

§4.2 几类特殊的环

欧几里得环、唯一因子分解环、整数剩余类环、有限除环

主理想整环 PID (principal ideal domain): 整环 R 称为 PID. 如果

其所有理想都是主理想, 即所有理想有形式 Ra , $a \in R$.

欧几里得环 ED (Euclidean domain): 整环 R 称为欧几里得环如果

$\exists \delta: R \setminus \{0\} \rightarrow \mathbb{Z}_{>0} = \{n \in \mathbb{Z} \mid n > 0\}$ 满足

$$E1) \forall a, b \in R \setminus \{0\}, \delta(ab) \geq \delta(a)$$

$$E2) \forall a \in R, b \in R \setminus \{0\}, \exists q, r \in R \text{ s.t. } a = qb + r \text{ 其中 } r = 0 \text{ 或 } \delta(r) < \delta(b)$$

例: $R = \mathbb{Z}$, $\delta: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z}_{>0}$
 $n \rightarrow |n|$

$R = P[x]$, $\delta: R \setminus \{0\} \rightarrow \mathbb{Z}_{>0}$ 其中 P 为域
 $f \rightarrow \deg(f)$

欧几里得环上存在带余除法: $\forall a_1 \in R, a_2 \in R \setminus \{0\}$.

$$a_1 = q_1 a_2 + a_3 \quad \delta(a_3) < \delta(a_2)$$

$$a_2 = q_2 a_3 + a_4 \quad \delta(a_4) < \delta(a_3)$$

$\vdots$

$$a_{n-1} = q_{n-1} a_n + 0$$

命题1: 欧几里得环是 PID.

证: 设 $I \subseteq R$ 为理想. 若 $I = \{0\}$ 则 $I = \langle 0 \rangle$, 无需证明. 设 $I \neq \{0\}$.

令 $m = \min \{ \delta(b) \mid b \in I \setminus \{0\} \}$. 设 $a \in I$ 满足 $\delta(a) = m$.

$\forall b \in I, \exists q, r \in R$ s.t. $b = qa + r$ 其中 $r = 0$ 或 $\delta(r) < \delta(a)$.

$\therefore \delta(a)$ 极小 $\therefore r = 0 \Rightarrow b \in Ra \Rightarrow I = Ra$ $\square$

命题2: 设 R 为带余除法的欧几里得环, $u \in R$. 则

$$\delta(u) = \delta(1) \Leftrightarrow u \in U(R) \Leftrightarrow \delta(ux) = \delta(x), \forall x \in R \setminus \{0\}.$$

①
②
③

证: $\forall a \in R \setminus \{0\}, \delta(a) = \delta(1 \cdot a) \geq \delta(1)$

① $\Rightarrow$ ② $\exists q, r \in R$ s.t. $1 = qu + r$ 其中 $r = 0$ 或 $\delta(r) < \delta(u)$

若 $r \neq 0$ 则 $\delta(r) \geq 1 = \delta(u) \therefore r = 0 \Rightarrow u \in U(R)$

② $\Rightarrow$ ③ $u \in U(R) \Rightarrow \exists u^{-1} \in R$ s.t. $u^{-1}u = 1$.

$$\delta(x) = \delta(u^{-1}ux) \geq \delta(ux) \geq \delta(x) \Rightarrow \delta(ux) = \delta(x)$$

③ $\Rightarrow$ ① 令 $x = 1$. $\square$

设 R 为整环, $p \in R \setminus \{0\}$ 称为素元 如果 $p \notin U(R)$ 且若 $p = ab$

其中 $a, b \in R$, 则 $a \in U(R)$ 或 $b \in U(R)$.

记号: $\beta | \alpha := \exists b \in R$ s.t. $\alpha = \beta b$.

②

命题3: 设 R 为主理想整环, 则 p 为素元 $\Leftrightarrow R_p$ 为极大理想

$$\textcircled{1} \Leftrightarrow \forall a, b \in R, p|ab \Rightarrow p|a \text{ 或 } p|b \quad \textcircled{3}$$

证: $\textcircled{1} \Rightarrow \textcircled{2}$ 设 $I \subseteq R$ 为理想且 $R_p \subseteq I$. 则 $I = Rb, b \in R$.

$$\exists a \in R \text{ s.t. } p = ab \Rightarrow a \in U(R) \text{ 或 } b \in U(R) \Rightarrow R_p \text{ 为极大理想}$$

$$R_p = I \Leftarrow \Rightarrow I = R$$

$$\textcircled{2} \Rightarrow \textcircled{3} \text{ 设 } p|a. \text{ 则 } a \notin R_p \Rightarrow R_p \subsetneq \langle p, a \rangle \Rightarrow \langle p, a \rangle = R$$

$$\Rightarrow \exists u, v \in R \text{ s.t. } up + va = 1 \Rightarrow ubp + vab = b \in R_p \Rightarrow p|b$$

$$\textcircled{3} \Rightarrow \textcircled{1} \text{ 设 } p = ab, a, b \in R. \text{ 则 } p|a \text{ 或 } p|b$$

$$p|a \Rightarrow \exists c \in R \text{ s.t. } a = pc \Rightarrow p = pcb \Rightarrow bc = 1 \Rightarrow b \in U(R)$$

$$\text{同理 } p|b \Rightarrow a \in U(R) \Rightarrow p \text{ 为素元} \quad \square$$

定理1: 高斯整数环 $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$ 是欧几里得环.

证: $\because \mathbb{Z}[i] \subseteq \mathbb{C} \therefore \mathbb{Z}[i]$ 是整环.

$$\text{定义映射: } \delta: \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{Z}_{>0} \quad \forall a, b \in \mathbb{Z}[i] \setminus \{0\}.$$

$$m + ni \longrightarrow m^2 + n^2 \quad \delta(ab) = \delta(a)\delta(b)$$

$$\delta(b) \geq 1$$

$$\therefore \delta(ab) \geq \delta(a) \quad E1) \text{ 满足}$$

$$\text{设 } a \in \mathbb{Z}[i], b \in \mathbb{Z}[i] \setminus \{0\}, \text{ 记 } ab^{-1} = \alpha + \beta i, \alpha, \beta \in \mathbb{Q}.$$

$$\text{令 } k, l \in \mathbb{Z} \text{ s.t. } |\alpha - k| \leq \frac{1}{2}, |\beta - l| \leq \frac{1}{2}, \text{ 记 } q = k + li. \text{ 则}$$

$$a = b(\alpha + \beta i) = b[(\alpha - k) + (\beta - l)i + q] = bq + b[(\alpha - k) + (\beta - l)i]$$

$$\delta(b[(\alpha - k) + (\beta - l)i]) = \delta(b)[(\alpha - k)^2 + (\beta - l)^2] \leq \frac{1}{2}\delta(b) < \delta(b)$$

$$\therefore E2) \text{ 满足} \quad \square$$

$$\text{由命题2: } u \in U(\mathbb{Z}[i]) \Leftrightarrow \delta(u) = \delta(1) = 1. \quad u = m + ni$$

$$\Leftrightarrow m^2 + n^2 = 1 \Leftrightarrow u = \pm 1, \pm i$$

$$\therefore U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}.$$

应用: 素数的平方和分解

命题4: 若素数 p 在 $\mathbb{Z}[i]$ 中是可约的, 则 $p = m^2 + n^2, m, n \in \mathbb{Z}$.

$$\text{证: 设 } p = \prod_{i=1}^s p_i, s > 1, p_i \text{ 为 } \mathbb{Z}[i] \text{ 中的素元. 则 } p^2 = \delta(p) = \prod_{i=1}^s \delta(p_i)$$

$$\because \delta(p_i) \in \mathbb{Z}_{>0}. \therefore s = 2, \delta(p_1) = \delta(p_2) = p.$$

$$\text{设 } p_1 = m + ni, m, n \in \mathbb{Z}. \text{ 则 } p = \delta(p_1) = m^2 + n^2. \quad \square$$

定理2: 素数 p 在 $\mathbb{Z}[i]$ 中是素元 $\Leftrightarrow p = 4k - 1$.

证: ($\Leftarrow$) (反证) 设 p 在 $\mathbb{Z}[i]$ 中可约. 由命题4, $p = m^2 + n^2, m, n \in \mathbb{Z}$.

$\because \forall t \in \mathbb{Z}, t^2 \equiv 0, 1 \pmod{4}$

$\therefore p = m^2 + n^2 \equiv 0, 1, 2 \pmod{4}$, 又 $\because p = 4k-1 \geq 3 \therefore p \equiv 1 \pmod{4}$

但 $p = 4k-1 \Rightarrow p \equiv 3 \pmod{4}$ 矛盾

($\Rightarrow$) p 为素数且 p 在 $\mathbb{Z}[i]$ 中不可约 $\Rightarrow p \equiv 1, 3 \pmod{4}$. 设 $p \equiv 1 \pmod{4}$, i.e. $p = 4k+1$.

令 $t = (2k)!$. 由 Wilson 定理 (BAI, §6.1), $t^2 + 1 \equiv 0 \pmod{p}$.

i.e. $t^2 + 1 = (t+i)(t-i) = \ell p, \ell \in \mathbb{Z}$.

$\because p$ 在 $\mathbb{Z}[i]$ 中为素元 $\therefore t+i = u p$ 或 $t-i = \tilde{u} p, u, \tilde{u} \in \mathbb{Z}[i]$

$\therefore 1 = p q, q \in \mathbb{Z}$ 不可能 $\therefore p \equiv 3 \pmod{4}$ i.e. $p = 4k-1. \square$

推论1: 若 $p = 4k+1$ 为素数则 $p = m^2 + n^2, m, n \in \mathbb{Z}$.

定理3: 设 $t \in \mathbb{Z}$ 且 $t = \prod_{i=1}^l p_i^{k_i}$, 其中 $p_i \in \mathbb{Z}$ 为相异素数, 则

$t = m^2 + n^2 \Leftrightarrow$ 若 $p_i = 4m_i - 1, m_i \in \mathbb{Z}$, 则 $2 \mid k_i$.

证: ($\Leftarrow$) 注意到 $\forall a, b, c, d \in \mathbb{Z}, (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bd)^2$.

不妨设 $p_i = 4k_i + 1, i = 1, \dots, q, p_i = 4k_i - 1, i = q+1, \dots, l$.

则 $t = N \prod_{i=1}^q p_i = N^2 \prod_{i=1}^q (a_i^2 + b_i^2) = a^2 + b^2, a, b \in \mathbb{Z}$.

($\Rightarrow$) $t = d^2 (\tilde{m}^2 + \tilde{n}^2), d, \tilde{m}, \tilde{n} \in \mathbb{Z}$ 且 $\gcd(\tilde{m}, \tilde{n}) = 1$.

设 $p_i = 4m_i - 1$ 且 $p_i \mid \tilde{m}^2 + \tilde{n}^2$, 则 p_i 在 $\mathbb{Z}[i]$ 中是素元 $\Rightarrow p_i \mid \tilde{m} + \tilde{n}i$ 或 $p_i \mid \tilde{m} - \tilde{n}i$
 $\Rightarrow p_i \mid \gcd(\tilde{m}, \tilde{n}) = 1$ 矛盾

$\therefore$ 若 $p_i = 4m_i - 1$, 则 $p_i \nmid \tilde{m}^2 + \tilde{n}^2 \Rightarrow p_i \mid d^2 \Rightarrow 2 \mid k_i$.

• 唯一因式分解环 UFD (unique factorization domain)

整环 R 称为 UFD, 如果 $\forall a \in R, a$ 可写成 $u p_1 p_2 \dots p_r$, 其中 $u \in U(R), p_i$ 为 R 中

的素元, 且若 a 还可写成 $v q_1 q_2 \dots q_m$, 其中 $v \in U(R), q_i$ 为 R 中素元, 则

$l = m$, 且适当调整次序后有: $p_i = \tilde{u}_i q_i, \tilde{u}_i \in U(R)$.

设 R 为整环, $a_1, \dots, a_n \in R$.

$\gcd(a_1, \dots, a_n) := a \in R$ 满足 1) $\forall 1 \leq i \leq n, a \mid a_i$ 2) 若 $b \in R$ s.t. $b \mid a_i, \forall 1 \leq i \leq n$, 则 $b \mid a$.

X 为未定元 $R[X] := \{ \sum_{i=0}^l a_i x^i \mid l \geq 0, a_i \in R \}$.

设 $f = \sum_{i=0}^n a_i x^i \in R[X]$. $\gcd(a_0, a_1, \dots, a_n)$ 称为 f 的容度 记作 $d(f)$:

若 $d(f) \in U(R)$, 则称 f 是本原的.

$\forall f \in R[X], f = d(f) \tilde{f}, \tilde{f}$ 是本原的.

高斯引理: 设 R 为 UFD, $f, g \in R[X]$. 若 f, g 本原则 fg 本原.

$f, g \in R[X]$ 称为相伴的 如果 $\exists u \in U(R)$ s.t. $f = ug$.

$$Q(R) := \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}. \text{ 定义 } +: \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$

$$\cdot \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

则 $(Q(R), +, \cdot)$ 构成域 称为 R 的分式域.

引理1: 1) 设 R 为 UFD, $f, g \in R[X]$ 为两个本原多项式, 则

f, g 在 $R[X]$ 中相伴 $\Leftrightarrow f, g$ 在 $Q(R)[X]$ 中相伴.

2) 设 R 为 UFD, $f \in R[X]$, 则若 f 为 $R[X]$ 中的素元 则 f 为 $Q(R)[X]$ 中的素元.
s.t. $\deg(f) > 0$.

证: 1) $(\Rightarrow)$ 显然.

$(\Leftarrow)$ 设 $f = ug, u \in Q(R)$. 令 $u = \frac{a}{b}, a, b \in R$ 且 $\gcd(a, b) \in U(R)$.

则 $bf = ag \Rightarrow d(bf) = bc_1 = d(ag) = ac_2, c_1, c_2 \in U(R)$

$\Rightarrow \frac{a}{b} = c_1 c_2^{-1} \in U(R) \Rightarrow f, g$ 在 $R[X]$ 中相伴

2) 设 $f = f_1 f_2, f_1, f_2 \in Q(R)[X]$ 且 $\deg(f_1) > 0, \deg(f_2) > 0$. 令 $b_i \in R$ s.t. $b_i f_i \in R[X]$.

记 $b_i f_i = d(b_i f_i) \tilde{f}_i, \tilde{f}_i$ 本原, $i = 1, 2$. 则 $b_1 b_2 f = (b_1 f_1)(b_2 f_2)$

$$= d(b_1 f_1) d(b_2 f_2) \tilde{f}_1 \tilde{f}_2$$

$$\Rightarrow b_1 b_2 d(f) = d(b_1 f_1) d(b_2 f_2) c, c \in U(R)$$

$\because f$ 为素元 $\therefore f$ 本原 i.e. $d(f) \in U(R)$

$$\therefore \tilde{c} := \frac{d(b_1 f_1) d(b_2 f_2)}{b_1 b_2} \in U(R) \Rightarrow f = \tilde{c} \tilde{f}_1 \tilde{f}_2 \quad \deg(\tilde{f}_i) > 0$$

$\Rightarrow f$ 可约 矛盾

□

定理4: 若 R 为 UFD, 则 $R[X]$ 为 UFD.

证: 设 $f \in R[X]$. 若 $\deg(f) = 0$ 则 $f \in R$ 无需证明.

下设 $\deg(f) > 0$. 记 $f = d(f) \tilde{f}, \tilde{f}$ 本原.

仅需证 $\tilde{f}$ 有唯一的素分解.

对 $\deg(\tilde{f})$ 归纳有. $\tilde{f} = \tilde{u} \tilde{f}_1 \cdots \tilde{f}_s, \tilde{f}_i$ 为 $R[X]$ 中的素元, $\tilde{u} \in U(R)$.

设 $\tilde{f} = \tilde{v} \tilde{g}_1 \cdots \tilde{g}_t, \tilde{v} \in U(R), \tilde{g}_i$ 为 $R[X]$ 中的素元.

$\because \tilde{f}$ 本原 $\therefore \deg(\tilde{g}_i) > 0$

由引理1. $\tilde{f}_i, \tilde{g}_i$ 为 $Q(R)[X]$ 中的素元

由 BAZ 169 定理 4: $\mathbb{Q}(R)[X]$ 为 UFD

$\therefore s=t$ 且适当调整次序后, $\tilde{f}_i$ 与 $\tilde{g}_i$ 在 $\mathbb{Q}(R)[X]$ 中相伴 $\forall 1 \leq i \leq s$

由引理 1, $\tilde{f}_i$ 与 $\tilde{g}_i$ 在 $R[X]$ 中相伴 $\forall 1 \leq i \leq s$

$\therefore f$ 有唯一素分解. □

定理 5: $\underbrace{\{\text{欧几里得环}\}}_A \subseteq \underbrace{\{\text{主理想环}\}}_B \subseteq \underbrace{\{\text{唯一因子分解环}\}}_C$

证: $A \subseteq B$ 由命题 1, 且 $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 为 PID 但不是欧氏环

$B \subseteq C$. 设 R 为 PID, $a \in R$. 断言: a 有素分解.

若 a 为素元, 则成立. 否则 $a = a_1 b_1$, $a_1, b_1 \in R$ 且 $a_1 \notin U(R)$, $b_1 \notin U(R)$.

此时 $Ra \subsetneq Ra_1$, $Ra \subsetneq Rb_1$.

若 a_1, b_1 为素元则成立, 否则对 a_1, b_1 做分解. 该过程有限步终止.

否则有: $Ra \subsetneq Ra_1 \subsetneq Ra_2 \subsetneq \dots$

令 $I = \bigcup_{i=1}^{\infty} Ra_i$, $a_0 = a$. 则 I 为理想. 设 $I = Rc$, $c \in I$.

$\exists i_0$ s.t. $c \in Ra_{i_0} \Rightarrow I = Ra_{i_0} \Rightarrow \forall i \geq i_0, Ra_i = I$

但 $Ra_i \subsetneq Ra_{i+1}$ 矛盾. $\therefore a = p_1 p_2 \dots p_s$, p_i 为 R 中素元.

唯一性: 设 $a = v q_1 \dots q_t$, $v \in U(R)$, q_i 为 R 中素元. 则 $p_1 \mid v q_1 \dots q_t$

$\exists j_0$ s.t. $p_1 \mid q_{j_0}$. 不妨设 $j_0 = 1$. 则 $p_1 \mid q_1 \therefore q_1$ 为素元

$\therefore q_1 = u_1 p_1$. $p_1 \dots p_s = v u_1 p_1 q_2 \dots q_t \Rightarrow p_2 \dots p_s = v u_1 q_2 \dots q_t$

利用归纳, 有 $s=t$ 且适当调整次序后有 $p_i = u_i q_i$, $u_i \in U(R)$, $2 \leq i \leq t$ □

中国剩余定理:

R 为含幺环, $J_1, \dots, J_n$ 为 R 的理想, $\pi_i: R \rightarrow R/J_i$ 自然同态

由直和之性质: $\varphi: R \rightarrow R/J_1 \oplus \dots \oplus R/J_n$ 为环同态

$a \mapsto (a+J_1, \dots, a+J_n)$

$\ker \varphi = \bigcap_{i=1}^n J_i$

定理 6: 若 $J_i + J_j = R \ \forall 1 \leq i \neq j \leq n$. 则 φ 为满同态

证: 设 $(b_1+J_1, \dots, b_n+J_n) \in R/J_1 \oplus \dots \oplus R/J_n$. 目标: 找 $a \in R$ s.t.

$a - b_i \in J_i \ \forall 1 \leq i \leq n$.

当 $n=1$ 时 令 $a=b_1$ 即可. 设 $\exists y \in R$ s.t. $y - b_i \in J_i \quad \forall 1 \leq i \leq k$.

由 §4.1 命题有 $J_1 \cap \dots \cap J_k + J_{k+1} = R \Rightarrow \exists a_1 \in J_1 \cap \dots \cap J_k, a_2 \in J_{k+1}$
s.t. $a_1 + a_2 = 1$

令 $a = ya_2 + b_{k+1}a_1$.

则 $\forall 1 \leq i \leq k, a - b_i = ya_2 + b_{k+1}a_1 - b_i = y(1 - a_1) + b_{k+1}a_1 - b_i$
 $= y - b_i + a_1(b_{k+1} - y) \in J_i$

$a - b_{k+1} = ya_2 + b_{k+1}a_1 - b_{k+1} = (y - b_{k+1})a_2 \in J_{k+1} \quad \square$

设 R 为整环, $a, b \in R$ 称为互素如果 $Ra + Rb = R$.

记号: $a \equiv b \pmod{p}$ 表 $p | a - b$.

推论2: 设 R 为整环, $a_1, \dots, a_n \in R$ 且当 $i \neq j$ 时 a_i 与 a_j 互素. 则对于 $\forall b_1, \dots, b_n \in R \exists a \in R$
s.t. $a \equiv b_i \pmod{a_i} \quad \forall 1 \leq i \leq n$

孙子算经(公元400~500年): "今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?"

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$\mathbb{Z}$ 的剩余类环 $\mathbb{Z}_n$ $n > 0$.

推论3: 设 $n = p_1^{m_1} \dots p_r^{m_r}$, p_i 为互异素数. 则

$$1) \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{m_r}} \quad (\text{环的同构})$$

$$2) U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{m_1}}) \times \dots \times U(\mathbb{Z}_{p_r^{m_r}})$$

证: 1) 由中国剩余定理, $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_{p_1^{m_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{m_r}}$ 为满同态.

$$l \mapsto (l + p_1^{m_1}\mathbb{Z}, \dots, l + p_r^{m_r}\mathbb{Z})$$

$$\ker \varphi = \bigcap_{i=1}^r p_i^{m_i} \mathbb{Z} = n\mathbb{Z}. \text{ 由同态基本定理: } \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{m_r}}.$$

2) 设 $R = R_1 \oplus \dots \oplus R_n$, R_i 为环. 则

$$(a_1, \dots, a_n) \in U(R) \Leftrightarrow \exists (b_1, \dots, b_n) \in R \text{ s.t. } (a_1 b_1, \dots, a_n b_n) = (1, \dots, 1)$$

$$\Leftrightarrow \forall 1 \leq i \leq n, a_i \in U(R_i)$$

$\therefore U(R) = U(R_1) \times \dots \times U(R_n)$. 将其应用于 $\mathbb{Z}$.

注: $d \in \{0, 1, 2, \dots, p_i^{m_i} - 1\}$ $\gcd(d, p_i^{m_i}) \neq 1 \Rightarrow d = sp_i^t \quad s=0, 1, \dots, p_i - 1, t=1, \dots, m_i - 1$

$$\Rightarrow |U(\mathbb{Z}_{p_i^{m_i}})| = p_i^{m_i} - p_i^{m_i-1} = p_i^{m_i-1}(p_i - 1)$$

$$\text{由推论3, } |U(\mathbb{Z}_n)| = \prod_{i=1}^r |U(\mathbb{Z}_{p_i^{m_i}})| = \prod_{i=1}^r p_i^{m_i-1}(p_i - 1) = \varphi(n). \rightarrow \text{欧拉函数}$$

$$\therefore \forall a \in \mathbb{Z}, \gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

设 $a \in \mathbb{Z}$, 当 $|\langle a + n\mathbb{Z} \rangle| = \varphi(n)$ 时称 a 为模 n 本原根 (或原根)

定理7: 设 $m \in \mathbb{Z}_{>0}$, 则

1) 当 p 为奇素数时, $U(\mathbb{Z}_p\mathbb{Z})$ 为循环群.

2) $|U(\mathbb{Z}_2\mathbb{Z})| = 1$, $|U(\mathbb{Z}_4\mathbb{Z})| = 2$. 而 $U(\mathbb{Z}_2^m\mathbb{Z}) \cong \langle a \rangle \times \langle b \rangle$, $|\langle a \rangle| = 2^{m-2}$, $|\langle b \rangle| = 2$.

证: (思路: 在 $U(\mathbb{Z}_p\mathbb{Z})$ 中找到阶为 $p-1$ 与 p^{m-1} 元素 α 与 β . $\because \gcd(p-1, p^{m-1}) = 1$)

$$\therefore |\langle \alpha\beta \rangle| = p^{m-1}(p-1) \Rightarrow \langle \alpha\beta \rangle = U(\mathbb{Z}_p^m\mathbb{Z})$$

由BACH定理11, $U(\mathbb{Z}_p\mathbb{Z}) = \langle d \rangle$, i.e. $d^{p-1} \equiv 1 \pmod{p}$ 且 $d^i \not\equiv 1 \pmod{p} \forall 0 < i < p-1$

令 $\alpha = d^{p^{m-1}}$. 则 $\alpha^i \not\equiv 1 \pmod{p^m} \forall 1 \leq i < p$. 否则 $\exists 1 \leq i_0 < p$ s.t. $\alpha^{i_0} \equiv 1 \pmod{p}$

$\therefore \alpha \equiv d \pmod{p} \therefore d^{i_0} \equiv 1 \pmod{p}$ 矛盾.

另一方面, $\alpha^{p-1} = d^{p^{m-1}(p-1)} = d^{\varphi(p^m)} \equiv 1 \pmod{p^m}$

$\therefore \alpha + p^m\mathbb{Z}$ 在 $U(\mathbb{Z}_p^m\mathbb{Z})$ 中生成 $p-1$ 阶循环群.

断言: $\forall i \geq 1, (1+p)^{p^i} \equiv 1 + p^{i+1}\gamma \pmod{p^{i+2}}$, 其中 $\gamma \in \mathbb{Z}$ 且 $p \nmid \gamma$.

(当 $i=1$ 时 $(1+p)^p = 1 + p^2 + \frac{p-1}{2}p^2 + \dots \equiv 1 + p^2 \pmod{p^3} \because p \geq 2$. 一般情况)

$$\begin{aligned} (1+p)^{p^{k+1}} &= [(1+p)^{p^k}]^p = (1 + p^{k+1}\gamma + p^{k+2}\delta)^p \\ &= 1 + p^{k+2}\gamma + p^{k+3}\delta \equiv 1 + p^{k+2}\gamma \pmod{p^{k+3}} \end{aligned}$$

令 $k=m-2$, 则 $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$ 但 $\forall 0 < i < m, (1+p)^{p^i} \equiv 1 + p^{i+1}\gamma + \dots \pmod{p^n}$

$\therefore p \nmid \gamma, \therefore p^{i+1}\gamma \not\equiv 0 \pmod{p^n} \therefore (1+p)^{p^i} \not\equiv 1 \pmod{p^m}$

$\therefore 1+p+p^m\mathbb{Z}$ 在 $U(\mathbb{Z}_p^m\mathbb{Z})$ 中生成 p^{m-1} 阶循环群.

2) $5 \equiv 1+2^2 \pmod{2^3}$ 设 $5^{2^i} \equiv 1+2^{i+2} \pmod{2^{i+3}}$

$$\text{则 } 5^{2^{i+1}} = (5^{2^i})^2 = (1+2^{i+2} + 2^{i+3}m)^2$$

$$= 1 + 2^{i+3} + 2^{i+4}m \equiv 1 + 2^{i+3} \pmod{2^{i+4}}$$

$$\Rightarrow 5^{2^{m-2}} \equiv 1 \pmod{2^m} \text{ 但 } 5^{2^{m-3}} \equiv 1 + 2^{m-1} \pmod{2^m}$$

$\therefore 5+2^m\mathbb{Z}$ 在 $U(\mathbb{Z}_2^m\mathbb{Z})$ 中生成 2^{m-2} 阶循环群.

另一方面, $-1+2^m\mathbb{Z}$ 在 $U(\mathbb{Z}_2^m\mathbb{Z})$ 中生成 2 阶循环群且 $-1+2^m\mathbb{Z} \notin \langle 5+2^m\mathbb{Z} \rangle$.

$$\left(\begin{aligned} \text{否则 } 5^j + 2^m\mathbb{Z} &= -1 + 2^m\mathbb{Z} \Rightarrow 5^j + 1 \equiv 0 \pmod{2^m} \\ \therefore m \geq 3, \therefore 5^j + 1 &\equiv 0 \pmod{4} \Rightarrow 1+1 \equiv 0 \pmod{4} \text{ 不可能} \end{aligned} \right)$$

$$\therefore |U(\mathbb{Z}_2^m\mathbb{Z})| = 2^{m-1} \therefore U(\mathbb{Z}_2^m\mathbb{Z}) = \langle 5+2^m\mathbb{Z} \rangle \times \langle -1+2^m\mathbb{Z} \rangle$$

□

推论: 设 $n > 1$. 则 $U(\mathbb{Z}_n)$ 为循环群 $\Leftrightarrow n = 2, 4, p^n$ 或 $2p^n$, 其中 p 为奇素数.

R 为环, $a \in R$

$Z_R(a) := \{b \in R \mid ab = ba\}$ a 的中心化子.

$Z_R := \{a \in R \mid ab = ba \ \forall b \in R\} = \bigcap_{a \in R} Z_R(a)$ 称为 R 的中心.

$Z_R(a)$ 为 R 的子环: $\forall b_1, b_2 \in Z_R(a), ab_1 = b_1a \Rightarrow a(b_1 - b_2) = (b_1 - b_2)a$
 $\Rightarrow b_1 - b_2 \in Z_R(a)$

$ab_1b_2 = b_1ab_2 = ab_1b_2 \Rightarrow b_1b_2 \in Z_R(a)$.

同样: Z_R 为 R 的子环. 设 R 为除环.

$\forall x \in Z_R \setminus \{0\}, a \in R. xa = ax \Rightarrow ax^{-1} = x^{-1}a \Rightarrow x^{-1} \in Z_R$

$\therefore Z_R$ 为除环.

分圆多项式:

$x^n - 1 = \prod_{d|n} \Phi_d(x) \quad \Phi_d(x) \in \mathbb{Z}[x]$ 首1且不可约.

$\Phi_d(x) = \prod_{\substack{\zeta^d = 1 \\ \zeta^i \neq 1 \ \forall 0 < i < d}} (x - \zeta)$ 称为分圆多项式 $\deg \Phi_d = \varphi(d)$.

例: $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

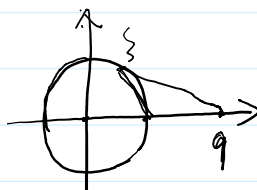
设 ζ 为 n 次本原根 i.e. $\zeta^n = 1$ 但 $\zeta^i \neq 1 \ \forall 0 < i < n$.

设 $d|n$ 且 $d < n$. 令 $f(x) = \frac{x^n - 1}{x^d - 1}$. 则 $f(\zeta) = 0 \Rightarrow \Phi_n(x) \mid f(x)$.

特别地: $\Phi_n(q) \mid f(q) \ \forall q \geq 2$.

当 $n \geq 2$ 且 $q \geq 2$ 时, $|\Phi_n(q)| > q - 1$.

$|\Phi_n(q)| = \prod_{\substack{\zeta^n = 1 \\ \zeta^i \neq 1 \ \forall 0 < i < n}} |q - \zeta| > |q - 1|$



$q \in \mathbb{Z}, q \geq 2, n > 0, m > 0, q^n - 1 \mid q^m - 1 \Rightarrow m \mid n$.

令 $n = sm + r \ 0 \leq r < m$. $q^n - 1 = q^{sm+r} - 1 = q^r(q^{sm} - 1) + q^r - 1$
 $= q^r \cdot (q^m - 1)(1 + q^m + \dots + q^{(s-1)m}) + q^r - 1$

$q^m - 1 \mid q^n - 1 \Rightarrow q^m - 1 \mid q^r - 1 \Rightarrow r = 0 \Rightarrow m \mid n$.

命题8: (Wedderburn) 有限除环为域.

证: 设 D 是有限除环且 $D \neq \{0\}$. 则 Z_D 为有限域且 $|Z_D| \geq 2$.

记 $q = |Z_D|$. D 为 Z_D 上的有限维向量, 设 $\dim D = n$. 则 $|D| = q^n$.

$$U(D) = D \setminus \{0\}. \text{ 考虑群作用: } U(D) \times U(D) \longrightarrow U(D) \\ (g, h) \longmapsto ghg^{-1}$$

$$\text{轨道公式: } |U(D)| = |Z_D \setminus \{0\}| + \sum_x (U(D) : Z_D(x) \setminus \{0\})$$

$Z_D(x)$ 为 Z 向量空间, 设 $\dim Z_D(x) = n(x)$. 则 $|Z_D(x) \setminus \{0\}| = q^{n(x)} - 1$

$$\therefore q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{n(x)} - 1}, \quad 1 \leq n(x) < n$$

$$q^{n(x)} - 1 \mid q^n - 1 \Rightarrow n(x) \mid n. \Rightarrow \mathbb{F}_n(q) \mid \left(\frac{q^n - 1}{q^{n(x)} - 1} \right)$$

$$\Rightarrow \mathbb{F}_n(q) \mid q - 1. \Rightarrow n = 1. \Rightarrow D = Z_D$$