

§4.1 环的构造

定义1: 集合 R 称为环 如果 $+$: $R \times R \rightarrow R$, $\cdot$: $R \times R \rightarrow R$
 $(a, b) \rightarrow a+b$ $(a, b) \rightarrow ab$

s.t. 1) $(R, +)$ 是个交换群 2) $(R, \cdot)$ 是半群

3) $\forall a, b, c \in R$, $(a+b) \cdot c = a \cdot c + b \cdot c$, $c(a+b) = ca + cb$

若 2) 替换成 2'), $(R, \cdot)$ 是么半群 则称 R 是含么环.

R 为环, 如果 $\forall a, b \in R$, $ab = ba$ 则称 R 为交换环

注: 1) 0 表 $(R, +)$ 中的单位元. 若 R 为交换环 则用 1 表示 $(R, \cdot)$ 中的单位元, 此时 1 也是唯一的.

2) $\forall r \in R$, $0 \cdot r = r \cdot 0 = 0$ $\left(\begin{array}{l} (0+0) \cdot r = 0 \cdot r = 2 \cdot 0 \cdot r \\ \Rightarrow 0 \cdot r = 0, \text{同理 } r \cdot 0 = 0 \end{array} \right)$

子环: $S \subseteq R$ 称为子环 如果 $\forall a, b \in S$, $a+b \in S$ 且 $ab \in S$

并且 S 在运算 $+$, $\cdot$ 下构成环. ($\Leftrightarrow \forall a, b \in S$, $a-b \in S$, $ab \in S$)

例: 1) $R = \{0\}$. 此时 $0=1$

2) $R = \mathbb{Z}$ 含么交换环.

$n\mathbb{Z}$ 是 $\mathbb{Z}$ 的子环. 当 $|n| > 1$ 时 $n\mathbb{Z}$ 无么元.

3) $H = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_i \in \mathbb{R}\}$ 四元数
含么的非交换环.

4) $M_n(F) = \{(a_{ij})_{n \times n} \mid a_{ij} \in F\}$ F 为域. 设 R 为含么环.
可逆元: $r \in R$ 称为可逆的, 如果 $\exists s \in R$ s.t.
 $s \cdot r = r \cdot s = 1$

5) $(A, +)$ 为交换群

$\text{End}(A) := \{\varphi: A \rightarrow A \text{ 群同态}\}$

$\varphi_1, \varphi_2 \in \text{End}(A)$, $x \in A$

$(\varphi_1 + \varphi_2)(x) := \varphi_1(x) + \varphi_2(x)$

$\varphi_1 \varphi_2 := \varphi_1 \circ \varphi_2$

$0 := 0$ 同态: $\begin{pmatrix} A \rightarrow A \\ x \rightarrow 0 \end{pmatrix}$

$1 := \text{id}_A$

记 $U(R) := \{R \text{ 中可逆元}\}$
 $U(R)$ 在 $\cdot$ 运算下构成群

若 $U(R) = R \setminus \{0\}$ 称 R 为除环

交换的除环称为域

设 R 为交换环, $a \in R \setminus \{0\}$. 若 $\exists$

$0 \neq b \in R$ s.t. $ab = 0$ 则称 a

为零因子. 若 $R \neq \{0\}$ 为含么交换环且不含零因子
则称 R 为整环.

设 R 为环

(双边)理想: $I \subseteq R$ 称为理想. 如果 1) I 为 R 的子环 (或 I 为 $(R, +)$ 的子群, 或 $\forall a, b \in I$, $a-b \in I$)

2) $\forall a \in I, r \in R$, $ra \in I, ar \in I$.

当 2) 替换为 2') $\forall a \in I, r \in R$, $ra \in I$ 称 I 为左理想

同样定义右理想.

设 I 为 $(R, +)$ 的子群. $R/I = \{r+I \mid r \in R\}$

$(R/I, +)$ 是个交换群. $(r_1+I) + (r_2+I) := r_1+r_2+I$

· 何时 R/I 可以定义自然的乘法, i.e. $(r_1+I)(r_2+I) := r_1r_2+I$?

$\forall a_1, a_2 \in I$. $r_1+a_1+I = r_1+I$, $r_2+a_2+I = r_2+I$

$$\begin{aligned}(r_1+I)(r_2+I) &= r_1r_2+I \\ &= (r_1+a_1+I)(r_2+a_2+I) \\ &= r_1r_2+r_1a_2+a_1r_2+a_1a_2+I\end{aligned}$$

$\Rightarrow r_1a_2+r_2a_1 \in I \Rightarrow I$ 是个理想

反之, 若 I 为理想 则 $(r_1+I)(r_2+I) := r_1r_2+I$ 是良定义的

· $(R/I, +, \cdot)$ 是个环: $(R/I, +)$ 是半群

$\forall a, b, c \in R$, 记 $\bar{a} = a+I$, $\bar{b} = b+I$, $\bar{c} = c+I$

$$\begin{aligned}(\bar{a} + \bar{b})\bar{c} &= (a+I+b+I)(c+I) \\ &= (a+b+I)(c+I) = (a+b)c+I \\ &= ac+I+bc+I = (a+I)(c+I) + (b+I)(c+I) \\ &= \bar{a}\bar{c} + \bar{b}\bar{c}\end{aligned}$$

同样可验证: $\bar{c}(\bar{a} + \bar{b}) = \bar{c}\bar{a} + \bar{c}\bar{b}$

$\therefore (R/I, +, \cdot)$ 构成环, 称为 R 模 I 的商环 ($\begin{smallmatrix} 0 = I \\ 1 = 1+I \end{smallmatrix}$)

设 R_1, R_2 为环. 映射 $\varphi: R_1 \rightarrow R_2$ 称为环同态 如果 $\forall a, b \in R_1$

$$1) \varphi(a+b) = \varphi(a) + \varphi(b), \quad 2) \varphi(ab) = \varphi(a)\varphi(b)$$

当 R_1, R_2 为含幺环时, 通常要求 $\varphi(1_{R_1}) = 1_{R_2}$.

同态核: $\ker \varphi := \{a \in R_1 \mid \varphi(a) = 0\}$

同构: 同态 $\varphi: R_1 \rightarrow R_2$ 称为同构 如果 $\exists \psi: R_2 \rightarrow R_1$ 为环同态 s.t.

$$\varphi \circ \psi = \text{id}_{R_2}, \quad \psi \circ \varphi = \text{id}_{R_1}. \quad (\text{此时记 } R_1 \cong R_2)$$

注: 1) 当 φ 为满同态时 $\varphi(1_{R_1}) = 1_{R_2}$ 自然满足.

$$\begin{aligned}(\text{令 } a \in R_1 \text{ s.t. } \varphi(a) = 1_{R_2}. \text{ 则 } \varphi(a) &= \varphi(1_{R_1} \cdot a) = \varphi(1_{R_1})\varphi(a) \\ &\Rightarrow \varphi(1_{R_1}) = 1_{R_2}.\end{aligned}$$

2) φ 为同构 $\Leftrightarrow \varphi$ 为同态 + 双射

③ φ 是 $(R_1, +)$ 到 $(R_2, +)$

引理 1: 设 $\varphi: R_1 \rightarrow R_2$ 为环同态, $I_2 \subseteq R_2$ 为理想 则 φ 是群同态

1) $\varphi^{-1}(I_2) := \{a \in R_1 \mid \varphi(a) \in I_2\}$ 为理想.

特别地: $\ker \varphi$ 是个理想.

2) $\text{Im } \varphi$ 为 R_2 的子环.

证: $\forall a, b \in \varphi^{-1}(I_2)$

$$\varphi(a), \varphi(b) \in I_2 \Rightarrow \varphi(a+b) = \varphi(a) + \varphi(b) \in I_2$$

$$\Rightarrow a+b \in \varphi^{-1}(I_2)$$

$\forall r \in R_1$,

$$\varphi(ra) = \varphi(r)\varphi(a) \in I_2, \quad \varphi(ar) = \varphi(a)\varphi(r) \in I_2$$

$\therefore ra, ar \in \varphi^{-1}(I_2) \therefore \varphi^{-1}(I_2)$ 为理想.

$\therefore \{0\}$ 为 R_2 中的理想

$\therefore \ker \varphi = \varphi^{-1}(0)$ 为 R_1 中的理想.

例: $R = \mathbb{Z}$, $m\mathbb{Z}$ 为理想

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \quad \text{为环同态}$$

$$n \longrightarrow n + m\mathbb{Z}$$

定理1: (同态基本定理) 设 I 为环 R 中的理想, 则 R/I 在加法运算 $(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$ 及乘法运算 $(r_1 + I)(r_2 + I) = r_1 r_2 + I$ 下构成环. 且 R/I 是 R 的同态像, 其核为 I . 反之, 设 $\varphi: R \rightarrow R'$ 为环同态, 则 $\ker \varphi$ 为理想且 $R/\ker \varphi \cong \text{Im } \varphi$

证: 仅需验证 $\pi: R \longrightarrow R/I$ 是环同态
$$r \longrightarrow r + I$$

$\forall r_1, r_2 \in R,$

$$\pi(r_1 + r_2) = r_1 + r_2 + I = r_1 + I + r_2 + I = \pi(r_1) + \pi(r_2)$$

$$\pi(r_1 r_2) = r_1 r_2 + I = (r_1 + I)(r_2 + I) = \pi(r_1) \pi(r_2)$$

(若 R 为含幺环, 则 $\pi(1_R) = 1_R + I$)

π 是满射, $\Rightarrow R/I = \text{Im } \pi$ (称 π 为自然同态)

由引理1知 $\ker \varphi$ 为理想, 记 $J = \ker \varphi$

定义映射: $f: R/J \longrightarrow \text{Im } \varphi$
$$r + J \longrightarrow \varphi(r)$$

• 良定的: $r_1 + J = r_2 + J \Rightarrow r_1 - r_2 \in J \Rightarrow \varphi(r_1 - r_2) = 0$

$$\Rightarrow \varphi(r_1) - \varphi(r_2) = 0 \Rightarrow \varphi(r_1) = \varphi(r_2)$$

• f 是环同态 (因为 φ 是环同态)

• f 是单的: $\varphi(r_1) = \varphi(r_2) \Rightarrow \varphi(r_1) - \varphi(r_2) = 0$
 $\Rightarrow \varphi(r_1 - r_2) = 0 \Rightarrow r_1 - r_2 \in J$
 $\Rightarrow r_1 + J = r_2 + J$

• f 是满的: 显然

$\therefore f$ 是同构, $\therefore R/J \cong \text{Im } \varphi$

定理2: 设 R 是环, $L \subseteq R$ 为子环, $I \subseteq R$ 为理想. 则

1) $I + L = \{x + y \mid x \in I, y \in L\}$ 为 R 的子环, 且 I 为其理想, $L \cap I$ 为 L 的理想

2) 映射 $\varphi: L/(L \cap I) \longrightarrow (I + L)/I$ 是环同构
$$y + (L \cap I) \longrightarrow y + I$$

从而 $L/(L \cap I) \cong (I + L)/I$.

证: 1) I, L 为 $(R, +)$ 的子群 $\Rightarrow I + L$ 为 $(R, +)$ 的子群

$$\forall a_1, a_2 \in I, b_1, b_2 \in L$$

$$(a_1 + b_1)(a_2 + b_2) = \underbrace{a_1 a_2}_I + \underbrace{a_1 b_2}_I + \underbrace{a_2 b_1}_I + \underbrace{b_1 b_2}_L \in I + L$$

$\therefore (I+L, \cdot)$ 为半群 $\Rightarrow (I+L, +, \cdot)$ 为子环

2) 考虑自然同态: $\pi: R \rightarrow R/I$ 令 $\pi_0 = \pi|_L$
 $r \mapsto r+I$

$$\text{则 } \text{Im } \pi_0 = \{r+I \mid r \in L\} = \{r+I \mid r \in I+L\} = (I+L)/I$$

$$\text{Ker } \pi_0 = \{r \in L \mid \pi(r) = 0\} = \{r \in L \mid r+I = I\} = I \cap L$$

由定理: $\pi_0: L/I \cap L \rightarrow (I+L)/I$ 为环同构.
 $r+I \cap L \mapsto r+I$

$$\therefore L/I \cap L \cong (I+L)/I \quad \square$$

R 为环 $I \subseteq R$ 为理想

记 $\Omega(R, I) = \{R \text{ 中包含 } I \text{ 的子环}\}$

$\Omega(R/I) = \{R/I \text{ 中所有子环}\}$

定理3: 设 R 为环, $L \subseteq R$ 为子环, $I \subseteq R$ 为理想且 $I \subseteq L$ 记 $\bar{L} = L/I$.

则 1) $\bar{L}$ 为 $\bar{R}$ 的子环

2) $\pi^*: \Omega(R, I) \rightarrow \Omega(\bar{R})$ 为双射
 $L \mapsto \bar{L}$

3) 若 $L \in \Omega(R, I)$ 则 L 为理想 $\Leftrightarrow \bar{L}$ 为理想, 此时有

$$R/L \cong \bar{R}/\bar{L} (= (R/I)/(\bar{L}/I))$$

证: 留作习题.

素理想: R 中理想 I 称为素理想, 如果 $I \neq R$ 且 $\forall a, b \in R$

$$ab \in I \Rightarrow a \in I \text{ 或 } b \in I.$$

极大理想: R 中理想 I 称为极大理想, 如果 $I \neq R$ 且若理想 J 满足

$$I \subseteq J, \text{ 则 } J = I \text{ 或 } J = R.$$

推论1: 设 R 为含幺交换环, 则 I 为极大理想 $\Leftrightarrow R/I$ 为域.

证: 注意到域只有平凡理想即零理想与其本身. 推论1由定理3

即可导出.

理想的运算: 设 $I_1, I_2, I_3, \dots$ 为 R 中理想

• 理想的乘积:

$$I_1 I_2 := \left\{ \sum_{i=1}^l a_i b_i \mid l > 0, a_i \in I_1, b_i \in I_2 \right\}$$

• 理想的和:

$$I_1 + I_2 := \{a + b \mid a \in I_1, b \in I_2\}$$

$$\text{易知: } (I_1 + I_2) I_3 = I_1 I_3 + I_2 I_3 \quad I_3 (I_1 + I_2) = I_3 I_1 + I_3 I_2$$

$$(I_1 I_2) I_3 = I_1 (I_2 I_3)$$

理想之交: $I_1 \cap I_2$ (对于任意多个理想其交依然是个理想)

$S \subseteq R$ 为子集: $\langle S \rangle :=$ 由 S 生成的理想 $= \bigcap_{\substack{I \text{ 理想} \\ S \subseteq I}} I$

$$= \text{包含 } I \text{ 的最小理想} = \left\{ \sum_{i=1}^l r_i a_i r'_i \mid l \geq 0, a_i \in S, r_i, r'_i \in R \right\}$$

$$\text{当 } R \text{ 为交换环时, 有 } \langle S \rangle = \left\{ \sum_{i=1}^l r_i a_i \mid l \geq 0, a_i \in S, r_i \in R \right\}$$

$$= \left\{ \sum_{a \in S} r_a a \mid r_a \in R \text{ 仅有有限个 } r_a \neq 0 \right\}$$

主理想: 理想 I 称为主理想, 如果 $\exists a \in I$ s.t. $I = \langle a \rangle$.

命题 1: 设 R 为交换环, $I, I_1, \dots, I_n$ 为理想满足: $I + I_i = R \quad \forall 1 \leq i \leq n$

$$\text{则 } I + I_1 \cap I_2 \cap \dots \cap I_n = R = I + I_1 I_2 \dots I_n$$

证: $I_1 I_2 \dots I_n \subseteq I_1 \cap I_2 \cap \dots \cap I_n \Rightarrow$ 只需证 $R = I + I_1 I_2 \dots I_n$

当 $n=1$ 时显然. 假设对 $n \leq k$ 时命题成立. 即 $I + I_1 I_2 \dots I_k = R$

$$\therefore \exists a_1 \in I, b_1 \in I_1 I_2 \dots I_k \text{ s.t. } a_1 + b_1 = 1.$$

另一方面, $\exists a_2 \in I, b_2 \in I_{k+1}$ s.t. $a_2 + b_2 = 1 \Rightarrow R = I + I_1 I_2 \dots I_k$

$$\therefore 1 = (a_1 + b_1)(a_2 + b_2) = a_1 a_2 + a_1 b_2 + b_1 a_2 + b_1 b_2 \in I + I_1 I_2 \dots I_k \quad \square$$

直和: 设 $R_1, \dots, R_n$ 为环. 令 $R = R_1 \times R_2 \times \dots \times R_n$ 笛卡尔积.

在 R 上定义: $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$$

易知 $(R, +, \cdot)$ 构成环. 称为 $R_1, \dots, R_n$ 的 (外) 直和. 记作 $R_1 \oplus R_2 \oplus \dots \oplus R_n$.

$\pi_i: R_1 \oplus \dots \oplus R_n \rightarrow R_i$ 为满同态.

$$(a_1, \dots, a_i, \dots, a_n) \rightarrow a_i$$

记 $I_i = \{ (0, \dots, 0, a_i, 0, \dots, 0) \mid a_i \in R_i \}$

则 $I_i \subseteq R_i$ 且 $I_i \subseteq R$ 为理想, $R = I_1 + \dots + I_n$

反之, 设 R 为环, $I_1, \dots, I_n$ 为理想满足 $R = I_1 + \dots + I_n$ 且

$$I_i \cap \left(\sum_{j \neq i} I_j \right) = \{0\}.$$

则称 R 为 $I_1, \dots, I_n$ 的 (内) 直和. $\leftarrow$ §2: 环论初步

欧几里得环: 整环 R 称为欧几里得环, 如果 $\exists \delta: R \setminus \{0\} \rightarrow \mathbb{Z}_{>0} = \{n \in \mathbb{Z} \mid n > 0\}$

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

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

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

$$r \rightarrow |r|$$

ii) $R = F[X], \delta: F[X] \setminus \{0\} \rightarrow \mathbb{Z}_{>0}$

$$f \rightarrow \deg(f).$$

设 R 为整环, $r \in R$ 称为不可约元, 如果 $r = ab$, 其中 $a, b \in R$, 则 $a \in U(R)$ 或 $b \in U(R)$.

直和泛性质: 设 K 为任意环

$\varphi_i: K \rightarrow R_i$ 为环同态

则 $\exists!$ 环同态 $\varphi: K \rightarrow R$

$$\text{s.t. } \varphi_i = \pi_i \circ \varphi$$

$$\forall 1 \leq i \leq n.$$

记号: $a|r$ 表示 $\exists b \in R$ s.t. $r = ab$.