Abstract Algebra

MATH1530

Professor Jordan Kostiuk

Brown University

Edited by

Richard Tang

Contents

Chapter 1

Set Theory

Set theory forms a basis for all of higher mathematics. We begin with a brief introduction.

§1.1 Sets

Definition 1.1.1: Sets

A **set** is a (possibly empty) collection of elements. If S is a set and a is some object, then a is either an element of S or not. We write:

- $a \in S$ if a is an element of S.
- $a \notin S$ if a is not an element of S.

The empty set is denoted $\varnothing$. We use $|S|$ or $\#S$ to denote the cardinality (number of elements) in a finite set.

Definition 1.1.2: Natural Numbers

The **natural numbers** are the set

$$\mathbb{N} = \{1, 2, \ldots\}.$$

Formally, we define $\mathbb{N}$ as follows:

1. $\mathbb{N}$ contains an initial element 1.
2. $\forall n \in \mathbb{N}$, there is an incremental rule that creates the next element $n + 1$.
3. We can reach every element of $\mathbb{N}$ by starting with 1 and repeatedly adding 1.

Remark 1. *$\mathbb{N}$ is totally ordered. We say m is less than n if n appears before n when we start from 1 and add repeatedly. In this case we write $m < n$ or $m \leq n$ if $m = n$.*

Example 1. *Let*

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$$

denote the set of integers, and

$$Q = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

the set of rationals.

Definition 1.1.3: Set Operations

Let S, T be sets.

1. S is a **subset** of T if every element of S is an element of T, i.e. $a \in S \to a \in T$. We write
$$S \subset T.$$
2. The **union** of S and T is the set of elements that belong to S or belong to T, denoted
$$S \cup T = \{a \mid a \in S \text{ or } a \in T\}.$$
3. The **intersection** of S and T is the set of elements that belong to both S and T, denoted
$$S \cap T = \{a \mid a \in S \text{ and } a \in T\}.$$
4. If $S \subset T$, the **complement** of S in T is the set of elements in T *not* in S:
$$S^c = T - S = T\S = \{a \in T \mid a \notin S\}.$$
5. The **product** of S and T is the set of ordered pairs
$$S \times T = \{(a, b) \mid a \in S, b \in T\}.$$
We have projection maps
$$\begin{aligned} proj_1 : S \times T &\longrightarrow S \\ (a, b) &\longmapsto a. \end{aligned}$$
and
$$\begin{aligned} proj_2 : S \times T &\longrightarrow T \\ (a, b) &\longmapsto b. \end{aligned}$$

These definitions extend to sets $S_1, \ldots, S_n$:

$$S_1 \cup \ldots \cup S_n = \bigcup_{i \in I} S_i = \{a \mid a \in S_1 \text{ and } \ldots \text{ and } a \in S_n\} \tag{1.1}$$

§1.1.1 The Well-Ordering Principle

Theorem 1.1.1: Well-Ordering Principle

Let $S \subset N$ be a non-empty subset of $\mathbb{N}$. Then S has a *minimal element*. That is,

$\exists m \in S$ s.t. $n \geq m, \forall n \in S$. Informally, there exists a minimum element that is smaller than all other natural elements.

Proof. Since S is non-empty, we can pick $k \in S$. By definition of $\mathbb{N}$, we can start with 1 and add 1 repeatedly to get k. So, there are only k elements of $\mathbb{N}$ less than or equal to k:

$$1 < 2 < \ldots < k - 1 < k.$$

So, we can keep moving down from k, until we find an element $j \notin S$; since there are no smaller elements than $j + 1 \in S$, $j + 1$ is the minimal element. □

§1.2 Functions

Definition 1.2.1: Functions

A **function** from S to T is a rule that assigns some element of T to each element of S :

$$f : S \to T, s \mapsto f(s).$$

S is the **domain** , and T the **codomain**.

Definition 1.2.2: Composition of Functions

If $f : S \to T$ and $S : T \to U$, then the **composition** of f and g is

$$g \circ f = S \to U, a \mapsto g(f(a)).$$

Definition 1.2.3: Bijectivity

Let $f : S \to T$ be a function.

1. f is **injective** or one-to-one if distinct elements of S go to distinct elements of T. In other words,
$$f(a) = f(b) \to a = b.$$
2. f is **surjective** or onto if every element of T comes from some element in S:
$$\forall t \in T, \exists s \in S \text{ s.t. } f(s) = t.$$
3. f is **bijective** if it is both injective and surjective.

Definition 1.2.4: Invertibility

Let $f : S \to T$ be a function. f is **invertible** if

$$\exists g : T \to S, (g \circ f)(s) = s, s \in S \text{ and } (f \circ g)(t) = t, t \in T.$$

Theorem 1.2.1: Bijective iff Invertible

Let $f : S \to T$ be a function. Then f is invertible $\iff$ f is bijective.

Proof. Suppose first that f is invertible. Let $g : T \to S$ denote the inverse. We need to prove that f is bijective.
To prove injectivity, suppose $f(a) = f(b)$ for some $a, b \in S$. Applying g to both sides and using the fact that g is the inverse of f, we have

$$g(f(a)) = g(f(b)) \Rightarrow a = b.$$

Thus f is injective.
To prove surjectivity, let $t \in T$; we need to find $s \in S$ such that $f(s) = t$. Using the inverse, let $s = g(t)$. Then

$$f(s) = f(g(t)) = t.$$

Thus f is surjective.
Since f is both injective and surjective, f is bijective.

Now, suppose that f is bijective. Then $\forall t \in T, !\exists s \in S$ s.t. $f(s) = t$. Define a new function $g : T \to S$

$$g(t) := \text{"the unique } s \in S \text{ s.t. } f(s) = t\text{"}.$$

We now show that $(g \circ f)(s) = s$ and $(f \circ g)(t) = t$ for $s \in S, t \in T$.
Given $t \in T$, $f(g(t))) = t$ by definition of t. Given $s \in S$, we know that s maps to $f(s)$; so, by definition of g, $g(f(s)) = s$.
Thus, g is the inverse of f. $\square$

Chapter 2

Groups: Part I

Groups are a fundamental baseline for abstract algebra. We start with motivating examples, then move on to a concrete definition.

§2.1 Motivation

§2.1.1 Permutations

Definition 2.1.1: Permutations

Let X be a set. A **permutation** of X is a bijective function

$$\pi : X \to X$$

with the property: $\forall x \in X, !\exists x' \in X$ such that $\pi(x') = x$. This allows us to define an inverse π^{-1} to be the permutation

$$\pi^{-1} : X \to X$$

with the rule that $\pi^{-1}(x) = x'$, where $x' \in X$ is the unique element such that $\pi(x') = x$.
The **identity permutation** of X is the identity map

$$e : X \to X, e(x) = x \forall x \in X.$$

In general, a *permutation* of a set X is a rule that "mixes up" the elements of X.

Example 2. *Let $X = \{1, 2, 3, 4\}$. Then a permutation $\sigma : X \to X$ can be thought of as a shuffling of X and visualized as follows:*

$$\begin{aligned} 1 &\Rightarrow 2 \\ 2 &\Rightarrow 3 \\ 3 &\Rightarrow 1 \\ 4 &\Rightarrow 4 \end{aligned}$$

σ^{-1} would be defined as

$$\begin{aligned} 1 &\Rightarrow 3 \\ 2 &\Rightarrow 1 \\ 3 &\Rightarrow 2 \\ 4 &\Rightarrow 4 \end{aligned}$$

Now, suppose τ is defined as $1 \Rightarrow 1, 2 \Rightarrow 3, 3 \Rightarrow 2, 4 \Rightarrow 4$. Then $\sigma \circ \tau$ is

$$\begin{aligned} 1 &\Rightarrow 2 \\ 2 &\Rightarrow 1 \\ 3 &\Rightarrow 3 \\ 4 &\Rightarrow 4 \end{aligned}$$

and $\tau \circ \sigma$ is

$$\begin{aligned} 1 &\Rightarrow 3 \\ 2 &\Rightarrow 2 \\ 3 &\Rightarrow 1 \\ 4 &\Rightarrow 4 \end{aligned}$$

From this, we gather some observations.

- Given any 2 permutations, we can compose to get a new one.
- There was a permutation that didn't do anything ($\sigma \circ \sigma^{-1}$).
- We can invert any permutation.
- If σ, τ are two permutations, then we don't necessarily have $\tau \circ \sigma = \sigma \circ \tau$ (in other words, the group of permutations with composition is not commutative).

Definition 2.1.2: Transformations

Let X be a figure in $\mathbb{R}^2$. Then $Trafo(X)$ is the set of transformations on X.

Consider the symmetries of a square (involving reflections/rotations on a square) as a motivating example of transformations; are they invertible? commutative?

Remark 2. *Each transformation gives a permutation of the vertices $\{A, B, C, D\}$.*

§2.2 (Abstract) Groups

Definition 2.2.1: Groups

A **group** $\{X, \cdot\}$ consists of a set X, together with a rule

$$\begin{aligned} \cdot : G \times G &\to G \\ (g_1, g_2) &\mapsto g_1 \cdot g_2 \end{aligned}$$

satisfying the following axioms:

1. (identity) there is an element $e \in G$ such that
$$e \cdot g = g \cdot e = g.$$
for all $g \in G$.
2. (inverse) For all $g \in G$, there is an $h \in G$ such that
$$g \cdot h = h \cdot g = e.$$
The element h is called g^{-1}, the inverse of g.
3. (associativity) Given g_1, g_2, g_3, we have
$$g_1(g_2 \cdot g_3) = (g_1 \cdot g_2)g_3.$$

If, in addition, the group satisfies

4. (commutative) Given $g_1, g_2 \in G$, we have
$$g_1 \cdot g_2 = g_2 \cdot g_1.$$

then G is an **Abelian** group.

Now, we observe some interesting properties that follow from the group axioms.

Proposition 2.2.1: Group Properties

Let G be a group.

1. The identity element is unique.
2. Each element of G has only one inverse.
3. If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.
4. Given $g \in G$, $(g^{-1})^{-1} = g$.

Proof of (b). Suppose $g \in G$and that both h_1, h_2 satisfy the inverse axiom. Then
$$g \cdot h_1 = e = g \cdot h_2.$$
By the inverse axiom, we multiply on the left by an inverse of g:
$$\begin{aligned} e \cdot h_1 &= e \cdot h_2 \\ h_1 &= h_2. \end{aligned}$$
Thus the inverse is unique. □

Definition 2.2.2: Order

- The **order**of a group G is denoted $\#G$ or $|G|$ is the number of elements in G if finite, and ∞ if infinite.
- If G is a group and $g \in G$, the smallest n in which $g^n = e$ is called **the order**

of g. If no n exists, we say g has infinite order.

Proposition 2.2.2: Individual Order and Group Order

Suppose G is a finite group and suppose $g^n = e$. Then the order of g divides n.

Proof. Let n be the order of $g \in G$. Then, by long division, we can write

$$m = n \cdot g + r,\ 0 \leq r < m.$$

Using this equality together with $g^n = e$ and $g^m = e$, we get

$$e = g^n = g^{m \cdot q + r} = (g^m)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r.$$

We find that $g^r = e$; but $r < m$ and m is the order of g.
[TODO]: Finish this exercise with a well-defined proof, not this bullshit □

§2.2.1 Examples of Groups

Example 3. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all Abelian groups with respect to addition. However, $\mathbb{Z}$ is not a group with respect to multiplication, as the multiplicative inverse does not exist. Additionally, $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are not groups with respect to multiplication, due to zero; but $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ are all groups under multiplication.*

Example 4. *Let $\mathbb{Z}/m\mathbb{Z}$ be the set of integers modulo m. Then $\mathbb{Z}/m\mathbb{Z}$ is a group under addition modulo m, $+_m$; $\mathbb{Z}/m\mathbb{Z}$ is finite with order m. We also observe that $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group.*

Example 5. *Let the set of $n \times n$ matrices be M_n. Then M_n is an Abelian group under addition, but not multiplication (since not all matrices have inverses).*

Let
$$GL_n(\mathbb{R}) = \{M \in M_n \mid \det(M) \neq 0\}$$
*, denote the **general linear group**. Then $GL_n(\mathbb{R})$ is a group using matrix multiplication (not Abelian though).*

§2.2.2 Cyclic Groups

Definition 2.2.3: Cyclic Groups

A group G is **cyclic** if there is a $g \in G$ such that

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}.$$

We call g a **generator**.

Some examples of cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$; both have generators 1. Another one is the permutation group.

Definition 2.2.4: Permutation Groups

Given X a set, let S_X denote the **symmetric group of** X, or the group of permutations of X. If

$$X = \{1, \dots, n\},$$

we use the notation S_n.
Let P_n be a regular n-gon with vertices $1, \dots, n$. The group of transformations of D_n (e.g. rotations, reflections, and compositions of such) is called the **dihedral group** D_n. We will later prove that D_n has order $2n$.

§2.3 Group Homomorphisms

Definition 2.3.1: Homomorphisms

Let G_1, G_2 be groups. A **homomorphism** from G_1 to G_2 is a function $\phi : G_1 \to G_2$ satisfying:

$$\phi(g_1 \cdot_{G_1} g_2) = \phi(g_1) \cdot_{G_2} \phi(g_2).$$

In other words, the map ϕ preserves the group operations.

Example 6. *Examples of homomorphisms:*

- *There exists a homomorphism from the dihedral group to the group* ± 1*:*

  $$\phi : D_n \to \{\pm 1\}$$

  , where $\phi(\sigma) = 1$ *if rotation,* $\phi(\sigma) = -1$ *if flip.*

- *For* $n \geq m \geq 1$*, there is an injective homomorphism*

  $$f : S_m \to S_n.$$

  Note that this homomorphism is not surjective. More generally, if $X_1 \subseteq X_2$*, then there is an injective homomorphism* $f : S_{X_1} \to S_{X_2}$*.*

- *There is a homomorphism*

  $$\log : (\mathbb{R}, \times) \to (\mathbb{R}, +)\,.$$

- *There is a homomorphism between the general linear group to the real numbers*

  $$\begin{aligned} det : GL_n(\mathbb{R}) &\longrightarrow \mathbb{R} \\ AB &\longmapsto det(AB) = det(A) \cdot det(B). \end{aligned}$$

Definition 2.3.2: Isomorphisms

Groups G_1, G_2 are **isomorphic** if there exists a **bijective homomorphism** $f : G_1 \to G_2$. In this case, f is called an **isomorphism**.

Example 7. *Let $\mathcal{C}_n = \{g_0, g_1, \ldots, g_{n-1}\}$ with operation $\cdot : \mathcal{C}_n \times \mathcal{C}_n \to \mathcal{C}_n$ defined by*

$$g_i \cdot g_j = \begin{cases} g_{i+j}, & i+j < n \\ g_{i+j-n}, & i+j \geq n \end{cases}$$

then $\mathcal{C}_n$ is called the abstract cyclic group of order n.

We've now seen two examples of cyclic groups of order n: $\mathbb{Z}/n\mathbb{Z}$ and $\mathcal{C}_n$. Naturally, we wonder if these groups are actually different (from the perspective of group theory). Equivalently, **are these two groups isomorphic**?

Example 8. *$\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathcal{C}_n$ ($\mathbb{Z}/n\mathbb{Z} \simeq \mathcal{C}_n$). Consider the map*

$$\begin{aligned} \phi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathcal{C}_n \\ a &\longmapsto \phi(a) = g_a. \end{aligned}$$

Then $\phi(a+b) = \phi(a) \cdot \phi(b)$ by definition of group operations. So ϕ is a homomorphism.
ϕ is surjective since $i \in \{0, \ldots, n-1\}$ maps to $g_i \in \{g_0, \ldots, g_{n-1}\}$.
Since $\mathbb{Z}/n\mathbb{Z}$ and $\mathcal{C}_n$ both have n elements, ϕ is injective as well.
So, ϕ is an isomorphism and $\mathcal{C}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Note that if a group is isomorphic, there isn't necessarily a unique isomorphism. Consider the same isomorphism as above, except map $a \mapsto g_{a+1}$. This is also an isomorphism.

Example 9. *Given any group G, and an element $g \in G$, then multiplication by g permutes the elements of G. This gives rise to an injective homomorphism $\phi : G \to S_G$.*

This implies that by knowing every symmetric group, one knows much about every other group.