

## 0.1 环

### 定义 0.1 (环)

我们称  $(R, +, \cdot)$  是一个**环**, 当  $(R, +)$  是个阿贝尔群,  $(R, \cdot)$  是个么半群, 且乘法对加法有左右分配律, 即

$$\forall a, b, c \in R, a(b+c) = ab+ac,$$

$$\forall a, b, c \in R, (a+b)c = ac+bc.$$



**注** 我们把环  $(R, +, \cdot)$  中的加法单位元记作  $0$ , 乘法单位元记作  $1$ . 对任意的  $a \in R$ , 我们将  $a$  的加法逆元记作  $-a$ , 乘法逆元记作  $a^{-1}$ .

**笔记** 最常见的环是整数环  $(\mathbb{Z}, +, \cdot)$ .

### 定义 0.2 (交换环)

设  $(R, +, \cdot)$  是一个环, 我们称  $R$  是一个**交换环**, 当  $R$  对乘法有交换律, 即

$$\forall a, b \in R, ab = ba.$$

也即  $(R, \cdot)$  是一个交换么半群.



### 例题 0.1

- $(\mathbb{Z}_n, +, \cdot)$  是一个交换环.
- $(M(n, \mathbb{R}), +, \cdot)$  是一个环 (不是交换环).

### 证明

- 由命题??可知  $(\mathbb{Z}_n, +)$  是一个 Abel 群. 又由命题??可知  $(\mathbb{Z}_n, \cdot)$  是一个交换么群. 因此我们只须证明分配律即可. 对  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ , 都有

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

$$(\bar{a} + \bar{b})\bar{c} = (\overline{a+b})\bar{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac} + \overline{bc} = \bar{a}\bar{c} + \bar{b}\bar{c}.$$

综上,  $(\mathbb{Z}_n, +, \cdot)$  是一个交换环.

- $(M(n, \mathbb{R}), +, \cdot)$  是一个环的证明是显然的.

□

### 命题 0.1

设  $(R, +, \cdot)$  是一个环, 而  $a, b, c \in R$ , 则

- $a0 = 0a = 0$ ,
- $a(-b) = (-a)b = -(ab)$ ,
- $(-a)(-b) = ab$ .



### 证明

- 首先, 利用分配律,

$$a0 = a(0+0) = a0 + a0.$$

因此  $a0 = 0$ . 根据对称性,  $0a = a$ .

- 根据对称性, 我们只须证明  $a(-b) = -(ab)$ . 而这是因为

$$a(-b) + ab = a(-b+b) = a0 = 0.$$

- 利用两次 (2) 的结论和命题??, 我们就得到

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

**定义 0.3 (零环)**

有一个重要的环是零环,它是最平凡的环,即  $(0, +, \cdot)$ , 也记作  $\{0\}$ . 它只有一个元素,既是加法单位元也是乘法单位元, 定义为

$$\begin{aligned} 00 &= 0, \\ 0 + 0 &= 0. \end{aligned}$$



**笔记** 很容易检验这是一个环.

**命题 0.2 (零环的充要条件)**

设  $(R, +, \cdot)$  是一个环, 则  $R = \{0\}$  当且仅当  $0 = 1$ .



**证明** 必要性 ( $\Rightarrow$ ) 是显然的.

我们来证明充分性 ( $\Leftarrow$ ). 假设  $0 = 1$ , 我们只须证明对所有  $a \in R$ , 都有  $a = 0$ .

$$a = a1 = a0 = 0$$

这就证明了这个命题.

**定义 0.4 (单位及所有单位构成的群)**

设  $(R, +, \cdot)$  是一个环, 则  $(R^\times, \cdot)$ , 是由  $R$  中所有乘法可逆元素构成的群.  $R$  中的乘法可逆元素又被称为  $R$  中的**单位**.



**注** 由引理??可知,  $R$  中所有乘法可逆元素构成了一个群. 故上述  $(R^\times, \cdot)$  的定义是良定义的.

**命题 0.3**

设  $(R, +, \cdot)$  是一个环, 若  $R \neq \{0\}$ , 则  $0$  一定不是单位,  $1$  一定是单位.



**证明** 因为  $R \neq \{0\}$ , 所以由**命题 0.2**可知  $0 \neq 1$ . 于是对  $\forall a \in R$ , 由**命题 0.1**可知  $a \cdot 0 = 0 \neq 1$ . 故  $0$  一定没有逆元, 即  $0$  不是单位.

由于  $1 \cdot 1 = 1$ , 因此  $1$  的逆元就是其自身, 故  $1$  一定是单位.

**定义 0.5 (除环)**

设  $(R, +, \cdot)$  是一个环, 我们称  $(R, +, \cdot)$  是一个**除环**, 若

$$R \setminus \{0\} = R^\times$$

也即, 所有非零元素都是单位.

**命题 0.4 (除环的充要条件)**

$(R, +, \cdot)$  是一个除环, 当且仅当同时满足下面三个条件

- (i)  $(R, +)$  是一个 Abel 群,
- (ii)  $(R \setminus \{0\}, \cdot)$  是一个群,
- (iii) 乘法对加法有左右分配律.



**证明** 根据定义, 这是显然的.



**定义 0.6 (交换的除环)**

设  $(R, +, \cdot)$  是一个除环, 我们称  $(R, +, \cdot)$  是一个**交换的除环**, 当  $R$  对乘法有交换律, 即

$$\forall a, b \in R, ab = ba.$$

即  $(R, \cdot)$  是一个交换么半群. 也即  $(R \setminus \{0\}, \cdot) = (R^\times, \cdot)$  是一个 Abel 群.

**定义 0.7 (域)**

设  $(R, +, \cdot)$  是一个环, 我们称  $(R, +, \cdot)$  是一个**域**, 若它是一个交换的除环.

**命题 0.5 (域的充要条件)**

$(R, +, \cdot)$  是一个域, 当且仅当同时满足下面三个条件


- (i)  $(R, +)$  是一个 Abel 群,
- (ii)  $(R \setminus \{0\}, \cdot)$  是一个 Abel 群,
- (iii) 乘法对加法有左右分配律.

**证明** 根据定义, 这是显然的. □

**定义 0.8 (子环)**

设  $(R, +, \cdot)$  是一个环, 而  $S \subset R$ . 我们称  $S$  是  $R$  的**子环**, 记作  $S < R$ , 若同时满足下面三个条件


- (i)  $0, 1 \in S$ ,
- (ii)  $\forall a, b \in S, a + b, ab \in S$ ,
- (iii)  $\forall a \in S, -a \in S$ .

 **笔记** 事实上, 这就是说  $(S, +)$  是  $(R, +)$  的子群,  $(S, \cdot)$  是  $(R, \cdot)$  的子么半群. 又因为  $(R, +)$  是 Abel 群, 所以  $(S, +)$  一定是  $(R, +)$  的正规子群.

**引理 0.1 (子环的充要条件)**

设  $(R, +, \cdot)$  是一个环, 而  $S \subset R$ , 则  $S < R$  当且仅当

$$\begin{aligned} 1 &\in S, \\ \forall a, b \in S, a - b, ab &\in S. \end{aligned}$$

 **笔记** 例如  $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ .

**证明** 假如满足了这两个条件, 那么  $0 = 1 - 1 \in S$ . 而  $-a = 0 - a \in S, a + b = a - (-b) \in S$ . 这就证明了这是个子环. 另一个方向是显然的. 假如  $S$  是子环, 那么  $a - b = a + (-b) \in S$ . □

**命题 0.6 (子环仍是环)**

设  $(R, +, \cdot)$  是一个环,  $S$  是其子环, 则  $(S, +, \cdot)$  也是环.

**证明** 由子环的定义可知  $S$  对加法和乘法满足封闭性, 从而加法和乘法是  $S$  上代数运算. 于是再结合  $0, 1 \in S$  且  $S \subset R$ , 将  $(R, +, \cdot)$  的性质照搬过来即可. □

**定义 0.9 (由子集生成的子环)**

设  $(R, +, \cdot)$  是一个环, 而  $A \subset R$ , 则  $A$  **生成的子环**, 记作  $\langle A \rangle$ , 定义为所有包含了  $A$  的子环的交集, 即

$$\langle A \rangle = \bigcap \{S \subset R : S \supset A, S < R\}.$$

**命题 0.7 (由子集生成的子环仍是子环)**

设  $(R, +, \cdot)$  是一个环, 而  $A \subset R$ , 则  $\langle A \rangle \leq R$ .

**证明** 首先这个集族是非空的, 因为  $R$  本身就是一个包含了  $A$  的子环.

接下来, 我们利用上面的引理. 令  $S$  是一个包含了  $A$  的子环. 因为  $1$  在每一个这样的  $S$  中, 所以  $1 \in \langle A \rangle$ .

令  $a, b \in \langle A \rangle$ , 则  $a - b, ab$  在每一个这样的  $S$  中, 因为每一个  $S$  都是子环. 因此  $a - b, ab \in \langle A \rangle$ .

综上所述,  $\langle A \rangle \leq R$ . □

**定义 0.10 (环的直积)**

设  $((R_i, +_i, \cdot_i)_{i \in I})$  是一族环. 我们定义这一族环的**直积**, 为  $(\prod_{i \in I} R_i, +, \cdot)$ . 对于  $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} R_i$ , 我们

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i +_i y_i)_{i \in I} \quad (1)$$

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I} \quad (2)$$

**命题 0.8 (环的直积仍是环)**

设  $((R_i, +_i, \cdot_i)_{i \in I})$  是一族环, 则它们的直积  $(\prod_{i \in I} R_i, +, \cdot)$  还是一个环.

**证明** 由命题??和命题??可知, 么半群和 Abel 群对直积是保持的, 从而我们立刻知道  $\prod_{i \in I} R_i$  对加法构成 Abel 群, 对乘法构成么半群. 因此只须检验乘法对加法的左右分配律. 根据对称性, 我们只证明左分配律.

由于  $((R_i, +_i, \cdot_i)_{i \in I})$  是一族环, 因此  $((R_i, +_i, \cdot_i)_{i \in I})$  的乘法对加法有左分配律. 故令  $(x_i)_{i \in I}, (y_i)_{i \in I}, (z_i)_{i \in I} \in \prod_{i \in I} R_i$ , 则

$$\begin{aligned} (x_i)_{i \in I} \cdot ((y_i)_{i \in I} + (z_i)_{i \in I}) &= (x_i \cdot_i (y_i +_i z_i))_{i \in I} = (x_i \cdot_i y_i +_i x_i \cdot_i z_i)_{i \in I} \\ &= (x_i \cdot_i y_i)_{i \in I} + (x_i \cdot_i z_i)_{i \in I} = (x_i)_{i \in I} \cdot (y_i)_{i \in I} + (x_i)_{i \in I} \cdot (z_i)_{i \in I}. \end{aligned}$$

因此,  $(\prod_{i \in I} R_i, +, \cdot)$  是一个环. 这就证明了这个命题. □