

# 第一章 环、模

## 1.1 环的定义

### 1.1.1 环的定义

#### 定义 1.1.1

$R$  是一个集合，如果存在两个运算  $+: R \times R \rightarrow R$  和  $\cdot: R \times R \rightarrow R$  分别称为加法和乘法，满足下列条件：

- ①（加法单位元存在）存在一个元素  $0_R \in R$ ，称为加法单位元，使得对于任意  $x \in R$ ，有  $x + 0_R = 0_R + x = x$ 。
  - ②（加法交换律） $\forall x, y \in R, x + y = y + x$
  - ③（加法结合律） $\forall x, y, z \in R, (x + y) + z = x + (y + z)$
  - ④（加法逆存在） $\forall x \in R, \exists -x \in R$ ，称为加法逆，使得  $x + (-x) = 0_R$
  - ⑤（乘法结合律） $\forall x, y, z \in R, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
  - ⑥（左分配律） $\forall x, y, z \in R, x \cdot (y + z) = x \cdot y + x \cdot z$   
（右分配律） $\forall x, y, z \in R, (y + z) \cdot x = y \cdot x + z \cdot x$
- 那么我们称  $(R, +, \cdot)$  是一个环，简称为环  $R$ 。

相比域的定义，环的定义仅涉及 6 条性质，去除了单位元存在、可交换、可逆三条性质。在研究环时，我们有时也会考虑存在单位元和可交换的环，因此有以下定义：

#### 定义 1.1.2: 交换环、幺环

如果环  $R$  满足： $\forall x, y \in R, x \cdot y = y \cdot x$ ，那么我们称  $R$  是一个交换环；

如果环  $R$  满足： $\exists 1_R \in R, \forall x \in R, 1_R \cdot x = x \cdot 1_R = x$ ，称为乘法单位元，

## 1.1.2 环的性质

## 1.1.3 整环

## 定义 1.1.3: 零因子

设  $R$  是一个环, 如果  $\exists x, y \in R, x, y \neq 0_R$ , 使得  $x \cdot y = 0_R$ , 那么我们称  $x, y$  是  $R$  的零因子。

## 定义 1.1.4: 整环

如果环  $R$  是一个交换幺环, 并且不包含零因子, 那么我们称  $R$  是一个整环。

## 定理 1.1.1: 循环的整环必有素零因子

设  $R$  是一个整环,

我们定义:  $N: \mathbb{Z} \ni n \mapsto n_R \in R$ , 满足  $(n+1)_F = n_F + 1_F$

如果  $\exists a \in R, a \neq 0, \exists n \in \mathbb{N}_+, n_F a = 0_R$

那么存在素数  $p$ ,  $\forall b \in R, p_R b = 0_R$

证明: 取  $\forall b \in R$ ,

$$0_R = 0_R \cdot b = (n_R a) b = a(n_R b)$$

因为  $a \neq 0$ , 而  $R$  是整环, 所以一定有  $n_R b = 0$ , 因此,  $\{k \in \mathbb{N}_+ | k_R b = 0\}$  不是空集。

取  $p$  为使  $p_R b = 0$  的最小正整数。如果  $p$  是素数, 命题成立;

如果  $p$  不是素数, 那么只需要对  $p$  作唯一分解, 那么有  $\left(\prod_{i=1}^q p_{i_R}\right) b = 0$

那么, 一定存在一个  $p_{i_R} b = 0$ , 此时命题也是成立的。□

## 1.1.4 子环

我们也类似地提出后续我们会提及的子环的概念。

## 定义 1.1.5: 子环

设  $R$  是一个环, 集合  $S \subseteq R$ ,

如果  $S$  对  $R$  上的加法和乘法也构成一个环, 那么我们称  $S$  是  $R$  的子环。

## 1.2 环的同态

我们类似于域的同态，定义出环的同态。

### 1.2.1 定义

#### 定义 1.2.1: 环同态

设  $R, S$  是两个环，如果映射  $\varphi: R \rightarrow S$  满足：

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

并且如果  $R, S$  均是幺环， $\varphi(1_R) = 1_S$

那么我们称  $\varphi$  是一个  $R$  到  $S$  的环同态。

显然，同态一定将零元映射到零元

**命题 1.2.1.** 设  $\varphi: R \rightarrow S$  是一个环同态，那么  $\varphi(0_R) = 0_S$

**证明:**  $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$

$$\Rightarrow -\varphi(0_R) + \varphi(0_R) = -\varphi(0_R) + \varphi(0_R) + \varphi(0_R)$$

$$\Rightarrow \varphi(0_R) = 0_S$$

□

#### 定义 1.2.2: 单同态、满同态、同构

假设有环同态  $\psi: R \rightarrow S$

如果  $\psi$  是单射，那么称它是一个单同态；

如果  $\psi$  是满射，那么称它是一个满同态；

如果  $\psi$  是双射，称它是一个同构；

同构是最严格的同态，表示两个环在结构上是完全相同的，有以下显而易见的事实：

**命题 1.2.2.** 如果  $\psi: R \rightarrow S$  是一个环同构，那么  $\psi^{-1}: S \rightarrow R$  也是一个环同构

**证明:**  $\psi(\psi^{-1}(a) + \psi^{-1}(b)) = \psi(\psi(a)) + \psi(\psi(b)) = a + b$

因为  $\psi$  是双射，所以有  $\psi^{-1}(a) + \psi^{-1}(b) = \psi^{-1}(a + b)$

同理， $\psi(\psi^{-1}(a)\psi^{-1}(b)) = \psi(\psi(a))\psi(\psi(b)) = ab$

$\Rightarrow \psi^{-1}(a)\psi^{-1}(b) = \psi^{-1}(ab)$ ，于是命题得证

□

## 1.2.2 同态的核、像

## 定义 1.2.3: 环同态的核、像

设  $\psi: R \rightarrow S$  是一个环同态, 我们定义:

$\ker \psi = \{a \in R | \psi(a) = 0_S\}$ , 称为  $\psi$  的核

$\text{Im } \psi = \{\psi(a) | a \in R\}$ , 称为  $\psi$  的像

与域的同态不同, 环的同态的核并不是平凡的, 因为域同态未必是单射。因此, 我们需要研究环同态的核与像。

但是, 受限于目前的知识, 我们暂时无法证明核与像的一些进阶性质, 我们仅仅证明一些简单的性质。

**命题 1.2.3.** 设  $\psi: R \rightarrow S$  是一个环同态, 那么  $\ker \psi$  是一个  $R$  的子环

**证明:** 取  $\forall a, b \in \ker \psi$ , 那么有  $\psi(a) = \psi(b) = 0$

我们注意到:  $\psi(0_R) = 0_S \Rightarrow 0_R \in \ker \psi, a + 0_R = a$

$\psi(a + (-a)) = 0_S \Rightarrow \psi(a) + \psi(-a) = 0_S \Rightarrow \psi(-a) = 0_S \Rightarrow -a \in \ker \psi, a + (-a) = 0_R$

加法的交换律、结合律, 乘法的结合律, 左、右分配律是显然成立的。□

**命题 1.2.4.** 设  $\psi: R \rightarrow S$  是一个环同态, 那么  $\text{Im } \psi$  是一个  $S$  的子环

**证明:** 取  $\forall a, b \in \text{Im } \psi$ , 那么有  $\exists x, y \in R, \psi(x) = a, \psi(y) = b$

我们注意到:  $\psi(0_R) = 0_S \Rightarrow 0_S \in \text{Im } \psi, \psi(x) + \psi(0_R) = \psi(x)$

$\psi(x) + \psi(-x) = \psi(x + (-x)) = \psi(0_R) = 0_S \Rightarrow \psi(-x) = -\psi(x) = -a \in \text{Im } \psi, a + (-a) =$

$0_S$

加法的交换律、结合律, 乘法的结合律, 左、右分配律是显然成立的。□

## 1.3 环的理想

### 1.3.1 理想的定义

#### 定义 1.3.1: 理想

设  $R$  是一个环,  $R$  是  $R$  的一个子环。

如果  $\forall a \in S, b \in R, ab \in S$ , 那么我们称  $S$  是  $R$  的一个左理想;

如果  $\forall a \in S, b \in R, ba \in S$ , 那么我们称  $S$  是  $R$  的一个右理想;

如果  $S$  既是  $R$  的左理想, 又是  $R$  的右理想, 那么我们称  $S$  是  $R$  的一个双理想。

显然,  $\{0_R\}, R$  都是  $R$  的理想, 我们称之为平凡理想。

我们观察到: 一些环, 比如说  $\mathbb{Z}$ , 他们有一种特殊的理想, 比如说  $\forall m \in \mathbb{Z}, m\mathbb{Z}$  是  $\mathbb{Z}$  的一个理想。我们把这种直接由一个元素“生成”的理想叫主理想。

#### 定义 1.3.2: 主理想

设  $R$  是一个环, 如果  $R$  的一个理想  $S$  满足:

$\exists a \in R, S = aR := \{ab | b \in R\}$ , 那么我们称  $S$  是由  $a$  生成的主理想, 记作  $(a)$

### 1.3.2 理想的性质

1.

**命题 1.3.1.** 设  $\psi: R \rightarrow S$  是一个环同态, 那么  $\ker \psi$  是  $S$  的一个理想

**证明:** 取  $\forall a \in \ker \psi$ , 依核的定义,  $\psi(a) = 0_S$

那么,  $\forall b \in R, \psi(ab) = \psi(a)\psi(b) = 0_S, \psi(ba) = \psi(b)\psi(a) = 0_S$

因此,  $ab, ba \in \ker \psi$ , 于是命题得证。□

2.

**命题 1.3.2.** 设  $R$  是一个么环,  $S$  是  $R$  的一个理想, 如果  $1_R \in S$ , 那么  $S = R$

**证明:**

□

3.

**命题 1.3.3.** 域只有平凡理想

证明:

□

## 1.4 商环

## 1.5 模

本节我们研究一种“环上的线性空间”，也就是模

### 1.5.1 模的定义

#### 定义 1.5.1: 左模

设  $R$  是一个环,  $M$  是一个集合, 如果存在两个运算  $+: M \times M \rightarrow M, \cdot_R: R \times M \rightarrow M$  分别称为称为加法和纯量乘法, 满足下列条件:

- ①  $\exists 0_M \in M$ , 称为加法单位元,  $\forall \alpha \in M, 0_M + \alpha = \alpha + 0_M = \alpha$
- ②  $\forall \alpha, \beta \in M, \alpha + \beta = \beta + \alpha$
- ③  $\forall \alpha, \beta, \gamma \in M, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
- ④  $\forall \alpha \in M, \exists -\alpha \in M$ , 称为加法逆, 使得  $\alpha + (-\alpha) = 0_M$
- ⑤  $\forall a, b \in R, \alpha \in M, a(b\alpha) = (ab)\alpha$
- ⑥  $\forall a \in R, \alpha, \beta \in M, a(\alpha + \beta) = a\alpha + a\beta$
- ⑦  $\forall a, b \in R, \alpha \in M, (a + b)\alpha = a\alpha + b\alpha$

那么我们称  $M$  是一个左  $R$ -模

类似地, 我们也有右模的定义:

**定义 1.5.2: 右模**

设  $R$  是一个环,  $M$  是一个集合, 如果存在两个运算  $+: M \times M \rightarrow M, \cdot_R: M \times R \rightarrow M$  分别称为称为加法和纯量乘法, 满足下列条件:

- ①  $\exists 0_M \in M$ , 称为加法单位元,  $\forall \alpha \in M, 0_M + \alpha = \alpha + 0_M = \alpha$
- ②  $\forall \alpha, \beta \in M, \alpha + \beta = \beta + \alpha$
- ③  $\forall \alpha, \beta, \gamma \in M, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
- ④  $\forall \alpha \in M, \exists -\alpha \in M$ , 称为加法逆, 使得  $\alpha + (-\alpha) = 0_M$
- ⑤  $\forall a, b \in R, \alpha \in M, (\alpha a)b = \alpha(ab)$
- ⑥  $\forall a \in R, \alpha, \beta \in M, (\alpha + \beta)a = \alpha a + \beta b$
- ⑦  $\forall a, b \in R, \alpha \in M, \alpha(a + b) = \alpha a + \alpha b$

那么我们称  $M$  是一个右  $R$ -模

如果  $M$  兼具左模和右模的特征, 我们称  $M$  是一个双模:

**定义 1.5.3: 双模**

如果  $M$  既是左  $R$ -模, 又是右  $S$ -模, 并且满足:

$$(a\alpha)b = a(\alpha b)$$

那么我们称  $M$  是一个  $(R, S)$ -双模

我们也知道, 环不一定有乘法单位元, 因此有以下定义:

**定义 1.5.4: 幺模**

设  $R$  是幺环,  $M$  是一个  $R$ -模

如果  $\forall \alpha \in M, 1_R \cdot \alpha = \alpha$ , 那么我们称  $M$  是一个幺模。

在后续中, 除非特别做区分, 我们都假定我们说的模指的是左模。

### 1.5.2 模的同态

#### 定义 1.5.5: 模同态

设  $M, N$  是两个  $R$ -模, 如果映射  $\psi: M \rightarrow N$  满足:

$$\forall \alpha, \beta \in M, \psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$$

$$\forall a \in R, \alpha \in M, \psi(a\alpha) = a\psi(\alpha)$$

那么称  $\psi$  是一个从  $M$  到  $N$  的模同态。