Algebra 1 and 2 Notes

Grant Talbert

Sem 2 2024

Abstract

owo
Notes from the text *Abstract Algebra* by Thomas W. Judson.

Contents

Chapter 1

Preliminaries

1.1 Sets and Equivalence Relations

Set Theory

Definition 1.1 (Set)**.** A set is any well-defined collection of objects; that is, it is defined in such a manner that we can tell whether x belongs to the set or not.

We denote sets by capital letters, and we refer to the objects that belong to them as their elements. We have two notations for defining sets. Sometimes we write all their elements within curly brackets:

$$X = \{x_1, x_2, \ldots, x_n\}$$

and sometimes we use set-builder notation:

$$X = \{x \mid x \text{ satisfies } \mathcal{P}\}$$

where all elements x of the set X must satisfy some property $\mathcal{P}$. For example, consider the set of even positive integers:

$$E = \{x \in \mathbb{N} \mid \frac{x}{2} \in \mathbb{N}\}$$

We write $2 \in E$ to denote set membership, and $-3 \notin E$ to denote set exclusion.
The following are shorthands for rather important sets:

- $\mathbb{N}$ is the set of all naturals.
- $\mathbb{Z}$ is the set of all integers.
- $\mathbb{Q}$ is the set of all rationals.
- $\mathbb{R}$ is the set of all reals.
- $\mathbb{C}$ is the set of all complex numbers.

We can define various relations and operations on sets.

Definition 1.2 (Subset)**.** if A and B are sets, we say that $A \subset B$, or A is a subset of B, if every element of A is also in B.

For example,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Trivially, all sets are their own subsets. We also find that two sets are equal if $A \subseteq B$ and $B \subseteq A$.

Definition 1.3 (Empty Set). The empty set, denoted $\varnothing$, is the set $\{\}$.

We can define two operations on sets to construct new sets from two sets:

Definition 1.4 (Union). The union $A \cup B$ of two sets A and B is defined as

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

In other words, all elements in either A, B, or both.

Definition 1.5 (Intersection). The intersection $A \cap B$ of two sets A and B is defined as

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

In other words, all elements in both A and B.

We can consider the union and intersection of more than just two sets with the big operators. The union is given as

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

and the intersection is

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

Definition 1.6 (Disjoint). Two sets A and B are disjoint if

$$A \cap B = \varnothing$$

Oftentimes, we will work within one fixed set U, called the *Universal Set.*

Definition 1.7 (Compliment of a Set). From the previous definition of a Universal Set, we define the compliment of a set A as

$$A' = \{x \mid x \in U \wedge x \notin A\}$$

Definition 1.8 (Set Difference). We define the difference between two sets A and B as

$$A \setminus B = A \cap B' = \{x \mid x \in A \wedge x \notin B\}$$

Proposition 1.9. Let A, B, and C be sets.

- $A \cup A = A, A \cap A = A,$ and $A \setminus A = \varnothing$
- $A \cup \varnothing = A$ and $A \cap \varnothing = \varnothing$
- $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \cup B = B \cup A$ and $A \cap B = B \cap A$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Cartesian Products and Mappings

Given sets A and B, we define the **Cartesian Product** $A \times B$ as a set of ordered pairs.

Definition 1.10 (Cartesian Product). The cartesian product of two sets $A \times B$ is given as

$$A \times B = \{(a, b) \mid a \in A \land b \in B\}$$

Proposition 1.11 (Generalization of Cartesian Product). The cartesian product generalizes to n sets:

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1 \land \cdots \land a_n \in A_n\}$$

We will often use the shorthand $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$.

Definition 1.12 (Function/Mapping). Subsets of $A \times B$ are known as **relations**. We define a **mapping** or **function** $f \subset A \times B$ from set A to B as a special type of relation where each element $a \in A$ has a unique element $b \in B$ such that $(a, b) \in f$.
Often, we write $f : A \to B$ and $f : a \mapsto b$.

If $f : A \to B$, then A is the **domain** of f, and

$$f(A) = \{f(a) \mid a \in A\} \subseteq B$$

is the **range** or **image** of f.

Definition 1.13 (Surjective). A map $f : A \to B$ is **onto** or **surjective** if

$$\forall (a \in A)(\exists (b \in B)(f(a) = b))$$

In other words, every element of the domain is mapped to an element in the image, **and** every element in the image is mapped from an element in the domain. The entirety of both sets is used.

Definition 1.14 (Injective). A map $f : A \to B$ is **one-to-one** or **injective** if

$$a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Equivalently, a function is injective if $a_1 = a_2 \implies f(a_1) = f(a_2)$.
In other words, each element of the domain is mapped to a **unique** element of the image.

Definition 1.15 (Bijective). A map is called **bijective** if it is both injective and surjective.

Definition 1.16 (Function Compositions). If we have the maps $f : A \to B$ and $g : B \to C$, we can define the **composition** of f and g from A to C as

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

where we have

$$g \circ f : A \to C$$

A map from $\mathbb{R}^n$ to $\mathbb{R}^m$ given by a matrix is known as a **linear map**, or **linear transformation**.

Definition 1.17 (Permutation). For some set S, a bijection from S to S, formally $\pi : S \to S$, is known as a **permutation** of S.

Theorem 1.18 (Properties of Compositions). Let $f : A \to B$, $g : B \to C$, and $h : C \to D$.

- The composition of mappings is associative: $(h \circ g) \circ f = h \circ (g \circ f)$
- If f and g are both injective, then $g \circ f$ is injective.
- If f and g are both surjective, then $g \circ f$ is surjective.
- If f and g are both bijective, then $g \circ f$ is bijective.

Definition 1.19 (Identity Mapping). For some set S, we will use id_S or id as the **identity mapping** from S to itself.

$$id(s) = s \forall s \in S$$

Definition 1.20 (Inverse Mappings). From 1.19, we can formally define an **inverse mapping** $g : B \to A$ of some map $f : A \to B$, where

$$g \circ f = id_A \text{ and } f \circ g = id_B$$

A map is said to be **invertible** if it has an inverse. We often give f^{-1} as the inverse of f.

Theorem 1.21. A Map is Invertible if and only if it is Bijective.

Proof. Suppose $f : A \to B$ is invertible with inverse $g : B \to A$. Then $g \circ f = id_A$ is the identity map, meaning $g(f(a)) = a$. If $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, then

$$a_1 = g(f(a_1)) = g(f(a_2)) = a_2$$

Thus, f is injective. Now suppose $b \in B$. Let $a \in A$ be the number such that $f(a) = b$. Recall that $f(g(b)) = b$. Thus, we have $a = g(b)$. This means each element of the domain will have some corresponding element in the image, and thus f is surjective.
Let f be bijective and let $b \in B$. Since f is surjective, there exists $a \in A$ where $f(a) = b$. Since f is injective, a is unique. Define $g(b) = a$. This is the inverse of f. ■

Definition 1.22 (Equivalent Relation). An equivalence relation on a set X is a relation $R \subset X \times X$ satisfying the properties

- $(x, x) \in R \; \forall x \in X$ **reflexive property**
- $(x, y) \in R \implies (y, x) \in R$ **symmetric property**
- $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$ **transitive property**

For an equivalence relation on X with $(x, y) \in R$, we often write $x \sim y$. If the relation has an associated notation such as $=, \equiv, \cong$, then that will be used.

Example. Suppose f and g are differentiable functions on $\mathbb{R}$. We can define an equivalence relation $f(x) \sim g(x)$ if $f'(x) = g'(x)$.

Definition 1.23 (Partition). A partition $\mathcal{P}$ of a set X is a collection of sets $X_1, X_2, \ldots \neq \varnothing$ such that

$$X_i \cap X_j = \varnothing \text{ for } i \neq j$$

and

$$\bigcup_k X_k = X$$

Definition 1.24 (Equivalence Class). Let $\sim$ be an equivalence relation on a set X with $x \in X$. Then the **equivalence class** of x is given as

$$[x] = \{y \in X \mid y \sim x\}$$

Theorem 1.25. Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X. Conversely, if $\mathcal{P} = X_i$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_i.

Corollary 1.26. Two equivalence classes of an equivalence relation are either disjoint or equal.

Chapter 2

The Integers

2.1 Mathematical Induction

Definition 2.1 (First Principle of Induction). Mathematical induction is a method of proof wherein a statement about integers with $n \in \mathbb{N}$. We prove the statement for a specific integer n_0, and then we show that the statement being true for some n implies the statement is true for $n+1$. This implies this statement holds for all integers $n \geq n_0$.

A standard example of induction follows.

Example. Show that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

for any $n \in \mathbb{N}$.
We can show this for $n = 1$:

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Now we can assume that we have verified the first n cases.

$$1 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + n + 1$$

$$= \frac{n^{2+3n+2}}{2}$$

$$= \frac{(n+1)((n+1)+1)}{2}$$

This is the formula for the $n+1$th case, so we are done.

Definition 2.2 (Second Principle of Induction). Let $S(n)$ be a statemenht about the integers for $n \in \mathbb{N}$. Suppose $S(n_0)$ is true. If $S(n_0), S(n_0+1), \ldots, S(k)$ implies $S(k+1)$ for $k \geq n_0$, then $S(n)$ is true for all integers $n \geq n_0$.

This is more complicated, so an example has not been given. Obviously.

Definition 2.3 (Principle of Well-Ordering). Every nonempty subset of the natural numbers is well-ordered.

Lemma 2.4. The principle of mathematical induction implies 1 is the least positive natural.

Theorem 2.5 (Principle of Well-Ordering)**.** The principle of well ordering can follow from the principle of mathematical induction. Furthermore, every nonempty subset of $\mathbb{N}$ contains at least one element.

2.2 The Division Algorithm

Theorem 2.6 (Division Algorithm)**.** Let a and b be integers with $b > 0$. Then there exists *unique* integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$.

Let $a, b \in \mathbb{Z}$. If $b = ak, k \in \mathbb{Z}$, then we write $a|b$. We say an integer d is a **common divisor** of a and b if $d|a$ and $d|b$. The **greatest common divisor** of integers a, b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d'|d$. We write $\gcd(a, b)$.

Definition 2.7 (Relatively Prime Numbers)**.** Two numbers $a, b \in \mathbb{Z}$ are relatively prime if $\gcd(a, b) = 1$.

Theorem 2.8. Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then there exist $r, s \in \mathbb{Z}$ such that

$$\gcd(a, b) = ar + bs$$

Corollary 2.9. For any two $a, b \in \mathbb{Z}$ that are relatively prime, there exist $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

The Euclidean Algorithm

2.8 allows us to compute the gcd of two integers. This will be illustrated with an example.

Example. Let's compute $\gcd(945, 2415)$. First, observe:

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0 \end{aligned}$$

Reversing our steps, we find that 105 divides 420, 105 divides 525, 105 divides 945, and 105 divides 2415. Hence, 105 divides both numbers. If d were another common divisor of 945 and 2415, then d would have to divide 105. Hence, $\gcd(2415, 945) = 105$.

To compute $\gcd(a, b) = d$, we are dividing multiple times to obtain a decreasing sequence of integers. We use the algorithm

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

where q_i is the highest integer number of times r_i can divide r_{i-1}, and r_{i+1} is the remainder.

Prime Numbers

Some $p \in \mathbb{N} \setminus \{1\}$ is a **prime number** if the only numbers that divide p are 1 and itself. Non-prime integers > 1 are known as **composite**.

Lemma 2.10 (Euclid). Let $a, b \in \mathbb{Z}$ and $p \in \mathbb{P}$, where $\mathbb{P}$ is the set of primes. Since $\gcd(a, p) = 1$, then there exists $r, s \in \mathbb{Z}$ such that $ar + ps = 1$.

Theorem 2.11 (Euclid). There exist an infinite number of primes.

Proof. We will do this proof via contradiction. Suppose there are a finite number of primes, say $\{p_1, \ldots, p_n\} = \mathbb{P}$.

$$\text{Let } P = 1 + \prod_{i \in \mathbb{P}} i$$

It follows that P is divisible by some p_i for $i \in [1, n]$. In this case, p_i must divide $P - p_1p_2 \cdots p_n = 1$. However, it does not, so there must either exist some $p_{n+1} \neq p_i$, or $P \in \mathbb{P}$. ■

Theorem 2.12 (Fundamental Theorem of Arithmetic). Let $n \in \mathbb{N}$ where $n > 1$. Then

$$n = p_1p_2 \cdots p_k$$

where $p_1, \ldots, p_k \in \mathbb{P}$, and are not necessarily distinct. Furthermore, this factorization is unique.

Chapter 3

Groups

3.1 Integer Equivalence Classes and Symmetries

Two integers $a, b \in \mathbb{Z}$ are equivalent mod n if n divides $a - b$ with no remainder. The integers mod n partition $\mathbb{Z}$ into n different equivalence classes, the set of which is denoted as $\mathbb{Z}_n$. For example, consider $\mathbb{Z}_{12}$, the set of the following equivalence classes:

$$\begin{aligned}[0] &= \{\ldots, -12, 0, 12, 24, \ldots\} \\ [1] &= \{\ldots, -11, 1, 13, 25, \ldots\} \\ &\vdots \\ [11] &= \{\ldots, -1, 11, 23, 35, \ldots\}\end{aligned}$$

We can define arithmetic over $\mathbb{Z}_n$, where we say addition modulo n is given as $(a + b) \mod n$.

Example. Operations modulo n:

$$\begin{aligned} 7 + 4 &\equiv 1 \mod 5 \\ 3 + 5 &\equiv 0 \mod 8 \\ 3 + 4 &\equiv 7 \mod 12 \end{aligned} \qquad \begin{aligned} 7 \cdot 3 &\equiv 1 \mod 5 \\ 3 \cdot 5 &\equiv 7 \mod 8 \\ 3 \cdot 4 &\equiv 0 \mod 12 \end{aligned}$$

Proposition 3.1. Let $\mathbb{Z}_n$ be the set of equivalence classes of the integers mod n and $a, b, c \in \mathbb{Z}_n$.

1. Addition and multiplication are commutative:

$$a + b \equiv b + a \mod n$$

$$ab \equiv ba \mod n$$

2. Addition and multiplication are associative:

$$(a + b) + c \equiv a + (b + c) \mod n$$

$$(ab)c \equiv a(bc) \mod n$$

3. There are both additive and multiplicative identities:

$$a + 0 \equiv a \mod n$$

$$a \cdot 1 \equiv a \mod n$$

4. Multiplication distributes over addition:

$$a(b + c) \equiv ab + ac \mod n$$

5. For every integer there exists an additive inverse:

$$a + (-a) \equiv 0 \mod n$$

6. If $a \neq 0$, then $\gcd(a, n) = 1$ iff there exists a multiplicative inverse b for $a \mod n$; that is, a $b \neq 0$ such that

$$ab \equiv 1 \mod n$$

3.2 Definitions and Examples

Definition 3.2 (Group). A group $(G, \circ)$ is a set G together with a **binary operation** (or **law of composition**) $G \times G \to G$ given as $(a, b) \mapsto a \circ b$ that satisfies the following axioms.

- The binary operation is **associative**. That is,

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

  Formally,

$$\forall (a, b, c \in G)((a \circ b) \circ c = a \circ (b \circ c))$$

- There exists an **identity element** $e \in G$, such that

$$e \circ a = a \circ e = a$$

  Formally,

$$\exists (e \in G)(\forall a \in G(a \circ e = e \circ a = a))$$

- For all $a \in G$, there exists an **inverse element** $a^{-1} \in G$, such that

$$a \circ a^{-1} = a^{-1} \circ a = e$$

  Formally,

$$\forall (a \in G)(\exists (a^{-1} \in G)(a \circ a^{-1} = a^{-1} \circ a = e))$$

The $\circ$ operator can be thought of as simply a placeholder for a binary operation such as addition, multiplication, or even an inner product-like operation.

Definition 3.3 (Abelian Group). A group $(G, \circ)$ with the property $a \circ b = b \circ a \ \forall a, b \in G$ is called **abelian** or **commutative**. A group not satisfying this property is known as **nonabelian** or **noncommutative**.

Notation. We will use ab to denote a binary operation associated with a set rather than $a \circ b$, partially for brevity but also to distinguish between group opperations and compositions. If a standard symbol is associated with the operation, such as $+$, that will be used instead.

For example, the set of integers $\mathbb{Z}$ forms a group under addition, because for all $a, b \in \mathbb{Z}$, we have $(a + b) \in \mathbb{Z}$, $a + 0 = a$, $a + (-a) = 0$, and $-a \in \mathbb{Z}$. We also have $a + b = b + a$, so the integers over addition $(\mathbb{Z}, +)$ form an abelian group.
The integers mod n also form a group under addition modulo n. Addition can be shown with a **Cayley table**, or a table describing addition/multiplication. Consider $\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

It's also to note that not every set with a binary operation defines a group. For example, the integers mod n are not necessarily closed under multiplication, so they cannot necessarily constitute

a group. However, we can recall from 3.1 that $ab \equiv 1 \mod n$ iff a, b are relatively prime; that is $\gcd(a, b) = 1$. Thus, we can define the multiplicative group of nonzero relatively prime numbers in $\mathbb{Z}_n$ as $U(n)$. For example, consider the Cayley table for $U(8)$:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Example. Let

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \hat{\imath} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\hat{\jmath} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad \hat{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

Notice the following.

$$\hat{\mathbf{i}}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$\hat{\mathbf{j}}^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$\hat{\mathbf{k}}^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$\implies \hat{\mathbf{i}}^2 = \hat{\mathbf{j}}^2 = \hat{\mathbf{k}}^2 = -1$$

The set $Q_8 = \{\pm 1, \pm\hat{\mathbf{i}}, \pm\hat{\mathbf{j}}, \pm\hat{\mathbf{k}}\}$ forms a group $(Q_8, \cdot)$ known as the **quaternion group**, which is nonabelian.

One final important example is the **general linear group**. This is the group of all invertible matrices over the multiplication operator, and is denoted $\mathrm{GL}(n, S)$ where the matrices are of order n with elements $a_{ij} \in S$.

Definition 3.4 (Order of a Group)**.** The order of a group G, denoted $|G|$, is the number of elements it has. If the group has **finite order**, we write $|G| = n$, where $n \in \mathbb{N}$. If a group has **infinite order**, we write $|G| = \infty$.

Basic Properties of Groups

Proposition 3.5. The identity element of a group is unique.

Proof. Suppose e and e' are both identities in G. Then $eg = ge = g$ and $e'g = ge' = g$ for all $g \in G$. However, $e, e' \in G$, so we can say

$$ee' = e'$$

$$ee' = e$$

$$\implies e = ee' = e'$$

$$\therefore e = e'$$

■

Proposition 3.6. If G is a group, then for any $g \in G$, its inverse g^{-1} is unique.

Proposition 3.7. Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. Let $a, b \in G$. Then $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, $b^{-1}a^{-1}ab = e$. By the previous proposition, we know that inverses are unique, and by 3.2 we know group operations are associative. Thus,

$$(ab)\left(b^{-1}a^{-1}\right) = e$$

$$\therefore (ab)^{-1} = b^{-1}a^{-1}$$

■

Proposition 3.8. If G is a group, then $\forall a \in G$, it will follow that $\left(a^{-1}\right)^{-1} = a$.

Proposition 3.9. If G is a group and $a, b, c \in G$, then $ba = ca \implies b = c$ and $ab = ac \implies b = c$.

The previous proposition shows that **right and left cancellation laws** hold in groups. This is due to the existance of inverses over the associated binary operation.

Notation. Oftentimes, exponential notation will be used in a group to denote repeated applications of the operation:

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

And

$$g^{-n} = \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}$$

Proposition 3.10. In a group G, the following properties of exponentiation hold for all $g, h \in G$:

- $g^m g^n = g^{m+n}\ \forall m, n \in \mathbb{Z}$
- $(g^m)^n = g^{mn}\ \forall m, n \in \mathbb{Z}$
- $(gh)^n = (h^{-1}g^{-1})^{-n}\ \forall n \in \mathbb{Z}$

Remark. In the above proposition, $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian. If the group is abelian, this property holds.

Remark. f the group has an addition operator, especially if the group is $\mathbb{Z}$ or $\mathbb{Z}_n$, we write the operation of exponentiation as multiplication, that is an rather than n^a for $n \in G$, $a \in \mathbb{Z}$.

3.3 Subgroups

Definitions and Examples

Definition 3.11 (Subgroup). A **subgroup** H of a group G is a subset $H \subseteq G$ such that when the group operation of G is restricted to H, then H is still a group. That is, if $H \subseteq G$ and $(G, \circ)$ is a group, then H is a subgroup if $(H, \circ)$ is a group.

Remark. The subgroup $H = \{e\}$ is called the **trivial subgroup**, and a proper subset that forms a group $H \subsetneq G$ is known as a **proper subgroup**.

Example. Consider the set of nonzero real numbers $\mathbb{R}^*$ over the operation of multiplication. The identity is 1 and the inverse of any $a \in \mathbb{R}^*$ is just a^{-1}. We can show that $\mathbb{Q}^*$ is a proper subgroup of $\mathbb{R}^*$. Trivially, $1 \in \mathbb{Q}^*$. Also, the inverse of any $\frac{p}{q} \in \mathbb{Q}^*$ must also be in $\mathbb{Q}^*$, since $\left(\frac{p}{q}\right)^{-1} = \frac{q}{p} \in \mathbb{Q}^*$. Since multiplication in $\mathbb{R}^*$ is associative, so is multiplication in $\mathbb{Q}^*$. Therefore, $\mathbb{Q}^*$ is a proper subgroup of $\mathbb{R}^*$.

Remark. A subset of some set G can be a group without being a *subgroup* of G, if it is a group under a different operation. For example, the general linear is not a subgroup of the additive group of $n \times n$ matrices, since it uses a different operation.

Example. Let $\mathrm{SL}(2, \mathbb{R}) \subset \mathrm{GL}(2, \mathbb{R})$ be the set of matrices $A \in \mathrm{SL}(2, \mathbb{R})$ satisfying $\det(A) = 1$. Multiplication is closed since $\det(A)\det(B) = \det(AB)$, and the other properties of groups follow directly from the general linear. This group is known as the **special linear group**.

Some Subgroup Theorems

Proposition 3.12. A subset H of G is a subgroup iff it satisfies the following conditions:

1. The identity $e \in G$ is in H.
2. If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proof. Trivial. ∎

Proposition 3.13. Let H be a subset of G. Then H is a subgroup of G iff $H \neq \varnothing$, and whenever $g, h \in H$ then $gh^{-1} \in H$.

Chapter 4

Cyclic Groups

4.1 Cyclic Subroups

Oftentimes, a subgroup can be constructed from a single element of a group. For example, consider $3 \in \mathbb{Z}$. now consider the set of all multiples of 3, that is

$$3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$$

Obviously, $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Specifically, it's a **cyclic subgroup** "generated" by 3.

Theorem 4.1 (Cyclic Subgroups). If G is a group and $a \in G$, then the set

$$\langle a \rangle = \left\{ a^k \mid k \in \mathbb{Z} \right\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G containing a.

Remark. If we use the $+$ notation, then we write

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

Definition 4.2 (Cyclic Groups and Subgroups). If G is a group with $a \in G$, then we say $\langle a \rangle$ is the **cyclic subgroup** generated by a. If there exists some $b \in G$ where $\langle b \rangle = G$, then G is a **cyclic group** generated by b. We call a and b the **generators** of their repsective groups.

Definition 4.3 (Order of a Cyclic Group). The **order** of a cyclic group $\langle a \rangle$ is the smallest **positive** integer $n \in \mathbb{Z}^+$ such that $a^n = e$, where $e \in \langle a \rangle$ is the identity element. If there does not exist some n, we say $|a| = \infty$.

Remark. When considering the above definition, it's important to note that $0 \notin \mathbb{Z}^+$.

Example. Notice that both 1 and 5 generate $(\mathbb{Z}_6, +)$. Also, not every element necessarily generates the group. The element $2 \in \mathbb{Z}_6$ generates $\langle 2 \rangle = \{0, 2, 4\}$.

Theorem 4.4. Every cyclic subgroup is abelian.

Proof. Let $\langle a \rangle = G$ and $a \in G$. If $g, h \in G$, then they can be written as powers of a. Let $r, s \in \mathbb{Z}$ such that $g = a^r, h = a^s$.

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg$$

Therefore G is abelian. ■

Subgroups of Cyclic Groups

Theorem 4.5. Every subgroup of a cyclic group is cyclic.

Corollary 4.6. The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n \in \mathbb{N} \cup \{0\}$.

Proposition 4.7. Let G be a cyclic subgroup of order n and suppose $\langle a \rangle = G$. Then $a^k = e$ iff n divides k with no remainder.

Theorem 4.8. Let G be a cyclic group of order n with $\langle a \rangle = G$. If $b = a^k$, then the order of b is $\frac{n}{d}$, where $d = \gcd(k, n)$.

Corollary 4.9. The generators of $\mathbb{Z}_n$ are the integers $r \in [1, n)$ where $\gcd(r, n) = 1$.

4.2 Multiplicative Group of Complex Numbers

Definition 4.10 (Complex Numbers)**.** The **complex numbers** are defined as

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

where $i = \sqrt{-1}$

Definition 4.11 (Arithmetic in $\mathbb{C}$)**.** If $z = a + bi$ and $w = c + di$ with $z, w \in \mathbb{C}$, then we have

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

$$zw = (a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i$$

Every nonzero complex number $z = a + bi$ has a multiplicative inverse, that is $z^{-1} \in \mathbb{C}$ such that $zz^{-1} = z^{-1}z = 1$.

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

Definition 4.12 (Complex Conjugate)**.** If $z = a + bi$, then the complex conjugate $\overline{z} = a - bi$.

Complex numbers can also be represented in **polar coordinates** of the form

$$z = a + bi = r(\cos\theta + i\sin\theta)$$

and

$$r = |z| = \sqrt{a^2 + b^2}$$

and

$$a = r\cos\theta \quad b = r\sin\theta$$

and

$$\theta = \arctan\left(\frac{b}{a}\right)$$

Notation. We can abbreviate $r(\cos\theta + i\sin\theta) =: r\operatorname{cis}\theta$.

Proposition 4.13. Let $z = r\operatorname{cis}\theta$ and $w = s\operatorname{cis}\phi$. Then

$$zw = rs\operatorname{cis}(\theta + \phi)$$

Theorem 4.14 (DeMoivre). Let $z = r\operatorname{cis}\theta \in \mathbb{C} \setminus \{0\}$. Then

$$(r\operatorname{cis}\theta)^n = r^n\operatorname{cis}(n\theta)$$

The Circle Group and the Roots of Unity

The multiplicative group of complex numbers $(\mathbb{C}, \cdot) \triangleq \mathbb{C}^*$ has interesting subgroups. Specifically, $\mathbb{R}^*$ and $\mathbb{Q}^*$ have no subgroups of finite order, but $\mathbb{C}^*$ has many.

Definition 4.15 (Circle Group). The circle group is the multiplicative group $\mathbb{T} \subsetneq \mathbb{C}$ defined as

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

Remark. This group forms a circle on the complex grid with radius 1.

Proposition 4.16. The circle group $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$

The circle group has many interesting subgroups, such as $\{1, -1, i, -i\}$. These numbers are the numbers satisfying $z^4 = 1$. These are known as the 4th **roots of unity**.

Definition 4.17 (Roots of Unity). The set of complex numbers z satisfying $z^n = 1$ for some $n \in \mathbb{N}$ are known as the n**th roots of unity**.

Theorem 4.18 (Roots of Unity Definition). If $z^n = 1$, then the nth roots of unity are

$$z = \operatorname{cis}\left(\frac{2k\pi}{n}\right)$$

where $k \in \{0, 1, \ldots, n-1\}$. Furthermore, the nth roots of unity are a subgroup of $\mathbb{T}$ of order n.

Definition 4.19 (Primitive nth root of unity). A primitive nth root of unity is some z that generates the nth roots of unity.

For example, the 8th roots of unity have 4 generators:

$$\begin{aligned} w &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ w^3 &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ w^5 &= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ w^7 &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \end{aligned}$$

4.3 The Method of Repeated Squares

looked boring ill come back to it later

Chapter 5

Permutation Groups

Consider an equilateral triangle $\triangle ABC$. The symmetries of this triangle actually consist of permutations of the three vetices, where a **permutation** of the set $S = \{A, B, C\}$ is a bijective map $\pi : S \to S$. The three vertices have the following six permuations:

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

In this case, the array

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

denotes the permuation that sends $A \to B$, $B \to C$, and $C \to A$:

$$A \mapsto B$$

$$B \mapsto C$$

$$C \mapsto A$$

The symmetries of a triangle form a group. In this chapter we study groups of this type.

5.1 Definitions and Notation

The permutations of a set X form a group S_X. If X is finite, then we assume $X = \{1, 2, \ldots, n\}$. In this case we write S_n instead of S_X. We call this the **symmetric group** on n letters.

Theorem 5.1 (Symmetric Group on n Letters). The symmetric group on n letters S_n is a group with $n!$ elements, wherein the binary operation is the composition of maps.

Proof. The identity of S_n is the identity map. If $f : S_n \to S_n$ is a permutation, then f^{-1} exists by 1.20 since f is bijective. Thus, every map has an inverse under the composition operation. By 1.18, compositions are associative. Thus, $(S_n, \circ)$ is a group. There are $n!$ ways to arrange sets of order n, so $|S_n| = n!$. ■

Definition 5.2 (Permutation Group). A subgroup of S_n is a **permutation group**.

Example. Consider the subgroup G of S_5 consisting of the identity permutation id and the permutations

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

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

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

We can construct this table defining how to operate with elements in this permutation group.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Remark. Functions are composed from right to left. That is, $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. We can thus adopt the convention of operating from right to left on permutations, that is given $\sigma\tau$ we will simply do τ first.

Example. Permutation groups are usually not abelian. Let

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

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

Then

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

and

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

Cycle Notation

Definition 5.3 (Permutations as Cycles). A permutation $\sigma \in S_X$ is a **cycle of length** k if there exists $a_1, \ldots, a_k \in X$ such that

$$\sigma(a_1) = a_2$$
$$\sigma(a_2) = a_3$$
$$\vdots$$
$$\sigma(a_k) = a_1$$

and $\sigma(x) = x$ for all other $x \in X$. We write $(a_1, \ldots, a_k)$ to denote the cycle σ.

Remark. Cycles are the building blocks of all permutations.
For example, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$$

is a cycle of length 6, and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

is a cycle of length 3. Not all permutations are cycles. For example,

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56)$$

coinsists of both a cycle of length 2 and of length 4.
Example. It's easy to compute compositions of cycles. Let

$$\sigma = (1352) \text{ and } \tau = (256)$$

We can think of σ as

$$\sigma \equiv \begin{cases} 1 \mapsto 3 \\ 3 \mapsto 5 \\ 5 \mapsto 2 \\ 2 \mapsto 1 \end{cases}$$

and we can think of τ as

$$\tau \equiv \begin{cases} 2 \mapsto 5 \\ 5 \mapsto 6 \\ 6 \mapsto 2 \end{cases}$$

Thus, we can find

$$(\sigma \circ \tau) \equiv \begin{cases} 2 \mapsto 5 \mapsto 2 \\ \quad 5 \mapsto 6 \\ 6 \mapsto 2 \mapsto 1 \\ \quad 1 \mapsto 3 \\ \quad 3 \mapsto 5 \\ 5 \mapsto 2 \mapsto 5 \end{cases} \equiv \begin{cases} 5 \mapsto 6 \\ 6 \mapsto 1 \\ 1 \mapsto 3 \\ 3 \mapsto 5 \end{cases} \equiv (1356)$$

Similarly, if $\mu = (1634)$, then $\sigma\mu = (1652)(34)$

Definition 5.4 (Disjoint Cycles). If $\sigma, \tau \in S_X$ are cycles such that $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_l)$, then σ and τ are **disjoint** if $a_i \neq b_j$ for all i, j.

The products of disjoint cycles cannot be simplified.

Proposition 5.5. Let σ and τ be disjoint cycles in S_X. $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_l)$. We must show $\sigma\tau(x) = \tau\sigma(x)$ for all $x \in X$. If $x \notin \{a_1, \ldots, a_k\}$ and $x \notin \{b_1, \ldots, b_l\}$, then both σ and τ **fix** x, meaning $\sigma(x) = x$ and $\tau(x) = x$. Thus,

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)) = \tau\sigma(x)$$

Now, suppose $x \in a_1, \ldots, a_k$. Thus, $\sigma(a_i) = a_{(i \mod k)+1}$, meaning

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_{k-1} &\mapsto a_k \\ a_k &\mapsto a_1 \end{aligned}$$

Since σ and τ are disjoint, then $\tau(a_i) = a_i$. Thus,

$$\begin{aligned} \sigma\tau(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{(i \mod k)+1} \\ &= \tau(a_{(i \mod k)+1}) \\ &= \tau(\sigma(a_i)) \\ &= \tau\sigma(a_i) \end{aligned}$$

The same logic holds for $x \in \{b_1, \ldots, b_l\}$. Since σ and τ are disjoint,

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \varnothing$$

■

Theorem 5.6 (Permutations as Cycles). Every permutation $\sigma \in S_n$ can be written as the product of disjoint cycles.

Proof. Assume $X = \{1, 2, \ldots, n\}$. Let $\sigma \in S_n$ and define $X_1 = \{\sigma(1), \sigma^2(1), \ldots\}$. The set X_1 must be finite, since the set X is finite. Let $i \in \mathbb{Z}$ be the first integer in X that is not in X_1, and let $X_2 = \{\sigma(i), \sigma^2(i), \ldots\}$. Again, this set is finite. Now we can define $X_3, X_4, \ldots$ in the same manner. Since X is finite, there will be a finite number of these **disjoint** sets. Let this number be r. If σ_i is given as

$$\begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i \end{cases}$$

Then $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$. Since the sets $X_1, \ldots, X_r$ are disjoint, then the cycles $\sigma_1, \ldots, \sigma_r$ are also disjoint. ■

Remark. Permutations will generally be represented by cycles for brevity, and the identity permutation will be given as (1).

Transpositions

Definition 5.7 (Transposition)**.** A transposition is a cycle of length 2.

Proposition 5.8. Any permutation of a finite set containing at least two elements can be given as the product of transpositions.

Example. For example, the permutation

$$(16)(253) = (16)(23)(25)$$

There is no unique representation of permutations as a product of transpositions. For example, the above permutation can also be given as

$$(16)(45)(23)(45)(25)$$

Interestingly, no permutation can be written as both an odd *and* an even number of transpositions.

Lemma 5.9. If the identity is written as the product of r transpositions

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_r$$

then r is even.

Theorem 5.10. If a permutation σ can be expressed as the product of an even number of transpositions, then all other products of transpositions equaling σ must contain an even number of transpositions. Similarly, if σ can be expressed as an odd number of transpositions, then any set of transpositions equaling σ must be odd.

Proof. Suppose

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n$$

where m is even. The inverse of σ is $\sigma_m\cdots\sigma_1$.

$$\mathrm{id} = \sigma\sigma_m\cdots\sigma_1 = \tau_1\cdots\tau_n\sigma_m\cdots\sigma_1$$

thus n is even by 5.9. ∎

The Alternating Groups

5.2 Dihedral Groups

The Motion Group of a Cube