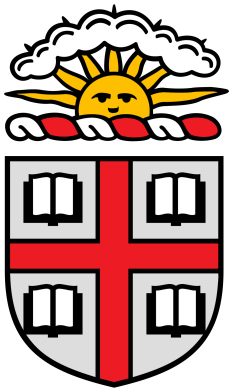
Abstract Algebra

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. □

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:*

$$1 \Rightarrow 2$$
$$2 \Rightarrow 3$$
$$3 \Rightarrow 1$$
$$4 \Rightarrow 4$$

σ^{-1} would be defined as

$$1 \Rightarrow 3$$
$$2 \Rightarrow 1$$
$$3 \Rightarrow 2$$
$$4 \Rightarrow 4$$

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

$$1 \Rightarrow 2$$
$$2 \Rightarrow 1$$
$$3 \Rightarrow 3$$
$$4 \Rightarrow 4$$

and $\tau \circ \sigma$ is

$$1 \Rightarrow 3$$
$$2 \Rightarrow 2$$
$$3 \Rightarrow 1$$
$$4 \Rightarrow 4$$

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

We now formally define the notion of a **group**.

Definition 2.2.1: Groups

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

$$\cdot : G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 \cdot g_2$$

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:
$$e \cdot h_1 = e \cdot h_2$$
$$h_1 = h_2.$$
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 m be the order of $g \in G$; then m is the smallest positive integer such that $g^m = e$. Dividing n by m yields

$$n = mq + r,\ q, r \in \mathbb{Z}, 0 \leq r < m.$$

In other words, dividing n by m leaves a quotient q and a remainder r.
Using this equality together with $g^n = g^m = e$, we have

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

Hence $g^r = e$, and $r \in [0, m)$. But by definition, m is the smallest integer such that $g^m = e$. Therefore $r = 0$, and $n = mq$, and so m, the order of g, divides n. □

Proposition 2.2.3: Order of Inverse

Let G be a finite group, and $g \in G$. Then $|g| = \left|g^{-1}\right|$.

Proof. Let $|g| = n$; then $g^n = e$. From this, we get

$$e = (g \cdot g^{-1})^n = g^n \cdot (g^{-1})^n = e \cdot (g^{-1})^n,$$

and so $(g^{-1})^n = e$.
Now we show that $\left|g^{-1}\right| = n$. Suppose $\left|g^{-1}\right| = m$, and $m < n$. Then

$$e = g^n \cdot (g^{-1})^m = g^{n-m}.$$

But we know that $|g| = n$, or equivalently, n is the smallest positive integer such that $g^n = e$; hence $g^{n-m} = e$ is a contradiction. Thus $m = n$, and so $\left|g^{-1}\right| = n$. □

§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 non-Abelian group under matrix multiplication.*

§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

$$G = \{\ldots, g^{-2}, g^{-1}, e \text{ (or } g^0), g, g^2, g^3, \ldots\}.$$

We call g a **generator**.
In general, for $n \geq 1$, the **abstract cyclic group order** n is the set

$$\mathcal{C}_n = \{g_0, g_1, \ldots, g_{n-1}\}$$

together with the composition rule

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

The identity element of $\mathcal{C}_n$ is g_0, and the inverse of g_i is g_{n-i} (except g_0, whose inverse is g_0). Further, $\mathcal{C}_n$ is an Abelian group, as $g_{i+j} = g_{j+i}$.

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

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

we use the notation S_n.
Let P_n be a regular n-gon with vertices $1, \ldots, n$. 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

Suppose that G, G' are groups, and suppose that ϕ is a function

$$\phi : G \longrightarrow G'$$

from elements of G to elements of G'. Many functions exist, but we're interested in the ones that preserve the "structure", or *group-i-ness*, of G and G'. But what makes a group a group? Specifically, groups are **associative**, and have **identity and inverse elements**. Thus, a function ϕ must preserve these qualities. We call such structure-preserving functions **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:

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2).$$

In other words, the map ϕ preserves the group operations. (Note that the composition law is different on the left and right sides! The left is the composition law of G_1, while the right is the composition law of G_2.)

It turns out this property is enough to force the identities and inverses to exist under a function.

Proposition 2.3.1

Let $\phi : G \to G'$ be a homomorphism of groups.

1. Let $e \in G$ be the identity element of G. Then $\phi(e) \in G'$ is the identity element of G'.
2. Let $g \in G$, and let $g^{-1} \in G$ be its inverse. Then $\phi(g^{-1}) \in G$ is the inverse of $\phi(g)$.

Proof. 1. Observe that $e = e \cdot e$, and that ϕ is a homomorphism (and so $\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$). Let $e' \in G'$ be the identity element of G'. Then

$$\begin{aligned} e' &= \phi(e) \cdot \phi(e)^{-1} \\ &= (\phi(e) \cdot \phi(e)) \cdot \phi(e)^{-1} \\ &= \phi(e) \cdot (\phi(e) \cdot \phi(e)^{-1}) \\ &= \phi(e) \cdot e' \\ &= \phi(e). \end{aligned}$$

Hence $e' = \phi(e)$.

2. We have

$$\begin{aligned} \phi(g^{-1}) \cdot \phi(g) &= \phi(g^{-1} \cdot \phi(g)) \\ &= \phi(e) \\ &= e'. \end{aligned}$$

The proof that $\phi(g) \cdot \phi(g^{-1}) = e'$ is similar. Hence $\phi(g^{-1})$ is the inverse of $\phi(g)$. □

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**.

Interestingly, isomorphic groups are really the same group, but their elements are given different names.
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 7. $\mathbb{Z}/n\mathbb{Z}$ *is isomorphic to* $\mathcal{C}_n$ *(*$\mathbb{Z}/n\mathbb{Z} \cong \mathcal{C}_n$*). 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 8. *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.

§2.4 Subgroups, Cosets, and Lagrange's Theorem

In all mathematics, a three-step process exists for studying complicated objects.

1. Deconstruction: Break your object into smaller and simpler pieces.
2. Analysis: Analyze the smaller, simpler pieces.
3. Fit the pieces back together.

For a group G, a natural way to form a smaller and simpler piece is by taking subsets $H \subseteq G$ that are themselves groups.

Definition 2.4.1: Subgroups

Let G be a group. A **subgroup of** G is a subset $H \subset G$ that is itself a group under G's group law. Explicitly, H needs to satisfy

1. (Closure Under Composition) For every $h_1, h_2 \in H$, $h_1 \cdot h2 \in H$
2. The identity element e is in H.
3. For every $h \in H$, its inverse h^{-1} is in H.

This is sometimes denoted $H < G$.

Note that since H uses G's composition law, associativity is automatically satisfied. If H is finite, the **order** of H is the number of elements in H.

Proposition 2.4.1: Easier Subgroup Checking

Let G be a group, and $H \subseteq G$ a subset. If

- $H \neq \varnothing$
- For every $h_1, h_2 \in H$, the element $h_1 h_2^{-1}$ is in H

then H is a subgroup of G.

Proof. Clearly, $H \neq \varnothing$ (otherwise the identity would not be in H).
To show that $e \in H$, let $h_2 = h_1$. Then

$$h_1 \cdot h_2^{-1} = h_1 \cdot h_1^{-1} = e \in H.$$

Thus the identity is in H.
To show that $\forall h \in H,\ h^{-1} \in H$, let $h_1 = e$. Then

$$h_1 \cdot h_2^{-1} = e \cdot h_2^{-1} = h_2^{-1} \in H.$$

Thus for any $h \in H$, its inverse h^{-1} is in H.
To show closure, observe that for any $h \in H$, $h^{-1} \in H$ (from above), and that $(h^{-1})^{-1} = h$. Let $h_2 = h^{-1}$. Then

$$h_1 \cdot h_2^{-1} = h_1 \cdot (h^{-1})^{-1} = h_1 \cdot h \in H.$$

Thus for any $h1, h \in H$, we have $h_1 \cdot h \in H$. Thus H is closed.

Hence H is a subgroup of G. □

Example 9. *Every group G has at least two subgroups, the **trivial subgroup** $\{e\}$ consisting of only the identity element, and the entire group G.*

Example 10. *Let G be a group, and let $g \in G$ be an element of order n. The **cyclic subgroup of G generated by** g, denoted $\langle g \rangle$, is the set*

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g^1, g^2, g^3, \ldots\}.$$

It is isomorphic to the cyclic group $\mathcal{C}_n$.

If g has infinite order, then $\langle g \rangle \cong \mathbb{Z}$ ($\langle g \rangle$ is isomorphic to $\mathbb{Z}$).

Example 11. *More examples of subgroups:*

- *Let $d \in \mathbb{Z}$; then we can form a subgroup of $\mathbb{Z}$ using multiples of d, or $d\mathbb{Z}$.*
- *The set of rotations in the dihedral group $\mathcal{D}_n$ is a subgroup of $\mathcal{D}_n$.*

Every group homomorphism has an associated subgroup, the **kernel**, which can be a convenient check to see if the homomorphism is injective.

Definition 2.4.2: Kernel

Let $\phi : G \to G'$ be a group homomorphism. The **kernel of** ϕ, denoted $\ker(\phi)$, is the set of elements of G that are sent to the identity element of G',

$$\ker(\phi) = \{g \in G \mid \phi(g) = e'\}.$$

Example 12. *The kernel of the determinant homomorphism*

$$\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R} \setminus \{0\}.$$

is

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}.$$

We now observe two important properties of the kernel.

Proposition 2.4.2: Kernel Properties

Let $\phi : G \to G'$ be a group homomorphism.

1. $\ker(\phi)$ is a subgroup of G.
2. ϕ is injective if and only if $\ker(\phi) = \{e\}$.

Proof. We know that $\phi(e) = e'$, so $e \in \ker(\phi)$. Next, let $g_1, g2 \in \ker(\phi)$. By the homomorphism property,

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) = e' \cdot e' \in G',$$

so $g_1, g_2 \in \ker(\phi)$. Finally, for $g \in \ker(\phi)$, we know $\phi(g^{-1}) = \phi(g)^{-1} = e'^{-1} = e$, so $g^{-1} \in \ker(\phi)$ Thus, $\ker(\phi)$ is a subgroup of G.

Now, we know again that $e \in \ker(\phi)$ (since $\phi(e) = e'$). If ϕ is injective, by definition $\ker(\phi) = \{e\}$ (at most one element $g \in G$ satisfies $\phi(g) = e'$).
Now, suppose $\ker(\phi) = \{e\}$. Let $\phi(g_1) = \phi(g_2)$ for some $g_1, g_2 \in G$. Observe that $g_2^{-1} \in G$, and $\phi(g_2^{-1}) = \phi(g_2)^{-1}$. Then

$$\phi(g_1) = \phi(g_2) \implies \phi(g_1) \cdot \phi(g_2)^{-1} = \phi(g_2) \cdot \phi(g_2)^{-1} = e',$$

and so $\phi(g_1) \cdot \phi(g_2)^{-1} = \phi(g_1 \cdot g_2^{-1}) = e'$, which means $g_1 \cdot g_2^{-1} \in \ker(\phi) = \{e\}$. Hence $g_1 \cdot g_2^{-1} = e \implies g_1 = g_2$, and so ϕ is injective. □

§2.4.1 Cosets

We can use a subgroup H of a group G to break G into pieces, called **cosets of** H.

Definition 2.4.3: Cosets

Let G be a group, and let $H < G$ be a subgroup. For each $g \in G$, the (left) **coset of** H **attached to** g is the set

$$gH = \{gh \mid h \in H\}.$$

In other words, gH is the resulting set we multiply g by every element $h \in H$.

Note that gH is **not** necessarily a subgroup of H; sometimes $e \notin gH$.

We now prove several properties of cosets that help explain their importance.

Proposition 2.4.3: Properties of Cosets

Let G be a finite group, and let $H < G$.

1. Every element in G is in some coset of H.
2. Every coset of H has the same number of elements (namely, $|H|$).
3. Let $g_1, g_2 \in G$. Then the cosets g_1H and g_2H satisfy either
$$g_1H = g_2H \text{ or } g_1H \cap g_2H = \varnothing.$$
In other words, g_1H and g_2H are either equal or disjoint.

Proof. 1. Let $g \in G$. Since $e \in H$ for any subgroup $H < G$, the coset gH contains $g \cdot e = g$.

2. Let $g \in G$. To prove that the cosets gH and H have the same number of elements, we show the map
$$\begin{aligned} F : H &\longrightarrow gH \\ h &\longmapsto F(h) = gh \end{aligned}$$
is a bijective map from H to gH.
We first check that F is injective. Suppose $h_1, h_2 \in H$ satisfy $F(h_1) = F(h_2)$. Then $gh_1 = gh_2$, and multiplying by g^{-1}, we get $h_1 = h_2$. Hence F is injective.
For surjectivity, observe that every element of gH looks like gh for some $h \in H$, and $F(h) = gh$, so every element of gH is the image of some element of H. Hence F is surjective.
Thus F is bijective, so H and gH have the same number of elements. Since this is true for any $ginnG$, every coset of H has the same number of elements.

3. If $g_1H \cap g_2H = \varnothing$, we are done, so assume the two cosets are not disjoint. Then there are some elements $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2$. Since $h_1^{-1} \in H$, we rewrite this as $g_1 = g_2h_2h_1^{-1}$. Now, take any element $a \in g_1H$. a is of the form g_1h for some $h \in H$. Then
$$a = g_1h = g_2h_2h_1^{-1}h \in g_2H,$$
as H is a subgroup, so $h_2h_1^{-1}h \in H$. Hence $g_1H \subseteq g_2H$; and from above, every coset has the same number of elements, so $g_1H \subseteq g_2H \implies g_1H = g_2H$.

□

These properties lead to a fundamental divisibility property for the orders of subgroups.

Theorem 2.4.1: Lagranges Theorem

Let G be a finite group, and let $H < G$. Then the order of H divides the order of G; or, $|G| = k\,|H|\,,\ k \in \mathbb{Z}$.

Proof. We start by choosing $g_1, \ldots, g_k \in G$ so that $g_1H, \ldots, g_kH$ is a list of every different coset of H. Since every element of G is in some coset of H, we have that G is equal to the union of the cosets of H, namely
$$G = g_1H \cup \ldots \cup g_kH.$$

Additionally, we know that distinct cosets share no elements, so if $i \neq j$, then $g_iH \cap g_jH = \varnothing$. Thus the union of cosets is a disjoint union, so the number of elements in G is the sum of the number of elements in each coset:

$$|G| = |g_1H| + \ldots + |g_kH|\,.$$

But we know that every coset of H has the same number of elements, so $|g_iH| = |H|$. Thus, we get

$$|G| = k\,|H|\,.$$

Thus the order of G is a multiple of the order of H. □

Definition 2.4.4: Index

Let G be a group, and $H < G$. The **index of H in G**, denoted $(G : H)$, is the number of distinct cosets of H. In Lagrange's Theorem, the index $(G : H) = k$; so

$$|G| = (G : H)\,|H|\,.$$

Corollary 2.4.1: Extension of Lagrange's Theorem to Finite Groups

Let G be a finite group, and let $g \in G$. Then the order of g divides the order of G.

Proof. The order of the subgroup $\langle g \rangle$ generated by G is equal to the order of the element g, and Lagrange's Theorem tells us that the order of $\langle g \rangle$ divides the order of G. □

We now give one application of Lagrange's Theorem, which marks the beginning of a long and ongoing mathematical journey that strives to classify finite groups according to their orders.

Proposition 2.4.4: Prime-Ordered Groups

Let p be a prime, and let G be a finite group of order p. Then G is isomorphic to the cyclic group $\mathcal{C}_p$.

Proof. Since $p \geq 2$, we know that G contains more than just the identity element, so we choose some non-identity element $g \in G$.
By Lagrange's Theorem, we know that the order of the subgroup $\langle g \rangle$ divides the order of G. But since $|G| = p$ is prime, the order of $\langle g \rangle$ is either 1 or p; and since $\langle g \rangle$ contains both e and g (and so $\langle g \rangle > 1$), we know $|\langle g \rangle| = p = |G|$. Thus the subgroup $\langle g \rangle$ has the same number of elements as the full group, so they are equal: $\langle g \rangle = G$.
Now, we denote the cyclic group $\mathcal{C}_p = \{g_0, g_1, \ldots, g_{p-1}\}$. We obtain an isomorphism

$$\begin{aligned} C_p &\longrightarrow G \\ g_i &\longmapsto g^i. \end{aligned}$$

Thus G is isomorphic to $\mathcal{C}_p$. □

Remark 3. *The vast theory of finite groups has many fascinating (and frequently unexpected) results, with easy to understand statements, yet surprisingly intricate proofs. Two such theorems are stated.*

Theorem 2.4.2

Let p be a prime number, and let G be a group of order p^2. Then G is an Abelian group.

On the other hand, we know that there exist non-Abelian groups of order p^3. For instance, $\mathcal{D}_4$ and the quaternion group $\mathcal{Q}$ are non-Abelian groups of order $8 = 2^3$.
The next result is a partial converse of Lagrange's Theorem.

Theorem 2.4.3: Sylow's Theorem

Let G be a finite group, let p be a prime, and suppose p^n divides $|G|$ for some power $n \geq 1$. Then G has a subgroup or order p^n.

One might hope, more generally, that if d is any number that divides the order of G, then G has a subgroup of order d. Unfortunately, this is not true; however, we have not yet seen a counterexample.
Both theorems will be proved later.

§2.5 Products of Groups

Subgroups provide a way to break complicated objects (groups) down into smaller, simpler pieces. We now look at a way in which two smaller groups can be used to build a larger group.

Definition 2.5.1: Products of Groups

Let G_1, G_2 be groups. The **product** of G_1 and G_2 is the group whose elements consist of ordered pairs

$$G_1 \times G_2 = \{(a, b) \mid a \in G_1 \text{ and } b \in G_2\},$$

and whose group operation is performed separately on each component. In other words, if the group operation of $G_1 \times G_2$ is $*$, the group operation of G_1 is $\cdot$, and the group operation of G_2 is $\circ$, we have

$$(a_1, b_1) * (a_2, b_2) = (a_1 \cdot a_2, b_1 \circ b_2).$$

It is clear that the identity element of $G_1 \times G_2$ is (e_1, e_2), and the inverse of an element $(a, b) \in G$ is given by

$$(a^{-1}, b^{-1}).$$

More generally, we can take any list of groups $G_1, \ldots, G_n$ and form the product

group

$$G_1 \times \ldots \times G_n.$$

Remark 4. *We observe that $G = G_1 \times G_2$ has order $|G_1| \cdot |G_2|$.*

Example 13. *For any non-zero numbers m, n, there is a homomorphism*

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ a \mod (mn) &\longmapsto (a \mod m, a \mod n). \end{aligned}$$

We claim that if $\gcd(m,n) = 1$, then it is an isomorphism. To see this, suppose that $a \mod mn$ is in the kernel. Then

$$a \equiv 0 \mod m \text{ and } a \equiv 0 \mod n.$$

In other words, a is divisible by both m and n, and then the assumption that $\gcd(m,n) = 1$ implies that a is divisible by mn. Thus $a \equiv 0 \mod mn$, which proves that the kernel of the homomorphism is $\{0\}$ (and thus the homomorphism is injective). Further, since the finite set $\mathbb{Z}/mn\mathbb{Z}$ has the same number of elements as $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}/mn\mathbb{Z}$ has mn elements, while $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has $m \cdot n = mn$ elements), so it is surjective, and thus the homomorphism is an isomorphism.

One interpretation of this example is that it tells us that if $\gcd(m,n) = 1$, then the large group $\mathbb{Z}/mn\mathbb{Z}$ may be broken down into the product of two smaller groups $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. Repeated applications demonstrate that any finite cyclic group is isomorphic to the product of cyclic groups of prime power order. The following theorem extends this to all finite Abelian groups.

Theorem 2.5.1: Structure Theorem for Finite Abelian Groups

Let G be a finite Abelian group. Then there are integers $m_1, \ldots, m_r$) so that

$$G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z}).$$

Example 14. *(**Projects and Inclusions**) Products of groups come with two natural **projection homomorphisms***

$$\begin{aligned} p_1 : G_1 \times G_2 &\longrightarrow G_1, & p_2 : G_1 \times G_2 &\longrightarrow G_2, \\ (a,b) &\longmapsto a, & (a,b) &\longmapsto b, \end{aligned}$$

*and two natural **inclusion homomorphisms***

$$\begin{aligned} \iota_1 : G_1 &\longrightarrow G_1 \times G_2 & \iota_2 : G_2 &\longrightarrow G_1 \times G_2 \\ a &\longmapsto (a, e_2) & b &\longmapsto (e_1, b). \end{aligned}$$

The inclusion maps are clearly injective, but the projections have kernels

$$\ker(p_1) = \{e_1\} \times G_2 \text{ and } \ker(p_2) = G_1 \times \{e_2\}.$$

Chapter 3

Rings: Part I

Unlike groups, which were completely new, the concept of a **ring** is mildly familiar! Some examples of rings include:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings ($\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are actually **fields**, a special type of ring; such is a discussion for later)
- The set of integers modulo m is a ring

These examples all share something in common: they each have two operations, "addition" and "multiplication", and each operation individually satisfies some axioms, along with the g̃reat and powerfuld̃istributive law.
In general, a ring is a set with two operations satisfying a bunch of axioms that are modeled after the properties of addition and muliplication of integers. We will later formalize this; but first, a little number theory.

§3.1 Review of Number Theory

§3.1.1 Equivalence Relations

We first introduce the notion of **equivalence relations**; while not strictly related to number theory, equivalence relations will be significant for modular arithmetic.

Definition 3.1.1: Equivalence Relations

An **equivalence relation** on a set S is a relation "$\sim$" satisfying

1. **Reflexivity**: For $a \in S$, $a \sim a$
2. **Symmetry**: For $a, b \in S$, $a \sim b$ implies $b \sim a$
3. **Transitivity**: For $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

$a \sim b$ means a is "related" to b; $a \not\sim b$ means a is "not related" to b.
Given an $a \in S$, the **equivalence class** of a is

$$S_a = \{b \in S \mid b \sim a\}.$$

Note that S_a is never empty; it always contains a.

Some examples of equivalence relations are equality ($=$) and congruence $\mod m$; on the other hand, order (e.g. $\leq$) is **not** an equivalence relation (symmetry does not hold). We now look further into the congruence $\mod m$ equivalence relation.

Example 15. *Given $a \in \mathbb{Z}$, $b \equiv a \mod m$ iff*

$$n|b-a \iff b-a = kn,\ k \in \mathbb{Z} \iff b = a+kn.$$

So $\mathbb{Z}_a$ actually forms a coset of $n\mathbb{Z}$:

$$\begin{aligned}\mathbb{Z}_a &= \{b \in \mathbb{Z} \mid b \equiv a \mod m\} \\ &= \{a+kn \mid k \in \mathbb{Z}\} \\ &= a + n\mathbb{Z}.\end{aligned}$$

That is, each equivalence class for congruence $\mod m$ is actually a coset of $m\mathbb{Z}$ in $\mathbb{Z}$:

$$\mathbb{Z}/m\mathbb{Z} = \text{ set of cosets of } m\mathbb{Z} \text{ in } \mathbb{Z}\ .$$

Theorem 3.1.1

Let S be a set with an equivalence relation $\sim$. Then

1. If $a, b \in S$, then either
$$S_a \cap S_b = \varnothing \text{ or } S_a = S_b.$$
2. Let $\{C_i\}_{i \in I}$ be the disjoint equivalence classes of S. Then
$$S = \coprod_{i \in I} C_i.$$
In particular, if S is finite, then
$$|S| = |C_1| + \ldots + |C_n|\,.$$

§3.1.2 Modular Arithmetic

We first observe an important characteristic of the gcd:

Proposition 3.1.1

Given integers u, v, there exists integers x, y such that

$$ux + vy = \gcd u, v.$$

§3.2 Abstract Rings and Ring Homomorphisms

Definition 3.2.1: Rings

A **ring** R is a set with two operations, generally called **addition** and **multipli-**

cation and written

$$\underbrace{a+b}_{\text{addition}} \qquad \text{and} \qquad \underbrace{a\cdot b \text{ or } ab}_{\text{multiplication}}$$

satisfying the following axioms:

1. The set R with addition law $+$ is an Abelian group, with identity 0 (or 0_R).
2. The set R with multiplication law $\cdot$ is a **monoid** (associative, identity, **but no inverse**), with identity 1 (or 1_R[a]).
3. **Distributive Law**: For all $a,\ b,\ c \in R$, we have
$$a\cdot(b+c) = a\cdot b + a\cdot c \qquad \text{and} \qquad (b+c)\cdot a = b\cdot a + c\cdot a.$$
4. If, in addition to these three properties, $a\cdot b = b\cdot a$ for all $a,\ b \in R$, then R is a **commutative** ring.

[a] to avoid the trivial ring, we require $1_R \neq 0_R$; however, this is not strictly required

Experience with the integers seems to suggest that $0_R \cdot a = 0_R$, and $(-a)\cdot(-b) = a\cdot b$; yet why are these true? 0_R is the definition of the identity element for *addition*, so why should it say anything about *multiplication*? Similarly, $-a$ relates to the definition of *additive* inverse, but what does that tell us about its product with other elements in R? To show these intuitively obvious claims, we need the distributive law.

Proposition 3.2.1

1. $0_R \cdot a = 0_R$ for all $a \in R$.
2. $(-a)\cdot(-b) = a\cdot b$ for all $a,\ b \in R$. In particular, we have $(-1_R)\cdot a = -a$.

Proof. 1. Note that $1_R = 0_R + 0_R$. Then

$$\begin{aligned} a &= 1_R \cdot a && [1_R \text{ is the muliplicative identity }] \\ &= (1_R + 0_R)\cdot a && [\text{ from above }] \\ &= 1_R\cdot a + 0_R \cdot a && [\text{ from distributivity }] \\ &= a + 0_R \cdot a \end{aligned}$$

.

Adding $-a$ to both sides, we get

$$0_R = 0_R + 0_R \cdot a,$$

and so $0_R \cdot a = 0_R$.

2. First, we show that $(-1_R)\cdot a = -a$:

$$\begin{aligned} a + (-1_R)\cdot a &= 1_R \cdot a + (-1_R)\cdot a \\ &= (1_R + -1_R)\cdot a \\ &= 0_R \cdot a \\ &= 0_R. \end{aligned}$$

Hence $(-1_R) \cdot a$ is the inverse of a, and so $-a = (-1_R) \cdot a$.

Now, observe that $-ab = (-a)b$ (this proof is left as an exercise for the reader). Then

$$\begin{aligned}(-a) \cdot (-b) + -ab &= (-a) \cdot (-b) + (-a) \cdot b \\ &= (-a) \cdot (-b + b) \\ &= (-a) \cdot 0_R \\ &= 0_R.\end{aligned}$$

Thus $(-a) \cdot (-b)$ is the inverse of $-ab$, and so $(-a) \cdot (-b) = ab$.

□

Just like groups, we want to investigate maps

$$\phi : R \to R'$$

from one ring to another that respect the *ring-i-ness* of R and R'. Since rings are characterized by their addition and multiplication properties, we get the following definition.

Definition 3.2.2: Ring Homomorphisms

Let R, R' be rings. A **ring homomorphism** from R to R' is a function $\phi : R \to R'$ satisfying[a]

1. $\phi(1_R) = 1_{R'}$
2. $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$
3. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in R$

The **kernel** of ϕ is the set of elements that are sent to 0:

$$\ker(\phi) = \{a \in R \mid \phi(a) = 0_{R'}\}.$$

As with groups, R and R' are **isomorphic** if here is a bijective ring homomorphism $\phi : R \to R'$, and we call such a map an **isomorphism**.

[a] we have the first axiom to disallow the boring and trivial zero map $\phi : R \to R'$, $\phi(a) = 0_{R'}$.