(associativity)}
\end{aligned}$$

so $(xy^{-1})s = s(xy^{-1})$ for all s in S. Thus, xy^{-1} is in $\mathrm{C}_G(S)$, so by subgroup test $\mathrm{C}_G(S) \leq G$. □

Remark. In the case where S has a single element, say $S = \{x\}$, we write $\mathrm{C}_G(x)$.

Example I.3.2.3. Let G be a group. The **center** of a group G is given by the set

$$\mathrm{Z}(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}.$$

We claim that $\mathrm{Z}(G)$ is a subgroup of G under the group operation of G.

Proof. Note that $e \in \mathrm{Z}(G)$ since $ge = eg$ for all $g \in G$.

Let x and y be in $\mathrm{Z}(G)$, meaning that $gx = xg$ and $gy = yg$ for all $g \in G$. Note that $gy = yg$ implies $g = ygy^{-1}$ (by right multiplying by y^{-1}) which further means that $y^{-1}g = gy^{-1}$ (by left multiplying by y^{-1}). Therefore, $y^{-1} \in \mathrm{Z}(G)$. Now,

$$\begin{aligned}
(xy^{-1})g &= x(y^{-1}g) \\
&= x(gy^{-1}) && (\text{since } y^{-1} \in \mathrm{Z}(G)) \\
&= (xg)y^{-1} && (\text{associativity}) \\
&= (gx)y^{-1} && (\text{since } x \in \mathrm{Z}(G)) \\
&= g(xy^{-1}) && (\text{associativity})
\end{aligned}$$

which means that $xy^{-1} \in \mathrm{Z}(G)$. Hence $\mathrm{Z}(G) \leq G$ by the subgroup test. □

Exercise I.3.2. Let G be a group, $H \leq G$, and $g \in G$. Define the set

$$S = \{ghg^{-1} \mid h \text{ is in } H\}.$$

Prove that $S \leq G$ under the group operation of G.

3.3 Cosets

We now introduce the idea of **cosets** of a group G.

Definition I.3.3.1. *Let G be a group, $H \leq G$, and g be an element of G. Then define*

- *the **left coset** of H in G by g, $gH = \{gh \mid h \in H\}$*
- *the **right coset** of H in G by g, $Hg = \{hg \mid h \in H\}$*

Remark. The subgroup H is both a left and right coset of H in G. This is because the element g in question is $g = e$, so $gH = eH = H$ and $Hg = He = e$.

Example I.3.3.2. Let $G = D_3$, and $H = \{e, s\} \leq G$. The distinct left cosets of H in G are:

- $eH = \{e, s\} = H$
- $rH = \{r, rs\}$
- $r^2H = \{r^2, r^2s\}$

Since all the elements of G have now appeared in one of these cosets, generating any more can not give new cosets, since a new coset would have to have an element in common with one of these and therefore be identical to one of these cosets. For example, $rsH = \{rs, rss\} = \{rs, r\} = rH$.

The distinct right cosets of H in G are:

- $He = \{e, s\} = H$
- $Hr = \{r, sr\} = \{r, r^2s\}$
- $Hr^2 = \{r^2, sr^2\} = \{r^2, rs\}$

Thus, for D_3, no left coset is a right coset, except for $H = eH = He$.

Exercise I.3.3. Let G be the group $(\mathbb{Z}_8, \oplus_8)$. Let $H \leq G$ such that $H = \{0, 4\}$.

(a) Explain why any left coset of H in G by an element g is the same as the right coset of H in G by g.

(b) Find all *distinct* left cosets of H in G.

We now state and prove a result that relates the equality of cosets.

Lemma I.3.3.3. *(Coset Equality) Let G be a group, $H \leq G$, and g_1 and g_2 be elements in G. Then the following statements are equivalent.*

(1) $g_1H = g_2H$

(2) $Hg_1^{-1} = Hg_2^{-1}$

(3) $g_1H \subseteq g_2H$

(4) $g_2 \in g_1H$

(5) $g_1^{-1}g_2 \in H$

Proof. We prove the statements in order.

- $\boxed{(1) \implies (2)}$ Suppose $g_1H = g_2H$. We will show $Hg_1^{-1} = Hg_2^{-1}$.

  Let $x \in Hg_1^{-1}$ Then $x = hg_1^{-1}$ for some h in H. Thus $x^{-1} = \left(hg_1^{-1}\right)^{-1} = g_1h^{-1}$ by Shoes and Socks. Since h^{-1} is in H thus $x^{-1} = g_1h^{-1}$ is in g_1H.

  Since $g_1H = g_2H$ thus $x^{-1} \in g_2H$. Write $x^{-1} = g_2\hat{h}$ for some $\hat{h}$ in H. Thus $x = (g_2\hat{h})^{-1} = \hat{h}^{-1}g_2^{-1}$ by Shoes and Socks. Since $\hat{h}^{-1}$ is in H thus $x = \hat{h}^{-1}g_2^{-1}$ is in Hg_2^{-1}.

  Hence, any element $x \in Hg_1^{-1}$ is also in Hg_2^{-1}, i.e. $Hg_1^{-1} \subseteq Hg_2^{-1}$. A similar argument shows that $Hg_2^{-1} \subseteq Hg_1^{-1}$. Thus $Hg_1^{-1} = Hg_2^{-1}$ as required.

- $\boxed{(2) \implies (3)}$ Suppose $Hg_1^{-1} = Hg_2^{-1}$ and take $x \in g_1H$. Thus $x = g_1h$ for some h in H. Therefore $x^{-1} = (g_1h)^{-1} = h^{-1}g_1^{-1} \in Hg_1^{-1}$ since h^{-1} is in H. By assumption $Hg_1^{-1} = Hg_2^{-1}$ so $x^{-1} \in Hg_2^{-1}$. Let $x^{-1} = \hat{h}g_2^{-1}$ for some $\hat{h}$ in H. Then $x = \left(\hat{h}g_2^{-1}\right)^{-1} = g_2\hat{h}^{-1} \in g_2H$ since $\hat{h}^{-1}$ is in H. Hence x is in g_2H. Therefore, for any $x \in g_1H$, x will also be in g_2H. Thus $g_1H \subseteq g_2H$.
- $\boxed{(3) \implies (4)}$ Suppose $g_1H \subseteq g_2H$. Then for all x in g_1H, x is also in g_2H. Note that $g_1 = g_1e$. Since e is in H (as $H \leq G$) thus $g_1e \in g_1H \subseteq g_2H$ by assumption. Thus $g_1 \in g_2H$ as needed.
- $\boxed{(4) \implies (5)}$ Suppose $g_1 \in g_2H$. Then $g_1 = g_2h$ for some h in H. Then:

$$\begin{aligned} g_1^{-1}g_1 &= g_1^{-1}g_2h && \text{(left multiply by } g_1^{-1}\text{)} \\ e &= g_1^{-1}g_2h \\ h^{-1} &= g_1^{-1}g_2hh^{-1} && \text{(right multiply by } h^{-1}\text{)} \\ h^{-1} &= g_1^{-1}g_2 \end{aligned}$$

  Since h^{-1} is an element in H thus $g_1^{-1}g_2 = h^{-1}$ is also in H, meaning $g_1^{-1}g_2 \in H$.
- $\boxed{(5) \implies (1)}$ Suppose $g_1^{-1}g_2$ is an element of H. Thus, $g_1^{-1}g_2 = \hat{h}$ for some $\hat{h}$ in H. Let x be an element from g_1H, so $x = g_1h$ for some h in H. Then

$$\begin{aligned} x^{-1} &= (g_1h)^{-1} \\ &= h^{-1}g_1^{-1} && \text{(Shoes and Socks)} \\ &= h_1^{-1}g_1^{-1}(g_2g_2^{-1}) && \text{(since } g_2g_2^{-1} = e\text{)} \\ &= h_1{-}1(g_1^{-1}g_2)g_2^{-1} \\ &= h^{-1}\hat{h}g_2^{-1} \end{aligned}$$

  which means $x = \left(h^{-1}\hat{h}g_2^{-1}\right)^{-1} = g_2\hat{h}^{-1}h$ which is an element of g_2H since $\hat{h}^{-1}h$ is in H.

Thus, for all x in g_1H, x is also in g_2H which means $g_1H \subseteq g_2H$. A similar argument can be used to show that $g_2H \subseteq g_1H$. Hence $g_1H = g_2H$.

Thus, (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (5) $\implies$ (1), completing the proof of this lemma. □

Exercise I.3.4. Let G be a group, $H \leq G$, and g_1 and g_2 be elements in G. Prove that if $g_1H \cap g_2H \neq \varnothing$ then $g_1H = g_2H$.

3.4 Lagrange's Theorem

Lagrange's theorem is an important result relating the order of a subgroup and the order of the group itself. Before that, though, we introduce the idea of the **index** of a subgroup.

Definition I.3.4.1. *Let G be a group and $H \leq G$. The **index** of H in G, denoted by $[G : H]$, is the number of left cosets of H in G.*

Note that since the number of left cosets is the number of right cosets, $[G : H]$ can be defined as the number of cosets of H in G.

We also require two lemmas.

Lemma I.3.4.2. *Let G be a group and $H \leq G$. Then distinct left cosets of H in G partition G.*

Proof. To prove that the distinct left cosets of H in G partition G, we need to show two things.

- The intersection of any 2 left cosets is either the empty set or is one of the left cosets (i.e., distinct left cosets are disjoint).
- The union of all left cosets is the group.

The first bullet point is proven by **Exercise I.3.4**, so we omit its proof here. We work only on the second bullet point.

Suppose g is in G. We will find a left coset that g is in. Clearly $g = ge$, and since e is an element of H, thus $g = ge$ is an element of the left coset gH. So any element in g belongs to a left coset of H in G. Thus the union of all left cosets is the group.

Hence, distinct left cosets of H in G partition G. □

Lemma I.3.4.3. *Let G be a group and $H \leq G$. Then $|H| = |gH|$ for all g in G.*

Proof. Define the map $\phi : H \to gH$ such that $\phi(h) = gh$. To prove that $|H| = |gH|$ we need to show that ϕ is a bijection, i.e. ϕ is both injective (one-to-one) and surjective (onto).

- **Injective**: Let h and $\hat{h}$ be elements in H such that $\phi(h) = \phi(\hat{h})$. Then $gh = g\hat{h}$ by definition of ϕ. By cancellation law, $h = \hat{h}$ which means ϕ is injective.
- **Surjective**: Let x be in gH. Thus $x = gh$ for some h in H. Clearly $\phi(h) = gh = x$ so a pre-image of x exists in H. Thus ϕ is surjective.

Since ϕ is both injective and surjective, it is thus bijective. Hence $|H| = |gH|$. □

We are now ready to state and prove Lagrange's theorem.

Theorem I.3.4.4 (Lagrange)**.** *Let G be a group and $H \leq G$. Then $|G| = [G : H]|H|$.*

Proof. Suppose $|G| = n$. Let the set $\mathcal{S} = \{g_1H, g_2H, g_3H, \ldots, g_kH\}$ contain all distinct left cosets of H in G. Thus $k = [G : H]$.

By **Lemma I.3.4.2**,

$$G = \bigcup_{i=1}^{k} g_iH = g_1H \cup g_2H \cup \cdots \cup g_kH$$

with $g_iH \cap g_jH = \varnothing$ if $i \neq j$. Thus,

$$\begin{aligned} |G| &= \sum_{i=1}^{k} |g_iH| \\ &= \sum_{i=1}^{k} |H| \qquad \text{(by } \textbf{Lemma I.3.4.3)} \\ &= k|H| \end{aligned}$$

and since $k = [G : H]$, therefore $|G| = [G : H]|H|$, proving Lagrange's theorem. □

Exercise I.3.5. Let G be the group $(\mathbb{Z}_{99}, \oplus_{99})$. It is given that $H = \{0, 33, 66\}$ is a subgroup of G. What is the index of H in G?

Let's look at some corollaries of Lagrange's theorem.

Corollary I.3.4.4.1. *Let G be a finite group and let g be an element in G. Then $|G|$ is a multiple of $|g|$.*

Proof. We want to show that $|G| = m|g|$ for some positive integer m.

Clearly $|e| = 1$ so $|G| = |G| \times 1 = |G||e|$. Thus for the identity, $m = |G|$.

Now suppose $g \neq e$ and $|g| = n < \infty$. Let $\mathcal{S} = \langle g \rangle = \{g, g^2, g^3, \ldots, g^n\}$. Note that $\mathcal{S}$ is a (cyclic) subgroup of G and $|\mathcal{S}| = n$. By Lagrange's theorem (**Theorem I.3.4.4**), $|G| = [G : \mathcal{S}]|\mathcal{S}| = [G : \mathcal{S}]|g|$. Hence, in this case, $m = [G : \mathcal{S}]$, proving the claim. □

Corollary I.3.4.4.2. *A finite group G with prime order p has no proper subgroups.*

Proof. By Lagrange's theorem, the order of a subgroup must be a factor of the order of the group. Since the order of the group is prime, it only has 2 factors, namely 1 and p. The subgroup of order 1 is $\{e\}$ and the subgroup of order $p = |G|$ is clearly G itself. Hence G has no proper subgroups. □

Exercise I.3.6. Let G be a finite group with prime order p. Let x be a non-identity element in G. Prove that $|x| = p$.

Corollary I.3.4.4.3. *A finite group G with prime order p is cyclic.*

Proof. By **Exercise I.3.6**, any element g in G where $g \neq e$ has $|g| = p$. Thus $\langle g \rangle \neq \{e\}$.

Note that $\langle g \rangle = \{g, g^2, g^3, \ldots, g^p\} \leq G$. However, by **Corollary I.3.4.4.2**, the only subgroups of G are $\{e\}$ and G. Since $\langle g \rangle \neq \{e\}$ thus $\langle g \rangle = G$, meaning G is cyclic with generator g. □

3.5 Normal Subgroups

We now look at a special type of subgroup, known as **normal subgroups**.

Definition I.3.5.1. *Let G be a group and $N \leq G$. We say that N is a **normal subgroup** of G if $gN = Ng$ for all g in G.*

If N is a normal subgroup of G, we write $N \trianglelefteq G$. Furthermore if N is a *proper* normal subgroup of G, we write $N \triangleleft G$.

Note that $gN = Ng$ is equivalent to the following two statements:

- $gNg^{-1} = N$ for all g in G. (One may interpret gNg^{-1} as either the left coset $g(Ng^{-1})$ or the right coset $(gN)g^{-1}$.)
- gng^{-1} is in N for all g in G and n in N.

Proposition I.3.5.2. *Every subgroup of an abelian group is normal.*

Proof. Let G be an abelian group and $H \leq G$. Let g be in G and h be in H. Then

$$\begin{aligned} ghg^{-1} &= gg^{-1}h && \text{(since } G \text{ is commutative)} \\ &= eh \\ &= h \end{aligned}$$

which is an element of H. Thus ghg^{-1} is an element of H for all g in G and h in H, meaning $H \lhd G$. □

Example I.3.5.3. Let's consider normal subgroups of the dihedral group of order 6, D_3.

Recall $D_3 = \{e, r, r^2, s, rs, r^2s\}$. Note that $|r| = 3$, $|s| = 2$, $\langle r \rangle = \{e, r, r^2\}$, and $\langle s \rangle = \{e, s\}$. We will show that $\langle r \rangle$ is a normal subgroup of D_3 but not $\langle s \rangle$. Note that since r and s are generators, we simply need to check $s\langle r \rangle$, $\langle r \rangle s$, $r\langle s \rangle$, and $\langle s \rangle r$ to check for normality.

For $\langle r \rangle$,

- $s\langle r \rangle = \{s, sr, sr^2\} = \{s, r^2s, rs\}$
- $\langle r \rangle s = \{s, rs, r^2s\}$

so $s\langle r \rangle = \langle r \rangle s$ which means $\langle r \rangle \lhd D_3$.

For $\langle s \rangle$,

- $r\langle s \rangle = \{r, rs\}$
- $\langle s \rangle r = \{r, sr\} = \{r, r^2s\}$

and since $rs \neq r^2s$ thus $r\langle s \rangle \neq \langle s \rangle r$. Hence, $\langle s \rangle$ is not a normal subgroup of D_3.

3.6 Quotient Groups

We end this chapter by looking at a special (and useful) group: the quotient group. But before we can do that, we look at the idea of the set of left cosets.

Definition I.3.6.1. *Let G be a group and $H \leq G$. The* ***set of left cosets*** *is denoted by*

$$G/H = \{gH \mid g \in G\}.$$

Remark. We may sometimes write G/H using fractions, such as $\frac{G}{H}$, if it serves to improve readability.

Note that the number of left cosets is $[G : H] = \frac{|G|}{|H|}$ by **Theorem I.3.4.4**. Also note that if G/H is **not** a group, it is read "G by H".

Theorem I.3.6.2. *Let G be a group and $N \lhd G$. Then G/N forms a group called the* ***quotient group*** *with group operation $\star$ such that*

$$(xN) \star (yN) = (xy)N.$$

Note that, as per usual, we suppress the operation $\star$ and just write $(xN)(yN) = (xy)N$. Also note that for the quotient group, G/N is read "G mod N".

Proof. Before we can prove that it forms a group, we need to show that $\star$ is well defined. This is because we worry that if $x_1N = x_2N$ and $y_1N = y_2N$ there may be a situation that $(x_1y_1)N \neq (x_2y_2)N$ under this operation. Thus we need to check if such an operation is well defined.

Suppose $x_1N = x_2N$ and $y_1N = y_2N$ where $x_1, x_2, y_1, y_2 \in G$. Then

$$\begin{aligned}
(x_1N)(y_1N) &= (x_1y_1)N && \text{(by definition)} \\
&= x_1(y_1N) && \text{(left coset of } y_1N \text{ in } G \text{ by } x_1) \\
&= x_1(y_2N) && \text{(since } y_1N = y_2N) \\
&= x_1(Ny_2) && \text{(since } N \text{ is normal, so } y_2N = Ny_2) \\
&= (x_1N)y_2 && \text{(right coset of } x_1N \text{ in } G \text{ by } y_2) \\
&= (x_2N)y_2 && \text{(since } x_1N = x_2N) \\
&= x_2(Ny_2) && \text{(left coset of } Ny_2 \text{ in } G \text{ by } x_2) \\
&= x_2(y_2N) && \text{(since } N \text{ is normal, so } y_2N = Ny_2) \\
&= (x_2y_2)N && \text{(left coset of } N \text{ in } G \text{ by } x_2y_2) \\
&= (x_2N)(y_2N) && \text{(by definition)}
\end{aligned}$$

so if $x_1N = x_2N$ and $y_1N = y_2N$ then $(x_1N)(y_1N) = (x_2N)(y_2N)$, meaning that $\star$ is well defined.

We can now prove the four group axioms.

1. **Closure**: Assume xN and yN are in G/N. Then $(xN)(yN) = (xy)N$. Since xy is in G thus $(xy)N$ is in G/N, meaning that G/N is closed under $\star$.

2. **Associativity**: Take xN, yN, and zN from G/N. Then

$$\begin{aligned}
(xN)\left((yN)(zN)\right) &= (xN)\left((yz)N\right) \\
&= (xyz)N \\
&= \left((xy)z\right)N \\
&= \left((xy)N\right)(zN) \\
&= \left((xN)(yN)\right)(zN)
\end{aligned}$$

   so $\star$ is associative.

3. **Identity**: Observe that e is in G so $eN = N$ is in G/N. Note that

$$(eN)(xN) = (ex)N = xN \text{ and } (xN)(eN) = (xe)N = xN$$

   for x in G, so $eN = N$ is the identity in G/N.

4. **Inverse**: Observe that for x in G, x^{-1} is also in G. Note that

$$(xN)(x^{-1}N) = (xx^{-1})N = eN = N$$

and

$$(x^{-1}N)(xN) = (x^{-1}x)N = eN = N$$

so $(xN)^{-1}$ is $x^{-1}N$.

Since the four group axioms are satisfied, thus G/N is a group under the operation $\star$. □

Example I.3.6.3. Let's look at possible quotients of the group D_3, which has the underlying set of $\{e, r, r^2, s, rs, r^2s\}$. Recall from a previous example that $\langle r\rangle \lhd D_3$. Thus $D_3/\langle r\rangle$ is a quotient group, with $|D_3/\langle r\rangle| = \frac{|D_3|}{|\langle r\rangle|} = \frac{6}{3} = 2$.

Let's now look at the elements of $D_3/\langle r\rangle$.

$$\begin{aligned}
D_3/\langle r\rangle &= \{x\langle r\rangle \mid x \in D_3\} \\
&= \big\{\{x, xr, xr^2\} \mid x \in D_3\big\} \\
&= \{\{e, r, r^2\}, \{r, r^2, r^3\}, \{r^2, r^3, r^4\}, \\
&\qquad \{s, sr, sr^2\}, \{rs, rsr, rsr^2\}, \{r^2s, r^2sr, r^2sr^2\}\} \\
&= \{\{e, r, r^2\}, \{r, r^2, e\}, \{r^2, e, r\}, \\
&\qquad \{s, sr, sr^2\}, \{sr^2, s, sr\}, \{sr, sr^2, s\}\} \\
&= \big\{\{e, r, r^2\}, \{s, sr, sr^2\}\big\} \\
&= \{\langle r\rangle, s\langle r\rangle\}
\end{aligned}$$

Note also that $(s\langle r\rangle)^2 = s^2\langle r\rangle = \langle r\rangle$, so in fact $D_3/\langle r\rangle$ has generator $\langle r\rangle$, i.e. $D_3/\langle r\rangle = \langle\langle r\rangle\rangle$.

Exercise I.3.7. Let G be a finite cyclic group. Let H be a subgroup of G.

(i) Explain why G/H is a quotient group.

(ii) Show that G/H is cyclic.

3.7 Problems

Problem I.3.1. Let $G = D_4$, the dihedral group of order 8. By considering the subgroup axioms, determine if the following form subgroups of G.

(a) $\{e\}$

(b) $\{e, r, s\}$

(c) $\{r, r^2, r^3\}$

(d) $\{r, r^3, r^4, r^6\}$

Problem I.3.2. Let G be a group and $H \leq G$. Let

$$K = \{x \in G \mid xhx^{-1} \in H \text{ for some } h \in H\}.$$

Prove the following statements.

(a) $K \leq G$

(b) $H \leq K$

Problem I.3.3. Let G be a group.

(a) Prove that $\mathrm{Z}(G)$ is a normal subgroup of G.

(b) Prove that $\mathrm{Z}(G) = G$ if and only if G is abelian.

(c) Find the center of the group D_4.

Problem I.3.4. Let G be a group, $H \leq G$ and $K \leq G$. Prove or disprove the following statements.

(a) $H \cap K \leq G$

(b) $H \cap K \leq H$

(c) $H \cup K \leq G$

(d) $H \cup K \leq H$

Problem I.3.5. Let G be a cyclic group with generator g. Prove that any subgroup of G must also be cyclic.

Problem I.3.6. Let G be a group of order 1024 and let H be a proper subgroup of G. Determine the maximum order of H. Give an example of the groups G and H such that H has this maximum order.

Problem I.3.7. Let G be a finite group with even order. Show that there exists an element with order 2 in G.

Problem I.3.8. Let G be a finite group and $H \leq G$. If the index of H in G is 2, prove that $H \lhd G$.

Problem I.3.9. Let G be a finite group, $H \leq G$, and $K \leq G$. Suppose the greatest common divisor (GCD) of the order of H and the order of K is 1. Show that the intersection of the groups H and K contains only the identity.

Problem I.3.10. Let G be a finite group, and let its order be m.

(a) Find the smallest value of m such that G is non-abelian.

(b) Prove that the value of m found in (a) is the smallest value that allows G to be non-abelian.

(c) Hence prove that there exists a non-abelian group of order n, where n is even and $n \geq m$.

Problem I.3.11. Let G be a group, and suppose $G/\mathrm{Z}(G)$ is cyclic. Prove that G is abelian.

4 Homomorphisms and Isomorphisms

4.1 Homomorphisms

Now that we have introduced the idea of a group, one wonders about how elements of one group can be mapped to elements of another group. Such a mapping can be defined between any two groups, but we look at a specific subset of the mapping between groups, called **homomorphisms**.

Definition I.4.1.1. *Suppose* $(G, *)$ *and* $(H, \star)$ *are groups. A map* $\phi : G \to H$ *is a* ***homomorphism*** *if*

$$\phi(x * y) = \phi(x) \star \phi(y)$$

for all x *and* y *in* G*.*

Remark. We usually suppress the binary operations of $*$ and $\star$ when working with homomorphisms. Thus, the above condition is usually written as

$$\phi(xy) = \phi(x)\phi(y).$$

It is important to note that xy uses the group operation on G (i.e., $*$) while $\phi(x)\phi(y)$ uses the group operation on H (i.e., $\star$).

Let's look at two examples of homomorphisms between groups.

Example I.4.1.2. Let G be any group. Take g from G. Let $\phi : \mathbb{Z} \to G$ (where $\mathbb{Z}$ is the additive group of integers) be such that $\phi(n) = g^n$ for all integers n. Then ϕ is a homomorphism, since

$$\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$$

which means that ϕ satisfies the homomorphism condition.

Example I.4.1.3. Let $S = \{z \in \mathbb{C} \mid |z| = 1\}$ (where $\mathbb{C}$ denotes the set of complex numbers) be a group under multiplication. Let $f : \mathbb{R} \to S$ (where $\mathbb{R}$ is the additive group of real numbers) be defined such that $f(x) = e^{\mathrm{i}x}$. Then f is a homomorphism as

$$f(x + y) = e^{\mathrm{i}(x+y)} = e^{\mathrm{i}x}e^{\mathrm{i}y} = f(x)f(y).$$

Exercise I.4.1. Let S be the set of positive integers. Let $G = (S, +)$ and $H = (S, \times)$. Let $\phi : G \to H$. Determine if the following are homomorphisms:

(a) $\phi(n) = n$

(b) $\phi(n) = 2^n$

4.2 Properties of Homomorphisms

With an understanding on what a homomorphism is, let's look at some properties that a homomorphism between two groups has.

Before stating (and proving) some properties of homomorphisms, let

- G_1 and G_2 be groups;
- $H_1 \leq G_1$ and $H_2 \leq G_2$;
- e_1 and e_2 be the identities of G_1 and G_2 respectively; and
- $\phi : G_1 \to G_2$ be a homomorphism.

Proposition I.4.2.1. $\phi(e_1) = e_2$

Proof. Let x in G_1. Then $e_1 x = x$. Thus $\phi(e_1 x) = \phi(x)$ by applying ϕ on both sides. Hence $\phi(e_1)\phi(x) = \phi(x)$ by applying the definition of a homomorphism. Therefore, by cancellation law, $\phi(e_1) = e_2$. □

Proposition I.4.2.2. *For all x in G_1, $\phi(x^{-1}) = (\phi(x))^{-1}$.*

Proof. Note that $xx^{-1} = e_1$. Thus, $\phi(xx^{-1}) = \phi(e_1) = e_2$ by applying ϕ on both sides. Note also that $\phi(xx^{-1}) = \phi(x)\phi(x^{-1})$ by definition of homomorphism. Hence, $\phi(x)\phi(x^{-1}) = e_2$ which quickly implies $\phi(x^{-1}) = (\phi(x))^{-1}$ after left-multiplying both sides by $(\phi(x))^{-1}$. □

For the next few properties, define

$$\phi(H_1) = \{\phi(h) \mid h \in H_1\},$$
$$\phi^{-1}(H_2) = \{g \in G_1 \mid \phi(g) \in H_2\}$$

Exercise I.4.2. Prove that $\phi(H_1) \leq G_2$.

Proposition I.4.2.3. $\phi^{-1}(H_2) \leq G_1$.

Proof. Clearly $e_1 \in \phi^{-1}(H_2)$ since $\phi(e_1) = e_2 \in H_2$. Now suppose that x and y are in $\phi^{-1}(H_2)$, meaning that $\phi(x)$ and $\phi(y)$ are in H_2. Since $H_2 \leq G_2$, therefore

$$\phi(x)\,(\phi(y))^{-1} \in H_2$$

as H_2 is closed. Note that $(\phi(y))^{-1} = \phi(y^{-1}$ by properties of homomorphism. Therefore,

$$\phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in H_2$$

which means that $xy^{-1} \in \phi^{-1}(H_2)$. By subgroup test, $\phi^{-1}(H_2) \leq G_1$. □

Proposition I.4.2.4. *Suppose $H_2 \lhd G_2$. Then $\phi^{-1}(H_2) \lhd G_1$.*

Proof. By previous proposition, since $H_2 \leq G_2$, therefore $\phi^{-1}(H_2) \leq G_1$. All that needs to be done is to prove normality.

Take $n \in \phi^{-1}(H_2)$ and $g \in G_1$. We will show that $gng^{-1} \in \phi^{-1}(H_2)$ which is sufficient to prove normality.

Consider $\phi(gng^{-1})$.

$$\begin{aligned}\phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g^{-1}) \\ &= \underbrace{\phi(g)}_{\text{In } G_2}\underbrace{\phi(n)}_{\text{In } H_2}\underbrace{(\phi(g))^{-1}}_{\text{In } G_2} \\ &= g'n'(g')^{-1}\end{aligned}$$

where $g' = \phi(g)$ and $n' = \phi(n)$. Since H_2 is normal, so for all g in G_2 and n in H_2 we know gng^{-1} is in H_2. Therefore $\phi(gng^{-1}) = g'n'(g')^{-1}$ is in H_2, meaning that gng^{-1} is in $\phi^{-1}(H_2)$.

This proves that $\phi^{-1}(H_2) \lhd G_1$. □

Exercise I.4.3. Prove or disprove: if $H_1 \lhd G_1$, then $\phi(H_1) \lhd G_2$.

4.3 Isomorphisms

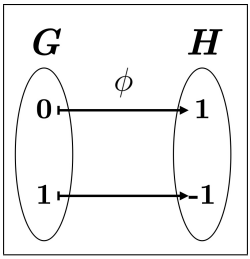
We now look a special (and important) category of homomorphisms: **isomorphisms**.

Definition I.4.3.1. *Let $(G, *)$ and $(H, \star)$ be groups. An **isomorphism** between G and H is a bijective homomorphism ϕ.*

If there exists an isomorphism from the group G to the group H, then we say that G and H are **isomorphic** and write $G \cong H$ (or $H \cong G$).

Example I.4.3.2. Let $G = (\mathbb{Z}_2, \oplus_2)$ and $H = \{1, -1\}$ be a group under regular multiplication. Define the map $\phi : G \to H$ such that $\phi(0) = 1$ and $\phi(1) = -1$. Then ϕ is an isomorphism.

- ϕ is clearly a bijection based on function mapping diagram shown.



- ϕ is a homomorphism:
  - $\phi(0 \oplus_2 0) = \phi(0) = 1 = 1 \times 1 = \phi(0)\phi(0)$
  - $\phi(0 \oplus_2 1) = \phi(1) = -1 = 1 \times (-1) = \phi(0)\phi(1)$
  - $\phi(1 \oplus_2 0) = \phi(1) = -1 = (-1) \times 1 = \phi(1)\phi(0)$
  - $\phi(1 \oplus_2 1) = \phi(0) = 1 = (-1) \times (-1) = \phi(1)\phi(1)$

Thus, $G \cong H$.

Example I.4.3.3. We show that $(\mathbb{R}, +) \cong ((0, \infty), \times)$ by considering the map $\phi : \mathbb{R} \to (0, \infty), x \mapsto e^x$.

- **Homomorphism**:

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

- **Injective**: Suppose x and y are elements in $\mathbb{R}$ such that $\phi(x) = \phi(y)$. Therefore $e^x = e^y$ which quickly implies $x = y$ by applying natural logarithm (ln) on both sides.
- **Surjective**: Suppose $y \in (0, \infty)$. Then $\ln y$ is a real number. So $\phi(\ln y) = e^{\ln y} = y$, meaning every element in the codomain $(0, \infty)$ has a preimage.

Thus, ϕ is an isomorphism, meaning that $(\mathbb{R}, +) \cong ((0, \infty), \times)$.

Exercise I.4.4. Let the groups $G = (\{1, 2, 3, 4\}, \otimes_5)$ and $H = (\{1, 3, 7, 9\}, \otimes_{10})$.

(i) Show that $G = \langle 3 \rangle$ and $H = \langle 7 \rangle$.

(ii) Prove that $G \cong H$ by considering the map $\phi : G \to H, 3^k \mapsto 7^k$.

4.4 Consequences of Isomorphisms

Isomorphisms between groups means that the two groups *share the same structure*, in a manner of speaking. We look at a theorem that showcases the sharing of some of these properties.

Theorem I.4.4.1. *Let $\phi : G \to H$ be an isomorphism between the groups G and H. Then*

1. *$|G| = |H|$;*
2. *$\phi^{-1} : H \to G$ is an isomorphism;*
3. *if G is abelian then so is H;*
4. *if G is cyclic then so is H; and*
5. *if G has a subgroup of order n, then so does H.*

Proof. We prove each of these statements individually.

1. Follows immediately from properties of a bijective function.
2. Since ϕ is an isomorphism, it is bijective, which means that ϕ^{-1} exists and is also bijective. All that remains is to show that ϕ^{-1} is a homomorphism.

   Let u and v be in H. Then there exist elements x and y in G such that

   $$\phi(x) = u \text{ and } \phi(y) = v$$

since ϕ is surjective. Hence,

$$\begin{aligned}\phi^{-1}(uv) &= \phi^{-1}\left(\phi(x)\phi(y)\right) \\ &= \phi^{-1}\left(\phi(xy)\right) \qquad \text{(since } \phi \text{ is a homomorphism)} \\ &= xy \\ &= \phi^{-1}(u)\phi^{-1}(v).\end{aligned}$$

Thus ϕ^{-1} is an isomorphism.

3. Suppose u and v are in H. Let x and y be elements in G such that

$$\phi(x) = u \text{ and } \phi(y) = v.$$

Thus,

$$\begin{aligned}uv = &= \phi(x)\phi(y) \\ &= \phi(\underbrace{xy}_{\text{In } G}) \\ &= \phi(yx) \qquad \text{(since } G \text{ is abelian)} \\ &= \phi(y)\phi(x) \\ &= vu\end{aligned}$$

which means that $uv = vu$. Hence H is abelian.

4. Suppose u is in H. Let x be in G such that $\phi(x) = u$. Since G is cyclic, suppose g is the generator of G, so $x = g^n$ for some integer n. This means that

$$\begin{aligned}u &= \phi(x) \\ &= \phi(g^n) \\ &= \underbrace{\phi(g)\phi(g)\phi(g)\cdots\phi(g)}_{n \text{ times}} \\ &= (\phi(g))^n \\ &\in \langle\phi(g)\rangle\,.\end{aligned}$$

Thus any element u in H is in $\langle\phi(g)\rangle$, meaning $H \subseteq \langle\phi(g)\rangle$.

However, $\left\langle \underbrace{\phi(g)}_{\text{In } H} \right\rangle \leq H$ which means that $\langle \phi(g) \rangle \subseteq H$. Therefore, we have $H \subseteq \langle \phi(g) \rangle$ and $\langle \phi(g) \rangle \subseteq H$ simultaneously, meaning $H = \langle \phi(g) \rangle$, i.e. H is a cyclic group.

5. Let $K \leq G$ with $|K| = n$. Consider the subgroup $\phi(K)$. By properties of homomorphism, $\phi(K) \leq H = \phi(G)$. Now by property (1), $|K| = |\phi(K)| = n$, meaning that there is a subgroup of H with order n, namely the subgroup $\phi(K)$.

This proves the theorem. □

Exercise I.4.5. Let $\phi : G \to H$ be an isomorphism between the groups G and H. Show that if G has a normal subgroup with order k, then H also has a normal subgroup of order k.

4.5 Links to Cyclic Groups

With the tool of isomorphism under our belt, we can prove two important theorems regarding cyclic groups. Before that, however, we need to introduce the idea of **infinite cyclic groups**.

Definition I.4.5.1. *An infinite cyclic group G generated by g is denoted by $\langle g \rangle$ and has order $|G| = \infty$. So,*

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

For brevity, we also have notation regarding the integers under addition. When we write $\mathbb{Z}_n$, we mean the group $(\mathbb{Z}_n, \oplus_n)$; when we write $\mathbb{Z}$, we mean the group $(\mathbb{Z}, +)$.

Theorem I.4.5.2. *If $G = \langle g \rangle$ and $|G| = \infty$, then $G \cong \mathbb{Z}$.*

Proof (see [Pro22], and [Coh82] §3.4 Theorem 1). Consider the map $\phi : \mathbb{Z} \to G$ such that $\phi(n) = g^n$. We need to prove that ϕ is an isomorphism.

- **Homomorphism**:

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$$

- **Injective**: Let m and n be integers such that $\phi(m) = \phi(n)$. Without loss of generality, assume that $m \leq n$. Since $\phi(m) = \phi(n)$ we have $g^m = g^n = g^m g^{n-m}$ which implies that $g^{n-m} = e$ by cancellation law.

  If $m < n$, let $k = n - m$. Clearly k is an integer. Thus, $g^k = e$ which means that $|g| = k$. However, g is a generator of G, which means that $|g| = |G| = \infty$. Hence, $k = \infty$ which is absurd. Therefore we have a contradiction, meaning $m \not< n$.

  Therefore, $m = n$ which means $k = 0 \implies g^0 = e$ which is valid. Hence, $\phi(m) = \phi(n)$ implies that $m = n$ which proves that ϕ is injective.

- **Surjective**: Suppose $x \in G = \langle g \rangle$, so $x = g^n$ for some integer n. Then $\phi(n) = g^n = x$ which means that x has a preimage of n. Hence ϕ is surjective.

Therefore, ϕ is a bijective homomorphism (i.e., isomorphism) which means that $G \cong \mathbb{Z}$. □

Theorem I.4.5.3. *If $G = \langle g \rangle$ and $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$.*

Proof (cf. [Cla84] §63). Consider $\phi : \mathbb{Z}_n \to G$ such that $\phi(m) = g^m$. We prove that ϕ is an isomorphism.

- **Homomorphism**:

$$\phi(l + m) = g^{l+m} = g^l g^m = \phi(l)\phi(m)$$

- **Injective**: Let l and m be integers such that $\phi(l) = \phi(m)$. Without loss of generality, assume that $l \leq m$. Since $\phi(l) = \phi(m)$ we have $g^l = g^m = g^l g^{m-l}$ which implies that $g^{m-l} = e$ by cancellation law.

  If $l < m$ then letting $k = m - l$ means that k belongs to the set $\{1, 2, 3, \ldots, n-1\}$. Therefore $g^k = e$ implies that $|g| = k \leq n-1 < n$. But since g is a generator of G, thus $|g| = |G| = n$. Therefore, we have $|g| < n$ and $|g| = n$ simultaneously, a contradiction. Thus $l \not< m$.

  Hence $l = m$, meaning ϕ is injective.

- **Surjective**: Suppose $x \in G = \langle g \rangle$, so $x = g^m$ for some integer m in $\mathbb{Z}_n$. Then $\phi(m) = g^m = x$ which means that x has a preimage of m. Hence ϕ is surjective.

Therefore, ϕ is a bijective homomorphism (isomorphism) which means that $G \cong \mathbb{Z}_n$. □

In summary:

- All cyclic groups with **infinite** order are isomorphic to the group of integers under addition, $\mathbb{Z}$.
- All cyclic groups with **finite** order n are isomorphic to the group of integers under addition modulo n, $\mathbb{Z}_n$.

Exercise I.4.6. Let $G = (\{1, 3, 7, 9\}, \otimes_{10})$ be a group. Show that G is cyclic and hence find the integer n such that $G \cong \mathbb{Z}_n$.

4.6 Problems

Problem I.4.1. Let G be a group and $g \in G$. Define the map $f : G \to G, x \mapsto gxg^{-1}$. Prove that f is an isomorphism.

Problem I.4.2. Let $\mathbb{Q}_{>0}$ denote the set of positive rational numbers. Let $G = (\mathbb{Q}, +)$ and $H = (\mathbb{Q}_{>0}, \times)$ be groups. Prove that $G \ncong H$.

Problem I.4.3. Let G and H **both** be the additive group of integers. Define a map $\phi : G \to H$ such that $\phi(n) = 2n$.

(a) Prove that ϕ is a homomorphism.

(b) Prove that ϕ is injective.

(c) Prove that there does **not** exist a homomorphism $\psi : H \to G$ such that $\psi(\phi(n)) = n$.

Problem I.4.4. Let G be a group. Define a map $f : G \to G$ such that $f(g) = g^{-1}$ for all g in G. Prove that G is abelian if and only if f is a homomorphism.

Problem I.4.5. Let G and H be groups. Suppose that we have a surjective homomorphism $\phi : G \to H$. Prove that if G is abelian, then so is H.

Problem I.4.6. Let G and H be groups. Suppose that we have a surjective homomorphism $\phi : G \to H$. Let $N \lhd G$. Show that $\phi(N) \lhd H$. (That is, the image of N under ϕ is a normal subgroup of H.)

Problem I.4.7. Let $G = (\mathbb{Z}_n, \oplus_n)$, and $H = \mathbb{Z}/(n\mathbb{Z})$ be under addition. Prove that $G \cong H$.

Problem I.4.8. Let G be a group and $N \lhd G$. Let B be a subgroup of the quotient group G/N. Prove that $B = A/N$, where A is a subgroup of G such that $N \subseteq A$.

5 Cayley's Theorem

This chapter is central to the relevance and analysis of group theory. Cayley's theorem links our ideas of symmetry with the idea of groups, and how groups are a form of *generalized symmetry*. It answers why group theory is oft called "the study of symmetry", and highlights the importance of bijections in our study of groups.

5.1 Permutations

A bijective function is too abstract an object. Such functions can take many forms. Thus, it is worth asking: what properties must a bijective function satisfy?

A bijective function is a function that maps all elements from one set to another set exactly. There are no leftovers (surjective), and each output has exactly one input that produces it (injective). In a sense, a bijective function *rearranges* the elements in a set; it renames elements and shuffles them around, without destroying the relative relationships between the elements.

For bijections between finite groups, each group has the same number of elements, so it is reasonable to talk about the rearrangement and enumeration of elements in such groups.

- What we mean by **rearrange** is to rename elements. We can give elements a new name and place it in the codomain.
- What we mean by **enumeration** is to assign each element in each finite group a unique 'index number', per se. Each element can have a unique number identifying its original *position* in the group, and its final position in the destination group.

Such bijections between finite groups are called **permutations**, since they simply permute the 'index number' of the elements in the groups.

Example I.5.1.1. Consider the set $S = \{1, 2, 3, 4, 5\}$. A bijection $f : S \to S$ could perform the following mapping:

- $1 \mapsto 2$
- $2 \mapsto 4$
- $3 \mapsto 3$
- $4 \mapsto 5$
- $5 \mapsto 1$

In this case, the function f is said to be a permutation because the ordered list $[2, 4, 3, 5, 1]$ is one rearrangement of the items in the set $\{1, 2, 3, 4, 5\}$.

Remark. It is certainly confusing that the operation of rearranging the items is also called *permuting* the items in the set, and one such rearrangement is called a permutation. In group theory, treat a "permutation" as a bijective function between finite groups.

Permutations come in many different forms, but the core thing that they do is to rearrange items. From the above example, one could form a 'cycle' of how each item is mapped to another:

- $1 \mapsto 2 \mapsto 4 \mapsto 5 \mapsto 1$
- $3 \mapsto 3$

We can describe a permutation based on how it cycles elements. Consider this alternate mapping performed by the map $\phi : S \to S$:

- $1 \mapsto 2$
- $2 \mapsto 4$
- $3 \mapsto 5$
- $4 \mapsto 1$
- $5 \mapsto 3$

How ϕ operates on an element can be described in **cycle notation**. Here's how to describe a permutation in cycle notation.

1. Start by opening a bracket: "(".
2. Write the first element that has not appeared yet in the cycle notation.
    - Initially, we write the number 1, so it currently looks like: "(1".
3. Find out where that element is mapped to.
    - For the case of the element 1, it is mapped to 2.
4. Write the mapped element next to the previous element.
    - In this case, we will write "(1 2"
5. Repeat previous two steps with the mapped element, until reaching an element that has already appeared in the cycle notation.
    - Since 2 maps to 4, we will continue to write: "(1 2 4"
    - Since 4 maps to 1, we terminate this process.
6. Close the bracket.
    - So our first cycle looks like "(1 2 4)"
7. Repeat above steps until all elements are used.
    - So our final cycle notation for g is "(1 2 4)(3 5)"

Some important things to note about this process:

- Omit any elements that maps to itself. For example, if $1 \mapsto 3$, $2 \mapsto 6$, $3 \mapsto 4$, $4 \mapsto 1$, $5 \mapsto 5$, $6 \mapsto 2$, and $7 \mapsto 7$, then the corresponding cycle notation is "(1 3 4)(2 6)", ignoring the 5 and 7.
- If the permutation is the identity permutation, then it has cycle notation of "(1)".

Example I.5.1.2. Consider the permutation α which has cycle notation $\begin{pmatrix}1 & 3 & 5 & 2\end{pmatrix}$. This means that:

- $\alpha(1) = 3$
- $\alpha(2) = 1$
- $\alpha(3) = 5$
- $\alpha(4) = 4$
- $\alpha(5) = 2$
- $\alpha(n) = n$ for $n \geq 6$

Example I.5.1.3. Consider the permutation β which has cycle notation $\begin{pmatrix}1 & 6 & 2 & 9 & 7 & 4\end{pmatrix}$. This means that:

- $\beta(1) = 6$
- $\beta(2) = 9$
- $\beta(3) = 3$
- $\beta(4) = 1$
- $\beta(5) = 5$
- $\beta(6) = 2$
- $\beta(7) = 4$
- $\beta(8) = 8$
- $\beta(9) = 7$
- $\beta(n) = n$ for $n \geq 10$

Exercise I.5.1. Write the cycle notation for these permutations:

(a) $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$

(b) $1 \mapsto 3$, $2 \mapsto 2$, $3 \mapsto 1$

(c) $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 5$, $5 \mapsto 2$

We now look at composing permutations.

Example I.5.1.4. Let the permutation f have cycle notation $\begin{pmatrix}1 & 3 & 5 & 2\end{pmatrix}$ and the permutation g have cycle notation $\begin{pmatrix}2 & 4 & 3\end{pmatrix}$. Then fg is a permutation.

Let $h = fg$. Then:

- $h(1) = f(g(1)) = f(1) = 3$
- $h(2) = f(g(2)) = f(4) = 4$
- $h(3) = f(g(3)) = f(2) = 1$
- $h(4) = f(g(4)) = f(3) = 5$
- $h(5) = f(g(5)) = f(5) = 2$

So h:

- $1 \mapsto 3$
- $2 \mapsto 4$
- $3 \mapsto 1$
- $4 \mapsto 5$
- $5 \mapsto 2$

and thus h has cycle notation $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4 & 5\end{pmatrix}$.

Example I.5.1.5. Consider $\begin{pmatrix}2 & 9 & 7 & 4\end{pmatrix}\begin{pmatrix}1 & 6 & 4\end{pmatrix}$. Then:

$$\begin{pmatrix}2 & 9 & 7 & 4\end{pmatrix}\begin{pmatrix}1 & 6 & 4\end{pmatrix} = \begin{pmatrix}1 & 6 & 2 & 9 & 7 & 4\end{pmatrix}.$$

We now consider how to find the inverse of a permutation. Given a cycle notation for the permutation f, simply read the cycle notation backwards, ensuring that the smallest element remains at the front.

Example I.5.1.6. $\begin{pmatrix}1 & 8 & 4 & 2\end{pmatrix}^{-1} = \begin{pmatrix}2 & 4 & 8 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 4 & 8\end{pmatrix}$.

Example I.5.1.7. $\begin{pmatrix}1 & 7 & 5 & 3 & 9\end{pmatrix}^{-1} = \begin{pmatrix}1 & 9 & 3 & 5 & 7\end{pmatrix}$.

Exercise I.5.2. Find the inverse of the permutation π, which has cycle notation

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

5.2 The Symmetric Group of a Set

With the definition of permutations out of the way, we can finally introduce a very important type of group: the **symmetric group** of a set X.

Definition I.5.2.1. *Let X be a set. Define*

$$\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ is a bijection}\}.$$

Proposition I.5.2.2. $(\mathrm{Sym}(X), \circ)$ *is a group, where $\circ$ is the function composition operator.*

Proof. We prove the 4 group axioms.

1. **Closure**: Let f and g be functions in $\mathrm{Sym}(X)$, so $f : X \to X$ and $g : X \to X$ are bijective functions. Define $h : X \to X$ where $h = f \circ g$. We show that h is bijective:

   - **Injective**: Let x and y be elements in X such that $h(x) = h(y)$. Then:

     $$\begin{aligned} f(g(x)) &= f(g(y)) && \text{(by definition of } h\text{)} \\ g(x) &= g(y) && \text{(since } f \text{ is bijective)} \\ x &= y && \text{(since } g \text{ is bijective)} \end{aligned}$$

     Therefore $h(x) = h(y)$ implies $x = y$.

   - **Surjective**: Let y be an element in X. Note that since f and g are bijective, therefore $f^{-1}(y)$ is in X and so is

$g^{-1}(f^{-1}(y))$. Note also that

$$h(g^{-1}(f^{-1}(y))) = f(g(g^{-1}(f^{-1}(y)))) = y$$

so a preimage of y exists in the domain, meaning that h is surjective.

Since h is injective and surjective, it is hence bijective. Thus $\mathrm{Sym}(X)$ is closed under $\circ$.

2. **Associativity**: Function composition is associative.
3. **Identity**: Let $\mathrm{id} : X \to X$ be such that $\mathrm{id}(x) = x$. Clearly id is in $\mathrm{Sym}(X)$:
   - **Injective**: If x and y are in X such that $\mathrm{id}(x) = \mathrm{id}(y)$ then clearly $x = y$.
   - **Surjective**: Let y be in X. Since $\mathrm{id}(y) = y$ thus y is its own pre-image under id.

   Now we show that id is indeed the identity in $\mathrm{Sym}(X)$. Let x be an arbitrary element of X, and f be any function in $\mathrm{Sym}(X)$. Then:
   $$(\mathrm{id} \circ f)(x) = \mathrm{id}(f(x)) = f(x)$$
   and
   $$(f \circ \mathrm{id})(x) = f(\mathrm{id}(x)) = f(x)$$
   so id is the identity in $\mathrm{Sym}(X)$.
4. **Inverse**: For all functions f in $\mathrm{Sym}(X)$, f^{-1} exists since f is a bijection. Furthermore, f^{-1} is a bijection from X to X, so f^{-1} is in $\mathrm{Sym}(X)$. By definition of f^{-1},
   $$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$$
   so f^{-1} is indeed the inverse of f in $\mathrm{Sym}(X)$.

Therefore $(\mathrm{Sym}(X), \circ)$ is a group. □

The group $(\mathrm{Sym}(X), \circ)$ is called the **symmetric group** of X. We usually suppress the function composition operator and call $\mathrm{Sym}(X)$ the symmetric group of X.

The most relevant type of symmetric group we encounter when working with finite groups is the **symmetric group of degree** n (or symmetric group of n letters).

Definition I.5.2.3. *The* ***symmetric group of degree*** n *is denoted by* S_n *and is equal to* $\mathrm{Sym}(\{1, 2, 3, \ldots, n\})$.

Let's look at a specific example of a symmetric group of degree n.

Example I.5.2.4. Consider the symmetric group of degree 3, S_3. We show all function mappings of S_3.

$1 \mapsto 1$ $2 \mapsto 2$ $3 \mapsto 3$	$1 \mapsto 2$ $2 \mapsto 3$ $3 \mapsto 1$	$1 \mapsto 3$ $2 \mapsto 1$ $3 \mapsto 2$
$1 \mapsto 2$ $2 \mapsto 1$ $3 \mapsto 3$	$1 \mapsto 1$ $2 \mapsto 3$ $3 \mapsto 2$	$1 \mapsto 3$ $2 \mapsto 2$ $3 \mapsto 1$

Figure 5.1: All Mappings of S_3

Thus, $|\mathrm{S}_3| = 6$.

Exercise I.5.3. Explain why $|\mathrm{S}_n| = n!$.

Remark. Elements of S_n are called permutations.

It should also be noted that subgroups of $\mathrm{Sym}(X)$ (where X is any set) are called **permutation groups**, primarily because they contain permutations. Since a group is its own subgroup, the symmetric group may sometimes be called *the* permutation group.

Finally, we prove one important proposition regarding the symmetric group of a finite set and the symmetric group of a certain degree.

Proposition I.5.2.5. $\mathrm{Sym}(G) \cong \mathrm{S}_n$ *if* G *is finite with order* n*.*

Proof. Since G has n elements, we can index them. Thus, let the set $G = \{x_1, x_2, \ldots, x_n\}$.

For brevity let σ denote an arbitrary permutation in S_n. Let the map $\phi : \mathrm{S}_n \to \mathrm{Sym}(G)$ be defined such that $(\phi(\sigma))(x_i) = x_{\sigma(i)}$ for all σ in S_n and x_i in G. We need to show that ϕ is an isomorphism.

- **Homomorphism**: Let σ and π be permutations in S_n. Let x_i be an element of G. Then

$$\begin{aligned}(\phi(\sigma\pi))(x_i) &= x_{\sigma(\pi(i))} \\ &= (\phi(\sigma))\left(x_{\pi(i)}\right) \\ &= ((\phi(\sigma))(\phi(\pi)))(x_i)\end{aligned}$$

  which means that ϕ is a homomorphism.

- **Injective**: Let σ and π be permutations in S_n such that $\phi(\sigma) = \phi(\pi)$, i.e. for all x_i in G, we have

$$x_{\sigma(i)} = (\phi(\sigma))(x_i) = (\phi(\pi))(x_i) = x_{\pi(i)}.$$

  Therefore $x_{\sigma(i)} = x_{\pi(i)}$. Now each element of G is uniquely indexed. Thus if two elements are equal, they have to have the same index. Hence, $\sigma(i) = \pi(i)$, for all *valid* i. This means $\sigma = \pi$ which proves that ϕ is injective.

- **Surjective**: Since $|\mathrm{Sym}(G)| = |G|! = n! = |\mathrm{S}_n|$ by **Exercise I.5.3**, thus ϕ is surjective.

Therefore there exists an isomorphism ϕ from S_n to $\mathrm{Sym}(G)$, meaning that $\mathrm{Sym}(G) \cong \mathrm{S}_n$. □

5.3 Cayley's Theorem

We now have sufficient background to state and prove Cayley's theorem.

Theorem I.5.3.1 (Cayley)**.** *Every group is isomorphic to a permutation group.*

The statement of the theorem, although simple, is the reason *why* group theorists study group theory: to explore all the ways that a group can be symmetric.

The proof of this theorem is involved and technical, but we'll try and simplify its proof as much as possible.

Proof. Let G be any group. We want to prove that there exists a group of bijective functions from G to G that is isomorphic to G (i.e., a permutation group).

For any g in G define the map $\lambda_g : G \to G$ such that $x \mapsto gx$. We claim that λ_g is a bijection.

- **Injective**: Let x and y be elements of G such that $\lambda_g(x) = \lambda_g(y)$. Then $gx = gy$ by definition of λ_g which immediately means $x = y$ by group cancellation law. Thus $\lambda_g(x) = \lambda_g(y)$ implies $x = y$, meaning λ_g is injective.
- **Surjective**: Let y be an element of G. Note that $g^{-1}y$ is an element of G (since G is closed), and that $\lambda_g(g^{-1}y) = g(g^{-1}y) = y$. Thus, a preimage of y is $g^{-1}y$ and it exists in the domain G, meaning λ_g is surjective.

Since λ_g is both injective and surjective it is thus bijective.

Now let $H = \{\lambda_g \mid g \in G\}$. Since λ_g is a bijective function from G to G, it thus is an element of $\mathrm{Sym}(X)$, meaning that $H \subseteq \mathrm{Sym}(G)$. It remains to show that $H \leq \mathrm{Sym}(G)$. We do this by using the subgroup test.

We first note that $\lambda_e = \mathrm{id}$ since

$$\lambda_e(x) = ex = x = \mathrm{id}(x)$$

for all x in G. Also, the inverse of any function λ_g is $\lambda_{g^{-1}}$ since

$$\lambda_g \circ \lambda_{g^{-1}}(x) = gg^{-1}x = x = \lambda_e(x)$$

and

$$\lambda_{g^{-1}} \circ \lambda_g(x) = g^{-1}gx = x = \lambda_e(x).$$

Now suppose $\lambda_{g_1}, \lambda_{g_2} \in H$ (where $g_1, g_2 \in G$). Note $g_1 g_2^{-1}$ is an element of G since G is closed. Therefore, for all x in G,

$$\begin{aligned}\lambda_{g_1} \circ (\lambda_{g_2})^{-1}(x) &= \lambda_{g_1} \circ \lambda_{g_2^{-1}}(x) \\ &= g_1 g_2^{-1} x \\ &= \lambda_{g_1 g_2^{-1}}(x)\end{aligned}$$

which is clearly an element of H. Thus if λ_{g_1} and λ_{g_2} are functions in H, then $\lambda_{g_1} \circ (\lambda_{g_2})^{-1}$ is also a function in H. Since H is non-empty, therefore by the Subgroup Test, we have shown $H \leq \mathrm{Sym}(G)$.

We finally show that $G \cong H$ by considering the map $\phi : G \to H, g \mapsto \lambda_g$. We need to show that ϕ is an isomorphism:

- **Homomorphism**: For any x in G,

$$\begin{aligned}\phi(gh)(x) &= \lambda_{gh}(x) \\ &= ghx \\ &= g(hx) \\ &= \lambda_g(\lambda_h(x)) \\ &= \lambda_g \circ \lambda_h(x) \\ &= (\phi(g)\phi(h))(x).\end{aligned}$$

  Thus, $\phi(gh) = \phi(g)\phi(h)$.

- **Injective**: Let g_1 and g_2 be elements in G such that $\phi(g_1) = \phi(g_2)$. Then $\lambda_{g_1} = \lambda_{g_2}$. Therefore, $\lambda_{g_1}(x) = \lambda_{g_2}(x)$ for all x in G, which means that $\lambda_{g_1}(e) = \lambda_{g_2}(e)$ when $x = e$. By definition of λ_g, we have $eg_1 = eg_2$ which ultimately means that $g_1 = g_2$. Thus if $\phi(g_1) = \phi(g_2)$ then $g_1 = g_2$.

- **Surjective**: The number of functions in H equals the number of elements of G by definition of H. Thus, since ϕ is surjective.

Therefore we have proven that ϕ is an isomorphism, which means that $G \cong H \leq \mathrm{Sym}(G)$, that is, any group G is isomorphic to a subgroup of the symmetric group of G (i.e., a permutation group). □

We note one corollary of this theorem.

Corollary I.5.3.1.1. *Let G be a finite group of order n. Then there exists a group $H \leq \mathrm{S}_n$ such that $G \cong H$.*

Proof. By Cayley's theorem (**Theorem I.5.3.1**), there exists a group $H \leq \mathrm{Sym}(G)$ such that $G \cong H$. Now since G is finite with order n, thus by **Proposition I.5.2.5**, $\mathrm{Sym}(G) \cong \mathrm{S}_n$. Thus, $H \leq \mathrm{S}_n$, and $G \cong H$. □

One might ask what the use of Cayley's Theorem is in group theory. To put it simply, it is a sanity check on the definition of a group. Before anyone had the idea of writing down the axioms for groups, people studied collections of bijections of sets closed under composition and inverses. Cayley's Theorem tells us that every abstract group is a type of the above collection, so the axioms of group theory capture the concrete phenomenon that groups were designed to capture.

5.4 Problems

Problem I.5.1. Let the permutations

$$\begin{aligned}\alpha &= \begin{pmatrix}1 & 5 & 2 & 3\end{pmatrix},\\ \beta &= \begin{pmatrix}1 & 5 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix},\\ \gamma &= \begin{pmatrix}1 & 2 & 5\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \text{ and}\\ \delta &= \begin{pmatrix}1 & 3 & 2 & 5\end{pmatrix}.\end{aligned}$$

What is the cycle notation of the permutation $\alpha\beta\gamma\delta$?

Problem I.5.2. Prove that the symmetric group of degree 3, S_3, is isomorphic to the dihedral group of order 6, D_3.

Problem I.5.3. State the number of elements in S_4.

(a) Let G be the cyclic group of order 4. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Find one such subgroup and prove that it is, indeed, isomorphic to G.

(b) Let G be the group with presentation

$$\langle a, b \mid a^2 = b^2 = (ab)^2 = e\rangle.$$

Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Find one such subgroup and prove that it is, indeed, isomorphic to G.

6 Direct Products of Groups

6.1 External Direct Product

The external direct product is one method of 'combining' groups together.

Definition I.6.1.1. *Let $(G, *)$ and $(H, \star)$ be groups. The **external direct product** of G and H is denoted by $G \times H$ and is the group $(G \times H, (*, \star))$, where $G \times H$ is the Cartesian product of G and H, and $(*, \star)$ are the operators performed component-wise.*

Note that $|G \times H| = |G||H|$ by definition of the Cartesian product.

Example I.6.1.2. $\mathbb{Z}_5 \times \mathbb{Z} = \{(m, n) \mid m \in \mathbb{Z}_5 \text{ and } n \in \mathbb{Z}\}$.

Thus, $(2, 5)(5, 9) = (2 \oplus_5 5, 5 + 9) = (2, 14)$.

Example I.6.1.3. Let $\mathcal{S} = \mathbb{R} \setminus \{0\}$ be a group under multiplication. Then $\mathcal{S} \times \mathbb{Z}_3 = \{(x, n) \mid x \in \mathcal{S} \text{ and } n \in \mathbb{Z}_3\}$.

So, $(3, 2)^{-1} = \left(\frac{1}{3}, 1\right)$ since

$$\begin{aligned}(3, 2)\left(\frac{1}{3}, 1\right) &= \left(3 \times \frac{1}{3}, 2 \oplus_3 1\right) \\ &= (1, 0) \\ &= (\text{Identity in } \mathcal{S}, \text{Identity in } \mathbb{Z}_3)\end{aligned}$$

Exercise I.6.1. What is $(s, rs)(r^2 s, r^3)$ in the group $D_3 \times D_4$?

We prove some results relating the external direct product.

Proposition I.6.1.4. *Let G_1 and G_2 be groups with identities e_1 and e_2 respectively. Let $(x, y) \in G_1 \times G_2$, $|x| = r$, $|y| = s$, and $e_{1,2}$ be the identity of $G_1 \times G_2$. Then $|(x, y)| = \operatorname{lcm}(r, s)$.*

Proof (see [Pro19]). For brevity let $l = \operatorname{lcm}(r, s)$, so $l = \alpha r = \beta s$ for some positive integers α and β. Let $m = |(x, y)|$.

Note that

$$\begin{aligned}(x, y)^l &= (x^l, y^l) \\ &= (x^{\alpha r}, y^{\beta s}) \\ &= \left((x^r)^\alpha, (y^s)^\beta\right) \\ &= (e_1^\alpha, e_2^\beta) \\ &= (e_1, e_2) \\ &= e_{1,2}.\end{aligned}$$

Therefore $l = k|(x, y)| = km$ for some positive integer k, i.e. $m|l$.

Note also that $(x, y)^m = (x^m, y^m)$ and $(x, y)^m = e_{1,2} = (e_1, e_2)$. Therefore $x^m = e_1$ and $y^m = e_2$. Hence,

$$m = p|x| = pr \text{ and } m = q|y| = qs$$

for some positive integers p and q, meaning that r and s both divide m. Therefore $\operatorname{lcm}(r, s) = l|m$.

Since $m|l$ and $l|m$, thus $m = l$, meaning $|(x, y)| = \operatorname{lcm}(|x|, |y|)$. □

Theorem I.6.1.5. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proof (see [Hum96] Proposition 13.1 (3)). We prove the forward direction first. Suppose $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. For brevity let $d = \gcd(m, n)$. Suppose on the contrary that $d > 1$.

Take $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Note that $\frac{mn}{d} = \text{lcm}(m,n)$ which is a positive integer. Then

$$\begin{aligned}\underbrace{(a,b)(a,b)(a,b)\cdots(a,b)}_{\frac{mn}{d} \text{ times}} &= \left(\frac{mn}{d}a, \frac{mn}{d}b\right) \\ &= \left(m\frac{na}{d}, n\frac{mb}{d}\right) \quad \text{(since } d|m \text{ and } d|n\text{)} \\ &= (\underbrace{0}_{\text{In } \mathbb{Z}_m}, \underbrace{0}_{\text{In } \mathbb{Z}_n})\end{aligned}$$

which implies $|(a,b)| \leq \underbrace{\frac{mn}{d}}_{\text{Since } d>1} < mn$ for all $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Hence, this means that $\mathbb{Z}_m \times \mathbb{Z}_n$ is *not* cyclic, since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ and no element in $\mathbb{Z}_m \times \mathbb{Z}_n$ has order mn.

However, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ which is cyclic, a clear contradiction. Hence, $d \not> 1 \implies d = 1$, meaning $\gcd(m,n) = 1$.

We now work on the reverse direction. Suppose $\gcd(m,n) = 1$. Note that $|1| = m$ in $\mathbb{Z}_m$ and $|1| = n$ in $\mathbb{Z}_n$. Thus

$$\begin{aligned}|(1,1)| &= \text{lcm}(m,n) && \textbf{(Proposition I.6.1.4)} \\ &= \frac{mn}{\gcd(m,n)} \\ &= mn && (\text{since } \gcd(m,n) = 1).\end{aligned}$$

Since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ and $|(1,1)| = mn$, thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. By **Theorem I.4.5.3**, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

This proves the theorem. □

Exercise I.6.2. Find all pairs of integers (m,n) with $1 < m < n$ such that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{180}$.

6.2 Internal Direct Product

Before we look at the internal direct product, we look at the **subgroup product**.

Definition I.6.2.1. *Let G be a group and $H, K \leq G$. Then*

$$HK = \{hk \mid h \in H, k \in K\}$$

*is called the **subgroup product of H and K**.*

Proposition I.6.2.2. *Let G be a group and $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. We first prove the forward direction; assume that $HK \leq G$. First take an arbitrary $kh \in KH$. Then we note

$$\begin{aligned} kh &= \left((kh)^{-1}\right)^{-1} \\ &= (\underbrace{h^{-1}}_{\text{In } H}\underbrace{k^{-1}}_{\text{In } K})^{-1} \\ &\in HK \end{aligned}$$

since $HK \leq G$ so the inverse of any element is in HK. Therefore any element in KH is also in HK, meaning that $KH \subseteq HK$. Now take an arbitrary $hk \in HK$. Note that $k^{-1}h^{-1} = (hk)^{-1} \in HK$, so set $k^{-1}h^{-1} = \hat{h}\hat{k}$ for some $\hat{h} \in H$ and $\hat{k} \in K$. Hence $hk = \left(k^{-1}h^{-1}\right)^{-1} = \hat{k}^{-1}\hat{h}^{-1} \in KH$, meaning $HK \subseteq KH$. Therefore $HK = KH$ as needed.

We now prove the reverse direction; assume that $HK = KH$. Clearly $e \in HK$ since $e \in H$ and $e \in K$. Now suppose $h_1k_1, h_2k_2 \in HK$. We

note

$$\begin{aligned}(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1(\underbrace{k_1k_2^{-1}h_2^{-1}}_{\text{In } KH=HK}) \\ &= h_1(h'k') \qquad\qquad (\text{set } (k_1k_2^{-1})h_2^{-1} = h'k') \\ &= (\underbrace{h_1h'}_{\text{In } H})k' \\ &\in HK\end{aligned}$$

so by subgroup test, $HK \leq G$. □

An important point to note is that $HK = KH$ does not imply that $hk = kh$ for all $h \in H$ and $k \in K$. Finding a counterexample to this claim is left as an exercise to the reader.

We now look at the **internal direct product**, another way of combining elements of two groups.

Definition I.6.2.3. *Let G be a group and $H, K \leq G$ such that*

1. *$G = HK$,*
2. *$H \cap K = \{e\}$, and*
3. *for all $h \in H$ and $k \in K$, $hk = kh$.*

*Then G is said to be the **internal direct product** of H and K.*

Example I.6.2.4. Consider $G = D_6$, $H = \langle r^3 \rangle$ and $K = \langle s, r^2 \rangle$. Note that

$$\begin{aligned}HK &= \{hk \mid h \in H, k \in K\} \\ &= \{e, r^2, r^4, s, r^2s, r^4s, r^3, r^5, r^7, r^3s, r^5s, r^7s\} \\ &= \{e, r^2, r^4, s, r^2s, r^4s, r^3, r^5, r, r^3s, r^5s, rs\} \\ &= D_6 \\ &= G\end{aligned}$$

so $G = HK$. Note also that $hk = kh$ for all h in H and k in K. Thus G is indeed the internal direct product of H and K.

Exercise I.6.3. Let $G = \{1, 5\}$ and $H = \{1, 7\}$ be groups under $\otimes_{12}$. Find the internal direct product of G and H.

6.3 The Isomorphism Between Them

It is certainly tiring to remember that there is an *external* direct product and an *internal* direct product. One might rightly wonder whether we can simplify both into one unified "direct product". In fact, there exists and isomorphism between the external direct product and the internal direct product of two groups.

Theorem I.6.3.1. *If G is the internal direct product of H and K then $G \cong H \times K$.*

Proof. Let $\phi : G \to H \times K$, $g \mapsto (h, k)$ where $g = hk$. We will show that ϕ is a well-defined isomorphism.

- **Well-defined**: Suppose $g = hk = h'k'$ where $h, h' \in H$ and $k, k' \in K$. Since $hk = h'k'$ thus $h^{-1}h' = k(k')^{-1}$.

  Note that $h^{-1}h' \in H$ and $k(k')^{-1} \in K$. So if $h^{-1}h' = k(k')^{-1}$ then $h^{-1}h' \in H \cap K$ and $k(k')^{-1} \in H \cap K$. But $H \cap K = \{e\}$. So $h^{-1}h' = e \implies h = h'$ and $k(k')^{-1} = e \implies k = k'$. Thus if $g = hk = h'k'$ then $h = h'$ and $k = k'$.

- **Homomorphism**: Let $g, g' \in G$, $h, h' \in H$, and $k, k' \in K$ such that $g = hk$ and $g' = h'k'$. Then

$$\begin{aligned}
\phi(gg') &= \phi(hkh'k') \\
&= \phi(h(kh')k') \\
&= \phi(h(h'k)k') && (hk = kh \text{ for all } h \text{ and } k) \\
&= \phi(\underbrace{hh'}_{\text{In } H}\underbrace{kk'}_{\text{In } K}) \\
&= (hh', kk') && (\text{by definition of } \phi) \\
&= (h, k)(h', k') \\
&= \phi(hk)\phi(h'k') \\
&= \phi(g)\phi(g')
\end{aligned}$$

- **Injective**: Let $g, g' \in G$, $h, h' \in H$, and $k, k' \in K$ such that $g = hk$, $g' = h'k'$, and $\phi(g) = \phi(g')$. Then $\phi(hk) = \phi(h'k')$, meaning $(h, k) = (h', k')$. Thus $h = h'$ and $k = k'$ by equality of ordered pairs, meaning $g = hk = h'k' = g'$.
- **Surjective**: Let $(h, k) \in H \times K$. Note that $hk \in G$ since G is the internal direct product of H and K, so $\phi(hk) = (h, k)$. Thus a pre-image of (h, k) is hk.

Therefore ϕ is a well-defined isomorphism from G to $H \times K$, meaning $G \cong H \times K$. □

Example I.6.3.2. Consider again $G = D_6$, $H = \langle r^3 \rangle$ and $K = \langle s, r^2 \rangle$. As we have found before, $G = HK$; but we now know that $G \cong H \times K$.

Note that $|H| = 2$ so $H \cong \mathbb{Z}_2$ and $K \cong D_3$ (we leave the latter as an exercise for the reader to prove). Thus,

$$D_6 = G = HK \cong H \times K = \mathbb{Z}_2 \times D_3.$$

Exercise I.6.4. Let $\mathcal{S} = \{1, 5, 7, 11\}$, $G = \{1, 5\}$ and $H = \{1, 7\}$ be groups under $\otimes_{12}$. Find the value of n such that $\mathcal{S} \cong (\mathbb{Z}_n)^2$.

6.4 Problems

Problem I.6.1. Let G and H be abelian groups. Prove that $G \times H$ is also an abelian group.

Problem I.6.2. Let G and H be groups. Prove that $G \times H \cong H \times G$.

Problem I.6.3. Let $G = \mathbb{Z}_6$, $H = \{0, 2, 4\}$, and $K = \{0, 3\}$. Determine if G is the internal direct product of H and K.

Problem I.6.4. Consider the *Klein four-group* V with presentation

$$\langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle.$$

Show that $\mathrm{V} \cong (\mathbb{Z}_2)^2$.

7 Further Properties of Homomorphisms

7.1 Image of a Homomorphism

As a homomorphism is a mapping between two groups, it is worthy to look at the image (or range) of the homomorphism.

Definition I.7.1.1. *The **image** (or **range**) of a homomorphism $\phi : G \to H$ is the set*

$$\operatorname{im} \phi = \{\phi(g) \mid g \in G\} \subseteq H.$$

Remark. Some authors (e.g. [Res22]) will use the notation $\phi(G)$ for the image of $\phi : G \to H$. The alternate notation Im ϕ may also be used (e.g. by [Cla84], [Hun80]).

Example I.7.1.2. Consider the simple homomorphism $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto 0$. Clearly, all possible values of x maps to 0, so im $f = \{0\}$ (or, alternatively, $f(\mathbb{Z}) = \{0\}$).

We note that the image of a homomorphism is a sub*set* of the codomain H. In fact, it is a sub*group*.

Proposition I.7.1.3. *Let $\phi : G \to H$ be a homomorphism. Then* im $\phi \leq H$.

Proof. We consider the subgroup test. Let e_G and e_H be the identities of G and H respectively. Note that $\phi(e_G) = e_H \in \operatorname{im} \phi$. Thus im ϕ is non-empty.

Now suppose h_1 and h_2 are in the image of ϕ, meaning that there exists g_1 and g_2 such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Note that $\phi(g_2^{-1}) = h_2^{-1}$ by homomorphism property. Hence $\phi(g_1 g_2^{-1}) = h_1 h_2^{-1} \in \text{im } \phi$.

Therefore, by subgroup test, im $\phi \leq H$. □

Exercise I.7.1. Consider the map $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6, n \mapsto 2n$. Determine whether ϕ is a homomorphism and, if so, find its image.

7.2 Kernel of a Homomorphism

Definition I.7.2.1. *The **kernel** of a homomorphism $\phi : G \to H$ is*

$$\ker \phi = \{x \in G \mid \phi(x) = e_H\}$$

where e_H is the identity in H.

Basically, the kernel of ϕ is the set of elements in G which map to the identity in H.

Remark. Some authors (e.g. [Res22]) will use the notation $\phi^{-1}(e_H)$ for the kernel of ϕ. The alternate notation Ker ϕ may also be used by some authors (e.g. [Cla84], [Hun80]).

Example I.7.2.2. Let the groups $G = (\mathbb{Z}^2, (+,+))$ and $H = (\mathbb{Z}, +)$. Let the map $\phi : G \to H, (a,b) \mapsto a+b$. Then, $(a,b) \in \ker \phi$ if $\phi((a,b)) = 0$. This means that $a + b = 0 \implies b = -a$. Hence the kernel of ϕ is $\{(a,-a) \mid a \in \mathbb{Z}\}$.

Exercise I.7.2. Let i be the imaginary unit, that is $i^2 = -1$. Let the group G be the integers under addition and $H = \langle i \rangle$ be under multiplication. Let the map $\phi : G \to H, n \mapsto i^n$. Show that ϕ is a homomorphism and hence find $\ker \phi$.

Like the image of ϕ, the kernel of ϕ is a subgroup of H. It is, in fact, a *normal* subgroup of H.

Proposition I.7.2.3. *Let $\phi : G \to H$ be a homomorphism. Then* $\ker \phi \lhd G$.

Proof. We will first show $\ker \phi \leq G$. Clearly $e_G \in \ker \phi$ since $\phi(e_G) = e_H$, so $\ker \phi$ is non-empty. Now let $x, y \in \ker \phi$. This means that $\phi(x) = \phi(y) = e_H$. Note

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

which means that $xy^{-1} \in \ker \phi$. By subgroup test $\ker \phi \leq G$.

Now we prove normality. Let $x \in G$ and $n \in \ker \phi$. We need to show that $xnx^{-1} \in \ker \phi$ to prove normality. Observe that

$$\begin{aligned} \phi(xnx^{-1}) &= \phi(x)\phi(n)\phi(x^{-1}) \\ &= \phi(x)e_H\phi(x)^{-1} && \text{(since } n \in \ker \phi\text{)} \\ &= \phi(x)\phi(x)^{-1} \\ &= e_H, \end{aligned}$$

which means that $xnx^{-1} \in \ker \phi$. Hence, $\ker \phi \lhd G$. □

Exercise I.7.3. Prove that a homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi$ is trivial, that is $\ker \phi = \{e_G\}$.

7.3 The Fundamental Homomorphism Theorem

We are now ready to tackle the three most important theorems regarding homomorphisms. We first state the **Fundamental Homomorphism Theorem**, which is also sometimes called the **First Isomorphism Theorem**.

Theorem I.7.3.1 (Fundamental Homomorphism Theorem)**.** *Let G and H be groups. Let $\phi : G \to H$ be a homomorphism, and let $\pi : G \to G/\ker\phi$ be a surjective homomorphism. Then there exists a unique isomorphism $\psi : G/\ker\phi \to \text{im } \phi$ such that $\psi\pi = \phi$.*

Equivalently, the Fundamental Homomorphism Theorem states that

$$G/\ker\phi \cong \text{im } \phi$$

for any homomorphism ϕ.

We include the commutativity diagram of the homomorphisms stated above to aid clarity:

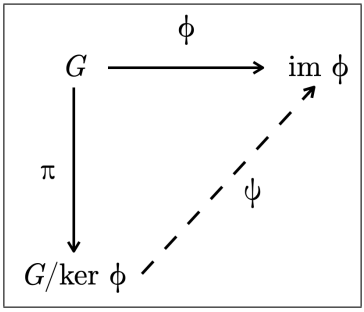


Figure 7.1: Commutivity Diagram For **Theorem I.7.3.1**

In the diagram, ϕ sends elements from G to im ϕ and π sends elements from G to $G/\ker\phi$. Then the map ψ is a unique map that sends elements from $G/\ker\phi$ to the image of ϕ.

Proof. We know by **Proposition I.7.1.3** that $\operatorname{im}\phi \leq H$. Let $\psi : G/\ker\phi \to \operatorname{im}\phi$ such that $\psi(x\ker\phi) = \phi(x)$. We are to check that ψ is a well-defined isomorphism.

- **Well-defined**: Suppose $x\ker\phi = y\ker\phi$.

$$\begin{aligned}
&\implies xy^{-1} \in \ker\phi && \text{(Coset Equality, \textbf{Lemma I.3.3.3})}\\
&\implies \phi(xy^{-1}) = e_H && \text{(Definition of kernel)}\\
&\implies \phi(x)\left(\phi(y)\right)^{-1} = e_H && \text{(Definition of homomorphism)}\\
&\implies \phi(x) = \phi(y)
\end{aligned}$$

  Thus,

$$\underbrace{\psi(x\ker\phi) = \phi(x)}_{\text{Definition of } \psi} = \underbrace{\phi(y) = \psi(y\ker\phi)}_{\text{Definition of } \psi}$$

  so ψ is well-defined.

- **Homomorphism**: Note that

$$\begin{aligned}
\psi((x\ker\phi)(y\ker\phi)) &= \psi((xy)\ker\phi)\\
&= \phi(xy)\\
&= \phi(x)\phi(y)\\
&= \psi(x\ker\phi)\psi(y\ker\phi)
\end{aligned}$$

  so ψ is a homomorphism.

- **Injective**: By **Exercise I.7.3**, we check that ψ is injective by showing that $\ker\psi$ is trivial, i.e. $\ker\psi = \{\ker\phi\}$.

  Suppose $x\ker\phi \in \ker\psi$. Then $\psi(x\ker\phi) = e_H$ by definition of kernel. Hence $\phi(x) = e_H$ by definition of ψ. Hence, $x \in \ker\phi$ by definition of kernel. This means that $xe^{-1} \in \ker\phi$. So $x\ker\phi = e\ker\phi = \ker\phi$ by Coset Equality (**Lemma I.3.3.3**) meaning that $\ker\psi = \{\ker\phi\}$. Therefore ψ is injective.

- **Surjective**: Suppose y is in the image of ϕ, meaning there exists a x in G such that $\phi(x) = y$. Note that $\psi(x\ker\phi) = \phi(x) = y$. Thus ψ is surjective.

Thus ψ is a well-defined isomorphism.

We now check that ψ satisfies the requirement that $\psi\pi = \phi$. Let $x \in G$. Note that $\pi(x) = x \ker \phi$, and

$$\psi\pi(x) = \psi(x \ker \phi) = \phi(x)$$

for all $x \in G$, so $\psi\pi = \phi$.

Finally we show that ψ is unique. Suppose $f : G/\ker \phi \to \text{im } \phi$ is an isomorphism satisfying $f\pi = \phi$. Take $x \ker \phi \in G/\ker \phi$. Note that

$$\begin{aligned} f(x \ker \phi) &= f(\pi(x)) \\ &= (f\pi)(x) \\ &= \phi(x) \\ &= (\psi\pi)(x) \\ &= \psi(\pi(x)) \\ &= \psi(x \ker \phi) \end{aligned}$$

for all $x \in G$, meaning that $f = \psi$. Therefore ψ is unique.

Hence, ψ is a unique isomorphism satisfying $\psi\pi = \phi$. □

Example I.7.3.2. Let $R = \{x \mid x > 0\}$, $G = \{x \in \mathbb{R} \mid x \neq 0\}$, and $H = \{1, -1\}$ be groups under multiplication. We show $G/H \cong R$.

Consider the map $\phi : G \to R$ where $x \mapsto |x|$. We show that ϕ is a homomorphism, then find the image of ϕ, and finally find its kernel.

- **Homomorphism**: ϕ is a homomorphism since $\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y)$.
- **Image**: We find the image of ϕ.

  $$\begin{aligned} \text{im } \phi &= \{\phi(x) \mid x \in G\} \\ &= \{|x| \mid x \neq 0\} \\ &= \{x \mid x > 0\} && \text{(by definition of } |x|) \\ &= R \end{aligned}$$

  which actually means that ϕ is surjective.

- **Kernel**: We find the kernel of ϕ.

$$\begin{aligned}\ker\phi &= \{x \in G \mid \phi(x) = 1\} \qquad \text{(since 1 is identity in } R\text{)}\\ &= \{x \in G \mid |x| = 1\}\\ &= \{1, -1\}\\ &= H\end{aligned}$$

Therefore, by the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**), $G/H \cong R$.

Exercise I.7.4. Let $\phi : G \to H$ be a homomorphism between finite groups G and H. Prove that

$$|G| = |\text{im } \phi| \times |\ker \phi|.$$

7.4 The Diamond Isomorphism Theorem

We now look at the next theorem, called the **Diamond Isomorphism Theorem** or the **Second Isomorphism Theorem**.

Theorem I.7.4.1 (Diamond Isomorphism Theorem)**.** *Let G be a group and let H and K be subgroups of G. Then*

1. *$H \cap K \leq H$ and $H \cap K \leq K$; and*
2. *$H \leq HK$ and $K \leq HK$.*

Furthermore, if $N \lhd G$, then

3. *$HN \leq G$;*
4. *$H \cap N \lhd H$;*
5. *$N \lhd HN$; and*
6. *$H/(H \cap N) \cong HN/N$.*

We can capture the overall relationships between the subgroups of G using a **subgroup lattice**.

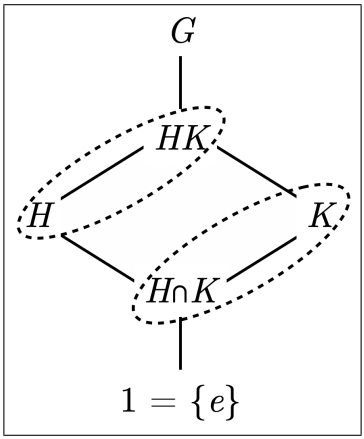


Figure 7.2: Subgroup Diagram for **Theorem I.7.4.1**

In the diagram, we only show subgroups that we care about. G has a (direct) subgroup HK; HK has subgroups H and K; and H and K has a common subgroup $H \cap K$. In the case where $K \lhd G$, the two dotted quotient groups are isomorphic to each other.

Proof. We prove each statement in sequence.

1. We only prove the first case (i.e., $H \cap K \leq H$) as the second follows symmetrically.

   Clearly $e_G \in H$ and $e_G \in K$ so $e_G \in H \cap K$.

   Take $x, y \in H \cap K$. To show that $xy^{-1} \in H \cap K$. Since $x, y \in H \cap K$, thus $x, y \in H$ and $x, y \in K$. Now since $H, K \leq G$, thus $xy^{-1} \in H$ and $xy^{-1} \in K$ by applying the subgroup test on H and K respectively. This thus means that $xy^{-1} \in H \cap K$. By the subgroup test, this means that $H \cap K \leq H$.

2. We only prove the first case ($H \leq HK$) as the second follows symmetrically. Note that $H = \{he_G \mid h \in H\} \subseteq \{hk \mid h \in H, k \in K\} = HK$, so we consider the subgroup test. Clearly $e_G \in H$ since $H \leq G$. Also since $H \leq G$, for all $x, y \in N$, $xy^{-1} \in G$. Thus, by the subgroup test, $H \leq HN$.

3. We note that, because N is normal, hence $hN = Nh$ for all $h \in H \subseteq G$, meaning that $HN = NH$. Therefore by **Proposition I.6.2.2**, $HN \leq G$.

4. We know $H \cap N \leq H$ by statement 1, so we only prove normality. Take $x \in H \cap N$, Since $H \leq G$, thus $x \in H \cap N \subseteq H$, meaning for all $g \in H$, $gxg^{-1} \in H$ (where we think of g and x as being in H). But since $x \in H \cap N \subseteq N$ and $N \lhd G$, thus $gxg^{-1} \in N$ (where we think of $g \in H$ and $x \in N$). Therefore $H \cap N \lhd H$.

5. We know $N \leq HN$ by statement 2, so we only prove normality. Take $n \in N$ and $x \in HN$ such that $x = h_x n_x$. Then

$$\begin{aligned} xnx^{-1} &= (h_x n_x) n (h_x n_x)^{-1} \\ &= (h_x n_x) n (n_x^{-1} h_x^{-1}) \qquad \text{(Shoes and Socks)} \\ &= \underbrace{h_x}_{\text{In } G} \underbrace{n_x n n_x^{-1}}_{\text{In } N} \underbrace{h_x^{-1}}_{\text{In G}} \\ &\in N \end{aligned}$$

   since $N \lhd G$. This proves that $N \lhd HN$.

6. This is the main result of this theorem.

   We define $\phi : H \to HN/N, h \mapsto hN$. Clearly ϕ is a homomorphism as

$$\phi(xy) = (xy)N = (xN)(yN) = \phi(x)\phi(y).$$

   We show that ϕ is surjective to show that im $\phi = HN/N$. Suppose $x \in HN$, meaning $x = hn$ where $h \in H$ and $n \in N$. Thus, $xN \in HN/N$. This implies that

$$xN = (hn)N = h(nN) = hN$$

meaning $\phi(h) = hN = xN$. Hence we have found a pre-image of the coset xN, meaning ϕ is surjective. Hence $\text{im}\,\phi = HN/N$.

We now claim that $\ker\phi = H \cap N$. Note that $\ker\phi = \{h \in H \mid \phi(h) = eN = N\}$ by definition of kernel. This means that if $h \in \ker\phi$ then $\phi(h) = N$. Hence,

$$\phi(h) = hN = N \implies h \in N$$

by Coset Equality (**Lemma I.3.3.3**). Thus, $h \in H$ and $h \in n$, meaning $h \in H \cap N$. Therefore $\ker\phi \subseteq H \cap N$.

Now suppose $x \in H \cap N$. This means that $x \in N$ necessarily, implying $xN = N$. Thus $\phi(x) = N$ which quickly implies $x \in \ker\phi$. Therefore $H \cap N \subseteq \ker\phi$.

Since $\ker\phi \subseteq H \cap N$ and $H \cap N \subseteq \ker\phi$ therefore $\ker\phi = H \cap N$.

By Fundamental Homomorphism Theorem (**Theorem I.7.3.1**),

$$H/\ker\phi \cong \text{im}\,\phi,$$

which means

$$H/(H \cap N) \cong HN/N.$$

This completes the proof of the Diamond Isomorphism Theorem. □

Corollary I.7.4.2. *Let G be a group. Let H and K be proper normal subgroups of G. Then $HK \lhd G$.*

Proof. By the Diamond Isomorphism Theorem (**Theorem I.7.4.1**), statement 3, we know that $HK \leq G$ since $H \lhd G$. We just need to prove normality. Suppose $hk \in HK$ and take $g \in G$. Then

$$\begin{aligned} g(hk)g^{-1} &= (gh)(kg^{-1}) \\ &= (hg)(g^{-1}k) && \text{(since } H, K \lhd G\text{)} \\ &= h(gg^{-1})k \\ &= hk \in HK \end{aligned}$$

which means that $HK \lhd G$. □

We look at a few examples for the use of the Diamond Isomorphism Theorem.

Example I.7.4.3. We say a group G is **metabelian** if and only if there exists $A \triangleleft G$ such that A and G/A are both abelian. We will prove the fact that any subgroup of a metabelian group is also metabelian.

Let $H \leq G$. Then by Diamond Isomorphism Theorem (**Theorem I.7.4.1**), $H \cap A \triangleleft H$ (statement 4) and $H/(H \cap A) \cong HA/A$ (statement 6). We just need to prove that $H \cap A$ is abelian and prove that $H/(H \cap A)$ is abelian.

- Consider any two elements from $H \cap A$, say x and y. Then $x \in A$ and $y \in A$, meaning $xy = yx$. Hence, elements from $H \cap A$ commute, meaning that $H \cap A$ is abelian.
- Consider HA/A. Note that $HA \leq G$ since $H \leq G$ and $A \leq G$. Thus, $HA/A \leq G/A$. Note that G/A is abelian by definition of metabelian group. Hence, $H/(H \cap A) \cong HA/A$ is also abelian.

Therefore, we have found a subgroup of H (in particular $H \cap A$) such that both $H \cap A$ and $H/(H \cap A)$ are both abelian. Hence, H is metabelian.

We look at another application of the Diamond Isomorphism Theorem, which has application in Number Theory.

Example I.7.4.4. We will prove that $\text{lcm}(m, n) \times \gcd(m, n) = mn$ by considering the Diamond Isomorphism Theorem. For brevity, let $d = \gcd(m, n)$ and $l = \text{lcm}(m, n)$.

Consider the groups $G = \mathbb{Z}$, $H = m\mathbb{Z}$, and $N = n\mathbb{Z}$ under addition. By Diamond Isomorphism Theorem (**Theorem I.7.4.1**),

$$m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}) \cong (m\mathbb{Z} + n\mathbb{Z})/(n\mathbb{Z}).$$

Now $m\mathbb{Z} \cap n\mathbb{Z}$ is the set of integers that are both a multiple of m and n. Hence, $m\mathbb{Z} \cap n\mathbb{Z} = \text{lcm}(m, n)\mathbb{Z} = l\mathbb{Z}$. On the other hand, $m\mathbb{Z} + n\mathbb{Z}$ is the set of all integers of the form $mx + ny$ where x and y are integers. Bezout's identity tells us that this set consists of the

multiples of $\gcd(m,n)$, i.e. $m\mathbb{Z}+n\mathbb{Z}=\gcd(m,n)\mathbb{Z}=d\mathbb{Z}$. Hence,

$$m\mathbb{Z}/(l\mathbb{Z}) \cong (d\mathbb{Z})/(n\mathbb{Z}).$$

We claim that

$$m\mathbb{Z}/(l\mathbb{Z}) \cong \mathbb{Z}_{\frac{l}{m}} \text{ and } d\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}_{\frac{n}{d}}.$$

This is a specific case of **Problem I.7.6** which we have left as a problem for later.

Hence, what we have shown is

$$\mathbb{Z}_{\frac{l}{m}} \cong m\mathbb{Z}/(l\mathbb{Z}) \cong d\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}_{\frac{n}{d}}$$

which means that $\mathbb{Z}_{\frac{l}{m}} \cong \mathbb{Z}_{\frac{n}{d}}$. We can now finally take orders on both sides:

$$\frac{l}{m}=\frac{n}{d},$$

which means that $ld=mn$. Hence, $\operatorname{lcm}(m,n)\times\gcd(m,n)=mn$.

Exercise I.7.5. Let G be a finite group, $H\leq G$, and $N\lhd G$. Prove that

$$|HN|=\frac{|H||N|}{|H\cap N|}.$$

7.5 The Third Isomorphism Theorem

We look at the last important theorem regarding homomorphisms and isomorphisms. This is often called the **Third Isomorphism Theorem** (e.g. [Coh82], [Hun80]). It should be noted that there is no consistency with the numbering of these theorems in books (cf. [Cla84] as "First Isomorphism Theorem" in §68, [Hum96] as Theorem 8.16 "Second Isomorphism Theorem"), but the name "Third Isomorphism Theorem" is the easiest to research. Hence, we use that name here.

Theorem I.7.5.1 (Third Isomorphism Theorem)**.** *Let G be a group. Let $H \lhd G$ and $N \lhd G$. Suppose $N \subseteq H$. Then*

1. *$N \lhd H$;*
2. *$H/N \lhd G/N$; and*
3. *$\frac{G/N}{H/N} \cong G/H$*

Proof. Like with the Diamond Isomorphism Theorem, we will prove the statements in sequence.

1. We first prove that it is a subgroup using the subgroup test before proving normality.

   Since $H, N \leq G$, thus $e_G \in H$ and $e_G \in N$, meaning that N is non-empty. Furthermore, since $N \leq G$, therefore $xy^{-1} \in N$ for all $x, y \in N$. Hence $N \leq H$.

   We now prove normality. Since H and N are normal subgroups of G, thus for all $g \in G$,

   $$gH = Hg \text{ and } gN = Ng.$$

   Now since $N \subseteq H \subseteq G$, thus for all n in N, $nH = Hn$ (since $n \in G$). This means that $N \lhd H$.

2. We first prove that it is a subgroup using the subgroup test, before proving normality.

   Clearly $N = eN \in H/N$. Let x and y be in H/N. Then $x = h_x N$ and $y = h_y N$ for some $h_x, h_y \in H$. Note that $y^{-1} = (h_y)^{-1} N$ by

group operator on cosets. Hence,

$$\begin{aligned} xy^{-1} &= (h_x N)(h_y^{-1} N) \\ &= (\underbrace{h_x h_y^{-1}}_{\text{In } H}) N \\ &\in H/N \end{aligned}$$

Hence, by subgroup test, $H/N \leq G/N$.

Now let $gN \in G/N$ and $hN \in H/N$. We need to show that $(gN)(hN)(gN)^{-1} \in H/N$. Note that $(gN)(hN)(gN)^{-1} = (ghg^{-1})N$. Since $H \lhd G$, thus $ghg^{-1} \in H$ which means that $(ghg^{-1})N \in H/N$.

Therefore $H/N \lhd G/N$.

3. This is the main result of the theorem.

   Define $\phi : G/N \to G/H, gN \mapsto gH$. We will check that ϕ is a well-defined surjective homomorphism and then find its kernel.

   - **Well-defined**: Suppose $gN = g'N$. Then $g(g')^{-1} \in N$ by Coset Equality (**Lemma I.3.3.3**). Since $N \subseteq H$ (assumption), thus $g(g')^{-1} \in H$ which implies $gH = g'H$ by **Lemma I.3.3.3**. Hence $\phi(gN) = gH = g'H = \phi(g'N)$, i.e. ϕ is well-defined.

   - **Homomorphism**: Take $gN, g'N \in G/N$. Then

     $$\begin{aligned} \phi((gN)(g'N)) &= \phi((gg')N) \\ &= (gg')H \\ &= (gH)(g'H) \\ &= \phi(gN)\phi(g'N) \end{aligned}$$

     which means that ϕ is a homomorphism.

   - **Surjective**: Suppose $gH \in G/H$. Then $\phi(gN) = gH$. Thus gN is a pre-image of gH, meaning that ϕ is surjective.

- **Kernel**: Suppose $gN \in \ker\phi = \{gN \mid \phi(gN) = eH = H\}$. Thus $\phi(gN) = H \implies gH = H$. Therefore, $ge^{-1} = g \in H$ by **Lemma I.3.3.3**. This means that $gN \in H/N$, further meaning that $\ker\phi \subseteq H/N$.

  Suppose now $hN \in H/N$. Since $H \lhd G \implies H \subseteq G$, thus $h \in G$. Therefore $hN \in G/N$ which means $\phi(hN) = hH = H$. Hence $hN \in \ker\phi$ which means $H/N \subseteq \ker\phi$.

  Since $\ker\phi \subseteq H/N$ and $H/N \subseteq \ker\phi$, we must have $\ker\phi = H/N$.

By Fundamental Homomorphism Theorem (**Theorem I.7.3.1**), $\frac{G/N}{\ker\phi} \cong \text{im}\ \phi$ which means

$$\frac{G/N}{H/N} \cong G/H,$$

hence proving statement 3.

This proves the theorem. □

Example I.7.5.2. Take $G = \mathbb{Z}$, $H = m\mathbb{Z}$ and $N = mn\mathbb{Z}$. Note that clearly $H, N \leq G$, and since G is abelian, we must also have $H \lhd G$ and $N \lhd G$. By the Third Isomorphism Theorem (**Theorem I.7.5.1**),

$$G/H \cong \frac{G/N}{H/N}.$$

Note $G/H = \mathbb{Z}/(m\mathbb{Z}) \cong \mathbb{Z}_m$ by **Problem I.4.7**. Note also

$$\frac{G/N}{H/N} = \frac{\mathbb{Z}/(mn\mathbb{Z})}{m\mathbb{Z}/(mn\mathbb{Z})}$$

and $\mathbb{Z}/(mn\mathbb{Z}) \cong \mathbb{Z}_{mn}$ by **Problem I.4.7**.

Consider now $\phi : m\mathbb{Z} \to \mathbb{Z}_{mn}, mx \mapsto mx \mod mn$. Clearly ϕ is a homomorphism. Note $\text{im}\ \phi = \langle m \rangle$ and $\ker\phi = mn\mathbb{Z}$. We leave the proof of these claims as an exercise to the reader.

By the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**),

$$m\mathbb{Z}/(mn\mathbb{Z}) \cong \langle m \rangle.$$

Thus,

$$\mathbb{Z}_m \cong G/H \cong \frac{G/N}{H/N} \cong \mathbb{Z}_{mn}/\langle m \rangle$$

which means $\mathbb{Z}_m \cong \mathbb{Z}_{mn}/\langle m \rangle$.

In other words, if d divides n, then

$$\mathbb{Z}_n/\langle d \rangle \cong \mathbb{Z}_d.$$

From this example we can come up with a more general proposition.

Proposition I.7.5.3. $\mathbb{Z}_n/\langle m \rangle \cong \mathbb{Z}_{\gcd(m,n)}$

Proof. We want to show that $\langle m \rangle = \langle \gcd(m,n) \rangle$. For brevity let $\gcd(m,n) = d$.

- $\boxed{\langle m \rangle \leq \langle d \rangle}$ Since $d \mid m$, thus $m = dk$ for some integer k. Hence, $\langle m \rangle = \{mx \mid x \in \mathbb{Z}\} = \{dkx \mid x \in \mathbb{Z}\} \leq \langle d \rangle$. Hence, $\langle m \rangle \leq \langle d \rangle d$.
- $\boxed{\langle m \rangle \geq \langle d \rangle}$ By the Extended Euclidean Algorithm we may write $d = \alpha m + \beta n$ for some integers α and β. In $\mathbb{Z}_n$, $d = \alpha m$ which quickly implies that $\langle d \rangle = \langle \alpha m \rangle \leq \langle m \rangle$.

Therefore $\langle d \rangle = \langle m \rangle$.

By previous example, the claim is proven. □

Exercise I.7.6. Suppose x and y are positive integers such that $x \mid y$. Let $H = x\mathbb{Z}$ and $N = y\mathbb{Z}$ be groups under addition.

(i) Explain why $N \subseteq H$.

(ii) Find a group G such that $H \lhd G$ and $N \lhd G$.

(iii) Hence find the order of H/N.

7.6 Problems

Problem I.7.1. Let G be a group. Prove that $G/G \cong \{e\}$.

Problem I.7.2. Let $G = \mathbb{R}^2$ be a group under component-wise addition,

$$H = \left\{ (r\sqrt{2}, r\sqrt{3}) \,\middle|\, r \in \mathbb{R} \right\}$$

be a group under component-wise addition, and $R = \mathbb{R}$ be a group under addition. Prove that $G/H \cong R$.

Problem I.7.3. Let $G = \mathbb{Z}^2$ under component-wise addition, $H = \mathbb{Z} \times \mathbb{Z}_5$ under $(+, \oplus_5)$, and $K = \langle (5,5) \rangle \lhd G$.

(i) Prove that $\phi : G \to H, (m,n) \mapsto (m-n, n \mod 5)$ is a group homomorphism.

(ii) Prove that ϕ is surjective.

(iii) Hence prove $G/K \cong H$.

Problem I.7.4. Let G be a group. Let H and K be subgroups of G such that $K \subseteq H$. Prove that $HK = H$.

Problem I.7.5. Let G be an abelian group under the operation $*$. Let $I = \{(g, g^{-1}) \mid g \in G\}$ be a group under component-wise application of $*$.

(i) Show that $I \cong G$.

(ii) Hence, by considering a suitable homomorphism, prove that $G^2/G \cong G$.

Problem I.7.6. Let $G = m\mathbb{Z}$ and $H = n\mathbb{Z}$ be groups under addition, where $m \mid n$ and $m \neq n$. Let the map $\phi : G \to \mathbb{Z}_{\frac{n}{m}}$ be defined such that

$$\phi(am) = a \mod \frac{n}{m}.$$

Prove that $G/H \cong \mathbb{Z}_{\frac{n}{m}}$.

8 More Types of Groups

8.1 More About Cyclic Groups

We previously covered several properties of cyclic groups:

- Every cyclic group is abelian. (**Proposition I.2.4.3**)
- A finite group G is cyclic if and only if there exists an element g in the group G with the same order as the group. (**Theorem I.2.4.4**)
- If G is cyclic and $H \leq G$ then G/H is cyclic. (**Exercise I.3.7**)
- Any subgroup of a cyclic group is also cyclic. (**Problem I.3.5**)
- $\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}_n$. (**Problem I.4.7**)
- $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$. (**Theorem I.6.1.5**)
- $\mathbb{Z}_n/\langle m \rangle \cong \mathbb{Z}_{\gcd(m,n)}$. (**Proposition I.7.5.3**)
- $m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{\frac{n}{m}}$. (**Problem I.7.6**)

Exercise I.8.1. Prove that for any positive integers m and n, we have

$$\mathbb{Z}_{mn}/\mathbb{Z}_m \cong \mathbb{Z}_n.$$

Note that we may denote the finite cyclic group of order n by C_n instead of $\mathbb{Z}_n$. This may be sometimes used to distinguish (finite) cyclic subgroups of a group from the integers modulo n.

We prove more facts about cyclic groups here.

Lemma I.8.1.1. *Let* C_n *have generator* g*. Then* $g^k = e$ *if and only if* $k = mn$ *where* m *is an integer.*
(Equivalently, this means that if $g^k = e$*, then* n *divides* k*, i.e.* $n|k$*.)*

Proof. The reverse direction is trivial to prove: if $k = mn$ for some integer m, then

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

We now work on the forward direction. Suppose that $g^k = e$. Applying the division algorithm on k yields $k = nq + r$ where q and r are integers such that $0 \leq r < n$. Thus, on one hand,

$$\begin{aligned} g^k &= g^{nq+r} \\ &= g^{nq} g^r \\ &= (g^n)^q \, g^r \\ &= e^q g^r \\ &= g^r. \end{aligned}$$

On the other hand, $g^k = e$. Therefore $g^r = e$ with $0 \leq r < n$. But $|g| = n$ since g is a generator of C_n. Hence, n is the smallest positive integer that allows $g^n = e$. If instead $g^r = e$ with $1 \leq r < n$ this contradicts the minimality of n, which implies $r = 0$. Therefore $k = nq$ (with $m = q$) completing the forward direction.

This completes the proof. □

Exercise I.8.2. The number 12 is equivalent to 0 in the group $\mathbb{Z}_n$ (under addition modulo n). What are the possible value(s) of n?

We are now ready to prove an important theorem on cyclic groups.

Theorem I.8.1.2. *Let* C_n *have generator* g*. Let* $x = g^k$ *for some integer* k*. Then the order of* x *is* $\frac{n}{\gcd(k,n)}$*.*

Proof. For brevity let $m = |x|$ and suppose $k = \lambda \gcd(k, n)$ for some positive integer λ.

Let $\mathcal{X} = \langle x \rangle = \{x, x^2, x^3, \ldots, x^m\}$. Note that $\mathcal{X}$ is a cyclic group with order m and generator x.

Observe that

$$x^m = \left(g^k\right)^m = g^{km}$$

and since $|x| = m$, this means that $x^m = e$. Hence

$$g^{km} = e.$$

By **Lemma I.8.1.1** on C_n, $n \mid km$. This implies that

$$\frac{n}{\gcd(k,n)} \,\Bigg|\, \frac{km}{\gcd(k,m)} = \lambda m.$$

Note that $\gcd\left(\lambda, \frac{n}{\gcd(k,n)}\right) = \gcd\left(\frac{k}{\gcd(k,n)}, \frac{n}{\gcd(k,n)}\right) = 1$. This means that $\frac{n}{\gcd(k,n)}$ does not divide λ, meaning $\frac{n}{\gcd(k,n)} \mid m$.

Also note that

$$\begin{aligned} x^{\frac{n}{\gcd(k,n)}} &= \left(g^k\right)^{\frac{n}{\gcd(k,n)}} \\ &= \left(g^n\right)^{\frac{k}{\gcd(k,n)}} \\ &= \left(g^n\right)^{\lambda} \\ &= e^{\lambda} && \text{(since } |g| = n\text{)} \\ &= e \end{aligned}$$

which implies $x^{\frac{n}{\gcd(k,n)}} = e$. By **Lemma I.8.1.1** on group $\mathcal{X}$, $m \Big| \frac{n}{\gcd(k,n)}$. Since $\frac{n}{\gcd(k,n)} \mid m$ and $m \mid \frac{n}{\gcd(k,n)}$ simultaneously, thus $m = \frac{n}{\gcd(k,n)}$, i.e. $|x| = \frac{n}{\gcd(k,n)}$. □

Exercise I.8.3. In the group $\mathbb{Z}_{210}$, find the order of 10, 42, 75, and 140.

We note one corollary of the theorem.

Corollary I.8.1.2.1. *Let* C_n *have generator* g*. Then* g^m *is also a generator if and only if* $\gcd(m, n) = 1$*.*

Proof. We prove the forward direction first. Suppose that C_n has a generator of g^m. On one hand, $|g^m| = n$ since a generator of a group necessarily has to have an order equal to that of the group. On another hand, by **Theorem I.8.1.2**, $|g^m| = \frac{n}{\gcd(m,n)}$. Hence, $n = \frac{n}{\gcd(m,n)}$ which quickly implies $\gcd(m, n) = 1$.

Now we prove the reverse direction. Suppose $\gcd(m, n) = 1$. Then $|g^m| = \frac{n}{\gcd(m,n)} = \frac{n}{1} = n$ by **Theorem I.8.1.2**. Hence g^m is a generator of the group C_n by **Theorem I.2.4.4**.

This completes the proof. □

Exercise I.8.4. Find all the generators of the following groups:

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{101}$

8.2 Quaternion Group

We look at an interesting group that has use in computer graphics: the **Quaternion Group**. We present one definition here.

Definition I.8.2.1. *The quaternion group is denoted by* Q *where*

$$\mathrm{Q} = \{1, -1, i, -i, j, -j, k, -k\}$$

such that

- *1 is the identity;*
- $(-1)^2 = 1$*;*
- $i^2 = j^2 = k^2 = -1$*;*
- $ij = k$ *and* $ji = -k$*;*
- $jk = i$ *and* $kj = -i$*; and*
- $ki = j$ *and* $ik = -j$*.*

Note that the proper subgroups of Q are

- $\langle -1 \rangle = \{\pm 1\}$;
- $\langle i \rangle = \{\pm 1, \pm i\}$;
- $\langle j \rangle = \{\pm 1, \pm j\}$; and
- $\langle k \rangle = \{\pm 1, \pm k\}$.

The correctness of these proper subgroups are left as an exercise to the reader.

With these subgroups, we can write a presentation for Q.

Proposition I.8.2.2. $\mathrm{Q} = \langle i, j \rangle$ *(with relationships as given above).*

Proof. For brevity let $G = \langle i, j \rangle$. We are to prove $G = \mathrm{Q}$.

We note that $i^0 = 1$, $i^4 = j^4 = 1$ and $ji = -k = -ij = i^3 j$. Hence,

$$\begin{aligned} G &= \{1, i, i^2, i^3, j, ij, i^2 j, i^3 j\} \\ &= \{1, i, -1, -i, j, ij, -j, -ij\} \\ &= \{1, -1, i, -i, j, -j, ij, -ij\} && \text{upon reordering} \\ &= \{1, -1, i, -i, j, -j, k, -k\} && \text{since } ij = k \\ &= \mathrm{Q}. \end{aligned}$$

Thus, $\mathrm{Q} = \langle i, j \rangle$. □

Thus, an alternate definition of Q is as follows:

$$\mathrm{Q} = \langle \alpha, \beta \mid \alpha^4 = e, \alpha^2 = \beta^2, \text{ and } \beta\alpha = \alpha^3\beta \rangle.$$

One sees clearly that in this definition, $\alpha = i$ and $\beta = j$.

Exercise I.8.5. Find all the normal subgroups of the quaternion group Q.
(*Hint: consider* ***Problem I.3.8***.)

8.3 Alternating Group

The alternating group is a very important group in the field of group theory. However, before we can properly define it, we need to introduce the idea of **transpositions**.

8.3.1 Transpositions

Definition I.8.3.1. *A* ***transposition*** *is a 2-cycle. That is, a transposition τ is represented as $(a \quad b)$ in cycle notation.*

For example, (1 5), (4 7), (3 6) etc. are transpositions, while (1 4 5), (3 4 6 5 9), (1 3 4 5) etc. are not. One clearly sees that every transposition is its own inverse.

We look at one lemma which can be said to help 'decompose' transpositions. Note that line breaks are to be ignored in the following lemma.

Lemma I.8.3.2. *Let a transposition $\tau = (i \quad i+d)$ where d is a positive integer. Then*

$$\begin{aligned}&(i \quad i+1)(i+1 \quad i+2)\cdots\\ &\quad (i+d-2 \quad i+d-1)(i+d-1 \quad i+d)(i+d-2 \quad i+d-1)\cdots\\ &\quad (i+1 \quad i+2)(i \quad i+1) = \tau.\end{aligned}$$

Proof. We induct on d.

When $d = 1$, $\tau = (i \quad i+1)$ so it is true.

Assume that the given representation of τ holds for some positive integer d. Note this means that it holds for all i, including $i+1$. We are to show that it works for $d+1$.

$$\begin{aligned}(i \quad i+(d+1)) &= (i \quad i+1)(i+1 \quad i+d+1)(i \quad i+1)\\ &= (i \quad i+1)\underbrace{((i+1) \quad (i+d)+1)}_{\text{apply induction hypothesis}}(i \quad i+1)\\ &= (i \quad i+1)((i+1) \quad (i+1)+1)\cdots((i+1) \quad (i+1)+1)\\ &\qquad (i \quad i+1)\\ &= (i \quad i+1)(i+1 \quad i+2)\cdots(i+1 \quad i+2)(i \quad i+1)\end{aligned}$$

which shows that $d+1$ works as well. □

Remark. In the above 'decomposition' of τ, $2d-1$ compositions were used.

Example I.8.3.3. As an example, let's look at the 'decomposition' of the transposition (4 9):

$$(4 \quad 9) = (4 \quad 5)(5 \quad 6)(6 \quad 7)(7 \quad 8)(8 \quad 9)(7 \quad 8)(6 \quad 7)(5 \quad 6)(4 \quad 5).$$

We leave it as an exercise for the reader to verify this particular case.

Exercise I.8.6. 'Decompose' the transposition (2 6).

Remark. We call transpositions of the form $(i \quad i{+}1)$ **adjacent transpositions**, and may denote them by α.

8.3.2 Links with Permutations

As mentioned before, transpositions are a 2-cycle permutation. However, transpositions are important as every permutation can be expressed as a product of transpositions.

Lemma I.8.3.4. *Every permutation can be expressed as a product of transpositions.*

Proof (see [Cla84] §80 Corollary). For the identity id it can be expressed as $(a \quad b)(a \quad b)$. For any permutation with length $k \geq 2$, say $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_k \end{pmatrix}$, write

$$\sigma = \begin{pmatrix} a_1 & a_k \end{pmatrix} \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \begin{pmatrix} a_1 & a_{k-2} \end{pmatrix} \cdots \begin{pmatrix} a_1 & a_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \end{pmatrix}$$

and since every permutation is a product of cycles, thus every permutation is a product of transpositions. □

We now look at the idea of **inversions** inside permutations.

Definition I.8.3.5. *Let σ be a permutation. An **inversion** of σ between i and j exists if $i > j$ and $\sigma(i) < \sigma(j)$.*

An inversion between i and j is denoted by either (i, j) or $(\sigma(i), \sigma(j))$.

Example I.8.3.6. In the permutation $\sigma = \begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}$, we see that $3 \mapsto 2$ but $2 \mapsto 4$. Thus there is an inversion $(3, 2) = (2, 4)$.

We now define the idea of **even** permutations and **odd** permutations.

Definition I.8.3.7. *A permutation σ is said to be **even** if there are an even number of inversions in σ. If σ is not even then it is said to be **odd**.*

Counting the number of inversions in a permutation may be too hard to do, and so we have an alternative definition for the evenness or oddness of a permutation. This idea is recorded in the following theorem.

Theorem I.8.3.8. *Let σ be a permutation. Then σ is even if and only if the number of transpositions that σ is 'decomposed' into is even.*

Proof. We only need to show that the *parity* of the number of inversions and permutations are equal to prove this.

By **Lemma I.8.3.4**, all permutations can be produced by a sequence of transpositions, say $\sigma = \tau_1\tau_2\tau_3\cdots\tau_k$.

By **Lemma I.8.3.2**, every transposition can be written as a product of $2d-1$ adjacent transpositions. Decomposing each $\tau_1, \tau_2, \ldots, \tau_k$ yields

$$\sigma = \alpha_1\alpha_2\cdots\alpha_m$$

where α_i is an adjacent transposition for $1 \leq i \leq m$. Note that the parity of m is the same as that of k.

It is clear that for any permutation π and adjacent permutation α, $\alpha\pi$ has either one more or one less inversion than π. Thus the parity of the number of inversions of a permutation is switched when composed with adjacent transpositions.

One sees clearly that the identity permutation id is an even permutation. So α_1 is odd, $\alpha_1\alpha_2$ is even, $\alpha_1\alpha_2\alpha_3$ is odd, etc., so $\alpha_1\alpha_2\cdots\alpha_m$ has parity of m. Therefore the parity of the number of inversions of σ is the parity of k, proving the theorem. □

Proposition I.8.3.9. *Let σ be a permutation. If σ is even then σ^{-1} is also even. Otherwise if σ is odd then σ^{-1} is also odd.*

Proof. One observes clearly that $\sigma\sigma^{-1} = \mathrm{id}$. Since id is even, thus $\sigma\sigma^{-1}$ must be composed of an even number of transpositions (by **Theorem I.8.3.8**).

- If σ is even, then σ is 'made up of' an even number of transpositions. Hence σ^{-1} must also be 'made up of' an even number of

transpositions in order for $\sigma\sigma^{-1} = \text{id}$ to be 'made up of' an even number of transpositions.

- If σ is odd, then σ is 'made up of' an odd number of transpositions. Hence σ^{-1} must also be 'made up of' an odd number of transpositions in order for $\sigma\sigma^{-1} = \text{id}$ to be even.

Thus, the proposition is proven. □

We look at one final useful construct: the sign of a permutation.

Definition I.8.3.10. *The **sign of a permutation** is $+1$ if the permutation is even and -1 if the permutation is odd.*

If σ is the permutation, $N(\sigma)$ denotes the number of inversions in σ and m the number of transpositions in the decomposition of σ, then the sign of σ is given by the signum function:

$$\text{sgn}(\sigma) = (-1)^{N(\sigma)} = (-1)^m.$$

Exercise I.8.7. Find the sign of the permutation (1 3 2 5 4).

As a final note, one observes that the number of inversions in $\sigma\tau$ is the same as the sum of inversions in σ and τ separately, meaning

$$N(\sigma\tau) = N(\sigma) + N(\tau)$$

which hence means that the sign of a permutation $\sigma\tau$ is

$$\begin{aligned}\text{sgn}(\sigma\tau) &= (-1)^{N(\sigma\tau)} \\ &= (-1)^{N(\sigma)+N(\tau)} \\ &= (-1)^{N(\sigma)}(-1)^{N(\tau)} \\ &= \text{sgn}(\sigma)\text{sgn}(\tau),\end{aligned}$$

meaning that sgn is a *multiplicative map*. One can then quickly verify **Proposition I.8.3.9** by noting

$$1 = \text{sgn}(\text{id}) = \text{sgn}(\sigma\sigma^{-1}) = \text{sgn}(\sigma)\text{sgn}(\sigma^{-1})$$

which means $\text{sgn}(\sigma)$ and $\text{sgn}(\sigma^{-1})$ have the same parity.

8.3.3 The Alternating Group

We are now ready to look at the alternating group.

Definition I.8.3.11. *The **alternating group of degree** n (where $n \geq 2$), denoted by A_n, is given by*

$$\mathrm{A}_n = \{\sigma \in \mathrm{S}_n \mid \sigma \text{ is even}\}$$

Proposition I.8.3.12. $\mathrm{A}_n \lhd \mathrm{S}_n$ *where* $n > 1$.

Proof. Clearly from definition $\mathrm{A}_n \subseteq \mathrm{S}_n$ so we consider the subgroup test. Note that the identity function $\mathrm{id} \in \mathrm{A}_n$ since $\mathrm{id} \in \mathrm{S}_n$ and the identity is even.

Suppose now that μ and σ are in A_n. We are to show that $\mu\sigma^{-1} \in \mathrm{A}_n$. By **Lemma I.8.3.4**, we may write

$$\mu = \tau_1\tau_2\cdots\tau_{2k} \text{ and } \sigma = \tau_1'\tau_2'\cdots\tau_{2m}'.$$

We note that any transposition is its own inverse, i.e. $\tau = \tau^{-1}$. Hence by Shoes and Socks, $\sigma^{-1} = \tau_{2m}'\tau_{2m-1}'\cdots\tau_2'\tau_1'$. Therefore,

$$\mu\sigma^{-1} = \underbrace{\tau_1\cdots\tau_{2k}\tau_{2m}'\cdots\tau_1'}_{2(k+m) \text{ transpositions}}$$

is an even permutation, meaning $\mu\sigma^{-1} \in \mathrm{A}_n$. By subgroup test, $\mathrm{A}_n \leq \mathrm{S}_n$.

Now take $\sigma \in \mathrm{S}_n$ and $\mu \in \mathrm{A}_n$. Note that $\mathrm{sgn}(\sigma\mu\sigma^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\mu)\mathrm{sgn}(\sigma^{-1})$. As above, we note $\mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma^{-1}) = 1$ and $\mathrm{sgn}(\mu) = 1$ since μ is even. Hence $\mathrm{sgn}(\sigma\mu\sigma^{-1}) = 1$ which means that $\sigma\mu\sigma^{-1}$ is an even permutation. Therefore $\sigma\mu\sigma^{-1} \in \mathrm{A}_n$, meaning that $\mathrm{A}_n \lhd \mathrm{S}_n$. □

Proposition I.8.3.13. *The order of* A_n *is* $\frac{n!}{2}$ *for* $n > 1$.

Proof. For brevity, let

$$\mathrm{O}_n = \{\sigma \in \mathrm{S}_n \mid \sigma \text{ is odd}\} = \mathrm{S}_n \setminus \mathrm{A}_n.$$

Clearly $A_n \cup \mathrm{O}_n = \mathrm{S}_n$ and $A_n \cap \mathrm{O}_n = \varnothing$.

Define a map $f : \mathrm{A}_n \to \mathrm{O}_n$ such that $\sigma \mapsto \begin{pmatrix}1 & 2\end{pmatrix}\sigma$. We will show that this is a bijective map.

- **Injective**: Let μ and σ be in A_n such that $f(\mu) = f(\sigma)$. This means that $\begin{pmatrix}1 & 2\end{pmatrix}\mu = \begin{pmatrix}1 & 2\end{pmatrix}\sigma$. Now by left-applying $\begin{pmatrix}1 & 2\end{pmatrix}$ on both sides yields $\mu = \sigma$.
- **Surjective**: Take $\mu \in \mathrm{O}_n$, say $\mu = \tau_1\tau_2\cdots\tau_{2k-1}$. Clearly,

$$\mu = \underbrace{\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}}_{\mathrm{id}}\tau_1\tau_2\cdots\tau_{2k-1}.$$

  Consider $\sigma = \begin{pmatrix}1 & 2\end{pmatrix}\tau_1\tau_2\cdots\tau_{2k-1}$, which is an even bijective function and thus is in A_n. Observe that

$$\begin{aligned} f(\sigma) &= \begin{pmatrix}1 & 2\end{pmatrix}\sigma \\ &= \begin{pmatrix}1 & 2\end{pmatrix}\left(\begin{pmatrix}1 & 2\end{pmatrix}\tau_1\tau_2\cdots\tau_{2k-1}\right) \\ &= \tau_1\tau_2\cdots\tau_{2k-1} \\ &= \mu \end{aligned}$$

  which means that $\mu \in \mathrm{O}_n$ has a pre-image σ in A_n.

This proves that f is bijective. Therefore $|\mathrm{A}_n| = |\mathrm{O}_n|$. Since $A_n \cup \mathrm{O}_n = \mathrm{S}_n$ and $A_n \cap \mathrm{O}_n = \varnothing$, thus $|\mathrm{S}_n| = |\mathrm{A}_n| + |\mathrm{O}_n| = 2|\mathrm{A}_n|$. Now because $|\mathrm{S}_n| = n!$ by **Exercise I.5.3**, therefore $|\mathrm{A}_n| = \frac{n!}{2}$. □

Exercise I.8.8. List all elements of A_3.

8.4 Group of Units Modulo n

We look at a useful group in number theory: the **group of units modulo** n.

Definition I.8.4.1. *For a positive integer $n \geq 2$, the **group of units modulo** n, denoted by $\mathcal{U}_n$, is the set*

$$\mathcal{U}_n = \{m \in \mathbb{Z} \mid 1 \leq m < n \text{ and } \gcd(m, n) = 1\}$$

together with the operation $\otimes_n$ (multiplication modulo n).

Proposition I.8.4.2. *$\mathcal{U}_n$ is an abelian group.*

Proof. We note that multiplication modulo n is commutative. So, we only need to prove that $\mathcal{U}_n$ satisfies the four group axioms to show that $\mathcal{U}_n$ is an abelian group.

1. **Closure**: Let $x, y \in \mathcal{U}_n$. Then $\gcd(x, n) = \gcd(y, n) = 1$. Hence $\gcd(xy, n) = 1$ which means that $\gcd(x \otimes_n y, n) = 1$. Thus $x \otimes_n y \in \mathcal{U}_n$.
2. **Associativity**: Since multiplication is associative, this is true.
3. **Identity**: Note that 1 is the identity in $\mathcal{U}_n$ since $1 \otimes_n x = x$.
4. **Inverse**: Let x be in $\mathcal{U}_n$, meaning $\gcd(x, n) = 1$. Thus there exists integers p and q such that $px + qn = 1$. Note that qn is a multiple of n, so $px \equiv 1 \pmod{n}$, which implies that $p \otimes_n x = 1$. Thus p is the left-inverse of x. Since multiplication is commutative, p is also the right-inverse of x. Hence p is the inverse of x.

This thus shows that $\mathcal{U}_n$ is an abelian group under $\otimes_n$. □

Exercise I.8.9. List the elements of $\mathcal{U}_{10}$.

There is, of course, another representation of $\mathcal{U}_n$, but we leave it to later in this section.

A useful number theory function that will occur frequently in this section is **Euler's totient function**.

Definition I.8.4.3. *The **Euler totient function** φ gives the number of numbers which are smaller than and coprime to a number x. That is,*

$$\varphi(x) = |\{n \in \mathbb{Z} \mid 1 \leq n < x \text{ and } \gcd(n, x) = 1\}|.$$

In particular, if $x = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $n_1, n_2, \ldots, n_k$ are positive integers, then

$$\varphi(x) = x\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Note by definition of $\mathcal{U}_n$, $|\mathcal{U}_n| = \phi(n)$.

Exercise I.8.10. Let a be in $\mathcal{U}_n$. Prove that $|a|$ divides $\varphi(n)$.

We look at the specific case where $|a| = \varphi(n)$.

Definition I.8.4.4. *If $\gcd(a, n) = 1$ we say that a is a **primitive root modulo** n if $|a| = \varphi(n)$ in $\mathcal{U}_n$.*

We state the following fact without proof:

> There is a primitive root modulo n if and only if n is 1, 2, 4, p^k, or $2p^k$ where p is an odd prime.

Proposition I.8.4.5. *$\mathcal{U}_n$ is cyclic if and only if there is a primitive root modulo n.*

Proof. We first prove the forward direction. Let $\mathcal{U}_n$ be cyclic. Then there exists an element $r \in \mathcal{U}_n$ such that $|r| = |\mathcal{U}_n| = \varphi(n)$. By definition of a primitive root, this means that r is a primitive root modulo n.

We prove the reverse direction. Let $r \in \mathcal{U}_n$ be a primitive root modulo n. Then $\langle r \rangle \cong \mathbb{Z}_{\varphi(n)}$. Note that since $|\langle r \rangle| = \phi(n) = |\mathcal{U}_n|$, therefore r is a generator of $\mathcal{U}_n$, proving that $\mathcal{U}_n$ is cyclic. □

Remark. In fact, what **Proposition I.8.4.5** shows is that $\mathcal{U}_n \cong \mathbb{Z}_{\varphi(n)}$ if there exists a primitive root modulo n.

We look at some results about the structure of the group of units.

Proposition I.8.4.6. *If* $\gcd(m,n) = 1$ *then* $\mathcal{U}_m \times \mathcal{U}_n \cong \mathcal{U}_{mn}$.

Proof. Let $(x,y) \in \mathcal{U}_m \times \mathcal{U}_n$. Set $a = n^{-1}$ in $\mathcal{U}_m$ and $b = m^{-1}$ in $\mathcal{U}_n$.

Define $\sigma : \mathcal{U}_m \times \mathcal{U}_n \to \mathcal{U}_{mn}$, where $(x,y) \mapsto xmb + yna$. We show that σ is an isomorphism:

- **Homomorphism**: Consider two pairs (x_1,y_1) and (x_2,y_2).

$$\begin{aligned}\sigma((x_1,y_1)(x_2,y_2)) &= \sigma((x_1x_2, y_1y_2)) \\ &= \underbrace{x_1x_2mb + y_1y_2na}_{\text{In } \mathcal{U}_{mn}} \\ &= x_1x_2mb + y_1y_2na + \underbrace{x_1y_2mnab + x_2y_1mnab}_{\equiv 0 \pmod{mn}} \\ &= (x_1mb + y_1na) \otimes_{mn} (x_2mb + y_2na) \\ &= \sigma((x_1,y_1))\sigma((x_2,y_2))\end{aligned}$$

  which shows that σ is a homomorphism.

- **Injective**: Suppose (x_1,y_1) and (x_2,y_2) are pairs such that $\sigma((x_1,y_1)) = \sigma((x_2,y_2))$. Then

$$x_1mb + y_1na = x_2mb + y_2na$$

  Reducing both sides by modulo m yields $0 + y_1na \equiv 0 + y_2na$. Note that $a = n^{-1}$ in $\mathcal{U}_m$, which quickly means $y_1 = y_2$ since $1 \leq y_1, y_2 < n$. Similar argument by reducing both sides by modulo n yields $x_1 = x_2$. This means that ϕ is injective.

- **Surjective**: Note that a property of Euler's totient function is that $\varphi(mn) = \varphi(m)\varphi(n)$. Thus

$$|\mathcal{U}_{mn}| = \varphi(mn) = \varphi(m)\varphi(n) = |\mathcal{U}_m||\mathcal{U}_n| = |\mathcal{U}_m \times \mathcal{U}_n|.$$

  Since σ is injective, and since $\mathcal{U}_{mn}$ is equinumerous with $\mathcal{U}_m \times \mathcal{U}_n$, σ has to be surjective.

This proves that σ is an isomorphism between $\mathcal{U}_m \times \mathcal{U}_n$ and $\mathcal{U}_{mn}$, i.e. $\mathcal{U}_m \times \mathcal{U}_n \cong \mathcal{U}_{mn}$. □

Proposition I.8.4.7. *For $m \geq 3$, $\mathcal{U}_{2^m} \cong \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_2$.*

Proof. We first claim that $|5| = 2^{m-2}$ in $\mathcal{U}_{2^m}$. We induct on m using two-step induction.

We first consider the case $m = 3$; we are to show that $|5| = 2$ in $\mathcal{U}_{2^3} = \mathcal{U}_8$. Since $5^2 = 25 = 24 + 1 \equiv 1 \pmod 8$, thus $|5| = 2$ in $\mathcal{U}_8$, meaning the case where $m = 3$ is true.

We next consider the case where $m = 4$; we are to show that $|5| = 4$ in $\mathcal{U}_{2^4} = \mathcal{U}_{16}$. Note that $5^1 = 5$, $5^2 = 25 \equiv 9 \pmod{16}$, $5^3 = 125 \equiv 13 \pmod{16}$, and $5^4 = 625 \equiv 1 \pmod{16}$, so $|5| = 4$ in $\mathcal{U}_{16}$, meaning the case where $m = 4$ is true.

Now assume that the cases where $m = k$ and $m = k + 1$ are true for $k \geq 3$, meaning $|5| = 2^{k-2}$ for $\mathcal{U}_{2^k}$ and $|5| = 2^{k-1}$ for $\mathcal{U}_{2^{k+1}}$. To prove that the case where $m = k + 2$ is true, that is $|5| = 2^k$ for $\mathcal{U}_{2^{k+2}}$.

By induction hypothesis, since $|5| = 2^{k-1}$ for $\mathcal{U}_{2^{k+1}}$,

$$5^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \text{ and } 5^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$$

since $2^{k-1} > 2^{k-2}$ and by definition of the order of the element 5. But since $|5| = 2^{k-2}$ for $\mathcal{U}_{2^k}$, thus

$$5^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

This implies that $5^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}$. Now if we reduce modulo 2^{k+2} instead,

$$5^{2^{k-2}} \equiv 1 + 2^k + b2^{k+1} \pmod{2^{k+2}}$$

where $b \in \{0, 1\}$. Squaring both sides,

$$\begin{aligned}
5^{2^{k-1}} &\equiv \left(1 + 2^k + b2^{k+1}\right)^2 \\
&\equiv 1 + 2\left(2^k + b2^{k+1}\right) + \left(2^k + b2^{k+1}\right)^2 \\
&\equiv 1 + 2^{k+1} + 2b(2^{k+1}) + 2^{2k}(1 + 4b + 4b^2) \\
&\equiv 1 + 2^{k+1} + 2^{k+2}b + 2^{k+2}\left(2^{k-2}(1 + 4b + 4b^2)\right) \quad (\text{since } k \leq 3) \\
&\equiv 1 + 2^{k+1} \pmod{2^{k+2}} \\
&\not\equiv 1 \pmod{2^{k+2}}
\end{aligned}$$

which means that, in summary, $5^{2^{k-1}} \not\equiv 1 \pmod{2^{k+2}}$.

Now, by **Exercise I.8.10**, $|5|$ divides $\varphi(2^{k+2}) = 2^{k+1}$ in $\mathcal{U}_{2^{k+2}}$, meaning that $2^{k+1} = a|5|$ for some integer a, i.e. $|5| = \frac{1}{a}2^{k+1}$.

Note that $|5| < 2^{k-1}$ for $\mathcal{U}_{2^{k+2}}$ since $|5| = 2^{k-1}$ for $\mathcal{U}_{2^{k+1}}$. Thus, $|5| \geq 2^{k-1}$.

But since $5^{2^{k-1}} \not\equiv 1 \pmod{2^{k+2}}$, thus $|5| > 2^{k-1}$. Now because $|5| = \frac{1}{a}2^{k+1}$ and $|5| > 2^{k-1}$, thus $|5| = 2^k$ (with $a = 2$) or $|5| = 2^{k+1}$ (with $a = 1$).

Suppose $|5| = 2^{k+1}$. Then $|5| = 2^{k+1} = |\mathcal{U}_{2^{k+2}}|$, meaning that $\mathcal{U}_{2^{k+2}}$ is cyclic. By **Proposition I.8.4.5** there must be a primitive root modulo 2^{k+2} in this case. However, by the "fact" about primitive roots, there is **not** a primitive root modulo 2^{k+2}. Thus, $|5| \neq 2^{k+1}$ in $\mathcal{U}_{2^{k+2}}$, meaning that $|5| = 2^k$ in $\mathcal{U}_{2^{k+2}}$. This completes the proof of the claim that $|5| = 2^{m-2}$ in $\mathcal{U}_{2^m}$.

We can finally prove the main result. Let $H = \langle 5 \rangle$ and let $K = \langle -5^{2^{m-3}} \rangle$. Note that:

- $|\mathbb{Z}_{2^{m-2}}| = 2^{m-2} = |\langle 5 \rangle|$ so $\mathbb{Z}_{2^{m-2}} \cong \langle 5 \rangle \leq \mathcal{U}_{2^m}$.
- $|-5^{2^{m-1}}| = 2$ since $\left(-5^{2^{m-3}}\right) \times \left(-5^{2^{m-3}}\right) = 5^{2^{m-2}}$ and $|5| = 2^{m-2}$ in $\mathcal{U}_{2^m}$. Thus $\mathbb{Z}_2 \cong \langle -5^{2^{m-3}} \rangle$.

We see that $\mathcal{U}_{2^m} = HK$ since $\mathcal{U}_{2^m} = HK$, $H \cap K = \{1\}$ (the identity), and $HK = KH$. By **Theorem I.6.3.1**, $HK \equiv H \times K$ so $\mathcal{U}_{2^m} \equiv H \times K$.

But $H \cong \mathbb{Z}_{2^{m-2}}$ and $K \cong \mathbb{Z}_2$. Thus, $\mathcal{U}_{2^m} \cong \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_2$ for $m \geq 3$. $\square$

Corollary I.8.4.8. *Let $p_1, p_2, \ldots, p_k$ be distinct odd primes. Then if $m \geq 3$,*

$$\mathcal{U}_{2^m p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{p_1^{n_1} - p_1^{n_1 - 1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k} - p_k^{n_k - 1}}.$$

Proof. We use the previously proved propositions to establish this result. For brevity let $G = \mathcal{U}_{2^m p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}}$.

$$\begin{aligned}
G &\cong \mathcal{U}_{2^m} \times \mathcal{U}_{p_1^{n_1}} \times \cdots \times \mathcal{U}_{p_k^{n_k}} && (\textbf{Prop. I.8.4.6}) \\
&\cong (\mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}) \times \mathcal{U}_{p_1^{n_1}} \times \cdots \times \mathcal{U}_{p_k^{n_k}} && (\textbf{Prop. I.8.4.7}) \\
&\cong (\mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}) \times \mathbb{Z}_{\varphi(p_1^{n_1})} \times \cdots \times \mathbb{Z}_{\varphi(p_k^{n_k})} && (\textbf{Prop. I.8.4.5}) \\
&\cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{p_1^{n_1} - p_1^{n_1 - 1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k} - p_k^{n_k - 1}}
\end{aligned}$$

proving the result. $\square$

Example I.8.4.9. Consider $\mathcal{U}_{600}$. Note that $600 = 2^3 \times 3 \times 5^2$. Thus,

$$\mathcal{U}_{600} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{20},$$

i.e., $\mathcal{U}_{600} \cong (\mathbb{Z}_2)^3 \times \mathbb{Z}_{20}$.

Exercise I.8.11. Find an isomorphism for $\mathcal{U}_{1680}$ in terms of "$\mathbb{Z}_n$"s.

We end this section by looking at an alternate representation of $\mathcal{U}_n$. Define the group

$$(\mathbb{Z}/(n\mathbb{Z}))^\times = \{m + n\mathbb{Z} \mid m \in \mathbb{Z}, 1 \leq m < n, \text{ and } \gcd(m, n) = 1\}$$

under the operation $*$ where $(a + n\mathbb{Z}) * (b + n\mathbb{Z}) = (a \otimes_n b) + n\mathbb{Z}$ for $n \geq 2$. We will show that $\mathcal{U}_n$ is isomorphic to this group.

Proof. Define the map $\phi : \mathcal{U}_n \to (\mathbb{Z}/(n\mathbb{Z}))^\times$ such that $m \mapsto m + n\mathbb{Z}$. We show that ϕ is an isomorphism.

- **Homomorphism**: Let $x, y \in \mathcal{U}_n$. Then ϕ is a homomorphism since

$$\begin{aligned}\phi(x \otimes_n y) &= (x \otimes_n y) + n\mathbb{Z} \\ &= (x + n\mathbb{Z}) * (y + n\mathbb{Z}) \\ &= \phi(x) * \phi(y).\end{aligned}$$

- **Injective**: Suppose we have $x, y \in \mathcal{U}_n$ such that $\phi(x) = \phi(y)$. Then this means that $x + n\mathbb{Z} = y + n\mathbb{Z}$. Thus

$$\{x + pn \mid p \in \mathbb{Z}\} = \{y + qn \mid q \in \mathbb{Z}\}.$$

  Hence we conclude that $x \equiv y \pmod{n}$. But since $1 \leq x, y < n$, therefore we must have $x = y$. Hence, $\phi(x) = \phi(y)$ implies $x = y$, meaning ϕ is injective.

- **Surjective**: Let $x+n\mathbb{Z} \in (\mathbb{Z}/(n\mathbb{Z}))^\times$. This means that $\gcd(x, n) = 1$. Performing division algorithm on x yields

$$x = qn + r, \text{ where } 0 \leq r < n.$$

  Note that

$$\begin{aligned}x + n\mathbb{Z} &= \{x + kn \mid k \in \mathbb{Z}\} \\ &= \{(qn + r) + kn \mid k \in \mathbb{Z}\} \\ &= \{r + n(\underbrace{q + k}_{\text{In } \mathbb{Z}}) \mid k \in \mathbb{Z}\} \\ &= r + n\mathbb{Z}\end{aligned}$$

  with $0 \leq r < n$. Note that if $r = 0$, this means that $x = qn$, which means that $\gcd(x, n) = \gcd(qn, n) = n \neq 1$. Thus, $r \neq 0$, meaning $1 \leq r < n$ so $r \in \mathcal{U}_n$.

  Observing that $\phi(r) = r + n\mathbb{Z} = x + n\mathbb{Z}$ shows that $x + n\mathbb{Z}$ has a pre-image r in $\mathcal{U}_n$, which means that ϕ is surjective.

Thus ϕ is an isomorphism, meaning $\mathcal{U}_n \cong (\mathbb{Z}/(n\mathbb{Z}))^\times$. □

8.5 Groups of Matrices

8.5.1 Introduction to Matrices

Before we can introduce the groups of matrices, we need to understand what they are, and to learn some operations that can be applied to matrices.

A matrix is a rectangular array numbers, symbols, or expressions, arranged in rows and columns. They are used to represent mathematical objects or properties of objects.

For example,

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

is a matrix. We consider only square matrices, which have the same number of rows as columns. For example,

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} -1 & 0 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 3 & 3 & 3 \end{pmatrix}, \text{ and } \mathbf{C} = \begin{pmatrix} x & x^2 \\ x^3 & x^4 \end{pmatrix}$$

are square matrices. For brevity, for a matrix $\mathbf{M}$, we denote the element in the ith row and the jth column as $m_{i,j}$ (where $1 \leq i, j \leq n$ with n being the number of rows and columns in $\mathbf{M}$). For example, using the above matrices, $a_{2,2} = 5$, $b_{2,4} = 1$, and $c_{1,1} = x$.

We now need to introduce the idea of **matrix multiplication**. Consider two square matrices $\mathbf{A}$ and $\mathbf{B}$ with the same number of rows and columns (say, n rows and columns). Let their product, $\mathbf{AB}$, be the matrix $\mathbf{C}$. Then

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

for $1 \leq i, j \leq n$. For example,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 \times 5 + 2 \times 7 & 1 \times 6 + 2 \times 8 \\ 3 \times 5 + 4 \times 7 & 3 \times 6 + 4 \times 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}.$$

Note that matrix multiplication is **not** commutative. For example,

$$\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\begin{pmatrix}5 & 6\\7 & 8\end{pmatrix}=\begin{pmatrix}19 & 22\\43 & 50\end{pmatrix}, \text{ but } \begin{pmatrix}5 & 6\\7 & 8\end{pmatrix}\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}=\begin{pmatrix}23 & 34\\31 & 46\end{pmatrix}$$

Exercise I.8.12. Find the matrix given by the product

$$\begin{pmatrix}1 & 1 & 0\\0 & 1 & 0\\0 & 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 1\\1 & 0 & 1\\1 & 1 & 1\end{pmatrix}.$$

Matrices can also be 'multiplied' by real numbers (known as scalar multiplication). For example,

$$1.23\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}=\begin{pmatrix}1.23 & 2.46\\3.69 & 4.92\end{pmatrix}.$$

We look at a special kind of square matrix: the **identity matrix of order** n. It is denoted by $\mathbf{I}_n$ and it is a matrix with n rows and columns with 1s on the main diagonal and 0s everywhere else. Thus,

$$\mathbf{I}_2=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \mathbf{I}_3=\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}, \text{ and } \mathbf{I}_4=\begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{pmatrix}.$$

We note that for any matrix $\mathbf{M}$ with n rows and columns,

$$\mathbf{M}\mathbf{I}_n=\mathbf{I}_n\mathbf{M}=\mathbf{M}.$$

A square matrix may have an **inverse**. Consider a square matrix $\mathbf{A}$ with n rows and columns. Then $\mathbf{B}$ is an inverse of $\mathbf{A}$ if

$$\mathbf{A}\mathbf{B}=\mathbf{B}\mathbf{A}=\mathbf{I}_n.$$

For example, consider the matrices

$$\mathbf{A}=\begin{pmatrix}1 & 1 & 0\\0 & 1 & 0\\0 & 1 & 1\end{pmatrix} \text{ and } \mathbf{B}=\begin{pmatrix}1 & -1 & 0\\0 & 1 & 0\\0 & -1 & 1\end{pmatrix}.$$

Note that

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_3$$

so $\mathbf{B}$ is the inverse of $\mathbf{A}$ (and $\mathbf{A}$ is the inverse of $\mathbf{B}$). We leave the verification of this claim as an exercise. We denote the inverse of a square matrix $\mathbf{M}$ by $\mathbf{M}^{-1}$. We note that $\mathbf{I}_n^{-1} = \mathbf{I}_n$ but not prove it here.

One last thing we introduce here is the idea of a **matrix determinant** (or simply the **determinant**). The determinant is only well defined for square matrices. The determinant of a square matrix $\mathbf{A}$ is denoted by $\det(\mathbf{A})$ or just $\det \mathbf{A}$. The rule for the determinant changes as we increase the number of rows and columns in the square matrix, so we only look at small cases.

- If the square matrix only has one row, then its determinant is the only element in the matrix. Thus, if $\mathbf{A} = (a_{1,1})$ then $\det \mathbf{A} = a_{1,1}$.
- If the square matrix has two rows, such as the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then its determinant is $ad - bc$.
- If the square matrix has three rows, for example $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, then its determinant is $aei + bfg + cdh - ceg - bdi - afh$.

An important property of the determinant is that it is a *multiplicative map*: for two square matrices $\mathbf{A}$ and $\mathbf{B}$,

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \times \det(\mathbf{B}).$$

Finally, not all square matrices has an inverse. The necessary and sufficient condition that determines whether a square matrix $\mathbf{M}$ has an inverse is whether $\det \mathbf{M} \neq 0$. That is,

$$\mathbf{M}^{-1} \text{ exists if and only if } \det \mathbf{M} \neq 0.$$

We leave this subsection with a few properties of the determinant that we state but not prove:

- $\det(\mathbf{I}_n) = 1$;
- $\det(\mathbf{M}^{-1}) = (\det \mathbf{M})^{-1}$; and
- $\det(k\mathbf{M}) = k^n \det \mathbf{M}$ for a matrix $\mathbf{M}$ with n rows and columns.

8.5.2 General Linear Group over the Real Numbers

With an introduction of matrices out of the way, we can introduce the first of two important matrix groups: the **General Linear Group of degree** n over the real numbers.

Definition I.8.5.1. *The* ***General Linear Group of degree*** n *over the real numbers is denoted by* $\mathrm{GL}_n(\mathbb{R})$ *and is the group with set*

$$\{\boldsymbol{M} \mid \boldsymbol{M} \text{ is a matrix with } n \text{ rows and columns, and } \det \boldsymbol{M} \neq 0\}$$

under matrix multiplication.

In other words, $\mathrm{GL}_n(\mathbb{R})$ is the group of real-valued matrices with n rows and columns that has an inverse. We show that $\mathrm{GL}_n(\mathbb{R})$ is in fact a group under matrix multiplication.

Proof. We need to prove the four group axioms.

1. **Closure**: Consider two matrices $\mathbf{A}$ and $\mathbf{B}$ that are in $\mathrm{GL}_n(\mathbb{R})$. Then that necessarily means that $\det \mathbf{A} \neq 0$ and $\det \mathbf{B} \neq 0$. Since $\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B})$, thus $\det(\mathbf{AB}) \neq 0$. Therefore $\mathbf{AB}$ is also in $\mathrm{GL}_n(\mathbb{R})$, meaning that it is closed under matrix multiplication.
2. **Associativity**: Consider three matrices $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ in $\mathrm{GL}_n(\mathbb{R})$.
    - Consider $(\mathbf{AB})\mathbf{C}$. Let $\mathbf{R} = \mathbf{AB}$ and $\mathbf{S} = (\mathbf{AB})\mathbf{C}$. Then

$$r_{i,k} = \sum_{l=1}^{n} a_{i,l} b_{l,k} \text{ and } s_{i,j} = \sum_{k=1}^{n} r_{i,k} c_{k,j}$$

which means that

$$s_{i,j} = \sum_{k=1}^{n} \left(\sum_{l=1}^{n} a_{i,l} b_{l,k} \right) c_{k,j} = \sum_{k=1}^{n} \sum_{l=1}^{n} (a_{i,l} b_{l,k}) c_{k,j}.$$

- Now consider $\mathbf{A}(\mathbf{BC})$. Let $\mathbf{R} = \mathbf{BC}$ and $\mathbf{S} = \mathbf{A}(\mathbf{BC})$. Then

$$r_{l,j} = \sum_{k=1}^{n} b_{l,k} c_{k,j} \text{ and } s_{i,j} = \sum_{l=1}^{n} a_{i,l} r_{l,j}$$

which means that

$$s_{i,j} = \sum_{l=1}^{n} a_{i,l} \left(\sum_{k=1}^{n} b_{l,k} c_{k,j} \right) = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{i,l} (b_{l,k} c_{k,j}).$$

Now, multiplication is associative. Thus,

$$(a_{i,l} b_{l,k}) c_{k,j} = a_{i,l} (b_{l,k} c_{k,j})$$

which means

$$\sum_{k=1}^{n} \sum_{l=1}^{n} (a_{i,l} b_{l,k}) c_{k,j} = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{i,l} (b_{l,k} c_{k,j}),$$

thereby proving that matrix multiplication is associative.

3. **Identity**: We note that $\det \mathbf{I}_n = 1 \neq 0$, so $\mathbf{I}_n$ is in $\mathrm{GL}_n(\mathbb{R})$. Since $\mathbf{M}\mathbf{I}_n = \mathbf{I}_n\mathbf{M} = \mathbf{M}$ for any matrix $\mathbf{M}$ in $\mathrm{GL}_n(\mathbb{R})$, thus $\mathbf{I}_n$ is indeed the identity of $\mathrm{GL}_n(\mathbb{R})$.

4. **Inverse**: Let $\mathbf{M}$ be a matrix in $\mathrm{GL}_n(\mathbb{R})$. Consider the matrix $\mathbf{M}^{-1}$. By determinant property, we know that $\det \mathbf{M}^{-1} = (\det \mathbf{M})^{-1}$ and since $\det \mathbf{M} \neq 0$ thus $\det \mathbf{M}^{-1} \neq 0$. Hence $\mathbf{M}^{-1}$ is in $\mathrm{GL}_n(\mathbb{R})$. Now because $\mathbf{M}\mathbf{M}^{-1} = \mathbf{M}^{-1}\mathbf{M} = \mathbf{I}_n$, thus $\mathbf{M}^{-1}$ is the inverse of $\mathbf{M}$ in $\mathrm{GL}_n(\mathbb{R})$.

Thus $\mathrm{GL}_n(\mathbb{R})$ is a group since all four group axioms are satisfied. □

8.5.3 Special Linear Group over the Real Numbers

We look at another group of matrices: the **Special Linear Group of degree** n over the real numbers.

Definition I.8.5.2. *The* ***Special Linear Group of degree*** n *over the real numbers is denoted by* $\mathrm{SL}_n(\mathbb{R})$ *and is the group with set*

$$\{\boldsymbol{M} \mid \boldsymbol{M} \text{ is a matrix with } n \text{ rows and columns, and } \det \boldsymbol{M} = 1\}$$

under matrix multiplication.

One sees clearly that $\mathrm{SL}_n(\mathbb{R})$ is a sub*set* of $\mathrm{GL}_n(\mathbb{R})$: the set of $\mathrm{GL}_n(\mathbb{R})$ requires non-zero determinant while the set of $\mathrm{SL}_n(\mathbb{R})$ requires the determinant to be 1, which obviously satisfies the non-zero determinant requirement. What we want to prove here is that $\mathrm{SL}_n(\mathbb{R})$ is a sub*group* of $\mathrm{GL}_n(\mathbb{R})$. In fact, $\mathrm{SL}_n(\mathbb{R})$ is a *normal* subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Proof. We consider the subgroup test. Clearly $\mathbf{I}_n$ is in $\mathrm{SL}_n(\mathbb{R})$ since its determinant is 1. Hence all we have to check the second condition of the subgroup test.

Let $\mathbf{A}$ and $\mathbf{B}$ be matrices in the set $\mathrm{SL}_n(\mathbb{R})$. This means that

$$\det \mathbf{A} = 1 \text{ and } \det \mathbf{B} = 1.$$

Note that $\det \mathbf{B}^{-1} = (\det \mathbf{B})^{-1} = 1^{-1} = 1$. Thus, $\det \mathbf{A}\mathbf{B}^{-1} = (\det \mathbf{A})(\det \mathbf{B}^{-1}) = 1 \times 1 = 1$ which means that $\mathbf{A}\mathbf{B}^{-1}$ is also in $\mathrm{SL}_n(\mathbb{R})$. Hence by the subgroup test, $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$.

Now let $\mathbf{M}$ be a matrix in $\mathrm{GL}_n(\mathbb{R})$ and $\mathbf{N}$ be a matrix in $\mathrm{SL}_n(\mathbb{R})$. We are to show that $\mathbf{M}\mathbf{N}\mathbf{M}^{-1}$ is in $\mathrm{SL}_n(\mathbb{R})$. Since $\mathbf{M} \in \mathrm{GL}_n(\mathbb{R})$ thus $\det \mathbf{M} \neq 0$, meaning $\det \mathbf{M}^{-1} = (\det \mathbf{M})^{-1} \neq 0$. Also, $\mathbf{N} \in \mathrm{SL}_n(\mathbb{R})$ implies $\det \mathbf{N} = 1$. Hence,

$$\det \mathbf{M}\mathbf{N}\mathbf{M}^{-1} = (\det \mathbf{M})(\det \mathbf{N})(\det \mathbf{M})^{-1} = \det \mathbf{N} = 1$$

which means that $\mathbf{M}\mathbf{N}\mathbf{M}^{-1}$ is in $\mathrm{SL}_n(\mathbb{R})$.

Therefore $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$. □

8.5.4 A Consequence of the Fundamental Homomorphism Theorem

We end this section with a corollary of the Fundamental Homomorphism Theorem regarding these groups of matrices.

For brevity denote $\mathbb{R}^\times$ as the group of non-zero real numbers under multiplication.

Proposition I.8.5.3. $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

Proof. Define the map $\phi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ where $\mathbf{M} \mapsto \det \mathbf{M}$.

- **Homomorphism**: Take $\mathbf{M}, \mathbf{N} \in \mathrm{GL}_n(\mathbb{R})$. Then we have

$$\phi(\mathbf{MN}) = \det \mathbf{MN} = \det(\mathbf{M}) \det(\mathbf{N}) = \phi(\mathbf{M})\phi(\mathbf{N})$$

  which means that ϕ is a homomorphism.

- **Image**: We prove that ϕ is surjective to show that $\operatorname{im} \phi = \mathbb{R}^\times$.

  Suppose $r \in \mathbb{R}^\times$. Then $r^{\frac{1}{n}} \in \mathbb{R}^\times$, and a matrix with $r^{\frac{1}{n}}$ on its main diagonal (written as $r^{\frac{1}{n}}\mathbf{I}_n$ where $\mathbf{I}_n$ is the identity matrix with n rows and columns) is in $\mathrm{GL}_n(\mathbb{R})$. Note that $\det(r^{\frac{1}{n}}\mathbf{I}_n) = \left(r^{\frac{1}{n}}\right)^n \det(\mathbf{I}_n) = r$. Thus there is a pre-image of r inside the codomain $\mathbb{R}^\times$, meaning that ϕ is surjective.

  Hence, $\operatorname{im} \phi = \mathbb{R}^\times$.

- **Kernel**: Note that 1 is the identity in $\mathbb{R}^\times$. Thus

$$\begin{aligned}\ker \phi &= \{\mathbf{M} \in \mathrm{GL}_n(\mathbb{R}) \mid \phi(\mathbf{M}) = 1\} \\ &= \{\mathbf{M} \in \mathrm{GL}_n(\mathbb{R}) \mid \det(\mathbf{M}) = 1\} \\ &= \mathrm{SL}_n(\mathbb{R})\end{aligned}$$

  by definition of the group $\mathrm{SL}_n(\mathbb{R})$.

By the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**), we have

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times,$$

proving the claim. □

8.6 Automorphism Groups

8.6.1 Group of Automorphisms of G

We look at automorphisms, an important type of map that we look in Group Theory.

Definition I.8.6.1. *An **automorphism** of a group G is an isomorphism from a group G to itself. That is, $\phi : G \to G$ is an automorphism if ϕ is an isomorphism.*

Clearly, from this definition, the identity function id is an automorphism.

We now look at the group of automorphisms of a group G.

Definition I.8.6.2. *Let G be a group. The **group of automorphisms of** G, denoted $\mathrm{Aut}(G)$, is given by*

$$\mathrm{Aut}(G) = \{\phi : G \to G \mid \phi \text{ is an isomorphism}\}$$

under function composition (denoted by $\circ$).

We prove that $\mathrm{Aut}(G)$ is indeed a group.

Proof. We look at the four group axioms.

- **Closure**: If $f, g \in \mathrm{Aut}(G)$, and $h = fg$, then $h : G \to G$ is a bijection. Furthermore h is a homomorphism since

  $$h(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) = h(x)h(y)$$

  so h is an isomorphism, meaning $h = fg \in \mathrm{Aut}(G)$.
- **Associativity**: Function composition is associative.
- **Identity**: As mentioned above, the identity isomorphism $\mathrm{id} : G \to G, g \mapsto g$ is in $\mathrm{Aut}(G)$. By definition of id, $f \circ \mathrm{id} = f$ and $\mathrm{id} \circ f = f$, so id is indeed the identity in $\mathrm{Aut}(G)$.
- **Inverse**: Suppose $f \in \mathrm{Aut}(G)$. Then f is an isomorphism. By **Theorem I.4.4.1**, $f^{-1} : G \to G$ is also an isomorphism, so

$f^{-1} \in \mathrm{Aut}(G)$. Recall also that

$$f \circ f^{-1} = \mathrm{id} \text{ and } f^{-1} \circ f = \mathrm{id}$$

so f^{-1} is indeed the identity of f.

Since the four group axioms are satisfied, thus $\mathrm{Aut}(G)$ is a group under function composition. □

8.6.2 Group of Inner Automorphisms of G

We now look at inner automorphisms and its group.

Definition I.8.6.3. *An **inner automorphism** of a group G is an automorphism $\iota : G \to G$ such that $\iota(x) = gxg^{-1}$ for some fixed $g \in G$.*

Definition I.8.6.4. *Let G be a group. The **group of inner automorphisms of** G, $\mathrm{Inn}(G)$, is given by*

$$\mathrm{Inn}(G) = \{\iota_g : G \to G \mid \iota_g(x) = gxg^{-1}, g \in G\}$$

under function composition (denoted by $\circ$).

We prove that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

Proof. Clearly $\mathrm{id} \in \mathrm{Inn}(G)$ since $\mathrm{id} = \iota_e$ and $\mathrm{id}(x) = \iota_e(x) = exe^{-1} = x$. Hence $\mathrm{Inn}(G)$ is non-empty and, furthermore, $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$.

Now take $\iota_x, \iota_y \in \mathrm{Inn}(G)$. Note that $(\iota_y)^{-1} = \iota_{y^{-1}}$ since

$$(\iota_y)\left(\iota_{y^{-1}}\right)(g) = (\iota_y)\left(y^{-1}gy\right) = y\left(y^{-1}gy\right)y^{-1} = g$$

which means $(\iota_y)\left(\iota_{y^{-1}}\right) = \mathrm{id}$. Therefore $\iota_x\,(\iota_y)^{-1} = \iota_{xy^{-1}}$ since

$$\begin{aligned}
\iota_x\,(\iota_y)^{-1}(g) &= \iota_x\iota_{y^{-1}}(g) \\
&= \iota_x\left(y^{-1}gy\right) \\
&= xy^{-1}gyx^{-1} \\
&= xy^{-1}g(xy^{-1})^{-1} \\
&= \iota_{xy^{-1}}
\end{aligned}$$

which means that $\iota_x (\iota_y)^{-1} = \iota_{xy^{-1}} \in \mathrm{Inn}(G)$.

Hence, by subgroup test, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. □

Exercise I.8.13. Let G be a group. Prove that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

8.6.3 A Consequence of the Fundamental Homomorphism Theorem

Before we can state the consequence, we revisit the idea of the center of a group as introduced in **Example I.3.2.3**.

The center of a group G is the normal subgroup

$$\mathrm{Z}(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}.$$

In other words, $\mathrm{Z}(G) = \{z \in G \mid z = gzg^{-1} \text{ for all } g \in G\}$.

Proposition I.8.6.5. $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$.

Proof. We define $\phi : G \to \mathrm{Inn}(G), g \mapsto \iota_g$ where $\iota_g(x) = gxg^{-1}$.

- **Homomorphism**: Let $g, h \in G$. Then for any $x \in G$,

$$\begin{aligned}(\phi(gh))(x) = \iota_{gh}(x) &= (gh)x(gh)^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= g(hxh^{-1})g^{-1} \\ &= g(\iota_h(x))g^{-1} \\ &= \iota_g(\iota_h(x)) \\ &= (\iota_g \circ \iota_h)(x) \\ &= (\phi(g)\phi(h))(x)\end{aligned}$$

  which means that ϕ is a homomorphism.

- **Image**: We show that ϕ is surjective to prove that $\mathrm{im}\ \phi = \mathrm{Z}(G)$. Suppose $\iota_g \in \mathrm{Inn}(G)$. Clearly $\phi(g) = \iota_g$ which means that ϕ is surjective.

- **Kernel**: Note that $\ker\phi = \{g \in G \mid \phi(g) = \mathrm{id}\}$. So, if $g \in \ker\phi$ then $(\phi(g))(x) = \iota_g(x) = \mathrm{id}(x) = x$ for all $x \in G$. This means that $gxg^{-1} = x \implies gx = xg$ for all $x \in G$, so $g \in \mathrm{Z}(G)$. Hence $\ker\phi = \mathrm{Z}(G)$.

Hence, by the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**),

$$G/\ker\phi \cong \mathrm{im}\ \phi \implies G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$$

which proves the result. □

8.7 Problems

Problem I.8.1. By considering the group $\mathbb{Z}_{10101}$, find the smallest positive integers a and b such that

(a) $1870a$ is a multiple of 10101.

(b) $3774b$ is a multiple of 10101.

Problem I.8.2. Find the largest integer n such that A_n is abelian, proving your claim. Hence find all integers k such that A_k is cyclic.

Problem I.8.3. Suppose r is an odd primitive root modulo p^k, where p is an odd prime and $k \geq 1$. Prove that r is also a primitive root modulo $2p^k$.

Problem I.8.4. Let G be a finite cyclic group of order n and generator g.

(i) Suppose $f : G \to G$ and $h : G \to G$ are homomorphisms. Prove that $f = h$ if and only if $f(g) = h(g)$.

(ii) Let $f : G \to G$ be a homomorphism. Explain why $f(g) = g^{m_f}$ where m_f is a integer unique to f.

(iii) Suppose $f : G \to G$ and $h : G \to G$ are homomorphisms. Prove that $m_{f \circ h} = m_f \otimes_n m_h$, where $\circ$ denotes function composition and $\otimes_n$ denotes multiplication modulo n.

(iv) Let $f : G \to G$ be a homomorphism. Prove that f is an automorphism if and only if m_f has a multiplicative inverse modulo n. That is, there exists $k \in \mathcal{U}_n$ such that $m_f k \equiv 1 \pmod{n}$ if and only if f is an automorphism.
(*Hint: consider* ***Proposition 0.4.0.2****, where* $ab \equiv 1 \pmod{m}$ *if and only if* $\gcd(a, m) = 1$.)

(v) Hence, by considering the map $\phi : \mathrm{Aut}(G) \to \mathcal{U}_n$ where $f \mapsto m_f$, prove $\mathrm{Aut}(G) \cong \mathcal{U}_n$.

9 Group Actions

9.1 Definition and Examples

A group action is a representation of the elements of a group as symmetries of a set. Many groups have a 'natural' group action coming from their construction. For example, the dihedral group of order 6, D_3, acts on the vertices of an equilateral triangle because the group is given as a set of symmetries of the equilateral triangle, by definition. A group action of a group on a set is a generalization of this idea, which can be used to derive useful facts about the group and the set it acts on.

Definition I.9.1.1. *Let G be a group, e be the identity in G, and X be a set. A **group action of** G **on** X is a function $\alpha : G \times X \to X$ satisfying the following conditions.*

- ***Identity**: $\alpha(e, x) = x$ for all $x \in X$.*
- ***Compatibility**: $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for all $g, h \in G$ and $x \in X$.*

Remark. Some sources will use f (e.g. [Bri]) or ϕ (e.g. [Row]) as the group action.

In this case, the group G is called a **transformation group** and X is called a **G-set**.

When the action is 'obvious', the function $\alpha(g, x)$ is often written as $g \cdot x$ instead. Note that we **will** write the dot in this book. With this notation, the axioms above become:

- $e \cdot x = x$ for all $x \in X$; and
- $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

Example I.9.1.2. Consider $G = \mathrm{S}_n$ and the set $X = \{1, 2, 3, \ldots, n\}$. Then G acts on X by the function α such that $\alpha(g, x) = g(x)$. That is, $g \cdot x = g(x)$ in this case. We note that the axioms are satisfied:

- **Identity**: $\mathrm{id} \cdot x = \mathrm{id}(x) = x$.
- **Compatibility**: $g \cdot (h \cdot x) = g(h(x)) = (g \circ h)(x) = (gh) \cdot x$.

Example I.9.1.3. Let G be any group and the function $\alpha : G \times G \to G$ be defined such that $\alpha(g, x) = gx$. We show that α is a group action of G on G:

- **Identity**: $e \cdot x = ex = x$.
- **Compatibility**: $g \cdot (h \cdot x) = g \cdot (hx) = ghx = (gh)x = (gh) \cdot x$.

Exercise I.9.1. Let G be a group and the function $\alpha : G \times G \to G$ be defined such that $\alpha(g, x) = gxg^{-1}$. Show that α is a group action of G on G.

We note that there is an equivalent definition of a group action from G to X.

Definition I.9.1.4. *Let G be a group and X be a set. Then a group action of G on X is a homomorphism $\phi : G \to \mathrm{Sym}(X)$.*

Theorem I.9.1.5. ***Definition I.9.1.1*** *and* ***Definition I.9.1.4*** *are equivalent.*

Proof. We first work forwards, assuming **Definition I.9.1.1** holds and proving **Definition I.9.1.4** holds as well. Assume $\alpha : G \times X \to X$ is a group action. Define $\psi : G \to \mathrm{Sym}(X)$ by $g \mapsto f_g$ where $f_g : X \to X, x \mapsto \alpha(g, x)$. We show that f_g is in fact a bijection.

- **Injective**: Suppose there exists $x, y \in X$ such that $f_g(x) = f_g(y)$. Then

$$\begin{aligned} x &= \alpha(e, x) \\ &= \alpha(g^{-1}g, x) \\ &= \alpha(g^{-1}, \alpha(g, x)) \\ &= \alpha(g^{-1}, f_g(x)) \\ &= \alpha(g^{-1}, f_g(y)) \\ &= \alpha(g^{-1}, \alpha(g, y)) \\ &= \alpha(g^{-1}g, y) \\ &= \alpha(e, y) \\ &= y \end{aligned}$$

  which proves that f_g is injective.

- **Surjective**: Suppose $y \in X$. We note that $\alpha(g^{-1}, y) \in X$ by definition of α. Hence observe that $f_g(\alpha(g^{-1}, y)) = \alpha(g, \alpha(g^{-1}, y)) = y$, which means that any element $y \in X$ has a pre-image in X. This shows that f_g is surjective.

Hence f_g is a bijection from X to X, which means $f_g \in \mathrm{Sym}(X)$. We just need to show that ψ is a homomorphism. Take $x \in X$, and let $g, h \in G$. Then

$$\begin{aligned} (\psi(gh))(x) &= f_{gh}(x) \\ &= \alpha(gh, x) \\ &= \alpha(g, \alpha(h, x)) \\ &= \alpha(g, f_h(x)) \\ &= f_g(f_h(x)) \\ &= (f_g \circ f_h)(x) \\ &= (\psi(g)\psi(h))(x) \end{aligned}$$

for any $x \in X$, which means $\psi(gh) = \psi(g)\psi(h)$. Hence ϕ is indeed a homomorphism, satisfying **Definition I.9.1.4**.

We now work in the reverse direction, assuming **Definition I.9.1.4** holds and proving **Definition I.9.1.1** holds as well. Suppose $\phi : G \to \mathrm{Sym}(X)$ is a group homomorphism. We define $\beta : G \times X \to X$ where $\beta(g, x) = (\phi(g))(x)$. We verify **Definition I.9.1.1** holds for β.

- **Identity**: Since ϕ is a homomorphism, it must map the identity in G to the identity in $\mathrm{Sym}(X)$, which is id. Hence, $\beta(e, x) = (\phi(e))(x) = \mathrm{id}(x) = x$.
- **Compatibility**: Let $g, h \in G$ and $x \in X$. Then

$$\begin{aligned}\beta(g, \alpha(h, x)) &= \beta(g, (\phi(h))(x)) \\ &= (\phi(g))((\phi(h))(x)) \\ &= (\phi(g) \circ \phi(h))(x) \\ &= (\phi(gh))(x) \\ &= \beta(gh, x).\end{aligned}$$

Therefore **Definition I.9.1.1** holds for β.

The final thing to prove equivalence of the definitions is to show that the above processes are 'inverses' of each other. That is, we want to show that

- if we start with α, derive ψ based on α, and then derive β based off ψ, then $\alpha = \beta$; and
- if we start with ϕ, derive β, and then derive ψ based off β, then $\phi = \psi$.

Suppose we have an α that is used to derive a ψ which is in turn used to derive β. Then the above processes yields

$$\psi(g) = f_g \text{ and } \beta(g, x) = (\psi(g))(x)$$

where $f_g(x) = \alpha(g, x)$. Hence $\alpha(g, x) = f_g(x) = (\psi(g))(x) = \beta(g, x)$ for any $g \in G$ and $x \in X$. Hence $\alpha = \beta$.

Now suppose we have a ϕ that is used to derive a β which is in turn used to derive a ψ. Then the above processes yields

$$\beta(g, x) = (\phi(g))(x) \text{ and } \psi(g) = f_g$$

where $f_g(x) = \beta(g, x)$ in this case. Hence $(\phi(g))(x) = \beta(g, x) = f_g(x) = (\psi(g))(x)$ for any $g \in G$ and $x \in X$. Hence $\phi = \psi$.

Therefore, this shows that the maps $\alpha \mapsto \phi$ and $\phi \mapsto \alpha$ are inverses of each other, so we have a one-to-one correspondence between **Definition I.9.1.1** and **Definition I.9.1.4**. □

Remark. What this theorem also shows is that a group action α induces a group homomorphism $\phi : G \to \mathrm{Sym}(X)$. In addition, if X is finite with n elements, a homomorphism $\phi : G \to \mathrm{S}_n$ exists (since $\mathrm{Sym}(X) \cong \mathrm{S}_n$ by **Proposition I.5.2.5**).

9.2 Fixed Points, Stabilizers, and Orbits

We first look at the definition of a **fixed point** in relation to group actions.

Definition I.9.2.1. *Let G be a group acting on a set X. A **fixed point of** $g \in G$ is an element $x \in X$ such that $g \cdot x = x$.*

Example I.9.2.2. Consider the group $G = \{\mathrm{id}, g\}$ (where $g^2 = \mathrm{id}$) and the set $X = \mathbb{Z}$. Let G act on X by the formulae $\mathrm{id} \cdot x = x$ and $g \cdot x = -x$. We find the fixed points of every element in G.

- For id, every element in X is a fixed point of it.
- For g, there is only one fixed point 0 since $g \cdot 0 = -0 = 0$.

Exercise I.9.2. Let $X = \{1, 2, 3\}$, and let S_3 act on X. What are the fixed points of each of the 6 actions in S_3?

With an understanding of fixed points, we can now look at the **stabilizer** of an element in X.

Definition I.9.2.3. *Let G be a group acting on a set X, and suppose $x \in X$. The **stabilizer of** x **by** G, denoted $\mathrm{Stab}_G(x)$, is the set of $g \in G$ such that x is a fixed point of g.*

Remark. Some authors will denote the stabilizer of x by G by G_x (e.g. [Cla84], [Hum96], [Bri]).

Example I.9.2.4. Consider again the group $G = \{\mathrm{id}, g\}$ and the set $X = \mathbb{Z}$ with relations defined in the above example.

- Let's find the stabilizer of 0, $\mathrm{Stab}_G(0)$. Thus we are finding the set of $f \in G$ such that 0 is a fixed point of f. Note that $\mathrm{id} \cdot 0 = 0$ and $g \cdot 0 = -0 = 0$, so the entirety of G forms the stabilizer of 0, i.e. $\mathrm{Stab}_G(0) = G$.
- Now consider the stabilizer of any non-zero integer in X, say $x \in X$. We are finding the set of $f \in G$ such that x is a fixed point of f. Note that $g \cdot x = -x \neq x$. Thus, the only element in G such makes x a fixed point is id, i.e. $\mathrm{Stab}_G(x) = \{e\}$ if $x \neq 0$.

To summarise, $\mathrm{Stab}_G(0) = G$ and $\mathrm{Stab}_G(x) = \{e\}$ if $x \neq 0$.

Exercise I.9.3. Let $X = \{1, 2, 3\}$, and let S_3 act on X. What are the stabilizers of each of the 3 elements in X?

What you might notice from the above example and exercise is that the stabilizers are subsets of the original group G. In fact, we will prove that the stabilizer is a subgroup of G.

Lemma I.9.2.5. *Let G be a group that acts on a set X. Then for any $x \in X$, $\mathrm{Stab}_G(x) \leq G$.*

Proof. We consider the subgroup test.

We note $e \in G$. From the group action axiom of **Identity**, we know that $e \cdot x = x$. Thus, for an element x, $e \in \mathrm{Stab}_G(x)$. Hence $\mathrm{Stab}_G(x)$ is non-empty.

Now consider $g, h \in \mathrm{Stab}_G(x)$. This means that $g \cdot x = x$ and $h \cdot x = x$.

We note that $h^{-1} \in \mathrm{Stab}_G(x)$ since

$$\begin{aligned} h^{-1} \cdot x &= h^{-1} \cdot (h \cdot x) && (\text{since } h \in \mathrm{Stab}_G(x), \text{ thus } h \cdot x = x) \\ &= (h^{-1}h) \cdot x && (\text{by } \textbf{Compatibility} \text{ Axiom}) \\ &= e \cdot x \\ &= x. \end{aligned}$$

Now consider gh^{-1}.

$$\begin{aligned} (gh^{-1}) \cdot x &= g \cdot (h^{-1} \cdot x) && (\text{by } \textbf{Compatibility} \text{ Axiom}) \\ &= g \cdot x && (\text{since } h^{-1} \in \mathrm{Stab}_G(x)) \\ &= x && (\text{since } g \in \mathrm{Stab}_G(x)) \end{aligned}$$

which means that $gh^{-1} \in \mathrm{Stab}_G(x)$.

Thus, by subgroup test, $\mathrm{Stab}_G(x) \leq G$ for any $x \in X$. □

Exercise I.9.4. Let G be a group that acts on a set X. Prove that $g \cdot x = h \cdot x$ if and only if $g^{-1}h \in \mathrm{Stab}_G(x)$.

We finally look at the definition of the **orbit** of an element in X.

Definition I.9.2.6. *Let G be a group acting on a set X, and suppose $x \in X$. The **orbit of** x **in** G, denoted* $\mathrm{Orb}_G(x)$*, is the set of elements $y \in X$ such that $g \cdot x = y$ for some $g \in G$.*

Remark. Some authors will denote the orbit of x in G by $G \cdot x$ (e.g. [Cla84]) or simply by Gx (e.g. [Mil21]).

Example I.9.2.7. Consider again the group $G = \{\mathrm{id}, g\}$ and let G act on the set $X = \mathbb{Z}$ with $g^2 = \mathrm{id}$, $\mathrm{id} \cdot x = x$ and $g \cdot x = -x$. Note that the orbit for any non-zero element $x \in X$ is the set $\{x, -x\}$, while the orbit for 0 is $\{0\}$ itself.

We say that a group action is **transitive** if and only if it has one orbit. That is to say, the group action is transitive if there exists $x \in X$ such that $\mathrm{Orb}_G(x) = X$.

Exercise I.9.5. Let G be a group that acts on a non-empty set X. Show that if the group action is transitive if and only if $\mathrm{Orb}_G(x) = X$ for **all** $x \in X$.

Exercise I.9.6. Let G be a group that acts on a non-empty set X. Prove that

(a) every element in X is in some orbit; and

(b) if $\mathrm{Orb}_G(x_1) \cap \mathrm{Orb}_G(x_2) \neq \varnothing$ where $x_1, x_2 \in X$, then $\mathrm{Orb}_G(x_1) = \mathrm{Orb}_G(x_2)$.

(That is, prove that distinct orbits partition X.)

9.3 The Orbit-Stabilizer Theorem

There is a natural relationship between orbits and stabilizers of a group action. We give the intuition of the theorem before stating it formally.

Let's think about the symmetric group of a cube (let's call it G) and suppose G acts on the set of faces of the cube, F. How many elements are there in G? We could do the following:

1. Fix one face (say the top face). There are 4 ways to move the cube because you can only rotate the cube now. These are the stabilizers.
2. Now there are 6 possible choices for which face to be fixed. This is the 'orbit'.

Thus, the total number of elements in the symmetric group of a cube, $|G| = 4 \times 6$. Generally, the number of elements of a transformation group G is the product of the orders of the stabilizer and orbit of an element x in the G-set.

Formally, this is captured in the **Orbit-Stabilizer Theorem**.

Theorem I.9.3.1 (Orbit-Stabilizer)**.** *Let G be a group that acts on a finite set X. Take $x \in X$. Then*

$$|G| = |\mathrm{Stab}_G(x)| \times |\mathrm{Orb}_G(x)|,$$

that is, the order of the group G is the product of the order of the stabilizer of x and the number of elements in the orbit of x.

Proof (see [Hum96]). We consider the map $f_x : G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x)$ given by $g\mathrm{Stab}_G(x) \mapsto g \cdot x$ (note that f_x is *not* a homomorphism as $\mathrm{Orb}_G(x)$ is not a group). We prove that f_x is a well-defined bijection.

- **Well-defined**: Suppose we have $g, h \in G$ such that $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$. By Coset Equality (**Lemma I.3.3.3**), this means that $g^{-1}h \in \mathrm{Stab}_G(x)$. Furthermore, by **Exercise I.9.4**, this means that $g \cdot x = h \cdot x$. Hence, $f_x(g\mathrm{Stab}_G(x)) = f_x(h\mathrm{Stab}_G(x))$, meaning that f_x is well-defined.
- **Injective**: Suppose we have $g, h \in G$ such that $f_x(g\mathrm{Stab}_G(x)) = f_x(h\mathrm{Stab}_G(x))$, meaning $g \cdot x = h \cdot x$. By **Exercise I.9.4**, this means that $g^{-1}h \in \mathrm{Stab}_G(x)$. By Coset Equality (**Lemma I.3.3.3**), this further means that $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$. Thus f_x is injective.
- **Surjective**: Suppose $y \in \mathrm{Orb}_G(x)$. This means that there exists $g \in G$ such that $g \cdot x = y$. Note $f_x(g\mathrm{Stab}_G(x)) = g \cdot x = y$ by definition of f_x. Hence, the pre-image of y is $g\mathrm{Stab}_G(x)$, meaning that f_x is surjective.

Hence f_x is a bijection from $G/\mathrm{Stab}_G(x)$ to $\mathrm{Orb}_G(x)$. Therefore, $|\mathrm{Orb}_G(x)| = |G/\mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$ by Lagrange's Theorem (**Theorem I.3.4.4**). This quickly implies $|G| = |\mathrm{Stab}_G(x)| \times |\mathrm{Orb}_G(x)|$. □

Exercise I.9.7. Let $G = \mathrm{S}_n$ be a transformation group and $X = \{1, 2, 3, \ldots, n\}$ be a G-set.

(i) Show that the group action is transitive.

(ii) Find the order of the stabilizer of n by G.

9.4 Burnside's Lemma

Burnside's lemma gives a way to count the number of orbits of a finite set acted on by a finite group. Before we get into it, we look at the **set of orbits of** X.

Definition I.9.4.1. *The* ***set of orbits*** *acted upon by the group G is the set*

$$X/G = \{\mathrm{Orb}_G(x) \mid x \in X\}.$$

In other words, X/G is the set of distinct orbits over all elements of X.

Remark. The number of orbits is given by the number of elements of the set X/G, i.e. $|X/G|$.

We are now ready to state and prove Burnside's lemma.

Lemma I.9.4.2 (Burnside)**.** *Let G be a finite group acting on a set X. Let the set $\mathrm{Fix}_X(g)$ denotes the set of all elements in X which is fixed by g, that is,*

$$\mathrm{Fix}_X(g) = \{x \in X \mid g \cdot x = x\}.$$

Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|.$$

In other words, the number of orbits equals the average number of fixed elements.

Proof (see [Pro21]). We start by noting that

$$\begin{aligned}
\sum_{g \in G} |\mathrm{Fix}_X(g)| &= \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}| \\
&= |\{(g, x) \mid g \in G,\ x \in X \text{ such that } g \cdot x = x\}| \\
&= \sum_{x \in X} |\{g \in G \mid g \cdot x = x\}| \\
&= \sum_{x \in X} |\mathrm{Stab}_G(x)|.
\end{aligned}$$

By Orbit-Stabilizer theorem (**Theorem I.9.3.1**), $|\mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Orb}_G(x)|}$. Thus,

$$\begin{aligned}\sum_{x\in X} |\mathrm{Stab}_G(x)| &= \sum_{x\in X} \frac{|G|}{|\mathrm{Orb}_G(x)|} \\ &= |G| \sum_{x\in X} \frac{1}{|\mathrm{Orb}_G(x)|}.\end{aligned}$$

We notice that X is the disjoint union of all its orbits in X/G (by **Exercise I.9.6**), which means the sum over X may be broken up into separate sums over each individual orbit. Thus,

$$\begin{aligned}\sum_{x\in X} \frac{1}{|\mathrm{Orb}_G(x)|} &= \sum_{\mathrm{Orb}_G(x)\in X/G} \left(\sum_{x\in \mathrm{Orb}_G(x)} \frac{1}{|\mathrm{Orb}_G(x)|} \right) \\ &= \sum_{\mathrm{Orb}_G(x)\in X/G} 1 \\ &= |X/G|.\end{aligned}$$

Putting everything together,

$$\sum_{g\in G} |\mathrm{Fix}_X(g)| = |G||X/G|$$

which the result follows immediately. □

Example I.9.4.3. We consider the number of distinct possible colourings of the corners on a square with n colours (up to rotation) using Burnside's Lemma.

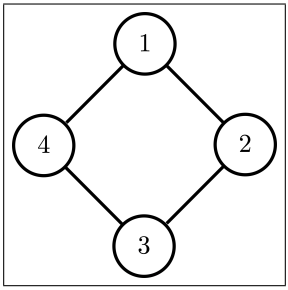


Figure 9.1: Square With Labelled Corners

Let X denote the set of colourings of the corners of the square, and let G denote the rotation group acting on X. Then two elements of X belong to the same orbit precisely when one is simply a rotation of the other. We note that G consists of 4 rotations.

1. Rotating the square $0°$ does not change the colourings at all, which means that the number of fixed points is the total number of possible colourings, which is n^4.
2. Rotating the square $90°$ results in all points affecting one another, so the only fixed points would be colourings of all the same color. Since there are n different colours, thus the number of fixed points is n.
3. Rotating the square $180°$ swaps two pairs of vertices that are across from each other. Thus, a fixed point will occur if the two pairs have the same colour. hence, there are n^2 fixed points.
4. Finally, rotating the square $270°$ is similar to rotating $90°$, so there are n fixed points.

Now there are 4 elements in G, so $|G| = 4$. By Burnside's Lemma,

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_X(g)| = \frac{1}{4}(n^4 + n + n^2 + n),$$

i.e., the number of distinct possible colourings of the corners on a square with n colours (up to rotation) is $\frac{n}{4}(n^3 + n + 2)$.

9.5 Conjugacy Classes

Before we look at the most important part of this chapter, the Class Equation, we look at the idea of conjugacy as a group action.

Definition I.9.5.1. *Let G be a group, and suppose $a, b \in G$. Then we say that b is a **conjugate** of a if there is an element $g \in G$ such that $b = gag^{-1}$ (or, alternatively, $a = g^{-1}bg$).*

We can frame this idea in terms of group actions.

Consider the function $\phi : G \times G \to G$ such that $\phi(g, x) = gxg^{-1}$. We showed that ϕ is a group action in **Exercise I.9.1**. Let's look at the orbit and stabilizer of an arbitrary element $x \in G$ under this group action.

- For orbits, we are to find $y \in G$ such that there exists a $g \in G$ such that $gxg^{-1} = y$. Hence, the orbit of x under this group action are the conjugates of x.
- For the stabilizer, we are to find elements $g \in G$ such that $gxg^{-1} = x$. Hence we find $gx = xg$. Therefore, $g \in \mathrm{C}_G(x)$ where $\mathrm{C}_G(x)$ is the centralizer of x (recall how it is defined in **Example I.3.2.2**).

Hence, under conjugation, $\mathrm{Orb}_G(x) =$ Conjugates of x, and $\mathrm{Stab}_G(x) = \mathrm{C}_G(x)$.

We can now look at conjugacy classes.

Definition I.9.5.2. *Let G be a group and take $x \in G$. The* ***conjugacy class of*** *x is the set*

$$\mathrm{Cl}(x) = \{gxg^{-1} \mid g \in G\}.$$

In other words, the set $\mathrm{Cl}(x)$ is a subset of G where all elements inside it are conjugates of each other.

Remark. We omit having the subscript of G for the conjugacy class since $x \in G$. Also, under the group action of conjugation, $\mathrm{Orb}_G(x) = \mathrm{Cl}(x)$.

Example I.9.5.3. We look at conjugacy classes of the group S_3.

- The first is the conjugacy class of the identity, id.

  $$\mathrm{Cl}(\mathrm{id}) = \{g \circ \mathrm{id} \circ g^{-1} \mid g \in G\} = \{\mathrm{id}\}.$$

  Thus the conjugacy class of the identity consists of only the identity.

- The second is the conjugacy class of transpositions. Let $\tau = \begin{pmatrix} a & b \end{pmatrix}$ be a transposition in S_3. Then

  $$\mathrm{Cl}(\tau) = \{g \circ \tau \circ g^{-1} \mid g \in G\}.$$

  Running through all 6 elements of S_3 reveals that $\mathrm{Cl}(\tau)$ is the set of all transpositions, i.e. the conjugacy class of transpositions is the set of transpositions.

- The third is the conjugacy class of 3-cycles. Let $\sigma = \begin{pmatrix} a & b & c \end{pmatrix}$ be a 3-cycle in S_3. One can see that $\mathrm{Cl}(\sigma)$ is the set of all 3-cycles.

Exercise I.9.8. Let G be a group and $x \in G$. Prove that

$$|\mathrm{Cl}(x)| = [G : \mathrm{C}_G(x)].$$

9.6 The Class Equation

The example of the previous section illustrates that the sum of the sizes of the conjugacy classes must be equal to the size of the group. This fact, along with the Orbit-Stabilizer theorem (**Theorem I.9.3.1**), can be used to derive an important equation known as **the class equation**.

Before we state and prove the class equation, we recall the idea of the center of a group as introduced in **Example I.3.2.3**.

The center of a group G is the normal subgroup

$$\mathrm{Z}(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}.$$

In other words, $\mathrm{Z}(G) = \{z \in G \mid z = gzg^{-1} \text{ for all } g \in G\}$.

We now state and prove the class equation.

Theorem I.9.6.1 (Class Equation)**.** *Let G be a finite group. Suppose G has k conjugacy classes, with l of them having more than 1 element. Suppose $g_1, g_2, \ldots, g_l$ are representatives of the conjugacy classes with more than 1 element. Then*

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} [G : \mathrm{C}_G(g_i)],$$

*which is known as **the class equation**.*

Proof. We know by **Exercise I.9.6** that distinct orbits partitions the set that the group is acting on. Hence, using the group action of conjugation, orbits under conjugation partition G. Hence,

$$G = \bigcup_{i=1}^{k} \mathrm{Orb}_G(\hat{g}_i) = \bigcup_{i=1}^{k} \mathrm{Cl}(\hat{g}_i)$$

where $\hat{g}_i$s are representatives of the k conjugacy classes (including those with only 1 element).

Suppose now that an element x has a conjugacy class with one element. This means that $gxg^{-1} = x$ for all $g \in G$. Hence, this means that $x \in \mathrm{Z}(G)$.

Therefore, one concludes that

$$G = (\mathrm{Z}(G)) \cup \left(\bigcup_{i=1}^{l} \mathrm{Cl}(g_i) \right).$$

Since this is a disjoint union, hence

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} |\mathrm{Cl}(g_i)|.$$

Finally, by **Exercise I.9.8**, $|\mathrm{Cl}(g_i)| = [G : \mathrm{C}_G(g_i)]$ which means that

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} [G : \mathrm{C}_G(g_i)],$$

proving the theorem. □

We look at one application of the class equation. Before that, we introduce the idea of p-**groups**.

Definition I.9.6.2. *A p-**group** G is a finite group with order p^n where p is prime and n is a positive integer.*

An immediate consequence of this is that every element must have an order that is a power of p, i.e. for any element $x \in G$, $|x| = p^k$ where $1 \leq k \leq n$.

Example I.9.6.3. Let G be a finite p-group, meaning $|G| = p^n < \infty$. We will show that G has a non-trivial center using the class equation.

We recall that $|\mathrm{Cl}(x)| = \frac{|G|}{|\mathrm{C}_G(x)|}$ by **Exercise I.9.8**. Hence, the order of the group must divide the order of any conjugacy class, i.e. $\frac{|G|}{|\mathrm{C}_G(x)|} \mid |G|$. Since $|G| = p^n$, it follows that $|\mathrm{Cl}(x)| = p^k$ for some $1 \leq k \leq n$ (assuming $x \notin \mathrm{Z}(G)$).

If $g_1, g_2, \ldots, g_l$ are representatives from the conjugacy classes with more than 1 element, then this means that

$$p^n = |G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} |\mathrm{Cl}(g_i)| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} p^{k_i}$$

where $1 \leq k_1, k_2, \ldots, k_l < n$. From this, we conclude that p must divide $|\mathrm{Z}(G)|$, meaning $|\mathrm{Z}(G)| > 1$.

Example I.9.6.4. We look at the class equation of the symmetric group of degree 3, S_3.

We recall from **Example I.9.5.3** that the conjugacy classes of S_3 are

$$\begin{aligned}
&\mathrm{Cl}(\mathrm{id}) = \{\mathrm{id}\} \\
&\mathrm{Cl}(\tau) = \{\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}\} \\
&\mathrm{Cl}(\sigma) = \{\begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}\}
\end{aligned}$$

where τ is a 2-cycle (transposition) and σ is a 3-cycle. Thus, the class equation of S_3 is

$$6 = 1 + 2 + 3$$

where $|\mathrm{Z}(\mathrm{S}_3)| = |\{e\}| = 1$.

Exercise I.9.9. The Cayley table of D_3 is in **Example I.2.5.1**.

(a) Find $\mathrm{Z}(D_3)$, the center of D_3.

(b) Find the conjugacy classes of D_3 with more than 1 element.

(c) Find the class equation of D_3.

9.7 Cauchy's Theorem

To end this chapter, we prove **Cauchy's Group Theorem**.

Theorem I.9.7.1 (Cauchy)**.** *Let G be a finite group such that $|G| = np$ where p is a prime and n is a positive integer. Then G contains an element of order p.*

Proof. We proceed with strong induction on n.

For the case where $n = 1$, $|G| = p$. Then by **Exercise I.3.6**, every element of the group has order p. Hence we proved the base case.

We now assume that the statement holds for all $n \leq k$ for some positive integer k. We need to prove the case for $k + 1$, that is, assuming that $|G| = (k + 1)p$. We split the proof into two cases.

The first case is when G is abelian. Take any non-identity element x, and define $H = \langle x \rangle \leq G$.

- If p divides $|H|$, say $|H| = mp$ where m is a positive integer, then x^m is an element of order p (since $(x^m)^p = x^{|H|} = e$). Hence we find an element with order p.
- If p does not divide $|H|$, then p must divide $[G : H] = |G/H| = \frac{|G|}{|H|}$ since p divides $|G| = kp$. Note that $H \lhd G$ since G is abelian (**Proposition I.3.5.2**). Hence G/H is a group. If $|x| = m$, then $(xH)^m = (x^m)H = eH = H \in G/H$. Thus, m is a multiple of $|G/H|$ (**Corollary I.3.4.4.1**) which is in turn a multiple of p. Hence p divides m. As before, $x^{\frac{m}{p}}$ is an element with order p (since $\left(x^{\frac{m}{p}}\right)^p = x^m = e$).

Therefore, for the abelian case, there exists an element with order equal to p.

We now consider the case when G is non-abelian. We assume by contradiction that G does not have an element of order p. Let $H \leq G$ be a proper subgroup. By the assumption, H has no element with order p. Therefore the contrapositive of the induction hypothesis means that $|H|$ is not a multiple of p. Note that Lagrange's Theorem (**Theorem**

I.3.4.4) further explains that $|G| = [G : H]|H|$. Since $|H|$ is not divisible by p and $|G|$ is divisible by p, we conclude that p divides $[G : H]$ for every proper subgroup H.

Since G is non-abelian, $G \neq \mathrm{Z}(G)$ meaning that there are conjugacy classes with more than 1 element. Suppose there are l such classes and let them be represented by $g_1, g_2, \ldots, g_l$. By the class equation (**Theorem I.9.6.1**),

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} [G : \mathrm{C}_G(g_i)].$$

Note that $|\mathrm{Cl}(g_i)| = [G : \mathrm{C}_G(g_i)] = \frac{|G|}{|\mathrm{C}_G(g_i)|} > 1$, which means that $|G| > |\mathrm{C}_G(g_i)|$. Thus $\mathrm{C}_G(g_i) \neq G$ for all i since their orders are different. Recall that $\mathrm{C}_G(g_i)$ is a proper subgroup of G, so by the above observation, p divides $[G : \mathrm{C}_G(g_i)]$.

In the class equation, p divides $|G|$ and p divides $[G : \mathrm{C}_G(g_i)]$, which means that p must divide $|\mathrm{Z}(G)|$. But $\mathrm{Z}(G) \leq G$ and by above observation, p does not divide any proper subgroup of G. Hence, $\mathrm{Z}(G) = \{e\}$ or $\mathrm{Z}(G) = G$. Note $\mathrm{Z}(G) \neq \{e\}$ because that would imply p divides 1 which is a contradiction. So $\mathrm{Z}(G) = G$, but that means that G is abelian (**Problem I.3.3**) which is a contradiction. We thus conclude that there exists an element of order p. □

Exercise I.9.10. Let G be a finite group with $|G| = np$, n is a positive integer, and p prime. Prove that G has a **subgroup** of order p.

9.8 Problems

Problem I.9.1. Let $G = D_5$, the dihedral group of order 10.

(a) Suppose H is a proper subgroup of G. What are the possible order(s) of H?

(b) For each of the possible order(s) identified, find such a subgroup.

Problem I.9.2. Let G be a group of order 25 and X be a G-set of 24 elements. Show that every $g \in G$ has a fixed point.

Problem I.9.3. Suppose G is a finite group with order $n > 1$ where, for all $g \in G$, $g^2 = e$. Prove that $n = 2^k$ where k is a positive integer.

Problem I.9.4. A group action is said to be **free** if $g \cdot x = x$ implies that g is the identity (i.e., only the identity fixes any x).
Let G be a group and S be a non-empty G-set. Suppose G acts on S freely and transitively. Prove that G and S have the same number of elements.

Problem I.9.5. A bracelet consists of 3 beads that each can be one of n colours. Two bracelets are considered to be identical if the rotation of one yields the other, or if one can be obtained via reflecting about a line, or any combination of these two actions. How many distinct bracelets are there?

Problem I.9.6. Let p be a prime number. Prove that a group of order p^2 must be abelian.
*(Hint: Consider **Problem I.3.3** and **Problem I.3.11**)*

Problem I.9.7. Let G be a finite p-group, and X be a G-set. Denote the set of points of X that are fixed under the action of G by Ω. Prove that $|X| \equiv |\Omega| \pmod{p}$.
(Hint: $\Omega = \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}$)

10 Sylow Theorems

The Sylow theorems are a collection of theorems named after the Norwegian mathematician Peter Ludwig Sylow that give detailed information about the number of subgroups of fixed order that a given finite group contains. The Sylow theorems form a fundamental part of finite group theory and have very important applications in the classification of finite simple groups.

10.1 First Sylow Theorem

Before we can state the First Sylow Theorem, we introduce some terminology.

Recall that a group with order p^k for some $k \geq 0$ is called a p-group. If G is a group with a subgroup of order p^k, then that subgroup is called a **p-subgroup**.

Definition I.10.1.1. *Let G be a finite group. Write the order of the group G as $p^k m$ where p is prime, $k \geq 0$, and $p \nmid m$. Then a subgroup H with order p^k is called a **Sylow p-subgroup** of G.*

We denote the set of all Sylow p-subgroups of the group G for a given prime p by $\mathrm{Syl}_p(G)$.

Exercise I.10.1. Find the Sylow 2-subgroup of $\mathbb{Z}_{12}$.

We are now ready to state and prove the **First Sylow Theorem**.

Theorem I.10.1.2 (Sylow I)**.** *Let G be a finite group with order $p^k m$ where p is prime, $k \geq 0$, and $p \nmid m$. Then* $\mathrm{Syl}_p(G) \neq \varnothing$.

Remark. Equivalently, for a finite group G, for every prime factor p with multiplicity k of its order, there is a Sylow p-subgroup of G.

Proof (see [Man11] pp. 1-3). We induct on the order of G.

When the order of G is 1, $|G| = p^0$ for any prime p, so G is clearly a Sylow p-subgroup of itself.

We assume now that the theorem holds for all groups of order strictly less than n, meaning that for any group H with order $p^k m < n$, $\mathrm{Syl}_p(H) \neq \varnothing$. We need to prove the case where the group has order n. We write $n = p^k m$ where p is prime, $k \geq 1$, and $p \nmid m$. We split the argument into two separate cases.

The first case is when p divides the order of the center of G, $|\mathrm{Z}(G)|$. By Cauchy's Theorem (**Theorem I.9.7.1**), $\mathrm{Z}(G)$ contains a subgroup of order p, say N. We note that $N \lhd G$ since for all $x \in N \subseteq \mathrm{Z}(G)$ and $g \in G$, $gxg^{-1} = (gx)g^{-1} = x(gg^{-1}) = x \in N$. Hence G/N is a group, and it has order $\frac{n}{p} = \frac{p^k m}{p} = p^{k-1}m$. Since $p^{k-1}m < p^k m = n$, thus by the Inductive Hypothesis G/N has a Sylow p-subgroup, say $\bar{S}$, meaning that $\bar{S} \leq G/N$ has order p^{k-1}.

We now construct the group $S = \{g \in G \mid gN \in \bar{S}\}$ under the group operation of G. Clearly S is non-empty since $e \in S$ (as $eN = N \in \bar{S} \leq G/N$). Suppose $g_1, g_2 \in S$, meaning that $g_1 N, g_2 N \in \bar{S}$. Therefore $(g_1 g_2^{-1})N = (g_1 N)(g_2 N)^{-1} \in \bar{S}$ which implies that $g_1 g_2^{-1} \in S$. By the subgroup test, $S \leq G$. Also, $N \leq S$ since for all $n \in N$, $nN = N \in \bar{S}$.

We construct the homomorphism $\phi : S \to \bar{S}$ such that $g \mapsto gN$. By construction one sees clearly that ϕ is surjective, meaning that $\mathrm{im}\ \phi =$

$\bar{S}$. Furthermore,

$$\begin{aligned}\ker\phi &= \{s \in S \mid \phi(s) = N\} \\ &= \{s \in S \mid sN = N\} \\ &= \{s \in S \mid s \in N\} \\ &= S \cap N \\ &= N \qquad\qquad \text{(since } N \leq S\text{)}.\end{aligned}$$

By the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**), $S/N \cong \bar{S}$, meaning that $p^{k-1} = |\bar{S}| = \frac{|S|}{|N|} = \frac{|S|}{p}$ which quickly implies that $|S| = p^k$. Hence, there exists a $S \leq G$ such that $|S| = p^k$, meaning that S is a Sylow p-subgroup of G.

We can now start on the second case where p does not divide the order of the center of G. We recall the class equation (**Theorem I.9.6.1**)

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{l} [G : \mathrm{C}_G(g_i)].$$

where $g_1, g_2, \ldots, g_l$ are representatives of the l distinct conjugacy classes with more than one element. We note that p divides $|G|$. Since p does not divide $|\mathrm{Z}(G)|$ in this case, thus $\sum_{i=1}^{l}[G : \mathrm{C}_G(g_i)]$ must also not divide p in order for their sum to be divisible by p. Hence, there is at least one conjugacy class with more than one element such that p does not divide $[G : \mathrm{C}_G(g_i)]$. We note that $[G : \mathrm{C}_G(g_i)] = \frac{|G|}{|\mathrm{C}_G(g_i)|}$ by Lagrange's Theorem (**Theorem I.3.4.4**). Therefore, if p does not divide $\frac{|G|}{|\mathrm{C}_G(g_i)|} = \frac{p^k m}{|\mathrm{C}_G(g_i)|}$, then we conclude that $|\mathrm{C}_G(g_i)| = p^k a$ for some a.

We now argue that $a < m$ (recalling that $|G| = p^k m$). Clearly $a \leq m$ since if $a > m$ then $\frac{p^k m}{|\mathrm{C}_G(g_i)|}$ is not an integer. If instead $a = m$ then $|\mathrm{C}_G(g_i)| = p^k m = |G|$, and since $\mathrm{C}_G(g_i) \leq G$ with them having equal orders, we conclude $G = \mathrm{C}_G(g_i)$. This means that every element in G commutes with g_i, which quickly implies $g_i \in \mathrm{Z}(G)$. But an element is in $\mathrm{Z}(G)$ if its conjugacy class has only one element, which is not the case. Hence $a \neq m$, meaning that $a < m$.

In summary, $\mathrm{C}_G(g_i) \leq G$ with $|\mathrm{C}_G(g_i)| = p^k a < p^k m = n$. Therefore we apply the Induction Hypothesis on $\mathrm{C}_G(g_i)$ to say that $\mathrm{C}_G(g_i)$ has a Sylow p-subgroup of order p^k. Clearly a subgroup of $\mathrm{C}_G(g_i)$ has to also be a subgroup of G, meaning that G has a Sylow p-subgroup.

Therefore, any finite group G with order written as $p^k m$ has a Sylow p-subgroup, meaning that $\mathrm{Syl}_p(G) \neq \varnothing$. □

Exercise I.10.2. Find the set of primes p such that $\mathrm{Syl}_p(\mathrm{S}_5) \neq \varnothing$.

10.2 Conjugate Subgroup

Before we look at the next Sylow theorem, we need to introduce two more things. The first is the notion of the **conjugate subgroup**.

Definition I.10.2.1. *Let G be a group, $H \leq G$, and $g \in G$. Then the **conjugate subgroup of H by g** is*

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

under the group operation of G.

We proved that gHg^{-1} is a subgroup of G in **Exercise I.3.2**.

Exercise I.10.3. Let G be a group and $H \leq G$. Prove that $gHg^{-1} \cong H$ for any $g \in G$.

We prove some results regarding the conjugate subgroup here.

Proposition I.10.2.2. *Let G be a group, and let x and y be elements in G such that there exists an element $a \in G$ such that $y = axa^{-1}$. Then $y^n = ax^n a^{-1}$ for all integers n.*

Proof. Trivially, when $n = 0$, $y^0 = e = y^0 = x^0 = ax^0 a^{-1}$.

We consider a proof by induction for positive integers n and then prove the negative case.

When $n = 1$, $y = axa^{-1}$ is given. Now assume $n = k$ holds true for some positive integer k, meaning that $y^k = ax^k a^{-1}$. We will prove that $y^{k+1} = ax^{k+1}a^{-1}$.

$$\begin{aligned} y^{k+1} &= y(y^k) \\ &= (axa^{-1})(ax^k a^{-1}) && \text{(Induction Hypothesis)} \\ &= axa^{-1}ax^k a^{-1} \\ &= axx^k a^{-1} \\ &= ax^{k+1}a^{-1} \end{aligned}$$

which completes this induction for positive integers n.

Now suppose n is a non-negative integer. Then

$$\begin{aligned} y^{-n} &= (y^n)^{-1} \\ &= (ax^n a^{-1})^{-1} && \text{(by above result)} \\ &= a(x^n)^{-1}a^{-1} \\ &= ax^{-n}a^{-1} \end{aligned}$$

which completes the proof for all integers. □

Proposition I.10.2.3. *Let G be a group. Then for all $g, x \in G$, we have $|gxg^{-1}| = |x|$.*

Proof. The proposition trivially holds true for $g = e$ so we assume $g \neq e$.

Suppose $|x| = n$, meaning $x^n = e$ and $x^k \neq e$ for all $1 \leq k < n$. Note we have

$$\begin{aligned} (gxg^{-1})^n &= gx^n g^{-1} && \textbf{(Proposition I.10.2.2)} \\ &= geg^{-1} && \text{(since } |x| = n\text{)} \\ &= e \end{aligned}$$

which means that $|gxg^{-1}| \leq n = |x|$.

Now consider $(gxg^{-1})^k = gx^kg^{-1}$. Suppose k is a positive integer such that $x^k = h$ where $h \neq e$. Then $gx^kg^{-1} = ghg^{-1}$. We argue that $ghg^{-1} \neq e$.

- If $gh = e$ then $gx^kg^{-1} = g^{-1} \neq e$ since $g \neq e$.
- If instead $hg^{-1} = e$ then $gx^kg^{-1} = g \neq e$.

Hence, if $x^k \neq e$, then $(gxg^{-1})^k = gx^kg^{-1} \neq e$, meaning that $|x| \leq |gxg^{-1}|$.

Therefore $|gxg^{-1}| = |x|$. □

Exercise I.10.4. Prove that for any group G, $|gh| = |hg|$ for all $g, h \in G$.

We note an important result with regards to the conjugate subgroup.

Theorem I.10.2.4. *Let G be a group. Suppose H is the only subgroup of G with a given order. Then $H \lhd G$.*

Proof. Suppose $g \in G$. By **Exercise I.10.3** we know $gHg^{-1} \cong H$ which means that $|gHg^{-1}| = |H|$. Furthermore, by **Exercise I.3.2** we know that $gHg^{-1} \leq G$. Since H is the only subgroup of that order (by assumption), we conclude that $gHg^{-1} = H$, which quickly means that $H \lhd G$ by definition of a normal subgroup. □

10.3 The Normalizer

We now look at the definition of the **normalizer**.

Definition I.10.3.1. *Let G be a group and S be a subset of G. The* ***normalizer of S in G*** *is given by*

$$\mathrm{N}_G(S) = \{g \in G \mid gS = Sg\}.$$

Remark. Equivalently, $\mathrm{N}_G(S) = \{g \in G \mid gSg^{-1} = S\}$.

Exercise I.10.5. Let G be a group and S be a subset of G. Prove that $\mathrm{N}_G(S) \leq G$.

We prove some properties of the normalizer here.

Proposition I.10.3.2. *Let G be a group, and $H \leq G$. Then $H \lhd \mathrm{N}_G(H)$.*

Proof. We first prove $H \leq \mathrm{N}_G(H)$ and then prove normality.

We know that both H and $\mathrm{N}_G(H)$ are subgroups of G, so both are groups. We just need to check that $H \subseteq \mathrm{N}_G(H)$ to prove that $H \leq \mathrm{N}_G(H)$.

Consider any $h \in H$. We note that $hH = H$ and $Hh^{-1} = H$ since $h^{-1} \in H$. Thus, if $h \in H$, then

$$hHh^{-1} = h(Hh^{-1}) = hH = H$$

which means that $h \in \mathrm{N}_G(H)$ by definition of the normalizer. Hence any element in H is also an element of $\mathrm{N}_G(H)$, meaning $H \subseteq \mathrm{N}_G(H)$.

It follows then that $H \leq \mathrm{N}_G(H)$ since $H \subseteq \mathrm{N}_G(H)$ and H is a group.

Now we prove normality. Consider any $n \in \mathrm{N}_G(H)$, which means that $nHn^{-1} = H$. This immediately implies that $H \lhd \mathrm{N}_G(H)$. □

Remark. Combining **Exercise I.10.5** and **Proposition I.10.3.2** means that $H \lhd \mathrm{N}_G(H) \leq G$.

Proposition I.10.3.3. *Let G be a group, and $H \leq G$. Then $\mathrm{N}_G(H)$ is the largest subgroup of G containing H as a normal subgroup.*

Remark. What we mean by "largest" here is that if there was another subgroup of G, say K, that permits $H \lhd K$, then it must be the case that $K \subseteq \mathrm{N}_G(H)$.

Proof. By **Proposition I.10.3.2** we know that $H \lhd \mathrm{N}_G(H)$. We just need to prove that any subgroup in which H is normal inside it must be a subset of $\mathrm{N}_G(H)$.

Consider any subgroup $N \leq G$ such that $H \lhd N \leq G$. Then for any $n \in N$ we have $nHn^{-1} = H$ by definition of normality, which immediately means that $n \in \mathrm{N}_G(H)$ by definition of the normalizer of H in G. Hence any element in N also belongs in $\mathrm{N}_G(H)$, meaning $N \subseteq \mathrm{N}_G(H)$.

This completes the proof that $\mathrm{N}_G(H)$ is the largest subgroup of G that contains H as a normal subgroup. □

Proposition I.10.3.4. *Let G be a finite group, P be a Sylow p-subgroup of G, and Q be a p-subgroup of $\mathrm{N}_G(P)$. Then $Q \subseteq P$. In particular, if Q is a Sylow p-subgroup of $\mathrm{N}_G(P)$ then $P = Q$.*

Proof (see [Hum96] Proposition 11.9). For brevity let $|G| = xp^n$ where $p \nmid x$, $|P| = p^n$, and $|Q| = p^m$.

Recall by the Diamond Isomorphism Theorem (**Theorem I.7.4.1**), statement 3, we have $PQ \leq \mathrm{N}_G(P)$ since $P \lhd \mathrm{N}_G(P)$ by **Proposition I.10.3.2**. As $\mathrm{N}_G(P) \leq G$ thus $PQ \leq G$. In addition, by **Exercise I.7.5**,

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^{n+m-s}$$

where we define $|P \cap Q| = p^s$. By Lagrange's Theorem (**Theorem I.3.4.4**) we know that $|G| = a|PQ|$ so $p^n = ap^{n+m-s}$ which implies $1 = ap^{m-s}$. Since a is a positive integer, thus $p^{m-s} = \frac{1}{a}$ which means $m \leq s$.

We note by **Problem I.3.4**, $P \cap Q \leq Q$, meaning $|Q| = b|P \cap Q|$ by Lagrange's Theorem. Thus $p^m = bp^s$ which implies $p^{m-s} = b \geq 1$ so $m \geq s$.

Hence $m = s$ which means $|P \cap Q| = |Q|$, i.e. $P \cap Q = Q$. Therefore $Q \subseteq P$ which is the first part of the proposition proved.

Now suppose Q is, in particular, a Sylow p-subgroup of $\mathrm{N}_G(P)$. Since $\mathrm{N}_G(P) \leq G$ by **Exercise I.10.5**, one concludes that $|G| = y|\mathrm{N}_G(P)|$ by Lagrange's Theorem. Hence $xp^n = y|\mathrm{N}_G(P)|$ which implies $|\mathrm{N}_G(P)| = \frac{x}{y}p^n = zp^n$ where $z = \frac{x}{y}$ and one observes $p \nmid z$. Therefore, if Q is a Sylow p-subgroup, then $|Q| = p^n = |P|$ which implies $P = Q$ as $Q \subseteq P$. □

10.4 Second Sylow Theorem

We can now look at the **Second Sylow Theorem**.

Theorem I.10.4.1 (Sylow II)**.** *Let G be a finite group and p be a prime number. Suppose H and K are both Sylow p-subgroups of G. Then there exists an element $g \in G$ such that $gHg^{-1} = K$.*

Proof (see [Hum96] Theorem 11.10 and [Man11] pp. 3-5). Suppose H be a Sylow p-subgroup of G. Let the set

$$\mathcal{X} = \{gHg^{-1} \mid g \in G\}$$

and denote an element from $\mathcal{X}$ by X.

Let the Sylow p-subgroup H act on $\mathcal{X}$ by conjugation, meaning $h \cdot X = hXh^{-1}$. We prove that this is, in fact, a group action.

- **Closure**: We have to prove closure because it is not implicit in the definition of this action.

  Let $X = gHg^{-1}$ for some $g \in G$. Then

  $$h \cdot X = hHh^{-1} = hgHg^{-1}h^{-1} = (hg)H(hg)^{-1}.$$

Since $h \in H \leq G$, then $hg \in G$, which thus means that $h \cdot X = (hg)H(hg)^{-1} \in \mathcal{X}$.

- **Identity**: $e \cdot X = eXe^{-1} = X$.
- **Compatibility**: Let $h_1, h_2 \in H$. Then

$$\begin{aligned} h_1 \cdot (h_2 \cdot X) &= h_1 \cdot (h_2 X h_2^{-1}) \\ &= h_1 h_2 X h_2^{-1} h_1^{-1} \\ &= (h_1 h_2) X (h_1 h_2)^{-1} \\ &= (h_1 h_2) \cdot X. \end{aligned}$$

We consider the orbits of this group action. We note that $\mathrm{Orb}_H(H) = \{X \in \mathcal{X} \mid h \cdot H = H \text{ for some } h \in H\}$ and $h \cdot H = hHh^{-1} = P$ since $h \in H$. Thus $\mathrm{Orb}_H(H) = \{H\}$, meaning $|\mathrm{Orb}_H(H)| = 1$. We now show that $X = H$ is the only element in $\mathcal{X}$ such that $|\mathrm{Orb}_H(X)| = 1$. If X has one element in its orbit, then for all $h \in H$, $h \cdot X = hXh^{-1} = X$. Since $X = gHg^{-1}$ for some g, thus

$$\begin{aligned} & h(gHg^{-1})h^{-1} = gHg^{-1} \\ \iff & hgHg^{-1} = gHg^{-1}h \\ \iff & hgH = gHg^{-1}hg \\ \iff & (g^{-1}hg)H = H(g^{-1}hg) \\ \iff & g^{-1}hg \in \mathrm{N}_G(H). \end{aligned}$$

By **Proposition I.10.2.3**, $|g^{-1}hg| = |h|$, and since the order of H is p^k, thus for all elements $g^{-1}hg \in X$, they have order p^k. By definition of a p-group, one sees that $g^{-1}Hg$ is a p-subgroup of $\mathrm{N}_G(H)$. Now clearly $g^{-1}Hg \cong H$ (by making the substitution $h = g^{-1}$ and then using **Exercise I.10.3** result) which means that $g^{-1}Hg$ has the same number of elements as H. Hence, $g^{-1}Hg$ is a Sylow p-subgroup of $\mathrm{N}_G(H)$. Therefore by **Proposition I.10.3.4**, $H = g^{-1}Hg$, which means $X = gHg^{-1} = H$. Hence H is the only element of $\mathcal{X}$ with $|\mathrm{Orb}_H(X)| = 1$. Therefore for any $g \notin H$, $|\mathrm{Orb}_H(gHg^{-1})| > 1$. In fact, by Orbit-Stabilizer Theorem (**Theorem I.9.3.1**), one sees that

$$|\mathrm{Stab}_H(gHg^{-1})| = \frac{|H|}{|\mathrm{Orb}_H(gHg^{-1})|}$$

and since $|H|$ is a power of p and $|\mathrm{Stab}_H(gHg^{-1})|$ is an integer, thus $|\mathrm{Orb}_H(gHg^{-1})|$ has to be a power of p, meaning $|\mathrm{Orb}_H(gHg^{-1})| \equiv 0 \pmod{p}$. Because distinct orbits partition $\mathcal{X}$ (**Exercise I.9.6**), thus $|\mathcal{X}| \equiv 1 \pmod{p}$.

Now let the Sylow p-subgroup K act on $\mathcal{X}$ by conjugation, meaning $k \star X = kXk^{-1}$. This is a group action as proven before, and the above conclusion means that there is at least one orbit of length 1. Hence there exists a $g \in G$ such that for all $k \in K$, we have $k(gHg^{-1})k^{-1} = gHg^{-1}$. Hence $g^{-1}kg \in \mathrm{N}_G(H)$ which means $g^{-1}Kg \subset \mathrm{N}_G(H)$. Therefore, since $|K| = |g^{-1}Kg|$ and by **Proposition I.10.3.4**, $g^{-1}Kg \subseteq H$, meaning $K \subseteq gHg^{-1}$. But because $|H| = |K|$ as they are both Sylow p-subgroups, therefore $K = gHg^{-1}$. □

Remark. What part of this proof shows is that if P is a Sylow p-subgroup but Q is only a p-subgroup, then $Q \subseteq gPg^{-1}$ for some $g \in G$.

We note one important corollary of the Second Sylow Theorem.

Corollary I.10.4.1.1. *Let G be a finite group and P be a Sylow p-subgroup for some prime p. Then P is a normal subgroup of G if and only if P is the only Sylow p-subgroup of G.*

Proof. The reverse direction is easy to prove. Since P is the only Sylow p-subgroup of G, this means that P is the only subgroup of order p^k. By **Theorem I.10.2.4**, this means that $P \lhd G$.

We work on the forward direction now and suppose P is a normal subgroup of G. Let $\hat{P}$ be a normal Sylow p-subgroup. By the Second Sylow Theorem (**Theorem I.10.4.1**), there exists $g \in G$ such that $g\hat{P}g^{-1} = P$. But since $\hat{P}$ is normal, thus $g^{-1}\hat{P}g = \hat{P}$ by definition of normality. Hence, $P = \hat{P}$, meaning that there is only one Sylow p-subgroup. □

Exercise I.10.6. Let G be a finite group, p be a prime number, and H and K be distinct Sylow p-subgroups of G. Prove that $H \cong K$.

10.5 Third Sylow Theorem

We now state and prove the **Third Sylow Theorem**.

Theorem I.10.5.1 (Sylow III)**.** *Let G be a finite group with order $p^k m$ where p is prime, $k \geq 1$, and $p \nmid m$. Let n_p denote the number of Sylow p-subgroups in G, i.e. $n_p = |\mathrm{Syl}_p(G)|$. Then,*

1. *$n_p = [G : \mathrm{N}_G(P)]$, where P is a Sylow p-subgroup of G;*
2. *n_p divides m; and*
3. *$n_p \equiv 1 \pmod{p}$.*

Proof (adapted from [Wie59]). We prove the three statements in order.

1. Let G act on $\mathrm{Syl}_p(G)$ by conjugation, meaning that for any $g \in G$ and $P \in \mathrm{Syl}_p(G)$, $g \cdot P = gPg^{-1}$. By the Second Sylow Theorem (**Theorem I.10.4.1**), all Sylow p-subgroups are conjugates of each other, so the orbit of any $P \in \mathrm{Syl}_p(G)$ is the set of all Sylow p-subgroups, meaning $|\mathrm{Orb}_G(P)| = |\mathrm{Syl}_p(G)| = n_p$. Now consider $\mathrm{Stab}_G(P)$; note

$$\mathrm{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\} = \mathrm{N}_G(P)$$

   by definition of the normalizer. By the Orbit-Stabilizer Theorem (**Theorem I.9.3.1**),

$$n_p = |\mathrm{Orb}_G(P)| = \frac{|G|}{|\mathrm{Stab}_G(P)|} = \frac{|G|}{|\mathrm{N}_G(P)|} = [G : \mathrm{N}_G(P)]$$

   by Lagrange's Theorem (**Theorem I.3.4.4**) and we are done.

2. Let P be a Sylow p-subgroup. We recall that $P \lhd \mathrm{N}_G(P) \leq G$. Note that by Lagrange's Theorem we know $|\mathrm{N}_G(P)| = [\mathrm{N}_G(P) : P]|P| = ap^k$ where $a \leq m$ (since $\mathrm{N}_G(P) \leq G$). Furthermore

$$mp^k = |G| = [G : \mathrm{N}_G(P)]|\mathrm{N}_G(P)| = n_p(ap^k)$$

   which means $m = an_p$. In other words, n_p divides m.

3. Let H be a Sylow p-subgroup and let it act on $\mathrm{Syl}_p(G)$ by conjugation, meaning that for any $h \in H$ and $P \in \mathrm{Syl}_p(G)$, $h \cdot P = hPh^{-1}$. Let Ω denote the set of fixed points of $\mathrm{Syl}_p(G)$ under this action.

   Suppose $Q \in \Omega$, which means that $hQh^{-1} = Q$ for all $h \in H$. Thus $H \subseteq \mathrm{N}_G(Q)$ as $\mathrm{N}_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$. In fact, since H is a Sylow p-subgroup, $H \leq \mathrm{N}_G(Q)$. We note $Q \lhd \mathrm{N}_G(Q)$ by **Proposition I.10.3.2**. Hence H and Q are Sylow p-subgroups of $\mathrm{N}_G(Q)$, which means there exists $n \in \mathrm{N}_G(Q)$ such that $nQn^{-1} = H$ by the Second Sylow Theorem (**Theorem I.10.4.1**). Furthermore $nQn^{-1} = Q$ since $Q \lhd \mathrm{N}_G(Q)$. Hence $Q = H$ which means that the only element in Ω is H.

   By a similar argument posed in the proof of the Second Sylow Theorem, for any $Q \in \mathrm{Syl}_p(G)$ where $Q \neq H$ we must have $|\mathrm{Orb}_H(Q)| \equiv 0 \pmod{p}$. Note $|\mathrm{Orb}_H(H)| = 1$. Now since distinct orbits partition $\mathrm{Syl}_p(G)$, we must have $n_p = |\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$.

This completes the proof of the Third Sylow Theorem. □

Example I.10.5.2. We will show that a group of order 4225 is abelian by using the Third Sylow Theorem and other results.

Note that $4225 = 5^2 \times 13^2$. Let G be a group of order 4225. By the Third Sylow Theorem (**Theorem I.10.5.1**), we know that

- $n_5 \mid 13^2 = 169$ and $n_{13} \mid 5^2 = 25$, which means $n_5 \in \{1, 13, 169\}$ and $n_{13} \in \{1, 5, 25\}$; and
- $n_5 \equiv 1 \pmod{5}$ and $n_{13} \equiv 1 \pmod{13}$, which means $n_5 \in \{1, 6, 11, \dots\}$ and $n_{13} \in \{1, 14, 27, \dots\}$.

Hence, $n_5 = 1$ and $n_{13} = 1$, meaning that there is only one Sylow 5-subgroup and one Sylow 13-subgroup.

Let P be the Sylow 5-subgroup and Q be the Sylow 13-subgroup. By **Corollary I.10.4.1.1**, $P \lhd G$ and $Q \lhd G$, so $pq = qp$ for any $p \in P$ and $q \in Q$. Furthermore, by **Problem I.3.9**, $P \cap Q = \{e\}$. Finally, notice

that

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = |P||Q| = 5^2 \times 13^2 = |G|$$

which means that PQ and G have the same number of elements. Hence, G is the internal direct product of P and Q. We note that

$$G = PQ \cong P \times Q$$

by direct product equivalence (**Theorem I.6.3.1**). In addition, since P and Q are groups of prime-squared order, they are abelian (**Problem I.9.6**), meaning that their external direct product $P \times Q$ is also abelian (**Problem I.6.1**). Hence G is also abelian since $G \cong P \times Q$.

Exercise I.10.7. Let G be a group of order 784, and let P be a Sylow 7-subgroup that is **not** a normal subgroup of G. Find the order of $\mathrm{N}_G(P)$.

10.6 Testing Non-Simplicity Of Groups

To end this chapter, we look at the idea of **simple groups** and devise a test to prove the non-simplicity of groups.

Definition I.10.6.1. *Let G be a non-trivial group. Then G is **simple** if the only normal subgroups of G are the identity and G itself.*

Remark. Equivalently, G is simple if G has no proper normal subgroups.

We may use part of the Third Sylow Theorem to create a test for non-simplicity.

Theorem I.10.6.2 (Sylow's Test)**.** *Let n be a non-prime integer and let p be a prime divisor of n. If 1 is the only divisor of n that is congruent 1 modulo p, then there does not exist a simple group of order n.*

Proof. We first suppose $n = p^k$ where $k > 1$. Let G be a group of order n. We consider two cases.

- Suppose G is abelian. By a corollary of Cauchy's Theorem (**Exercise I.9.10**) and writing p^k as $p \times p^{k-1}$, we know there exists a subgroup of order p. Since every subgroup of an abelian group is normal (**Propopsition I.3.5.2**), thus there exists a proper normal subgroup of G, meaning G is non-simple.
- Suppose now G is non-abelian. By **Example I.9.6.3**, G has a non-trivial center. Furthermore, $G \neq \mathrm{Z}(G)$ because G is non-abelian (**Problem I.3.3**). Since the center is a normal subgroup of G, it is thus a proper normal subgroup of G, meaning G is non-simple.

Hence any group of order p^k where $k > 1$ is non-simple.

Now suppose n is not a prime power. By the Third Sylow Theorem (**Theorem I.10.5.1**), the number of Sylow p-subgroups, n_p, is congruent to 1 modulo p and divides n. Since 1 is the only such number by our assumption, thus $n_p = 1$, meaning that there is only one Sylow p-subgroup. By **Corollary I.10.4.1.1** this means that that Sylow p-subgroup (which is non-trivial) is normal, which thus means that any group of order n is non-simple. □

Example I.10.6.3. Consider a group with order 15. Note $15 = 3 \times 5$, and consider $p = 5$. The divisors of 15 are 1, 3, 5, and 15, and clearly only 1 is congruent to 1 modulo 5. Hence by Sylow's Test we know that a group of order 15 cannot be simple.

For some groups of orders that do not satisfy the condition in Sylow's Test, we can still can prove that they cannot be simple.

Example I.10.6.4. We will show that a group of order 2552 is non-simple.

We note first that $2552 = 2^3 \times 11 \times 29$. By the Third Sylow Theorem (**Theorem I.10.5.1**), we know $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.

The divisors of the m given the following primes are listed below.

- $p = 2$: $m = 319$ and so divisors are $\{1.11, 29, 319\}$.
- $p = 11$: $m = 232$ and so divisors are $\{1, 2, 4, 8, 29, 58, 116, 232\}$.
- $p = 29$: $m = 88$ and so divisors are $\{1, 2, 4, 8, 11, 22, 44, 88\}$.

Thus, since $n_p \equiv 1 \pmod{p}$, we must have $n_2 \in \{1, 11, 29, 319\}$, $n_{11} \in \{1, 232\}$, and $n_{29} \in \{1, 88\}$.

Suppose first that all n_2, n_{11}, n_{29} are not equal to 1. Then $n_{11} = 232$ and $n_{29} = 88$. Recall that one element in a Sylow p-subgroup has order 1 (i.e., the identity). Thus, the number of elements of order 11 is $232 \times (11 - 1) = 2320$ and the number of elements of order 29 is $88 \times (29 - 1) = 2464$. Hence, the total number of elements in the group of order 2552 must be at least $2320 + 2464 = 4764$, a contradiction.

Hence, we conclude that at least one of n_2, n_{11}, n_{29} must be 1, meaning that there is a non-trivial normal subgroup, which therefore means that any group of order 2552 is non-simple.

Example I.10.6.5. We show that any group of order 36 is non-simple by considering the kernel of a homomorphism.

We note $36 = 2^2 \times 3^2$. Let G be a group of order 36 and let P be a Sylow 3-subgroup of the group of order 36. Let G act on the set of cosets G/P by left multiplication, meaning $g \cdot xP = (gx)P$. Then by **Theorem I.9.1.5** this induces a homomorphism $\phi : G \to \mathrm{S}_4$ since there are 4 cosets in G/P. We note $\phi(g) = \sigma_g$ where $\sigma_g(xP) = g \cdot xP = (gx)P$.

We consider the kernel of ϕ.

$$\begin{aligned}
\ker\phi &= \{g \in G \mid \phi(g) = \mathrm{id}\} \\
&= \{g \in G \mid \sigma_g = \mathrm{id}\} \\
&= \{g \in G \mid \sigma_g(xP) = xP \text{ for all } x \in G\} \\
&= \{g \in G \mid (gx)P = xP \text{ for all } x \in G\} \\
&= \{g \in G \mid x^{-1}gx \in P \text{ for all } x \in G\}\} \qquad \text{(by Coset Equality)} \\
&= \{g \in G \mid g \in xPx^{-1} \text{ for all } x \in G\}\} \\
&= \bigcap_{x \in G} xPx^{-1}.
\end{aligned}$$

We note that $\ker\phi \neq \{e\}$ since that would imply that ϕ is injective (**Exercise I.7.3**), which would mean $36 = |G| \leq |\mathrm{S}_4| = 4! = 24$. We also note $\ker\phi \neq G$ otherwise

$$36 = |G| = |\ker\phi| = \left|\bigcap_{x \in G} xPx^{-1}\right| \leq |xPx^{-1}| = |P| = 9,$$

a contradiction. Hence $\ker\phi$ is a proper subgroup of G. We note that $\ker\phi \lhd G$, so we have found a proper normal subgroup of G, meaning that G is non-simple.

Exercise I.10.8. Show that any group of order 130 is non-simple.

10.7 Problems

Problem I.10.1. Show that a group of order 200 has a normal Sylow 5-subgroup.

Problem I.10.2. Show that any Sylow p-subgroup of a group of order 33 must be normal.

Problem I.10.3. A perfect number is a positive integer that is equal to the sum of its positive divisors, excluding the number itself. All even perfect numbers are of the form $2^{p-1}(2^p - 1)$ where both p and $2^p - 1$ are primes. Prove that any group with an order that is an even perfect number is not simple.

Problem I.10.4. Let p and q be primes such that $p < q$. Let G be a group of order pq.

(i) Prove that there is only one subgroup H of G of order q. Deduce that $H \lhd G$.

(ii) Prove also that if $q \not\equiv 1 \pmod{p}$ then G is cyclic.

Problem I.10.5. Show that any group of order 3325 is abelian.

Problem I.10.6. Let G be a finite group, and write the order of G as $p^k m$ where $k \geq 0$ and $p \nmid m$. Let $N \lhd G$ such that p does not divide the index of N in G.

(i) Prove that any Sylow p-subgroup of N is also in G.

(ii) Prove that any Sylow p-subgroup of G is also in N.

Problem I.10.7. Let G be a finite group such that $|G| = p^k m$ where $k \geq 1$, $m > 1$, and $p \nmid m$. Prove that if $m! < |G|$ then G is non-simple.

Problem I.10.8. Let p, q, and r be distinct primes such that $p < q < r$. Let G be a group of order pqr. Prove that G is non-simple.

Exercise Solutions

Chapter 1

1. There are 6! = 720 possible permutations of 6 points, so there are 720 symmetries in the group given. That is, the order of the symmetric group of degree 6 is 720.

Chapter 2

1. The group table of $(\mathbb{Z}_6, \otimes_n)$ is as follows:

$\otimes_n$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

   Notice that 0 does not have an inverse. Since the identity is 1, and the row (and column) of 0 does not have a 1, thus 0 does not have an inverse.

2. Note that $(xx^{-1})^{-1} = (x^{-1})^{-1}x^{-1}$ by the Shoes and Socks and $(xx^{-1})^{-1} = e^{-1} = e$. Thus $(x^{-1})^{-1}x^{-1} = e$. Multiplying both sides on the right by x yields $(x^{-1})^{-1} = ex = x$, i.e. $(x^{-1})^{-1} = x$.

3. (i) The identity is 1 since:

   - $1 \times 1 = 1$

- $1 \times (-1) = (-1) \times 1 = -1$
- $1 \times i = i \times 1 = i$
- $1 \times (-i) = (-i) \times 1 = -i$

(ii) The order of the identity 1 is 1, so we look at the other elements:

- $|-1| = 2$ since $-1 \neq 1$ and $(-1)^2 = -1 \times -1 = 1$
- $|i| = 4$ since $i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, but $i^4 = 1$
- $|-i| = 4$ since $-i \neq 1$, $(-i)^2 = -1 \neq 1$, $(-i)^3 = i \neq 1$, but $(-i)^4 = 1$

4. $-i$ is the other generator since $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, and $(-i)^4 = 1$.

5. We work slowly:

$$\begin{aligned} rsr^4sr^3 &= r(sr^4)(sr^3) \\ &= r(r^2s)(r^3s) \\ &= r^3sr^3s \\ &= r^3(sr^3)s \\ &= r^3(r^3s)s \\ &= r^6s^2 \\ &= e \end{aligned}$$

Chapter 3

1. We will prove this claim by using the 3 axioms. For brevity let $H = \{e\}$. Clearly $H \subseteq G$.

   - The only element in H is e, and $e * e = e$ which is in H. Hence H is closed.
   - The identity of the group G is e which is in H by definition of H.

- The only element in H is e and the inverse of e is e.

Hence, $\{e\} \leq G$.

2. Clearly e is in S since e is in H and $geg^{-1} = gg^{-1} = e$, so S is non-empty.

   Now suppose x and y are in S. Then there exist elements h_x and h_y in H such that $x = gh_xg^{-1}$ and $y = gh_yg^{-1}$. Note that

$$\begin{aligned} xy^{-1} &= (gh_xg^{-1})(gh_yg^{-1})^{-1} \\ &= (gh_xg^{-1})(gh_y{}^{-1}g^{-1}) && \text{(Shoes and Shocks)} \\ &= gh_xg^{-1}gh_y{}^{-1}g^{-1} && \text{(associativity)} \\ &= gh_xh_y{}^{-1}g^{-1} && (g^{-1}g = e). \end{aligned}$$

   Note that since $H \leq G$ thus $h_xh_y{}^{-1}$ is an element of H (by forward direction of subgroup test). Hence $xy^{-1} = g(h_xh_y{}^{-1})g^{-1}$ is in S. By subgroup test, $S \leq G$.

3. (a) Since $\oplus_8$ is commutative, thus $gH = Hg$.
   (Actually, since G is an additive group, we really should be writing $g \oplus_4 H = H \oplus_4 g$.)

   (b) There are 4 distinct left cosets of H in G.

   - $0 \oplus_4 H = \{0, 4\} = H$
   - $1 \oplus_4 H = \{1, 5\}$
   - $2 \oplus_4 H = \{2, 6\}$
   - $3 \oplus_4 H = \{3, 7\}$

4. Let x be in $g_1H \cap g_2H$. Then $x \in g_1H$ and $x \in g_2H$ simultaneously. Hence, $x = g_1h = g_2\hat{h}$ for some h and $\hat{h}$ in H. Thus by rearrangement, $g_2^{-1}g_1 = \hat{h}h^{-1} \in H$. By coset equality lemma (in particular, statement 5), $g_1H = g_2H$.

5. Note that $|G| = 99$ and $|H| = 3$, so $[G : H] = 99 \div 3 = 33$ by Lagrange's theorem.

6. Let x be an element of G with $x \neq e$. Then $|x| > 1$. By **Corollary I.3.4.4.1**, the order of x is a factor of $|G| = p$. Since p is prime $|x| = 1$ (which is not possible) or $|x| = p$. Hence $|x| = p$.

7. (i) By **Proposition I.3.5.2** every subgroup of G is normal. Hence H is a normal subgroup of G, meaning G/H is a quotient group by **Theorem I.3.6.2**.

   (ii) Let g be the generator of G. Consider $xH \in G/H$. Since $x \in G$, thus there exists an integer k such that $x = g^k$ since G is cyclic. Hence, $xH = g^k H = (gH)^k$ which means that gH generates any element in G/H. Therefore gH is a generator of G/H, meaning G/H is cyclic.

Chapter 4

1. (a) Is **not** a homomorphism, since $\phi(m+n) = m+n$ while $\phi(m)\phi(n) = mn \neq m+n$.

   (b) Is a homomorphism, since $\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n)$.

2. Clearly $e_2 \in \phi(H_1)$ since $e_2 = \phi(e_1)$ and $e_1 \in H_1$. Now suppose x and y are in $\phi(H_1)$, meaning that $\phi(h_x) = x$ and $\phi(h_y) = y$ for some h_x and h_y in H. So, $h_x h_y^{-1}$ is in H. Furthermore,

$$\begin{aligned} \phi(h_x h_y^{-1}) &= \phi(h_x)\phi(h_y^{-1}) && \text{(definition of homomorphism)} \\ &= \phi(h_x)\left(\phi(h_y)\right)^{-1} && \text{(property of homomorphism)} \\ &= xy^{-1} \end{aligned}$$

   meaning that xy^{-1} is in $\phi(H_1)$. Therefore, by subgroup test, $\phi(H_1) \leq G_2$.

3. Disprove. Let $G_1 = H_1 = \mathbb{Z}$ be the additive group of integers and let $G_2 = H_2 = D_n$, the dihedral group of order $2n$. Consider the map $\phi : G_1 \to G_2$ where $\phi(m) = s^m$. Clearly, $H_1 \leq G_1$. Note that $\phi(H_1) = \{e, s\} = \langle s \rangle$. From **Example I.3.5.3**, we know

that $\langle s \rangle$ is not a normal subgroup of $D_3 = G_2$, so $\phi(H_1)$ is not a normal subgroup of G_2.

4. (i) Since $3^0 = 1$, $3^1 = 3$, $3^2 = 9 \equiv 4 \pmod 5$, and $3^3 = 27 \equiv 2 \pmod 5$, thus $G = \langle 3 \rangle$. Since $7^0 = 1$, $7^1 = 7$, $7^2 = 49 \equiv 9 \pmod{10}$, and $7^3 = 343 \equiv 3 \pmod{10}$, thus $H = \langle 7 \rangle$.

   (ii) We need to prove that it is a bijection and a homomorphism.

   - **Homomorphism**:

   $$\phi(3^m 3^n) = \phi(3^{m+n}) = 7^{m+n} = 7^m 7^n = \phi(3^m)\phi(3^n)$$

   - **Bijection**: Note that $1 \mapsto 1$, $3 \mapsto 7$, $4 \mapsto 9$, $2 \mapsto 3$ which clearly shows that ϕ is bijective.

   Therefore ϕ is an isomorphism, meaning $G \cong H$.

5. Suppose $N \lhd G$ such that $|N| = k$. Then $\phi(N) \leq H$ with order k by the theorem. All that remains to prove is that $\phi(N)$ is normal.

   Let n be in N and $\hat{n} \in \phi(N)$ such that $\hat{n} = \phi(n)$. Let $h \in H$ be an arbitrary element. To prove that $h\hat{n}h^{-1}$ is in N.

   Let g be in G such that $\phi(g) = h$. Then

   $$\begin{aligned} h\hat{n}h^{-1} &= \phi(g)\phi(n)\phi(g^{-1}) \\ &= \phi(\underbrace{gng^{-1}}_{\text{In } N}) \in \phi(N) \end{aligned}$$

   which proves that $\phi(N)$ is normal. Hence there exists a normal subgroup of order k, namely $\phi(N)$.

6. Since $7^0 = 1$, $7^1 = 7$, $7^2 = 49 \equiv 9 \pmod{10}$, and $7^3 = 343 \equiv 3 \pmod{10}$, thus $G = \langle 7 \rangle$. Note $|7| = 4$ so $G \cong \mathbb{Z}_4$, i.e. $n = 4$.

Chapter 5

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

(b) $\begin{pmatrix}1 & 3\end{pmatrix}$

(c) $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4 & 5\end{pmatrix}$

2. This exercise can be solved in two ways.

   - Notice that

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

     and so $\pi^{-1} = \begin{pmatrix}4 & 3 & 5 & 1\end{pmatrix} = \begin{pmatrix}1 & 4 & 3 & 5\end{pmatrix}$.

   - Using Shoes and Socks,

     $$\pi^{-1} = \left(\begin{pmatrix}1 & 5 & 2\end{pmatrix}\begin{pmatrix}2 & 5 & 3 & 4\end{pmatrix}\right)^{-1} = \begin{pmatrix}2 & 5 & 3 & 4\end{pmatrix}^{-1}\begin{pmatrix}1 & 5 & 2\end{pmatrix}^{-1}.$$

     Now, $\begin{pmatrix}2 & 5 & 3 & 4\end{pmatrix}^{-1} = \begin{pmatrix}4 & 3 & 5 & 2\end{pmatrix} = \begin{pmatrix}2 & 4 & 3 & 5\end{pmatrix}$ and $\begin{pmatrix}1 & 5 & 2\end{pmatrix}^{-1} = \begin{pmatrix}2 & 5 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 5\end{pmatrix}$. Therefore $\pi^{-1} = \begin{pmatrix}2 & 4 & 3 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 5\end{pmatrix} = \begin{pmatrix}1 & 4 & 3 & 5\end{pmatrix}$.

3. To see why, consider the fact that elements of S_n are permutations. Each element is only able to permute the elements of the set $X = \{1, 2, 3, \ldots, n\}$. For a set of n elements, there are $n!$ permutations. Thus, $|\mathrm{S}_n| = n!$ since S_n is the set of all permutations of n letters.

Chapter 6

1. We work component-wise:

$$\begin{aligned}(s, rs)(r^2s, r^3) &= (sr^2s, rsr^3)\\ &= (s(r^2s), r(sr^3))\\ &= (s(sr), r(rs))\\ &= ((ss)r, (rr)s)\\ &= (r, r^2s)\end{aligned}$$

2. Note that $180 = 2^2 \times 3^2 \times 5$. By **Theorem I.6.1.5**, we must have $mn = 180$ and $\gcd(m, n) = 1$. Thus, the valid pairs of (m, n) are (4, 45), (5, 36), and (9, 20).

3. Note that $5 \otimes_{12} 7 = 11$. Hence $GH = \{1, 5, 7, 11\}$.

4. From above exercise, $GH = \mathcal{S}$. Now $G = \langle 5 \rangle \cong \mathbb{Z}_2$ and $H\langle 7 \rangle \cong \mathbb{Z}_2$. Thus, $\mathcal{S} = GH = \cong G \times H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = (\mathbb{Z}_2)^2$, meaning $n = 2$.

Chapter 7

1. ϕ is a homomorphism since

$$\begin{aligned} \phi(a \oplus_3 b) &= 2(a+b) \pmod 6 \\ &= 2a + 2b \pmod 6 \\ &= 2a \oplus_6 2b \\ &= \phi(a) \oplus_6 \phi(b). \end{aligned}$$

   The image is $\{0, 2, 4\}$.

2. ϕ is a homomorphism since

$$\begin{aligned} \phi(a+b) &= i^{a+b} \\ &= i^a i^b \\ &= \phi(a)\phi(b). \end{aligned}$$

   The kernel is the set of values which map to the identity of H, i.e. $\{n \in \mathbb{Z} \mid \phi(n) = 1\}$. Now note H is a cyclic group and $|i| = 4$. Thus $i^4 = 1$. Furthermore $i^8 = (i^4)^2 = 1, i^{12} = 1, \ldots, i^{4k} = 1$. Thus $\ker \phi = \{4n \mid n \in \mathbb{Z}\} = 4\mathbb{Z}$ (by using coset notation).

3. We prove the forward direction first. Suppose ϕ is one-one. Clearly $\phi(e_G) = e_H$. Let x be an element which is in the kernel of ϕ, meaning $\phi(x) = e_H$. Then, $\phi(x) = \phi(e_G) = e_H$ which means $x = e_G$ by injectivity of ϕ. Hence the kernel is trivial.

   Now we prove the reverse direction. Suppose the kernel of ϕ is trivial, i.e. $\ker \phi = \{e_G\}$. Suppose now there exists elements x and y in G such that $\phi(x) = \phi(y)$. This means that $(\phi(x))^{-1} = \phi(x^{-1}) = \phi(y^{-1}) = (\phi(y))^{-1}$. Hence,

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\left(\phi(y)\right)^{-1} = e_H.$$

Now since the kernel is trivial, this must mean that $xy^{-1} = e_G$ which immediately leads the $x = y$. Hence ϕ is injective.

4. The Fundamental Homomorphism Theorem states that $G/\ker\phi \cong \text{im}\,\phi$. Lagrange's Theorem states that $|G/\ker\phi| = \frac{|G|}{|\ker\phi|}$. Hence, $\frac{|G|}{|\ker\phi|} = |\text{im}\,\phi|$ which leads to the result quickly.

5. The Diamond Isomorphism Theorem (statement 6) states that $H/(H\cap N) \cong HN/N$. Taking orders on both sides yields $\frac{|H|}{|H\cap N|} = \frac{|HN|}{|N|}$. Rearranging yields required result.

6. (i) Since $x \mid y$, y is a multiple of x, say $y = kx$. Thus $H = x\mathbb{Z} = \{ax \mid a \in \mathbb{Z}\}$ and $N = kx\mathbb{Z} = \{a(kx) \mid a \in \mathbb{Z}\}$, which necessarily means $N \subseteq H$.

   (ii) Let $G = \mathbb{Z}$. Then both H and N are clearly subgroups of G. Now since G is abelian (since addition is commutative), therefore H and N are normal by **Proposition I.3.5.2**.

   (iii) By Third Isomorphism Theorem (**Theorem I.7.5.1**),

   $$(G/N)/(H/N) \cong G/H.$$

   Now by **Problem I.4.7**, $|G/H| = |\mathbb{Z}/(x\mathbb{Z})| = x$ and $|G/N| = |\mathbb{Z}/(y\mathbb{Z})| = y$. Hence

   $$\frac{x}{|H/N|} = y$$

   which quickly implies $|H/N| = \frac{y}{x}$.

Chapter 8

1. Consider $G = \mathbb{Z}_{mn}$. Clearly $H = \{0, n, 2n, \ldots, (m-1)n\}$ is a subgroup of $\mathbb{Z}_{mn}$ of order m. By **Problem I.3.5** we know H is normal and cyclic with order m and by **Exercise I.3.7** we know G/H is cyclic. The order of G/H is $\frac{|G|}{|H|} = \frac{mn}{m} = n$ by Lagrange's Theorem (**Theorem I.3.4.4**), meaning that $G/H \cong \mathbb{Z}_n$. Hence, $\mathbb{Z}_{mn}/\mathbb{Z}_m \cong G/H \cong \mathbb{Z}_n$.

2. Note 0 is the identity in $\mathbb{Z}_n$. By **Lemma I.8.1.1**, we know that if 12 is equivalent to the identity in $\mathbb{Z}_n$, then $12 = mn$ for some integer m. Since $n > 0$ we restrict m to positive integers. Now $12 = 2^2 \times 3$. Thus the possible cases are:
   - $n = 1$ with $m = 12$
   - $n = 2$ with $m = 6$
   - $n = 3$ with $m = 4$
   - $n = 4$ with $m = 3$
   - $n = 6$ with $m = 2$
   - $n = 12$ with $m = 1$
3. $|10| = \frac{210}{\gcd(10,210)} = \frac{210}{10}21$, $|42| = \frac{210}{\gcd(42,210)} = \frac{210}{42} = 5$, $|75| = \frac{210}{\gcd(75,210)} = \frac{210}{15} = 14$, and $|140| = \frac{210}{\gcd(140,210)} = \frac{210}{70} = 3$.
4. (a) Note that $10 = 2 \times 5$. Generators of the group $\mathbb{Z}_n$ (which has order 10) has to satisfy $\gcd(m, n) = 1$ by corollary. The positive integers that satisfy this requirement (and which are less than 10) are 1, 3, 7, 9. Thus they are the generators of $\mathbb{Z}_10$.

   (b) Note that 101 is prime. Hence all positive integers from 1 to 100 (inclusive) are generators.

5. We show that all subgroups of Q are, in fact, normal. We consider the first definition of the quaternion group.
   - Clearly $\{1\} \lhd \mathrm{Q}$ and $\mathrm{Q} \lhd \mathrm{Q}$.
   - The subgroups $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$ have order 4, so they have index 2 by Lagrange's Theorem (**Theorem I.3.4.4**). Hence by **Problem I.3.8** these subgroups are normal.
   - Consider the subgroup $\langle -1\rangle = \{1, -1\}$.
     - $1\langle -1\rangle = \langle -1\rangle 1$ since 1 is the identity;
     - $-1\langle -1\rangle = \{1, -1\} = \langle -1\rangle(-1)$;

- $i\langle -1\rangle = \{-i, i\} = \langle -1\rangle i$ and $-i\langle -1\rangle = \{i, -i\} = \langle -1\rangle(-i)$;
- $j\langle -1\rangle = \{-j, j\} = \langle -1\rangle j$ and $-j\langle -1\rangle = \{j, -j\} = \langle -1\rangle(-j)$; and
- $k\langle -1\rangle = \{-k, k\} = \langle -1\rangle k$ and $-k\langle -1\rangle = \{k, -k\} = \langle -1\rangle(-k)$.

Thus $\langle -1\rangle$ is normal.

Hence all subgroups of Q are normal.

6. $(2\ 6) = (2\ 3)(3\ 4)(4\ 5)(5\ 6)(4\ 5)(3\ 4)(2\ 3)$.
7. Note that $(1\ 3\ 2\ 5\ 4) = (1\ 4)(1\ 5)(1\ 2)(1\ 3)$. Thus by **Theorem I.8.3.8**, $(1\ 3\ 2\ 5\ 4)$ is even and thus has a sign of $+1$.
8. Note that A_3 has order $\frac{3!}{2} = 3$ so we should expect 3 permutations. Clearly the identity is one such permutation. Looking at **Example I.5.2.4** we can find two more: $(1\ 2\ 3)$ and $(1\ 3\ 2)$.
9. $\mathcal{U}_{10} = \{1, 3, 7, 9\}$.
10. By a corollary of Lagrange's Theorem (specifically, **Corollary I.3.4.4.1**), the order of a dives the order of the group $\mathcal{U}_n$. Now the order of $\mathcal{U}_n = \phi(n)$. Thus the order of a divides $\phi(n)$.
11. Note $1680 = 2^4 \times 3 \times 5 \times 7$. By the corollary we thus know

$$\mathcal{U}_{1680} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{4-2}} \times \mathbb{Z}_{3^1-3^0} \times \mathbb{Z}_{5^1-5^0} \times \mathbb{Z}_{7^1-7^0},$$

i.e. $\mathcal{U}_{1680} \cong (\mathbb{Z}_2)^2 \times (\mathbb{Z}_4)^2 \times \mathbb{Z}_6$.

12. The matrix product should be $\begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 2 \end{pmatrix}$.
13. We already proved that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ so we only need to prove normality.

    Let $\phi \in \mathrm{Aut}(G)$ and $\iota_g \in \mathrm{Inn}(G)$. For brevity let $f = \phi\iota_g\phi^{-1}$. We note that $f \in \mathrm{Aut}(G)$; we need to prove that $f \in \mathrm{Inn}(G)$.

Suppose $x \in G$ such that $w = \phi^{-1}(x)$ (as ϕ is an isomorphism, there exists a $w \in G$). Then

$$\begin{aligned} f(x) &= \phi\iota_g\phi^{-1}(x) \\ &= \phi(\iota_g(\phi^{-1}(x))) \\ &= \phi(\iota_g(w)) \\ &= \phi(gwg^{-1}) \\ &= \phi(g)\phi(w)\phi(g^{-1}) \\ &= \phi(g)x\left(\phi(g)\right)^{-1} \end{aligned}$$

which shows that $f \in \mathrm{Inn}(G)$. Hence, $f \in \mathrm{Inn}(G)$.

Chapter 9

1. We prove the two group action axioms.
   - **Identity**: $\alpha(e, x) = exe^{-1} = x$.
   - **Compatibility**: $\alpha(g, \alpha(h, x)) = \alpha(g, hxh^{-1}) = ghxh^{-1}g^{-1}$. Note that $(gh)^{-1} = h^{-1}g^{-1}$ by Shoes and Socks. Thus, $\alpha(g, \alpha(h, x)) = (gh)x(gh)^{-1} = \alpha(gh, x)$.

   Therefore α is a group action of G on G.

2. Recall there are 6 elements in S_3: id, $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$, $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$, $\begin{pmatrix}1 & 2\end{pmatrix}$, $\begin{pmatrix}1 & 3\end{pmatrix}$, and $\begin{pmatrix}2 & 3\end{pmatrix}$. Clearly the identity has all elements of X as fixed points. It is also clear that $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$ have no fixed points since they permute all elements. For the rest, the fixed points are the missing element from the cycle notation, i.e. $\begin{pmatrix}1 & 2\end{pmatrix}$ has fixed point 3, $\begin{pmatrix}1 & 3\end{pmatrix}$ has fixed point 2, and $\begin{pmatrix}2 & 3\end{pmatrix}$ has fixed point 1.

3. For 1, it is $\{\mathrm{id}, \begin{pmatrix}2 & 3\end{pmatrix}\}$. For 2, it is $\{\mathrm{id}, \begin{pmatrix}1 & 3\end{pmatrix}\}$. For 3, it is $\{\mathrm{id}, \begin{pmatrix}1 & 2\end{pmatrix}\}$.

4. We work from the statement forwards. Note that each of these

statements are "if and only if" statements.

$$\begin{aligned} g \cdot x = h \cdot x &\iff g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (h \cdot x) \\ &\iff (g^{-1}g) \cdot x = (g^{-1}h) \cdot x \\ &\iff e \cdot x = (g^{-1}h) \cdot x \\ &\iff x = (g^{-1}h) \cdot x \\ &\iff (g^{-1}h) \cdot x = x \\ &\iff g^{-1}h \in \mathrm{Stab}_G(x) \end{aligned}$$

5. We prove the forward direction first: suppose the action is transitive. Then there exists $x \in X$ such that $\mathrm{Orb}_G(x) = X$. Now consider any other element $y \in X$. Since the action is transitive, this means that there exists a $\hat{g} \in G$ such that $\hat{g} \cdot x = y$. Note that $\mathrm{Orb}_G(y) = \mathrm{Orb}_G(\hat{g} \cdot x)$, and that $\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}$. Hence,

$$\mathrm{Orb}_G(\hat{g} \cdot x) = \{g \cdot (\hat{g} \cdot x) \mid g \in G\} = \{(g\hat{g}) \cdot x \mid g \in G\}.$$

Since G is a group, $g\hat{g} \in G$. In particular, we may pick $g = g'\hat{g}^{-1}$ to obtain any arbitrary element $g' \in G$. Thus, this means that

$$\{(g\hat{g}) \cdot x \mid g \in G\} = \{g' \cdot x \mid g' \in G\} = \mathrm{Orb}_G(x) = X.$$

Hence, for any element $y \in X$, $\mathrm{Orb}_G(y) = \mathrm{Orb}_G(g \cdot x) = X$.

The reverse direction is trivial: suppose $\mathrm{Orb}_G(x) = X$ for all $x \in X$. Then certainly there exists an element $x \in X$ such that $\mathrm{Orb}_G(x) = X$.

6. (a) Clearly $e \cdot x = x$, so $x \in \mathrm{Orb}_G(x)$.

   (b) Suppose $x \in \mathrm{Orb}_G(x_1) \cap \mathrm{Orb}_G(x_2)$ (as their intersection is non-empty). Then there exists $g_1, g_2 \in G$ such that $g_1 \cdot x_1 =$

$x = g_2 \cdot x_2$. Thus,

$$\begin{aligned} x_1 &= e \cdot x_1 \\ &= (g_1^{-1} g_1) \cdot x_1 \\ &= g_1^{-1} \cdot (g_1 \cdot x_1) \\ &= g_1^{-1} \cdot (g_2 \cdot x_2) \\ &= (g_1^{-1} g_2) \cdot x_2. \end{aligned}$$

Now suppose $y \in \mathrm{Orb}_G(x_1)$. Then $y = g \cdot x_1$ for some $g \in G$. Hence,

$$\begin{aligned} y &= g \cdot x_1 \\ &= g \cdot \big((g_1^{-1} g_2) \cdot x_2\big) \\ &= (\underbrace{g g_1^{-1} g_2}_{\text{In } G}) \cdot x_2 \\ &\in \mathrm{Orb}_G(x_2) \end{aligned}$$

which means that any element in $\mathrm{Orb}_G(x_1)$ is also in $\mathrm{Orb}_G(x_2)$. Hence, $\mathrm{Orb}_G(x_1) \subseteq \mathrm{Orb}_G(x_2)$. A similar argument can be used to show that $\mathrm{Orb}_G(x_2) \subseteq \mathrm{Orb}_G(x_1)$. Hence $\mathrm{Orb}_G(x_1) = \mathrm{Orb}_G(x_2)$.

7. (a) Consider $x = n$. The orbit of n is all of X. Consider the permutation $\sigma = \begin{pmatrix} k & n \end{pmatrix}$ where $1 \leq k \leq n$. Clearly $\sigma \in \mathrm{S}_n$. Note that $\sigma \cdot n = \sigma(n) = k$. Thus, $\mathrm{Orb}_G(n) = X$, meaning that the group action $\cdot$ given by $g \cdot x \mapsto g(x)$ is transitive.

   (b) Note that $|X| = n$ and $|\mathrm{S}_n| = n!$. By Orbit-Stabilizer theorem, the stabilizer of x by G must have order $\frac{n!}{n} = (n-1)!$.

8. By the Orbit-Stabilizer theorem (**Theorem I.9.3.1**),

$$|\mathrm{Orb}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(x)|} = [G : \mathrm{Stab}_G(x)].$$

Under the group action of conjugation, $\mathrm{Orb}_G(x) = \mathrm{Cl}(x)$ and $\mathrm{Stab}_G(x) = \mathrm{C}_G(x)$. Hence, $|\mathrm{Cl}(x)| = [G : \mathrm{C}_G(x)]$ as required.

9. (a) One sees that $\mathrm{Z}(D_3) = \{e\}$ based on the group table of D_3.

(b) Recall that every element in D_3 can be expressed in the form $r^a s^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. One finds that $\mathrm{Cl}(r) = \{r, r^2\}$ and $\mathrm{Cl}(s) = \{s, rs, rs^2\}$.

(c) The class equation is $6 = 1 + 2 + 3$.

10. By Cauchy's Theorem (**Theorem I.9.7.1**) there exists an element (say x) with order p. Consider $H = \langle x \rangle$. Note that $|H| = p$ and $H \leq G$. Hence we found a subgroup of G of order p.

Chapter 10

1. We note that $12 = 2^2 \times 3$. Thus a Sylow 2-subgroup must have order 4. Clearly $|3| = 4$ so $\langle 3 \rangle = \{0, 3, 6, 9\}$ is the Sylow 2-subgroup of $\mathbb{Z}_{12}$.

2. Recall that $|\mathrm{S}_5| = 120 = 2^3 \times 3 \times 5$. By the First Sylow Theorem (**Theorem I.10.1.2**), $\mathrm{Syl}_p(G) \neq \varnothing$ if p is 2, 3, or 5.

3. We prove this by constructing the map $\phi : H \to gHg^{-1}$ where $h \mapsto ghg^{-1}$. We note that ϕ is an isomorphism.

   - **Homomorphism**: Let $x, y \in H$. Then

     $$\phi(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi(x)\phi(y)$$

     which clearly means that ϕ is an isomorphism.

   - **Injective**: Suppose $x, y \in H$ such that $\phi(x) = \phi(y)$. Then $gxg^{-1} = gyg^{-1}$ which quickly implies $x = y$ by cancellation law.

   - **Surjective**: Suppose $ghg^{-1} \in gHg^{-1}$. Clearly $\phi(h) = ghg^{-1}$.

   Hence $H \cong gHg^{-1}$.

4. By **Proposition I.10.2.3** we know that $|xyx^{-1}| = |y|$ for all $x, y \in G$. Substitute $x = g, y = hg$ yields

   $$|xyx^{-1}| = |ghgg^{-1}| = |gh|, |y| = |hg|$$

and the result follows.

5. Clearly $e \in \mathrm{N}_G(S)$ since $eSe^{-1} = eSe = S$, meaning that $\mathrm{N}_G(S)$ is non-empty. Consider $x, y \in \mathrm{N}_G(S)$, meaning that $xSx^{-1} = S$ and $ySy^{-1} = S$. Note that $y^{-1} \in \mathrm{N}_G(S)$ since

$$\begin{aligned} y^{-1}S\left(y^{-1}\right)^{-1} &= y^{-1}Sy \\ &= y^{-1}\left(ySy^{-1}\right)y \qquad (\text{since } y \in \mathrm{N}_G(S)) \\ &= (y^{-1}y)S(y^{-1}y) \\ &= S. \end{aligned}$$

Therefore

$$\begin{aligned} \left(xy^{-1}\right)S\left(xy^{-1}\right)^{-1} &= \left(xy^{-1}\right)S\left(yx^{-1}\right) \\ &= x\left(y^{-1}Sy\right)x^{-1} \\ &= xSx^{-1} \qquad (\text{since } y^{-1} \in \mathrm{N}_G(S)) \\ &= S \qquad (\text{since } x \in \mathrm{N}_G(S)) \end{aligned}$$

which means that $xy^{-1} \in \mathrm{N}_G(S)$. Hence by subgroup test $\mathrm{N}_G(S) \leq G$.

6. By the Second Sylow Theorem (**Theorem I.10.4.1**), we know that $gHg^{-1} = K$. Since $H \cong gHg^{-1}$ by **Exercise I.10.3** thus $H \cong gHg^{-1} = K$ as required.

7. We note $784 = 2^4 \times 7^2$, so $m = 16$, $p = 7$, and $k = 2$. By the Third Sylow Theorem (**Theorem I.10.5.1**), we know that

   a) $n_7 = [G : \mathrm{N}_G(P)] = \frac{|G|}{|\mathrm{N}_G(P)|}$;

   b) $n_7 \mid 16$, which implies $n_7 \in \{1, 2, 4, 8, 16\}$; and

   c) $n_7 \equiv 1 \pmod 7$, which implies $n_7 \in \{1, 8, 15, 22, \dots\}$.

   Hence $n_7 = 1$ or $n_7 = 8$. But since P is not a normal subgroup of G, by **Corollary I.10.4.1.1**, P cannot be the only Sylow 7-subgroup, meaning $n_7 \neq 1$. Hence $n_7 = 8$, so

$$8 = n_7 = \frac{|G|}{|\mathrm{N}_G(P)|} = \frac{784}{|\mathrm{N}_G(P)|}$$

which means that $|\mathrm{N}_G(P)| = 98$.

8. Note $130 = 2 \times 5 \times 13$. Consider the number of Sylow 13-subgroups, $n_1 3$. By the Third Sylow Theorem (**Theorem I.10.5.1**),

   - $n_1 3 \mid 2 \times 5 = 10$, so $n_1 3 \in \{1, 2, 5, 10\}$, and
   - $n_1 3 \equiv 1 \pmod{13}$ so $n_1 3 \in \{1, 14, 27, \dots\}$.

   Hence $n_1 3 = 1$. But by **Corollary I.10.4.1.1** this means that the only Sylow 13-subgroup is normal. Hence a group of order 130 is non-simple.

Problem Solutions

Chapter 1

1. (a) This is a group. The addition is clearly closed and associative. The identity is 0. The inverse of any element x is $-x$.

   (b) This is not a group. Inverses do not exist. For example, the element 2 does not have an inverse under multiplication.

   (c) This is a group. The multiplication is clearly closed and associative. The identity is 1. The inverse of any element x is $\frac{1}{x}$.

   (d) This is a group. The multiplication is clearly closed and associative. The identity is 0 and the inverse is 0.

   (e) This is not a group. The addition is not closed: $1 + 1 = 2$ which is not in the group.

   (f) This is a group. The multiplication is clearly closed and associative. The identity is 1 and the inverse is 1.

Chapter 2

1. The group table of D_4 is given below.

   (a) D_4 is not abelian because $rs \neq sr = r^3 s$.

$*$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

(b) We simplify $r^3srsr^3sr^3sr^2$.

$$\begin{aligned} r^3srsr^3sr^3sr^2 &= r^3sr(sr^3)(sr^3)sr^2 \\ &= r^3sr(e)sr^2 \\ &= r^3srsr^2 \\ &= r^3(srsr)r \\ &= r^3(e)r \\ &= r^4 \\ &= e \end{aligned}$$

2. If every element in G is its own inverse, then for every element g in G, $g^{-1} = g$. Consider $(gh)^{-1}$ where g and h are elements in g. On one hand, by Shoes and Socks, $(gh)^{-1} = h^{-1}g^{-1} = hg$ since each element is its own inverse. On the other hand, since gh is an element in G, thus $(gh)^{-1} = gh$. Thus, $gh = hg$ which means G is abelian.

3. (a) Note that $(gh)^2 = ghgh$. Given that $(gh)^2 = ghgh = g^2h^2 = gghh$. By cancellation law, $hg = gh$ which means G is abelian.

   (b) Suppose G is abelian. Clearly $(gh)^1 = gh$. Suppose $(gh)^k =$

$g^k h^k$ for some positive integer k. Then

$$\begin{aligned}
(gh)^{k+1} &= (gh)(gh)^k \\
&= (gh)(g^k h^k) && \text{by assumption} \\
&= ghg^k h^k \\
&= g(hg^k)h^k \\
&= g(g^k h)h^k && \text{since } G \text{ is abelian} \\
&= gg^k hh^k \\
&= g^{k+1}h^{k+1}
\end{aligned}$$

so $(gh)^{k+1} = g^{k+1}h^{k+1}$ assuming $(gh)^k = g^k h^k$. By mathematical induction, the claim is proven.

4. Note that $|1| = n$ since $1^2 = 1 \oplus_n 1 = 2$, $1^3 = 1 \oplus_n 1 \oplus_n 1 = 3$, $1^4 = 4$, ..., $1^{n-1} = n - 1$ and $1^n = 0$ which is the identity. Since the group $(\mathbb{Z}_n, \oplus_n)$ has an element with the same order as the group, it is thus cyclic with order n and generator 1.

5. We show that $(A, \circ)$ is a group.

   - **Closure**: Function composition is closed by definition.
   - **Associativity**: Function composition is associative.
   - **Identity**: Notice by brute-force computation, that $T^6(x, y) = (x, y)$. Hence T^6 is the identity of A.
   - **Inverse**: If r is a multiple of 6 then T^r is its own inverse. Otherwise, T^{6-r} is the inverse of T^r.

   Thus, $(A, \circ)$ is a group, with order 6.

Chapter 3

1. We note that the elements of G are $\{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$.

   (a) Yes, this is the trivial group.

(b) No, it is not closed. (rs can be generated by $r * s$ but is not in the set)

(c) No, the identity e is missing.

(d) Yes, $\{r, r^3, r^4, r^6\} = \{r, r^3, e, r^2\} = \langle r \rangle$.

2. (a) Clearly $e \in K$ since $e \in G$ and $ehe^{-1} = h \in H$ for all h in H.

Suppose x and y are in K, meaning $xhx^{-1} \in H$ and $yhy^{-1} \in H$ for all h in H. Supposing $yhy^{-1} = \hat{h}$, then $(xy^{-1})\hat{h}(xy^{-1})^{-1} = xy^{-1}\left(yhy^{-1}\right)yx^{-1} = xhx^{-1}$ which is clearly and element of h. Thus xy^{-1} is in K. By subgroup test, $K \leq G$.

(b) Note that the identity of K, e, is also the identity of G. Since $H \leq G$, thus $e \in H$. Since H is a subgroup of G, $xy^{-1} \in H$ by subgroup test. Hence $H \leq K$.

3. (a) We have proved that $\mathrm{Z}(G) \leq G$ so we only prove normality. Let g and z be arbitrary elements from G and $\mathrm{Z}(G)$ respectively. Then

$$\begin{aligned} gzg^{-1} &= g(zg^{-1}) \\ &= g(g^{-1}z)(\text{since } z \in \mathrm{Z}(G)) \\ &= (gg^{-1})z \\ &= z \\ \in \mathrm{Z}(G) & \end{aligned}$$

which proves that $\mathrm{Z}(G) \lhd G$.

(b) We first work in the forward direction by assuming $G = \mathrm{Z}(G)$. Then by definition for all $z \in \mathrm{Z}(G) = G$ we have $gz = zg$ for any $g \in G$, which means that G is abelian.

We now work in the reverse direction by assuming that G is abelian. The normal subgroup $\mathrm{Z}(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}$. But since G is abelian, $gh = hg$ for all g and h in G. Thus every element in G satisfies the condition to be in the center of G, meaning $\mathrm{Z}(G) = G$.

(c) We note that $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$. Since $\mathrm{Z}(D_4)$ is a subgroup of D_4 it has a maximum order of 2, by Lagrange's theorem. Since 2 is prime the subgroups must be cyclic. Thus the non-trivial subgroups of D_4 are $\{e, r^2\}$ and $\{e, s\}$ (since $|r^2| = |s| = 2$). Now like how we proved that $\langle s\rangle = \{e, s\}$ is not a normal subgroup in D_3 in **Example I.3.5.3**, $\{e, s\}$ is not a normal subgroup of D_4. One verifies easily that $\{e, r^2\} = \langle r^2\rangle$ is a normal subgroup of D_4. Thus $\mathrm{Z}(D_4) = \langle r^2\rangle$ since $\mathrm{Z}(D_4)$ must be a normal subgroup of D_4 with order not exceeding 2 (and since $\{e\} \leq \langle r^2\rangle$).

4. (a) We will prove this statement.

   Clearly $e \in H \cap K$ since $e \in H$ and $e \in K$ as both are subgroups of G.

   Let x and y be in $H \cap K$, meaning that $x, y \in H$ and $x, y \in K$. Thus $xy^{-1} \in H$ and $xy^{-1} \in K$ as both are subgroups of G. Hence $xy^{-1} \in H \cap K$. By subgroup test, $H \cap K \leq G$.

   (b) We will prove this statement. One sees that $H \cap K \subseteq H$. Since $H \cap K \leq G$, it is thus a group. Hence $H \cap K \leq H$ by definition of a subgroup.

   (c) We will disprove this statement. Consider:

   $$G = \{0, 1, 2, 3, 4, 5\} \text{ under } \oplus_6,$$
   $$H = \{0, 2, 4\}, \text{ and}$$
   $$K = \{0, 3\}.$$

   Clearly $H \leq G$ and $K \leq G$. Note $H \cup K = \{0, 2, 3, 4\}$. But $H \cup K$ is not closed since $2 \oplus_6 3 = 5 \notin H \cup K$. Hence $H \cup K \not\leq G$.

   (d) We will disprove this statement. Since $H \cup K$ is not closed it is not a group, meaning it cannot be a subgroup.

5. Suppose $G = \langle g\rangle$ and $H \leq G$. Then any element in H is of the form g^a where a is an integer. Suppose m is the smallest integer m such that $g^m \in H$. Suppose now $h = g^n$ for some n. By the

division algorithm, $n = mq + r$ where q and r are non-negative integers such that $0 \leq r < m$. Hence,

$$g^n = g^{mq}g^r = (g^m)^q g^r.$$

Now, m is the smallest integer m such that $g^m \in H$. This means that if $r \neq 0$, $g^r \notin H$ as $0 \leq r < m$. Hence, $r = 0$, which means

$$g^n = (g^m)^q.$$

Thus, every element in the subgroup H can be formed by applying g^m a certain number of times, meaning $H = \langle g^m \rangle$ which means H is cyclic.

6. By Lagrange's Theorem (**Theorem I.3.4.4**), the order of a subgroup must divide the order of the group. Since $H \leq G$ is non-trivial, and since $1024 = 2^1 0$, the largest order that H can be is 512 with $[G : H] = 2$. An example is $G = \mathbb{Z}_{1024}$ and $H = \langle 2 \rangle$, since $|2| = 512$ as $2 \times 512 = 1024 \equiv 0 \pmod{1024}$.

7. Let $|G| = 2n$. Suppose on the contrary that there does not exist an element with order 2, so every element (except the identity) has order greater than 2.

   Suppose we have an element in the group which has even order, say the element x with order $2m$. This means that $x^{2m} = e$. But this means that $(x^m)^2 = e$, meaning that the element x^m has order 2. This contradicts the assumption that every non-identity element has order greater than 2. Hence, we conclude that every element must have odd order. However, a corollary of Lagrange's Theorem (**Corollary I.3.4.4.1**) states that the order of the element must be a multiple of the order of the group. Hence, Thus means that all elements, which have odd order, divides the order of the group, which is an even number, which is a contradiction.

   Therefore, we contradicted our original premise that a finite group with even order does not have an element with order 2. Hence, there must be an element in G with order 2.

8. Let xH be a coset in G. Since cosets partition G, either $xH = H$ or $xH = G \setminus H$ (since there are only two distinct cosets).

- If $xH = H$, then x is in H, meaning $xH = H = Hx$.
- If $xH \neq H$, then $x \in G \setminus H$. Hence $xH = G \setminus H = Hx$.

Therefore H is a normal subgroup of G, i.e. $H \lhd G$.

9. Suppose we have an element $x \in H \cap K$, meaning that $x \in H$ and $x \in K$. By a corollary of Lagrange's Theorem (**Corollary I.3.4.4.1**), the order of x must divide the order of its group. Hence, $|x|$ divides $|H|$ and $|x|$ divides $|K|$ simultaneously, meaning that $|x| = \gcd(|H|, |K|)$. But the GCD of the orders of both subgroups is 1. Hence, $|x| = 1$, meaning the only element in the intersection $H \cap K$ is the identity e.

10. (a) $m = 6$.

    (b) We first prove that all groups of order less than 6 are abelian, and then find a non-abelian group of order 6.

    We note that a group of order 1 is the trivial group which is abelian. The groups of order 2, 3, and 5 are groups of prime order, meaning that they are cyclic and hence abelian. We are left with a group of order 4.

    By a corollary of Lagrange's Theorem (**Corollary I.3.4.4.1**), the order of an element of a group of order 4 must divide 4. Hence the possible orders of an element in such a group is 1, 2, or 4. An element of order 1 is the identity. If an element with order 4 exists, then the group is cyclic and hence abelian. So we assume that all elements are either order 1 or order 2 (in fact, the orders are 1, 2, 2, 2). This is precisely the group

    $$D_2 = \langle r, s \mid r^2 = s^2 = e, rs = sr \rangle$$

    which clearly is abelian. Hence all groups of order 4 are abelian.

    We now show that a group of order 6 can be non-abelian. We note that the group

    $$D_3 = \langle r, s \mid r^3 = s^2 = e, rs = sr^2 \rangle$$

has order 6 and because $rs = sr^2 \neq sr$, thus D_3 is non-abelian. Hence $m = 6$.

(c) For all even $n \geq 6$, the group $D_{\frac{n}{2}}$ has n elements and $rs = sr^{\frac{n}{2}-1} \neq sr$, so $D_{\frac{n}{2}}$ is non-abelian.

11. Suppose $G/\mathrm{Z}(G)$ is cyclic. Then by definition, $G/\mathrm{Z}(G) = \langle g\mathrm{Z}(G)\rangle$ for some $g \in G$, and any element in $G/\mathrm{Z}(G)$ is of the form $g^n\mathrm{Z}(G)$.

Now take $x, y \in G$. By **Lemma I.3.4.2** left cosets partition the group, so we may assume $x \in g^m\mathrm{Z}(G)$ and $y \in g^n\mathrm{Z}(G)$, meaning $x = g^m z_1$ and $y = g^n z_2$ for some $z_1, z_2 \in \mathrm{Z}(G)$. We note

$$\begin{aligned}
xy &= (g^m z_1)(g^n z_2) \\
&= g^m(z_1 g^n)z_2 \\
&= g^m(g^n z_1)z_2 && \text{(since } z_1 \in \mathrm{Z}(G)\text{)} \\
&= (g^m g^n)(z_1 z_2) \\
&= g^{m+n} z_1 z_2 \\
&= g^{n+m} z_2 z_1 \\
&= g^n g^m z_2 z_1 \\
&= g^n(g^m z_2)z_1 \\
&= g^n(z_2 g^m)z_1 \\
&= (g^n z_2)(g^m z_1) \\
&= yx
\end{aligned}$$

which means that $xy = yx$ for any $x, y \in G$. Hence G is abelian.

Chapter 4

1. We will prove that f is a homomorphism, is injective, and is surjective.

- **Homomorphism**: Let $x, y \in G$. Then

$$\begin{aligned} f(xy) &= g(xy)g^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= f(x)f(y) \end{aligned}$$

  which means that f is a homomorphism.

- **Injective**: Let $x, y \in G$ be such that $f(x) = f(y)$. Then $gxg^{-1} = gyg^{-1}$. By cancellation law, $x = y$.

- **Surjective**: Suppose $y \in G$. Set $x = g^{-1}yg$. Since G is closed, thus $x \in G$. Note $f(x) = g(g^{-1}yg)g^{-1} = y$. Hence y has a pre-image of $g^{-1}yg$ in G.

Therefore f is an isomorphism.

2. Suppose on the contrary there exists an isomorphism $\phi : G \to H$. Since ϕ is an isomorphism, it is surjective. Hence, there must exists a rational number $r \in G$ such that $\phi(r) = 2$. As r is rational, so is $\frac{r}{2}$.

   Now consider $\phi\left(\frac{r}{2} + \frac{r}{2}\right)$. On one hand, $\phi\left(\frac{r}{2} + \frac{r}{2}\right) = \phi(r) = 2$. On another hand, $\phi(\frac{r}{2} + \frac{r}{2}) = \left(\phi\left(\frac{r}{2}\right)\right)^2$ as ϕ is a homomorphism. Therefore, $\left(\phi\left(\frac{r}{2}\right)\right)^2 = 2$ which quickly implies $\phi\left(\frac{r}{2}\right) = \sqrt{2}$ since $\phi\left(\frac{r}{2}\right)$ must be positive. However, $\sqrt{2} \notin H$, meaning we have reached a contradiction.

   Hence, $G \ncong H$.

3. (a) Let $m, n \in G$. Then

$$\phi(m + n) = 2(m + n) = 2m + 2n = \phi(m) + \phi(n)$$

   which means ϕ is a homomorphism.

   (b) Suppose $m, n \in G$ such that $\phi(m) = \phi(n)$. Then $2m = 2n$. Clearly this means that $m = n$. Thus ϕ is injective.

   (c) Suppose on the contrary there existed a homomorphism $\psi : H \to G$ such that $\psi(\phi(n)) = n$. Then $\psi(2n) = n$ by defini-

tion of ϕ. Note that

$$\psi(2n) = \psi(n+n) = \psi(n) + \psi(n) = 2\psi(n)$$

since ψ is a homomorphism. Hence $2\psi(n) = n$ which implies that $\psi(n) = \frac{n}{2}$. But for the case of $n = 1$, $\psi(1) = \frac{1}{2} \notin G$. Hence ψ does not exist.

4. We prove the forward direction first: assume that G is abelian. Then f is a homomorphism since

$$f(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = f(g)h(g).$$

We now prove the reverse direction: assume that f is a homomorphism, meaning $f(gh) = f(g)f(h) = g^{-1}h^{-1}$. But $f(gh) = (gh)^{-1} = h^{-1}g^{-1}$. Therefore we have $g^{-1}h^{-1} = h^{-1}g^{-1}$ which clearly shows that the group operation is commutative. Hence G is abelian.

5. Suppose $\phi : G \to H$ is a surjective homomorphism and G is abelian. Since ϕ is surjective, thus im $\phi = H$. Consider $\phi(g_1g_2)$ where $g_1, g_2 \in G$ such that $\phi(g_1) = h_1 \in H$ and $\phi(g_2) = h_2 \in H$.

   - On one hand, $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = h_1h_2$.
   - On another hand, $\phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1$.

   Hence $h_1h_2 = h_2h_1$ which means that H is abelian.

6. We first prove $\phi(N)$ is a subgroup of H by using subgroup test before proving normality.

   Note that $e_H \in \phi(N)$ since $e_G \in N$ and $\phi(e_G) = e_H$. Now let $x, y \in \phi(N)$. As ϕ is surjective, we know that there exists $n_x, n_y \in N$ where $\phi(n_x) = x$ and $\phi(n_y) = y$. Note that $\phi(n_y^{-1}) = y^{-1}$ and $n_xn_y^{-1} \in N$. Hence, $xy^{-1} = \phi(n_xn_y^{-1}) \in \phi(N)$. By subgroup test, $\phi(N) \leq H$.

   We now show that $\phi(N)$ is a normal subgroup of H. Take $g \in G$, $h \in H$, $n \in N$, and $x \in \phi(N)$, such that $\phi(g) = h$ and $\phi(n) = x$.

Note that since $N \lhd G$, thus $gng^{-1} \in N$. Therefore,

$$\begin{aligned} hxh^{-1} &= \phi(g)\phi(n)\phi(g^{-1}) \\ &= \phi(\underbrace{gng^{-1}}_{\text{In } N}) \\ &\in \phi(N) \end{aligned}$$

which means that $\phi(N) \lhd H$.

7. Consider the map $\phi : G \to H, a \mapsto a + n\mathbb{Z}$ (note that G and H are additive groups, so we use $+$ instead of $\times$). We show that ϕ is an isomorphism:

   - **Homomorphism**: Let a and b be in G. Then

   $$\begin{aligned} \phi(a \oplus_n b) &= (a + b) + n\mathbb{Z} \\ &= \{a + b + pn \mid p \in \mathbb{Z}\} \\ &= \{a + b + pn + qn \mid p, q \in \mathbb{Z}\} \\ &= a + b + n\mathbb{Z} + n\mathbb{Z} \\ &= (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \\ &= \phi(a) + \phi(b). \end{aligned}$$

   - **Injective**: Let a and b be in G such that $\phi(a) = \phi(b)$. Thus

   $$\{a + pn \mid p \in \mathbb{Z}\} = \{b + qn \mid q \in \mathbb{Z}\}$$

   by definition of ϕ. Hence $a \equiv b \pmod{n}$. But since $0 \leq a, b < n$, we must have $a = b$.

   - **Surjective**: Let $x + n\mathbb{Z} \in H$. We perform the division algorithm on x to yield

   $$x = qn + r, \text{ where } 0 \leq r < n.$$

Note that

$$\begin{aligned} x + n\mathbb{Z} &= \{x + kn \mid k \in \mathbb{Z}\} \\ &= \{(qn + r) + kn \mid k \in \mathbb{Z}\} \\ &= \{r + n(\underbrace{q + k}_{\text{In } \mathbb{Z}}) \mid k \in \mathbb{Z}\} \\ &= r + n\mathbb{Z} \end{aligned}$$

with $0 \leq r < n$, meaning $r \in G$. Now observe $\phi(r) = r + n\mathbb{Z} = x + n\mathbb{Z}$ which means that there is a pre-image for every element in H, hence proving that ϕ is surjective.

Therefore ϕ is an isomorphism, proving $G \cong H$.

8. Consider the map $\phi : G \to G/N$ such that $g \mapsto gN$. We note that ϕ is a homomorphism as

$$\phi(gh) = (gh)N = (gN)(hN) = \phi(g)\phi(H).$$

We note by **Proposition I.4.2.3** that $A = \phi^{-1}(B) \leq G$. Note that

$$\begin{aligned} \phi^{-1}(N) &= \{g \in G \mid \phi(g) = N\} \\ &= \{g \in G \mid gN = N\} \\ &= \{g \in G \mid g \in N\} \\ &= G \cap N \\ &= N \subseteq A \end{aligned}$$

by assumption. Since N is a group we know $N \leq A$. Furthermore $N \leq A \leq G$ and $N \lhd G$, meaning $N \lhd A$ (since $gN = Ng$ for all $g \in G$, including those in A). Hence A/N is a group.

Now clearly ϕ is surjective (since for any $gN \in G/N$ we know $\phi(g) = gN$), which means that $\phi(\phi^{-1}(B)) = B$. Since $\phi^{-1}(B) = A$ hence $\phi(A) = B$. Finally,

$$\begin{aligned} \phi(A) &= \{\phi(a) \mid a \in A\} \\ &= \{aN \mid a \in A\} \\ &= A/N \end{aligned}$$

which means $B = A/N$.

Chapter 5

1. We work from the right to the left.
   - $\gamma\delta$ has cycle notation $\begin{pmatrix}1 & 2 & 5\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}1 & 3 & 2 & 5\end{pmatrix} = \begin{pmatrix}1 & 4 & 3 & 5 & 2\end{pmatrix}$;
   - $\beta\gamma\delta$ has cycle notation $\begin{pmatrix}1 & 5 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}1 & 4 & 3 & 5 & 2\end{pmatrix} = \begin{pmatrix}1 & 3 & 2 & 5\end{pmatrix} = \delta$; and
   - $\alpha\beta\gamma\delta$ has cycle notation $\begin{pmatrix}1 & 5 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 3 & 2 & 5\end{pmatrix} = (1)$, the identity.

   Hence $\alpha\beta\gamma\delta = \mathrm{id}$.

2. Recall that D_3 has presentation
$$\langle r, s \mid r^3 = s^2 = e, rs = sr^2 \rangle.$$
   Let the map $\phi : D_3 \to \mathrm{S}_3$ be given such that $r \mapsto \begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and $s \mapsto \begin{pmatrix}1 & 2\end{pmatrix}$. We show that $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and $\begin{pmatrix}1 & 2\end{pmatrix}$ obey the two rules above. For brevity let $\sigma = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and $\tau = \begin{pmatrix}1 & 2\end{pmatrix}$.
   - We check that $\phi(r^3) = \phi(s^2) = \phi(e)$:
     - $\sigma^2 = \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\end{pmatrix}$ and $\sigma^3 = \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 3 & 2$ id; and
     - $\tau^2 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \mathrm{id}$.
   - We check that $\phi(rs) = \phi(sr^2)$.
     - $rs \mapsto \sigma\tau = \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix}$; and
     - $sr^2 \mapsto \tau\sigma^2 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix}$.

   Thus $D_3 \cong \mathrm{S}_3$.

3. $|\mathrm{S}_4| = 4! = 24$.
   (a) Consider $H = \left\langle \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} \right\rangle$. For brevity let $\sigma = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}$. Note that

- $\sigma^2 = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}$;
- $\sigma^3 = \begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}$; and
- $\sigma^4 = \mathrm{id}$.

Thus, $|\sigma| = 4$ which means $|H| = 4$. Therefore, $G \cong H \leq \mathrm{S}_4$.

(b) Let $\sigma = \begin{pmatrix}1 & 2\end{pmatrix}$ and $\tau = \begin{pmatrix}3 & 4\end{pmatrix}$. Let H have presentation $\langle \sigma, \tau \rangle$. Construct the map $\phi : G \to H$ such that $a \mapsto \sigma$ and $b \mapsto \tau$. Notice that

- $\sigma^2 = \mathrm{id}$;
- $\tau^2 = \mathrm{id}$; and
- $(\sigma\tau)^2 = \mathrm{id}$.

Therefore, $G \cong H \leq \mathrm{S}_4$.

Chapter 6

1. Let $g_1, g_2 \in G$ and $h_1, h_2 \in H$. Then note $(g_1, h_1), (g_2, h_2) \in G \times H$, and observe

$$\begin{aligned}(g_1, h_1)(g_2, h_2) &= (g_1 g_2, h_1 h_2) \\ &= (g_2 g_1, h_2 h_1) \\ &= (g_2, h_2)(g_1, h_1)\end{aligned}$$

which means that $G \times H$ is abelian.

2. We note that we **cannot** directly apply 'direct product equivalence' since we do not know whether G and H are subgroups of a larger group (and whether that larger group is indeed the inner product of G and H). Thus we need to construct an explicit isomorphism.

Let the map $\phi : G \times H \to H \times G, (g, h) \mapsto (h, g)$. We prove that ϕ is an isomorphism:

- **Homomorphism**: Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then

$$\begin{aligned}\phi((g_1, h_1)(g_2, h_2)) &= \phi((g_1 g_2, h_1 h_2)) \\ &= (h_1 h_2, g_1 g_2) \\ &= (h_1, g_1)(h_2, g_2) \\ &= \phi((g_1, h_1))\phi((g_2, h_2))\end{aligned}$$

  which proves that ϕ is a homomorphism.

- **Injective**: Suppose there exists $(g_1, h_1), (g_2, h_2) \in G \times H$ such that $\phi((g_1, h_1)) = \phi((g_2, h_2))$. Then $(h_1, g_1) = (h_2, g_2)$ by definition of ϕ. Clearly by comparing component parts of each ordered pair, we have $g_1 = g_2$ and $h_1 = h_2$, meaning $(g_1, h_1) = (g_2, h_2)$. Hence ϕ is injective.

- **Surjective**: Let $(h, g) \in H \times G$. Clearly $(g, h) \in G \times H$ and $\phi((g, h)) = (h, g)$, meaning that (h, g) has a pre-image of (g, h). Therefore ϕ is surjective.

Therefore ϕ is an isomorphism, meaning $G \times H \cong H \times G$.

3. We need to check 3 things.

   - $\boxed{G = HK}$ Observe that

$$\begin{aligned}HK &= \{h \oplus_6 k \mid h \in H, k \in K\} \\ &= \{0 \oplus_6 0, 0 \oplus_6 3, 2 \oplus_6 0, 2 \oplus_6 3, 4 \oplus_3 0, 4 \oplus_3 3\} \\ &= \{0, 3, 2, 5, 4, 1\} \\ &= \mathbb{Z}_6 \\ &= G\end{aligned}$$

     so in fact $G = HK$.

   - $\boxed{H \cap K = \{e\}}$ Clearly $H \cap K = \{0\}$.

   - $\boxed{hk = kh}$ Since $\oplus_6$ is commutative, thus $h \oplus_6 k = k \oplus_6$.

   Thus G is the internal direct product of H and K.

4. Define the subgroups $H = \{e, a\}$ and $K = \{e, b\}$. We show the V is the internal direct product of H and K.

   - $\boxed{\text{V} = HK}$ Observe that

   $$\begin{aligned} HK &= \{hk \mid h \in H, k \in K\} \\ &= \{ee, eb, ae, ab\} \\ &= \{e, b, a, ab\} \\ &= \text{V} \end{aligned}$$

   so in fact $\text{V} = HK$.

   - $\boxed{H \cap K = \{e\}}$ Clearly $H \cap K = \{e\}$.

   - $\boxed{hk = kh}$ Clearly if one of the elements is the identity then result follows. So assume that h and k are both non-identity elements, i.e. $h = a$, $k = b$. Note

   $$\begin{aligned} kh &= ba \\ &= (ba)\,((ab)(ab)) && (\text{since } (ab)^2 = e) \\ &= (baab)(ab) \\ &= (bb)(ab) && (\text{since } a^2 = e) \\ &= ab && (\text{since } b^2 = e) \\ &= hk \end{aligned}$$

   so in fact $hk = kh$ for all $h \in H$, $k \in K$.

   Therefore V is the internal direct product of H and K. We note $H = \langle a \rangle \cong \mathbb{Z}_2$ and $K = \langle b \rangle \cong \mathbb{Z}_2$. By direct product equivalence (**Theorem I.6.3.1**) we know $\text{V} \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = (\mathbb{Z}_2)^2$.

Chapter 7

1. Construct the map $\phi : G \to \{e\}$ where $\phi(g) = e$. Clearly ϕ is a homomorphism as

$$\phi(gh) = e = ee = \phi(g)\phi(h).$$

Also, one sees that $\operatorname{im}\phi = \{e\}$ and $\ker\phi = G$, so by the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**) we have

$$G/\ker\phi \cong \operatorname{im}\phi$$

which immediately implies $G/G \cong \{e\}$.

2. Consider $\phi : G \to R$ where $(x, y) \mapsto x\sqrt{3} - y\sqrt{2}$. We note that ϕ is indeed a homomorphism as

$$\begin{aligned}\phi((x_1, y_1)(x_2, y_2)) &= \phi((x_1 + x_2, y_1 + y_2)) \\ &= (x_1 + x_2)\sqrt{3} - (y_1 + y_2)\sqrt{2} \\ &= (x_1\sqrt{3} - y_1\sqrt{2}) + (x_2\sqrt{3} - y_2\sqrt{2}) \\ &= \phi((x_1, y_1)) + \phi((x_2, y_2)).\end{aligned}$$

We note that ϕ is surjective. This is because for any $r \in R$, we have $\phi((\frac{r}{\sqrt{3}}, 0)) = \frac{r}{\sqrt{3}} \times \sqrt{3} + 0 = r$ and $(\frac{r}{\sqrt{3}}, 0) \in G$. Hence ϕ is surjective, meaning $\operatorname{im}\phi = R$.

We now find the kernel of ϕ.

$$\begin{aligned}\ker\phi &= \{(x, y) \in G \mid \phi((x, y)) = 0\} \\ &= \{(x, y) \in G \mid x\sqrt{3} - y\sqrt{2} = 0\} \\ &= \{(x, y) \in G \mid y = \frac{\sqrt{3}}{\sqrt{2}}x\} \\ &= \{(x, \frac{\sqrt{3}}{\sqrt{2}}x) \mid x \in \mathbb{R}\} \\ &= \{(r\sqrt{2}, \frac{\sqrt{3}}{\sqrt{2}}(r\sqrt{2})) \mid r \in \mathbb{R}\} \\ &= \{(r\sqrt{2}, r\sqrt{3}) \mid r \in \mathbb{R}\} \\ &= H.\end{aligned}$$

Thus, by the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**, we have $G/H \cong R$.

3. (i) Let $(m_1, n_1), (m_2, n_2) \in G$. Then

$$\begin{aligned}\phi((m_1, n_1)(m_2, n_2)) &= \phi((m_1 + m_2, n_1 + n_2)) \\ &= (m_1 + m_2 - n_1 - n_2, (n_1 + n_2) \mod 5) \\ &= ((m_1 - n_1) + (m_2 - n_2), \\ &\qquad (n_1 \mod 5) + (n_2 \mod 5)) \\ &= (m_1 - n_1, n_1 \mod 5)(m_2 - n_2, n_2 \mod 5) \\ &= \phi((m_1, n_1))\phi((m_2, n_2))\end{aligned}$$

which means that ϕ is a homomorphism.

(ii) Suppose $(x, y) \in H$. We note $(x + y, y) \in G$ and $0 \leq y < 5$. Observe $\phi((x + y, y)) = ((x + y) - y, y \mod 5) = (x, y)$. Hence ϕ is surjective.

(iii) We first compute the kernel of ϕ.

$$\begin{aligned}\ker \phi &= \{(m, n) \in G \mid \phi((m, n)) = (0, 0)\} \\ &= \{(m, n) \in G \mid (m - n, n \mod 5) = (0, 0)\} \\ &= \{(m, 5k) \in G \mid (m - 5k, 0) = (0, 0)\} \\ &= \{(5k, 5k) \mid k \in \mathbb{Z}\} \\ &= K\end{aligned}$$

Hence by Fundamental Homomorphism Theorem (**Theorem I.7.3.1** we have $G/K \cong H$.

4. We are given that $K \subseteq H$. Hence

$$\begin{aligned}HK &= \{hk \mid h \in H, k \in K \subseteq H\} \\ &\subseteq \{hk \mid h \in H, k \in H\} \\ &= \{h_1 h_2 \mid h_1, h_2 \in H\} \\ &= H. \qquad (H \text{ is closed since } H \leq G)\end{aligned}$$

Therefore $HK \subseteq H$. Also, we know that $H \leq HK$ by the Diamond Isomorphism Theorem (**Theorem I.7.4.1**), statement 3. Hence we obtain the fact that $H \leq HK \subseteq H$ which means $HK = H$ as required.

5. (i) Consider the map $\phi : I \to G, (g, g^{-1}) \mapsto g$. We show that ϕ is an isomorphism:

   - **Homomorphism**: Recall that G is abelian, so $gh = hg$ for any $g, h \in G$. Consider $(g, g^{-1}), (h, h^{-1}) \in I$. Then

   $$\begin{aligned}\phi((g, g^{-1})(h, h^{-1})) &= \phi((gh, g^{-1}h^{-1})) \\ &= \phi((gh, h^{-1}g^{-1})) \\ &= \phi((gh, (gh)^{-1})) \\ &= gh \\ &= \phi((g, g^{-1}))\phi((h, h^{-1})).\end{aligned}$$

   - **Injective**: Suppose $(g, g^{-1}), (h, h^{-1}) \in I$ such that $\phi((g, g^{-1})) = \phi((h, h^{-1}))$. Then $g = h$ by definition of ϕ which clearly means $(g, g^{-1}) = (h, h^{-1})$.
   - **Surjective**: Suppose $g \in G$. Then $(g, g^{-1}) \in I$ and $\phi((g, g^{-1})) = g$.

   Hence ϕ is an isomorphism, meaning $I \cong G$.

   (ii) Consider the map $\psi : G^2 \to G, (g_1, g_2) \mapsto g_1 g_2$. We note ψ is a homomorphism since

   $$\begin{aligned}\psi((g_1, g_2)(h_1, h_2)) &= \psi((g_1 g_2, h_1 h_2)) \\ &= g_1 g_2 h_1 h_2 \\ &= g_1 h_1 g_2 h_2 \\ &= (g_1 h_1)(g_2 h_2) \\ &= \psi((g_1, h_1))\psi((g_2, h_2)).\end{aligned}$$

   We now show that ψ is surjective. Consider any $g \in G$. Clearly we have $\psi((g, e)) = ge = g$, so ψ is surjective, meaning $\text{im}\, \psi = G$.

We now find the kernel of ψ.

$$\begin{aligned}\ker\psi &= \{(g,h) \in G^2 \mid \psi((g,h)) = e\} \\ &= \{(g,h) \in G^2 \mid gh = e\} \\ &= \{(g,h) \in G^2 \mid h = g^{-1}\} \\ &= \{(g,g^{-1}) \mid g \in G\} \\ &= I.\end{aligned}$$

Thus, by the Fundamental Homomorphism Theorem (**Theorem I.7.3.1**, we have $G^2/I \cong G$. But since $I \cong G$, we further have $G^2/G \cong G$ as needed.

6. We will prove that ϕ is a homomorphism first:

$$\begin{aligned}\phi(am+bm) &= \phi((a+b)m) \\ &= a+b \mod \frac{n}{m} \\ &= (a \mod \frac{n}{m}) + (b \mod \frac{n}{m}) \\ &= \phi(am) + \phi(bm).\end{aligned}$$

Now ϕ is clearly surjective since for any $x \in \mathbb{Z}_{\frac{n}{m}}$, $\phi(xm) = x \mod \frac{n}{m}$. Thus $\operatorname{im}\phi = H$.

We find the kernel of ϕ:

$$\begin{aligned}\ker\phi &= \{am \in mz \mid \phi(am) = 0\} \\ &= \{am \in mz \mid a \equiv 0 \pmod{\frac{n}{m}}\} \\ &= \{am \in mz \mid am \equiv 0 \pmod{n}\} \\ &= \{am \in mz \mid am \in n\mathbb{Z}\} \\ &= n\mathbb{Z}\end{aligned}$$

By Fundamental Homomorphism Theorem,

$$G/H \cong \mathbb{Z}_{\frac{n}{m}}.$$

Chapter 8

1. We note that the two questions are equivalent to finding the orders of 3774 and 1870 in the group $\mathbb{Z}_{10101}$. Notice that:

$$\begin{aligned} 1870 &= 2 \times 5 \times 11 \times 17 \\ 3774 &= 2 \times 3 \times 17 \times 37 \\ 10101 &= 3 \times 7 \times 13 \times 37 \end{aligned}$$

   Therefore, $\gcd(1870, 10101) = 1$ and $\gcd(3774, 10101) = 3 \times 37 = 111$. Hence $|1870| = 10101$ and $|3774| = \frac{10101}{111} = 91$. Therefore, $a = 10101$ and $b = 91$.

2. We claim that A_n is non-abelian for $n > 3$. Note that $\pi = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$ are both even permutations, and hence are in A_n for $n > 3$. We note

   - $\pi\sigma = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$; and
   - $\sigma\pi = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}$.

   Hence $\pi\sigma \neq \sigma\pi$ for A_n where $n > 3$, meaning that A_n is non-abelian for $n > 3$. Thus the largest integer n for which A_n is abelian is $n = 3$.

   Now a cyclic group necessarily has to be abelian. Thus $k = 2$ or $k = 3$ are the only possibilities. We note $|\mathrm{A}_2| = \frac{2!}{2} = 1$ so A_2 is isomorphic to the trivial group (which is cyclic) and $|\mathrm{A}_3| = \frac{3!}{2} = 3$ and so by a corollary of Lagrange's Theorem (**Corollary I.3.4.4.3**) we know A_3 is cyclic. Hence $k = 2$ or $k = 3$.

3. We first note that

$$\varphi(2p^k) = 2p^k \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p}\right) = p^k \left(1 - \frac{1}{p}\right) = \varphi(p^k).$$

   Now we are given that r is an odd primitive root of p^k. Then $\gcd(r, 2p^k) = 1$ since $\gcd(r, p^k) = 1$ (as $r \in \mathcal{U}_{p^k}$) and because r is odd, so $r \in \mathcal{U}_{2p^k}$. Let $n = |r|$ in $\mathcal{U}_{2p^k}$. Then by **Exercise I.8.10**, n divides $\varphi(2p^k)$. But at the same time, r is a generator in $\mathcal{U}_{p^k} \cong$

$\mathbb{Z}_{\phi(p^k)}$, so $\varphi(p^k) = \varphi(2p^k)$ divides n by **Lemma I.8.1.1**. Since n divides $\varphi(2p^k)$ and $\varphi(2p^k)$ divides n simultaneously, therefore $n = \varphi(2p^k) = |\mathcal{U}_{2p^k}|$ which means that r is a primitive root modulo $2p^k$.

4. (i) The forward direction is clearly true so we only prove the reverse direction. Assume $f(g) = h(g)$. Note that

$$f(g^k) = (f(g))^k = (h(g))^k = h(g^k)$$

for any integer k. Since g is a generator, thus we have $f(x) = h(x)$ for all $x \in G$, meaning $f = h$.

(ii) We note $f(g) \in G$. Since g is a generator hence $f(g) = g^k$ for some k. Hence any homomorphism from G to G is of the form $f(g) = g^{m_f}$ where $0 \leq m_f \leq n-1$.

(iii) Consider $f(h(g))$. On one hand,

$$f(h(g)) = f(g^{m_h}) = (f(g))^{m_h} = g^{m_f m_h},$$

while on the other,

$$f(h(g)) = (f \circ h)(g) = g^{m_{f\circ h}}.$$

Therefore $m_{f\circ h} \equiv m_f m_h \pmod{n}$. In other words, $m_{f\circ h} = m_f \otimes m_h$.

(iv) We prove the forward direction first by assuming that f is an automorphism. Hence f is surjective, meaning that there exists an $a \in G$ such that $f(a) = g$. Since $a \in G$ thus $a = g^k$ for some $k \in \mathbb{Z}_n$ (we will show $k \in \mathcal{U}_n$ later). Observe

$$g = f(a) = f(g^k) = (f(g))^k = g^{m_f k}$$

which means $m_f k \equiv 1 \pmod{n}$. By **Proposition 0.4.0.2**, this means that $\gcd(m_f, n) = 1$ and $\gcd(k, n) = 1$, so $m_f, k \in \mathcal{U}_n$. Hence k is the multiplicative inverse of m_f.

We now prove the reverse direction. Assume m_f has a multiplicative inverse (say k), meaning $m_f k \equiv 1 \pmod{n}$. As above this means $m_f, k \in \mathcal{U}_n$. We show that f is an isomorphism.

- **Injective**: Suppose $x, y \in G$ such that $f(x) = f(y)$. Since g is a generator we may take $x = g^p$ and $y = g^q$. Hence we have $g^{m_f p} = g^{m_f q}$. Then

$$(g^{m_f p})^k = g^{k m_f p} = \left(g^{k m_f}\right)^p = g^p$$

and $(g^{m_f q})^k = g^q$. Hence this implies $g^p = g^q$ which means $x = y$.

- **Surjective**: Suppose $x \in G$. Since g is a generator we may take $x = g^p$. Then $f(g^{kp}) = g^{m_f kp} = g^p = x$.

Hence f is an isomorphism. Since $f : G \to G$, it is thus an automorphism.

(v) We prove that ϕ is an isomorphism.

- **Homomorphism**: Let $f, h \in \mathrm{Aut}(G)$. Then $\phi(f \circ h) = m_{f\circ h} = m_f \otimes_n m_h = \phi(f) \otimes_n \phi(h)$.
- **Injective**: Suppose $f, h \in \mathrm{Aut}(G)$ such that $\phi(f) = \phi(h)$, meaning $m_f = m_h$. By (i) and (ii), the value of m uniquely defines a homomorphism from G to G. Hence $f = h$.
- **Surjective**: Suppose $r \in \mathcal{U}_n$. Define $f : G \to G$ where $f(g) = g^r$. Since $r \in \mathcal{U}_n$ it has a multiplicative inverse, which means that f is an automorphism by (iii). Clearly $\phi(f) = r$, so r has a pre-image.

Hence ϕ is an isomorphism, meaning $\mathrm{Aut}(G) \cong \mathcal{U}_n$.

Chapter 9

1. (a) Since $G = D_5$ has order $10 = 2 \times 5$, by **Theorem I.9.7.1**, G must have subgroups of orders 2 and 5.

   (b) For the one with order 2, $\{e, s\} \leq G$. For the one with order 5, $\{e, r, r^2, r^3, r^4\} \leq G$.

2. Let $x \in X$. By the Orbit-Stabilizer theorem (**Theorem I.9.3.1**), $|\text{Orb}_G(x)| = \frac{|G|}{|\text{Stab}_G(x)|}$. Since $\text{Stab}_G(x) \leq G$ thus it has order of either 1, 5, or 25 by Lagrange's Theorem. Hence, the number of elements in $\text{Orb}_G(x)$ is either 1, 5, or 25.

   Now X has 24 elements. Thus $|\text{Orb}_G(x)| \neq 25$ since $\text{Orb}_G(x)$ can, at most, be the entire set X which has 24 elements. Hence $\text{Orb}_G(x)$ has either 1 or 5 elements. Now by **Exercise I.9.6**, distinct orbits must partition the set X. Let the number of orbits of size 1 be a and the number of orbits of size 5 be b. Hence, $1a + 5b = 24$. Since b is an integer, thus $5b$ must be a multiple of 5, which means that $a \geq 1$. Hence, there exists an orbit of size 1, which means that there is a fixed point.

3. Suppose that $n = kp$ where p is an odd prime. Then there must exist an element, say x, such that $x^p = e$ by Cauchy's Theorem (**Theorem I.9.7.1**). But all elements in G satisfy $x^2 = e$. Since p is odd thus $x^p \neq e$ which is a contradiction. Hence, n cannot be a multiple of an odd prime, meaning that $n = 2^k$ where k is a positive integer.

4. We define the map $\phi : G \to S, g \mapsto g \cdot x$ where $x \in S$ is a fixed element. We show that ϕ is a bijection.

   - **Injective**: Suppose $g, h \in G$ are such that $\phi(g) = \phi(h)$, meaning that $g \cdot x = h \cdot x$. Hence $(g^{-1}h) \cdot x = x$ which quickly implies that $g^{-1}h = e$ since the group action is free. Therefore $g = h$ which proves that ϕ is injective.
   - **Surjective**: Suppose $y \in S$. Then since the group action is transitive, there must exist an element $g \in G$ such that $g \cdot x = y$. Hence, $\phi(g) = g \cdot x = y$, meaning that the pre-image of y is g. Therefore ϕ is surjective.

   Thus ϕ is bijective, which means that $|G| = |S|$.

5. We note that the group in question that acts upon the bracelet is the group D_3. We consider Burnside's Lemma (**Lemma I.9.4.2**) to answer this question. There are 6 actions to consider:

- $\boxed{e}$: The number of fixed points is the total number of colourings, n^3.
- $\boxed{r}$: Rotating bracelet 120° results in all points affecting one another, so the only fixed points would be colourings of the same colour. There are n such arrangements.
- $\boxed{r^2}$: Similar argument as r yields n arrangements.
- $\boxed{s}$: This 'fixes' one bead and flips the other two about a line. A fixed point thus requires the two beads that flipped about the line to be of the same colour, while the third bead is free. Hence, there are n^2 possible colourings.
- $\boxed{rs}$: We note that rs is yet another reflection. Thus a similar argument as s yields n^2 arrangements.
- $\boxed{r^2s}$: Similar argument as s yields n^2 arrangements.

Note that $|D_3| = 6$, so by Burnside's Lemma,

$$|X/G| = \frac{1}{6}\left(n^3 + n + n + n^2 + n^2 + n^2\right) = \frac{1}{6}n(n+1)(n+2)$$

meaning that the total number of distinct braces of 3 beads with n colours is $\frac{1}{6}n(n+1)(n+2)$.

6. Let G be a group of order p^2. We note that $\mathrm{Z}(G) \leq G$, so by Lagrange's Theorem (**Theorem I.3.4.4**) the order of $\mathrm{Z}(G)$ must divide the order of G, meaning $|\mathrm{Z}(G)|$ divides p^2. Hence $|\mathrm{Z}(G)|$ is 1, p, or p^2.

   We note that $|\mathrm{Z}(G)| \neq 1$ by **Example I.9.6.3**, so we consider the case where $|\mathrm{Z}(G)| = p$. We note

   $$|G/\mathrm{Z}(G)| = \frac{|G|}{|\mathrm{Z}(G)|} = \frac{p^2}{p} = p$$

   so $G/\mathrm{Z}(G)$ is a non-trivial group of prime order. Hence by a corollary of Lagrange's Theorem (**Corollary I.3.4.4.3**), $G/\mathrm{Z}(G)$ is cyclic. Hence, by **Problem I.3.11**, $G = \mathrm{Z}(G)$. But this means $p^2 = |G| = |\mathrm{Z}(G)| = p$ which is a contradiction.

Hence $|\mathrm{Z}(G)| = p^2$. Since $\mathrm{Z}(G) \leq G$ and $|G| = |\mathrm{Z}(G)| = p^2$, therefore $G = \mathrm{Z}(G)$, meaning G is abelian by **Problem I.3.3**.

7. We first look at elements inside Ω. Suppose $x \in \Omega$. Then $g \cdot x = x$ for any $g \in G$. Recall that $\mathrm{Orb}_G(x) = \{y \in X \mid g \cdot x = y \text{ for some } x \in X\}$. Hence if $x \in \Omega$ then $\mathrm{Orb}_G(x) = \{x\}$ which means $|\mathrm{Orb}_G(x)| = 1$.

   Now consider $x \notin \Omega$, meaning $|\mathrm{Orb}_G(x)| \neq 1$. Recall $|G| = p^n$ for some $n \geq 1$ and prime p. By Orbit-Stabilizer theorem (**Theorem I.9.3.1**), one obtains

   $$|\mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Orb}_G(x)|} = \frac{p^n}{|\mathrm{Orb}_G(x)|}.$$

   Since $|\mathrm{Stab}_G(x)|$ is an integer, thus $\frac{p^n}{|\mathrm{Orb}_G(x)|}$ must be an integer, meaning $|\mathrm{Orb}_G(x)|$ divides p^n. Therefore if $x \notin \Omega$ then $|\mathrm{Orb}_G(x)| \equiv 0 \pmod{p}$.

   Finally, recall that by **Exercise I.9.6** distinct orbits partition X. Hence the number of elements in X is the sum of the number of elements in each of the distinct orbits of X. Now for each orbit $\mathrm{Orb}_G(x)$ where $x \notin \Omega$, the number of elements in it is a multiple of p, while for $x \in \Omega$ there is only one element in its orbit. Hence, $|X| \equiv |\Omega| \pmod{p}$ since there are $|\Omega|$ orbits with only one element.

Chapter 10

1. Note $200 = 2^3 \times 5^2$. Note that when $p = 5$ we have $m = 8$ and the factors of 8 are 1, 2, 4, and 8. Futhermore by the Third Sylow Theorem (**Theorem I.10.5.1**) we must have $n_5 \equiv 1 \pmod{5}$. Hence $n_5 = 1$. By a corollary of the Second Sylow Theorem (**Corollary I.10.4.1.1**) this means that the only Sylow 5-subgroup is normal.

2. Note $33 = 3 \times 11$. Note that

- when $p = 3$ we have $m = 11$ and the factors of 11 are 1 and 11; and
- when $p = 11$ we have $m = 3$ and the factors of 3 are 1 and 3.

Furthermore $n_p \equiv 1 \pmod{p}$ by the Third Sylow Theorem (**Theorem I.10.5.1**). Hence we must have $n_3 = n_{11} = 1$. By a corollary of the Second Sylow Theorem (**Corollary I.10.4.1.1**) this means that the only Sylow 3-subgroup and Sylow 11-subgroup are normal.

3. For simplicity let $q = 2^p - 1$, and we are given that q is a prime. By the Third Sylow Theorem (**Theorem I.10.5.1**), $n_q \mid 2^{p-1}$ and $n_q \equiv 1 \pmod{p}$. The factors of 2^{p-1} are $1, 2, 4, 8, \ldots, 2^{p-1}$. We note $2^{p-1} < 2^p - 1 = q$ for any prime p since

$$2^{p-1} + 1 < 2^{p-1} + 2^{p-1} = 2(2^{p-1}) = 2^p$$

which result immediately follows by subtracting 1 on both sides. Hence, the only possible value that satisfies both conditions is $n_q = 1$. By a corollary of the Second Sylow Theorem (**Corollary I.10.4.1.1**) this means that the only Sylow q-subgroup is normal, hence showing that a group with an order that is an even perfect number is non-simple.

4. (i) The divisors of p are 1 and p itself. By the Third Sylow Theorem (**Theorem I.10.5.1**), n_q divides p and $n_q \equiv 1 \pmod{q}$. Since $p < q$ hence $p \not\equiv 1 \pmod{q}$ meaning that $n_q = 1$. By a corollary of the Second Sylow Theorem (**Corollary I.10.4.1.1**) the only Sylow q-subgroup is normal.

   (ii) The divisors of q are 1 and q itself. By the Third Sylow Theorem (**Theorem I.10.5.1**), n_p divides q and $n_p \equiv 1 \pmod{p}$. Since by assumption $q \not\equiv 1 \pmod{p}$ hence $n_p = 1$.

   Now a corollary of Lagrange's Theorem (**Corollary I.3.4.4.1**) tells us that the order of an element in a group of order pq must divide pq. Hence the possible orders of an element in such a group are 1, p, q, or pq.

- There is only one element of order 1, the identity.
- There are $p-1$ elements of order p, all belonging in the single Sylow p-subgroup. Note that we subtract 1 because one element in the Sylow p-subgroup is the identity.
- There are $q-1$ elements of order q, all in the single Sylow q-subgroup.

Hence, since the total number of elements in a group of order pq is pq, the number of elements of order pq is

$$\begin{aligned} pq - ((p-1) + (q-1) + 1) &= pq - (p + q - 1) \\ &= pq - p - q + 1 \\ &> 2q - 2 - q + 1 \\ &= 2q - q - 1 \\ &= q - 1 \\ &> 0 \end{aligned}$$

which means that there is at least one element of order pq. By **Theorem I.2.4.4** this means that such a group is cyclic.

5. We note $3325 = 5^2 \times 7 \times 19$. Let the group of order 3325 be G. We know that
   - for $p = 5$ we have $m = 7 \times 19 = 133$ and so divisors of m are $\{1, 7, 19, 133\}$;
   - for $p = 7$ we have $m = 5^2 \times 19 = 475$ and so divisors of m are $\{1, 5, 19, 25, 95, 475\}$; and
   - for $p = 19$ we have $m = 5^2 \times 7 = 175$ and so divisors of m are $\{1, 5, 7, 25, 35, 175\}$.

   Furthermore, by the Third Sylow Theorem (**Theorem I.10.5.1**), $n_p \equiv 1 \pmod{p}$. Thus $n_5 = n_7 = n_{19} = 1$. Let P, Q, and R be the Sylow 5-subgroup, the Sylow 7-subgroup, and the Sylow 19-subgroup respectively.

Denote the group QR by H. Since Q and R are of prime order, their intersection is the identity (**Problem I.3.9**). Therefore $H \cong Q \times R$, so $|H| = |Q||R| = 7 \times 19 = 133$. Furthermore as Q and R are of prime order, thus Q and R are abelian and so is H. Hence H is an abelian group of order 133.

Now consider the group PH. Since 5 and 133 are coprime, thus $P \cap H = \{e\}$. In addition P is abelian by **Problem I.9.6**, and H is also abelian as discussed above, so $gh = hg$ for all $g \in P$ and $h \in H$. Finally,

$$|PH| = \frac{|P||H|}{|P \cap H|} = |P||H| = 5^2 \times 133 = 3325 = |G|$$

so G is the internal direct product of P and H, meaning $G \cong P \times H$. As the external direct product of two abelian groups is also abelian (**Problem I.6.1**) thus G is abelian.

6. (i) Let P be a Sylow p-subgroup of N. Lagrange's Theorem (**Theorem I.3.4.4**) tells us that $|G| = [G : N]|N|$. Since p does not divide $[G : N]$ we must have $|N| = p^k a$ where a divides m. Hence $|P| = p^k$. Since P has order p^k and $P \leq N \leq G$, thus P is also a Sylow p-subgroup of G.

   (ii) Suppose Q is a Sylow p-subgroup of G. By the Second Sylow Theorem (**Theorem I.10.4.1**), we know there exists $g \in G$ such that $Q = gPg^{-1}$. Recall by definition of normality that $gNg^{-1} = N$ for any $g \in G$. Note also that $P \leq N$. Hence,

   $$Q = gPg^{-1} \leq gNg^{-1} = N$$

   which means that Q is also a Sylow p-subgroup of N.

7. Let P be a Sylow p-subgroup of G. We note that $|G/P| = \frac{p^k m}{p^k} = m$. Let G act on the set of cosets G/P by left multiplication, meaning $g \cdot xP = (gx)P$. By **Theorem I.9.1.5**, this induces a homomorphism $\phi : G \to \mathrm{S}_m$ where $\phi(g) = \sigma_g$ such that $\sigma_g(xP) = g \cdot xP = (gx)P$. By **Example I.10.6.5**, $\ker \phi = \bigcap_{x \in G} xPx^{-1}$.

   We note $\ker \phi \neq \{e\}$ since otherwise it would imply that ϕ is injective (**Exercise I.7.3**), which is impossible as that would

mean $p^k m = |G| \leq |\mathrm{S}_m| = m!$ which is a contradiction. Suppose $\ker \phi = G$, then

$$p^k m = |G| = |\ker \phi| = \left| \bigcap_{x \in G} xPx^{-1} \right| \leq |xPx^{-1}| = |P| = p^k,$$

which would mean $m = 1$, a contradiction. Thus $\ker \phi \neq G$. Hence $\ker \phi$ is a proper subgroup of G. We note that $\ker \phi \lhd G$, so we have found a proper normal subgroup of G, meaning that G is non-simple.

8. We prove that G has a normal subgroup of order p, q, or r. By **Corollary I.10.4.1.1**, subgroups of order p, q, or r are normal if they are unique. By way of contradiction, assume that they are not unique, meaning $n_p, n_q, n_r > 1$.

   By the Third Sylow Theorem (**Theorem I.10.5.1**), $n_r \equiv 1 \pmod{r}$ and $n_r \mid pq$. The divisors of pq are 1, p, q, and pq. We note that since $p, q < r$, thus $p \not\equiv 1 \pmod{r}$ and $q \not\equiv 1 \pmod{r}$. The only possibility that is left is $n_r = pq$ as we assume $n_r \neq 1$. Similarly, $n_q \equiv 1 \pmod{q}$ and $n_q \mid pr$. The divisors of pr are 1, p, r, and pr. Since $p < q$ thus $p \not\equiv 1 \pmod{q}$. Hence $n_q \geq r$ as we assume $n_q \neq 1$. Similarly, $n_p \geq q$.

   We consider now the number of elements of order p, q, and r.

   - $\boxed{p}$ With $n_p \geq q$, there are at least $q(p-1)$ elements of order p. We minus 1 because one of the elements in a Sylow p-subgroup is the identity with order 1.
   - $\boxed{q}$ With $n_q \geq r$, there are at least $r(q-1)$ elements of order q.
   - $\boxed{r}$ We know $n_r = pq$ so there are exactly $pq(r-1)$ elements of order r.

   Since the total number of elements, pqr, must be at least the sum

of the numbers of these elements, thus

$$\begin{aligned} pqr &\geq q(p-1) + r(q-1) + pq(r-1) \\ &= pq - q + qr - r + pqr - pq \\ &= pqr + qr - q - r \end{aligned}$$

which means $qr - q - r \leq 0$. Rearranging, we see $q \leq \frac{r}{r-1} = 1 + \frac{1}{r-1}$. Since $p < q$ and they are both primes, we must have $q \geq 3$. Hence one sees

$$3 \leq q \leq 1 + \frac{1}{r-1} \leq 2$$

which is a clear contradiction. Hence, at least one of n_p, n_q, or n_r is 1, meaning that there exists a proper normal subgroup in G by **Corollary I.10.4.1.1**. Therefore G is non-simple.

Image Acknowledgements

Images are cited as they appear.

Chapter 1

- Image of the triangle is released under the public domain by user `Jim.belk` on Wikimedia at `https://commons.wikimedia.org/wiki/File:Labeled_Triangle_Reflections.svg`.
- Image of the circular decorative knot with twelve crossings is released under the public domain by user `AnonMoos` on Wikimedia at `https://commons.wikimedia.org/wiki/File:Circular-cross-decorat` `svg`.
- Points in the pane is my own work.

Chapter 2

- Images of symmetries of an equilateral triangle and a square taken from [Mil21] p. 13.

Chapter 4

- The function mapping diagram is my own work.

Chapter 5

- All possible function mappings in S_3 is my own work.

Chapter 7

- Commutativity diagram for the Fundamental Homomorphism Theorem is my own work.
- Subgroup lattice for the Diamond Isomorphism Theorem was adapted from the image by user `Aleksandr Omelchenko` on Wikimedia at `https://commons.wikimedia.org/wiki/File:Diagram_for_the_First_Isomorphism_Theorem.png`.

Chapter 9

- Labelled square is my own work.

References and Bibliography

[Wie59] Helmut Wielandt. "Ein Beweis für die Existenz der Sylowgruppen". In: *Archiv der Mathematik* 10.1 (1959), pp. 401–402. DOI: 10.1007/bf01240818.

[Hun80] Thomas W. Hungerford. *Algebra*. 8th ed. Springer, 1980. ISBN: 978-0-387-90518-1.

[Coh82] Paul Moritz Cohn. *Algebra*. 2nd ed. Vol. 1. Wiley, 1982. ISBN: 978-0-471-10169-7.

[Cla84] Allan Clark. *Elements of abstract algebra*. 47.3. Dover Publications, 1984. ISBN: 978-0-486-64725-8.

[Hum96] John F. Humphreys. *A course in group theory*. 1st ed. Oxford University Press, 1996. ISBN: 978-0-198-53459-4.

[CB09] Mariana Ruth Cook and Richard Ewen Borcherds. "Richard Ewen Borcherds". In: *Mathematicians: An Outer View of the Inner World*. 1st ed. Princeton University Press, 2009, p. 24. ISBN: 978-0-691-13951-7.

[Man11] Kathryn Mann. *NOTES ON SYLOW'S THEOREMS*. 2011. URL: https://math.berkeley.edu/~kpmann/SylowNotes.pdf.

[Pro19] ProofWiki. *Order of group element in group direct product*. 2019. URL: https://proofwiki.org/wiki/Order_of_Group_Element_in_Group_Direct_Product.

[Mil21] James S. Milne. *Group Theory (v4.00)*. 2021. URL: www.jmilne.org/math/.

[Pro21] ProofWiki. *Burnside's Lemma*. 2021. URL: https://proofwiki.org/wiki/Burnside%27s_Lemma.

[Pro22] ProofWiki. *Infinite cyclic group is isomorphic to integers*. 2022. URL: https://proofwiki.org/wiki/Infinite_Cyclic_Group_is_Isomorphic_to_Integers.

[Res22] Google Research. *4.3: Image and kernel*. 2022. URL: https://math.libretexts.org/@go/page/675.

[Bri] *Group actions*. URL: https://brilliant.org/wiki/group-actions/.

[Row] Todd Rowland. *Group action*. URL: https://mathworld.wolfram.com/GroupAction.html.