Math 100A Notes

Abstract Algebra

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 $S \times S \to S$.

More formally, a binary operation $*$ over a set S is a function mapping $f : S \times S \to S$. 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:
$$a * b = e \qquad b * a = 1$$

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 e is a left identity if $f(e,s) = s$ for all $s \in S$. e is a right identity if $f(s,e) = s$ for all $s \in S$. Then, e 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 $f : S \times S \to S$ with a two-sided identity e, 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:

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

  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:

  $$f(s^{-1}, s) = f(s, s^{-1}) = e$$
  $$s^{-1} * s = s * s^{-1} = e$$

  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/Neutral Element: There is an element $e \in G$ such that for all $x \in G$:
$$e * x = x * e = x$$
3. Inverse: Corresponding to each $a \in G$, there is an element $a^{-1} \in G$ such that:
$$a * a^{-1} = a^{-1} * a = e$$
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 $G \times G \to G$.

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 $(G, \times)$	$h^{-1} = \frac{1}{h}$	$e = 1$
Addition $(G, +)$	$h^{-1} = -h$	$e = 0$

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 e is the identity element of $\mathbb{Z} - \{0\}$ under $\times$, then by definition:

  $$e \times x = x \times e = x$$

  Which implies that $e = 1$. 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 $a^{-1} \in \mathbb{Z} - \{0\}$:

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

  But, since we know that $e = 1$, 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 e is a unique element of $(\mathbb{Z}_{\geq 0}, +)$, then by definition, we know that:

  $$e + x = x + e = x$$

  It is obvious that $e = 0$. 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 $a^{-1} \in \mathbb{Z}_{\geq 0}$:

  $$a^{-1} + 1 = 1 + a^{-1} = e$$

  But, as $e = 0$, 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 e_1 and e_2, both of which are unique two-sided identity elements. Then, we know that $e_1 * e_2 = e_2$ since e_1 is an identity. But, since e_2 is also an identity, then $e_1 * e_2 = e1$. So, it follows that e_1 and e_2 are not unique; in other words, $e_1 = e_2$. □

2.2.2 Uniqueness of Inverses.

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

$$g_1 * h = h * g_2 = e$$

Additionally, we know that:

$$g_1 * (h * g_2) = g_1 * e = g_1$$
$$(g_1 * h) * g_2 = e * g_2 = g_2$$

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 $g_1 * h = e$ and $h * g_2 = e$. Then:

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

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:

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

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:

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

So:

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

Similarly:

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

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 $g^{-1} * g = e$. Multiplying both sides by $(g^{-1})^{-1}$ from the left, we now have:

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

Hence, $e * g = (g^{-1})^{-1}$ 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:

$$(g^n)^m = e$$

$$g^{nm} = e$$

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

$$(g^n)^m = e^m = e$$

$$g^{mn} = e$$

Here, we notice that $e * \cdots * e = e$ and $e^{-1} = e$, and so $e^m = e$. 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 $m = \text{sign}(m)r$ and $n = \text{sign}(n)s$ where $r = |m|$ and $s = |n|$, where:

$$\text{sign} : \mathbb{R} \to \{-1, 1\}$$

- 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:

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

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

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

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 $e \in H$ (where the same $e \in G$) such that for all $x \in H$:
$$e * x = x * e = x$$
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:
$$a * a^{-1} = a^{-1} * a = e$$
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 $\{e\}$ 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:
$$e = x^0 \in G$$
- 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 $H = \{e_G\}$, then it is generated by e_G and so it is cyclic. Otherwise, we can assume (without loss of generality), we can and will assume that $H \neq \{e_G\}$. 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:

$$p : S \to S$$

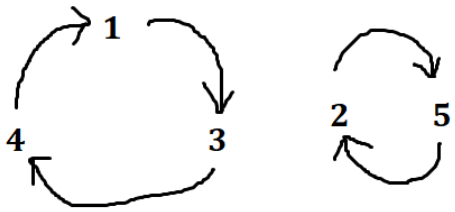
For instance, consider the following table:

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:

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

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

This mapping can be represented like so:

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

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:

$$\varphi : G \to G'$$

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:

$$\varphi : G \to G'$$

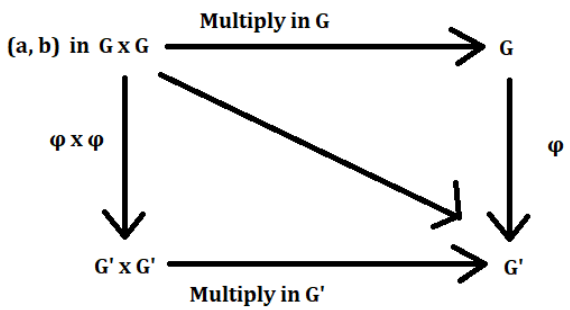
Such that for all $a, b \in G$, $\varphi(a * b) = \varphi(a) \cdot \varphi(b)$.

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:

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

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:

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

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:

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

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:

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

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:

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

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:

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

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:

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

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 $\varphi : G \to G'$ be a group homomorphism.*

(a) φ maps the identity to the identity: $\varphi(e_G) = e_{G'}$.

(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:

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

(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 e_G is the identity element of G, it follows that $e_G * e_G = e_G$. Because φ is a group homomorphism, it follows that:

$$\boxed{\varphi(e_G * e_G)} = \varphi(e_G) * \varphi(e_G)$$

Since $e_G * e_G = e_G$, it follows that $\varphi(e_G * e_G) = \varphi(e_G)$, so:

$$\varphi(e_G) * \varphi(e_G) = \boxed{\varphi(e_G)}$$

Thus:

$$\varphi(e_G) * \varphi(e_G) = \varphi(e_G) * e_{G'}$$

[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:

$$\varphi(e_G) = e_{G'}$$

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

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

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

$$\varphi(a) * \varphi(a^{-1}) = e_{G'}$$

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

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

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 $\varphi : G \to G'$ is simply the image of φ as a map of sets:

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

More simply:

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

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 $\varphi : G \to G'$ is the set of elements of G that are mapped to the identity in G':

$$\ker(\varphi) = \{a \in G \mid \varphi(a) = e_{G'}\}$$

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

6.7.1 Example: Matrices

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

$$\varphi : G \to G$$

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.

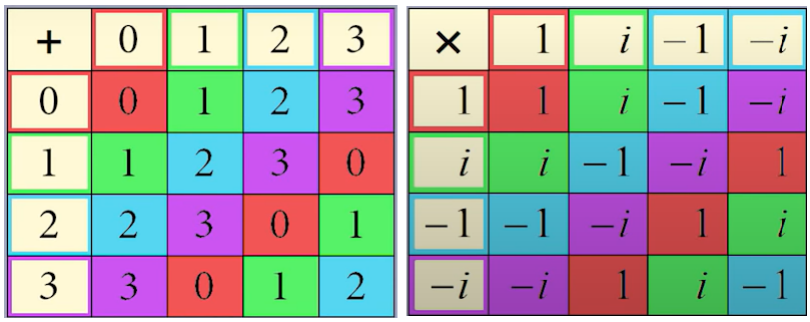
Consider the table that represents group 1:

$+$	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*:

$$\varphi : G \to G'$$

If there is a isomorphism $\varphi : G \to G'$, 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:

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

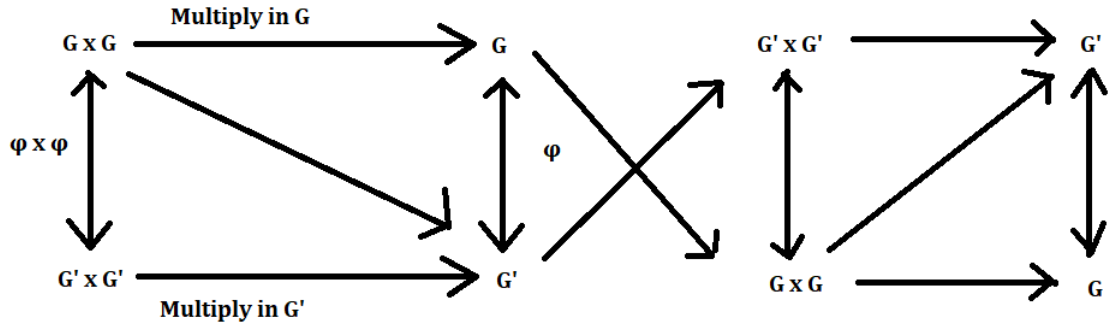
Since $\varphi : G \mapsto G'$ is surjective, there exists $a, b \in G$ such that $\varphi(a) = x$ and $\varphi(b) = y$. Then:

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

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:

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

8.1.1 Example: Relations

Suppose X and Y are two non-empty sets and $f : X \to Y$ 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. □

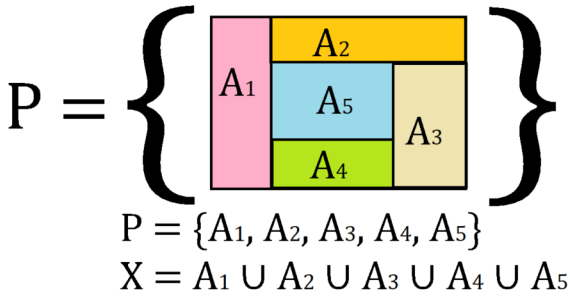
8.2 Equivalence Relation Partitions

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:

$$X \to P$$

$$x \mapsto [x]_P$$

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 $[x]_P$.

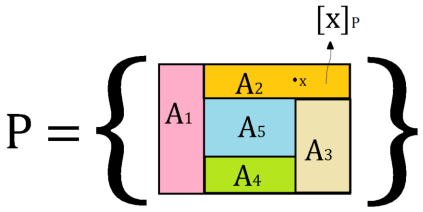
Notice that, because of the **covering** condition, x is contained in some element of P; additionally, because of the **disjointness** condition, x is in an unique element of P (i.e. it is in one of the sets which is in P). So, it follows that the function is well-defined.

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 $X \to P$. 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.

Remark: The subgroup H is a particular left coset because $H = eH$, where e 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 and Cyclic Groups

Let $G = S_3$ and $H = \langle x \rangle$ where $x = (12) \in S_3$. The left cosets are:

$$eH = H = \{(1), x\}$$

$$xH = H = \{x, x^2\} = \{x, (1)\} = H$$

Let $y = (123) \in S_3$. Then:

$$yH = \{y, yx\} = \{(123), (13)\}$$

$$yxH = \{yx, yxx\} = \{yx, y\} = yH$$

We also have:

$$y^2H = \{y^2, y^2x\} = \{(132), (23)\}$$

$$y^2xH = \{y^2x, y^2x^2\} = \{y^2x, y^2\} = y^2H$$

So, there are three left cosets.

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.

To show that this is the case, we note that:

- Every $a \in G$ is in the same left coset (because $e \in H$).

- If $a, b \in G$, then $aH = bH$ or $aH \cap bH = \emptyset$. In other words, if $aH \cap bH \neq \emptyset$, then $aH = bH$. To show this, suppose $c \in aH \cap bH$. Then:

$$c = ah_1 \qquad \text{for some } h_1 \in H$$

$$c = bh_2 \qquad \text{for some } h_2 \in H$$

By transitivity, we know that:

$$ah_1 = bh_2$$

Since H has inverses and closure, then:

$$b^{-1}ah_1 = b^{-1}bh_2$$

$$b^{-1}ah_1h_1^{-1} = h_2h_1^{-1}$$

$$b^{-1}a = \underbrace{h_2h_1^{-1} \in H}_{\text{By closure of } H}$$

Now, for any $d \in aH$:

$$d = ah_3 \qquad \text{for some } h_3 \in H$$

It follows that:

$$d = bh_2h_1^{-1}h_3 \in bH$$

Where $b^{-1}a = h_2h_1^{-1}$. Therefore:

$$aH \subseteq bH$$

And reverse by the same logic.

9.3 Lagrange's Theorem

Theorem 9.1: Lagrange's Theorem

et 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. □

Remark: We can write $\frac{|G|}{|H|}$ as $[G : H]$. This notation denotes the number of left cosets of a subgroup, and is called the **index** of H in G.

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. □

Corollary 9.3

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

Proof. Pick any $g \in G - \{1\}$. Then, g has order a divisor of p but not 1. Then, g has order p so it follows that:

$$G = \langle g \rangle$$

□

9.4 Link to Homomorphism

We can think of homomorphisms in terms of cosets like so. Let:

$$\varphi : G \to G'$$

Be a homomorphism of groups. Let $a, b \in G$ be two elements. Then, the following are equivalent:

- $\varphi(a) = \varphi(b)$
- b is in the coset aK where $K = \ker(\varphi)$.
- The partition defined by φ is the partition into left cosets.

To show that the first point and the second points are the same, we have that:

$$\begin{aligned} \varphi(a) = \varphi(b) &\iff \varphi(a^{-1})\varphi(a) = \varphi(a^{-1})\varphi(b) \\ &\iff \varphi(a^{-1}a) = \varphi(a^{-1}b) \\ &\iff \varphi(e) = \varphi(a^{-1}b) \\ &\iff e = \varphi(a^{-1}b) \qquad \iff a^{-1}b \in K \\ &\iff b \in aK \end{aligned}$$

Corollary 9.4

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

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. If we consider the symmetric group from above, evaluating all left and right cosets will give us different cosets.

9.6 Definition of Normal Subgroups

Definition 9.3: Normal Subgroup

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

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

Remarks:

- The operation $g^{-1} * h * g \in H$ is known as conjugating h by g.
- The left cosets are equal to the right cosets.

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 $\phi_g : G \to G$ can be defined by:

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

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

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

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

  Or, in other words, g commutes with a.

10.2 Center of a Group

We now talk about the *center* of a group, which is also an important topic.

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:

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

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

Consider the following proposition:

Proposition. *Z is an abelian subgroup.*

To show that this is the case, we give a proof:

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

- Identity: We know that $e \in Z$.
- 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.

10.3 Automorphisms

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

$$\phi_g : G \to G$$

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:

$$\varphi : G \to G$$

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

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

$$g \to \phi_g$$

Consider:

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

Which we can define by:

$$\phi_{g*h} = \phi_g \circ \phi_h$$

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

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

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

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

$$S_n \to \mathrm{Aut}(S_n)$$

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

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

10.4 Conjugation in Symmetric Groups

Let's suppose we have $g = (12345)$ and $a = (12)(34)$. 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.

10.5 Commutator

The commutator of a and g is given by:

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

This is e (the identity) if and only if g commutes with a.

10.6 Normal Subgroups

Recall the following definition:

Definition 10.4: Normal Subgroup

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

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

Where H in the right-side of the equality is treated as a *set*, not term-by-term.

A few examples of normal subgroups:

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

10.6.1 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:

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

10.7 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 $\varphi : G \to G'$ and if g is any element of G, then:

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

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

10.8 Cosets and Normal Groups

Finally, we consider the following proposition.

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

- *H is a normal subgroup.*
- *For all $g \in G$, $g * H * g^{-1} = H$. In particular, for all $g \in G$, $g * H * g^{-1} \subseteq H$. The same applies to g^{-1}; $g^{-1} * H * g \subseteq H \iff H \subseteq g * H * g^{-1}$.*
- *For all $g \in G$, the left coset $g * H$ is equal to the right coset $H * g$.*
- *Every left coset of H in G is a right coset. In other words:*

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

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

The **quotient group** of G by H, when it exists (it will exist if H is normal), is a group $\overline{G}$ together with a *surjective* homomorphism:

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

Where the kernal is denoted H.

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

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

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

By performing the following mapping:

$$a \to a \mod n$$

Assume H is normal. Then, we call it N instead. So, we define the set $\overline{G} = \frac{G}{N}$ as the partition of G into (left or right) cosets for H.

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:

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

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 $\overline{G}$:

$$a * N * b * N = a * b * N$$

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

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

The proof is as follows:

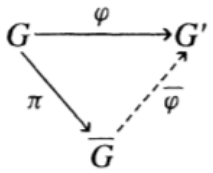
Proof. The partition defined by π and φ are the same; namely, the cosets of N. Define $\overline{\varphi}$ by saying that for $\overline{g} \in \overline{G}$, $\overline{\varphi}(\overline{g})$ is the unique element of G' such that $\pi^{-1}(\overline{g}) = \varphi^{-1}(h)$ as cosets of N.

$\overline{\varphi}$ 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 $\varphi : G \to G'$ 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 $\varphi(g_1^{-1} * g_2) = \varphi(g_1)^{-1} \cdot \varphi(g_2) = e$. So:

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

So, we are done. □

12.2 Correspondence Theorem

We now talk about the correspondence theorem.

Theorem 12.2: Correspondence Theorem

Let $\varphi : G \to G'$ 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:

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

Definition 12.1: Restriction

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

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

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

Remarks:

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

12.2.1 Example: Permutations and Sign

Let $\sigma : S_n \to \{\pm 1\}$ 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:

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

Here, we note that $\left|\operatorname{im}\left(\frac{\varphi}{H}\right)\right|$ 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 $\varphi : G \to G'$ 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 $(\mathbb{Z}, +) \to (\mathbb{Z}/\mathbb{Z}n)$, 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 $4(4) = 16 \equiv 2 \mod 6$.