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 $q = q'$. □

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:

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

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

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

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

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

and finally:

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

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. □

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. □

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 $nk \bmod p = 1$ □

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 $a \equiv b \pmod{n}$. □

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

$$a^{p-1} \equiv 1 \pmod{p}$$ □

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. □

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. □

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 $e_1 = e_2$. □

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 $P^T S P = S$.[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 $G = \{g_1, \ldots, g_n\}$. Then the elements $gg_1, gg_2, \ldots, gg_n$ are a permutation of $g_1, \ldots, g_n$.

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. □

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,

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

and by Lemma 2.3,

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

so $g^n = e$ by cancellation. □

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 **(external) direct product** 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

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

Then we have

Proposition 2.8

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

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 $x = \text{rot}_{2\pi/n}$ and $y = \text{refl}_0$. 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 $d_A Q_B = dA d_B P$, 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. $e_H\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$ 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 $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e_H e_h = e_H$, so $g_1 g_2 \in \ker \phi$.

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. □

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. □

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

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

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 $\{1, 2, \ldots, n\}$ 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

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

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

$$(a_1 a_2 \ldots a_t)$$

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.

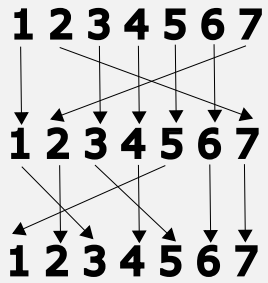
Definition 2.20

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 $(a_1 a_2 \dots a_n)$ be a cycle. Then $(a_1 a_2 \dots a_n) = (a_1 a_2) \dots (a_{n-2} a_{n-1})(a_{n-1} a_n)$. 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. □

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. □

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. □

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 $A_n = \ker(\text{sgn})$, 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 $b^{-1}a = k'k^{-1} \in K$. □

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 $|aK| = m$. □

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. □

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 $\text{ord}(g) | n$.
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 $G = \langle g \rangle$. □

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 $G \curvearrowright X$ to denote that G acts on X by some group action $\cdot$.

Definition 2.28

Let $G \curvearrowright X$ 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 $S_n \curvearrowright \{1, \ldots, n\}$. 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 $G \curvearrowright X$ 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 $\mathbb{Z}/4\mathbb{Z} \curvearrowright \mathbb{Z}/2\mathbb{Z}$ by

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

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

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

Definition 2.30

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

Example 2.36

Let $D_3 \curvearrowright \{1,2,3\}$ 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

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

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

We make the following observations:

Proposition 2.33

Let $G \curvearrowright X$. 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. $\operatorname{ad} : G \to \mathrm{Bij}(X)$ is a homomorphism (where $\mathrm{Bij}(X)$ is a group under composition).
5. ad is injective if and only if $G \curvearrowright X$ 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 $G \curvearrowright X$ 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 $G \curvearrowright X$ is faithful. □

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 $G \curvearrowright G$ 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 $\operatorname{ad} : G \to \mathrm{Bij}(G)$ is injective. Note that $\mathrm{Bij}(G)$ 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 $G \cong \phi \operatorname{ad} G \leqslant S_n$. □

We can use similar logic to show that if $G \curvearrowright H$ 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 $G \curvearrowright X$. 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. □

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 $G \curvearrowright X$ 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 $\operatorname{Stab}(x) \leqslant G$. □

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. □

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

$$gH \star g'H \coloneqq (g \cdot g')H$$

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 $3\left(\mathbb{Z}/6\mathbb{Z}\right), \overline{1} + 3\left(\mathbb{Z}/6\mathbb{Z}\right), \overline{2} + 3\left(\mathbb{Z}/6\mathbb{Z}\right)$.

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

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

So our cosets are

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

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:.

$$G \xrightarrow{\text{can}} {}^{G}\!/_{K} \xrightarrow{\psi} G' \qquad (\phi : G \to G')$$

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 $\psi \circ \text{can} = \phi$. □

Corollary 2.44

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

Proof. Consider the corresponding map $\psi : G \to \operatorname{im} G$. ψ is a surjective homomorphism, so by the first isomorphism theorem, $\operatorname{im} G \cong {}^{G}\!/_{K}$. 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. □

In this case, G is called the **(internal) direct product** of M, N.

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, and G is abelian, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Proof. Homework. □

The above theorem is true for nonabelian groups under mild conditions, which we will prove later:

Theorem

If $|G| = pq$ where $p < q$ are distinct and not equal to exactly $2, 3$, and $q \not\equiv 1 \pmod{p}$, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

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

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

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

3.1 The Class Equation

Definition 3.1

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 3.1

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

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 3.2

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

Proof. For all k we have

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

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 3.2

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

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

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

Definition 3.3

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 3.3

The following are true:

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

Proof. 1. EXERCISE.

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

□

Definition 3.4

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 3.4

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

Proof. Follows from the observation above. □

Proposition 3.5

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 3.6

$x \in Z(g)$ 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 3.7

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 3.6, the number of conjugacy classes of size 1 is the size of $|Z(G)|$. Thus we have the following:

Theorem 3.8: 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 3.1

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 3.2

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 3.9

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 3.3

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 3.4

$(135)(246)$ 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 3.5

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

3.2 p-Groups

Definition 3.5

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

Lemma 3.10

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. □

Corollary 3.11

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. □

Corollary 3.12

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

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

3.3 Simple Groups

Definition 3.6

A **simple group** is a group G which has no normal subgroups other than $\{e\}$ or G.

It turns out that every finite group is built from simple groups using semidirect products and group cohomologies, which motivates the study of simple finite groups.

Moreover, one finds that many simple groups fall naturally into a family of related simple groups.

Example 3.6

Some examples of families of simple groups are $A_n, n \geq 5$ and $\mathrm{PSL}_n(\mathbb{F}_p)$, $n > 2$ (where $\mathrm{PSL}_n(\mathbb{F}) = {}^{\mathrm{SL}_n(\mathbb{F})}\!/_{\{\pm I_n\}}$).

In fact, the only families of simple groups are the alternating groups, $n \geq 5$, cyclic groups ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, and 16 families of Lie type.

Example 3.7

The sporadic groups are those which do not fall in one of the infinite families of simple groups. The smallest sporadic group is the Mathieu group M_{11}, and the largest is the Monster group, which has order $\approx 8 \times 10^{52}$.

Lemma 3.13

Let $N \trianglelefteq G$. Then

1. If $x \in N$ then $C(x) \subseteq N$.
2. N is the union of some conjugacy classes of G.
3. The order of N is the sum of the orders of conjugacy classes it contains.

Proof. 1 is clear since N is closed under conjugation. 2 follows from 1, and 3 follows from 2 since conjugacy classes are disjoint. □

Example 3.8

Let us show that A_5 is simple.

We first write the class equation of A_5 as

$$60 = 1 + 20 + 12 + 12 + 15$$

1 corresponds to the conjugacy class $\{e\}$, 20 corresponds to the classes of 3-cycles $\{(xyz)\}$, $12+12$ corresponds to the classes of 5-cycles $\{(xyzwe)\}$, and 15 corresponds to the class of pairs of transpositions $\{(xy)(zw)\}$.

Note that although we previously showed that equal order permutations are in the same conjugacy class. However, this only holds in S_5; and thus 5-cycles split into two conjugacy classes in A_5 (because the only elements that conjugate between these classes lie in $S_5 \setminus A_5$.)

Now, we apply Lemma 3.13. We know that any normal subgroup must have order dividing 60, but it also has to be the sum of some conjugacy classes. Moreover, the normal group must have the identity element. This requirement means that adding any other combination of $12, 12, 15, 20$ does not result in a proper divisor of 60. Thus there is no normal subgroup. So A_5 is simple.

3.4 Sylow's Theorems

In this section we demonstrate three important results due to Sylow, which are known as Sylow's Thoerems. These theorems serve as powerful tools to produce subgroups of a given group.

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

Definition 3.7

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 3.14: First Sylow Theorem

Let G be finite and p prime. Then there is a Sylow p-subgroup.

Proof. The theorem is only interesting if p divides $|G|$, as otherwise the trivial subgroup is a Sylow p-subgroup.

We will progress by defining an appropriate group action $G \curvearrowright X$, and we want to have our Sylow p-subgroup to be a stabilizer of some $x \in X$. By the Orbit-Stabilizer Theorem, we would have $|G| = |\operatorname{Stab}(x)| \cdot |O(x)|$. If $|G| = p^k m$ where $\gcd(p, m) = 1$, then we would need $|O(x)| = m$, which is in particular not divisible by p. Then if we choose X in such a way that p does not divide $|X|$, this will guarantee that at least one orbit size is not divisible by p.

Let Ω be the set of all subsets of G of size p^k. Let $G \curvearrowright \Omega$ by multiplication, such that $\omega \mapsto g\omega$.

Claim: p does not divide $|\Omega|$.

To see this, note that

$$|\Omega| = \binom{p^k m}{p^k} = \prod_{j=0}^{p^k-1} \frac{p^k m - j}{p^k - j}$$

Write $v_p(m)$ to be the maximum l such that $p^l | m$. Because j ranges over $[0, p^k - 1]$, $v_p(p^k m - j) = v_p(j)$. Similarly, $v_p(p^k - j) = v_p(j)$. Thus we may divide out appropriate powers of p from the numerator and denominator, and after simplification we see that it is not divisible by p. So $|\Omega|$ is the product of numbers which are not divisible by p and thus not divisible by p either.

So p does not divide $|\Omega|$, which is the sum of the orbit sizes. Thus there is some ω such that $|O(\omega)|$ is not divisible by p. By the Orbit-Stabilizer theorem, p^k divides $|\operatorname{Stab}(\omega)| \cdot |O(\omega)|$, so p^k divides $|\operatorname{Stab}(\omega)|$.

To conclude, we need to show that $|\operatorname{Stab}(\omega)|$ is exactly equal to p^k. To argue this, take $\alpha \in \omega$. Then $|\operatorname{Stab}(\omega)| = |\operatorname{Stab}(\omega)\alpha|$. But since $\alpha \in \omega$, each element of $\operatorname{Stab}(\omega)\alpha$ is in ω. Thus $|\operatorname{Stab}(\omega)\alpha| \leq |\omega| = p^k$. So $\operatorname{Stab}(\omega)$ is a Sylow p-subgroup. □

Theorem 3.15: Second Sylow Theorem

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

Proof. Let $\Omega = \{gK | g \in G\}$ and let $P \curvearrowright \Omega$ by left multiplication. We know $|\Omega| = [G : K] = m$ (if $|G| = p^k m = |K|m$). Thus p does not divide $|\Omega|$. By the Orbit formula,

$$|\Omega| = 1 + \ldots + 1 + |O_1| + \ldots + |O_j|$$

where the 1's correspond to orbits of size 1, and the O_i correspond to orbits of length greater than 1. Now, the size of each O_i divides $|P| = p^k$, so $|O_i| = p^{k_i}$ for each i, where $k_i \geq 1$. Thus there exists some orbit of length 1, say of gK. Then for all $p \in P$, $pgK = gK$, meaning $PgK = gK$. Then multiplying by g^{-1} on both sides we have $g^{-1}PgK = K$. Picking $e \in K$ on the left side, $g^{-1}Pg \subseteq K$, but they are the same size so $g^{-1}Pg = K$. □

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

Corollary 3.16

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. □

Definition 3.8

Let $H \leqslant G$. Then the **normalizer** of H is the set

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

One can show that $N(H) \leqslant G$. Then essentially by definition we observe that $H \trianglelefteq N(H)$.

Proposition 3.17

Let $H \leqslant G$. Then

1. $H \trianglelefteq N(H)$.
2. $H \trianglelefteq G$ if and only if $N(H) = G$.
3. $|H|$ divides $|N(H)|$ and $|N(H)|$ divides G.

Proof. 1 follows by definition, 2 is clear, and 3 follows from Lagrange's Theorem. □

We can interpret the normalizer as the stabilizer of H under the group action of conjugation by G on the set of all subgroups of G.

Theorem 3.18: Third Sylow Theorem

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

Proof. To show that n_p divides $|G|$, we let Ω be the set of all Sylow p-subgroups. Let $G \curvearrowright \Omega$ by conjugation, that is, for any Sylow p-subgroup P we define $g \star P := gPg^{-1}$. Note that by the Second Sylow Theorem we know that this action is closed. Moreover, we know that any two Sylow p-subgroups are conjugates of each other. Thus there is only one orbit and it is all of Ω.

Pick some $P \in \Omega$. By the Orbit-Stabilizer theorem,

$$|G| = |\operatorname{Stab}(P)| \cdot |O(P)| = |\operatorname{Stab}(P)| \cdot |\Omega| = |\operatorname{Stab}(P)| \cdot n_p$$

Thus n_p divides $|G|$.

For the second part, take $P \in \Omega$ and let $P \curvearrowright \Omega$. The size of each orbit divides $|P| = p^k$ so must be a power of p. Of course, $O(P) = \{P\}$. We claim that this is the only orbit of length 1. Indeed, if $H \in \Omega$ has $|O(H)| = 1$, then $pHp^{-1} = H$ for all $p \in P$. So $P \subseteq N(H)$. Now apply the Second Sylow Theorem to $N(H)$. We know $P.H \subseteq N_G(H)$ are Sylow p-subgroups. So they are conjugate in $N(H)$. But $H \trianglelefteq N(H)$ so $H = P$ by Corollary 3.16.

We now conclude with the Orbit formula:

$$n_p = |\Omega| = 1 + |O_1| + \ldots + |O_j|$$

where each O_j has length greater than 1 and a power of p. Thus $n_p \equiv 1 \pmod{p}$. □

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 3.9

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.

3.5 Semidirect Products

In this section we will develop the theory of semidirect products, which generalize the direct products we have already considered. We saw from the product theorem that a group G is said to be the (internal) direct product of two normal subgroups if every element is written as a unique product of elements from the subgroups. However, this structure means that elements from the groups commute with one another, so that they essentially don't interact. Put another way, we recall that the operation on the (external) direct product just applies the individual operations separately, with no interaction. While this works for some groups, there are many groups which can be built out of two smaller groups, but require those groups to interact somehow.

A key example of this is the dihedral group D_n. This group may be seen to be built out of the normal subgroup of rotations and the subgroup $\{e, y\}$, where y is a reflection. Moreover, the rotations are isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and the reflections isomorphic to $\mathbb{Z}/2\mathbb{Z}$. However, this does not form a direct product:

$$D_n \neq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

In particular, the left side is not abelian while the right side is. Thus, we need to find a new, more general way to combine groups that will account for more types of groups.

Definition 3.9

If G is a group then $\mathrm{Aut}(G)$ is the set of all automorphisms on G. In particular, it is a group under composition and is called the **automorphism group** on G.

Example 3.10

Let $k \in \mathbb{Z}$ and define $\psi_k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$\overline{a} \mapsto \overline{ka}$$

This is easily verified to be a homomorphism. However, it is only an isomorphism if $\gcd(k, n) = 1$, and in this case its inverse is given by $\psi_{k^{-1}}$. Moreover, note that if $k \equiv l \pmod{n}$ then $\psi_k = \psi_l$.

Lemma

$\operatorname{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$.

Proof. Consider the map $\Psi : \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} \to \operatorname{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ defined by $\overline{k} \mapsto \psi_k$. We noted in the example above that this is well defined. We check that this is an isomorphism:

1. Ψ is a homorphism: We have

   $$\Psi(\overline{k_1} \cdot \overline{k_2}) = \Psi(\overline{k_1 k_2}) = \psi_{k_1 k_2}$$

   Now, note that for $x \in \mathbb{Z}/n\mathbb{Z}$,

   $$\psi_{k_1 k_2} x = k_1 k_2 x = k_1(k_2 x) = \psi_{k_1} \circ \psi_{k_2}(x)$$

   so $\psi_{k_1 k_2} = \psi_{k_1} \circ \psi_{k_2}$. Summarizing,

   $$\Psi(\overline{k_1} \cdot \overline{k_2}) = \Psi(\overline{k_1 k_2}) = \psi_{k_1 k_2} = \psi_{k_1} \circ \psi_{k_2} = \Psi(\overline{k_1}) \circ \Psi(\overline{k_2})$$

   Thus Ψ is a homomorphism.

2. Ψ is injective: Let $\overline{k} \in \ker \Psi$. Then

   $$\overline{k} = \psi_k(\overline{1}) = \mathrm{id}(\overline{1}) = \overline{1}$$

   so $\overline{k} = \overline{1}$ and thus the kernel is trivial.

3. Ψ is surjective: Let $\varphi \in \operatorname{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ and let $\overline{k} = \varphi(\overline{1})$. I claim that $\Psi(\overline{k}) = \varphi$.

   Note that $\varphi(\overline{1})$ has order n since $\overline{1}$ does. Thus $\varphi(\overline{1})$ is a generator of $\mathbb{Z}/n\mathbb{Z}$. Then for any $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ there exists $l \in \mathbb{Z}$ such that $\overline{b} = \varphi(\overline{1}) \cdot l$. Pick $b = \overline{1}$. Then $\overline{1} = \varphi(\overline{1}) \cdot l$ for some l. So $\varphi(\overline{1})$ has a multiplicative inverse and is therefore in $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$. Now,

   $$\varphi(\overline{a}) = a\varphi(\overline{1}) = \overline{ka} = \psi_k(\overline{a})$$

   So $\varphi = \psi_k = \Psi(\overline{k})$. Thus Ψ is surjective.

□

Example 3.11

Let us show this by example for $n = 3$.

Note that $\left(\mathbb{Z}/3\mathbb{Z}\right)^{\times}$ has two elements and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Consider the automorphisms of $\mathbb{Z}/3\mathbb{Z}$. Let $\psi_1 = \mathrm{id}$. Define ψ_2 by

$$\overline{0} \mapsto \overline{0}, \overline{1} \mapsto \overline{2}, \overline{2} \mapsto \overline{1}$$

These are the only automorphisms since $\overline{0}$ must map to itself. We also have $\psi_2 \circ \psi_2 = \psi_1$ so this group is cyclic and also isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

We can now use the automorphism group to define our generalized product.

Definition 3.10

Let N, H be groups. Let $\phi : H \to \mathrm{Aut}(N)$ be a homomorphism. Then the **(external) semidirect product** of N, H with respect to ϕ, denoted $N \rtimes_\phi H$, is the set $N \times H$ with the operation $\star$ defined as

$$(n_1, h_1) \star (n_2, h_2) \coloneqq (n_1 \phi_{h_1}(n_2), h_1 h_2)$$

where $\phi_{h_1} = \phi(h_1)$.

Note that if ϕ maps all elements of H to the identity on N, then $N \rtimes_\phi H \cong N \times H$.

Example 3.12

Let $H = \mathbb{Z}/2\mathbb{Z}$ and $N = \mathbb{Z}/3\mathbb{Z}$. We showed previously that $\mathrm{Aut}(N) \cong \mathbb{Z}/2\mathbb{Z}$. There are only two subgroups of $\mathbb{Z}/2\mathbb{Z}$, so there are two choices for ϕ: ϕ_1, which maps both elements of H to id_N, and ϕ_2, which satisfies

$$\phi_2(\overline{0}) = \mathrm{id}_N$$
$$\phi_2(\overline{1}) = \begin{cases} \overline{0} \mapsto \overline{0} \\ \overline{1} \mapsto \overline{2} \\ \overline{2} \mapsto \overline{1} \end{cases}$$

Now, we noted above that $N \rtimes_{\phi_1} H \cong N \times H$. On the other hand $N \rtimes_{\phi_2} H$ is not even abelian, and is actually isomorphic to $D_3 \cong S_3$.

We may use the semidirect product to generalize the product theorem:

Theorem 3.19

Let $N \trianglelefteq G$ and $H \leqslant G$. Suppose also that $N \cap H = \{e\}$ and $G = NH$. Then $G \cong N \rtimes_\phi H$ with ϕ mapping h to the automorphism given by conjugation by h; that is $\phi(h) = \varphi_h$ where $\varphi_h(n) = hnh^{-1}$.

Proof. We construct an isomorphism $f : N \rtimes_\phi H \to G$. Noting that $N \rtimes_\phi H$ is just $N \times H$ as a set, we define $f(n, h) = nh$.

By assumption $G = NH$ so this is surjective.

To show injectivity, if $n_1 h_1 = n_2 h_2$ then $n_1 n_2^{-1} = h_2 h^{-1}$. The left side is in N and the right in H, so both are the identity. So $n_1 = n_2$ and $h_1 = h_2$. Thus f is bijective.

To check that f is a group homomorphism, we have

$$f(n_1, h_1) \cdot f(n_2, h_2) = n_1 h_1 n_2 h_2$$

On the other hand, we also have

$$f((n_1, h_1) \star (n_2, h_2)) = n_1 n_2 h_1 h_2$$

$$f((n_1, h_1) \star (n_2, h_2)) = f(n_1 \phi_{h_1}(n_2), h_1 h_2) = n_1 h_1 n_2 h_1^{-1} h_2 h_2 = n_1 h_1 n_2 h_2 \qquad \square$$

In the case that $G \cong N \rtimes_\phi H$ as above, with $N \trianglelefteq G$ and $H \leqslant G$, G is said to be the **(internal) semidirect product** of N and H. We also note that as in the case of the product theorem, if G is finite and $|G| = |N| \cdot |H|$ then we need not verify that $G = NH$.

Example 3.13

To see that S_3 is isomorphic to the external semidirect product of $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$, we note that $\mathbb{Z}/3\mathbb{Z} \cong \langle(123)\rangle$ and $\mathbb{Z}/2\mathbb{Z} \cong \langle(12)\rangle$. $\langle(123)\rangle$ is normal since its index is 2. Moreover, since their intersection is trivial and their orders multiply to $6 = |S_3|$, the semidirect product theorem applies and we have $S_3 \cong \langle(123)\rangle \rtimes_\phi \langle(12)\rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$.

Example 3.14

This work will allow us to classify all groups up to order 6 up to isomorphism. Let $n = |G|$. Clearly if $n = 1$ then G is trivial. If $n = 2, 3, 5$, then $G \cong \mathbb{Z}/n\mathbb{Z}$ since n is prime. If $n = 4 = 2^2$, then Corollary 3.12 says that $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Thus the only new case is $n = 6$. If $n = 6$, then Sylow's Theorem says we have subgroups N, H of order 3 and 2, respectively. $N \trianglelefteq G$ since it has index 2. Those subgroups have trivial intersection. So G is the internal semidirect product of N, H, and the only semidirect products are $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong S_3 \cong D_3$.

We summarize:

$n = 1$	$G \cong \{e\}$		
$n = 2$	$G \cong \mathbb{Z}/2\mathbb{Z}$		
$n = 3$	$G \cong \mathbb{Z}/3\mathbb{Z}$		
$n = 4$	$G \cong \mathbb{Z}/4\mathbb{Z}$	or	$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$n = 5$	$G \cong \mathbb{Z}/5\mathbb{Z}$		
$n = 6$	$G \cong \mathbb{Z}/6\mathbb{Z}$	or	$G \cong S_3 \cong D_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Chapter 4

Rings

4.1 Elementary Definitions

Having surveyed the general theory of groups, we now study rings, which are groups bestowed with additional structure. Specifically, rings are equipped with two operations, analogous to addition and multiplication on familiar structures such as integers, rationals, and reals. In particular, the rationals and reals have a richer multiplicative structure, which we will encounter further in fields. Thus, the main object which is abstracted by rings is the set of integers $\mathbb{Z}$.

Definition 4.1

A **ring** is a nonempty set R together with two binary operations $+, \times : R \times R \to R$ such that:

1. $+, \times$ are associative.
2. $+$ is commutative.
3. $+$ has an identity, denoted 0_R.
4. Each $r \in R$ has an additive inverse $-r$.
5. $\times$ has an identity, denoted 1_R.
6. $\times$ left and right distributes over $+$; that is,

$$a \times (b + c) = a \times b + a \times c$$
$$(a + b) \times c = a \times c + b \times c$$

We denote a ring by $(R, +, \times)$.

Essentially, a ring is an abelian group (given by its additive structure), together with some multiplicative structure, and the multiplication distributes over addition. Although

we only assume that addition is commutative in R, it is often the case that we work with rings where multiplication is commutative as well.

Definition 4.2

A ring R such that $\times$ is commutative is called a **commutative ring**.

Some key examples of rings are fields, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$. In particular, a field is a commutative ring with the additional assumption that $0_R \neq 1_R$ and every $r \in R \setminus \{0_R\}$ admits a multiplicative inverse.

Example 4.1

For some examples of rings which are not fields, we have $\mathbb{Z}$, as well as $\mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{N}$.

Given some rings, we can also construct new rings out of them. For instance, polynomials only consist of additive and multiplicative structure, so they may be defined over rings. These produce another ring, which is an important application of ring theory.

Definition 4.3

Let R be a ring. Then the **polynomial ring** $R[x]$ is the set of polynomial expressions in a single variable x; that is, $R[x] \coloneqq \{a_0 + a_1 x + \ldots + a_n x^n : a_i \in R, a_n \neq 0_R\} \cup \{0\}$.

Remark

We note that although polynomial expressions are most familiar as functions, the ring of polynomials is distinct from polynomial functions. Rather, they should be treated as formal expressions, with multiplication and addition defined analogously to those of normal polynomials. Of course, any polynomial expression may be evaluated as though it were a polynomial. However, some polynomials may evaluate to the same function, yet be distinct formal expressions. For instance $x^2 + x \equiv 0$ as an element of $\mathbb{Z}/2\mathbb{Z}[x]$, but we consider $x^2 + x$ to be distinct from the 0 polynomial.

Definition 4.4

Given two rings R, S, the **product ring** is the set $R \times S$, with addition and multiplication componentwise.

Example 4.2

For some noncommutative examples of rings, the set of all square matrices $M_{n\times n}(\mathbb{F})$ is a ring. We can also adjoin a square root of -1 to the integers to produce the **Gaussian integers**, which are $\mathbb{Z}[i] \coloneqq \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$.

As we noted above, given a ring $(R, +, \times)$, we can consider the abelian group $(R, +)$. Unlike in the case of fields, we cannot necessarily form a multiplicative group of R simply by removing 0_R, since there may be other noninvertible elements. However, we can fix this by simply removing every noninvertible element:

Definition 4.5

A **unit** of a ring R is an element $x \in R$ such that x has a multiplicative inverse in R. We write $R^\times$ to denote the set of all units in R. The set $(R^\times, \times)$ is a group.

Example 4.3

$\mathbb{Z}^\times$ is the set $\{-1, 1\}$, which is isomorphic (as a group) to $\mathbb{Z}/2\mathbb{Z}$.

Example 4.4

$(M_{n\times n}(\mathbb{R}))^\times = \mathrm{GL}_n(\mathbb{R})$.

For a field $\mathbb{F}$, this reduces to our previous definition of $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. We also emphasize that $R^\times$ is a group and not a ring.

Proposition 4.1

We can immediately apply the ring axioms to observe the following:

1. 0_R and 1_R are the unique additive and multiplicative identities.
2. Additive and multiplicative inverses are unique.
3. $0_R \times a = 0_R$ for all $a \in R$.

Definition 4.6

Given a ring R, a **subring** of R is a nonempty subset $S \subseteq R$ such that $(S, +_S, \times_S)$ is a ring, where $+_S, \times_S$ are the operations on R restricted to S, and moreover that $1_R = 1_S$ and $0_R = 0_S$.

Remark

Unlike with subgroups, we do not adopt the notation $S \leqslant R$ for subrings. Instead, we simply write $S \subseteq R$.

As in the case of groups, the fact that operations are inherited from a larger group means that we only need to check a few conditions:

Proposition 4.2

$S \subseteq R$ is a subring if and only if all of the following are true:

1. $0_R, 1_R \in S$.
2. S is closed under $+$.
3. S is closed under $\times$.
4. For all $s \in S$, $-s \in S$.

Example 4.5

The following are some examples of subrings:

1. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
2. $\mathbb{Z} \subseteq \mathbb{Z}[i]$.
3. $\mathbb{R} \subseteq \mathbb{R}[z]$.

Note that for examples 2 and 3 in 4.5, we identify $\mathbb{R}$ with the constant polynomials in $\mathbb{R}[x]$, and $\mathbb{Z}$ with the elements $a + 0i \in \mathbb{Z}[i]$. As a nonexample, $n\mathbb{Z} \subseteq \mathbb{Z}$ for $n > 1$ (since $n\mathbb{Z}$ is not even a ring in that case).

4.2 Domains

Beginning in this section, we adopt the convention that all rings are commutative rings.

We often prefer to work in settings which do not admit zero divisors, as this assumption allows for many algebraic tricks to be valid, even without division.

Definition 4.7

A (commutative) ring R is a **domain** if $0_R \neq 1_R$ and $ab = 0_R$ implies that $a = 0_R$ or $b = 0_R$.

Example 4.6

Any field is a domain. The integers $\mathbb{Z}$ are a domain.

Example 4.7

$\mathbb{Z}/6\mathbb{Z}$ is a nonexample, since $\overline{2} \cdot \overline{3} = \overline{0}$.

Proposition 4.3

If R is a domain and $S \subseteq R$ is a subring, then S is a domain.

Theorem 4.4

Let R be a ring. Then R is a domain if and only if $R[x]$ is a domain.

Proof. ($\Longleftarrow$) Follows since R is a subring of $R[x]$.

($\Longrightarrow$) Let $p, q \in R[x]$ be nonzero and suppose

$$p(x) = p_0 + p_1 x + \ldots + p_n x^n$$
$$q(x) = q_0 + q_1 x + \ldots + q_m x^m$$

with $p_n, q_m \neq 0_R$. Then

$$p(x)q(x) = \ldots + p_n q_m x^{n+m}$$

Since R is a domain, $p_n q_m \neq 0_R$. Thus pq is of degree $n+m$ and is not equal (at least as a formal expression) to the zero polynomial. □

Theorem 4.5

Let R be a domain. Then $(R[x])^\times = R^\times$.

The above theorem allows us to show some examples of $R[x]$ which are not domains, to justify the need for Theorem 4.4.

Example 4.8

Take $R = {}^{\mathbb{Z}}\!/_{8\mathbb{Z}}$, which is not a domain. Then

$$(\overline{1} + \overline{4}x)(\overline{1} - \overline{4}x) = \overline{1} - \overline{16}x^2 = \overline{1}$$

Note that for the last equality, we did not simplify modulo 8, but instead used the fact that $\overline{16} = \overline{0}$, so these are equivalent as formal expressions in R. Thus $1 + 4x$ is a nonconstant polynomial in $R[x]$ which is a unit, which only occurs when R is not a domain.

4.3 Ring Homomorphisms

As with group theory, we will see that one way to understand the structure of a ring is to study structure-respecting maps in and out of the ring.

Definition 4.8

For rings R, S, a function $\phi : R \to S$ is a **ring homomorphism** if

1. $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in R$.
2. $\phi(x \times y) = \phi(x) \times \phi(y)$ for all $x, y \in R$
3. $\phi(1_R) = 1_S$.

Once again, we can use our understanding of rings as an additive group and a multiplicative group of units to break down ϕ into two group homomorphisms $\psi : (R, +) \to (S, +)$ and $\varphi : (R^\times, \times) \to (S^\times, \times)$.

Example 4.9

The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto \overline{a}$ is a ring homomorphism, since $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{ab} = \overline{a}\overline{b}$, and $\overline{0}$ is the identity in $\mathbb{Z}/n\mathbb{Z}$.

Example 4.10

For any ring R, the map $R[x] \to R$ which takes f to the constant term a_0 is a ring homomorphism.

Example 4.11

The embedding map $\mathbb{Z} \to \mathbb{Q}$ which takes $a \mapsto \frac{a}{1}$ is a ring homomorphism. More generally, if $S \subseteq R$ is a subring, then the embedding map is a ring homomorphism.

As a nonexample, the map $\mathbb{Z} \to \mathbb{Z}$ given by $n \mapsto 2n$ is not a ring homomorphism. For another nonexample, the differentiation operator on polynomials $\mathbb{R}[x] \xrightarrow{\partial_x} \mathbb{R}[x]$ is not a ring homomorphism as $\partial_x(x^2) \neq \partial_x(x)\partial_x(x)$ (although it is a group homomorphism, since it is linear).

Recall that in the case of group homomorphisms, any two groups admitted group homomorphism $\varphi : G \to H$ where $\varphi(G) = e_H$. However, this does not work in the case of rings, due to the requirement that $\phi(1_R) = 1_S$.

Proposition 4.6

Let $\phi : S \to T$ be a ring homomorphism. Then:

1. $\phi(0_S) = 0_T$.
2. $-\phi(x) = -\phi(-x)$ for all $x \in S$.
3. If $u \in S$ is a unit, then $\phi(u) \in T$ is a unit.

Proof. 1. $\phi(0_S) = \phi(0_S + 0_S) = \phi(0_S) + \phi(0_S) \implies 0_T = \phi(0_S)$.

2. $\phi(-x) + \phi(x) = \phi(x - x) = \phi(0_S) = 0_T$ so $-\phi(x) = \phi(x)$.

3. If $u \in S$ is a unit, then there exists $v \in S$ such that $uv = 1_S$. But then $1_T = \phi(1_S) = \phi(uv) = \phi(u)\phi(v)$ so $\phi(u)$ is a unit in T. In particular, ϕ preserves multiplicative inverses.

□

Remark 4.1

Observe that if $\phi : R \to S$ is a function and S is a domain, then condition (3) in the definition of a ring homomorphism may be replaced by the condition that ϕ is not the zero map, since

$$1_S\phi(1_R) = \phi(1_R) = \phi(1_R)\phi(1_R)$$

so $\phi(1_R)(1_S - \phi(1_R)) = 0_S$. Since S is a domain, we must have $\phi(1_R) = 0$ or $1_S - \phi(1_R) = 0$. If $\phi(1_R) = 0$ then ϕ is just the zero map. So ϕ is either the zero map or we recover condition (3).

Analogously to groups, we define the following:

Definition 4.9

$\phi : R \to S$ is a **ring isomorphism** if it is a bijective ring homomorphism. In this case, we write $R \cong S$.

As in the case of groups, a ring homomorphism should be seen as a structure preserving map which simply acts to relabel the elements of R, S, with no effect on the underlying structure. As such, we can often consider rings as essentially the same if they are equal up to isomorphism.

Example 4.12

We define a ring homomorphism $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by $\overline{a} \mapsto (\overline{a}, \overline{a})$. Moreover, this is bijective, so $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ as rings.

Theorem 4.7

Let $\phi : R \to S$ be a ring isomorphism. Then $\phi^{-1} : S \to R$ is a ring isomorphism.

Proof. Bijectivity is automatic, so we just need to check that ϕ^{-1} is a ring homomorphism. Let $s_1, s_2 \in S$. Then

$$\phi(\phi^{-1}(s_1 + s_2)) = s_1 + s_2 = \phi(\phi^{-1}(s_1)) + \phi(\phi^{-1}(s_2)) = \phi(\phi^{-1}(s_1) + \phi^{-1}(s_2))$$

By applying ϕ^{-1} on both sides, we then have

$$\phi^{-1}(s_1 + s_2) = \phi^{-1}(s_1) + \phi^{-1}(s_2)$$

Similarly, we have

$$\phi(\phi^{-1}(s_1 s_2)) = s_1 s_2 = \phi(\phi^{-1}(s_1))\phi(\phi^{-1}(s_2)) = \phi(\phi^{-1}(s_1)\phi^{-1}(s_2))$$

which implies that

$$\phi^{-1}(s_1 s_2) = \phi^{-1}(s_1)\phi^{-1}(s_2)$$

Lastly,

$$\phi(\phi^{-1}(1_S)) = 1_S = \phi(1_R) \implies \phi^{-1}(1_S) = 1_R$$ □

In the setting of groups, we check whether a group homomorphism is injective by checking if its kernel is trivial. For rings, we can apply the same theory to the inherited group structure.

Definition 4.10

Let $\phi : R \to S$ be a ring homomorphism. Then the **kernel** of ϕ is

$$\ker \phi \coloneqq \{r \in R : \phi(r) = 0_S\}$$

Theorem 4.8

A ring homomorphism $\phi : R \to S$ is injective if and only if $\ker \phi = \{0_R\}$.

Proof. ϕ is also a group homomorphism. So ϕ is injective if and only if $\ker \phi = \{0_R\}$. □

Definition 4.11

Let R be a ring. Then for $n \in \mathbb{N}$, define $n_R = \underbrace{1_R + \ldots + 1_R}_{n \text{ times}}$.

Definition 4.12

A ring R has **characteristic** n if n is the smallest positive integer such that $n_R = 0_R$. If no such integer exists, then we say R has **characteristic zero**.

Example 4.13

$\operatorname{char}(\mathbb{Z}) = 0$. $\operatorname{char}\left(\mathbb{Z}/n\mathbb{Z}\right) = n$. $\operatorname{char}\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} = 24$.

4.4 Ideals and Quotient Rings

We now investigate a way to properly define a structure similar to the quotient group structure. Unlike in the case of groups, it does not necessarily make sense to quotient by a subring. To see why, consider the following: let $S \subseteq R$ be some additive subgroup of $(R, +)$ (not necessarily with any multiplicative structure). Then consider the group R/S of

all additive cosets of S (note this is a group since $(R,+)$ is abelian). We want multiplication on these cosets to be well defined with respect to choice of representatives. In particular, for $x+S, y+S \in R/S$, we have

$$(x+S)(y+S) = xy + xS + yS + SS$$

For this to be equal to $xy+S$, we would need to know that $(x+y)S = S$. We can define the following structure, which guarantees that this occurs:

Definition 4.13

An **ideal** of a ring R is a nonempty subset $I \subseteq R$ such that:

1. If $x_1, x_2 \in I$ then $x_1 + x_2 \in I$.
2. If $x \in I$ and $r \in R$, then $rx \in I$.

Note that if $1 \in I$, then for $r \in R$ we have $r1 = r \in I$. Thus $I = R$.

We can compare the definitions of subrings and ideals, both of which are structured subsets of a ring:

	Subring	Ideal
Closed under addition	✓	✓
Closed under multiplication by itself	✓	✓
Contains 0	✓	✓
Closed under multiplication by elements of R	✗	✓
Contains 1	✓	✗

Notice that ideals contain additive inverses, since if $x \in I$ then $(-1) \in R$ and $(-1)x = -x \in I$. Thus both ideals and subrings are subgroups under addition of $(R,+)$, but differ in their multiplicative structure.

Proposition 4.9

The following are true about ideals:

1. Every ideal contains 0.
2. Every ideal contains additive inverses. In particular, $(I,+) \leqslant (R,+)$.
3. If $1 \in I$ then $I = R$.
4. If R is a field, then every ideal is $I = \{0\}$ or $I = R$.

The first three are straightforward or have been discussed.

Proof of 4. Let $I \subseteq R$ be an ideal. Suppose there is some $x \in I$ nonzero. Then there exists $x^{-1} \in R$. It follows that $x^{-1}x = 1 \in R$. By 3, $I = R$. □

Example 4.14

The following are ideals:

1. $I = \{2n : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
2. $I = \{18a + 24b : a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
3. $I = \{f : f(0) = 0\} \subseteq \mathbb{R}[x]$.
4. $I = \{f = b_0 + b_1 x + \ldots + b_n x^n : n \in \mathbb{N}, b_i \text{ even } \} \subseteq \mathbb{Z}[x]$.
5. $I = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \subseteq {}^{\mathbb{Z}}\!/_{12\mathbb{Z}}$.

Example 4.15

The following are not ideals:

1. $I = \{2n + 1 : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
2. $I = \{f : f(0) \neq 0\} \subseteq \mathbb{R}[x]$.

In the case of groups, kernels of homomorphisms were subgroups. In the case of rings, however, kernels are not necessarily subrings, but ideals.

Proposition 4.10

Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \subseteq R$ is an ideal.

Proof. Let $x, x_1, x_2 \in \ker(\phi)$, and $r \in R$. Then

$$\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2) = 0 + 0 = 0$$

and

$$\phi(rx) = \phi(r)\phi(x) = 0$$

so $\ker \phi$ is an ideal. □

In fact, if $\phi : R \to S$ is a ring homomorphism and $1_S \neq 0_S$, then $\ker \phi$ is not a subring, since $\phi(1_R) = 1_S \neq 0_S$. Thus $1_R \notin \ker \phi$, meaning $\ker \phi$ is not a subring.

On the other hand, $\text{im}(\phi)$ is always a subring, but in general is not an ideal (since $1_S \in \text{im}\, \phi$. If $\text{im}\, \phi$ is an ideal, then $\text{im}\, \phi = S$).

Definition 4.14

Let $r_1, \ldots, r_k \in R$. Then the **ideal generated by** $r_1, \ldots, r_k$ is the set

$$(r_1, \ldots, r_k) \coloneqq \{x_1 r_1 + \ldots + x_k r_k : x_1, \ldots, x_k \in R\} \subseteq R$$

An ideal of the form $(r) = Rr$ is called a **principal ideal**.

One may verify that the above structures are indeed ideals.

Definition 4.15

A domain R is called a **principal ideal domain**, or PID, if every ideal in R is principal and R is a domain.

Example 4.16

We showed that every additive subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z} = (n)$. Any ideal is an additive subgroup, so all additive subgroups of $\mathbb{Z}$ are principal ideals. Thus $\mathbb{Z}$ is a PID.

Proposition 4.11

Let K be a field. Then $K[x]$ is a PID.

Proof. Let $I \subseteq K[x]$ be a nonzero ideal. Let $f \in I$ be a nonzero element of minimal degree. We want to show that $I = (f)$. To prove this, let $g \in I$. Then apply Euclidean division to write

$$g = qf + r$$

where $q \in K[x]$ and $r \in K[x]$ is zero or $\deg(r) < \deg(f)$. By the ideal structure, $qf \in I$ so

$$r = g - qf \in I$$

But f is of minimal degree so $r = 0$. Thus $(f) = I$. So $K[x]$ is a PID. □

Definition 4.16

Let K be a field. Then $K[x, y]$ is the set of all multivariate polynomials in x, y, defined by

$$K[x,y] = \left\{ \sum_{i=0}^{n} \left(\prod_{j=0}^{i} a_{i,j} x^i y^j \right) \middle| n \in \mathbb{N}, a_{i,j} \in K \right\}$$

Example 4.17

Let us consider some rings which are not PIDs.

Let $R = K[x, y]$ for some field K. Then $(x, y) \subseteq K[x, y]$ is not principal. To see this, suppose $(x, y) = (f)$ for some $f \in K[x, y]$. Then $f|x$ and $f|y$. This is not possible unless f is a unit. But (x, y) is the set of all polynomials with no constant term, so $(f) \neq (x, y)$.

Definition 4.17

Let $I \subseteq R$ be an ideal. Then I is called a **maximal ideal** if $I \neq R$ and the only ideal $J \in R$ such that $I \subsetneq J$ is $J = R$. An ideal is called **prime** if for any $r, s \in R$ with $rs \in I$, we have $r \in I$ or $s \in I$.

4.5 Symmetric Polynomials

In this section we lay the foundation for some of our later study of Galois theory.

Recall that for R a ring, $R[x_1, \ldots, x_n]$ represents the set of all multivariable polynomials over R in variables $x_1, \ldots, x_n$.

Definition 4.18

A polynomial $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a **symmetric polynomial** if for any permutation $\tau \in S_n$ we have

$$p(x_{\tau(1)}, \ldots, x_{\tau(n)}) = p(x_1, \ldots, x_n)$$

In other words, p is stable under a permutation of the variables.

Example 4.18

$x^2 + y^2$ and $x^2 + 5xy + y^2$ are symmetric polynomials in $\mathbb{R}[x, y]$. x^2, $xy + y^2$, and $x^2 + 5xy + 2y^2$ are not symmetric polynomials in $\mathbb{R}[x, y]$.

For some key examples of symmetric polynomials, we have the following:

Definition 4.19

An **elementary symmetric polynomial** in $R[u_1, \ldots, u_n]$ is a polynomial of the form s_m for some $0 \leq m \leq n$, where

$$\begin{aligned}
s_0 &= 1 \\
s_1 &= \sum_i u_i = u_1 + \ldots + u_n \\
s_2 &= \sum_{i<j} u_i u_j = u_1 u_2 + u_1 u_3 + \ldots \\
s_3 &= \sum_{i<j<k} u_i u_j u_k \\
&\vdots \\
s_n &= u_1 u_2 \cdots u_n
\end{aligned}$$

Example 4.19

In $R[x, y]$, the symmetric polynomials are $1, x + y, xy$. In $R[x, y, z]$, the elementary symmetric polynomials are $1, x + y + z, xy + yz + xz, xyz$.

Elementary symmetric polynomials are important since they generate the set of all symmetric polynomials:

Theorem 4.12: Symmetric Function Theorem

Every symmetric polynomial $g(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ can be written uniquely (up to ordering) as a multivariable polynomial in the elementary symmetric polynomials $s_1, \ldots, s_n$.

We do not provide a proof of the Symmetric Function Theorem here; however, the following examples demonstrate that the general strategy is to reduce the degree and factor the resulting polynomial:

Example 4.20

$$x^2 + y^2 = (x + y)^2 - 2xy = s_1^2 - 2s_2$$

Example 4.21

$$\begin{aligned} x^3 + y^3 + z^3 &= (z^3 + y^3 + z^3) - 3(x^2y + x^2z + y^2x + y^2z + z^2x + z^2y) \\ &= s_1^3 - 3(xy + yz + zx)(x + y + z) + 9xyz \\ &= s_1^3 - 3s_2s_1 + 9s_3 \end{aligned}$$

Remark 4.2

Let $p(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$ be a polynomial with roots $u_1, \ldots, u_n$. By Vieta's formulas, p may be written as

$$p(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \ldots \pm s_n$$

So Vieta's formulas tell us that the coefficients of a polynomial are the symmetric functions in the roots of the polynomial.

Example 4.22

$$(x - u_1)(x - u_2) = x^2 - (u_1 + u_2)x + u_1u_2 = x^2 - s_1x + s_2$$

and similarly

$$(x-u_1)(x-u_2)(x-u_3) = x^3 - s_1x^2 + s_2x - s_3$$

4.6 Quotient Rings

In this section we investigate a proper definition of quotient rings. As in the case of quotient groups, quotient rings have the intuition of treating elements as equal up to an element of the quotienting object. We will also use the intuition we have developed so far, where as much work as possible in ring theory is delegated to group theory. For instance, a quotient ring of a ring should also be a quotient group under addition. Thus, the important part is to consider which choices of subgroup ensure that multiplication is well defined.

First, note that addition is commutative, so we can quotient by any subgroup. Let $S \subseteq R$ be an additive subgroup. Let $x, y \in R$. Then we have

$$(x+S)(y+S) = xy + xS + yS + S^2$$

We want the right side to be equal to $xy + S$. This certainly happens when S is an ideal of R. In fact, this only happens when S is an ideal. Thus the objects which make sense to quotient rings by are not subrings, but ideals.

Definition 4.20

If $I \subseteq R$ is an ideal and $x, y \in R$, then we write

$$x =\!\equiv y \pmod{I} \iff x - y \in I$$

Definition 4.21

Let $I \subseteq R$ be an ideal. Then the **quotient ring** of R by I is the additive group R/I, with the multiplicative operation

$$(x+I)(y+I) \coloneqq xy + I$$

and additive identity I, multiplicative identity $1 + I$.

We can formally show that multiplication well defined:

Proposition 4.13

R/I is a ring.

Proof. We check that multiplication is well defined:

Let $r' \equiv r \pmod I$ and $s \equiv s' \pmod I$. Write $r' = r + a$ and $s' = s + b$ for $a, b \in I$. Then

$$r's' = (r + a)(s + b) = rs + as + rb + ab \in rs + I$$

Thus multiplication is well defined.

Most of the other properties are inherited from R. The only one we check is distributivity: Let $\overline{x}, \overline{y}, \overline{z} \in {}^{R}\!/_{I}$. We have

$$(\overline{x} + \overline{y})\overline{z} = \overline{x + y}\overline{z} - \overline{(x + y)z} = \overline{xz + yx} = \overline{xz} + \overline{yz} = \overline{xz} + \overline{yz} \qquad \square$$

Consider the canonical map $\text{can} : R \to {}^{R}\!/_{I}$. From the fact that can is a group homomorphism, we know that $\ker \text{can} = I$.

As in the case of groups, this shows a deep connection between quotient objects, ideals, and homomorphisms, which can be summarized in the first isomorphism theorem for rings.

Theorem 4.14: First Isomorphism Theorem for Rings

Let $\phi : R \to S$ be a surjective ring homomorphism. Let $K = \ker \phi$. Then there exists an isomorphism $\psi : {}^{R}\!/_{K} \xrightarrow{\cong} S$ such that the following diagram commutes:

$$R \xrightarrow{\text{can}} {}^{R}\!/_{K} \xrightarrow{\psi} S, \qquad R \xrightarrow{\phi} S$$

Proof. Define ψ such that $\psi(\overline{r}) = \phi(r)$. This is Well-definedness and bijection follow from the first isomorphism theorem for groups. To check that it is a ring homomorphism, let $r, s \in R$. Then

$$\psi(\overline{r}\,\overline{s}) = \psi(\overline{rs}) = \phi(rs) = \phi(r)\phi(s) = \psi(\overline{r})\psi(\overline{s})$$

Also $\psi(\overline{1}) = \phi(1) = 1$. $\square$

Example 4.23

Consider the ring $\mathbb{R}[x]$ quotiented by the ideal $I = (x^2+1)$. We claim that ${}^{\mathbb{R}[x]}\!/_{I} \cong \mathbb{C}$. Note that $f(x) \equiv r(x) \pmod I$ when $r(x)$ is the remainder of division by I. IN particular, r has degree ≤ 1, so ${}^{\mathbb{R}[x]}\!/_{(x^2+1)} = \{\overline{a + bx} : ab \in \mathbb{R}\}$ where $x^2 \equiv 1 \pmod I$. Thus the map sending $\overline{ab + x} \mapsto a + bi$ is an isomorphism ${}^{\mathbb{R}[x]}\!/_{(x^2+1)} \xrightarrow{\cong} \mathbb{C}$.

Another way to prove this isomorphism is to consider the homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by

$$\begin{aligned}\phi(b_0 + b_1 x + \ldots + b_m x^m) &= b_0 + b_1 i + b_2 i^2 + \ldots + b_m i^m \\ &= (b_0 - b_2 + b_4 - \ldots) + i\,(b_1 - b_3 + b_5 - \ldots)\end{aligned}$$

This isomorphism is essentialy given by $\phi(f) = f(i)$. This is surjective. To calculate

$\ker\phi$, pick $g(x) \in \ker\phi$. Then $g(i) = 0$. Since g has real coefficients, $g(-i) = \overline{g(i)} = \overline{0} = 0$. Thus $(x-i)(x+i) = (x^2+1) | g(x)$. So $\ker\phi \subseteq (x^2+1)$. Also, one can manually check that $(x^2+1) \subseteq \ker\phi$. So by the first isomorphism theorem,

$$\mathbb{R}[x]/(x^2+1) \cong \operatorname{im}\phi = \mathbb{C}$$

We observe that a similar construction can be done in other rings, giving

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$$

and

$$\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}[i]$$

We can also use quotient rings to construct finite fields with non-prime numbers of elements.

Example 4.24

Consider

$$K = \mathbb{F}_2[x]/(x^2+x+1)$$

This consists only of polynomials of degree at most 1, so

$$K = \{\overline{a+bx} : a, b \in \mathbb{F}_2\} = \{\overline{0}, \overline{1}, \overline{x}, \overline{1+x}\}$$

We can also calculate the multiplication table as

	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{x}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

We can see that K is a nonzero ring where each nonzero element is invertible. Thus it is a field with four elements.

Definition 4.22

A polynomial is $f \in R[x]$, where R is a ring, is called **monic** if the coefficient of the highest degree term is 1_R.

The importance of monic polynomials is that we can run long division by monic polynomials. That is, if $f \in R[x]$ is monic and $g \in R[x]$ is arbitrary, then we can write $g(x) = q(x)f(x) + r(x)$ where $q, r \in R[x]$ and $r = 0$ or $\deg(r) < \deg(f)$.

Theorem 4.15

Let $f \in R[x]$ be monic and of degree n. Then every element of $R[x]/(f)$ can be uniquely written as

$$\overline{r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}}$$

for $r_0, \ldots, r_{n-1} \in R$.

The intuition is that if $f(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} + x^n$, then $R[x]/(f)$ considers all R-polynomials under the relation $x^n = -(b_0 + \ldots + b_{n-1}x^{n-1})$.

Proof. Existence: every element of $R[x]/(f)$ is of the form $\overline{g}$ for some $g \in R[x]$. Then write

$$g(x) = q(x)f(x) + r(x)$$

for $q, r \in R[x]$ with $r = 0$ or $\deg r < n$. It follows that

$$\overline{g(x)} = \underbrace{\overline{q(x)f(x)}}_{\in(f)} + \overline{r(x)} = r(x)$$

Uniqueness: Suppose that

$$\overline{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}} = \overline{b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}}$$

Then their difference is in (f), so

$$(a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1} \in (f)$$

But since f is monic, every nonzero element of (f) has degree at least n. Thus $a_0 = b_0, \ldots, a_{n-1} = b_{n-1}$. □

Theorem 4.16

Let K be a field and $f \in K[x]$ an irreducible polynomial. Then $K[x]/(f)$ is a field.

Proof. We just need to show that every nonzero element is invertible. Let $g \in K[x]$ such that $\overline{g} \neq \overline{0}$, which is equivalent to assuming that f does not divide g. Since f is irreducible, this means that $\gcd(f, g) = 1$. So by the Extended Euclidean algorithm, there exist $u, v \in K[x]$ such that

$$ug + vf = 1 \implies \overline{ug} = \overline{1}$$

So $\overline{g}$ is invertible. □

4.7 Algebraic Number Theory

Because rings are generalizations of $\mathbb{Z}$, we can use results of ring theory to study the structure of the integers, which is the field of algebraic number theory. Here, we will prove some results to demonstrate how this may happen.

Example 4.25

Find all integer solutions of the equation $y^2 = x^3 + 1$ with y even.

Write $x^3 = y^2 - 1 = (y+1)(y-1)$. We claim that $d = \gcd(y+1, y-1) = 1$. To see this, we know $d|(y+1) - (y-1) = 2$, so $d = 1, 2$. But $y-1, y+1$ are odd so $d = 1$.

Since $y+1, y-1$ multiply to a cube but share no common factors, they must both be cubes. So $u^3 = y+1, v^3 = y-1$ for $u, v \in \mathbb{Z}$. But the only cubes that differ by 2 (we can make a list and observe) are $u = 1, v = -1$. Thus the only solution is $y = 0, x = -1$.

The above problem was purely number theoretic and required no ring theory. However, if we instead change the problem to finding all integer solutions to $y^2 = x^3 + 2$, then our approach cannot be purely number theoretic, since we will have to factor using $\sqrt{2}$. In other words, we will need to make sense of prime decomposition and the gcd in $\mathbb{Z}[\sqrt{2}]$. This will motivate our work in the following.

Definition 4.23

Assume R is a domain. Then:

1. $u \in R$ is called a **unit** if $us = 1$ for some $s \in R$, or equivalently if $1 \in (u)$.
2. $a|b$ if there exists $q \in R$ such that $aq = b$.
3. a and b are called **associates** if there exists a unit u such that $au = b$.
4. a is **irreducible** if it is not a unit and its only divisors are its associates or units.
5. p is **prime** if it is not a unit and given $ab \in R$ such that $p|ab$, then $p|a$ or $p|b$.

Proposition 4.17

Let R be a domain and let $p \in R$ be a prime element. Then p is irreducible.

Proof. Let $p = ab$ for $a, b \in R$. Since p is prime, we have $p|a$ or $p|b$. Assume without loss of generality that $p|a$. Then there exists $r \in R$ such that $pr = a$. Then

$$a = pr = abs$$

so $a(1 - bs) = 0$. Thus b is a unit. So a is an associate and b is a unit. Thus p is irreducible. □

Note that over $\mathbb{Z}$ or $K[x]$ where K is a field, then being prime and irreducible are equivalent.

We note that when we began studying our elementary number theory in $\mathbb{Z}$, we progressed in the following order:

1. Division Algorithm
2. Extended Euclidean Algorithm
3. Prime factorization

The above three do not always hold in rings. Thus we will separately study Euclidean rings, where the division algorithm holds, PIDs, where the extended Euclidean algorithm holds, and unique factorization domains, where prime factorization holds.

Definition 4.24

A domain R is called a **Euclidean ring** if there exists a function (called a **valuation**)

$$\nu : R \to \mathbb{Z}_{\geq 0}$$

such that for $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $\nu(r) < \nu(b)$.

Example 4.26

1. $\mathbb{Z}$ is Euclidean under the valuation $\nu(a) = |a|$.
2. $K[x]$ is Euclidean under the valuation $\nu(f) = \deg(f)$.
3. $\mathbb{Z}[i]$ is Euclidean under the valuation $\nu(x + iy) = x^2 + y^2 = |z|^2$.
4. $\mathbb{Z}[\sqrt{-2}]$ is Euclidean under the valuation $\nu(x + y\sqrt{-2}) = x^2 + 2y^2$.

Note that $\mathbb{Z}[\sqrt{d}]$ is Euclidean with the valuation $\nu(x + y\sqrt{d}) = x^2 - dy^2$ if and only if $d = -2, -1, 2, 3, 6, 7, 11, 19$. It is also multiplicative (even when it is not actually a valuation).

Proposition 4.18

Let $d \geq 1$. Then $z \in \mathbb{Z}[\sqrt{-d}]$ is a unit if and only if $\nu(z) = 1$ (even when ν is not a valuation).

In particular, if $\nu(a + b\sqrt{-d}) = 1$, then $a^2 + db^2 = 1$, so:

- If $d = 1$ then $a = \pm 1$ or $b = \pm 1$. In other words, the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.
- If $d > 1$ then $b = 0$ and $a = \pm 1$. So the only units are ± 1.

Proof. If z is a unit, then $zw = 1$ for $w \in \mathbb{Z}[\sqrt{-d}]$. Thus $1 = \nu(zw) = \nu(z)\nu(w)$ so $\nu(z) = 1$. □

Example 4.27

To see that not all values of d work, consider $\mathbb{Z}[\sqrt{-3}]$. We show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, which we define shortly. We will also show that being a Euclidean domain implies that a ring is a UFD. Thus if $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, it is not Euclidean. To see this, first note that

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

So we have two distinct factorizations. We need to show that the factorizations are by irreducible elements. To show that 2 is irreducible, suppose $2 = zw$ for some $z, w \in \mathbb{Z}[\sqrt{-3}]$. Since ν is multiplicative (we don't know a priori that it is a valuation, since it is not, but it is multiplicative regardless),

$$4 = \nu(2) = \nu(z)\nu(w)$$

If 2 is reducible then by Proposition 4.18, $\nu(z) = \nu(w) = 2$. But $a^2 + 3b^2$ is never equal to 2. So 2 is irreducible. The same argument holds since $\nu(1 + \sqrt{-3}) = 4$ as well. Thus if $\mathbb{Z}[\sqrt{-2}]$ is UFD, we must have that $2|1 + \sqrt{-3}$ or $1 - \sqrt{-3}$. But if $1 + \sqrt{-3} = 2(a + b\sqrt{-3})$ then $2|1$, which is impossible. So $\mathbb{Z}[\sqrt{-3}]$ is not a UFD and hence not Euclidean.

We now consider PIDs. Let R be a PID and let $d \in R$ be such that $(r, s) = (d)$. We define $\gcd(r, s) = d$, which is well defined up to associates. In particular, if $\gcd(r, s)$ is a unit, then $(r, s) = (1)$ so there exist $u, v \in R$ such that $uv + rs = 1$.

Proposition 4.19: Euclid's Lemma

Let R be a PID and $p \in R$ irreducible. Then p is prime.

Definition 4.25

A **unique factorization domain** is a domain R such that for any $r \in R$, there exist $p_1, \ldots, p_k$ irreducible such that $r = p_1 \cdots p_k$, and the factorization is unique up to reordering and associates.

Theorem 4.20

Every PID is a UFD.

Proof. The uniqueness follows as in $\mathbb{Z}$. To show existence, we apply the following algorithm:

1. If r is irreducible then we are done.
2. Otherwise, write $r = ab$. If a, b are irreducible, then we are done.
3. Otherwise pick one which is reducible and split it again.

4. Continue until this terminates.

Showing that the process terminates in the general case is somewhat difficult. However, in cases such as $\mathbb{Z}, K[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}]$, the valuation of the reducibles decreases at each step, so by infinite descent it will terminate. □

We use the following to give some more proofs from number theory in the first few sections of these notes.

Theorem

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

Recall the following:

Lemma

If p is odd then -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 4$.

The point is that $x^2 + y^2 = (x + iy)(x - iy)$, so if p can be written as a sum of squares, then it is not prime in $\mathbb{Z}[i]$. Thus we need to find when p is or is not prime in $\mathbb{Z}[i]$.

Lemma

Let p be a prime in $\mathbb{Z}$. If $p \equiv 1 \pmod 4$, then p is not prime in $\mathbb{Z}[i]$.

Proof. By the previous lemma, there exists $x \in \mathbb{Z}$ such that $p | x^2 + 1$. Suppose p is prime in $\mathbb{Z}[i]$. Then $p|(x - i)(x + i)$ but p divides neither since it does not divide ± 1. □

Proof of Theorem. Suppose $p \equiv 3 \pmod 4$. Then p is not a sum of squares since -1 is not a quadratic residue. If $p \equiv 1 \pmod 4$ then p is not a prime in $\mathbb{Z}[i]$. Thus there exist nonunits $z, w \in \mathbb{Z}[i]$ such that $p = zw$. Since $p^2 = \nu(p) = \nu(z)\nu(w)$, then $\nu(z) = \nu(w) = p$. Write $z = x + yi$. Then $p = \nu(z) = x^2 + y^2$. □

4.8 Modules

We now arrive at the concept of modules, which generalize the concept of a vector space to work over rings instead of fields. Indeed, the vector space axioms all make sense when expressed in terms of ring elements; however, many nice properties do not hold in modules. Nevertheless, the concept of a module is very important for extending linear algebra to even more general settings.

Definition 4.26

Let R be a ring. Then a **module** over R, or an R-module, is an abelian group $(M, +)$ admitting an action $\cdot : R \times M \to M$ such that for all $r, s \in R, v, v' \in M$,

1. $1 \cdot v = v$ for all $v \in M$,
2. $(rs) \cdot v = r \cdot (s \cdot v)$,
3. $(r + s) \cdot v = r \cdot v + s \cdot v$,
4. $r \cdot (v + v') = r \cdot v + r \cdot v'$.

Notice that the module axioms are precisely those for a vector space, just over a ring instead of a vector space. In particular, a vector space over a field K is a K-module. Let us consider some other examples of modules.

Example 4.28

If R is a ring, then R^n is an R-module. For instance, the lattice $\mathbb{Z}^2$ is a module over $\mathbb{Z}$.

Example 4.29

If I is an ideal of R, then R/I is an R-module.

The definition of a module implies that a module is an abelian group. But moreover we can a $\mathbb{Z}$-module structure over any abelian group using repeated addition. That is, for $n \in \mathbb{N}, g \in G$ we define

$$n \cdot g = \underbrace{g + \ldots + g}_{n \text{ times}}$$

and $(-n) \cdot g = -(n \cdot g)$. Thus abelian groups and $\mathbb{Z}$-modules are precisely the same things.

Definition 4.27

Let M be an R-module. Then a subset $N \subseteq M$ is called a **submodule** if it is closed under addition and scalar multiplication by R.

Example 4.30

$\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module. Then $2\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ is a submodule.

Note that the correspondence between abelian groups and $\mathbb{Z}$-modules implies that any submodule of a $\mathbb{Z}$-module is just a subgroup.

Definition 4.28

Let M, N be R-modules. Then $\varphi : M \to N$ is an R-**module homomorphism** if:

1. φ is a group homomorphism.

2. $\varphi(rm) = r\varphi(m)$ for all $r, \in R, m \in M$.

In particular, a bijective module homomorphism is a **module isomorphism**

Definition 4.29

Let $N \subseteq M$ be a submodule. Then we define the **quotient module** to be

$$M/N \coloneqq \{m + N : m \in M\}$$

In particular, this is indeed an R-module.

Definition 4.30

Let M be a R-module and let $m_1, \ldots, m_k \in M$.

1. We say that $m_1, \ldots, m_k$ **span** or **generate** M if every $m \in M$ can be written as
$$m = r_1 m_1 + \ldots + r_k m_k$$
for $r_1, \ldots, r_k \in R$. If M admits a finite spanning set then M is said to be **finitely generated**.
2. We say that $m_1, \ldots, m_k$ are R-**linearly independent** if
$$r_1 m_1 + \ldots + r_k m_k = 0 \implies r_1 = \ldots = r_k = 0$$
3. We say that $m_1, \ldots m_k$ is a **basis** of M if 1 and 2 hold.

Definition 4.31

An R-module is called a **free module** if $M \cong R^n$ for some n.

Proposition 4.21

An R-module M is free if and only if it admits a basis.

Proof. ($\implies$) If $M \cong R^n$ then a basis is $e_1, \ldots, e_n$, where

$$e_i = \begin{bmatrix} 0 & \ldots & 1 & \ldots & 1 \end{bmatrix}^T$$

($\impliedby$). If M admits a basis, then we construct an isomorphism $R^n \to M$ by defining

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \mapsto r_1 m_1 + \ldots + r_k m_k$$

which is an isomorphism. □

Example 4.31

$\mathbb{Z}/5\mathbb{Z}$ is not a free $\mathbb{Z}$-module, since for any $x \in \mathbb{Z}/5\mathbb{Z}$, $5x = 0$. So it admits no linearly independent sets. (It is also of finite cardinality, and every free $\mathbb{Z}$-module is infinite.)

Example 4.32

Let us construct a basis for

$$V = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \middle| x + y + z \right\} \subseteq \mathbb{Z}^3$$

Since $z = -x - y$, we have

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}$$

and we can check that these are $\mathbb{Z}$-linearly independent, so

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix} \right\}$$

is a basis.

Example 4.33

Let us construct a basis for

$$V = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \middle| 5x + 7y = 0 \right\} \subseteq \mathbb{Z}^2$$

We cannot apply the same trick from the previous example since we cannot divide by 5. Instead, we observe that if $5x + 7y = 0$, then $5|y$ and $7|x$. So if $y = 5a, x = 8b$, then $35b + 35a = 0$, which implies that $b = -a$. So any vector in V is given (uniquely) by

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7a \\ -5a \end{bmatrix} = a \begin{bmatrix} 7 \\ -5 \end{bmatrix}$$

Example 4.34

Let

$$V = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \middle| 5x + 7y + 11z = 0 \right\} \subseteq \mathbb{Z}^3$$

Over $\mathbb{Q}$ this suggest the basis

$$\left\{ \begin{bmatrix} -\frac{7}{5} \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -\frac{11}{5} \\ 0 \\ 1 \end{bmatrix} \right\}$$

which suggest the following basis over $\mathbb{Z}$:

$$\left\{ \begin{bmatrix} -7 \\ 5 \\ 0 \end{bmatrix}, \begin{bmatrix} -11 \\ 0 \\ 5 \end{bmatrix} \right\}$$

However, the element

$$\begin{bmatrix} -5 \\ 2 \\ 1 \end{bmatrix} \notin \operatorname{span} \left\{ \begin{bmatrix} -7 \\ 5 \\ 0 \end{bmatrix}, \begin{bmatrix} -11 \\ 0 \\ 5 \end{bmatrix} \right\}$$

This because every element in the span has a third coordinate divisible by 5. Instead, we can run the extended Euclidean algorithm to instead get the basis

$$\left\{ \begin{bmatrix} -7 \\ 5 \\ 0 \end{bmatrix}, \begin{bmatrix} -5 \\ 2 \\ 1 \end{bmatrix} \right\}$$

Definition 4.32

Let M be an R-module for R a domain. We say that M is **torsion-free** if given $R \in R$, $m \in M \setminus \{0\}$, we have

$$rm = 0 \iff r = 0$$

Example 4.35

$\mathbb{Z}^2$ is torsion free over $\mathbb{Z}$, but $\mathbb{Z}/5\mathbb{Z}$ is not (nor is any $\mathbb{Z}/n\mathbb{Z}$).

The following is a weak version of the main theorem for modules.

Theorem 4.22

Let R be a PID. If M is a torsion-free, finitely generated R-module, then M admits a basis.

However, many modules are not torsion-free. To generalize this, we need to weaken our notion of a basis.

Definition 4.33

If R is a domain and M an R-module, then $\{m_1, \ldots, m_k\} \subseteq M$ is called a **weak basis** with torsion $\{d_1, \ldots, d_k\} \subseteq R$ if:

1. $m_1, \ldots, m_k$ span M.
2. $d_1 m_1 = d_2 m_2 = \ldots = d_k m_k = 0$.
3. Any linear relation $r_1 m_1 + \ldots + r_k m_k = 0$ is an R-linear combination of relations in (2).

Example 4.36

Let $M = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times \mathbb{Z}$ be a $\mathbb{Z}$-module (recall that any abelian group can be considered canonically as a $\mathbb{Z}$-module). Then e_1, e_2, e_3 span M, and is a weak basis with torsion $2, 3, 0$.

Notice that if M is torsion free, then the only choice of d_i for (2) is $d_1 = \ldots = d_k = 0$. Thus (3) gives us that any weak basis is actually just a basis.

The key point here is that if M admits a weak basis $m_1, \ldots, m_k$ with torsion $d_1, \ldots, d_k \in R$, then

$$M \cong {}^{R}\!/_{(d_1)} \times \ldots \times {}^{R}\!/_{(d_k)}$$

This can be seen using the mapping from the RHS to the LHS given by

$$\begin{bmatrix} \overline{r_1} \\ \vdots \\ \overline{r_k} \end{bmatrix} \mapsto r_1 m_1 + \ldots + r_k m_k$$

where $\overline{r_i} \in {}^{R}\!/_{(d_i)}$. This is defined since $d_i m_i = 0$.

We can now state the stronger version of the main theorem for modules, as well as an immediate corollary, which we will then prove.

Theorem 4.23

Let R be a PID and M a finitely generated R-module. Then M admits a weak basis, and therefore there exist $d_1, \ldots, d_k \in R$ such that

$$M \cong {}^{R}\!/_{(d_1)} \times \ldots \times {}^{R}\!/_{(d_k)}$$

Since we can consider abelian groups as $\mathbb{Z}$-modules, we can then apply this theorem to classify all finitely generated abelian groups.

Corollary 4.24: Classification of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then there exist nonzero integers $a_1, \ldots, a_k \in \mathbb{Z}$ and $m \in \mathbb{Z}$ such that

$$G \cong {}^{\mathbb{Z}}\!/_{a_1} \times \ldots \times {}^{\mathbb{Z}}\!/_{a_k} \times \mathbb{Z}^m$$

Note that $\mathbb{Z}^m$ factor comes from a number of products of the form ${}^{\mathbb{Z}}\!/_{0}$, which represents the non-torsion part of the group. In particular, any finite abelian group is a product of finite cyclic groups.

We now consider the main theorem. Consider the setting of a vector space V over some field K, with $L : V \to V$ a linear map.

Definition 4.34

Let V be a finite dimensional vector space over K a field, and $L : V \to V$ a linear map. Define V as a module over $K[x]$ by defining

$$p(x) \cdot v \coloneqq p(L)v$$

for $p \in K[x], v \in V$.

For instance, we define $(2+3^2)v = 2v+3L^2(v)$. Note that as a K-module, V is isomorphic to the free module $K \times \ldots \times K$. However, using $K[x]$-structure, we get a different result.

Theorem 4.25

Let V be a vector space over K, and $L : V \to V$ a linear map. Define V as a module over $K[x]$ as above. Then in the category of $K[x]$ modules,

$$V \cong {}^{K[x]}\!/_{(f_1)} \times \ldots \times {}^{K[x]}\!/_{(f_k)}$$

for $f_1, \ldots, f_k \in K[x]$ nonzero.

Note that by the Chinese remainder theorem, we may assume $f_i = g_i^{\alpha_i}$ where g_i are each

irreducible, since otherwise we would have $f = gh$ and

$$K[x]/(f) \cong K[x]/(g) \times K[x]/(h)$$

This result allows us to prove the Jordan canonical form much more easily than we did by hand in linear algebra.

Corollary 4.26

Let V be a finite dimensional complex vector space and A an $n \times n$ matrix. Then A is similar to a matrix of the form

$$A \sim \begin{bmatrix} \mathfrak{J}_1 & & O \\ & \ddots & \\ O & & \mathfrak{J}_k \end{bmatrix}$$

where each $\mathfrak{J}_i$ is a Jordan block of the form

$$\mathfrak{J}_i = \begin{bmatrix} \lambda_i & 1 & & O \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ O & & & \lambda_i \end{bmatrix}$$

Proof. By the fundamental theorem of algebra, irreducible polynomials in $\mathbb{C}[x]$ are linear, so applying the previous theorem with $L = L_A$, there exist $a_i \in \mathbb{C}, b_i \in \mathbb{N}$ such that

$$V \cong \mathbb{C}[x]/(x-a_1)^{b_1} \times \ldots \times \mathbb{C}[x]/(x-a_k)^{b_k}$$

Consider first the case that $k = 1$. Then $\mathbb{C}[x]/(x-a)^b$ has a basis

$$1, (x-a), (x-a)^2, \ldots, (x-a)^{b-1}$$

Then passing through the isomorphism, these map to some basis of V given by $v_0, \ldots, v_{b-1}$. Let us consider how A acts on each v_i. Factoring through the isomorphism and our choice module structure, Av_i corresponds to multiplying $(x-a)^i$ by x on the left, which is

$$x(x-a)^i = (x-a)^{i+1} + a(x-a)^i$$

so

$$Av_i = v_{i+1} + av_i$$

(If $i = b-1$, then $(x-a)^b = 0$ so that term drops out). Thus the matrix of A in the coordinates of $v_{b-1}, \ldots, v_0$ (note the order of the basis), we have

$$A \sim \begin{bmatrix} a & 1 & & O \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ O & & & a \end{bmatrix}$$

For the general case, we can take each of the factors $\mathbb{C}[x]/(x-a_i)^{b_i}$ and concatenate the bases. $\square$

We now prove the main theorem in the case of finitely generated abelian groups ($\mathbb{Z}$-modules), but the thoerem holds with more work for arbitrary R-modules for R a PID.

To do this, we first examine the Gaussian algorithm for integer matrices. This algorithm presents a method of reducing an arbitrary $n \times m$ matrix with integer coefficients to a diagonal matrix, using only elementary row and/or column operations.

Example 4.37

Let $A = \begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix}$. Then we apply operations:

$$\begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix} \to \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix} \to \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 1 \\ -4 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 2 & -4 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & -4 \end{bmatrix}$$

Notice that in the above example, we essentially just ran the Euclidean algorithm on the rows of the matrix. This procedure leads to the Gaussian algorithm:

1. Given $a, b \in \mathbb{Z}$ we can run the extended Euclidean algorithm, so that by swapping a, b and replacing (a, b) with $(a-b, b)$ or $(a, b-a)$, we eventually end up with $(d, 0)$, where $d = \gcd(a, b)$.

2. If we have a list of integers $(a_1, \ldots, a_k)$, then we can do the same to get $(d, 0, \ldots, 0)$ where $d = \gcd(a_1, \ldots, a_k)$.

3. We can run this algorithm on the first column of A by adding, subtracting, and swapping rows to get
$$A \mapsto \begin{bmatrix} d & * & * & * \\ 0 & * & * & * \\ \vdots & * & * & * \\ 0 & * & * & * \end{bmatrix}$$

4. Multiply by -1 if necessary, so we assume $d \geq 0$. Then:
   (a) If $d = 0$ then the whole column is zero, and we just run the algorithm on the remaning $n \times (m-1)$ submatrix.
   (b) If $d > 0$ and every other element in the first row is divisible by d, then we can clear the first row and then run the algorithm on the remaining $(n-1) \times (m-1)$ matrix.
   (c) If $d > 0$ but it does not divide some element in the first row, then we can run (3) on the first row instead of the first column. This will give us a matrix of the form
$$\begin{bmatrix} d' & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix}$$

where $d' < d$. We now return to (3) and run it again. Since $d' < d$, our new gcd will be less than d. By infinite descent, this process must terminate at some point, so we will eventually end up in case (a) or (b).

Thus we have shown that we may reduce the matrix to the form

$$\begin{bmatrix} d_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_k & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

With some extra work, we can also guarantee that $d_1 | d_2 | \dots | d_k$.

Example 4.38

Consider the $\mathbb{Z}$-module $M = {}^{\mathbb{Z}^2}\!/_N$, where

$$N = \mathbb{Z}\begin{bmatrix} 2 \\ 3 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 2 \\ 5 \end{bmatrix}$$

and consider $e_1, e_2 \in M$. We have $2e_1 + 3e_2 = 0$, and $2e_1 + 5e_2 = 0$. So we have the system of equations

$$\begin{cases} 2e_1 + 3e_2 = 0 \\ 2e_1 + 5e_2 = 0 \end{cases}$$

We can add and subtract these relations to get equivalent relations, which gives

$$\begin{cases} e_1 + 3e_2 = 0 \\ \quad 2e_2 = 0 \end{cases}$$

We could have also added or subtracted columns, which amounts to a change of basis. For instance, let $r \in \mathbb{Z}$ and set $v_1 = e_1 - re_2, v_2 = e_2$. Then

$$\begin{cases} v_1 + (3 + 2r)v_2 = 0 \\ 2v_1 + (5 + 2r)v_2 = 0 \end{cases}$$

so as a matrix operation, we have performed column addition:

$$\begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 3 + 2r \\ 2 & 5 + 2r \end{bmatrix}$$

Thus adding and subtracting columns is a change of basis. By applying the Gaussian algorithm to the matrix, which we did before, we observe that

$$w_1 = e_2 + (2e_1 + e_2), \qquad w_2 = e_1 + e_2$$

satisfies the relations and thus we have found a weak basis.

We now prove the main theorem.

Proof of Theorem 4.23. Let $x_1, \ldots, x_n \in G$ be generators. Consider the set of all relations between them; that is,

$$a_1 x_1 + \ldots + a_n x_n = 0$$

for $a_i \in \mathbb{Z}$.

Considering a simplified case, assume that finitely many relations generate the rest (under $\mathbb{Z}$-linear combinations). Then we can embed these into a $m \times n$ matrix, and then run the Gaussian algorithm. This gives us a diagonal matrix of the form

$$\begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

This gives us generators $y_1, \ldots, y_k \in G$ such that $d_1 y_1 = \ldots = d_k y_k = 0$, with $d_i \neq 0$. Then we have a weak basis, and

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}$$

In the general case, let $m > 0$ and pick m of the relations. Then disregarding the other relations,

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}$$

If we add another relation which is independent of the rest, we will have

$$G \cong \mathbb{Z}/c_1\mathbb{Z} \times \ldots \times \mathbb{Z}/c_l\mathbb{Z} \times \mathbb{Z}^{n-l}$$

where $l \leq k$ and $c_i \leq d_i$. By descent, this process terminates at some point, and we are done. $\square$

Chapter 5

Fields and Galois Theory

We now turn our attention to the final algebraic structure in this course: fields. In this chapter, our primary motivating examples will be $\mathbb{Q}$ and $\mathbb{C}$. We will see how the theory of field extensions leads to results in algebraic number theory, and we will examine basic results in Galois theory as well.

5.1 Field Extensions

Here we will work with abstract fields, but our primary examples will be $K = \mathbb{Q}$, $L = \mathbb{C}$. This is because $\mathbb{C}$ is the algebraic closure of $\mathbb{Q}$, and we don't want to take $K = \mathbb{R}$ since $\mathbb{R}$ only admits a single extension, which is directly to $\mathbb{C}$.

Definition 5.1

We say that $K \subseteq L$ is a **field extension** if K is a subfield of L. For a field extension $K \subseteq L$, we say $\alpha \in L$ is **algebraic** over K if there exists $p \in K[x]$ such that $p(\alpha) = 0$.

Example 5.1

i is algebraic over $\mathbb{Q}$, since it is the root of $x^2 + 1$. Similarly $\sqrt{3}$ is algebraic over $\mathbb{Q}$ since it is the root of $x^2 - 3$. On the other hand, π, e are not algebraic over $\mathbb{Q}$ (so they are transcendental.)

Definition 5.2

If $K \subseteq L$ is a field extension and $\alpha \in L$ is algebraic, then $f \in K[x]$ is called a **minimal polynomial** of α if $f(\alpha) = 0$ and $\deg(f)$ is minimal among monic polynomials vanishing on α.

Note that this is precisely the definition of the minimal polynomial of a matrix, so it is no surprise that we also have uniqueness here:

Proposition 5.1

Let f be a minimal polynomial of $\alpha \in L$. Let $g \in K[x]$ be such that $g(\alpha) = 0$. Then $f|g$.

Proof. Run the division algorithm to write

$$g = qf + r$$

where $r = 0$ or $\deg(r) < \deg(f)$. It follows that $r(\alpha) = 0$, but if $\deg(r) < \deg(f)$ then this contradicts minimality (r may not be monic but we can rescale it), so $r = 0$ and thus $f|g$. □

Proposition 5.2

The minimal polynomial of $\alpha \in L$ is unique.

Proof. If f, g are minimal polynomials, then $f|g$ and $g|f$. Both are monic, so $f = g$. □

Lemma 5.3

Minimal polynomials are irreducible.

Proof. Let f be the minimal polynomial of $\alpha \in L$, and write $f = f_1 f_2$ for $f_1, f_2 \in K[x]$ nonunits. Then

$$0 = f(\alpha) = f_1(\alpha) f_2(\alpha)$$

Since we are working over a field, $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$, contradiction. □

We now formalize a specific way of constructing a field extension, which is critical to the study of fields.

Definition 5.3

Let $K \subseteq L$ be a field extension and $\alpha \in L$. Then define $K[\alpha] \subseteq L$ (read "K **adjoin** α) to be

$$K[\alpha] \coloneqq \{b_0 + b_1\alpha + \ldots + b_m\alpha^m : m \in \mathbb{N}, b_i \in K\}$$

Example 5.2

We can write $\mathbb{Q}[i] = \{a + b_i : a, b \in \mathbb{Q}\}$. We do not need higher powers of i since they reduce back to $\mathbb{Q}$ using the relation $i^2 = -1$.

Example 5.3

$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. Again, we only need two terms since $(\sqrt{3})^2 = 3$.

Example 5.4

$\mathbb{Q}[\zeta_3]$, with $\zeta_3 = e^{\frac{2\pi i}{3}}$. This is $\{a + b\zeta_3 : a, b \in \mathbb{Q}\}$, since $\zeta_3^2 = -\zeta_3 - 1$.

As we saw from the above examples, we can often consider only combinations with a bounded number of terms. Thge following gives a sufficient condition for this:

Lemma 5.4

Let f be the minimal polynomial of α, and let $n = \deg f$. Then every element in $K[\alpha]$ can be uniquely written as

$$b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

where $b_i \in K$.

Proof. Uniqueness follows easily by subtracting two such presentations, since otherwise we have a polynomial of smaller degree than n vanishing on α.

To show existence, write $\gamma = g(\alpha)$ for $\gamma \in K[\alpha]$. Then running the division algorithm, we have

$$\gamma = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$$

and since $\deg(r) < \deg(f) = n$,

$$\gamma = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$ □

The following theorem allows us to tie together our study of polynomials and algebraic extensions:

Theorem 5.5

Let $\alpha \in L$ be algebraic over K, and f be the minimal polynomial of α. Then

$$K[\alpha] \cong {}^{K[x]}\!/_{(f)}$$

Proof. Consider the homomorphism $\phi : K[x] \to K[\alpha]$ defined by $\phi(f) = f(\alpha)$. The image is all of $K[\alpha]$ by definition, so ϕ is surjective. The kernel is those polynomials that vanish on α, but Proposition 5.1 showed that this is precisely (f). □

Corollary 5.6

For $\alpha \in L$ algebraic over K, $K[\alpha]$ is a field.

Proof. f is minimal, so it is irreducible, and thus ${}^{K[x]}\!/_{(f)} \cong K[\alpha]$ is a field. □

Definition 5.4

For a field extension $K \subseteq L$, we define $K(\alpha)$ to be the smallest subfield of L containing $\alpha \in L$ and K. We have just shown that when α is algebraic, $K[\alpha] = K(\alpha)$.

We observe that if $K \subseteq L$ is a field extension, then L is a vector space over K.

Definition 5.5

Let $K \subseteq L$ be a field extension. Then we define the **degree** of the extension L/K to be $[L : K] = \dim(L)$ as a K-vector space. We say that a field extension L/K is a **finite extension** if $[L : K] < \infty$.

Example 5.5

Since $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Similarly $[\mathbb{C} : \mathbb{R}] = 2$.

Notice that if f is the minimal polynomial of $\alpha \in L$, then $[K(\alpha) : K] = \deg f$. This is because we can uniquely write elements of $K[\alpha]$ as $b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$, so $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$. This also implies that $K(\alpha)$ is always a finite extension for algebraic $\alpha \in L$. Later we will see that every finite extension is of this form.

Proposition 5.7

Let L/K be a field extension, and let $\alpha \in L$. Then $[K(\alpha) : K]$ is finite if and only if α is algebraic over K.

Proof. ($\Longleftarrow$) As we just stated, $[K(\alpha) : K] = \deg(f) = n < \infty$.

($\Longrightarrow$) Let $[K(\alpha) : K] = n$. Then consider $1, \alpha, \ldots, \alpha^n$. These elements are linearly dependent so there exists a relation

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

with $a_i \in K$. This implies that α is algebraic over K. □

Proposition 5.8

Let $F \subseteq K \subseteq L$ be field extensions. Then $[L : F] = [L : K][K : F]$.

Proof. Pick a basis $\alpha_1, \ldots, \alpha_m \in L$ over K, and a basis $\beta_1, \ldots, \beta_n \in K$ over F. We want to show that the collection of $\alpha_i\beta_j$ is a basis for L over F.

To show it is a spanning set, pick $\alpha \in L$ and write

$$\alpha = \sum_i k_i\alpha_i$$

for $k_i \in K$. Then for each k_i we can write

$$k_i = \sum_j f_{ij}\beta_j$$

for $f_{ij} \in F$. Then

$$\alpha = \sum_{i,j} f_{ij}\alpha_i\beta_j$$

so the set spans L.

To show linear independence over F, suppose we have some linear relation

$$\sum_{i,j} f_{ij}\alpha_i\beta_j = 0$$

for $f_{i,j} \in F$. Then we can rewrite this as

$$\sum_i \left(\sum_j f_{i,j}\beta_j \right) \alpha_i = 0$$

By the linear independence of the α_i over K, each $\sum_j f_{i,j}\beta_j$ must be zero. But then by linear independence of the β_j over F, the $f_{i,j}$ must all be zero. So the $\alpha_i\beta_j$ are linearly independent over F. □

Example 5.6

Consider the field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2})$. We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, so $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$.

So far we have allowed field extensions to be arbitrary inclusions, and not necessarily produced by adjoining elements. However, the following theorem (whose proof we omit), shows that in the case of fields with characteristic zero, fields produced by adjoining elements account for all extensions.

Definition 5.6

Let $K \subseteq L$ be a field extension. Then $\alpha \in L$ is **primitive** if $L = K(\alpha)$.

Theorem 5.9: Primitive Element Theorem

Let L/K a finite field extension of fields of characteristic zero. Then L contains a primitive element.

Example 5.7

Consider $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

To see this, we of course have the inclusion

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

But we can check that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, and one can check that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ is $x^4 - 10x^2 + 1$, so $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. So $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2} + \sqrt{3})] = 1$ and thus $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

5.2 Splitting Fields

In this section we consider fields K such that $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$. More generally, we can consider algebraically closed fields instead of $\mathbb{C}$.

Definition 5.7

Let $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ and let $f \in K[x]$. By the fundamental theorem of algebra, we can write

$$f = (x - \alpha_1) \cdots (x - \alpha_n)$$

for $\alpha_i \in \mathbb{C}$. Then we define the **splitting field** of f over K to be

$$\mathrm{Split}_{\mathbb{C}/K}(f) \coloneqq K[\alpha_1, \ldots, \alpha_n] \subseteq \mathbb{C}$$

Proposition 5.10

A splitting field is indeed a field.

In particular, a splitting field is the smallest field extension of K in which f splits into linear factors. Thus we will also write $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$.

Definition 5.8

A **number field** is a field $K \supseteq \mathbb{Q}$ which is of finite degree.

Example 5.8

The splitting field of $x^2 + 1$ over $\mathbb{Q}$ is

$$\mathrm{Split}_{\mathbb{C}/\mathbb{Q}} = \mathbb{Q}(i, -i) = \mathbb{Q}(i)$$

Example 5.9

The splitting field of $x^4 - 2$ over $\mathbb{Q}$ can be seen by writing

$$x^4 - 2 = (x - \sqrt[4]{2})(x - \zeta_4\sqrt[4]{2})(x - \zeta_4^2\sqrt[4]{2})(x - \zeta_4^3\sqrt[4]{2})$$

Also, $\zeta_4 = i$. So the splitting field is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, i^2\sqrt[4]{2}, i^3\sqrt[4]{2})$. But some of these are redundant, and we can just write this as $\mathbb{Q}(\sqrt[4]{2}, i)$.

Example 5.10

The splitting field of $x^3 - 2$ over $\mathbb{Q}$ can be seen by writing

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$$

so

$$\mathrm{Split}_{\mathbb{C}/\mathbb{Q}}(x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

To calculate its degree, we have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$.

Now consider what happens when we adjoin ζ_3 to $\mathbb{Q}(\sqrt[3]{2})$. The polynomial $x^3 - 2$ is no longer irreducible since we have adjoined a root, so can be factored over $\mathbb{Q}(\sqrt[3]{2})$ into

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

But since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, and $\sqrt[3]{2}\zeta_3$ is a strictly complex root of the second factor, the second factor must be irreducible. Also, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Thus $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2})] = 2$ so $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.

So far we have defined a splitting field of a polynomial, as though splitting fields are objects associated with polynomials. But in fact, we will see that fields which are splitting fields posses an important property which is independent of the polynomial: every polynomial with one root in the splitting field splits completely into linear factors.

To see that this is true for f over $\mathrm{Split}_{\mathbb{C}/K}(f)$ is clear: by definition, the roots of f, which are $\alpha_1, \ldots, \alpha_n$, are all in $\mathrm{Split}_{\mathbb{C}/K}(f)$. But then this means that f factors into linear terms:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

Definition 5.9

For $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$, L is called a **splitting field** over K if it is a splitting field of some polynomial with coefficients in K.

Example 5.11

To see a demonstration of this property, consider $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \text{Split}_{\mathbb{C}/\mathbb{Q}}(x^3 - 2)$. Take $f = x^3 - 4$, which is an irreducible polynomial in $\mathbb{Q}[x]$ which has a root in L. This polynomial indeed splits, since

$$x^3 - 4 = (x - \sqrt[3]{4})(x - \sqrt[3]{4}\zeta_3)(x - \sqrt[3]{4}\zeta_3^2)$$

Theorem 5.11

Let $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ L be a splitting field over K. Let $g \in K[x]$ be irreducible. Then if one root of g is in K, then all roots of g are in L.

A corollary to this theorem allows us to finally decouple the notion of a splitting field from an arbitrary choice of polynomial:

Corollary 5.12

Let $K \subseteq L \subseteq \mathbb{C}$. Then L is a splitting field over K if and only if every irreducible polynomial in $K[x]$ with a root in L splits completely over L.

5.3 Automorphism Groups and Galois Groups

In this section we will consider the automorphisms of a field extension, which essentially tell us how many degrees of freedom or how "unique" the extension is.

Definition 5.10

A **field automorphism**, or just an automorphism, of a field K is a field isomorphism $\psi : K \to K$.

Example 5.12

Consider the map $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ defined by $\sigma(a + bi) = \overline{a + bi} = a - bi$. Complex conjugation is an automorphism of $\mathbb{C}$, and this operation is closed over $\mathbb{Q}(i)$, so it is a field automorphism of $\mathbb{Q}(i)$. Importantly, we also note that σ fixes the subfield $\mathbb{Q}$.

Definition 5.11

If $K \subseteq L$, we call $\sigma : L \to L$ a **K-automorphism** if it is an automorphism of L which fixes K.

Definition 5.12

The **Galois group** of a field extension K/L is the group $\mathrm{Gal}\left(L/K\right)$ of all K-automorphisms of L.

K-automorphisms generalize the notion of conjugation over the complex numbers, which is a $\mathbb{R}$-automorphism. As such, we adopt analogous terminology.

Definition 5.13

Let $K \subseteq L \subseteq \mathbb{C}$ and let $\alpha \in L$. Then we say that $\beta \in L$ is **conjugate** to α if there exists a K-automorphism $\sigma : L \to L$ such that $\sigma(\alpha) = \beta$.

This now allows us to define the norm of an element with respect to a field extension. Roughly speaking, the norm of α is the product of all conjugates of α.

Definition 5.14

For $\alpha \in L$ a field and $L \subseteq K$, we define the **norm** of α over K to be

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}\left(L/K\right)} \sigma(\alpha)$$

We will see later that that $N_{L/K}(\alpha) \in K$, and that $N_{L/K}$ is multiplicative.

In particular, $N_{L/K}(k) = k$ for $k \in K$.

The important property of Galois groups is that

$$\left|\mathrm{Gal}\left(L/K\right)\right| \leq [L : K] \qquad (*)$$

Before proving this, we will first use this property to calculate some Galois groups.

Example 5.13

For $\mathbb{R} \subseteq \mathbb{C}$, $\mathrm{Gal}\left(\mathbb{R}/\mathbb{C}\right) = \{\mathrm{id}, z \mapsto \overline{z}\}$ (there are no more since $[\mathbb{C} : \mathbb{R}] = 2$). This induces the norm $N_{\mathbb{C}/\mathbb{R}}(a + bi) = \mathrm{id}(a + bi) \cdot \overline{a + bi} = a^2 + b^2$ which coincides with the typical norm.

Example 5.14

For $\mathbb{Q} \subseteq \mathbb{Q}(i)$, $\mathrm{Gal}\left(\mathbb{Q}(i)/\mathbb{Q}\right) = \{\mathrm{id}, z \mapsto \overline{z}\}$.

Example 5.15

For $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) = \{\mathrm{id}, a + b\sqrt{2} \mapsto a - b\sqrt{2}\}$, which induces the norm $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$.

Example 5.16

For $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3)$, $\mathrm{Gal}\left(\mathbb{Q}(\zeta_3)/\mathbb{Q}\right) = \{\mathrm{id}, a + b\zeta_3 \mapsto a + b\zeta_3^2\}$.

To prove $(*)$, we need the important fact that the conjugations admitted by the Galois group map roots of polynomials to roots:

Lemma 5.13

Let $K \subseteq L$ be a field extension and $\alpha \in L$. Let $p \in K[x]$ be such that $p(\alpha) = 0$. Then for any $\sigma \in \mathrm{Gal}\left(L/K\right)$, $p(\sigma(a)) = 0$.

Proof. Write $p(x) = b_0 + b_1 x + \ldots + b_m x^m$ with $b_i \in K$. Then σ fixes b_i, so

$$0 = \sigma(p(\alpha)) = \sigma(b_0 + b_1\alpha + \ldots + b_m\alpha^m) = b_0 + b_1\sigma(\alpha) + \ldots + b_m\sigma(\alpha)^m = p(\sigma(\alpha)) \qquad \square$$

Example 5.17

Let $\sigma : \mathbb{C} \to \mathbb{C}$ be the conjugation operator, and taking $p(x) = x^8 - 1 \in \mathbb{R}[x]$, $\alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ is a root, and

$$p(\sigma(\alpha)) = \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)^8 - 1 = 0$$

Corollary 5.14

For $K \subseteq L$ and any $\alpha \in L$ algebraic over K with minimal polynomial $f \in K[x]$, and $\sigma \in \mathrm{Gal}\left(L/K\right)$, the minimal polynomial of $\sigma(\alpha)$ is also f.

Proof. Let g be the minimal polynomial of $\sigma(\alpha)$. Then $f(\alpha) = f(\sigma(\alpha)) = 0$, so $g|f$. By applying the same to σ^{-1}, $f|g$, so $f = g$. $\square$

We now need to investigate how to compute the Galois group. Assuming we are working over a field of characteristic zero, this is simplified by the Primitive Element Theorem, which tells us that field extensions have primitive elements.

Lemma 5.15

Let $L = K(\alpha)$ for some $\alpha \in L$. Let $\sigma \in \mathrm{Gal}\left(L/K\right)$. Then σ is uniquely determined by $\sigma(\alpha)$.

Proof. Let $\sigma(\alpha) = \beta \in L$. Any element of L may be written as

$$b_0 + b_1\alpha + \ldots + b_m\alpha^m$$

for $b_i \in K$. Since σ is a K-automorphism,

$$\sigma(b_0 + b_1\alpha + \ldots + b_m\alpha^m) = b_0 + b_1\beta + \ldots + b_m\beta^m$$ □

Lemma 5.16

Let $L = K(\alpha)$ and let $f \in K[x]$ be the minimal polynomial of α over K. Let $\beta \in L$ be another root of f. Then there exists a unique $\sigma : L \to L$ such that $\sigma(\alpha) = \beta$. We denote this by $\sigma_{\alpha\to\beta}$.

Proof. Uniqueness follows immediately by Lemma 5.15.

f is irreducible over K, since it is a minimal polynomial. Thus f is also the minimal polynomial of β over K. Thus $[K(\alpha) : K] = [K(\beta) : K] = \deg f$. Since $\beta \in L$, $K \subseteq K(\beta) \subseteq L = K(\alpha)$, so it follows that $K(\beta) = K(\alpha)$.

We want to find an isomorphism between $K(\beta), K(\alpha)$ that sends α to β. This is straightforward, since we know there exist

$$\phi : K[x]/(f) \xrightarrow{\cong} K(\alpha), \overline{x} \mapsto \alpha$$
$$\psi : K[x]/(f) \xrightarrow{\cong} K(\beta), \overline{x} \mapsto \beta$$

It follows that $\psi \circ \phi^{-1}$ is an isomorphism $K(\alpha) \xrightarrow{\cong} K(\beta)$ such that $\psi \circ \phi^{-1}(\alpha) = \beta$. It is moreover a K-automorphism since both ϕ, ψ are. □

The above lemmas allow us to calculate the Galois group of an arbitrary field extension in $\mathbb{C}$. Indeed, for $\sigma : L \to L$ a K-automorphism and $L = K(\alpha)$, $\beta = \sigma(\alpha)$ is conjugate to α and they have the same minimal polynomial. So we must have $\sigma = \sigma_{\alpha\to\beta}$.

Corollary 5.17

Let $K \subseteq L$ be a field extension with $L = K(\alpha)$. Let f be the minimal polynomial of α over K, and let $\alpha_1, \ldots, \alpha_k$ be the roots of f which are contained in L. Then

$$\mathrm{Gal}\left(L/K\right) = \{\sigma_{\alpha\to\alpha_1}, \ldots, \sigma_{\alpha\to\alpha_k}\}$$

Corollary 5.18

Let $K \subseteq L \subseteq \mathbb{C}$ be a finite field extension. Then

$$\left|\mathrm{Gal}\left(L/K\right)\right| \leq [L : K]$$

Proof. We know $L = K(\alpha)$ for some $\alpha \in L$. By the previous corollary, $\left|\mathrm{Gal}\left(L/K\right)\right| = k$, where k is the number of roots in L of the minimal polynomial of α over K. $k \leq n = \deg f$, and $[L : K] = \deg f$, so we are done. □

In particular, equality holds if and only if the minimal polynomial for α over K splits completely over L.

Example 5.18

Let ζ_3 be the third root of unity, and let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_3)$. Then $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ since $\zeta_3^2 + \zeta_3 + 1 = 0$ is the minimal polynomial. We can factor this over L as

$$x^2 + x + 1 = (x - \zeta_3)(x - \zeta_3^2)$$

so this splits over L and thus

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_3)/\mathbb{Q}\right) = \left\{\sigma_{\zeta_3 \to \zeta_3}, \sigma_{\zeta_3 \to \zeta_3^2}\right\} = \{\mathrm{id}, \sigma\}$$

Notice also that $\sigma^2 = \mathrm{id}$, so $\mathrm{Gal}\left(\mathbb{Q}(\zeta_3)/\mathbb{Q}\right)$ admits a group structure.

Example 5.19

Consider ζ_5. We know from that optional class that since 5 is prime, the minimal polynomial is given by

$$\frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4 = \Phi_5(x)$$

We can decompose this over $\mathbb{Q}(\zeta_5)$ as

$$\Phi_5(x) = (x - \zeta_5)(x - \zeta_5^2)(x - \zeta_5^3)(x - \zeta_5^4)$$

Thus $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$, and

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) = \left\{\sigma_{\zeta_5 \to \zeta_5}, \sigma_{\zeta_5 \to \zeta_5^2}, \sigma_{\zeta_5 \to \zeta_5^3}, \sigma_{\zeta_5 \to \zeta_5^4}\right\} = \{\sigma_1 = \mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$$

Thus we know the Galois group has order 4. Thus it is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To show that it is in fact isomorphic to $\mathbb{Z}/4\mathbb{Z}$, we show that

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/5\mathbb{Z}\right)^\times \cong \mathbb{Z}/4\mathbb{Z}$$

To see this, define the mapping

$$\overline{i} \mapsto \sigma_i = \sigma_{\zeta_5 \to \zeta_5^i}$$

This is a group homomorphism since

$$\overline{ij} = \overline{ij} \mapsto \sigma_{ij}$$

We want to show that $\sigma_{ij} = \sigma_i \circ \sigma_j$. Indeed, $(\zeta_5^j)^i = \zeta_5^{ij}$, and

$$\sigma_i(\sigma_j(\zeta_5)) = \sigma_i(\zeta_5^j) = \sigma_i(\zeta_5)^j = (\zeta_5^j)^i = \zeta_5^{ij} = \sigma_{ij}(\zeta_5)$$

Example 5.20

Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The degree of the extension is 4. We can explicitly calculate that

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) \big/ \mathbb{Q}\right) = \{\mathrm{id}, \tau, \rho, \tau \circ \rho\}$$

where τ, ρ are conjugation along $\sqrt{2}, \sqrt{3}$, respectively. Each conjugation is of order 2 so this group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Definition 5.15

Let $K \subseteq L$ be a finite field extension. We say that this is a **Galois extension** if

$$\mathrm{Gal}\left(L/K\right) = [L : K]$$

The above examples were all Galois extensions. This does not always hold, however.

Example 5.21

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial is $x^3 - 2$, but the other roots of this polynomial are $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$, which are not in $\mathbb{Q}(\sqrt[3]{2})$. Thus this extension is not Galois.

It follows from the above work that we have simply shown that splitting fields enjoy a group structure:

Corollary 5.19

$K \subseteq L$ is a Galois extension if and only if L is a splitting field over K.

Proof. Pick a primitive element α for the extension. Let f be its minimal polynomial. Then

$\left|\mathrm{Gal}\left(L/K\right)\right|$ is the number of roots of f in L, and $[L:K] = \deg f$. So f splits over K if and only if $\left|\mathrm{Gal}\left(L/K\right)\right| = [L:K]$. □

To find the minimal polynomial of arbitrary $\alpha \in L$ over K, we have two approaches. First, we can consider $1, \alpha, \ldots, \alpha^n$, where $n = [L:K]$. These are linearly dependent, so we get a linear relation. Alternatively, we can use the following lemma:

Lemma: Minimal Polynomial Lemma

Let $K \subseteq L$ be a Galois extension and $\alpha \in L$. Let $\alpha_1 = \alpha, \ldots, \alpha_k$ be the orbit of α under $\mathrm{Gal}\left(L/K\right)$. Then the coefficients of

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_k)$$

are contained in K, and moreover p is the minimal polynomial of α.

In other words, the minimal polynomial is calculated by considering linear factors using the conjugates. The fact that the extension is Galois ensures this is actually the minimal polynomial.

Example 5.22

For $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the minimal polynomial is given by

$$p(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})) = x^4-10x^2+1$$

To prove the minimal polynomial lemma, we will take a detour into some other important facts in Galois theory.

5.4 Fixed Fields

Given a field extension L/K, K is fixed under $\mathrm{Gal}\left(L/K\right)$ by definition. The question we investigate here is whether the opposite inclusino holds; that is, if $\alpha \in L$ is fixed by all $\sigma \in \mathrm{Gal}\left(L/K\right)$, is it necessarily the case that $\alpha \in K$?

Example 5.23

In the case of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the answer is yes. If $\alpha = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$, then α is fixed if and only if $a + b\sqrt{2} = a - b\sqrt{2}$, or equivalently if and only if $b = 0$. So $\alpha \in \mathbb{Q}$.

Definition 5.16

Let $H \leqslant \text{Gal}\left(L/K\right)$ and let $H \curvearrowright L$. Then we define the **fixed subfield** of L under H to be

$$L^H := \{\alpha \in L : \forall \sigma \in H, \sigma(\alpha) = \alpha\}$$

Example 5.24

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and let $H = \{\text{id}, \tau\}$, where $\tau(\sqrt{3}) = \sqrt{3}, \tau(\sqrt{2}) = -\sqrt{2}$. Then

$$\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

Thus the fixed field is precisely those elements for which $b = d = 0$. So

$$L^H = \mathbb{Q}(\sqrt{3})$$

Lemma 5.20: Minimal Polynomial Lemma for Fixed Fields

Let L/K be Galois and let $H \leqslant \text{Gal}\left(L/K\right)$. Let $F = L^H$, so that $K \subseteq F \subseteq L$. Let $\alpha \in L$ and let $O(\alpha) = \{\alpha_1, \ldots, \alpha_k\}$ be the orbit of α under the action $H \curvearrowright L$. Then

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_k)$$

is contained in $F[x]$ and is the minimal polynomial of α over F.

Proof. We first show that $p \in F[x]$. By Vieta's formulas, the coefficients of $(x - \alpha_1) \cdots (x - \alpha_k)$ are symmetric polynomials in $\alpha_1, \ldots, \alpha_k$. Also, for $\sigma \in H$, $\sigma(\alpha_1), \ldots, \sigma(\alpha_k)$ is a permutation of $\alpha_1, \ldots, \alpha_k$, so H does not change the symmetric polynomials. Thus the coefficients of p are fixed by H, so $p \in L^H[x] = F[x]$.

Let $q \in F[x]$ be the minimal polynomial of α. Then $q(\alpha_1) = \ldots = q(\alpha_k) = 0$, since elements of H must map roots to roots for polynomials in $F[x]$ (this is essentially the same as the proof of the more general case). Then it follows that $p|q$, so $p = q$. Thus p is the minmal polynomial for α over F. □

In the case where we take $H = \text{Gal}\left(L/K\right)$, the minimal polynomial lemma for fixed fields tells us that the minimal polynomial of α over $F = L^{\text{Gal}(L/K)}$ is $(x - \alpha_1) \cdots (x - \alpha_k)$ where the α_i are all the conjugates of α under $\text{Gal}\left(L/K\right)$. Importantly, our work will show that $L^{\text{Gal}(L/K)} = K$, so that this is the minimal polynomial of α over K. Thus this lemma, in combination with the proof of the statement $L^{\text{Gal}(L/K)} = K$, will prove the minimal polynomial lemma.

Theorem 5.21: Fixed Field Theorem

Let L/K be Galois and let $H \leqslant \mathrm{Gal}\left(L/K\right)$. Then $[L : L^H] = |H|$.

Proof. Denote $F = L^H$, so that $K \subseteq F \subseteq L$. Then let $\alpha \in L$ be a primitive element, such that $L = F(\alpha)$. Let $H \curvearrowright L$.

We claim that $\mathrm{Stab}(\alpha) = \{\mathrm{id}\}$. Indeed, suppose $\sigma \in H$ is such that $\sigma(\alpha) = \alpha$. σ fixes F by definition. So $\sigma \in \mathrm{Gal}\left(L/F\right)$, and σ is determined by the value of $\sigma(\alpha)$, so $\sigma = \mathrm{id}$.

Then by the orbit stabilizer theorem, $|O(\alpha)| = |H|$, where the orbit is taken under $H \curvearrowright L$. Let $f \in F[x]$ be the minmial polynomial for α over F. By the minimal polynomial lemma for fixed fields, f has degree $|O(\alpha)| = |H|$. It follows that $[L : L^H] = \deg f = |H|$. □

Corollary 5.22

If L/K is Galois, then $L^{\mathrm{Gal}(L/K)} = K$.

Proof. We have the following:

$$K \xrightarrow{\quad} L^{\mathrm{Gal}(L/K)} \xrightarrow[\left[L:L^{\mathrm{Gal}(L/K)}\right]]{} L \qquad \overset{[L:K]}{\frown}$$

By the fixed field theorem, $\left[L : L^{\mathrm{Gal}(L/K)}\right] = \left|\mathrm{Gal}\left(L/K\right)\right|$. Since the extension is Galois, $\left|\mathrm{Gal}\left(L/K\right)\right| = [L : K]$. So we must have

$$K \xrightarrow[1]{} L^{\mathrm{Gal}(L/K)} \xrightarrow[[L:K]]{} L \qquad \overset{[L:K]}{\frown}$$

Thus it follows that $L^{\mathrm{Gal}(L/K)} = K$. □

Lemma 5.23: Minimal Polynomial Lemma

Let L/K be Galois and let $\alpha \in L$. Let $\alpha_1, \ldots, \alpha_k$ be the orbit of α under $\mathrm{Gal}\left(L/K\right)$. Then the minimal polynomial for α over K is

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_k)$$

Proof. As we observed previously, this is a consequence of the minimal polynomial lemma and Corollary 5.22. □

We can also present a stronger version of the fixed field theorem that will lead us to the fundamental theorem of Galois theory.

Proposition 5.24

Let $K \subseteq F \subseteq L$ and let L/K be Galois. Then L/F is Galois.

Proof. Homework. □

Theorem 5.25

Let L/K be Galois. Let $H \subseteq \mathrm{Gal}\left(L/K\right)$. Let $F = L^H$, so that $K \subseteq F \subseteq L$. Then $\mathrm{Gal}\left(L/F\right) = H$.

Proof. $H \subseteq \mathrm{Gal}\left(L/L^H\right)$ essentially by definition, since the elements of H are automorphisms of L which fix L^H.

By the proposition above, L/F is Galois, so $\left|\mathrm{Gal}\left(L/F\right)\right| = [L : F] = [L : L^H] = |H|$. So $H = \mathrm{Gal}\left(L/F\right)$. □

The next theorem may be thought of as a reversed version of the fixed field theorem.

Theorem 5.26

Let $K \subseteq F \subseteq L$ be such that L/F is Galois. Then $F = L^{\mathrm{Gal}(L/F)}$.

Proof. We simply apply Corollary 5.22. □

The intuition for this theorem is that every intermediate field may be written as the fixed field of a subgroup of $\mathrm{Gal}\left(L/K\right)$.

Theorem 5.27: Fundamental Theorem of Galois Theory

Let L/K be Galois and denote $G = \mathrm{Gal}\left(L/K\right)$. Then there exists a one-to-one ocrrespondence between subgroups of G and intermediate field extensions $K \subseteq F \subseteq L$.

Indeed, the above correspondence is given by

$$H \longrightarrow L^H$$

$$\mathrm{Gal}\left(L/F\right) \longleftarrow F$$

Proof. Theorem 5.25 tells us that for $H \leqslant G$, $H = \mathrm{Gal}\left(L/L^H\right)$. For $K \subseteq F \subseteq L$, Theorem 5.26 says that $F = L^{\mathrm{Gal}(L/F)}$, and $\mathrm{Gal}\left(L/F\right) \leqslant \mathrm{Gal}\left(L/K\right)$. □

In pacticular, note that for $\{e\} \leqslant H \leqslant G$ we have

$$\begin{array}{ccccc} \{e\} & \longrightarrow & L & = & L^{\{e\}} \\ \vdots & & \vdots & & \\ H & \longrightarrow & L^H & & \\ \vdots & & \vdots & & \\ G & \longrightarrow & K & = & L^G \end{array}$$

In the other direction, for $K \subseteq F \subseteq L$ we have

$$\begin{array}{ccccc} \{e\} & = & \mathrm{Gal}\left(L/L\right) & \longleftarrow & L \\ & & \vdots & & \vdots \\ & & \mathrm{Gal}\left(L/F\right) & \longleftarrow & F \\ & & \vdots & & \vdots \\ & & \mathrm{Gal}\left(L/K\right) & \longleftarrow & K \end{array}$$

We know that for an intermediate extension $K \subseteq F \subseteq L$ where L/K is Galois, L/F is always Galois. It is not necessarily the case that F/K is Galois. However, this correspondence allows us to cast the condition in terms of the group structure of $\mathrm{Gal}\left(L/K\right)$.

Theorem 5.28

Let $K \subseteq F \subseteq L$ and let L/K be Galois. Then F/K is Galois if and only if $\mathrm{Gal}\left(L/F\right) \trianglelefteq \mathrm{Gal}\left(L/K\right)$.

Example 5.25

Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) = \{\mathrm{id}, \rho, \tau, \rho\tau\}$, where ρ maps $\sqrt{2} \mapsto -\sqrt{2}$ and τ maps $\sqrt{3} \mapsto -\sqrt{3}$. There are three nontrivial proper subgroups, which are $\{\mathrm{id}, \rho\}, \{\mathrm{id}, \tau\}, \{\mathrm{id}, \rho\tau\}$. All are normal since $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is

abelian. These correspond to the subextensions

$$\{\mathrm{id}, \rho\} \sim \mathbb{Q}(\sqrt{3})$$
$$\{\mathrm{id}, \tau\} \sim \mathbb{Q}(\sqrt{2})$$
$$\{\mathrm{id}, \rho\tau\} \sim \mathbb{Q}(\sqrt{6})$$

Then the fundamental theorem of Galois theory tells us that these are the only intermediate field extensions.

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 $G \circlearrowright V$ (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 $\varphi = \lambda \operatorname{id}$.

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 approprate $v \in V$. 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. □

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

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

Appendix B

Special Topics in Group Theory

B.1 Free Groups

Definition B.1

A **free group** on a set of n distinct symbols is the set of finite strings which are formed by concatenation of the symbols, together with their inverses. The group operation is concatenation. If there are n generators, then this set may be denoted as the **free product** of cyclic groups $\mathbb{Z} * \mathbb{Z} * \ldots * \mathbb{Z}$.

Since the elements of any group may be written as strings which are their algebraic representations in terms of the generators, the elements of every group may be represented as elements of the free groups. However, in this case, we need to use the algebraic relations which tells us which strings are equal algebraically – that is, we need to know what cancellation manipulations are valid. In this way, each group (say, finitely generated for now) is a quotient of the free group on its generators.

B.2 Connections with Algebraic Topology

Example B.1

Let X be a topological space and let $x \in X$ be a point. The **fundamental group** of X at x is the set $\pi_1(X, x)$, which is the set of all loops that start and end at x, identified up to homotopy. The group operation is concatenation.

Example B.2

$\pi_1(S^1)$ is composed of the set of all n counterclockwise wraps for $n \in \mathbb{Z}$, so $\pi_1(S^1) \cong \mathbb{Z}$. Similarly, $\pi_1(\mathbb{R}^2 \backslash \{0\}) \cong \mathbb{Z}$. In contrast, π_1 of the torus is $\mathbb{Z} \times \mathbb{Z}$, since wraps around the long ring and the inner ring commute with each other. Lastly, $\pi_1(\mathbb{R}^2 \setminus \{0, 1\}) \cong$

$\mathbb{Z} * \mathbb{Z}$, since loops around 0 and 1 do not commute or cancel in any way.

Definition B.2

An (associative) **division algebra**, also called a **division ring** or **skew field**, is a field without the assumption that multiplication is commutative (however, left and right inverses both exist).

The following is a theorem due to Frobenius:

Theorem B.1

The only associative division algebras of finite dimension over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$, and $\mathbb{H}$, where $\mathbb{H}$ is the quaternions.

Note that the dimensions of $\mathbb{R}, \mathbb{C}, \mathbb{H}$ are 1, 2, and 4. Let us investigate why this is. We can use the multiplicative structures of the algebras to construct a group structure on the unit sphere. For instance, $\mathbb{C} \cong \mathbb{R}^2 \supseteq S^1$, so $\mathbb{C}$ induces a group structure on S^1, which is the group of rotations. Similarly, $\mathbb{Q} \cong R^4 \supseteq S_3$, and we showed in homework that the group structure on S^3 is the quaternions. (Note in both cases that we quotient out by any scaling factors). In general, an associative division algebra K of dimension n over $\mathbb{R}$ induces a group structure on S^{n-1}. Moreover, these group structures are smooth, meaning the group operation is differentiable (that is, the groups induced are **Lie groups**). However, methods of topology show that the only spheres which admit such a group structure are S^0, S^1, S^3. This shows that the only possible dimensions are 1, 2, and 4.

Definitions