Math 100A Notes

Abstract Algebra: Group Theory

Fall 2021

Taught by Professor Kiran Kedlaya

Table of Contents

1 Introduction to Binary Operations

We want to explore the idea behind *algebraic structures*. In particular, we want to explore these structures in more detail compared to earlier courses (either in past college or high school algebra classes).

To do this, we need to think about *what* algebra really is. We might think about solving equations like $x^2 + 3x + 5 = 0$ for x. In particular, what is really happening here?

Well, there are a couple of operations going on. Specifically, we have *addition* and *multiplication*.

$$x \times x + 3 \times x + 5 = 0$$

We now want to examine these operations. Both of these operations $(+, \times)$ take in two numbers and output one number. The question we might have, then, is: how can we can generalize these operations?

1.1 Binary Operations

A **binary operation** is a way of taking in two values and outputting one value. Of course, we might now ask: what can these values be? These values can come from any specific set.

For example, we can consider addition over the integers ($\mathbb{Z}$). The sum of two integers is an integer. Similarly, we could consider multiplication over the integers. Again, the product of two integers is an integer. We could also consider multiplication or addition over the real, rational, or complex numbers.

The idea is that whatever "type" we give our binary operation, we will get that same "type" for our output. To formalize this, we have the following definition:

Definition 1.1: Binary Operation

A binary operation (also known as the law of composition) consists of:

- A set S.
- An operation; more concretely, a function $S \times S \mapsto S$.

More formally, a binary operation $*$ over a set S is a function mapping $f : S \times S \mapsto S$. For each $(a, b) \in S \times S$, we can denote the element $f(a, b)$ of S by $a * b$.

In this class, for $a, b \in S$, we will represent binary operations in one of several ways:

- ab
- $f(a, b)$
- $a * b$

Remark:

- An element $a \in S$ (where S is a set equipped with a binary operation $*$) is *invertible* if there is another element b such that:
$$a * b = \text{id} \qquad b * a = \text{id}$$

1.1.1 Examples of Binary Operations

Some common examples of binary operations are:

- $\mathbb{Z}$ under addition.
- $\mathbb{Z}$ under subtraction.

- $\mathbb{Z}$ under multiplication.
- $\mathbb{R}$ under addition.
- $\mathbb{R}$ under subtraction.
- $\mathbb{R}$ under multiplication.
- M_2 ($\mathbb{R}$) under multiplication (here, M_2 denotes a 2×2 square matrix).
- String concatenation.

1.1.2 Non-Examples of Binary Operations

One common non-example of a binary operation is $\mathbb{R}$ under division. This is because:

- Dividing a non-zero number by 0 (for example, $\frac{5}{0}$) produces undefined behavior. In other words, what is the result of this?
- Dividing 0 by 0 is ambiguous. For example, this could be infinity, or it could be undefined.

If we were to assume some value for a division-by-zero operation, then the operation would **not be closed**. That is, while we know that $0 \in \mathbb{R}$ and $n \in \mathbb{R}$ (denote n to be any number in $\mathbb{R}$), we could say that $\frac{n}{0} = \infty$, but we know that $\infty \notin \mathbb{R}$, so the operation is not closed.

1.2 More on Binary Operations

Anything that is "like" addition or multiplication is probably a binary operation. For example, let's consider **matrices**.

- Addition of matrices of a fixed dimension. More specifically, the set of $n \times m$ matrices (here, n and m are fixed positive integers) over the integers, rationals, reals, or complex numbers under matrix addition is a binary operation.

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

- Multiplication of matrices of a fixed dimension. More specifically, the set of $n \times n$ matrices (square matrices). We could also just multiply a $n \times m$ matrix by a $k \times l$ matrix assuming $m = k$ (otherwise, multiplying these two matrices will result in undefined behavior).

So far, we considered binary operations on infinite sets in which we need some sort of formula to describe (e.g. $f_{\cup}(A, B) = A \cup B$). Now, if we have a finite set, we could define a binary operation exhaustively by just saying what the binary operation does on every pair of entries.

For example, given the set $S = \{a, b, c, d, e\}$. We can define a binary operation on S with the below **function table**:

	a	b	c	d	e
a	a	c	d	d	e
b	b	c	c	b	a
c	d	e	e	b	b
d	a	a	a	c	a
e	b	b	c	c	d

Denote the binary operation to be #.

- What is $c\#d$? The answer is b.
- What is $e\#((a\#b)\#c)$? The answer is d.
- Suppose we have $X\#a = a$. What is X? The answer is $X = a, d$.

1.3 Properties of Binary Operations

What properties could binary operations have?

- **Commutativity:** A binary operation is commutative if the order of the two inputs does not matter. For example, if f is a function corresponding to a binary operation, then:

  $$f(a,b) = f(b,a) \quad \forall a, b \in S$$

  More commonly:

  $$a * b = b * a \quad \forall a, b \in S$$

  For example, addition or multiplication of numbers is commutative. Unions and intersections of sets is also commutative. *However*, matrix multiplication is *not* commutative. Our example above is also not commutative.

- **Associativity:** A binary operation is associative if the order of applying the operation (in a string) does not matter. Specifically:

  $$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$$

  Which means that we can write $a * b * c$ (or even abc) without ambiguity.

  For example, addition or multiplication of numbers is associative. Addition or multiplication of matrices is also associative. Our example above is not associative.

- **Identity:** A binary operation has a two-sided identity element and a two-sided inverse for every element.

  More specifically, we say that id is a left identity if $f(\text{id}, s) = s$ for all $s \in S$. id is a right identity if $f(s, \text{id}) = s$ for all $s \in S$. Then, id is a two-sided identity if it is both a left identity and right identity.

  For example, 0 is a two-sided identity for addition and 1 is a two-sided identity for multiplication. For matrix addition, the zero-matrix is a two-sided identity. For matrix multiplication, the matrix with ones on the diagonal and zeros everywhere else is the identity element. In our example above, # does not have a left or right identity.

  As a fact, there can be **at most** one identity element for any given binary operation. The proof is discussed later.

- **Inverse:** For a general associative binary operation $f : S \times S \mapsto S$ with a two-sided identity id, an element $s \in S$ has a two-sided inverse if it has a left inverse (denote this $l \in S$) and a right inverse (denote this $r \in S$); that is:

  $$\overbrace{f(l,s)}^{\text{Left Inverse}} = \underbrace{f(s,r)}_{\text{Right Inverse}} = \text{id}$$

  We often write s^{-1} to mean an inverse of s when it exists. So, for instance (both ways are the same thing), we could have written:

  $$f(s^{-1}, s) = f(s, s^{-1}) = \text{id}$$
  $$s^{-1} * s = s * s^{-1} = \text{id}$$

  There are several common examples. In addition, this is the negative/negation. In other words, the additive inverse of x is $-x$. In multiplication, this is the reciprocal. The multiplicative inverse of x is $\frac{1}{x}$ (for all $x \neq 0$).

  Several facts to keep in mind:

- Any element has at most one inverse.
- An element with a left inverse and a right inverse also has an inverse (this was shown above).
- If every element has an inverse and the binary operation (or composition) is associative, then the cancellation property holds:

$$a * b = a * c \implies b = c$$

$$b * a = c * a \implies b = c$$

Remark: Commutativity does not imply associativity.

2 Groups

Of course, the properties of binary operations that were discussed just now are very much applicable in something called **groups**. Simply put, we can say that a group is a set combined with an operation. However, it's a little more complicated than that. The following definition will make that clearer: First, we show that

Definition 2.1: Group

A group is a set G, closed under a binary operation $*$, satisfying the following properties:

1. Associativity: For all $a, b, c \in G$, we have:
$$(a * b) * c = a * (b * c)$$
2. Identity Element: There is an element $\mathrm{id} \in G$ such that for all $x \in G$:
$$\mathrm{id} * x = x * \mathrm{id} = x$$
3. Inverse: Corresponding to each $a \in G$, there is an element $a^{-1} \in G$ such that:
$$a * a^{-1} = a^{-1} * a = \mathrm{id}$$
4. Closure: For all $a, b \in G$, we have:
$$a * b \in G$$
It should be noted that this property is *implied* by the definition of a binary operation (law of composition); namely, that $G \times G \mapsto G$.

Remark:

- Notationally, this can be represented by $(G, *)$ or $\langle G, * \rangle$. This is saying that we are pairing a set with a binary operation.
- The *order* of a group G is the number of elements that it contains. We will often denote the order by $|G|$. Remember that G is a set, so you can think of the order of G as its cardinality.

Definition 2.2: Abelian Group

A group is **abelian** if it is commutative.

Remark:

- Recall that a group is commutative if applying the group operation to two group elements does not depend on the order in which they are written.

Important Note

The two most common groups are additive and multiplicative groups. Thus, for some $h \in G$, where $(G, *)$ is a group, it is important to mention what their inverses and identity elements are. As mentioned in the previous section:

Group	Inverse	Identity
Multiplicative $(G, \times)$	$h^{-1} = \frac{1}{h}$	$\text{id} = 1$
Addition $(G, +)$	$h^{-1} = -h$	$\text{id} = 0$

We will discuss these more in the examples.

For any other group, the inverse and identity element depends on how the group and its binary operation is defined. Refer to the definition of a group.

Important Note

In *Algebra, Second Edition* by Michael Artin, groups are denoted by the set followed by the binary operation (or law of composition) as the power. For example:

- $\mathbb{Z}^+$ is the set of integers, with addition as its binary operation.
- $\mathbb{R}^+$ is the set of real numbers, with adition as its binary operation.
- $\mathbb{R}^\times$ is the set of nonzero real numbers, with multiplication as its binary operation.

2.1 Basic Examples of Groups

Here, we briefly describe some basic examples of groups.

2.1.1 Example: Addition

For example, the integers under addition are a group. Notationally, this is represented by $(\mathbb{Z}, +)$.

- It's obvious that addition is associative. That is:

$$(a + b) + c = a + (b + c) = a + b + c$$

- The identity element is 0 (we note that $0 \in \mathbb{Z}$). This is because:

$$0 + x = x + 0 = x$$

- The inverse is $-x$. This is because:

$$x + (-x) = (-x) + x = 0$$

We also know that the reals, rationals, or complex numbers under addition are also groups. Notationally, this is represented by $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, or $(\mathbb{C}, +)$, respectively.

Additionally, these are all considered to be **abelian groups**.

2.1.2 Example: Multiplication

Let's now consider multiplication. In particular, multiplication does give a binary operation over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. It's obvious that this is associative and 1 is the two-sided identity element. However, what about the inverse?

- If we try to take the integers under multiplication as a group, then we'll run into problems. This is because the multiplicative inverse of every integer except ± 1 is not an integer. For example, if we tried 2, then the multiplicative inverse of 2 is $\frac{1}{2}$. However, $\frac{1}{2} \notin \mathbb{Z}$.

- Rational numbers are closer. For instance, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. However, this is only defined if $a \neq 0$. The solution is to remove 0. So, $(\mathbb{Q} - \{0\}, \times)$ is a group. Similarly, we can make $\mathbb{R}$ and $\mathbb{C}$ groups under multiplication by removing 0.

  We note that this change does not affect the closure property because we can only achieve $a \times b = 0$ if and only if $a = 0$ or $b = 0$. Since $a \notin \mathbb{R} - \{0\}$ and $b \notin \mathbb{R} - \{0\}$ (or $\mathbb{Q}$ or $\mathbb{C}$), then we are still closed and our binary operation is still well-defined.

2.1.3 Example: Matrices

Consider the $n \times n$ general linear group, or the group of all invertible[1] $n \times n$ matrices. This is denoted by:

$$GL_n = \{n \times n \text{ invertible matrices } A\}$$

If we wanted to indicate that we are working with real or complex matrices, we write $GL_n(\mathbb{R})$ and $GL_n(\mathbb{C})$, respectively.

2.1.4 Non-Example: Addition and Multiplication

We mentioned that $(\mathbb{Q}-\{0\}, \times)$, $(\mathbb{R}-\{0\}, \times)$, and $(\mathbb{C}-\{0\}, \times)$ are groups. However, we note that $(\mathbb{Z}-\{0\}, \times)$ and $(\mathbb{Z}_{\geq 0}, +)$ are *not* groups.

- We already briefly explained why $\mathbb{Z}$ under multiplication is not a group. The same idea applies even if we do not include 0; that is, $\mathbb{Z} - \{0\}$ is not a group. We know that $\mathbb{Z} - \{0\}$ has a unique identity element under $\times$; this element is 1. This is the case because, if id is the identity element of $\mathbb{Z} - \{0\}$ under $\times$, then by definition:

  $$\text{id} \times x = x \times \text{id} = x$$

  Which implies that id $= 1$. We also know that $2 \in \mathbb{Z} - \{0\}$. However, 2 does not have an inverse in $\mathbb{Z} - \{0\}$. To show this, we prove by contradition. If 2 has an inverse in $\mathbb{Z} - \{0\}$, then by definition it follows that for some $a^{-1} \in \mathbb{Z} - \{0\}$:

  $$2 \times a^{-1} = a^{-1} \times 2 = \text{id}$$

  But, since we know that id $= 1$, it follows that:

  $$2 \times a^{-1} = 1$$

  But, as the only solution to this is $\frac{1}{2}$, we know that $\frac{1}{2} \notin \mathbb{Z} - \{0\}$. Thus, this is a contradiction. Thus, $\mathbb{Z} - \{0\}$ under multiplication is not a group.

- We know that $\mathbb{Z}_{\geq 0}$ has a unique identity element under addition and that is 0. This is because if id is a unique element of $(\mathbb{Z}_{\geq 0}, +)$, then by definition, we know that:

  $$\text{id} + x = x + \text{id} = x$$

  It is obvious that id $= 0$. Now, we want to show that 1 does not have an inverse with respect to addition in $\mathbb{Z}_{\geq 0}$. We'll prove this by contradiction. Suppose 1 does have an inverse. Recall that if 1 does have an inverse, then there is an $x \in \mathbb{Z}_{\geq 0}$ such that for some $a^{-1} \in \mathbb{Z}_{\geq 0}$:

  $$a^{-1} + 1 = 1 + a^{-1} = \text{id}$$

  But, as id $= 0$, it follows that:

  $$a^{-1} + 1 = 0 \iff a^{-1} = -1$$

  However, we note that $-1 \notin \mathbb{Z}_{\geq 0}$ so this is a contradiction. Thus, $\mathbb{Z}_{\geq 0}$ under addition is not a group.

[1] Here, keep in mind that the determinant of an invertible matrix is not 0 (otherwise, it wouldn't have an inverse.)

2.2 Properties of Groups

Suppose $(G, *)$ is a group. Then, we note the following properties of groups.

2.2.1 Uniqueness of the Identity.

Could we have two unique two-sided identities in G? The answer is no. The proof is as follows.

Proof. Assume by contradiction that we had id_1 and id_2, both of which are unique two-sided identity elements. Then, we know that $\mathrm{id}_1 * \mathrm{id}_2 = \mathrm{id}_2$ since id_1 is an identity. But, since id_2 is also an identity, then $\mathrm{id}_1 * \mathrm{id}_2 = e1$. So, it follows that id_1 and id_2 are not unique; in other words, $\mathrm{id}_1 = \mathrm{id}_2$. □

2.2.2 Uniqueness of Inverses.

If g_1, g_2 are both inverses of some element h, then[2]:

$$g_1 * h = h * g_2 = \mathrm{id}$$

Additionally, we know that:

$$g_1 * (h * g_2) = g_1 * \mathrm{id} = g_1$$
$$(g_1 * h) * g_2 = \mathrm{id} * g_2 = g_2$$

And so it follows that $g_1 = g_2$, thus h will have a unique inverse. To be more concrete, we have the proof.

Proof. We note that $g_1 * h = \mathrm{id}$ and $h * g_2 = \mathrm{id}$. Then:

$$\begin{aligned} g_1 &= g_1 * \mathrm{id} && \mathrm{id} \text{ is the identity element.} \\ &= g_1 * (h * g_2) \\ &= (g_1 * h) * g_2 && \text{Associativity} \\ &= \mathrm{id} * g_2 \\ &= g_2 && \mathrm{id} \text{ is the identity element.} \end{aligned}$$

So, it follows that $g_1 = g_2$. Thus, an element h will have a unique inverse. □

2.2.3 Cancellation.

Suppose we have the expression $g * a = g * b$. This implies that $a = b$. Similarly, the expression $a * g = b * g$ can be simplified to $a = b$.

Proof. From the definition of a group, we know that an inverse exists for every element in G. Let g^{-1} be the inverse of g. Then:

$$\begin{aligned} g * a = g * b &\implies g^{-1} * (g * a) = g^{-1} * (g * b) \\ &\implies (g^{-1} * g) * a = (g^{-1} * g) * b && \text{Associativity (Prop. 1)} \\ &\implies \mathrm{id} * a = \mathrm{id} * b && \text{Definition of Inverse (Prop. 3)} \\ &\implies a = b && \text{Definition of Identity (Prop. 2)} \end{aligned}$$

The other way is similar. □

Remark: Although $g * a = g * b$, $g * a \neq b * g$ ($g * a$ is not necessarily equal to $b * g$).

[2]Here, we denote g_1 as the left-inverse and g_2 is the right-inverse.

2.2.4 Inverse of Operation of Two Elements.

Lemma 2.1

Suppose $(G, *)$ is a group. Then, for every $g, h \in G$, we have:

$$(g * h)^{-1} = h^{-1} * g^{-1}$$

Proof. Since the inverse of an element is unique, it is enough to check that:

$$(g * h) * (h^{-1} * g^{-1}) = (h^{-1} * g^{-1}) * (g * h) = \mathrm{id}$$

So:

$$\begin{aligned}
(g * h) * (h^{-1} * g^{-1}) &= g * (h * h^{-1}) * g^{-1} && \text{Associativity (Prop. 1)} \\
&= g * \mathrm{id} * g^{-1} && \text{Definition of Inverse (Prop. 3)} \\
&= (g * \mathrm{id}) * g^{-1} && \text{Associativity (Prop. 1)} \\
&= g * g^{-1} && \text{Definition of Identity (Prop. 2)} \\
&= \mathrm{id} && \text{Identity Element}
\end{aligned}$$

Similarly:

$$\begin{aligned}
(h^{-1} * g^{-1}) * (g * h) &= h^{-1} * (g^{-1} * g) * h && \text{Associativity (Prop. 1)} \\
&= h^{-1} * \mathrm{id} * h && \text{Definition of Inverse (Prop. 3)} \\
&= (h^{-1} * \mathrm{id}) * h && \text{Associativity (Prop. 1)} \\
&= h^{-1} * h && \text{Definition of Identity (Prop. 2)} \\
&= \mathrm{id} && \text{Identity Element}
\end{aligned}$$

So, the proof is complete. □

2.2.5 Inverse of an Inverse.

We should note that, despite using the -1 superscript to denote a multiplicative inverse, this applies to any valid binary operation under a group.

Lemma 2.2

For every $g \in G$, $(g^{-1})^{-1} = g$.

Proof. We have that $g^{-1} * g = \mathrm{id}$. Multiplying both sides by $(g^{-1})^{-1}$ from the left, we now have:

$$((g^{-1})^{-1} * g^{-1}) * g = (g^{-1})^{-1} * \mathrm{id} = (g^{-1})^{-1}$$

Hence, $\mathrm{id} * g = (g^{-1})^{-1}$ and so $g = (g^{-1})^{-1}$. □

2.2.6 Exponents of Elements

Suppose $(G, *)$ is a group and $g \in G$. For a positive integer n, we let:

$$g^n = \underbrace{g * \cdots * g}_{n \text{ times}}$$

For a negative integer n, we let:

$$g^n = \underbrace{(g^{-1}) * \cdots * (g^{-1})}_{-n \text{ times}}$$

Lemma 2.3

For $n, m \in \mathbb{Z}$, $(g^n)^m = g^{nm}$.

Proof. We will consider various cases depending on the signs of m and n.

- Case 1: Suppose m and n are positive. Then:

$$(g^n)^m = \underbrace{g^n * \cdots * g^n}_{m \text{ times}} = \underbrace{\overbrace{(g * \cdots * g)}^{n \text{ times}} * \cdots * \overbrace{(g * \cdots * g)}^{n \text{ times}}}_{m \text{ times}} = \underbrace{g * \cdots * g}_{mn \text{ times}} = g^{mn}$$

  Here, g^n means we need to multiply g n times. But, since we need to multiply g^n m times, it follows that this is simply g^{nm}.

- Case 2: Suppose m is positive and n is negative. Then:

$$(g^n)^m = \underbrace{g^n * \cdots * g^n}_{m \text{ times}} = \underbrace{\overbrace{(g^{-1} * \cdots * g^{-1})}^{-n \text{ times}} * \cdots * \overbrace{(g^{-1} * \cdots * g^{-1})}^{-n \text{ times}}}_{m \text{ times}} = \underbrace{g^{-1} * \cdots * g^{-1}}_{-mn \text{ times}} = g^{mn}$$

  Here, we note that $mn < 0$.

- Case 3: Suppose m is negative and n is positive. Then:

$$(g^n)^m = \underbrace{(g^n)^{-1} * \cdots * (g^n)^{-1}}_{-m \text{ times}} = \underbrace{(\overbrace{g * \cdots * g}^{n \text{ times}})^{-1} * \cdots * (\overbrace{g * \cdots * g}^{n \text{ times}})^{-1}}_{-m \text{ times}}$$

  We note that, by the previous lemma, $(\underbrace{g * \cdots * g}_{n \text{ times}})^{-1} = \underbrace{g^{-1} * \cdots * g^{-1}}_{n \text{ times}}$. Hence:

$$(g^n)^m = \underbrace{\overbrace{(g^{-1} * \cdots * g^{-1})}^{n \text{ times}} * \cdots * \overbrace{(g^{-1} * \cdots * g^{-1})}^{n \text{ times}}}_{-m \text{ times}} = \underbrace{g^{-1} * \cdots * g^{-1}}_{-mn \text{ times}} = g^{mn}$$

  Here, we note that $mn < 0$.

- Case 4: Suppose m and n are negative. Since it is easier to work with positive numbers, let $m = -r$ and $n = -s$ where $r, s > 0$. Then, we have to show that $(g^{-r})^{-s} = g^{rs}$. By definition, we know that $g^{-r} = \underbrace{g^{-1} * \cdots * g^{-1}}_{r \text{ times}}$. Hence, $(g^{-r})^{-s} = [(g^{-1})^r]^{-s}$. By the case where $n > 0$ and $m < 0$, we deduce that $(x^r)^{-s} = x^{-rs}$. Therefore:

$$(g^{-r})^{-s} = (g^{-1})^{-rs} = \underbrace{(g^{-1})^{-1} * \cdots * (g^{-1})^{-1}}_{rs \text{ times}} = \underbrace{g * \cdots * g}_{rs \text{ times}} = g^{rs}$$

- Case 5: Suppose $m = 0$. Since $m = mn = 0$, it follows that:

$$(g^n)^m = \text{id}$$

$$g^{nm} = \text{id}$$

- Case 6: Suppose $n = 0$. By the same reasoning as case 5, we have that $n = mn = 0$. So:

$$(g^n)^m = \mathrm{id}^m = \mathrm{id}$$

$$g^{mn} = \mathrm{id}$$

Here, we notice that $\mathrm{id} * \cdots * \mathrm{id} = \mathrm{id}$ and $\mathrm{id}^{-1} = \mathrm{id}$, and so $\mathrm{id}^m = \mathrm{id}$. So, we showed that $(g^n)^m = g^{mn}$ for every $m, n \in \mathbb{Z}$. □

Important Note

- When we are working with an multiplicative group $(G, \times)$, then g^n means:

$$g^n = \begin{cases} \underbrace{g \times \cdots \times g}_{n \text{ times}} & n > 0 \\ 1 & n = 0 \\ \underbrace{\frac{1}{g} \times \cdots \times \frac{1}{g}}_{-n \text{ times}} & n < 0 \end{cases}$$

- When we are working with an additive group $(G, +)$, instead of writing g^n, we write ng. So, in $(G, +)$:

$$ng = \begin{cases} \underbrace{g + \cdots + g}_{n \text{ times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-g) + \cdots + (-g)}_{-n \text{ times}} & n < 0 \end{cases}$$

  So, instead of writing $(g^n)^m = g^{mn}$, we write $m(ng) = (mn)g$.

- For other valid groups, it depends on how you define the operation for the group.

Lemma 2.4

For every $m, n \in \mathbb{Z}$:

$$g^m * g^n = g^{m+n}$$

Proof. Like the previous proof, we will consider various cases depending on the signs of m and n. Since it is easier to work with positive numbers, we will write $m = \mathrm{sign}(m)r$ and $n = \mathrm{sign}(n)s$ where $r = |m|$ and $s = |n|$, where:

$$\mathrm{sign} : \mathbb{R} \mapsto \{-1, 1\}$$

- Case 1: Suppose m and n are positive. Then:

$$g^m * g^n = (\underbrace{g * \cdots * g}_{m \text{ times}}) * (\underbrace{g * \cdots * g}_{n \text{ times}}) = \underbrace{g * \cdots * g}_{m+n \text{ times}} = g^{m+n}$$

- Case 2: Suppose $m = -r$ (m is negative), $n = s$ (n is positive), $r < s$ ($m + n$ is positive). Then, by the previous case:

$$g^r * g^{s-r} = g^s \implies g^{s-r} = (g^r)^{-1} * g^s = g^{-r} * g^s$$

- Case 3: Suppose $m = -r$, $n = s$, $r > s$ ($m + n$ is negative). Then, by the first case:

$$\begin{aligned} g^s * g^{r-s} = g^r &\implies g^{r-s} = (g^s)^{-1} * g^r \\ &\implies (g^{r-s})^{-1} = ((g^s)^{-1} * g^r)^{-1} \\ &\implies g^{-(r-s)} = (g^r)^{-1} * ((g^s)^{-1})^{-1} \\ &\implies g^{-r+s} = g^{-r} * g^s \end{aligned}$$

- Case 4: Suppose $m = 0$. Then:

$$g^m * g^n = \mathrm{id} * g^n = g^n = g^{m+n}$$

- Case 5: Suppose $n = 0$. Then:

$$g^m * g^n = g^m * \mathrm{id} = g^m = g^{m+n}$$

By the above cases, we obtain the claim when $n \geq 0$ and $m \in \mathbb{Z}$. So:

- Case 6: Suppose $n = -s$ (n is negative) and $s > 0$. Then:

$$g^{m-s} * g^s = g^m \implies g^{m-s} = g^m * (g^s)^{-1} \implies g^{m-s} = g^m * g^{-s}$$

This concludes the proof. □

3 Subgroups

The definition of a subgroup is very similar to that of a group. It states the following.

Definition 3.1: Subgroup

A subset H of a group $(G, \circ)$ is a **subgroup** $(H, \circ)$ if it has the following properties:

1. Identity/Neutral Element: The identity element of G belongs in H. In other words, there is an element $\mathrm{id} \in H$ (where the same $\mathrm{id} \in G$) such that for all $x \in H$:
$$\mathrm{id} * x = x * \mathrm{id} = x$$
2. Inverse: For some $a \in H$, its inverse in G belongs to H. More generally, corresponding to each $a \in H$, there is an element $a^{-1} \in H$ such that:
$$a * a^{-1} = a^{-1} * a = \mathrm{id}$$
3. Closure: For all $a, b \in H$, we have:
$$a * b \in H$$
It should be noted that this property is *implied* by the definition of a binary operation (law of composition). This binary operation is inherited from the group G.

We denote this by $H \leq G$.

Remarks:

- More concisely, a subgroup of a group $(G, \cdot)$ is a subset $H \subseteq G$ such that $(H, \circ)$ is also a group.
- Because associativity is a property that is in a group, it is also implicitly a property that is in a subgroup.
- This also implies that the subgroup H is a group.
- If G is a group, then G is a subgroup of itself. If we want to exclude this property (i.e. we don't want G to be classified as a subgroup of itself), we would want H to be a *proper subgroup* of G.
- The identity element $\{\mathrm{id}\}$ by itself is known as a *trivial subgroup*.

3.1 Examples of Subgroups

Here, we briefly describe some examples of subgroups.

3.1.1 Example: Complex Numbers Under Multiplication

Consider the group $\mathbb{C}^\times = (\mathbb{C} - \{0\}, \times)$. $\{z \in \mathbb{C} \mid |Z| = 1\}$ (the set of all elements of the complex plane with absolute value 1) is a subgroup of $(\mathbb{C} - \{0\}, \times)$.

3.1.2 Example: Matrices

Consider the set $GL_n(\mathbb{R})$, or the set of all $n \times n$ invertible matrices, under matrix multiplication. Then, define:
$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$$
We have that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

3.1.3 Example: Real Numbers Under Addition

Consider the group $(\mathbb{R}, +)$. Some possible subgroups are:

- $(\mathbb{Z}, +)$. The group of integers under addition.
- $(\mathbb{Z}a, +)$. Here, we note that:

$$(\mathbb{Z}a, +) = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

- $(\{0\}, +)$. The trivial subgroup, consisting of only the identity element.
- $(\mathbb{R}, +)$. The whole group.

Effectively, a subgroup H of a group G with law of composition written **additively** is a subgroup if it has the following properties:

- **Closure:** If $a, b \in H$, then $a + b \in H$.
- **Identity:** $0 \in H$.
- **Inverses:** If $a \in S$, then $-a \in S$.

3.1.4 Example: Integers Under Addition

Consider the group $(\mathbb{Z}, +)$. Some subgroups include:

- $(\{0\}, +)$: the trivial subgroup.
- $(\mathbb{Z}, +)$: the group itself.
- $(\mathbb{Z}2, +)$: the group where the set is all even integers.
- $(\mathbb{Z}a, +)$. The group where the set consists of all elements that is divisible by a. That is:

$$(\mathbb{Z}a, +) = \{n \in Z \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

3.2 Subgroups of the Additive Group of Integers

An important theorem to consider is the following:

Theorem 3.1

Let S be a subgroup of the additive group $(\mathbb{Z}, +)$. Either S is the trivial subgroup $\{0\}$, or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof. Let S be a subgroup of $(\mathbb{Z}, +)$. Then, by definition, $0 \in S$. If 0 is the only element of S, then S is the trivial subgroup and we are done.

Otherwise, S contains an integer n that is different from 0, and either n or $-n$ is positive. We know that $-n \in S$ (inverse property) so, in either case, S has a positive integer. Now, we need to show that S is equal to $\mathbb{Z}a$ when a is the smallest positive integer in S.

First, we show that $\mathbb{Z}a \subseteq S$; in other words, that ka is in S for every integer k. If k is a positive integer, then $ka = \underbrace{a + a + \cdots + a}_{k \text{ times}}$. Since $a \in S$, closure and induction shows us that $ka \in S$. Since inverses are in S, $-ka \in S$. Finally, $0 = 0a \in S$.

To show $\mathbb{Z}a = S$, assume by contradiction that it's not. Pick some $n \in S$ with $n \notin \mathbb{Z}a$. By Euclidean division, $n = qa + r$ for some $q, r \in \mathbb{Z}$, where $0 \leq r < a$. Additionally, we cannot have $r = 0$ because

$n \notin \mathbb{Z}a$. Then, $n \in S$ and $qa \in S$, $-qa \in S$, and therefore $n - qa = r \in S$. But, r is positive and $r < a$, which is a contradiction. □

3.3 Relation to GCD, LCM, and Prime Numbers

In this section, we will briefly talk about subgroups in the context of the greatest common divisor, least common multiple, and prime numbers.

3.3.1 Relation to GCD

One application of the above theorem relates to subgroups that contain two integers a and b. We can define the set of all integer combinations $ra + sb$ of a and b as follows:

$$S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ra + sb \text{ for some integers } r, s\} \leq (\mathbb{Z}, +)$$

This is called the subgroup *generated* by a and b because it is the smallest subgroup that contains both a and b. If a and b aren't both zero, then S is not the trivial group $\{0\}$. By the above theorem, we know that S has the form $\mathbb{Z}d$, which is the set of integers divisible by d. Here, $d = \gcd(a, b)$, the greatest common divisor of a and b.

Proposition. *Let a and b be integers, not both zero, and let $d = \gcd(a, b)$, the positive integer that generates the subgroup $S = \mathbb{Z}a + \mathbb{Z}b$. So, $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$ and:*

(a) d divides a and b.

(b) If an integer x divides both a and b, then it also divides d.

(c) There are integers r and s such that $d = ra + sb$.

Proof. We know that part (c) of this proposition simply restates the original proposition. Now, if a, $b \in S$ and $S = \mathbb{Z}d$, then it follows that d divides a and b, thus satisfying the first proposition. Finally, if $x \in \mathbb{Z}$ divides both a and b, then it must be true that x divides the integer combination $ra + sb = d$. □

As an example, consider $a = 4$ and $b = 6$. Then, $d = \gcd(4, 6) = 2$ and:

$$\mathbb{Z}a = \mathbb{Z}4 = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$\mathbb{Z}b = \mathbb{Z}6 = \{\dots, -12, -6, 0, 6, 12, \dots\}$$

So:

$$\begin{aligned}
\mathbb{Z}a + \mathbb{Z}b &= \mathbb{Z}4 + \mathbb{Z}6 \\
&= \{\dots, -8 - 12, -8 - 6, \dots, -4 - 12, \dots 0 - 12, 0 - 6, \dots 4 - 12, 4 - 8, \dots, 8 - 6, \dots\} \\
&= \{\dots, -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \dots\} \\
&= \mathbb{Z}2 \\
&= \mathbb{Z}d
\end{aligned}$$

3.3.2 Relation to Prime Numbers

We now introduce the notion of prime numbers, which is closely related to this topic. Two nonzero integers a and b are said to be *relatively prime* if the only positive integer that divides both of them is 1. That is, $\gcd(a, b) = 1$. It follows that $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$.

Corollary 3.1

A pair a, b of integers is relatively prime if and only if there are integers r and s such that $ra + sb = 1$.

Corollary 3.2

Let p be a prime integer. If p divides a product ab of integers, then p divides a or p divides b.

Proof. Suppose that the prime p divides ab but not a. Then, the only positive divisors of p are 1 and p. Since p does not divide a, it follows that $\gcd(a, p) = 1$. Therefore, we know that there must be integers r and s such that $ra + sp = 1$. Multiplying both sides by b gives us:

$$rab + spb = b$$

Which we note that p divides both rab and spb. So, p divides b. By symmetry, p divides a as well. □

As an example, consider $a = 3$ and $b = 4$. These two numbers are relatively prime; that is, $\gcd(3, 4) = 1$. It follows that:

$$\mathbb{Z}a = \mathbb{Z}3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$$
$$\mathbb{Z}b = \mathbb{Z}4 = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

And so:

$$\begin{aligned}\mathbb{Z}a + \mathbb{Z}b &= \mathbb{Z}3 + \mathbb{Z}4 \\ &= \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\} \\ &= \mathbb{Z}1 \\ &= \mathbb{Z}\end{aligned}$$

We know that, for $a = 3$ and $b = 4$, $ab = 12$. Take $p = 3$. Then, we know that 3 divides 3 but 3 does not divide 4. Likewise, take $p = 2$. Then, we know that 2 divides 4 but 2 does not divide 3.

3.3.3 Relation to LCM

Another subgroup of $(\mathbb{Z}, +)$ associated to a pair of integers a and b is the intersection; that is, $\mathbb{Z}a \cap \mathbb{Z}b$, the set of integers contained in both $\mathbb{Z}a$ and $\mathbb{Z}b$. Assuming that neither a nor b is zero, $\mathbb{Z}a \cap \mathbb{Z}b$ is a subgroup that is not trivial (since we know that a and b are not zero, $ab \neq 0$). So, $\mathbb{Z}a \cap \mathbb{Z}b$ has the form $\mathbb{Z}m$ for some positive integer m. This m is known as the *least common multiple* of a and b, and is commonly denoted by $\operatorname{lcm}(a, b)$.

Proposition. *Let A and b be integers different from zero, and let $m = \operatorname{lcm}(a, b)$, the positive integer that generates the subgroup $S = \mathbb{Z}a \cap \mathbb{Z}b$. Then, $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$ and so:*

(a) m is divisible by both a and b.

(b) If an integer n is divisible by a and by b, then it is divisible by m.

Proof. Both statements follow from the fact that an integer is divisible by a and by b if and only if it is contained in $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$. □

As an example, consider again $a = 4$ and $b = 6$. Then, $m = \operatorname{lcm}(4, 6) = 12$ and:

$$\mathbb{Z}a = \mathbb{Z}4 = \{\dots, -24, -20, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, 24, \dots\}$$

$$\mathbb{Z}b = \mathbb{Z}6 = \{\dots, -24, -18, -12, -6, 0, 6, 12, 18, 24 \dots\}$$

So:

$$\begin{aligned}\mathbb{Z}a \cap \mathbb{Z}b &= \mathbb{Z}4 \cap \mathbb{Z}6 \\ &= \{\dots, -24, -12, 0, 12, 24, \dots\} \\ &= \mathbb{Z}12 \\ &= \mathbb{Z}m\end{aligned}$$

3.3.4 LCM and GCD

Corollary 3.3

Let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Then, $ab = dm$.

Proof. Since b/d is an integer, a divides ab/d. Similarly, b divides ab/d, so m divides ab/d. We can write $d = ra + sb$, implying that $dm = ram + sbm$. Both terms on the right is divisible by ab, so ab divides dm and so ab and dm are positive and each one divides the other, leading to $ab = dm$. □

As an example, take $a = 4$ and $b = 10$ so that $d = \gcd(4, 10) = 2$ and $m = \text{lcm}(4, 10) = 20$. Then, it follows that:

$$ab = 4(10) = 40 = 2(20) = dm$$

4 Cyclic Groups

Here, we will briefly talk about cyclic groups, subgroups, and order of elements.

4.1 Definitions

Definition 4.1: Cyclic Subgroup

Let G be a group. Let $x \in G$ be an element. A **cyclic subgroup** $H = \langle x \rangle$ generated by x is the subset:

$$H = \{\dots, x^{-2}, x^{-1}, x^0, x^1, x^2, \dots\} \subseteq G$$

Namely, we note that:

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

We will now verify that a cyclic subgroup is, indeed, a subgroup.

Proof. To check that H is a subgroup, we show that it meets the properties of a subgroup. In particular:

- Closure: We have that (regardless of signs):
$$x^m x^n = x^{m+n}$$
- Identity: We know that:
$$\text{id} = x^0 \in G$$
- Inverse: We know that (regardless of signs):
$$x^n = x^{-n}$$

So, a cyclic subgroup is a subgroup. □

Remark: H may or may not be infinite. For example, consider the (sub)group $(\mathbb{Z}a, +)$. If $a = x$ (some positive integer), then the following is infinite:

$$H = \mathbb{Z}x = \{\dots, -3x, -2x, -x, 0, x, 2x, 3x, \dots\}$$

However, if $a = 0$, then the following is finite:

$$H = \{0\}$$

Another example we can consider is the group $(\mathbb{R} - \{0\}, \times)$. Then, if $x = -1$, we have a group with two elements:

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

A final example we can consider for now is the group $(\mathbb{C} - \{0\}, \times)$. Then, if $x = i$, we have:

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

By which it cycles around (hence the name).

Definition 4.2: Cyclic Group

A group $(G, *)$ is called a **cyclic group** if $G = \langle x \rangle$ for some $x \in G$. In this case, we say that x is a **generator** of $\langle x \rangle$.

4.2 Properties of Cyclic Subgroups

Now, we'll talk about some important properties of cyclic subgroups.

4.2.1 Cyclic Groups are Abelian

To show that cyclic groups are abelian, we provide a proof.

Proof. Suppose $(G, *)$ is cyclic. Then, $G = \langle g \rangle$ for some $g \in G$. Hence, $G = \{g^n \mid n \in \mathbb{Z}\}$. For every $x, y \in G$, there are integers m and n such that $x = g^m$ and $y = g^n$. Hence:

$$x * y = g^m * g^n = g^{m+n}$$

$$y * x = g^n * g^m = g^{n+m}$$

Since integers are abelian, it follows that $g^{n+m} = g^{m+n}$ so it follows that $x * y = y * x$. □

4.2.2 Subgroup of Cyclic Groups

Theorem 4.1

Every subgroup of a cyclic group is cyclic.

The proof for this theorem is as follows:

Proof. Suppose $(G, *)$ is generated by g and H is a subgroup of G. So, $G = \{g^n \mid n \in \mathbb{Z}\}$. If $H = \{\mathrm{id}_G\}$, then it is generated by id_G and so it is cyclic. Otherwise, we can assume (without loss of generality), we can and will assume that $H \neq \{\mathrm{id}_G\}$. Hence, for some $l \in \mathbb{Z} - \{0\}$, $g^l \in H$. Because H is a subgroup, we know that $(g^l)^{-1} \in H$. Thus, $g^{-l} \in H$. Either $l > 0$ or $-l > 0$, so there is a positive integer m such that $g^m \in H$. By the well-ordering principle, there is:

$$s = \min\{m \in \mathbb{Z} \mid m > 0, g^m \in H\}$$

Since $s \in \{m \in \mathbb{Z} \mid m > 0, g^m \in H\}$, it follows that $g \in H$. Because H is a subgroup of G and $g^r \in H$, $\langle g^s \rangle \subseteq H$. This implies that:

$$\{(g^s)^k \mid k \in \mathbb{Z}\} \subseteq H$$

Which further implies that:

$$\{g^{sk} \mid k \in \mathbb{Z}\} \subseteq H$$

Which completes this proof. □

4.2.3 Order of a Cyclic Subgroup

Proposition. *Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by an element x, and let $S \subseteq \mathbb{Z}$ denote the set of integer k such that $x^k = 1$.*

(a) The set S is a subgroup of the additive group $(\mathbb{Z}, +)$ (closed under addition, contains 0, and closed under inverses).

(b) Two powers $x^r = x^s$, with $r \geq s$, are equal if and only if $x^{r-s} = 1$; in other words, if and only if $r - s \in S$.

(c) Suppose that S is not the trivial subgroup. Then, $S = \mathbb{Z}n$ for some positive integer n. The powers $1, x, x^2, \ldots, x^{n-1}$ are the distinct elements of the subgroup $\langle x \rangle$, and the order of $\langle x \rangle$ is n.

4.3 Order of a Cyclic Group

Definition 4.3: Order of a Cyclic Group

The group $\langle x \rangle = \{1, x, \ldots, x^{n-1}\}$ described in part (c) of the proposition above is called the **cyclic group of order** n. The order of $\langle x \rangle$ is the same thing as saying the cardinality of $\langle x \rangle$, or the group generated by this element.

We note that $\langle x \rangle$ can have infinitely many elements; in this case, we say that this cyclic subgroup is *infinite cyclic*.

Definition 4.4: Order of an Element

For a group G, an element $x \in G$ has **order** n if n is the smallest positive integer with the property that:

$$x^n = 1 \quad \text{(Identity Element)}$$

This is the same thing as saying that the cyclic subgroup $\langle x \rangle$ generated by x has order n.

An element might have infinite order if the corresponding cyclic subgroup never cycles back. In this case, we say that there is no positive integer n such that $x^n = 1$ (again, the identity element).

Warning: The order of an element is *not* the same thing as the order of a group, although they are related. Recall that the *order* of a group G is the number of elements that it contains.

Remark: For a finite cyclic subgroup, we can say that $\boxed{x^n = 1}$ and $x^r \neq 1$ for $r \in [1, \ldots, n-1]$. To demonstrate, we note that:

$$x^a = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$$

Essentially, it wraps around back to the identity element, so in that sense you can think of the exponents as the residue classes modulo n.

Summary: So, really, when we say that some element $x \in G$ has order n, we mean that $x^n = 1$, the identity element.

4.4 Examples of Cyclic Subgroups

Here, we briefly explain some examples of cyclic subgroups.

4.4.1 Example: Trivial

The identity element, 1, has order 1. It cycles back immediately. This is represented by the set:

$$\{1\}$$

4.4.2 Non-Example: Symmetric Group of Size 3

Consider $G = S_3$. Then, we have:

- $x = (12)$: has order 2.
- $y = (123)$: has order 3.
  - $y^2 = (132)$
  - $y^3 = (1)$

Which elements of $S_3 = \{(1), (12), (23), (13), (123), (132)\}$ have order 6? Well, none of these elements have order 6, so S_3 is not a cyclic group. This is particularly because, by the definition of a cyclic group, there has to be an element of $x \in S_3$ that generates the entire set S_3. However, as none of these elements of S_3 actually have an order of 6, S_3 *itself* cannot be generated by any of its elements.

4.4.3 Example: Matrices

Consider $G = GL_2(\mathbb{R})$. The element $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order. This is because:

$$x^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \qquad x^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \qquad x^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

As you can see, we can never get back to the identity element. So, x has infinite order.

4.4.4 Example: Matrices

The matrix $x = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ has finite order. This is because:

$$x^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \qquad x^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I_2 \qquad x^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} = -x$$

$$x^5 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} = -x^2 \qquad x^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

So, x has order 6. We note that $x^6 = x^0 = I_2$, the identity matrix.

4.5 More on Cyclic Groups

Consider the following proposition:

Proposition. *Let $x \in G$ be an element of finite order n, and let k be an integer that is written as $k = nq + r$ where q and r are integers and r is in the range $0 \leq r < n$. Then:*

- $x^k = x^r$
- $x^k = 1$ *if and only if* $r = 0$
- *Let $d = \gcd(k, n)$. The order of x^k is equal to $\frac{n}{d}$.*

There is a corollary that follows from this proposition, specifically the last part.

Corollary 4.1

The gneerators of $\mathbb{Z}/\mathbb{Z}n = \{0, 1, 2, \ldots, n-1\}$ are the elements of $\{0, 1, 2, \ldots, n-1\}$ which are relatively prime to n.

4.5.1 Example: Finding Order of Element

Suppose we wanted to find the order of the element a^4 in the cyclic group $G = \{1, a, a^2, \ldots, a^8, a^9\}$ (that is, G has order $n = 10$). From the proposition, it follows that:

$$\frac{10}{\gcd(10, 4)} = \frac{10}{2} = 5$$

So, it follows that a^4 has order 5. To check that this is the case, we have that:

$$(a^4)^5 = a^{20} = a^{10} = 1$$

4.5.2 Example: Finding Order of Element

Suppose G is a cyclic group of order 12. Then, we know that the positive integers that can occur as the order of an element of G are 1, 2, 3, 4, 6, 12 (these all divide[3] the order of G).

- Now, suppose we wanted to find the order of the element x^{11}. From the proposition, we note that:

$$\frac{12}{\gcd(12,11)} = \frac{12}{1} = 12$$

  Therefore, x^{11} has order 12. To check this, we note that:

$$(x^{11})^{12} = x^{132} = x^{12} = 1$$

- Suppose we wanted to find the order of the element x^9. From the proposition, we note that:

$$\frac{12}{\gcd(12,9)} = \frac{12}{3} = 4$$

  Therefore, x^9 has order 4. To check this, we note that:

$$(x^9)^4 = x^{36} = x^{12} = 1$$

4.6 More Examples of Groups

Here, we'll discuss several more examples of groups.

4.6.1 Klein Four Group

The Klein four group is the group of order 4 that can be represented by the four matrices:

$$V = \{\mathbf{I}, \mathbf{a}, \mathbf{b}, \mathbf{c}\}$$

Where $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{a} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{b} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and $\mathbf{c} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Consider the following table, which shows every operation possible under this group:

$\cdot$	$\mathbf{I}$	$\mathbf{a}$	$\mathbf{b}$	$\mathbf{c}$
$\mathbf{I}$	$\mathbf{I}$	$\mathbf{a}$	$\mathbf{b}$	$\mathbf{c}$
$\mathbf{a}$	$\mathbf{a}$	$\mathbf{I}$	$\mathbf{c}$	$\mathbf{b}$
$\mathbf{b}$	$\mathbf{b}$	$\mathbf{c}$	$\mathbf{I}$	$\mathbf{a}$
$\mathbf{c}$	$\mathbf{c}$	$\mathbf{b}$	$\mathbf{a}$	$\mathbf{I}$

This group is commutative but *not* cyclic (more on this later).

4.6.2 Quaternion Group

The quaternion group is the group of order 8 that can be represented by the eight matrices:

$$H = \{\pm\mathbf{I}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\} \subset GL_2(\mathbb{C})$$

Where $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and $\mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$. By some computation, we note that:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{I}$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$$

$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$$

$$\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

This group is *not* commutative and not cyclic.

[3] See applications of Lagrange's Theorem.

5 Permutations

Let's briefly discuss permutations, since these are important.

5.1 Introduction to Permutations

Definition 5.1: Permutation

A **permutation** of a set S is a bijective map p from a set S to itself:

$$p : S \mapsto S$$

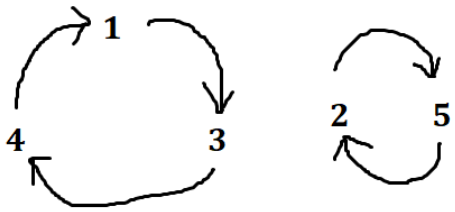
For instance, consider the following table:

i	1	2	3	4	5
$p(i)$	3	5	4	1	2

This is a permutation p of the set $\{1, 2, 3, 4, 5\}$. It is bijective because every element appears exactly once in the $p(i)$ row (i.e. we're only using each element once). In this particular table, there are two cycles:

- Cycle 1:
  - $p(1) = 3$ (1 goes to 3)
  - $p(3) = 4$ (3 goes to 4)
  - $p(4) = 1$ (4 goes to 1)
- Cycle 2:
  - $p(2) = 5$ (2 goes to 5)
  - $p(5) = 2$ (5 goes to 2)

If we drew this out, this would look like:



This can be written in **cycle notation**:

$$p = (134)(25)$$

The first cycle (134) is a 3-cycle and the second cycle (25) is a 2-cycle. This brings us to our next definition:

Definition 5.2: Transposition

A 2-cycle is also known as a **transposition**. More precisely, a transposition is a permutation that swaps two elements and fixes the rest.

Now, permutations do have inverses For example, the inverse of p is $p^{-1} = (143)(52) = (143)(25)$. Drawing it out yields:

Essentially, all we did was change what directions the arrow pointed to.

5.2 Writing Cycles and Fixed Elements

Suppose we had the permutation $p = (2143)(5)$. We note that all this is saying is:

- 2 goes to 1.
- 1 goes to 4.
- 4 goes to 3.
- 3 goes to 2.

We can write the first cycle like so:

$$(2143) = (3214) = (4321) = (1432)$$

These all say the same thing. So, to be consistent, we write cycles out like so:

1. Start at `1`, trace it out as it cycles.
2. Find the smallest unused index in the next cycle. Repeat.
3. Omit cycles of length 1. If all cycles are of length 1, then it is the identity permutation and so we can write (1).

In this permutation example, we do have a cycle of length 1: that would be (5). All *this* is saying is that 5 goes to 5. Usually, we omit it since it doesn't tell us anything. Then, it follows that *if a number isn't in the cycle representation of a permutation*, then that number is fixed. For example, $q = (134)$ means that:

- 1 goes to 3.
- 3 goes to 4.
- 4 goes to 1.
- 2 is fixed.

5.3 Symmetric Groups

Now, we can introduce the notion of a symmetric group.

Definition 5.3: Symmetric Group

For some $n \in \mathbb{Z}^+$, a **symmetric group** is the group of all permutations of the indices $\{1, 2, \ldots, n\}$ and is denoted by S_n. This is denoted by S_n and has order $n!$.

Remark: While the order of a symmetric group of n elements is $n!$, the order of a *permutation* is the least common multiple of the lengths of the *disjoint* cycles. For example, the order of (12)(3456)(78) is $\text{lcm}(2, 4) = 4$.

A common symmetric group is $S_3 = \{(1), (12), (13), (23), (123), (132)\}$.

5.4 Decomposition of Permutations

A permutation σ can be decomposed into non-disjoint transpositions like so:

$$\sigma = (a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2)(a_2, a_3)\ldots(a_{n-2}, a_{n-1})(a_{n-1}, a_n) \in S_n$$

For instance, suppose $\sigma = (123)(4567)$. Then, we can decompose this permutation like so:

$$(123)(4567) = \underbrace{(12)(23)}_{(123)}\overbrace{(45)(56)(67)}^{(4567)}$$

5.5 Sign of a Permutation

We can define the sign of a permutation by the following function:

$$\text{sgn} : S_n \mapsto \{\pm 1\}$$

A permutation is said to be **even** if its sign is 1. Conversely, a permutation is odd if its sign is -1.

5.5.1 Sign of a Cycle

The sign of a cycle is simply $(-1)^{\ell-1}$, where ℓ is the length of the given cycle. For example, consider the permutation $\sigma = (12345) \in S_5$, which consists of an individual cycle. σ has a length of 5, so its sign is:

$$(-1)^{5-1} = (-1)^4 = 1$$

5.5.2 Sign of Permutations

Of course, we can represent permutations with multiple cycles. So, we can find the sign of any permutation by multiplying the sign of each cycle together. For instance, consider the permutation $\sigma = (123)(4567) \in S_7$. Then:

$$\begin{aligned}\text{sgn}(\sigma) &= \text{sgn}((123)(4567)) \\ &= \text{sgn}((123))\text{sgn}((4567)) \\ &= (-1)^{3-1}(-1)^{4-1} \\ &= (-1)^2(-1)^3 \\ &= -1\end{aligned}$$

This can be extended to three, four, or more cycles. For n cycles, we can generalize this formula like so:

$$\begin{aligned}\text{sgn}(\sigma) &= \text{sgn}(\text{Cycle 1}) \cdot \text{sgn}(\text{Cycle 2}) \cdot \ldots \cdot \text{sgn}(\text{Cycle n}) \\ &= (-1)^{(\text{Length of Cycle 1})-1} \cdot (-1)^{(\text{Length of Cycle 2})-1} \cdot \ldots \cdot (-1)^{(\text{Length of Cycle n})-1}\end{aligned}$$

Remark: In this example, we made use of the fact that sgn is a *homomorphism*; this will be discussed in the next major section.

5.5.3 Sign of Transpositions

Recall that we can also decompose permutations into non-disjoint transpositions. The number of transpositions also defines the sign. In particular:

$$\text{sgn}(\sigma) = (-1)^{\text{Number of Transpositions}}$$

Take our example $\sigma = (123)(4567) \in S_7$. We know that σ can be decomposed like so:

$$\sigma = (123)(4567) = (12)(23)(45)(56)(67) \in S_7$$

So, σ can be represented by **5** transpositions. Therefore:

$$(-1)^5 = -1$$

So, actually, a better definition of even and odd permutations is as follows:

- A permutation is *even* if it can be written as a product of an even number of transpositions.
- A permutation is *odd* if it can be written as a product of an odd number of transpositions.

5.6 Alternating Group

We now talk about alternating groups, a subgroup of the symmetric group.

Definition 5.4: Alternating Group

he **alternating group** A_n is the group of *even* permutations.

We now show that this is a subgroup of the symmetric group.

Proof. To show that A_n is a subgroup, we need to show that all properties of a subgroup are satisifed. First, We know that (1), the identity permutation, is an even permutation, so $(1) \in A_n$. Next, if τ and σ are even, then it follows that τ^{-1} is even (decompose τ into transpositions and write the product backwards). Therefore, $\sigma\tau^{-1}$ is even and so $\sigma\tau^{-1} \in A_n$. □

For example, we know that $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. So:

$$A_3 = \{(1), (123), (132)\}$$

The alternating group has order $\frac{n!}{2}$, where n is the number of elements.

6 Homomorphisms

We will now discuss homomorphisms, which is one of the more important concepts to know.

6.1 Motivating Examples

We begin the discussion of homomorphisms with two motivating examples.

6.1.1 Motivating Example 1: Modulo Addition

Let's suppose we are given two groups:

- Group 1: $(\mathbb{Z}, +)$.
- Group 2: $(\mathbb{Z}/\mathbb{Z}2, +)$.

These two groups may look completely unrelated at first. However, we note the following behaviors between the two groups:

Operation in $(\mathbb{Z}, +)$	Operation in $(\mathbb{Z}/\mathbb{Z}2, +)$
Even + Even = Even.	$0 + 0 \equiv 0 \mod 2$.
Even + Odd = Odd.	$0 + 1 \equiv 1 \mod 2$.
Odd + Even = Odd.	$1 + 0 \equiv 1 \mod 2$.
Odd + Odd = Even.	$1 + 1 \equiv 0 \mod 2$.

Something to note here is that we can easily map:

- `Even` (in first group) $\mapsto$ `0` (in second group).
- `Odd` (in first group) $\mapsto$ `1` (in second group).

This mapping can be represented like so:

$$\varphi : \mathbb{Z} \mapsto \mathbb{Z}/\mathbb{Z}2$$

Where:

- If $x \in \mathbb{Z}$ is even, map it to $0 \in \mathbb{Z}/\mathbb{Z}2$.
- If $x \in \mathbb{Z}$ is odd, map it to $1 \in \mathbb{Z}/\mathbb{Z}2$.

Although these two groups appear to be completely unrelated, they are, in fact, related.

6.1.2 Example 2: Generalized Tables

Suppose we have two groups $(G, *)$ and $(G', \cdot)$. They can be infinite, finite, commutative, non-commutative, etc. Suppose we have two elements $x, y \in G$. Then, we also know that $x * y \in G$ (closure).

Let's suppose we can represent the operations of the above group using a table, like so:

- Group 1: $(G, *)$. Since we know that x, y, and $x * y \in G$, they'll appear in this table.

$*$	$\cdots$ $\cdots$ $\cdots$	y	$\cdots$
$\vdots$			
x		$x * y$	
$\vdots$			

- Group 2: $(G', \cdot)$. In order for these groups to have similar group behavior, x, y, and $x * y$ in G must correspond to the elements in G'. This can be represented by a function:

$$\varphi : G \mapsto G'$$

We want this function to send a specific part of the table for G to a similar part of the table for G'. In this sense, we can say that the place where $x \in G$ is (in the above table) can be mapped to a similar place in the below table for G'; the same idea applies to $y \in G$ and $x * y \in G$.

$\cdot$	$\dots$ $\dots$ $\dots$	$\varphi(y)$	$\dots$ $\dots$
$\vdots$			
$\varphi(x)$		$\varphi(x * y)$	
$\vdots$			

Here, we got $\varphi(x)$, $\varphi(y)$, and $\varphi(x * y)$ from the function mapping. The function mapping essentially mapped x, y, and $x * y$ to "similar" locations in the G' table.

An observation to note here is that the square where $\varphi(x * y)$ is at (in the table above) must also contain $\varphi(x) \cdot \varphi(y)$.

6.2 Definition of Homomorphism

Definition 6.1: Homomorphism

Let $(G, *)$ and $(G', \cdot)$ be two different groups. A **homomorphism** (also known as a *group homomorphism*) from G to G' is a function:

$$\varphi : G \mapsto G'$$

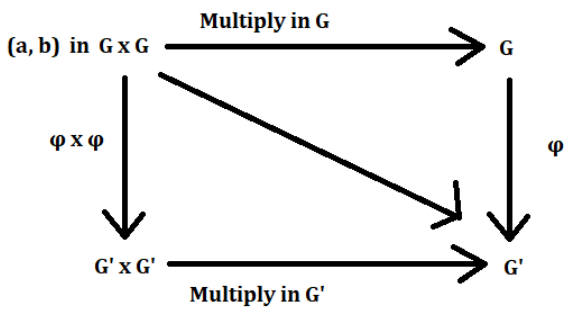
Such that for all $a, b \in G$, $\varphi(a * b) = \varphi(a) \cdot \varphi(b)$.

Remark: Here, we say that:

$$\underbrace{\varphi(a * b)}_{\text{Binary operation in } G} = \overbrace{\varphi(a) \cdot \varphi(b)}^{\text{Binary operation in } G'}$$

6.3 Pictorial Interpretation

A visualization of this process is shown below:



This is known as a *commutative diagram*.

6.4 Examples of Homomorphisms

We will now discuss some simple example of homomorphisms.

6.4.1 Example: Integers

Consider the following function:

$$c_n : (\mathbb{Z}, +) \mapsto (\mathbb{Z}/\mathbb{Z}n, +)$$

Defined by:

$$c_n(a) = [a]_n$$

We can say that c_n is a group homomorphism since for all $a, b \in \mathbb{Z}$:

$$c_n(a + b) = [a + b]_n = [a]_n + [b]_n = c_n(a) + c_n(b)$$

6.4.2 Example: Function Negation

Consider the following function:

$$f : (\mathbb{Z}, +) \mapsto (\mathbb{Z}, +)$$

Defined by:

$$f(x) = -x$$

Then, we say that f is a group homomorphism since for all $x, y \in \mathbb{Z}$:

$$f(x + y) = -(x + y) = (-x) + (-y) = f(x) + f(y)$$

6.4.3 Example: Exponential Map

Consider the following function:

$$\varphi : (\mathbb{R}, +) \mapsto (\mathbb{R} - \{0\}, \times)$$

Defined by:

$$\varphi(x) = e^x$$

Then, φ is a group homomorphism since for all $x, y \in \mathbb{R}$:

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

6.4.4 Example: Generalized Exponential Map

Suppose $(G, *)$ is a group and $g \in G$. Then, we can consider the following function:

$$f : (\mathbb{Z}, +) \mapsto (G, *)$$

Defined by:

$$f(n) = g^n$$

We know that this is a group homomorphism because for every $m, n \in Z$:

$$f(m + n) = g^{m+n} = g^m * g^n = f(m) * f(n)$$

6.4.5 Example: Logarithmic Map

Consider the following logarithmic function:

$$\ln : (\mathbb{R}_{>0}, \times) \mapsto (\mathbb{R}, +)$$

We know that this is a group homomorphism since for all $x, y \in \mathbb{R}_{>0}$:

$$\ln(x \times y) = \ln(x) + \ln(y)$$

6.4.6 Example: Complex Numbers

Consider the following function:

$$N : (\mathbb{C} - \{0\}, \times) \mapsto (\mathbb{R}_{>0}, \times)$$

Defined by:

$$N(z) = |z|$$

This is a group homomorphism because for every $z \in \mathbb{C} - \{0\}$ and $|z| \in \mathbb{R}_{>0}$:

$$|z_1 \times z_2| = |z_1| \times |z_2|$$

6.4.7 Example: Matrices

Define $(GL_n(\mathbb{R}), \cdot)$ be the set of invertible $n \times n$ real matrices under matrix multiplication.[4] Consider the function:

$$\theta : GL_n(\mathbb{R}) \mapsto GL_n(\mathbb{R})$$

Defined by[5]:

$$\theta(x) = (x^T)^{-1}$$

We know that θ is a group homomorphism because:

$$\theta(x \cdot y) = ((x \cdot y)^T)^{-1} = (y^T \cdot x^T)^{-1} = (x^T)^{-1} \cdot (y^T)^{-1} = \theta(x) \cdot \theta(y)$$

6.5 Properties of Homomorphisms

Proposition. *Let $\varphi : G \mapsto G'$ be a group homomorphism.*

(a) φ maps the identity to the identity: $\varphi(\mathrm{id}_G) = \mathrm{id}_{G'}$.

(b) φ maps inverses to inverses; in other words, for every $a \in G$, $\varphi(a^{-1}) = \varphi(a)^{-1}$ where a^{-1} is the inverse of a in G and $\varphi(a)^{-1}$ is the inverse of $\varphi(a)$ in G'. This can also be written as:

$$\mathrm{id}_G = \varphi(a)\varphi(a^{-1})$$

(c) If $a_1, \ldots, a_k$ are elements of G, then $\varphi(a_1, \ldots, a_k) = \varphi(a_1) \ldots \varphi(a_k)$.

The proof is as follows:

Proof. We need to show that all three properties hold.

(a) We note that since id_G is the identity element of G, it follows that $\mathrm{id}_G * \mathrm{id}_G = \mathrm{id}_G$. Because φ is a group homomorphism, it follows that:

$$\boxed{\varphi(\mathrm{id}_G * \mathrm{id}_G)} = \varphi(\mathrm{id}_G) * \varphi(\mathrm{id}_G)$$

Since $\mathrm{id}_G * \mathrm{id}_G = \mathrm{id}_G$, it follows that $\varphi(\mathrm{id}_G * \mathrm{id}_G) = \varphi(\mathrm{id}_G)$, so:

$$\varphi(\mathrm{id}_G) * \varphi(\mathrm{id}_G) = \boxed{\varphi(\mathrm{id}_G)}$$

Thus:

$$\varphi(\mathrm{id}_G) * \varphi(\mathrm{id}_G) = \varphi(\mathrm{id}_G) * \mathrm{id}_{G'}$$

[4] From linear algebra, we know that matrix multiplication is associative, the product of two invertible $n \times n$ is invertible, and for every $a \in GL_n(\mathbb{R})$, $a \cdot I_n = I_n \cdot a = a$ where I_n is the identity matrix.

[5] If x is a matrix, then x^T is the transpose of said matrix.

Canceling the first element in each side, we now have:

$$\varphi(\mathrm{id}_G) = \mathrm{id}_{G'}$$

(b) For every $a \in G$, we know that $a * a^{-1} = \mathrm{id}_G$. Applying φ to both sides, we have that:

$$\varphi(a * a^{-1}) = \varphi(\mathrm{id}_G)$$

By the first part and the fact that φ is a group homomorphism, we deduce that:

$$\varphi(a) * \varphi(a^{-1}) = \mathrm{id}_{G'}$$

Multiplying both sides by the inverse $\varphi(a)^{-1}$ of $\varphi(a)$ in G', we obtain:

$$\varphi(a)^{-1} * \varphi(a) * \varphi(a^{-1}) = \varphi(a)^{-1} * \mathrm{id}_H$$

And so:

$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

(c) We can simply make use of induction from the definition. □

6.6 Image

Definition 6.2: Image

The **image** of a general homomorphism $\varphi : G \mapsto G'$ is simply the image of φ as a map of sets:

$$\mathrm{im}(\varphi) = \{x \in G' \mid x = \varphi(a) \text{ for some } a \in G\}$$

More simply:

$$\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G\}$$

The image of φ is a subgroup of G'. Say $a, b \in G'$ are in the image; that is, $\exists x, y \in G$ such that $\varphi(x) = a$, $\varphi(y) = b$. Then:

$$\varphi(xy) = ab$$

This implies that the image has closure. The image has the identity (consider the second property in the propositions). Finally, the image has the inverse since $\varphi(x^{-1}) = a^{-1}$.

6.7 Kernal

Definition 6.3: Kernal

The **kernal** of a general homomorphism $\varphi : G \mapsto G'$ is the set of elements of G that are mapped to the identity in G':

$$\ker(\varphi) = \{a \in G \mid \varphi(a) = \mathrm{id}_{G'}\}$$

Here, the kernal of φ is a subgroup of G.

6.7.1 Example: Matrices

For example, we have that $\varphi : \det GL_n(\mathbb{R}) \mapsto (\mathbb{R} - \{0\}, \times)$, which means that:

$$\ker(a) = SL_n$$

Where SL_n is the special linear group of $n \times n$ matrices.

6.8 Conjugation

For a fixed $g \in G$ where the binary operation is $*$, the function:

$$\varphi : G \mapsto G$$

Defined by:

$$\varphi(a) = g^{-1} * a * g$$

Is a homomorphism. In particular, we call this the conjugate. This is a homomorphism because:

$$\begin{aligned}\varphi(a * b) &= \varphi(a) * \varphi(b) \\ &= (g^{-1} * a * g) * (g^{-1} * b * g) \\ &= g^{-1} * a * (g * g^{-1}) * b * g \\ &= g^{-1} * a * b * g\end{aligned}$$

We will discuss this more in-depth later on.

7 Isomorphisms

We now discuss isomorphisms, a special type of homomorphisms.

7.1 Motivating Example

Before we talk about isomorphisms, let's first talk about two motivating examples.

7.1.1 Motivating Example 1: Tables

Let's suppose we are given two groups.

- Group 1: $(\mathbb{Z}/\mathbb{Z}4, +)$.
- Group 2: $(\{1, -1, i, -i\}, \times)$

At first, these groups don't look at all related to each other. They even have completely different operations. However, they are structurally similar.

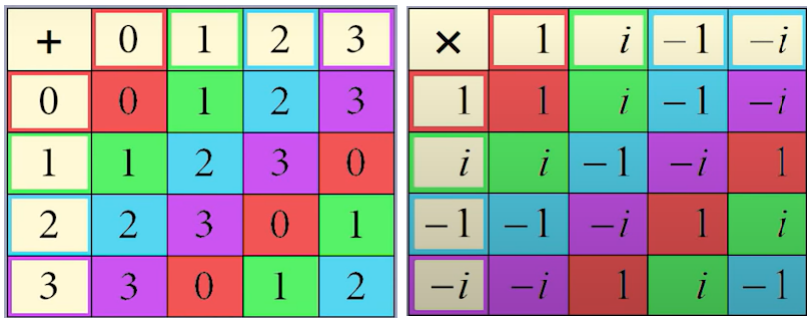
Consider the table that represents group 1:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Now, consider the table that represents group 2:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

One thing that should be clear (after some observation) is how the elements in both tables correspond with each other. Consider the same tables from above, now highlighted:



Both tables exhibit the same patterns. They're essentially identical groups; they just use different elements and different operations. For instance, in both tables, if we combined a green element with a blue element, we get a purple element. If we combined a blue element with a blue element, we get a red element. In other words, any statement about one table can be said for the other.

We say that these two groups are *isomorphic* (equal form).

7.1.2 Motivating Example 2: Addition Table

Consider the following addition table of $(\mathbb{Z}/\mathbb{Z}_3, +)$.

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Now, consider the Roman numbers:

$+$	0	I	II
0	0	I	II
I	I	II	0
II	II	0	1

It's clear that both of these are the same groups, only written with different symbols. We only need a *translator* to tell us which one is which. What is a translator (in the context of a group)? It should be a *bijection* which preserves the operation table. Notice that preserving the operation table simply means that it should be a group homomorphism. This brings us to the definition of group isomorphism.

7.2 Definition of Isomorphism

Definition 7.1: Isomorphism

An **isomorphism** of two groups $(G, *)$ and $(G', \cdot)$ is a bijective *homomorphism*:

$$\varphi : G \mapsto G'$$

If there is a isomorphism $\varphi : G \mapsto G'$, we say that G is isomorphic to G' and write $G \cong G'$.

Remark: To say that two groups are isomorphic is to say that they are the same as *groups*. The elements of the two groups, and the associated group operations, may be different; however, both groups have the same exact structures.

7.3 Inverse of Isomorphism

Lemma 7.1

A homomorphism $\varphi : G \mapsto G'$ is an isomorphism if and only if it is invertible. In this case, φ^{-1} is also a homomorphism, hence an isomorphism.

Proof. The first statement here is trivial, since a map of sets is bijective if and only if it has an inverse. Now, suppose $\varphi : G \mapsto G'$ is an isomorphism. Then, we need to show that $\varphi^{-1} : G' \mapsto G$ is a homomorphism. To make things explicit, suppose G has the binary operation $*$ and G' has the binary operation $\cdot$. Let $x, y \in G'$; then, we need to show that:

$$\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) * \varphi^{-1}(y)$$

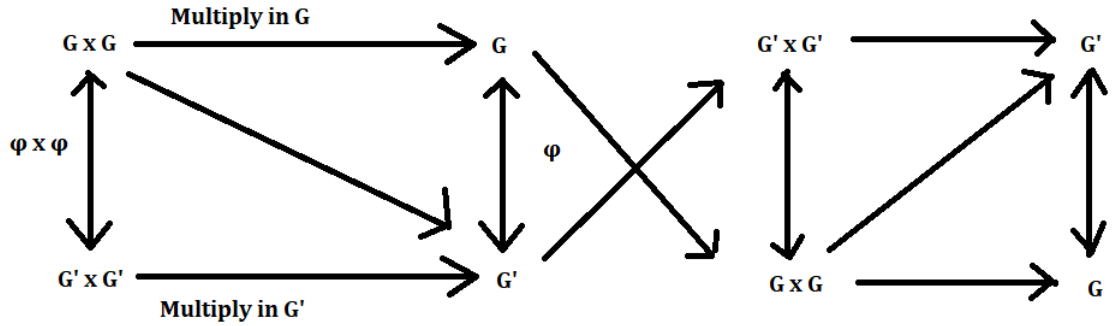
Since $\varphi : G \mapsto G'$ is surjective, there exists $a, b \in G$ such that $\varphi(a) = x$ and $\varphi(b) = y$. Then:

$$\varphi^{-1}(x \cdot y) = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(x) * \varphi^{-1}(y)$$

Therefore, φ^{-1} is a homomorphism. Since φ^{-1} is invertible, its inverse being φ, it is an isomorphism by the first part of the lemma. □

7.4 Pictorial Interpretation

A pictorial interpretation can be seen as follows:



7.5 Properties of Isomorphisms

We say that G and G' are isomorphism if there exists some isomorphism between them. Any *purely structural* property of a group is isomorphism-stable in the sense that if G and G' are isomorphic and G has a property, then G' does as well.

Some examples of structural properties include:

- Being finite.
- Having order n for any n.
- Being cyclic.
- Being abelian/commutative.
- Number of elements of a given order.

Remarks:

- $\mathbb{Z}/\mathbb{Z}6$ is not isomorphic to S_3 because $\mathbb{Z}/\mathbb{Z}6$ is commutative but S_3 is not.
- Any two cyclic groups of the same order are isomorphic.

7.5.1 Abelian Structure

Proposition. *Suppose G and G' are isomorphic groups. If G is abelian, then so is G'.*

Proof. We once again take G to have binary operation $*$ and G' to have binary operation $\cdot$. Take $x, y \in G'$. Since G and G' are isomorphic, then let $\varphi(a) = x$ and $\varphi(b) = y$ where $a, b \in G$. Then:

$$\begin{aligned} x \cdot y &= \varphi(a) \cdot \varphi(b) \\ &= \varphi(a * b) && \varphi \text{ is a homomorphism.} \\ &= \varphi(b * a) && G \text{ is abelian (commutative).} \\ &= \varphi(b) \cdot \varphi(a) && \varphi \text{ is a homomorphism.} \\ &= y \cdot x \end{aligned}$$

Therefore, G' is abelian. □

7.5.2 Order Structure

Proposition. *Suppose G and G' are isomorphic groups. If G has a subgroup K of order n, so does G'.*

Proof. Since K is a subgroup of G and $|K| = n$, then $\varphi(K)$ is a subgroup of G'. Since φ maps K bijectively onto $\varphi(K)$, it follows that $|\varphi(K)| = n$. □

7.5.3 Examples of Non-Cyclic Isomorphisms

The following examples are isomorphic to each other:

- The Klein Four Group:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

- $H \subseteq S_4$:

$$\{1, (12)(34), (13)(24), (14)(23)\}$$

- $(\mathbb{Z}/\mathbb{Z}8 - \{0\}, \times)$

$$\{1 \pmod 8, 3 \pmod 8, 5 \pmod 8, 7 \pmod 8\}$$

Even though these examples are completely different, they are isomorphic (they are very similar in *structure*).

8 Equivalence Relations

We will briefly talk about equivalence relations, which are particularly important for near-future topics like cosets.

Note: A lot of the notes here was taken from Professor Golsefidy's Math 103A notes.

8.1 Definition

Let S be a non-empty set. Then, a **relation** over S is a subset R of $S \times S$. If $(x, y) \in R$, we say that x is R-related to y and write xRy.

So, for these relations, we should think about inequalities equalities, or congruences between integers.

Suppose R is a relation over S. Then:

- R is called **reflexive** if $\forall x \in S$, xRx. That is, every $x \in S$ is related to itself.
- R is called **symmetric** if $\forall x, y \in S$, $xRy \implies yRx$. In other words, if x is related to y, is y related to x?
- R is called **transitive** if $\forall x, y, z \in S$, xRy and yRz implies that xRz.

Definition 8.1: Equivalence Relation

An **equivalence relation** on a set S is a relation that holds between certain pairs of elements of S. We may write it as $a \sim b$ and speak of it as *equivalence* of a and b (or simply, a is equivalent to b). An equivalence relation is required to be:

- Reflexive: For all a, $a \sim a$.
- Symmetric: $\forall a, b \in S$, if $a \sim b$, then $b \sim a$.
- Transitive: $\forall a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Remarks:

- An equivalence relation is essentially an equality with respect to a certain measurement. In life, we often measure things or people with respect to properties (for example, scores or ratings). So, when we want to compare things, we pick a certain property and then, *from that point of view*, determine whether these things are equal. In this regard, equivalence relations are exactly equalities.
- Another way we can think of an equivalence relation is through a function:

$$S \times S \mapsto \{\text{true}, \text{false}\}$$

8.1.1 Example: Relations

Suppose X and Y are two non-empty sets and $f : X \mapsto Y$ is a function. Let $\sim$ be the following relation over X:

$$\forall x_1, x_2 \in X \quad x_1 \sim x_2 \iff f(x_1) = f(x_2)$$

Then, $\sim$ is an equivalence relation[6].

[6] Another way of interpreting this statement is as follows: x_1 is in relation to x_2 precisely when $f(x_1) = f(x_2)$. The claim here, then, is that this is an equivalence relation.

Proof. We determine if an relation is an equivalence relation if it satisfies the three properties mentioned above.

- Reflexivity:
$$\forall x \in X, f(x) = f(x) \implies x \sim x$$
- Symmetric:
$$x_1 \sim x_2 \implies f(x_1) = f(x_2) \implies f(x_2) = f(x_1) \implies x_2 \sim x_1$$
- Transitive: We know that:
$$\forall x_1, x_2 \in X \qquad x_1 \sim x_2 \implies f(x_1) = f(x_2)$$
We also know that:
$$\forall x_2, x_3 \in X \qquad x_2 \sim x_3 \implies f(x_2) = f(x_3)$$
It follows that if $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$, then $f(x_1) = f(x_3)$ and thus, $x_1 = x_3$. Namely, $x_1 \sim x_2$ and $x_2 \sim x_3$, then $x_1 \sim x_3$.

It follows that this is an equivalence relation. □

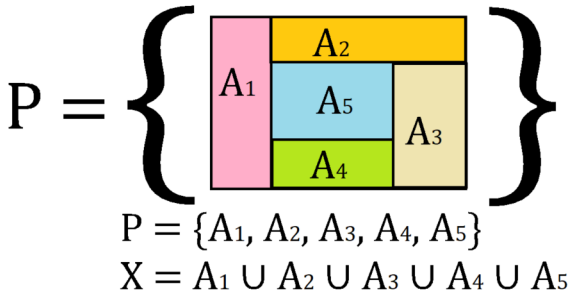
8.2 Equivalence Relation Partitions

Recall that P is called a **partition** of a non-empty set X if:

- Subsets: P consists of non-empty subsets of X.
- Disjointness: $A, B \in P$ and $A \neq B \implies A \cap B = \emptyset$. In other words, the subsets are disjoint.
- Covering: $\forall x \in X$, $\exists A \in P$ such that $x \in A$. In other words, every element in X will be in one of the subsets. Alternatively, $\bigcup_{A \in P} A = X$.

Remark:

- As mentioned, P is a set of sets. For instance, if we have $X = \{1, 2, 3\}$, one possible P is $P = \{\{1\}, \{2, 3\}\}$.
- Below is a visual diagram of what a partition may look like.



Suppose P is a partition of X. Then, we can get a classification function from X to P:

$$X \mapsto P$$

$$x \mapsto [x]_P$$

Here, $[x]_P$ is the unique element of P which contains x. In other words, if we refer to the above diagram, we can think of $[x]_P$, a set, as one of the sets A_1, A_2, A_3, A_4, or A_5 which contains x. So, we can think of this function as saying that every $x \in X$ belongs to one of the sets $[x]_P$.

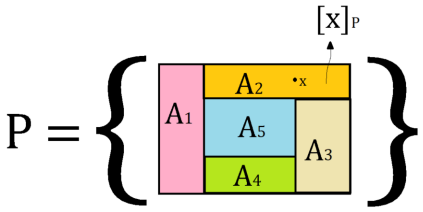
Notice that, because of the **covering** condition, x is contained in some element of P; additionally, because of the **disjointness** condition, x is in an unique element of P (i.e. it is in one of the sets which is in P). So, it follows that the function is well-defined.

By the previous example, $x \sim_P y \iff [x]_P = [y]_P$ is an equivalence relation. So, we obtain the following lemma.

Lemma 8.1

Suppose P is a partition of a non-empty set X. For $x, y \in X$, $x \sim y$ if x and y are in the same element of P. Then, $\sim$ is an equivalence relation.

Remark: Essentially, what this lemma is saying is that if $x \sim y$, then both x and y are in the same set which is in P. In other words, if we refer to the above diagram again, we can think of this situation as saying that both x and y are in one of A_1, A_2, A_3, A_4, or A_5. The diagram below complements the proof.



Proof. For $x \in X$, let $[x]_P$ to be the unique element of P which contains x. So, $x \mapsto [x]_P$ is a function from $X \mapsto P$. By the previous example, $x \sim y \iff [x]_p = [y]_p$ is an equivalence relation over X. Notice that this means $x \sim y$ exactly when x and y are in the same element of P. □

8.3 Equivalence Relation Classes

Now, suppose that $\sim$ is the equivalence relation over a non-empty set X, we can partition X with respect to $\sim$.

For $x \in X$, we let $[x] = \{y \in X \mid y \sim x\}$ (all the elements that are $\sim$-related to x).[7] We call $[x]$ the **equivalence class of x with respect to $\sim$**. When $x \sim y$, we can say that x is equivalent to y with respect to $\sim$.

Proposition. *Suppose $\sim$ is an equivalence relation over a non-empty set X. Then, $\{[x] \mid x \in X\}$ is a partition of X.*

This proposition is essentially asking us to show the following properties:

- Covering: Every element of this set belongs to one of these equivalence classes.
- Disjointness: If we pick two equivalence classes, they do not intersect.

The following lemma follows from this proposition.

Lemma 8.2

$$x \sim y \iff [x] = [y]$$

[7] So, it's obvious that $[x] \subseteq X$.

Proof. We want to show that $[x] = [y] \implies x \sim y$. Recall that the equivalence class of x ($[x]$) and the equivalence class of y ($[y]$) are *sets* and, in particular, we know that $[x]$ consists of all elements that are related to x, including x. Since $\sim$ is reflexive, we know that:

$$x \sim x \implies x \in [x]$$

But, since $[x] = [y]$, then it follows that $x \in [y] \implies x \sim y$. Thus, $[x] = [y] \implies x \sim y$.

To show that $x \sim y \implies [x] = [y]$, we need to show equality of sets $[x] = [y]$. This means that it is necessary and sufficient to prove $[x] \subseteq [y]$ and $[y] \subseteq [x]$.

- To prove $[x] \subseteq [y]$, we let $z \in [x]$. This means that $z \sim x$. However, since $x \sim y$, by transitivity, it follows that $y \sim z$, which implies that $z \in [y]$. Hence, $[x] \subseteq [y]$.
- We note that $x \sim y \implies y \sim x$ by symmetry. Therefore, by the first bullet point, $[y] \subseteq [x]$.

So, it follows that $x \sim y \implies [x] = [y]$. □

Now that we proved the lemma, we can now prove the proposition.

Proof. As mentioned, we need to show that the covering and disjointness properties exist in this partition.

- Covering: $\forall x \in X$, we know that $x \sim x$ by the reflexive property (since $\sim$ is an equivalence relation). Thus, it follows that $x \in [x]$. This means that x is related to x and x is an equivalence class of x, so every element in X belongs to one of the equivalence classes. This implies that the $[x]$ sets are non-empty subsets and cover X.
- Disjointness: Suppose $z \in [x] \cap [y]$ (both equivalence classes are not disjoint). We need to show that they are equal. We know that:

  $$z \in [x] \cap [y] \implies z \in [x] \implies z \sim x \implies [z] = [x]$$

  $$z \in [x] \cap [y] \implies z \in [y] \implies z \sim y \implies [z] = [y]$$

  Where the last two steps came from the lemma. Then, putting these two together, we have:

  $$[z] = [x] \text{ and } [z] = [y] \implies [x] = [y]$$

  We showed that $[x] \cap [y] \neq \emptyset \implies [x] = [y]$, the contrapositive of the disjointness property.

Thus, the proof is complete. □

9 Cosets

There aree two types of cosets: *left* cosets and *right* cosets.

9.1 Left Cosets

Definition 9.1: Left Coset

Let G be a group and H be a subgroup. A **left coset** of H in G is a subset of H of the form:

$$aH = \{ah \mid h \in H\}$$

Where $a \in G$ is a fixed element and is called the *representative* of the coset aH.

Remark: The subgroup H is a particular left coset because $H = \mathrm{id}\, H$, where id is the identity element of H.

9.1.1 Abelian Example: Integers

Let $G = (\mathbb{Z}, +)$ and $H = (\mathbb{Z}n, +)$. For some $a \in G$, the left coset is defined by:

$$aH = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}$$

This represents the entire residue class of $a \pmod n$.

9.1.2 Non-Abelian Example: Permutations

Let $G = S_3 = \{(1), x, x^2, y, xy, x^2y\}$. Define $x = (123)$ and $y = (12)$. Finally, define the subgroup:

$$H = \langle y \rangle = \{(1), y\}$$

Then:

$\mathbf{a \in S_3}$	$\mathbf{aH}$
(1)	$(1)H = \{1, y\}$
x	$xH = \{x, xy\}$
x^2	$x^2H = \{x^2, x^2y\}$
y	$yH = \{y, 1\} = \{1, y\} = (1)H$
xy	$xyH = \{xy, x\} = \{x, xy\} = xH$
x^2y	$x^2yH = \{x^2y, x^2\} = \{x^2, x^2y\} = x^2H$

So, there are three left cosets:

$$\underbrace{\{(1), y\}}_{(1)H = yH} \qquad \underbrace{\{x, xy\}}_{xH = xyH} \qquad \underbrace{\{x^2, x^2y\}}_{x^2H = x^2yH}$$

Notice that the left cosets here partition S_3.

9.2 Left Cosets and Partitions

Consider the following corollary:

Corollary 9.1

The left cosets of H in G form a partition of G. Equivalently, the left cosets of H in G form an equivalence relation:

$$a \sim b \text{ if } b = ah \text{ for some } h \in H$$

Proof. We'll show that the left cosets of H form an equivalence relation. To do so, we show that the three properties of an equivalence relation is satisifed.

- Reflexive: For all $a \in G$, we know that:
$$a = a * \text{id}$$
Where $\text{id} \in H$ is the identity element. Therefore, $a \sim a$; a is in its own left coset.
- Symmetric: If $a \sim b$, this implies that $b = ah$ for some $h \in H$. This further implies that $a = bh^{-1}$ for $h^{-1} \in H$, which shows that $b \sim a$.
- Transitivity: If $a \sim b$ and $b \sim c$, then $b = ah_1$ and $c = bh_2$. Then, $c = (ah_1)h_2 = a(h_1h_2)$ for $h_1, h_2 \in H$. By closure, it follows that $a \sim c$.

So, we are done. □

An alternative proof is as follows:

Proof. We need to show that the union of the left cosets is the whole group, and that different cosets do not overlap. Let $g \in G$. Since $\text{id} \in H$ (the identity element), it follows that $g * \text{id} = g$ is in gH. This shows that every element of G lies in some coset of H, so the union of the cosets is all of G.

Suppose aH and bH are two cosets of H, and suppose $aH \cap bH \neq \emptyset$ (i.e. they are not disjoint). Then, it must be the case that $aH = bH$ (or else we would have overlaps). To show that this is the case, take $g \in aH \cap bH$. We write $g = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then:

$$g = ah_1 \iff gh_1^{-1} = a$$

So:

$$a = gh_1^{-1} = bh_2h_1^{-1}$$

Let $ah \in aH$. Then:

$$ah = bh_2h_1^{-1}h$$

We now note that $bh_2h_1^{-1}h \in bH$ since $h_2h_1^{-1}h \in H$. Therefore, $ah \in bH$ and so $aH \subset bH$. By symmetry, we know that $bH \subset aH$ so that $aH = bH$, as expected. □

Remark: To summarize, let H be a subgroup of a group G and let $a, b \in G$. The following are equivalent:

- $b = ah$ for some $h \in H$, or $a^{-1}b \in H$.
- b is an element of the left coset aH.
- The left cosets aH and bH are equal.

Remark: The number of left cosets of a subgroup is called the *index* of H in G. The index is denoted by:

$$[G : H]$$

So, in the S_3 example above, $[S_3, \langle y \rangle] = 3$.

9.2.1 Partition and Order

Lemma 9.1

All left cosets aH of a subgroup H of a group G have the same order. Alternatively, any two left cosets have the same number of elements.

Proof. Multiplication by a defines a map $H \mapsto aH$ that sends $h \mapsto ah$. This map is bijective, with the inverse of this map being multiplication by a^{-1}. □

Remarks:

- Another way to think about it is as follows: if H has cardinality n, then aH must also have cardinality n since all we're doing is multiplying a to each element of H. The same idea applies with bH.
- Since left cosets have the same order, and since they partition the group, we obtain the important *counting formula:*

$$|G| = |H|[G : H]$$

So, in the S_3 example above, $6 = 2[G : H] \iff [G : H] = 3$.

9.3 Lagrange's Theorem

Theorem 9.1: Lagrange's Theorem

Let G be a finite group (not necessarily cyclic) and let H be a subgroup. Then, the order of H always divides the order of G.

Proof. The ratio $\frac{|G|}{|H|}$ (the order of G divided by the order of H) is simply the number of left cosets. □

Corollary 9.2

For a finite group G and an element $a \in G$, the order of a divides the order of G.

Proof. The order of an element a of a group G is equal to the order of the cyclic subgroup $\langle a \rangle$ generated by a. □

As an example, the possible orders of elements of a group with order 12 are 1, 2, 3, 4, 6, and 12.

Corollary 9.3

Suppose G is a group of prime order p. Then, G is a cyclic group.

Proof. Suppose G is a group of order p, a prime number. Let $g \in G$ such that g is not the identity. Then, $\langle g \rangle \leq G$ and since $g \neq 1$, it follows that $|\langle g \rangle| \neq 1$. However, by Lagrange's Theorem, $|\langle g \rangle|$ divides $|G|$. The only positive integers which divide $|G| = p$ are 1 and p, so it follows that $|\langle g \rangle| = p$. This means that $\langle g \rangle = G$, so G is cyclic with generator g. □

9.4 Relationship to Homomorphisms

We can apply the counting formula to the homomorphism

$$\varphi : G \mapsto G'$$

Here, we see that elements $a, b \in G$ are congruent, i.e. $\varphi(a) = \varphi(b)$ if and only if b is in the coset aK of the kernal K.

Proposition. *Let $\varphi : G \mapsto G'$ be a homomorphism with $\ker(\varphi) = K$. Then, for each $a, b \in G$, the following are equivalent:*

(a) $\varphi(a) = \varphi(b)$.

(b) $a^{-1}b \in K$.

(c) $b \in aK$.

(d) $bK = aK$.

We'll provide a proof for the first statement.

Proof.

$$\begin{aligned}
\varphi(a) = \varphi(b) &\iff \varphi(a^{-1})\varphi(a) = \varphi(a^{-1})\varphi(b) \\
&\iff \varphi(a^{-1}a) = \varphi(a^{-1}b) \\
&\iff \varphi(\mathrm{id}) = \varphi(a^{-1}b) && \varphi \text{ is a homomorphism} \\
&\iff \mathrm{id} = \varphi(a^{-1}b) \\
&\iff a^{-1}b \in K && \text{Definition of kernal} \\
&\iff b \in aK
\end{aligned}$$

So, the first point is done. □

Corollary 9.4

The homomorphism $\varphi : G \mapsto G'$ is injective if and only if $\ker(\varphi) = \{\mathrm{id}\}$ (the trivial group).

Another corollary comes from the counting formula. In particular, for a homomorphism $\varphi : G \mapsto G'$, the following counting formula holds:

$$[G : \ker \varphi] = |\operatorname{im} \varphi|$$

Corollary 9.5

Let $\varphi : G \mapsto G'$ be a homomorphism of finite groups. Then:

- $|G| = |\ker \varphi| \cdot |\operatorname{im} \varphi|$.
- $|\ker \varphi|$ divides $|G|$.
- $|\operatorname{im} \varphi|$ divides both $|G|$ and $|G'|$.

9.5 Right Cosets

Of course, we cannot forget the right coset.

Definition 9.2: Right Coset

Let G be a group and H be a subgroup. A **right coset** of H in G is a subset of H of the form:

$$Ha = \{ha \mid h \in H\}$$

Where $a \in G$ is a fixed element.

We note that right cosets also partition the group G; however, right cosets aren't always the same as left cosets. To showcase this, consider again $G = S_3$ with $H = \langle y \rangle$ where $x = (\overline{123}) \in S_3$ and $y = (12) \in S_3$. Then:

$\mathbf{a \in S_3}$	$\mathbf{Ha}$
(1)	$H(1) = \{1, y\}$
x	$Hx = \{x, yx\}$
x^2	$Hx^2 = \{x^2, yx^2\} = \{x^2, xy\}$
y	$Hy = \{y, 1\} = \{1, y\} = H(1)$
xy	$Hxy = \{xy, yxy\} = \{x^2, xy\} = Hx^2$
x^2y	$Hx^2y = \{x^2y, yx^2y\} = \{x^2, x^2y\} = Hx$

That being said, the left and right cosets *would* be equal if the subgroup H is normal. This will be discussed in the next section.

10 Conjugation and Normal Subgroups

In this section, we place significantly more emphasis on conjugations and normal subgroups.

10.1 Conjugation

Let's first recall the definition of conjugation.

Definition 10.1: Conjugation

Let G be a group. Let $a, g \in G$ be elements. Then, the **conjugate** of a by g is the element:

$$g * a * g^{-1} \in G$$

Why is this important?

- If we fix g, then we know that:

  $$(g * a * g^{-1}) * (g * b * g^{-1}) = g * (a * b) * g^{-1}$$

  In other words, the function $\varphi_g : G \mapsto G$ can be defined by:

  $$\varphi_g(a) = g * a * g^{-1}$$

  This is a homomorphism. We also note that its inverse can be defined by the function $\varphi_{g^{-1}}$.

- Suppose we have an element that doesn't "move" when conjugated by g. In particular:

  $$g * a * g^{-1} = a \iff g * a = a * g$$

  Then, g commutes with a.

10.2 Conjugation in Symmetric Groups

Let's suppose we have $g = (12345)$ and $a = (12)(34)$, and we wanted to find gag^{-1}. Then:

$$g^{-1} = (15432)$$

Mapping each of $i \in [1, 2, 3, 4, 5]$, we have:

- $1 \xrightarrow{g^{-1}} 5 \xrightarrow{a} 5 \xrightarrow{g} 1$
- $2 \xrightarrow{g^{-1}} 1 \xrightarrow{a} 2 \xrightarrow{g} 3$
- $3 \xrightarrow{g^{-1}} 2 \xrightarrow{a} 1 \xrightarrow{g} 2$
- $4 \xrightarrow{g^{-1}} 3 \xrightarrow{a} 4 \xrightarrow{g} 5$
- $5 \xrightarrow{g^{-1}} 4 \xrightarrow{a} 3 \xrightarrow{g} 4$

So, our result is:

$$g * a * g^{-1} = (1)(23)(45)$$

We notice a few things. In general:

- $g * a * g^{-1}$ has the same cycle structure as a, which implies that they have the same order.
- We also get the new cycle structure from the old one by applying g to the cycle notation of a.

10.3 Conjugacy as an Equivalence Relation

Conjugation is an example of an equivalence relation on a group. Two group elements $a, b \in G$ are conjugate, $a \sim b$ if $b = gag^{-1}$ for some $g \in G$. This will be formalized in the following lemma.

Lemma 10.1

Conjugacy is an equivalence relation.

Proof. We simply show that all three properties of an equivalence relation is satisifed.

- Reflexive: $x = exe^{-1}$. Here, x is in the same conjugacy class as itself so $x \sim x$.
- Symmetric: $x = gyg^{-1} \implies y = g^{-1}yg$. Here, x is conjugate to y implies that y is conjugate is to x, or that $x \sim y \implies y \sim x$.
- Transitive: $x = gyg^{-1}$ and $y = hzh^{-1}$ implies that $x = (gh)z(gh)^{-1}$. Here, this means that $x \sim y$ and $y \sim z$ implies that $x \sim z$.

So, conjugacy is an equivalence relation. □

Since conjugacy is an equivalence relation, it partitions the group G into equivalence classes, known as **conjugacy classes**.

10.4 Conjugacy Classes

Given some fixed $a \in G$, something that we may ask is: which elements can be written as gag^{-1} for some $g \in G$? The set of all such elements in G is called the conjugacy class of a and is denoted by $C(a)$. Formally, this is the set:

$$C(a) = \{gag^{-1} \mid g \in G\}$$

Some remarks to consider:

- In any group, $C(\mathrm{id}) = \{\mathrm{id}\}$ where id is the identity element. This is because $g\,\mathrm{id}\,g^{-1} = \mathrm{id}$ for any $g \in G$.
- If a and g commute, then $gag^{-1} = a$. Thus, when computing $C(a)$, we only need to check gag^{-1} for those $g \in G$ that do not commute with a.
- Moreover, $C(x) = \{x\}$ if and only if x commutes with everything in G.

Note: This will be further discussed later.

10.4.1 Example: Symmetric Group of 3 Elements

For any symmetric group, cycle type determines conjugacy classes. Consider the symmetric group of 3 elements. It has the following conjugacy classes:

Cycle Structure	Elements	Size of Conjugacy Class
`(a)(b)(c)`	$\{(1)\}$	1
`(ab)(c)`	$\{(12), (23), (13)\}$	3
`(abc)`	$\{(123), (132)\}$	2

10.4.2 Example: Symmetric Group of 4 Elements

For any symmetric group, cycle type determines conjugacy classes. Consider the symmetric group of 4 elements. It has the following conjugacy classes:

Cycle Structure	Elements	Size of Conjugacy Class
(a)(b)(c)(d)	$\{(1)\}$	1
(ab)(c)(d)	$\{(12), (13), (14), (23), (24), (34)\}$	6
(ab)(cd)	$\{(12)(34), (13)(24), (14), (23)\}$	3
(abc)(d)	$\{(123), (132), (234), (243), (341), (314), (412), (421)\}$	8
(abcd)	$\{(1234), (1243), (1324), (1342), (1423), (1432)\}$	6

10.5 Center of a Group

Definition 10.2: Center of a Group

The **center** of G is the set Z of elements which commute with all of G. In particular, it is defined by:

$$Z = \{z \in G \mid z * x = x * z \text{ for all } x \in G\}$$

Remarks:

- Z is always a normal subgroup of G.
- The center of the general linear group $GL_n(\mathbb{R})$ consists of all scalar matrices. In other words:

$$\left\{ \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & a \end{bmatrix} \;\middle|\; a \in \mathbb{R} - \{0\} \right\}$$

- The center of the special linear group $SL_2(\mathbb{R})$ consists of $\{I, -I\}$.
- The center of the special linear group $SL_n(\mathbb{R})$ consists of:

$$\begin{cases} \{\pm \mathbf{I}\} & n \text{ even} \\ \{\mathbf{I}\} & n \text{ odd} \end{cases}$$

- The center of the symmetric group S_n is trivial if $n \geq 3$.

Consider the following proposition:

Proposition. *Z is an abelian subgroup.*

Proof. We need to show that Z meets all the properties of a subgroup.

- Identity: We know that $\text{id} \in Z$.
- Closure: If we have $g, h \in Z$ with some random $a \in G$, we know that:

$$g * h * a = g * a * h = a * g * h \in Z$$

- Inverse: Suppose we have $g \in Z$ with corresponding inverse $g^{-1} \in Z$ and some $a \in G$. Then:

$$g^{-1} * a = a * g^{-1} \iff a * g = g * a$$

□

Hence, Z is a subgroup.

10.6 Automorphisms

Recall that, when we talked about conjugations, we mentioned that this was a homomorphism:

$$\varphi_g : G \mapsto G$$

In fact, we can say that this is an *automorphism*. We define this like so:

Definition 10.3: Automorphism

An **automorphism** is an *isomorphism* on a group G to itself. It is defined by:

$$\varphi : G \mapsto G$$

We also note that the **automorphism group** of a group G form a group under *composition*. Notationally, this is represented by $\text{Aut}(G)$.

Conjugation defines a homomorphism from $G \mapsto \text{Aut}(G)$, which is defined by:

$$g \mapsto \varphi_g$$

Consider:

$$(g * h) * a * (h^{-1} * g^{-1}) = g * (h * a * h^{-1}) * g^{-1}$$

Which we can define by:

$$\varphi_{g*h} = \varphi_g \circ \varphi_h$$

One interesting case to note is: if G is *abelian*, then:

$$\varphi_g(a) = a \qquad \forall a \in G$$

In other words, $\varphi_g = \text{id}_g$. This implies that the homomorphism $G \mapsto \text{Aut}(G)$ is *trivial*.

On the other hand, for $n \geq 3$, the following is isomorphic:

$$S_n \mapsto \text{Aut}(S_n)$$

However, this is not isomorphic[8] when $n = 6$.

10.7 Commutator

The commutator of a and g is given by:

$$g * a * g^{-1} * a^{-1}$$

This is id (the identity) if and only if g commutes with a. In particular:

Lemma 10.2

Two element a and b of a group commute, $a * b = b * a$, if and only if $a * b * a^{-1} = b$, and this is true if and only if $a * b * a^{-1} * b^{-1} = 1$.

[8] If interested, look up "outer automorphism of S_6."

10.8 Normal Subgroups

Recall the following definition:

Definition 10.4: Normal Subgroup

A subgroup H of a group G is (with binary operation $*$) **normal** if $\forall g \in G$ and $\forall h \in H$:

$$g * h * g^{-1} \in H$$

Notationally, we can write this as $H \triangleleft G$. Equivalently, we can say that:

- $g^{-1} * h * g \in H$.
- $g * H * g^{-1} \subseteq H$ and $H \subseteq g * H * g^{-1}$. We can do this by multiplying the left side of the first expression by g^{-1} and the right side by g.
- $g * H * g^{-1} = H$.

A few examples of normal subgroups:

- The trivial subgroup is normal.
- G is normal in itself.

Now, we briefly talk about a proposition:

Proposition. *Let H be a subgroup of a group G. The following conditions are equivalent:*

(i) H is a normal subgroup. For all $h \in H$ and all $g \in G$, $g * h * g^{-1} \in H$.

(ii) For all $g \in G$, $g * H * g^{-1} = H$.

(iii) For all $g \in G$, $gH = Hg$.

(iv) Every left coset of H in G is a right coset. In other words:

$$\underbrace{g * H}_{\text{Left coset.}} = \underbrace{H * g}_{\text{Right coset.}}$$

Proof. The notation $g * H * g^{-1}$ stands for the set of all elements $g * h * g^{-1}$ with $h \in H$. Suppose that H is normal. Then, it's obvious that (i) holds, and implies that $g * H * g^{-1} \subseteq H$ for all $g \in G$. Substituting g^{-1} for g shows that $g^{-1} * H * g \subseteq H$ as well. If we multiply this inclusion on the left by g and on the right by g^{-1}, we now have that $H \subseteq g * H * g^{-1}$. Therefore, $g * H * g^{-1} = H$, proving (ii). We can work backwards to show that (ii) implies (i).

With $g * H * g^{-1} = H$, multiply both sides on the right by g gives us:

$$g * H = H * g$$

Which shows that (ii) implies (iii). We can reverse this operation easily, so (iii) implies (ii).

For the last part, we need to know when a left coset is equal to a right coset. Remember that the right coset partitions the group G, and we note that the left coset gH and the right coset Hg have an element in common: $g = g * 1 = 1 * g$. So, if the left coset gH is equal to any right coset, that coset must be Hg. □

Proposition. *(a) If H is a subgroup of a group G and g is an element of G, the set $g * H * g^{-1}$ is also a subgroup.*

(b) If a group G has just one subgroup H of order r, then that subgroup is normal.

We now introduce another example of normal subgroups in example.

Proposition. *Let H be a subgroup of G. If $[G : H] = 2$, then H is normal.*

Proof. Since $[G : H] = 2$, it follows that H has two left and right cosets. The cosets are H itself (the identity element), which means that gH and Hg are the other left and right cosets, respectively. By the definition of a coset, we know that:

$$H \cup gH = G = H \cup Hg$$

Because these are disjoint unions, it follows that $gH = Hg$, so it follows that $gHg^{-1} = H$. This equation holds for any g in the coset gH, and clearly holsd for any element of the trivial coset H. So, the equation holds for all G, and H is normal. □

Finally, we can relate conjugacy classes to normal subgroups.

Theorem 10.1

Let G be a group and let H be a subgroup of G. Then, H is normal in G if and only if H is a union of conjugacy classes of G.

Proof.

$$\begin{aligned}
H \triangleleft G &\iff \forall g \in G, gHg^{-1} \subseteq H && \text{Definition of Normal Subgroup} \\
&\iff \forall h \in H, \forall g \in G, ghg^{-1} \in H && \text{Definition of Normal Subgroup} \\
&\iff \forall h \in H, C(h) \subseteq H && \text{Where } C(h) \text{ is the conjugacy class of } h \in G \\
&\iff H = \bigcup_{h \in H} C(h)
\end{aligned}$$

So, we are done. □

Remark: So, we can say that a normal subgroup is a **subgroup** that is a **union of conjugacy classes**.

10.8.1 Example: Symmetric Group of 4 Elements

Recall our example from above. For any symmetric group, cycle type determines conjugacy classes. Consider the symmetric group of 4 elements. It has the following conjugacy classes:

Cycle Structure	Elements	Size of Conjugacy Class
(a)(b)(c)(d)	$\{(1)\}$	1
(ab)(c)(d)	$\{(12), (13), (14), (23), (24), (34)\}$	6
(ab)(cd)	$\{(12)(34), (13)(24), (14), (23)\}$	3
(abc)(d)	$\{(123), (132), (234), (243), (341), (314), (412), (421)\}$	8
(abcd)	$\{(1234), (1243), (1324), (1342), (1423), (1432)\}$	6

So, a normal subgroup of S_4 will be a union of these *conjugacy classes*. For example, the union of conjugacy classes shown below is a normal subgroup of S_4:

$$C((1)) \cup C((12)(34)) = \{(1), (12)(34), (13)(24), (14), (23)\}$$

Of course, we can't simply just take any conjugacy classes and take the union of them. In fact, for S_4, the above subgroup is the only non-trivial proper normal subgroup.

- For example, if we tried to take the conjugacy class of the identity and the conjugacy class of the transpositions, e.g. $C((1)) \cup C((12))$, then we won't have closure. So, this isn't even a subgroup.
- If we don't have the identity to begin with, then that's a problem.

So, making a subgroup by taking the union of the conjugacy classes is *not a given*. To show that S_4 only has one non-trivial proper normal subgroup, it is important to realize that:

- Each conjugacy class is disjoint one from another. So, taking the union of two conjugacy classes will result in the number of elements being the sum of the number of the elements from those classes.
- Every subgroup must have the identity element, so we must always pick the identity conjugacy class.
- By Lagrange's Theorem, the order of the subgroup must divide the order of the group. Since $|S_4| = 24$, we need to find a subgroup of order 1, 2, 3, 4, 6, 8, 12, or 24. Since it cannot be trivial or the entire group, we need to find a subgroup of order 2, 3, 4, 6, 8, or 12.
- By looking at the orders of each conjugacy class, we note that we can only hae $C(1)$ and $C((12)(34))$. This is because $1 + 3$ divides 24. However, $1 +$ any even number (which are the other sizes of the conjugacy classes) will result in an odd number, which does not divide 24.

10.8.2 Example: Symmetric Group of 5 Elements

Suppose we wanted to show that S_5 contains no normal subgroup of order 5.

Proof. First, we note that normal subgroups are simply unions of conjugacy classes. For symmetric groups, the conjugacy classes are permutations of the same cycle structure. Recall that $|S_5| = 5! = 120$. Getting the number of occurrences of each cycle involves using some combinatorics.

- $\underline{(a)(b)(c)(d)(e)}$: The identity permutation is the only permutation with order 1, so there is $\mathbf{1}$.
- $\underline{(ab)(c)(d)(e)}$: There are $\binom{5}{2}$ ways to pick two elements from a set of 5 elements, and then $\frac{2!}{2}$ ways to rearrange these elements uniquely in a cycle. The result is $\binom{5}{2}\frac{2!}{2} = 10$.
- $\underline{(ab)(cd)(e)}$: There are $\binom{5}{2}$ ways to pick the first two elements from a set of 5 elements and $\frac{2!}{2}$ ways to rearrange these elements uniquely in the first 2-cycle. Then, there are $\binom{3}{2}$ ways to pick the next two elements from a set of 3 elements (note that we took out the first two elements) and $\frac{2!}{2}$ ways to rearrange these elements in a 2-cycle. This results in $\binom{5}{2}\frac{2!}{2}\binom{3}{2}\frac{2!}{2}$. But, because this does not account for the possibility that $(ab)(cd) = (cd)(ab)$, we need to divide by 2 to get the correct answer. Thus, the result is $\frac{\binom{5}{2}\frac{2!}{2}\binom{3}{2}\frac{2!}{2}}{2} = 15$.
- $\underline{(abc)(d)(e)}$: There are $\binom{5}{3}$ ways to pick three elements from a set of 5 elements, and $\frac{3!}{3}$ ways to rearrange these elements in a 3-cycle uniquely. Thus, the result is $\binom{5}{3}\frac{3!}{3} = 20$.
- $\underline{(abc)(de)}$: There are $\binom{5}{3}$ ways to pick 3 elements from a set of 5 elements and $\frac{3!}{3}$ ways to rearrange these elements in a 3-cycle uniquely. There are $\binom{2}{2}$ ways to pick 2 elements from the set of 2 remaining elements (we took out 3 elements for the previous cycle) and $\frac{2!}{2}$ ways to rearrange these elements in a 2-cycle uniquely. Thus, the result is $\binom{5}{3}\frac{3!}{3} \cdot \binom{2}{2}\frac{2!}{2} = 20$.
- $\underline{(abcd)(e)}$: There are $\binom{5}{4}$ ways to pick four elements from a set of 5 elements, and $\frac{4!}{4}$ ways to rearrange these elements in a 4-cycle uniquely. Thus, the answer is $\binom{5}{4}\frac{4!}{4} = 30$.
- $\underline{(abcde)}$: As we are dealing with the entire set, there is only one way to pick 5 elements from a set of 5 elements. There are $\frac{5!}{5}$ ways to rearrange these elements in a 5-cycle uniquely. Thus, the

answer is $\binom{5}{5}\frac{5!}{5} = 24$.

So, the orders are as follows:

Structure/Class	Occurance
(1)	1
(ab)	10
$(ab)(cd)$	15
(abc)	20
$(abcd)$	30
$(abcde)$	24

By Lagrange's Theorem, we know that any subgroup of S_5 must have order that divides $|S_5| = 120$. We also know that the a normal subgroup is a subgroup that is also the union of conjugacy classes. Since our subgroup must have the identity element, our subgroup has at least order 1. However, the rest of the conjugacy classes have order that is greater than 4 (since we already picked the identity conjugacy class). Therefore, S_5 cannot have a normal subgroup of order 5. □

10.8.3 Example: Alternating Group

The alternating group A_n is a normal subgroup of S_n. This is because the even permutations make up half of S_n, so $[S_n : A_n] = 2$. Therefore, A_n is normal.

10.8.4 Example: Symmetric Group

Consider $G = S_3$ with $H = \langle(123)\rangle$. Then, H is normal. This is because conjugation by g must send h to an element of order 3, namely h or h^{-1}. We know that:

$$\langle h\rangle = \langle h^{-1}\rangle = H$$

10.9 Kernal of a Homomorphism

Consider the following proposition:

Proposition. *The kernal of a homomorphism is a normal subgroup.*

The proof is as follows:

Proof. If a is in the kernal of the homomorphism $\varphi : G \mapsto G'$ and if g is any element of G, then:

$$\varphi(g * a * g^{-1}) = \varphi(g) \cdot \varphi(a) \cdot \varphi(g) = \varphi(g) \cdot \mathrm{id}_{G'} \cdot \varphi(g)^{-1}.$$

Therefore, $g * a * g^{-1}$ is in the kernal too. □

11 Quotient Groups

We can use the properties of a normal subgroup to talk more about quotient groups.

11.1 Definition of a Quotient Group

First, as always, we begin with a definition.

Definition 11.1: Quotient Group

Let N be a normal subgroup of a group G. We define the **quotient group** of N in G, written $\overline{G} = G/N$, and read "G modulo N," as the set of cosets of N in G.

We also note the following theorem:

Theorem 11.1

Let N be a normal subgroup of a group G, and let $\overline{G}$ denote the set of cosets of N in G. We can define a surjective homomorphism:

$$\pi : G \mapsto \overline{G}$$

Defined by:

$$\pi(a) = \overline{a}$$

Here, $\ker(\pi) = N$.

11.1.1 Example: Integers

For example, if $G = (\mathbb{Z}, +)$ and $H = \mathbb{Z}n$, then $\overline{G} = \mathbb{Z}/\mathbb{Z}n$. We can define:

$$\varphi : G \mapsto \overline{G}$$

$$\varphi : \mathbb{Z}^+ \mapsto \mathbb{Z}/\mathbb{Z}n$$

By performing the following mapping:

$$a \mapsto a \mod n$$

11.1.2 Example: Symmetric Group

Let $G = S_3$ and $N = \langle (123) \rangle$. Then:

$$S_3/\langle (123) \rangle = \{N, (12)N\}$$

Where:

$$N = \{(1), (123), (132)\}$$

$$(12)N = \{(12), (23), (13)\}$$

11.2 Product of Cosets

Here, we will show that the product of two cosets is a coset.

Lemma 11.1

Let N be a normal subgroup for G. Let $s_1 = a * N$ and $s_2 = b * N$ be two cosets of N in G. Then:

$$s_1 * s_2 = \boxed{a * b * N} = \{g_1 * g_2 \mid g_1 \in s_1, g_2 \in s_2\}$$

Proof. The proof is as follows:

$$\begin{aligned} a*N*b*N &= \{a*n_1*b*n_2 \mid n_1, n_2 \in N\} \\ &= \{a*b* \underbrace{\underbrace{(b^{-1}*n_1*b)}_{\in N \text{ by conjugation}} *n_2}_{\in N \text{ by subgroup}} \mid n_1, n_2 \in N\} \end{aligned}$$

We also know that:

$$\begin{aligned} a*b*N &= \{a*b*n \mid n \in N\} \\ &= \{a*\mathrm{id}*b*n \mid n \in N\} \end{aligned}$$

As these are equal, the proof is complete. □

11.3 Showing Group Properties

Now that we know that the product of two cosets is a cosets, we define a law of composition on $\overline{G}$:

$$aN * bN = ab * N$$

The above lemma states that this is a well-defined operation. We now need to check that this is a group. In particular, we need to show:

- Associativity.
- Identity.
- Inverse.
- Homomorphism (By definition).

Proof. Let G be a group. We know that $\varphi : G \mapsto \overline{G}$ is a surjective function and $\varphi(a) \cdot \varphi(b) = \varphi(a*b)$. Pick three elements $\overline{x_1}$, $\overline{x_2}$, and $\overline{x_3}$. Write these as $\varphi(\overline{x_1})$, $\varphi(\overline{x_2})$, and $\varphi(\overline{x_3})$ for some x_1, x_2, and $x_3 \in G$. Then, in G, we have that:

$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$$

Applying φ to both sides:

$$\begin{aligned} \varphi(x_1 * (x_2 * x_3)) &= \varphi(x_1) \cdot \varphi(x_2 * x_3) \\ &= \varphi(x_1) \cdot (\varphi(x_2) \cdot \varphi(x_3)) \\ &= \overline{x_1} \cdot (\overline{x_2} \cdot \overline{x_3}) \end{aligned}$$

We can apply the same steps to the expression on the left side. Therefore, this is associative. The rest of the group properties will be omitted.

We have now proved that for every normal subgroup N of G, $\varphi : G \mapsto \overline{G}$ is a surjective homomorphism. □

12 First Isomorphism Theorem and Correspondence Theorem

Let G be a group and N a normal subgroup of G. In other words, $\forall g \in G$, we have that $g * N * g^{-1} = N$. We also defined the quotient group $\overline{G}$, which is a group with a surjective homomorphism $\pi : G \mapsto \overline{G}$ with kernal N.

We can use this information to introduce the First Isomorphism Theorem.

12.1 First Isomorphism Theorem

Theorem 12.1: First Isomorphism Theorem

Let $\varphi : G \mapsto G'$ be a surjective group homomorphism with kernal N. The quotient group $\overline{G}$ is isomorphic to the image of G'. To be precise, let $\pi : G \mapsto \overline{G}$ be the canonical map. There is a unique $\overline{\varphi} : \overline{G} \mapsto G'$ such that:

$$\varphi = \overline{\varphi} \circ \pi$$

A significantly more concise definition of the First Isomorphism Theorem is as follows:

Theorem 12.2: First Isomorphism Theorem (Concise)

Let $\varphi : G \mapsto G'$ be a homomorphism. Then, there is a well-defined induced isomorphism $\overline{\varphi} : G/\ker(\varphi) \mapsto \text{im}(\varphi)$.

The proof is as follows:

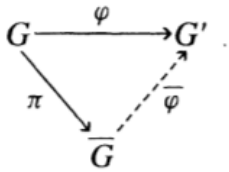
Proof. The partition defined by π and φ are the same; namely, the cosets of N. Define $\overline{\varphi}$ by saying that for $\overline{g} \in \overline{G}$, $\overline{\varphi}(\overline{g})$ is the unique element of G' such that $\pi^{-1}(\overline{g}) = \varphi^{-1}(h)$ as cosets of N.

$\overline{\varphi}$ is a homomorphism because $\overline{g}, \overline{h} \in \overline{G}$ whose $g, h \in G$ with $\pi(g) = \overline{g}$ and $\pi(h) = \overline{h}$, which implies that $\pi(g * h) = \overline{g} \cdot \overline{h}$. Then:

$$\begin{aligned}
\overline{\overline{g} * \overline{h}} &= \overline{\varphi}(\pi(g * h)) \\
&= \varphi(g * h) \\
&= \varphi(g) \cdot \varphi(h) \\
&= \overline{\varphi}(\pi(g)) \cdot \overline{\varphi}(\pi(h)) \\
&= \overline{\varphi}(\overline{g})\overline{\varphi}(\overline{\overline{h}})
\end{aligned}$$

Thus, we are done. □

Consider the following diagram, which highlights this theorem:



Any surjective homomorphism with the kernal N are preimages of elements that have cosets of N.

Recall this lemma, which we may or may not have talked about at some point.

Lemma 12.1

Let $\varphi : G \mapsto G'$ be a surjective homomorphism with kernal N. Then, for every $g' \in G'$:

$$\varphi^{-1}(g') = \{g \in G \mid \varphi(g) = g'\}$$

Represents a left/right coset of N.

Its proof is as follows:

Proof. Since φ is surjective, we can pick a $g_1 \in G$ with $\varphi(g_1) = g'$. We claim that $g_1 * N = \varphi^{-1}(g') = N * g$. We show that $g_1 N \subseteq \varphi^{-1}(g')$. For any $n \in N$, we note that $\varphi(g * n) = \varphi(g_1) \cdot \varphi(n) = \varphi(g_1)$. Now we show that $\varphi^{-1}(g') \subseteq g_1 * N$. Pick any $g_2 \in G$ with $\varphi(g_2) = g'$. Then, $\varphi(g_1) = \varphi(g_2)$ implies that $\varphi(g_1^{-1} * g_2) = \varphi(g_1)^{-1} \cdot \varphi(g_2) = \text{id}$. So:

$$g_1^{-1} * g_2 \in N \implies g_2 \in g_1 * N$$

So, we are done. □

The following corollary is probably the most useful:

Corollary 12.1

Let $\varphi : G \mapsto G'$ be a group homomorphism with kernal N and image H'. The quotient group $\overline{G} = G/N$ is isomorphic to the image H'.

So, if we need to show that there is an isomorphism of the form:

$$G/N \cong H$$

All we need to do is:

- Find $\varphi : G \mapsto H$ (a homomorphism).
- Show that $\ker(\varphi) = N$.
- Show that $\text{im}(\varphi) = H$.

12.1.1 Example 1: Matrices

Suppose we wanted to show that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R} - \{0\}$.

- Consider $\varphi : GL_n(\mathbb{R}) \mapsto \mathbb{R} - \{0\}$, the determinant function.
- The kernal of φ is all matrices with determinant 1. Thus:

$$\ker(\varphi) = SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$$

- The image of φ is simply all possible determinants; that is:

$$\text{im}(\varphi) = \mathbb{R} - \{0\}$$

Therefore, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R} - \{0\}$.

12.1.2 Example 2: Permutations

Suppose we wanted to show that $S_n/A_n \cong \{\pm 1\}$.

- Consider $\varphi : S_n \mapsto \{\pm 1\}$, the sign function.
- By definition, $\ker(\varphi) = A_n$ (recall that the sign of any even permutation is 1).
- By definition, the sign function is surjective if $n \geq 2$.

Therefore, $S_n/A_n \cong \{1\}$.

12.1.3 Example 3: Group Itself

Suppose we wanted to show that $G/G \cong \{1\}$.

- Consider $\varphi : G \mapsto G$ by the function $\varphi(g) = 1$, which is a surjective homomorphism.
- The kernal of φ is all elements $g \in G$ such that $\varphi(g) = 1$. So, this is trivially just G. Thus, $\ker(\varphi) = G$.
- Because φ is surjective, $\text{im}(\varphi) = \{1\}$.

So, $G/G \cong \{1\}$.

12.2 Correspondence Theorem

We now talk about the correspondence theorem.

Theorem 12.3: Correspondence Theorem

Let $\varphi : G \mapsto G'$ be a surjective homomorphism with kernal N. Then, there is a bijection from the subgroups of G' to the subgroups of G containing N defined by:

$$H' \mapsto \varphi^{-1}(H')$$

Definition 12.1: Restriction

Let $\varphi : G \mapsto G'$ be a homomorphism. Let H be a subgroup (not necessarily normal) of G. We define:

$$\varphi|_H : H \mapsto G'$$

To be the restriction. It can be written as the composition $H \mapsto G \xrightarrow{\varphi} G'$ (the inclusion homomorphism).

Remarks:

- $\ker\left(\frac{\varphi}{H}\right) = (\ker(\varphi)) \cap H$.
- $\text{im}\left(\frac{\varphi}{H}\right) = \varphi(H) = \{\varphi(h) \mid h \in H\}$

12.2.1 Example: Permutations and Sign

Let $\sigma : S_n \mapsto \{\pm 1\}$ be the sign homomorphism. We define the alternating group A_n to be $\ker(\sigma)$. In other words:

$$A_n = \ker(\sigma)$$

Suppose H is a subgroup of S_n of odd order. (e.g., $\langle g \rangle$ where g is a cycle of odd length). Then:

$$|H| = |\ker(\varphi\,|_H)| \cdot \underbrace{\left|\text{im}\left(\frac{\varphi}{H}\right)\right|}_{\substack{\text{Order must divide} \\ \text{order of } \{\pm 1\}}}$$

Here, we note that $\left|\text{im}\left(\frac{\varphi}{H}\right)\right|$ must be 1. This means that $H \subseteq A_n$.

12.3 Inverse Image

We now define an inverse image.

Definition 12.2: Inverse Image

Let $\varphi : G \mapsto G'$ be a homomorphism. Then, for $H' \subseteq G'$ a subgroup, the **inverse image** (preimage) is defined by:

$$\varphi^{-1}(H') = \{g \in G \mid \varphi(g) \in H\}$$

THis is a subgroup because it has all three characteristics of a subgroup (which we will not show).

For example, if the homomorphism is $(\mathbb{Z}, +) \mapsto (\mathbb{Z}/\mathbb{Z}n)$, then for any d that divides n, the multiples of d in $\mathbb{Z}/\mathbb{Z}n$ form a subgroup whose inverse image in $\mathbb{Z}$ is $\mathbb{Z}d$. For instance, if $d = 4$ and $n = 6$, then the multiples of 4 in $\mathbb{Z}/\mathbb{Z}6$ are $4(4) = 16 \equiv 2 \mod 6$.

13 Product Groups

Now, we talk about product groups.

13.1 Definition of a Product Group

Definition 13.1: Product Group

Let $(G, *)$ and $(G', \cdot)$ be two groups. The product set $G \times G'$, the set of pairs of elements (a, a') with $a \in G$ and $a' \in G'$, can be made into a group by component-wise multiplication; that is, multiplication of pairs is defined by the rule:

$$(a, a') \cdot (b, b') = (a * b, a' \cdot b')$$

This is known as the **product group**.

The proof that this is actually a group is as follows:

Proof. Let $(G, *)$ and $(G', \cdot)$ be two groups. We note that $(\mathrm{id}, \mathrm{id}')$ is the identity (where $\mathrm{id} \in G$ and $\mathrm{id}' \in G'$ are the corresponding identity elements), the inverse of (a, a') is $(a, a')^{-1} = (a^{-1}, (a')^{-1})$, and associativity implicitly applies. Therefore, the product group is a group. □

13.2 Properties of Product Groups

Now, we focus on some properties of product groups.

13.2.1 Prime Order and Isomorphism

Proposition. *Let r and s be relatively prime integers; that is, $\gcd(r, s) = 1$. A cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.*

13.2.2 Product Groups and Isomorphism

Proposition. *Let H and K be subgroups of a group G and let $f : H \times K \mapsto G$ be the multiplication map, defined by $f(h, k) = hk$. Its image is the set $HK = \{hk \mid h \in H, k \in K\}$.*

(a) f is injective if and only if $H \cap K = \{\mathrm{id}\}$ (the identity).

(b) f is a homomorphism from the product group $H \times K$ to G if and only if the elements of K commute with the elements of H: $hk = kh$.

(c) If H is a normal subgroup of G, then HK is a subgroup of G.

(d) f is an isomorphism from the product group $H \times K$ to G if and only if $H \cap K = \{1\}$, $HK = G$, and also H and K are both normal subgroups of G.

13.2.3 Order

- The order of a direct product $G_1 \times G_2 \times \cdots \times G_n$ is:

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$$

- The order of an element (g, h) is:

$$|(g, h)| = \mathrm{lcm}(|g|, |h|)$$

  Or, more verbosely, the order of (g, h) is the least common multiple of the orders of g and h.

14 Symmetries and Isometries

One major application of groups is the idea of symmetries. In fact, groups were invented to analyze symmetries of certain algebraic structures. In this section and the following sections, we will talk about symmetries, isometries, and more.

14.1 Types of Symmetries

Let's begin with a brief introduction on the types of symmetries.

14.1.1 Bilateral Symmetry

Bilaterial symmetry is the property of being divisible into symmetrical halves on either side of a unique plane. For example, consider the following figures:

14.1.2 Rotational Symmetry

Rotational symmetry is essentially the property an object has when it looks the same after some rotation by a partial turn.

14.1.3 Translational Symmetry

Translational symmetry is the property an object has when a particular translation does not change the object.

Figures like these are supposed to extend indefinitely in both directions.

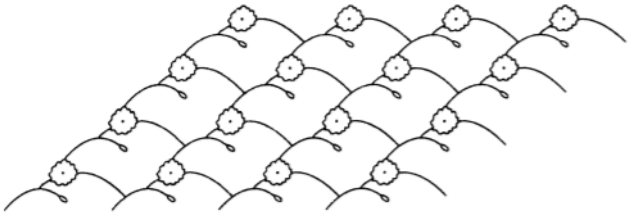
14.1.4 Glide Symmetry

Glide symmetry is the operation that usually involves reflection in a plane, followed by a translation parallel with that plane.

Figures like these are supposed to extend indefinitely in both directions.

14.1.5 Combining Symmetries

Of course, we can combine multiple symmetries. For instance, the following wallpaper pattern may have two independent translational symmetries:



The star from the first few images has bilaterial as well as rotational symmetry. The figure below has both translational and rotational symmetries combined:

14.2 Isometries

Here, we say that a rigid motion of the plane is called an **isometry**. In particular, these are:

- Translations.
- Rotations.
- Reflections.
- Glide Reflections.

We note that all of these rigid motions preserve the overall figure. Of course, there is a more precise definition.

Definition 14.1: Isometry

An **isometry** of n-dimensional space $\mathbb{R}^n$ is a distance-preserving map f from $\mathbb{R}^n$ to itself, a map such that for all $u, v \in \mathbb{R}^n$:

$$|f(u) - f(v)| = |u - v|$$

An isometry will map a figure to a congruent figure.

14.2.1 Example: Orthogonal Linear Operations

An orthogonal operation φ is linear, which means that $\varphi(u) - \varphi(v) = \varphi(u - v)$ so that $|varphi(u) - \varphi(v)| = |\varphi(u-v)|$. Additionally, because φ is orthogonal, it preserves dot products and lengths. So, $|\varphi(u-v)| = |u-v|$.

14.2.2 Example: Translation

The *translation* t_a by a vector a, the map defined by $t_a(x) = x + a$, is an isometry.

14.2.3 Example: Compositions

The composition of isometries is, of course, an isometry.

14.3 Properties of Isometries

Now, we'll talk about some properties of isometries.

Theorem 14.1

The following conditions on a map $\varphi : \mathbb{R}^n \mapsto \mathbb{R}^n$ are equivalent:

- φ is an isometry that fixes the origin: $\varphi(0) = 0$.
- φ preserves the dot product: for all u and v, $\varphi(v) \cdot \varphi(w) = v \cdot w$.
- φ is an orthogonal linear operator.

Lemma 14.1

Let x and y be points of $\mathbb{R}^n$. If the three dot products $(x \cdot x)$, $(x \cdot y)$, and $(y \cdot y)$ are equal, then $x = y$.

Corollary 14.1

Every isometry f of $\mathbb{R}^n$ is the composition of an orthogonal linear operator and a translation. More precisely, if f is an isometry and if $f(0) = a$, then $f = t_a\varphi$ where t_a is a translation and φ is an orthogonal linear operator. This expression for f is unique.

Remark: To work with the expressions $t_a\varphi$ for isometries, we need to determine the product (i.e. compositions) of two such expressions. Some rules to consider:

- $t_a t_b = t_{a+b}$.
- $\varphi t_a = t_{a'}\varphi$ where $a' = \varphi(a)$.

The last relation can be verified like so:

$$\varphi t_a(x) = \varphi(x + a) = \varphi(x) + \varphi(a) = \varphi(x) + a' = t_{a'}\varphi(x)$$

Corollary 14.2

The set of all isometries of $\mathbb{R}^n$ forms a group that we denoted by M_n, with composition of functions as its law of composition.

Proof. The composition of isometries is an isometry, and the inverse of an isometry is an isometry because orthogonal vectors and translations are invertible. Additionally, if $f = t_a\varphi$, then $f^{-1} = \varphi^{-1}t_a^{-1} = \varphi^{-1}t_{-a}$, which is a composition of isometries. □

14.3.1 Homomorphism of the Group of Isometries

Consider the map $\pi : M_n \mapsto O_n$, defined by dropping the translation part of an isometry f. We can write f in the form $f = t_a\varphi$ and define:

$$\pi(f) = \varphi$$

Here, O_n is the group of isometries preserving the origin. More specifically, it is the group of distance-preserving transformations of an Euclidean space of dimension n that preserves a *fixed point*, where the group operation is (like with M_n) composing transformations/isometries.

Proposition. *The map π is a surjective homomorphism. Its kernal is the set $T = \{t_v\}$ of translations, which is a normal subgroup of M_n.*

Corollary 14.3

The homomorphism $\pi : M_n \mapsto O_n$ does not change when the origin is shifted by a translation.

14.3.2 Orientation

The determinant of an orthogonal operator φ on $\mathbb{R}^n$ is ± 1. The operator is said to be:

- **Orientation-preserving** if the determinant is 1.
- **Orientation-reversing** if the determinant is -1.

Similarly, we note that an orientation-preserving isometry f is one such that, when written in the form $f = t_a\varphi$, the φ operator is orientation-preserving. The same can be applied for orientation-reversing. It should be noted that:

$$\sigma : M_n \mapsto \{\pm 1\}$$

That sends an orientation-preserving isometry to 1 and an orientation-reversing isometry to -1 is a group homomorphism.

14.4 Isometries of the Plane

First, we dneote the group of isometries of the plane by M. We choose a coordinate system and use it to identify the plane with the space $\mathbb{R}^2$. Then, we choose as generators the *translations*, the *rotations* about the origin, and the *reflection* about the e_1-axis (an axis). We denote the rotation through the angle θ by ρ_θ, and the reflection about the e_1-axis by r.

Essentially, to summarize, we have the following operations:

1. *Translation* t_a by a vector a.
$$t_a(x) = x + a = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$$
2. *Rotation* ρ_θ by an angle θ about the origin.
$$\rho_\theta(x) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$
3. *Reflection* r about the e_1-axis.
$$r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Although we didn't include rotation about a point (other than the origin) or reflections about other lines or glides, every element of M is a product of these isometries.

Theorem 14.2

Let $m \in M$ be an isometry of the plane. Then, for a uniquely determined vector v and an angle θ that is possibly zero:

$$m = t_v\rho_\theta$$
$$m = t_v\rho_\theta r$$

Remark: An isometry of the form $t_v\rho_\theta$ preserves orientation while $t_v\rho_\theta r$ reverses orientation.

Proof. We know that any isometry m is written uniquely in the form $m = t_v\varphi$ where φ is an orthogonal operator. In $\mathbb{R}^2$, those orthogonal linear operators are the rotations ρ_θ about the origin and the reflection about lines through the origin. The reflections have the form $\rho_\theta r$. □

Computation in M can be done using the symbols t_v, ρ_θ, and r, using the following rules for composing them:

- $\rho_\theta t_v = t_{v'}\rho_\theta$ where $v' = \rho_\theta(v)$.
- $rt_v = t_{v'}r$ where $v' = r(v)$.
- $r\rho_\theta = \rho_{-\theta}r$.
- $t_v t_w = t_{v+w}$.
- $\rho_{\theta_1}\rho_{\theta_2} = \rho_{\theta_1+\theta_2}$.
- $rr = 1$.

Theorem 14.3

Every isometry of the plane has one of the following forms:

(a) Orientation-preserving isometries.

- Translation: a map t_v that sends $p \rightsquigarrow p + v$.
- Rotation: rotation of the plane through a nonzero angle θ about some point.

(b) Orientation-reversing isometries:

- Reflection: a bilaterial symmetry about a line ℓ.
- Glide Reflection (or *glide* for short): reflection about a line ℓ, followed by a translation by a nonzero vector parallel to ℓ.

14.5 Finite Group of Orthogonal Operators on the Plane

Theorem 14.4

Let G be a finite subgroup of the orthogonal group O_2. There is an integer n such that G is one of the following groups:

- C_n: the *cyclic group* of order n generated by the rotation ρ_θ where $\theta = 2\pi/n$.
- D_n: the *dihedral group* of order $2n$ generated by two elements: the rotation ρ_θ, where $\theta = 2\pi/n$, and a reflection r about a line ℓ through the origin.

Remark: Recall that O_n is the group of isometries that preserve a fixed point (in our case, most of the time, the origin). So, it makes sense to drop the translation part of the isometry.

14.5.1 Dihedral Groups: An Introduction

As mentioned, the dihedral group is comprised of rotations ρ_θ and a reflection r'. Let us define $x = \rho_\theta$ and $y = r$.

Proposition. *The dihedral group D_n has order $2n$. It is generated by two elements x and y that satisfy the relations:*

$$x^n = \mathrm{id} \qquad y^2 = \mathrm{id} \qquad yx = x^{-1}y$$

The elements of D_n are:

$$\{\text{id}, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$$

We can write more relations. In particular:

$$xyxy = \text{id} \qquad yx = x^{n-1}y \qquad xy = yx^{-1}$$

Remarks:

- Rotations (x) will always have order n.
- Reflections (y or $x^a y$ for some a) will always have order 2.

Corollary 14.4

The dihedral group D_3 and the symmetric group S_3 are isomorphic.

Proof. Since these groups are sufficiently small enough as both have order 6, we can count the orders of each element. In particular, for D_3:

Order	Elements	Count
1	id	1
2	xy, y, x^2y	3
3	x, x^2	2

And for S_3:

Order	Elements	Count
1	id	1
2	(12), (13), (23)	3
3	(123), (132)	2

Since both groups have the same number of elements with the same number of orders, they are isomorphic to each other. □

Remarks:

- For $n > 3$, S_n and D_n are no longer isomorphic since D_n has order $n!$ while S_n has order $n!$.
- When $n \geq 3$, the elements of the dihedral group D_n are orthogonal operators that carry a regular n-sided polygon $\triangle$ to itself: the group of symmetries of $\triangle$.
- D_1 and D_2 are too small to be symmetry groups of an n-gon in the usual sense.
  - In particular, we can think of D_1 as the group $\{\text{id}, r\}$ of two elements, or a cyclic group.
  - D_2 contains the four elements $\{\text{id}, \rho, r, \rho r\}$ where ρ is the rotation with angle π and ρr is the reflection about the vertical axis, and is isomorphic to the Klein four group.

14.5.2 Discrete Subgroups

Definition 14.2: Discrete Subgroup

A subgroup Γ of the additive group $(\mathbb{R}, +)$ is called **discrete** if there is a (small) positive real number ϵ such that every nonzero element c of Γ satisfies the property $|c| \geq \epsilon$.

14.5.3 Fixed Point Theorem

Theorem 14.5: Fixed Point Theorem

Let G be a finite group of isometries of the plane. There is a point in the plane that is fixed by every element of G, a point p such that $g(p) = p$ for all $g \in G$.

14.6 Discrete Groups of Isometries

Definition 14.3: Discrete Group

A group G of isometries of the plane P is **discrete** if it does not contain arbitrarily small translations or rotations. More precisely, G is discrete if there is a positive real number ϵ so that:

(i) If an element of G is the translation by a nonzero vector a, then the length of a is at least ϵ: $|a| \geq \epsilon$.

(ii) If an element of G is the rotation through a nonzero angle ϵ about some point of the plane, then the absolute value of θ is at least ϵ: $|\theta| \geq \epsilon$.

Remark: Since the translation vectors and the rotation angles form different sets, it might seem more appropriate to have separate lower bounds for them. However, in this definition, we do not care about the best bounds for the vectors and the angles, so we choose ϵ small enough to take care of both at the same time.

There are three main tools for analyzing a discrete group G:

- The translation group L, a subgroup of the group V of translation vectors.
- The point group $\overline{G}$, a subgroup of the orthogonal group O_2.
- An operation of $\overline{G}$ on L.

14.6.1 Translation Group

The translation group L of G is the set of vectors v such that the translation t_v is in G:

$$L = \{v \in G \mid t_v \in G\}$$

Since $t_v t_w = t_{v+w}$ and $t_v^{-1} = t_{-v}$, it follows that L is a subgroup is the additive group V^+ of all translation vectors. The bound ϵ on translations in G bounds the lengths of the vectors in L.

15 Group Action (Operations)

We now focus on the aspect of groups as the symmetries of sets, of which we use group actions to formalize.

15.1 Definition of a Group Action

Definition 15.1: Group Action

If $(G, \cdot)$ is a group with identity element id and X is a set, then a left **group action** m of G on X is a function:

$$m : G \times X \mapsto X \qquad (g, x) \mapsto g * x$$

That satisfies the following two axioms:

- Identity: For all $x \in X$,
$$m(\text{id}, x) = x$$
- Associativity: For $g_1, g_2 \in G$ and $x \in X$,
$$m(g_1, \alpha(g_2, x)) = m(g_1 \cdot g_2, x)$$

When it's clear that we're performing a group action, we can shorten the axioms as follows:

- Identity: For all $x \in X$,
$$\text{id} * x = x$$
- Associativity: For all $g_1, g_2 \in G$ and $x \in X$,
$$g_1 * (g_2 * x) = (g_1 \cdot g_2) * x$$

In this sense, we say that G acts on X with m and write $G \curvearrowright X$.

15.1.1 Example: Symmetric Group

Take $G = S_n$ and $X = \{1, 2, \ldots, n\}$. Then, for some $\sigma \in S_n$ and $i \in X$:

$$\sigma * i = \sigma(i)$$

Here, we apply σ to x, or we say that σ acts on x.

Proof. Here, we show that this a group action.

- Identity:
$$\text{id} * i = \text{id}(i) = i$$
- Associativity:
$$\begin{aligned} \sigma_1 * (\sigma_2 * i) &= \sigma_1 * \sigma_2(i) \\ &= \sigma_1(\sigma_2(i)) \\ &= (\sigma_1\sigma_2)(i) \\ &= \sigma_1\sigma_2 * i \end{aligned}$$

So, we are done. □

15.1.2 Example: Group on Itself via Multiplication

Suppose $(G, \cdot)$ is a group. Then, G acts on G by left multiplication. Take $g \in G$ and $x \in G$. Then:

$$g * x = g \cdot x$$

15.1.3 Example: Group on Itself via Conjugation

Suppose $(G, \cdot)$ is a group. Then, G acts on G by conjugation. Take $g \in G$ and $x \in G$. Then:

$$g * x = g \cdot x \cdot g^{-1}$$

Proof. Here, we show that this is a group action.

- Identity:
$$\mathrm{id} * x = \mathrm{id} \cdot x \cdot \mathrm{id}^{-1} = x$$
- Associativity:
$$\begin{aligned} g_1 * (g_2 * x) &= g_1 * (g_2 \cdot x \cdot g_2^{-1}) \\ &= g_1 \cdot (g_2 \cdot x \cdot g_2^{-1}) \cdot g_1^{-1} \\ &= (g_1 \cdot g_2) \cdot x \cdot (g_2^{-1} \cdot g_1^{-1}) \\ &= (g_1 \cdot g_2) \cdot x \cdot (g_1 \cdot g_2)^{-1} \\ &= (g_1 \cdot g_2) * x \end{aligned}$$

So, we are done. □

15.2 Orbit

Given an operation of a group G on a set X, an element $x \in X$ will be sent to various other elements by the group action. We collect together these elements, obtaining a subset called the orbit.

Definition 15.2: Orbit

Suppose G acts on X. Then, the **orbit** of $x \in X$ is defined by:

$$O_x = \{x' \in X \mid x' = g * x \text{ for some } g \in G\} = \{g * x \mid g \in G\}$$

The orbits for a group action are equivalence classes for the equivalence relation:

$$x \sim y \text{ if } y = g * x \text{ for some } g \in G$$

Since they are equivalence classes, the orbits partition the set X. If X consists of just one orbit, then the action of G is called **transitive**; this means that every element of X is carried to every other one by some element of the group.

15.2.1 Example: Symmetric Group

Suppose we're asked to describe the orbits of the group operation of S_n on $\{1, 2, \ldots, n\}$ by:

$$\sigma * i = \sigma(i)$$

Proof. Consider the orbits of the group operation S_n on $\{1, 2, \ldots, n\}$ by $\sigma * i = \sigma(i)$. Then, for $\sigma \in S_n$, we have:

$$O_i = \{\sigma(i) \mid \sigma \in S_n\} = \{1, 2, \ldots, n\}$$

In this case, we consider the action of S_n to be transitive. Consider the following permutation:

$$\sigma = (i, k) \in S_n$$

If $i \in \{1, 2, \ldots, n\}$ is our input and k is the number that we're trying to find, then we note that i maps to k so that there is always a way to get some $k \in \{1, 2, \ldots, n\}$. □

As an example, suppose we have the group S_4 with the set $S = \{1, 2, 3, 4\}$. Then, you are able to get every element in S like so:

- $\sigma = (2, 4) \in S_4$. Then, $\sigma(2) = 4$. In other words, 2 maps to 4.
- $\sigma = (2, 3) \in S_4$. Then, $\sigma(2) = 3$. In other words, 2 maps to 3.
- $\sigma = (1) \in S_4$. Then, $\sigma(2) = 2$. In other words, 2 maps to 2.
- $\sigma = (2, 1) \in S_4$. Then, $\sigma(2) = 1$. In other words, 2 maps to 1.

15.2.2 Example: Symmetric Group, Tuple Pair

Suppose we're asked to describe the orbits of the group operation of S_n on $\{1, 2, \ldots, n\}$ by:

$$\sigma * (i_1, i_2) = (\sigma(i_1), \sigma(i_2))$$

Proof. We claim that the orbits of the group operation mentioned above are:

$$O_{(a,b)} = \text{All tuples such that both elements are unique, i.e. not the same.}$$

$$O_{(a,a)} = \text{All tuples such that both elements are the same.}$$

To show that this is the case, we can work with O_a and O_b individually. For some $a \in \{1, 2, \ldots, n\}$, we note that $O_a = \{1, 2, \ldots, n\}$ by the same logic we used in the previous example. We can do the same with b. If $a \neq b$, then it follows that $O_{(a,b)}$ will generate all unique possibilities of (c, d) such that $c, d \in \{1, 2, \ldots, n\}$ where $c \neq d$. But, suppose $a = b$. Then, the resulting orbit will be all tuples where the first and second elements are the same. Taking the union of both orbits, we have:

$$O_{(a,b)} \cup O_{(a,a)} = \{1, 2, \ldots, n\}^2$$

As expected. □

15.2.3 Example: Conjugation

Consider again the example of conjugation. In particular, if G acts on G by conjugation, then the orbit is defined as:

$$\begin{aligned} O_x &= \{g * x \mid g \in G\} \\ &= \{g \cdot x \cdot g^{-1} \mid g \in G\} \\ &= C_x \end{aligned}$$

This is the set of all conjugates of x, and the set of all conjugates of x is called the conjugacy class of x.

15.3 Stabilizer

Definition 15.3: Stabilizer

The **stabilizer** of an element $x \in X$ is the set of group elements that leave x fixed. It is a *subgroup* of G that we denoted by G_x:

$$G_x = \{g \in G \mid g * s = s\}$$

Proposition. *Let X be a set on which a group G acts on. Let $x \in X$ and let H be the stabilizer of x. Then:*

(a) If a and b are elements of G, then $a * s = b * s$ if and only if $a^{-1} \cdot b \in H$, and this is true if and only if b is in the coset aH.

(b) Suppose that $a * s = s'$. The stabilizer H' of s' is a conjugate subgroup:

$$H' = aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$$

15.3.1 Example: Permutations

Consider the permutation group $S = \{(1), (12), (34), (12)(34)\}$ and the set $\{1, 2, 3, 4\}$. Then:

$$G_1 = \{g \in G \mid g(1) = 1\} = \{(1), (34)\}$$

$$G_2 = \{g \in G \mid g(2) = 2\} = \{(1), (34)\}$$

$$G_3 = \{g \in G \mid g(3) = 3\} = \{(1), (12)\}$$

$$G_4 = \{g \in G \mid g(4) = 4\} = \{(1), (12)\}$$

Proposition. *Let X be a set on which a group G operates, and let $x \in X$ and let H be a stabilizer of x.*

(a) If $a, b \in G$, then $a * x = b * x$ if and only if $a^{-1}b \in H$, and this is true if and only if $b \in aH$.

(b) Suppose that $a * x = x'$. The stabilizer H' of x' is a conjugate subgroup*:*

$$H' = aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$$

15.4 Operation on Cosets

Let H be a subgroup of G. The left cosets aH partition G. We often denote the set of left cosets of H in G by G/H, copying this from the notation used for quotient groups when the subgroup is normal, and we used the bracket notation $[C]$ or $\overline{a}$ (a being a representative element for a coset) for a coset C, when it is considered as an element of the set G/H. **Note** that the set of cosets G/H is not a group unless H is a normal subgroup. However, the group G operates on G/H in a natural way.

15.4.1 The Operation

If $g \in G$ and C is a coset, then $g[C]$ is defined to be the coset $[gC]$, where $gC = \{gc \mid c \in C\}$. Thus, if $[C] = [aH]$, then $g[C] = [gaH]$.

Proposition. *Let H be a subgroup of a group G.*

- *The operation of G on the set G/H of cosets is transitive.*
- *The stabilizer of the coset $[H]$ is the subgroup H.*

15.4.2 Example: Symmetric Group

Let $G = S_3$. Note that $x = (123)$ and $y = (12)$. Then, let $H = \{1, y\}$. Its left cosets are:

$$C_1 = H = \{1, y\}$$

$$C_2 = xH = \{x, xy\}$$

$$C_3 = x^2H = \{x^2, x^2y\}$$

Here, G operates on the set of cosets $G/H = \{[C_1], [C_2], [C_3]\}$. The elements x and y operate in the same way as on the set $\{1, 2, 3\}$:

$$m_x \longleftrightarrow (123)$$

$$m_y \longleftrightarrow (23)$$

For example, $yC_2 = \{yx, yxy\} = \{x^2y, x^2\} = C_3$.

15.4.3 Example: Symmetric Group on Power Set

If S_3 operates on $[3] = \{1, 2, 3\}$, then S_3 operates on $\mathcal{P}([3])$. For instance, take $\sigma = (123) \in S_3$. Then:

$$\sigma * \emptyset = \emptyset$$

$$\sigma * \{1\} = \{2\}$$

$$\sigma * \{1, 3\} = \{2, 1\}$$

$$\sigma * \{1, 2, 3\} = \{2, 3, 1\} = \{1, 2, 3\}$$

15.5 The Counting Formula

Let H be a subgroup of a finite group G. All cosets of H in G have the same number of elements, and with the notation G/H for the set of cosets, the order $|G/H|$ is what is called the index $[G : H]$ of H in G. The counting formula from a few sections ago, then, stated:

$$|G| = |H| \cdot |G/H|$$

A similar formula exists for orbits of any group operation.

Proposition. *Let X be a finite set on which a group X operates on, and let G_x and O_x be the stabilizer and orbit of an element $x \in X$, respectively. Then:*

$$|G| = |G_s| \cdot |O_s|$$

(Order of G) = (Order of Stabilizer) · (Order of Orbit)

The order of the orbit is equal to the index of the stabilizer.

$$|O_s| = [G : G_s]$$

This divides the order of the group. There is one such formula for every $x \in X$.

Another formula uses the partition of the set X into orbits to count its elements. This formula is:

$$|X| = |O_1| + |O_2| + \cdots + |O_n|$$

Where $1, 2, \ldots, n$ are for labeling purposes.

15.6 Operations on Subsets

Suppose that G operates on a set X. If U is a subset of X of order r, then:

$$gU = \{gu \mid u \in U\}$$

Is another subset of order r. This allows us to define an operation of G on the set of subsets of order r of S.

15.7 Finite Subgroups of the Rotation Group

We will now apply the Counting Formula to classify the finite subgroups of SO_3, the group of rotations of $\mathbb{R}^3$.

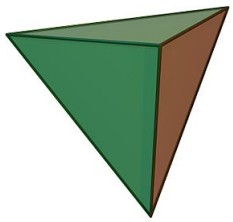
Theorem 15.1

A finite subgroup of SO_3 (the group of all rotations about the origin of $\mathbb{R}^3$ under the operation of composition) is one of the following groups:

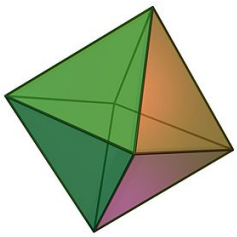
- C_k: The cyclic group of rotations by multiples of $2\pi/k$ about a line, with k arbitrary.
- D_k: The dihedral group of symmetries of a regular k-gon, with k arbitrary.
- T: The tetrahedral group of 12 rotational symmetries of a tetrahedron.
- O: The octahedral group of 24 rotational symmetries of a cube or an octahedron.
- I: The icosahedral group of 60 rotational symmetries of a dodecahedron or an icosahedron.

Remarks:

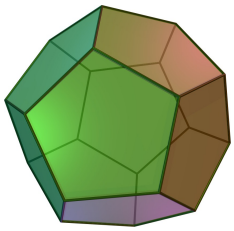
- This is what a tetrahedron (i.e. triangular pyramid) looks like:



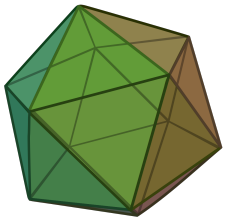
- This is what an octahedron looks like:



- This is what an dodecahedron looks like:



- This is what an icosahedron looks like:



Definition 15.4: Pole

For $g \in SO_3$, call $p \in \mathbb{S}^2$ (the unit sphere) a **pole** of g if $g * p = p$.

Remarks:

- If $g \neq \text{id}$, then g has two distinct poles.
- If $G \subseteq SO_3$ is a subgroup, we say p is a pole of G if p is a pole of some $g \in G - \{\text{id}\}$.

Lemma 15.1

The set P of poles of G is a union of G-orbits.

Remark: This is an abstract way of saying that vertices are sent to vertices, center of faces are sent to center of faces, and center of edges are sent to center of edges.

Lemma 15.2

Let $|G| = N$ and $|G_p| = r_p$. Then:

$$\sum_{i=1}^{k} \left(1 - \frac{1}{r_i}\right) = 2 - \frac{2}{N}$$

Where $P = O_1 \cup O_2 \cup \cdots \cup O_k$ is a union of k G-orbits and $r_i = r_p$ for some $p \in O_i$.

16 More Applications of Group Theory

Here, we will talk about several important topics. A lot of these will involve conjugation (once again).

16.1 Cayley's Theorem

Theorem 16.1: Cayley's Theorem

Every finite group is isomorphic to a subgroup of a permutation group. A group of order n is isomorphic to a subgroup of the symmetric group S_n.

16.2 The Class Equation

Definition 16.1: Centralizer

The stabilizer of an element $x \in G$ for the operation of conjugation is called the **centralizer** of x. It is often denoted by $Z(x)$:

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

The centralizer of x is the set of elements that commute with x.

Remarks:

- The centralizer of an element $g \in G$ is a *subgroup* of G.
- This should not be confused with the center of a group $Z(G)$, which is the set of elements that commute with every element of the group:

$$Z(G) = \{z \in G \mid zy = yz \text{ for all } y \in G\}$$

Definition 16.2: Conjugacy Class

The orbit for x for conjugation is called the **conjugacy class** of x, and is often denoted by $C(x)$. It consists of all of the conjugates $g \cdot x \cdot g^{-1}$:

$$C(x) = \{gxg^{-1} \mid g \in G\}$$

The counting formula tells us that:

$$|G| = |Z(x)| \cdot |C(x)|$$
$$|G| = |\text{Centralizer}| \cdot |\text{Conjugacy Class}|$$

Proposition. *(a) The centralizer $Z(x)$ of an element $x \in G$ contains x, and it contains the center Z.*

(b) An element $x \in G$ is in the center if and only if its centralizer $Z(x)$ is the whole group G, and this happens if and only if the conjugacy class $C(x)$ consists of the element x alone.

Since the conjugacy classes are orbits for a group operation, they partition the group. This fact gives us the **class equation** of a finite group:

$$|G| = \sum_{\substack{\text{Conjugacy} \\ \text{Classes C}}} |C|$$

If we number the conjugacy classes, writing them as $C_1, C_2, \ldots, C_k$, then the class equation reads:

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

A few facts to remember:

- The conjugacy class of the identity element id consists of that element alone, so it seems natural to list that class first. Thus, $|C_1| = 1¿$
- If there are any other occurrences of 1 on the right side of the class equation, then those correspond to the elements of the center Z of G.
- Each term on the right side divides the left side since it is the order of an orbit. In other words, the numbers on the right side of the class equation divide the order of the group.
- At least one of the numbers on the right side must be equal to 1 (the identity conjugacy class).

16.2.1 Example: Class Equation of Symmetric Group of 4 Elements

Find the class equation of the symmetric group of 4 elements, or S_4.

Proof. We note that cycle type determines conjugacy classes. We know that S_4 has the following cycle structures (i.e. conjugacy classes):

Cycle Structure	Size of Conjugacy Class
(a)(b)(c)(d)	1
(ab)(c)(d)	6
(ab)(cd)	3
(abc)(d)	8
(abcd)	6

So, the class equation for S_4 is:

$$|S_4| = 1 + 6 + 3 + 8 + 6$$

And we are done. □

16.2.2 Example: Class Equation of Dihedral Group of 5 Elements

Find the class equation for the dihedral group of 5 elements, or D_5.

Proof. Recall that $D_5 = \{\text{id}, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\}$, where x is a rotation and y is a reflection.

- First, the identity element will always be in its own conjugacy class. So, $C(\text{id}) = \{\text{id}\}$ and $|C(\text{id})| = 1$.
- Let's now consider $C(x)$. Iterating over every element in D_5, we find that all rotations will give us back x. Let's consider different variations of reflections.

$$y \cdot x \cdot y^{-1} = yyx = x$$

$$xy \cdot x \cdot (xy)^{-1} = xy \cdot x \cdot y^{-1}x^{-1} = xy \cdot x \cdot yx^{-1} = xyyx^{-1}x^{-1} = xx^{-2} = x^{-1} = x^4$$

Omitting the rest of the computations, we find that:

$$C(x) = \{x, x^4\} \qquad |C(x)| = 2$$

- We now consider $C(x^2)$. Again, iterating over every element in D_5, we find that all rotations will give us back x^2. Let's consider different variations of reflections.

$$xy \cdot x^2 \cdot (xy)^{-1} = xy \cdot x^2 \cdot y^{-1}x^{-1} = xy \cdot x^2 \cdot yx^{-1} = xyyx^{-2}x^{-1} = xx^{-2}x^{-1} = x^{-2} = x^3$$

Omitting the rest of the computations, we find that:

$$C(x^2) = \{x^2, x^3\} \qquad |C(x^2)| = 2$$

At this point, we've found all conjugacy classes for rotations only. This is because:

$$C(x) = C(x^4) \qquad C(x^2) = C(x^3)$$

So, we now consider different variations of reflections.

- Let's consider $C(y)$. Iterating over every element in D_5 gives us:

$$x \cdot y \cdot x^{-1} = xxy = x^2y$$

$$x^2 \cdot y \cdot x^{-2} = x^2x^2y = x^4y$$

$$x^3 \cdot y \cdot x^{-3} = x^3x^3y = x^6y = xy$$

$$x^4 \cdot y \cdot x^{-4} = x^4x^4y = x^8y = x^3y$$

  We no longer need to check the rest of the reflections since, if we did, we would end up getting the same result from the computations we just did. Therefore:

$$C(y) = \{y, xy, x^2y, x^3y, x^4y\} \qquad |C(y)| = 5$$

We have now found which conjugacy classes each element in D_5 goes to. It follows that the class equation for D_5 is:

$$|D_5| = |C(\text{id})| + |C(x)| + |C(x^2)| + |C(y)| = 1 + 2 + 2 + 5$$

And so we are done. □

16.2.3 Example: Valid and Invalid Class Equations

Rule out as many class equations for a group of order 10 as possible:

$$1+1+1+2+5 \qquad 1+2+2+5 \qquad 1+2+3+4 \qquad 1+1+2+2+2+2$$

Proof. We begin with $1+1+1+2+5$. We note that there are 3 conjugacy classes with 1 element each; these are the center (note that the identity is in the center), so $|Z| = 3$. Since the center of a group is a subgroup, we note that this means that the center has order 3. However, by Lagrange's Theorem, 3 does not divide 10 so the center of this group cannot be 3.

We now turn our attention to $1 + 2 + 2 + 5$. We just proved that this was actually the conjugacy class for D_5, so nothing needs to be done here.

Now, let's look at $1 + 2 + 3 + 4$. We note that there is a conjugacy class of 3 elements; however, rememeber that all orders of each conjugacy class must divide the order of the group. As 3 does not divide 10, we can rule this out.

Finally, we look at $1 + 1 + 2 + 2 + 2 + 2$. Note that there are 2 conjugacy classes with 1 element each; these are the center of the group, so $|Z| = 2$. Recall that Z is a normal subgroup, so G/Z has order $|G|/|Z| = 5$, which is cyclic as 5 is prime. If G/Z is cyclic, then G must be abelian. But, abelian groups can only have the class equation $1 + 1 + \cdots + 1 + 1$ since every element commutes with each other. So, this cannot be the class equation. □