Contents

Chapter 1

preface

1.1 Aim

- abstract algebraic structures on math objects.
- Basic language of modern math.

1.2 Ref

- Dummit & Foote: Abstract algebra, 3rd edition.
- 聂灵沼 & 丁石孙: 代数学引论 (第二版)

Chapter 2

2.1

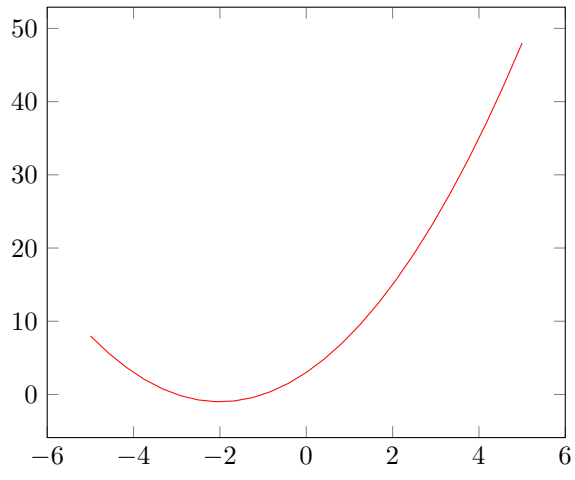
for an equation:

$$x^2 + 4x + 3 = 0$$

Analysis $x^2 + 4x + 3 = 0 \Rightarrow (x+3)(x+1) = 0 \Rightarrow x = -1$ or $x = -3$

Algebra Vary the coefficients, consider $ax^2 + bx + c = 0$ general solution is $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Geometry



For the analysis, we solve the problem itself, for algebra,, we abstract the problem (using abstract def and notations) and for geometry, we care about the graph and shapes.

Part I

The integers $\mathbb{Z}$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

There are two binary operations: addition and multiplication.

2.2 Addition:

$\exists!$(exists uniquely) $0 \in \mathbb{Z}$ such that

$$n + 0 = n$$

$\forall n, \exists -n \in \mathbb{Z}$ s.t. $n + (-n) = 0$
and

$$n + m = m + n$$

2.3 multiplication

$\exists! 1 \in \mathbb{Z}$ s.t.

$$n \cdot 1 = n$$

and

$$m \cdot n = n \cdot m \quad \forall m, n \in \mathbb{Z}$$

Only ± 1 have multiplication inverses.

Chapter 3

The fundamental theorem of arithmetic

3.1 Def

For $a, b \in \mathbb{Z}$ a divides b (written as $a \mid b$) if

$$\exists c \text{ s.t } b = ac$$

3.2 Theorem: The division algorithm

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then $\exists!(q, r) \in \mathbb{Z}^2$ such that

$$a = b \cdot q + r \text{ and } 0 \leq r < b$$

Proof

Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\} \subseteq \mathbb{N}$ If $0 \in S$ then $b \mid a$, then $q = \frac{a}{b}, r = 0$ Now assume $0 \notin S (\Rightarrow a \neq 0)$. Since $S \neq \varnothing$, by well ordering principle of $\mathbb{N}$, we have a smallest number, say $r = a - bq > 0$. It remains to show $r < b$. If $r \geq b$

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

and

$$a - b(q + 1) = r - b < r$$

contradiction.

For uniqueness, assume $a = bq + r$ and $a = bq' + r'$. Suppose $r' \geq r$ then

$$bq + r = a = bq' \;\Rightarrow\; b(q - q') = r' - r \geq 0$$

$\Rightarrow b \mid r' - r$ and $0 \leq r' - r \leq r' < b$, thus we have

$$r' - r = 0$$

so as $q = q'$

3.3 Def

- $\gcd(a, b)$ is the greatest common divisor of a and b
- If $\gcd(a, b) = 1$ then we say a and b are relative prime or coprime.

3.4 Corollary of 3.2

Let $a, b \in \mathbb{Z}$ no both zero, and let $c = \gcd(a, b)$. Then $\exists(xx, y) \in \mathbb{Z}^2$ such that $ax + by = c$

Proof

Let $S = \{ax + by \mid (x, y) \in \mathbb{Z}^2\} \cap \mathbb{Z}_{>0} \neq \varnothing$. Let $d = \min S$. We claim that

$$d = c = \gcd(a, b)$$

First note that $c \mid a \& c \mid b \Rightarrow c \mid ax + by \quad \forall x, y \in \mathbb{Z} \Rightarrow c \mid d$. With division algorithm, we write

$$a = dq + r \quad =\leq r < d$$

Note that $r \in S$ Hence $r = 0$ i.e. $d \mid a$ similarly $d \mid b \Rightarrow d \mid c$ They are positive hence $d = c$

3.5 Def

For $a \in \mathbb{Z} \setminus \{0, \pm 1\}$

- a is called **irreducible** in $\mathbb{Z}$, if $\forall$ factorization $a = bc$, we have

$$b \in \pm 1 \text{ or } c \in \pm 1$$

- a is called **prime** in $\mathbb{Z}$, if $a \mid bc \Rightarrow a \mid b$ or $a \mid c$

3.6 Euclid's Lemma

In $\mathbb{Z}$, irreducible $\Leftrightarrow$ prime.

Proof

$\subseteq$

Assume a is irreducible and $a \mid bc$. Without loss of generality(WLOG), we assume $a > 0$ and $a \not| b$. We show $a \mid c$ in the following way:

$$\left.\begin{array}{r} a\text{irreducible} \\ a > 0 \\ a \not| b \end{array}\right\} \Rightarrow gcd(a,b) = 1$$

$$\stackrel{3.4}{\Rightarrow} \exists x, y \in \mathbb{Z} s.t ax + by = 1$$

$$\Rightarrow c = acx + acy = a(cx + \frac{bc}{a}y)$$

$$\Rightarrow a \mid c$$

$\supseteq$

Assume a is prime and $a = bc$. WLOG, assume that $a \mid b$, then

$$|b| \stackrel{a=bc}{=} \gcd(a,b) \stackrel{a|b}{=} |a| \Rightarrow c = \pm 1$$

3.7 The fundamental theorem of arithmetic

$\forall n \in \mathbb{Z}_{\geq 2}$ is a product of positive primes. This prime factorization is unique in the following sense:

- if $n = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ with p_i, q_j are primes. Then $s = t$ and after reordering and relabeling, $p_i = q_i \forall i$

Proof

For existence, using induction on n. For $n = 2$, 2 is prime. Assume that the prime factorization exists for any integer k that $k < n$

If n is prime, done. If n not a prime, using Euclid's lemma 3.6, $n = bc$ with $1 < b < n, 1 < c < n$ By induction hypothesis, n is also a product of primes.

For uniqueness, using induction on $l = \max\{s,t\}$ If $l = 1$, $n = p_1 = q_1$. If $p_s \mid q_1 \cdots q_t \Rightarrow \exists i$ s.t. $p_s \mid q_i$ But q_i is prime, so $p_s = p_i$. Reindex and we may assume $p_s = q_t$. Cancel p_s with q_t we get

$$p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}$$

. By induction hypothesis, $s - 1 = t - 1$ and after reindex, $p_i = q_i \forall i$

3.8 Corollary

$\forall n \in \mathbb{Z} \setminus \{0, \pm 1\}$, $n = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ with p_i are primes and $\alpha_i \in \mathbb{Z}_{\geq 0}$

Chapter 4

Congruence in $\mathbb{Z}$

4.1 Def

Let $a, b, n \in \mathbb{Z}$ with $n > 0$ a is **congruent** ot b **modulo** n, written as

$$a \equiv b \mod n$$

if $n \mid a - b$

Remark

- It is an equivalence relation.
- Reflexive: $a \equiv a \mod n$
- Symmetric: $a \equiv b \mod n \Rightarrow b \equiv a \mod n$
- Transitive: $a \equiv b \mod n \& b \equiv c \mod n \Rightarrow a \equiv c \mod n$
- $$\begin{matrix} a \equiv b \mod n \\ c \equiv d \mod n \end{matrix} \overset{\Rightarrow}{} \begin{matrix} a + c \equiv b + d \mod n \\ ac \equiv bd \mod n \end{matrix}$$

So we can have congruence class modulo n:

$$[a]_n := \{b \in \mathbb{Z} \mid b \equiv a \mod n\} = a + n\mathbb{Z}$$

They are only n disjoint congruence class modulo n:

$$[0]_n, \cdots, [n-1]_n$$

The set of congruence classes modulo n is denoted as $\mathbb{Z}/n\mathbb{Z}$

4.2 Lemma

If $[a]_n = [i]_n, [b]_n = [j]_n$ thenn

$$[a+b]_n = [i+j]_n \quad [ab]_n = [ij]_n \quad [a-b]_n = [i-j]_n$$

Therefore, we define the following binary operations on $\mathbb{Z}/n\mathbb{Z}$:

$$[i]_n + [j]_n := [i+j]_n$$
$$[i]_n \cdot [j]_n := [ij]_n$$

We have addition and multiplication satisfying associativity law, distribution law, additive inverse.

4.3 Remark

In $\mathbb{Z}$, if a, b are non-zero, then $ab \neq 0$. But in $\mathbb{Z}/n\mathbb{Z}$, $[a]_n[b]_n = [0]_n$ if $n \mid ab$. In $\mathbb{Z}$ for $2x = 1$ it have no solution. But in $\mathbb{Z}/3\mathbb{Z}$,$[2]_3 x = [1]_3 \Rightarrow x = [2]_3$

4.4 Theorem(The structure of $\mathbb{Z}/p\mathbb{Z}$, p prime)

For $p \in \mathbb{Z}_{\geq 2}$. The following are equivalent(TFAE):

1 p is prime

2 $\forall a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, $ax = 1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$

3 whenever $bc = 0$ in $\mathbb{Z}/p\mathbb{Z}$, $b = 0$ or $c = 0$

Proof

$1 \Rightarrow 2$

$0 \neq [a]_p \Rightarrow p \neq a$ so $\gcd(a, p) = 1$ then $\exists (x, y) \in \mathbb{Z}$ s.t. $ax + py = 1$. So moduloing p we get $ax \equiv 1 \mod p$. then $ax = 1$ in $\mathbb{Z}/p\mathbb{Z}$ has a solution

$2 \Rightarrow 3$

Suppose $bc = 0$ in $\mathbb{Z}/p\mathbb{Z}$, WLOG, we assume $b \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, $\exists \in \mathbb{Z}/p\mathbb{Z}$ s.t. $xb = 1$.

$$\Rightarrow c = c \cdot 1 = xbc = 0$$

$3 \Rightarrow 1$

$bc = 0$ in $\mathbb{Z}/p\mathbb{Z} \Rightarrow p \mid bc$ Hence it follows from the define of prime.

4.5 Chinese remainder theorem

If we have n and n' are relative prime, $b, b' \in \mathbb{Z}$, then the congruence equation

$$\begin{cases} x \equiv b \mod n \\ x \equiv b' \mod n' \end{cases}$$

have a common solution in $\mathbb{Z}$, and any two solutions are congruence modulo $n \cdot n'$.

Proof

$x \equiv b \mod n \Rightarrow x = b + kn$ for some $k \in \mathbb{Z}$. We need to find k s.t.

$$b + kn = b' \mod n'$$

i.e.

$$kn \equiv b' - b \mod n'$$

Since $\gcd(n, n') = 1$, then $\exists u, v \in \mathbb{Z}$ s.t.

$$nu + n'v = 1$$

$$b' - b = (b' - b)1 = nu(b' - b) + n'v(b' - b)$$

Therefore $k = u(b' - b)$ satisfies $b + kn \equiv b' \mod n'$. If y in another solution in $\mathbb{Z}$, then $n \mid x - y, n' \mid x - y$. We write

$$x - y = nt = n't'$$

for some $t, t' \in \mathbb{Z}$

$$x - y = (x - y)1 = (x - y)(nu + n'v) = nun't' + n'vnt$$

$\Rightarrow nn' \mid x - y$

Remark

In other words, CRT claims that the mapping

$$\begin{aligned} \mathbb{Z}/nn'\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \\ [a]_{nn'} &\mapsto ([a]_n, [a]_{n'}) \end{aligned}$$

is surjective, hence bijective.

Chapter 5

Rings

5.1 Def

A **ring** is a nonempty set R equipped with two binary operations (usually written as addition and multiplication) that satisfy the following:

Addition
- If $a \in R, b \in R, a + b \in R$ (Close for addition)
- $(a + b) + c = a + (b + c)$ (Associative)
- $a + b = b + a$ (Commutative)
- $\exists 0_R \in R$ s.t. $a + 0_R = a$ (neutral element)
- $\forall a \in R, a + x = 0_R$ has a solution in R (additive inverse)

Multiplication
- If $a \in R, b \in R, ab \in R$ (Close for multiplication)
- $(ab)c = a(bc)$ (Associative)
- $\exists 1_R \in R$ s.t. $a \cdot 1_R = a = 1 \cdot a$ (neutral element)
- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ (Distribution law)

Warning

- A ring R cannot be empty.
- All rings will have the identify element.

A **commutative ring** is a ring that satisfying

$$ab = ba \quad \forall a, b \in R$$

Let $S \subseteq R$ be a subset of a ring R. If S is a ring under the addition and multiplication in R, then we say S is a **subring** of R

Remark

- $\forall a \in R$, $a + x = 0_R$ has a unique solution denoted as $-a$
- In R, we have $a0_R = 0_R = 0_R a$
- $a + b = a + c \Rightarrow b = c$ and $-(a - b) = -a + b$

5.2 Def

Let R be a non-trivial ring.

- An element $r \in R$ is called **unit** if $\exists s \in R$ s.t.

$$rs = 1_R = sr$$

  In this case, s is called the **multiplicative inverse** of r

- We denote $R^\times$ the set of all units in R.
- An element $r \in R$ is called **zero-divisor** if $rs = 0_R$ for some $s \neq 0 \in R$ (then 0_R is also a zero divisor)

Remark

For a commutative ring R, $r \in R$ we can define

$$\begin{aligned} \varphi_r : R &\to R \\ x &\mapsto rx \end{aligned}$$

a mapping of sets.

$$r \text{ is a unit} \Leftrightarrow \varphi_r \text{ is bijective}$$

$\Rightarrow rs = 1 \Rightarrow \varphi_r \circ \varphi_s = Id = \varphi_s \circ \varphi_r$
$\Leftarrow \exists s \in R$ s.t. $1 = \varphi_r(s) = rs$
r is non a zero divisor $\Leftrightarrow (rs_1 = rs_2 \Rightarrow r(s_1 - s_2) = 0 \Rightarrow s_1 = s_2) \Leftrightarrow \varphi_r$ is injective.

Example

The only unit in $\mathbb{Z}$ are ± 1, but ni non-zero divisor. And also 2 is neither a unit nor a zero divisor.

- In $\mathbb{Z}/6\mathbb{Z}$ the zero-divisor:0,2,3,4; units: 1,5. So Any elements is either a unit or a zero-divisor in $\mathbb{Z}/6\mathbb{Z}$ (this holds for $\mathbb{Z}/n\mathbb{Z}$)

5.3 Def

- A **division ring**(skew filed) is a non-trivial ring R s.t. $\forall 0_R \neq a \in R$, is a unit
- A non-trivial commutative ring R is an **integral domain** if it has no non-zero zero-divisor.
- A non-trivial commutative division ring is called a **filed**.

EXample

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- $\mathbb{Z}/p\mathbb{Z}$ is a filed $\Leftrightarrow p$ is a prime.
- $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/6\mathbb{Z}$ is not.
- Any field is an integral domain($0 \neq r \in R$ φ_r is bijective $\Rightarrow$ is injective)
- Real Hamilton quaternions is a division ring, but not a field.

5.4 Theorem

Every finite integral domain R is a filed.

Proof

$\forall r \neq 0 \in R$ we define $\varphi_r : x \mapsto rx$ is injective. But R is a finite set, hence φ_r is bijective $\Rightarrow r$ is a unit.

5.5 Def

Let R and S are rings. A mapping $f : R \to S$ is called a **ring homomorphism** if

$$f(a+b) = f(a) + f(b) \quad f(ab) = f(a)f(b) \text{ and } f(1_R) = 1_S$$

A ring homomorphism is called ring isomorphism if it is bijective, denoted as $\cong$

Remark

- We have $f(0_R) = 0_S : f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$
- We require f sending 1_R to 1_S, hence $f \equiv 0$ is not a ring morphism unless $S = 0$
- Id_R is a isomorphism

- If $f : R \to S, g : S \to T$ are morphism, then $f \circ g$ also morphism.
- If $f : R \to S$ a ring isomorphism, so does f^{-1}.
- The image of a ring homomorphism $f : R \to S$ is a subring of S
- There's no morphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$

5.6 Def

For rings R and S, we have a ring structure on the Cartesian product $R \times S$ defined coordinatewise:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \quad (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$$

We have a mapping:

$$\begin{aligned} f : \mathbb{Z}/nn'\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \\ [a]_{nn'} &\mapsto ([a]_n, [a]_{n'}) \end{aligned}$$

It's in fact a ring morphism

$$\begin{aligned} f([a]_{nn'} + [b]_{nn'}) &\overset{\text{on } \mathbb{Z}/nn'\mathbb{Z}}{=} f([a+b]_{nn'}) \\ &\overset{definition}{=} ([a+b]_n, [a+b]_{n'}) \\ (on \mathbb{Z}/n\mathbb{Z} and \mathbb{Z}/n'\mathbb{Z}) &= ([a]_n + [b]_n, [a]_{n'} + [b]_{n'}) \\ (\text{on } \mathbb{Z}n\mathbb{Z} \times \mathbb{Z}n'\mathbb{Z}) &= ([a]_n, [a]_{n'}) + ([b]_n, [b]_n) \\ &= f([a]_{nn'}) + f([b]_{nn'}) \end{aligned}$$

Similarly, for $f([a]_{nn'}[b]_{nn'}) = f([ab]_{nn})$. If $\gcd(n, n') = 1$, by CRT, f is surjective, hence bijective. We have a ring morphism:

$$\mathbb{Z}/nn'\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$$

if $\gcd(n, n') = 1$ But injective is much easier:

If $f([a]_{nn'}) = 0 \Rightarrow ([a]_n, [a]_{n'}) = 0 \Rightarrow n \mid a, n' \mid a \Rightarrow nn' \mid a \Rightarrow [a]_{nn'} = 0$ This gives an "abstract" proof of CRT.

There are 24 bijections $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But none of theses bijections is ring morphism. For $x \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ $x + x = 0$ However,

$$[1]_4 + [1]_4 = [2]_4 \neq 0 \quad \text{in } \mathbb{Z}/4\mathbb{Z}$$

cannot be a ring morphism.

Remark

In general, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with p_i primes. We have

$$\begin{gathered} \mathbb{Z}/n\mathbb{Z} \overset{\cong}{\to} \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{\alpha_s} \\ [a]_n \mapsto ([a]_{p_1^{\alpha_1}}, \cdots, [a]_{p_s^{\alpha_s}}) \end{gathered}$$

Moreover, $[a]_n \in^{\alpha_1} Z/n^{\alpha_1}Z$ is unit $\Leftrightarrow$ $[a]_{p_i^{\alpha_i}}$ is a unit in $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ $\forall i$. Therefore,

$$(\mathbb{Z}/n\mathbb{Z})^\times \overset{1=1}{\to} (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^\times$$

bijective.

5.7 Def

Euler φ-function is defined as:

$$\varphi(n) := \#\{x < n \in \mathbb{N}_+ \mid \gcd(x, n) = 1\}$$

5.8 Prop

Euler φ-function is multiplicative:

$$\varphi(n) \overset{CRT}{=} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_s})$$

for $\varphi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^\alpha(1 - \frac{1}{p})$

Chapter 6

The polynomial ring

The polynomial rings enjoy one feature that $\mathbb{Z}$ does not:
The notion of a root of a polynomial. $\rightsquigarrow$ The theory of equations.

6.1 Def

Let R be a ring

- A **polynomial with coefficients** in R is defined to be an infinite sequence $(a_n)_{n\in\mathbb{N}}$ such that $a_i \in R$ and only finitely many of the a_i are nonzero. That's, for some index k, $a_i = 0_R, \forall i > k$
- Two polynomial $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are **equal** if they are equal as sequence; That's $a_i = b_i \forall i \geq 0$
- **Addition**:
$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$$
Multiplication:
$$(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} = (\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}}$$

6.2 Theorem

Let R be a ring, and let P be the set of all polynomials with coefficients in R. Then

1 P is a ring. If R is commutative, so as P

2 Let $\tilde{R}$ be the set of all polynomial in P of the form $(r_n)_{n\in\mathbb{N}}$ with $r \in R$. Then $\tilde{R}$ is a subring of P and is isomorphic to R

Proof

2

Consider the mapping from R to $\tilde{R}$

$$\begin{aligned} f : R &\to \tilde{R} \\ r &\mapsto (r, 0, 0, \cdots) \end{aligned}$$

This recovers the old notion for polynomials

$$(a, 0, \cdots) \in \tilde{R}$$

will be denoted as a

$$(0, 1, 0, \cdots)$$

will be denoted as x. Hence

$$x_n = (\underbrace{0, 0, \cdots}_{n}, 1, 0, \cdots)$$

6.3 Theorem

Let P be the polynomials with coefficients in R. Then P contains an isomorphic copy $\tilde{R}$ of R and an element x s.t.

1 $ax = xa, \forall a \in \tilde{R}$

2 Every element in P can be written in the form

$$a_0 + a_1 x + \cdots + a_n x^n \quad \text{for some } n \in \mathbb{Z}_{\geq 0}$$

3 If $a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m$ with $n \leq m$, then $a_i = b_i$ for $i \leq n$ and $b_i = 0_R$ for $i > n$

Proof

2 If $(a_n) \in P$ then $\exists n$ s.t. $a_i = 0_R$ for i>n

$$(a_i) = a_0 + a_1 x + \cdots + a_n x^n$$

6.4 Def

- Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ with $a_n \neq 0$ Then a_n is called the leading coefficients of $f(x)$ n is called the degree of $f(x)$ denoted as $\deg f(x)$

  Remark:leading coefficients of 0 is 0,

  $$\deg(0_R) = -\infty$$

- Let $f(x), g(x) \in R[x]$ with $g(x) \neq 0_R$, we say $g(x)$ divide $f(x)$ written as $g(x) \mid f(x)$, if $f(x) = g(x)q(x)$ for some $q \in R[x]$

6.5 Theorem

Let R be a ring

1 For any $f(x), g(x) \in R[x]$,

$$\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

$$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$$

2 If R is an integral domain. So as $R[x]$ and $(R[x])^\times = R^\times$

6.5.1 Proof

1 Assume $f, g \neq 0_R$ Suppose $f(x) = a_0 + a_1x + \cdots + a_nx^n, g(x) = b_0 + b_1x + \cdots + b_mx^m$ with $a_n \neq 0_R, b_m \neq 0_R$ WLOG we assume $n \geq m$

$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_m)x^n+(a_{n+1}b_{n+1})x^{n+1}+\cdots$

$\Rightarrow$

$$\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

similarly for multiplication.

2 By expression of $f(x)g(x)$ the product of two nonzero polynomials in $R[x]$ is nonzero $(\deg(f(x)g(x)) = \deg f + \deg g)$

It's clear that $R^\times \subset (R[x])^\times$ For any $f(x) \in (R[x])^\times$, there exists $g(x) \in R[x]$, s.t. $f(x)g(x) = 1_R$

$$0 \leq \deg f(x) + \deg g(x) = \deg(f(x)g(x)) = \deg(1_R) = 0$$

so $\deg f = \deg g = 0$ meaning

$$f(x) = a \in R, g(x) = b \in R$$

with $ab = 1_R \Rightarrow f(x) = a \in R^\times$

6.6 Division algorithm

Let k be a field. $f(x), g(x) \in k[x]$ with $g(x) \neq 0$ Then there exists $q(x), r(x) \in k[x]$ uniquely s.t.

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

and

$$\deg r < \deg g$$

Proof

Existence

If $g(x) \mid f(x)$ then $f(x) = q(x)g(x)$ for some $q(x) \in k[x]$
If $g(x) \not| f(x)$, then consider

$$S = \{f(x) - q(x)g(x) \in k[x] \mid f(x) - q(x)g(x) \neq 0, q(x) \in k[x]\}$$

Let $r(x) = f(x) - q(x)g(x) \in S$ be a polynomial of the minimal deg. It suffices to show

$$\deg r < \deg g$$

We write

$$g(x) = s_0 + s_1x + \cdots + s_nx^n \quad r(x) = r_0 + r_1x + \cdots + r_mx^m$$

with $s_n, r_m \neq 0$.
If $\deg r \geq \deg g$, then we could define:

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} g(x)$$

but $\deg h < \deg r$. By the minimal degree of $r(x)$, we have $h(x) = 0$ Then

$$f(x) = q(x)g(x) + t_m s_n^{-1} x^{m-n} g(x)$$

$\Rightarrow \quad g(x) \mid f(x)$

Uniqueness

$f(x) = q(x)g(x) + r(x) = \tilde{q}(x)g(x) + \tilde{r}(x) \Rightarrow$

$$\tilde{r}(x) - r(x) = (q(x) - \tilde{q}(x))g(x)$$

$$\tilde{r}(x) = r(x) \quad \tilde{q}(x) = q(x)$$

$$\deg(\tilde{r}(x) - r(x)) < \deg g(x)$$

$$\deg(\tilde{r}(x) + r(x)) = \deg g + \deg(q(x) - \tilde{q}(x))$$

Remark

The division algorithm holds for

- k a filed $\rightsquigarrow$ R any commutative ring
- $g(x) \neq 0 \rightsquigarrow$ the leading coefficients of g is unit

6.7 Corollary

Let R a commutative ring. $a \in R$ and $f(x) \in R[x]$. When we divide $f(x)$ by $x - a$, the remainder if $f(a)$

Proof

We have $f(x) = q(x)(x-a) + r(x)$ with $\deg r < 1$ Then $r(x)$ is a constant. Evaluating both sides at $x = a$, we get $r =: f(a)$

6.8 Def

Let R be a commutative ring.

- $\forall r \in R$, the evaluation mapping is

$$\begin{aligned} \varphi_r : R[x] &\to R \\ f(x) = \sum_{i=0}^{n} a_i x^i &\mapsto f(r) := \sum_{i=0}^{n} a_i r^i \end{aligned}$$

  which is a ring homomorphism.

- If $f(r) = 0_R$, then we say that r is a root of $f(x)$

6.9 Theorem

Let R be an **integral domain**. Then a nonzero polynomial $f(x) \in R[x]$ of degree n has at most n roots $\in R$ counting multiplicity.

Proof

If $f(a_1) = 0$, then possibly applied coro6.7 several times, we have

$$f(x) = q_1(x)(x-a_1)^{n_1}$$

with $q_1(a_1) \neq 0$, $\deg q_1 = n - n_1$. If $a_2 \in R$ is another root of $f(x)$, the

$$0 = f(a_2) = q(a_2)(a_2 - a_1)^{n_1}$$

$\Rightarrow q_1(a_2)0$ so

$$q_1(x) = q_2(x)(x-a_2)^{n_2}$$

with $q_2(a_2) \neq 0$ and $\deg q_2 = n - n_1 - n_2$.

After n application of coro6.7, the quotient becomes constant, and we write

$$f(x) = c(x-a_1)^{n_1} \cdots (x-a_k)^{n_k}$$

with $n = n_1 + \cdots + n_k$ Since R is an integral domain, the only possible roots are $a_1, \cdots, a_k$

(This is a tricky proof, for a_n 's existence doesn't guaranteed. But we can use induction to prove it)

Remark

$f(x) = x^3$ in $\mathbb{Z}/8\mathbb{Z}[x]$ but

$$f(0) = f(2) = f(4) = f(6) = 0$$

in $\mathbb{Z}/8\mathbb{Z}$

Chapter 7

Unique factorization for the polynomial ring

In $\mathbb{Z}$, we deduce the existence of the gcd and unique factorization property from the division algorithm. There results will follow identically for the polynomial ring once we have the appropriate notions of primes and gcd.

7.1 Def

Let k bea non-constant polynomial $f(x) \in k[x]$ is called **irreducible** in $k[x]$ if it cannot be expressed as a product of non-constant polynomials in $k[x]$.

Remark

The irreducibility of a polynomial depends on the field k. For instance, x^2-2 is irreducible in $\mathbb{Q}[x]$, but reducible in $\mathbb{R}[x]$.

7.2 Theorem

Given two nonzero polynomials $f(x), g(x) \in k[x]$. Let

$$S := \{a(x)f(x) + b(x)g(x) \in k[x] \mid a(x), b(x) \in k[x]\}$$

Then there's certain polynomial $d(x) \in S$ of smallest degree, and every $h(x) \in S$ is divisible by $d(x)$.

Proof

Use well-ordering principle for $S \setminus \{0\}$

7.3 Def

Let k be a field. Let $f(x), g(x) \in k[x]$ be two nonzero polynomials.

- We define the greatest common divisor of $f(x), g(x)$ is

$$d(x) := \gcd(f(x), g(x))$$

to be the monic polynomial in $k[x]$ satisfying:

  - $d(x) \mid f(x)$ and $d(x) \mid g(x)$
  - $\forall e(x) \in k[x]$ if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $d(x) \mid e(x)$

- if

$$\gcd(f(x), g(x)) = 1$$

then we say $f(x)$ and $g(x)$ are relative prime.

7.4 Theorem

Let k be a field.

- Suppose that $f(x)$ is irreducible in $k[x]$ and

$$f(x) \mid g(x)h(x)$$

then

$$f(x) \mid g(x) \text{ or } f(x) \mid h(x)$$

- (unique factorization in $k[x]$) Every common non-constant polynomial $f(x) \in k[x]$ can be written as a product of irreducible polynomials in $k[x]$; the resulting expression is unique, except for rearrangement and non-zero constant factors.

Proof

As before in $\mathbb{Z}$

Remark

We have pointed out how similar the situation is for $\mathbb{Z}$ and $k[x]$. This suggests that there should be a wider class of rings, of which $\mathbb{Z}$ and $k[x]$ are special cases, for which much of the argumentation works.

7.5 Def

An integral domain R is a **Euclidean domain**(or *Euclidean ring*) if there is a function $d : R^* := R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ s.t.

i For $a \in R^*, b \in R^*$, have
$$d(a) \leq d(ab)$$

ii For $a \in R, b \in R^*$, there exists $q, r \in R$ s.t.
$$a = qb + r$$
where $r = 0$ or $d(r) < d(b)$

7.6 Example

The following are standard examples, we have seen before:

- The ring of integers $\mathbb{Z}$ with $d(n) = |n|$ the absolute value of n. Note that when we use the absolute value, then the quotient q and the reminder r are not unique anymore. For instance $51 = 6 \times 8 + 3 = 6 \times 9 - 3$
- The polynomial ring $k[x]$ with coefficients in a field k, and d is given by degree.
- The ring of Gaussian integers
$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$
with
$$d(a + bi) = a^2 + b^2$$

Remark

1

In Definition7.5, (i) is not essential. Indeed, given (R, d) which only satisfies (ii) there, we can define $\tilde{d}$ as
$$\tilde{d}(a) = \min\{d(ab) \mid b \in R^*\}$$
for any $a \in R^*$. Then $(R, \tilde{d})$ is a Euclidean domain defined as in Def7.5(Exercise)

2

Division in $\mathbb{Z}[i]$ does not have a unique quotient and a remainder. For example:
$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i$$
$$1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i$$
which both remainders have norm 5 and less then $N(2 - 4i) = 20$

3

We have the following fact: If R is a Euclidean domain where the quotient and remainder are unique, then R is a field or $R = k[x]$ for a field k.

Chapter 8

Ideals and Quotients

We start from a special kind of ideals.

8.1 Def

Let $f : R \to S$ be a ring homomorphism between two rings. Then kernel of f is denoted as

$$\ker f = \{a \in R \mid f(a) = 0_S\}$$

Note that, if $a_1, a_2 \in \ker f$, then $a_1 \pm a_2 \in \ker f$, $r_1, r_2 \in \ker f$ and $r_2, r_1 \in \ker f$. This set is almost to be a ring but $1_R \notin \ker f$. But this set is more special, it satisfies a absorptive properties: if $a_1 \in \ker f$ and $a \in R$, then we have:

$$f(aa_1) = f(a)f(a_1) = f(a) \cdot 0_S = 0_S$$

hence $aa_1 \in \ker f$, similarly, we also have $a_1 a \in \ker f$. This type subset has its own name.

8.2 Def

Let R be a ring, let $I \subseteq R$ be a subset. I is called an ideal of R if it satisfies:

- $0 \in I$
- if $a_1, a_2 \in I$, then
$$a_1 + a_2 \in I$$
- if $a_1 \in I$, $\forall a \in R$, then
$$aa_1 \in I \text{ and } a_1 a \in I$$

Example

- If $b \in I$, then $-b = (-1_R) \cdot b \in I$. Therefore $a - b \in I$ if $a, b \in I$
- Let $\varphi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the natural ring homomorphism $a \mapsto [a]_n$. Then,

  $$\ker(\varphi_n) = n\mathbb{Z}$$

  is an ideal.
- $\forall f(x) \in R[x]$ be a polynomial with coefficients in a ring R, then

  $$f(x)R[x] := \{f(x)g(x) \mid g(x) \in R[x]\}$$

  is an ideal of $R[x]$

8.3 Def

Let R be a commutative ring

- $\forall a \in R$, $aR := \{ab \mid b \in R\}$ is an ideal of R, denoted as (a), called the principal ideal generated by a
- Let $a_1, \cdots, a_n \in R$. The ideal generated by $a_1, \cdots, a_n$ is denoted as

  $$(a_1, \cdots, a_n) := \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, \forall i\}$$

8.4 Example

- Given $m, n \in \mathbb{Z}$, the ideal generated by (m, n) is

  $$\{mx + ny \mid x, y \in \mathbb{Z}\} = (gcd(m, n))$$

  which is a principal ideal.
- Let R be a commutative ring, consider the evaluation map at $a \in R$:

  $$\begin{aligned} ev_a : R[x] &\to R \\ f(r) &\mapsto f(a) \end{aligned}$$

  The kernel of this mapping is given by

  $$\begin{aligned} \ker(ev_a) &= \{f(x) \in R[x] \mid f(a) = 0_R\} \\ &= \{f(x) \in R[x] \,|x - a \mid f(x)\,\} \end{aligned}$$

  which is just the ideal $(x - a)$. It also a principal ideal.

8.5 Def

Let R be a ring, $I \subseteq R$ be an ideal. For $a, b \in R$, we say a is congruent to b modulo I, written as $a \equiv b \mod I$ if $a - b \in I$

8.6 Lemma

Let R be a ring, $I \subseteq R$ be an ideal.

- Congruence modulo I is an equivalence relation
- If $a \equiv b \mod I$ and $c \equiv d \mod I$, then $a \pm c \equiv b \pm d \mod I$. That is, this congruence relation is compatible with addition and multiplication on R.