Math 100A Notes

Abstract Algebra

Fall 2021

Taught by Professor Kiran Kedlaya

Table of Contents

1 Introduction to Binary Operations and Group Theory

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.

1.4 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:

Definition 1.2: 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.

Definition 1.3: 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.

1.4.1 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**.

1.4.2 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.

1.4.3 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.

1.4.4 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.)

1.5 Basic Properties of Groups

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

1.5.1 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, $e_1 = e_2$. □

1.5.2 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. □

1.5.3 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.

1.5.4 Inverse of Operation of Two Elements.

Lemma 1.1

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. □

1.5.5 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 1.2

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 $g = (g^{-1})^{-1}$. □

1.6 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 1.3

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 1.4

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. □

1.7 Subgroups

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

Definition 1.4: Subgroup

A subset H of a group G is a **subgroup** 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.

Remarks:

- 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*.

1.7.1 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 $(\mathbb{C} - \{0\}, \times)$.

1.7.2 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 $GL_n(\mathbb{R})$.

1.7.3 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:

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

- $(\{0\}, +)$. 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 $-a \in S$.

1.7.4 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:

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

We will discuss the last example right now.

1.8 More on Subgroups

Of course, we now need to discuss some theorems and applications of subgroups.

Theorem 1.1

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. □

1.9 Cyclic Groups

Definition 1.5: Cyclic Subgroup

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

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

To check that H is a commutative 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):
$$x^n = x^{-n}$$

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

$$H = \mathbb{Z}a$$

However, if $x = 0$, 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).

We now consider the following proposition.

Proposition. *Let $< x >$ 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 $x^k = 1 \in G$ (the identity element).*

(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 $< x >$, and the order of $< x >$ is n.

Remarks:

- The order of $< x >$ is the same thing as saying the cardinality of $< x >$, or the number of elements.
- An element $x \in G$ (a group) has order n if $< x >$ has order n. However, it's not correct to say that x has a cardinality.
- We can say that $x^n = 1$ and $x^r \neq 1$ for $r \in [1, \ldots, n-1]$.
- For the third point, we can demonstrate this like so:

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

  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.
- An element might have infinite order if it never cycles.

1.9.1 Example: Trivial

The identity element, 1, has order 1. It cycles back immediately.

1.9.2 Example: Symmetric Group of Size 3

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

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

Which elements of S_3 have order 6?

- (1)
- (12)

- (23)
- (13)
- (123)
- (132)

None of these elements have order 6, so S_3 is not a cyclic group.

1.9.3 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:

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

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

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

As you can see, we can never get back to the identity element.

1.9.4 Example: Matrices

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

$$x^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

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

$$x^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} = -x$$

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

$$x^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

So, x has order 6. We note that $x^6 = x^0$.

1.10 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 be the greatest common divisor of k and n. The order of x^k is equal to $\frac{n}{d}$.*

For example, consider a cyclic group with order $n = 10$ and $k = 4$. Then:

$$x^4, x^{2\cdot 4}, x^{3\cdot 4}, \ldots, x^{m\cdot 4}$$

Here:

$$4m \equiv 0 \pmod{10}$$

The smallest m possible is:

$$\frac{\operatorname{lcm}(n,k)}{k} = \frac{n}{\gcd(n,k)}$$

2 Permutations

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

Definition 2.1: Permutation

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

$$p : S \to S$$

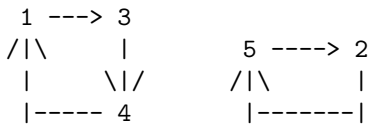
For instance, consider the following table:

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[3].

[3] 2-cycles are also known as **transpositions**.

2.1 Symmetric Groups

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

Definition 2.2: Symmetric Group

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

For instance, S_3 consists of the following permutations:

- (123)
- (132)
- (21)
- (231)
- (312)
- (321)

2.2 Inverse of a Permutation

Recall the permutation example used:

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