

## 第二章 整数

## §2.0 自然数与整数

## 2.0.1 自然数的公理化定义

定义1 (Peano 1881, Dedekind 1888, Peano 1889)

满足下列性质的 (Peano 公理) 的集合称为一个自然数集.

PA1.  $0 \in \mathbb{N}$ PA2.  $\forall x \in \mathbb{N}$  存在  $\mathbb{N}$  中唯一的元素记为  $Sx$ , 称为  $x$  的后继PA3.  $\forall x \in \mathbb{N}, Sx \neq 0$ PA4.  $Sx \neq Sy \Rightarrow x \neq y$ PA5. (归纳公理) 设  $M \subseteq \mathbb{N}$ . 若  $0 \in M$ , 且  $\forall x \in M$  有  $Sx \in M$ , 则  $M = \mathbb{N}$ 注: 存在性:  $0 = \emptyset, 1 = S0 = \{\emptyset\}, 2 = S1 = \{\emptyset, \{\emptyset\}\}, 3 = S2 = \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$   
唯一性 (思考题)注: 要证明  $P(n)$  对  $\forall n \in \mathbb{N}$  成立,  $\Leftrightarrow \begin{cases} 1^\circ P(0) \text{ 成立} \\ 2^\circ P(m) \text{ 成立} \Rightarrow P(Sm) \text{ 成立} \end{cases}$ 注 自然数集为一个三元组  $(\mathbb{N}, 0, S)$ , 其中

- $\mathbb{N}$  为集合 (非空)
- $0 \in \mathbb{N}$  为特定元素
- $S: \mathbb{N} \rightarrow \mathbb{N}$  为映射, 满足

(i)  $0 \notin \text{Im} S = \{Sx \mid x \in \mathbb{N}\}$ (ii)  $S$  为单射, 即  $Sx \neq Sy \Rightarrow x \neq y$ (iii)  $M \subseteq \mathbb{N}$ , 若 (i)  $0 \in M$ , (ii)  $SM \subseteq M$   
则  $M = \mathbb{N}$ .

## 命题2

(1)  $Sx \neq x \quad \forall x \in \mathbb{N}$ (2)  $\text{Im} S = \mathbb{N} \setminus \{0\}$  (即  $\forall x \neq 0, \exists y$  使得  $x = Sy$ ,  $y$  称为  $x$  的 predecessor)证: (1) 令  $M = \{x \in \mathbb{N} \mid Sx \neq x\}$  则 $1^\circ 0 \in M$  ( $0 \neq S0 \quad \forall x$  (PA3)) $2^\circ x \in M$  则  $Sx \neq x \xrightarrow{\text{PA4}} S(Sx) \neq Sx \Rightarrow Sx \in M$  $\xRightarrow{\text{PA5}} M = \mathbb{N}$ (2) 只需证明  $\text{Im} S \cup \{0\} = \mathbb{N}$ . ( $0 \notin \text{Im} S$  由 (PA3))令  $M = \text{Im} S \cup \{0\}$ 则  $1^\circ 0 \in M$  $2^\circ x \in M$  则  $Sx \in \text{Im} S \subseteq M \Rightarrow Sx \in M$   
 $\xRightarrow{\text{PA5}} M = \mathbb{N}$ 

## 2.0.2 自然数的运算

定义3 自然数  $\mathbb{N}$  上的一个加法. 记作  $+$ , 是指某是如下性质的二元运算:

$$(*) \quad \begin{cases} x + 0 = x \\ x + Sy = S(x + y) \end{cases} \quad \begin{matrix} \forall x \in \mathbb{N} \\ \forall x, y \in \mathbb{N} \end{matrix}$$

逆:  $+$   $\Leftrightarrow \forall x \in \mathbb{N}, x_+ : \mathbb{N} \rightarrow \mathbb{N}, (x_+(y) \triangleq x+y)$  满足

$$\begin{cases} x_+(0) = x \\ x_+(sy) = S(x_+(y)) \end{cases} \quad \forall y \in \mathbb{N}.$$

引理:  $x \in \mathbb{N}$ . 若  $f, \tilde{f} : \mathbb{N} \rightarrow \mathbb{N}$  均满足  $(**)$ , 即

$$\begin{cases} f(0) = x \\ f(sy) = S(f(y)) \end{cases} \quad \forall y \quad \Leftrightarrow \quad \begin{cases} \tilde{f}(0) = x \\ \tilde{f}(sy) = S(\tilde{f}(y)) \end{cases} \quad \forall y.$$

$f = \tilde{f}$ , 即  $f(y) = \tilde{f}(y) \quad \forall y \in \mathbb{N}$ .

PF: 令  $M = \{y \in \mathbb{N} \mid f(y) = \tilde{f}(y)\}$  则

- 1°  $0 \in M$ .
- 2°  $y \in M$ , 即  $f(y) = \tilde{f}(y) \Rightarrow f(sy) = S(f(y)) \stackrel{(**)}{=} S(\tilde{f}(y)) \stackrel{\text{归纳假设}}{=} S(\tilde{f}(y)) \stackrel{(**)}{=} \tilde{f}(sy)$   
 $\Rightarrow sy \in M$ .

PAS  $\Rightarrow M = \mathbb{N}$ .  $\#$

定理4 定义3中的  $+$  存在, 唯一.

证明: 唯一性由引理可得.

下证存在性. 只需证明 对  $x$ , 存在函数  $x_+ : \mathbb{N} \rightarrow \mathbb{N}$  满足  $(**)$  即可.

令  $M = \{x \in \mathbb{N} \mid \text{存在 } x_+ : \mathbb{N} \rightarrow \mathbb{N} \text{ 使得 } \begin{cases} x_+(0) = x \\ x_+(sy) = S(x_+(y)) \end{cases} \forall y\}$ ,

则 1°  $0 \in M$ . 考察函数  $0_+(y) = y$

2°  $x \in M$ . 即存在  $x_+ : \mathbb{N} \rightarrow \mathbb{N}$  使得  $\begin{cases} x_+(0) = x \\ x_+(sy) = S(x_+(y)) \end{cases} \forall y$   
 构造  $(Sx)_+ : \mathbb{N} \rightarrow \mathbb{N}$ ,  $(Sx)_+(y) \triangleq S(x_+(y))$ .

则  $\begin{cases} (Sx)_+(0) = S(x_+(0)) = Sx \\ (Sx)_+(sy) \stackrel{\text{构造}}{=} S(x_+(sy)) \stackrel{x_+ \text{ 满足 } (**)}{=} S(S(x_+(y))) \stackrel{(Sx)_+ \text{ 定义}}{=} S((Sx)_+(y)) \end{cases}$

PAS  $\Rightarrow \forall Sx \in M$   
 $\Rightarrow M = \mathbb{N}$   $\#$

定理5

- (1)  $0+y = y \quad \forall y$
- (2)  $Sx+y = S(x+y) \quad \forall x, y$

证明: (1) 令  $M = \{y \in \mathbb{N} \mid 0+y = y\}$  则

- 1°  $0 \in M$ . ( $0+0=0$  由定义)

2°  $y \in M$ . 即  $0+y = y \Rightarrow 0+Sy \stackrel{\text{定义}}{=} S(0+y) \stackrel{y \in M}{=} Sy \Rightarrow Sy \in M$ .

PAS  $\Rightarrow M = \mathbb{N}$ .

(2) 固定  $x$ . 令  $M = \{y \in \mathbb{N} \mid Sx+y = S(x+y)\}$ .

1°  $0 \in M$  ( $Sx+0 = Sx = S(x+0)$ )

2°  $y \in M$  即  $Sx+y = S(x+y)$ , 归纳假设  
 $\Rightarrow Sx+Sy \stackrel{\text{归纳假设}}{=} S(Sx+y) = S(S(x+y)) \stackrel{\text{定义}}{=} S(x+Sy)$   
 $\Rightarrow Sy \in M$ .

PAS  $\Rightarrow M = \mathbb{N}$ .  $\#$

- 定理6
- (1)  $x+y = y+x$
  - (2)  $(x+y)+z = x+(y+z)$
  - (3)  $x+y = x+z \Rightarrow y=z$

(对  $x$  归纳)

定义7 自然数  $N$  上的一个乘法, 记作  $\cdot$ , 是指某定如下性质的二元运算.

$$(*) \quad \begin{cases} x \cdot 0 = 0 \\ x \cdot sy = x \cdot y + x \end{cases} \quad \begin{matrix} \forall x \in N \\ \forall x, y \in N \end{matrix}$$

定理8 定义7中的乘法存在唯一.

- 定理9
- (1)  $0 \cdot y = 0$
  - (2)  $sx \cdot y = x \cdot y + y$

- 定理10
- (1)  $x \cdot y = y \cdot x$
  - (2)  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
  - (3)  $x \cdot (y+z) = x \cdot y + x \cdot z$
  - (4)  $xy = 0 \Rightarrow x=0$  或  $y=0$

} 对  $x$  归纳

PF of (4): 若  $x \neq 0, y \neq 0$ . 则  $x = su, y = sv$ . (PAS)  
 $\Rightarrow xy = (su) \cdot (sv) = (su)v + su = s(sv)v + u \neq 0$   
 矛盾.

## 2.0.3 自然数上的序

定义11 称  $x$  小于或等于  $y$ , 记作  $x \leq y$ . 若存在  $u$  使得  $y = x + u$ .  
 $\dots$  小于  $\dots$   $x < y, \dots u \neq 0 \dots$   
 $(\Leftrightarrow x \leq y, x \neq y)$

定理12  $(N, \leq)$  为全序关系. 即:

- (i)  $x \leq x \quad \forall x$
- (ii)  $x \leq y, y \leq z \Rightarrow x \leq z$ , 此时  $x=z \Leftrightarrow x=y=z$ .
- (iii)  $\forall x, y \in N. x \leq y$  或  $y \leq x$  必居其一.

PF: (i) ~~显然~~  $x = x + 0$

(ii)  $\begin{cases} x \leq y \Rightarrow y = x + u \\ y \leq z \Rightarrow z = y + v \end{cases} \Rightarrow z = (x + u) + v = x + (u + v) \Rightarrow x \leq z$

此时  $x = z \Leftrightarrow u + v = 0 \Leftrightarrow u = 0 = v \Leftrightarrow x = y = z$ .

(iii)  $\forall x \in N$ . 令  $M = \{y \in N \mid x \leq y \text{ 或 } y \leq x \text{ 成立}\}$ .

即  $M$  为所有可以与  $x$  比较的数的全体. 则

1°  $0 \in M \quad (0 \leq x \text{ 或 } x)$

2°  $y \in M$ . 则  $y < x \Rightarrow x = y + u, u \neq 0 \Rightarrow x = y + sv = sy + v \Rightarrow sy < x \Rightarrow sy \in M$ .  
 命题2

或  $x \leq y \Rightarrow y = x + u \Rightarrow sy = s(x + u) = x + su \Rightarrow sy = x \Rightarrow sy \in M$ .

PAS  $\Rightarrow M = N$ .

##

定理13 (三歧律 trichotomy)  $\forall x, y \in N$ . 下述三者必居其一:

$x < y \quad x = y \quad \text{或} \quad x > y$ .

定理14  $x < y \Rightarrow sx \leq y$ .

定理15 ( $\mathbb{N}$  良序性)  $\phi \neq L \subseteq \mathbb{N}$ , 则  $L$  中存在最小数.

即存在  $l \in L$ , 使得  $l \leq x \quad \forall x \in L$ .

证 上述  $l$  的存在是必然的?

PF. 令  $M = \{y \in \mathbb{N} \mid y \leq x \quad \forall x \in L\}$

断言  $M \cap L \neq \phi$ .

(否则, 设  $M \cap L = \phi$ , 则)

1°  $0 \in M$ .

2°  $y \in M$ , 则  $y \leq x \quad \forall x \in L$

$\Rightarrow y < x \quad \forall x \in L \quad (M \cap L = \phi)$ ,

$\Rightarrow sy \leq x \quad \forall x \in L$

$\Rightarrow sy \in M$ .

PAS  $\Rightarrow M = \mathbb{N}$ .

矛盾. 事实上, 任取  $x \in L$ ,  $sx > x$  从而  $sx \notin M$

取  $l \in M \cap L$  即为所求.  $\#$

定理16 (第二归纳法) 设命题  $P(n)$  满足

(i)  $P(0)$  成立

(ii)  $P(k)$  对所有  $k < m$  成立  $\Rightarrow P(m)$  成立

则  $P(n)$  对所有  $n \in \mathbb{N}$  成立.

PF. 令  $A = \{n \in \mathbb{N} \mid P(n) \text{ 不成立}\}$

则  $A = \phi$ . 否则  $A \neq \emptyset$  则  $A$  中存在最小数  $m$ .

从而 1°  $P(m)$  不成立

2°  $P(k)$  成立  $\forall k < m$ . (由  $m$  最小性,  $k < m \Rightarrow k \notin A$ )

与定理假设矛盾.

## 2.0.4 整数的构造

$(\mathbb{N}, +, \cdot)$ : 满足

$$(x+y)+z = x+(y+z)$$

$$x+0 = 0+x = x$$

$$x+y = y+x$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$x \cdot 1 = x = 1 \cdot x$$

$$x \cdot y = y \cdot x$$

$$x \cdot (y+z) = xy + xz$$

希望构造  $-x$ , 使得  $x + (-x) = (-x) + x = 0$ .

本原就是要能作减法.



在  $\mathbb{N} \times \mathbb{N}$  上定义关系  $\sim$  如下:

$$(m, n) \sim (m', n') \iff m+n' = n+m'$$

( $m, n$ ) 就是心目中  $m-n$ , 不同  $m-n$  可能取值相同

定理 17  $\sim$  为  $\mathbb{N} \times \mathbb{N}$  上等价关系:

PE: (i)  $(m, n) \sim (m, n) \quad [m+n = m+n]$

(ii)  $(m, n) \sim (m', n') \implies (m', n') = (m, n)$

$$\begin{aligned} & \begin{matrix} \oplus & & \oplus \\ m+n' = n+m' & \iff & m'+n = n'+m \end{matrix} \end{aligned}$$

(iii)  $(m, n) \sim (m', n'), (m', n') \sim (m'', n'')$

$$\downarrow \quad \begin{matrix} m+n' = n+m' & m'+n'' = n'+m' \end{matrix}$$

$$\implies m+n' + \cancel{m'} + n'' = n + \cancel{m'} + n' + m''$$

加法消去律  $\implies m+n'' = n+m'$

$$\text{令 } \mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$

定义  $\mathbb{Z}$  上  $+$ ,  $\cdot$  如下:

$$(m, n) + (m', n') = (m+m', n+n')$$

$$(m, n) \cdot (m', n') = (mm' + nn', mn' + nm')$$

定理 18 (1) 上述  $+$ ,  $\cdot$  定义合理.

(2)  $(\mathbb{Z}, +, \cdot)$  形成一个交换环.

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim, \quad f, \dots$$

$$(m, n) \sim (m', n') \iff m+n = n'+m'$$

$$\mathbb{N} \hookrightarrow \mathbb{Z}, \quad a \mapsto (a, 0),$$

$$|\cdot|: \mathbb{Z} \rightarrow \mathbb{N}$$

$$a \mapsto \begin{cases} a \\ -a \end{cases}$$

$$(m, n) \sim \begin{cases} (a, 0) & m > n \quad m = n + a \\ (0, 0) & m = n \\ (0, a) & m < n \quad n = m + a \end{cases}$$

$$(0, a) = -(a, 0). \quad \mathbb{Z} = -\mathbb{N}_+ \cup \{0\} \cup \mathbb{N}_+$$

$$|ab| = |a| |b|$$

$$b \neq 0, \forall a \in \mathbb{Z} \setminus \{0\} : |a| \leq |ab| \iff b = \pm 1 \quad \left( \begin{array}{l} a, b \in \mathbb{N}, b \neq 0 \Rightarrow b = su \exists u \\ a \cdot su = a + au \geq a \end{array} \right)$$

$$(\mathbb{Z}, \leq): \quad \forall a, b \in \mathbb{N} \quad a \leq b$$

- $a \leq b$

$$-a \leq b, -b \leq a$$

$$\cdot \neg b \leq -a$$

$$[(m, n)] \leq [(m', n')] \iff m+n' \leq n+m'$$

设  $\phi \neq \Gamma \subseteq \mathbb{Z}$

若  $L \subseteq \mathbb{R}$  中有下界，即  $\exists x \in \mathbb{R}$  使得  $x \leq l$   $\forall l \in L$ . 则  $L$  中有最大数.

§2.1. 整除.

### 2.1.1 带余除法

定义 2.1 :  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . 若存在  $u \in \mathbb{Z}$  使得  $a = bu$ , 则称  $b$  整除  $a$ , 或称  $a$  被  $b$  整除, 记作  $b|a$ . 此时称  $b$  为  $a$  的 因子 (或 约数, divisor / factor)  $a$  为  $b$  的 倍数 (multiple).

· 若  $a \nmid bu \quad \forall u \in \mathbb{Z}$  则称  $b$  不整除  $a$ , 记作  $b \nmid a$

注:  $a \neq 0 \vee a \neq 0$

例 2.2  $a, b, c \in \mathbb{Z}$ .

(1)  $b, c \neq 0$ .  $a \mid b/a \iff bc/ac$ .  $b/a \iff \pm b / \pm a$

(2)  $b, c \neq 0, b|c, c|a \Rightarrow b|a$

(3)  $a|b, a|c \Rightarrow a|bx+cy \quad \forall x, y \in \mathbb{Z}$  ( $b, c$  的整线性组合)

(4)  $b|a, a \neq 0 \Rightarrow |b| \leq |a|$ .  $\Leftrightarrow \exists \frac{a}{b}, b|a \Rightarrow b = \pm a$ .

PF (i)  $\Rightarrow$   $b|a \Rightarrow a = bu \exists u \Rightarrow ac = (bu)c = (bc)u \Rightarrow bc|ac$   
 $\Leftarrow$   $bc|ac \Rightarrow ac = (bc)u = (bu)c \exists u \xRightarrow{c \neq 0} a = bu \Rightarrow b|a$

$$(2) \quad \begin{array}{l} b/c \Rightarrow b=cu \exists u \\ c/a \Rightarrow a=bv \exists v \end{array} \Rightarrow a=(cu)v = c(uv) \Rightarrow c/a$$

$$(3) \quad \left. \begin{array}{l} a/b \Rightarrow b=au \exists u \\ a/c \Rightarrow c=av \exists v \end{array} \right\} \Rightarrow bx+cy = a(ux+vy) \quad \forall x,y \Rightarrow a/bx+cy \quad \forall x,y$$

(4)  $a \neq 0, b|a \Rightarrow a = bu \quad \exists u \neq 0 \Rightarrow |b| \leq |a|$   
 $\nexists a|b, b|a \Rightarrow |a| = |b| \Rightarrow a = \pm b$

立同 余数

定理 2.3 (带余除法)  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . 则存在唯一确定的  $q, r \in \mathbb{Z}$ , 使得  $a = qb + r$ .

$$0 \leq r < |b|$$

证明: 存在性: 令  $I = \{a - qb \mid q \in \mathbb{Z}\} \cap \{x \mid x < |b|\}$ . 则  $I$  非空.

从而  $I$  中有最大元, 记作  $r$ . 且  $r = a - qb \exists q$ . 即有  $a = qb + r$ .

唯一性: 若  $\exists r_1, r_2$  满足  $a = qb + r_1$

$$\text{则 } qb + r_1 = qb + r_2 \Rightarrow (r_1 - r_2)b = r_2 - r_1$$

$$0 \leq r_1, r_2 < |b| \Rightarrow |r_1 - r_2| < |b| \Rightarrow r_1 - r_2 = 0 \text{ 且 } r_1 - r_2 = 0$$

$$\text{否则 } r_1 - r_2 \neq 0 \Rightarrow |r_1 - r_2| \geq |b| \text{ 矛盾.}$$

## §2.1.2 最大公因子

定义 2.4  $a, b$  不全为 0.  $d$  称为  $a, b$  的 最大公因子 (最大公约数, greatest common divisor)

若 (i)  $d|a, d|b$  (ii)  $\forall d' \in \mathbb{Z}, d'|a, d'|b \Rightarrow d' \leq d$ . 记作  $(a, b)$  或  $\gcd(a, b)$ .

若  $(a, b) = 1$ , 则称  $a, b$  互素 (coprime)

注: 1. 最大公因子存在. 记  $D = \{d \mid d|a, d|b\}$  则  $D \subseteq \mathbb{N}$ .

$1 \in D \Rightarrow D \neq \emptyset$  从而  $D$  中有最大元, 即为最大公因子.

2.  $(a, b) > 0$ .

命题 2.5 设  $a, b \in \mathbb{Z}$ . 则

$$(1) (\pm a, \pm b) = (a, b)$$

$$(2) (a, b) = (b, a)$$

$$(3) a \neq 0 \text{ 则 } (a, a) = (a, 0) = |a|$$

$$(4) (a, b) = (a + by, b) = (a, b + ax)$$

$$\text{PF (1)} \quad d|a \Leftrightarrow d|-a, \quad d|b \Leftrightarrow d|-b,$$

$$(a, b) = \max \{d \mid d|a, d|b\} = \max \{d \mid d|\pm a, d|\pm b\}$$

(2) 显然:

$$(3) a \neq 0, d|a \Rightarrow |d| \leq |a|. \text{ 而 } |a| | a.$$

$$(4) d|a, d|b \Rightarrow d|a + by$$

$$d|b, d|a + by \Rightarrow d|(a + by) - by \text{ 即 } d|a$$

$$\text{从而 } \{d \mid d|a, d|b\} = \{d \mid d|a + by, d|b\} = \{d \mid d|ax + by, d|a\} \neq \emptyset$$

定理 2.6  $a, b$  不全为 0. 则

(1) 若  $d > 0$  为  $a, b$  公因子即  $d|a, d|b$  且存在  $x, y \in \mathbb{Z}$  使得  $d = ax + by$  则  $d = (a, b)$ .

(2) 存在  $x, y \in \mathbb{Z}$  使得  $(a, b) = ax + by$ . 特别地, 若  $a, b$  互素, 则存在  $x, y$  使得  $ax + by = 1$ .

PF. (1) 若  $d'|a, d'|b$ , 则  $d'|d = ax + by \Rightarrow d' \leq |d| = d$ . 此外, 由假设,  $d|a, d|b$ ,

由定义知  $d = (a, b)$ .

(2) 令  $I = \{ax + by \mid x, y \in \mathbb{Z}\}$ .  $I_+ = I \cap \mathbb{N}_+ \neq \emptyset$  ( $|a|, |b| \in I$ ).

从而  $I_+$  中有最小元记作  $d$ . 设  $d = ax + by$ .

断言  $d = (a, b)$ .

由 (1) 只须证  $d$  为  $a, b$  公因子.

•  $d|a$ . 事实上, 由带余除法.  $a = qd + r, 0 \leq r < d$ .

$$\text{且 } a = q(ax + by) + r \Rightarrow r = (1 - qx)a + (-by) \in I$$

$$0 \leq r < d \Rightarrow r = 0 \text{ 则 } r < d \text{ 且 } r \in I_+ \text{ 与 } d \text{ 最小性矛盾.}$$

证毕.  $\square$

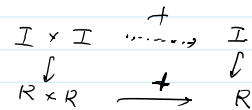
$0 \leq r < d \Rightarrow r=0$  则  $k| r < d$  且  $r \in I_+$  与  $d$  最小性矛盾.  
 同理,  $d|b$ . \*

定义 2.7 设  $R$  为含么环,  $\emptyset \neq I \subseteq R$ . 若  $I$  满足

- (1)  $\forall a, b \in I, a-b \in I$   
 (2)  $\forall a \in I, r \in R, ar, ra \in I$ .

则称  $I$  为  $R$  的一个 理想 (ideal)

证 = 1. (i)  $\Leftrightarrow \begin{cases} 0 \in I \\ -a \in I & \forall a \in I \\ a+b \in I & \forall a, b \in I \end{cases}$   
 $\Leftrightarrow (I, +)$  形成一子群.



2. 定义  $R$  上关系,  $r_1 \sim r_2$  若  $r_1 \in I + r_2$

则  $\sim$  为等价关系:  $\begin{cases} r \sim r & \Leftrightarrow 0 \in I \\ r_1 \sim r_2 \Rightarrow r_2 \sim r_1 & \Leftrightarrow "a \in I \Rightarrow -a \in I" \\ r_1 \sim r_2, r_2 \sim r_3 \Rightarrow r_1 \sim r_3 & \Leftrightarrow a, b \in I \Rightarrow a+b \in I \end{cases}$

令  $R/I = \{[r] | r \in R\}$  上  $\sim$

$$\begin{aligned} +: [a] + [b] &= [a+b] \\ \cdot: [a] \cdot [b] &= [ab] \end{aligned}$$

则  $+$  定义合理, 且  $(R/I, +, \cdot)$  形成一含么环.

3.  $I_1, I_2$  为理想. 则

$I_1 + I_2 \triangleq \{x+y | x \in I_1, y \in I_2\}$  为  $R$  理想.

例  $R$  交换环,  $a \in R$ . 则  $aR = \{ar | r \in R\}$  为  $R$  的一个理想. 称为  $a$  生成的 主理想. Principal ideal

- $aR = 0 \Leftrightarrow a = 0$
- $aR = R \Leftrightarrow a$  为  $R$  中乘法可逆元.

命题 2.8  $a, b \in \mathbb{Z}, b \neq 0$ . 则  $b|a \Leftrightarrow a \in b\mathbb{Z} \Leftrightarrow a\mathbb{Z} \subseteq b\mathbb{Z}$ .  
 证

定理 2.9  $I$  为  $\mathbb{Z}$  理想. 则  $\exists d \geq 0$  使得  $I = d\mathbb{Z}$ . ( $\mathbb{Z}$  为主理想整环)

证  $I = 0$ . 则取  $d = 0$

$I \neq 0$ . 则  $I_+ = I \cap \mathbb{N}_+ \neq \emptyset$ . ( $\forall a \in I \Rightarrow |a| \in I_+$ )  
 取  $d = \min I_+$ . 则  $I = d\mathbb{Z}$ .

定理 2.6'  $a, b \in \mathbb{Z}, a, b$  不全为 0,  $d > 0$ . 则  $d = (a, b) \Leftrightarrow d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

## 命题 2.10 7. 述成立

- (i)  $a, b$  的公因子均为  $(a, b)$  的因子
- (ii)  $m > 0, m(a, b) = (ma, mb)$
- (iii)  $(a, b) = d \Rightarrow (\frac{a}{d}, \frac{b}{d}) = 1$
- (iv)  $(a, m) = 1 = (b, m) \Rightarrow (ab, m) = 1$
- (v)  $c | ab, (c, b) = 1 \Rightarrow c | a$
- (vi)  $((a, b), c) = (a, (b, c))$

PF

- (i)  $(a, b) = ax + by, d | a, d | b \Rightarrow d | ax + by$
- (ii)  $m(a, b) | ma, m(a, b) | mb, \left. \begin{aligned} (a, b) = ax + by \Rightarrow m(a, b) &= (am)x + (bm)y \end{aligned} \right\} \Rightarrow m(a, b) = (ma, mb)$
- (iii)  $d = (a, b) = ax + by \Rightarrow \exists x, y$   
 $\text{is } \frac{a}{d}x + \frac{b}{d}y = 1$
- (iv)  $\left. \begin{aligned} (a, m) = 1 &\Rightarrow ax_1 + my_1 = 1 \\ (b, m) = 1 &\Rightarrow bx_2 + my_2 = 1 \end{aligned} \right\} \Rightarrow \begin{aligned} (ax_1 + my_1)(bx_2 + my_2) &= 1 \\ (ab)x_1x_2 + m(y_1bx_2 + y_1my_2 + ax_1y_2) &= 1 \end{aligned}$
- (v)  $cx + by = 1 \Rightarrow acx + aby = a$   
 $\left. \begin{aligned} c | ab \\ c | ac \end{aligned} \right\} \Rightarrow c | a$
- (vi)  $\left. \begin{aligned} ((a, b), c) &| (a, b) | a, \\ ((a, b), c) &| b \end{aligned} \right\} \Rightarrow ((a, b), c) | (a, (b, c))$   
 $\text{同理 } (a, (b, c)) | ((a, b), c)$

注 • 对  $a_1, \dots, a_n \neq 0$ , 可归纳定义  $(a_1, \dots, a_n) \triangleq ((a_1, \dots, a_{n-1}), a_n)$ ,  
 •  $(a_1, \dots, a_n)\mathbb{Z} = a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$ .

## 2.1.3 欧氏算法

$a, b \neq 0$ . 令  $r_1 = a, r_0 = b$

反复应用带余除法

$$\begin{aligned} r_{-1} &= q_0 r_0 + r_1 & 0 \leq r_1 < |b| \\ r_0 &= q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + r_{n+1} & r_{n+1} = 0 \end{aligned}$$

$\Rightarrow$  •  $r_1, r_2, \dots, r_n$  均为  $a, b$  整线性组合.  
 •  $r_n | r_{n-1}, r_{n-2}, \dots, r_1, r_0, r_{-1}$   
 $\Rightarrow r_n = (a, b)$

## 2.1.4 最小公倍数

定义 2.11 设  $a, b \neq 0$ ,  $m \neq 0$  称为  $a, b$  的最小公倍数 (最小公倍元, least common multiple)

记作  $m = [a, b]$  或  $\text{lcm}(a, b)$ . 满足:

$$(1) \quad a|m, \quad b|m \quad (2) \quad a|m', \quad b|m' \Rightarrow m \leq |m'|$$

命题 2.12 设  $a, b \neq 0$ .  $|m|$

(1)  $a, b$  的公倍数均为  $[a, b]$  的倍数

$$(2) \quad [ma, mb] = m[a, b]$$

$$(3) \quad (a, b) [a, b] = |ab|$$

$$(4) \quad [[a, b], c] = [a, [b, c]]$$

PF. (1)  $a|m', \quad b|m' \Rightarrow [a, b] \leq |m'|$  由

$$|m'| = q[a, b] + r, \quad 0 \leq r < [a, b]$$

$$\Rightarrow a|r. \quad \text{由 } [a, b] \text{ 最小性知 } r=0.$$

$$(2) \quad \left. \begin{array}{l} ma|m[a, b], \quad mb|n[a, b] \\ a|\frac{[ma, mb]}{m}, \quad b|\frac{[ma, mb]}{m} \end{array} \right\} \Rightarrow [a, b] | \frac{[ma, mb]}{m} \Rightarrow m[a, b] = [ma, mb]$$

(3) 若  $(a, b) = 1$ .  $a|m, \quad b|m$

$$ax + by = 1 \Rightarrow axm + bym = m$$

$$ab|axm, \quad ab|bym \Rightarrow ab|m.$$

$$\Rightarrow |ab| = [a, b].$$

$$(a, b) [a, b] = \left| \frac{a}{(a, b)} \cdot \frac{b}{(a, b)} \right| \quad \left( \left( \frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1 \right)$$

$$\Rightarrow (a, b) [a, b] = |a||b|.$$

$$(4) \quad \left. \begin{array}{l} a|[a, b] | [[a, b], c] \\ b|[a, b] | [[a, b], c] \\ c|[a, b], c \end{array} \right\} \Rightarrow [b, c] | [[a, b], c] \Rightarrow [a, [b, c]] | [[a, b], c]$$

$$[a, [b, c]] | [[a, b], c].$$

证.  $[a, b] \mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}.$

$$\text{由定义} \quad [a_1, a_2, \dots, a_n] \triangleq [[a_1, \dots, a_{n-1}], a_n]$$

## 第三章 同余理论

### §3.1 同余

定义 3.1 设  $m$  为正整数,  $a, b \in \mathbb{Z}$ . 若  $m | a - b$ , 则称  $a$  与  $b$  模  $m$  同余 (congruent modulo  $m$ ), 记作  $a \equiv b \pmod{m}$ .

否则, 称  $a$  与  $b$  模  $m$  不同余, 记作  $a \not\equiv b \pmod{m}$ .

命题 3.2 同余关系为等价关系, 其等价类称为同余类.

PF. (反身性)  $m | 0 = a - a \Rightarrow a \equiv a \pmod{m}$ .

(对称性)  $m | (a - b) \Leftrightarrow m | (b - a)$   
 $\Downarrow \text{定义} \quad \quad \quad \Downarrow \text{定义}$   
 $a \equiv b \pmod{m} \quad \quad \quad b \equiv a \pmod{m}$

(传递性)  $m | a - b, \quad m | b - c \Rightarrow m | a - c$   
 $\Downarrow \quad \quad \quad \Downarrow \quad \quad \quad \Downarrow$   
 $a \equiv b \pmod{m}, \quad b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

$[a]$  记作  $\bar{a}$ , 或  $a + m\mathbb{Z}$ .

命题 3.3  $a \equiv b \pmod{m}, \quad c \equiv d \pmod{m}$ . 则

(1)  $a \pm b \equiv c \pm d \pmod{m}$

(2)  $ab \equiv cd \pmod{m}$

推论 3.4 设  $f(x_1, x_2, \dots, x_n)$  为关于  $x_1, \dots, x_n$  的整系数多项式.  $a_i \equiv b_i \pmod{m} \quad (i=1, \dots, n)$

$$f(a_1, \dots, a_n) \equiv f(b_1, \dots, b_n) \pmod{m}$$





命题 3.5 (1)  $a \equiv b \pmod{m}$   $\Leftrightarrow \exists d \mid m, d > 0, a \equiv b \pmod{d}$

$$(2) \quad d > 0 \quad \exists d \mid a \equiv b \pmod{m} \Leftrightarrow ad \equiv bd \pmod{md}$$

$$(3) \quad c \neq 0 \quad \exists c \mid ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$$

特别地,  $(c, m) = 1 \quad ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$

$$(4) \quad a \equiv b \pmod{m_i} \quad i=1, \dots, n \Rightarrow a \equiv b \pmod{[m_1, \dots, m_n]}$$

PF (1)  $a \equiv b \pmod{m} \stackrel{\text{定义}}{\Leftrightarrow} m \mid a-b$

$$\wedge d \mid m \Rightarrow d \mid a-b \Rightarrow a \equiv b \pmod{d}$$

$$(2) \quad d > 0 \quad a \equiv b \pmod{m} \quad ad \equiv bd \pmod{md}$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ m \mid (a-b) & \Leftrightarrow & md \mid (ad-bd) \end{array}$$

$$(3) \quad c \neq 0 \quad ac \equiv bc \pmod{m}$$

$\uparrow$

$$m \mid ac-bc \Leftrightarrow m \mid (a-b)c \Leftrightarrow \frac{m}{(m,c)} \mid (a-b) \frac{c}{(m,c)}$$

$$\left(\frac{m}{(m,c)}, \frac{c}{(m,c)}\right) = 1 \xrightarrow{\text{定义}} \frac{m}{(m,c)} \mid (a-b)$$

$$\stackrel{\text{定义}}{\Leftrightarrow} a \equiv b \pmod{\frac{m}{(m,c)}}$$

$$(4) \quad a \equiv b \pmod{m_i} \quad i=1, \dots, n$$

$$\Leftrightarrow m_i \mid (a-b) \quad i=1, \dots, n$$

$$\Leftrightarrow [m_1, \dots, m_n] \mid (a-b)$$

$$\Leftrightarrow a \equiv b \pmod{[m_1, \dots, m_n]}$$

命题 3.6 同余方程  $ax \equiv b \pmod{m}$  有解  $\Leftrightarrow (a, m) \mid b$

此时, 方程解集为模  $\frac{m}{(a,m)}$  的一个同余类. 特别地,

$$ax \equiv 1 \pmod{m} \text{ 有解 } \Leftrightarrow (a, m) = 1$$





PF (1) 若存在整数  $x_0$  使得  $ax_0 \equiv b \pmod{m}$ .  
 即  $ax_0 + my = b$  (存在  $y \in \mathbb{Z}$ ).  
 从而  $(a, m) \mid b$ .

反之, 由裴蜀定理 存在  $x_0, y_0 \in \mathbb{Z}$  使得  
 $ax_0 + my_0 = (a, m)$ .

则  $x_0 \cdot \frac{b}{(a, m)}$  即为方程  $ax \equiv b \pmod{m}$   
 的一个解

(2) 若方程  $ax \equiv b \pmod{m}$  有一个特解  $x_0$ .

则  $x_0 + \frac{m}{(a, m)} \cdot y, y \in \mathbb{Z}$  为方程的解.

反之, 若  $x_1$  为  $ax \equiv b \pmod{m}$  的一个解, 则  
 $ax_0 \equiv ax_1 \equiv b \pmod{m}$

即有  $m \mid a(x_0 - x_1)$ , 故  $\frac{m}{(m, a)} \mid x_0 - x_1$ .

从而方程的解集为一个模  $\frac{m}{(m, a)}$  的同余类.

例 求解  $5x \equiv 12 \pmod{13}$

解: 由欧氏除法:  $13 = 5 \times 2 + 3, \quad 5 = 3 \times 2 - 1, \quad 3 = 2 \times 1 + 1$

$\Rightarrow 1 = (5, 13) = 13 \times 2 + 5 \times (-5)$ .

$5x \equiv 1 \pmod{13}$  的解为  $x \equiv -5 \pmod{13}$

$\Rightarrow 5x \equiv 12 \pmod{13}$  的解为

$x \equiv 12 \cdot (-5) \equiv 5 \pmod{13}$ .

### § 3.2. 中国剩余定理

$m_1, \dots, m_n$  两两互素.

$a_1, \dots, a_n \in \mathbb{Z}$ .

考虑同余方程组

$$(*) \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$



定理 3.7. (中国剩余定理). 上述同余方程必有解, 且解集为模  $m_1 m_2 \dots m_n$  的一个同余类.

证明. 考察方程组  $L_1: \begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases}$

由于  $m_2 \dots m_n$  与  $m_1$  互素, 有

$$m_2 \dots m_n y \equiv 1 \pmod{m_1}$$

有解  $x_0$ . 令  $\alpha_1 = m_2 \dots m_n x_0$ . 则

$\alpha_1$  为  $L_1$  的一组解.

同理, 令  $\alpha_2, \dots, \alpha_n$  分别为方程组

$$L_2, \dots, L_n \text{ 的一组解. 其中 } L_i = \begin{cases} x \equiv 0 \pmod{m_1} \\ \vdots \\ x \equiv 0 \pmod{m_{i-1}} \\ x \equiv 1 \pmod{m_i} \\ x \equiv 0 \pmod{m_{i+1}} \\ \vdots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

则  $\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n$  为

方程组 \* 的一组解.

不难证明, 若  $\alpha$  为方程 \* 的一组解, 则  $\alpha$  的所有解具有形式  $\alpha + m_1 m_2 \dots m_n y, y \in \mathbb{Z}$ .

例 
$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \rightarrow x \equiv 70 \times 2 + 21 \times 3 + 15 \times 2 \pmod{105} \equiv 23 \pmod{105}$$

注:  $\frac{\mathbb{Z}}{m_1 m_2 \dots m_n \mathbb{Z}} \xrightarrow{1-1} \frac{\mathbb{Z}}{m_1 \mathbb{Z}} \times \frac{\mathbb{Z}}{m_2 \mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_n \mathbb{Z}}$

$\hookrightarrow \{a + m_1 m_2 \dots m_n \mathbb{Z} \mid a \in \mathbb{Z}\} \mapsto (a + m_1 \mathbb{Z}, a + m_2 \mathbb{Z}, \dots, a + m_n \mathbb{Z})$   
模  $m_1 m_2 \dots m_n \mathbb{Z}$  同余类与  $n$  元组  $(a + m_1 \mathbb{Z}, \dots, a + m_n \mathbb{Z})$  为集合双射.



定理 3.8  $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$  形成一个交换环, 其中:

•  $\mathbb{Z}/m\mathbb{Z}$  为模  $m$  同余类的集合,

•  $+$ :  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ ,  $0_{\mathbb{Z}/m\mathbb{Z}} = \bar{0}$   
 $\bar{a} + \bar{b} \triangleq \overline{a+b}$

•  $\times$ :  $\bar{a} \cdot \bar{b} \triangleq \overline{a \cdot b}$ ,  $1_{\mathbb{Z}/m\mathbb{Z}} = \bar{1}$

定理 3.9  $(\mathbb{Z}/m\mathbb{Z})^\times = \{ \bar{a} \mid (a, m) = 1, 0 \leq a < m \}$

其中  $(\mathbb{Z}/m\mathbb{Z})^\times$  定义为  $\mathbb{Z}/m\mathbb{Z}$  中乘法可逆元的集合.

定义 3.10 欧拉函数,  $\varphi: \mathbb{N}_+ \rightarrow \mathbb{N}_+$  定义为

$$\varphi(n) \triangleq |(\mathbb{Z}/n\mathbb{Z})^\times|$$

例:  $m = 3 \times 5$ , 则  $\varphi(m) = 8$ .

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{ \bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14} \}$$

•  $m = p^r$   $p$  为素数  $r \geq 1$ .

$$\varphi(p^r) = p^{r-1}(p-1).$$

定理 3.11 下述等价

(1)  $\mathbb{Z}/m\mathbb{Z}$  为整环. 即  $\bar{a} \neq 0, \bar{b} \neq 0 \Rightarrow \bar{a}\bar{b} \neq 0$ .

(2)  $m$  为素数

(3)  $\mathbb{Z}/m\mathbb{Z}$  为域. 即非 0 元可逆.

PF. (1)  $\Rightarrow$  (2). 设  $\mathbb{Z}/m\mathbb{Z}$  为整环. 若  $m$  有非平凡因子, 即  $m = x \cdot y$ ,  $1 < x, y < m$ . 则

$m \nmid x, m \nmid y \Rightarrow \bar{x} \neq 0, \bar{y} \neq 0$ . 但  $m \mid xy$  即  $\bar{x} \cdot \bar{y} = 0$ . 与  $\mathbb{Z}/m\mathbb{Z}$  整环矛盾.





取  $m$  为素数

(2)  $\Rightarrow$  (3)  $m$  素, 则  $\forall 1 \leq x < m, (x, m) = 1$ . 即  $x$  在  $\mathbb{Z}/m\mathbb{Z}$  中可逆, 故  $\mathbb{Z}/m\mathbb{Z}$  为域

(3)  $\Rightarrow$  (1) 显然

注:  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  称为  $p$ -元-素域. 若  $p$  为素数,

$\{a_1, \dots, a_m\}$  称为模  $m$  的一个完全剩余系. 若  $a_i \not\equiv a_j \pmod{m} \quad \forall i \neq j$ .

$\{a_1, \dots, a_{q(m)}\}$  称为模  $m$  的一个缩系. 若  $a_i \not\equiv a_j \pmod{m} \quad \forall i \neq j, (a_i, m) = 1, \forall i$ .

注: 设  $(c, m) = 1, c \in \mathbb{Z}$ .

$\{a_1, \dots, a_m\}$  为完全  $\Rightarrow \{ra_1+c, \dots, ra_m+c\}$  为完全.

$\{a_1, \dots, a_{q(m)}\}$  为缩系  $\Rightarrow \{ra_1, \dots, ra_m\}$  为缩系.

环的直积:

$R_1, R_2$  为环 (不一定交换). 在  $R_1 \times R_2$  上

定义  $+$ :  $(R_1 \times R_2) \times (R_1 \times R_2) \rightarrow R_1 \times R_2$

$\cdot$ :  $(R_1 \times R_2) \times (R_1 \times R_2) \rightarrow R_1 \times R_2$ .

$(a_1, a_2) + (b_1, b_2) \triangleq (a_1 + b_1, a_2 + b_2)$

$(a_1, a_2) \cdot (b_1, b_2) \triangleq (a_1 \cdot b_1, a_2 \cdot b_2)$

则  $R_1 \times R_2$  在上述运算下形成一个环. 其 0 元为

$(0_{R_1}, 0_{R_2})$ ,  $(a_1, a_2)$  的负元为  $(-a_1, -a_2)$ .

1 元为  $(1_{R_1}, 1_{R_2})$ .

注  $(R_1 \times R_2)^{\times} = R_1^{\times} \times R_2^{\times}$



定义 3.12  $R_1, R_2$  为环. 映射  $f: R_1 \rightarrow R_2$  称为一个 环同态 (homomorphism of rings), 若

$$(1) \quad f(a+b) = f(a) + f(b)$$

$$(2) \quad f(ab) = f(a)f(b)$$

$$(3) \quad f(1_{R_1}) = 1_{R_2}$$

证: 1.  $f(0_{R_1}) = 0_{R_2}$

$$(f(0_{R_1}) = f(0_{R_1} + 0_{R_1}) = f(0_{R_1}) + f(0_{R_1}))$$

2.  $f(1_{R_1}) = 1_{R_2}$  不能由 (1) (2) 推出, 证:

$$\varphi: R_1 \longrightarrow R_1 \times R_2$$

$$a \longmapsto (a, 0)$$

满足定义中的 (1), (2). 但不满足 (3)

定理 3.13 (同态基本定理)  $f: R_1 \rightarrow R_2$  为环同态. 则

$$(1) \quad \text{Ker } f = f^{-1}(0_{R_2}) = \{a \in R_1 \mid f(a) = 0_{R_2}\} \text{ 为 } R_1 \text{ 理想.}$$

$$(2) \quad \text{Im } f = \{f(a) \mid a \in R_1\} \text{ 为 } R_2 \text{ 的子环.}$$

$$(3) \quad f \text{ 诱导环的同构 } \bar{f}: R_1/\text{Ker } f \xrightarrow{\sim} \text{Im } f$$

$$[r] \longmapsto f(r)$$

PF. (1)  $a \in \text{Ker } f, \quad b \in \text{Ker } f \quad a+b \in \text{Ker } f.$

$$\begin{array}{ccc} \downarrow & \downarrow & \uparrow \\ f(a)=0 & f(b)=0 & \Rightarrow f(a-b)=0 \end{array}$$

(2)  $a \in \text{Ker } f, \quad r \in R_1$

$$\Rightarrow f(ra) = f(r)f(a) = 0 \Rightarrow ra \in \text{Ker } f$$

$$f(ar) = f(a)f(r) = 0 \Rightarrow ar \in \text{Ker } f.$$

即  $\text{Ker } f$  为  $R_1$  理想

(2) 显然.



(3)  $f$  为单射, 必为环同态.

$f$  为满射, (由于  $\ker f$  为  $f$  的零点集)

$f$  为单射, ( $\Leftrightarrow \ker f = 0$ .)

##

定理 3.14 (中国剩余定理)  $m_1, \dots, m_n$  两两互素, 则

有环同构  $\mathbb{Z}/m_1 \cdots m_n \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/m_n \mathbb{Z}$

$$r + m_1 \cdots m_n \mathbb{Z} \mapsto (r + m_1 \mathbb{Z}, \dots, r + m_n \mathbb{Z})$$

推论 3.15  $m_1, \dots, m_n$  两两互素, 则

$$(1) (\mathbb{Z}/m_1 \cdots m_n \mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m_1 \mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_n \mathbb{Z})^\times$$

$$(2) \varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n)$$

$$(3) \varphi(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = p_1^{\alpha_1-1}(p_1-1) p_2^{\alpha_2-1}(p_2-1) \cdots p_s^{\alpha_s-1}(p_s-1)$$





### § 3.3 Euler定理与 Fermat 小定理

$m > 0$ .  $r_1, \dots, r_{\varphi(m)}$  为  $m$  的一个系.

$\forall a, (a, m) = 1 \Rightarrow ar_1, \dots, ar_{\varphi(m)}$  为  $m$  的一个系.

从而  $\bar{ar}_1, \dots, \bar{ar}_n$  为  $\bar{r}_1, \dots, \bar{r}_n$  的一个排列.

$$\begin{aligned} \text{即有 } r_1 \cdots r_{\varphi(m)} &\equiv (ar_1) \cdots (ar_{\varphi(m)}) \pmod{m} \\ &\equiv a^n r_1 \cdots r_{\varphi(m)} \pmod{m} \end{aligned}$$

$$\Rightarrow a^n \equiv 1 \pmod{m}$$

从而有

定理 3.16 (Euler) 对  $\forall a \in \mathbb{Z}$ ,  $(a, m) = 1$  均有  
 $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

推论 3.17 (Fermat) 素数  $p$ , 则  $a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{Z}$ .

PF.  $\cdot (a, p) \neq 1$  则  $p \mid a$ ,  $a^p \equiv a \equiv 0 \pmod{p}$

$\cdot (a, p) = 1$ . 由定理 3.16 以及  $\varphi(p) = p-1$  知

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{从而 } a^p \equiv a \pmod{p}.$$

命题得证.

3.16 与 3.17 的环论解释:

注意到  $\in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  中,  $\forall a \in \mathbb{Z}$ ,  $\overbrace{p \cdot \bar{a}}^{p \times \bar{a}} = \bar{a} + \dots + \bar{a} = \bar{0}$ .

另一方面,  $\forall 1 \leq k \leq p-1$ ,  $p \nmid C_p^k = \frac{p!}{k!(p-k)!}$ ,

( $p \nmid p!$ ,  $p \nmid k!$ ,  $p \nmid (p-k)!$ )

从而由二项式定理有

命题 3.18  $\in \mathbb{F}_p$  中,  $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p \quad \forall \bar{a}, \bar{b} \in \mathbb{F}_p$ .





## Fermat + 归纳法证明

$$0^p \equiv 0 \pmod{p} \quad 1^p \equiv 1 \pmod{p}$$

$$\text{若 } n^p \equiv n \pmod{p} \quad \text{则}$$

$$(n+1)^p \equiv n^p + 1^p \equiv n+1 \pmod{p}$$

从而由归纳法  $n^p \equiv n \pmod{p}$  恒成立

$$(证 \quad a \equiv b \pmod{p} \iff \bar{a} = \bar{b} \in \mathbb{F}_p)$$

## 引理 3.19

$$a \equiv b \pmod{p} \quad p \text{ 素}$$

$$\text{则 } a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}} \quad \forall n \geq 0$$

PF 由归纳法知 事实  $\hookrightarrow$

$$\cdot n=0, \quad a \equiv a^{p^0} \equiv b^{p^0} \equiv b \pmod{p} \text{ 即为引理条件}$$

$$\cdot \text{若 } a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$$

$$\text{则 } a^{p^n} = b^{p^n} + p^{n+1} \cdot x \quad \exists x \in \mathbb{Z}$$

$$\text{从而 } a^{p^{n+1}} = (b^{p^n} + p^{n+1}x)^p$$

$$= b^{p^{n+1}} + p^{n+2}y, \quad y = b^{p^n(p-1)} \cdot x + \dots$$

$$\text{即有 } a^{p^{n+1}} \equiv b^{p^{n+1}} \pmod{p^{n+2}} \quad \#$$

## Euler 定理证明

$$m = p_1^{\alpha_1} \dots p_s^{\alpha_s} \quad \text{则 } \varphi(m) = p_1^{\alpha_1-1} \dots p_s^{\alpha_s-1} (p_s-1)$$

$$(a, m) = 1 \quad \text{由中国剩余定理,}$$

$$\text{要证: } a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$\text{只需证明 } a^{\varphi(m)} \equiv 1 \pmod{m_i} \quad i=1, \dots, s$$

$$\text{由 Fermat 小定理 } a^{p_i-1} \equiv 1 \pmod{p_i} \quad \forall i$$

$$\text{从而由 3.19 知 } (a^{p_i-1})^{p_i^{\alpha_i-1}} \equiv 1 \pmod{p_i^{\alpha_i}} \quad \forall i$$

$$\text{从而 } a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}} \quad \forall i \quad \#$$



群论解释:

回顾:  $(G, \cdot)$  为群. 若

(1)  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$

(2)  $\exists 1_G \in G$ , 使得  $1_G \cdot a = a = a \cdot 1_G \quad \forall a \in G$

(3)  $\forall a \in G, \exists b \in G$  使得  $a \cdot b = b \cdot a = 1_G$

满足 (3) 的  $b$  由  $a$  唯一确定, 称为  $a$  的逆, 记作  $a^{-1}$ .

定义 3.20 设  $g \in G$ . 若存在正整数  $n \in \mathbb{N}$ , 使得  $g^n = 1$

则称满足  $g^n = 1$  的最小正整数  $n$  为  $g$  的 阶 (order),

记作  $\text{ord}(g)$  或  $o(g)$ .

若上述  $n$  不存在, 则称  $g$  的阶为无限, 或

记作  $o(g) = \infty$ .

证:  $o(g) = 1 \iff g = 1_G$

$g^m = 1, g^n = 1 \implies g^{(m,n)} = 1$

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

$$g^{(m,n)} = g^{mx+ny} = g^{mx} \cdot g^{ny} = (g^m)^x \cdot (g^n)^y = 1.$$

其中: 
$$g^m = \begin{cases} \overbrace{g \cdot g \cdots g}^m & m > 0 \\ 1 & m = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_m & m < 0 \end{cases}$$

则有 
$$\begin{cases} g^m \cdot g^n = g^{m+n} \\ g^m \cdot n = (g^m)^n \end{cases} \quad \forall m, n \in \mathbb{Z}$$

即 
$$\begin{array}{ccc} f: & (\mathbb{Z}, +) & \longrightarrow G \\ g: & m & \longmapsto g^m \end{array} \quad \text{为群同态}$$





$$\text{Ker } f_g = \{n \in \mathbb{Z} \mid f_g(n) = g^n = 1\}$$

$$\text{则 } o(g) = \begin{cases} \text{Ker } f_g \text{ 中的最小正整数, 若 } \text{Ker } f_g \neq \{0\} \\ \infty & \text{Ker } f_g = \{0\} \end{cases}$$

例  $(\mathbb{Z}/n\mathbb{Z}, +)$

$$o(\bar{1}) = n, \quad o(\bar{d}) = \frac{n}{(n, d)}$$

$$S' = \{z \in \mathbb{C} \mid |z| = 1\} \quad (S', \cdot) \text{ 为群}$$

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

$$= \left\{ e^{\frac{2k\pi i}{n}} \mid k=0, 1, \dots, n-1 \right\}$$

$$= \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k=0, 1, \dots, n-1 \right\}$$

命题 3.2  $G$  为有限交换群 则  $\forall g, o(g) < \infty$  且  $o(g) \mid |G|$ .

PF. (1) 考察集合  $\{g, g^2, g^3, \dots\}$  由于  $|G| < \infty$  知  $\exists i < j$  使得  $g^i = g^j$ .

从而  $g^{j-i} = 1$ . 即有  $o(g) < \infty$ .

(2) 令  $G = \{g_1, \dots, g_n\}$   $n = |G|$ .

则  $\forall g \in G, G = \{gg_1, \dots, gg_n\}$ .

( $gg_i = gg_j \Rightarrow g_i = g_j$ )

从而  $gg_1, \dots, gg_n$  为  $g_1, \dots, g_n$  的一个排列.

由于  $G$  为交换群

$$g_1 \cdots g_n = (gg_1) \cdots (gg_n) = g^n (g_1 \cdots g_n)$$

$$\Rightarrow g^n = 1.$$

另一方面  $g^{o(g)} = 1$ . 有  $g^{(o(g), n)} = 1$ .

由  $o(g)$  的最小性知  $o(g) \mid n = |G|$ .



## 第四章 原根与指数

## §4.1 子群与循环群

定义 4.1  $G$  为群  $G$  的非空子集  $H$  称作  $G$  的一个子群, 若

$$(1) \quad 1_G \in H$$

$$(2) \quad h^{-1} \in H \quad \forall h \in H$$

$$(3) \quad h_1, h_2 \in H \quad \forall h_1, h_2 \in H$$

注  $\emptyset \neq H \subseteq G$  则下述等价

$$H \text{ 为 } G \text{ 的子群} \Leftrightarrow gh^{-1} \in H, \forall g, h \in H$$

$$\Leftrightarrow H \text{ 在 } \cdot \text{ 下封闭, 且 } (H, \cdot) \text{ 形成一个群}$$

- $\emptyset \neq S \subseteq G$   $G$  中包含  $S$  的最小的子群称为  $S$  生成的子群, 记作  $\langle S \rangle$ . 若  $G = \langle S \rangle$  则称  $S$  为  $G$  的生成元.
- 若存在  $g$ , 使得  $G = \langle g \rangle$ . 则称  $G$  为循环群 (cyclic group)  $g$  为  $G$  的一个生成元.

例  $(\mathbb{Z}, +)$  ,  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$(\mathbb{Z}/n\mathbb{Z}, +)$  ,  $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle \quad \forall (k, n) = 1$

命题 4.2 设  $G$  为循环群. 则

$$(1) \quad G \cong \mathbb{Z} \text{ 或}$$

$$(2) \quad \text{存在 } n > 0 \text{ 使得 } G \cong \mathbb{Z}/n\mathbb{Z}$$

PF: 任取  $G$  的一个生成元  $g$ . 考察映射

$$f_g: \mathbb{Z} \rightarrow G$$

则  $f_g$  为满同态.

$$(1) \quad \text{若 } f_g \text{ 为单同态. 则 } f_g \text{ 为同构. 即 } G \cong \mathbb{Z},$$

$$(2) \quad f_g \text{ 不为单同态. 此时 } g \text{ 的阶 } o(g) = n < \infty.$$

$$\ker f_g = \{m \mid g^m = 1\} = n\mathbb{Z}.$$

$$(g^m = 1 \Leftrightarrow o(g) \mid m)$$

$$\text{由同态基本定理, } \mathbb{Z}/n\mathbb{Z} \cong G.$$

$$\left( \text{或直接构造群同构 } \mathbb{Z}/n\mathbb{Z} \rightarrow G \right)$$

$$\bar{m} \mapsto g^m$$

由上述命题证明可知, 对循环群  $G$ ,  $G$  任一生成元的阶等于群  $G$  的阶.

有限群  $G$  为循环群  $\Leftrightarrow G$  中存在元素  $g$ , 使得  $o(g) = |G|$

例  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  为循环群  $\Leftrightarrow (m, n) = 1$

注意到  $gh = hg \Rightarrow o(gh) = [o(g), o(h)]$

" $\Leftarrow$ "  $(m, n) = 1$  则  $(\bar{1}, \bar{1})$  的阶为  $[m, n] = mn$

" $\Rightarrow$ "  $\forall (g_1, g_2) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ,

$o(g_1) \mid m, o(g_2) \mid n$ , 从而  $o((g_1, g_2)) \mid [m, n]$

若  $(m, n) \neq 1$  则  $o((g_1, g_2)) \leq [m, n] < mn$ ,  $G$  中无  $mn$  阶元.

命题 4.3  $g \in G$  则  $o(g) = |\langle g \rangle|$

循环群  $G$  的性质可总结如下.

命题 4.4  $n > 0, G = \mathbb{Z}/n\mathbb{Z}$

(1)  $\forall 0 \leq k < n, o(\bar{k}) = \frac{n}{(k, n)}$

(2)  $G$  的所有生成元为  $\bar{k}, (k, n) = 1$

(3)  $G$  的任一子群均为循环群.

(4)  $\forall 1 \leq d \mid n, G$  有唯一  $d$  阶子群, 其所有生成元为  $a \cdot \frac{n}{d}, (a, d) = 1$ .

(5)  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

PF (1) 只须证明: a)  $\frac{n}{(k, n)} \cdot \bar{k} = \bar{0}$

b)  $d \cdot \bar{k} = \bar{0}, d > 0 \Rightarrow \frac{n}{(k, n)} \leq d$

a)  $\frac{n}{(k, n)} \bar{k} = \bar{0} \Leftarrow n \mid \frac{n}{(k, n)} k$

b)  $d \bar{k} = \bar{0} \Leftrightarrow n \mid dk$

$\Leftrightarrow \frac{n}{(k, n)} \mid d \frac{k}{(k, n)}$

$\Rightarrow \frac{n}{(k, n)} \mid d \quad \left( \left( \frac{n}{(k, n)}, \frac{k}{(k, n)} \right) = 1 \right)$

$\Rightarrow \frac{n}{(k, n)} \leq d$

(2) 由 (1) 及命题 4.3 易得.

(3) 设  $H \leq G$  令  $\tilde{H} = \bigcup_{\bar{a} \in H} \bar{a} \subseteq \mathbb{Z}$  ( $\bar{a}$  为  $\mathbb{Z}$  中元素)

易证  $\tilde{H}$  为  $\mathbb{Z}$  的子群.



$$\left[ \begin{array}{l} \tilde{H} \text{ 由所有形如 } a + nx \text{ 的元素组成, 其中 } \bar{a} \in H, x \in \mathbb{Z} \\ \cdot \quad 0 \in \tilde{H} \quad \bar{0} \in H \\ \cdot \quad a + nx \in \tilde{H} \Rightarrow \bar{a} \in H \Rightarrow -\bar{a} \in H \\ \quad \quad \quad \Rightarrow -a - nx \in \tilde{H} \\ \cdot \quad a + nx \in \tilde{H}, b + ny \in \tilde{H} \\ \quad \Rightarrow \bar{a} \in H, \bar{b} \in H \Rightarrow \overline{a+b} \in H \\ \quad \Rightarrow a+b + n(x+y) \in \tilde{H} \end{array} \right]$$

从而  $\tilde{H} = d\mathbb{Z}$ . 其中  $d$  为  $\tilde{H}$  中的最小正整数.

我们断言  $H = \langle \bar{d} \rangle = \{ \bar{0}, \bar{d}, \bar{2d}, \dots, \overline{n-d} \}$

- 由  $\tilde{H}$  构造知  $\bar{d} \in H$ , 从而  $H \supseteq \langle \bar{d} \rangle$ .
- $\forall \bar{m} \in H$ , 知  $m \in \tilde{H} \Rightarrow d \mid m$   
从而  $\bar{m} \in \langle \bar{d} \rangle$ . 即有  $H \subseteq \langle \bar{d} \rangle$ .

(4) 由 (3),  $\mathbb{Z}/n\mathbb{Z}$  子群均为循环群. 从而子群的阶均为  $n$  的因子.

设  $H$  为  $G$  的  $d$  阶子群. 则  $d \mid n$ .  
令  $H_d = \{ \bar{0}, \frac{n}{d}, \frac{2n}{d}, \dots, \frac{(d-1)n}{d} \}$

易证  $H_d$  为一个  $d$  阶子群.

另一方面,  $\forall \bar{m} \in H$ ,  $\bar{m}$  阶为  $d$  的因子.

从而  $d\bar{m} = \bar{0}$  即

$$n \mid dm \Leftrightarrow \frac{n}{d} \mid m.$$

$$\Rightarrow \bar{m} \in \langle \frac{n}{d} \rangle \Rightarrow H \subseteq H_d \quad \left. \begin{array}{l} |H| = |H_d| = d \end{array} \right\} \Rightarrow H = H_d$$

从而  $H_d$  为  $\mathbb{Z}/n\mathbb{Z}$  唯一的一个  $d$  阶子群

(5) 令  $\text{End}(\mathbb{Z}/n\mathbb{Z}) = \{ f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \mid f \text{ 为群同态} \}$ .

则  $\text{End}(\mathbb{Z}/n\mathbb{Z})$  在映射复合下形成一个含么半群. 么元为  $\text{id}$ .

显然  $f \in \text{End}(\mathbb{Z}/n\mathbb{Z})$  由  $f(\bar{1})$  唯一确定,

$$\text{事实上, } f(\bar{m}) = m f(\bar{1})$$

从而我们得到映射

$$\begin{aligned} \Phi: \text{End}(\mathbb{Z}/n\mathbb{Z}) &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ f &\longmapsto f(1) \end{aligned}$$

我们断言:  $\Phi(f \circ g) = \Phi(f) \Phi(g)$

$$\begin{aligned} \Phi(f \circ g) &= (f \circ g)(1) = f(g(1)) = g(1)f(1) \\ &= \Phi(g)\Phi(f) = \Phi(f)\Phi(g) \end{aligned}$$

$$\text{且有 } \Phi(\text{Id}) = 1$$

即  $\Phi$  为含么半群  $(\text{End}(\mathbb{Z}/n\mathbb{Z}), \circ)$  与  $(\mathbb{Z}/n\mathbb{Z}, \cdot)$  之间的同态. 易证  $\Phi$  为双射, 从而为同构.

•  $f$  由  $f(1)$  唯一确定  $\Rightarrow \Phi$  单

•  $\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z}$ , 构造映射

$$\begin{aligned} f_{\bar{k}}: \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \bar{m} &\longmapsto \overline{mk} \end{aligned}$$

$$\text{则 } f_{\bar{k}} \in \text{End}(\mathbb{Z}/n\mathbb{Z}), \text{ 且 } \Phi(f_{\bar{k}}) = f_{\bar{k}}(1) = \bar{k}$$

从而诱导群同构  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ .  $\times$

推论 4.5  $\sum_{1 \leq d|n} \varphi(d) = n$

证明 考察  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

$$\text{令 } S_d = \{ \bar{g} \in \mathbb{Z}/n\mathbb{Z} \mid o(g) = d \}$$

$$\text{则 } \mathbb{Z}/n\mathbb{Z} = \bigsqcup_{1 \leq d|n} S_d \quad (\text{每一元素的阶唯一确定且整除 } n)$$

显然,  $S_d \subseteq H_d$ ,  $\mathbb{Z}/n\mathbb{Z}$  中阶为  $d$  的子群

而  $H_d$  为  $d$  阶循环群, 其  $d$  阶元个数恰好为  $\varphi(d)$ .

$$\text{即有 } |S_d| = \varphi(d)$$

$$\text{从而 } n = \sum_{1 \leq d|n} \varphi(d)$$

## §4.2 陪集分解与 Lagrange 定理

$H \leq G$  可在  $G$  上定义关系  $\sim$ :  $\{bh \mid h \in H\}$   
 $a \sim b$  若  $a = bh \exists h \in H$  或等价地  $a \in bH$ .

命题 4.6 上述关系为一个等价关系, 其等价类均具有形式  $aH$ ,  $a \in G$ , 称为  $G$  对于子群  $H$  的一个左陪集 (left coset)

PF:  $H$  为子群, 则

- $1_G \in H$
- $h^{-1} \in H \quad \forall h \in H$
- $h_1 h_2 \in H, \quad \forall h_1, h_2 \in H$

$\sim$  为等价关系.

$$a \sim a : a = a \cdot 1_H$$

$$a \sim b \quad b \sim a \Rightarrow a = bh, \exists h \in H \Rightarrow b = ah^{-1}, h^{-1} \in H$$

$$a \sim b, b \sim c \Rightarrow a \sim c$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ a = bh_1, h_1 \in H & & b = ch_2, h_2 \in H \Rightarrow a = ch_2h_1, h_2h_1 \in H \end{array}$$

$$\text{显然, } [a] = aH \quad \forall a \in G. \quad \#$$

注: 可类似定义右陪集 (right coset)

称  $\{a_i \mid i \in I\} \subseteq G$  为  $G$  对于子群  $H$  的一个左陪集完全代表元素, 若  $\forall g \in G, \exists ! i \in I$ , 使得  $g \in a_i H$ . 即有

$$G = \bigsqcup_{i \in I} a_i H$$

定义 4.7  $G$  对于子群  $H$  的左陪集的个数称为  $H$  在  $G$  中的指数 (index). 记作  $[G:H]$ .

定理 4.8 (Lagrange 定理) 若  $|G| < \infty, H \leq G$ , 则

$$|G| = |H| \cdot [G:H]$$

PF:  $G = \bigsqcup_{i \in I} a_i H \Rightarrow |G| = \sum_{i \in I} |a_i H|$

而  $|a_i H| = |H| \quad \left( f: H \rightarrow a_i H \text{ 为双射} \right)$   

$$h \mapsto a_i h$$

从而  $|G| = |I| \cdot |H| = [G:H] \cdot |H|$

注: 由定理 4.8 及命题 4.3 知  $o(g) = |\langle g \rangle| \mid |G|$ .

即有  $g^{|G|} = 1 \quad \forall g \in G$ .



## §4.3 原根与指数

本节研究  $(\mathbb{Z}/m\mathbb{Z})^\times$  的结构, 特别是何时为循环群.

定义 4.9 设  $(a, m) = 1$ . 称满足  $a^n \equiv 1 \pmod{m}$  的最小正整数  $n$  称为  $a$  模  $m$  的阶.

若存在  $g \in \mathbb{Z}$ ,  $(g, m) = 1$ .  $g$  模  $m$  的阶为  $\varphi(m)$  则称模  $m$  有原根 (primitive root),  $g$  为模  $m$  的一个原根.

注:  $a$  模  $m$  的阶即为  $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$  中的阶

$$a^l \equiv a^k \pmod{m} \iff l \equiv k \pmod{o(\bar{a})}$$

模  $m$  有原根即  $(\mathbb{Z}/m\mathbb{Z})^\times$  为循环群,  $g$  为一个原根即  $\bar{g}$  为  $(\mathbb{Z}/m\mathbb{Z})^\times$  的生成元.

引理 4.10 设  $m \neq 2, 4, p^l, 2p^l$  ( $p$  奇素数,  $l \geq 1$ ) 则模  $m$  无原根.

证明. 由定义, 只需说明不存在  $a$ , 使得  $a$  模  $m$  阶为  $\varphi(m)$ .

$$(1) \text{ 若 } m = 2^l, l \geq 3 \text{ 则 } \forall (a, m) = 1, a^2 \equiv 1 \pmod{2^3}$$

$$\Rightarrow a^{2^{l-2}} \equiv 1 \pmod{2^l} \quad \forall l \geq 3$$

$$\Rightarrow o(\bar{a}) \leq 2^{l-2} < \varphi(2^l) = 2^{l-1}$$

$$(2) \text{ 若 } m \text{ 满足引理条件, 且 } m \neq 2^l \text{ 则}$$

$$m = r \cdot s, \quad r, s > 2, \quad (r, s) = 1.$$

$$\text{由 Euler 定理} \quad a^{\varphi(r)} \equiv 1 \pmod{r} \quad \forall (a, m) = 1$$

$$a^{\varphi(s)} \equiv 1 \pmod{s}$$

$$(\text{中国剩余定理}) \quad a^{[\varphi(r), \varphi(s)]} \equiv 1 \pmod{rs}$$

而  $\varphi(r), \varphi(s)$  均为偶数, 知

$$o(a) \leq [\varphi(r), \varphi(s)] = \frac{\varphi(r)\varphi(s)}{(\varphi(r), \varphi(s))} \leq \frac{1}{2} \varphi(r)\varphi(s) < \varphi(rs) = \varphi(r)\varphi(s) \neq$$

注 设  $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$  则

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^\times$$

$(\mathbb{Z}/m\mathbb{Z})^\times$  为循环群  $\Leftrightarrow (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$  为循环群  $\forall i$   
 $\Downarrow \varphi(p_i^{e_i})$  两两互素.

定理 4.11

$p$  素, 则模  $p$  有原根.

引理 4.12

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \equiv 0 \pmod{p}$   
 模  $p$  最多有  $n$  个根.

PF.

对  $n$  进行归纳.

结论对  $n=1$  成立.

设结论对  $n$  成立. 即  $n$  次首一整系数多项式模  $p$  最多有  $n$  个根.

考察  $n+1$  次首一整式

$$f(x) = x^{n+1} + a_nx^n + \dots + a_1x + a_0$$

设  $f(x)$  模  $p$  有  $m$  个互异根  $\alpha_1, \alpha_2, \dots, \alpha_m$

$$f(x) - f(\alpha_1) = x^{n+1} - \alpha_1^{n+1} + a_n(x^n - \alpha_1^n) + \dots + a_1(x - \alpha_1)$$

$$= (x - \alpha_1) g(x)$$

其中  $g(x)$  为  $n$  次首一整式. 则

$\alpha_2, \dots, \alpha_m$  为  $g(x)$  模  $p$  的互异根

$$[p \mid (\alpha_i - \alpha_1) g(\alpha_i) \mid p \mid \alpha_i - \alpha_1, \forall i \geq 2 \Rightarrow p \mid g(\alpha_i) \quad i \geq 2]$$

由归纳假设  $m \leq n+1$ .

即命题对  $n+1$  成立

☆

定理 4.11 证明

记  $S(d) = \{1 \leq a \leq p-1 \mid a \text{ 模 } p \text{ 的阶为 } d\}$

则  $|S(d)| \leq \varphi(d)$

$$\left[ \begin{array}{l} x^d \equiv 1 \pmod{p} \quad \text{最多有 } d \text{ 个根} \\ \cdot S(d) \neq \emptyset. \quad \text{取 } a \in S(d). \text{ 则} \\ \quad 1, \bar{a}, \bar{a}^2, \dots, \bar{a}^{d-1} \text{ 为 } x^d \equiv 1 \pmod{p} \\ \quad \text{所有解, 其中共有 } \varphi(d) \text{ 个 } d \text{ 阶元} \\ \text{或} \cdot S(d) = \emptyset \end{array} \right]$$

$$p-1 = \sum_{1 \leq d \mid p-1} |S(d)| \leq \sum_{1 \leq d \mid p-1} \varphi(d) = p-1$$

$$\Rightarrow S(d) = \varphi(d) \quad \forall d \mid p-1$$

特别地,  $S(p-1) = \varphi(p-1) \geq 1$ .  $\star$

定理 4.13  $p$  为奇素数,  $l \geq 1$ . 则模  $p^l$  必有原根.

证明.  $a$  为模  $p^l$  原根  $\xrightarrow{\text{引理 3.19}}$   $a$  为模  $p^r$  原根  $\forall 1 \leq r \leq l$

特别地, 若  $l \geq 2$ ,  $g$  为模  $p^l$  原根  $\Rightarrow \begin{cases} g \text{ 为模 } p \text{ 原根} \\ g \text{ 为模 } p^2 \text{ 原根} \end{cases}$

即有  $\begin{cases} g \text{ 为模 } p \text{ 原根} \\ g^{p-1} \not\equiv 1 \pmod{p^2} \end{cases} \quad (*)$

断言: (1) 存在  $g$  满足  $(*)$

(2) 满足  $(*)$  的  $g$  必为模  $p^l$  原根

断言证明:

(1) 取  $g$  为一个模  $p$  原根, 则

$\cdot g^{p-1} \not\equiv 1 \pmod{p^2}$  或

$\cdot g^{p-1} \equiv 1 \pmod{p^2}$ , 此时

$$(g+p)^{p-1} \equiv g^{p-1} + p(p-1)g^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2}$$

从而  $g$  或  $g+p$  必有一个满足  $(*)$

(2) 设  $g$  满足  $(*)$  即  $g$  为模  $p$  原根, 且  $g^{p-1} \not\equiv 1 \pmod{p^2}$

由归纳可证:  $g^{\varphi(p^r)} = 1 + p^r k_r, (k_r, p) = 1$ .

$$\left[ \begin{array}{l} r=1, \quad g^{p-1} \equiv 1 + pk_1, (k_1, p) = 1. \\ \cdot \text{ 设结论对 } r \text{ 成立. 即} \\ \quad g^{\varphi(p^r)} = 1 + p^r k_r \quad (k_r, p) = 1. \\ \text{则 } g^{\varphi(p^{r+1})} = (g^{\varphi(p^r)})^p = (1 + p^r k_r)^p \\ \quad \equiv 1 + p^{r+1} k_r \pmod{p^{r+2}} \\ \text{从而 } g^{\varphi(p^{r+1})} = 1 + p^{r+1} k_{r+1} \quad (k_{r+1}, p) = 1. \end{array} \right]$$

另一方面, 设  $g$  模  $p^l$  阶为  $d$ , 则  $d \mid \varphi(p^{l-1}) = \varphi(p^l)$

由  $g$  为模  $p$  原根知  $p-1 \mid d$ .

从而  $d = (p-1) \cdot p^{r-1} \quad 1 \leq r \leq l$

而  $r < l$  时,  $g^{\varphi(p^r)} \not\equiv 1 \pmod{p^l}$

故  $r = l$ , 即  $d = \varphi(p^l)$ .  $g$  为模  $p^l$  原根.

定理 4.14  $p$  为奇素数,  $l \geq 1$ . 则模  $2p^l$  有原根.

证明. 设  $g$  为模  $p^l$  的一个原根. 则  $g+p^l$  亦为模  $p^l$  的一个原根. 则  $g, g+p^l$  中必有一个奇数.

记为  $g_0$ .

设  $g_0$  模  $2p^l$  阶为  $d$ , 则  $d \leq \varphi(2p^l) = \varphi(p^l)$

另一方面  $g_0^d \equiv 1 \pmod{p^l}$

$$\Rightarrow \varphi(p^l) \mid d$$

$\Rightarrow d = \varphi(p^l)$  即  $g_0$  为模  $2p^l$  原根.

注:  $(\mathbb{Z}/2p^l\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^l\mathbb{Z})^\times \cong (\mathbb{Z}/p^l\mathbb{Z})^\times$

故模  $p^l$  有原根  $\Rightarrow$  模  $2p^l$  有原根.

定理 4.15  $m > 1$  模  $m$  有原根  $\Leftrightarrow m = 2, 4, p^l, 2p^l$  ( $p$  奇素数)

总结: (原根计算)

(1) 求模  $p$  原根  $g$  (概率算法,  $\frac{\varphi(p-1)}{p-2}$ )

(2) 求  $g^{p-1}$  模  $p^2$

$g^{p-1} \not\equiv 1 \pmod{p^2} \Rightarrow g$  为模  $p^l$  原根

$g^{p-1} \equiv 1 \pmod{p^2} \Rightarrow g+p$  为模  $p^l$  原根

(3) 设  $g$  为模  $p^l$  原根.

$g$  奇  $\Rightarrow g$  为模  $2p^l$  原根

$g$  偶  $\Rightarrow g+p$  为模  $2p^l$  原根.

定义 若  $m$  有原根  $g$ , 则  $1, g, g^2, \dots, g^{\varphi(m)}$  为模  $m$  的一个循系.  $\forall (a, m) = 1, \exists ! 0 \leq k < \varphi(m)$ , 使得

$$a \equiv g^k \pmod{m}$$

$k$  称为  $a$  (对于原根  $g$ ) 的指数 (index), 记作  $k = \text{ind}_g a$ .

也称为  $a$  对于原根  $g$  的离散对数, 记作  $\log_g a$ .

注.  $a$  对于  $g$  的指数为  $k$ , 则  $\langle a \rangle \in (\mathbb{Z}/m\mathbb{Z})^\times$  中的指数为  $(\varphi(m), k)$ .

定理 4.16 设  $g$  为模  $m$  的一个原根.  $(a, m) = (b, m) = 1$ . 则

$$(1) \quad \text{ind } 1 = 0 \quad \text{ind } g = 1$$

$$(2) \quad \text{ind}(ab) \equiv \text{ind } a + \text{ind } b \pmod{\varphi(m)}$$

$$(3) \quad \text{ind}(a^n) = n \text{ind } a \pmod{\varphi(m)}$$

$$(4) \quad g_1 \text{ 为模 } m \text{ 的另一个原根}$$
$$\text{ind}_g(a) = \text{ind}_g g_1 \text{ind}_{g_1} a \pmod{\varphi(m)}$$

$$(5) \quad a \equiv b \pmod{m} \iff \text{ind } a = \text{ind } b$$

证:  $\text{ind}_g: (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/\varphi(m)\mathbb{Z}, +)$   
 $\bar{a} \longmapsto \overline{\text{ind}_g(a)}$   
为群同构.



## §4.4. 二次剩余

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad p \text{ 素数}, (a, p) = 1$$

- $p = 2$  平凡
- $p > 2$  为奇素数

$$\text{方程与 } 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p} \text{ 同解}$$

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

$$\text{方程有解} \Leftrightarrow y^2 \equiv b^2 - 4ac \pmod{p} \text{ 有解}$$

一般地  $x^2 \equiv a \pmod{p}$  有解, 则称  $a$  为二次剩余. 否则  $a$  为二次非剩余. 由定理 4.17 有

定理 4.18 设  $p$  为奇素数. 则任一模  $p$  的缩系中恰有  $\frac{p-1}{2}$  个二次剩余, 以及  $\frac{p-1}{2}$  个二次非剩余. 且模  $p$  的全部二次剩余所在同余类为  $1^2, 2^2, 3^2, \dots, (\frac{p-1}{2})^2$  所属同余类.

证明 由定义, 模  $p$  的二次剩余为

$$1^2, 2^2, 3^2, \dots, (\frac{p-1}{2})^2, (\frac{p+1}{2})^2, \dots, (p-1)^2$$

所在同余类, 而

$$1^2 \equiv (p-1)^2, 2^2 \equiv (p-2)^2, \dots, (\frac{p-1}{2})^2 \equiv (\frac{p+1}{2})^2 \pmod{p} \quad (*)$$

$$\text{且 } \forall 1 \leq i < j \leq \frac{p-1}{2}, \quad p+(i+j), \quad p+(i-j), \text{ 从而}$$

$$i^2 - j^2 = (i+j)(i-j) \not\equiv 0 \pmod{p} \quad (**)$$

故  $1^2, 2^2, \dots, (\frac{p-1}{2})^2$  模  $p$  所在同余类两两不同. 故为模  $p$  所有二次剩余.

注: 由定理 4.17 (3) 有  $\frac{p-1}{2}$  个二次剩余, 这里给出  $p$  奇素数,  $k=2$  情形的证明, 此方法适用于一般情形.

· 设  $g$  为一个模  $p$  原根. 则二次剩余为  $\{1, g^2, g^4, \dots, g^{p-3}\}$ .

二次非剩余为  $\{g, g^3, \dots, g^{p-2}\}$

·  $a$  为二次剩余  $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . (Euler 判别法)

定义 4.19 (Legendre 符号) 设  $p$  为素数. 定义函数  $\left(\frac{\cdot}{p}\right): \mathbb{Z} \rightarrow \{-1, 0, 1\}$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ 模 } p = \text{二次剩余} \\ -1 & a \text{ 模 } p = \text{二次非剩余} \\ 0 & p \mid a \end{cases}$$

注: · 同余方程  $x^2 \equiv 1 \pmod{p}$  的解数恰为  $\left(\frac{a}{p}\right) + 1$ .

·  $\left(\frac{\cdot}{p}\right): \mathbb{F}_p \rightarrow \{-1, 0, 1\}$  可看作  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  上的函数.

定理 4.20 设  $p$  为素数. 则  $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \quad \forall a, b \in \mathbb{Z}$ .

即 两个二次剩余的乘积为二次剩余.

一个二次剩余和一个二次非剩余的乘积为二次非剩余.

证明: (1) 显然  $x^2 \cdot y^2 = (xy)^2$  知二次剩余乘以二次剩余为二次剩余.

(2) 设  $a_1, \dots, a_{\frac{p-1}{2}}$  为所有二次剩余类.

$b_1, \dots, b_{\frac{p-1}{2}}$  为二次非剩余类.

显然  $\forall a_i$  由 (1) 知

$$a_i a_1, \dots, a_i a_{\frac{p-1}{2}}, a_i b_1, \dots, a_i b_{\frac{p-1}{2}}$$

为一个缩系. 而由 (1) 知

$a_i a_1, \dots, a_i a_{\frac{p-1}{2}}$  为互不相同的二次剩余类.

从而  $a_i b_1, \dots, a_i b_{\frac{p-1}{2}}$  为互不相同的二次非剩余类.

即二次剩余乘以二次非剩余为二次非剩余.

(3) 由 (2) 同样方法知二次非剩余的乘积为二次剩余.

注: ·  $\left(\frac{\cdot}{p}\right): \mathbb{F}_p^\times \rightarrow \{\pm 1\}$  为群同态.

定理 4.21 (Euler 判别法)  $p$  为奇素数. 则  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

证明:  $p \nmid a$  显然. 设  $(p, a) = 1$ .

$$\left(\frac{a}{p}\right) = 1 \Rightarrow a = x^2 \Rightarrow a^{\frac{p-1}{2}} = x^{2 \cdot \frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}$$

$\left(\frac{a}{p}\right) = -1$ . 记  $r = \frac{p-1}{2}$ , 设  $a_1, \dots, a_r$  为模  $p$  所有二次非剩余.

则  $a a_1^{-1}, \dots, a a_r^{-1}$  为所有二次非剩余. 故

$$a_1 \cdots a_r \cdot (a a_1^{-1}) \cdots (a a_r^{-1}) \equiv (p-1)! \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p} \quad \square$$

推论 4.22 设  $p$  为奇素数. 则

$$(1) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$$

$$(2) \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

证明 (1) 由定理 4.20,  $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(2) 考察如下同余式:

$$p-1 \equiv (-1)^1 \cdot 1 \pmod{p}$$

$$2 \equiv (-1)^2 \cdot 2 \pmod{p}$$

$$p-3 \equiv (-1)^3 \cdot 3 \pmod{p}$$

$$4 \equiv (-1)^4 \cdot 4 \pmod{p}$$

...

$$r \equiv (-1)^{\frac{p-1}{2}} \cdot \frac{p-1}{2} \pmod{p}$$

$$\text{其中 } r = \begin{cases} \frac{p-1}{2}, & p \equiv 1 \pmod{4} \\ \frac{p+1}{2} = p - \frac{p-1}{2}, & p \equiv 3 \pmod{4} \end{cases}$$

$$\Rightarrow 2 \cdot 4 \cdot \dots \cdot (p-1) \equiv (-1)^{1+2+\dots+\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$\Rightarrow \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

例 1: 证明形如  $4n+1$  的素数有无穷个.

PF. 设存在有限个素数  $p_1, \dots, p_n$  模 4 余 1. 考虑

$$m = (p_1 \cdots p_n)^2 + 1. \quad \text{则显然, } p_1, \dots, p_n \text{ 与 } m \text{ 互素.}$$

$$\text{易知 } m \equiv 2 \pmod{4}. \quad \text{从而 } m \neq 2^k \quad \forall k.$$

$$\text{对 } \forall p \mid m, \text{ 知 } \left(\frac{-1}{p}\right) = 1. \quad \text{从而 } p \equiv 1 \pmod{4}.$$

这与  $p_1, \dots, p_n$  的选取矛盾. 故存在无穷个模 4 余 1 的数.

注:  $a = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  求  $\left(\frac{a}{p}\right) \Leftrightarrow$  求  $\left(\frac{\pm 1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)$  陪.

## §4.5 二次互反律

引理 4.23 (Gauss 引理)  $p$  奇素数,  $p \nmid a$ .  $r = \frac{p-1}{2}$ . 记  $\mu$  为数集

$\{a, 2a, 3a, \dots, ra\}$  中模  $p$  的余数大于  $\frac{p}{2}$  的个数. 则

$$\left(\frac{a}{p}\right) = (-1)^\mu$$

证明：设  $a, 2a, \dots, ra$  中被  $p$  除的余数中  $\leq \frac{p}{2}$  的数为  $b_1, \dots, b_\lambda$ ，大于  $\frac{p}{2}$  的数为  $c_1, \dots, c_\mu$ ，其中  $\lambda + \mu = r$   
 $\{a, 2a, \dots, ra\}$  两两互不同余，从而  
 $b_1, \dots, b_\lambda$  两两互不同余

$p-c_1, \dots, p-c_\mu$  两两互不同余

且  $b_i$  与  $p-c_j$  不同余  $\forall i, j$ 。 ( $p \nmid (as+at), 1 \leq s, t \leq \frac{p-1}{2}$ )

显然  $b_i, p-c_j < \frac{p}{2} \forall i, j$ 。

从而  $b_1, \dots, b_\lambda, p-c_1, \dots, p-c_\mu$  为  $\{1, \dots, r\}$  的一个全排列

$$r! = b_1 \cdots b_\lambda (p-c_1) \cdots (p-c_\mu) \equiv (-1)^\mu b_1 \cdots b_\lambda c_1 \cdots c_\mu \equiv (-1)^\mu a^r r! \pmod{p}$$

$$\Rightarrow a^r (-1)^\mu \equiv 1 \pmod{p} \Rightarrow \left(\frac{a}{p}\right) \equiv a^r \equiv (-1)^\mu \pmod{p} \neq$$

例  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$

|            |                                                         |              |
|------------|---------------------------------------------------------|--------------|
| $p = 8k+1$ | $2 \cdot (2k+1), 2 \cdot (2k+2), \dots, 2 \cdot (4k)$   | $\mu = 2k$   |
|            | $2 \cdot (2k+1), 2 \cdot (2k+2), \dots, 2 \cdot (4k+1)$ | $\mu = 2k+1$ |
| $p = 8k+5$ | $2 \cdot (2k+2), 2 \cdot (2k+3), \dots, 2 \cdot (4k+2)$ | $\mu = 2k+1$ |
| $p = 8k+7$ | $2 \cdot (2k+2), 2 \cdot (2k+3), \dots, 2 \cdot (4k+3)$ | $\mu = 2k+2$ |

注：若  $a$  为奇数  $\forall 1 \leq i \leq r = \frac{p-1}{2}$

$$a_i = p \left[ \frac{a_i}{p} \right] + r_i$$

其中  $\left[ \frac{a_i}{p} \right]$  为不超过  $\frac{a_i}{p}$  的最大整数，即 Gauss 函数

将  $r_i$  中  $\leq \frac{p}{2}$  和  $> \frac{p}{2}$  的数分别记为

$b_1, \dots, b_\lambda$  以及  $c_1, \dots, c_\mu$ ， $\lambda + \mu = r$ 。

$$r) \sum_{i=1}^r a_i = p \sum_{i=1}^r \left[ \frac{a_i}{p} \right] + \sum_{i=1}^r r_i$$

$$\Rightarrow \frac{p^2-1}{8} \cdot a = p \cdot A + B + C$$

$$其中 A = \sum_{i=1}^r \left[ \frac{a_i}{p} \right], B = \sum b_i, C = \sum c_i$$

另一方面  $b_1 + \dots + b_\lambda + (p-c_1) + \dots + (p-c_\mu) = 1+2+\dots+r$

$$\mu p - C + B = \frac{p^2-1}{8}$$

$$\Rightarrow \frac{p^2-1}{8} (a-1) = (A-\mu)p + 2C$$

$p$  奇， $\frac{p^2-1}{8}$  为整数，而  $a-1$  为偶数。知  $A \equiv \mu \pmod{2}$

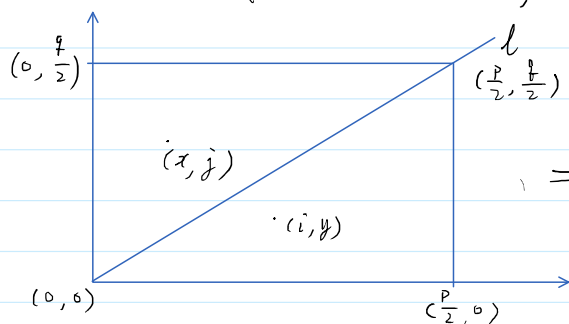
从而  $\left(\frac{a}{p}\right) = (-1)^A$ 。特别地，对素数  $p, q$ ，有

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^r \left[\frac{q_i}{p}\right]}, \quad r = \frac{p-1}{2}; \quad \left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^s \left[\frac{p_j}{q}\right]}, \quad s = \frac{q-1}{2}$$

定理 4.24 (二次互反律 quadratic reciprocity) 设  $p, q$  互不相同的奇素数. 则

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} -1 & p \equiv q \equiv 3 \pmod{4} \\ 1 & \text{其它} \end{cases}$$

PF. 由上面的证可知:  $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^r \left[\frac{q_i}{p}\right] + \sum_{j=1}^s \left[\frac{p_j}{q}\right]}$ ,  
其中  $r = \frac{p-1}{2}, s = \frac{q-1}{2}$ .



考察  $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq x < \frac{p}{2}, 1 \leq y < \frac{q}{2}\}$

$(x, y)$  在  $l$  下方的三角形区域

$\Rightarrow 1 \leq y \leq \frac{q}{p}x$  故  $l$  下方三角形区域

内整点个数为  $\sum_{i=1}^r \left[\frac{q_i}{p}\right]$ .

同理,  $l$  上方三角形区域整点个数为  $\sum_{j=1}^s \left[\frac{p_j}{q}\right]$

为平面, 对角线  $l$  上无整点,

$$\text{故 } \sum_{i=1}^r \left[\frac{q_i}{p}\right] + \sum_{j=1}^s \left[\frac{p_j}{q}\right] = r \cdot s$$

✱

例 判断方程  $x^2 \equiv 219 \pmod{383}$  是否有解.

解:  $383$  素.  $219 = 3 \times 73$

$$\Rightarrow \left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right)$$

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right) \cdot (-1)^{\frac{3-1}{2} \cdot \frac{383-1}{2}} = -\left(\frac{2}{3}\right) = 1$$

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right) = 1$$

故  $\left(\frac{219}{383}\right) = 1$ , 方程有解.

Euler 猜想 1783:  $p, q$  为奇素数. 则

$$\left(\frac{q}{p}\right) = 1 \iff \exists x, \text{ 使 } p \equiv (-1)^{\frac{p-1}{2}} x^2 \pmod{4q}$$



命题 4.25

Euler 猜想  $\Leftrightarrow$  二次互反律. 特别地, Euler 猜想成立.

PF: " $\Rightarrow$ " 设 Euler 猜想成立.

•  $p \equiv 1 \pmod{4}$

$$\left(\frac{q}{p}\right) = 1 \xRightarrow{\text{Euler 猜想}} p \equiv x^2 \pmod{4q} \quad \exists x \Rightarrow \left(\frac{p}{q}\right) = 1.$$

$$\text{此时} \quad \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = 1 = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$$\left(\frac{q}{p}\right) = -1 \xRightarrow{\text{Euler 猜想}} p \not\equiv x^2 \pmod{4q} \quad \forall x \Rightarrow \left(\frac{p}{q}\right) = -1$$

$$\text{此时} \quad \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = 1 = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

•  $p \equiv 3 \pmod{4}$

$$\left(\frac{q}{p}\right) = 1 \xRightarrow{\text{Euler}} p \equiv -x^2 \pmod{4q} \quad \exists x \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)$$

$$\left(\frac{q}{p}\right) = -1 \xRightarrow{\text{Euler}} p \not\equiv -x^2 \pmod{4q} \quad \forall x \Rightarrow \left(\frac{p}{q}\right) = -\left(\frac{-1}{q}\right)$$

$$\text{此时均有} \quad \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

" $\Leftarrow$ " 证明类似.

## §5.1 多项式环

设  $R$  为含么环,  $x$  为未定元. 则形如  $a_0 + a_1x + a_2x^2 + \dots$  的形式和称为  $R$  上的一个(以  $x$  为未定元)的一元多项式, 其中  $a_i \in R, i \geq 0$ , 且  $a_i = 0$  对  $i \gg 0$ , 一般记作

$$f(x) = a_n x^n + \dots + a_0 \quad (a_{n+1} = a_{n+2} = \dots = 0)$$

•  $g(x) = b_m x^m + \dots + b_0$ , 则  $f(x) = g(x) \Leftrightarrow a_i = b_i \quad \forall i$  (leading term)

•  $a_n \neq 0, a_{n+1} = a_{n+2} = \dots = 0$  则称  $a_n x^n$  为  $f(x)$  的首项,  $a_n$  为首项系数 (leading term),  $n$  为  $f$  的次数 (degree), 记为  $\deg f = n$

• 若  $a_0 = a_1 = \dots = 0$  则  $f$  称为 0 多项式. 0 多项式的次数约定为  $-\infty$ .

•  $a_0$  称为常数项 (constant term)

• 若  $a_1 = a_2 = \dots = 0$ , 则称  $f$  为常多项式.

$\deg f = 0 \Leftrightarrow f$  为非 0 常多项式.

•  $a_n x^n$  称为单项式 (monomial)

•  $f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0$  称作首一多项式 (monic polynomial).

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid n \geq 0, a_i \in R\}$$

在  $R[x]$  上定义  $+$ ,  $\cdot$  如下:

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \quad g(x) = \sum_{j=0}^{\infty} b_j x^j$$

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} a_i b_j \right) x^k = \sum_{k=0}^{\infty} \left( \sum_{i=0}^k a_i b_{k-i} \right) x^k$$

命题 5.1 (1)  $(R[x], +, \cdot)$  形成一个含么环:

$$\cdot \quad 0_{R[x]} = 0$$

$$\cdot \quad -f(x) = -a_n x^n - a_{n-1} x^{n-1} - \dots - a_0$$

$$\cdot \quad 1_{R[x]} = 1 = 1 + 0 \cdot x + 0 \cdot x^2 + \dots$$

且  $R$  为  $R[x]$  的子环. ( $R$  可看作常多项式全体)

(2)  $R[x]$  为交换环  $\Leftrightarrow R$  为交换环.

$R[x]$  为整环  $\iff R$  为整环.

命题 3.2 设  $f(x), g(x) \in R[x]$ . 则

$$(1) \deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$$

$$(2) \deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$$

若  $R$  为整环, 则等号成立.

注:  $\forall a \in Z(R)$ , 即  $ar = ra \quad \forall r \in R$ . 有映射

$$\varphi_a: R[x] \rightarrow R$$

$$f(x) = a_0 + a_1x + \dots + a_nx^n \mapsto a_0 + a_1a + \dots + a_na^n$$

为环同态.

若  $a \notin Z(R)$ , 结论是否成立?

## §5.2 整除理论

$R = F$  为域,  $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$

定义 5.3 设  $f(x), g(x) \in F[x], g(x) \neq 0$ . 若存在  $h(x) \in F[x]$ , 使得  $f(x) = g(x)h(x)$ , 则称  $g(x)$  为  $f(x)$  的因子 (因式),  $f(x)$  为  $g(x)$  的倍元 (倍数) 记作  $g(x) \mid f(x)$ .

注:  $\forall a \in F^\times$ ,  $a$  与  $a f(x)$  均为  $f(x)$  的因子, 称为  $f(x)$  的平凡因子.

定理 5.4 (带余除法) 设  $f(x), g(x) \in F[x], g(x) \neq 0$ . 则存在唯一的

$q(x), r(x) \in F[x]$ . 使得

$$(i) \quad f(x) = q(x)g(x) + r(x), \quad (ii) \quad \deg r(x) < \deg g(x).$$

$q(x)$  与  $r(x)$  分别称为  $f(x)$  被  $g(x)$  整除的商和余数.

证明. "存在性".

$$\text{令 } I = \{f(x) - h(x)g(x) \mid h(x) \in F[x]\} \subseteq F[x]$$

$f(x) \in I$  中. 令  $r(x)$  为  $I$  中次数最小的一个多项式.

则  $\deg r(x) < \deg g(x)$

$$\left[ \begin{array}{l} \text{则, 设} \\ g(x) = a_nx^n + \dots + a_1x + a_0 \\ r(x) = b_mx^m + \dots + b_1x + b_0 \\ m \geq n \Rightarrow r(x) = r(x) - \frac{b_m}{a_n}g(x) \cdot x^{m-n} \\ \quad = (b_{m-1} - \frac{a_{n-1}}{a_n}b_m)x^{m-1} + \dots \in I \end{array} \right]$$

$$\left. \begin{aligned} m \geq 1 \Rightarrow r(x) &= r(x) - \frac{a_n}{a_m} g(x) \cdot x \\ &= (b_{m-1} - \frac{a_{n-1}}{a_m} b_m) x^{m-1} + \dots \in I \\ \deg r(x) &< \deg r(x), \text{ 矛盾} \end{aligned} \right\}$$

“唯一性” 设  $f(x) = q(x)g(x) + r(x) = \tilde{q}(x)g(x) + \tilde{r}(x)$   
 $\deg r(x), \deg \tilde{r}(x) < \deg g(x)$   
 $\Rightarrow r(x) - \tilde{r}(x) = g(x)(\tilde{q}(x) - q(x))$   
 $\Rightarrow \deg g(x) > \deg(r(x) - \tilde{r}(x)) = \deg g(x) + \deg(\tilde{q}(x) - q(x))$   
 上式仅当  $\tilde{q}(x) - q(x) = 0$  时成立.  
 故有  $q(x) = \tilde{q}(x)$ , 且  $r(x) = \tilde{r}(x) \neq$

注: 若  $R$  不为域 问  $R[x]$  中是否有带余除法?

定义 5.5 设  $f(x), g(x) \in F[x]$ ,  $f(x), g(x)$  不全为 0.  $f(x)$  与  $g(x)$  的最大因子 (最大公因子) 是指一个首一多项式  $d(x)$ , 满足:  
 (i)  $d(x)$  为  $f(x)$  与  $g(x)$  的公因子 即  $d(x) | f(x), d(x) | g(x)$ .  
 (ii) 若  $\tilde{d}(x)$  为  $f(x), g(x)$  的公因子, 则  $\deg \tilde{d}(x) \leq \deg d(x)$ .  
 此时, 记  $d(x) = (f(x), g(x))$ . 若  $d=1$ , 则称  $f(x)$  与  $g(x)$  互素.

注: 最大公因子存在. 下证唯一性.

定理 5.6 (贝祖等式) 设  $f(x), g(x) \in F[x]$ ,  $d(x) = (f(x), g(x))$ . 则

- (1) 存在  $u(x), v(x) \in F[x]$ , 使得  $d(x) = f(x)u(x) + g(x)v(x)$ . 特别地, 若  $\tilde{d}(x)$  为  $f(x), g(x)$  公因子, 则  $\tilde{d}(x) | d(x)$ .
- (2)  $f(x), g(x)$  互素  $\Leftrightarrow$  存在  $u(x), v(x) \in F[x]$ , 使得  $f(x)u(x) + g(x)v(x) = 1$ .

证明: (1) 令  $I = \{f(x)\alpha(x) + g(x)\beta(x) \mid \alpha(x), \beta(x) \in F[x]\} \subseteq F[x]$ .

则  $d \in I$ . 令  $h(x)$  为  $I$  中次数最小的首一多项式. 则

由  $I$  的定义, 存在  $u(x), v(x) \in F[x]$ , 使得  $h(x) = f(x)u(x) + g(x)v(x)$ .

由带余除法,  $f(x) = q(x)h(x) + r(x)$ , 其中  $\deg r(x) < \deg h(x)$ ,

$$r(x) = f(x) - q(x)h(x)$$

$$= f(x) - q(x)\alpha(x)f(x) - q(x)\beta(x)g(x) \in I$$

由  $h$  的极小性知  $r(x) = 0$ . 即  $h(x) | f(x)$ ,

同理  $h(x) | g(x) \Rightarrow \deg h(x) \leq \deg d(x) \Rightarrow d(x) = h(x)$   
 另一方面,  $d(x) | f(x), d(x) | g(x) \Rightarrow d(x) | h(x)$

即有  $d(x) = h(x) = f(x)u(x) + g(x)v(x)$ .

若  $\tilde{d}(x) | f(x), \tilde{d}(x) | g(x)$ , 则  $\tilde{d}(x) | d(x) = f(x)u(x) + g(x)v(x)$ .

(2) " $\Rightarrow$ "  $(f(x), g(x)) = 1$ , 则由 (1),  $\exists u(x), v(x) \in F[x]$  使得  
 $f(x)u(x) + g(x)v(x) = 1$

" $\Leftarrow$ " 若存在  $u(x), v(x) \in F[x]$ ,  $f(x)u(x) + g(x)v(x) = 1$ .

则  $\forall d(x) | u(x), d(x) | v(x) \Rightarrow$

$d(x) | 1 = f(x)u(x) + g(x)v(x)$

从而  $(f(x), g(x)) | 1 \Rightarrow (f(x), g(x)) = 1$ .

命题 5.7 7. 述成立  $f(x), g(x) \in F[x]$ , 不全为 0. 则

(i)  $f(x), g(x)$  的公因子均为  $(f(x), g(x))$  的因子

(ii)  $m(x)$  首一,  $m(x)(f(x), g(x)) = (m(x)f(x), m(x)g(x))$

(iii) 令  $d(x) = (f(x), g(x))$ , 则  $(\frac{f(x)}{d(x)}, \frac{g(x)}{d(x)}) = 1$

(iv)  $(f(x), m(x)) = 1, (g(x), m(x)) = 1 \Rightarrow (f(x)g(x), m(x)) = 1$

(v)  $m(x) | f(x)g(x), (m(x), g(x)) = 1 \Rightarrow m(x) | f(x)$

(vi)  $((f(x), g(x))h(x)) = (f(x), g(x), h(x))$

注:  $d(x) = (f(x), g(x)) \iff$  (i)  $d(x)$  为  $\mathbb{A}$ -多项式

(ii)  $d(x) | f(x), d(x) | g(x)$

(iii)  $\forall \tilde{d}(x) | f(x), \tilde{d}(x) | g(x) \Rightarrow \tilde{d}(x) | d(x)$

定理 5.8 (1)  $I$  为  $F[x]$  理想, 则存在  $f(x)$ , 使得  $I = f(x)F[x] = \{f(x)\alpha(x) | \alpha(x) \in F[x]\}$

(2) 设  $f(x), g(x) \in F[x]$ ,  $f(x), g(x)$  不全为 0. 则

$$(f(x), g(x))F[x] = f(x)F[x] + g(x)F[x] \\ (\triangleq \{f(x)\alpha(x) + g(x)\beta(x) | \alpha(x), \beta(x) \in F[x]\})$$

注:  $d(x) = (f(x), g(x)) \iff$  (i)  $d(x)$  首一 (ii)  $d(x) | f(x), d(x) | g(x)$   
 (iii)  $d(x) \in f(x)F[x] + g(x)F[x]$

欧几里得算法求  $(f(x), g(x))$ .

不妨设  $g(x) \neq 0$ . 则令  $r_0(x) = g(x), r_{-1}(x) = f(x)$

$$r_{-1}(x) = q_0(x)r_0(x) + r_1(x)$$

$$r_0(x) = q_1(x)r_1(x) + r_2(x)$$

$$r_1(x) = q_2(x)r_2(x) + r_3(x)$$

...

$$r_{n-1}(x) = q_n(x)r_n(x) + r_{n+1}(x)$$

$$\deg r_2 < \deg r_1$$

$$\deg r_1 < \deg r_0$$

$$\deg r_{n+1} = -\infty$$

$$\text{从而 } (f(x), g(x)) = (r_{-1}(x), r_0(x)) = (r_0(x), r_1(x))$$

$$= (r_1(x), r_2(x)) = \dots = (r_{n-1}(x), r_n(x)) = r_n(x)$$

$r_n(x)$  为  $f(x)$  与  $g(x)$  的线性组合.

## 不可约多项式

定义 5.9  $p(x) \in F[x]$ ,  $\deg p(x) \geq 1$ . 若  $p(x)$  的因子只有平凡因子, 即  $c$  或  $cp(x)$ ,  $c \in F^\times$ , 则称  $p(x)$  为 不可约多项式. 否则, 称为 可约多项式, 并称其 在  $F$  上可约.

注: 1. 一次多项式为不可约多项式  
2.  $x^2+1 \in \mathbb{R}[x]$  不可约. 但  $x^2+1 \in \mathbb{C}[x]$  为可约.

引理 5.10 (Euclid 引理) 设  $p$  不可约.  $p \mid fg \Rightarrow p \mid f$  或  $p \mid g$ .

PF: 若  $p \nmid f$ ,  $p \nmid g \Rightarrow (p, f) = 1, (p, g) = 1$   
 $\Rightarrow (p, fg) = 1 \Rightarrow p \nmid fg$ . 矛盾.

定理 5.11 设  $f(x) \in F[x]$ ,  $\deg f \geq 1$ . 则存在首一不可约多项式  $p_1(x), \dots, p_r(x)$ , 使得  $f(x) = c p_1(x) \dots p_r(x)$ , 其中  $c$  为  $f(x)$  首项系数, 且  $p_1(x), \dots, p_r(x)$  在不计次序意义下惟一.

注:  $f(x) = c p_1^{v_{p_1}(f)} p_2^{v_{p_2}(f)} \dots p_s^{v_{p_s}(f)}$   
其中  $p_1, \dots, p_s$  两两不同,  $v_{p_1}(f), \dots, v_{p_s}(f) \geq 1$ .

推论 5.12 设  $f(x) = c_1 p_1^{\alpha_1} \dots p_s^{\alpha_s}$ ,  $g(x) = c_2 p_1^{\beta_1} \dots p_s^{\beta_s}$   
则  $(f(x), g(x)) = p_1^{\min(\alpha_1, \beta_1)} \dots p_s^{\min(\alpha_s, \beta_s)}$ .

类似地, 可定义 最小公倍数.



### §5.3 多项式的零点与韦达定理

定理5.13  $f(x) \in F[x]$ . 则  $\forall a \in F$ , 存在唯一  $q(x) \in F[x]$ , 使得  
 $f(x) = q(x)(x-a) + f(a)$ .  
 特别地,  $(x-a) \mid f(x) \iff f(a) = 0$

PF 由带余除法, 存在唯一的  $q(x), r(x)$ , 使得  
 $f(x) = q(x)(x-a) + r(x)$  且  $\deg r(x) < \deg(x-a) = 1$ .  
 从而  $r(x) = r \in F$  为常多项式  
 将  $x=a$  代入上式而也有  $f(a) = q(a)(x-a) + r(a) = r$   
 即有  $f(x) = q(x)(x-a) + f(a)$ .  
 最后一个结论由定义可知.  $\square$

注, 满足  $f(a) = 0$  的点  $a$  称为  $f(x)$  的零点.

注:  $f(x) \in F[x]$ .  $\deg f = 2, 3$ . 则  $f(x)$  不可约  
 $\iff f(x)$  在  $F$  中无零点

" $\Rightarrow$ " 显然

" $\Leftarrow$ "  $\deg f = 2, 3$ . 若  $f$  可约, 则  $f$  必有 1 次因子, 从而有零点.

定理5.14 (多项式的 Lagrange 定理)  $f(x) \in F[x]$   $\deg f = n$ . 则  $f$   
 零点个数  $\leq n$ .

PF 设  $a_1, \dots, a_s$  为  $f(x)$  的不同零点. 则  
 $f(x) = (x-a_1)f_1(x)$ .  
 $f_1(x) = (x-a_2)f_2(x)$  ( $f(a_2)=0 \Rightarrow (a_1-a_2)f_1(a_2)=0 \Rightarrow f_1(a_2)=0$ )  
 $\dots$   
 $f_{s-1}(x) = (x-a_s)f_s(x)$ .  
 从而  $f(x) = (x-a_1)(x-a_2)\dots(x-a_s)f_s(x)$ .  
 故  $\deg f = n = \deg(x-a_1)\dots(x-a_s) = s$ .  $\square$

注, 一般环中结论不成立.  
 在  $\mathbb{H}[x]$  中,  $x^2 + 1 = 0$  有无穷个解.

与  $R = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  则  $\in R[x]$  中,  
 $x^2 = (\bar{1}, \bar{1})$  的解为  $(\pm \bar{1}, \pm \bar{1})$ .

### 定理 5.15 (Vieta 定理)

$f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x], a_n \neq 0$

(1) 若  $f(x)$  有  $n$  个互异根  $\alpha_1, \dots, \alpha_n$  则

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

(2) 若  $f(x) = a_n (x - \alpha_1) \cdots (x - \alpha_n)$  ( $\alpha_i$  可能相同), 则

$$\sum_{1 \leq i_1 < \dots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

特别地,  $\alpha_1 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n}, \alpha_1 \cdots \alpha_n = (-1)^n \frac{a_0}{a_n}$

PF (1)  $x - \alpha_i \mid f(x), x - \alpha_1, \dots, x - \alpha_n$  两两互素, 从而  
 $(x - \alpha_1) \cdots (x - \alpha_n) \mid f(x)$ .

比较次数与首项系数知  $f(x) = a_n (x - \alpha_1) \cdots (x - \alpha_n)$ .

(2) 考虑右边展开式中  $x^{n-k}$  前面的系数.

### 推论 5.16

(1)  $f(x) = ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2), a \neq 0$  则

$$\alpha_1 + \alpha_2 = -\frac{b}{a}, \alpha_1 \alpha_2 = \frac{c}{a}$$

(2)  $f(x) = x^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

$$\text{则} \begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -b \\ \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = c \\ \alpha_1 \alpha_2 \alpha_3 = -d \end{cases}$$

### 命题 5.17

$p$  为素数. 则  $\in \mathbb{F}_p[x]$  中,

$$x^p - x = x(x-1)(x-2) \cdots (x-(p-1)).$$

PF:  $0, 1, 2, \dots, p-1$  为  $x^p - x$  所有零点  $\#$

定理 5.18  $f(x) \in F[x], m \geq 1$ . 若  $f(x) = (x - a)^m g(x)$ , 其中  $(x - a)$  与  $g(x)$  互素,  
 则称  $a$  为  $f(x)$  的  $m$  重零点,  $m=1$  称为单零点.  $m \geq 2$  为重根.

定义 5.19  $f(x) = \sum a_i x^i$  的形式幂级数定义为  $f(x) = \sum_{i=0}^{\infty} a_i x^i$

引理 5.20

$$(1) (f+g)' = f' + g' \quad f, g \in F[x]$$

$$(2) (cf)' = cf' \quad c \in F$$

$$(3) (fg)' = f'g + fg'$$

PF. (1), (2) 由定义显然.

(3) 由分配律及 (1) (2) 可知, 只需对  $f, g$  为单项式证明.

$$\begin{aligned} (x^m \cdot x^n)' &= (m+n) x^{m+n-1} \\ &= m x^{m-1} \cdot x^n + x^m \cdot n x^{n-1} \\ &= (x^m)' x^n + x^m (x^n)' \end{aligned} \quad \#$$

命题 5.21 (1) 若  $a \in f(x)$  中重数  $\geq m$ , 则  $a'$  在  $f(x)$  中重数  $\geq m-1$

(2)  $(f, f') = 1$  则  $f$  无重根.

(3)  $a$  为  $f$  单零点  $\iff f(a) = 0, f'(a) \neq 0$

PF. (1)

$$\begin{aligned} f(x) &= (x-a)^m g(x) \\ \Rightarrow f'(x) &= ((x-a)^m)' g(x) + (x-a)^m g'(x) \\ &= (x-a)^{m-1} (m g(x) + (x-a) g'(x)) \end{aligned}$$

(2) 由 (1), 若  $a$  为  $f$  的重根, 则  $x-a \mid f'(x)$  故  $x-a \mid (f, f')$  与  $(f, f') = 1$  矛盾.

(3) " $\Rightarrow$ "  $f$  为单零点, 即  $f(x) = (x-a)g(x), g(a) \neq 0$   
 $\Rightarrow \begin{cases} f(a) = 0 \\ f'(a) = g(a) \neq 0. \end{cases}$

" $\Leftarrow$ "  $f(a) = 0 \Rightarrow a$  为  $f$  零点.  
设  $a$  为  $f$   $m$  重零点, 若  $m \geq 2$  则 (1) 知  $a$  为  $f'$  零点. 与  $f'(a) \neq 0$  矛盾. 故  $m=1$ .

例

1.  $f(x) = x^p - x \in \mathbb{F}_p[x]$

$$f'(x) = px^{p-1} - 1 = -1$$

$$(f, f') = 1 \Rightarrow f \text{ 无重根}$$

2.  $f(x) = x^{p-1} \in \mathbb{F}_p[x]$

$$f'(x) = px^{p-2} = 0 \Rightarrow (f, f') = f$$

$$f(x) = (x-1)^p$$

## §5.4 多项式同余理论

定义 5.22  $f(x), g(x) \in F[x], 0 \neq m(x) \in F[x]$ . 称  $f(x)$  与  $g(x)$  模  $m(x)$  同余, 若  $m(x) \mid f(x) - g(x)$ . 记作  $f \equiv g \pmod{m}$ .

命题 5.23 (1) 模  $m(x)$  同余为  $F[x]$  上的等价关系.  
 (2)  $f_1(x) \equiv f_2(x) \pmod{m(x)}, g_1(x) \equiv g_2(x) \pmod{m(x)}$   
 则 
$$\begin{aligned} f_1(x) \pm g_1(x) &\equiv f_2(x) \pm g_2(x) \pmod{m(x)} \\ f_1(x) \cdot g_1(x) &\equiv f_2(x) \cdot g_2(x) \pmod{m(x)} \end{aligned}$$

PF (1)  $f \equiv f \pmod{m(x)} \iff m(x) \mid f - f = 0$   
 $f \equiv g \pmod{m(x)} \iff m(x) \mid f - g$   
 $\Downarrow$   
 $g \equiv f \pmod{m(x)} \iff m(x) \mid g - f$   
 $f \equiv g, g \equiv h \iff m(x) \mid f - g, m \mid g - h$   
 $\Downarrow$   
 $f \equiv h \pmod{m(x)} \iff m \mid f - h$

(2)  $f_1 \equiv f_2, g_1 \equiv g_2 \pmod{m} \Rightarrow m \mid f_1 - f_2, m \mid g_1 - g_2$   
 $\Rightarrow m \mid (f_1 \pm g_1) - (f_2 \pm g_2)$   
 $m \mid f_1 g_1 - f_2 g_2 = (f_1 - f_2)g_1 + f_2(g_1 - g_2)$

令  $(m(x)) = m(x)F[x] = \{m(x)\alpha(x) \mid \alpha(x) \in F[x]\}$

$F[x]/(m(x))$  为模  $m(x)$  同余类的集合.

记  $\bar{f} = [f] = f + (m(x))$  为  $f$  所在的同余类

命题 5.23 本例上定义了  $F[x]/(m(x))$  上的两个运算

$$\overline{f(x)} + \overline{g(x)} \triangleq \overline{f+g}$$

$$\overline{f} \cdot \overline{g} \triangleq \overline{fg},$$

### 定理 5.24

$0 \neq m(x) \in F[x]$ . 则

- (1)  $(m(x))$  为  $F[x]$  的理想, 从而  $F[x]/(m(x))$  为交换环, 且

$$F[x]/(m(x)) = \{ \bar{r}(x) \mid r(x) \in F[x], \deg r(x) < \deg m(x) \}$$

$$(F[x]/(m(x)))^\times = \{ \bar{r}(x) \mid r(x) \in F[x], \deg r(x) < \deg m(x), (m(x), r(x)) = 1 \}$$

- (2)  $\deg m(x) > 0$ . 下述等价:

(a)  $F[x]/(m(x))$  为整环

(b)  $F[x]/(m(x))$  为域

(c)  $m(x)$  为不可约多项式

PF

- (1) 由定义, 可验证  $(m(x))$  为  $F[x]$  的理想. 故有商环  $F[x]/(m(x))$ .

- 由带余除法, 任一多项式  $f(x)$  可唯一同余到一个次数小于  $m(x)$  的多项式. 从而有

$$F[x]/(m(x)) = \{ \bar{r}(x) \mid r(x) \in F[x], \deg r(x) < \deg m(x) \}$$

- 设  $r(x) \in F[x]$ ,  $\deg r(x) < \deg m(x)$ .

- $(r(x), m(x)) = 1$

则由贝祖等式, 存在  $\alpha(x), \beta(x) \in F[x]$ , 使得

$$r(x)\alpha(x) + m(x)\beta(x) = 1$$

即有  $r(x)\alpha(x) \equiv 1 \pmod{m(x)}$

$$\text{或 } \bar{r}(x) \cdot \bar{\alpha}(x) = \bar{1} \quad (\text{在 } F[x]/(m(x)) \text{ 中})$$

- 若  $\bar{r}(x)$  在  $F[x]/(m(x))$  中可逆, 则存在  $\alpha(x) \in F[x]$  使得  $\bar{r}(x)\bar{\alpha}(x) = \bar{1}$ . 即存在  $\beta(x) \in F[x]$ ,  $r(x)\alpha(x) = 1 - m(x)\beta(x)$ . 故  $(r(x), m(x)) = 1$ .

- (2) (c)  $\Rightarrow$  (b)

设  $m(x)$  不可约, 则  $\forall 0 \neq r(x)$ ,  $\deg r(x) < \deg m(x)$  均有  $(m(x), r(x)) = 1$ . 从而由 (1) 知  $\bar{r}(x)$  可逆. 即  $F[x]/(m(x))$  为域

(b)  $\Rightarrow$  (a) 显然域为整环

(a)  $\Rightarrow$  (c)

设  $F[x]/(m(x))$  为整环. 若  $m(x) = m_1(x)m_2(x)$

则  $0 = \overline{m(x)} = \overline{m_1(x)} \overline{m_2(x)}$  ( $\in F[x]/(m(x))$  中)

故由整环性质知  $\overline{m_1(x)} = 0$  或  $\overline{m_2(x)} = 0$

从而  $m(x) \mid m_1(x)$  或  $m(x) \mid m_2(x)$ .

即  $m(x)$  无非平凡因子.  $m$  为不可约元.

推论 5.25  $0 \neq m(x) \in \mathbb{F}_p[x]$ .  $\deg m(x) = n > 0$  且

$\mathbb{F}_p[x]/(m(x))$  为  $p^n$  元环. 若  $m(x)$  不可约, 则  $F[x]/(m(x))$  为  $p^n$  元域.

PF  $F[x]/(m(x)) = \{ \overline{r(x)} \mid r(x) = a_{n-1}x^{n-1} + \dots + a_1x + a_0, a_i \in \mathbb{F}_p \}$   
 $\Rightarrow |F[x]/(m(x))| = p^n$ .

注. (1)  $\mathbb{F}_p$  上  $n$  次不可约多项式存在, 例如  $n$  次分圆多项式, 从而存在  $p^n$  元域.

(2) 若  $F$  为有限域, 则存在素数  $p$  及  $n > 0$  使得  
 $|F| = p^n$ .

$m(x) \mid n(x)$ .  $n(x) = m(x) \cdot h(x)$ . 则  
 $f \equiv g \pmod{n(x)} \Rightarrow f \equiv g \pmod{m(x)}$   
从而有映射  
$$\begin{aligned} F[x]/(n(x)) &\longrightarrow F[x]/(m(x)) \\ f + (n(x)) &\longmapsto f + (m(x)) \end{aligned}$$

定理 5.26 (中国剩余定理)  $m(x) = m_1(x) \cdots m_s(x)$ ,  $m_i$  两两互素.

则有环同构

$$\begin{aligned} \frac{F[x]}{m(x)} &\xrightarrow{\sim} \frac{F[x]}{(m_1(x))} \times \frac{F[x]}{(m_2(x))} \times \dots \times \frac{F[x]}{(m_s(x))}, \\ f + (m(x)) &\longmapsto (f + (m_1(x)), f + (m_2(x)), \dots, f + (m_s(x))) \end{aligned}$$

从而诱导群同构  $(\frac{F[x]}{m(x)})^\times \simeq (\frac{F[x]}{m_1(x)})^\times \times \dots \times (\frac{F[x]}{m_s(x)})^\times$

证明: 由商环与环的直积的定义知上述映射为环同态, 而为同构则由上面中国剩余定理



弱形式给出.

定理 5.27  $m(x) = m_1(x) m_2(x) \cdots m_s(x)$ ,  $m_i(x)$  两两互素.  
 $a_1(x), \dots, a_s(x) \in F[x]$ . 则同余方程组

$$\begin{cases} f(x) \equiv a_1(x) \pmod{m_1(x)} \\ f(x) \equiv a_2(x) \pmod{m_2(x)} \\ \vdots \\ f(x) \equiv a_s(x) \pmod{m_s(x)} \end{cases}$$

必有解. 且解集为模  $m(x)$  的一个同余类.

证明. 设  $f_i(x)$  为方程组

$$\begin{cases} f(x) \equiv 1 \pmod{m_i(x)} \\ f(x) \equiv 0 \pmod{m_j(x)} \quad j \neq i \end{cases}$$

的解. ( ? 解存在 )

则  $a_1 f_1 + \cdots + a_s f_s$  为原方程组的一个解.

· 设  $f$  为方程一个特解. 则  $g$  为方程的解

$$\Leftrightarrow g \equiv f \pmod{m_i} \quad i=1, \dots, s$$

$$\Leftrightarrow g \equiv f \pmod{m}$$

故解集为模  $m$  的一个同余类.

$p(x)$  为不可约多项式. 则  $F[x]/(p(x))$  为域. 而  $F$  上的有限域扩张均由此式给出. 多项式不可约性判断尤为重要.

命题 5.28  $f(x) \in F[x]$ ,  $\deg f(x) \geq 1$ .

(1)  $f(x)$  所有非常值因子中次数最小的必为不可约多项式

(2)  $\deg f(x) = 2, 3$ . 则  $f(x)$  不可约  $\Leftrightarrow f(x)$  无零点.

定理 5.29 (代数学基本定理)

$f(x) \in \mathbb{C}[x]$ ,  $\deg f(x) \geq 1$ .

则  $f(x) \in \mathbb{C}$  中必有零点.

推论 5.30 (1)  $f(x) \in \mathbb{C}[x]$ ,  $\deg f = n \geq 1$  则  $f(x) \in \mathbb{C}$

中恰有  $n$  个根 (计重数). 即  $f(x) = c(x-\alpha_1)^{n_1} \cdots (x-\alpha_s)^{n_s}$ ,  
 $n_1 + \cdots + n_s = n$ . 特别地,  $f$  不可约  $\Leftrightarrow \deg f(x) = 1$ .

(2)  $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$  ( $a \neq 0$ ) 不可约  
 $\Leftrightarrow b^2 - 4ac < 0$ .

(3)  $f(x) \in \mathbb{R}[x]$  为不可约元, 则  $\deg f(x) = 1$  或  $2$ .

PF (1)  $f(x) \in \mathbb{C}[x]$ .  $\deg f = n \geq 1$ . 则由 5.29 知  
 $f$  有零点  $\alpha_1$ , 则  $f(x) = (x-\alpha_1) \cdot f_1(x)$ ,  $\deg f_1(x) = n-1$ .  
由归纳可知  $f(x) = c(x-\alpha_1) \cdots (x-\alpha_n)$ .

(2)  $f(x) \in \mathbb{R}[x]$  不可约  $\Leftrightarrow f(x)$  无实根  $\Leftrightarrow \Delta = b^2 - 4ac < 0$ .

(3)  $f(x) \in \mathbb{R}[x]$  不可约, 由 5.29 知  $f(x)$  有复零点  $\alpha$ ,  
从而  $\bar{\alpha}$  也为  $f(x)$  零点.

- 若  $\alpha \in \mathbb{R}$ . 则  $x - \alpha \mid f(x)$ .
- 若  $\alpha \notin \mathbb{R}$ . 则  $(x-\alpha)(x-\bar{\alpha}) \mid f(x)$ .  
 $(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$ . #

## §5.5 整系数多项式

 $\mathbb{Z}[x]$  与  $\mathbb{Q}[x]$  比较:

- $2x$  与  $3x \in \mathbb{Q}[x]$  中相互整除.  
 $2x \nmid 3x, 3x \nmid 2x$  在  $\mathbb{Z}[x]$  中
- 在  $\mathbb{Q}[x]$  中带余除法存在, 而在  $\mathbb{Z}[x]$  中不一定存在.  
 例:  $f(x) = 3x^2, g(x) = 2x + 1$
- $\mathbb{Q}[x]$  中理想为主理想, 但  $\mathbb{Z}[x]$  中不存在主理想  
 例:  $(2, x)$

定理 5.30 (带余除法)  $f(x) \in F[x]$  为首一多项式, 则  $\forall f(x) \in F[x]$ ,  
 存在唯一的一组  $q(x), r(x)$ , 使得  

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x).$$

证明与定理 5.4 证明类似.

定义 5.31  $f(x) \in \mathbb{Z}[x]$  称为不可约多项式 (或在  $\mathbb{Z}$  上不可约)  
 是指若  $f(x) = g(x)h(x)$ , 则  $g(x) = \pm 1$  或  $f(x) = \pm 1$ .

注: 对一般交换环  $R$ ,  $a \in R$  不可约若  $a$  元非平凡因子.  
 即  $a = xy \Rightarrow x \in R^\times$  或  $y \in R^\times$ .

例:  $2x+1, x^2+x+1 \in \mathbb{Z}[x]$  不可约.

例  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$   
 则  $f(x) = (a_n, a_{n-1}, \dots, a_1, a_0) \cdot (\tilde{a}_n x^n + \dots + \tilde{a}_1 x + \tilde{a}_0)$   
 $\tilde{a}_i = a_i / (a_n, a_{n-1}, \dots, a_1, a_0)$   
 故若  $(a_n, \dots, a_0) \neq 1$ ,  $\deg f \geq 1$  则  $f$  可约.

定义 5.32  $f(x) = a_n x^n + \dots + a_1 x + a_0$  称  $(a_n, a_{n-1}, \dots, a_2, a_1)$   
 为  $f(x)$  的容量 (content), 记作  $c(f)$ .  
 若  $c(f) = 1$ , 则称  $f$  为本原多项式 (primitive polynomial)

引理 5.33 (1)  $c(fg) = c(f)c(g)$ , 从而本原多项式乘积为本原多项式.  
 (2)  $f = gh, f, g \in \mathbb{Z}[x], h \in \mathbb{Q}[x]$ .  $g$  本原.

则  $h \in \mathbb{Z}[x]$ .

PF (1) 显然  $f = c(f) \cdot f_1$ , 则  $f_1$  本原.  
 $g = c(g) \cdot g_1$ ,  $g_1$  本原

只须证  $f_1, g_1$  本原. 则有

$$c(fg) = c(f)c(g) = c(f_1g_1) = c(f_1)c(g_1)$$

$$\text{令 } f_1 = a_n x^n + \dots + a_1 x + a_0$$

$$g_1 = b_m x^m + \dots + b_1 x + b_0$$

$$c(f_1) = c(g_1) = 1, \text{ 即 } (a_n, \dots, a_0) = (b_m, \dots, b_0) = 1$$

$$\forall \text{ 素数 } p, \text{ 设 } p \nmid a_0, \dots, p \nmid a_{i-1}, p \nmid a_i \quad (\exists! 0 \leq i \leq n-1)$$

$$p \nmid b_0, \dots, p \nmid b_{j-1}, p \nmid b_j \quad (\exists! 0 \leq j \leq m-1)$$

$$(p \nmid c(f)) \Rightarrow i \text{ 存在}, p \nmid c(g) \Rightarrow j \text{ 存在}$$

$$\text{令 } f_1 g_1 = \sum_{k=0}^{m+n} c_k x^k \quad (2)$$

$$p \nmid c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + \dots + a_0 b_{i+j} \\ + a_{i+1} b_{j-1} + \dots + a_n b_{i+j-n}$$

$$\text{故 } c(f_1 g_1) = 1.$$

$$(2) \quad f, g \in \mathbb{Z}[x], \quad h \in \mathbb{Q}[x] \Rightarrow h = \frac{1}{d} h_1(x), \quad d =$$

$$d > 0, h_1(x) \in \mathbb{Z}[x], (d, c(h_1)) = 1.$$

$$\text{于是 } d f(x) = g(x) h_1(x)$$

$$\Rightarrow d \cdot c(f(x)) = c(g) c(h_1) = c(h_1)$$

$$\Rightarrow d \mid c(h_1) \Rightarrow d = 1$$

$$\text{于是 } h = h_1(x) \in \mathbb{Z}[x]$$

注: 命题 5.33 (1) 也可通过带因式证:

$$\text{对 } \forall \text{ 素数 } p, \quad \pi: \mathbb{F}[x] \rightarrow \mathbb{F}_p[x] \quad \sum a_i x^i \mapsto \sum \bar{a}_i x^i$$

$$\text{为环同态. } \left. \begin{array}{l} c(f) = 1 \Rightarrow \pi(f) \neq 0 \\ c(g) = 1 \Rightarrow \pi(g) \neq 0 \end{array} \right\} \Rightarrow \pi(fg) \neq 0 \Rightarrow p \nmid c(fg)$$

定理 5.34 (Gauss 引理)  $f(x) \in \mathbb{Z}[x]$ . 若  $f(x) = g(x) \cdot h(x)$ ,  
 $g(x), h(x) \in \mathbb{Q}[x], \quad 0 < \deg g(x), \deg h(x) < \deg f(x)$ .

则存在  $d \in \mathbb{Q}^*$ , 使得  $g(x) = d g_1(x), h_1(x) = \frac{1}{d} h(x) \in \mathbb{Z}[x]$

特别地  $f(x)$  在  $\mathbb{Q}[x]$  中可约  $\Rightarrow f(x)$  在  $\mathbb{Z}[x]$  中可约.

PF  $h(x) \in \mathbb{Q}[x]$ . 则  $h(x) = \frac{v}{u} h_1(x)$ , 其中  $u, v \in \mathbb{Z} \setminus \{0\}$ ,

$$h_1(x) \in \mathbb{Z}[x], \quad c(h_1) = 1 \quad \text{取 } d = \frac{v}{u}$$

$$\text{则 } f(x) = d g_1(x) h_1(x), \text{ 由 } \exists \text{ 引理 } d g_1(x) \in \mathbb{Z}[x]. \quad \#$$

命题 5.35  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ ,  $a_n \neq 0$ .  $a = \frac{p}{q}$  为  $f(x)$  的有理根,  $(p, q) = 1$ . 则  $p \mid a_0$ ,  $q \mid a_n$ .

PF:  $f(x) = (qx - p) g(x)$ ,  $\exists g(x) \in \mathbb{Q}[x]$ .  
 $\Rightarrow g(x) \in \mathbb{Z}[x]$ .  $\Rightarrow q \mid a_n$ ,  $p \mid a_0$   $\#$

例  $f(x) = 3x^3 + x + 7$  无有理根.  
 验证  $\pm 1, \pm \frac{1}{3}, \pm 7, \pm \frac{7}{3}$ .

定理 5.36 (Eisenstein 判别法)  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$   
 $p$  素.  $p \nmid a_n$ ,  $p \mid a_i, 0 \leq i \leq n-1$ ,  $p^2 \nmid a_0$ . 则  $f(x) \in \mathbb{Q}[x]$  不可约.

证明: 反设, 类似 5.33 (1) 证明

方法:  $f(x) \in \mathbb{Q}[x]$  中可约

$\Rightarrow f(x) = g(x) h(x)$ ,  $0 < \deg g(x) < n$ ,  $g(x), h(x) \in \mathbb{Z}[x]$ .

$\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$

$\bar{f}(x) = \bar{g}(x) \bar{h}(x)$ .

$\bar{f}(x) = \bar{a}_n x^n \Rightarrow \bar{g}(x) = \bar{b}_m x^m, \bar{h}(x) = \bar{c}_k x^n$

$\Rightarrow p \mid b_0, p \mid c_0 \Rightarrow p^2 \mid b_0 c_0$  矛盾.

例  $p$  次分圆多项式  $\Phi_p(x) = 1 + x + \dots + x^{p-1} = \prod_{n=1}^{p-1} (x - \zeta_p^n)$   
 $\zeta_p = e^{\frac{2\pi i}{p}}$  为  $n$  次本原单位根.

$\Phi_p(x+1) = x^{p-1} + \sum_{k=1}^{p-1} C_p^k x^{k-1}$ .

$p \mid C_p^k, k=1, \dots, p-1, \quad p^2 \nmid C_p^1 = p$   $\#$

## 第六章 对称群与多元多项式

## § 6.1 置换及其表示

定义 6.1  $n \geq 1$ ,  $n$  阶对称群, 记作  $S_n$ , 为集合  $\{1, 2, \dots, n\}$  的对称群, 其元素为  $\{1, \dots, n\}$  的  $n$ -置换, 或排列 (permutation)

注: 集合  $A$  的对称群即  $A$  到  $A$  双射在映射复合下的群.

命题 6.2  $|S_n| = n!$ , 且当  $n \geq 3$  时  $S_n$  为非交换群.

证.  $|S_n| = \# \text{ 全排列} = n!$

$S_1 = \{1\}$   $S_2 = \{1, \sigma\}$ . 其中  $\sigma(1)=2$   
 $\sigma(2)=1$   
 为交换群.

若  $n \geq 3$  考虑

$$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}, \quad \begin{array}{l} 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1 \\ i \mapsto i \quad i \geq 4 \end{array}$$

$$\tau: \{1, \dots, n\} \rightarrow \{1, \dots, n\}, \quad \begin{array}{l} 1 \mapsto 2, 2 \mapsto 1 \\ i \mapsto i \quad i \geq 3 \end{array}$$

$$\sigma\tau(1) = \sigma(2) = 3 \quad \sigma\tau \neq \tau\sigma$$

$$\tau\sigma(1) = \tau(2) = 1$$

记法:  $\left( \begin{array}{cccccc} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{array} \right)$  或  $\left( \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{array} \right)$

$\sigma^{-1} = \left( \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 5 & 1 \end{array} \right)$   $\overset{11}{\sigma}$

定义 6.3  $\{i_1, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$ . 置换  $(i_1 i_2 \dots i_k)$

是指  $i_1 \mapsto i_2 \mapsto i_3 \mapsto \dots \mapsto i_k \mapsto i_1$ ,  $j \mapsto j \quad \forall j \notin \{i_1, \dots, i_k\}$

称为一个  $k$ -轮换 (k-cycle).

2-轮换称为对换 (transposition).

注: 1-轮换为单位元, 记作 1.

定义 6.4 若  $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$ , 则称轮换  $(i_1 \dots i_k)$  与  $(j_1 \dots j_l)$  不相交. 否则称它们相交.



# 定理 6.5

(1) 两个互不相交的轮换可交换

(2)  $S_n$  中任一元素可以写成若干个两两互不相交的轮换的乘积, 且不计先后次序并排除 1-轮换情况下唯一.

证明

(1)  $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$ . 令  $i_{k+1} = i_1, j_{l+1} = j_1$

则  $\sigma = (i_1 \dots i_k) \quad \tau = (j_1 \dots j_l)$

$$\sigma\tau(i_r) = \sigma(i_r) = i_{r+1}$$

$$\sigma\tau(j_s) = \sigma(j_s) = j_{s+1}$$

$$\sigma\tau(x) = x \quad \forall x \notin \{i_1, \dots, i_k, j_1, \dots, j_l\}$$

对  $\tau\sigma$  进行计算可知  $\tau\sigma = \sigma\tau$ .

(2) 设  $\sigma \in S_n$ . 定义  $\{1, \dots, n\}$  上关系如下:

$$i \sim j \quad \text{若} \exists k \geq 0, \sigma^k(i) = j.$$

易知  $\sim$  为  $S_n$  上等价关系.

令  $X^1, \dots, X^r$  为  $\{1, \dots, n\}$  在此等价关系下

的等价类. 设  $|X^\alpha| = k_\alpha \quad \forall 1 \leq \alpha \leq r$

可令  $X_\alpha = \{x_1^\alpha, \dots, x_{k_\alpha}^\alpha\}$  使得  
 $\sigma \cdot x_i^\alpha = x_{i+1}^\alpha$ , 其中  $x_{k_\alpha+1}^\alpha \triangleq x_1^\alpha$ .

则显然

$$\sigma = (x_1^1 \dots x_{k_1}^1) \dots (x_1^r \dots x_{k_r}^r).$$

反之, 若  $\sigma = (y_1^1 \dots y_{k_1}^1) \dots (y_1^s \dots y_{k_s}^s)$  为互不相交的轮换乘积. 添加上若干个 1-轮换. 不妨设  
 $\{y_1^1, \dots, y_{k_1}^1\} \cup \dots \cup \{y_1^s, \dots, y_{k_s}^s\} = \{1, 2, \dots, n\}$ .

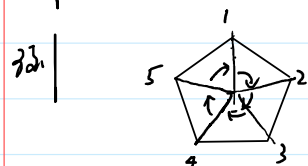
显然  $\{1, \dots, n\}$  在  $\sim$  下的等价类恰如为

$$Y^1 = \{y_1^1, \dots, y_{k_1}^1\}, \dots, Y^s = \{y_1^s, \dots, y_{k_s}^s\}$$

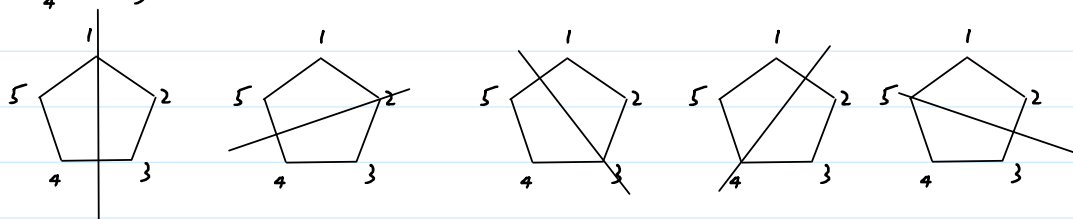
从而  $Y^1, \dots, Y^s$  为  $X^1, \dots, X^r$  的一个排列  
 唯一性即证.

例  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix}$

$\sigma = (16)(243)(5) = (16)(243)$



$D_\sigma = \left\{ \begin{aligned} &1, (12345), (13524), (14253), (154321), \\ &(25)(34), (13)(45), (24)(15), (31)(12), (14)(23) \end{aligned} \right\}$



例  $S_1 = \{1\}, S_2 = \{1, (12)\}, S_3 = \{1, (12), (13), (23), (123), (132)\}$

$S_4 = \left\{ \begin{aligned} &1, \\ &(12), (13), (14), (23), (24), (34) \\ &(123), (132), (234), (243), (124), (142), (134), (143) \\ &(12)(34), (13)(24), (14)(23) \\ &(1234), (1243), (1324), (1342), (1423), (1432) \end{aligned} \right\}$

注 (1)  $(i_1 i_2 \dots i_k) = (i_2 \dots i_k i_1) = \dots = (i_k i_1 i_2 \dots i_{k-1})$

(2)  $(i_1 i_2 \dots i_k)^{-1} = (i_k i_{k-1} \dots i_1)$

定义 6.6 将  $\sigma \in S_n$  写成不相交轮换乘积时, 其中  $k$ -轮换个数记作  $\lambda_k$  则称  $\sigma$  的型为  $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$

注 满足  $\sum_{i=1}^n i \lambda_i = n$  的  $(\lambda_1, \dots, \lambda_n)$  称为  $n$  的一个分拆 (partition)  
 $n$  的分拆的个数称为分拆函数记作  $p(n)$ .

例  $n=3: 1^3, 1^1 2^1, 3^1$   
 $n=4: 1^4, 1^2 2^1, 2^2, 1^1 3^1, 4^1$   
 $n=5: 1^5, 1^3 2^1, 1^2 3^1, 1^1 2^2, 1^1 4^1, 2^1 3^1, 5$

命题 7  $\sigma, \sigma' \in S_n$ .  $\sigma$  与  $\sigma'$  同型当且仅当  $\sigma$  与  $\sigma'$  共轭.  
特别地,  $S_n$  共轭类共有  $p(n)$  个.

PF: 注意到  $\sigma(i_1 \dots i_k) \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$ . (\*)  
 $(\sigma(i_1' \dots i_k') = (\sigma(i_1) \dots \sigma(i_k)) \sigma)$

$\Rightarrow$  设  $\sigma, \sigma'$  同型.  $\sigma$  中出现的轮换长度为  $k_1 \geq k_2 \geq \dots \geq k_s$

$$\text{设 } \sigma = (x_{11} \dots x_{1k_1})(x_{21} \dots x_{2k_2}) \dots (x_{s1} \dots x_{sk_s})$$

$$\sigma' = (x'_{11} \dots x'_{1k_1})(x'_{21} \dots x'_{2k_2}) \dots (x'_{s1} \dots x'_{sk_s})$$

$$\text{令 } \tau = \begin{pmatrix} x_{11} \dots x_{1k_1} & x_{21} \dots x_{2k_2} & \dots & x_{s1} \dots x_{sk_s} \\ x'_{11} \dots x'_{1k_1} & x'_{21} \dots x'_{2k_2} & \dots & x'_{s1} \dots x'_{sk_s} \end{pmatrix}$$

$$\text{则 } \tau(x_{ij}) = x'_{ij} \quad \text{则}$$

$$\tau\sigma\tau^{-1} = \sigma'$$

$\Leftarrow$  利用  $\tau\sigma_1\tau^{-1} = \tau\sigma_1\tau^{-1} \cdot \tau\sigma_2\tau^{-1}$  以及 (\*) 可知.

## §6.2 置换的奇偶性与交错群

命题 6.8 (1) 任一  $k$ -轮换可写成  $k-1$  个对换乘积.

(2)  $(12), (13), \dots, (1n)$  为  $S_n$ -组生成元.

$$\text{PF. (1) } (i_1 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k) \\ = (i_1 i_k) \dots (i_1 i_3)(i_1 i_2)$$

$$(2) (ij) = (1j)(1i)(1j)$$

定义 6.9  $\sigma \in S_n$ .  $\sigma$  的 逆序数 定义为  
 $\# \{ (i, j) \mid i < j, \sigma(i) > \sigma(j) \}$ .

例. 1 逆序数为 0.

$\begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$  的逆序数为  $\frac{1}{2}n(n-1)$ .

引理 6.10 设  $\sigma \in S_n$ .  $\tau \in S_n$  为对换. 则  $\sigma\tau$  与  $\sigma$  逆序数奇偶性互异.

PF. 首先设  $\tau = (i, i+1)$ .

$$\text{设 } \sigma = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \sigma(i+1) & \dots & \sigma(n) \end{pmatrix} \quad \text{则 } \sigma\tau = \begin{pmatrix} 1 & 2 & \dots & i+1 & i & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \sigma(i+1) & \dots & \sigma(n) \end{pmatrix}$$

则  $\sigma\tau$  逆序数 =  $\sigma$  逆序数  $\pm 1$ .

另一方面,  $\forall j > i$ .

$$(ij) = (i, i+1)(i+1, i+2) \dots (j-1, j)(j, j+1) \dots (i+1, i)$$

故  $\sigma$  逆序数奇偶性与  $\sigma$  奇偶性互异.

引理 6.11 设  $\sigma \in S_n$  奇偶数为  $l$ . 则  $\sigma$  可写成  $l$  个对换乘积.

PF 对  $n$  归纳.

•  $n=1, 2$  显然成立.

• 设结论对  $\leq n-1$  成立. 下面考察  $S_n$ .

$l = l_n + l_{n-1} + \dots + l_2$ , 其中  $l_i = \#\{ (r, s) \mid r < s, \sigma_{(rs)} < \sigma_{(r)} = i \}$

设  $n = \sigma(k)$ . 则  $l_n = n - k$

$$\begin{aligned} \begin{pmatrix} 1 & 2 & \dots & k & \dots & n \\ \sigma_{(1)} & \sigma_{(2)} & \dots & \sigma_{(k)} & \dots & \sigma_{(n)} \end{pmatrix} &= (\sigma_{(k)} \sigma_{(k+1)}) \cdot \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots & n \\ \sigma_{(1)} & \sigma_{(2)} & \dots & \sigma_{(k+1)} & \sigma_{(k)} & \dots & \sigma_{(n)} \end{pmatrix} \\ &= \dots = (\sigma_{(k)} \sigma_{(k+1)}) (\sigma_{(k)} \sigma_{(k+2)}) \dots (\sigma_{(k)} \sigma_{(n)}) \begin{pmatrix} 1 & \dots & k-1 & k & k+1 & \dots & n-1 & n \\ \sigma_{(1)} & \dots & \sigma_{(k-1)} & \sigma_{(k+1)} & \sigma_{(k+2)} & \dots & \sigma_{(n)} & n \end{pmatrix} \\ \text{令 } \sigma_1 &= \begin{pmatrix} 1 & \dots & k-1 & k & k+1 & \dots & n-1 \\ \sigma_{(1)} & \dots & \sigma_{(k-1)} & \sigma_{(k+1)} & \sigma_{(k+2)} & \dots & \sigma_{(n)} \end{pmatrix} \in S_{n-1} \end{aligned}$$

且  $\sigma_1$  逆序数恰为  $l - l_n = l_2 + \dots + l_{n-1}$

由归纳假设  $\sigma_1$  可写为  $l_2 + \dots + l_{n-1}$  个对换乘积.  $\#$

定理 6.12 存在群同态  $\text{sgn}: S_n \rightarrow \{\pm 1\}$ , 使得  $\text{sgn}(\tau) = -1$  对任一-对换  $\tau$

PF. 令  $\text{sgn}(\sigma) = (-1)^l$ . 其中  $l$  为  $\sigma$  逆序数.  
则  $\text{sgn}(\sigma)$  即为所求.

定义 6.13  $\sigma \in S_n$  若可写成奇数个对换乘积. 则称  $\sigma$  为奇置换.  
偶  
偶置换  
记  $A_n$  为  $S_n$  中偶置换形成的子群. 称为  $n$  阶交错群.

例 所有 3-轮换为  $A_n$  一组生成元:  $i, j, k, l$  互不相同

$$(ij)(kl) = (ijk)(ikl)$$

$$(ij)(ik) = (ikj)$$

任一-偶置换可写成偶数个对换乘积.

定义 6.14  $G$  为群.  $N \leq G$  为子群. 若  $\forall g \in G, gNg^{-1} = N$   
则称  $N$  为正规子群. 记作  $N \triangleleft G$ .

- 证: 1.  $G$  为阿贝尔群. 则  $\forall H \leq G$  为  $H$  正规子群  
 2.  $A_n \triangleleft S_n$ .

定理 6.15 (1) 在  $G/N$  上可定义乘法  $gN \cdot hN = ghN$ , 使得  $G/N$  形成一个群. 称为  $G$  对于子群  $N$  的商群.

(2) 设  $f: G \rightarrow H$  为群同态. 则  $\ker f = \{g \in G \mid f(g) = 1\} \triangleleft G$   
 且  $\bar{f}: G/\ker f \rightarrow \text{Im } f$ ,  $\bar{f}(g\ker f) \triangleq f(g)$   
 为群同构.

证明: 由定义验证可知.

定理 6.16 设  $N \triangleleft A_5$ , 则  $N = \{1\}$  或  $N = A_5$ .

证明: 设  $N \triangleleft A_5$ .  $N \neq \{1\}$ . 只需证明  $N$  中含有一个 3-轮换. 则由  $N$  正规性知  $N$  包含所有 3-轮换故  $N = A_5$ .

$A_5$  中偶置换具有型  $1^2 2^2$ ,  $1^2 3^1$ ,  $5^1$ . 设  $1 \neq \sigma \in N$ .

•  $\sigma$  具有型  $1^2 2^2$ . 不妨设  $\sigma = (12)(34)$

则令  $\tau = (12)(45)$   $\tilde{\sigma} = \tau\sigma\tau^{-1} = (12)(35) \in N$

从而  $\tilde{\sigma} \cdot \sigma = (345) \in N$ .

•  $\sigma$  具有型  $1^2 3^1$  ✓

•  $\sigma$  具有型  $5^1$ . 设  $\sigma = (12345)$

令  $\tau = (123)$ . 则  $\tilde{\sigma} = \tau\sigma\tau^{-1} = (23145) \in N$ .

$\sigma^{-1}\tilde{\sigma} = (54321)(23145) = (135) \in N$ . #

定义 6.17 若  $G$  仅含有平凡的正规子群. 则称  $G$  为单群

例:  $(\mathbb{Z}/n\mathbb{Z}, +)$  为单群  $\iff n$  素.

$A_5$  为单群.

$A_2 \cong \{1\}$ .

$A_3 = \{1, (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}$

$A_4 = \left\{ 1, (12)(34), (14)(23), (13)(24), \right. \\ \left. (123), (124), (132), (142), (134), (143), (234), (243) \right\}$

$$K_4 = \{1, (12)(34), (14)(23), (13)(24)\} \triangleleft A_4.$$

定理 6.18  $A_n$  ( $n \geq 5$ ) 为单群.

注: 有限单群:  $\mathbb{Z}/p\mathbb{Z}$ ,  $A_n$  ( $n \geq 5$ ), 李型单群  
26 个 散在单群.

阶最大的魔群 (monster):

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

忠实不可约表示维数最低为 196883

阶次大的小魔群 (baby monster)

$$41\,5478\,1481\,2264\,2619\,1177\,5805\,4400\,0000$$

# 对称多项式

2021年1月4日 20:11

定义 1.19  $F$  为域,  $x_1, \dots, x_n$  为  $n$  个不定元.  $F$  上的一个  $n$  元多项式 是指

一个有限形式和  $\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$

$$\sum a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} = \sum b_{j_1, \dots, j_n} x_1^{j_1} \dots x_n^{j_n}$$

$$\Leftrightarrow a_{i_1, \dots, i_n} = b_{i_1, \dots, i_n} \quad \forall (i_1, \dots, i_n) \in \mathbb{N}^n$$

$F$  上  $n$  元多项式的集合记作  $F[x_1, \dots, x_n]$

形如  $a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$  的单项式称为单项式

$i_1 + i_2 + \dots + i_n$  记为单项式  $a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$  的次数

$f(x)$  的次数 为  $f(x)$  中所出现单项式次数最高者. 记作  $\deg f$ .

$\in F[x_1, \dots, x_n]$  上定义  $+$ ,  $\cdot$  如下:

$$\sum a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} + \sum b_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} = \sum (a_{i_1, \dots, i_n} + b_{i_1, \dots, i_n}) x_1^{i_1} \dots x_n^{i_n}$$

$$\sum a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} \cdot \sum b_{j_1, \dots, j_n} x_1^{j_1} \dots x_n^{j_n} = \sum_{(k_1, \dots, k_n) \in \mathbb{N}^n} c_{k_1, \dots, k_n} x_1^{k_1} \dots x_n^{k_n}$$

$$\text{其中 } c_{k_1, \dots, k_n} = \sum_{\substack{i_1, \dots, i_n, j_1, \dots, j_n \in \mathbb{N} \\ i_1 + j_1 = k_1, \dots, i_n + j_n = k_n}} a_{i_1, \dots, i_n} b_{j_1, \dots, j_n}$$

注  $F[x_1, x_2] = (F[x_1])[x_2] = (F[x_2])[x_1]$

$$F[x_1, \dots, x_n] = ((F[x_1])[x_2]) \dots [x_n]$$

$\sigma \in S_n$  置换

$$f(x_1, \dots, x_n) = \sum a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$$

$$(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

$$= \sum a_{i_1, \dots, i_n} x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n}$$

例:  $\sigma = (123), \quad f(x) = x_1^2 - x_2$

$$(\sigma f)(x) = x_2^2 - x_3$$



引理 6.20

$$(1) \quad \sigma = 1 \Rightarrow \sigma \cdot f = f$$

$$(2) \quad \sigma, \tau \in S_n, \forall f \quad (\sigma\tau)f = \sigma(\tau f).$$

$$(3) \quad \sigma(\lambda f + \mu g) = \lambda \sigma f + \mu \sigma g, \text{ 其中 } \lambda, \mu \in F, f, g \in F[x_1, \dots, x_n], \sigma \in S_n.$$

证明: 我们仅对 (2) 进行证明. 易知, 只需对单项式证明即可.

$$\text{设 } f(x) = x_1^{i_1} \cdots x_n^{i_n}.$$

$$\text{则 } (\sigma\tau) \cdot f(x) = x_{\sigma\tau(1)}^{i_1} \cdots x_{\sigma\tau(n)}^{i_n}$$

$$\text{而 } (\tau f)(x) = x_{\tau(1)}^{i_1} \cdots x_{\tau(n)}^{i_n}$$

$$\Rightarrow \sigma(\tau f) = \sigma(x_{\tau(1)}^{i_1} \cdots x_{\tau(n)}^{i_n}) = x_{\sigma(\tau(1))}^{i_1} \cdots x_{\sigma(\tau(n))}^{i_n} \\ = x_{(\sigma\tau)(1)}^{i_1} \cdots x_{(\sigma\tau)(n)}^{i_n} \quad \#$$

证. 引理 6.20 说明  $S_n$  “作用”  $F[x_1, \dots, x_n]$  上.

$G$  作用在集合  $X$  上 拆映射

$$G \times X \rightarrow X \quad s.t. \\ (g, x) \mapsto g \cdot x.$$

$$(1) \quad g(h \cdot x) = (gh) \cdot x$$

$$(2) \quad 1 \cdot x = x$$

$$\text{例} \quad \text{令 } f(x) = \prod_{i < j} (x_i - x_j) \quad \text{则 } \sigma \cdot f = (-1)^{\text{sgn}(\sigma)} f.$$

另一方面,  $S_n$  作用在集合  $\{f(x), -f(x)\}$  上.

$$\forall \tau = (i, j), \Rightarrow \tau f = -f$$

从而可给出定理 6.12 的一个证明.

$$\text{例} \quad \text{令 } P_1(x) = x_1 + \cdots + x_n, \quad P_2(x) = x_1^2 + \cdots + x_n^2, \quad \dots, \quad P_n(x) = x_1^n + \cdots + x_n^n$$

$$\text{则 } \sigma \cdot P_k(x) = P_k(x) \quad \forall \sigma \in S_n.$$

$$\text{例} \quad \text{令 } e_1(x) = x_1 + \cdots + x_n, \quad e_2(x) = \sum_{1 \leq i < j \leq n} x_i x_j \quad \dots$$

$$e_k(x) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

$$\dots \\ e_n(x) = x_1 x_2 \cdots x_n.$$

$$\text{则 } \sigma \cdot (e_k) = e_k \quad \forall \sigma \in S_n.$$

显然若  $\alpha_1, \dots, \alpha_n$  为  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  的  $n$  个根, 则  $a_i = (-1)^{n-i} e_{n-i}(\alpha_1, \dots, \alpha_n)$ .

例 令  $h_1(x) = x_1 + \dots + x_n$ ,  $h_2(x) = \sum_{1 \leq i < j \leq n} x_i x_j$  ...  
 $h_k(x) = \sum_{i_1 + \dots + i_n = k} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$   
 $h_n(x) = \sum_{i_1 + \dots + i_n = n} x_1^{i_1} \dots x_n^{i_n}$   
 则  $\sigma \cdot h_k = h_k \quad \forall \sigma \in S_n$

定义 6.21 设  $f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} \in F[x_1, \dots, x_n]$ .  
 称为域  $F$  上的  $n$  元对称多项式 (symmetric polynomial),  
 若  $\sigma \cdot f = f \quad \forall \sigma \in S_n$ . 即  $a_{i_1, \dots, i_n} = a_{i_{\sigma(1)}, \dots, i_{\sigma(n)}} \quad \forall \sigma \in S_n$ .

$e_1, \dots, e_n$  称为初等对称多项式. elementary ...  
 $p_1, \dots, p_n$  幂和对称多项式 power sum ...  
 $h_1, \dots, h_n$  完全齐次对称多项式 complete homogeneous ...

例  $n=3$   $p_1 = x_1 + x_2 + x_3$   $p_2 = x_1^2 + x_2^2 + x_3^2$   $p_3 = x_1^3 + x_2^3 + x_3^3$   
 $e_1 = x_1 + x_2 + x_3$   $e_2 = x_1x_2 + x_1x_3 + x_2x_3$   $e_3 = x_1x_2x_3$

易知:  $p_1 = e_1$   
 $p_2 = e_1^2 - 2e_2$   
 $p_3 = e_1^3 - 3e_1e_2 + 3e_3$

定理 6.22  $F$  上  $n$  元对称多项式均可表示为初等对称多项式的全多项式. 即  
 $f \in F[x_1, \dots, x_n]$ ,  $\sigma f = f \quad \forall \sigma \in S_n$  则存在  $g \in F[e_1, \dots, e_n]$  使得  
 $f(x_1, \dots, x_n) = g(e_1, e_2, \dots, e_n)$ .

PF. 对单项式  $x_1^{i_1} \dots x_n^{i_n}$  定义其权重  $w = i_1 + 2i_2 + \dots + ni_n$ .

对一个多项式  $f(x) \in F[x_1, \dots, x_n]$ , 其权重  $w(f)$  定义为  $f(x)$  中出现的单项式中的最大权重.

$\in \mathbb{N}^n$  上定义字典序如下:

$(i_1, i_2, \dots, i_n) < (j_1, j_2, \dots, j_n)$  若

$$\begin{aligned}
 & \text{或 } i_n = j_n, i_{n-1} < j_{n-1} \\
 & \text{或 } i_n = j_n, i_{n-1} = j_{n-1}, i_{n-2} < j_{n-2} \\
 & \vdots \\
 & \text{或 } i_n = j_n, i_{n-1} = j_{n-1}, i_{n-2} = j_{n-2}, \dots, i_2 = j_2, i_1 = j_1.
 \end{aligned}$$

显然, 上述关系为  $\mathbb{N}^n$  上的全序.

称  $(i_1, \dots, i_n) \in \mathbb{N}^n$  为单项式  $x_1^{i_1} \dots x_n^{i_n}$  的 **总次数**  
 $f(x_1, \dots, x_n)$  的 **总次数** 为  $f$  中出现单项式的最大总次数, 记  
 作  $\deg f = (i_1, \dots, i_n)$ . 记  $|\deg f| = i_1 + \dots + i_n$ .

$$\text{显然 } \deg f \geq |\deg f|$$

断言:  $f \in F[x_1, \dots, x_n]$ .  $\deg f = d$ . 则存在权重  $\leq d$  的  
 多项式  $g(y_1, \dots, y_n)$ , 使得  $f(x_1, \dots, x_n) = g(e_1, \dots, e_n)$

对  $\deg f$  和  $|\deg f|$  进行归纳:

$$\left( \text{注意到 } \forall d \geq 0, \text{ 仅存在有限个 } (i_1, \dots, i_n) \in \mathbb{N}^n, \text{ 使得 } \right. \\
 \left. i_1 + i_2 + \dots + i_n = d \right)$$

- $\deg f = 0$ .  $f$  为常值多项式, 结论平凡.
- 设  $\deg f < d$  时结论成立. 下设  $\deg f = d$ .

设  $\deg f = (i_1, \dots, i_n)$ ,  $0 \neq a_{i_1, \dots, i_n}$  为  $x_1^{i_1} \dots x_n^{i_n}$  项的系数.

由定义有  $i_1 \leq i_2 \leq \dots \leq i_n$ .

$$(f \text{ 对称}, a_{i_{\sigma(1)}, \dots, i_{\sigma(n)}} = a_{i_1, \dots, i_n} \quad \forall \sigma \in S_n)$$

$$\text{取 } g(y_1, \dots, y_n) = a_{i_1, \dots, i_n} y_1^{i_n - i_{n-1}} y_2^{i_{n-1} - i_{n-2}} \dots y_n^{i_1}$$

$$\text{则 } W(g) = n i_1 + (n-1)(i_2 - i_1) + \dots + i_n - i_{n-1} = |\deg f| \leq d.$$

$$\text{且 } \deg g_1(e_1, \dots, e_n) = (i_1, i_2, \dots, i_n) \quad (\text{看作 } x_1, \dots, x_n \text{ 多项式})$$

$$\text{令 } f_1(x) = f(x) - g_1(e_1, \dots, e_n) \in F[x_1, \dots, x_n]$$

$$\text{显然 } \sigma \cdot f_1 = f_1 \quad \forall \sigma \in S_n. \text{ 且 } \deg f_1 < \deg f$$

重复上述步骤, 可得

$$f_2 = f_1 - g_2(e_1, \dots, e_n), \dots, f_m = f_{m-1} - g_m(e_1, \dots, e_n), \dots$$

使得  $g_1, \dots, g_m \in F[y_1, \dots, y_n]$ .  $\deg f_{i+1} < \deg f_i$ .

故  $\exists m > 0$ , 使得  $\deg f_m < d$

由归纳知  $f_m = g_{m+1}(e_1, \dots, e_n)$ ,  $g_{m+1} \in F[y_1, \dots, y_n]$

故  $f(x) = (g_1 + g_2 + \dots + g_{m+1})(e_1, \dots, e_n)$   $\neq$

定义 6.23  $f(x) = (x-x_1) \dots (x-x_n)$ . 称

$$D(f) = D(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j)^2$$

为  $f(x)$  的 判别式 (discriminant).

$D_f$  可看作关于  $f(x)$  的  $n$  个根的对称多项式, 从而可写成  $f(x)$  各次系数的多项式.

命题 6.24 (1)  $f(x) = x^2 + bx + c \Rightarrow D(f) = b^2 - 4c$

(2)  $f(x) = x^3 + ax + b \Rightarrow D(f) = -4a^3 - 27b^2$

PF. (1)  $D_f = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c$

(2)  $D_f = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_1 - x_3)^2$

$$= \alpha_1 e_1^6 + \alpha_2 e_1^4 e_2 + \alpha_3 e_1^3 e_3 + \alpha_4 e_1^2 e_2^2 + \alpha_5 e_1 e_2 e_3 + \alpha_6 e_2^3 + \alpha_7 e_3^2$$

$$e_1 = x_1 + x_2 + x_3 = 0 \quad e_2 = x_1x_2 + x_1x_3 + x_2x_3 = a, \quad e_3 = x_1x_2x_3 = -b$$

$$\Rightarrow D_f = \alpha_6 a^3 + \alpha_7 b^2$$

待定系数, 取  $x_1 = 1, x_2 = -1, x_3 = 0$  则  $a = -1, b = 0, D = 4$

$$\text{从而 } \alpha_6 = -4$$

$$x_1 = 1 = x_2, x_3 = -2 \quad \text{则 } a = -3, b = -2, D = 0$$

$$\text{从而 } 4\alpha_7 + 4 \cdot 27 = 0 \Rightarrow \alpha_7 = -27$$

$$\Rightarrow D_f = -4a^3 - 27b^2 \quad \neq$$