

MATH340 Review Notes

By Jack 'jryzkns' Zhou

1 Axiomatic Approach to \mathbb{N}

Definition: \mathbb{N} is a set with 3 axioms (sometimes referred to as the "Peano Axioms"):

1. $1 \in \mathbb{N}$
2. For every $a \in \mathbb{N}$, there is an element called the *successor* of a , written as $\text{succ}(a) = a + 1 \in \mathbb{N}$
3. Every element $a \in \mathbb{N}$ arises in this manner:

$$\mathbb{N} = \{\text{succ}^k(1) \mid k \geq 0\}$$

2 Mathematical Induction

Principle of Mathematical Induction:

Suppose $X \subseteq \mathbb{N}$ and:

1. $1 \in X$
2. $a \in X \Rightarrow a + 1 \in X$

Then $X = \mathbb{N}$.

This is taken as an axiom and cannot be proven from the 3 axioms presented in section 1.

Strong Induction:

Suppose $X \subseteq \mathbb{N}$ satisfies the properties

1. $1 \in X$
2. $\forall i \in [1, n] \ i \in X \Rightarrow n + 1 \in X$

This variant of induction is logically equivalent to the simple form of induction, but in a proof it may be desirable to refer to more than 1 case that is taken to be true, in which case a strong induction is preferred.

The Well-Ordering Principle (WP):

Every non-empty subset $Y \subseteq \mathbb{N}$ has a minimal element.

We can use WP to prove the Principle of Induction:

Suppose $X \subseteq \mathbb{N}$ has the properties $1 \in X$ and $k \in X \Rightarrow k + 1 \in X$, WTS $X = \mathbb{N}$. Suppose $Y = \{n \in \mathbb{N} \mid n \notin X\}$, then $X = \mathbb{N} \Leftrightarrow Y = \emptyset$

We proceed to show that $Y = \emptyset$ by contradiction, assuming $Y \neq \emptyset$. By WP, Y has a minimum element $n^* \in Y$. As $1 \notin Y$ (because $1 \in X$), $n^* > 1$ so $n^* - 1 \in \mathbb{N}$ and $n^* - 1 \notin Y$ because n^* is the minimal element of Y . Therefore $n^* - 1 \in X$, but then $\text{succ}(n^* - 1) = n^* - 1 + 1 = n^* \in X$ by the inductive hypothesis. As $n^* \in Y$, we have come to a contradiction, and therefore $Y = \emptyset$ and $X = \mathbb{N}$.

Note: WP is false for other sets of numbers. For example, there is no minimal element in \mathbb{R}^+ as $\forall x \in \mathbb{R}^+ \ \frac{1}{2}x < x$.

3 Operations on \mathbb{N}, \mathbb{Z}

Multiplication on \mathbb{N} :

Inductively defined with $1 \cdot a := a$ as the base case. If $n \cdot a$ is defined, then $(n + 1) \cdot a := n \cdot a + a$.

The Peano Axioms imply the following properties:

- Commutativity: $ab = ba$
- Associativity: $a(bc) = (ab)c$
- Distribution over Addition: $a(b + c) = ab + ac$

Defining \mathbb{Z} from \mathbb{N}

Suppose we want to solve an equation like $x + 5 = 2$ in \mathbb{N} , there are no solutions, because $x = 2 - 5 \notin \mathbb{N}$. Therefore, we need to invent the notion of negative numbers.

To do this, we can say that \mathbb{Z} is the set $\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$ with an equivalence relation $(a, b) = (a + c, b + c)$ for any $a, b, c \in \mathbb{N}$. The ordered tuple (a, b) represents $a - b$. We can see that $(a + c) - (b + c) = a - b$. More concretely, consider $(5, 0) = (6, 1) = (500, 495)$ and $5 - 0 = 6 - 1 = 500 - 495$. A negative number $-a$ could then be represented as $(0, a)$.

Induction in \mathbb{Z}

WP does not apply to \mathbb{Z} , so in practice we either treat +ive and -ive numbers separately, or we go by the absolute value of the numbers.

4 The Division Theorem in \mathbb{Z}

Theorem:

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exists unique $q \in \mathbb{Z}, r \in (0, b)$ such that $a = qb + r$.

Proof: We proceed in two steps, showing existence then uniqueness.

Existence: We have $a \in \mathbb{Z}, b \in \mathbb{N}$, we define

$$X = \{n \in \mathbb{N} \cup \{0\} \mid n = a - qb\}$$

For some integer q . X is nonempty as $a - qb \geq 0$ by choice of q . If $a > 0$, we pick $q = 0$. If $a \leq 0$, we pick $q = a$. By WP, X has a minimal element that we will call r ; $r = a - qb$ for some $q \in \mathbb{Z}$. Since $r \in \mathbb{N} \cup \{0\}$, $r \geq 0$. r also satisfies $r < b$. If $r \geq b$, then $r - b \in X$ as $r - b = (a - qb) - b = a - (q + 1)b$. This contradicts minimality of r . Rearranging $r = a - qb$ we get $a = qb + r$.

Uniqueness: Suppose we have (q_1, r_1) and (q_2, r_2) both satisfying the theorem, WTS $q_1 = q_2$ and $r_1 = r_2$.

We have $a = q_1b + r_1 = q_2b + r_2$ with $r_1, r_2 \in (0, b)$. If we collect the terms with b on one side, we have $(q_1 - q_2)b = r_2 - r_1$. So, $r_2 - r_1$ is a multiple of b . Given the constraint $r_1, r_2 \in (0, b)$, we can see that $r_2 - r_1 \in [-(b - 1), (b - 1)]$. Therefore it is only possible that $r_2 - r_1 = 0$ is a multiple a multiple of b . Therefore $r_2 = r_1$ and $(q_1 - q_2)b = 0 \Rightarrow q_1 = q_2$.

4.1 What if $b < 0$?

$a = qb + r \Leftrightarrow a = (-q)(-b) + r$. The theorem still works, but $0 \geq r \geq |b|$ needs to be guaranteed.

5 Divisibility in \mathbb{Z}

Definition: Let $d, a \in \mathbb{Z}$, we say that d divides a , written as $d|a$, if $a = qd$ for some $q \in \mathbb{Z}$.

Equivalently: d is a *divisor* of a , a is a *multiple* of d , or a is *divisible* by d .

Some Facts:

- $\forall d \in \mathbb{Z} \quad d|0$ but $0 \nmid a$ unless $a = 0$.
- If d divides $a \neq 0$ then $|d| \leq |a|$. In particular, the set of divisors of a non-zero integer is finite.
- $d|a \Leftrightarrow |d| \mid |a|$

6 GCD in \mathbb{Z}

Definition: Let $a, b \in \mathbb{Z}$, not both 0. The *greatest common divisor* of a and b , $\gcd(a, b)$ is the greatest $d \in \mathbb{Z}$ such that $d|a$ and $d|b$.

Lemmas:

- $(d|a \wedge d|b) \rightarrow d|(a - b)$
- $(d|(a - b) \wedge d|b) \rightarrow d|a$

Note that these lemmas mean that if d is a common divisor of (a, b) then it is equivalent to d is a common divisor of $(b, a - b)$; $\gcd(a, b) = \gcd(b, a - b)$.

7 Bezout's Identity in \mathbb{Z}

Theorem:

Let $g = \gcd(a, b)$. Then $g = ax + by$ for some $x, y \in \mathbb{Z}$.

Proof: Suppose we have two sets:

$$D = \{d \in \mathbb{Z} \mid d|a \wedge d|b\}$$

$$I = \{ax + by \mid x, y \in \mathbb{Z}\}$$

D is the set of all common divisors between a, b and I is the set of all integer combinations of a, b .

From this we make claim (1): If $d \in D$ and $n \in I$, then $d|n$. In particular, if $n \neq 0$, $|d| \leq |n|$.

Since $d \in D$, we have $a = q_1d$ and $b = q_2d$ for some $q_1, q_2 \in \mathbb{Z}$. Similarly, since $n \in I$, we have $n = ax + by$ for some $x, y \in \mathbb{Z}$. We can see that $n = ax + by = q_1dx + q_2dy = d(q_1x + q_2y) \Rightarrow d|n$.

Suppose now we look at $I \cap \mathbb{N}$, the integer multiples of a, b that are natural numbers, we let $n^* = \min(I \cap \mathbb{N}) = ax^* + by^*$.

We proceed to make claim (2) that $n^*|a$ and $n^*|b$ (i.e. $n^* \in D$).

Suppose $n^* \nmid a$, we divide a by n^* to get $a = qn^* + r$, $r \in (0, n^*)$. By definition of n^* , we see that

$$\begin{aligned} r &= a - qn^* \\ &= a - q(ax^* + by^*) \\ &= a - qax^* + qby^* \\ &= a(1 - qx^*) + b(qy^*) \end{aligned}$$

This means that $n^* \in I$ and that contradicts the minimality of n^* as $r \in (0, n^*)$.

Finally, we make our last claim (3): $n^* = \max(D) = \gcd(a, b)$. By claim (2), n^* is a common divisor of a, b . If $d \in D$ is any other common divisor, then $d \leq n^*$ by claim (1). We can see that $d \leq |d| \leq |n^*| = n^*$.

Therefore, we have two interpretations of $\gcd(a, b)$:

- $\gcd(a, b) = \max(D)$
maximal element in set of common divisors
- $\gcd(a, b) = \min(I \cap \mathbb{N})$
smallest positive integer combination of a, b .

8 Euclidean Algorithm

Theorem:

If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof:

It is given that $\gcd(a, b) = \gcd(a - qb, b)$. As $r = a - qb$, we can consider applying the $a - b$ operation q times: $\gcd(a, b) = \gcd(b, a - qb) = \gcd(b, r)$.

Algorithm

Given: (a, b) with $a > b > 0$ and repeatedly apply division theorem on (a, b) . After each division, we replace a with b and b with the remainder of the division:

$$\begin{aligned} (a, b) \quad a &= q_1b + r_1 \\ (b, r_1) \quad b &= q_2r_1 + r_2 \\ (r_1, r_2) \quad r_1 &= q_3r_2 + r_3 \\ &\vdots \\ (r_{k-2}, r_{k-1}) \quad r_{k-2} &= q_k r_{k-1} + r_k \\ (r_{k-1}, r_k) \quad r_{k-1} &= q_{k+1} r_k + 0 \\ (r_k, 0) \end{aligned}$$

The algorithm stops when we reach a point where the second value in the tuple is 0, in which case $\gcd(a, b) = r_k$.

This algorithm is guaranteed to terminate as each of the r_i up to terminating r_k are strictly decreasing natural numbers. By WP there is a minimal element to which this procedure will terminate on.

9 Factoring of Integers

Definition:

An integer $p \neq \pm 1$ is said to be *irreducible* if its only divisors are itself and 1 or -1.

Definition:

An integer $p \neq 0, \pm 1$ is said to be *prime* if for some $a, b \in \mathbb{Z}$, $p|ab$ implies $p|a$ or $p|b$.

Theorem:

If $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of irreducible integers.

Proof:

We will proceed by strong induction. The base case $n = 2$ is irreducible. In the general case, suppose $n > 2$ and the

theorem is true for all $i \in [2, n]$. If n is irreducible, then we are done. Otherwise, $n = ab$ for some $a, b \in [2, n]$, in which case $2 \geq a, b < n$ and a, b are products of primes. A product of products of primes is still a product of primes.

10 Euclid's Lemma

Lemma:

An integer p is prime if and only if p is irreducible.

Proof:

(\Rightarrow): Let p be prime. To show that p is irreducible, suppose $p = ab$ for some $a, b \in \mathbb{Z}$, WTS a or b is ± 1 . As $p = ab$, we know that $p|a$ or $p|b$. WLOG, suppose $p|a$. This means that $a = pd$ for some $d \in \mathbb{Z}$. So, $p = ab = (pd)b$. Suppose we divide $p = (pd)b$ by p , we get $1 = db$. Therefore, $d, b = \pm 1$; p is irreducible.

(\Leftarrow): Let p be irreducible. To show that p is prime, suppose $p|ab$ for some $a, b \in \mathbb{Z}$ and show $p|a$ or $p|b$. As p is irreducible, $\gcd(p, a)$ is either 1 or p . If $\gcd(p, a) = p$, then $p|a$ and we are done. Otherwise, if $\gcd(p, a) = 1$, then by Bezout's Identity, we have $1 = px + ay$ for some $x, y \in \mathbb{Z}$. Therefore,

$$b = b(px + ay) = pbx + aby$$

Note that $p|ab$ is equivalent to saying $ab = pn$ for some $n \in \mathbb{Z}$, we can substitute this in:

$$b = pbx + pny = p(bx + ny)$$

From this we can see that $p|b = p(bx + ny)$; p is prime.

11 Fundamental Theorem of Arithmetic

Theorem:

Let $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of prime numbers. Moreover, given two prime factorizations $n = p_1 \cdots p_k = q_1 \cdots q_l$, $k = l$ and it's possible to re-enumerate q_1, \dots, q_l so that $\forall i \ p_i = \pm q_i$.

Proof:

We proceed by showing existence then uniqueness.

Existence: This is already proven with a previous theorem showing that if $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of irreducible integers. By Euclid's Lemma, we can also say that such n is a product of prime integers.

Uniqueness: Suppose $n = p_1 \cdots p_k = q_1 \cdots q_l$. We proceed by induction on k . For the base case $k = 1$, we have $n = p_1 = q_1$. In the general case, suppose $n = p_1 \cdots p_{k+1} = q_1 \cdots q_l$. We look at p_1 , since $p_1|n = q_1 \cdots q_l$, then $p_1|q_i$ for some i . Therefore $p_1 = \pm q_i$. Suppose we let q_i swap indices with q_1 , then we have $n = p_1 \cdots p_{k+1} = q_1 q_2 \cdots q_l = p_1 q_2 \cdots q_l$. We can divide $p_1 \cdots p_{k+1} = p_1 q_2 \cdots q_l$ by p_1 , which leaves us with $p_2 \cdots p_{k+1} = q_2 \cdots q_l$ and we can repeat this procedure to set $p_j = \pm q_i$ for all remaining j factors in $p_2 \cdots p_{k+1}$.

12 Modular Arithmetic

Let $a\mathbb{Z}$ and $m \in \mathbb{Z} \setminus \{0\}$, where m is commonly referred to as the *modulus*, we explore some definitions:

Definition:

The *residue* of a modulo m is the remainder of a when divided by m .

Definition:

The *congruence class* of a modulo m is defined as the set

$$[a]_m := \{a' \in \mathbb{Z} \mid a \equiv a' \pmod{m}\}$$

We say that a is a *representative* of $[a]_m$.

Congruence classes under the same modulus m are either equal or disjoint. If $x, x' \in [a]_m$, then $x' - x|m$.

Alternatively, we can generate $[a]_m$ in the following way:

$$[a]_m = \{a + km \mid k \in \mathbb{Z}\}$$

Definition:

The integers modulo m , $\mathbb{Z}/m\mathbb{Z}$, is the set of congruence classes modulo m .

13 Algebra and Operations on $\mathbb{Z}/m\mathbb{Z}$

Definition:

In $\mathbb{Z}/m\mathbb{Z}$, addition is defined as

$$[a]_m + [b]_m = [a + b]_m$$

and multiplication is defined as

$$[a]_m \cdot [b]_m = [ab]_m$$

Definition:

An element x is said to be *invertible* if there exists an element y such that $[xy]_m = [1]_m$. We say x and y are multiplicative inverses

Definition:

An element x is said to be a *zero divisor* if $x \neq 0$ and there exists an element $y \neq 0$ such that $[xy]_m = [0]_m$

14 Theorems about $\mathbb{Z}/m\mathbb{Z}$

Theorem:

An element of $\mathbb{Z}/m\mathbb{Z}$ cannot be both an invertible element and a zero divisor.

Proof:

Suppose $[a]_m$ is invertible, then there exists $[a']_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m [a']_m = [1]_m$. Suppose that also $[a]_m [b]_m = [0]_m$ for some $b \in \mathbb{Z}/m\mathbb{Z}$. Suppose we multiply $[a]_m [b]_m = [0]_m$ by $[a']_m$, we have

$$\begin{aligned} [a]_m [b]_m &= [0]_m \\ ([a']_m [a]_m) [b]_m &= [a']_m [0]_m \\ [b]_m &= [0]_m \end{aligned}$$

Therefore, the only possible b that satisfies $[a]_m [b]_m = [0]_m$ is 0, therefore $[a]_m$ cannot be both invertible and a zero divisor.

Theorem:

In $\mathbb{Z}/m\mathbb{Z}$, multiplicative inverses are unique whenever they exist.

Proof:

Let $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ be an invertible element and suppose $[a]_2$ has two inverses b_1, b_2 :

$$[a]_m[b_1]_m = [1]_m \quad [a]_m[b_2]_m = [1]_m$$

We can attempt to evaluate $[b_1]_m[a]_m[b_2]_m$:

$$([b_1]_m[a]_m)[b_2]_m = [b_2]_m \quad [b_1]_m([a]_m[b_2]_m) = [b_1]_m$$

We can see that depending on the order of operations taken, we get either b_1 or b_2 . but as $[b_1]_m[a]_m[b_2]_m$ is always the same value, we can conclude that $b_1 = b_2$.

Theorem:

$[a]_m$ is an invertible class $\Leftrightarrow \gcd(a, m) = 1$

Proof:

(\Rightarrow): If $[a]_m$ is invertible, then there exists $[b]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m[b]_m = [1]_m$. We can see that $ab = 1 + km$ for some $k \in \mathbb{Z}$. We can rearrange this to $ab + (-k)m = 1$. As the $\gcd(a, m)$ is the smallest natural number to $ax + my$, we have $ab + (-k)m = 1$ so $\gcd(a, m) = 1$.

(\Leftarrow): The same logic applies but in the reverse direction.

Theorem:

$[a]_m$ is a zero divisor $\Leftrightarrow \gcd(a, m) > 1$

Proof:

(\Rightarrow): If $[a]_m$ is a zero divisor, $[a]_m$ is not invertible (by previous theorem: an element cannot be both invertible and zero divisor). So $\gcd(a, m) \neq 1$. As $\gcd(a, m) \in \mathbb{N}$ and $\gcd(a, m) \neq 1$, $\gcd(a, m) > 1$.

(\Leftarrow): Suppose $\gcd(a, m) = g > 1$, let $b = m/g$. If we take the product $ab = a \cdot (m/g) = m \cdot (a/\gcd(a, m))$, we can see that $ab|m$ or $[a]_m[b]_m = [0]_m$; $[a]_m$ is a zero divisor.

Theorem:

If $[a] \in \mathbb{Z}/m\mathbb{Z}$ is invertible and $[b] \in \mathbb{Z}/m\mathbb{Z}$ is arbitrary, then the equation

$$[a]_m x = [b]_m$$

has exactly one solution. Namely, $x = [a]^{-1}_m [b]_m$.

Proof:

We can show the uniqueness of the solution by solving:

$$\begin{aligned} [a]_m x &= [b]_m \\ ([a]^{-1}_m [a]_m) x &= [a]^{-1}_m [b]_m \\ [1]_m x &= [a]^{-1}_m [b]_m \end{aligned}$$

Therefore, x must be $[a]^{-1}_m [b]_m$.

15 Invertible elements in $\mathbb{Z}/m\mathbb{Z}$

Definition:

The set of invertible elements of $\mathbb{Z}/m\mathbb{Z}$ is denoted as $(\mathbb{Z}/m\mathbb{Z})^\times$ or $(\mathbb{Z}/m\mathbb{Z})^*$:

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{[a]_m \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$$

Definition:

The cardinality of $(\mathbb{Z}/m\mathbb{Z})^\times$ is denoted $\phi(m)$, where ϕ is the Euler Totient function. ϕ has the following properties:

(1) If $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$

(2) If p is prime and $k \geq 1$, then $\phi(p^k) = (p-1)p^{k-1}$

We proceed to prove these properties of ϕ :

Proof(taken from HW3 Q2):

(1): In $\mathbb{Z}/mn\mathbb{Z}$ where $\gcd(m, n) = 1$, the element $[a]_{mn}$ is invertible if and only if $[a]_m$ and $[a]_n$ are invertible as well. Therefore, each invertible element in $(\mathbb{Z}/mn\mathbb{Z})^\times$ correspond to a pair of elements in $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$; there is a bijection between $(\mathbb{Z}/m\mathbb{Z})^\times$ and $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

Therefore $\phi(mn) = \#((\mathbb{Z}/mn\mathbb{Z})^\times) = \#((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times) = \#((\mathbb{Z}/m\mathbb{Z})^\times) \cdot \#((\mathbb{Z}/n\mathbb{Z})^\times) = \phi(m)\phi(n)$.

(2): We wish to count all elements in $\mathbb{Z}/p^k\mathbb{Z}$ that are invertible. Since we are working with a prime number p , it would be easier to count all zero-divisors instead. Namely, only the values $p, 2p, 3p, \dots$ divide into p^k since p is prime. Out of a total of p^k classes, every p^{th} class is a zero divisor. Therefore there are $p^k/p = p^{k-1}$ zero divisors. Taking this amount (p^{k-1}) out of the total (p^k), we have $\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

Theorem:

If $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ is invertible, then $[a]_m^{\phi(m)} = [1]_m$. Note that this implies that $[a]_m^{\phi(m)-1} = [a]_m^{-1}$ because $[a]_m^{\phi(m)-1}[a]_m = [a]_m^{\phi(m)} = [1]_m$. In the case where m is a prime number p , we have *Fermat's Little Theorem*:

If p is prime and $p \nmid a$, then $[a]_p^{p-1} = [1]_p$ in $\mathbb{Z}/p\mathbb{Z}$.

Proof:

Given $(\mathbb{Z}/m\mathbb{Z})^\times$, we multiply each element by $[a]_m$. If we get $[a]_m[a_i]_m = [a]_m[a_j]_m$, then we multiply by $[a]_m^{-1}$, ensuring every element in $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$ is distinct. If two elements are invertible, their product is invertible as well. Therefore, $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$ is just $(\mathbb{Z}/m\mathbb{Z})^\times$ with rearranged elements. Now we take the product over $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$:

$$\begin{aligned} \prod_{i \in [a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times} i &= [a]_m^{\#((\mathbb{Z}/m\mathbb{Z})^\times)} \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} i \\ &= [a]_m^{\phi(m)} \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} i \\ &= [a]_m^{\phi(m)} [1]_m \\ &= [a]_m^{\phi(m)} \\ &= [1]_m \end{aligned}$$

Notice that as $(\mathbb{Z}/m\mathbb{Z})^\times$ contains both invertible elements are their inverses, the product over every element in $(\mathbb{Z}/m\mathbb{Z})^\times$ would simply equal to $[1]_m$. From this we can see that $[a]_m^{\phi(m)} = [1]_m$.

16 Polynomials

Definition:

A polynomial is a formal (symbolic) algebraic expression. A polynomial f in the variable/symbol x is of the form

$$f = \sum_{i \geq 0} a_i x^i$$

where each a_i is said to be a *coefficient* of the corresponding x^i term. It is critical to note that x is a symbol and not an element of whatever number system f is in.

Addition, subtraction, and multiplication are defined in the standard way. Two polynomials are said to be equal if and only if their coefficients are the same.

Definition:

A polynomial f is said to be *monic* if its leading coefficient is equal to 1.

Definition:

The set of polynomials in x with coefficients in a given number system \mathbb{S} is denoted as $\mathbb{S}[x]$, we call this set \mathbb{S} *adjoin* x . For example, the set of all polynomials with coefficients in \mathbb{Q} is denoted $\mathbb{Q}[x]$. Common polynomial number systems include $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$.

Definition:

The *degree* of a polynomial f , denoted by $\deg(f)$, is the largest n such that $a_n \neq 0$. If $f = 0$ (zero polynomial), then by convention $\deg(f) = -\infty$.

Theorem:

Let f, g be polynomials over \mathbb{Q}, \mathbb{R} , or \mathbb{Z} , then

- (1) $\deg(f + g) \leq \max(\deg(f), \deg(g))$
- (2) $\deg(fg) = \deg(f) + \deg(g)$

By (2), there are no zero divisors in $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{Z}[x]$. If the coefficient number system has zero divisors (ex. $\mathbb{Z}/m\mathbb{Z}$), then (2) does not hold.

17 The Division Theorem in $\mathbb{Q}[x]$

Theorem:

Let $f, g \in \mathbb{Q}[x]$ with $g \neq 0$. When dividing f by g , there exists unique polynomials $q, r \in \mathbb{Q}[x]$ such that:

- $f = gq + r$
- $\deg(r) < \deg(g)$

Proof:

Existence: We proceed by strong induction on $\deg(f)$.

In the base case we have $\deg(f) < \deg(g)$, we take $q = 0$, $r = f$, in which case $f = gq + r = 0 + f$, and this satisfies $\deg(r) < \deg(g)$.

In the inductive step, suppose $\deg(f) \geq \deg(g)$ and existence of q, r is known for all lower degrees of f . We can cancel off the leading term of f with one step of division:

Let f have the leading term $a_n x^n$ and g have the leading term $b_m x^m$. We can define a lower degree polynomial

$$\tilde{f} := f - \left(\frac{a_n}{b_m} x^{n-m} \right) \cdot g$$

Note that the coefficient $\frac{b_m}{a_n}$ is valid in \mathbb{Q} .

By induction, the existence statement applies to \tilde{f} : there exists \tilde{q}, \tilde{r} such that $\tilde{f} = \tilde{q}g + \tilde{r}$ and $\deg(\tilde{r}) < \deg(g)$. So, we rewrite f in terms of g and show that q, r exists:

$$\begin{aligned} f &= \tilde{f} + \left(\frac{a_n}{b_m} x^{n-m} \right) \cdot g \\ f &= (\tilde{q}g + \tilde{r}) + \left(\frac{a_n}{b_m} x^{n-m} \right) \cdot g \\ f &= \tilde{q}g + \left(\frac{a_n}{b_m} x^{n-m} \right) \cdot g + \tilde{r} \\ f &= \left(\tilde{q} + \frac{a_n}{b_m} x^{n-m} \right) \cdot g + \tilde{r} \end{aligned}$$

Letting $q = \tilde{q} + \frac{a_n}{b_m} x^{n-m}$ and $r = \tilde{r}$, we can see that we have satisfied the existence of q, r for f .

Uniqueness: Suppose (q_1, r_1) and (q_2, r_2) both satisfy $f = q_i g + r_i$ and $\deg(r_i) < \deg(g)$. We have $f = q_1 g + r_1 = q_2 g + r_2$. Alternatively, $f/g = q_1 + r_1/g = q_2 + r_2/g$. We require that $\deg(q_1) = \deg(q_2)$, so $r_1/g = r_2/g$. This implies that $r_1 = r_2$. In turn, this also implies that $q_1 = q_2$.

18 Divisibility in Polynomials

Definition:

Given polynomials f, g , we say that $f|g$ if $g = qf$ for some $q \in \mathbb{Q}[x]$. This implies that $\deg(f) \leq \deg(g)$ if $g \neq 0$, which is useful for induction.

Definition:

Given polynomials f, g , we say that f and g are associates if $f|g$ and $g|f$. This means that $f = cg$ for some $c \in \mathbb{Q}$, so we can have $g = \frac{1}{c}f$.

Associate elements have the same divisors, which matters in uniqueness of factorization.

Definition:

Let f be a polynomial of degree greater than 0. We say that f is *prime* if $f|gh$ implies $f|g$ or $f|h$.

Further, we say that f is *irreducible* if its only divisors are associates of 1 and itself. Equivalently, f cannot be factored as $f = ab$ where $1 \leq \deg(a), \deg(b)$.

From this definition we can see that every polynomial of degree 1 is irreducible.

19 Evaluating Polynomials as a Function

Since the arithmetic operations on polynomials are compatible with the operations on functions, we can evaluate $f \in \mathbb{Q}[x]$ at any element $a \in \mathbb{Q}$.

We can say that equality of polynomials implies equality of functions. However, the converse is not true for over all number systems.

Definition:

We say that $a \in \mathbb{Q}$ is a *root* of f if and only if $f(a) = 0$.

20 Root Theorem

Theorem:

Let $f \in \mathbb{Q}[x]$, $a \in \mathbb{Q}$. Then a is a root of f iff $(x - a) \mid f$.

Proof:

(\Rightarrow): By the division theorem, there exists $q, r \in \mathbb{Q}[x]$ such that $f = (x - a)q + r$ and $\deg(r) < \deg(x - a)$. Assume a is a root of f , then $f(a) = 0 = (a - a)q(a) + r$, so $r = 0$. Therefore, $f = (x - a)q$.

(\Leftarrow): If $f = (x - a)g$, then $f(a) = (a - a)g(a) = 0$, so a is a root.

Corollary:

A nonzero polynomial of degree d in $\mathbb{Q}[x]$ has at most d distinctive roots.

Proof:

Refer to notes_sep30.2 for full proof. The rough gist is to apply induction on a polynomial f and repeatedly apply root theorem each time to reduce its degree by 1.

Corollary:

If $\deg(f) = \deg(g) = n$ and $f(a) = g(a)$ for all $n + 1$ distinct values of a , then $f = g$.

Proof:

Refer to notes_sep30.2 for full proof; or look at it from the linear algebra.

Corollary:

If $f, g \in \mathbb{Q}[x]$ are equal as functions (i.e. $\forall a \in \mathbb{Q} \ f(a) = g(a)$), then $f = g$ in $\mathbb{Q}[x]$. Here, Equality of functions implies equality of polynomials, but only for $\mathbb{Q}[x]$.

21 Polynomial Theorems

Theorem:

Given polynomials f, g , $\gcd(f, g)$ is a common divisor h of **greatest degree**. That is if \tilde{h} is any other common divisor, $\deg(h) \geq \deg(\tilde{h})$.

Note that if h is a gcd of f and g , so is any associate of h . If we are referring to the gcd of two polynomials, we mean the unique monic associate.

Theorem:

If h is a gcd of f and g , there exist polynomials $v, w \in \mathbb{Q}[x]$ such that $h = vf + wg$. Moreover, every nonzero polynomial of the form $\tilde{v}f + \tilde{w}g$ is divisible by h .

Theorem:

A polynomial is *prime* iff it is *irreducible*.

Note that this is essentially Euclid's lemma for $\mathbb{Q}[x]$.

Theorem:

Let $f \in \mathbb{Q}[x]$, f is a product of prime/irreducible polynomials. Moreover, given two such factorizations, it is possible to reorder the factors so that the two factorizations match up to an associate.

This is the unique factorization theorem for $\mathbb{Q}[x]$. The proof for this theorem is similar to that of the integers.

Theorem:

If f factors in $\mathbb{Z}[x]$ and $\deg(f) = \deg(\bar{f})$, then \bar{f} is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$.

The proof for this theorem is omitted but the key insight this theorem brings is that we can work with the contrapositive of this theorem: If a polynomial \bar{f} is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Z}[x]$. This resets the amount of possible elements to check for the root theorem down to p , rather than an infinite amount.

22 Gauss's Lemma

Lemma:

Suppose f is reducible over $\mathbb{Q}[x]$, then f also factors over $\mathbb{Z}[x]$, where each factors are associates of each other.

The proof is omitted for this lemma, but as a rough idea behind this proof is that an irreducible factor in $\mathbb{Q}[x]$ could be rewritten as a product between an irreducible factor in $\mathbb{Z}[x]$ and a constant. (ex. $(x-1/2) = 1/2(2x-1)$)

23 Rational Root Theorem

Theorem:

Let $f = \sum_i a_i x^i \in \mathbb{Z}[x]$, suppose $f(r) = 0$ for some $r \in \mathbb{Q}$, and $r = a/b$ in lowest terms (ie. $\gcd(a, b) = 1$). Then $a \mid a_0$ (a divides the constant term of f) and $b \mid a_n$ (b divides the leading coefficient of f).

Proof:

By the root theorem, $f = (x - \frac{a}{b})g$ for some $g \in \mathbb{Q}[x]$. By Gauss's lemma, $f = (bx - a)g'$ for some $g' \in \mathbb{Z}[x]$. We can distribute the factor to get $f = bg'x - ag'$. Therefore, the leading term of f will have a factor of b , and similarly the constant term of f will have a factor of a .

24 Ring terminologies

Definition:

If X, Y are sets, the Cartesian product of X and Y is the set of ordered pairs

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

Definition:

A *binary operation* on a set S is a function $*$: $S \times S \mapsto S$. This means that $*$ takes an ordered pair $(s, t) \in S \times S$ and outputs $*(s, t) \in S$. This is usually written in infix notation $s * t$.

Let $*$ be a binary operation on S :

- $*$ is *commutative* if $\forall s, t \in S, s * t = t * s$
- $*$ is *associative* if $\forall s, t, u \in S, (s * t) * u = s * (t * u)$
- An element $e \in S$ is an *identity element* of $*$ if $\forall s \in S, e * s = s * e = s$
- Suppose $*$ has an identity element e , given $s \in S$, an element $t \in S$ is an *inverse* of s if $s * t = t * s = e$

25 Groups

Definition:

A *group* is an ordered pair $(G, *)$, where G is a set and $*$ is a binary operation on G with the following conditions:

- $*$ is associative
- There exists an identity element for $*$
- For every $g \in G$, there exists an inverse

Note that in the context of groups, $*$ is usually called the *multiplication* operator.

In a group, $*$ is not required to be commutative. If $*$ happens to be commutative, then said group is an *abelian* or commutative group.

Theorem:

Let $(G, *)$ be a group, then the following holds:

- (1) The identity element of G is unique
- (2) The inverse of each element is unique

Note that (2) justifies using g^{-1} to denote the inverse of an element $g \in G$.

Proof:

- (1) Suppose we have two identities $e, e' \in G$, then

$$e = e * e' = e'$$

- (2) Suppose we have an element $g \in G$ and let $g, g'' \in G$ both be inverses of g . Then we have the following:

$$\begin{aligned} & g' * g * g'' \\ &= (g' * g) * g'' \\ &= (e) * g'' \\ &= g'' \end{aligned}$$

Now proceed in the other direction by associativity:

$$\begin{aligned} & g' * g * g'' \\ &= g' * (g * g'') \\ &= g' * (e) \\ &= g' \end{aligned}$$

Therefore, $g' = g''$.

Theorem:

Let $(G, *)$ be a group.

Cancellation: Let $a, b, c \in G$. $a * b = a * c \Rightarrow b = c$.

Proof:

Let $a, b, c \in G$ and suppose $a * b = a * c$:

$$\begin{aligned} a * b &= a * c \\ a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

26 Rings

Definition:

A *ring* is an ordered triple $(R, +, *)$ where R is a set and $+, *$ are binary operations (commonly referred to as addition and multiplication, respectively) on S such that:

- $(R, +)$ is an abelian group
 - $+$ is associative
 - $+$ is commutative
 - $+$ has an identity, denoted 0
 - Every $r \in R$ has an additive inverse $-r$
- $*$ is associative
- $*$ distributes over addition: For every $a, b, c \in R$, $a * (b + c) = a * b + a * c$

Note that for the ring $(R, +, *)$, $*$ is not required to be commutative, if it is commutative, then $(R, +, *)$ is a commutative ring.

Definition:

If $(R, +_R, *_R)$ and $(S, +_S, *_S)$ are rings, we can define $R \times S$, a *direct product* on R and S by:

- $(r, s) + (r', s') = (r +_R r', s +_S s')$
- $(r, s) * (r', s') = (r *_R r', s *_S s')$

$R \times S$ is a ring as well.

Theorem:

Let $(R, +, *)$ be a ring:

- (1) For all $r \in R$, $0 * r = r * 0 = 0$
- (2) For all $r, s \in R$, $(-r) * s = r * (-s) = -(r * s)$
- (3) For all $r \in R$, $-(-r) = r$

Proof:

- (1) As 0 is the additive inverse, we have $0 = 0 + 0$. Therefore, $0 * r = (0 + 0) * r$. After distribution, we have $0 * r = 0 * r + 0 * r$, and so $0 = 0 * r$. The same argument goes for the $r * 0$ case.
- (2) WTS $(-r) * s = -(r * s)$. By definition of additive inverses, $r + (-r) = 0$. Suppose we multiply by s , we have $(r + (-r)) * s = 0 * s = 0$.

$$\begin{aligned} r + (-r) &= 0 \\ (r + (-r)) * s &= 0 \\ r * s + (-r) * s &= 0 \\ (-r) * s &= -(r * s) \end{aligned}$$

- (3) By uniqueness of additive inverses (of groups; recall that $(R, +)$ is an abelian group), the inverse of an inverse is the element itself.

27 Subrings

Definition:

Let R be a ring, a *subring* of R is a subset $S \subseteq R$ that is, itself, a ring under the same $(+, \cdot)$ operations as R .

Lemma:

Let S be a subring of R , then

- (1) $0_R = 0_S$ (same additive identity)
- (2) If $r \in S$ then $(-r)_R = (-r)_S$ (same inverse)

Proof:

- (1) $0_S + 0_S = 0_S = 0_S + 0_R$. By additive cancellation in R , $0_S = 0_R$.
- (2) Let $r \in S \subseteq R$, r has an additive inverse $(-r)_S \in S$ since S is a ring. By definition, this means $r + (-r)_S = 0_S$. By (1) we can see that that also $r + (-r)_S = 0_R$. By uniqueness of additive inverses, $(-r)_S = (-r)_R$.

27.1 Subring Criterion

Theorem:

Let $S \subseteq R$, S is a subring iff:

- (1) $0 \in S$
- (2) S is closed under addition and multiplication
- (3) If $r \in S$, then $-r \in S$

Alternatively, we can rephrase the theorem by the following conditions:

- (a) S is closed under subtraction
- (b) S is closed under multiplication

28 Unity

Definition:

Let R be a ring. R is a ring with *unity* if R has a multiplicative identity denoted $1 \in R$ and called *one* or *unity*. This means that for all $r \in R$, $1 \cdot r = r \cdot 1 = r$. Rings with no unity is sometimes called a rng.

Lemma:

Let R be a ring with unity:

- The multiplicative identity is unique
- For all $r \in R$, $(-1) \cdot r = -r = r \cdot (-1)$
- If R is not the zero ring, then $1 \neq 0$

29 Unity and Subrings

If S is a subring of R , it may happen that:

- R has unity and S doesn't.
ex. $2\mathbb{Z} \subseteq \mathbb{Z}$
- R does not have unity, but S does.
ex. $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times 2\mathbb{Z}$
- R and S have different unities; $1_R \neq 1_S$
ex. $[2]\mathbb{Z}/10\mathbb{Z} \subseteq \mathbb{Z}/10\mathbb{Z}$.

Note that $[2]\mathbb{Z}/10\mathbb{Z}$ is all the even elements in $\mathbb{Z}/10\mathbb{Z}$, and its unity is $[6]$.

30 Zerodivisors and Invertibility in Rings

Definition:

Let R be a ring, an element $r \neq 0 \in R$ is a zero divisor if there exists $s \neq 0 \in R$ such that $rs = 0$ or $sr = 0$.

Definition:

Let R be a ring with *unity*, an element $r \in R$ is a unit or invertible if there exists $s \in R$ such that $rs = sr = 1$

Lemma:

Let R be a ring with unity, and element R cannot be both a zero divisor and a unit.

The proof for this lemma is in similar structure to that of the same statement in $\mathbb{Z}/m\mathbb{Z}$.

31 Homomorphisms and Isomorphisms

Definition:

A function $f : x \mapsto y$ is said to be *injective* if

$$\forall x, x' \in X, f(x) = f(x') \Rightarrow x = x'$$

Definition:

A function $f : x \mapsto y$ is said to be *surjective* if

$$\forall y \in Y, \exists x \in X, s.t. y = f(x)$$

Definition:

A function $f : x \mapsto y$ is said to be *bijective* if it is both an injection and a surjection.

Definition:

Suppose $(R, +, \cdot)$ and (S, \oplus, \odot) are rings. A function $f : R \mapsto S$ is a ring *homomorphism* if for all $r_1, r_2 \in R$,

- $f(r_1 + r_2) = f(r_1) \oplus f(r_2)$: (f preserves addition)
- $f(r_1 \cdot r_2) = f(r_1) \odot f(r_2)$: (f preserves multiplication)

We say that f is a ring *isomorphism* and write $f : R \xrightarrow{\sim} S$ if f is a bijective ring homomorphism.

If there exists an isomorphism $R \xrightarrow{\sim} S$, we say that R and S are isomorphic: $R \cong S$.

Proposition:

Let $f : R \mapsto S$ be a ring homomorphism:

- $f(0) = 0$
- for any $r \in R$, $f(-r) = -f(r)$
- If R, S both have unity and $f(1) = 1$, then for all units $u \in R$, $f(u)$ is a unit and $f(u)^{-1} = f(u^{-1})$
- If, in addition to f , there is another ring homomorphism $g : S \mapsto T$, then the composition $g \circ f : R \mapsto T$ is also a homomorphism.

32 Integral Domains and Fields

Suppose R is a commutative ring with unity with $1 \neq 0$:

Definition:

R is an *integral domain* if R has no zero divisors.

Definition:

R is a *field* if every non-zero element of R is a unit.

As units can't be zero divisors, R being a field implies it is also an integral domain. The converse is not true. In a sense, R being a field is a stronger statement.

Lemma:

An element $r \neq 0 \in R$ is not a zero divisor iff *multiplicative cancellation* holds for r , that is:

$\forall a, b \in R, ra = rb \Rightarrow a = b$ and $ar = br \Rightarrow a = b$.

Proof:

(\Rightarrow): Suppose $r \neq 0 \in R$ is not a zero divisor.

to show the cancellation laws hold, suppose $a, b \in R$ and $ra = rb$. Move everything on one side to obtain $ra - rb = 0$. We can write as $r(a - b) = 0$ by distributivity. Since $r \neq 0$ and r is not a zero divisor, $a - b = 0$. therefore, $a = b$.

(\Leftarrow): Suppose that the multiplicative cancellation laws hold, and given $r \neq 0 \in R$ and $s \in R$ with $rs = 0$.

WTS $s = 0$: We know that $rs = 0$, and $r \cdot 0 = 0$.

Therefore $rs = r \cdot 0$, and by cancellation $s = 0$.

Theorem:

A finite integral domain is a field.

Proof:

Suppose R is a finite integral domain with elements $\{r_1, \dots, r_n\}$, note that $0, 1 \in R$.

To show that R is a field, let $r \neq 0 \in R$.

Since r is not a zero divisor, the elements rr_1, rr_2, \dots, rr_n must all be distinct. This means that those elements are just elements of R again in a different order.

So, $rr_i = 1$ for some i , so r is a unit.

33 Ring Characteristic

Definition:

Let R be a ring with unity, the *characteristic* for R , $\text{char}(R)$ is the smallest $n \in \mathbb{N}$ such that $n \cdot 1 = 0$. If no such n exists, then the characteristic is 0.

Similarly, $\text{char}(R)$ can also be defined as the smallest $n \in \mathbb{N}$ such that $nr = 0$ for every $r \in R$, with $n = 0$ if no such n exists. This definition is sometimes used when the ring in question has no unity.

Lemma:

If R is an integral domain, $\text{char}(R)$ is 0 or a prime $p \in \mathbb{Z}$.

Proof:

By contrapositive, if $\text{char}(R) = n$ where n is nonzero and not prime, then $n = ab$ for some $1 < a, b < n$: $n \cdot 1 = a \cdot b = 0$, so R is not an integral domain.

Corollary:

A finite field R has $\text{char}(R) = p > 0$ where p is prime.

Proof:

The prime aspect is covered in the lemma above. We still proceed with a contrapositive: The characteristic can't be 0 or else the elements $1, 1 + 1, 1 + 1 + 1, \dots$ would all be distinct, and that implies R is infinite.

34 Polynomial Rings

Definition:

The ring of polynomials with coefficients in R (a commutative ring with unity) is

$$R[x] = \left\{ \sum_{i=0}^n r_i x^i \mid n \geq 0 \in \mathbb{Z}; \forall i, r_i \in R \right\}$$

Theorem:

$R[x]$ is a commutative ring with unity.

Theorem:

If R is an integral domain, so is $R[x]$.

Proof:

In rough strokes: Suppose f, g have nonzero leading terms $f_n x^n$ and $g_m x^m$, the product fg will have the leading term $f_n g_m x^{n+m}$. Since R is an integral domain, the product $f_n g_m \neq 0$. the same applies to any term in fg .

35 Polynomials over a field

Suppose F is a field, $F[x]$ shares many properties that $\mathbb{Q}[x]$ has, as \mathbb{Q} is a field; $\mathbb{Q}[x]$ is an instance of $F[x]$.

35.1 Division theorem for $F[x]$

Theorem:

Let $f, g \in F[x], g \neq 0$. Then there exist unique polynomials $q, r \in F[x]$. such that $f = gq + r$ and $\deg(r) < \deg(g)$.

Proof:

The proof is the same structure as for the division theorem in $\mathbb{Q}[x]$. Given that F is a field, the coefficients of f, g have multiplicative inverses. Instead of the expression $f - \frac{a_n}{b_m} \cdot g$ we would instead have $f - a_n b_m^{-1} \cdot g$ instead.

35.2 Overview

The properties in $F[x]$ matches with many in $\mathbb{Q}[x]$, with the same proofs:

- Bezout's Identity
- Euclidean Algorithm
- Euclid's Lemma

- Unique Factorization
- Root Theorem

36 Irreducibility over $\mathbb{R}[x]$, $\mathbb{C}[x]$

Definition:

A field F is *algebraically closed* if every non constant polynomial $f \in F[x]$ has a root in F .

For such F , the only irreducible polynomials are linear. Every $f \in F[X]$ of $\deg(f) \geq 1$ splits into linear factors.

Theorem:

The Fundamental theorem of Algebra:

\mathbb{C} is an algebraically closed field.

There is no purely algebraic proof of this theorem, and requires complex analysis.

Theorem:

The irreducible monic polynomials in $\mathbb{R}[x]$ are:

- linear polynomial $x - r$; $r \in \mathbb{R}$
- quadratic polynomials $x^2 + rx + s$; $r, s \in \mathbb{R}$
with $r^2 - 4s \leq 0$ (negative discriminant)

Proof:

Let $f \in \mathbb{R}[x]$ with $\deg(f) \geq 1$. WTS f has a linear or irreducible quadratic factor. (By induction on $\deg(f)$, this implies that all the factors of f are of this form).

By the Fundamental Theorem of Algebra, f has a root $z \in \mathbb{C}$. In which case there are two cases:

(1): If $\text{Im}(z) = 0$; $z \in \mathbb{R}$, then by the root theorem for $\mathbb{R}[x]$, $f = (x - z)g$ for some $g \in \mathbb{R}[x]$.

(2): If $\text{Im}(z) \neq 0$, then $f(z) = 0 = \sum_{i=0}^n a_i x^i$. Suppose we apply complex conjugation σ , we have:

$$\begin{aligned} f(z) = 0 &= \sum_{i=0}^n a_i z^i \\ \sigma(0) = 0 &= \sigma\left(\sum_{i=0}^n a_i z^i\right) \\ &= \sum_{i=0}^n \sigma(a_i z^i) \\ &= \sum_{i=0}^n a_i \sigma(z^i) \\ &= f(\sigma(z)) \end{aligned}$$

Therefore, z is a root to f and so is $\sigma(z)$. In $\mathbb{C}[x]$, f has $(x - z)$ and $(x - \sigma(z))$ as roots:

$$f = (x - z)(x - \sigma(z))g; \quad g \in \mathbb{C}[x]$$

If $z = a + bi$, then $(x - z)(x - \sigma(z)) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$, an irreducible polynomial.

By uniqueness of division theorem, the quotient and remainder of f when divided by $x^2 - 2ax + (a^2 + b^2)$ in $\mathbb{R}[x]$ are the same as in $\mathbb{C}[x]$. So, we have shown that a quadratic factor exists for f .

37 Ideals

Definition:

Let R be a commutative ring, an *ideal* is a subset $i \subseteq R$ such that:

- $0 \in I$
- $r, s \in I \Rightarrow (r + s \in I \wedge -r \in I)$
- $(\forall r \in I \wedge \forall s \in R) \Rightarrow rs \in I$

An ideal is usually denoted as $\langle x \rangle$ (most common), (x) , or xR , where $\langle x \rangle$ is a *principal ideal* with *generator* x :

$$\langle x \rangle := \{x \cdot r \mid r \in R\} \subseteq R$$

An ideal can have multiple generators:

$$\langle a_1, \dots, a_n \rangle = \{r_1 a_1 + \dots + r_n a_n \mid r_1, \dots, r_n \in R\}$$

It is noteworthy that $1 \in I \Rightarrow I = R$.

Proposition:

Suppose R is a commutative ring with unity, then the following properties hold:

- Let $r, s \in R$, $s \in \langle r \rangle$ iff $\langle s \rangle \subseteq \langle r \rangle$
- Let $r \in R$, $\langle r \rangle = R$ iff r is a unit
- If R is an integral domain and $r, s \in R$, then $\langle r \rangle = \langle s \rangle$ iff $r = s \cdot u$ for some unit u

Proposition:

Let R be a commutative ring and $I, J \subseteq R$ ideals.

Then the sets $I \cap J$ and $I + J$ are ideals, where

$$I + J = \{x + y \mid x \in I, y \in J\} \subseteq R$$

38 Principal Ideal Domains

Theorem:

In \mathbb{Z} , $\mathbb{Q}[x]$, $F[x]$ where F is a field, every ideal is principal. Such rings are principal ideal domains (PID's)

Proof:

We proceed with $F[x]$. Let $I \subseteq F[x]$ be an ideal.

If $I = \{0\}$, then $I = \langle 0 \rangle$, which is principal.

Otherwise let $f \in I$ be a nonzero element of minimal degree. Claim: $\langle f \rangle = I$

(\subseteq): Let $g \in \langle f \rangle$, say $g = f \cdot q$ for some $q \in F[x]$. $g \in I$ by absorption under multiplication.

(\supseteq): Let $g \in I$. By the division theorem we have $g = f \cdot q + r$ for some $q, r \in F[x]$ and $\deg(r) < \deg(f)$. Then $r = g - f \cdot q \in I$. As r has lower degree than f , $r = 0$ is required. therefore, $g = f \cdot q \in \langle f \rangle$.

39 Quadratic Extensions of \mathbb{Z}

Definition:

An integer $n \in \mathbb{Z}$ is *square-free* if n has no non-trivial square divisors.

Lemma:

$\mathbb{Z}[\sqrt{n}]$ is a subring of \mathbb{C} . If $n > 0$, then $\mathbb{Z}[\sqrt{n}] \subset \mathbb{R}$.

40 Norms & Conjugation

Definition:

A complex conjugation $\sigma : \mathbb{C} \mapsto \mathbb{C}$ is a ring isomorphism

$$\sigma(a + bi) = a - bi$$

Using conjugation we can write down the inverse of an element in \mathbb{C} :

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2}$$

Note that $(a + bi)(a - bi) = a^2 + b^2$, which is sometimes referred to as the *norm* of $a + bi$.

In a struction light, let $\alpha = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

Let the *norm* of α be defined as

$$N(\alpha) := |\alpha \cdot \sigma(\alpha)| = |a^2 - b^2n|$$

Proposition:

For all $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$, $N(\alpha\beta) = N(\alpha)N(\beta)$

Proof:

$$\begin{aligned} N(\alpha\beta) &= |\alpha\beta \cdot \sigma(\alpha\beta)| \\ &= |\alpha\beta \cdot \sigma(\alpha)\sigma(\beta)| \\ &= |\alpha\sigma(\alpha)| \cdot |\beta\sigma(\beta)| \\ &= N(\alpha)N(\beta) \end{aligned}$$

40.1 Units

Suppose $\alpha = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ and α is a unit. Then there exists $\beta \in \mathbb{Z}[\sqrt{n}]$ such that $\alpha\beta = 1$. If we apply the norm, we would have

$$N(\alpha\beta) = N(1) = 1 \cdot 1 = 1$$

Therefore $N(\alpha) = a^2 - b^2n = 1$. Therefore (a, b) satisfies the *Diophantine equation* $a^2 - b^2n = 1$ for any integers a, b .

Theorem:

If $n < -1$, then the only units in $\mathbb{Z}[\sqrt{n}]$ are ± 1 .

In reference to the Diophantine equation above, suppose $n < -1$ then we need to find a, b such that $a^2 + b^2n = 1$ holds, and the only possible solutions are $(a, b) = (\pm 1, 0)$.

Theorem:

An element $\alpha \in \mathbb{Z}[\sqrt{n}]$ is a unit iff $N(\alpha) = 1$.

Theorem:

$\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

Proof:

If α and β are units, so is $\alpha\beta$. There $(1 + \sqrt{2}), (1 + \sqrt{2})^2, (1 + \sqrt{2})^3, \dots$ are all distinct units.

41 Factorization in $\mathbb{Z}[\sqrt{n}]$

In any integral domain, associates, irreducible, and prime elements can be defined.

Factorization is complicated in non-integral domains because multiplicative cancellation does not hold. However, $\mathbb{Z}[\sqrt{n}]$ is an integral domain.

Definition:

Let R be an integral domain.

$r, s \in R$ are *associates* if $r = s \cdot u$ for some $u \in R$.

$r \in R$ is said to be *irreducible* if $r \neq 0$, and whenever $r = a \cdot b$ which $a, b \in R$, then either a or b is unit.

Theorem:

Let $\alpha \in \mathbb{Z}[\sqrt{n}]$. Suppose $N(\alpha)$ is a prime integer, then α is irreducible.

Proof:

Suppose $\alpha \in \mathbb{Z}[\sqrt{n}]$ and $N(\alpha) = p$, a prime integer.

To show that α is irreducible, we know that $N(\alpha) > 1$ so α isn't a unit nor 0. Suppose $\alpha = x \cdot y$ for some $x, y \in \mathbb{Z}[\sqrt{n}]$. WTS x or y is unit.

Since $\alpha = x \cdot y$ for some $N(\alpha) = p = N(x) \cdot N(y)$. Since p is prime, then either $N(x) = 1$ or $N(y) = 1$. Therefore, x or y is unit.

Theorem:

Every nonzero non-unit $\alpha \in \mathbb{Z}[\sqrt{n}]$ can be factored into irreducibles.

Proof:

We proceed by induction on $N(\alpha)$. If $N(\alpha) = 2$, then α is irreducible. Otherwise $N(\alpha)$ is prime or composite. Suppose $N(\alpha)$ is prime, then α is irreducible. Otherwise, $\alpha = x \cdot y$ for some $x, y \in \mathbb{Z}[\sqrt{n}]$ and $N(\alpha) = N(x) \cdot N(y)$, where $N(x), N(y) < N(\alpha)$. By strong induction $N(x), N(y)$ are irreducible, so α can be factored into irreducibles.

Definition:

Let R be an integral domain and let $r \in R$.

We say two factorizations of r , $r = a_1 \dots a_n$ and $r = b_1 \dots b_m$ are equivalent if $n = m$ and it's possible to renumber the b_i 's so that for each i , a_i and b_i are associates.

Definition:

Let R be an integral domain, we say that R is a *Unique Factorization Domain* (UFD) if every nonzero nonunit element in R has a unique factorization into irreducibles.

Definition:

Let R be an integral domain and $r \in R$. We say that r is *prime* if (1) r isn't unit or 0, and (2) whenever $r|ab$ with $a, b \in R$, then $r|a$ or $r|b$. Alternatively if $ab \in \langle r \rangle$, then either $a \in \langle r \rangle$ or $b \in \langle r \rangle$.

Proposition:

Let R be an integral domain and $r \in R$. If $r \in R$ is prime, then r is irreducible.

Proof:

To show r is irreducible, suppose $r = xy$. WTS x or y is a unit. We know that $xy \in \langle r \rangle$ since $xy = r \cdot 1$. Since r is prime, $x \in \langle r \rangle$ or $y \in \langle r \rangle$.

Without loss of generality $x \in \langle r \rangle$. So $x = r \cdot z$ for some $z \in R$. This means that $r = xy = rzy$. By cancellation, $r = rzy \Rightarrow 1 = zy$; y is a unit.

Proposition:

Let R be an integral domain and $r \in R$ a nonzero non-unit. Suppose we have two factorizations $r = p_1 \dots p_n$

and $r = q_1 \dots q_m$ for primes $p_i, q_j \in R$. Then the factorizations are equivalent.

So, factorization into prime elements is guaranteed to be unique, up to equivalence. The proof for this proposition is very similar to \mathbb{Z} by induction on n .

If we knew that irreducible elements in $\mathbb{Z}[\sqrt{n}]$ were prime, then $\mathbb{Z}[\sqrt{n}]$ would be a UFD.

42 Factorization and Ideals

There are several properties of elements in terms of ideals:

- r is unit $\Leftrightarrow \langle r \rangle = R$
- $r|s \Leftrightarrow s \in \langle r \rangle \Leftrightarrow \langle s \rangle \subseteq \langle r \rangle$
- If R is an integral domain, $\langle s \rangle = \langle r \rangle \Leftrightarrow r, s$ are associates.

For *irreducible* and *prime* elements, there are similar notions in terms of ideals.

Definition:

Let R be a commutative ring with unity, and let $I \subseteq R$ be an ideal. We say I is a *prime ideal* if:

- $I \neq R$
- whenever $ab \in I$, then $a \in I$ or $b \in I$

Theorem:

Let R be an integral domain, and let $r \neq 0 \in R$. r is prime $\Leftrightarrow \langle r \rangle$ is a *prime ideal*.

Theorem:

Let R be an integral domain and let $r \in R$. r is irreducible iff

- $\langle 0 \rangle \subsetneq \langle r \rangle \subsetneq R$
- If $\langle r \rangle \subsetneq \langle a \rangle \subsetneq R$, either $\langle r \rangle = \langle a \rangle$ or $\langle a \rangle = R$.

$\langle r \rangle$ is said to be maximal among principal ideals in R . Meaning, it is not contained in any strictly larger principal ideal, except for R itself.

If R is an PID, then any irreducible element generates a maximal ideal.

Theorem:

Let R be a commutative ring with unity. R is an integral domain iff $\{0\}$ is a prime ideal.

Proof:

By definition, R is an integral domain iff $1 \neq 0$ (so $R \neq \{0\}$) and R has no zero divisors.

Not having zerodivisors means: if $xy = 0$ then $x = 0$ or $y = 0$. Equivalently, if $xy \in \{0\}$ then $x \in \{0\}$ or $y \in \{0\}$, by definition of a prime ideal.

Theorem:

Let R be a commutative ring with unity. $\{0\}$ is a maximal ideal iff R is a field.

Note that this asserts that in a field, the only ideals are $\{0\}$ and R itself.

Proof:

By definition, R is a field iff $1 \neq 0$ and every $r \neq 0 \in R$ is unit.

(\Rightarrow): Suppose $\{0\}$ is maximal. Let $r \neq 0 \in R$. Then $\{0\} \subsetneq \langle r \rangle \subseteq R$, as $\{0\}$ is maximal, $\langle r \rangle = R$. Therefore r is a unit.

(\Leftarrow): Suppose R is a field. To show $\{0\}$ is maximal, suppose $\{0\} \subseteq J \subseteq R$. WTS $\{0\} = J$ or $J = R$.

Suppose $J \neq \{0\}$, there exists $r \neq 0 \in J$. Therefore $\langle r \rangle \subseteq J$. Since R is a field, r is a unit. Therefore $\langle r \rangle = R$, so $R = J$.

Theorem:

Maximal ideals are prime ideals.

Proof:

Suppose R is a commutative ring with unity and I is a maximal ideal. WTS I is a prime ideal as well.

By definition of maximal ideals, $I \neq R$.

Suppose $ab \in I$ for some $a, b \in R$, WTS $a \in I$ or $b \in I$. The approach is to assume $a \notin I$, then show this implies $b \in I$.

Let $J = I + \langle a \rangle$ be a sum of ideals. Note that $I \subsetneq J$ since $a \in J$ but $a \notin I$.

Since I is maximal, it follows that $J = R$.

In particular $1 \in J$, so $1 = x + ra$ with $x \in I$, $ra \in \langle a \rangle$.

Suppose we multiply both sides by b , we have $b = xb + rab$. $x \in I \Rightarrow xb \in I$ and $ab \in I \Rightarrow rab \in I$, so $b \in I$.

43 Unique Factorization and Ideals

Suppose R is an integral domain. To prove that R is a UFD, we need to show that (1) every nonzero non-unit factors into irreducibles. and (2) irreducible elements are prime.

(1) can be shown by induction on other integral domains. \mathbb{Z} (via $|n|$), $F[x]$ for field F (via $\deg(f)$), and $\mathbb{Z}[\sqrt{n}]$ (via $N(\alpha)$). Each of the examples given above have some scalar quantity that denotes "size" of sorts to perform induction upon.

However, in a general integral domain, there may not always be such scalar quantity, so the inductive argument may not apply. Instead, we take an ideal-centric approach.

Suppose $r \in R$ is a nonzero non unit and it can't be factored into a product of irreducibles (and isn't itself irreducible). Suppose we call such r a *spooky* element.

Suppose $r = ab$, then a, b are *spooky* as well.

To factor r , we would keep on factoring forever and never be finished. So, we can say that $r \in \langle a \rangle$, or $\langle r \rangle \subsetneq \langle a \rangle$.

By the same logic applied to a , suppose $a = a_1c$ and $a_1 = a_2d$ and so on. we can have

$$\langle r \rangle \subsetneq \langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$$

Note that this chain would go on forever, if we are truly dealing with *spooky* elements. However, to rule out the existence of spooky elements, it would be enough to prove that every ascending chain of principal ideals terminates. In more formal terms:

Definition:

For every chain

$$\langle r \rangle \subseteq \langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_3 \rangle \subseteq \dots$$

in R , there exists $k \in \mathbb{N}$ such that $\langle a_k \rangle = \langle a_{k+1} \rangle = \langle a_{k+2} \rangle = \dots$. This is called the Ascending Chain Condition on Principal ideals (ACCP).

Theorem:

If an integral domain satisfies ACCP, then every nonzero nonunit in R can be factored into irreducibles.

Definition:

A commutative ring R satisfying the ACCP for all ideals (more than just principal ideals) is called a *Noetherian* ring.

44 PID's are UFD's

Theorem:

Every PID is a UFD.

Lemma:

Every PID satisfies the ACCP on principal ideals.

Proof:

Suppose $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \dots$ is an ascending chain. WTS there exists $k \geq 1$ such that $\langle a_k \rangle = \langle a_{k+1} \rangle = \langle a_{k+2} \rangle = \dots$.

Let J be an ideal defined as

$$J = \bigcup_{n \geq 1} \langle a_n \rangle = \{x \in R \mid \forall n \ x \in \langle a_n \rangle\}$$

Since R is a PID, J is principal, so $J = \langle x \rangle$ for some $x \in R$. Since $x \in J$, $x \in \langle a_k \rangle$ for some k . So, $\langle x \rangle \subseteq \langle a_k \rangle$. Finally,

$$J = \langle x \rangle \subseteq \langle a_k \rangle \subseteq \langle a_{k+1} \rangle \subseteq \langle a_{k+2} \rangle \subseteq \dots \subseteq J = \langle x \rangle$$

Therefore, all the containments in the chain are equalities.

Lemma:

In a PID, irreducible elements are prime, so factorizations are unique to reordering and associates.

Proof:

Let $x \in R$ be an irreducible element (nonzero non-unit). $\langle x \rangle$ is maximal among principal ideals (and $\langle x \rangle \neq R$). This means that there does not exist $\langle a \rangle$ such that $\langle x \rangle \subsetneq \langle a \rangle \subsetneq R$. Since R is a PID, this simply means that $\langle x \rangle$ is a maximal ideal. Maximal ideals are prime ideals, so $\langle x \rangle$ is a prime ideal, and x is a prime ideal.

Theorem:

$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\sqrt{3}]$ are PIDs. Each of these rings have variants of the division theorem.

Theorem:

$\mathbb{Z}[\sqrt{199}]$ is a PID but doesn't have a Division theorem. It's unknown for exactly which n , $\mathbb{Z}[\sqrt{n}]$ is a PID. It's not even known whether there are infinitely many such n .