代数学基础期末复习

杨柳依 y

2024.01.11

目录

0 引言

本文为作者复习代数学基础使用，内容顺序为杨老师授课顺序。可能会出现笔误，本文一切解释权归作者所有。

1 群、环、域

1.1 群、环、域基本概念

1.1.1 域的定义

称 $(K,+,\cdot)$ 为一个域，若满足

0、封闭性

加法
$$\begin{cases}1、加法结合律\ \forall a,b,c\in K,(a+b)+c=a+(b+c)\\2、零元存在性\ \exists 0_k\in K,s.t.a+0_K=a=0_K+a\\3、负元存在性\ \forall a\in K,\exists b\in K,a+b=0_k=b+a\\4、加法交换律\ \forall a,b\in K,a+b=b+a\end{cases}$$

$+$、$\bullet$ 相容:5、分配律 $\forall a,b,c\in K,a(b+c)=ab+ac,(a+b)c=ac+bc$

乘法
$$\begin{cases}6、乘法结合律\ \forall a,b,c\in K,(ab)c=a(bc)\\7、单位元存在性\ \exists 1_k\in K,s.t.a\cdot 1_K=a=1_K\cdot a\\8、乘法交换律\ \forall a,b\in K,ab=ba\\9、逆元存在性\ \forall a\in K\backslash\{0\},\exists b\in K,s.t.ab=1_k=ba\end{cases}$$

域区别于环的最显著特征是非零元均可逆

1.1.2 子域的判定

$$\text{F 为子域}\Leftrightarrow\begin{cases}1_K\in F\\\text{F 关于 }-、\bullet\text{ 封闭}\\\text{若 }a\in F\backslash\{0\},\text{则 }a^{-1}\in F\end{cases}$$

1.1.3 环的定义与基本性质

若 $(R,+,\cdot)$ 满足上述 $1\sim 7$，则称 R 为 (含幺) 环

若 $(R,+,\cdot)$ 满足上述 $1\sim 8$，则称 R 为 (含幺) 交换环

• 特别地，$2\mathbb{Z}=\{2n \mid n\in\mathbb{Z}\}$ 为不含幺元的环

• $(M_2(\mathbb{R}),+,\cdot)$ 为含幺非交换环 ($M_2(\mathbb{R})$ 为 2 阶实矩阵)

• 零环：$0_R=1_R$

• 乘法消去律不一定成立！($x^n=0, x=0$ 不一定成立!)

又如 $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$

整环的定义: 设 (R,+, •) 为交换环，若对 $\forall a,b\in R\backslash\{0\}$，

有 $ab\neq 0$，则称 R 为整环 (整环 = 交换环 + 消去律)

1.1.4 子环的判定

$(R,+,\cdot)$ 为环 $T\subseteq R$，则

$$\text{T 为子环}\Leftrightarrow\begin{cases}1_R\in T\\ \text{T 关于 }-\text{、}\bullet\text{ 封闭}\end{cases}$$

1.1.5 群的定义

设 (G, •) 为带一个二元运算的代数系统,$G\neq\varnothing$

0、封闭性

$$\begin{cases}1\text{、结合律 }\forall a,b,c\in G,(ab)c=a(bc)\\ 2\text{、单位元存在性 }\exists 0_G\in K, s.t. a\cdot 1_G=a=1_G\cdot a\\ 3\text{、逆元存在性 }\forall a\in G,\exists b\in G ab=1_G=ba\\ 4\text{、交换律 }\forall a,b\in G, ab=ba\end{cases}$$

1° 若 G 满足 $1\sim 4$，则称 G 为交换群 (阿贝尔群)

2° 若 G 满足 $1\sim 3$，则称 G 为群

3° 若 G 满足 $1\sim 2$，则称 G 为含幺半群

4° 若 G 满足 1，则称 G 为半群

注: 若是乘法群, 则单位元为 1; 若是加法群, 则单位元为 0, 逆元为负元

例：$(\{1,2,\cdots\},+)$ 半群不含幺

$(\{0,1,2,\cdots\},+)$ 含幺半群

单位群: 设 R 为非零环，则 $R^\times:=\{r\in R \mid \text{r 乘法可逆}\}$

例:$GL_2(\mathbb{R}):=\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2\mathbb{R}\mid ad-bc\neq 0\}$ 为群但非交换

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的乘法逆元为 $\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$

1.1.6 子群的判定

(G, •) 为群

H 为 G 的子群 $\Leftrightarrow \forall a,b \in H, \begin{cases} a \cdot b \in H \\ a^{-1} \in H \end{cases} \Leftrightarrow \forall a,b \in H, a \cdot b^{-1} \in H$

1.2 同态与同构

1.2.1 群同态与群同构

定义: 设 $(G, \cdot), (G', *)$ 为两群, 设映射 $\varphi : G \to G'$

1° 若对 $\forall a,b \in G$ 有 $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ 则称 φ 为群同态

2° 若 φ 为群同态且为双射，则称 φ 为群同构

例:$det : GL_2 \to \mathbb{R}^\times \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto ad - bc$ 为群同态

群同态的性质:

设 $f : G_1 \to G_2$ 为群同态，则

1°$f(1) = 1, f(g^{-1}) = (f(g))^{-1}$

2°$Ker(f) := \{g \in G \mid f(g) = 1_{G2}\}$ 为 G_1 的子群，称为 f 的核 (kernel)

$imf := \{f(g) \mid g \in G_1\}$ 为 G_2 的子群，称为 f 的像 (image)

3°f 为同构，则 f^{-1} 为同构

pf:

1° $f(1) = f(1 \cdot 1) = f(1) * f(1)$

由 G_2 中的消去律，$f(1) = 1_{G2}$

所以，$1 = f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$

$\Rightarrow f(g^{-1}) = (f(g))^{-1}$

2° 要证明子群，只需证明除法封闭

• Ker(f)：$\forall g_1, g_2 \in Ker(f)$

$f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1)(f(g_2))^{-1} = 1 \cdot 1^{-1} = 1$

$\Rightarrow g_1 g_2^{-1} \in Ker(f)$

• im(f)：$\forall g_1^{'} = f(g_1), g_2^{'} = f(g_2) \in im(f)$

$g_1^{'}(g_2^{'})^{-1} = f(g_1)(f(g_2))^{-1} = f(g_1 g_2^{-1}) \in im(f)$

3° 由 f 为双射知，f^{-1} 也为双射

只需再证 f^{-1} 为群同态

$\forall g^{'}, h^{'} \in G_2, \exists! g, h \in G_1, s.t. f(g) = g^{'}, f(h) = h^{'}$

f 为群同态 $\Rightarrow f(gh) = f(g)f(h)$

$\Rightarrow gh = f^{-1}(f(g)f(h))$

$LHS = gh = f^{-1}(g^{'})f^{-1}(h^{'})$

$RHS = f^{-1}(f(g)f(h)) = f^{-1}(g^{'}h^{'})$

PROPERTY: 若 φ 为群同态, 则 φ 为单射 $\Leftrightarrow Ker(\varphi) = \{1\}$

1.2.2 环同态与环同构

定义: 设 $(R_1, +, \cdot), (R_2, \oplus, \otimes)$ 为两环,$\varphi : R_1 \to R_2$ 为映射

1° 若对 $\forall a, b \in R_1$, 有 $\begin{cases} \varphi(a+b) = \varphi(a) \oplus \varphi(b) \\ \varphi(ab) = \varphi(a) \otimes \varphi(b) \\ \varphi(1_{R1}) = 1_{R2} \end{cases}$

则称 φ 为环同态

2° 若 $\varphi : R_1 \to R_2$ 为环同态且 φ 为双射，则称 φ 为环同构

环同态的性质:

设 $f : R_1 \to R_2$ 为环同态，则

1°$f(0_{R1}) = 0_{R2}, f(1_{R1}) = 1_{R2}$

2°$f(g) = -f(-g)$

3° 若 g 乘法可逆, 则 $f(g^{-1}) = (f(g))^{-1}$

4°$f : (R_1^{\times}, \cdot) \to (R_2^{\times}, \otimes)$ 为群同态

5°$im(f)$ 为 R_2 的子环

6° 若 R_2 为非零环，则 Ker(f) 不为 R_1 的子环

但 $Ker(f)$ 关于加、减、数乘都封闭 (理想)

pf: 仅证明 5,6

5° $1_{R2} = f(1_{R1}) \in im(f)$

$f(r_1) - f(r_2) = f(r_1 - r_2) \in im(f)$

$f(r_1)f(r_2) = f(r_1 r_2) \in im(f)$

6° 只需注意环中 $Ker(f) := \{a \in R \mid f(a) = 0\}$

从而 $f(1)=1, 1\notin Ker(f)\Rightarrow Ker(f)$ 不为子环

2 整除理论

2.1 整除的定义和性质

定义: 若 $a,b\in\mathbb{Z},\exists a=bc,c\in\mathbb{Z}$

则称 b 整除 a, 记为 $b\mid a$

b 为 a 的因子，a 为 b 的倍数

性质:

1° $b\mid a\Leftrightarrow bc\mid ac$

2° $a\mid b,b\mid c\Rightarrow a\mid c$(整除的传递性)

3° $a\mid b,a\mid c\Rightarrow a\mid bx+cy$(b 和 c 的线性组合)

4° $a\mid bc,gcd(a,b)=1\Rightarrow a\mid c$

pf:$gcd(a.b)=1\Leftrightarrow\exists x,y\in\mathbb{R},ax+by=1$

$\Rightarrow axc+byc=c,bc=ka\Rightarrow a(xc+ky)=c\Rightarrow a\mid c$

2.2 最大公因数与最小公倍数

2.2.1 最大公因数

称集合 $\{d\in\mathbb{Z}|d\mid a,d\mid b\}$ 的最大元为 a 与 b 的最大公因子

记为 gcd(a,b) 或 (a,b)

换句话说,d 为最大公因数 $\Leftrightarrow\begin{cases}d\mid a,d\mid b\\ \forall d',d'\mid a,d'\mid b,d'\leqslant d\end{cases}$

• 称 a 与 b 互素, 若 gcd(a,b)=1

性质:

1° $gcd(a,a)=gcd(a,0)=|a|$

2° $gcd(a+by,b)=gcd(a,b+ax)$

pf: $\begin{cases}d\mid a\\ d\mid b\end{cases}\Longleftrightarrow\begin{cases}d\mid a+by(a=a+by-by)\\ d\mid b\end{cases}$

所以,$gcd(a,b)=max\{d\in\mathbb{Z}|d\mid a,d\mid b\}$

$=max\{d\in\mathbb{Z}|d\mid a+by,d\mid b\}$

$= gcd(a + by, b)$

3° $d \mid a, d \mid b \Rightarrow d \mid gcd(a, b)$

4° $m > 0 \Rightarrow m \cdot gcd(a, b) = gcd(ma, mb)$

pf:$m \cdot gcd(a, b) = m(ax + by) = (ma)x + (mb)y = gcd(ma, mb)$

5° $gcd(a, b) = d \Rightarrow gcd(\frac{a}{d}, \frac{b}{d}) = 1$

设 $gcd(a, b) = d$

由 4° 知 $d = d \cdot gcd(\frac{a}{d}, \frac{b}{d}) = gcd(a, b)$

$\Rightarrow gcd(\frac{a}{d}, \frac{b}{d}) = 1$

6° $gcd(a, m) = 1 = gcd(b, m) \Rightarrow gcd(ab, m) = 1$

$$\begin{cases} gcd(a, m) = 1 \Leftrightarrow ax_1 + my_1 = 1 \\ gcd(b, m) = 1 \Leftrightarrow bx_2 + my_2 = 1 \end{cases}$$

$1 = (ax_1 + my_1)(bx_2 + my_2) = ab(x_1x_2) + m(y_1bx_2 + y_2ax_1 + my_1y_2)$

$\Rightarrow gcd(ab, m) = 1$

2.2.2 带余除法

定理:$\forall a, b \in \mathbb{Z}, b \neq 0, \exists! q, r \in \mathbb{Z}, s.t. a = bq + r, (0 \leq r < b)$

pf: 存在性: 记 I:=$\{a - bk | k \in \mathbb{Z}\} \Rightarrow I \cap \mathbb{N}_+ \neq \varnothing \Rightarrow I \cap \mathbb{N}_+$ 有最小值 r

(即 r 为形如 a-bk 的最小非负整数)

$Claim : 0 \leq r < b$

(否则，$r' = r - |b| \in I \cap \mathbb{N}_+$ 且 $r\prime < r$, 与 r 为最小元矛盾！)

$\Rightarrow r = a - bq (a = bq + r)$ 符合要求

唯一性: 假设存在 $(q_1, r_1), (q_2, r_2), s.t. a = q_1b + r_1 = q_2b + r_2$

则 $|r_1 - r_2| = |b||q_1 - q_2|$

$Claim : q_1 = q_2$

否则，$b|r_1 - r_2$ 且 $r_1 - r_2 \neq 0$

因此,$|b| \leq |r_1 - r_2|$

但 $0 \leq r_1, r_2 < b$, 矛盾！

所以 $q_1 = q_2$ 进一步,$r_1 = r_2$

应用: 欧式算法

input:$a, b \in \mathbb{Z}$

output:$gcd(a, b)$、$x, y, s.t. gcd(a, b) = ax + by$

原理: 反复使用带余除法:$a = qb + r \Rightarrow gcd(a, b) = gcd(b, r)$

$r_n = gcd(a, b) = a \cdot x_n + b \cdot y_n$

quotient	remainder	x	y
	r_{-1}	$x_{-1} = 1$	$y_{-1} = 0$
q_0	r_0	$x_0 = 0$	$y_0 = 1$
q_1	r_1	$x_1 = x_{-1} - q_0 x_0$	$y_1 = y_{-1} - q_0 y_0$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
q_{i+1}	r_{i+1}	$x_{i+1} = x_{i-1} - q_i x_i$	$y_{i+1} = y_{i-1} - q_i y_i$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
q_n	r_n	$x_n = x_{n-2} - q_{n-1} x_{n-1}$	$y_n = y_{n-2} - q_{n-1} y_{n-1}$
	0		

例: 求 gcd(1517,481) 并将其表示为两数的线性组合

	1517	1	0
3	481	0	1
6	74	1	-3
2	37	-6	19
	0		

$37 = gcd(1517, 481) = (-6) \times 1517 + 19 \times 481$

2.2.3 贝祖等式

设 $a, b \in \mathbb{Z}$ 且不全为 0，则

$1^\circ \exists x, y \in \mathbb{Z} s.t. gcd(a, b) = ax + by$

2° 若 $d > 0$ 为 a,b 的公因子且 $\exists x, y \in \mathbb{Z}, s.t. d = ax + by$ 则 $d = gcd(a, b)$

pf:1° 记 $I_+ := \{ax + by > 0 | x, y \in \mathbb{Z}\} \neq \varnothing$

从而 I_+ 中有最小元，记作 d，设 d=ax+by

$Claim : d = gcd(a, b)$

从整除的角度，要证明两个数相等，只需证明他们相互整除即可

一方面，显然 $gcd(a, b) \mid d$

另一方面，需证明 $d \mid a, d \mid b$

由带余除法，$a = qd + r (0 \leq r < d)$

$\Rightarrow a = q(ax + by) + r$

$\Rightarrow r = a(1-qx) + b(-qy)$

$\Rightarrow r = 0$ 否则，$r \in I_+$ 且 $r < d$ 与 d 为最小元矛盾!

所以,$a = qd \Rightarrow d \mid a$, 同理,$d \mid b$

所以,$d \mid gcd(a,b) \Rightarrow gcd(a,b) = ax + by$

pf:2° 由上面已证，设 $d = gcd(a,b) = ax + by$

$\forall d^{'}, d^{'} \mid a, d^{'} \mid b \Rightarrow d^{'} \mid ax + by = d \Rightarrow |d^{'}| \leqslant d$

则任意 a,b 的公因子小于等于 $d = gcd(a,b) = ax + by$，则 $d = gcd(a,b)$

2.2.4 最小公倍数

称 m 为 a,b 的最小公倍数，若

$1°m > 0, a \mid m, b \mid m$

$2°$ 设 $m^{'}$ 为 a,b 公倍数，则 $m \leq |m^{'}|$

性质:

$1°$ $a \mid m, b \mid m \Leftrightarrow lcm(a,b) \mid m$

pf: 设 $|m| = q \cdot lcm(a,b) + r(0 \leq r < lcm(a,b))$

$r = |m| - q \cdot lcm(a,b) \Rightarrow \begin{cases} a \mid r \\ b \mid r \end{cases} \Rightarrow r = 0$

否则，$lcm(a,b) \leq r$，矛盾!

$\Rightarrow lcm(a,b) \mid m$

$2°$ $lcm(ma,mb) = |m| lcm(a,b)$

pf: 证明二者相互整除即可

一方面

$\begin{cases} ma \mid m \cdot lcm(a,b) \\ mb \mid m \cdot lcm(a,b) \end{cases} \Rightarrow lcm(ma,mb) \mid m \cdot lcm(a,b)$

另一方面

$\begin{cases} ma \mid lcm(ma,mb) \Rightarrow a \mid \dfrac{lcm(ma,mb)}{m} \\ mb \mid lcm(ma,mb) \Rightarrow b \mid \dfrac{lcm(ma,mb)}{m} \end{cases} \Rightarrow lcm(a,b) \mid \frac{lcm(ma,mb)}{m}$

所以 $m \cdot lcm(a,b) \mid lcm(ma,mb)$

$3°$ $gcd(a,b) \cdot lcm(a,b) = |ab|$

特别地，若 $gcd(a,b) = 1 \Rightarrow lcm(a,b) = ab$

pf: 记 $d = gcd(a,b)$

一方面 $\begin{cases} a \mid a \cdot \dfrac{b}{d} \\ b \mid b \cdot \dfrac{a}{d} \end{cases} \Rightarrow lcm(a,b) \mid \frac{ab}{d} \Rightarrow d \cdot lcm(a,b) \mid ab$

另一方面，设 $d = gcd(a,b) = ax + by$

$\begin{cases} ab \mid a \cdot lcm(a,b) \\ ab \mid b \cdot lcm(a,b) \end{cases} \Rightarrow ab \mid (ax+by)lcm(a,b) = d \cdot lcm(a,b)$

所以，$gcd(a,b) \cdot lcm(a,b) = |ab|$

可归纳地定义:$lcm(a_1, \cdots, a_n) := lcm(lcm(a_1, \cdots, a_{n-1}), a_n)$

推广:$\forall i = 1, \cdots, n$ 有 $a_i \mid b \Leftrightarrow lcm(a_1, \cdots, a_n) \mid b$

2.3 理想

2.3.1 理想的定义与性质

定义: 设 R 为环，$I \neq \varnothing \subseteq R$，若 I 满足：

1° $\forall a, b \in I, a - b \in I$(减法封闭)

2° $\forall a \in I, \forall r \in R, ra = ar \in I$(数乘封闭)

则称 I 为 R 的一个理想，记为 $I \lhd R$

注意：$(I, +)$ 形成 $(R, +)$ 的子群

PROPERTIES: 设 I_1, I_2 为环 R 的理想，则

$I_1 + I_2 := \{r_1 + r_2 | r_1 \in I_1, r_2 \in I_2\}$

$I_1 \cap I_2 := \{r \in R | r \in I_1, r \in I_2\}$

$I_1 \cdot I_2 := \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I_1, b_i \in I_2\}$

均为 R 的理想

pf: 仅证明 $I_1 \cdot I_2$ 为环 R 的理想

一方面，先证明关于加法构成子群，即证明关于减法封闭

$\forall a_1b_1 + \cdots + a_mb_m, c_1d_1 + \cdots + c_nd_n \in I \cdot J$

$(a_1b_1 + \cdots + a_mb_m) - (c_1d_1 + \cdots + c_nd_n)$

$= a_1b_1 + \cdots + a_mb_m + (-c_1)d_1 + \cdots + (-c_n)d_n \in I \cdot J$

另一方面，需证明对数乘封闭

$\forall a_i \in I, r \in R, ra_i \in I$

所以,$r(a_1b_1 + \cdots + a_mb_m) = (ra_1)b_1 + \cdots + (ra_m)b_m$

3° 设 R 为交换环，$a_1, \cdots, a_n \in R$，则

1)$(a) := aR := \{ar|r \in R\}$
为包含 a 的最小理想, 称为由 a 生成的主理想
2)$(a_1, \cdots, a_n) = \{a_1r_1 + \cdots + a_nr_n|r_1, \cdots, r_n \in R\}$
为包含 $a_1, \cdots, a_n$ 的最小理想，称为由 $a_1, \cdots, a_n$ 生成的主理想
pf: 只需证明 2)
一方面，证明 $(a_1, \cdots, a_n)$ 为环 R 的理想
$\forall x = a_1r_1 + \cdots + a_nr_n, y = a_1r_1^{'} + \cdots + a_nr_n^{'}, \forall r \in R$
• $x - y = a_1(r_1 - r_1^{'}) + \cdots + a_n(r_n - r_n^{'}) \in (a_1, \cdots, a_n)$
(因为 $r_i - r_i^{'} \in R$)
• $rx = r(a_1r_1 + \cdots + a_nr_n) = a_1(rr_1) + \cdots + a_n(rr_n) \in (a_1, \cdots, a_n)$
另一方面，证明 $(a_1, \cdots, a_n)$ 的最小性
任意 I 为 R 中理想，且 $a_1, \cdots, a_n \in I$
则对 $\forall r_1, \cdots, r_n \in R$, 有 $a_1r_1 + \cdots + a_nr_n \in I$
因此 $(a_1, \cdots, a_n) \subseteq I$，从而 $(a_1, \cdots, a_n)$ 是最小的
注: 设 R 为交换环,$a_1, \cdots, a_n \in R$
1° $aR = 0 \Leftrightarrow a = 0$
2° $aR = R \Leftrightarrow a$ 为 R 中乘法可逆元
3° $(a_1, \cdots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$
定理:1)$\forall d \in \mathbb{N} = \mathbb{Z}_{\geqslant 0}, d\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想
2) 任取 $\mathbb{Z}$ 的理想 I，存在 $d \in \mathbb{N}, s.t. I = d\mathbb{Z}$

$$\begin{aligned} \mathbb{N} &\xrightarrow{1:1} \{I|I \in \mathbb{Z}\} \\ d &\longmapsto d\mathbb{Z} \end{aligned}$$

pf:2) 若 I=0，则取 d=0(trivial)
若 $I \neq 0$，令 $I_+ := I \cap \mathbb{Z}_{\geqslant 0} \neq \varnothing$
取 $d = minI_+$，我们断言:$I = d\mathbb{Z}$(相互包含)
• $d\mathbb{Z} \subseteq I$ 显然
• $\forall n \in I$，由带余除法，$n = dq + r(0 \leqslant d < r)$
$\Rightarrow r = n - dq \in I$
$\Rightarrow r = 0$ 否则与 d 为最小元矛盾!$\Rightarrow n = dq \in d\mathbb{Z}$
所以，$I \subseteq d\mathbb{Z}$
注:$d\mathbb{Z}$ 有两个生成元:d,-d

2.3.2 用理想语言描述整除理论

引理:1)$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$

2)$a = \pm b \Leftrightarrow (a) = (b)$

3)a,b 互素 $(a, b) = \mathbb{Z}$ 或 $(a) + (b) = \mathbb{Z}$

整除 $\begin{cases} 1、(a) \subseteq (b) \overset{c\neq 0}{\Longleftrightarrow} (ac) \subseteq (bc) \\ 2、(c) \subseteq (b), (b) \subseteq (a) \Rightarrow (c) \subseteq (a) \\ 3、(b) \subseteq (a), (c) \subseteq (a) \Rightarrow (b) + (c) = (a) \end{cases}$

最大公因数与最小公倍数：

$a, b \in \mathbb{Z}$ 不全为零,d=gcd(a,b)，

则 $(1) d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \Leftrightarrow (d) = (a) + (b)$

$(2)(lcm(a, b)) = (a) \cap (b)$

即 $gcd(a, b)$ 为 $(a) + (b)$ 的生成元

$lcm(a, b)$ 为 $(a) \cap (b)$ 的生成元

pf:(1) 一方面,$d = gcd(a, b) = ax + by \in (a) + (b)$

$\Rightarrow (d) \subseteq (a) + (b)$

另一方面,$d \mid a, d \mid b \Rightarrow (a) \subseteq (d), (b) \subseteq (d)$

$(a) + (b) \subseteq (d)$

所以,$(d) = (a) + (b)$

$(2) \begin{cases} a \mid n \\ b \mid n \end{cases} \Leftrightarrow lcm(a, b) \mid n \Leftrightarrow (a) \cap (b) = (lcm(a, b))$

• $((a) \cap (b))(a, b) = (a) \cdot (b)$

特别地若 a,b 互素，则 $(a) \cap (b) = (a) \cdot (b)$

推广:$(lcm(a_1, \cdots, a_n)) = (a_1) \cap \cdots \cap (a_n)$

2.4 算术基本定理

2.4.1 素数

素数:$p \in \mathbb{Z}_{\geq 2}$, 若 p 的正因子只有 1 和 p，则称 p 为素数 (prime)

反之则为合数

素数的性质:

1° $gcd(p,a)=\begin{cases}1 & p\nmid a\\ p & p\mid a\end{cases}$

2° $n\in\mathbb{Z}_{\geq 2}\Rightarrow n$ 有素因子

pf: 记 $I_+:=\{d\geqslant 2|d\mid n\}\neq\varnothing(n\in I_+)$

即 p 为 I_+ 中的最小元，Claim:p 为素数

设 d 为 p 的正因子且不为 1，则只需证 d=p

因为 $d\mid p\mid n\Rightarrow d\in I_+\Rightarrow p\leqslant d\Rightarrow d=p$

• 欧几里得引理:p 为素数,$p\mid ab\Rightarrow p\mid a$ 或 $p\mid b$

$\begin{cases}\text{不妨设 } p\nmid a\Rightarrow gcd(p,a)=1\\ p\mid ab\Rightarrow gcd(p,ab)=p\end{cases}\Leftrightarrow gcd(p,b)\overset{gcd(p,a)=1}{=}gcd(p,ab)=p$

推论:$p\mid a_1\cdots a_n\Rightarrow\exists i\in\{1,2,\cdots,n\},s.t.p\mid a_i$

• 欧几里得定理: 素数有无穷多个

pf: 假设有有限个素数 $\{p_1,\cdots,p_n\}$

考虑 $N=p_1p_2\cdots p_n+1$, 依据假设,N 是合数

$\Rightarrow\exists p_i\mid N$, 又有 $p_i\mid p_1p_2\cdots p_n$

$\Rightarrow p\mid N-p_1p_2\cdots p_n=1$，矛盾!

2.4.2 算术基本定理

$\forall n\in\mathbb{Z}_{\geq 2}$

1)$\exists$ 素数 $p_1,p_2,\cdots,p_r,s.t.n=p_1p_2\cdots p_r$

2) 不计次序下，表达唯一

pf:1) 存在性: 对 n 归纳

n=2 或素数，显然

n 为合数，设 n=ab，将 a,b 的分解乘在一起即可

2) 唯一性:n=2 显然, 对 n 归纳, 设 n<k 时表达均唯一

设 $n=p_1p_2\cdots p_n=q_1q_2\cdots q_m$

则 $p_i\mid n\Rightarrow\exists q_j,s.t.p_i\mid q_j$

因为 p_i,q_j 均为素数 $\Rightarrow p_i=q_j$

等式两边同时消去 p_i

$\Rightarrow p_1\cdots p_{i-1}p_{i+1}\cdots p_n=q_1\cdots q_{j-1}q_{j+1}\cdots q_m$

由归纳假设知，$q_1\cdots q_{j-1}q_{j+1}\cdots q_m$ 是 $p_1\cdots p_{i-1}p_{i+1}\cdots p_n$ 的一个排列

所以 $q_1q_2\cdots q_m$ 是 $p_1p_2\cdots p_n$ 的一个排列，故表达唯一

另一形式:$n=p_1^{\alpha 1}p_2^{\alpha 2}\cdots p_n^{\alpha n}$

$\forall n\in\mathbb{Z}\setminus\{0\},n=sgn(n)\cdot\prod\limits_{p\ prime}p_i^{v_{p_i}(n)}$

$1)sgn(a)=\frac{a}{|a|}$

$2)v_p(a)\in\mathbb{Z}_{\geqslant 0}$ 且 p 素数足够大时，$v_p(a)=0$

$3)p\mid n\Rightarrow v_p(n)>0$

应用:$1)n\in\mathbb{Z}_{\geq 0},d=sgn(d)\cdot\prod\limits_{p\ prime}p_i^{v_{p_i}(d)}$

$d\mid n\Leftrightarrow v_p(d)\leq v_p(n),\forall p$

$2)gcd(a,b)=\prod\limits_{p\ prime}p^{min\{v_p(a),v_p(b)\}}$

pf: 要证明两个数相等，只需证两个数的所有因数相等

$$\forall d\mid gcd(a,b)\Leftrightarrow\begin{cases}d\mid a\Leftrightarrow\forall p,v_p(d)\leqslant v_p(a)\\ d\mid b\Leftrightarrow\forall p,v_p(d)\leqslant v_p(b)\end{cases}\Leftrightarrow\forall p,v_p(d)\leqslant min\{v_p(a),v_p(b)\}$$

$d\mid\prod\limits_{p\ prime}p^{min\{v_p(a),v_p(b)\}}$, 即得证

$lcm(a,b)=\prod\limits_{p\ prime}p^{max\{v_p(a),v_p(b)\}}$

pf: 思路同上，只需证明 $\forall m,lcm(a,b)\mid m$ 有 $\prod\limits_{p\ prime}p^{max\{v_p(a),v_p(b)\}}\mid m$

$$\forall m,lcm(a,b)\mid m\Leftrightarrow\begin{cases}a\mid m\Leftrightarrow\forall p,v_p(a)\leqslant v_p(m)\\ b\mid m\Leftrightarrow\forall p,v_p(b)\leqslant v_p(m)\end{cases}$$

$\Leftrightarrow\forall p,max\{v_p(a),v_p(b)\}\leqslant v_p(m)\Leftrightarrow\prod\limits_{p\ prime}p^{max\{v_p(a),v_p(b)\}}\mid m$

• 推广到有理数,$n=\frac{\alpha}{\beta},(\alpha,\beta)=1$

$n\overset{!}{=}sgn(n)\prod\limits_{p\ prime}p^{v_p(n)}$

$v_p(n)=v_p(a)-v_p(b)$

$a=\prod\limits_{v_{p_i}(n)\geq 0}p_i^{v_{p_i}(n)},b=\prod\limits_{v_{p_i}(n)<0}p_i^{-v_{p_i}(n)}$

• 实际上 v_p 是一个群同态

$$v_p:(Q^\times,\cdot)\longrightarrow(\mathbb{Z},+)$$
$$a\longmapsto v_p(a)$$

$v_p(ab)=v_p(a)+v_p(b)$

3 同余理论

3.1 同余

3.1.1 同余的概念与性质

$m \in \mathbb{N}_+$, 若 $m \mid a-b$, 则称 a 与 b 模 m 同余, 记作 $a \equiv b(modm)$

PROPERTIES:

1) $\begin{cases} a \equiv b(modm) \\ c \equiv d(modm) \end{cases} \Leftrightarrow \begin{cases} a \pm c \equiv b \pm d(modm) \\ ac \equiv bd(modm) \end{cases}$

pf: 仅证明乘法

$\begin{cases} a \equiv b(modm) \Leftrightarrow m \mid a-b \\ c \equiv d(modm) \Leftrightarrow m \mid c-d \end{cases} \Leftrightarrow m \mid (a-b)c + (c-d)b = ac - bd$

2) 若 $\forall i \in \{1, \cdots, n\}, a_i \equiv b_i(modm)$, 则对任意整系数多项式

我们有 $f(a_1, \cdots, a_n) \equiv f(b_1, \cdots, b_n)(modm)$

3) $\begin{cases} a \equiv b(modm) \\ d \mid m \end{cases} \Leftrightarrow a \equiv b(modd)$

4)$a \equiv b(modm) \overset{d \neq 0}{\Longleftrightarrow} da \equiv db(moddm)$

5)$a \equiv b(modm_i), i = 1, \cdots, n \Leftrightarrow a \equiv b(mod(lcm(m_1, \cdots, m_n)))$

pf:($\Leftarrow$)$a \equiv b(mod(lcm(m_1, \cdots, m_n))) \overset{m_i \mid (lcm(m_1, \cdots, m_n))}{\Longrightarrow} a \equiv b(modm_i)$

$\Rightarrow a \equiv b(modm_i)(\forall i) \Rightarrow m_i \mid a-b(\forall i)$

$\Rightarrow lcm(m_1, \cdots, m_n) \mid a-b \Rightarrow a \equiv b(mod(lcm(m_1, \cdots, m_n)))$

6)$ac \equiv bc(modm) \Rightarrow a \equiv b(mod\frac{m}{gcd(m,c)})$

特别地, 若 m 与 c 互素, 则 $ac \equiv bc(modm) \Rightarrow a \equiv b(modm)$

pf:$ac \equiv bc(modm) \Rightarrow m \mid c(a-b) \Rightarrow \frac{m}{gcd(m,c)} \mid \frac{c}{gcd(m,c)}(a-b)$

因为 $gcd(\frac{m}{gcd(m,c)}, \frac{c}{gcd(m,c)}) = 1$

所以 $\frac{m}{gcd(m,c)} \mid (a-b) \Rightarrow a \equiv b(mod\frac{m}{gcd(m,c)})$

例: 一个数字模 9 等于各个数位上数字之和

3.1.2 同余方程

• 同余类的定义:$\forall r \in \mathbb{Z}$，称 $\mathbb{Z}$ 的子集

$[r] := r + m\mathbb{Z} := \{\cdots, r-2m, r-m, r, r+m, r+2m, \cdots\}$

即 $[r] = \{r + km | k \in \mathbb{Z}\}$

为 r 所在的模 m 的同余类, 也记作 $\bar{r}$, 称 r 为 [r] 的一个代表

注:1.$a \equiv b(modm) \Leftrightarrow [a] = [b]$

2.$a \not\equiv b(modm) \Leftrightarrow [a] \cap [b] = \varnothing$

3.$\mathbb{Z} = \bigsqcup_{i=0}^{m-1} [i]$

• 同余方程

定理:$ax \equiv b(modm)$ 有解 $\Leftrightarrow gcd(a,m) \mid b$ 且此时，解集为模 $\frac{m}{gcd(a,m)}$ 的一个同余类, 也为 gcd(a,m) 个模 m 的同余类的并

特别地 $ax \equiv 1(modm)$ 有解 $\Leftrightarrow gcd(a,m) = 1$

pf: 有解:$ax \equiv b(modm) \Leftrightarrow m \mid ax - b \Leftrightarrow ax - b = my$

$\Leftrightarrow b = ax + my \overset{Bezout}{\Leftrightarrow} gcd(a,m) \mid b$

解集的形式: 不放设 x_0 为一个解 $ax_0 \equiv b(modm)$

若 x 也为解:$a(x - x_0) \equiv 0(modm) \Leftrightarrow m \mid a(x - x_0)$

$\overset{d=gcd(a,m)}{\Longleftrightarrow} \frac{m}{d} \mid \frac{a}{d}(x - x_0) \overset{gcd(\frac{m}{d}, \frac{a}{d})=1}{\Longleftrightarrow} \frac{m}{d} \mid (x - x_0)$

$\Longleftrightarrow x \equiv x_0(mod \frac{m}{gcd(m,a)})$

例:$15x \equiv 9(mod 21)$

解: 先验证是否有解,$gcd(15,21) = 3 \mid 9$

原同余方程可先同除 $3 \Rightarrow 5x \equiv 3(mod 7)$

解:$gcd(5,7) = 1 = 3 \times 5 + 7 \times (-2)$

即 5 在模 7 下的逆元为 3

$3 \cdot 5x \equiv 3 \cdot 3(mod 7)$

$x \equiv 9 \equiv 2(mod 7)$

3.1.3 中国剩余定理与解同余方程组

设 $m = m_1 m_2 \cdots m_n$, 其中 $m_1, \cdots, m_n$ 两两互素,$a_1, \cdots, a_n \in \mathbb{Z}$

则方程组 $\begin{cases} x \equiv a_1 mod m_1 \\ x \equiv a_2 mod m_2 \\ \quad \cdots \\ x \equiv a_n mod m_n \end{cases}$

有解, 且解集为模 m 的一个同余类

pf:(1) 记 $\widehat{m_i} = m_1 \cdots m_{i-1} m_{i+1} \cdots m_n$ 则 $gcd(m_i, \widehat{m_i}) = 1$

$\Rightarrow \exists x_i, y_i \in \mathbb{Z}, s.t. x_i\widehat{m_i} + y_i m_i = 1$

所以,$x_i\widehat{m_i} \equiv 1(modm_i)$

同时, 有 $x_i\widehat{m_i} \equiv 0(modm_j)(j \neq i)$

所以对于 $x_i\widehat{m_i}$, 有 $\begin{cases} x_i\widehat{m_i} \equiv 0(modm_1) \\ x_i\widehat{m_i} \equiv 0(modm_2) \\ \quad \cdots \\ x_i\widehat{m_i} \equiv 1(modm_i) \\ \quad \cdots \\ x_i\widehat{m_i} \equiv 0(modm_{n-1}) \\ x_i\widehat{m_i} \equiv 0(modm_n) \end{cases}$

记 $x_0 = \sum_{i=1}^{n} a_i x_i \widehat{m_i}$

所以,$x_0 \equiv a_i x_i \widehat{m_i} \equiv a_i(modm_i)$

(2) 解是模 m 的一个同余类

x 为方程组的解 $\Leftrightarrow x \equiv x_0(modm_i), \forall i \Leftrightarrow m_i \mid x - x_0$

$\Leftrightarrow lcm(m_1, \cdots, m_n) = m \mid x - x_0$

$x \equiv x_0(modm)$

例: 解同余方程组 $\begin{cases} x \equiv 3mod14 \\ x \equiv 13mod15 \\ x \equiv 7mod11 \end{cases}$

Step1: $\widehat{m_1} = 15 \times 11 = 165 \quad m_1 = 14 \quad 1 = 165 \times (-5) + 14 \times (59)$

$\widehat{m_2} = 14 \times 11 = 154 \quad m_2 = 15 \quad 1 = 154 \times 4 + 15 \times (-41)$

$\widehat{m_3} = 14 \times 15 = 210 \quad m_3 = 11 \quad 1 = 210 \times 1 + 11 \times (19)$

Step2: $x_0 = 3 \times (-5) \times 165 + 13 \times 4 \times 154 + 7 \times 1 \times 210 = 7003$

所以 $x \equiv 7003(mod15 \times 14 \times 11)$

即 $x \equiv 73(mod2310)$

• 思考: 若上述同余方程组 $m_1, \cdots, m_n$ 不两两互素, 该怎么解?

先考虑只有两个方程时:

引理: $\begin{cases} x \equiv a_1 modm_1 \\ x \equiv a_2 modm_2 \end{cases} \cdots\cdots (*)$

记 $d = gcd(m_1, m_2)$

1) 方程组 $(*)$ 有解 $\Leftrightarrow d \mid a_1 - a_2$

2) 若 $d \mid a_1 - a_2$, 则 $x \equiv rm_1s_1 + a_1(modlcm(m_1, m_2))$

其中,$r = \frac{a_2-a_1}{d}$, $m_1s_1 + m_2s_2 = d$(贝祖定理)

pf:1)$(\Rightarrow)$ 设 $x = x_0$ 为一个解, 记 $d = gcd(m_1, m_2)$

$$\begin{cases} x_0 \equiv a_1 mod m_1 \\ x_0 \equiv a_2 mod m_2 \end{cases} \Longrightarrow \begin{cases} x_0 \equiv a_1 mod d \\ x_0 \equiv a_2 mod d \end{cases} \Rightarrow d \mid a_1 - a_2$$

1)$(\Leftarrow)$2)$x_0 = rm_1s_1 + a_1$

$x_0 \equiv a_1(modm_1)$

$x_0 = r(d - m_2s_2) + a_1 \equiv rd + a_1 \equiv a_2(modm_2)$

还需证明所有解均落在上述同余类中

设 $x = x_1$ 为另一解

$$\begin{cases} x_1 \equiv a_1 mod m_1 \\ x_2 \equiv a_2 mod m_2 \end{cases} \Leftrightarrow \begin{cases} x_1 - x_0 \equiv 0 mod m_1 \\ x_2 - x_0 \equiv 0 mod m_2 \end{cases} \Leftrightarrow \begin{cases} m_1 \mid x_1 - x_0 \\ m_2 \mid x_1 - x_0 \end{cases}$$

$\Leftrightarrow lcm(m_1, m_2) \mid x_1 - x_0 \Leftrightarrow x_1 \equiv x_0 modlcm(m_1, m_2)$

• 若为多个方程, 先解其中两个, 坚持与努力

例: 解同余方程组 $\begin{cases} x \equiv 13 mod 15 \\ x \equiv 3 mod 35 \\ x \equiv 31 mod 42 \end{cases}$

先解前两个 $\begin{cases} x \equiv 13 mod 15 \\ x \equiv 3 mod 35 \end{cases}$

Step1: 验证可解性:$d_1 = gcd(15, 35) = 5, 5 \mid 13 - 3 = 10$

Step2: 算 r, m_1s_1

$r_1 = \frac{a_2-a_1}{d_1} = \frac{3-13}{5} = -2$

由欧式算法:$15 \times (-2) + 35 \times 1 = 5$

$m_1s_1 = -30$

所以 $x \equiv (-2)(-30) + 13(modlcm(15, 35))$

$x \equiv 73(mod 105)$

再解剩下两个 $\begin{cases} x \equiv 73 mod 105 \\ x \equiv 31 mod 42 \end{cases}$

Step1: 验证可解性:$d_2 = gcd(105, 42) = 21 \mid (73 - 31) = 42$

Step2: 算 r, m_1s_1

$r_2 = \frac{a_2 - a_1}{d_2} = \frac{31-73}{42} = -2$
由欧式算法:$105 \times 1 + 42 \times (-2) = 21$
$m_1 s_1 = 105$
$x \equiv (-2)(105) + 73(modlcm(105, 42))$
因此，上述同余方程组的解集为 $x \equiv 73(mod210)$

3.2 欧拉定理与费马小定理

• 欧拉函数 $\varphi : \mathbb{Z}_{\geqslant 1} \longrightarrow \mathbb{Z}_{\geqslant 1}$

$$m \longmapsto \#\{i \in \{0, 1, \cdots, m-1\} | gcd(i, m) = 1\}$$

如:$m = 1, \varphi(1) = \#\{0\} = 1$
$m = 2, \varphi(2) = \#\{1\} = 1$
$m = 6, \varphi(6) = \#\{1, 5\} = 2$
• 欧拉定理: 若 $gcd(a, m) = 1$ 则 $a^{\varphi(m)} \equiv 1(modm)$
pf: 考虑集合 $\Sigma := \{i | 0 \leq i < m, gcd(i, m) = 1\}$
对 $\forall i \in \Sigma, \exists! q_i, r_i, s.t. ai = mq_i + r_i \Rightarrow ai \equiv r_i(modm)$
另一方面
$gcd(ai, m) = 1 \Rightarrow gcd(r_i, m) = 1 \Rightarrow r_i \in \Sigma$
因此我们构造一个映射 $\chi : \Sigma \longrightarrow \Sigma$

$$i \longmapsto r_i$$

断言:χ 为双射
由于是自身映射，只需验证单射即可
若 $r_i = r_j \Rightarrow ai \equiv aj(modm) \Rightarrow i \equiv j(modm) \Rightarrow i = j$
于是,$\prod\limits_{i \in \Sigma} ai \equiv \prod\limits_{i \in \Sigma} r_i \equiv \prod\limits_{i \in \Sigma} i(modm)$
即 $a^{\varphi(m)} \equiv 1(modm)(\forall i, gcd(i, m) = 1)$
• 费马小定理: 若 p 为素数, 则对任意 $a \in \mathbb{Z}$, 有 $a^p \equiv a(modp)$
pf:$p \nmid a$: 由欧拉定理,$a^{p-1} \equiv 1(modp) \Rightarrow a^p \equiv a(modp)$
$p \mid a :\Rightarrow a^p \equiv 0 \equiv a(modp)$

3.3 同余的环论解释

3.3.1 环 $\mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z} := \{[0], [1], \cdots, [m-1]\}$

例:$\mathbb{Z}/2\mathbb{Z}$ =｛偶数集, 奇数集｝

在 $\mathbb{Z}/m\mathbb{Z}$ 上可以定义二元运算：

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

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

上述运算是良定义的

i.e. 若 $[a] = [a^{'}], [b] = [b^{'}]$ 则 $[a + b] = [a^{'} + b^{'}], [ab] = [a^{'}b^{'}]$

$$\begin{cases} [a] = [a^{'}] \Leftrightarrow a \equiv a^{'}(modm) \\ [b] = [b^{'}] \Leftrightarrow b \equiv b^{'}(modm) \end{cases} \Leftrightarrow \begin{cases} a + b \equiv a^{'} + b^{'}(modm) \\ ab \equiv a^{'}b^{'}modm) \end{cases}$$

$[a + b] = [a^{'} + b^{'}], [ab] + [a^{'}b^{'}]$

• $(\mathbb{Z}/m\mathbb{Z}, +)$ 构成 m 元交换环

• 单位群:$(\mathbb{Z}/m\mathbb{Z})^{\times} = \{[a] | gcd(a, m) = 1, 0 \leqslant a < m\}$

$\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^{\times}$

解同余方程组 $ax \equiv b(modm)$ 实际上是找 [a] 在 $(\mathbb{Z}/m\mathbb{Z})^{\times}$ 中的逆元

• p 为素数,$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ 为 p 元有限域

3.3.2 中国剩余定理的环论证明

• 为引入中国剩余定理的环论证明，我们考虑映射 φ

若 $d \mid m, \varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$

$$i + m\mathbb{Z} \longmapsto i + d\mathbb{Z}$$

先验证 φ 的良定性:

i.e. 若 $i + m\mathbb{Z} = i^{'} + m\mathbb{Z}$, 是否有 $i + d\mathbb{Z} = i^{'} + d\mathbb{Z}$

因为 $i + m\mathbb{Z} = i^{'} + m\mathbb{Z} \Rightarrow m \mid i - i^{'} \overset{d|m}{\Rightarrow} d \mid i - i^{'} \Leftrightarrow i + d\mathbb{Z} = i^{'} + d\mathbb{Z}$

• 性质:φ 为环同态

pf: 单位元:$\varphi(1 + m\mathbb{Z}) = 1 + d\mathbb{Z}$

加法保持群结构:$\varphi((i + m\mathbb{Z}) + (j + m\mathbb{Z})) = i + j + d\mathbb{Z}$

$\varphi(i + m\mathbb{Z}) + \varphi(j + m\mathbb{Z}) = i + d\mathbb{Z} + j + d\mathbb{Z} = i + j + d\mathbb{Z}$

所以加法保持群结构, 同理验证乘法保持群结构即可

• 为引入中国剩余定理的环论证明，我们引入环的笛卡尔积

$R_1, R_2, \cdots, R_n$ 为环

$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) | r_i \in R_i\}$

$+ : (r_1, r_2, \cdots, r_n) + (r_1^{'}, r_2^{'}, \cdots, r_n^{'}) = (r_1 + r_1^{'}, r_2 + r_2^{'}, \cdots r_n + r_n^{'})$

$\cdot : (r_1, r_2, \cdots, r_n) \cdot (r_1^{'}, r_2^{'}, \cdots, r_n^{'}) = (r_1 r_1^{'}, r_2 r_2^{'}, \cdots r_n r_n^{'})$

• 中国剩余定理 (环论证明)

若 $m_1, m_2, \cdots, m_n$ 两两互素, 记 $m = m_1 m_2 \cdots m_n$

则 $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cdots \mathbb{Z}/m_n\mathbb{Z}$

$\quad i + m\mathbb{Z} \longmapsto (i + m_1\mathbb{Z}, \cdots, i + m_n\mathbb{Z})$

Claim:φ 是环同构

pf:1).$\varphi(1 + m\mathbb{Z}) = (1 + m_1\mathbb{Z}, \cdots, 1 + m_n\mathbb{Z})$

2). 加法保持群结构, 乘法保持群结构同上可证

3) 双射: 因为 $\#\mathbb{Z}/m\mathbb{Z} = m = m_1 \cdots m_n = \#(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z})$

只需证明 φ 是单射即可

若 $\varphi(i + m\mathbb{Z}) = \varphi(j + m\mathbb{Z})$

$\Rightarrow \forall k, i + m_k\mathbb{Z} = j + m_k\mathbb{Z} \Rightarrow \forall k, m_k \mid i - j \Rightarrow gcd(m_1, m_2, \cdots, m_n) \mid i - j$

即 $m \mid i - j \Rightarrow i + m\mathbb{Z} = j + m\mathbb{Z}$

综上,φ 为环同构

对于同余方程组 $\begin{cases} x \equiv a_1 mod m_1 \\ x \equiv a_2 mod m_2 \\ \quad \cdots \\ x \equiv a_n mod m_n \end{cases}$

由环同构可知每一组 $a_1, a_2, \cdots, a_n$ 都对应一个 x

解集的形式为模 m 的一个同余类

• 中国剩余定理在含幺交换环上的推广:

若 $I = I_1 I_2 \cdots I_n, I_1, \cdots, I_n$ 两两互素

则 $R/I \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$

• 由 $\varphi : R_1 \to R_2$ 为环同态可知,$\varphi : R_1^{\times} \to R_2^{\times}$ 为群同构 (乘法)

则根据 $(\mathbb{Z}/m\mathbb{Z})^{\times} \cong (\mathbb{Z}/m_1\mathbb{Z})^{\times} \times (\mathbb{Z}/m_2\mathbb{Z})^{\times} \cdots (\mathbb{Z}/m_n\mathbb{Z})^{\times}$

有两边集合元素个数相等

因此我们得到欧拉函数的重要性质:

若 $m_1, m_2, \cdots, m_n$ 两两互素,$m = m_1 m_2 \cdots m_n$, 则
$\varphi(m) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_n)$
另一形式:$m = p_1^{\alpha 1} p_2^{\alpha 2} \cdots p_n^{\alpha n}$
$\varphi(m) = \varphi(p_1^{\alpha 1})\varphi(p_2^{\alpha 2})\cdots\varphi(p_n^{\alpha n})$
其中,$\varphi(p_i^{\alpha i}) = p_i^{(\alpha i - 1)}(p_i - 1)$
例:$\varphi(100) = \varphi(2^2)\varphi(5^2) = 2^1(2-1)5^1(5-1) = 40$
例: 求 2^{81} 的最后两位数
即求 $x \equiv 2^{81}(mod 100)$
$$\Leftrightarrow \begin{cases} x \equiv 2^{81}(mod 4) \\ x \equiv 2^{81}(mod 25) \end{cases}$$
对同余方程组进一步处理:$x \equiv 2^{81} \equiv 0(mod 4)$
由欧拉定理,$2^{\varphi(25)} = 2^{20} \equiv 1(mod 25)$
所以 $2^{81} \equiv 2^{20^4} \cdot 2 \equiv 2(mod 25)$
$$\Leftrightarrow \begin{cases} x \equiv 0(mod 4) \\ x \equiv 2(mod 25) \end{cases}$$
由中国剩余定理或瞪眼法知,$x \equiv 52(mod 100)$

4 群论基础

4.1 循环群

4.1.1 幂次与倍数

幂次：考虑群 $(G, \cdot), g \in G$
$$g^n = \begin{cases} g \cdots g(n个g) & n > 0 \\ 1 & n = 0 \\ g^{-1} \cdots g^{-1}(-n个g) & n < 0 \end{cases}$$
倍数：考虑群 $(A, +), a \in A$
$$na(数乘) = \begin{cases} a + \cdots a(n个g) & n > 0 \\ 0_A & n = 0 \\ (-a) + \cdots (-a)(-n个g) & n < 0 \end{cases}$$
Prop：1)$g^m \cdot g^n = g^{m+n}, g^{mn} = (g^m)^n$

2)$g^m = 1_G = g^n \Leftrightarrow g^{gcd(m,n)} = 1_G$

4.1.2 最小生成子群

Def: 设 $(G, \cdot)$ 为群，$g \in G$，则 $< g >:= \{g^k | k \in \mathbb{Z}\}$ 为 G 中包含 g 的最小的子群，称为由 g 生成的子群。

proof：$g^k \cdot (g^l)^{-1} = g^{k-l} \in < g > \Rightarrow g$ 为子群

$g \in < g >$，这是显然的

若 $g \in H \leqslant G$，则 $g^k \in H(\forall k > 0) \Rightarrow g^k = (g^{-k})^{-1} \in H, \forall k < 0$

$\Rightarrow < g > \subseteq H \Rightarrow < g >$ 最小

Def：设 $(G, \cdot)$ 为群，$g \in G, S \subseteq G$，称包含 S 的最小子群为由 S 生成的子群，记为 $< S >$，若 $S = \{x_1, x_2 \cdots, x_n\}$，则记 $< S >=< \{x_1, x_2 \cdots, x_n\} >$

例: 在 $\mathbb{Z}$ 中，$< m_1, \cdots, m_n >=< gcd(m_1, \cdots m_n) >$，特别地，$< m, n >=< gcd(m, n) >$

proof：$\subseteq$: $m = \frac{m}{gcd(m,n)} \cdot gcd(m, n) \in < gcd(m, n) >$

n 同理，所以 $< m, n > \subseteq < gcd(m, n) >$

$\supseteq$: $gcd(m, n) = ms + nt \in < m, n > \Rightarrow < gcd(m, n) > \subseteq < m, n >$

4.1.3 阶

Def:$g \in G$，若存在 $n \in \mathbb{N}_+$ 使得 $g^n = 1$，则称满足 $g^n = 1$ 的最小整数 n 为 g 的阶 (order)，记作 $ord(g)$ 或 $o(g)$，若上述 n 不存在，则称 g 的阶为无限，记作 $ord(g) = \infty$ 或 $o(g) = \infty$，若 $o(g) = 1$，则 $g = 1_G$。

注：在证明有关阶的问题时，需考虑阶有限还是无限

Property:1) 若 $ord(g) = k < \infty$，则 $a) g^n = 1 \Leftrightarrow n \equiv 0(mod k)$

$b) g^i = g^j \Leftrightarrow i \equiv j(mod k)$

$c) < g >= \{1, g, \cdots, g^{k-1}\}$

2) 若 $ord(g) = \infty$，则 $\forall i \neq j$，均有 $g^i \neq g^j$

3) $ord(g) = \# < g >$

proof:$a) : \forall n = kq + r(0 \leqslant r < k)$，$g^n = 1 \Leftrightarrow g^r = 1(0 \leqslant r < k)$

$\overset{ord(g)=k}{\Leftrightarrow} r = 0 \Leftrightarrow k \mid n$

$b) : g^i = g^j \Leftrightarrow g^{i-j} = 1 \Leftrightarrow k \mid i - j$

$c) : \forall g^m \in < g >, m = kq_m + r_m(0 \leqslant r_m < k)$

$g^m = g^{kq_m + r_m} = (g^k)^{q_m} \cdot g^{r_m} = g^{r_m} \in \{1, g, \cdots, g^{k-1}\}$

2): 反证，若 $i \neq j$ 且 $i \neq j$，不妨设 $j > i$，则 $\Leftrightarrow g^{i-j} = 1 \Rightarrow ord(g) \neq \infty$，矛盾！

3): 由 1), 2) 立得

4.1.4 循环群

设 G 为群

1) 若 $S \subseteq G$ 满足 $G =< S >$，则称 G 由 S 生成

2) 若存在有限子集 $S \subseteq G$，使得 $G =< S >$，则称 G 为有限生成群 (finitely generated group)

3) 若存在 $g \in G$ 使得 $G =< g >$，则称 G 为循环群 (cyclic group)，称 g 为 G 的一个生成元 (generator)

例：$(\mathbb{Z}, +)$ 和 $(\mathbb{Z}/n\mathbb{Z}, +)$ 都是循环群，$(\mathbb{Z}/8\mathbb{Z})^\times$ 不是循环群，但可由两个元素生成，即 $(\mathbb{Z}/8\mathbb{Z})^\times =< \bar{3}, \bar{5} >=< \bar{3}, \bar{7} >=< \bar{5}, \bar{7} >$

例：$(\mathbb{Q}, +)$ 不是有限生成群

proof: 假设 $(\mathbb{Q}, +)$ 是有限生成群，设 $(\mathbb{Q}, +) =< a_1, \cdots, a_n >, a_i = \frac{p_i}{q_i}$

$< a_1, \cdots, a_n > \subseteq < \frac{1}{q_1 \cdots q_n} > \neq \mathbb{Q}$

4.1.5 循环群结构定理

设 G 为循环群，则

1)$\#G = n \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$

2)$\#G = \infty \Rightarrow G \cong \mathbb{Z}$

proof: 设 $G =< g >$

1°$\#G = \infty$，定义 $\varphi : \mathbb{Z} \to G, k \mapsto g^k$，则 φ 为群同态

单射：$\varphi(i) = \varphi(j) \Leftrightarrow g^i = g^j \Leftrightarrow i = j$

满射：$\forall g^k \in G$，均有原像 $k \in \mathbb{Z}$

2°$\#G = n < \infty$，则 $G = \{1, g, \cdots, g^{n-1}\}$

定义 $\varphi : \mathbb{Z}/n\mathbb{Z} \to G, \bar{i} \mapsto g^i$

验证 φ 的良定义性：若 $\bar{i} = \bar{j}$，则 $n \mid i - j \Rightarrow g^{i-j} = 1_G \Rightarrow g^i = g^j$

验证 φ 保持群结构：即证明 $\varphi(\bar{i} + \bar{j}) = \varphi(\bar{i})\varphi(\bar{j})$

$LHS = g^{i+j} = g^i \cdot g^j = RHS$

验证双射：因为 $\#\mathbb{Z}/n\mathbb{Z} = \#G$，验证单射即可

若 $\varphi(\bar{I}) = \varphi(\bar{j}) \Rightarrow g^i = g^j \Rightarrow g^{i-j} = 1 \Rightarrow n \mid i - j \Rightarrow \bar{i} = \bar{j}$

4.1.6 循环群的生成元及其自同构群

设 $G=<g>$，则 1)$\#G=\infty \Rightarrow G$ 的生成元为 g 或 g^{-1}

2)$\#G=n<\infty \Rightarrow G$ 的生成元集合为 $\{g^k|0\leqslant k<n, gcd(k,n)=1\}$

3)$Aut(G)\cong \begin{cases}\mathbb{Z}/2\mathbb{Z} & \#G=\infty \\ (\mathbb{Z}/n\mathbb{Z})^\times & \#G=n<\infty\end{cases}$

注：$Aut(G)=\{\varphi: G\to G|\varphi$为群同构$\}$

proof:1)2): 设 $G=<g>$，任取一元素 $g^\alpha(\alpha\in\mathbb{Z})$

若 g^α 为生成元，则 $g\in G=<g^\alpha>=\{g^{\alpha k}|k\in\mathbb{Z}\}$

$\Rightarrow \exists\beta\in\mathbb{Z}, s.t. g=g^{\alpha\beta}$

1) 若 $G=\infty$，则 $1=\alpha\beta\Rightarrow\alpha=\pm1$

2) 若 $G=n<\infty$，由 $g^{\alpha\beta-1}=1\Rightarrow n\mid\alpha\beta-1\overset{s\in\mathbb{Z}}{\Rightarrow}\alpha\beta+ns=1\overset{贝祖}{\Rightarrow}gcd(\alpha,n)=1$

反之，$\forall 0\leqslant k<n, gcd(k,n)=1$，要验证 g^k 为生成元，只需验证 g^k 能生成 g 即可

$\Rightarrow\exists s,t, s.t. sk+tn=1\Rightarrow g=g^1=g^{sk+tn}=(g^k)^s\cdot(g^n)^t=(g^k))^s$

3)Step1: 设 $\varphi: G\to G$ 为自同构

$G=\{\varphi(g^k)|k\in\mathbb{Z}\}=\{(\varphi(g))^k|k\in\mathbb{Z}\}\Rightarrow\varphi(g)$ 为 G 的一个生成元，φ 由 $\varphi(g)$ 唯一决定，可构造如下映射：

$1^\circ\#G=\infty\quad \psi: Aut(G)\to\{\pm1\}=\mathbb{Z}^\times$

$\psi(\varphi)=\begin{cases}1 & \varphi(g)=g \\ -1 & \varphi(g)=-g\end{cases}$

$2^\circ\#G=n\quad \psi: Aut(G)\to(\mathbb{Z}/n\mathbb{Z})^\times$

$\varphi(g)=g^\alpha\Rightarrow\psi(\varphi)=\alpha(modn)$

Step2: 下面验证 ψ 为群同构

$1^\circ\#G=\infty$

由一个生成元对应一个自同构知，G 只有两个自同构：$\varphi_1(g)=g, \varphi_2(g)=g^{-1}$

不难验证 ψ 为群同构

$2^\circ\#G=n<\infty$

• 群同态：设 $\varphi_1(g)=g^\alpha, \varphi_2(g)=g^\beta, gcd(n,\alpha)=gcd(n,\beta)=1$，则 φ_1,φ_2 为群 G 的两个自同构

只需验证 $\psi(\varphi_1\circ\varphi_2)=\psi(\varphi_1)\psi(\varphi_2)$

因为 $\varphi_1\circ\varphi_2(g)=\varphi_1(g^\beta)=g^{\alpha\beta}, gcd(n,\alpha\beta)=1$，则 $g^{\alpha\beta}$ 唯一确定了群同构 $\varphi_1\circ\varphi_2$

则 $\psi(\varphi_1\circ\varphi_2)=\alpha\beta=\psi(\varphi_1)\psi(\varphi_2)$

• 单射：假设 $\psi(\varphi_1)=\psi(\varphi_2)$，则由自同构的唯一确定知，$\varphi_1=\varphi_2$

• 满射：$\forall\alpha\in(\mathbb{Z}/n\mathbb{Z})^\times\Rightarrow gcd(\alpha,n)=1\Rightarrow\varphi_\alpha:G\to G,g\mapsto g^\alpha$ 为自同构

例：1)$\mathbb{Z}/n\mathbb{Z}$ 的生成元 $\{1\leqslant\alpha<n|gcd(\alpha,n)=1\}$

2)μ_n 的生成元：$\{\zeta_n^\alpha|1\leqslant\alpha<n,gcd(\alpha,n)=1\}$

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

4.1.7 循环群的子群分类

Thm:1)$\forall d\in\mathbb{N}=\mathbb{Z}_{\geqslant0}\Rightarrow<d>=\{0,\pm d,\pm2d,\cdots\}$ 为 $\mathbb{Z}$ 的循环子群

2)$\mathbb{Z}$ 的所有子群均为 1) 中的形式

3)$<a_1,a_2,\cdots,a_n>=<gcd(a_1,a_2,\cdots,a_n)>\subseteq\mathbb{Z}$

proof:2) 设 H 为 $(\mathbb{Z},+)$ 的子群，则 H 为 $\mathbb{Z}$ 的理想

(理想满足 $\forall h_1,h_2\in H,h_1+h_2\in H,nh=h+\cdots+h\in H$)

$\exists d\geqslant0,s.t.H=(d)\Rightarrow H=\{0,\pm d,\pm2d,\cdots\}$

3)$\subseteq$: 记 $d=gcd(a_1,\cdots,a_n)$

则 $d\mid a_i\Rightarrow a_i\in<d>\Rightarrow<a_1,\cdots,a_n>\subseteq<d>$

$\supseteq$: 由贝祖定理，$\exists t_i(i=1,\cdots,n),s.t.d=a_1t_1+\cdots+a_nt_n\in<a_1,\cdots,a_n>$

$\Rightarrow<d>\subseteq<a_1,\cdots,a_n>$

Thm:1)$\forall d\mid m(d>0)$，则 $<\bar d>=\{\bar0,\bar d,\cdots,(\frac md-1)\bar d\}$ 为 $\mathbb{Z}/m\mathbb{Z}$ 的 $\frac md$ 阶循环子群

2)$\mathbb{Z}/m\mathbb{Z}$ 的所有子群均为 1) 中的形式

3)$<\overline{a_1},\cdots,\overline{a_n}>=<\overline{gcd(a_1,\cdots,a_n,m)}>\subseteq\mathbb{Z}/m\mathbb{Z}$，特别地，$<\bar a>=<\overline{gcd(a,m)}>$

proof:1) 容易证明 $ord(\bar d)=\frac md$

2) 设 $H\leqslant\mathbb{Z}/m\mathbb{Z}$，设 $I_H:=\{i\in\mathbb{Z}|\bar i\in H\}$，则 I_H 为 $\mathbb{Z}$ 的子群，($\forall i,j\in I_H$，$\overline{i-j}=\bar i-\bar j\in H\Rightarrow i-j\in I_H$)

$\Rightarrow\exists d\geqslant0,s.t.I_H=<d>\subseteq\mathbb{Z}$

$\Rightarrow H=\{\bar i|i\in I_H\}=\{\overline{kd}|k\in\mathbb{Z}\}=<d>$

3):$\subseteq$: 显然

$\supseteq$: 由贝祖定理，$gcd(a_1,\cdots a_n)=a_1x_1+\cdots+a_nx_n+ym$

同时模 m，则 $\overline{gcd(a_1,\cdots a_n)}=\overline{a_1x_1+\cdots+a_nx_n}\in<\overline{a_1},\cdots,\overline{a_n}>$

推论：G 为 m 阶循环群，设 x 为 G 的生成元，$\forall d\mid m$，记 $H_d=\{1,x^{\frac md},\cdots,x^{\frac{(d-1)m}{d}}\}$

则 1)H_d 为 G 的 d 阶循环子群

2)G 的任意子群均为这一形式

proof:1) 容易证明 $ord(x^{\frac{m}{d}}) = d \Rightarrow H_d =< x^{\frac{m}{d}} >$ 为 G 的 d 阶循环子群

2)$\forall H \leqslant G$，考虑 $m \in I_H := \{i \in \mathbb{Z} | x^i \in H\} \leqslant \mathbb{Z}$

因此 $I_H =< \frac{m}{d} > (d \mid m)$，从而 $H = \{x^i | i \in I_H =< x^{\frac{m}{d}} >\} = \{1, x^{\frac{m}{d}}, \cdots, x^{\frac{(d-1)m}{d}}\}$

推论：$n = \sum\limits_{1 \leqslant d \mid n} \varphi(d)$

proof: 记 H_d 为 $\mathbb{Z}/m\mathbb{Z}$ 的 d 阶子群的生成元组成的子集

$\Rightarrow \mathbb{Z}/m\mathbb{Z} = \bigsqcup\limits_{d \mid m} H_d \Rightarrow m = \sum\limits_{d \mid m} \#H_d = \sum\limits_{d \mid m} \varphi(d)$

4.2 拉格朗日定理

4.2.1 陪集

Def:$H < G, \forall a \in G$，定义 $\begin{cases} aH = \{ah | h \in H\} \text{ 为 H 的左陪集 (left coset)} \\ Ha = \{ha | h \in H\} \text{ 为 H 的右陪集 (rigit coset)} \end{cases}$

Properties:1)$\forall a \in H, aH = H$

2) 以下三个命题等价

a)$aH = bH$

b)$aH \cap bH \neq \varnothing$

c)$b^{-1}a \in H$

proof:1):$\forall h \in H, h = a(a^{-1}h), a^{-1}h \in H \Rightarrow H = aH$

2):$a) \Rightarrow b)$: 显然

$b) \Rightarrow c)$: $\exists h_1, h_2 \in H, s.t. ah_1 = bh_2 \Rightarrow b^{-1}a = h_2 h_1^{-1} \in H$

$c) \Rightarrow a)$: $b^{-1}a \in H \Rightarrow b^{-1}aH = H \Rightarrow aH = b(b^{-1}aH) = bH$

4.2.2 左 (右) 陪集代表元素

G 的一个分拆：设 $\{a_iH | i \in I\}$ 为 G 关于 H 的所有左陪集构成的集合，即 a_iH 过所有 G 关于 H 的左陪集且两两不交，则 $G = \bigsqcup\limits_{i \in I} a_iH$

Def: 上式中的指标集 $\{a_i | i \in I\}$ 称为 G 的一个左陪集代表元系，类似地，我们可以定义右陪集代表元系。容易看出，$\{b_j | j \in J\}$ 为 G 的一个右陪集代表元系当且仅当 $G = \bigsqcup\limits_{j \in J} Hb_j$

Lemma: 若 $S \subseteq G$ 为 G 的左陪集代表元系，则 $S^{-1} := \{s^{-1} | s \in S\}$ 为 G 的右陪集代表元系

proof: 因为作为集合 $(aH)^{-1} = \{(ah)^{-1} | h \in H\} = \{h^{-1}a^{-1} | h \in H\} = Ha^{-1}$

4.2.3 指数

Def:$H < G$，称 H 在 G 中的左 (右) 陪集总个数为 G 关于 H 的指数 (index)，记作 $(G : H)$ 或 $[G : H]$，若有无穷多个陪集，则记为 $(G : H) = \infty$

4.2.4 群论中的拉格朗日定理

Thm:$\#G = \#H \cdot (G : H)$

proof:$G = \bigsqcup_{i \in I} a_i H$(此时 $(G : H) = \#I$)

因为 $H \overset{1:1}{\to} aH \Rightarrow \#(a_i H) = \#H$

1° 若 $\#G = \infty$，则 $\#H = \infty$ 或 $\#I = \infty$(否则右边为有限集合)

因此，$\#G = \#H \cdot (G : H)$

2° 若 $\#G < \infty$，则 $\#G = \sum_{i \in I} \#(a_i H) = \sum_{i \in I} (\#H) = \#H \cdot \#I = \#H \cdot \#(G : H)$

推论：若 $\#G < \infty$，则

1)$H < G \Rightarrow \#H \mid \#G$

2)$\forall x \in G \Rightarrow ord(x) \mid \#G \Rightarrow x^{\#G} = 1$

推论：欧拉定理、费马小定理

1)$gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 (mod m)$

2)p 素数，$p \nmid a \Rightarrow a^{p-1} \equiv 1 (mod p)$

proof:1)$gcd(a, m) = 1 \Rightarrow a \in (\mathbb{Z}/m\mathbb{Z})^\times$

而 $\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m) \Rightarrow \bar{a}^{\varphi(m)} = 1$

推论：p 素数，则

1)p 阶群同构于 $(\mathbb{Z}/p\mathbb{Z}, +)$

2)p 阶域同构于 $\mathbb{F}_p$

proof:1) 因为 $\#G = p \Rightarrow \forall g \in G \backslash \{1\}, ord(g) \mid \#G = p \Rightarrow ord(g) = p$

所以 $G =< g > \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$

2) 设 $\mathbb{F}$ 为 p 阶域，则由 1)，$(\mathbb{F}, +) \cong (\mathbb{Z}/p\mathbb{Z}, +)$

因为 $ord(1_\mathbb{F}) = p$(对于加法)，所以 $\mathbb{F} = \{0_\mathbb{F}, 1_\mathbb{F}, 2 \cdot 1_\mathbb{F} \cdots, (p-1) \cdot 1_\mathbb{F}\}$

根据倍数的定义 $(i \cdot 1_\mathbb{F})(j \cdot 1_\mathbb{F}) = ij \cdot 1_\mathbb{F}$

对于乘法，考虑映射 $\varphi : \mathbb{F} \to \mathbb{Z}/p\mathbb{Z}, i \cdot 1_\mathbb{F} \mapsto \bar{i} = i + p\mathbb{Z}$

所以，$\varphi((i \cdot 1_\mathbb{F})(j \cdot 1_\mathbb{F})) = \overline{ij} = \bar{i} \cdot \bar{j} = \varphi(i \cdot 1_\mathbb{F}) \cdot \varphi(j \cdot 1_\mathbb{F})$

4.3 正规子群与商群

4.3.1 正规子群

Def:$H \leqslant G$

1)$\forall x, g \in G$，称 gxg^{-1} 为 x 的共轭元

2) 若任意 H 中元素的任意共轭元均在 H 中，也就是说 $\forall g \in G, ghg^{-1} \in H$，则称 H 为 G 的正规子群，记作 $H \lhd G$

特别地，若 G 为交换群，则 $gxg^{-1} = x$，即交换群的任意子群均为正规子群

Lemma:$H \leqslant G, a \in G$，则 $aHa^{-1} = H \Leftrightarrow aH = Ha$

proof:$(\Rightarrow) : aHa^{-1} := \{aha^{-1} | h \in H\}$

$Ha := \{ha | h \in H\} = \{h^{'}a | h^{'} \in aHa^{-1}\} = \{(ah^{''}a^{-1})a | h^{''} \in H\} = \{ah^{''} | h^{''} \in H\} = aH$

$(\Leftarrow) : aHa^{-1} := \{aha^{-1} | h \in H\} = \{ga^{-1} | g \in aH\} = \{ga^{-1} | g \in Ha\} = \{h^{'}aa^{-1} | h^{'} \in H\} = \{h^{'} | h^{'} \in H\} = H$

Property:$H \leqslant G$，则 $H \lhd G \Leftrightarrow gH = Hg, \forall g \in G$

4.4 群同态中的正规子群

Property: 若 $\varphi : G \to G^{'}$ 为群同态，则 $Ker(\varphi)$ 为正规子群 (反之也对，需要构造 φ 使得 $Ker(\varphi)$ 为该正规子群)

proof:$Ker(\varphi) := \varphi^{-1}(1_{G'}) = \{g \in G | \varphi(g) = 1_{G'}\}$

$\forall h \in Ker(\varphi), \forall g \in G, \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g) \cdot 1_{G'} \cdot \varphi(g)^{-1} = 1_{G'}$

4.4.1 商群与陪集运算

Def:$N \lhd G \Rightarrow$ 称 $G/N = \{gN | g \in G\}$ 为商群

Def(商群下的陪集运算):$(g_1N) \cdot (g_2N) := (g_1g_2)N$

良定性：需要验证若 $g_1N = g_1^{'}N, g_2N = g_2^{'}N$，是否有 $(g_1g_2)N = (g_1^{'}g_2^{'})N$

$$\left.\begin{array}{l} g_1N = g_1^{'}N \Rightarrow (g_1^{'})^{-1}g_1 \in N \\ g_2N = g_2^{'}N \Rightarrow (g_2^{'})^{-1}g_2 \in N \end{array}\right\} g_2^{'-1}g_1^{'-1}g_1g_2 = (g_2^{'-1}g_2)(g_2^{-1}g_1^{'-1}g_1g_2) \in N$$

所以 $(g_1g_2)N = (g_1^{'}g_2^{'})N$

Property:$N \lhd G$，则 $(G/N, \cdot)$ 构成群

结合律:$(g_1N \cdot g_2N)g_3N = g_1g_2N \cdot g_3N = g_1g_2g_3N = g_1N \cdot g_2g_3N = g_1N(g_2g_3N)$

幺元:N
逆元:$(gN)^{-1} = g^{-1}N$
类比 $i \mapsto \bar{i}$，我们考虑映射 $\varphi : G \to G/N, g \mapsto gN$，则若 $N \lhd G$
1)φ 为群同态
2)$Ker(\varphi) = N$

4.5 群同态基本定理

设 $\varphi : G \to G'$ 为群同态，则
$$im(\varphi) \cong G/Ker(\varphi)$$

proof: 考虑 $\psi : \varphi(a) \mapsto aKer(\varphi)$

5 域 $\mathbb{F}_p$ 上的算术

5.1 单位群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的结构

5.1.1 原根

Def: 设 $m \geqslant 1$，如果 $(\mathbb{Z}/m\mathbb{Z})^\times$ 为循环群，则它的一个生成元 $g \ mod \ m$ 称为模 m 的一个原根 (primitive root)

5.2 单位群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 何时为循环群

Thm:$(\mathbb{Z}/m\mathbb{Z})^\times$ 是循环群 $\Leftrightarrow m = 2, 4, p^\alpha$ 或 $2p^\alpha$(p 为奇素数)
接下来我们开始证明这个定理
若记 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，则由中国剩余定理，有
$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$
$rmodm \mapsto (rmodp_1^{\alpha_1}, \cdots, rmodp_k^{\alpha k})$
推广至一般群，我们给出以下引理
Lemma: 设 $G = H_1 \times H_2 \times \cdots \times H_s$ 为有限群，则
$$\text{G 循环} \Leftrightarrow \begin{cases} H_1, \cdots, H_s \text{ 循环} \\ gcd(\#H_i, \#H_j) = 1, \forall i \neq j \end{cases}$$
proof:($\Leftarrow$) : 记 $m_i := \#H_i, \#G = m = \prod_{i=1}^{s} m_i$

则 $G = H_1 \times \cdots \times H_s \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$，故 G 为循环群

$(\Rightarrow): \exists g = (h_1, \cdots, h_s) \in G = H_1 \times \cdots \times H_s$，使得 $G =< g >$

则 G 中元素均为 $g^k = (h_1^k, \cdots, h_s^k)$

$\Rightarrow H_i$ 中元素均为 $h_i^k \Rightarrow H_i =< h_i >$ 为循环群

接下来我们要说明 $gcd(\#H_i, \#H_j) = 1, \forall i \neq j$

记 $m^{'} = lcm(\#H_1, \cdots, \#H_s)$，因为 $h_i^{\#H_i} = 1$，所以 $h_i^{m^{'}} = 1$

$g^{m^{'}} = (h_1^{m^{'}}, \cdots, h_s^{m^{'}}) = (1, \cdots, 1) = 1_G$

所以 $\#G = ord(h_1, \cdots, h_s) \mid m^{'} = lcm(\#H_1, \cdots, \#H_s) \mid \#H_1 \cdots \#H_s = m_1 \cdots m_s = m = \#G$

即 $lcm(m_1, \cdots, m_s) = m_1 \cdots m_s \Rightarrow m_1, \cdots, m_s$ 两两互素

Lemma:$(\mathbb{Z}/2^\alpha)^\times$ 循环 $\Leftrightarrow \alpha \leqslant 2$

proof:$(\Leftarrow)$：逐一验证即可

$(\Rightarrow): (\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = 1$ 不为循环群

$\alpha > 3$ 时，考虑满同态 $\varphi(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times, i + 2^\alpha\mathbb{Z} \mapsto i + 8\mathbb{Z}$

假设 $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ 为循环群，有生成元 $g \mapsto \varphi(g)$

则 $\varphi(g)$ 为 $(\mathbb{Z}/8\mathbb{Z})^\times$ 的生成元，矛盾！

由此我们可以开始证明定理

proof:$(\Rightarrow)$：由引理知，m=2 或 4 时为循环群，下面验证 $m = p^\alpha$ 时

Thm:$\mathbb{F}_p$ 为 $p-1$ 阶循环群

proof: 构造集合 $S_d := \{a \in \mathbb{F}_p^\times | ord(a) = d\} \subseteq \{x \in \mathbb{F}_p | x^d = 1\}$

fact: 域上的 d 次多项式最多有 d 个解

所以，若 $a^d = 1$，则 $1, a, \cdots, a^{d-1}$ 为 $x^d = 1$ 的 d 个解，且恰有 $\varphi(d)$ 个解为 d 阶元

则 $\#S_d \leqslant \varphi(d)$

因此，$p - 1 = \sum_{1 \leq d \mid p-1} \#S_d \leq \sum_{1 \leq d \mid p-1} \varphi(d) = p - 1$

所以上式中不等号应为等号，即 $\#S_{p-1} = \varphi(p-1) \neq \varnothing$

$\Rightarrow$ 存在 p-1 阶元，即 $\mathbb{F}_p$ 为 p-1 阶循环群

Thm:p 为奇素数，$k \geqslant 2$，则 $(\mathbb{Z}/p^k\mathbb{Z})^\times$ 为循环群

Lemma1:$\varphi: G \to G^{'}, g \mapsto \varphi(g)$ 为群同态，则 $\forall g \in G$，有 $ord(\varphi(g)) \mid ord(g)$

proof: 设 $n = ord(g) \Rightarrow g^n = 1_G, \varphi(g^n) = \varphi(g)^n = 1_{G'} \Rightarrow ord(\varphi(g)) \mid n$

Lemma2(升幂引理): 设 p 为奇素数或 $\alpha \geqslant 2, \forall a, b$ 与 p 互素，$\forall k \geqslant 0$，则

$p^\alpha || a - b \Rightarrow p^{\alpha+k} || a^{p^k} - b^{p^k}$(恰好整除：$p^\alpha || n \Leftrightarrow p^\alpha \mid n$ 且 $p^{\alpha+1} \nmid n$)

proof: 对 k 归纳，k=0 时，显然，假设 k=n 时命题成立，下证 k=n+1 时也成立

根据归纳假设，我们有 $a^{p^n}-b^{p^n}=p^{\alpha+n}\cdot c$

$a^{p^{n+1}}=(a^{p^n})^p=(b^{p^n}+p^{\alpha+n}\cdot c)^p$

$\quad=(b^{p^n})^p+\binom{p}{1}(b^{p^n})^{p-1}(p^{\alpha+n}\cdot c)+\binom{p}{2}(b^{p^n})^{p-2}(p^{\alpha+n}\cdot c)^2+\cdots+\binom{p}{p}(p^{\alpha+n}\cdot c)^n$

两边同时模 $p^{\alpha+n+1}$ 得 $a^{p^{n+1}}\equiv b^{p^{n+1}}(modp^{\alpha+n+1})$

两边同时模 $p^{\alpha+n+2}$ 得 $a^{p^{n+1}}\equiv b^{p^{n+1}}+\binom{p}{1}(b^{p^n})^{p-1}(p^{\alpha+n}\cdot c)(modp^{\alpha+n+2})$

即 $p^{\alpha+n+1}||a^{p^{n+1}}-b^{p^{n+1}}$

proof(Thm):k=1 时已证，设 g 为 $\mathbb{F}_p$ 的生成元

k=2 时考虑满同态 $\varphi:\mathbb{Z}/p^2\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z},g+p^2\mathbb{Z}\mapsto g+p\mathbb{Z}$

因为 $\varphi(g+p+p^2\mathbb{Z})=\varphi(g+p^2\mathbb{Z})=g+p\mathbb{Z}$

由 Lemma1: $\begin{cases}ord(g+p\mathbb{Z})\mid ord(g+p^2\mathbb{Z})\\ ord(g+p\mathbb{Z})\mid orrd(g+p+p^2\mathbb{Z})\end{cases}$

因为 $\#(\mathbb{Z}/p^2\mathbb{Z})^\times=p(p-1)$

所以 $\begin{cases}p-1\mid ord(g+p^2\mathbb{Z})\mid p(p-1)\\ p-1\mid orrd(g+p+p^2\mathbb{Z})\mid p(p-1)\end{cases}$

$\Rightarrow ord(g+p^2\mathbb{Z}),ord(g+p+p^2\mathbb{Z})\in\{p-1,p(p-1)\}$

因为 $(g+p)^{p-1}-g^{p-1}=\binom{p-1}{1}g^{p-2}p+\binom{p-1}{2}g^{p-3}p^2+\cdots+\binom{p-1}{p-1}p^{p-1}$

同时模 p^2 得

$(g+p)^{p-1}-g^{p-1}\equiv g^{p-2}p(p-1)\not\equiv 0(modp^2)$

因此，二者不可能同时模 p^2 余 1

所以 $ord(g+p^2\mathbb{Z})\neq p-1$ 或 $ord(g+p+p^2\mathbb{Z})\neq p-1$

即 $ord(g+p^2\mathbb{Z})=p(p-1)$ 或 $ord(g+p+p^2\mathbb{Z})=p(p-1)$

即 g 或 g+p 为生成元，$(\mathbb{Z}/p^2\mathbb{Z})^\times$ 为 p(p-1) 阶循环群

$k\geqslant 3$ 时，我们不妨设 $g+p^2\mathbb{Z}$ 生成 $(\mathbb{Z}/p^2\mathbb{Z})^\times$

则 $g^{p-1}\not\equiv 1(modp^2)$ 且 $g^{p-1}\equiv 1(modp)\Rightarrow p||g^{p-1}-1$

由升幂引理， $\begin{cases}k=\alpha-1\Rightarrow p^\alpha\mid\mid(g^{p-1})^{p^{\alpha-1}}-1\\ k=\alpha-2\Rightarrow p^{\alpha-1}\mid\mid(g^{p-1})^{p^{\alpha-2}}-1\end{cases}$

即 $\begin{cases}g^{p^{\alpha-1}(p-1)}\equiv 1(modp^\alpha)\\ g^{p^{\alpha-2}(p-1)}\not\equiv 1(modp^\alpha)\end{cases}\Leftrightarrow\begin{cases}ord(g+p^\alpha\mathbb{Z})\mid p^{\alpha-1}(p-1)\cdots①\\ ord(g+p^\alpha\mathbb{Z})\nmid p^{\alpha-2}(p-1)\cdots②\end{cases}$

考虑满同态 $\varphi:(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\to(\mathbb{Z}/p\mathbb{Z})^\times,g+p^\alpha\mathbb{Z}\mapsto g+p\mathbb{Z}$

由 Lemma1 知，$ord(g+p\mathbb{Z})=p-1\mid ord(g+p^\alpha\mathbb{Z})\cdots③$

综上，由①②③知，$ord(g+p^{\alpha\mathbb{Z}})=p^{\alpha-1}(p-1)=\varphi(p^\alpha)$
即 $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ 由 $g+p^\alpha\mathbb{Z}$ 生成
因此，找模 p^α 的原根只需找模 p 的原根，再验证其是不是模 p^2 的原根即可
$m=2p^\alpha$ 时，$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times\cong(\mathbb{Z}/2\mathbb{Z})^\times\times(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\cong(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ 为循环群

5.3 $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times(\alpha\geqslant 3)$ 的结构

Thm:$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times=<\bar{5},\bar{-1}>$
proof:Claim:$ord(\bar{5})=2^{\alpha-2}$
proof of claim: 因为 $8=2^3||5^2-1$
由升幂引理，取 $k=\alpha-3\Rightarrow 2^\alpha||(5^2)^{2^{\alpha-3}}-1=5^{2^{\alpha-2}}-1$
所以，$5^{2^{\alpha-2}}\equiv 1(mod 2^\alpha)\Rightarrow ord(\bar{5})\leqslant 2^{\alpha-2}$
注意到 $4||5-1$，由升幂引理，取 $k=\alpha-3$，则 $2^{\alpha-1}||5^{2^{\alpha-3}}-1$，即 $2^\alpha\nmid 5^{2^{\alpha-3}}-1$
所以 $5^{2^{\alpha-3}}\not\equiv 1(mod 2^\alpha)$，所以，$ord(\bar{5})=2^{\alpha-2}$
考虑 $\varphi:<\bar{5}>\times<\overline{-1}>\to(\mathbb{Z}/2^\alpha\mathbb{Z})^\times,(\bar{5}^k,(\overline{-1})^l)\mapsto(\overline{-1})^k\bar{5}^l$
Claim:φ 为群同构
$\varphi(((-1)^{k_1},5^{l_1})((-1)^{k_2},5^{l_2}))=(-1)^{k_1}5^{l_1}(-1)^{k_2}5^{l_2}=\varphi((-1)^{k_1},5^{l_1})\varphi((-1)^{k_2},5^{l_2})$
因为 $\#<\bar{5}>\times\#<\overline{-1}>=2^{\alpha-2}\cdot 2=2^{\alpha-1}=\#(\mathbb{Z}/2^{\alpha\mathbb{Z}})^\times$
只需验证单射即可，即验证 $Ker(\varphi)=\{(1,1)\}$
若 $\bar{5}^k(\overline{-1})^l=\bar{1}\Rightarrow 5^k\equiv(-1)^l(mod 2^\alpha)\Rightarrow 5^k\equiv(-1)^l(mod 8)$
注意到 $5^1\equiv 5(mod 8),5^2\equiv 1(mod 8),\cdots$
$(-1)^1\equiv -1(mod 8),(-1)^2\equiv 1(mod 8),\cdots$
所以若 $5^k(-1)^l\equiv 1(mod 8)$，只能是 $5^k\equiv(-1)^l\equiv 1(mod 8)$
所以 $Ker(\varphi)=\{(1,1)\}$
所以，$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times=<\bar{5},\overline{-1}>$

5.4 小结

设 $gcd(a,m)=1$
a 模 m 的阶 $\Leftrightarrow a+m\mathbb{Z}$ 在 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中的阶
g 为模 m 的原根 $\Leftrightarrow g+m\mathbb{Z}$ 生成 $(\mathbb{Z}/m\mathbb{Z})^\times$
模 m 有原根 $\Leftrightarrow(\mathbb{Z}/m\mathbb{Z})^\times$ 为循环群

5.5 $\mathbb{F}_p$ 中的平方元与二次剩余

5.5.1 二次剩余

Def: 如果 $amodp$ 是 $\mathbb{F}_p$ 中的平方元，称 amodp 为二次剩余，反之，则称为非二次剩余
Prop:$\mathbb{F}_p$ 中的二次剩余共有 $\frac{p-1}{2}$ 个
proof:$\mathbb{F}_p = \{-\frac{p-1}{2}, \cdots, -1, 1, \cdots, \frac{p-1}{2}\}$
平方后得到 $1^2, 2^2, \cdots, (\frac{p-1}{2})^2$，下面只需证明这 $\frac{p-1}{2}$ 个数两两不等
假设 $i^2 \equiv j^2(modp), i \neq j$
则 $(i+j)(i-j) \equiv 0(modp)$，而 $-(p-1) < i+j < p-1$
则只能是 $i = j$，矛盾！
• $(\mathbb{F}_p^\times)^2 := \{a^2 | a \in \mathbb{F}_p\}$ 为 $(\mathbb{F}_p)^\times$ 的 $\frac{p-1}{2}$ 阶子群

5.5.2 勒让德符号

$$a \in \mathbb{F}_p, (\frac{a}{p}) = (\frac{amodp}{p}) = \begin{cases} 1 & \text{a 为二次剩余} \\ 0 & \text{a=0} \\ -1 & \text{a 为非二次剩余} \end{cases}$$

Prop: 方程 $x^2 \equiv a(modp)$ 在 $\mathbb{F}_p$ 中的解数为 $(\frac{a}{p}) + 1$
Property:$(\frac{\cdot}{p}) : (\mathbb{F}_p)^\times \to \{\pm 1\}$ 为群同态，$Ker(\frac{\cdot}{p}) := \{a, -a | a\text{为二次剩余}\}$
proof: 即证 $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$，设 $(\mathbb{F}_p)^\times =< g >, a = g^k, b = g^l$
则 $(\frac{a}{p})(\frac{b}{p}) = (-1)^k(-1)^l = (-1)^{k+l} = (\frac{ab}{p})$
($a = g^k$ 为二次剩余 $\Leftrightarrow 2 \mid k \Rightarrow (\frac{a}{p}) = (-1)^k$)

5.5.3 勒让德符号的计算

$a = sgn(a) \cdot p_1^{\alpha_1} \cdots p_k^{\alpha k}$
$\Rightarrow (\frac{a}{p}) = (\frac{sgn(a)}{p})(\frac{p_1}{p})^{\alpha_1}, \cdots, (\frac{p_k}{p})^{\alpha_k}$
只需计算 $(\frac{-1}{p}), (\frac{2}{p}), (\frac{q}{p})$ 即可 (q 是与 p 不同的奇素数)

5.5.4 欧拉判别法

p 为奇素数，$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(modp)$
proof: 设 $(\mathbb{F}_p)^\times =< g >, a = g^k$
由欧拉定理，$a^{p-1} \equiv 1(modp)$，则 $a^{\frac{p-1}{2}} \equiv \pm 1(modp)$

因为 $a^{\frac{p-1}{2}} = g^{p-1\cdot\frac{k}{2}} \equiv 1(modp)$ 当且仅当 $p-1$ 是 $\frac{p-1}{2}$ 的因子，即 k 为偶数，a 为模 p 二次剩余，命题得证

例：$a=-1$ 时，$(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}}(modp) = \begin{cases} 1, p=4k+1 \\ -1, p=4k+3 \end{cases}$

5.5.5 高斯引理

Lemma:p 为奇素数，$gcd(a,p)=1$，记 $r=\frac{p-1}{2}, \mu := \#\{i|1\leqslant i\leqslant r|ia$模 p 余数大于$\frac{p}{2}\}$

则 $(\frac{a}{p}) = (-1)^{\mu}$

proof: 将 $\{a, 2a, \cdots, ra\}$ 按与 $\frac{p}{2}$ 大小，并模 p 后重排得到 $\{b_1, \cdots, b_\alpha, c_1, \cdots, c_\beta\}$

其中 $b_1 < \cdots < b_\alpha < \frac{p}{2} < c_1 < \cdots < c_\beta, \alpha+\beta = r$

Claim:$\{b_1, \cdots, b_\alpha, p-c_1, \cdots, p-c_\beta\} = \{1, 2, \cdots, r\}$(模 p 意义下)

因为对于 $\forall i_1 \neq i_2, j_1 \neq j_2, i \neq j$

均有 $b_{i_1} \not\equiv b_{i_2}(modp), p-c_{j_1} \not\equiv p-c_{j_2}(modp), b_i \not\equiv p-c_j(modp)$

若 $b_{i_1} \equiv b_{i_2}(modp) \Rightarrow \exists s_1, s_2, s_1 a \equiv s_2 a(modp) \Rightarrow s_1 = s_2$，矛盾

若 $p-c_{j_1} \not\equiv p-c_{j_2}(modp) \Rightarrow \exists t_1, t_2, p-t_1 a \equiv p-t_2 a(modp) \Rightarrow t_1 = t_2$，矛盾

若 $b_i \not\equiv p-c_j(modp) \Rightarrow \exists s, t, sa \equiv p-ta(modp) \Rightarrow s+t \equiv 0(modp)$，与 $1 \leqslant s, t \leqslant \frac{p-1}{2}$ 矛盾

所以 $\{b_1, \cdots, b_\alpha, p-c_1, \cdots, p-c_\beta\}$ 中元素两两模 p 不同余且均 $\in [1, \frac{p-1}{2}]$

断言得证，进一步，两边同时累乘 (模 p 意义下)

$b_1 \cdots b_\alpha (p-c_1) \cdots (p-c_\beta) \equiv r!(modp)$

即 $b_1 \cdots b_\alpha c_1 \cdots c_\beta (-1)^\mu \equiv r!(modp)$

$\Rightarrow (-1)^\mu (a \cdot 2a \cdots ra) \equiv r!(modp)$

$\Rightarrow (-1)^\mu r! a^{\frac{p-1}{2}} \equiv r!(modp)$

因为 $gcd(r!, p) = 1$，所以 $(-1)^\mu a^{\frac{p-1}{2}} \equiv 1(modp) \Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^\mu (modp)$

由欧拉引理，$(\frac{a}{p}) = (-1)^\mu$

例：a=2 时，$\forall i \in [1, r], 2i \in [2, p-1]$

$\mu = \frac{p}{2}$ 到 p 间的偶数个数 $=0$ 到 p 间的偶数个数 -0 到 $\frac{p}{2}$ 间的偶数个数

$\mu = [\frac{p}{2}] - [\frac{p}{4}] \Rightarrow (\frac{2}{p}) = \begin{cases} 1, p \equiv \pm 1(mod 8) \\ -1, p \equiv \pm 3(mod 8) \end{cases}$

5.5.6 二次互反律

Thm:p,q 为奇素数，则 $(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

也就是说 $(\frac{p}{q})=\begin{cases}(\frac{q}{p}),p\equiv 1(mod4)\text{或}q\equiv 1(mod4)\\-(\frac{q}{p}),p\equiv q\equiv 3(modp)\end{cases}$

proof:$ia=p[\frac{ia}{p}]+r_i$

沿用高斯引理证明过程中的记号，$r_i\in\{b_1,\cdots,b_\alpha,c_1,\cdots,c_\beta\}$

其中 $b_1<\cdots<b_\alpha<\frac{p}{2}<c_1<\cdots<c_\beta,\alpha+\beta=r$

记 $B=b_1+\cdots+b_\alpha,C=c_1+\cdots+c_\beta$

累加得 $a(1+\cdots+r)=\frac{p^2-1}{8}a=p\sum\limits_{i=1}^{r}[\frac{ia}{p}]+B+C$

另一方面，$\{b_1,\cdots,b_\alpha,p-c_1,\cdots,p-c_\beta\}=\{1,2,\cdots,r\}$(模 p 意义下)

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

联立两式消去 C，$(a+1)\frac{p^2-1}{8}=p(\mu+\sum\limits_{i=1}^{r}[\frac{ia}{p}])+2B$

a 为奇素数，则 $p(\mu+\sum\limits_{i=1}^{r}[\frac{ia}{p}])=(a+1)\frac{p^2-1}{8}-2B$ 为偶数

即 μ 与 $\sum\limits_{i=1}^{r}[\frac{ia}{p}]$ 同奇偶，$\Rightarrow(\frac{a}{p})=(-1)^{\mu}=(-1)^{\sum\limits_{i=1}^{r}[\frac{ia}{p}]}$

令 a=q 为奇素数，即 $(\frac{q}{p})=(-1)^{\mu}=(-1)^{\sum\limits_{i=1}^{r}[\frac{iq}{p}]}$

交换 p 和 q 的位置，则 $(\frac{p}{q})=(-1)^{\mu}=(-1)^{\sum\limits_{i=1}^{r}[\frac{ip}{q}]}$

所以 $(\frac{q}{p})(\frac{p}{q})=(-1)^{\sum\limits_{i=1}^{r}[\frac{ip}{q}]+\sum\limits_{i=1}^{r}[\frac{iq}{p}]}$，只需证 $\sum\limits_{i=1}^{r}[\frac{ip}{q}]+\sum\limits_{i=1}^{r}[\frac{iq}{p}]=\frac{p-1}{2}\frac{q-1}{2}$

观察下图，上式中等号两边为在由 $(0,0),(0,\frac{q}{2}),(\frac{p}{2},0),(\frac{p}{2},\frac{q}{2})$ 构成的矩形中的整点个数的两种表达方式，则原命题得证

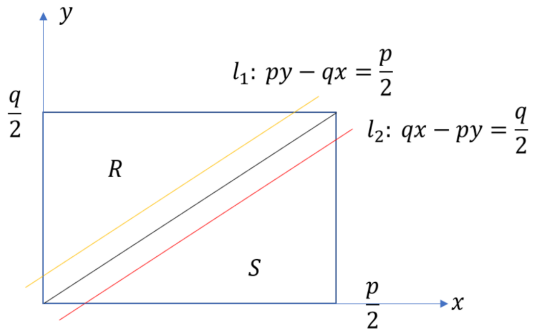

图 1: 二次互反律

例：$(\frac{219}{383}) = (\frac{73}{383})(\frac{3}{383}) = (\frac{383}{73})(-1)(\frac{383}{3}) = (-1)(\frac{18}{73})(\frac{2}{3}) = (\frac{18}{73}) = (\frac{2}{73})(\frac{3}{73})^2 = (\frac{2}{73}) = 1$

6 多项式理论

6.1 引入

设 $\mathcal{R}$ 为含幺环，则形式和

$$a_0 + a_1x + a_2x^2 + \cdots$$

称为 $\mathcal{R}$ 上的一元多项式，其中 $a_i \in \mathbb{R}(\forall i \geqslant 0)$ 且 $a_i = 0(\forall i \gg 0)$
一般记作

$$f(x) = a_nx^n + \cdots + a_1x + a_0$$

其中 a_n 为首项系数，n 为次数，记作 $deg(f) = n$，a_0 为常数项
记 $\mathcal{R}$ 上的多项式环为 $\mathcal{R}[x] = \{a_nx^n + \cdots + a_1x + a_0 | n \in \mathbb{N}, a_i \in \mathcal{R}, \forall i\}$
可通过 $\mathcal{R}$ 上的加法和乘法来定义 $\mathcal{R}[x]$ 上的加法和乘法
Prop:$(\mathcal{R}[x], +, \cdot)$ 为含幺环，且
1)$\mathcal{R}$ 交换 $\Leftrightarrow \mathcal{R}[x]$ 交换
2)$\mathcal{R}$ 为整环 $\Rightarrow \mathcal{R}[x]$ 为整环

6.2 域上的多项式理论

6.2.1 整除理论

$g \mid f \overset{def}{\Leftrightarrow} \exists h, s.t. f = gh$，称 f 为 g 的倍式，g 为 f 的因子

例 (平凡因子)：$a \in \mathbb{F}^{\times}$ 和 af 均为 f 的因子

6.2.2 带余除法

Thm(带余除法):$\forall f, g \neq 0 \in \mathbb{F}[x], deg(g) < deg(f)$，则 $\exists! q, r \in \mathbb{F}[x], s.t. f = qg + r(deg(r) < deg(g))$

proof: 存在性: 构造集合 $I := \{f - ag | a \in \mathbb{F}[x]\}$，取 I 中次数最小的多项式 r，则 $deg(r) < deg(g)$

唯一性: 假设 $f = qg + r = q^{'}g + r^{'} \Rightarrow g(q - q^{'}) = r - r^{'}$

则 $g \mid r - r^{'}$，由 $deg(r) < deg(g)$ 知，只能是 $r = r^{'}$，则 $q = q^{'}$

问：若 $\mathcal{R}$ 不为域，$\mathcal{R}[x]$ 上是否有带余除法?

答：对一般的 g 没有，但对首项系数可逆的 g 有

6.2.3 最大公因子

Def:$\forall f, g \in \mathbb{F}[x]$，称 $d \in \mathbb{F}[x]$ 为 f 与 g 的最大公因子，若

1)d 首一 (保证唯一性)

2)$d \mid f$ 且 $d \mid g$

3)$\forall d^{'}$ 满足 $d^{'} \mid f$ 且 $d^{'} \mid g$，则 $deg(d^{'}) < deg(d)$

此时记 $d = gcd(f, g)$，若 $d = 1$，则称 f 与 g 互素

6.2.4 贝祖定理

回忆：$(S) \lhd \mathcal{R}$ 为包含 S 的最小理想

Thm(贝祖定理)：$(gcd(f, g)) = (f, g) \lhd \mathbb{F}[x]$

proof:$\supseteq$: 显然

$\subseteq$: 设 $f \neq 0$ 或 $g \neq 0$，记 d 为 (f, g) 中次数最小的非零首一多项式

带余除法 $\Rightarrow \begin{cases} d \mid f \\ d \mid g \end{cases} \Rightarrow o < deg(d) \leqslant deg(gcd(f, g))$

另一方面，$d \in (f, g)$，$gcd(f, g) \mid d \Rightarrow d = deg(f, g)$

推论 (贝祖等式)：1)$\forall f,g,\exists u,v$，使得 $gcd(f,g)=fu+gv$，特别地，若 d 为 f 和 g 的公因子，则 $d \mid gcd(f,g)$

2)$gcd(f,g)=1 \Leftrightarrow \exists u,v$，使得 $fu+gv=1$

6.2.5 $\mathbb{F}[x]$ 为主理想整环

proof:$\forall I \lhd \mathbb{F}[x]$

$1°I=\{0\} \Rightarrow I=(0)$

$2°I \neq 0$，记 d 为 I 中次数最小的非零多项式，下证 $I=(d)$

$\supseteq$: 显然

$\subseteq$: $\forall f \in I, f=dq+r(deg(r)<deg(d))$

$\Rightarrow r=f-dq \in I \Rightarrow r=0$，否则与 d 次数最小矛盾!

所以，$f=dq \in (d)$

6.2.6 初等数论的推广

初等数论中最大公因子的性质都可以推广到多项式上，如下

Prop:1).$a,b \in \mathbb{F}^{\times} \Rightarrow gcd(af,bg)=gcd(f,g)$

2).$gcd(f,g)=gcd(g,f)$

3).$f \neq 0$，$gcd(f,0)=gcd(f,f)=\frac{f}{lc(f)}$(lc(f) 为 f 的首项系数)

4).$d \mid f, d \mid g \Rightarrow d \mid gcd(f,g)$

5).h 首一，则 $h \cdot gcd(f,g)=gcd(fh,gh)$

6).$d=gcd(f,g) \Rightarrow gcd(\frac{f}{d},\frac{g}{d})=1$

7).$gcd(f,h)=1 \Rightarrow gcd(f,gh)=gcd(f,g)$

8).$h \mid fg, gcd(h,f)=1 \Rightarrow h \mid g$

类似地，我们还可以定义 $gcd(f_1,f_2\cdots,f_n), lcm(f,g), lcm(f_1,f_2\cdots,f_n)$

6.2.7 欧式算法

目的：求 u,v，使得 $gcd(f,g)=fu+gv$

例:$f=x^4+x^3, g=x^4-1$

$x^4+x^3=x^4-1+x^3+1$

$x^4-1=x(x^3+1)+(-x-1)$

$x^3+1=(-x-1)(-x^2+x-1)$

则 $gcd(x^4+x^3, x^4-1) = x+1$(首项系数为 1)

用表格表示如下

	x^4+x^3	1	0
1	x^4-1	0	1
x	x^3+1	1	-1
$-x^2+x-1$	$-x-1$	-x	1+x

则 $-x-1 = -x(x^4+x^3) + (1+x)(x^4-1)$

$\Rightarrow x+1 = x(x^4+x^3) - (1+x)(x^4-1)$

6.2.8 不可约元

Def:$\forall p \in \mathbb{F}[x]$ 且 $p \notin \mathbb{F}$，称 p 不可约，若它满足

$p = fg \Rightarrow f \in \mathbb{F}^\times$ 或 $g \in \mathbb{F}^\times$(p 只有平凡拆分)

注：不可约元对应的是素数这一概念

欧几里得引理：p 不可约，则 $p \mid fg \Rightarrow p \mid f$ 或 $p \mid g$

proof:$gcd(p, fg) = cp(c \in \mathbb{F}^\times)$ 且 cp 首一

设 $p \nmid f \Rightarrow gcd(p, f) = 1 \Rightarrow gcd(p, g) = cp \Rightarrow p \mid g$

注：域上多项式是否可约，判断其是否有根即可

6.2.9 唯一分解定理

$\mathbb{F}[x]$ 为唯一分解整环，也就是说，$\forall f \in \mathbb{F}[x], f \notin \mathbb{F}$，则存在首一多项式 $p_1, \cdots, p_s$ 以及 $c \in \mathbb{F}^\times$，使得 $f = cp_1p_2\cdots p_s$，且在不计次序下，该表达唯一

$\Rightarrow f = cp_1^{\alpha_1}\cdots p_k^{\alpha_k}(p_i \neq p_j, \forall i \neq j)$

推论：1)$gcd(c_1p_1^{\alpha_1}\cdots p_k^{\alpha_k}, c_2p_1^{\beta_1}\cdots p_k^{\beta_k}) = p_1^{min\{\alpha_1,\beta_1\}}\cdots p_k^{min\{\alpha_k,\beta_k\}}$

2)$lcm(c_1p_1^{\alpha_1}\cdots p_k^{\alpha_k}, c_2p_1^{\beta_1}\cdots p_k^{\beta_k}) = p_1^{max\{\alpha_1,\beta_1\}}\cdots p_k^{max\{\alpha_k,\beta_k\}}$

3)$\frac{fg}{lc(fg)} = gcd(f,g)\cdot lcm(f,g)$

6.3 同余理论

6.3.1 基本定义与等价类

设 $deg(m) \geqslant 1$，$f \equiv g(mod m) \overset{def}{\Leftrightarrow} m \mid f-g$，称 f 与 g 模 m 同余

$\forall r \in \mathbb{F}[x]$，$[r] := r$ 所在的模 m 等价类 $= \{r + mf | f \in \mathbb{F}[x]\}$

也可写作 $\bar{r}, r mod m, r+m\mathbb{F}[x], r+(m)$

类比 $\mathbb{Z}/m\mathbb{Z}$，我们定义 $\mathbb{F}[x]/m\mathbb{F}[x]=\{[r]|r\in\mathbb{F}[x]\}$

定义同余类的加法和乘法：$\forall[r_1],[r_2]\in\mathbb{F}[x]/m\mathbb{F}[x]$

$[r_1]+[r_2]=[r_1+r_2],[r_1]\cdot[r_2]=[r_1\cdot r_2]$

Thm:1)$\mathbb{F}[x]/m\mathbb{F}[x]$ 为含幺交换环

2)$\mathbb{F}[x]/m\mathbb{F}[x]$ 中的元素都可唯一地表示为 $[r]$，其中 $r=0$ 或 $deg(r)\leqslant deg(m)$

3)$(\mathbb{F}[x]/m\mathbb{F}[x])^\times=\{[a]|gcd(a,m)=1\}$

4)①$\mathbb{F}[x]/m\mathbb{F}[x]=$整环 ⇔②$\mathbb{F}[x]/m\mathbb{F}[x]=$域 ⇔③$m$为不可约元

proof:4)③⇒②:$\forall[r]\neq 0\in\mathbb{F}[x]/m\mathbb{F}[x]\Rightarrow m\nmid r\Rightarrow gcd(m,r)=1$(否则,$m=gcd(m,r)\cdot\frac{m}{gcd(m,r)}$与 m 不可约矛盾！)，则由贝祖定理知，$[r]$ 可逆，即 $\mathbb{F}[x]/m\mathbb{F}[x]=$域

②⇒①根据定义立得

①⇒③设 $m=pq$，则 $[p][q]=0$，而整环无零因子，则 $[p]=0$ 或 $[q]=0\Rightarrow m\mid p$ 或 $m\mid q$，则 $\begin{cases}deg(m)=deg(p)+deg(q)\\deg(m)\leqslant deg(p)\text{ 或 }deg(m)\leqslant deg(q)\end{cases}\Rightarrow deg(p)=0\text{ 或 }deg(q)=0$

则 p 或 q 为单位，m 为不可约元

6.3.2 构造 p^d 元域

若 $\mathbb{F}=\mathbb{F}_p$，fact:∃ 不可约 d 次多项式 m

因为 $r=a_{d-1}x^{d-1}+\cdots+a_1x+a_0(a_i\in\mathbb{F}_p,\forall i)$ 共有 p^d 种取法

1)$\#\mathbb{F}[x]/m\mathbb{F}[x]=p^d$

2) 若 m 不可约，则 $\mathbb{F}[x]/m\mathbb{F}[x]$ 为 p^d 元域

例：$\mathbb{F}=\mathbb{F}_2, m=x^2+x+1$ 不可约

则 $\mathbb{F}[x]/(x^2+x+1)\mathbb{F}[x]$ 为 4 元域

6.3.3 中国剩余定理

设 $m_1,\cdots,m_n$ 两两互素，记 $m=m_1\cdots m_n\in\mathbb{F}[x]$，则

1)$\mathbb{F}[x]/m\mathbb{F}[x]\cong\mathbb{F}[x]/m_1\mathbb{F}[x]\times\cdots\times\mathbb{F}[x]/m_n\mathbb{F}[x]$

2)$(\mathbb{F}[x]/m\mathbb{F}[x])^\times\cong(\mathbb{F}[x]/m_1\mathbb{F}[x])^\times\times\cdots\times(\mathbb{F}[x]/m_n\mathbb{F}[x])^\times$

$\varphi: rmodm\mapsto(rmodm_1,\cdots,rmodm_n)$

证明过程与之前类似

另一种表述形式：方程 $\begin{cases} f \equiv r_1(modm_1) \\ \cdots \\ f \equiv r_n(modm_n) \end{cases}$ 有解，且解集为模 m 的一个同余类

6.4 其他性质

6.4.1 低次多项式的不可约性

Prop: 域上的 2 次或 3 次多项式不可约当且仅当其在域上没有零点
proof:($\Rightarrow$) : 反证，假设有零点，设 $f(a) = 0, a \in \mathbb{F}$
则 $f = q(x-a) + r$，将 x=a 带入得，$r = f(a) = 0$
则 $f(x) = q(x-a)$，故 f 可约
($\Leftarrow$) : 反证，假设可约，设 $f = f_1 f_2 (f_1, f_2 \notin \mathbb{F}) \Leftrightarrow deg(f_1), deg(f_2) \geqslant 1$
$deg(f) = 2$ 或 $3 \Rightarrow deg(f_1) = 1$ 或 $deg(f_2) = 1$
不妨设 $deg(f_1) = 1, f_1 = ax - b$
则 $f(\frac{a}{b}) = f_1(\frac{a}{b}) f_2(\frac{a}{b}) = 0$，有根！

6.4.2 余数定理

$\forall f \in \mathbb{F}[x], \forall a \in \mathbb{F}, \exists! q, s.t. f(x) = q(x)(x-a) + f(a)$
推论：$f(a) = 0 \Leftrightarrow x - a \mid f$

6.4.3 多项式的拉格朗日定理

若 $deg(f) = n$，则 f 的零点个数 $\leqslant n$
proof: 设 $a_1, \cdots, a_m$ 为 f 的零点
$f(a_1) = 0 \Rightarrow x - a_1 \mid f \Rightarrow f = (x - a_1) f_1(x)$
其中 $f_1(a_2) = f_1(a_3) = \cdots = f_1(a_m) = 0$
归纳假设：$deg(f_1) \geqslant m - 1$
则 $deg(f) = deg(f_1) + 1 \geqslant m$

6.4.4 韦达定理

$\mathbb{F}$ 为域，$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x] (a_n \neq 0)$
1) 若 f 有 n 个不同的根 $x_1, \cdots, x_n$，则 $f(x) = a_n (x - x_1) \cdots (x - x_n)$

2) 若 $f(x)=a_n(x-x_1)\cdots(x-x_n)$(可有重根)，则

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

proof:1) 因为 $x-x_i\mid f$ 且 $gcd(x-x_i,x-x_j)=1,\forall i\neq j$

所以 $(x-x_1)\cdots(x-x_n)\mid f$，设 $f(x)=g(x)(x-x_1)\cdots(x-x_n)$

由拉格朗日定理，$deg(g)=0\Rightarrow g=a_n$

所以，$f(x)=a_n(x-x_1)\cdots(x-x_n)$

2) 展开对比系数即可

例：$k=1$ 时，$\sum\limits_{i=1}^{n}x_i=-\frac{a_{n-1}}{a_n}$

$k=2$ 时，$\sum\limits_{1\leqslant i<j\leqslant n}x_ix_j=\frac{a_{n-2}}{a_n}$

$k=n$ 时，$x_1x_2\cdots x_n=\frac{a_0}{a_n}$

例：$\sum\limits_{1\leqslant i<j\leqslant p-1}ij\equiv?(modp)$

由费马小定理，$\forall x\in\mathbb{F}_p,x^{p-1}-1\equiv 0(modp)$

则 $1,2,\cdots,p-1$ 为 $x^{p-1}-1=0$ 在 $\mathbb{F}_p$ 下的 p-1 个根

由韦达定理，k=2 时，$\sum\limits_{1\leqslant i<j\leqslant p-1}ij\equiv 0(modp)$

6.4.5 根的重数

$\forall f\in\mathbb{F}[x],\forall a\in\mathbb{F},\exists m\in\mathbb{N}$ 且 $g\in\mathbb{F}[x],s.t.g(a)\neq 0$ 且

$$f(x)=(x-a)^mg(x)$$

我们称 m 为根 $x=a$ 的重数，$m=1$ 为单根，$m\geqslant 2$ 为重根

proof: 存在性: 对 f 每次提出一个 (x-a) 在有限次后停止

唯一性: 假设 $f(x)=(x-a)^mg_1(x)=(x-a)^ng_2(x)$

假设 $m\neq n$，不妨设 $m<n$，则 $g_1(x)=(x-a)^{n-m}g_2(x)$

$g(a)=(a-a)^{n-m}g_2(a)=0$，矛盾！

所以只能是 $m=n$，进一步，$g_1(x)=g_2(x)$

6.4.6 形式微商

问：如何判断给定 f 是否有重根？

Def(形式微商)：$\forall f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,(a_kx_k)'=ka_kx^{k-1}$

$f'(x)=na_nx^{n-1}+\cdots+a_1$，称 $f'(x)$ 为 $f(x)$ 的形式微商

Prop:1)$(cf)^{'}=c\cdot f^{'}\forall c\in\mathbb{F}$

2)$(f+g)^{'}=f^{'}+g^{'}$

3)$(fg)^{'}=f^{'}g+g^{'}f$

Prop:1)$(x-a)^m\mid f\overset{m\geqslant 1}{\Rightarrow}(x-a)^{m-1}\mid f^{'}$(反之不成立)

2)$gcd(f,f^{'})=1\Rightarrow f$ 无重根 (反之不成立，$\mathbb{F}=\mathbb{R},f(x)=(x^2+1)^2,f^{'}(x)=2x(x^2+1),gcd(f,f^{'})=x^2+1$ 但 f 无重根)

3)a 为 f 的重根 $\Leftrightarrow$a 为 $gcd(f,f^{'})$ 的零点 $\Leftrightarrow f(a)=f^{'}(a)=0$

4)a 为 f 的单根 $\Leftrightarrow f(a)=0,f^{'}(a)\neq 0$

proof:1) 设 $f=(x-a)^mg$

则 $f^{'}=m(x-a)^{m-1}g+(x-a)^mg^{'}=(x-a)^{m-1}(mg+(x-a)g^{'})$

所以，$(x-a)^{m-1}\mid f^{'}$

注：若 $\mathbb{F}=\mathbb{F}_p$，$m=p$，则 $mg+(x-a)g^{'}|_{x=a}=0$

2) 假设 a 为 f 的重根 $\Rightarrow(x-a)^2\mid f\overset{1)}{\Rightarrow}(x-a)\mid f^{'}$

$\Rightarrow(x-a)\mid gcd(f,f^{'})$，与 $gcd(f,f^{'})=1$ 矛盾！故命题得证

3)$(\Rightarrow)(x-a)^2\mid f\Rightarrow(x-a)\mid f^{'}$

$(\Leftarrow)$ 已知 $f(a)=f^{'}(a)=0\Rightarrow$ 设 $f=(x-a)f_1$

则 $f^{'}=f_1^{'}(x-a)+f_1\overset{f^{'}(a)=0}{\Rightarrow}f_1(a)=0$

$x-a\mid f_1(x)\Rightarrow(x-a)^2\mid f(x)$，则 a 为 f 的重根

4)$(\Rightarrow)$: 设 $f=(x-a)g,g(a)\neq 0$

则 $f^{'}=g+(x-a)g^{'}\Rightarrow f^{'}(a)=g(a)\neq 0$

$(\Leftarrow):\exists g,s.t.f=(x-a)g$，则 $f^{'}=g+(x-a)g^{'}$

$f^{'}(a)=g(a)\neq 0\Rightarrow(x-a)||f\Rightarrow$a 为单根

例：$\mathbb{F}=\mathbb{F}_p,f=x^p-x,f^{'}=px^{p-1}-1=-1,gcd(f,f^{'})=1,f$ 无重根

例：$\mathbb{F}=\mathbb{F}_p,f=x^p-2,f^{'}=0,gcd(f,f^{'})=f$

$2^p=2,x^p-2=x^p-2^p=(x-2)^p$(模 p 意义下) $\Rightarrow 2$ 为 f 的 p 重根

6.4.7 代数学基本定理

Def(代数封闭域): 称域 $\mathbb{F}$ 是代数封闭的，若 $\forall f\in\mathbb{F}[x]\backslash\mathbb{F},\exists a\in\mathbb{F},s.t.f(a)=0$

Prop: 若 $\mathbb{F}$ 为代数封闭域，则 $gcd(f,f^{'})=1\Leftrightarrow f$ 无重根

Thm(代数学基本定理):$\mathbb{C}$ 为代数封闭域

推论：$\forall f\in\mathbb{C}[x],gcd(f,f^{'})=1\Leftrightarrow f$ 无重根

推论：$f \in \mathbb{C}[x]$，则

1)f 不可约 $\Leftrightarrow deg(f)=1$

2)$\exists x_1,\cdots,x_s \in \mathbb{C}, \alpha_1,\cdots,\alpha_s \in \mathbb{N}$，使得

$f(x)=a_n(x-x_1)^{\alpha_1}\cdots(x-x_s)^{\alpha_s}$，其中 $\alpha_1+\cdots+\alpha_s=deg(f)$

推论：$p,f\in\mathbb{R}[x]$，则 1)p 不可约 $\Leftrightarrow deg(p)=1$ 或 $\begin{cases} p=ax^2+bx+c(a\neq 0) \\ b^2-4ac<0 \end{cases}$

2)$\exists p_1,\cdots,p_s, s.t. f=p_1\cdots p_s$，其中 p_i 为一次多项式或 $\begin{cases} p_i=ax^2+bx+c(a\neq 0) \\ b^2-4ac<0 \end{cases}$

proof:1)($\Rightarrow$) : 不妨设 $deg(p)>1$ 且 p 不可约，则 $\exists a,b\in\mathbb{R}, s.t. f(a+bi)=0$

$\Rightarrow b\neq 0$，否则 $p(a)=0\Rightarrow x-a \mid p \Rightarrow p=(x-a)\cdot\frac{p}{x-a}$，矛盾

Lemma: 若 $f(x)=a_nx^n+\cdots+a_1x+a_0, f(a+bi)=0$，则 $f(a-bi)=0$

由引理，(在 $\mathbb{C}[x]$ 上) 我们有 $p(a-bi)=0\Rightarrow \begin{cases} x-(a+bi)\mid p \\ x-(a-bi)\mid p \end{cases}$

$\Rightarrow (x-(a+bi))(x-(a-bi))=x^2-2ax+a^2+b^2 \mid p$

在 $\mathbb{R}$ 上有 $x^2-2ax+a^2+b^2 \mid p \Rightarrow$ 设 $p(x)=(x^2-2ax+a^2+b^2)p_1(x)$

$p(x)$ 不可约 $\Rightarrow p_1(x)\in\mathbb{R}\backslash\{0\}$

例：在 $\mathbb{R}$ 上因式分解 x^4+1

法 1(技巧性较强):$x^4+1=x^4+2x^2+1-2x^2=(x^2+1)^2-(\sqrt{2}x)^2=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$

法 2: 算出四个复根 $x=\frac{\sqrt{2}}{2}(1\pm i),\frac{\sqrt{2}}{2}(-1\pm i)$

$x^4+1=(x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(1-i))(x-\frac{\sqrt{2}}{2}(-1+i))(x-\frac{\sqrt{2}}{2}(-1-i))=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$

6.5 整系数多项式环

6.5.1 基本定义和定理

Def:$\mathbb{Z}[x]=\{a_nx^n+\cdots+a_0 | a_i\in\mathbb{Z},\forall i\}$

Thm:$\mathbb{Z}[x]$ 为唯一分解整环 (UFD)

更一般地，$\mathcal{R}=UFD\Rightarrow\mathcal{R}[x]=UFD$

Def(不可约元):$\mathcal{R}$ 整环，称 $p\in\mathcal{R}$ 为不可约元，若 1)$p\notin\mathcal{R}^\times, p\neq 0$ 2)$p=ab\Rightarrow a\in\mathcal{R}^\times$ 或 $b\in\mathcal{R}^\times$，如 $2x+1, x^2-2$ 在 $\mathbb{Z}[x]$ 上为不可约元

例：$4x+2 \in \mathbb{Z}[x]$ 可约？

答：$4x+2=2(2x+1)$，可约！

更一般地，$\forall f \in \mathbb{Z}[x], f$ 不可约 $\Rightarrow \pm f$ 为素数或 $deg(f) \geqslant 1$ 且 f 的所有系数最大公因子为 1

Def(单位): 可逆元，$\mathcal{R}[x]^{\times}=\mathcal{R}^{\times}$，如 $\mathbb{Z}[x]^{\times}=\{\pm 1\}$

• $\mathbb{Z}[x]$ 中不是所有多项式都有带余除法！

如 $f=x^2, g=2x+1$，若 $\exists q, r(deg(r)<deg(g)), s.t. x^2=(2x+1)q+r$

显然，$deg(q)=1$，设 $q=mx+n, m, n, r \in \mathbb{Z}$

对比二次项系数，$\Rightarrow 2m=1$，矛盾！

• $\mathbb{Z}[x]$ 不是主理想整环!

如 $I=(2,x)=\{2f+xg|f,g \in \mathbb{Z}[x]\}$

假设 I 为主理想，设 $I=(2,x)=(h)$

一方面，$2 \in (2,x)=(h) \Rightarrow \exists s, s.t. hs=2 \Rightarrow deg(h)=deg(s)=0 \Rightarrow h=\pm 1, \pm 2$

另一方面，$x \in (2,x)=(h)$

则 $\exists t, s.t. x=ht \Rightarrow h=\pm 1$

所以 $(2,x)=(1)$ 或 $(2,x)=(-1) \Rightarrow \exists f, g, s.t. 1=2f+xg$，对比常数项，显然矛盾！

实际上，(p,x)(p 为整数) 均不是主理想，证法类似

6.5.2 带余除法

Def:$\forall f \in \mathbb{Z}[x], \forall g \in \mathbb{Z}[x], g$ 首一，则 $\exists q, r, s.t. f=qg+r$，其中 $deg(r)<deg(g)$

proof:(存在性) 记 $I:=\{f(x)-a(x)g(x)|a(x) \in \mathbb{Z}[x]\}$

设 r 为 I 中次数最小的非零多项式，则 r 即为所求，不妨设 $r(x)=f(x)-g(x)q(x)$

假如 $deg(g)<deg(r)$，取 $r^{'}(x)=r(x)-c(r(x))g(x)x^{deg(r(x))-deg(g(x))}$

$c(r(x))$ 为 $r(x)$ 的首项系数

则 $deg(r^{'})<deg(r), r^{'}(x) \in I$，矛盾！

6.5.3 本原多项式

Def:$\forall f(x) \in \mathbb{Z}[x]$，称 f 为本原多项式，若 f 的所有系数最大公因子为 1

接下来我们要讨论哪些本原多项式不可约

6.5.4 容度

$\forall a \in \mathbb{Q}[x]\backslash\{0\}, \exists! c \in \mathbb{Q} \& a_1 \in \mathbb{Z}[x], s.t. a = ca_1$

其中 a_1 为首项系数为正的本原多项式，则称 c 为 a 的容度

proof:(存在性) 取 $N \in \mathbb{Z}\backslash\{0\}, s.t. Na = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Z}[x]$ 且 $\alpha_n > 0$

令 $\alpha := gcd(\alpha_0, \alpha_1, \cdots, \alpha_n) \in \mathbb{Z}$

$\Rightarrow a_1 = \frac{Na}{\alpha}$ 为首项系数为正的本原多项式

(唯一性) 若 $a = c_2 a_1 = c_1 a_2 (a_1, a_2$ 本原且首系数大于零)，$\exists M \in \mathbb{N}, s.t. Mc_1, Mc_2 \in \mathbb{Z}$

记 $d = gcd(Mc_1, Mc_2) \Rightarrow \frac{c_1 M}{d} a_1 = \frac{c_2 M}{d} a_2$

$\Rightarrow \frac{c_1 M}{d} \mid \frac{c_2 M}{d} a_2$ 的所有系数

a_2 本原 $\Rightarrow \frac{c_1 M}{d} = \pm 1$，同理，$\frac{c_2 M}{d} = \pm 1$

所以，$c_1 = \pm c_2$，由 a_1, a_2 首项系数大于零之，c_1, c_2 同号，即 $c_1 = c_2$

6.5.5 高斯引理

设 $f, g, h \in \mathbb{Z}[x]\backslash\{0\}$，若 $f = gh$，则 f 本原 $\Leftrightarrow g, h$ 本原

proof:($\Rightarrow$) : 反证，不妨设 g 非本原，则 $\exists c \in \mathbb{Z}\backslash\{0, \pm 1\}$

$c \mid g \Rightarrow c \mid f \Rightarrow c \mid f$ 的所有系数 $\Rightarrow f$ 非本原

($\Leftarrow$) : 假设 $f \neq$ 本原，则 $\exists$ 素数 p，使得 p 整除 f 的所有系数

考虑环同态 $\varphi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x], a_n x^n + \cdots, + a_1 x + a_0 \mapsto \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0}$

则对上述 $f, \varphi_p(f) = 0 \Rightarrow \varphi_p(g) \cdot \varphi_p(h) = 0 \overset{\text{整环无零因子}}{\Longrightarrow} \varphi_p(g) = 0$或$\varphi_p(h) = 0 \Rightarrow g$ 或 h 非本原，矛盾！

6.5.6 $\mathbb{Z}[x]$ 与 $\mathbb{Q}[x]$ 的联系

Thm:$f \in \mathbb{Z}[x]$ 本原，则 f 在 $\mathbb{Z}[x]$ 中不可约 $\Leftrightarrow f$ 在 $\mathbb{Q}[x]$ 中不可约

proof:($\Rightarrow$) : 设 $f = gh$，其中 $g, h \in \mathbb{Q}[x]$

则 $\exists$ 首项为正数的本原多项式 g_1, h_1，使得 $g = c(g)g_1, h = c(h)h_1$

所以，$f = c(g)c(h)g_1 h_1$，由 f 不可约知，$c(g)c(h) = \pm 1 \Rightarrow f = \pm g_1 h_1$ 在 $\mathbb{Z}[x]$ 中不可约

$\Rightarrow g_1 = \pm 1$ 或 $h_1 = \pm 1$

$\Rightarrow g = c(g)g_1 \in \mathbb{Q}^\times$ 或 $h = c(h)h_1 \in \mathbb{Q}^\times \Rightarrow f$ 在 $\mathbb{Q}[x]$ 中不可约

($\Leftarrow$) : 设 $f = gh (g, h \in \mathbb{Z}[x])$，则 g, h 本原

f 在 $\mathbb{Q}[x]$ 中不可约 $\Rightarrow g\in\mathbb{Q}^\times$ 或 $h\in\mathbb{Q}^\times\Rightarrow g=\pm1$ 或 $h=\pm1$

f 在 $\mathbb{Z}[x]$ 中不可约

推论：$f\in\mathbb{Z}[x]$ 不可约 $\Leftrightarrow\pm f$ 为素数或 $\begin{cases}f\text{ 本原}\\ f\text{ 在 }\mathbb{Q}[x]\text{ 中可约}\end{cases}$

6.5.7 $\mathbb{Z}[x]$ 是唯一分解整环 (UFD)

Thm:$\forall f\in\mathbb{Z}[x]\backslash\{0\}$，则 f 可唯一地 (不计顺序) 写成 $f=c\pi_1\pi_2\cdots\pi_r$，其中 $c=\pm1$ 为 f 的首项系数符号，$\pi_1,\cdots,\pi_r$ 为素数或首项系数为正的本原多项式

proof:(存在性)$f=c(f)f_1$，其中 $c(f)=\pm p_1^{\alpha_1}\cdots p_s^{\alpha_s},f_1\in\mathbb{Z}[x]$

将 f_1 看作 $\mathbb{Q}[x]$ 中元素，则 $f_1=g_1\cdots g_r(g_i\in\mathbb{Q}[x],g_i$ 在 $\mathbb{Q}[x]$ 中不可约)

而 $g_i=c(g_i)g_i^{'}(g_i^{'}$ 本原且首系数大于零)

$\Rightarrow f_1=c(g_1)\cdots c(g_r)g_1^{'}\cdots g_r^{'}$

$\Rightarrow c(f_1)=c(g_1)\cdots c(g_r)$，而 f_1 本原，$c(f_1)=\pm1$

$\Rightarrow f_1=\pm g_1^{'}\cdots g_r^{'}$

$\Rightarrow f=\pm p_1^{\alpha_1}\cdots p_s^{\alpha_s}g_1^{'}\cdots g_r^{'}$

(唯一性) 假设 $f=c\pi_1\pi_2\cdots\pi_r=c^{'}\pi_1^{'}\pi_2^{'}\pi_r^{'}$

不妨将 f 拆为两部分 $c\pi_1\cdots\pi_\alpha$、$\pi_{\alpha+1}\cdots\pi_r$，其中前者为系数，后者为本原多项式

f 的两种拆分相当于系数的两种重排和本原多项式的两种重排 (用归纳法)，故唯一性得证

更一般地，若 $\mathcal{R}=UFD$，则 $\mathcal{R}[x]=UFD$

Prop:$f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x](n\geqslant1,a_n\neq0)$，若 $x=\frac{q}{p}(gcd(p,q)=1)\in\mathbb{Q}$ 为 f 的根，则 $q\mid a_0,p\mid a_n$

proof: 若 $x=\frac{q}{p}(gcd(p,q)=1)$ 是 $f(x)$ 的一个有理根，则 $px-q$ 为本原多项式，且在 $\mathbb{Z}[x]$ 中，$px-q\mid f(x)$，设 $f(x)=(px-q)g(x),g(x)=b_{n-1}x^{n-1}+\cdots+b_1x+b_0\Rightarrow f(x)=pb_{n-1}x^n+\cdots+qb_0\Rightarrow q\mid a_0,p\mid a_n$

例：$3x^3+x+7$ 是否有有理根?

若 $a=\frac{q}{p}(gcd(p,q)=1)$ 为有理根，则 $q\in\{\pm1,\pm7\},p\in\{\pm1,\pm3\}$

将 $x=\pm1,\pm\frac{1}{3},\pm\frac{7}{3},\pm7$ 逐一带入验证即可

6.5.8 艾森斯坦判别法

p 为素数，$f=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x](a_n\neq0,n\geqslant1)$

若 $p\nmid a_n,(p\mid a_{n-1},\cdots,p\mid a_1),p||a_0$，则 f 在 $\mathbb{Q}[x]$ 中不可约

proof: 假设 f 在 $\mathbb{Q}[x]$ 上可约，设 $f=gh(g,h\in\mathbb{Q}[x],g=c(g)g_1,h=c(h)h_1)$，其中 g_1,h_1 为首项系数为正的本原多项式 $\Rightarrow f=c(g)c(h)g_1h_1$

考虑环同态 $\varphi_p:\mathbb{Z}[x]\to\mathbb{F}_p[x],a_nx^n+\cdots,+a_1x+a_0\mapsto\overline{a_n}x^n+\cdots+\overline{a_1}x+\overline{a_0}$

$\varphi_p(f)=\varphi_p(c(g)c(h))\varphi_p(g_1)\varphi_p(h_1)$，其中 $\varphi_p(c(g)c(h))$ 为常数

由条件，$\varphi_p(f)=a_nx^n\Rightarrow\varphi_p(g_1)\mid a_nx^n,\varphi_p(h_1)\mid a_nx^n$

假设 $deg(g_1)\geqslant 1\&deg(h_1)\geqslant 1\Rightarrow lc(f)=c(f)lc(g_1)lc(h_1)$(lc(f) 表示 f 的首项系数)

由 $p\nmid a_n$ 知，$p\nmid lc(g_1)\&p\nmid lc(h_1)$

$$\Rightarrow\begin{cases}deg(g_1)=deg(\varphi_p(g_1))\\deg(g_2)=deg(\varphi_p(g_2))\end{cases}\Rightarrow\varphi_p(g_1)=bx^{d_1},\varphi_p(g_2)=cx^{d_2},d_1+d_2=n$$

不妨设 $g_1=b_{d_1}x^{d_1}+\cdots+b_1x+b_0,h_1=c_{d_2}x^{d_2}+\cdots+c_1x+c_0$

由环同态知，$p\mid b_0,p\mid c_0$，而 $a_0=c(f)b_0c_0\Rightarrow p^2\mid a_0$，矛盾！

例：分圆多项式不可约

$\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$

作变量替换，$x=T+1$，仍保持其不可约性

这是因为 $f(x)=g(T+1)(aT+b,a\neq 0$均可$),f(x)$ 不可约 $\Leftrightarrow g(T)$ 不可约

则 $\Phi_p(T+1)=\frac{(T+1)^p-1}{(T+1)-1}=\binom{p}{p}T^{p-1}+\binom{p}{p-1}T^{p-2}+\cdots+\binom{p}{2}T+\binom{p}{1}$

满足艾森斯坦判别法的条件，故不可约

7 对称群与对称多项式

7.1 对称群

$A\neq\varnothing,S_A:=\{\sigma:A\to A|\sigma$为双射$\}$ 在映射复合下构成群

称 $(S_A,\circ)$ 为 A 的对称群，S_A 的单位元为恒等映射

Prop: 若 $\#A=\#B>0$，则 $(S_A,\circ)\cong(S_B,\circ)$，其中，恒等映射 id 为单位元

因此，我们只需考虑 $A=\{1,2,\cdots,n\}$ 即可

Def:$\forall n\geqslant 1$，$S_n=S_{\{1,2,\cdots,n\}}$ 为 n 阶对称群，称 S_n 中的元素为 $\{1,2,\cdots,n\}$ 的置换

Prop:1)$\#S_n=n!$

2)$n\geqslant 3$，S_n 非交换

7.1.1 简化表达

设 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&4&2&3&5&1\end{pmatrix}$

其中，$1\mapsto 6\mapsto 1, 2\mapsto 4\mapsto 3\mapsto 2, 5\mapsto 5$

则 $\sigma=(16)(243)(5)$，括号内只有一个数可以省略，即

$\sigma=(16)(243)$

例：$S_3=\{id,(12),(13),(23),(123),(132)\}$

7.1.2 轮换

• $(i_1,i_2,\cdots,i_k)\in S_n$ 称为 k 轮换，称 2 轮换为对换

Prop:$(i_1,i_2,\cdots,i_k)^{-1}=(i_k,i_{k-1},\cdots,i_1)$(颠倒方向)

Def: 若 $\{i_1,i_2,\cdots,i_k\}\cap\{j_1,j_2,\cdots,j_l\}=\varnothing$，$\sigma=(i_1,i_2,\cdots,i_k),\tau=(j_1,j_2,\cdots,j_l)$

则称 σ 与 τ 不相交，否则称它们相交

Prop: 若轮换 σ 与 τ 不相交，则 $\sigma\circ\tau=\tau\circ\sigma$

proof: 即证 $\forall t,\sigma\circ\tau(t)=\tau\circ\sigma(t)$

$1^\circ t\notin\{i_1,i_2,\cdots,i_k\}\cup\{j_1,j_2,\cdots,j_l\}$

则 $\sigma\circ\tau(t)=\tau\circ\sigma(t)=t$

2° 不妨设 $t\in\{i_1,i_2,\cdots,i_k\}\&t\notin\{j_1,j_2,\cdots,j_l\}$

则 $\sigma\circ\tau(t)=\sigma(t)$

$\tau\circ\sigma(t)=\tau(\sigma(t))=\sigma(t)$(因为 $\sigma(t)\notin\{j_1,j_2,\cdots,j_l\}$)

7.1.3 用对换表示对称群元素

Thm:$\forall\sigma\in S_n$，则存在两两不交的轮换 $\sigma_1,\cdots,\sigma_s,s.t.\sigma=\sigma_1\sigma_2\cdots\sigma_s$ 且表达在除 1 轮换下唯一

证明过程略，详见老师讲义

例：$(15)(24)(13)=(135)(24)$

$(1234)(3456)=(13)(26)(45)$

7.1.4 型

例:$S_4=\{(1)\quad 4=1+1+1+1$

$(12),(13),(14),(23),(24),(34)\quad 4=2+1+1$

$(123),(132),(124),(142),(134),(143),(234),(243)\quad 4=3+1$

$(12)(34),(13)(24),(14)(23)\quad 4=2+2$

$(1234),(1243),(1324),(1342),(1423),(1432)\}\quad 4=4$

例：$5=1+1+1+1+1=2+1+1+1=3+1+1=2+2+1=3+2=4+1=5$，共 7 种拆分

类似地，我们记 n 的拆分数为 $P(n)\Rightarrow P(2)=2,P(3)=3,P(4)=5,P(5)=7\cdots$

更一般地，有 $n=\lambda_1\cdot 1+\lambda_2\cdot 2+\cdots+\lambda_n\cdot n(\lambda_1,\lambda_2,\cdots,\lambda_n\geqslant 0)$

Def:$\sigma\in S_n$，若 σ 写为两两不交轮换乘积中 k 轮换的个数为 λ_k

则称 σ 的型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$

例：S_4 中，(1) 的型为 1^4，(12) 的型为 1^22^1，(123) 的型为 1^13^1，(12)(34) 的型为 2^2，(1234) 的型为 4^1

Prop:1)$\forall\sigma_1,\sigma_2\in S_n$，$\sigma_1$ 与 σ_2 共轭 $\Leftrightarrow\sigma_1,\sigma_2$ 有相同的型

2)S_n 中恰有 $P(n)$ 个共轭类

proof:1)$(\Rightarrow)\forall\sigma=(i_1,\cdots,i_{k_1})(j_1,\cdots,j_{k_2})\cdots$

$\forall\tau\in S_n,\tau\circ\sigma\circ\tau^{-1}$ 为 σ 的共轭

考虑 $\tau\circ\sigma\circ\tau^{-1}(\tau(i_1))=\tau\circ\sigma(i_1)=\tau(i_2)$

$\tau\circ\sigma\circ\tau^{-1}(\tau(i_k)=\tau\circ\sigma(i_k)=\tau(i_1)$

$\tau\circ\sigma\circ\tau^{-1}(\tau(j_1)=\tau\circ\sigma(j_1)=\tau(j_1)=j_2$

所以依此类推，$\tau\circ\sigma\circ\tau^{-1}=(\tau(i_1),\cdots,\tau(i_{k_1}))(\tau(j_1),\cdots,\tau(j_{k_2}))\cdots$

因此，σ 与 $\tau\circ\sigma\circ\tau^{-1}$ 有相同的型

$(\Leftarrow)\forall\sigma_1,\sigma_2\in S_n,\sigma_1,\sigma_2$ 有相同的型

设 $\sigma_1=(i_{11},\cdots,i_{1k_1})(i_{21},\cdots,i_{2k_2})\cdots$，$\sigma_2=(j_{11},\cdots,j_{1k_1})(j_{21},\cdots,j_{2k_2})$

构造 $\tau=\begin{pmatrix}i_{11}&\cdots&i_{1k_1}&i_{21}&\cdots&i_{2k_2}&\cdots\\ j_{11}&\cdots&j_{1k_1}&j_{21}&\cdots&j_{2k_2}&\cdots\end{pmatrix}$

则 $\tau\sigma_1\tau^{-1}=\sigma_2$

7.1.5 奇置换与偶置换

Prop:1)$(i_1,\cdots,i_k)=(i_1,i_k)(i_1,i_{k-1})\cdots(i_1,i_2)$

2)$(ij)\overset{i\leq j}{=}(i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)(j-2,j-1)\cdots(i+1,i+2)(i,i+1)$

3)$(ij)=(1,i)(i,j)(1,i)$

4)S_n 可由 $(1,2),(1,3)\cdots,(1,n)$ 生成

5)S_n 可由 $(1,2),(2,3),\cdots,(n-1,n)$ 生成

Thm: 将一个置换写成对换乘积时，对换个数的奇偶性不依赖于写法

Def: 偶置换：偶数个对换的乘积；奇置换：奇数个对换的乘积

Prop: 偶 $\circ$ 偶 $=$ 偶，偶 $\circ$ 奇 $=$ 奇，奇 $\circ$ 奇 $=$ 偶

推论：$\exists!$ 群同态 $\varepsilon: S_n \to \{\pm 1\}$，使得 ε(对换) $=-1$

7.1.6 交错数

Def:$\forall \sigma \in S_n$，$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

$n(\sigma) = \#\{(\sigma(i),\sigma(j)) | i<j 但 \sigma(i)>\sigma(j)\}$，称 $n(\sigma)$ 为 σ 的交错数

例：$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}$

$n(\sigma) = \#\{(5,3),(5,4),(6,3),(6,4)\} = 4$

例：$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 6 & 4 \end{pmatrix}$

$n(\sigma) = \#\{(5,3),(5,4),(6,4)\} = 3$

由上面两例可以看出，对调一组数，$n(\sigma) \pm 1$

Prop:σ 可以写成 $n(\sigma)$ 个对换的乘积

proof:$n(\sigma)=0$，此时 $\sigma = id$，显然

假设 $n(\sigma)<k$ 时均成立，现证明 $n(\sigma)=k$ 时也成立

若 $n(\sigma)=k>0$，则 $\exists i, s.t. \sigma(i)>\sigma(i+1)$，否则，$\sigma = id$

$\tau = (\sigma(i),\sigma(i+1)) \circ \sigma$

则 $n(\tau) = n(\sigma)-1 \Rightarrow \tau$ 可写成 k-1 个对换的乘积

$\sigma = (\sigma(i),\sigma(i+1)) \circ \sigma$ 可写为 k 个对换的乘积

例：$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix}$ 判断其为奇置换还是偶置换

法 1：$\sigma = (16)(243), typr(\sigma) = 1^1 2^1 3^1 \Rightarrow$ 奇置换

法 2：算逆序数 $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5) = (5,3,1,1,1) \Rightarrow \sum \alpha_i = 11 \Rightarrow$ 奇置换

7.2 交错群

7.2.1 定义及举例

Def:n 阶交错群 $A_n :=$ {偶置换}

Prop:1)$A_n \lhd S_n$，$\#A_n = \frac{n!}{2}$

2)$K_4 := \{id, (12)(34), (13)(24), (14)(23)\}, K_4 \lhd S_4, K_4 \lhd A_4$

proof:1)$\forall \sigma \in A_n, \tau \in S_n$，$\tau \circ \sigma \circ \tau^{-1}$ 也为偶置换

$(i, i+1)A_n \sqcup A_n = S_n$

2)K_4 中逆元均为自身，且有 $(12)(34) \circ (13)(24) = (14)(23)$

$(12)(34) \circ (14)(23) = (13)(24)$

$(14)(23) \circ (13)(24) = (12)(34)$

按照正规子群的定义验证即可

7.2.2 单群

Def: 若群 $G \neq 1$ 无非平凡正规子群，则称 G 为单群 (single group)

Prop:$G \neq 1$ 为交换群，则 G 为单群 $\Leftrightarrow \#G$ 为素数

proof:($\Leftarrow$) 显然 (群论中的拉格朗日定理)

($\Rightarrow$)$\forall g \in G \backslash \{1\} \Rightarrow < g > \lhd G$，而交换群的任意子群均为正规子群，与单群的定义矛盾，即 G 没有非平凡子群，由群论中的拉格朗日定理知，$\#G =$ 素数

Thm:$A_n (n \geqslant 5)$ 为单群

fact:A_5 为最小的非交换单群

7.3 交换多项式

7.3.1 定义及举例

Def: 称 $f \in \mathcal{R}[x_1 x_2 \cdots x_n]$ 为对称多项式，若 $\forall \sigma \in S_n$，皆有

$$f(x_{\sigma_1}, x_{\sigma_2}, \cdots, x_{\sigma_n}) = f(x_1, x_2, \cdots, x_n)$$

即 $\sigma(f) = f, \forall \sigma \in S_n$，也就是说，$x_1, \cdots, x_n$ 地位等价

例：1)$f = x_1^k + \cdots + x_n^k$

2)$f = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - S_1 x^{n-1} + \cdots + (-1)^n S_n$

韦达定理：$S_1 = x_1 + x_2 + \cdots + x_n$

$S_2 = \sum_{1 \leqslant i < j \leqslant n} x_i x_j$

$S_n = x_1 x_2 \cdots x_n$

称多项式 $S_k, \forall k$ 为初等对称多项式

Thm: 任意对称多项式均可由初等对称多项式通过 $+, -, \cdot$ 组合出来

7.3.2 判别式

称 $D_f = D(x_1, \cdots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2$ 为 $f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$ 的判别式

例：$f = x^2 + bx + c, \Delta = b^2 - 4a$

$f = x^3 + ax + b, \Delta = -4a^3 - 27b^2$

Prop:$\Delta = 0 \Leftrightarrow f$ 有重根