Notes for Math 412

Albon Wu

January 27, 2024

Contents

0 Introduction

Rings, groups, fields, and some other topics.

Professor: David Stapleton.

Textbook: *Abstract Algebra: An Introduction* by Hungerford.

1 Arithmetic in $\mathbb{Z}$

1.1 The Division Algorithm

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ is the set of integers. In this course, we will deal with a few results concerning division in $\mathbb{Z}$. The first is:

> **Theorem 1.1.1** (Division algorithm)**.** *Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique q, r such that*
>
> $$n = qd + r \quad \textit{and} \quad 0 \leq r < d.$$

Proof. We will first show the existence of q, r. Define $S := \{n - dq | q \in \mathbb{Z}, n - dq \geq 0\}$. We claim that S has a minimal element. To show this, recall the well-ordering axiom:

> *Every non-empty set of non-negative integers contains a smallest element.*

By definition, S is a set of non-negative integers, and clearly it is non-empty since $n = n - 0d \in S$. So S has a minimal element; denote it r.

We claim that $r < d$. Suppose toward a contradiction that $r \geq d$. Then

$$0 \leq r - d = n - d(q + 1) \in S.$$

But $r - d < r$, contradicting the minimality of r. So $r < d$. This r, along with the q that yields it, satisfies

$$n = qd + r \quad \text{and} \quad 0 \leq r < d,$$

as desired.

Now we will show that q, r are unique. Take $n, d \in \mathbb{Z}$. Let $n = qd + r = q'd + r'$ for $q, q', r, r' \in \mathbb{Z}$ and $0 \leq r, r' < d$. We can write

$$\begin{aligned} qd - q'd + r - r' &= 0 \\ \implies -d(q - q') &= r - r'. \end{aligned} \tag{$*$}$$

So $d|(r - r')$. Now, using the definition of r, r', we have

$$\begin{aligned} 0 \leq r < d \\ 0 \leq r' < d. \end{aligned}$$

Multiplying the second inequality by -1 gives $-d < -r' \leq 0$. We add this to the first inequality to obtain $-d < r - r' < d$. But since $d|(r - r')$, we conclude $r - r' = 0 \implies r = r'$.

Now we substitute $(*)$ into $-d < r - r' < d$, which gives

$$\begin{aligned} -d < -d(q - q') < d \\ -1 < q - q' < 1. \end{aligned}$$

Since $q - q'$ is an integer, we also conclude $q - q' = 0 \implies q = q'$. Thus, q and r are unique. This completes the proof. □

The Division Algorithm implies the following terminology.

> **Definition 1.1.1.** Take $a, b \in \mathbb{Z}$. *a divides b* if $b = aq$ for some $q \in \mathbb{Z}$. We can write this as $a|b$.

1.2 The Euclidean Algorithm

Definition 1.2.1. Let $a, b \in \mathbb{Z}$. The **greatest common divisor** or **GCD** of a and b, denoted (a, b), is the largest integer d such that $d|a$ and $d|b$.

The Euclidean algorithm is an efficient way to compute the GCD of two integers.

Theorem 1.2.1 (Euclidean algorithm)**.** *For $a, b \in \mathbb{Z}$, given the following sequence*

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

where each equation is an application of the division algorithm, the final nonzero remainder is (a, b).

We will show the following result to provide intuition into the correctness of the Euclidean algorithm.

Claim. Apply the division algorithm on $a, b \in \mathbb{Z}$ to obtain $a = bq + r$. Then $(a, b) = (b, r)$.

Proof. If d is a common divisor of a and b, then $a = dn$ and $b = dm$ for $m, n \in \mathbb{Z}$. Then $r = dn - dmq$, so $d|r$. So d is also a common divisor of b and r. This implies $(a, b) \leq (b, r)$ since (a, b) is also a common divisor of b and r, but it need not be the largest.

Conversely, if d is a common divisor of b and r, then we can simply factor it out of the RHS of the division algorithm to obtain an expression for a as the product of d and an integer. So $d|a$, and by an analogous argument as above, $(b, r) \leq (a, b)$.

So $(a, b) = (b, r)$. □

This suggests a general strategy for simplifying the computation of (a, b): find the GCD of b and the remainder from division of a by b, and repeat.

Example 1.2.1. To find $(528, 148)$, we can perform the following:

$$\begin{aligned} 528 &= 148 \cdot 3 + 80 \\ 148 &= 80 \cdot 1 + 68 \\ 80 &= 68 \cdot 1 + 12 \\ 68 &= 12 \cdot 5 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2 + 0. \end{aligned}$$

The last nonzero remainder is 4, so $(528, 148) = 4$.

Theorem 1.2.2 (Bezout's identity)**.** *For $a, b \in \mathbb{Z}$ such that a and b are not both zero, there exist $r, s \in \mathbb{Z}$ such that $ra + sb = (a, b)$. r, s are sometimes called **Bezout coefficients**.*

Proof. Consider $S := \{am + bn | m, n \in \mathbb{Z}\}$, the set of all linear combinations of a and b. Since $a^2 + b^2 \in S$ and at least one of a and b is nonzero, S contains a non-empty subset of positive integers. Therefore, it has a minimal positive element (call it t) by the Well-Ordering Axiom. We claim that $(a, b) = t$.

Since $t \in S$, we can write $t = am + bn$ for $m, n \in \mathbb{Z}$. To prove our claim, we must first show $t|a$ and $t|b$. Applying the division algorithm on a and t, we obtain $a = qt + r$, where q and r have the usual properties. Then

$$\begin{aligned} r &= a - qt \\ r &= a - q(am + bn) \\ r &= a(1 - qm) + b(-qn) \end{aligned}$$

So r is a linear combination of a and b; hence, $r \in S$. But since $r < t$ and t is the minimal positive element of S, it must be that $r \leq 0$. By definition, however, $r \geq 0$. So $r = 0$ and $t|a$. We can show $t|b$ analogously.

Now we will show t is the *greatest* common factor of a and b. Take $c \in \mathbb{Z}$ such that $c|a$ and $c|b$. Then $a = cx$ and $b = cy$ for $x, y \in \mathbb{Z}$. We can thus write $t = cxm + cyn = c(xm + yn)$, which gives $c|t$. So $c \leq |t|$, implying $c \leq t$ since $t > 0$. This completes the proof. □

> **Remark.** This proof shows a result even stronger than the original statement of the theorem. Not only is (a, b) a linear combination of a and b, but it is also the *smallest* linear combination.

It is a common problem, particularly in cryptography, to find the Bezout coefficients given a, b. We can achieve this by "working backward" using the Euclidean algorithm.

> **Example 1.2.2.** We want to find m, n such that $582m + 148n = (528, 148)$.
>
> The first step is to perform the Euclidean algorithm, as in Example 1.2.1. Recall the second-to-last equation: $12 = 8 \cdot 1 + 4$. Since $(528, 148) = 4$, we can isolate 4 to obtain $12 - 8 \cdot 1 = 4$.
>
> Now recall the equation above: $68 = 12 \cdot 5 + 8$. We isolate 8 to obtain $68 - 12 \cdot 5 = 8$ and substitute it into the previous equation: $12 - (68 - 12 \cdot 5) \cdot 1 = 12 \cdot 6 - 68 = 4$.
>
> What's the motivation for this substitution? Recall that
>
> $$(582, 148) = (148, 80) = (80, 68) = (68, 12) = (12, 4).$$
>
> In each step of the Euclidean algorithm, we reduce $(582, 148)$ into GCD expressions containing increasingly smaller numbers.
>
> In this example, we work our way upward, expressing 4 in terms of increasingly larger numbers and their Bezout coefficients. We started with $12 - 8 \cdot 1 = 4$, which is in fact $(12, 8) = 4$ expressed in terms of its Bezout coefficients. When we substitute for 8, we obtain a new expression in terms of 68 and 12 of the same form.
>
> The idea is to work our way up the Euclidean algorithm chain of equations until we get to an expression in terms of 528 and 148. Three substitutions later, we arrive at $528 \cdot (-7) + 148 \cdot 25 = 4$.

1.3 The Fundamental Theorem of Arithmetic

Definition 1.3.1. Take nonzero $p \in \mathbb{Z}$ such that $p \neq \pm 1$. We say p is *prime* if its only divisors are ± 1 and $\pm p$.

Theorem 1.3.1 (The Fundamental Theorem of Arithmetic)**.** *A nonzero $n \in \mathbb{Z}$, where $n \neq \pm 1$, can be written as a product of primes. If $p_1 \cdots p_s = q_1 \cdots q_t$ are two prime factorizations of n, then $s = t$ and the $\{q_j\}$ can be reordered such that $q_i = \pm p_i$ for all i.*

To prove this, we start by showing the following result about primes:

Theorem 1.3.2. *For nonzero $a \in \mathbb{Z}$ such that $a \neq \pm 1$, p is prime iff it has the following property:*

$$\text{if } p|bc, \text{ then } p|b \text{ or } p|c.$$

Proof. Suppose p is prime and divides bc. Then consider (p, b). By definition, $(p, b)|p$, but since p is prime, we have either $(p, b) = 1$ or $(p, b) = p$ (negative if p is negative). In the second case, $p|b$. For the first case, we claim that $(p, b) = 1 \implies p|c$.

To show this, we apply Bezout given that $(p, b) = 1$ to get $pu + bv = 1$ for $u, v \in \mathbb{Z}$. Multiplying both sides by c, we get $cpu + cbv = c$. But since $p|bc$, we can write $bc = pk$ for $k \in \mathbb{Z}$.

Now we substitute this expression of bc into the equation found previously, which gives $cpu + pkv = p(cu + kv) = c$. So $p|c$, as desired.

Therefore, either $p|b$ or $p|c$, completing the proof. □

It is fairly straightforward to generalize the above result:

Corollary 1.3.1. *If $p \in \mathbb{Z}$ is prime and $p|(a_1 \cdots a_n)$, where $a_i \in \mathbb{Z}$ for all i, then $p|a_i$ for some i.*

Proof. We induce on n. In the base case $n = 1$, we trivially have $p|a_1 \implies p|a_1$. Now suppose the result holds for $n = k$. We wish to show that if p is prime and $p|(a_1 \cdots a_{k+1})$, then $p|a_i$ for some i. Suppose the antecedent is true. By Theorem 1.3.1, we have that either $p|a_1 \cdots a_k$ or $p|a_{k+1}$.

In the second case, we are done. In the first, the result follows from the inductive hypothesis. □

Now we can start showing the components of FTA. First, we show the existence of prime factorizations.

Lemma 1.3.1. Every $n \in \mathbb{Z}$ except $0, \pm 1$ is a product of primes.

Proof. We need only show this for positive n because we can obtain a prime factorization of $-n$ by negating any prime in the factorization of n.

Let S be the set of positive n that do not have prime factorizations, and denote its smallest element by m. Note that m is not prime, since otherwise it would have the prime factorization m. So it has positive divisors other than 1 and itself.

Let $m = ab$ where $1 < a, b < m$. Then $a, b \notin S$ because m is minimal. This implies that a and b have prime factorizations; that is, $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$. We can then write $m = p_1 \cdots p_2 q_1 \cdots q_s$, a prime factorization of m. So $m \notin S$ and $m \in S$, a contradiction. Therefore, S is empty. □

Lemma 1.3.2. Prime factorizations are unique up to order and sign.

Proof. Suppose that n has two prime factorizations: $p_1 \cdots p_s$ and $q_1 \cdots q_t$. Then, because $p_1 | n$, we know p_1 divides one of the q_i by Corollary 1.3.1. Since q_i is prime and $p_1 \neq \pm 1$, $p_1 = \pm q_i$.

Now let n be the smallest positive integer with two prime factorizations that differ in more than order and sign: $p_1 \cdot p_s$ and $q_r \cdot q_t$. We can use the above property to write

$$n/p_1 = p_2 \cdots p_s = q_1 \cdots \hat{q}_i \cdots q_t.$$

We renumber the $\{q_i\}$ to obtain $q_2 \cdots q_t$. Since $n/p_1 < n$, there exists a reordering of $\{q_i\}$ such that $q_i = \pm p_i$ for all $i > 1$. But we have previously shown this property for $i = 1$. In sum, this implies that there exists a reordering of the original prime factorizations such that $q_i = \pm p_i$ for all $i \geq 1$.

This contradicts the assumption on n, completing the proof. □

We finally return to the titular theorem of this section.

Theorem 1.3.1 (The Fundamental Theorem of Arithmetic)**.** *A nonzero $n \in \mathbb{Z}$, where $n \neq \pm 1$, can be written as a product of primes. If $p_1 \cdots p_s = q_1 \cdots q_t$ are two prime factorizations of n, then $s = t$ and the $\{q_j\}$ can be reordered such that $q_i = \pm p_i$ for all i.*

Proof. The first sentence is given by Lemma 1.3.3, and the second by Lemma 1.3.4. □

Alright, time for an example using the FTA.

Example 1.3.1. Consider positive $a, b \in \mathbb{Z}$. Write

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \text{and} \quad b = q_1^{b_1} \cdots q_n^{b_n},$$

where $a_1, \ldots, a_n, b_1 \ldots, b_n \geq 0$ and $p_1, \ldots, p_n > 0$ are primes. We want to show that if d is a common divisor of a, b, then $d | (a, b)$.

The common divisors of a and b are of the form $p_1^{k_1} \cdots p_n^{k_n}$, where $k_i \leq \min(a_i, b_i)$ is a positive integer. On the other hand, (a, b) is simply $p_1^{\min(a_1, b_1)} \cdots p_n^{\min(a_n, b_n)}$. We write

$$p_1^{k_1} \cdots p_n^{k_n} (p_1^{\min(a_1, b_1) - k_1} \cdots p_n^{\min(a_n, b_n) - k_n}) = p_1^{\min(a_1, b_1)} \cdots p_n^{\min(a_n, b_n)}.$$

By the definition of k_i, $p_i^{\min(a_i, b_i) - k_i} \in \mathbb{Z}$. Thus the second term on the LHS is an integer, implying that $d | (a, b)$.

2 Congruences and Modular Arithmetic

2.1 Congruence in $\mathbb{Z}$

Definition 2.1.1. Take a nonzero $n \in \mathbb{Z}$. Then $a, b \in \mathbb{Z}$ are **congruent** modulo (or "mod") n if $n|(a-b)$. In other words,

$$n|(a-b) \iff a, b \text{ congruent mod } n \iff a \equiv b \pmod{n}.$$

First, we will show some fairly routine properties of congruence modulo n that will become helpful shortly.

Claim. Congruence modulo n is an equivalence relation.

Proof. We will show that congruence modulo n is reflexive, symmetric, and transitive.

Reflexive: Trivially, $a \equiv a \pmod{n}$.

Symmetric: $a \equiv b \pmod{n} \implies n|(a-b)$. Then $kn = a - b$ for $k \in \mathbb{Z}$ and thus

$$-kn = b - a \implies n|(b-a) \implies a \equiv b \pmod{n}.$$

Transitive: Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $nk = a - b$ and $nj = b - c$ for $k, j \in \mathbb{Z}$. Adding the equations, we get

$$n(k+j) = a - c \implies n|(a-c) \implies a \equiv c \pmod{n}.$$

□

Claim. For $n > 0$, every $a \in \mathbb{Z}$ is congruent mod n to some $r \in \mathbb{Z}$ where $0 \leq r < n$.

Proof. Apply the division algorithm on n and a to obtain $a = qn + r$, where $q \in \mathbb{Z}$ and $0 \leq r < n$. Then $a - r = qn$, implying $n|(a-r)$ and $a \equiv r \pmod{n}$. □

Claim. We can add and multiply congruences. If $a \equiv b \pmod{n}$ and $c \equiv b \pmod{n}$, then the following hold:

$$a + c \equiv b + d \pmod{n}$$

$$ac \equiv bd \pmod{n}.$$

Proof. We know that $a - b = kn$ and $c - d = jn$ for $k, n \in \mathbb{Z}$. Thus,

$$(a+c) - (b+d) = kn + jn = (k+j)n$$

and

$$\begin{aligned} ac - bd &= ac - bc + bc - bd = c(a-b) + b(c-d) \\ &= ckn + bjn = (ck + bj)n. \end{aligned}$$

□

We might want some concrete way to think about all the numbers congruent to a fixed number mod n. For instance, we will probably want to express the notion of "wrapping around" when a number exceeds its modulus. This motivates the following definition:

Definition 2.1.2. The **congruence class of a mod n** is

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod{N}\}.$$

When unambiguously referring to one modulus, we omit the subscript so that $[a]_n = [a]$. When we are clearly dealing with $\mathbb{Z}_n$, we drop the brackets altogether. For instance, in $\mathbb{Z}_5$, we can write $2 + 3 = 0$.

Here is a result that makes intuitive sense:

Theorem 2.1.1. *Congruence classes mod n partition the integers into exactly n non-overlapping subsets of $\mathbb{Z}$.*

Proof. Firstly, we will establish a criterion for determining that two equivalence classes are equal. We claim that if $a \equiv b \pmod{n}$, then $[a] = [b]$. Take some $c \in [a]$; then $a \equiv c \pmod{n}$. By symmetry and transitivity, $b \equiv c \pmod{n}$, so $c \in [b]$. Thus, $[a] \subseteq [b]$. Analogously, $[b] \subseteq [a]$. We conclude $[a] = [b]$.

Note that it is also easy to show the converse:

$$[a] = [b] \implies a \in [b] \implies a \equiv b \pmod{n}.$$

Now suppose two congruence classes $[a], [b]$ are not disjoint; in other words, $[a] \cap [b] \neq \emptyset$. Then there exists some c such that $c \in [a]$ and $c \in [b]$. Respectively, these imply $a \equiv c \pmod{n}$ and $b \equiv c \pmod{n}$.

By transitivity, $a \equiv b \pmod{n}$, so $[a] = [b]$ from the above result. So either $[a]$ and $[b]$ are disjoint or $[a] = [b]$. This shows the non-overlapping part of the theorem.

Since every $a \geq n$ will reduce to some $0 \leq r < n \bmod n$, the distinct congruence classes mod n are given by $[0], [1], \ldots, [n-1]$. To show that these are unequal, it suffices to show that $0, 1, \ldots, n-1$ are pairwise incongruent mod n, per the converse of our criterion above.

Let s and t be distinct integers in the range $[0, n)$. WLOG, let $s < t$. Then $0 < t - s < n$, so $n \nmid (t - s)$. Therefore, $t \not\equiv s$ and thus $[0], [1], \ldots, [n-1]$ are distinct. □

Example 2.1.1. Consider the following mapping:

$$[a]_7 \mapsto [\text{"round down } a \text{ to the nearest multiple of 10"}]_7.$$

Why isn't this a well-defined function? On the other hand, why is the following mapping well-defined?

$$[a]_7 \mapsto [-a]_7.$$

The first is not well-defined because it maps different representations of the same input to different outputs. Note that $[5] = [12]$ but the map sends the first to 0 and the second to $[10] = [3]$.

To show the second is well-defined, we write the same congruence class two different ways and show they map to the same result. Let $[a] = [b]$. Then $7|(a - b)$, which implies $7| - (a - b)$, so $7|((-a) - (-b))$. Therefore, $[-a] = [-b]$, as desired.

2.2 Arithmetic in $\mathbb{Z}_n$

Since the representatives of congruence classes are integers, it seems natural to extend arithmetic in $\mathbb{Z}$ to $\mathbb{Z}_n$. We will show that the following operations are well-defined on congruence classes in $\mathbb{Z}_n$:

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab].$$

Proof. Define $[c] = [a]$ and $[d] = [b]$. Then we want to show $[c+d] = [a+b]$. We already know $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Therefore, $(a+b) \equiv (c+d) \pmod{n}$, so $[a+b] = [c+d]$. □

Unsurprisingly, these operations work similarly to those in $\mathbb{Z}$.

Claim. Multiplication is commutative and distributes over addition.

Proof. Commutativity:

$$[a][b] = [ab] = [ba] = [b][a]$$

and distributivity:

$$\begin{aligned}[a] \cdot ([b] + [c]) &= [a] \cdot [b + c] \\ &= [a(b + c)] = [ab + ac] \\ &= [ab] + [ac].\end{aligned}$$

□

Let's solve some equations in $\mathbb{Z}_n$.

Example 2.2.1. Given that $(a, n) = 1$, solve $[a]x = [1]$, where $x \in \mathbb{Z}_n$.

From the first condition, we can write $au + nv = 1$ for $u, v \in \mathbb{Z}$. This implies $1 - au = nv$, so $au \equiv 1 \pmod{n}$. Thus, $[au] = [a][u] = [1]$; in other words, x is the congruence class represented by the Bezout coefficient of a.

Example 2.2.2. If p is prime and $[a] \neq 0$, show that $[a]x = [b]$ always has a unique solution in $\mathbb{Z}_p$.

First, we will show a solution exists. Note that multiplying any solution to $[a]x = [1]$ by $[b]$ will give the result. The solution to this equation exists by the previous example and the fact that $[a] \neq 0 \implies p \nmid a \implies (a, p) = 1$.

To show uniqueness, suppose $[a]x_1 = [a]x_2 = [b]$. Then $[a]x_1 - [a]x_2 = [a](x_1 - x_2) = [0]$. But since $(a, p) = 1$, we conclude $p|(y_1 - y_2)$, where y_1, y_2 are representatives for x_1, x_2, respectively. So $y_1 \equiv y_2 \pmod{p}$ and $x_1 = x_2$.

Example 2.2.3. When does $[a]x = [b]$ have a solution in $\mathbb{Z}_n$? When does it have multiple solutions?

Let $[y] = x$. Note that $[a]x = [b]$ having a solution is equivalent to finding y such that $ay \equiv b \pmod{n}$, or $ay - b = kn$ for $k \in \mathbb{Z}$. We can rearrange this equation to express b as a linear combination of a and n.

But since the smallest linear combination of a and n is (a, n), it is easy to see that *any* linear combination is a multiple of (a, n). Similarly, any multiple of (a, n) is an LC of a and b. So we see that a solution x exists iff b can be written as an LC of a and n; that is, when $(a, n)|b$.

There are multiple solutions when $(a, n) \neq 1$. In this case, we can find d such that $d \cdot (a, n) = n$ and $[d] \neq 0$, which implies $[ad] = [0]$. Therefore, if $[a]x = [b]$, we also have $[a](x + [d]) = [b]$.

Remark. In the special case $b = 1$, the only way to satisfy $(a, n)|b = 1$ is if $(a, n) = 1$. We can restate this as "$[a]$ is a unit in $\mathbb{Z}_n$ iff $(a, n) = 1$."

3 Rings

3.1 The Basics

Definition 3.1.1. A **ring** is a non-empty set R equipped with two binary operations + and × such that

- + and × are associative
- + is commutative
- + has an identity, denoted 0_R
- Any $r \in R$ has an inverse for +, denoted $-r$
- × has an identity, denoted 1_R
- × distributes over +.

  Some definitions do not require the existence of 1_R; rings that contain it are also called **rings with identity/unity**.

Definition 3.1.2. A **commutative ring** is a ring R in which × is commutative.

Remark. Although it is intuitive in $\mathbb{Z}$, $0_R \times x = 0_R$ is not explicitly mentioned in the ring axioms. We must show it as follows:

$$\begin{aligned} 0_R \times x = (0_R + 0_R) \times x &= 0_R \times x + 0_R \times x \\ \implies 0_R &= 0_R \times x, \end{aligned}$$

where in the last step we add $-(0_R \times x)$ to both sides.

Definition 3.1.3. A nonempty subset S of a ring R is a **subring** of R if S is a ring with the same operations and identities as R.

Theorem 3.1.1. *If $S \subset R$ is nonempty and R is a ring, S is a subring of R if*

- $0_R, 1_R \in S$
- *S is closed under addition*
- *S is closed under additive inverse*
- *S is closed under multiplication*

3.2 Ring Homomorphisms

Definition 3.2.1. Given rings R and S, a mapping $R \xrightarrow{\phi} S$ is a **ring homomorphism** if it has the following properties:

- $\phi(x + y) = \phi(x) + \phi(y)$ for $x, y \in R$
- $\phi(xy) = \phi(x)\phi(y)$ for $x, y \in R$
- $\phi(1_R) = 1_S$

Definition 3.2.2. A **ring isomorphism** is a bijective ring homomorphism. If there exists an isomorphism between rings R and S, then we say they are isomorphic, or $R \cong S$.

Definition 3.2.3. The **kernel** of a ring homomorphism ϕ is defined as

$$\ker \phi = \{r \in R \mid \phi(r) = 0_S\}.$$

As with linear transformations, ring homomorphisms have the following property:

Theorem 3.2.1. *A ring homomorphism from R to S is injective iff its kernel is $\{0_R\}$.*

Proof. Suppose ϕ is injective. Then, for $x, y \in R$, we have $\phi(x) = \phi(y) \implies x = y$. Therefore,

$$\phi(0_S) = \phi(x - y) = \phi(x) - \phi(y) = x - y = 0_T.$$

But since ϕ is injective, this is the only value that maps to 0_T. Thus, $\ker \phi = \{0_S\}$.

Now suppose $\ker \phi = \{0_R\}$. Take $x, y \in R$ such that $\phi(x) = \phi(y)$. Then $0_T = \phi(x) - \phi(y) = \phi(x - y)$. By assumption, $x - y = 0_R$, so $x = y$ and ϕ is injective. □

Here are some rapid-fire properties of ring homomorphisms given ϕ from S to T:

Claim. $\phi(0_S) = 0_T$.

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

Claim. ϕ respects additive inverses.

Proof. Take $x \in S$. Then $0_T = \phi(x - x) = \phi(x) + \phi(-x)$, so $\phi(x)$ is the additive inverse of $\phi(-x)$. Thus, $-\phi(x) = \phi(x)$. □

Claim. If $u \in S$ is a unit, $\phi(u) \in T$ is a unit.

Proof. Let $uv = 1_S$. Then

$$1_T = \phi(1_S) = \phi(uv) = \phi(u)\phi(v).$$

So $\phi(u)$ is a unit whose inverse is $\phi(v)$. □

Here is a useful result about ring isomorphisms:

Theorem 3.2.2. *Let $\phi : R \longrightarrow S$ be a ring isomorphism. Then $\phi^{-1} : S \longrightarrow R$ is also a ring isomorphism.*

Proof. Since ϕ is bijective, we know its inverse exists and is bijective. We only need to show it is a ring homomorphism. Clearly, it maps 1_S to 1_R.

Take $s, s' \in S$ such that $\phi(r) = s$ and $\phi(r') = s'$ for $r, r' \in R$. Then

$$\phi^{-1}(s + s') = \phi^{-1}(\phi(r) + \phi(r')) = \phi^{-1}(\phi(r + r')) = r + r' = \phi^{-1}(s) + \phi^{-1}(s').$$

For multiplication,

$$\phi^{-1}(ss') = \phi^{-1}(\phi(r)\phi(r')) = \phi^{-1}(\phi(rr')) = rr' = \phi^{-1}(s)\phi^{-1}(s').$$

□

3.3 More Rings

Definition 3.3.1. A **domain** is a commutative ring R in which $0_R \neq 1_R$ and if $ab = 0$ for $a, b \in R$, then $a = 0$ or $b = 0$.

Definition 3.3.2. A **field** is a commutative ring R in which $0_R \neq 1_R$ and every nonzero element has a multiplicative inverse.

Given a commutative ring R:

Definition 3.3.3. The **polynomial ring over** R is the set

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R, n \in \mathbb{N}\}$$

Definition 3.3.4. The **ring of** $n \times n$ **matrices over** R is the set $M_n(R)$ of $n \times n$ matrices with entries in R with matrix arithmetic defined analogously as with $+$ and $\times$.

Below is a familiar property of polynomials:

Theorem 3.3.1. *If R is a domain and f, g are nonzero polynomials in $R[x]$, then*

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x).$$

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$. Then the leading term of $f(x)g(x)$ is $a_n b_m x^{m+n}$. But since R is a domain, $a_n b_m \neq 0$. Thus, $f(x)g(x)$ is nonzero and its degree is $n + m = \deg f(x) + \deg g(x)$. □

Corollary 3.3.1. *$R[x]$ is a domain iff R is a domain.*

Proof. The forward direction is straightforward since R is a subring of $R[x]$. The converse follows from Theorem 3.3.1, which implies that the product of nonzero polynomials in $R[x]$ is nonzero. □

Corollary 3.3.2. *For any domain R, the units in $R[x]$ are the units in the subring R.*

Proof. First, we will show that any unit in R is a unit in $R[x]$. Take a unit r in R; it satisfies $rs = 1$ for some $s \in R \subset R[x]$. So both r and s are also units in $R[x]$.

Now we will show the converse; that every unit in $R[x]$ is a constant polynomial i.e., a member of R. Recall that $\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$. When $f(x)g(x) = 1$, we have $\deg[f(x)g(x)] = 0$. Since degree is non-negative, it must be that $\deg f(x) = \deg g(x) = 0$. So $f(x)$ and $g(x)$ are constant polynomials. □

3.4 Polynomial Rings

Definition 3.4.1. A polynomial is **monic** if its leading term (term of highest degree) has coefficient 1.

Theorem 3.4.1. *Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

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

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Theorem 3.4.2. *Let F be a field and $a(x), b(x) \in F[x]$, not both zero. Then there is a unique monic polynomial that is the GCD $d(x)$ of $a(x)$ and $b(x)$. Moreover, there exist $u(x), v(x) \in F[x]$ such that $a(x)u(x) + b(x)v(x) = d(x)$.*

Theorem 3.4.3. *Let F be a field. Every non-constant polynomial in $F[x]$ can be factored into **irreducible polynomials**. This factorization is unique up to order and unit multiples.*

Example 3.4.1. In the ring $\mathbb{Z}_2[x]$, we can divide the polynomial $x^5 + 3x^3 + x^2 + 1$ by $x^2 + 1$ by first reducing the coefficients and then applying trial and error; we obtain $x^3 + 1$.

Note, however, that the field that creates the polynomial ring can affect division. For instance, we cannot divide $x^2 - 3$ by $2x - 1$ in $\mathbb{Z}[x]$ because the quotient would be a polynomial with linear term $\frac{1}{2}x \notin \mathbb{Z}[x]$.

Thus, the division algorithm for polynomials is not true in general if F is a domain but not a field.

Recall that in elementary algebra, the presence of a root of a polynomial implies that the polynomial is reducible. For instance, 2 is a root of $x^2 - 3x + 2$, so we can factor it as $(x-2)(x-1)$. We will now generalize this idea to elements of any polynomial ring. For the next two theorems, fix $f \in \mathbb{F}[x]$.

Theorem 3.4.4 (Remainder theorem)**.** *For $\lambda \in \mathcal{F}$, the remainder when f is divided by $(x - \lambda)$ is $f(\lambda)$.*

Proof. We apply the division algorithm on f and $(x - \lambda)$:

$$f(x) = q(x)(x - \lambda) + r(x),$$

where $q(x), r(x) \in \mathbb{F}[x]$ and $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Since $g(x)$ is linear, $r(x)$ has degree 0; in other words, it is constant. Now we evaluate $f(x)$ at λ to obtain

$$f(\lambda) = q(x)(\lambda - \lambda) + r = r.$$

□

Theorem 3.4.5 (Factor theorem)**.** *$(x - \lambda)$ divides f iff $f(\lambda) = 0$.*

Proof. Let $r(x)$ be the remainder on division of f by $(x - \lambda)$.

$$(x - \lambda) | f \implies r(x) = 0 \implies f(\lambda) = 0.$$

Now suppose $f(\lambda) = 0$. Then $\deg r(x) < \deg(x - \lambda) = 1$, so $r(x)$ is constant. But, by assumption, $r(x) = 0$, so it is the constant 0. This implies $(x - \lambda) | f$. □

Shockingly, the factor theorem can be useful when we want to factor polynomials.

Example 3.4.2. Factor $x^5 - x$ in $\mathbb{Z}_5[x]$.

Firstly, we write $x^5 - x = x(x^4 - 1)$. Note that every integer from 1 to 4 inclusive is one more than a multiple of 5 when raised to the fourth power. Therefore, they are all roots of $x^4 - 1$, implying that the roots of $x^5 - x$ are 0, 1, 2, 3, and 4. We can thus factor it as such:

$$x(x-1)(x-2)(x-3)(x-4).$$

This result gives us a strategy for determining whether certain polynomials are irreducible. Note that if $f \in \mathbb{F}[x]$ is reducible, it must be the product of two polynomials of lesser degree; when $\deg f$ is 2 or 3, then, one of these polynomials must have degree 1. But it is easy to see that every linear polynomial has roots.

Therefore, if an f with degree 2 or 3 has no roots, it has no linear factors, meaning that it is irreducible.

This is, of course, generally untrue for polynomials of degree > 3. For instance, $x^4 + 2x^3 + 3x^2 + 2x + 1 = (x^2 + x + 1)^2$ has no linear factors and thus no roots.

As with the integers, we can define congruence in polynomial rings:

Definition 3.4.2. Fix $f(x) \in \mathbb{F}[x]$. Define $g, h \in \mathbb{F}[x]$ to be **congruent modulo** f if $f|(g - h)$. This is equivalent to $g \equiv h \pmod{f}$ and $h \in [g]_f$.

Theorem 3.4.6. *Congruence in polynomial rings is an equivalence relation.*

Proof. Exercise. □

Theorem 3.4.7. *Take $f(x) \in \mathbb{F}[x]$ with degree $d > 0$. Every congruence class $[g]_f$ contains a unique polynomial from $S = \{h(x) \in \mathbb{F}[x] \mid h(x) = 0$ or $\deg h(x) < d\}$.*

Proof. Apply the division algorithm on division of g by f to obtain $g(x) = q(x)f(x) + r(x)$, where q and r are unique polynomials in $\mathbb{F}[x]$ and $r = 0$ or $\deg r < \deg f$. So r is exactly the unique polynomial in question. □

Remark. We can also show uniqueness by supposing r and s are two polynomials in S in the same congruence class. Then $f|(r - s)$, but r and s both have lower degree than f. The only way for the relation to hold is if $r - s = 0$, or $r = s$.

Example 3.4.3. How many distinct congruence classes are there for $\mathbb{Z}_2[x]$ mod $x^3 + x$? How about $\mathbb{Z}_3[x]$ mod $x^2 + x$?

By the previous remark, any polynomial in $\mathbb{Z}_2[x]$ with degree less than $\deg x^3 + x = 3$ will be in its own congruence class. This is any polynomial of the form $a_2x^2 + a_1x + a_0$, where $a_i \in \mathbb{Z}_2$. So we have $2^3 = 8$ distinct congruence classes.

Similarly, the second example has $3^2 = 9$ classes.

4 Ideals and Quotient Rings

4.1 Ideals

Definition 4.1.1. An **ideal** of a ring R is a non-empty subset I satisfying

- I is closed under addition
- If $x \in I$ and $r \in R$, then $rx \in I$ and $xr \in I$. This is sometimes called the **absorption property**.

Example 4.1.1. The following are ideals:

- The set of polynomials with even constant in the ring $\mathbb{Z}[x]$.
- For a fixed a, $\{ak \mid k \in \mathbb{Z}\}$ in $\mathbb{Z}$.
- $\{0\}$ in any ring.

The following are not:

- The set of odd integers in the ring $\mathbb{Z}$.
- The set of polynomials with nonzero constant in $\mathbb{Z}[x]$.

The second example is called the **principal ideal generated by** a and is denoted (a). For $r, s \in R$, we have $(r) \subseteq (s)$ when $s|r$, and $(r) = (s)$ when $r|s$ and $s|r$. If R is a domain, then $r = us$ for a unit u (think about it).

Definition 4.1.2. Let I be an ideal of a ring R. Two elements $x, y \in R$ are **congruent mod** I if $x - y \in I$. We write $x \equiv y \pmod{I}$.

Definition 4.1.3. The **congruence class of** y **mod** I is the set $\{y + z \mid z \in I\}$ of all elements of R congruent to y mod I, denoted $y + I$.

Presented without proof, here are some easy-to-show yet useful properties of ideals.

Claim. For an ideal I of a ring R:

- I contains 0
- I is closed under additive inverses
- $1_R \in I \implies I = R$

Example 4.1.2. Let $R = \mathbb{Z}[x]$ and I be the set of polynomials in R with even constant. Show that I is an ideal but that I is not a principal ideal generated by any value.

Proof. I is an ideal because the sum of even constants is even, and the product of even constants with any constant is also even. To show it is not principal, note that $2 \in I$. Then, if c generates I, we have $c|2$, so $c = \pm 2, \pm 1$.

$x \in I$ as well, so $c = \pm 1$ since $\pm 2 \nmid x$. But $1 \notin I$, a contradiction. □

In some rings, we can actually characterize *all* ideals.

Theorem 4.1.1. *The only two ideals in* $\mathbb{F}$ *are* $\mathbb{F}$ *and* $\{0\}$.

Proof. Take an nontrivial ideal I in $\mathbb{F}$. Then let $r \in I$, which implies $1 = r^{-1}r \in I$; hence, $I = \mathbb{F}$. □

Theorem 4.1.2. *Every ideal in* $\mathbb{Z}$ *is a principal ideal.*

Proof. Consider the smallest positive element c in I. Then, by definition, $(c) \subseteq I$. Now take any $x \in I$; we wish to show $c|x$. Using the division algorithm, we can write $x = cq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < c$.

Note that $c \in I \implies cq \in I \implies -cq \in I$. Since ideals are closed under addition, $x - cq = r$ is in I. By minimality of c, we have $r = 0$, which implies $x = cq \in (c)$. □

Remark. Note that not every ideal in every ring is a principal ideal; for instance, the I in Example 4.1.2 in $R = \mathbb{Z}[x]$.

Definition 4.1.4. The set

$$I = \{r_1c_1 + r_2c_2 + \cdots + r_tc_t \mid r_i \in R\},$$

is denoted $(c_1, c_2, \ldots, c_t)$ and is called the **ideal generated by** $c_1, c_2 \ldots, c_n$.

Claim. The above set is an ideal. Moreover, an ideal generated by two integers m, n is a principal ideal generated by (m, n).

Proof. It is pretty clear the set is an ideal; adding two elements, we can combine each c_i pair to obtain a linear combination like the original form. Multiplying an element in the set just scales each coefficient while preserving the linear combination's structure.

Denote $x = (m, n)$. We will first show $I \subseteq (x)$. We can take any element in S and write it as $k_1m + k_2n$ for $k_1, k_2 \in R$. Since $x|k_1m$ and $x|k_n$, we have $x|(k_1m + k_2n)$. So $I \subseteq (x)$.

Now we will show $(x) \subseteq I$. It suffices to show $x \in I$ since S is closed under multiplication by any element of R, which is enough to produce any member of (x). By Bezout, there exist $k_1, k_2 \in \mathbb{Z}$ such that $k_1m + k_2n = x$. So $x \in I$ and $(x) \subseteq I$. Therefore, $(x) = I$, implying that (m, n) generates I. □

4.2 Quotient Rings

In this section, we generalize the notion of congruence classes to arbitrary ideals in arbitrary rings.

Definition 4.2.1. Let I be an ideal of ring R. Then, for $x, y \in R$, we say x **is congruent to** y **mod** I if $x - y \in I$. The analogous notation follows.

Definition 4.2.2. The **congruence class of** y **mod** I is the set $\{y + z \mid z \in I\}$ of all the elements of R congruent to y mod I, denoted $y + I$.

Definition 4.2.3. The **quotient ring** of R by I is the set R/I of all congruence classes mod I in R. Addition and multiplication are defined as such:

$$(x + I) + (y + I) := (x + y) + I \qquad (x + I) \times (y + I) := (x \times y) + I$$

A familiar example of a quotient ring is $\mathbb{Z}_n = \mathbb{Z}/(n)$. It is the set of all congruence classes mod (n) in $\mathbb{Z}$: namely, $\{[0]_n, [1]_n, \dots, [n-1]_n\}$. Note that addition/multiplication agree with Definition 4.2.3.

In the language of quotient rings, we can also write $[k]_n = k + (n)$; it is easy to check that congruence mod the ideal (n) is equivalent to our familiar definition of congruence mod n.

Example 4.2.1. Let $R = \mathbb{Z}_6$ and consider the subset $I = \{[0], [2], [4]\}$.

The elements in the congruence class of $[0]$ are those whose difference with $[0]$ is in I. This is simply the set $\{[0], [2], [4]\}$. Note that this is exactly the congruence class of $[2]$. For $[1]$, we obtain $\{[1], [3], [5]\}$.

Now consider the ring $\mathbb{Z}_6/I$. It has two elements—the two distinct classes we found above. We can also express them as $0 + I$ and $1 + I$, or just 0 and 1 if we abuse notation.

This leads us to the observation that $\mathbb{Z}_6/I \cong \mathbb{Z}_2$ under the mapping $0 + I \longrightarrow [0]_2$ and $1 + I \longrightarrow [1]_2$.

Example 4.2.2. Consider $I = \{(r, 0_S) \mid r \in R\}$, which is an ideal of $R \times S$. We claim that $(R \times S)/I \cong S$.

To see this, take any element in $R \times S$, say (r, s), given $r \in R$ and $s \in S$. In $(R \times S)/I$, this is a member of the coset $(0_R, s) + I$ since $(r, s) - (0_R, s) = (r, 0_S) \in I$. We thus obtain the mapping $(0_R, s) \longrightarrow s$, which is clearly an isomorphism.

Let $\mathbb{F}$ be a field and let $R = \mathbb{F}$. Consider the ideal $I = (f(x)) = \{f(x)g(x) \mid g(x) \in R\}$.

Theorem 4.2.1. *$h(x) + I$ is a zerodivisor iff $(f(x), h(x)) \neq 1$.*

Proof. Suppose $(f(x), h(x)) \neq 1$. Then denote it by $d(x) \in R$. We can write $f(x) = a(x)d(x)$ and $h(x) = d(x)b(x)$ for $a(x), b(x) \in R$. Then

$$(h(x) + I)(a(x) + I) = h(x)a(x) + I = d(x)b(x)a(x) + I = f(x)b(x) + I = 0 + I.$$

So either $a(x) + I = 0 + I$ or $h(x)$ is a zerodivisor. Suppose the former. Then $d(x) = 1$, since it must be a monic polynomial of degree 0, a contradiction. Therefore, $h(x)$ is a zerodivisor.

We will show the converse via contrapositive. Suppose $(h(x), f(x)) = 1$; then there exist polynomials $u(x), v(x)$ such that $h(x)u(x) + f(x)v(x) = 1$, so $h(x)u(x) + I = 1 + I$.

Now, for some polynomial $g(x)$, suppose $h(x)g(x) + I = 0 + I$. Then we multiply both sides by $u(x)$, which gives

$$0 + I = h(x)g(x)u(x) + I = (1 + I)(g(x) + I).$$

Then $g(x) + I = 0$, which implies that $h(x) + I$ is not in general zero or a zerodivisor. □

Theorem 4.2.2. *$h(x) + I$ is a unit in $R/(f(x))$ iff $(f(x), h(x)) = 1$.*

Proof. Suppose $(f(x), h(x)) = 1$. Then we can write $f(x)u(x) + h(x)v(x) = 1$, so $1 - h(x)v(x) = f(x)u(x)$ and $h(x)v(x) + I = 1 + I$. So $h(x) + I$ is a unit.

Now suppose $h(x) + I$ is a unit. Then there exists some $a(x) + I$ such that $h(x)a(x) + I = 1 + I$. This implies $h(x)a(x) - 1 = f(x)b(x)$ for $b(x) \in R$. We can rearrange this to obtain a linear combination of $f(x)$ and $h(x)$ equal to 1; hence, $(f(x), h(x))$ is a multiple of 1. We conclude $(f(x), h(x)) = 1$. □

Theorem 4.2.3. *If $\mathbb{F}$ is a field, then $f(x)$ is irreducible iff $R/(f(x))$ is a field.*

Proof. Follows directly from Theorem 4.2.1 and 4.2.2. □

There exists a more general form of this result: a necessary and sufficient condition for whether a quotient ring is a field. First, we introduce the concept of maximal ideals.

Definition 4.2.4. A proper ideal I in a ring R is **maximal** if $I \subsetneq J \implies J = R$ for any ideal J.

That is, a maximal ideal is one whose only proper superset ideals are itself and the parent ring.

Theorem 4.2.4. *Take a commutative ring R and let I be an ideal of R. Then R/I is a field if and only if I is maximal.*

Proof. Suppose I is maximal. We will first show that if $a \notin I$, then $a + I$ is a unit in R/I.

Consider the set $S = \{ax + b \mid x \in R, b \in I\}$, which consists of every element of I added to every possible multiple of a. Clearly, $I \subseteq S$, so $S = R$ by definition of maximal ideal. Therefore, $1 \in S$, so there exist $x' \in R$ and $b' \in I$ such that $ax' + b' = 1$.

But this implies $ax' - 1 = b'$, so $ax' \equiv 1 \pmod{I}$. Hence $(a + I)^{-1} = x' + I$, and $a + I$ is a unit.

Now we return to the main result. If $a \notin I$, then $a + I$ is nonzero, but by the previous result, $a + I$ is also a unit. Otherwise, $a \in I$ and thus $a + I = 0 + I$. Therefore, every nonzero element of R/I is a unit, so the quotient is a field.

To show the converse, suppose R/I is a field and that there exists an ideal J such that $I \subsetneq J$. Now take some $a \in J \backslash I$. By assumption, there exists some $b + I \in R/I$ such that $ab + I = 1 + I$. So $1 - ab \in I \subsetneq J$.

By choice of a and b, we have $ab \in J$, so we conclude $1 \in J$. Therefore, $J = R$ and I is maximal. □

Remark. In showing the converse, our condition $a \in J \backslash I$ was equivalent to picking a such that $a + I$ was nonzero and thus a unit.

Example 4.2.3. Fix $a \in \mathbb{R}$. Prove that $(x - a)$ is maximal in $\mathbb{R}[x]$ for all a.

Proof. One way to show this is to show $\mathbb{R}[x]/(x - a)$ is a field. We claim $\mathbb{R}[x]/(x - a) \cong \mathbb{R}$.

Consider the map $\eta : \mathbb{R}[x] \longrightarrow \mathbb{R}$ that sends $f(x)$ to its remainder when divided by $(x - a)$. By the division algorithm, η is well-defined. It is surjective because the codomain is simply $\mathbb{R}$, and any $r \in \mathbb{R}$ is mapped to by the constant polynomial r.

To show injectivity, let $f(x)$ and $g(x)$ map to the same $r(x)$ so that $f(x) - p(x)(x-a) = g(x) - q(x)(x-a)$ for $p(x), q(x) \in \mathbb{R}[x]$. Then $f(x) - g(x) = (x-a)(p(x) - q(x))$, so $f(x)$ and $g(x)$ are representative of the same congruence class in $\mathbb{R}[x]/(x-a)$.

Therefore, η is a bijection, so $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$. Since the quotient is isomorphic to a field, it is itself a field. □

4.3 Noether's First Isomorphism Theorem

Here, we introduce a powerful result that greatly simplifies proofs like Example 4.2.3.

> **Theorem 4.3.1** (Noether's FIT). *Let $\phi : R \longrightarrow S$ be a surjective ring homomorphism, and let* $\ker \phi = I$. *Then $R/I \cong S$.*

Proof. Fix a surjective ring homomorphism $\phi : R \longrightarrow S$ with kernel I. Define $\overline{\phi} : R/I \longrightarrow S$ such that $\overline{\phi}(r + I) = \phi(r)$. The goal is to show $\overline{\phi}$ is an isomorphism.

First, we show it is well-defined. Take $r, s \in R$ such that $r - s \in I$ (that is, they are representatives of the same congruence class mod I). Then $\overline{\phi}(r + I) - \overline{\phi}(s + I) = \phi(r) - \phi(s) = \phi(r - s) = 0$.

Next, we show it is a homomorphism.

$$\overline{\phi}(1 + I) = \phi(1) = 1.$$

$$\overline{\phi}((r + I) + (s + I)) = \overline{\phi}((r + s) + I) = \phi(r + s) = \phi(r) + \phi(s) = \overline{\phi}(r + I) + \overline{\phi}(s + I).$$

$$\overline{\phi}((r + I) \cdot (s + I)) = \overline{\phi}((r \cdot s) + I) = \phi(r \cdot s) = \phi(r) \cdot \phi(s) = \overline{\phi}(r + I) \cdot \overline{\phi}(s + I).$$

Finally, we show bijectivity. Take any $s \in S$. Since ϕ is surjective, we can pick $r \in R$ where $\phi(r) = s$. Then $r + I$ maps to s; hence, $\overline{\phi}$ is surjective.

For injectivity, note that $\overline{\phi}(r + I) = 0$ implies $\phi(r) = 0$. Since $\ker \phi = I$, we have $r \in I$, so $r + I$ is always $0 + I$. Hence, $\ker \overline{\phi}$ is trivial.

We conclude that $\overline{\phi}$ is an isomorphism from R/I to S. □

Let's rework Example 4.2.3 using FIT.

> **Example 4.3.1.** Fix $a \in \mathbb{R}$. Prove that $(x - a)$ is maximal in $\mathbb{R}[x]$ for all a.

Proof. Consider the evaluation map $\eta : \mathbb{R}[x] \longrightarrow \mathbb{R}$ where $f \mapsto f(a)$. It is straightforward to check η is a homomorphism, and surjectivity follows since any $\lambda \in \mathbb{R} \subset \mathbb{R}[x]$ maps to itself.

Now consider the ideal $(x - a)$. Then $(x - a) \subseteq \ker \eta$ follows immediately. If we take $g(x) \in \ker \eta$, then we can write $\eta(g(x)) = \eta(h(x)(x - a) + r) = 0$, so $r = 0$. This implies $g(x) \in (x - a)$, so $(x - a) = \ker \eta$.

Result follows from FIT. □

We only had to show a homomorphism was surjective and prove two sets were equal—much easier than naming an explicit isomorphism.

> **Definition 4.3.1.** An ideal $P \subsetneq R$ in a commutative ring R is **prime** if $fg \in P$ implies $f \in P$ or $g \in P$.

Example 4.3.2. Show that the ideal (x, y) in $\mathbb{Z}[x, y]$ is prime.

Proof. Note that

$$(x, y) \text{ is prime } \iff \mathbb{Z}[x, y]/(x, y) \text{ is a domain.}$$

For intuition, suppose $\mathbb{Z}[x, y]/(x, y)$ is a domain. Then if two elements' representatives multiply to an element of (x, y), one must also belong to (x, y), which is equivalent to saying the ideal is prime.

To prove $\mathbb{Z}[x, y]/(x, y)$ is a domain, we can show it is isomorphic to $\mathbb{Z}$. By a similar argument as above, we know $\eta : \mathbb{Z}[x, y] \longrightarrow \mathbb{Z}$ where $f(x, y) \mapsto f(0, 0)$ is a surjective ring homomorphism. Also, $\ker \eta = (x, y)$. Therefore, by FIT, $\mathbb{Z}[x, y]/(x, y) \equiv \mathbb{Z}$. □

5 Groups

5.1 The Basics

Definition 5.1.1. A **group** $(G, *)$ is a nonempty set G with an operation $*$ with the following axioms:

- For $g_1, g_2, g_3 \in G$, we have $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
- There exists $e \in G$ such that for all $g \in G$, $e * g = g * e = g$.
- For all $g \in G$, there exists $h \in G$ such that $g * h = h * g = e$.

Definition 5.1.2. An **abelian group** is a group $(G, *)$ with the following axiom:

- For $g_1, g_2 \in G$, we have $g_1 * g_2 = g_2 * g_1$.

Definition 5.1.3. A **subgroup** of a group $(G, *)$ is a subset H that is also a group under $*$.

Definition 5.1.4. Fix a group $(G, *)$. The **order** of $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such element exists, g has infinite order.

Often, we will abuse notation and say "the group G" instead of $(G, *)$. Groups are often used as abstractions for symmetry.

Example 5.1.1. Consider the ways to manipulate an equilateral triangle without changing its position.

- k: do nothing
- r_{120}: rotate 120° counterclockwise
- r_{240}: rotate 240° CCW
- f_1: flip over vertical axis
- f_2: flip over axis 60° CCW from vertical
- f_3: flip over axis 60° CW from vertical

Now consider what happens when we compose two of these actions. The column corresponds to the first operation applied, and the row the second.

$*$	k	r_{120}	r_{240}	f_1	f_2	f_3
k	k	r_{120}	r_{240}	f_1	f_2	f_3
r_{120}	r_{120}	r_{240}	k	f_2	f_3	f_1
r_{240}	r_{240}	k	r_{120}	f_3	f_1	f_2
f_1	f_1	f_3	f_2	k	r_{240}	r_{120}
f_2	f_2	f_1	f_3	r_{120}	k	r_{240}
f_3	f_3	f_2	f_1	r_{240}	r_{120}	k

By inspection, the set combined with $*$ satisfies the identity/inverse axioms. Since function composition is associative, the operation is too. So the symmetries of an equilateral triangle form a group with composition; note, however, that the abelian axiom is not satisfied.

We call this the **dihedral group** of degree 3, or the **symmetry group** of an equilateral triangle, or D_3.

Here are some basic properties of groups.

Theorem 5.1.1. *Fix a group $(G, *)$. Then the following hold:*

- *The identity of G is unique.*
- *Cancelation holds in G.*
- *The inverse of each element in G is unique.*

Proof.

- Let e, e' be two identities of G. Then $e' = ee' = e$.
- Suppose $ab = ac$; then $b = c$ follows from left multiplication by a^{-1}. We can show $ba = ca$ implies $b = c$ using right multiplication.
- Let d, d' be inverses of a. Then $ad = e = ad'$, so $d = d'$ by the previous part.

□

For any ring R, it is true that $(R, +)$ and $(R^\times, \times)$ are always groups; that is, some groups come from rings. Others do not:

Example 5.1.2. $GL_2(\mathbb{R})$ is the set of 2×2 invertible matrices with entries in $\mathbb{R}$. We can quickly check that $GL_2(\mathbb{R})$, together with multiplication, satisfies, the group axioms. This group is also called the **general linear group** of degree 2.

Rotation by 90° is an element of order 4, rotation by 180° has order 2, and scaling by 2 has infinite order.

Definition 5.1.5. Fix a group G. The **cyclic subgroup generated by** $g \in G$ is the following subgroup $\langle g \rangle$:

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

Here, we use multiplicative notation, but addition is defined similarly.

Definition 5.1.6. A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$.

So $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic groups generated by 1. Incidentally, the order of 1 in $\mathbb{Z}_n$ is n, which is also the group's order. This is expected.

Theorem 5.1.2. *For an element a in a group G, the order of a equals the order of $\langle a \rangle \leq G$.*

Proof. First, suppose $|a|$ is infinite. We claim that the powers of a are distinct. Toward a contradiction, suppose $a^m = a^n$ for $m \neq n$; then the order of a is at most $m - n$ (exercise), and we are done. So if $|a|$ is infinite, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is infinite in order.

Now suppose $|a| = m$. By minimality of m, the elements $1, a, a^2, \dots, a^{m-1}$ are distinct. Now take any $n \in \mathbb{Z}$. Using the division algorithm, we write $a^n = a^{mq+r} = (a^q)^m a^r = a^r$ for $0 \leq r < m$, so a^n is exactly one of the elements stated previously. □

Definition 5.1.7. Given two groups G and H, their **product** is the group with underlying set

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

The operation is given by

$$(g, h)(a, b) = (ga, hb).$$

So $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the group containing ordered pairs of elements in $\mathbb{Z}_2$. However, note that while $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 = |\mathbb{Z}_4|$, the groups are not isomorphic because $\mathbb{Z}_4$ has an element of order 4 while the first does not.

Definition 5.1.8. Take a group G. The **subgroup generated by** $g_1, g_2, \dots, g_n \in G$, denoted $\langle g_1, g_2, \dots, g_n \rangle$, is the set of finite products of the **generators** $g_1, g_2, \dots, g_n$ and their inverses.

Additive notation defined analogously.

Note that $\langle g_1, \dots, g_n \rangle$ is the smallest subgroup of G containing $g_1, \dots, g_n$.

Also, if G and H are both cyclic groups of order n, then G and H are isomorphic via the isomorphism sending one group's generator to the other. For this reason, we sometimes abuse notation and refer to *the* cyclic group of order n, or $\mathbb{Z}_n$.

5.2 Group Homomorphisms

In this section, we will classify all groups of orders 2, 3, and 4.

Definition 5.2.1. A **group homomorphism** is a map $\phi : G \longrightarrow H$ between groups that satisfies $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$.

An **isomorphism** of groups is a bijective homomorphism between them.

Definition 5.2.2. The **kernel** of a group homomorphism $\phi : G \longrightarrow H$ is the subset of G:

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

Example 5.2.1. The map $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ sending $A \mapsto \det A$ is a group homomorphism because $\det AB = \det A \det B$. The kernel is the set of matrices with determinant 1, or $SL_n(\mathbb{R})$, the **special linear group**.

Theorem 5.2.1. *Fix a group homomorphism $\phi : G \longrightarrow H$. Then the following hold:*

1. $\phi(e_G) = e_H$
2. $\operatorname{im} \phi \leq H$
3. $\ker \phi \leq G$
4. *ϕ is injective iff* $\ker \phi = \{e_G\}$

Proof. Exercise; some of these are identical to their ring homomorphism counterparts. □

Finding an isomorphism shows that two groups are equivalent up to relabeling, so our strategy for classification will be to find all unique groups *up to isomorphism.*

Claim. All groups of order 2 are isomorphic.

Proof. Consider any two groups of order 2, say $G = \{e_G, g\}$ and $H = \{e_H, h\}$.

We can construct a map $\phi : G \to H$ where $e_G \mapsto e_H$ and $g \mapsto h$; by construction, this is a bijection. It only remains to show that it is a homomorphism, which we quickly check by exhaustion.

- $\phi(e_G * e_G) = e_H = e_H * e_H = \phi(e_G) * \phi(e_G)$
- $\phi(e_G * g) = e_H * h = \phi(e_G) * \phi(g)$
- $\phi(g * e_G) = h * e_H = \phi(g) * \phi(e_G)$
- $\phi(g * g) = \phi(e_G)$ since g must have an inverse. Then $\phi(g * g) = e_H = h * h$ by the same argument, which is simply $\phi(g) * \phi(g)$.

So ϕ is an isomorphism, and $G \cong H$. For intuition, we could draw tables of G and H and see that the entries differ only in name. □

Claim. All groups of order 3 are isomorphic.