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

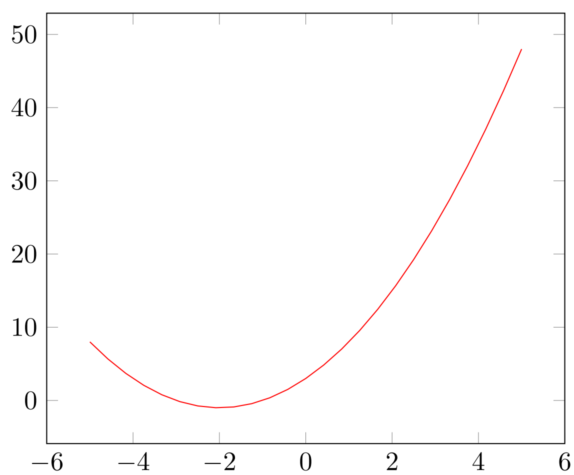
2.1

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:

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

$$\begin{aligned} &\overset{3.4}{\Rightarrow} \exists x, y \in \mathbb{Z} s.t. ax + by = 1 \\ &\Rightarrow c = acx + acy = a(cx + \frac{bc}{a}y) \\ &\Rightarrow a \mid c \end{aligned}$$

$\supseteq$

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

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

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: $a \equiv b \mod n \& b \equiv c \mod n \Rightarrow a \equiv c \mod n$
- $$\begin{array}{l} a \equiv b \mod n \\ c \equiv d \mod n \end{array} \Rightarrow \begin{array}{r} a + c \equiv b + d \mod n \\ ac \equiv bd \mod n \end{array}$$

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$ φ_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

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

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