MAT 345 Notes

Max Chien

Fall 2024

Contents

Introduction

This document contains notes taken for the class MAT 345: Algebra I at Princeton University, taken in the Fall 2024 semester. These notes are primarily based on lectures and lecture notes by Professor Jakub Witaszek. Other references used in these notes include *Algebra* by Michael Artin, *Abstract Algebra* by David Dummit and Richard Foote, *Contemporary Abstract Algebra* by Joseph Gallian, and *A Book of Abstract Algebra* by Charles Pinter. Since these notes were primarily taken live, they may contains typos or errors.

Chapter 1

Elementary Number Theory

This course will study algebraic structures, primarily groups, rings, and fields. These objects serve as abstractions of objects which we are familiar with performing algebra over, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. As such, we will begin with a brief survey of algebraic operations over these familiar objects, before progressing to their abstracted counterparts.

1.1 The Euclidean Algorithm

The most important theorem of the structure of the integers is the following:

Theorem 1.1: Fundamental Theorem of Arithmetic

Let $n \in \mathbb{N}$. Then there is a unique representation of n as a product of powers of primes (up to ordering), as

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$$

Another important operation to abstract is that of division. This requires phrasing it in terms that are easily generalized to other objects:

Theorem 1.2: Division Algorithm

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$n = qd + r$$

and

$$0 \leq r < d$$

Proof. **Existence:** Define

$$S = \{n - dx | x \in \mathbb{Z}, n - dx \geq 0\}$$

Let $r = \min S$ and let $q \in \mathbb{Z}$ be the corresponding value such that $n - qd = r$. Suppose that $r \geq d$. Then

$$n - (q+1)d = n - qd - d = r - d \geq 0$$

so $r - d \in S$, contradicting $r = \min S$. So $0 \leq r < d$. Thus we have shown existence.

Uniqueness: Let $n = qd + r = q'd + r'$. Then

$$d(q - q') + r - r' = 0$$

so $d | r - r'$. But we also have $-d < r - r' < d$, so $r - r' = 0$ and thus $r = r'$. It follows that $q = q'$. $\square$

We call d the divisor, q the quotient, and r the remainder. Explicitly, we have

$$n = \left\lfloor \frac{n}{d} \right\rfloor d + (n \bmod d)$$

The proof of the Fundamental Theorem of Arithmetic requires the proof of some other lemmas:

Definition 1.1

Let $a, b \in \mathbb{Z}$. We write $a|b$ if there exists $c \in \mathbb{Z}$ such that $ac = b$.

Lemma 1.3: Euclid's lemma

Let p be prime and $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

This, in turn, relies on another identity.

Definition 1.2

Let $a, b \in \mathbb{N}$. Then define $\gcd(a, b)$ to be a common divisor which divides any other common divisor.

We should note that we have not shown that $\gcd(a, b)$ exists and is unique. However, consideration of the extended Euclidean algorithm shows both of these, and moreover that $\gcd(a, b)$ is the largest common divisor of a and b.

Proposition 1.4: Bezout's Identity

Let $a, b \in \mathbb{Z}$ be nonzero. Then there exist $k, l \in \mathbb{Z}$ such that

$$ka + lb = \gcd(a, b)$$

Example 1.1

if $a = 9$ and $b = 24$, then

$$3 \cdot 9 + (-1) \cdot 24 = 3 = \gcd(9, 24)$$

Bezout's Identity follows from the **extended Euclidean Algorithm**.

The extended Euclidean algorithm takes two nonzero integers a, b and an integer m which is divisible by $\gcd(a, b)$, and produces integers k, l such that

$$ka + lb = m$$

First, we define the standard Euclidean algorithm. Note that we have the following:

$$\gcd(a, b) = \begin{cases} \gcd(a - b, b), & a \geq b \\ \gcd(a, b - a), & a < b \end{cases}$$

This holds since if $k|a$ and $k|b$, then $k|a - b$ and $k|b - a$. If $k|a - b$ and $k|b$, then $k|a$, so the top equality is proved. Similarly the second is true. Thus we proceed by applying the above equality repeatedly, until we have either $\gcd(a, a) = a$.

Example 1.2

We have

$$\gcd(24, 9) = \gcd(15, 9) = \gcd(6, 9) = \gcd(6, 3) = \gcd(3, 3) = 3$$

We can also skip steps by using the rule

$$\gcd(a, b) = \begin{cases} \gcd(a \bmod b, b), & a \geq b \\ \gcd(a, b \bmod a), & a < b \end{cases}$$

which holds by repeated application of the previous rule. This would give

$$\gcd(24, 9) = \gcd(6, 9) = \gcd(6, 3) = \gcd(3, 3) = 3$$

To extend the algorithm, we use the Euclidean algorithm and apply it to the following:

$$\begin{gathered} \blacksquare \cdot x + \blacksquare \cdot y = m \\ \blacksquare \cdot (x \bmod y) + \blacksquare \cdot y = m \\ \vdots \\ \blacksquare \cdot \gcd(x, y) + \blacksquare \cdot 0 = m \end{gathered}$$

We can then solve the bottom equality and pass back up the chain of equalities, preserving values which are unchanged in each step of the Euclidean algorithm.

Example 1.3

Let $x = 9, y = 24$ and $m = 12$. We have

$$\begin{aligned}
\blacksquare \cdot 9 + \blacksquare \cdot 24 &= 12 \\
\blacksquare \cdot 9 + \blacksquare \cdot 6 &= 12 \\
\blacksquare \cdot 3 + \blacksquare \cdot 6 &= 12 \\
\blacksquare \cdot 3 + \blacksquare \cdot 3 &= 12 \\
\blacksquare \cdot 3 + \blacksquare \cdot 0 &= 12
\end{aligned}$$

We can then fill in the bottom line:

$$\begin{aligned}
\blacksquare \cdot 9 + \blacksquare \cdot 24 &= 12 \\
\blacksquare \cdot 9 + \blacksquare \cdot 6 &= 12 \\
\blacksquare \cdot 3 + \blacksquare \cdot 6 &= 12 \\
\blacksquare \cdot 3 + \blacksquare \cdot 3 &= 12 \\
4 \cdot 3 + 0 \cdot 0 &= 12
\end{aligned}$$

To move up to the next line, since the right term was changed when progressing down, the coefficient should stay the same when progressing up. In fact, the left hand coefficient stays the same as well:

$$\begin{gathered}
4 \cdot 3 + 0 \cdot 3 = 12 \\
\Uparrow \\
4 \cdot 3 + 0 \cdot 0 = 12
\end{gathered}$$

In the next line, we again change the left hand coefficient and keep the right hand (once again this changes nothing):

$$\begin{gathered}
4 \cdot 3 + 0 \cdot 6 = 12 \\
\Uparrow \\
4 \cdot 3 + 0 \cdot 3 = 12
\end{gathered}$$

Now, we keep the left hand coefficient and switch the right hand:

$$\begin{gathered}
4 \cdot 9 + (-4) \cdot 6 = 12 \\
\Uparrow \\
4 \cdot 3 + 0 \cdot 3 = 12
\end{gathered}$$

and finally:

$$\begin{gathered}
12 \cdot 9 + (-4) \cdot 24 = 12 \\
\Uparrow \\
4 \cdot 9 + (-4) \cdot 6 = 12
\end{gathered}$$

So we have found $k = 12, l = -4$.

Proof of Euclid's Lemma. If $p|a$, then we are done. So suppose it doesn't. Then $\gcd(p, a) = 1$. By Bezout's identity, there exist $k, l \in \mathbb{Z}$ such that

$$kp + la = 1$$

So $kpb + lab = b$. p divides the left hand side since it is in the product, and divides the right hand side since it divides ab. $\square$

1.2 Modular Arithmetic

Definition 1.3

Let $a, b \in \mathbb{Z}$, and let $n > 0$ be an integer. Then a is **congruent** to b modulo n (denoted $a \equiv b \pmod{n}$) if

$$n|a - b$$

It follows that congruence modulo n is an equivalence relation for any n, dividing the integers into n classes based on their remainders after dividing by n.

We may equivalently define this congruence as follows:

Proposition 1.5

$a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$ (where $a \bmod n$ represents the remainder of a when divided by n.)

A convenient example of modular arithmetic is the use of a 12-hour clock system, where the hour hand resets after each multiple of 12. We may similarly visualize modular arithmetic for any n as movement around a circle with n distinct positions.

Lemma

Let $a, b, c, d \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that

$$\begin{cases} a \equiv c \pmod{n} \\ b \equiv d \pmod{n} \end{cases}$$

Then

$$\begin{cases} a + b \equiv c + d \pmod{n} \\ ab \equiv cd \pmod{n} \end{cases}$$

Essentially, the above lemma says that we may replace any number by another number which is equivalent modulo n (for addition and multiplication).

Example 1.4

We have

$$7 \cdot 22 \equiv 1 \cdot 4 \equiv 4 \pmod 6$$

Similarly,

$$(5+12)8+13 \equiv (5+5)1+6 \equiv 3 \cdot 1+6 \equiv 2 \pmod 7$$

Theorem 1.6

Let p be prime and let $k \in \mathbb{Z}$, and suppose p does not divide k. Then

$$k \bmod p, 2k \bmod p, \ldots, (p-1)k \bmod p$$

is a permutation of

$$1, 2, \ldots, p-1$$

Proof. Suppose that not all of these values are different, such that there exist $1 \leq n_1, n_2 \leq p-1$ but $n_1 k \bmod p = n_2 k \bmod p$. But this means that $(n_2 - n_1)k \bmod p = 0$, so p divides $(n_2 - n_1)k$. It doesn't divide k, so it divides $n_2 - n_1$. But $-p < n_2 - n_1 < p$. The only number in this range which p divides is 0, so $n_1 = n_2$.

Thus the list

$$k \bmod p, \ldots, (p-1)k \bmod p$$

is a list of $p-1$ distinct numbers between 1 and $p-1$. So each number occurs at least once, and we have just shown that they are distinct, so each number occurs exactly once. $\square$

One interpretation of this is that if you repeatedly take k steps around a circle with p positions, then if p does not divide k, we will not repeat spaces until we have covered all of them.

Corollary 1.7

Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a. Then there exists $b \in \mathbb{Z}$ such that

$$ab \equiv 1 \pmod p$$

For any b which satisfies the above, we call b a **multiplicative inverse** of a.

Proof. By Theorem 1.6, there exists some n with $1 \leq n \leq p-1$ such that $nk \bmod p = 1$ $\square$

Note that multiplicative inverses found this way are *not* unique. Thus it is improper to write an expression of the form $\frac{1}{a} \pmod p$.

Remark

A multiplicative inverse may be found using the extended Euclidean algorithm.

Theorem 1.8: Fermat's Little Theorem

Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a. Then

$$a^{p-1} \equiv 1 \pmod p$$

Example 1.5

With $a = 2, p = 7$ we have

$$\begin{aligned} 2^0 &= 1 \equiv 1 \pmod 7 \\ 2^1 &= 2 \equiv 2 \pmod 7 \\ 2^2 &= 4 \equiv 4 \pmod 7 \\ 2^3 &= 8 \equiv 1 \pmod 7 \\ 2^4 &= 16 \equiv 2 \pmod 7 \\ 2^5 &= 32 \equiv 4 \pmod 7 \\ 2^6 &= 64 \equiv 1 \pmod 7 \end{aligned}$$

Note that $7 - 1 = 6$ is not the first b with $a^b \equiv 1 \pmod p$. However, the remainders do occur in cycles, and the period of this cycle divides $p - 1$.

Lemma

Suppose n does not divide k. If

$$ak \equiv bk \pmod n$$

then

$$a \equiv b \pmod n$$

Proof. We have $n|(a-b)k$, so by Euclid's Lemma $n|a-b$. Thus $a \equiv b \pmod n$. $\square$

Proof of Fermat's Little Theorem. Take the product

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv a^{p-1}(p-1)! \pmod p$$

(Note that this is a simple equality). But Theorem 1.6 tells us that modulo p, these factors are a rearrangement of $1, \ldots, p-1$. So we have

$$(p-1)! \equiv a \cdot 2 \ldots \cdot (p-1) \pmod p$$

Combining these two congruences and applying the Lemma, we have

$$a^{p-1} \equiv 1 \pmod p$$ $\square$

1.3 Fields

We recall the definition of a field:

Definition 1.4

A field is a nonempty set F together with two operations $+ : F \times F \to F$ and $\cdot : F \times F \to F$ as well as distinct elements $0 \neq 1 \in F$ such that

- $+$ and $\cdot$ are commutative.
- $+$ and $\cdot$ are associative.
- 0 is an additive identity and 1 a multiplicative identity.
- Additive inverses exist (denoted $-\alpha$).
- Multiplicative inverses exists for any $\alpha \neq 0$ (denoted α^{-1}).
- $\cdot$ distributes over $+$.

Some familiar examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. A nonexample is $\mathbb{Z}$ (which does not have multiplicative inverses.)

Definition 1.5

Let p be prime. Then we define $\mathbb{F}_p = \{\ldots, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \ldots\}$, where the elements $\overline{k}$ are defined such that

$$\overline{a} = \overline{b} \iff a \equiv b \pmod{p}$$

We define

$$\overline{a} + \overline{b} = \overline{a+b}$$

and

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Example 1.6

With $p = 5$, we have

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$$

Equivalently, since we identify numbers congruent modulo p, Theorem 1.6 we can simply write

$$\mathbb{F}_p = \{\overline{0}, \ldots, \overline{p-1}\}$$

all of which are distinct. Moreover, Corollary 1.7 assures us of the existence of multiplicative inverses. The remaining axioms are simpler to check, but this demonstrates that $\mathbb{F}_p$ is in fact a field.

Definition 1.6

The set $\mathbb{Z}/n\mathbb{Z}$ is defined similarly to $\mathbb{F}_p$ (where n is not necessarily prime), with only the operation of addition defined.

We can use this to prove the following theorem:

Theorem 1.9

Let p be prime with $p \equiv 1 \pmod 4$. Then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

We can check the first few cases by hand:

$$\begin{aligned} 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \end{aligned}$$

For the cases $p \geq 37$, we will develop a bit more theory.

Proof. □

Definition 1.7

$a \in \mathbb{F}_p$ is called a **quadratic residue** if $a = x^2$ for some $x \in \mathbb{F}_p$.

Equivalently:

Definition 1.8

$a \in \mathbb{Z}$ is a quadratic residue mod p if $a \equiv x^2 \pmod p$ for some $x \in \mathbb{Z}$.

Example 1.7

With $p = 5$, we have

$$\begin{cases} 0^2 \equiv 0 \\ 1^2 \equiv 1 \\ 2^2 \equiv 4 \\ 3^2 \equiv 4 \\ 4^2 \equiv 1 \end{cases} \pmod 5$$

so the quadratic residues are $0, 1, 4$ (note that 0 is always a quadratic residue.)

The necessary result is as follows:

Lemma

-1 (or $p-1$) is a quadratic residue mod p if and only if $p \equiv 1 \pmod 4$.

Proof. Skipped. $\square$

We can now return to the previous proof.

Proof of Theorem 1.9. **Claim 1:** There exists $x, y \in \mathbb{Z}$ with $0 < x, y < p$ and

$$x^2 + y^2 \equiv 0 \pmod p$$

To show this, by the Lemma we have that -1 is a quadratic residue, so there exists $a \in \mathbb{Z}$ with

$$a^2 \equiv -1 \pmod p$$

or

$$1^2 + a^2 \equiv 0 \pmod p$$

Now let $x = 1$, $y = a \bmod p$. Claim 1 is proved.

Claim 2: There exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 < 2p$ and $x^2 + y^2 \equiv 0 \pmod p$.

To show this, apply Claim 1 to produce x, y with $x^2 + y^2 \equiv 0 \pmod p$. Then let S be the set

$$S = \{(x_0, y_0), \ldots, (x_{p-1}, y_{p-1})\} \subseteq \mathbb{Z}^2$$

where

$$(x_i, y_i) = (ix \bmod p, iy \bmod p)$$

This set may be seen as the set of integer multiples of the point (x, y), modulo p.

Now, we claim that there exists $0 \leq i < j \leq p-1$ such that

$$d((x_i, y_i), (x_j, y_j)) < \sqrt{2p}$$

To show this, we draw circles of radius

$$\frac{\sqrt{2p}}{2}$$

around. If the claim is false then the circles do not overlap. All the circles are subsetes of

$$\left[-\frac{\sqrt{2p}}{2}, p + \frac{\sqrt{2p}}{2}\right]^2$$

If they do not overlap, then the total area is less than that of the square. But

$$1.57 \approx \frac{\pi}{2}p^2 = p\pi(\frac{\sqrt{2p}}{2})^2 \leq (p + \sqrt{2p})^2 = p(1 + \sqrt{\frac{2}{p}}) \leq p(1 + \sqrt{\frac{2}{37}})^2 \approx 1.51$$

We checked the lower cases, so the claim is proved. Then pick

$$(x', y') = (|x_j - x_i|, |y_j - y_i|)$$

We then show that p divides $(x')^2 + (y')^2$, but also this number is less than $2p$, so it is p. $\square$

Chapter 2

Elementary Group Theory

In this chapter, we will introduce our first algebraic structure: the group. This will take some of the ideas we have discovered about number theory and translate it to the setting of an arbitrary set with one operation, sbuject to certain axioms which ensure the operation is "nice enough." Some motivating examples, then, will be the groups $\mathbb{Z}$ and ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, where we have already proved a few results in the preceding chapter.

2.1 Binary Operations

Definition 2.1

A **binary operation** on a set S is a function $* : S \times S \to S$.

In other words, $\star$ takes in two inputs in S and returns another. We typically denote $\star(a, b)$ as $a \star b$.

Example 2.1

- If $S = \mathbb{R}$, then we may define $a \star b = a + b$, or $a \star b = a \cdot b$.
- If S is the set of functions $f : X \to X$ for some set X, we may define $f \star g = f \circ g$.
- If S is the set of $n \times n$ matrices over a field, then the operation may be taken as addition or multiplication.

Certain operations possess properties which make them particularly nice to work with. In particular, we say that an operation $\star$ is **commutative** if $a \star b = b \star a$ for all $a, b \in S$, and it is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$. In the case that $\star$ is associative, then any finite combination of elements may be written without parentheses, as the order is irrelevant, so we may simply denote this as $a_1 \star a_2 \star \ldots \star a_n$.

Example 2.2

- Addition and multiplication are both commutative and associative on $\mathbb{R}$.
- Function composition is only associative.
- Matrix addition is commutative and associative, but multiplication is only associative.

As we see from the example above, commutativity is nice but not always present, but associativity is an extremely common property of operations that we work with often. However, for arbitrary binary operations it is not necessarily the case.

Example 2.3

Define a binary operation $\star$ on the set $S = \{0, 1\}$ by

$$\begin{cases} 0 \star 0 = 1 \\ 0 \star 1 = 1 \\ 1 \star 0 = 1 \\ 1 \star 1 = 0 \end{cases}$$

Then

$$(0 \star 1) \star 1 = 1 \star 1 = 0$$

but

$$0 \star (1 \star 1) = 0 \star 0 = 1$$

so this operation is not associative.

Definition 2.2

Let $\star$ be a binary operation on S. An element $e \in S$ is called an **identity** for $\star$ if

$$e \star x = x \star x = x$$

for all $x \in S$.

Proposition 2.1

Every binary operation has at most one identity.

Proof. Suppose e_1, e_2 are identities for $\star$ on S. Then

$$e_1 = e_1 \star e_2 = e_2$$

so $e_1 = e_2$. $\square$

Definition 2.3

Let $\star$ be a binary operation on S with identity e. Then for $x \in S$, we say that $y \in S$ is an **inverse** of x if

$$x \star y = y \star x = e$$

If x has an inverse we say it is invertible.

Proposition 2.2

For $x \in S$ with $\star$ an associative binary operation on S with identity e,

1. x has at most one inverse $y \in S$.
2. If $la = e$ and $ar = e$, then $l = r$.
3. If a, b are invertible, then $a \star b$ is invertible and $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
4. An element may have (multiple) left inverse(s) or right inverse(s), but not be invertible (but not both).

Proof.

1. Suppose y_1, y_2 are both inverses for x. Then
$$y_1 = y_1 e = y_1 x y_2 = e y_2 = y_2$$
so $y_1 = y_2$.
2. Similarly
$$l = le = lar = er = r$$
3. We have
$$(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star b = e$$
and
$$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star a^{-1} = e$$
4. Let $f : \mathbb{N} \to \mathbb{N}$ by $x \mapsto 2x$. Then let $g : \mathbb{N} \to \mathbb{N}$ be any function which halves the even naturals and assigns any value to the odd naturals. Then
$$g \circ f = \mathrm{id}$$
but $f \circ g$ is not necessarily the identity. So f has left inverses (many of them), but not right inverses.

   If an element has left and right inverses, it is invertible by 2), the inverses are equal by 2), and they are unique by 1).

□

2.2 Groups

We will now use our definition of binary operations to study sets equipped with the structure imposed by such an operation.

Definition 2.4

A **group** $(G, \star)$ consists of a nonempty set G with a binary operation $\star$ on G such that

1. $\star$ is associative.
2. There exists $e \in G$ which is an identity for $\star$.
3. For each $g \in G$, there exists an inverse element $h \in G$ for g under $\star$.

Under a slight abuse of notation, we will typically refer to $(G, \star)$ as G when the operation is clear.

Noting that we only required that $\star$ be associative, but not commutative, we give a special name for groups where $\star$ is commutative.

Definition 2.5

$(G, \star)$ is called **abelian** if $\star$ is commutative on G.

Let us make a few comments about notation. In general, e represents the identity of $\star$. However, we may sometimes write $+$ to denote a commutative operation and 0 its identity, and $\cdot$ an arbitrary operation with identity 1. When $\star$ is abelian we may write $-g$ to denote the inverse of g, and g^{-1} otherwise. We will also denote the n-fold repeated composition $\underbrace{g \star \ldots \star g}_{n \text{ times}}$ as ng for abelian groups and g^n for arbitrary groups.

Example 2.4

The following are examples of abelian groups:

- $(\mathbb{Z}, +)$
- $(\mathbb{F}, +)$
- $(\mathbb{F} \setminus \{0\}, \times)$
- $(M_{n \times m}(\mathbb{F}), +)$

The following are examples of nonabelian groups:

- $(\mathrm{GL}_n(\mathbb{R}), \times)$, where $\mathrm{GL}_n(\mathbb{R})$ is the set of $n \times n$ invertible real matrices.
- $(\mathrm{SL}_n(\mathbb{Z}), \times)$, where $\mathrm{SL}_n(\mathbb{Z})$ is the set of $n \times n$ matrices with determinant 1 and integer entries.
- S_n, where S_n is the group of **permutations** (a permutation on S is a bijection $f : S \to S$) on n elements.
- D_n, where D_n is the group of symmetries of the n-gon.[a]

[a]This is sometimes referred to as D_{2n}, since it has $2n$ elements.

Some other important matrix groups, which will not necessarily be important in this class, are:

- O_n, which is the set of real orthogonal matrices.
- SO_n, which is the set of real orthogonal matrices with determinant 1.
- U_n which is the set of complex orthogonal matrices.
- SU_n, which is the set of complex orthogonal matrices with determinant 1.
- SP_{2n}, which is the set of $P \in \mathrm{GL}_{2n}(\mathbb{R})$ such that $P^T SP = S$ for all S.[1]
- $O_{3,1}$ (the Lorentz group), which is the set of $P \in \mathrm{GL}_4(\mathbb{R})$ with $P^T I_{3,1} P = I_{3,1}$.

Definition 2.6

The **order** of an element $g \in G$ is the smallest natural number $n \in \mathbb{Z}_{>0}$ such that

$$g^n = e$$

If no such number exists, then g has infinite order.

Definition 2.7

The **order** of a group G is the number of elements in G.

Although the word order appears to be used for different notions here, we will see that the order of $g \in G$ is the order of the subgroup $\langle g \rangle$ generated by g.

Consider the set $\mathbb{Z}/n\mathbb{Z}$. Under addition, it is an abelian group, but under multiplication it is not, since there are inverses missing. However, removing $\{0\}$ is not sufficient. For instance, consider $\overline{4} \in \mathbb{Z}/24\mathbb{Z}$. Every multiple of 4 mod 24 is a multiple of 4, so 1 is not equal to $n4$ for any $n \geq 1$. This only works when n is prime, which is why $\mathbb{F}_p$ is only a group for p prime. Alternatively, we can fix the set as follows:

Definition 2.8

Define $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times := \{\overline{a} | a \in \mathbb{Z}, \gcd(a, n) = 1\}$.

Then $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \times\right)$ is a group. Moreover, its order is $\phi(n)$, where $\phi(n)$ is Euler's totient function.

[1] Here, S is the matrix of a certain nondegenerate skew-symmetric bilinear form in a certain basis.

Example 2.5

For $n = 5$, $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times = \{1, 2, 3, 4\}$. In particular, if p is prime then $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ contains all nonzero elements.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The orders of of 1, 2, 3, 4 are 1, 4, 4, and 2, respectively.

Note that the interior of the table above resembles a Sudoku board, in the sense that each row and column contains each of the elements 1, 2, 3, 4 exactly once.

Lemma 2.3

Let G be a finite group $G = \{g_1, \dots, g_n\}$. Then the elements $gg_1, gg_2, \dots, gg_n$ are a permutation of $g_1, \dots, g_n$.

Proof. We need to show that $\phi_g : G \to G$ given by $\phi_g(x) = gx$ is a bijection. But if we consider $\phi_{g^{-1}}$, we have

$$(\phi_g \circ \phi_{g^{-1}})(x) = gg^{-1}x = x$$

and

$$(\phi_{g^{-1}} \circ \phi_g)(x) = g^{-1}gx = x$$

so ϕ_g has an inverse and is thus a bijection. $\square$

Corollary 2.4

Let G be a finite abelian group of order n. Then for $g \in G$, $g^n = e$.

Proof. Since G is abelian,

$$(gg_1)(gg_2)\dots(gg_n) = g^n(g_1g_2\dots g_n)$$

and by Lemma 2.3,

$$(gg_1)(gg_2)\dots(gg_n) = g_1g_2\dots g_n$$

so $g^n = e$ by cancellation. $\square$

Though the above proof is only valid for abelian groups, the conclusion is actually true of all groups. We will see that this follows from Lagrange's Theorem.

Note that the above corollary applied to $\left(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times\right)$ recovers Fermat's Little Theorem, and applied to $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \times\right)$ for arbitrary n recovers Euler's Theorem.

Definition 2.9

A subgroup of a group $(G, \star)$ is a group $(H, \star|_H)$, where $H \subseteq G$ and $\star_H$ is the restriction of $\star$ to $H \times H$. We will sometimes write $H \leqslant G$.

Equivalently, we have the following condition, which will allow for easier verification of subgroups.

Proposition 2.5

$H \subseteq G$ is a subgroup of G if and only if

1. $a, b \in H$ implies that $a \star b \in H$.
2. $e \in H$.
3. $a \in H$ implies $a^{-1} \in H$.

Proof. The other axioms are inherited from the fact that $(G, \star)$ is a group. □

Note that if H is nonempty, then 2 follows from 1 and 3.

Example 2.6

- $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under $+$.
- $\mathrm{SL}_n(\mathbb{R}) \leqslant \mathrm{GL}_n(\mathbb{R})$.
- $\{\overline{0}, \overline{2}\} \leqslant \mathbb{Z}/4\mathbb{Z}$.

Definition 2.10

Let $(G, \star_G), (H, \star_H)$ be groups. Then the **product group** of G and H is the Cartesian product $G \times H$, with the operation

$$(g_1, h_1) * (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2)$$

Example 2.7

The multiplication table for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

2.3 Special Groups

Here we will develop some theory of the groups $\mathbb{Z}, D_n$, and $\mathbb{F}_p^\times$.

Theorem 2.6

The only subgroups of $\mathbb{Z}$ are $\{0\}$ and $a\mathbb{Z}$ for some $a \in \mathbb{N}$.

Proof. Suppose $S \leqslant \mathbb{Z}$. Pick some $a \in S$ to be the smallest positive number in S. Then $a\mathbb{Z} \subseteq S$ by closure. Now pick any $n \in S$. Then apply Euclidean division to write $n = aq + r$ where q, r are integers. But $aq \in S$, so $r \in S$, but $0 \leq r \leq a - 1$, and a was chosen to be the smallest positive number, so $r = 0$ and thus $n = aq$. So $S \subseteq a\mathbb{Z}$. Thus $S = a\mathbb{Z}$. □

This allows us to reprove Bezout's identity in the setting of groups.

Corollary 2.7: Bezout's Identity

If $a, b \in \mathbb{Z}$ then $ra + sb = \gcd(a, b)$ admits a solution $r, s \in \mathbb{Z}$.

Proof. Observe that the set $a\mathbb{Z} + b\mathbb{Z} = \{ra + sb | r, s \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. Then by Theorem 2.6, $S = d\mathbb{Z}$ for some d.

Claim: $d = \gcd(a, b)$. To see this, note that $a \in S = d\mathbb{Z}$ and $b \in d\mathbb{Z}$ so d is a common divisor of a, b. Moreover, $d \in a\mathbb{Z} + b\mathbb{Z}$ so $d = ra + sb$ and thus any common divisor of a, b divides d. So $\gcd(a, b) = d$. It follows that $ra + sb = \gcd(a, b)$ has a solution with $r, s \in \mathbb{Z}$. □

Recall that D_n is the set of symmetries of the n-gon, which consist of rotations by $2\pi/n$, reflection, and combinations thereof.

Example 2.8

D_3 is the symmetry group of the triangle, whose elements are the identity, rotation by $2\pi/3$, and rotation by $4\pi/3$, as well as reflections over the lines between each vertex and the opposite side.

Example 2.9

D_4 has rotation by $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$. The reflections are those over lines between opposing vertices, and between midpoints of opposing sides.

Note that the reflections are slightly different when n is odd and when n is even. Recall also that a reflection over ℓ followed by a reflection over ℓ' is a rotation by 2α, where α is the angle between ℓ and ℓ'. It follows that reflection over ℓ followed by rotation by α is reflection over ℓ', where ℓ and ℓ' make an angle of $\alpha/2$. As a result, we adopt the following notation: we write refl_γ to denote reflection over the line through the origin which makes an angle of $\gamma/2$ with the x-axis.

Thus

$$D_3 = \{\mathrm{rot}_0, \mathrm{rot}_{2\pi/3}, \mathrm{rot}_{4\pi/3}, \mathrm{refl}_0, \mathrm{refl}_{2\pi/3}, \mathrm{refl}_{4\pi/3}\}$$

Then we have

Proposition 2.8

1. $\mathrm{rot}_\beta \circ \mathrm{refl}_\gamma = \mathrm{refl}_{\beta+\gamma}$
2. $\mathrm{refl}_\gamma \circ \mathrm{rot}_\beta = \mathrm{refl}_{\gamma-\beta}$
3. $\mathrm{refl}_{k\alpha} = (\mathrm{rot}_\alpha)^k \circ \mathrm{refl}_0$

It follows that D_n may be written as $\{e, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$, where $x = \mathrm{rot}_{2\pi/n}$ and $y = \mathrm{refl}_0$. Thus we say that D_n is generated by x, y under the relations $x^n = e, y^2 = e, xyx = y$.

Theorem 2.9

For $(\mathbb{F}_p)^\times = \{1, \ldots, p-1\}$, there exists an element $g \in (\mathbb{F}_p)^\times$ such that $\mathbb{F}_p^\times = \{1, g, g^2, \ldots, g^{p-1}\}$.

Proof. We will prove this later. □

Example 2.10

For $\mathbb{F}_5$, the choices $\overline{2}, \overline{3}$ both work. Then we say that $\mathbb{F}_p$ is generated by g with the relation $g^4 = \overline{1}$.

2.4 Elliptic Curves (∗)

Definition 2.11

An **elliptic curve** over $\mathbb{R}$ is a set E of the form

$$E = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}$$

where $a, b \in \mathbb{R}$ satisfy $4a^3 + 27b^2 \neq 0$ and ∞ is a point at infinity in the projective plane (for now, we may just take it symbolically).

The requirement $4a^3 + 27b^2 \neq 0$ ensures that no cusps form, so the curve is smooth.

The key point about elliptic curves is that we may endow them with a group structure according to the following:

Definition 2.12

Let $P, Q \in E$ be points which are not ∞. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. The define the following operations:

1. $-P$ is defined as $(x_P, -y_P)$. Since E is symmetric over the x-axis, this is in E.
2. If $P \neq Q$, then the line through $P + Q$ intersects the curve in three locations. Let R be the third point of intersection. Then $P + Q \coloneqq -R$.
   (a) If $P = Q$, then we take this line to be the tangent line of E at P.
   (b) If this line is vertical, then it only intersects E twice, so we take $P+Q = \infty$.
3. For any P, $\infty + P \coloneqq P$.

Theorem 2.10

The set E with the operation as defined above is a group, and moreover it is abelian.

Proof. The main thing to prove is that the operation here is associative. This follows from the Cayley-Bacharach theorem (see the MAT 217 notes). □

Example 2.11

Consider the curve $y^2 = x^3 - 5x$. Then take the points $(0, 0)$ and $(-1, 2)$. The line through them is the line $y = -2x$ or $2x + y = 0$. Then the simultaneous solutions to this and E are

$$4x^2 = x^3 - 5x \implies x(x^2 - 4x - 5) = 0 \implies x = 0, -1, 5$$

so our potential points are $(0, 0), (-1, 2), (5, -10)$. Since the first two points are P, Q, we have $R = (5, -10)$ and $P + Q = -R = (5, 10)$.

We can also consider the same definition of the operation, but work in a field other than $\mathbb{R}$.

Example 2.12

Let $y^2 = x^3 + 3x + 4$ be a curve in $\mathbb{Z}/7\mathbb{Z}$. By checking all pairs, the only points in this curve is

$$(\overline{0}, \overline{2}), (\overline{0}, \overline{5}), (\overline{1}, \overline{1}), (\overline{1}, \overline{6}), (\overline{2}, \overline{2}), (\overline{2}, \overline{5}), (\overline{5}, \overline{2}), (\overline{5}, \overline{5}), (\overline{6}, \overline{0}), \infty$$

so E is a group of order 10.

We now discuss an application of elliptic curves to cryptography. Pick some elliptic curve E and a point $P \in E$, and consider the map from $k \in \mathbb{N}$ to $kP \in E$. This can be calculated in $\log k$ time using binary addition. Consider the reverse question: if we know Q

is a multiple of P, then how do we find k such that $Q = kP$? This turns out to be a very difficult problem, which makes elliptic curves powerful for encryption.

Example 2.13

Consider the following encryption scheme. Alice and Bob together pick a public elliptic curve E and public point $P \in E$. Each picks a point $Q_A = d_A P, Q_B = d_B P$, where $d_A, d_B \in \mathbb{N}$ are both private but Q_A, Q_B are public. Then Alice can calculate $d_A Q_B = dAd_B P$, and Bob can calculate $d_B Q_A = d_B d_A P$, so Alice and Bob can both find the x-coordinate of $d_A d_B P$, but this is nearly impossible to solve without finding one of d_A, d_B.

The above algorithm serves as a powerful encryption scheme which is both faster and stronger than RSA.

2.5 Group Homomorphisms

In this section, we investigate homomorphisms, which can generally be seen as structure respecting maps. We will see that studying the homomorphisms between groups will allow us to better understand their underlying structures.

Definition 2.13

If $(G, \star_G), (H, \star_H)$ are groups, then $\phi : G \to H$ is a **group homomorphism** if for all $a, b \in G$ we have

$$\phi(a \star_G b) = \phi(a) \star_H \phi(b)$$

Example 2.14

- $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$.
- $\exp : \mathbb{R} \to \mathbb{R}^\times$.
- $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$.
- $\mathrm{tr} : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $x \mapsto \overline{x}$.
- $\sigma : D_n \to \{\pm 1\}$ which takes α to $+1$ if it preserves orientation and -1 otherwise.

Example 2.15

The function $\det : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ is not a homomorphism when $\mathbb{R}$ is an additive group, since $\det(A + B) \neq \det(A) + \det(B)$.

We can prove some basic facts about homomorphisms:

Proposition 2.11

If G, H are groups with respective identities e_G, e_H, and $\phi : G \to H$ is a homomorphism, then

1. $\phi(e_G) = e_H$.
2. $\phi(a^{-1}) = [\phi(a)]^{-1}$

Proof. 1. $e_H\phi(e_G) = \phi(e_Ge_G) = \phi(e_G)\phi(e_G)$ so $e_H = \phi(e_G)$ by cancellation.

2. $e_H = \phi(e_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ so $\phi(a^{-1}) = [\phi(a)]^{-1}$.

□

Example 2.16

If V is a vector space, then any linear map from $V \to V$ is a homomorphism on $(V, +)$.

Definition 2.14

Given a homomoprhism $\phi : G \to H$, the **kernel** of ϕ is the preimage of e_H, defined as

$$\ker\phi = \{g \in G | \phi(g) = e_H\} \subseteq G$$

Proposition 2.12

$\phi : G \to H$ is injective if and only if $\ker\phi = \{e_G\}$.

Proof. ($\implies$) Let $a \in \ker\phi$. Then $\phi(a) = e_H = \phi(e_G)$ so $a = e_G$.

($\impliedby$) Suppose $\ker\phi = \{e_G\}$. Then let a, b be such that $\phi(a) = \phi(b)$. Since ϕ is a homomorphism,

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)[\phi(b)]^{-1} = e_H$$

So $ab^{-1} = e_G$ and thus $a = b$. □

We will now begin to prove results that highlight the close relationships between group homomorphisms and subgroups.

Proposition 2.13

Let $\phi : G \to H$ be a group homomorphism. Then $\ker\phi \leqslant G$.

Proof. $\phi(e_G) = e_H$ so $e_G \in \ker\phi$.

Let $g_1, g_2 \in \ker\phi$. Then $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = e_He_h = e_H$, so $g_1g_2 \in \ker\phi$.

Let $g_1 \in \ker\phi$. Then $\phi(g_1^{-1}) = [\phi(g_1)]^{-1} = e_H^{-1} = e_H$ so $g_1^{-1} \in \ker\phi$. Thus $\ker\phi$ is a subgroup. $\square$

Example 2.17

Using the homomorphisms listed in Example 2.14,

- $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ has kernel $\mathrm{SL}_n(\mathbb{R})$.
- $\exp : \mathbb{R} \to \mathbb{R}^\times$ has kernel $\{0\}$.
- $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$ has kernel S^1.
- $\mathrm{tr} : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ has kernel $\mathrm{sl}_n(\mathbb{R})$.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $x \mapsto \overline{x}$ has kernel $n\mathbb{Z}$.
- $\sigma : D_n \to \{\pm 1\}$ which takes α to $+1$ if it preserves orientation and -1 otherwise has kernel given by the rotations in D_n.
- For a homomorphism $\mathbb{Z} \to G$ given by $n \to g^n$ for fixed g, the kernel is 0 if g has infinite order, or $\mathrm{ord}(g)\mathbb{Z}$ if $\mathrm{ord}(g)$ is finite.

Proposition 2.14

Let $\phi_1 : G \to H_1$ and $\phi_2 : G \to H_2$ be homomorphisms. Then $g \mapsto (\phi_1(g), \phi_2(g))$ is a homomorphism from G to $H_1 \times H_2$.

The concept of homomorphisms allow for a convenient proof of the Chinese Remainder Theorem (proved in homework using modular arithmetic).

Theorem 2.15: Chinese Remainder Theorem

Let $n, m \in \mathbb{Z}_{>0}$ with $\gcd(n,m) = 1$, and let ϕ_1, ϕ_2 be the canonical quotient maps $\phi_1 : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and $\phi_2 : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, where

$$\begin{cases} \phi_1\left(\overline{a}_{\mathbb{Z}/nm\mathbb{Z}}\right) = \overline{a}_{\mathbb{Z}/n\mathbb{Z}} \\ \phi_2\left(\overline{a}_{\mathbb{Z}/nm\mathbb{Z}}\right) = \overline{a}_{\mathbb{Z}/m\mathbb{Z}} \end{cases}$$

Then we construct a homomorphism $\phi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ using Proposition 2.14. ϕ is a bijection.

Proof. Note that $\mathbb{Z}/nm\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ have the same number of elements. Thus it suffices to prove that $\ker\phi = \overline{0}$, since if ϕ is injective it must be bijective by the pigeonhole principle.

Let $\overline{a}_{\mathbb{Z}/nm\mathbb{Z}} \in \ker\phi$. Then $\phi\left(\overline{a}_{\mathbb{Z}/nm\mathbb{Z}}\right) = (\overline{0}, \overline{0})$. Thus $\overline{a}_{\mathbb{Z}/n\mathbb{Z}} = \overline{a}_{\mathbb{Z}/m\mathbb{Z}} = \overline{0}$. So $n|a, m|a$. Since

n, m are coprime, $nm|a$. Thus $\overline{a}_{\mathbb{Z}/nm\mathbb{Z}} = \overline{0}$. So we are done. $\square$

Definition 2.15

Let $\phi : G \to H$ be a group homomorphism. Then define the **image** of ϕ to be

$$\operatorname{im}\phi = \phi(G) = \{\phi(g) | g \in G\} \subseteq H$$

Proposition 2.16

If $\phi : G \to H$ is a homomorphism, then $\operatorname{im}\phi \leqslant H$.

Proof. $\phi(e_G) = e_H$ so $\operatorname{im}\phi$ contains the identity. Let $x, y \in \operatorname{im}\phi$. Then $x = \phi(a), y = \phi(b)$ for some $a, b \in G$. Then $\phi(ab) = \phi(a)\phi(b) = xy$ so $xy \in \operatorname{im}\phi$, and $\phi(a^{-1}) = [\phi(a)]^{-1} = x^{-1}$ so $\operatorname{im}\phi$ contains inverses. $\square$

2.6 Isomorphisms

Having discussed homomorphisms (maps which respect the underlying group structure), we will now discuss isomorphisms (maps that preserve the underlying group structure).

Definition 2.16

$\phi : G \to H$ is an **isomorphism** if it is a group homomorphism and a bijection. We say that G, H are **isomorphic** (denoted $G \cong H$) if there exists an isomorphism between them.

Example 2.18

The set of rotations by $k \cdot \frac{\pi}{2}$ for $k \in \mathbb{Z}$ has an isomorphism with $z \bmod 4$. To see this, send $\overline{k} \mapsto \mathrm{rot}_{k\pi/2}$. This is well defined, since if $\overline{k} = \overline{l}$, then $k \equiv l \pmod 4$, and thus $\mathrm{rot}_{k\pi/2} = \mathrm{rot}_{l\pi/2}$. It is also a homomorphism, since $\overline{k} + \overline{l} \mapsto \mathrm{rot}_{(k+l)\pi/2} = \mathrm{rot}_{k\pi/2} \circ \mathrm{rot}_{l\pi/2}$. It is a bijection since both groups have four elements.

To justify why it makes sense to speak of G, H be isomorphic with no reference to direction, we show the following:

Lemma

If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism.

Proof. Clearly ϕ^{-1} is bijective. Let $x, y \in H$. Then $x = \phi(a), y = \phi(b)$ for appropriate a, b. Since ϕ is a homomorphism, $\phi(ab) = \phi(a)\phi(b)$. So

$$\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(x)\phi^{-1}(y) \qquad \square$$

The intuition behind isomorphic groups is that although the elements themselves are not necessarily equal, they can be renamed in such a way that the multiplication tables look the same. Thus, the groups have the same group structure. As long as we are making statements about the structure of groups, it suffices to prove something up to isomorphism.

Example 2.19

Let us show that $\left(\mathbb{Z}/8\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The elements which have gcd of 1 with 8 are precisely the odd elements. So $\mathbb{Z}/8\mathbb{Z} = \{1, 3, 5, 7\}$. Define a map by

$$\begin{aligned}
\overline{1} &\mapsto (\overline{0}, \overline{0}) \\
\overline{3} &\mapsto (\overline{0}, \overline{1}) \\
\overline{5} &\mapsto (\overline{1}, \overline{0}) \\
\overline{7} &\mapsto (\overline{1}, \overline{1})
\end{aligned}$$

Referring to the composition tables shows this is a homomorphism, and isomorphism follows since they have the same number of elements.

We can isolate the group structure of a given group by using **group presentations**, which list the relations between generators which determine the structure of a group.

Example 2.20

In the above example, if we write $e = (0, 0), x = (0, 1), y = (1, 0)$, then this group is subject to (and completely determined by) the relations $2x = e, 2y = e, x + y = y + x$. The group $\left(\mathbb{Z}/8\mathbb{Z}\right)^\times$ is also subject to these relations. Thus the groups are isomorphic.

Example 2.21

The torus is bijective to $S^1 \times S^1$. This induces a group structure on the torus.

Example 2.22

Consider a complex elliptic curve $E_\mathbb{C}$ defined by $y^2 = x^3 + 1$. If $x = a + bi, y = c + di$, then $E_\mathbb{C} \subseteq \mathbb{C}^2 \cong \mathbb{R}^4$. We can split this into two equations on a, b, c, d, using the real and imaginary parts, respectively. Then $E_\mathbb{C}$ should be a two dimensional locus. One can show that $E_\mathbb{C}$ is bijective with the torus, but moreover that it is isomorphic in the category of groups. (We can see this by considering real elliptic curves as horizontal cross sections of a complex curve. Looking at the shape generated in projective space this way shows that it is vaguely torus-like.)

2.7 Cyclic Groups

In this section, we consider cyclic groups, which are particularly simple groups that allow for easy calculations.

Proposition 2.17

Every subgroup of $\mathbb{Z}/_{n\mathbb{Z}}$ is of the form $\langle \overline{d} \rangle = \{\overline{kd} | k \in \mathbb{Z}\}$ where $d|n$. Moreover, the order of $\overline{d}$ is $\frac{n}{d}$.

Definition 2.17

The **generated subgroup** of G generated by $g \in G$ is the subgroup

$$\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$$

Example 2.23

The generated subgroup

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \subseteq \mathrm{GL}_n(\mathbb{R})$$

has infinite order, since

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

so this is isomorphic to $\mathbb{Z}$.

Definition 2.18

A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$.

Theorem 2.18

Let $\langle x \rangle \subseteq G$ be finite. Then there exists $d \in \mathbb{N}$ such that $x^d = e$ and $\langle x \rangle = \{e, x, x^2, \ldots, x^{d-1}\}$ where $x^i, 0 \leq i < d$ are distinct.

Proof. If $\langle x \rangle$ is finite then there exists $n < m \in \mathbb{Z}$ with $x^n = x^m$. Then $x^{m-n} = e$. Set d to be the smallest positive integer such that $x^d = e$. Pick some $x^a \in \langle x \rangle$. We may write $a = dq + r$ by the division algorithm, and $x^a = x^{dq+r} = (x^d)^q \cdot x^r = x^r$.Thus $\langle x \rangle = \{e, x, \ldots, x^{d-1}\}$. To see that they are distinct, suppose $x^i = x^j$ for $0 \leq i \leq j < d$. Then $x^{j-i} = e$. But d is the smallest positive integer for which this is true, and $j - i < d$, so $j - i = 0$. Thus $i = j$. $\square$

Corollary 2.19

If G is cyclic of order d, then $G \cong \mathbb{Z}/d\mathbb{Z}$.

Proposition 2.20

If G is cyclic of infinite order, then $G \cong \mathbb{Z}$.

Proof. Let g be a generator of G. Then every element of G may be written uniquely as g^n for some n (if $g^n = g^m$, then $g^{n-m} = e$ so $n = m$). Then define $\phi(g^n) = n$. This is clearly bijective. It is a homomorphism since

$$\phi(g^n) + \phi(g^m) = n + m = \phi(g^{n+m})$$

□

This important result means that when considering cyclic groups, the structure is completely determined by the order of the group.

2.8 Permutations

Definition 2.19

A **permutation** on n elements is a bijection from $\{1, 2, \dots, n\}$ to itself. The set of all permutations on n elements is denoted S_n.

Proposition 2.21

$|S_n| = n!$.

We will notate permutations in a few ways. To be completely explicit, we may write

$$\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

where $i \mapsto k_i$. Alternatively, we may write

$$(a_1 a_2 \dots a_t)$$

where $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, and so on, with $a_t \mapsto a_1$. Note that if an element is fixed by a permutation, we do not list it in this notation.

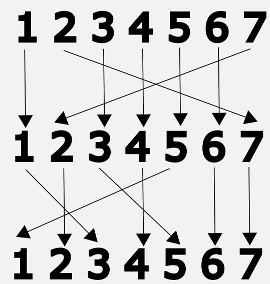
Definition 2.20

A **transposition** or 2-cycle is a permutation of the form (ab).

Since permutations are functions, we can juxtapose them to denote composition.

Example 2.24

Consider the permutation $(135)(27) \in S_7$. By following where each element goes:



this permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 1 & 6 & 2 \end{pmatrix}$$

Example 2.25

Given the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 2 & 4 & 7 & 5 \end{pmatrix}$$

we may use cycle notation to write this as $(26754)(13)$.

Example 2.26

The group S_3 contains the cycles

$$S_3 = \{e, (12), (23), (13), (123), (132)\}$$

Note that $(123) = (231)$.

Proposition 2.22

Every permutation can be written as a composition of disjoint cycles (where disjoint cycles have no elements in common). Moreover, disjoint cycles commute.

To write a permutation in disjoint cycle notation, we can use the following process: begin by writing the number 1. Evaluate the permutation to see where 1 is mapped to, and write down that number. See where that number is mapped to, and write down the next. Continue until we return to 1. Then, in a new cycle, write the next number which wasn't listed in the first cycle. Continue until all numbers have been exhausted. This not only proves that disjoint cycle decomposition exists, but also that it is unique (up to ordering).

Proposition 2.23

Every permutation can be written as a product of (not necessarily disjoint) transpositions.

Proof. Let $(a_1a_2\dots a_n)$ be a cycle. Then $(a_1a_2\dots a_n) = (a_1a_2)\dots(a_{n-2}a_{n-1})(a_{n-1}a_n)$. Reading right to left, each element a_k will get transposed once into a_{k+1}, except a_n, which moves in all the transpositions and ends up at a_1. $\square$

Proposition 2.24

Let π be the identity permutation on n elements. If $\tau_1, \dots, \tau_,$ are transpositions and $\pi = \tau_1 \dots \tau_l$, then l is even.

Proof. It suffices to prove that π may be written as $l-2$ transpositions. Then if l were odd, we could write π as a single transposition, which is clearly false.

Pick any $i \in \{1, \dots, n\}$ which is in one of the transpositions other than τ_1. Let $\tau_m = (ij)$ be the last transposition where it appears, such that $\tau_{m+1}, \dots, \tau_l$ do not permute i. Consider τ_{m-1}.

1. If $\tau_{m-1} = \tau_m$, then we can cancel them and we are done.
2. If $\tau_{m-1} = (ik)$, where $k \neq i, j$, then

$$\pi = \tau_1 \dots (ik)(ij) \dots \tau_l = \tau_1 \dots (ij)(kj) \dots \tau_l$$

   So we have moved the last transposition where i appears to position $m-1$.
3. If $\tau_{m-1} = (kj)$, where $k \neq i, j$, then

$$\pi = \tau_1 \dots (kj)(ij) \dots \tau_l = \tau_1 \dots (ik)(kj)$$

   and again we have moved up the last transposition.
4. If $\tau_{m-1} = (ab)$ for $a, b \neq i, j$, then disjoint cycles commute so

$$\pi = \tau_1 \dots (ab)(ij) \dots \tau_l = \tau_1 \dots (ij)(ab) \dots \tau_l$$

In any of Cases 2, 3, 4, we simply repeat the process with our new decomposition at π. At some point we must reduce to Case 1, otherwise i only appears in one transposition, which is impossible since π is the identity. Thus the claim is proved. $\square$

Proposition 2.25

If $\sigma \in S_n$ and $\sigma = \tau_1 \dots \tau_k = \tau_1' \dots \tau_j'$ for τ_i, τ_i' transpositions, then k, j have the same parity.

Proof. We have

$$\pi = \sigma\sigma^{-1} = \tau_1 \dots \tau_k(\tau'_j) \dots (\tau'_1)$$

(since transpositions are their own inverses). But this implies that $j + k$ is even, which means they have the same parity. $\square$

Then we may define

Definition 2.21

If $\tau \in S_n$ is written as a product of an even number of transpositions, it is called an **even permutation**. The same is true for an **odd permutation**. Then the **sign** of τ is $+1$ if τ is even and -1 if it is odd.

Definition 2.22

The set $A_n \subseteq S_n$ is the set of all even permutations.

Note that $A_n = \ker(\mathrm{sgn})$, so $A_n \leqslant S_n$.

Example 2.27

A_3 consists of $\{e, (123), (132)\}$, which is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and also the group of rotations of a triangle.

2.9 Cosets and Lagrange's Theorem

In this section, we will prove Lagrange's Theorem, a powerful result that will reveal many facts about the structure of subgroups. In doing so, we will also cover cosets, which will allow us to consider quotient groups later. First, we will make a few observations about equivalence relations, which are not specific to the setting of groups.

Definition 2.23

A **equivalence relation** on a nonempty set X is a relation[a] $\sim$ such that $\sim$ is:

1. Reflexive: $a \sim a$ for all $a \in X$
2. Symmetric: $a \sim b \implies b \sim a$.
3. Transitive: $a \sim b$ and $b \sim c$ implies $a \sim c$.

[a] Recall that a relation is a subset R of $X \times X$, where we write $a \sim b$ when $(a, b) \in R$

Definition 2.24

If $\sim$ is an equivalence relation on X and $a \in X$, then the **equivalence class** of a under $\sim$ is

$$C_a \coloneqq \{x \in X : x \sim a\}$$

Example 2.28

The relation $a \equiv b \pmod{n}$ is an equivalence relation on $\mathbb{Z}$. If we take $n = 3$, then the equivalence classes are

$$\begin{aligned} C_0 &= 3\mathbb{Z} \\ C_1 &= 1 + 3\mathbb{Z} \\ C_2 &= 2 + 3\mathbb{Z} \\ C_3 &= 3 + 3\mathbb{Z} = 3\mathbb{Z} = C_0 \\ C_4 &= 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z} = C_1 \\ &\vdots \end{aligned}$$

Thus we see that the equivalence class of any k is either C_0, C_1, C_2.

Proposition 2.26

If $a, b \in X$ then either $C_a = C_b$ or $C_a \cap C_b = \varnothing$. Moreover, $C_a = C_b$ if and only if $a \sim b$. As a result, X is the disjoint union of equivalence classes.

An equivalent idea is that if we know that X is the disjoint union of some sets X_i, then this induces an equivalence relation (where $a \sim b$ if and only if a, b are in the same X_i). Thus we see that partitions of a set are intrinsically linked with equivalence relations on a set.

Definition 2.25

Let $K \leqslant G$. Then define the left and right K-**cosets** of b to be

$$\begin{aligned} bK &= \{bk : k \in K\} \\ Kb &= \{kb : k \in K\} \end{aligned}$$

The intuition here is that a K-coset is a copy of K, translated by a. This is similar to the cosets of a subspace in a vector space.

Example 2.29

Let $G = D_3$, and let K be the subgroup of rotations. Let y be reflection along the x-axis. Then $G = K \sqcup yK$.

Example 2.30

Let $G = \mathbb{Z}$ and let $K = 3\mathbb{Z}$. Then the cosets are $3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$ (left and right cosets clearly coincide when G is abelian.)

Proposition 2.27

Let $K \leqslant G$. Then the following are equivalent:

1. $aK = bK$.
2. $b^{-1}aK = K$.
3. $b^{-1}a \in K$.
4. $aK \cap bk \neq \varnothing$.

Proof. ($1 \iff 2$) This is clear by multiplying on the left by b^{-1}.

($2 \implies 3$) $b^{-1}a \in b^{-1}aK = K$.

($3 \implies 2$) Sudoku rule.

($3 \implies 4$) If $b^{-1}a \in K$ then $b(b^{-1}a) \in bK$, but this is also $a \in aK$.

($4 \implies 3$) Suppose $ak = bk'$ for $k, k' \in K$. Then we have $b^{-1}a = k'k^{-1} \in K$. $\square$

Corollary 2.28

If X, Y are left cosets for $K \leqslant G$ then they are either equal or disjoint. The same holds for right cosets.

Corollary 2.29

The left K-cosets define a partition of G:

$$G = \bigcup_{a \in G} aK$$

where either $aK = bK$ or $aK \cap bK = \varnothing$. The same holds for right cosets.

Thus we have produced a partition of G, which from above we have shown induces an equivalence relation on G. In particular, we write

$$a \sim_L b \iff aK = bK \iff b^{-1}a \in K$$

or $b - a \in K$ using additive notation. We can similarly define the right coset equivalence relation $a \sim_R b \iff ab^{-1} \in K$.

Proposition 2.30

If aK, bK are left cosets in a finite group G, then

$$|aK| = |bK|$$

The same is true for right cosets.

Proof. It suffices to show that $|aK| = |K|$. We have $K = \{k_1, \ldots, k_m\}$ with $|K| = m$. By definition, $aK = \{ak_1, \ldots, ak_m\}$. But each ak_i is distinct, since $ak_i = ak_j \implies k_i = k_j$. Thus $|aK| = m$. $\square$

This discussion leads us to the following powerful theorem:

Definition 2.26

Let $K \leqslant G$ and define $[G : K]_L$ to be the number of left K-cosets. Similarly define $[G : K]_R$.

Theorem 2.31: Lagrange's Theorem

If $K \leqslant G$ and G is finite, then

$$|G| = [G : K]_L |K| = [G : K]_R |K|$$

Proof. Since G partitions into distinct cosets, let $\mathcal{L}$ be the set of all left K-cosets. Then

$$|G| = \sum_{L \in \mathcal{L}} |L| = |K| \sum_{L \in \mathcal{L}} 1 = [G : K]_L |K|$$

The same is true for right cosets. $\square$

Corollary 2.32

Lagrange's Theorem has the following immediate consequences:

1. $|K|$ divides $|G|$.
2. $[G : K]_L = [G : K]_R$ (thus we will only write $[G : K]$).
3. If $g \in G$ and $|G| = n$, then $\mathrm{ord}(g)|n$.
4. $g^n = e$ for all $n \in G$.
5. If $|G|$ is prime, then G is cyclic.

Proof. (1) and (2) are obvious from the equation.

For (3), $\langle g \rangle = \{e, g, \ldots, g^{m-1}\}$. This is a subgroup of G, so m divides $|G|$.

(4) follows immediately.

Take some $g \in G$ which is not e. Then $\text{ord}(g)$ divides $|G|$ prime. Thus $\text{ord}(g)$ is 1 or p, but $g \neq e$ so $\text{ord}\, g = p$. Thus $G = \langle g \rangle$. $\square$

Note that (4) recovers Fermat's Little Theorem and Euler's Theorem.

2.10 Group Actions

While studying isomorphisms, we noted that the actual elements of a group are less important than the role they serve in the group's structure. We also saw that multiplication on the left or right by a certain element is a bijective mapping from G into itself. Thus, specifying the binary operation on a group is equivalent to specifying a composition rule between these maps.

In this way, it is possible to understand the entire structure of G by simply looking at these maps. We could similarly define a structure similar to this on maps from sets other than G to themselves. Now we have fully removed the elements G from this discussion, and merely consider the maps they represent and the way those maps combine.

Definition 2.27

Let $(G, \star)$ be a group. Let X be a set. Then a **group action** of G on X is a function $\cdot : G \times X \to X$ which obeys the following axioms:

1. $e \cdot x = x$.
2. $h \cdot (g \cdot x) = (h \star g) \cdot x$.

We may also use the notation $G \circlearrowright X$ to denote that G acts on X by some group action $\cdot$.

Definition 2.28

Let $G \circlearrowright X$ and $x \in X$. Then define the **orbit** of X to be the set

$$O(x) = \{g \cdot x | g \in G\} \subseteq X$$

Example 2.31

Let $S_n \circlearrowright \{1, \ldots, n\}$. If $n = 3$ and $\tau = (12)$, then $\tau \cdot 1 = 2, \tau \cdot 2 = 1, \tau \cdot 3 = 3$.

Example 2.32

Let $\mathbb{Z}/n\mathbb{Z}$ act on S^1 by rotation by $2\pi/n$. Then

$$\overline{k} = e^{i\theta} = e^{i(\theta + k\frac{2\pi}{n})}$$

Example 2.33

D_n acts on the n-gon in the natural way.

We would like to be able to speak of when this specification loses some information about G. As we cannot use isomorphisms, since X is not necessarily a group, we make the following definition:

Definition 2.29

A group action $G \circlearrowright X$ is **faithful** if the only element $g \in G$ such that $g \cdot x = x$ for every $x \in X$ is $g = e$.

Example 2.34

Suppose $\mathbb{Z}/4\mathbb{Z} \circlearrowright \mathbb{Z}/2\mathbb{Z}$ by

$$\overline{k}_{\mathbb{Z}/4\mathbb{Z}} + \overline{l}_{\mathbb{Z}/2\mathbb{Z}} := \overline{k+l}_{\mathbb{Z}/2\mathbb{Z}}$$

This is not faithful, since $\overline{2}$ acts as the identity for all $\overline{l} \in \mathbb{Z}/2\mathbb{Z}$.

Example 2.35

Let $D_4 \circlearrowright \{1,2,3,4\}$ as vertices of a square. Then $\text{refl}_{\overline{13}} \cdot 1 = 1$ and $\text{refl}_{\overline{13}} \cdot 3 = 3$, but $\text{refl}_{\overline{13}} \cdot 2 = 4$ and $\text{refl}_{\overline{13}} \cdot 4 = 2$.

In other words, a group action is faithful if every map moves some element of x.

Definition 2.30

Let $G \circlearrowright X$. Let $\text{Bij}(X) = \text{Bij}(X,X)$ be the set of bijections from X to itself. Then define the **adjoint** to be the map $g \mapsto \operatorname{ad} g$, where $\operatorname{ad} g$ is the map $x = g \cdot x$.

Example 2.36

Let $D_3 \circlearrowright \{1,2,3\}$ and denote $D_3 = \{e, x, x^2, y, xy, x^2y\}$, where x is rotation and y

is reflection over the line through 1. Then

$$\operatorname{ad} e = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases} \quad \operatorname{ad} x = \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} \quad \operatorname{ad} x^2 = \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}$$

$$\operatorname{ad} y = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases} \quad \operatorname{ad} xy = \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \quad \operatorname{ad} x^2y = \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$$

We make the following observations:

Proposition 2.33

Let $G \circlearrowright X$. Then

1. $\operatorname{ad} e = \mathrm{id}$.
2. If $g, h \in G$, then $\operatorname{ad} g \circ \operatorname{ad} h = \operatorname{ad} gh$.
3. $[\operatorname{ad} g]^{-1} = \operatorname{ad} g^{-1}$ (this shows that each $\operatorname{ad} g$ is indeed a bijection).
4. $\operatorname{ad} : G \to \operatorname{Bij}(X)$ is a homomorphism (where $\operatorname{Bij}(X)$ is a group under composition).
5. ad is injective if and only if $G \circlearrowright X$ is faithful.

Proof. 1, 2, and 3 are straightforward from the axioms. 4 follows from 2. For 5, note that $\ker \operatorname{ad} = \{g \in G : \operatorname{ad} g = \mathrm{id}\}$. But $G \circlearrowright X$ is faithful if and only if the only g such that $\operatorname{ad} g = \mathrm{id}$ is e. So $\ker \operatorname{ad}$ is trivial if and only if $G \circlearrowright X$ is faithful. $\square$

The language of group actions allows us to prove the following:

Theorem 2.34

Every finite group is isomorphic to a subgroup of S_n, where $n = |G|$.

Proof. Let $(G, \star)$ be a group. Define a group action $G \circlearrowright G$ using $g \cdot h = g \star h$. This is faithful, because if $\operatorname{ad} g = \mathrm{id}$, then $e = \operatorname{ad} ge = g \cdot e = g$ and thus $e = g$. Thus $\operatorname{ad} : G \to \operatorname{Bij}(G)$ is injective. Note that $\operatorname{Bij}(G)$ is naturally isomorphic to S_n (say under some map ϕ), so then $\phi \operatorname{ad} : G \to S_n$ is an injective homomorphism and thus $G \cong \phi \operatorname{ad} G \leqslant S_n$. $\square$

We can use similar logic to show that if $G \circlearrowright H$ is a faithful action on another group H, where the group action also respects the operation on H, then G is isomorphic to a subgroup of H.

Example 2.37

${}^{\mathbb{Z}}\!/\!{}_{n\mathbb{Z}}$ and D_n are isomorphic to subgroups of O_2. They are also isomorphic to subgroups of SO_3 (not SO_2, since reflections are not orientation preserving in only two dimensions.) There are also the subgroups T, O, I, where T is the tetrahedral symmetry group of order 12, O the octahedral symmetry group if order 24, and I the icosahedral group of 60 symmetries. These are the platonic solids. Note that the cube and octahedron have the same symmetries, as well as the dodecahedron and icosahedron.

Theorem 2.35: Orbit Theorem

Let X be a finite set, and let $G \circlearrowleft X$. Then

$$|X| = |O_1| + \ldots + |O_k|$$

where the O_i are the distinct orbits of the group action.

Proof. Define the relation $x \sim y$ when $x \in O(y)$. We claim that $\sim$ is an equivalence relation. $e \cdot x = x$ so $x \sim x$. If $x \sim y$, then $x = g \cdot y$. But then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1} \star g) \cdot y = e \cdot y = y$ so $y \sim x$. Lastly, if $x \sim y$ and $y \sim z$, then $x = g \cdot y$ and $y = h \cdot z$. Then $x = g \cdot (h \cdot z) = (g \star h) \cdot z$ and thus $x \sim z$. So membership in an orbit is an equivalence relation. Therefore, X is partitioned into disjoint orbits. The claim follows. $\square$

Example 2.38

Take a group $\{e, \mathrm{refl}_{13}\}$ and let it act on $\{1, 2, 3, 4\}$. Then $O(1) = \{1\}$ and $O(3) = \{3\}$, but $O(2) = O(4) = \{2, 4\}$. So

$$|X| = 4 = 1 + 1 + 2 = |O(1)| + |O(3)| + |O(2)|$$

Definition 2.31

Let $G \circlearrowleft X$ and let $x \in X$. Then the **stabilizer** of x is the set

$$\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

Example 2.39

If D_4 acts on $\{1, 2, 3, 4\}$, $\mathrm{Stab}(2) = \mathrm{Stab}(4) = \{\mathrm{id}, \mathrm{refl}_{24}\}$, and $\mathrm{Stab}(1) = \mathrm{Stab}(3) = \{\mathrm{id}, \mathrm{refl}_{13}\}$. Rotations are never in the stabilizer (besides id).

Proposition 2.36

$\mathrm{Stab}(x) \leqslant G$ for all $x \in X$.

Proof. $e \in \operatorname{Stab}(x)$ since $e \cdot x = x$. If $g, h \in \operatorname{Stab}(x)$, then $(g \star h) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$. Lastly, if $g \in \operatorname{Stab}(x)$, then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} \star g) \cdot x = e \cdot x = x$. So $\operatorname{Stab}(x) \leqslant G$. $\square$

Theorem 2.37: Orbit-Stabilizer Theorem

Let $G \circlearrowright X$ where G is finite. Then for all $x \in X$,

$$|G| = |O(x)| \cdot |\operatorname{Stab}(x)|$$

In particular, $|O(x)|$ divides $|G|$.

The above formula resembles Lagrange's Theorem. Thus, the proof proceeds by finding a way to embed $O(x)$ into G.

Proof. Let $x \in X$ and consider the set $G/\operatorname{Stab}(x)$ of left $\operatorname{Stab}(x)$-cosets. Define a map $G/\operatorname{Stab}(x) \to O(x)$ by

$$g \operatorname{Stab}(x) \mapsto g \cdot x$$

This map is well defined, since if $g \operatorname{Stab}(x) = g' \operatorname{Stab}(x)$, then $g^{-1}g' \in \operatorname{Stab}(x)$ and thus $g \cdot x = g \cdot (g^{-1}g' \cdot x) = g' \cdot x$.

Clearly this map is well defined, since the orbit is by definition the set of all $g \cdot x$. To show injectivity, let $g \cdot x = g' \cdot x$. Then $g^{-1} \cdot (g \cdot x) = x$. But then $g^{-1}g \in \operatorname{Stab}(x)$ so $g \operatorname{Stab}(x) = g^{-1} \operatorname{Stab}(x)$. Thus we have a bijection between $O(x)$ and $G/\operatorname{Stab}(x)$, so $|O(x)| = [G : \operatorname{Stab}(x)]$ and the conclusion follows by Lagrange's Theorem. $\square$

Example 2.40

Let I be the group of symmetries of the icosahedron. Let it act on the faces of the icosahedron. Then let f be a face and consider $\operatorname{Stab}(f)$. Each element is a rotation around the face, and there are five of them (since each face is a pentagon), so $|\operatorname{Stab}(f)| = 5$. Thus $|I| = |O(f)| \cdot |\operatorname{Stab}(f)|$. But f can be mapped to any other face (of which there are 12), so $|O(f)| = 12$. Thus $|I| = |O(f)| \cdot |\operatorname{Stab}(f)| = 12 \cdot 5 = 60$.

Example 2.41

Let D_n act on the n-gon. For any vertex, the stabilizer is the identity and the unique reflection passing through that vertex. The orbit is n. So $|D_n| = n \cdot 2$.

The following is a theorem due to Cauchy. This result will be one of the first steps toward our classification of finite groups.

Theorem 2.38

Let G be a finite group and let p prime divide $|G|$. Then there exists an element $g \in G$ of order p.

Proof. Consider the set X of p-tuples that multiply to the identity:

$$X = \left\{ (g_1, \ldots, g_p) \middle| \prod g_i = e \right\}$$

For each choice of $g_1, \ldots, g_{p-1}$, there is exactly one choice of g_p. Thus $|X| = |G|^{p-1}$.

Let $\mathbb{Z}/_{p\mathbb{Z}}$ act on X cyclically, such that $\overline{1}$ maps $(g_1, \ldots, g_p) \mapsto (g_p, g_1, \ldots, g_{p-1})$. By the orbit formula, $|G|^{p-1} = |X| = \sum_{O(x)} |O(x)|$. Each orbit is either of length 1 (if all g_i are the same), or length p. We also see this using the orbit stabilizer theorem: $|O(x)|$ divides $\left|\mathbb{Z}/_{p\mathbb{Z}}\right|$, so it must be either 1 or p. By the orbit formula,

$$|G|^{p-1} = |X| = (\#\text{ of orbits of size } 1) \cdot 1 + (\#\text{ of orbits of size } p) \cdot p$$

Now, p divides $|G|$, so it divides the right side. Thus p divides the number of orbits of size 1. Since $\{(e, \ldots, e)\}$ is one such orbit, there are at least p of them, so there exists some other element such that $\{(g, \ldots, g)\}$ is an orbit. Then $g^p = e$ by construction. ☐

The above theorem is certainly not true if p is not prime: consider the Klein four-group, which is of order 4 but has no element of order 4.

2.11 Quotient Groups

Recall that in linear algebra, the quotient space of a vector space V by a subspace W is the set of all W-cosets in V, with operations defined by picking an arbitrary representative. This was justified by the fact that the operation does not depend on the choice of representative. Unfortunately, the following is not true in general for groups. Instead, we must restrict ourselves to specific subgroups:

Definition 2.32

A subgroup $H \leqslant G$ is called **normal** if $gH = Hg$ for all $g \in G$. This can be denoted $H \trianglelefteq G$.

Proposition 2.39

A subgroup $H \leqslant G$ is normal if and only if $gHg^{-1} = H$ for all $g \in G$, if and only if $ghg^{-1} \in H$ for all $g \in G, h \in H$.

The operation ghg^{-1} is called **conjugation** by g. Roughly speaking, the condition above says that g is invariant under a change of coordinates by g.

Recall that a and b belong to the same left H-coset if and only if $aH = bH$, if and only if $b^{-1}a \in H$.

Definition 2.33

Let $H \leqslant G$. Then the **quotient** ${}^{G}\!/\!_{H}$ is defined as the set of all left H-cosets.

We can take another approach here: for each $g \in G$, define a formal symbol $\overline{g}$, and declare $\overline{g} = \overline{g'}$ if and only if g and g' are in the same left H-coset. We would like to endow G/H with a natural group structure. We might first define the following operation:

Definition 2.34

Let $H \leqslant G$. Let $\cdot$ be the operation on G. Define an operation $\star$ on ${}^{G}\!/\!_{H}$ by

$$gH \star g'H := (g \cdot g')H$$

For the above to make any sense, we must show that the above definition is independent of the choice of representative. This occurs if $H \trianglelefteq G$:

Suppose $aH = a'H$ and $bH = b'H$. The normality condition lets us switch $bH = Hb$ and $b'H = Hb'$. So

$$abH = ab'H = aHb' = a'Hb' = a'b'H$$

To check the other axioms, we have associativity inherited from G:

$$(aH \star bH) \star (cH) = abH \star cH = (ab)cH = a(bc)H = aH \star bcH = aH \star (bH \star cH)$$

Inverses and identity are also easy to check:

$$eH \star gH = egH = gH = geH = gH \star eH$$
$$gH \star g^{-1}H = (gg^{-1})H = eH$$

Example 2.42

If $G = {}^{\mathbb{Z}}\!/\!_{6\mathbb{Z}}$, then $3\left({}^{\mathbb{Z}}\!/\!_{6\mathbb{Z}}\right)$ is a subgroup. The cosets are $3\left({}^{\mathbb{Z}}\!/\!_{6\mathbb{Z}}\right), \bar{1} + 3\left({}^{\mathbb{Z}}\!/\!_{6\mathbb{Z}}\right), \bar{2} + 3\left({}^{\mathbb{Z}}\!/\!_{6\mathbb{Z}}\right)$.

Example 2.43

${}^{S_n}\!/\!_{A_n} \cong {}^{\mathbb{Z}}\!/\!_{2\mathbb{Z}}$, and the cosets are the sets of even permutations and odd permutations.

Example 2.44

Consider $\left(\mathbb{Z}/25\mathbb{Z}\right)^{\times}/\left\langle\overline{7}\right\rangle$:

$$\begin{aligned}
\left\langle\overline{7}\right\rangle &= \{\overline{1},\overline{7},\overline{24},\overline{18}\}\\
\overline{2}\left\langle\overline{7}\right\rangle &= \{\overline{2},\overline{14},\overline{23},\overline{11}\}\\
\overline{3}\left\langle\overline{7}\right\rangle &= \{\overline{3},\overline{21},\overline{22},\overline{4}\}\\
\overline{4}\left\langle\overline{7}\right\rangle &= \overline{3}\left\langle\overline{7}\right\rangle\\
\overline{6}\left\langle\overline{7}\right\rangle &= \{\overline{6},\overline{17},\overline{19},\overline{8}\}\\
\overline{7}\left\langle\overline{7}\right\rangle &= \overline{1}\left\langle\overline{7}\right\rangle\\
\overline{8}\left\langle\overline{7}\right\rangle &= \overline{6}\left\langle\overline{7}\right\rangle\\
\overline{9}\left\langle\overline{7}\right\rangle &= \{\overline{9},\overline{13},\overline{16},\overline{12}\}
\end{aligned}$$

So our cosets are

$$\left(\mathbb{Z}/25\mathbb{Z}\right)^{\times}/\left\langle\overline{7}\right\rangle = \{\left\langle\overline{7}\right\rangle,\overline{2}\left\langle\overline{7}\right\rangle,\overline{3}\left\langle\overline{7}\right\rangle,\overline{6}\left\langle\overline{7}\right\rangle,\overline{9}\left\langle\overline{7}\right\rangle\}$$

Example 2.45

Consider $S_3/\{e,(12)\}$. $\{e,(12)\}$ is a not a normal subgroup, and this is a nonexample. We have

$$(123)\{e,(12)\} = \{(123),(13)\} = (13)\{e,(12)\}$$

Now,

$$(123)(123)\{e,(12)\} = (132)\{e,(12)\}$$

but‘

$$(13)(13)\{e,(12)\} = \{e,(12)\}$$

so our operation is not well defined.

There are some conditions which allow us to skip checking for normality:

Proposition 2.40

If $H \leqslant G$ and G is abelian, $H \trianglelefteq G$.

Proposition 2.41

If $H \leqslant G$ and $[G:H]=2$, $H \trianglelefteq G$.

Proposition 2.42

If $\phi : G \to G'$ is a group homomorphism, then $\ker\phi \trianglelefteq G$.

2.12 The First Isomorphism Theorem

We conclude this chapter with an important result that unifies many of the ideas we have discussed up to this part. This is know as the first isomorphism theorem.

Definition 2.35

Let $K \trianglelefteq G$. Then the **canonical projection** map, denoted can, is the map $g \mapsto gK$.

Theorem 2.43: First Isomorphism Theorem

Let $\phi : G \to G'$ be a surjective homomorphism, and let $K = \ker\phi$. Then there exists an isomorphism $\psi : G/K \xrightarrow{\cong} G'$ such that the following diagram commutes:.

$$\begin{tikzcd} G \arrow[r, "\mathrm{can}"] \arrow[rr, bend right, "\phi"'] & G/K \arrow[r, "\psi"] & G' \end{tikzcd}$$

Proof. We know from homework that defining $\psi(gK) = \phi(g)$ is well defined. This map is surjective since ϕ is surjective. It is also injective (again from homework), so ψ is a bijection. To see that it is a homomorphism, since K is normal we have $\psi(gKg'K) = \psi(gg'K) = gg' = \psi(gK)\psi(g'K)$. From our definition of ψ it follows that $\psi \circ \mathrm{can} = \phi$. □

Corollary 2.44

Let $\phi : G \to G'$ be a homomorphism and $K = \ker\phi$. Then $\mathrm{im}(\phi) \cong G/K$, and $|G| = |K| \cdot |\mathrm{im}\,\phi|$.

Proof. Consider the corresponding map $\psi : G \to \mathrm{im}\,G$. ψ is a surjective homomorphism, so by the first isomorphism theorem, $\mathrm{im}\,G \cong G/K$. By Lagrange's Theorem, $|G| = |K| \cdot [G : K]$, and $[G : K] = \left|G/K\right|$. □

Theorem 2.45: Product Theorem

If G is a group and $M, N \trianglelefteq G$, with $M \cap N = \{e\}$ and $G = MN$ (meaning that every $g \in G$ can be written as mn for $m \in M, n \in N$). Then $G \cong M \times N$. In particular, if G is finite, it suffices to show that $|G| = |M| \cdot |N|$.

Proof. Homework. □

Example 2.46

Consider $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$. We wish to show it is congruent to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Pick

$$N = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\} \cong \mathbb{Z}/4\mathbb{Z}$$

and

$$M = \{\overline{1}, \overline{11}\} \cong \mathbb{Z}/2\mathbb{Z}$$

These are disjoint and $4 \times 2 = \left|\mathbb{Z}/15\mathbb{Z}\right|$, so $G \cong M \times N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Corollary 2.46

If $|G| = pq$ where P, q are distinct, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Proof. Homework. □

Chapter 3

Advanced Group Theory

One of the important results in group theory is the complete classification of finite simple groups. In general, it is of interest to us to classify and understand group structure as much as possible. For instance, one theorem that we will see later is the following:

Theorem: Classification of Finite Abelian Groups

Let G be finite and G be abelian. Then there exist $n_1, \ldots, n_k$ such that

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

A similar statement holds for abelian groups which are only finitely generated.

3.1 Sylow's Theorems

In this section we demonstrate three important results due to Sylow, which are known as Sylow's Thoerems.

Theorem 3.1: First Sylow Theorem

Let G be finite and p prime. Suppose p^k divides $|G|$. Then there exists a subgroup $H \leqslant G$ such that $|H| = p^k$.

In particular, subgroups of orders which are maximal possible prime orders are important enough that we give them a name:

Definition 3.1

A **Sylow p-subgroup** is a subgroup $H \leqslant G$ such that $|H| = p^k$, p^k divides $|G|$, and p^{k+1} does not divide $|G|$.

Theorem 3.2: Second Sylow Theorem

Suppose $P, K \leqslant G$ are Sylow p-subgroups. Then there exists $x \in G$ such that $P = xKx^{-1}$.

In other words, Sylow p-subgroups are conjugates of one another.

Corollary 3.3

A group G has only one Sylow p-subgroup H (for a particular p) if and only if $H \trianglelefteq G$.

Proof. ($\implies$) Suppose G has just one Sylow p-subgroup H. Then for any $x \in G$, xHx^{-1} is another subgroup of the same size, so it is also a Sylow p-subgroup. Then by assumption $xHx^{-1} = H$. This holds for all x so H is normal.

($\impliedby$) Suppose $H \trianglelefteq G$ and H, K are Sylow p-subgroups. Then $K = xHx^{-1}$ for some $x \in G$. But H is normal so $K = H$. Thus there is only one Sylow p-subgroup. $\square$

Theorem 3.4: Third Sylow Theoerm

Let n_p be the number of Sylow p-subgroups. Then n_p divides $|G|$ and $n_p \equiv 1 \pmod p$.

Remark 3.1

Let $|G| = p^k m$ where p does not divide m. Then n_p divides $p^k m$, but $n_p \equiv 1 \pmod p$ so n_p does not divide p (unless $n_p = 1$). Thus $n_p | m$ (even if $n_p = 1$).

These results allow us to completely classify all groups of some orders.

Example 3.1

We may see that the only group of size 15 is $\mathbb{Z}/15\mathbb{Z}$.

We write $|G| = 3 \cdot 5$. Thus there are Sylow p-subgroups of size 3 and 5. So $n_3 | 5$ and $n_3 \equiv 1 \pmod 3$. $n_3 = 1, 5$ but $5 \not\equiv 1 \pmod 3$ so $n_3 = 1$. Similarly $n_5 = 1$. Thus there is one Sylow 3-subgroup and one Sylow 5-subgroup. Then let H, K be the unique Sylow 3- and 5- subgroups, respectively. Since they are unique they are normal. Now $H \cap K$ is a subgroup of both H, K. By Lagrange's Theorem its order divides both 3 and 5, so it must be 1. By the product theorem we conclude that $G \cong H \times K$. Now H, K have prime order so they are isomorphic to $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ respectively. Then by the Chinese remainder theorem we have

$$G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$$

Note that the above also follows from our corollary to the product theorem last chapter.

3.2 The Class Equation

Definition 3.2

Define the **conjugation action** of $(G, \star)$ on itself by

$$G \times G \to G \quad (h, g) \mapsto h \star g \star h^{-1}$$

Proposition 3.5

The conjugation action is indeed a group action $G \circlearrowleft G$.

Proof. EXERCISE. □

For any given h, the image of G under conjugation by h is an isomorphism. Roughly speaking, conjugating the group in this way may be seen as a kind of change of variables. Thus we have the following:

Proposition 3.6

Let $g, h \in G$. Then $\mathrm{ord}(hgh^{-1}) = \mathrm{ord}(g)$.

Proof. For all k we have

$$\left(hgh^{-1}\right)^k = hg^k h^{-1}$$

which equals the identity if and only if g^k is the identity. □

We will give special names to the orbits and stabilizers of G under the conjugation action.

Definition 3.3

The **centralizer** of an element $x \in G$ is the set

$$Z(x) := \{g \in G | gxg^{-1} = x\} \leqslant G$$

Note that the centralizer of x is just the stabilizer of x under conjugation.

Definition 3.4

The **conjugacy class** of an element $x \in G$ is the set

$$C(x) = \{gxg^{-1} | g \in G\}$$

The conjugacy class of x is the orbit of x under conjugation.

Then by applying the Orbit-Stabilizer theorem, we note that for all $x \in G$ we have

$$|G| = |Z(x)| \cdot |C(x)|$$

Proposition 3.7

The following are true:

1. $Z(x) \leqslant G$.
2. $C(x) \leqslant G$.
3. $x \in C(x)$.
4. $z \in Z(x)$.

Proof.
1. EXERCISE.
2. EXERCISE.
3. $x = exe^{-1}$.
4. $xxx^{-1} = x$.

□

Definition 3.5

The **center** of a group G is the set of elements which commute with all elements of G:

$$Z(G) \coloneqq \{g \in G : \forall x \in G, xg = gx\}$$

Notice that the notation for the center and the centralizer are very similar. In particular, note that $xgx^{-1} = g$ if and only if $xg = gx$; that is, if and only if g, x commute. Thus the center of a group is the set of elements that commute with all elements of G, and the centralizer of x is the set of elements that commute with specifically x (which therefore includes the center).

Proposition 3.8

For all $x \in G$, $Z(G) \subseteq Z(x)$.

Proof. Follows from the observation above. □

Proposition 3.9

The center is the intersection of all centralizers; that is,

$$Z(G) = \bigcap_{x \in G} Z(x)$$

Proof. Both sides are the set of all elements which commute with all $x \in G$. □

Proposition 3.10

$x \in Z(g)$ if and only if $C(x) = \{x\}$.

Proof. If $x \in Z(g)$, then for all $g \in G$, $gxg^{-1} = gg^{-1}x = x$ so $C(x) = \{x\}$. The reverse implication is similar. □

Now, we may use the fact that conjugation is an action to show the following:

Proposition 3.11

G is the disjoint union of its conjugacy classes, and in particular,

$$|G| = \sum_{\text{conjugacy classes}} |C|$$

Proof. Orbit formula. □

In particular, by Proposition 3.10, the number of conjugacy classes of size 1 is the size of $|Z(G)|$. Thus we have the following:

Theorem 3.12: Class Equation

Let $C_1, \ldots, C_k$ be the distinct conjugacy classes which are of size greater than one. Then

$$|G| = |Z(g)| + |C_1| + \ldots + |C_k|$$

This is called the **class equation** for G.

Example 3.2

Consider S_3. The class equation is $6 = 1 + 2 + 3$. To see this, observe the following:

1. If x is a 2-cycle, say (12), then

$$\begin{aligned} C((12)) &= \{e(12)e^{-1}, (13)(12)(13), (12)(12)(12), (23)(12)(23), \ldots\} \\ &= \{(12), (23), (12), (13), \ldots\} \end{aligned}$$

   Now recall that the order of a transposed element will be the order of (12) and thus must also be a 2-cycle. Thus the remaining transposed elements have been enumerated and

$$C((12)) = \{(12), (23), (13)\}$$

2. Similarly, if y is a 3-cycle,

$$C(y) = \{(123), (132)\}$$

3. The conjugacy class of e is $\{e\}$.

Thus we have one element in the center, a conjugacy class of size 2, and a conjugacy class of size 3. So the class equation is

$$6 = |S_3| = |Z(g)| + |C(x)| + |C(y)| = 1 + 3 + 2 = 1 + 2 + 3$$

Example 3.3

The class equation for $\mathrm{SL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ is

$$24 = \underbrace{1 + 1}_{Z(G)} + 4 + 4 + 4 + 4 + 6$$

with $|Z(G)| = 2$.

Theorem 3.13

Let ρ, ρ' be permutations. Then ρ, ρ' are conjugate if and only if their cycle decomposition has the same order. This means the cycles in the decomposition have the same orders: they have the same number of 2-cycles, 3-cycles, and so on.

Example 3.4

Using the above theorem, the conjugacy classes in S_4 are

$$\begin{aligned}
&\{e\} && \text{(identity)}\\
&\{(12), (13), (14), (23), (24), (34)\} && \text{(2-cycles)}\\
&\{(123), (132), (124), (142), (123), (143), (234), (243)\} && \text{(3-cycles)}\\
&\{(12)(34), (13)(24), (14)(23)\} && \text{(Disjoint 2-cycles)}\\
&\{(1234), (1243), (1324), (1342), (1423), (1432)\} && \text{(4-cycles)}
\end{aligned}$$

Thus the class equation is

$$24 = |S_4| = 1 + 3 + 6 + 6 + 8$$

Example 3.5

(135)(246) are conjugate: let $\tau = (12)(34)(56)$. Then

$$\tau(135)\tau^{-1} = (12)(34)(56)(135)(12)(34)(56) = (246)$$

The above example shows why the theorem is true: if a two permutations permute the same number of elements in the same number of ways, then we apply a renaming such that each element is permuted in the same way. Because cycle decomposition guarantees disjoint cycles, we can always apply this renaming.

Example 3.6

Consider the permutations $(123)(45)$ and $(67)(89a)$ (where $a = 10$). Using the renaming intuition, we let $\tau = (18)(29)(3a)(46)(57)$.

3.3 p-Groups

Definition 3.6

Let p be a prime. Then a ***p*-group** is a group whose order is a power of p.

Lemma 3.14

The center of a p-group is nontrivial.

Proof. Let $|G| = p^n$. The class equation shows that

$$p^n = |Z(G)| + |C_1| + \ldots + |C_k|$$

Now, by the Orbit-Stabilizer formula, the size of each conjugacy class divides $|G|$ (note that it is not necessarily a subgroup). The C_i have order greater than 1, so each is divisible by 1. Thus p divides $|C_i|$ for each i, and thus p divides $|Z(G)|$, so $Z(G)$ is nontrivial. $\square$

Corollary 3.15

Every group of order p^2 is abelian.

Proof. By the previous lemma, $|Z(G)|$ is either p or p^2. If it is p^2 we are done, so assume $|Z(G)| = p$. Then pick some $x \notin Z(G)$. We know that $Z(G) \subseteq Z(x)$, and $x \in Z(x)$, so $Z(G)$ is a proper subset of $Z(x)$. Thus $|Z(x)| > p$, and it is a subgroup, so by Lagrange's Theorem $|Z(x)| = p^2$. But this implies x commutes with all elements of g and thus $x \in Z(G)$, contradiction. Thus $Z(G) = G$ and G is abelian. $\square$

Corollary 3.16

Every group G of size p^2 is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. If there exists an element of order p^2, then G is cyclic and isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$. Otherwise, assume that every nontrivial has order p. Pick some such $x \in G$ and consider $\langle x \rangle$. This is of order p, so pick another nontrivial $y \notin \langle x \rangle$. Then $\langle x \rangle, \langle y \rangle$ are subgroups, and $\langle x \rangle \cap \langle y \rangle = \{e\}$: this is because the intersection is a strict subgroup of both $\langle x \rangle, \langle y \rangle$ and thus has order 1. Now, G is abelian, so these are normal subgroups and by the product theorem

$$G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$ $\square$

Appendix A

Representation Theory

A.1 Motivations

A powerful approach to understanding group structures is by analyzing maps between groups. In particular, we can consider maps between arbitrary groups and groups of linear maps, can be understood well using linear algebra.

In particular, the structure of finite **simple groups** (which are groups with no nontrivial normal subgroups) is completely understood. Thus, it is of interest to find all normal subgroups of a given group.

Recall that for any group homomorphism $\phi : G \to H$, $\ker \phi \trianglelefteq G$. Thus, finding a nontrivial, noninjective homomorphism out of G (regardless of its target) will show that G is not simple. In particular, we will consider homomorphisms from G into $\mathrm{GL}_n(\mathbb{F})$ (where $\mathbb{F}$ is often $\mathbb{R}, \mathbb{C}$).

Some groups may be easily embedded into $\mathrm{GL}_n(\mathbb{R})$ using geometric interpretations.

Example A.1

D_n is the set of symmetries of $\mathbb{R}^2$.

Example A.2

${\mathbb{Z}}/{n\mathbb{Z}}$ acts on $\mathbb{R}^2$ by rotation using the map

$$1 \mapsto \begin{bmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{bmatrix}$$

Consider a function $f : \mathbb{H} \to \mathbb{C}$ ($\mathbb{H}$ is the upper half complex plane) defined by

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

This is called a modular form. The modularity conjecture (now a theorem) says that modular forms on certain elliptic curves are in one to one correspondence with representations of $\mathrm{SL}_2(\mathbb{Z})$.

A.2 Key Definitions

Definition A.1

A **representation** of a group G is a group homomorphism $R : G \to \mathrm{GL}_n(\mathbb{R})$. We say that it is **faithful** if R is injective.

R is faithful only if it is an isomorphism between G and a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Definition A.2

If V is a vector space, $\mathrm{GL}(V)$ is the set of invertible linear maps on $V \to V$.

Note that matrices in $\mathrm{GL}_n(\mathbb{R})$ uniquely correspond to maps in $\mathrm{GL}(V)$ (where $n = \dim V$) when V is fixed and real. We can make the same definitions for $\mathrm{GL}_n(\mathbb{C})$. The key idea is that the information contained in a representation $G \to \mathrm{GL}(V)$ is the same as the information contained in a linear group action of G on V; in other words a function $(g, v) \mapsto gv$ such that

1. $ev = v$ for all $v \in V$;
2. $h(gv) = (h \star g)v$ for all $g, h \in G, v \in V$;
3. $g(\alpha v + \beta w) = \alpha gv + \beta gw \in V$ (linearity).

Example A.3

Define a map $R : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to \mathrm{GL}(\mathbb{R}^2)$ by

$$1 \mapsto \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$

For convenience, we write R_g to denote $R(g)$, since the elements R_g are matrices and we will need them to act on vectors.

Now, we can see that if we have defined a representation $R : G \to \mathrm{GL}(V)$, then we define a group action by $g \cdot v \coloneqq R_g v$. To check that this is a group action if R is a linear homomorphism:

$$h \cdot (g \cdot v) = h \cdot (R_g v) = R_h R_g v = R_{h \star g} v = (h \star g) \cdot v$$

In the other direction, given a group action, the map R_g is defined as $v \mapsto g \cdot v$. From here, you can check that R is a linear homomorphism.

Note that there are many possible representations of a given group.

Example A.4

Define a group homomorphism by $D_n \mapsto \{\pm 1\} \subseteq \mathrm{GL}_1(\mathbb{R})$, where reflections map to -1.

Example A.5

Let us consider the representations of $D_3 = \{1, x, x^2, y, xy, x^2y\}$ where x is rotation and y reflection over the x axis. One representation is the standard representation S from $D_3 \mapsto \mathrm{GL}_2(\mathbb{R})$, which is given by

$$1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$x \mapsto \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$
$$y \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

We may also consider the signature representation $\mathrm{sgn} : D_3 \to \mathbb{R}^\times$ which maps $x \mapsto 1, y \mapsto -1$.

We have the trivial representation $T : D_3 \to \mathbb{R}^\times$ by $T(\tau) = 1$ for all τ (this is always a representation).

We will later see that every representation may be found by combining these representations. For now, consider one-dimensional representations $R : D_3 \to \mathrm{GL}_1(\mathbb{R})$. The group presentation of D_3 is given by the relations

$$\begin{cases} x^3 = e \\ y^2 = e \\ xy = yx^{-1} \end{cases}$$

R must respect these, so we must have

$$R_x R_y = R_{xy} = R_{yx^{-1}} = R_y [R_x]^{-1}$$

so

$$(R_x)^2 = 1$$

and thus $R_x = \pm 1$. But we also know that

$$1 = R_e = R_{x^3} = (R_x)^3$$

so we must have $R_x = 1$. Then $R_y = \pm 1$, which correspond to sgn and T, respectively. (When n is even the parity means that we have more interesting one-dimensional representations as x may be mapped to -1, but not when n is odd. This is reflected in even dimensional groups having reflections across midpoints as well as vertices.)

We now consider how we may build representations out of smaller ones.

Definition A.3

Let $R : G \to \mathrm{GL}(V)$ and $R' : G \to \mathrm{GL}(W)$ be representations (or actions $G \circlearrowright V$ and $G \circlearrowright W$). Then the **direct sum** of R, R' corresponds to the action

$$G \circlearrowright V \times W : g(v, w) = (gv, gw)$$

or is given explicitly by $R \oplus R' : G \to \mathrm{GL}(V \oplus W)$ defined by

$$(R \oplus R')_g = R_g \oplus R'_g$$

where the right side $\oplus$ means concatenation along the diagonal.

Example A.6

Consider $T \oplus \mathrm{sgn} : D_3 \to \mathrm{GL}_2(\mathbb{R})$. The matrix of rotation is given by

$$R_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R_y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

as $\mathrm{sgn}(x) = 1, \mathrm{sgn}(y) = -1$. (The upper left corner is 1 for both as $T(x) = T(y) = 1$)

Thus we see that representations may be built out of others. The natural question to ask is which representations may be seen as the "building blocks" of all others.

Definition A.4

A G**-invariant** subspace is a subspace $W \subseteq V$ such that for all $g \in G$, $w \in W$, $gw \in W$.

Definition A.5

$G \circlearrowright V$ is called **irreducible** if there is no G-invariant subspace of V besides $\{0\}, V$. In other words, we use all of the space in V.

Definition A.6

Let $G \circlearrowright V$ and $G \circlearrowright W$. Then a G**-equivariant** map is a map $\phi : V \to W$ is a map which is linear and

$$\phi(gv) = g\phi(v)$$

for all $g \in G, v \in V$ (where the left product is taken in $G \circlearrowright V$ and the right in $G \circlearrowright W$.)

Example A.7

Consider an action $\{\pm 1\} \circlearrowright \mathbb{R}^2$ which acts by multiplication: $1(a,b) = (a,b)$ but $-1(a,b) = (-a,b)$. Consider a map $\phi : \mathbb{R}^2 \to \mathbb{R}$ by $(x,y) \mapsto x$. Define an action iof $\{\pm 1\} \circlearrowright \mathbb{R}$ by multiplication. Then

$$\phi(-1(a,b)) = \phi(-a,b) = -a$$

and

$$-1\phi(a,b) = -a$$

Definition A.7

Two representations are **isomorphic** if there exists a G-equivariant isomorphism.

Theorem A.1

Consider a representation $G \circlearrowright V$. Then we may write $V \cong W \oplus U$.

Definition A.8

Let G be finite. The **G-invariant inner product** is defined by

$$\langle v, w \rangle = \frac{1}{|G|} \sum \langle gv, gw \rangle$$

A.3 Characters and Character Tables

Definition A.9

Let $R : G \to \mathrm{GL}(V)$ be a representation. Then the **character** of R is the function $\chi_R : G \to \mathbb{R}$ given by $\chi_R(g) = \operatorname{tr} R_g$.

The values of characters may be written in a character table:

D_3	1	x	y	...
T	1	1	1	
sgn	1	1	-1	
S	2	-1	0	

Note that the columns of the table are orthogonal. Moreover, if we wrote the rest of the table we would see that the rows are as well. (Column orthonormality is only because we have all irreducible representations here).

Proposition A.2

Let $R : G \to \mathrm{GL}(V)$ with V n-dimensional and complex, and let $\chi : G \to \mathbb{C}^\times$ be its character. Then

1. $\chi(e) = n$.
2. $\chi(ghg^{-1}) = \chi(h)$.
3. If $g^k = e$ then $\chi(g)$ is the sum of k-th roots of unity.
4. $\chi(g^{-1}) = \overline{\chi(g)}$.
5. $\chi_{R\oplus R'} = \chi_R + \chi_{R'}$.

Proof.

1. $\chi(e) = I_n$.
2. $\mathrm{tr}(R_g R_n R_{g^{-1}}) = \mathrm{tr}(R_n R_g R_{g^{-1}}) = \mathrm{tr}(R_n)$.
3. $I_n = R_{g^k} = (R_g)^k$. So R_g satisfies $X^k - 1 = 0$ and thus its eigenvalues are some of the k-th roots of unity. Then the trace is the sum of k-th roots of unity.
4. If the eigenvalues of R_g are $\lambda_1, \ldots, \lambda_n$, then the eigenvalues of $R_{g^{-1}}$ are $\lambda_i^{-1} = \overline{\lambda_i}$ (since λ_i are roots of unity by the previous). Thus
$$\mathrm{tr}\, R_{g^-1} = \mathrm{tr}(R_g)^{-1} = \sum \lambda_i^{-1} = \sum \overline{\lambda_i} = \overline{\mathrm{tr}\, R_g}$$
5. Obvious since we have block matrices.

□

We see that characters are constant on conjugacy classes.

Definition A.10

Let χ, χ' be characters of some representation $G \circlearrowleft V$ (G finite). Then we define the **inner product** by
$$\langle \chi, \chi' \rangle \coloneqq \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{\chi'(g)}$$

For infinite groups we integrate over G with respect to an appropriate measure:
$$\langle \chi, \chi' \rangle = \frac{1}{V(G)} \int_G \chi(g)\overline{\chi'(g)}\, \mathrm{d}\mu$$
but we will not discuss this farther.

We now arrive at the main theorem for characters.

Theorem A.3: Main Theorem

Let R, R' be nonisomorphic and irreducible, with characters χ, χ'. then

1. $\langle \chi, \chi' \rangle = 0$.
2. Every representation is determined by its character.
3. The number of irreducible representations is equal to the number of conjugacy classes in G.

Lemma A.4: Schur's Lemma

Consider a G-equivariant map $\varphi : V \to W$ for a group G with irreducible representations $G \circlearrowright V, G \circlearrowright W$ (complex spaces). Then either φ is an isomorphism or it is the zero map. Moreover, if $\varphi : V \to V$, then $\varphi = \lambda \,\mathrm{id}$.

Proof. Suppose φ is not zero. Consider $\ker \varphi$. Then we want to show that $\ker \varphi$ is a G-invariant subspace. Pick $v \in \ker \varphi, g \in G$. Then

$$\varphi(gv) = g\varphi(v) = g0 = 0$$

so $gv \in \ker \varphi$. So $\ker \varphi$ is a G-invariant subspace. $G \circlearrowright V$ is irreducible, so $\ker \varphi$ is trivial or V, but it must be trivial as φ is nonzero. Thus it is injective. We want to show also that $\operatorname{im} \varphi$ is a G-invariant subspace of W. Let $w \in \operatorname{im} \varphi$. Then $w = \varphi(v)$ for appropriate $v \in V$. Then for all $g \in G$, $gw = g\varphi(v) = \varphi(gv) \in \operatorname{im} \varphi$. Irreducibility again shows that $\operatorname{im} \varphi = W$. So φ is an isomorphism.

Now if $W = V$, then there exists an eigenvector v with eigenvalue λ. $\lambda \neq 0$ so the eigenspace of λ is G-invariant, and therefore is all of V. $\square$

Proposition A.5

Let A, B be $n \times n$ matrices over $\mathbb{C}$ and let $\Phi : M_{n\times n} \to M_{n\times n}(\mathbb{C})$ be a linear map given by $M \mapsto AMB$. Then $\operatorname{tr}(\Phi) = \operatorname{tr}(A)\operatorname{tr}(B)$.

Proof. Consider a basis of $M_{n\times n}(\mathbb{C})$. Let E_{ij} be the matrix $\delta_{(x,y)(i,j)}$. Then E_{ij} maps to a matrix with $a_{ii}b_{jj}$ in the i,j-th entry. Then

$$\operatorname{tr} \varphi = \sum_{i,j} (i,j)\text{-th coordinate of } \varphi(E_{ij}) = \sum_{i,j} a_{ii}b_{jj} = \operatorname{tr}(A)\operatorname{tr}(B) \qquad \square$$

Definitions