

## 0.1 主理想整环与 Euclid 环

### 定义 0.1

若交换幺环的每个理想都是主理想，则称此环为**主理想环**。一个主理想环若又是整环，则称此环为**主理想整环**，记为 p.i.d..



**例题 0.1** 整环  $\mathbf{Z}$  是主理想整环。

**证明** 事实上，设  $I$  为  $\mathbf{Z}$  的一个非平凡理想，于是  $\exists m \in I$  满足

$$m = \min\{|k| \mid k \in I, k \neq 0\}.$$

$\forall k \in I$ ，若  $k = 0$ ，则  $k = 0 \cdot m$ ；若  $k \neq 0$ ，则  $\exists q, r \in \mathbf{Z}$ ，满足  $k = qm + r (0 \leq r < m)$ ，由  $I \triangleleft \mathbf{Z}$  和  $m \in I$  知  $qm \in I$ ，于是  $r \in I$ 。由  $m$  的取法知  $r = 0$ ，即  $k = qm$ ，否则与  $m$  的最小值定义矛盾！故  $I = \{xm \mid x \in \mathbf{Z}\} = \langle m \rangle$ ，因而  $\mathbf{Z}$  是主理想整环。



**例题 0.2**  $\mathbf{Z}[x]$  不是主理想整环。

**证明** 事实上，若  $\mathbf{Z}[x]$  是主理想整环，则有  $g(x)$ ，使得  $\langle 2, x^2 + 1 \rangle = \langle g(x) \rangle$ 。由定理????知

$$\{2u(x) + (x^2 + 1)v(x) \mid u(x), v(x) \in \mathbf{Z}[x]\} = \langle 2, x^2 + 1 \rangle = \langle g(x) \rangle = \{u(x)g(x) \mid u(x) \in \mathbf{Z}[x]\}. \quad (1)$$

因为  $2 \in \langle 2, x^2 + 1 \rangle$ ，所以由(1)式知存在  $f(x) \in \mathbf{Z}[x]$ ，使  $2 = f(x)g(x)$ ，即  $g(x) \mid 2$ ，故  $g(x) = \pm 1, \pm 2$ 。另一方面，由  $g(x) \in \langle 2, x^2 + 1 \rangle$ ，故由(1)式有  $u(x), v(x) \in \mathbf{Z}[x]$ ，使得

$$g(x) = 2u(x) + (x^2 + 1)v(x).$$

令  $x = 1$ ，则有  $g(1) = 2(u(1) + v(1))$ 。于是  $g(x) = \pm 2$ ，但  $\pm 2 \nmid (x^2 + 1)$ ，即  $g(x) \nmid (x^2 + 1)$ ，从而  $x^2 + 1 \notin \langle g(x) \rangle$ 。这与(1)式矛盾！因而  $\mathbf{Z}[x]$  不是主理想整环。



### 定理 0.1

设  $R$  是交换整环，则

- (1)  $a \mid b \iff \langle a \rangle \supseteq \langle b \rangle$ .
- (2)  $a \sim b \iff \langle a \rangle = \langle b \rangle$ .
- (3)  $a \sim 1 \iff \langle a \rangle = \langle 1 \rangle = R$ .
- (4)  $R$  满足因子链条件当且仅当  $R$  满足**主理想的升链条件**，即任一**主理想升链**

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \langle a_{n+1} \rangle \subseteq \cdots,$$

一定存在  $m \in \mathbf{N}$ ，使得当  $n \geq m$  时， $\langle a_n \rangle = \langle a_m \rangle$ 。



**证明**

(1) 若  $a \mid b$ ，则存在  $r_1 \in R$ ，使  $b = r_1a$ 。从而由定理????知

$$\langle b \rangle = \{rb \mid r \in R\} = \{rr_1a \mid r \in R\} \subseteq \{ra \mid r \in R\} = \langle a \rangle.$$

若  $\langle b \rangle \subseteq \langle a \rangle$ ，则由定理????知

$$\langle b \rangle = \{rb \mid r \in R\} \subseteq \{ra \mid r \in R\} = \langle a \rangle.$$

于是由  $b \in \langle b \rangle$  知存在  $r_1 \in R$ ，使得  $b = r_1a$ ，故  $a \mid b$ 。

(2) 这就是(1)的直接推论。

(3) 这就是(2)的直接推论。

(4) 对任一**主理想升链**

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \langle a_{n+1} \rangle \subseteq \cdots,$$

由结论(2)知  $a_{n+1} \mid a_n$  ( $n \in \mathbb{N}$ ). 故

$$a_1, a_2, \dots, a_n, a_{n+1}, \dots$$

是  $R$  的因子链. 若  $R$  满足因子链条件, 则存在  $m \in \mathbb{N}$ , 使得当  $n \geq m$  时, 有  $a_n \sim a_m$ . 由结论(2), 此即  $\langle a_n \rangle = \langle a_m \rangle$ .

若存在  $m \in \mathbb{N}$ , 使得当  $n \geq m$  时,  $\langle a_n \rangle = \langle a_m \rangle$ . 由结论(2), 此即  $a_n \sim a_m$ . 故此时  $R$  满足因子链条件.

□

### 定理 0.2

主理想整环一定是唯一析因环.

♡

**证明** 由定理 0.1(4) 与定理????, 只需证一个主理想整环  $R$  满足主理想升链条件与最大公因子条件. 设

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots \subseteq \langle a_n \rangle \subseteq \dots$$

是  $R$  中一个主理想升链. 令  $I = \bigcup_{i=1}^{\infty} \langle a_i \rangle$ . 若  $a, b \in I$ , 则  $\exists i, j \in \mathbb{N}$ , 使  $a \in \langle a_i \rangle, b \in \langle a_j \rangle$ . 不妨设  $j \geq i$ . 由此知  $a - b \in \langle a_j \rangle \subseteq I$ , 故  $I$  是  $R$  中加法子群, 也是 Abel 群. 显然  $I$  对乘法封闭且满足结合律, 故  $I$  是  $R$  的子环. 又由定理????知  $\forall c \in R, ca \in \langle a_i \rangle \subseteq I$ , 故  $I$  是  $R$  中理想. 由  $R$  是主理想整环知  $\exists d \in R$ , 使  $I = \langle d \rangle$ . 因  $d \in I$ , 故  $\exists m \in \mathbb{N}$ , 使  $d \in \langle a_m \rangle$ , 因而当  $n \geq m$  时, 由定理??有

$$I = \langle d \rangle \subseteq \langle a_m \rangle \subseteq \langle a_n \rangle \subseteq \bigcup_{i=1}^{\infty} \langle a_i \rangle = I,$$

即  $\langle a_n \rangle = \langle a_m \rangle = I$ . 这就证明了  $R$  满足主理想升链条件.

其次, 设  $a, b \in R^*$ . 由定理????知  $\langle a \rangle + \langle b \rangle$  是  $R$  的子环, 利用定理??显然有  $R(\langle a \rangle + \langle b \rangle) \subseteq \langle a \rangle + \langle b \rangle$ , 故  $\langle a \rangle + \langle b \rangle$  是  $R$  中理想. 由  $R$  是主理想整环知  $\exists d \in R$ , 使  $\langle a \rangle + \langle b \rangle = \langle d \rangle$ , 因而有  $\langle a \rangle \subseteq \langle d \rangle, \langle b \rangle \subseteq \langle d \rangle$ , 由定理 0.1(1) 知  $d \mid a, d \mid b$ , 即  $d$  为  $a, b$  的公因子. 又若  $c \mid a, c \mid b$ , 则由定理 0.1(1) 知  $\langle a \rangle \subseteq \langle c \rangle, \langle b \rangle \subseteq \langle c \rangle$ , 故  $\langle d \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$ , 由定理 0.1(1) 知  $c \mid d$ , 故  $d$  为  $a, b$  的最大公因子.

综上知  $R$  为唯一析因环.

□

### 推论 0.1

设  $R$  是主理想整环, 若  $d$  为  $a, b$  的最大公因子, 则存在  $u, v \in R$ , 使得

$$d = au + bv.$$

♡

**证明** 设  $a, b \in R^*$ . 由定理????知  $\langle a \rangle + \langle b \rangle$  是  $R$  的子环, 利用定理??显然有  $R(\langle a \rangle + \langle b \rangle) \subseteq \langle a \rangle + \langle b \rangle$ , 故  $\langle a \rangle + \langle b \rangle$  是  $R$  中理想. 由  $R$  是主理想整环知  $\exists d_1 \in R$ , 使  $\langle a \rangle + \langle b \rangle = \langle d_1 \rangle$ , 因而有  $\langle a \rangle \subseteq \langle d_1 \rangle, \langle b \rangle \subseteq \langle d_1 \rangle$ , 由定理 0.1(1) 知  $d_1 \mid a, d_1 \mid b$ , 即  $d_1$  为  $a, b$  的公因子. 又若  $c \mid a, c \mid b$ , 则由定理 0.1(1) 知  $\langle a \rangle \subseteq \langle c \rangle, \langle b \rangle \subseteq \langle c \rangle$ , 故  $\langle d_1 \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$ , 由定理 0.1(1) 知  $c \mid d_1$ , 故  $d_1$  为  $a, b$  的最大公因子. 从而  $d_1 \sim d$ , 再由定理 0.1(2) 知  $\langle d \rangle = \langle d_1 \rangle = \langle a \rangle + \langle b \rangle$ . 由定理??知

$$\langle d \rangle = \langle a \rangle + \langle b \rangle = \{ua + bv \mid u, v \in R\}.$$

又  $d \in \langle d \rangle$ , 故存在  $u, v \in R$ , 使得

$$d = au + bv.$$

□

### 推论 0.2

设  $R$  是主理想整环, 若  $d$  为  $a, b$  的最大公因子, 则存在  $a_1, b_1 \in R$ , 使得  $a = da_1, b = db_1$  且  $(a_1, b_1) = 1$ .

♡

**证明** 由  $d \mid a, b$  知存在  $a_1, b_1 \in R$ , 使  $a = da_1, b = db_1$ . 于是由引理????知  $d = (a, b) = (da_1, db_1) \sim d(a_1, b_1)$ . 从

而存在  $r \in R$ , 使  $d = d(a_1, b_1)r$ . 由命题????知  $R^*$  对乘法满足消去律, 故  $1 = (a_1, b_1)r$ . 因此  $(a_1, b_1) \in U$ , 再由定理????知  $(a_1, b_1) \sim 1$ .

□

### 推论 0.3

设  $R$  是主理想整环,  $a, b$  互素 (即  $(a, b) \sim 1$ ) 的充要条件是  $\exists u, v \in R$ , 使得

$$au + bv = 1.$$

♡

**证明** 必要性已含于推论 0.1 中. 下证充分性. 设  $au + bv = 1 (u, v \in R)$ , 若  $d = (a, b)$ , 则  $d \mid a, d \mid b$ , 故  $d \mid au + bv$ , 因而  $d \mid 1$ , 故  $d \sim 1$ .

□

### 定义 0.2 (Euclid 环)

设  $R$  为交换整环. 若存在  $R$  到非负整数集  $\mathbf{N} \cup \{0\}$  的映射  $\delta$ , 使得  $\forall a, b \in R, b \neq 0, \exists q, r \in R$  满足

$$a = qb + r, \quad \delta(r) < \delta(b), \tag{2}$$

则称  $R$  为 Euclid 环.

♣

**例题 0.3**  $\mathbf{Z}$  是 Euclid 环.

**证明** 事实上, 任何两个整数之间都可做带余除法, 故只需取  $\delta(m) = |m|$  即可验证  $\delta$  满足定义.

□

**例题 0.4** 设  $\mathbf{P}$  为数域, 则  $\mathbf{P}[x]$  是 Euclid 环. 定义  $\delta$  为

$$\delta(f(x)) = \begin{cases} 2^{\deg f(x)}, & f(x) \neq 0, \\ 0, & f(x) = 0. \end{cases}$$

不难验证  $\delta$  满足 Euclid 环所要求的条件.

**例题 0.5** Gauss 整数环  $\mathbf{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbf{Z}\}$  是 Euclid 环.

**证明** 事实上, 令  $\delta(a + b\sqrt{-1}) = a^2 + b^2$ , 则显然有

$$\delta(\alpha\beta) = \delta(\alpha)\delta(\beta), \quad \forall \alpha, \beta \in \mathbf{Z}[\sqrt{-1}].$$

设  $\beta \neq 0$ . 不难看出其乘法逆元  $\beta^{-1} \in \mathbf{Q}[\sqrt{-1}]$ , 即有

$$\alpha\beta^{-1} = \mu + \nu\sqrt{-1}, \quad \mu, \nu \in \mathbf{Q}.$$

于是  $\exists c, d \in \mathbf{Z}$ , 使得  $|c - \mu| \leqslant 1/2, |d - \nu| \leqslant 1/2$ . 令  $\varepsilon = \mu - c, \eta = \nu - d$ , 则有  $|\varepsilon| \leqslant 1/2, |\eta| \leqslant 1/2$ , 而

$$\alpha = \beta((c + \varepsilon) + (d + \eta)\sqrt{-1}) = \beta q + r,$$

其中,  $q = c + d\sqrt{-1} \in \mathbf{Z}[\sqrt{-1}], r = \beta(\varepsilon + \eta\sqrt{-1}) = \alpha - \beta q \in \mathbf{Z}[\sqrt{-1}]$ . 又

$$\delta(r) = |r|^2 = \delta(\beta)(\varepsilon^2 + \eta^2) \leqslant \delta(\beta)(1/4 + 1/4) < \delta(\beta),$$

故  $\mathbf{Z}[\sqrt{-1}]$  为 Euclid 环.

□

### 定理 0.3

Euclid 环是主理想环. 因而也是唯一析因环.

♡

**注** 确有主理想整环不是 Euclid 环. 例如, 环

$$D = \left\{ a + \frac{b}{2}(1 + \sqrt{-19}) \mid a, b \in \mathbf{Z} \right\}$$

是一个主理想整环, 但不是 Euclid 环.

**证明** 设  $I$  是 Euclid 环  $R$  中的一个理想. 若  $I = \{0\}$ , 显然是主理想, 故假设  $I \neq \{0\}$ . 取  $I$  中元素  $b$ , 使得

$$\delta(b) = \min\{\delta(c) \mid c \in I, c \neq 0\}. \quad (3)$$

设  $a \in I$ , 则有  $q, r \in R$ , 使

$$a = qb + r, \quad \delta(r) < \delta(b).$$

因  $a, b \in I$ , 故  $r = a - qb \in I$ . 由  $b$  的取法知  $r \notin I \setminus \{0\}$ , 否则与  $\delta(b)$  的最小值定义矛盾! 故  $r = 0$ , 因而  $a \in \langle b \rangle$ , 故  $I = \langle b \rangle$ . 即  $R$  为主理想环. 再由定理 0.2 知 Euclid 环也是唯一析因环.

□

### 命题 0.1 (辗转相除法)

设  $R$  是 Euclid 环,  $R^* = R \setminus \{0\}, a, b \in R^*$ , 求  $a$  与  $b$  的最大公因子.

◆

**笔记** 在 Euclid 环中, 可用辗转相除法来求两个元素的最大公因子.

**解** 不妨设  $\delta(a) \geq \delta(b)$ , 并记  $a = a_1, b = a_2$ . 于是  $\exists q_1, a_3 \in R$ , 使

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

若  $a_3 = 0$ , 则由引理????和定理????知

$$(a_1, a_2) = (q_1 a_2, a_2) = (q_1, 1) a_2 \sim a_2,$$

设  $a_3 \neq 0$ , 由推论 0.2 知存在  $a'_2, a'_3 \in R$ , 使  $a_2 = a'_2(a_2, a_3), a_3 = a'_3(a_2, a_3)$  且  $(a'_2, a'_3) = 1$ . 再由推论 0.3 知存在  $u, v \in R$ , 使

$$u a'_2 + v a'_3 = 1.$$

从而

$$v(q_1 a'_2 + a'_3) + (u - vq_1) a'_2 = u a'_2 + v a'_3 = 1.$$

又  $v, u - vq_1 \in R$ , 故由推论 0.3 知  $(q_1 a'_2 + a'_3, a'_2) \sim 1$ . 再利用引理????和定理????得

$$(a_1, a_2) = (q_1 a_2 + a_3, a_2) = (q_1 a'_2(a_2, a_3) + a'_3(a_2, a_3), a'_2(a_2, a_3)) \sim (q_1 a'_2 + a'_3, a'_2)(a_2, a_3) \sim (a_2, a_3).$$

再对  $a_2, a_3$  作除法运算

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

若  $a_4 = 0$ , 则同理可知  $(a_1, a_2) \sim (a_2, a_3) \sim a_3$ , 若  $a_4 \neq 0$ , 则同理可知  $(a_1, a_2) \sim (a_2, a_3) \sim (a_3, a_4)$ . 再继续下去有

$$\delta(a_1) \geq \delta(a_2) > \delta(a_3) > \delta(a_4) > \cdots,$$

因为  $\delta(a_1)$  是有限数, 所以在有限步后必然终止, 即有  $a_n \neq 0$ , 而  $a_{n+1} = 0$ . 于是  $(a_1, a_2) \sim a_n$ . 综上, 存在  $a_3, a_4, \dots, a_n$  以及  $q_1, q_2, \dots, q_{n-1}$ , 使得

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

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

.....

$$a_{n-2} = q_{n-2} a_{n-1} + a_n, \quad \delta(a_n) < \delta(a_{n-1});$$

$$a_{n-1} = q_{n-1} a_n, \quad \delta(a_n) < \delta(a_{n-1}).$$

并且

$$(a_1, a_2) \sim (a_2, a_3) \sim \cdots \sim (a_{n-1}, a_n) \sim a_n.$$

□