Abstract Algebra

Muchang Bahng

Spring 2024

Contents

With set theory, we have established what sets, along with functions and relations are. Abstract algebra extends on this by studying *algebraic structures*, which are sets S with specific *operations* acting on their elements. This is a very natural extension and to be honest does not require much motivation. Let's precisely define what operations are.

Definition 0.1 (Operation)

A **p-ary operation**[a] $*$ on a set A is a map

$$* : A^p \longrightarrow A \tag{1}$$

where A^p is the p-fold Cartesian product of A. In specific cases,

1. If $p = 1$, then $*$ is said to be **unary**.
2. If $p = 2$, then $*$ is **binary**.

We can consider for $p > 2$ and even if p is infinite.

[a] or called an operation of arity p.

Definition 0.2 (Algebraic Structure)

An **algebraic structure** is a nonempty set A with a finite set of operations $*_1, \dots, *_n$ and satisfying a finite set of axioms. It is written as $(A, *_1, \dots, *_n)$.

If we consider functions between algebraic structures $f : A \to B$, there are some natural properties that we would like f to have.

Definition 0.3 (Preservation of Operation)

Given algebraic structures (A, μ_A), (B, μ_B), where μ_A and μ_B have the same arity p, a function $f : A \to B$ is said to **preserve the operation** if for all $x_1, \dots, x_p \in A$,

$$f(\mu_A(x_1, \dots, x_p)) = \mu_B(f(x_1), f(x_2), \dots, f(x_p)) \tag{2}$$

Functions that preserve operations are generally called *homomorphisms*. However, given that preservation is defined with respect to each operation, a map may preserve one operation but not the other. Therefore, we will formally define homomorphisms for each class of algebraic structures we encounter.

Definition 0.4 (Commutative, Associative Operations)

A binary operation $\cdot : A \times A \to A$ is said to be

1. **associative** if for all $a, b, c \in A$, $(ab)c = a(bc)$.
2. **commutative** if for all $a, b \in A$, $ab = ba$.

Associativity is a particularly important property that we would like to have, and it is quite rare to work with algebraic structures that don't have associativity. It basically states that when doing an operation sequentially over 3 elements, it doesn't matter if we evaluate ab or bc first. Therefore, associativity allows us to throw the parentheses away since the evaluated result does not change.

Commutativity on the other hand is not as prevalent. It simply tells us that we can "swap" terms when evaluating. This usually is a another nice convenience, and in the theory of rings commutativity is very prevalent. Either way, in both of these scenarios we can extend to any finite sequence of operations.

Theorem 0.1 (Generalized Associativity)

Given that a binary operation $\cdot$ is associative on a set S, it is always the case that for any finite collection $a_1, \dots, a_n$, the value $a_1 \dots a_n$ is unique.

Proof.

We prove by strong induction on n from $n = 3$. Clearly $(a_1a_2)a_3 = a_1(a_2a_3)$ by definition of associativity. The rest is a bit tedious but is mentioned in Jacobson's *Basic Algebra 1*.

Theorem 0.2 (Generalized Commutativity)

Given that a binary operation $\cdot$ is commutative and associative on a set S, with $\alpha = a_1 + \dots + a_n$, we have

$$\alpha = a_{i_1} + \dots + a_{i_n} \tag{3}$$

for any permutation $(i_1, \dots, i_n)$ of $(1, \dots, n)$.

Now that we've gotten these out of the way, we can start talking about algebraic structures. I've went through 4 main textbooks, plus Google and talking to friends/professors in creating these notes.

1. Vinberg's *A Course in Algebra*.
2. Nathan Jacobson's *Basic Algebra 1*, given to me by Marty.
3. Ted Shifrin's *Abstract Algebra, A Geometric Approach*, used in Duke Math 401.
4. Dummit and Foote's *Abstract Algebra, 3rd Edition*, used in Duke Math 501.

1 Group-Like Structures

1.1 Semigroups and Monoids

Now the endowment of some structures gives rise to the following. Usually, we will start with the most general algebraic structures and then as we endow them with more structure, we can prove more properties. Let's talk about the most basic type of algebraic structure. If you have a set S and some associative operation on it, we have a semigroup.

Definition 1.1 (Semigroup)

A **semigroup** $(S, \cdot)$ is a set S with an associative binary operation

$$\cdot : S \times S \to S \tag{4}$$

Example 1.1 (Continuous Time Markov Chain)

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $(S, \mathcal{S})$ a measurable space. Then, a homogeneous continuous-time Markov chain is a stochastic process $\{X_t\}_{t\geq 0}$ taking values in S (i.e. $X_t : \Omega \to S$) satisfying the **Markov property**: for every bounded measurable f and and $t, s \geq 0$,

$$\mathbb{E}[f(X_{t+s}) \mid \{X_r\}_{r\leq t}] = \mathbb{E}[f(X_{t+s}) \mid X_t] = (P_s f)(X_t) \tag{5}$$

The set $\{P_t\}_{t\geq 0}$ with the composition operation gives us the *Markov semigroup*.

To be honest the above example is the only time I have every seen a semigroup come up, so we proceed immediately to the next structure.

Definition 1.2 (Monoid)

A **monoid** $(M, \cdot, e)$ is a semigroup with an identity element $e \in M$ such that given a $m \in M$

$$e \cdot m = m \cdot e = m \tag{6}$$

We first should ask whether the identity is unique in a monoid. It turns out it is.

Lemma 1.1 (Uniqueness of Monoid Identity)

The identity e of a monoid M is unique.

Proof.

Assume not, i.e. there are 2 identities $e \neq e'$. But then

$$e = ee' = e' \implies e = e' \tag{7}$$

where the implication follows from transitivity of equivalence relations.

From set theory, we have directly worked with two examples of monoids.

Example 1.2 (Set Operations)

Let S be any nonempty set. Then $(2^S, \cup, \emptyset)$ and $(2^S, \cap, S)$ are monoids. So it seems that there are flavors of algebra that aren't really separable from set theory.

Definition 1.3 (Submonoid)

Given a monoid $(M, *)$, let $M' \subset M$. If the restriction of $*$ to $M' \times M'$ is closed in M', then we can define the **submonoid** $(M', *)$.

It may seem like the identity of a submonoid must be the identity of the monoid, but this is not always the case. We may take a subset $M' \subset M$ such that $\cdot$ is closed in M' and there may be some $e' \in M', e' \neq e$ such that it acts like an identity on M'.

Example 1.3 (Identities of Submonoids May Not be the Same)

Let $(M, \times, I)$ be the monoid of 2×2 matrices over $\mathbb{R}$ with the identity matrix I, and let M' be the set of matrices of form

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \text{ for } a \in \mathbb{R}, \qquad I' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{8}$$

Then $(M', \times, I')$ is a submonoid with a different identity element.

Example 1.4 ($\mathbb{N}$ is a Monoid)

The natural numbers, defined here are a monoid. More specifically,

1. $(\mathbb{N}, +, 0)$ is a monoid under addition.
2. $(\mathbb{N}, \times, 1)$ is a monoid under multiplication.
3. $(2\mathbb{N}, +, 0)$ is a monoid under addition, where $2\mathbb{N}$ is the set of all even numbers.
4. $2\mathbb{N}$ cannot be a monoid since $1 \notin 2\mathbb{N}$.

Definition 1.4 (Monoid of Transformations)

Given a set S, consider the set of all functions $S^S \coloneqq \{f : S \to S\}$. Then, with function composition $\circ$, $(S^S, \circ)$ is a monoid with the identity function $e : x \mapsto x$ as the identity element. This is called the **monoid of transformations** of S.

Theorem 1.1 (Cardinality of Monoid of Transformations)

If $|S| = n$, then the monoid of transformations has cardinality n^n.

1.2 Groups

Now we look at a specific case of monoids where invertibility is defined. The existence of inverses produces a whole suite of interesting properties, as we will see.

Definition 1.5 (Group)

A **group** $(G, \cdot)$ is a set with binary operation $x \cdot y$—also written as xy—having the following properties.

1. *Closure.* $x, y \in G \implies xy \in G$[a]
2. *Associativity.* $\forall x, y, z \in G, x(yz) = (xy)z$
3. *Identity.* $\exists e \in G$ s.t. $\forall x \in G, xe = ex = x$
4. *Inverses.* $\forall x \in G\ \exists x^{-1} \in G$ s.t. $xx^{-1} = x^{-1}x = e$

The **order** of a group is the cardinality $|G|$. An **abelian group** $(A, +)$ is a group where $+$ is commutative.[b]

[a] but not necessarily $xy = yx$

[b] Note that I switched the notation from $*$ to $+$. By convention and to avoid confusion, $+$ denotes commutative operations.

This is an extremely simple structure, and the first thing we should prove is the uniqueness of the identity and inverses.

Lemma 1.2 (Uniqueness of Identity and Inverse)

The identity and the inverse is unique, and for any a, b, the equation $x * a = b$ has the unique solution $x = b * a^{-1}$.

Proof.

Assume that there are two identities of group $(G, *)$, denoted e_1, e_2, where $e_1 \neq e_2$. According to the properties of identities, $e_1 = e_1 * e_2 = e_2 \implies e_1 = e_2$.
As for uniqueness of a inverses, let a be an element of G, with its inverses a_1^{-1}, a_2^{-1}. Then,

$$\begin{aligned} a * a_1^{-1} = e &\implies a_2^{-1} * \left(a * a_1^{-1}\right) = a_2^{-1} * e \\ &\implies \left(a_2^{-1} * a\right) * a_1^{-1} = a_2^{-1} \\ &\implies e * a_1^{-1} = a_2^{-1} \end{aligned}$$

Since the inverse is unique, we can operate on each side of the equation $x * a = b$ to get $x * a * a^{-1} = b * a^1 \implies x * e = x = b * a^{-1}$. Clearly, the derivation of this solution is unique since the elements that we have operated on are unique.

At this point, we can see that for each group there is a corresponding "multiplication table" defined by the operation. For example, we can create a set of 6 elements $\{r_0, r_1, r_2, s_0, s_1, s_2\}$ and define the operation $\times$ as the following.

$\times$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Figure 1: Multiplication table for some group. Note that we can only write such a table explicitly for a group of finite elements. But even for arbitrary groups, we should think of the operation completely defining a possibly "infinite" table.

It is clear that in an abelian group, the multiplication table must be symmetric across the diagonal.

Example 1.5 (Familiar Groups)

So what are some examples of groups?

1. $(\mathbb{N}, +)$ is not a group since $3 \in \mathbb{N}$ but $-3 \notin \mathbb{N}$. It is a commutative monoid.
2. $(\mathbb{N}, \times)$ is not a group but is a commutative monoid.
3. $(\mathbb{Z}, +)$ is an abelian group.
4. $(\mathbb{Z}, \times)$ is not a group.
5. $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \times)$ are both abelian groups.
6. $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$ are both abelian groups.
7. The set of all invertible $n \times n$ matrices with matrix multiplication, denoted $(\mathrm{GL}(\mathbb{R}^n), \times)$ is a non-abelian group.
8. The set of all functions on a given interval $[a, b]$ is abelian with respect to addition, defined as

$$(f+g)(x) \equiv f(x) + g(x).$$

Example 1.6 (Group of Invertible Elements of a Monoid)

Given $x \in (M, \cdot, e)$, let x be **invertible** if there exists $x^{-1} \in M$ s.t. $xx^{-1} = x^{-1}x = e$. Then, the submonoid M' of invertible elements of M is a group. This must be proved.

1. *Closure.* If $x, y \in M'$, then $x^{-1}, y^{-1} \in M'$ since $(x^{-1})^{-1} = x$. Therefore $y^{-1}x^{-1} = (xy)^{-1} \in M'$, and so $xy \in M'$.
2. *Identity.* $e^{-1} = e$ so $e \in M'$.
3. *Inverses.* Exists by definition.
4. *Associativity.* Is inherited from associativity of $\cdot$ in M.

Let's prove a little more about groups so that we have more tools for manipulation.

Lemma 1.3 (Properties of Group Operation)

Given $a, b, c \in G$,

1. $ab = cb \implies a = c$.
2. $\forall a \in G$, $(a^{-1})^{-1} = a$.
3. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

TBD.

Theorem 1.2 ()

Given group G, $(ab)^2 = a^2b^2$ for all $a, b \in G$ iff G is abelian.

Definition 1.6 (Subgroup)

Given group $(G, *)$, a **subgroup** $(H, *)$ is a group such that $H \subset G$. H is called a **proper subgroup** if $H \subsetneq G$.

Theorem 1.3 ()

If $H, K \subset G$ are subgroups, then $H \cap K$ is a subgroup.

Finally we end with an analogous result of the monoid of transformations. The problem with these transformations is that they may not be invertible, but if they are, i.e. bijective, then we can endow them with a group structure.

Definition 1.7 (Group of Transformations)

Given a set S, $\text{Sym}(S)$ is the group of bijective maps $f : S \to S$ with composition as the operator. This is also called the **symmetric group** of S.

Lemma 1.4 (Cardinality of Group of Transformations)

If S has cardinality n, then the order of $\text{Sym}(S)$ is $n!$.

1.3 Group Homomorphisms

At this point, we would like to try and classify groups (e.g. can we find *all* possible groups of a finite set?). But consider the two groups.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Figure 2: Two isomorphic groups.

These groups have different elements, but the operation behaves in exactly the same way between them (it may be a little harder if I relabeled the elements or permuted the rows/columns). Since we can trivially make arbitrary sets there really isn't much meaning to having two versions of the same group (at least in the algebraic sense). Therefore, these groups should be labeled "equivalent" in some way, and we will precisely define this notion now.

Definition 1.8 (Group Homomorphism)

Let $(G, \circ)$ and $(H, *)$ be two groups. The mapping $f : (G, \circ) \longrightarrow (H, *)$ is a **group homomorphism** if for all $a, b \in G$,

$$f(a \circ b) = f(a) * f(b) \tag{9}$$

Furthermore,

1. A **group isomorphism** is a bijective group homomorphism, and we call groups M, N **isomorphic**, denoted $M \simeq N$, if there exists an isomorphism between them.
2. An **endomorphism** is a homomorphism from a group to itself.
3. An **automorphism** is a isomorphism from a group to itself.

It turns out that from the simple property that $f(ab) = f(a)f(b)$, it also maps identities to identities, and inverses to inverses!

Lemma 1.5 (Homomorphisms Maps Identities/Inverses to Identities/Inverses)

Given a homomorphism $f : (G, *) \to (H, \times)$ and $a \in G$,

$$f(e_G) = e_H, \qquad f(a^{-1}) = f(a)^{-1} \tag{10}$$

Proof.

Let $a \in G$. Then

$$f(a) = f(ae_G) = f(a)f(e_G) \implies e_H = f(a)^{-1}f(a) = f(a)^{-1}f(a)f(e_G) = f(e_G) \tag{11}$$

To prove inverses, we see that

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H \tag{12}$$

from above, and this implies that $f(a^{-1}) = f(a)^{-1}$. We can also do this with right hand side multiplication.

Example 1.7 (Exponential Map)

The map $a \mapsto 2^a$ is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ since

$$2^{a+b} = 2^a \times 2^b \tag{13}$$

which is proved in my real analysis notes when constructing the exponential map on the reals.

Example 1.8 (Determinant)

The determinant $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$ is a homomorphism because of the product rule for determinants.

Example 1.9 (Projection onto Unit Circle)

Given $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ with $\times$ and $S^1 = \{x \in \mathbb{C} \mid |x| = 1\}$ (which is a group under multiplication), the map $f : \mathbb{C}^* \to S^1$ defined $f(z) = z/|z|$ is a group homomorphism since

$$f(z_1 z_2) = \frac{z_1 z_2}{|z_1 z_2|} = \frac{z_1 z_2}{|z_1||z_2|} = f(z_1) f(z_2) \tag{14}$$

Therefore, we can see that an isomorphism is really just a "renaming" of the elements, which aligns with our view of equivalence as above. Not only does it renamee the elements, but it preserves all the algebraic properties of the group and each element.

Theorem 1.4 (Preservation of Properties in Isomorphism)

If $f : G \to H$ is an isomorphism, then

1. f^{-1} is also an isomorphism.
2. $|G| = |H|$.
3. $\forall a \in G$, $\mathrm{ord}(a) = \mathrm{ord}(f(a))$.
4. G is abelian $\implies$ H is abelian.

Proof.

Listed.

1. Since f is bijective by definition, f^{-1} is well-defined and bijective as well. Now we show that f^{-1} is a group homomorphism. Given $c, d \in H$, take

$$f\big(f^{-1}(c), f^{-1}(d)\big) = f\big(f^{-1}(c)\big)\, f\big(f^{-1}(d)\big) = cd \tag{15}$$

   where the first equality follows since f is a homomorphism, and the second since f^{-1} is the inverse mapping. Now mapping both sides through f^{-1}, we get

$$f^{-1}(c) f^{-1}(d) = f^{-1}(cd) \tag{16}$$

   and so f^{-1} is a homomorphism.
2. This is trivial by bijectivity.
3. TBD.
4. Let $c, d \in H$. Then $c = f(a), d = f(b)$ for some $a, b \in G$, and so $cd = f(a)f(b) = f(ba) = f(b)f(a) = dc$.

A trivial example is the identity map, which is an automorphism. But can we generalize this a bit better?

Theorem 1.5 ()

Let G be a group with $a \in G$. Then the following is an automorphism on G.

$$\phi : G \longrightarrow G,\ \phi(x) = axa^{-1} \tag{17}$$

Proof.

The map $\psi : G \longrightarrow G,\ \psi(x) = a^{-1}xa$ is clearly the inverse of ϕ, with $\phi\psi = \psi\phi = I$ for all $x \in G \implies \phi$ is bijective. Secondly, $\phi(x)\phi(y) = axa^{-1}aya^{-1} = a(xy)a^{-1} = \phi(xy) \implies \phi$ preserves the group structure.

Definition 1.9 (Kernel)

Given group homomorphism $f : G \to H$, the **kernel** of f is the preimage of the identity.

$$\ker(f) \coloneqq \{g \in G \mid f(g) = e_H\} \tag{18}$$

Theorem 1.6 (Kernels are Subgroup)

Given a group homomorphism $f : G \to H$,
1. $\ker(f)$ is a subgroup of G.
2. f is injective $\iff \ker(f) = \{e_G\}$.

Proof.

For the first part, we prove the properties of a group. To show closed, consider $a, b \in \ker(f)$. Then $f(ab) = f(a)f(b) = e_He_H = e_H \implies ab \in \ker(f)$. Since $f(e_G) = e_H$, $e_G \in \ker(f)$. If $a \in \ker(f)$, then $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \implies a^{-1} \in \ker(f)$. Finally associativity follows from associativity of the supgroup.
For the second part, we prove bidirectionally.
1. $(\to)$. Since f is injective, $f(a) = f(b) \implies a = b$. Let $a \in \ker(f)$. Then $f(a) = e_H$, and so $f(e_G) = e_H = f(a)$. By injectivity, $a = e_G$, and so $\ker(f) = \{e_G\}$.
2. $(\leftarrow)$. Let $a, b \in G$ s.t. $f(a) = f(b)$. Then $f(a)f(b)^{-1} = e_H \implies af(a)f(b^{-1}) = f(ab^{-1}) = e_H \implies ab^{-1} \in \ker(f)$. But by hypothesis $\ker(f) = \{e_G\} \implies ab^{-1} = e_G \implies a = b$.

1.4 Group Presentations

A group G may be very abstract and complicated, and so working with all its elements can be a bit painful. It would be more useful to work with a smaller subset S of G that can completely characterize G.[1] We would like to formalize this notion, which will be very useful later on. For now, let's start off with a simple element $a \in G$, and perhaps we can consider the elements

$$\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots \tag{19}$$

However, there are two interpretations to a^{-2} is it the inverse of a^2 or $a^{-1}a^{-1}$? It turns out that these are equivalent.

Lemma 1.6 (Power to an Integer is Well-Defined)

For all $n \in \mathbb{N}$,

$$(a^{-1})^n = (a^n)^{-1} \tag{20}$$

[1] Note that this is similar to the basis that generates a topology.

Proof.

We prove by induction on n. It is trivially true for $n = 1$. Now given that it is true for some $n \in \mathbb{N}$, we have

$$(a^{-1})^{n+1} = (a^{-1})^n a^{-1} = (a^n)^{-1} a^{-1} = (aa^n)^{-1} = (a^{n+1})^{-1} \tag{21}$$

Therefore it makes sense to just write it as a^{-n}. It may or may not be the case that a may cycle back to itself for some n, i.e. $a = a^n$.

Definition 1.10 (Order of an Element)

The **order** of a group element $a \in G$ is the minimum number $n \in \mathbb{N}$ s.t. $a = a^n$, denoted $|a|$ or $\text{ord}(a)$.[a]

[a] Note that this is different from the order of a group. This is confusing but is the convention.

Now the set of all multiples of a may or may not be the group, but if we take a certain subset of these elements and take all multiples of all combinations of them, we may have better coverage of the group.

Definition 1.11 (Word)

A **word** is any written product of group elements and inverses. They are generally in the form

$$s_1^{\epsilon_1} s_2^{\epsilon_2} s_3^{\epsilon_3} ... s_k^{\epsilon_k}, \text{ where } e_i \in \mathbb{Z} \tag{22}$$

e.g. given a set $\{x, y, z\}$, $xy, xz^{-1}yyx^{-2}, ...$ are words.

Definition 1.12 (Generating Set)

The **generating set** $\langle S \rangle$ of a group G is a subset of G such that every element of the group can be expressed as a word of finitely many elements under the group operations. The elements of the generating set are called **generators**.

Definition 1.13 (Group Presentations)

The **free group** F_S over a given set S consists of all words that can be built from elements of S. Often with this generating set S, we have a set of relations R that tell us which elements are equal. The **group presentation** writes both S and R in the form

$$\langle S \mid R \rangle \tag{23}$$

Theorem 1.7 ()

If every element other than the identity has order 2, then G is abelian.

With these group presentations we can start identifying specific groups. Let's start with the simplest group with one generator and zero/one relation: the cyclic group.

Definition 1.14 (Cyclic Group)

A **cyclic group** is a group generated by a single element.

1. In an infinite cyclic group, there is no relation and we write

$$Z \coloneqq \langle a \rangle = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\} \tag{24}$$

2. In a finite cyclic group, there exists a $n \in \mathbb{N}$ such that $a^n = e$ and we write

$$Z_n := \langle a \mid a^n = e \rangle = \{e, a, a^2, \dots, a^{n-1}\} \tag{25}$$

Example 1.10 (Cyclic Groups)

Here are some examples of cyclic groups.

1. $(\mathbb{Z}_n, +)$, the integers mod n, is a cyclic group of order n, generated by 1.[a]
2. The nth roots of unity in $\mathbb{C}$ is a cyclic group of order n, generated by the counterclockwise rotation $e^{2\pi/n}$.
3. The set of discrete angular rotations in $SO(2)$, in the form of

$$R = \left\{ \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \;\middle|\; \theta \in \left\{ \frac{2\pi}{n} k \right\}_{k=0}^{n-1} \right\} \tag{26}$$

4. $(\mathbb{Z}, +)$ is an infinite cyclic group.

[a] In fact, the generator of $\mathbb{Z}_n$ can be any integer relatively prime to n and less than n.

That's really it for cyclic groups, and to make things simpler, there is a complete characterization of them.

Theorem 1.8 (Cyclic Groups are Unique up to Order)

Given a cyclic group, Z or Z_n

1. If it is finite, then $(Z_n, +) \simeq (\mathbb{Z}_n, +) \simeq \langle 1 \rangle$.
2. If it is infinite, then $(Z, +) \simeq (\mathbb{Z}, +) \simeq \langle 1 \rangle$.

Proof.

Therefore, we have completely characterized all cyclic groups! Furthermore, cyclic groups are contained in the sense that any subgroup is also a cyclic group. So you won't find any weird groups embedded in cyclic groups; you can safely assume that they are all cyclic. The proof for this is quite a useful technique, where we try to arrive at a contradiction between some minimally chosen k and the remainder r that must be less than k.

Theorem 1.9 (Subgroups of Cyclic Groups)

Any subgroup of a cyclic group is cyclic.

Proof.

Let $G = \langle a \rangle$ be a cyclic group. Then given a subgroup H, we must have $e \in H$. If there are no other elements we are done, and if there are extra elements then let $k \in \mathbb{N}$ be the smallest natural (which exists due to the well-ordering principle) such that $a^k \in H$. Now we claim that $H = \langle a^k \rangle$. Given any $a^n \in H$, we can use Euclidean algorithm on the integers to write $n = qk + r$ for $0 \leq r < k$. Therefore,

$$a^n = a^{qk+r} = (a^k)^q \cdot a^r \implies a^r = a^n (a^k)^{-q} \tag{27}$$

$$\implies a^r \in H \tag{28}$$

but this contradicts the fact that k is minimal, and so $r = 0$. This means that $a^n = (a^k)^q$ and so a^n is a multiple of a^k.

Example 1.11 (Integers to Even Integers)

Let $2\mathbb{Z}$ denote the set of all even integers with addition. Then we can verify that this is a group, and

$$\mathbb{Z} \simeq 2\mathbb{Z} \tag{29}$$

Theorem 1.10 (Homomorphisms between Cyclic Groups)

There are precisely $\gcd(n, m)$ homomorphisms $f : Z_n \to Z_m$.

Proof.

The next type of group we will focus on is the dihedral group. These are usually introduced as the symmetry group (group of rotations and flips you can do on a polygon) to preserve its symmetry. However, it seems a bit disconnected with cyclic groups and group presentations, so I introduce it in the following way. Once I define it, I connect to its geometric interpretations in the following examples.

Definition 1.15 (Dihedral Group)

The **Dihedral Group** of order $2n$ is the group

$$\text{Dih}(n) \coloneqq \langle r, f \mid r^n = f^2 = e, rfr = f \rangle \tag{30}$$

To parse this definition a bit, note that the relation $r^n = e$ behaves like a cyclic group of order n, and so we can interpret these as rotations of an object by $2\pi/n$. The second is that $f^2 = e$ is also a cyclic group of order 2, but it behaves more like a flip in that if you flip twice, you get back to the original. With these relations, we can think of the Dihedral group as having two "copies" of cyclic groups that have some extra properties.

Finally, the relation $rfr = f$ is a bit harder to parse, but it just means that a rotation, then flip, then rotation (which rotates backwards since we flipped), is equal to flipping once. Symbolically, this relation allows us to "push" all of the flips to the back.

$$fr = r^n fr = r^{n-1} f \tag{31}$$

Perhaps a slightly more complicated example for $n = 5$.

$$fr^3 f^3 r = fr^3 fr = fr^2 f = r^5 fr^2 f = r^4 frf = r^3 f^2 = r^3 \tag{32}$$

and after this the relation $r^n = f^2 = e$ allows us to cancel some out.

Example 1.12 (Dihedral Group of Order 4, aka Klein-4 Group)

We use the following group presentation to write the dihedral group of order 4. However, we can relabel them to get a simpler table.

	e	r	f	rf
e	e	r	f	rf
r	r	e	rf	f
f	f	rf	e	r
rf	rf	f	r	e

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Figure 3: Cayley multiplication table for the Klein 4-group.

It can be described as the symmetry group of a non-square rectangle. With the three non-identity elements being horizontal reflection, vertical reflection, and 180-degree rotation.

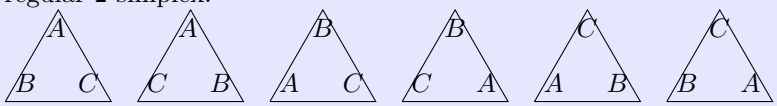
Example 1.13 (Dihedral Group of Order 6)

The group of rotations and flips you can do on a equilateral triangle is called the Dihedral Group Dih(3). It is not abelian.

	e	r	r^2	f	rf	r^2f
e	e	r	r^2	f	rf	r^2f
r	r	r^2	e	rf	r^2f	f
r^2	r^2	e	r	r^2f	f	rf
f	f	r^2f	rf	e	r^2	r
rf	rf	f	r^2f	r	e	r^2
r^2f	r^2f	rf	f	r^2	r	e

Figure 4: Multiplication table for D_3 using simplified notation.

Dih(3) is the group of all rotations and reflections that preserve the structure of the equilateral triangle in $\mathbb{R}^2$, a regular 2-simplex.



Example 1.14 (Dihedral Group of Order 8)

The group of rotations and reflections that preserve the structure of a square in $\mathbb{R}^2$. is called the Dihedral Group Dih(4).

	e	r	r^2	r^3	f	rf	r^2f	r^3f
e	e	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	e	rf	r^2f	r^3f	f
r^2	r^2	r^3	e	r	r^2f	r^3f	f	rf
r^3	r^3	e	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	e	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	e	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	e	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	e

Figure 5: Multiplication table for D_4 using simplified notation.

Note that this is **not** the same as the symmetry group of the regular tetrahedron!

Following this pattern, we can extrapolate to find that the Dihedral group is a symmetry group.

Theorem 1.11 (Dihedral Groups as Symmetry Groups)

Dih(n) is similarly the group of all rotations and reflections that preserve the structure of a regular n-gon in $\mathbb{R}^2$.

Example 1.15 (Groups of Order 3)

$\text{Dih}(3) \simeq S_3$, since permutations of the vertices of a triangle are isomorphic to a permutations of a 3-element set.

Theorem 1.12 (Tip)

To prove a group homomorphism, show that every element of G and H can be written as a word of certain g_i's in G and then h_i's in H, and map the g_i's to h_i's.

1.5 Symmetric and Alternating Groups

We have seen the natural construction of the symmetric group of a set as the set of bijective transformations. Now the reason that symmetric groups are nice is that we can embed a group into its symmetric group.

Theorem 1.13 (Cayley's Theorem)

This applies for both monoids and groups.

1. Any monoid is isomorphic to a monoid of transformations, i.e. there exists an injective monoid homomorphism
$$f : M \to M^M \tag{33}$$
2. Any group is isomorphic to a group of transformations, i.e. there exists an injective group homomorphism
$$f : G \to \text{Sym}(G) \tag{34}$$

Proof.

Let $(M, \cdot, 1)$ be a monoid. Then we will construct a homomorphism $f : M \to M^M$, the monoid of transformations from M to itself. For any $a \in M$, we define the *left translation* $a_L : x \mapsto ax$. We claim that the set $M' \coloneqq \{a_L \in M^M \mid a \in M\}$ is indeed a monoid.

1. *Closure.* Given $a, b \in M$, $ab \in M$ and so $ab_L \in M'$. But $(ab_L)(x) = (ab)x = a(bx) = a_L(bx) = a_L(b_L(x)) = (a_L \circ b_L)(x)$, so $ab_L = a_L \circ b_L$.
2. *Identity.* $e \in M \implies e_L \in M$ where $e_L : x \mapsto x$.

Next we claim that is is an isomorphism.

1. This is a homomorphism due to the closure and identity properties proved above.
2. It is injective since given $a \neq b$ in M, a_L and b_L acts on the identity in different ways $a_L(e) = a \neq b = b_L(e)$, so $a_L \neq b_L$.
3. It is surjective by definition.

We have proved for monoids. For groups, we have the additional assumption that inverses exist in G, and we must prove that the set of left translations G' is indeed a group. It suffices to prove that inverses exist in G'. Given $a \in G$, $a_L \in G'$. But $a^{-1} \in G$ since G is a group, and so $a_L^{-1} \in G'$ as well. We can see that

$$(a_L^{-1} a_L)(x) = (a^{-1}a)x = ex = x \tag{35}$$
$$(a_L a_L^{-1})(x) = (aa^{-1})x = ex = x \tag{36}$$

and so indeed $(a^{-1})_L = (a_L)^{-1}$. From this additional fact all the rest follows exactly as for monoids.

Corollary 1.1 (Cayley)

Every group G is isomorphic to a subgroup of its symmetric group.

Now we limit our scope to only finite sets, i.e. finite symmetric groups, which are often called **permutation** groups. For such finite sets the labeling does not matter since such groups are always isomorphic, so we can say $S = \{1, 2, \dots, n\}$.

Theorem 1.14 (Symmetric Group as a Symmetry Group)

The symmetric group S_n is isomorphic to the symmetry group of the n-simplex in $\mathbb{R}^{n-1}$.

Proof.

Now armed with group presentations and generating sets, let attempt to find a group presentation for a permutation group. Given set $S = \{1, 2, \dots, n\}$, a permutation $\gamma \in \text{Sym}(S)$ is denoted

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n-2 & n-1 & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_{n-2} & i_{n-1} & i_n \end{pmatrix} \in \text{Sym}(S) \tag{37}$$

We begin by introducing a specific instance of a permutation.

Definition 1.16 (Cyclic Permutation)

A permutation is said to be **cyclic** if there exists some subset $A \subset S$ such that γ acts as

$$a_1 \mapsto a_2 \mapsto a_3 \dots \mapsto a_k \mapsto a_1 \tag{38}$$

and leaves the rest unchanged. The notation for this is

$$\begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \in \text{Sym}(S) \tag{39}$$

A cycle acting on a subset of 2 elements, i.e. a swap of two elements, is called a **transposition**. Two cyclic rotations γ_1, γ_2 are **disjoint** if the subsets that they act on are disjoint: $A \cap B = \emptyset$.

Example 1.16 (Some Cyclic Permutations)

This notation can be a bit weird, so let's give some simple examples.

1. (12) is a mapping $1 \to 2,\ 2 \to 1$.
2. (123) is a mapping $1 \to 2,\ 2 \to 3,\ 3 \to 1$.
3. $(123)(45)$ is a mapping $1 \to 2,\ 2 \to 3,\ 3 \to 1,\ 4 \to 5,\ 5 \to 4$.

The reason that cyclic permutations are so important is that they are the building blocks of regular permutations.

Theorem 1.15 (Cycle Decomposition of Permutations)

Every element in S_n except the identity element can be written uniquely (up to order) as the product of disjoint cycles.

Proof.

We can compute $\gamma(1), \gamma^2(1), \dots$. Since $S = \{1, \dots, n\}$ is finite, there is some smallest positive natural k s.t.
$gamma^k(1) = 1$. This yields a k-cycle. Now remove the numbers $1, \pi(1), \dots, \gamma^{k-1}(1)$ and continue the process. Since S is finite this must terminate, and we have such a decomposition. Proof of uniqueness omitted for now, but this whole theorem can be proved using proof by strong induction.

Example 1.17 (Cyclic Decompositions)

For the following permutation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 4 & 8 & 2 & 7 & 1 \end{pmatrix} = (7)(4)(26)(1358) \tag{40}$$

One of the rewards of cycle decompositions is that we can easily compute the effect of conjugation in S_n.

Lemma 1.7 (Conjugation is Easy with Cycle Notation)

Given a k-cycle $\gamma = (i_1, i_2, \dots, i_k) \in S_n$ and any permutation $\sigma \in S_n$, we have

$$\sigma\pi\sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_k) \end{pmatrix} \tag{41}$$

This shows that the cyclic permutations actually form a generating set of S_n. But can we do better? The answer is yes: there is a more minimal generating set.

Corollary 1.2 (Transposition Decomposition of Permutations)

The set of all transpositions forms a generating set of S_n.

Proof.

It suffices to prove that the cycles can be decomposed into transpositions. Indeed, we can just write out by hand

$$\begin{pmatrix} 1 & 2 & \dots & k \end{pmatrix} = \begin{pmatrix} 1 & k \end{pmatrix} \begin{pmatrix} 1 & k-1 \end{pmatrix} \dots \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \tag{42}$$

which by relabeling generalizes for those of form $(i_1 \dots i_k)$.

Recognizing that the set of transpositions is the generating set of the permutation group, we must prove a few more statements before constructing the alternating group. One such fact is that transpositions allow us talk about the parity of an arbitrary permutation, through its signature.

Lemma 1.8 (Parity of Transpositions)

Every permutation can be written as the product of either an even number or an odd number of transpositions, but not both.

Proof.

Now that this is established, the following is well-defined.

Definition 1.17 (Signature)

The **signature** of a permutation is a homomorphism

$$\text{sgn} : S_n \longrightarrow \{1, -1\} \tag{43}$$

Lemma 1.9 ()

The signature of a permutation changes for every transposition that is applied to it.

Now we are ready to introduce another fundamental type of group.

Definition 1.18 (Alternating Group)

The **alternating group** is the kernel of the signature homomorphism $\text{sgn} : S_n \to \{\pm 1\}$.

$$A_n \coloneqq \ker \text{sgn} \tag{44}$$

It is the set of even permutations with order $n!/2$.[a]

[a]Note that the set of odd permutations do not form a group, since the composition of two odd permutations (each having signature -1 is an even permutation.

This construction might seem arbitrarily specific to study so early into algebra, but as we will see later, we will find that that for $n \geq 5$, they will be simple groups that can't be decomposed and therefore fundamental in a sense.

In lecture, we talked about the number of all finite set is e. Since $n!$ is the order of permutation groups, i.e. the order of automorphism groups, we can sum their inverses over all $n \in \mathbb{N}$ to get e.

1.6 Group Actions

We have studied the general properties of groups, but historically group theory arose from the study of transformation groups (which is why I also introduced is so early on). These transformation groups can be thought of as an abstract group it itself, but another way to interpret it is to see how it *acts* on a set.

Definition 1.19 (Group Action)

Let G be a group, S a set. Then, a (left) group action of G on S is a function

$$\sigma : G \times S \to S, \qquad \sigma(g, a) = g \cdot a \tag{45}$$

satisfying two axioms.

1. *Identity.* $\forall a \in S, \sigma(e, a) = a$.
2. *Compatibility.* $\forall g, h \in G$ and $\forall x \in X, \sigma(gh, x) = \sigma(g, \sigma(h, x))$.

The group G is said to **act on** S, and the evaluation $\sigma(g, a)$ can be interpreted as the result after transforming a through g.

Theorem 1.16 (Group Action as a Homomorphism onto the Symmetric Group)

We have the immediate facts.

1. For a fixed $g \in G$, the group action $\sigma_g(s) \coloneqq \sigma(g, s) : S \to S$ is a bijection, i.e. an element of $\text{Sym}(S)$. The inverse is the function mapping $x \mapsto \sigma(g^{-1}, x)$.
2. The map from G to $\text{Sym}(S)$ defined by $g \mapsto \sigma_g$ is a homomorphism.

Proof.

Example 1.18 (Permutations and Dihedral Groups as Group Actions)

In fact, we have seen two concrete examples of such group actions.

1. The permutation group acts on the set $S = \{1, \dots, n\}$ by permuting its elements. It also acts on a set of n-simplexes by rotating/flipping them.
2. The dihedral group acts on the set of regular n-gons by rotating/flipping them.

2 Subgroups

We have seen a few examples of subgroups, but we will heavily elaborate on here. We know that given a set, we can define an equivalence relation on it to get a quotient set. Now if we have a group, defining any such equivalence relation may not be compatible with the group structure. Therefore, it would be nice to have some principles in which we can construct such compatible equivalence classes, i.e. through a **congruence relation** that preserves the operations.

We introduce some standard notation.

Definition 2.1 (Subgroup of Integer Multiples)

The set $k\mathbb{Z}$ is the set of all integer multiples of k. This is a group under addition.

2.1 Cosets

Fortunately, we can do such a thing by taking a subgroup $H \subset G$ and "shifting" it to form the cosets of G, which are the equivalence classes.

Definition 2.2 (Coset)

Given a group G, $a \in G$, and subgroup H,
1. A **left coset** is $aH \coloneqq \{ah \mid h \in H\}$.
2. A **right coset** is $Ha \coloneqq \{ha \mid h \in H\}$.
3. When G is abelian, the **coset** is denoted $a + H$.

With this, we can take arbitrary elements $a, b \in G$ and determine if they are in the same coset as such. Since $a \in aH$, $b \in aH$ iff $b = ah$ for some $h \in H$. Therefore, we have the equivalence relation.

$$a \equiv b \pmod{H} \iff a = bh \text{ for some } h \in H \tag{46}$$

Proof.

We show that this indeed forms an equivalence class.
1. *Reflexive.* $a \equiv a \pmod{H}$ since $e \in H \implies a = ae$.
2. *Symmetric.* Let $a \equiv b \pmod{H}$. Then $a = bh$ for some $h \in H$, but since H is a group, $h^{-1} \in H \implies ah^{-1} = b \implies b \equiv a \pmod{H}$.
3. *Transitive.* Let $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. Then $a = bh$ and $b = ch'$ for some $h, h' \in H$. But then
$$a = bh = (ch')h = c(h'h) \tag{47}$$
where $h'h \in H$ due to closure.

Note that a coset is *not* a subgroup. It is only the case that $eH = H$ is a subgroup, but for $a \neq e$, aH does not even contain the identity. We should think of a coset as a *translation* of the subgroup H.

Example 2.1 (Familiar Cosets)

Here are some examples. Note that all it takes is to find *some* subgroup, and the cosets will naturally pop up.
1. Let $H = 2\mathbb{Z} \subset (\mathbb{Z}, +)$ be the even integers. Then $0 + H$ and $1 + H$ are the even and odd integers, respectively.
2. Let $H = \{e, f\} \subset \text{Dih}(3)$. Then
$$H = \{e, f\}, rH = \{r, rf\}, r^2H = \{r^2, r^2f\} \tag{48}$$
are the cosets.

With this partitioning scheme in mind, the following theorem on the order of such groups becomes very intuitive, and has a lot of consequences.

Theorem 2.1 (Lagrange's Theorem)

Let G be a finite group and H its subgroup. Then

$$|G| = [G : H]|H| \tag{49}$$

where $[G : H]$, called the **index of** H, is the number of cosets in G. Therefore, the order of a subgroup of a finite group divides the order of the group.

Proof.

The union of the $[G : H]$ disjoint cosets is all of G. On the other hand, every H is in one-to-one correspondence with each coset aH, so every coset has $|H|$ elements. Therefore, there are $[G : H]|H|$ elements altogether.

Therefore, Lagrange's theorem says that *given* that you find a subgroup, the order of the subgroup must divide the order of G. However, that doesn't mean that such a subgroup may even exist. For example, there is a group of order 12 having no subgroup of order 6.

Corollary 2.1 ()

The order of any element of a finite group divides the order of the group.

Proof.

Take any $a \in G$ and construct the cyclic subgroup $\langle a \rangle \subset G$. Then by Lagrange's theorem, $|a| = |\langle a \rangle|$ divides $|G|$.

Corollary 2.2 ()

Every finite group of a prime order is cyclic.

Proof.

Let $a \in G$ be any element other than the identity e, and consider $\langle a \rangle \subset G$. The order must divide $|G|$ which is prime, so $|a| = 1$ or $|G|$. But $|a| \neq 1$ since we did not choose the identity, so $|a| = |G| \implies \langle a \rangle = G$.

Corollary 2.3 ()

If $|G| = n$, then for every $a \in G$ $a^n = e$.

Proof.

Let $|a| = k$. Then $k \mid n$, and so $a^n = a^{kl} = (a^k)^l = e^l = e$.

Corollary 2.4 (Fermant's Little Theorem)

Let p be a prime number. The multiplicative group $\mathbb{Z}_p \setminus \{0\}$ of the field $\mathbb{Z}_p$ is an abelian group of order $p-1 \implies g^{p-1} = 1$ for all $g \in \mathbb{Z}_p \setminus \{0\}$. So,

$$a^{p-1} \equiv 1 \iff a^p \equiv a \pmod{p} \tag{50}$$

We can generalize this.

Definition 2.3 (Euler's Totient Function)

Euler's Totient Function, denoted $\varphi(n)$, consists of all the numbers less than or equal to n that are coprime to n.

Theorem 2.2 (Euler's Theorem)

For any n, the order of the group $\mathbb{Z}_n \setminus \{0\}$ of invertible elements of the ring $\mathbb{Z}_n$ equals $\varphi(n)$, where φ is Euler's totient function. In other words with $G = \mathbb{Z}_n \setminus \{0\}$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \quad \text{where } a \text{ is coprime to } n \tag{51}$$

Example 2.2 ()

In $\mathbb{Z}_{125} \setminus \{0\}$, $\varphi(125) = 125 - 25 = 100 \implies 2^{100} \equiv 1 \pmod{125}$

2.2 Normal Subgroups

By introducing cosets, we have successfully constructed an equivalence relation on G. This set of cosets is indeed a partition of G, but we would like to endow it with a group structure that respects that of G. That is, let $a, b \in G$ and its corresponding cosets be aH, bH. Then, we would like to define an operation $\cdot$ on the cosets such that

$$(aH) \cdot (bH) \coloneqq (ab)H \tag{52}$$

That is, we would like to upgrade the equivalence relation to a *congruence relation*. If we try to show that this is indeed a well-defined operation, we run into some trouble. Suppose $aH = a'H$ and $bH = b'H$. Then with our definition, we should be able to derive that $(aH)(bH) = (a'H)(b'H)$ through the equation

$$(aH)(bH) = (ab)H = (a'b')H = (a'H)(b'H) \tag{53}$$

We have $a' = ah_1$, $b' = bh_2$, and $a'b' = abh$. Then,

$$(ab)H = (a'b')H \implies a'b' = abh \text{ for some } h \in H \tag{54}$$

$$\implies ah_1bh_2 = abh \text{ for some } h_1, h_2, h \in H \tag{55}$$

But the final statement is not true in general. In an abelian group, we could just swap h_1 and b to derive it completely, but perhaps there is a weaker condition on just the subgroup H that allows us to "swap" the two.

Definition 2.4 (Normal Subgroups)

A subgroup $N \subset G$ is a **normal subgroup** iff the left cosets equal the right cosets. That is, $\forall g \in G, h \in H$.

$$g^{-1}hg \in H \tag{56}$$

We call $g^{-1}hg$ the **conjugate** of h by g.

Example 2.3 (Normal Subgroups)

For intuition, we provide some examples of normal subgroups.

1. If G is abelian, every subgroup is normal. So $(2\mathbb{Z}, +)$ is normal, and $(\mathbb{Q}, \times) \subset (\mathbb{R}, \times)$ is also normal.
2. Given $G = (\mathbb{R} \setminus \{0\}, \times)$, let $H = (\mathbb{R}^+, \times) \subset G$ be a subgroup. Then H is normal since for any $g \in \mathbb{R}$, g, g^{-1} are either both positive or both negative, and so $ghg^{-1} > 0 \implies ghg^{-1} \in H$. H and $(-1)H$ are two cosets of $\mathbb{R}$.
3. $\mathrm{SL}_n(\mathbb{F}) \subset \mathrm{GL}_n(\mathbb{F})$ is a normal subgroup since the determinant of the inverse is ihe inverse of the determinant, and so for any $g \in \mathrm{GL}_n(\mathbb{F})$,
$$\det(ghg^{-1}) = \det(g)\det(h) = \det(g^{-1}) = \det(g) \cdot 1 \cdot \frac{1}{\det(g)} = 1 \implies ghg^{-1} \in \mathrm{SL}_n(\mathbb{F}) \tag{57}$$
4. The subgroup $H = \{e, r^2\} \subset \mathrm{Dih}(4)$ is a normal subgroup. It is clearly a subgroup isomorphic to Z_2, and to see normality, note that r^2 commutes with any $g = r^n \in \mathrm{Dih}(4)$. If g contains a flip, then we can just check the 4 cases knowing that $fr = r^3 f$.
$$fr^2f^{-1} = fr^2f = (fr)(rf) = r^3frf = r^3r^3f^2 = r^2 \tag{58}$$
$$(rf)r^3(rf)^{-1} = \ldots = r^2 \tag{59}$$
Therefore $\mathrm{Dih}(4)/H$ has order 4, which means it must be isomorphic to either the cyclic group or the Klein 4 group. It turns out it's the Klein 4 group.

Example 2.4 (Subgroups that are Not Normal)

Here are some subgroups that are not normal.

1. Given $G = \mathrm{Dih}(3)$, $H = \{e, f\}$ is not normal since $rfr^{-1} = rfr^2 = r^2f \notin H$.
2. The subgroup
$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; ac \neq 0 \right\} \subset \mathrm{GL}_2(\mathbb{R}) \tag{60}$$
is not normal since
$$h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H, a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \implies aha^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \notin H \tag{61}$$

Finally, we present some relevent results of alternating subgroups.

Theorem 2.3 (Alternating Group is Normal in Symmetric)

A_n is a normal subgroup of S_n, of index[a] 2.

[a] i.e. the number of cosets

Proof.

Lemma 2.1 (Cycles in Alternating Group)

We have the following.

1. Every element of A_n can be written as the product of 3-cycles.
2. If $n \geq 4$, H is a normal subgroup of A_n, and H contains one 3-cycle, then $H = A_n$.

Proof.

Since we've proved that every permutation is the product of transpositions, it suffices to prove that the product of two transpositions can be written as the product of 3-cycles. We check this case by case, where distinct symbols represent distinct values.

1. $(\alpha\ \beta)(\gamma\ \delta) = (\alpha\ \beta\ \gamma)(\beta\ \gamma\ \delta)$
2. $(\alpha\ \beta)(\alpha\ \gamma) = (\alpha\ \gamma\ \beta)$
3. $(\alpha\ \beta)(\alpha\ \beta) = e$

Therefore every even permutation is the product of 3-cycles.

Definition 2.5 (Simple Group)

A **simple group** is a group with no proper normal subgroup. That is, the only normal subgroups are the trivial group and itself.

Theorem 2.4 (Alternating Groups are Simple)

For $n \geq 5$, A_n is a simple group.

Proof.

Let $H \subset A_n$ be a normal subgroup containing more than the identity. If we can find a single 3-cycle in H, then it follows from 2.2 that $H = A_n$. Let $\gamma \in H$, $\gamma \neq e$, and write $\gamma = \gamma_1 \dots \gamma_m$ as a product of disjoint cycles. We have 4 cases.

1. Let $k \geq 4$ and suppose that some factor, say γ_1 is a k-cycle. WLOG let us assume that $\gamma_1 = (1 \dots k)$. Since H is normal, $(1,2,3)\gamma(1,2,3)^{-1} \in H$ and $(1,2,3)$ commutes with all the factors of γ except γ_1 (since the cycles are disjoint and so γ_i for $i \neq 1$ does not contain $1,2,3$). Thus letting
$$\sigma = (1,2,3)\gamma(1,2,3)^{-1} = (2,3,1,4,\dots,k)\gamma_2 \dots \gamma_m \in H \tag{62}$$
since H is a group we have
$$\sigma\gamma^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 \dots & k \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & k \end{pmatrix}^{-1} \tag{63}$$
$$= \begin{pmatrix} 2 & 3 & 1 & 4 & \dots & k \end{pmatrix} \begin{pmatrix} k & \dots & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \tag{64}$$
2. Suppose γ has at least two 3-cycles as factors, say $\gamma_1 = (1,2,3), \gamma_2 = (4,5,6)$. Then
$$\sigma = (3,4,5)\gamma(3,4,5)^{-1} = (1,2,4)(3,6,5)\gamma_3 \dots \gamma_m \in H \tag{65}$$
and again we have
$$\sigma\gamma^{-1} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 4 & 5 & 6 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}^{-1} \tag{66}$$
$$= \begin{pmatrix} 1 & 6 & 3 & 4 & 5 \end{pmatrix} \tag{67}$$
which is a 5-cycle, and we are done by case 1.
3. Suppose γ has precisely one 3-cycle factor and all others are transposisions. If the 3-cycle is $\gamma_1 = (1,2,3)$, then $\gamma^2 = (1,2,3)^2 = (1,3,2)$ is a 3-cycle.
4. Suppose γ is the product of disjoint transpositions. Say $\gamma_1 = (1,2), \gamma_2 = (3,4)$. Then as before
$$\sigma = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \gamma \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}^{-1} \implies \sigma\gamma^{-1} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \in H \tag{68}$$
Since $n \geq 5$ by our theorem hypothesis, the permutation $\tau = (2,3,5) \in A_n$, and so
$$\tau \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \tau^{-1} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} \in H \tag{69}$$
$$\implies \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 3 \end{pmatrix} \in H \tag{70}$$

2.3 Quotient Groups

Now that we know about normal subgroups, this allows us to endow on the quotient set a group structure.

Definition 2.6 (Quotient Group)

Given a group G and a normal subgroup H, the **quotient group** G/H is the group of left cosets aH with

1. the operation $(aH) \cdot (bH) \coloneqq (ab)H$
2. the identity element eH.
3. inverses $(aH)^{-1}) = (a^{-1})H$.

and order $|G/H| = |G|/|H|$.

Proof.

We verify the properties of a group.

1. Suppose as above that $aH = a'H$ and $bH = b'H$. Then $a' = ah$ and $b' = bk$ for some $h, k \in H$. Since H is normal, $b^{-1}hb = h'$ for some $h' \in H$. Therefore,

$$a'b' = (ah)(bk) = a(hb)k = (abh')k = (ab)(h'k) \in (ab)H \tag{71}$$

   and so $(ab)H = (a'b')H$.
2. eH is indeed the identity since $(aH)(eH) = (ae)H = aH$ and $(eH)(aH) = (ea)H = aH$.
3. Inverses are the same logic.
4. Associativity follows from associativity in G.

Finally, by Lagrange's theorem, the order is as stated.

Since the quotient defines a *congruence* class, this makes it a group homomorphism.

Theorem 2.5 (Quotient Maps are Homomorphisms)

The map $p : G \to G/H$ is a group homomorphism.

Proof.

Follows immediately from the definition.

It's a bit hard thinking of an intuitive picture of a normal subgroup. Unless you sit down and try to prove that a subgroup is normal, it's difficult to tell right away. The following lemma characterizes normal subgroups in a different manner.

Lemma 2.2 (Normal Subgroup as Kernel)

A subgroup $H \subset G$ is normal if and only if there exists a group homomorphism $\phi : G \to G'$ with $\ker \phi = H$.

Proof.

We prove bidirectionally.

1. $(\to)$. Since H is normal, we can form the quotient group G/H. Let $\phi : G \to G/H$ be defined $\phi(a) = aH$. Then,

$$\ker \phi = \phi^{-1}(eH) = \{a \in G \mid aH = eH = H\} \tag{72}$$
$$= \{a \in G \mid a \in H\} \tag{73}$$

Therefore, ϕ is a homomorphism because $\phi(ab) = abH = (aH)(bH)$.

2. ($\leftarrow$) Assume there is a group homomorphism ϕ. Then, $\ker\phi \subset G$ is a subgroup proven in 1.3. Now consider any $g \in G$. Then

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\cdot e\cdot\phi(g)^{-1} = e \implies ghg^{-1} \in \ker\phi \tag{74}$$

Now that we can construct quotient groups, we would like to see if they are isomorphic to any current groups that we know. More specifically, if we have a normal subgroup $H \subset G$, we can cleverly think of some other group G' and construct a group homomorphism $f : G \to G'$ such that $H = \ker f$. If we can do this, then we can construct a nice isomrophism from G/H to G'.

Theorem 2.6 (Fundamental Group Homomorphism Theorem)

Let $f : G \to G'$ be a surjective homomorphism.[a] Then $G/\ker f \simeq G'$.[b]

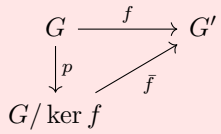


Figure 6: Given f and the projection map $p : G \to G/\ker f$, this induces an isomorphism $\bar{f}$ such that $f = \bar{f}\circ p$.

[a] Sometimes called an *epimorphism*.
[b] Note that if f is not surjective, we can just have it be surjective by restricting G' to be the image of f.

Proof.

Let $H = \ker f$, which is then a normal subgroup from 2.3. Now we define a homomorphism

$$\bar{f} : G/H \to G', \qquad \bar{f}(aH) = f(a) \tag{75}$$

We check the following.

1. $\bar{f}$ is well defined. If we have $a, a' \in G$ with $aH = a'H$, then $a' = ah$ for some $h \in H = \ker f$. So $f(a') = f(ah) = f(a)f(h) = f(a)$.
2. $\bar{f}$ is a homomorphism. We see that

$$\begin{aligned} \bar{f}((aH)(bH)) &= \bar{f}((ab)H) && (76)\\ &= f(ab) && (77)\\ &= f(a)f(b) && (78)\\ &= \bar{f}(aH)\bar{f}(bH) && (79) \end{aligned}$$

3. $\bar{f}$ is surjective. This is trivially true since if not, then $f = \bar{f}\circ p$ cannot be surjective.
4. $\bar{f}$ is injective. By 1.3, it suffices to show that $\ker\bar{f}$ is trivial. Suppose $aH \in \ker\bar{f}$. Then $\bar{f}(aH) = f(a) = e_{G'} \implies a \in H \implies aH = eH$.

Example 2.5 (Cyclic Groups)

$(k\mathbb{Z}, +) \subset (\mathbb{Z}, +)$ is a normal subgroup. Our intuition might tell us that the cosets of the form $k\mathbb{Z}, 1 + k\mathbb{Z}, \ldots, (k-1) + k\mathbb{Z}$ behave like integers modulo k, i.e. a cyclic group. Therefore, we can construct the map

$$f : \mathbb{Z} \to Z_k, \qquad f(x) = x \pmod k \tag{80}$$

This is a homomorphism and also $\ker f = k\mathbb{Z}$, and so by the fundamental homomorphism theorem

$$\frac{\mathbb{Z}}{k\mathbb{Z}} \simeq Z_k \tag{81}$$

By establishing the connection between the integers and cyclic groups, we establish the notation $Z_k = \mathbb{Z}_k$.

Example 2.6 (Quotient of Reals over Integers)

We can see that $(\mathbb{Z}, +) \subset (\mathbb{R}, +)$ is a normal subgroup. Our intuition might tell us that the cosets (which are disconnected sets consisting of isolated points $\{\dots, x-1, x, x+1, \dots\}$) behave sort of like the rotations on a circle S^1. Therefore, let us construct a map

$$f : \mathbb{R} \to S^1, \qquad f(x) = \cos 2\pi x + i \sin 2\pi x \subset \mathbb{C} \tag{82}$$

Since $f(x+y) = f(x)f(y)$, it follows that f is a homomorphism. On the other hand, $\ker f = \{x \in \mathbb{R} \mid \cos 2\pi x = 1, \sin 2\pi x = 0\} = \mathbb{Z}$. Therefore by the fundamental homomorphism theorem, we have

$$\mathbb{R}/\mathbb{Z} \simeq S^1 \tag{83}$$

2.4 Orbits and Stabilizers

Definition 2.7 (Orbits)

Let G be a transformation group on set X. Points $x, y \in X$ are equivalent with respect to G if there exists an element $g \in G$ such that $y = gx$. This has already been defined through the equivalence of figures before. This relation splits X into equivalence classes, called **orbits**. Note that cosets are the equivalence classes of the transformation group G; oribits are those of X. We denote it as

$$Gx \equiv \{gx \mid g \in G\} \tag{84}$$

By definition, transitive transformation groups have only one orbit.

Definition 2.8 ()

The subgroup $G_x \subset G$, where $G_x \equiv \{g \in G | gx = x\}$ is called the **stabilizer** of x.

Example 2.7 ()

The orbits of $O(2)$ are concentric circles around the origin, as well as the origin itself. The stabilizer of 0 is the entire $O(2)$.

Example 2.8 ()

The group S_n is transitive on the set $\{1, 2, ..., n\}$. The stabilizer of $k, (1 \leq k \leq n)$ is the subgroup $H_k \simeq S_{n-1}$, where H_k is the permutation group that does not move k at all.

Theorem 2.7 ()

There exists a 1-to-1 injective correspondence between an orbit G_x and the set G/G_x of cosets, which maps a point $y = gx \in Gx$ to the coset gG_x.

Corollary 2.5 ()

If G is a finite group, then

$$|G| = |G_x||Gx| \tag{85}$$

In fact, there exists a precise relation between the stabilizers of points of the same orbit, regardless of G being finite or infinite:

$$G_{gx} = gG_xg^{-1} \tag{86}$$

2.5 Centralizers and Normalizers

2.6 Lattice of Subgroups

3 Group Actions

3.1 Sylow Theorems

4 Classification of Groups

4.1 Direct Products

Definition 4.1 (Direct Product)

The **direct product** of two groups G and H is denoted

$$G \times H \equiv \{(g, h) \mid g \in G, h \in H\} \tag{87}$$

Note that the product need not be binary (nor must it be of finite arity).

Example 4.1 ()

The **general affine group** is defined

$$\mathrm{GA}(V) \equiv \mathrm{Tran}\, V \times \mathrm{GL}(V) \tag{88}$$

Example 4.2 ()

The **Galileo Group** is the transformation group of spacetime symmetries that are used to transform between two reference frames which differ only by constant relative motion within the constructs of Newtonian physics. It is denoted

$$\mathrm{Tran}\, \mathbb{R}^4 \times H \times \mathrm{O}(3) \tag{89}$$

where H is the group of transformations of the form

$$(x, y, z, t) \longmapsto (x + at, y + bt, z + ct, t) \tag{90}$$

Example 4.3 ()

The **Poincaré Group** is the symmetry group of spacetime within the principles of relativistic mechanics, denoted

$$G = \mathrm{Tran}\, \mathbb{R}^4 \times \mathrm{O}_{3,1} \tag{91}$$

where $\mathrm{O}_{3,1}$ is the group of linear transformations preserving the polynomial

$$x^2 + y^2 + z^2 - t^2 \tag{92}$$

4.2 Semidirect Products

4.3 Classification of Finite Abelian Groups

Theorem 4.1 (Groups of Order 1, 2, 3)

We have the following.

1. There is only one group of order 1.
$$Z_1 \simeq S_1 \simeq A_2 \tag{93}$$
2. There is only one group of order 2.
$$Z_2 \simeq S_2 \simeq D_2 \tag{94}$$
3. There is only one group of order 3.
$$Z_3 = A_3 \tag{95}$$

Theorem 4.2 (Groups of Order 4)

There are two groups of order 4.

$$Z_4, \qquad Z_2^2 \simeq D_4 \tag{96}$$

4.4 Group Extensions

4.5 Classification of Simple Groups of Small Order

Theorem 4.3 (Classification of Simple Groups of Small Order)

The following are the only groups of order n. You can notice that it is dominated by direct products of cyclic groups, since they exist for every order, while the other types increase in order very fast.

n	**Abelian Groups**	**Non-Abelian Groups**
1	$\{e\}$ (trivial group)	None
2	$\mathbb{Z}_2 = S_2 = \text{Dih}(1)$	None
3	$\mathbb{Z}_3 = A_3$	None
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 = \text{Dih}(2)$	None
5	$\mathbb{Z}_5$	None
6	$\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$	$S_3 = \text{Dih}(3)$
7	$\mathbb{Z}_7$	None
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 = \text{Dih}(4)$, Q_8 (quaternion)
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	None
10	$\mathbb{Z}_{10} = \mathbb{Z}_5 \times \mathbb{Z}_2$	$D_5 = \text{Dih}(5)$
11	$\mathbb{Z}_{11}$	None
12	$\mathbb{Z}_{12} = \mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	A_4, $D_6 = \text{Dih}(6)$, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ (dicyclic)

Figure 7: Classification of groups up to order 12.