

## 0.1 环与域

### 定义 0.1 (环)

若在非空集合  $R$  中定义了加法和乘法两种二元运算，并满足下列条件：

- (1)  $R$  对加法为 Abel 群；
- (2)  $R$  对乘法为半群；
- (3) 加法与乘法间有分配律，即  $\forall a, b, c \in R$ ,

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca,$$

则称  $R$  是一个环.



### 命题 0.1

一切数域都是环.



### 证明



### 例题 0.1

- (1)  $\mathbb{Z}$  对加法与乘法是环，称为整数环。
- (2) 数域  $P$  上的  $n$  元多项式集合  $P[x_1, x_2, \dots, x_n]$  对多项式的加法和乘法是环，称为  $P$  上的  $n$  元多项式环。
- (3)  $R^{n \times n}$  表示以环  $R$  中元素为矩阵元的  $n$  阶方阵的集合，即  $\alpha \in R^{n \times n}$  可写成

$$\alpha = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad a_{ij} \in R.$$

记  $a_{ij} = \text{ent}_{ij}(\alpha)$ . 由下面的两个关系：

- (i)  $\text{ent}_{ij}(\alpha + \beta) = \text{ent}_{ij}(\alpha) + \text{ent}_{ij}(\beta)$ ;
- (ii)  $\text{ent}_{ij}(\alpha\beta) = \sum_{k=1}^n \text{ent}_{ik}(\alpha)\text{ent}_{kj}(\beta)$

定义的  $R^{n \times n}$  加法与乘法使其成为一个环，称为  $R$  上的  $n$  阶方阵环。

- (4) 设  $C([a, b])$  是闭区间  $[a, b]$  上的连续函数的集合，它对函数的加法与乘法是一个环，称为  $[a, b]$  上的连续函数环。
- (5) 设  $A$  是一个 Abel 群， $A$  的运算是加法。在  $A$  中定义乘法运算为  $ab = 0 (\forall a, b \in A)$ ，则  $A$  为一环，这种环称为零环。

**注** (5) 说明，任何 Abel 群均可作为零环的加法群，但是并非所有 Abel 群都可成为非零环的加法群。

### 证明



### 定理 0.1 (环的基本性质)

- (1) 在环  $R$  中可定义任何整数的倍数及正整数次乘幂，并且满足

- (i)  $\forall m, n \in \mathbb{Z}, a, b \in R$ ,

$$(m+n)a = ma + na,$$

$$(mn)a = m(na),$$

$$m(a+b) = ma + mb;$$

- (ii)  $a^m \cdot a^n = a^{m+n}$ ,  $(a^m)^n = a^{mn}$ ,  $\forall m, n \in \mathbb{N}, a \in R$ ;  
 (iii) 若  $a, b \in R$  且  $ab = ba$ , 则  $(ab)^m = a^m b^m$ ,  $\forall m \in \mathbb{N}$ .

(2) 由分配律成立有

$$\sum_{i=1}^m \sum_{j=1}^n a_i b_j = \sum_{j=1}^n \sum_{i=1}^m a_i b_j.$$

- (3)  $\forall a, b \in R$  有  $a0 = 0a = 0$ ,  $(-a)b = a(-b) = -ab$ ,  $(-a)(-b) = ab$ .



## 证明

(1)

(2)

(3) 事实上, 由  $a \cdot 0 + ab = a(0 + b) = ab$  知  $a \cdot 0 = 0$ . 同样  $0 \cdot a = 0$ ,  $a(-b) = a(-b) + ab + (-ab) = -ab$ . 最后  $(-a)(-b) = -(a(-b)) = -(-ab) = ab$ .



## 定义 0.2

1. **交换环:** 乘法是交换半群的环.
2. **么环:** 乘法是么半群的环, 通常记么元为 1.
3. **交换么环:** 乘法是交换么半群的环.
4. **无零因子环:** 任意两个非零元的积不为零的环.
5. 设  $R$  是环.  $a, b \in R$  且  $a \neq 0, b \neq 0$ . 若  $ab = 0$ , 则称  $a$  是  $R$  的一个左零因子,  $b$  是  $R$  的一个右零因子, 都简称为零因子. 有时为方便也将 0 称为零因子.
6. **整环:** 无零因子的么环. 即若  $a, b \in \mathbb{R} \setminus \{0\}$ , 则  $ab \neq 0$ . 也即若  $a, b \in \mathbb{R}$  且  $ab = 0$ , 则  $a = 0$  或  $b = 0$ .
7. **体:** 非零元素集合对乘法构成群的环, 即非零元素都可逆的么环.
8. **域:** 交换的除环, 即非零元素集合对乘法为 Abel 群的环.



**注** 当  $n > 1$  时,  $R$  上的  $n$  阶方阵环  $R^{n \times n}$  就不是无零因子环.

显然, 一切数域  $P$  都是域, 因而也是体.

## 定义 0.3

1. 设  $R$  是一个体, 若  $R_1$  对  $R$  中的加法和乘法也构成体且  $R_1 \subseteq R$ , 则称  $R_1$  是  $R$  的子体.
2. 设  $R$  是一个域, 若  $R_1$  对  $R$  中的加法和乘法也构成域且  $R_1 \subseteq R$ , 则称  $R_1$  是  $R$  的子域.  
若  $R$  是域  $F$  的子域, 则称  $F$  是  $R$  的扩域.



## 命题 0.2

- (1) 体一定是整环, 进而域也一定是整环.
- (2) 若  $R$  是一个体, 则  $G$  的任意子体的交也是  $R$  的子体.
- (3) 若  $R$  是一个域, 则  $G$  的任意子体的交也是  $R$  的子域.



## 证明

(1) 设  $R$  是一个体,  $a, b \in R$  且  $ab = 0$ . 若  $a \neq 0$ , 则  $b = a^{-1}(ab) = 0$ ; 若  $b \neq 0$ , 则  $a = (ab)b^{-1} = 0$ . 故  $R$  是整环.

(2)

(3)



**命题 0.3**

- (1) 环  $R$  为整环的充要条件是  $R$  的非零元素集合  $R^* = R \setminus \{0\}$  是乘法幺半群  $R$  的子幺半群.  
(2) 若  $R$  是交换整环, 则  $R^* = R \setminus \{0\}$  对乘法构成交换幺半群且消去律成立, 即

$$ax = bx \text{ (或 } xa = xb), \text{ 则 } a = b, \forall a, b, x \in R^*$$

- (3) 若  $R$  是整环且  $\prod_{i=1}^k a_i = 0, a_i \in R$ , 则存在  $i_0 \in [1, k] \cap \mathbb{N}$ , 使  $a_{i_0} = 0$ .

**证明**

- (1)  
(2) 因为  $R$  是交换整环且  $R^* \subseteq R$ , 所以  $R$  对乘法构成交换幺半群. 设  $a, b, x \in R^*$  且  $ax = bx$ , 则  $(a - b)x = 0$ . 由于  $R$  是整环且  $x \neq 0$ , 故  $a - b = 0$ , 即  $a = b$ .  $xa = xb$  的情况同理可证.  
(3) 由整环定义易得.

**命题 0.4**

设  $p$  是一个素数, 则  $\mathbb{Z}_p = \{0, 1, \dots, \overline{p-1}\}$  是只含  $p$  个元素的域且非数域.



**证明** 由  $p$  是一个素数易知  $\mathbb{Z}$  中关系  $a \equiv b \pmod{p}$  对加法及乘法都是同余关系, 因而在  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$  中有加法运算, 使  $\mathbb{Z}_p$  为 Abel 群, 而且在  $\mathbb{Z}_p$  中有乘法运算, 使  $\mathbb{Z}_p$  为交换幺半群.  $\mathbb{Z}_p = \{0, 1, \dots, \overline{p-1}\}$ . 又  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$  有

$$\bar{a}(\bar{b} + \bar{c}) = \overline{\bar{a}(\bar{b} + \bar{c})} = \overline{\bar{a}\bar{b} + \bar{a}\bar{c}} = \overline{\bar{a}\bar{b}} + \overline{\bar{a}\bar{c}} = \bar{a}\bar{b} + \bar{a}\bar{c},$$

即分配律成立. 故  $\mathbb{Z}_p$  是交换幺环. 又对  $a \in \mathbb{N}, a < p$ , 由  $p$  为素数知有  $m, n \in \mathbb{Z}$ , 使  $ma + np = 1$ , 因而  $\overline{m} \cdot \bar{a} = \bar{1}$ , 即  $\mathbb{Z}_p$  中每个非零元素可逆, 因而  $\mathbb{Z}_p$  是只含  $p$  个元素的域且非数域.

**定理 0.2**

设  $\mathbb{C}$  为复数域. 考虑  $\mathbb{C}^{2 \times 2}$  中子集

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}.$$

证明  $H$  是体, 称  $H$  为  $\mathbb{R}$  上的四元数体.



**证明** 容易验证  $H$  对矩阵的加法为 Abel 群. 又对  $\forall \alpha, \beta, \gamma, \delta \in \mathbb{C}$  有

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\bar{\alpha}\bar{\delta} - \bar{\beta}\gamma & \bar{\alpha}\bar{\gamma} - \bar{\beta}\delta \end{pmatrix} \in H,$$

故  $H$  对矩阵乘法为幺半群. 显然加法与乘法间有分配律, 故  $H$  为幺环. 又若

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq 0,$$

则

$$\begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta} > 0.$$

此时有

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}^{-1} = (\alpha\bar{\alpha} + \beta\bar{\beta})^{-1} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} \in H,$$

即  $H^* = H \setminus \{0\}$  为群, 因而  $H$  是体. 又  $H$  中有元素

$$\mathbf{A} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

由  $\mathbf{AB} \neq \mathbf{BA}$ , 故  $H$  是体, 但不是域.

□

### 命题 0.5

设  $\mathbb{H}$  为四元数体, 令

$$\begin{aligned} \mathbf{i} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \mathbf{j} &= \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \\ \mathbf{j} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \mathbf{k} &= \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}. \end{aligned}$$

则

$$\begin{aligned} \mathbf{i} \cdot \mathbf{j} &= \mathbf{k}, & \mathbf{i} \cdot \mathbf{k} &= -\mathbf{j}, \\ \mathbf{j} \cdot \mathbf{i} &= -\mathbf{k}, & \mathbf{j} \cdot \mathbf{k} &= \mathbf{i}, \\ \mathbf{k} \cdot \mathbf{i} &= \mathbf{j}, & \mathbf{k} \cdot \mathbf{j} &= -\mathbf{i}, \\ \mathbf{i}^2 &= \mathbf{i}, & \mathbf{j}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{i}, \\ \mathbf{i} \cdot \mathbf{i} &= \mathbf{i} \cdot \mathbf{i} = \mathbf{i}, & \mathbf{i} \cdot \mathbf{j} &= \mathbf{j} \cdot \mathbf{i} = \mathbf{j}, & \mathbf{i} \cdot \mathbf{k} &= \mathbf{k} \cdot \mathbf{i} = \mathbf{k}. \end{aligned}$$

并且有下面结论:

(1)  $\forall \alpha \in \mathbb{H}$ , 存在唯一的一组  $(a, b, c, d) \in \mathbb{R}^{1 \times 4}$ , 使得  $\alpha = a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k}$ . 进而

$$\mathbb{H} = \{a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}.$$

(2)  $\mathbb{H}$  的变换  $\sigma$ :

$$\sigma(a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k}) = a\mathbf{i} - b\mathbf{j} - c\mathbf{j} - d\mathbf{k}$$

是  $\mathbb{H}$  的一个对合.



**注** 我们一般省略不写  $\mathbf{i}$ , 即将  $a\mathbf{i}$  简写成  $a$ .

**证明**

(1) 根据定理 0.2,  $\alpha \in \mathbb{H}$  有  $a, b, c, d \in \mathbb{R}$ , 使得

$$\alpha = \begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix} = a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k}.$$

由

$$\begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix} = \begin{pmatrix} a_1 + b_1\sqrt{-1} & c_1 + d_1\sqrt{-1} \\ -c_1 + d_1\sqrt{-1} & a_1 - b_1\sqrt{-1} \end{pmatrix},$$

知当且仅当  $a_1 = a, b_1 = b, c_1 = c, d_1 = d$  结论 (1) 成立.

(2) 再设  $\beta = a_1\mathbf{i} + b_1\mathbf{j} + c_1\mathbf{j} + d_1\mathbf{k}, a_1, b_1, c_1, d_1 \in \mathbb{R}$ , 则

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta), \quad \forall \alpha, \beta \in \mathbb{H}.$$

$$\begin{aligned} \sigma(\alpha\beta) &= \sigma((a\mathbf{i} + b\mathbf{j} + c\mathbf{j} + d\mathbf{k})(a_1\mathbf{i} + b_1\mathbf{j} + c_1\mathbf{j} + d_1\mathbf{k})) \\ &= \sigma((aa_1 - bb_1 - cc_1 - dd_1)\mathbf{i} + (ab_1 + ba_1 + cd_1 - dc_1)\mathbf{j} + (ac_1 + ca_1 + db_1 - bd_1)\mathbf{j} + (ad_1 + da_1 + bc_1 - cb_1)\mathbf{k}) \\ &= (aa_1 - bb_1 - cc_1 - dd_1)\mathbf{i} - (ab_1 + ba_1 + cd_1 - dc_1)\mathbf{j} - (ac_1 + ca_1 + db_1 - bd_1)\mathbf{j} - (ad_1 + da_1 + bc_1 - cb_1)\mathbf{k} \\ &= (a_1\mathbf{i} - b_1\mathbf{j} - c_1\mathbf{j} - d_1\mathbf{k})(a\mathbf{i} - b\mathbf{j} - c\mathbf{j} - d\mathbf{k}) = \sigma(\beta)\sigma(\alpha). \end{aligned}$$

因此  $\sigma$  是  $\mathbb{H}$  的反自同构. 又因

$$\sigma^2(\alpha) = \sigma(a\mathbb{K} - b\mathbb{M} - c\mathbb{J} - d\mathbb{L}) = a\mathbb{K} + b\mathbb{M} + c\mathbb{J} + d\mathbb{L} = \alpha,$$

故  $\sigma$  是对合.

□

#### 定义 0.4

若环  $R$  的非空子集  $R_1$  对  $R$  的加法与乘法也构成环, 则称  $R_1$  为  $R$  的子环. 若  $R_1$  还满足  $RR_1 \subseteq R_1$  (或  $R_1R \subseteq R_1$ ), 则称  $R_1$  为  $R$  的左理想(或右理想). 若环  $R$  的非空子集  $I$  既是左理想又是右理想, 也即  $RR_1R \subseteq R_1$ , 则称  $I$  为  $R$  的双边理想, 简称理想.

♣

**注**  $\{0\}$  与  $R$  都是  $R$  的理想, 称为平凡理想. 在交换环中, 左理想、右理想与理想这三个概念是一致的.

#### 定理 0.3

- (1) 一个环中任意多个理想之交还是理想.
- (2) 若  $A$  是环  $R$  的理想,  $B$  是环  $R$  的子环且  $B \supseteq A$ , 则  $A$  也是环  $B$  的理想.
- (3) 若  $A$  是环  $R$  的非空子集, 则所有包含  $A$  的理想之交仍是一个包含  $A$  的理想, 称为由  $A$  生成的理想, 记为  $\langle A \rangle$ .

♡

#### 证明

- (1)
- (2)
- (3)

□

#### 定义 0.5

设  $R$  是一个环, 对于  $a \in R$ , 我们定义  $\langle a \rangle = \langle \{a\} \rangle$  为由  $a$  生成的主理想.

对于  $a_1, \dots, a_n \in R$ , 我们定义

$$\langle a_1, \dots, a_n \rangle = \langle \{a_1, \dots, a_n\} \rangle.$$

为由  $a_1, a_2, \dots, a_n$  有限生成的理想. 一般地, 若一个理想能被有限个元素生成, 我们就称其为有限生成的理想.

♣

#### 定理 0.4

- (1) 若  $R$  是幺环,  $a, a_1, a_2, \dots, a_n \in R$ , 则

$$\langle a \rangle = RaR \triangleq \left\{ \sum_{i=1}^m x_i a y_i \mid m \in \mathbb{N}, x_i, y_i \in R \right\},$$

$$\langle a_1, \dots, a_n \rangle = Ra_1R + \dots + Ra_nR = \left\{ \sum_{i=1}^n s_i \mid s_i \in Ra_iR \right\} = \left\{ \sum_{i=1}^n \sum_{j=1}^{m_i} x_{ij} a_i y_{ij} \mid m_i \in \mathbb{N}, x_{ij}, y_{ij} \in R \right\}.$$

进而显然有  $\langle 1 \rangle = R$ . 若还有  $I$  是  $R$  的理想且  $a_1, a_2, \dots, a_n \in I$ , 则显然有  $\langle a_1, a_2, \dots, a_n \rangle \subseteq I$ .

- (2) 若  $R$  是交换幺环,  $a, a_1, a_2, \dots, a_n \in R$ , 则

$$\langle a \rangle = aR = Ra = \{xa \mid x \in R\} = \{ax \mid x \in R\},$$

$$\langle a_1, \dots, a_n \rangle = Ra_1 + \dots + Ra_n = a_1R + \dots + a_nR = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\} = \left\{ \sum_{i=1}^n a_i r_i \mid r_i \in R \right\}.$$

再设  $U$  是  $R$  中所有可逆元素构成的集合, 则当且仅当  $u \in U$  时, 有  $\langle u \rangle = uR = R$ .

若还有  $I$  是  $R$  的理想且  $a_1, a_2, \dots, a_n \in I$ , 则显然有  $\langle a_1, a_2, \dots, a_n \rangle \subseteq I$ .

♡

**证明**

(1) 只须证明第二个等式. 设  $\sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij}, \sum_{i=1}^n \sum_{j=1}^{m_2} r_{ij} a_i s_{ij} \in Ra_1 R + \cdots + Ra_n R$ , 记  $x_{i,m_1+j} = -r_{ij}, y_{i,m_1+j} = s_{ij}$  ( $i = 1, 2, \dots, n; j = 1, 2, \dots, m_2$ ), 则

$$\begin{aligned} & \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} - \sum_{i=1}^n \sum_{j=1}^{m_2} r_{ij} a_i s_{ij} = \sum_{i=1}^n \left( \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} + \sum_{j=1}^{m_2} (-r_{ij}) a_i s_{ij} \right) \\ &= \sum_{i=1}^n \left( \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} + \sum_{j=1}^{m_2} x_{i,m_1+j} a_i y_{i,m_1+j} \right) \\ &= \sum_{i=1}^n \sum_{j=1}^{m_1+m_2} x_{ij} a_i y_{ij} \in Ra_1 R + \cdots + Ra_n R. \end{aligned}$$

故  $Ra_1 R + \cdots + Ra_n R$  对加法构成  $R$  的子群. 又因为  $R$  对加法构成 Abel 群, 所以  $Ra_1 R + \cdots + Ra_n R$  也对加法构成 Abel 群.

注意到

$$\left( \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} \right) \left( \sum_{k=1}^n \sum_{l=1}^{m_2} r_{kl} a_k s_{kl} \right)$$

的每一项都形如  $(x_{ij} a_i y_{ij} r_{kl}) a_k s_{kl} \in Ra_k R$ , 故

$$\left( \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} \right) \left( \sum_{k=1}^n \sum_{l=1}^{m_2} r_{kl} a_k s_{kl} \right) \in Ra_1 R + \cdots + Ra_n R.$$

因为  $R$  对乘法满足结合律, 所以  $Ra_1 R + \cdots + Ra_n R$  对乘法也满足结合律. 故  $Ra_1 R + \cdots + Ra_n R$  对乘法构成半群. 因此  $Ra_1 R + \cdots + Ra_n R$  是  $R$  的子环.

对  $\forall r \in R$ , 都有

$$\begin{aligned} r \left( \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} \right) &= \sum_{i=1}^n \sum_{j=1}^{m_1} (rx_{ij}) a_i y_{ij} \in Ra_1 R + \cdots + Ra_n R, \\ \left( \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i y_{ij} \right) r &= \sum_{i=1}^n \sum_{j=1}^{m_1} x_{ij} a_i (y_{ij} r) \in Ra_1 R + \cdots + Ra_n R, \end{aligned}$$

故  $R(Ra_1 R + \cdots + Ra_n R) \subseteq Ra_1 R + \cdots + Ra_n R, (Ra_1 R + \cdots + Ra_n R)R \subseteq Ra_1 R + \cdots + Ra_n R$ , 因此  $Ra_1 R + \cdots + Ra_n R$  是  $R$  的理想, 且显然有  $Ra_1 R + \cdots + Ra_n R \supseteq \langle a_1, a_2, \dots, a_n \rangle$ . 故  $Ra_1 R + \cdots + Ra_n R \supseteq \langle a_1, \dots, a_n \rangle$ .

又设  $I$  也是  $R$  的理想且包含  $a_1, \dots, a_n$ , 则由理想的定义和加法的封闭性知

$$I \supseteq Ra_1 R + \cdots + Ra_n R.$$

故  $Ra_1 R + \cdots + Ra_n R \subseteq \langle a_1, \dots, a_n \rangle$ . 综上可得  $\langle a_1, \dots, a_n \rangle = Ra_1 R + \cdots + Ra_n R$ .

(2) 只须证明第二个等式. 设  $r_1 a_1 + \cdots + r_n a_n, s_1 a_1 + \cdots + s_n a_n \in Ra_1 + \cdots + Ra_n (r_i, s_i \in R)$ , 我们有

$$(r_1 a_1 + \cdots + r_n a_n) - (s_1 a_1 + \cdots + s_n a_n) = (r_1 - s_1) a_1 + \cdots + (r_n - s_n) a_n \in Ra_1 + \cdots + Ra_n.$$

因此  $Ra_1 + \cdots + Ra_n$  对加法构成子群. 又因为  $R$  对加法构成 Abel 群, 所以  $Ra_1 + \cdots + Ra_n$  对加法构成 Abel 群.

注意到

$$(r_1 a_1 + \cdots + r_n a_n) (s_1 a_1 + \cdots + s_n a_n) = \left( \sum_{i=1}^n r_i a_i \right) \left( \sum_{j=1}^n s_j a_j \right)$$

的每一项都形如  $(r_i a_i s_j) a_j \in Ra_j$ . 因此

$$(r_1 a_1 + \cdots + r_n a_n)(s_1 a_1 + \cdots + s_n a_n) = \left( \sum_{i=1}^n r_i a_i \right) \left( \sum_{j=1}^n s_j a_j \right) \in Ra_1 + \cdots + Ra_n.$$

又因为  $R$  对乘法满足结合律, 所以  $Ra_1 + \cdots + Ra_n$  对乘法也满足结合律. 故  $Ra_1 + \cdots + Ra_n$  对乘法构成半群. 因此  $Ra_1 + \cdots + Ra_n$  是  $R$  的子环.

对  $\forall r \in R$ , 由  $R$  是交换幺环可得

$$r(r_1 a_1 + \cdots + r_n a_n) = (r_1 a_1 + \cdots + r_n a_n)r = rr_1 a_1 + \cdots + rr_n a_n \in Ra_1 + \cdots + Ra_n,$$

故  $R(Ra_1 + \cdots + Ra_n) \subseteq Ra_1 + \cdots + Ra_n$ ,  $(Ra_1 + \cdots + Ra_n)R \subseteq Ra_1 + \cdots + Ra_n$ . 因此  $Ra_1 + \cdots + Ra_n$  是个理想, 而且显然包含  $a_1, \dots, a_n$ . 故  $Ra_1 + \cdots + Ra_n \supseteq \langle a_1, \dots, a_n \rangle$ .

设  $I$  是一个包含了  $a_1, \dots, a_n$  的理想, 那么根据理想的定义和加法的封闭性, 有

$$I \supseteq Ra_1 + \cdots + Ra_n.$$

故  $Ra_1 + \cdots + Ra_n \subseteq \langle a_1, \dots, a_n \rangle$ . 综上可得  $\langle a_1, \dots, a_n \rangle = Ra_1 + \cdots + Ra_n$ .

若  $u \in U$ , 设  $r \in R$ , 则  $r = u(u^{-1}r) \in uR$ , 故  $R \subseteq uR$ . 又显然有  $uR \subseteq R$ , 故  $uR = R$ .

若  $uR = R$ , 则由  $1 \in R$  知存在  $r \in R$ , 使  $ur = 1$ , 又  $R$  可交换, 故  $r = u^{-1}$ , 即  $u \in U$ .

□

### 定理 0.5

设  $I$  为环  $R$  的子环. 在  $R$  中定义关系 “~”,

$$a \sim b, \quad a + (-b) = a - b \in I,$$

则关系 “~” 对加法为同余关系.  $a$  所在的等价类为  $a + I$ . 关系 “~” 对乘法也为同余关系的充分必要条件是  $I$  为  $R$  的理想.

若  $I$  为理想, 则将  $R$  对等价关系  $I$  的商集合记为  $R/\sim = R/I$ , 并且  $R/\sim = R/I$  中可定义加法、乘法为

$$(a + I) + (b + I) = (a + b) + I, \quad \forall a, b \in R, \tag{1}$$

$$(a + I) \cdot (b + I) = ab + I, \quad \forall a, b \in R. \tag{2}$$

$R/I$  对这种加法与乘法也构成环, 称为  $R$  对  $I$  的商环.

♡

**证明** 因  $R$  对加法为 Abel 群, 故  $R$  的加法子群  $I$  为正规子群. 由定理?? 知 “~” 对  $R$  的加法为同余关系, 再由命题?? 知在  $R/I$  中有加法运算 (1) 且为 Abel 群.

现设 “~” 对乘法也是同余关系. 对  $\forall a \in I, b \in R$  有  $a \sim 0, b \sim b$ , 因而  $ab \sim 0, ba \sim 0$ , 故  $ab, ba \in I$ , 因而  $I$  为  $R$  的理想.

反之, 设  $I$  是  $R$  的理想,  $a, b, c, d \in R$  且  $a \sim b, c \sim d$ , 即  $a - b, c - d \in I$ . 此时有  $ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d \in I$ , 即  $ac \sim bd$ , 故 “~” 对乘法也是同余关系.

当  $I$  为理想时, 在  $R/I$  中可定义乘法如式 (2) 且对  $\forall a, b, c \in R$  有

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

并且

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

类似有

$$(a + I)((b + I) + (c + I)) = (a + I)(b + I) + (a + I)(c + I),$$

即  $R/I$  为半群, 且对加法乘法的分配律成立. 故  $R/I$  是一个环.

□

**推论 0.1**

若  $R$  为交换环, 则  $R/I$  也是交换环.

♡

**证明**

□

**推论 0.2**

若  $R$  为幺环, 则  $R/I$  也是幺环且  $1+I$  为幺元.

♡

**证明**

□

**例题 0.2** 从定理 0.5 知  $m\mathbb{Z}$  为  $\mathbb{Z}$  的理想, 故  $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$  对剩余类  $(\text{mod } m)$  的加法与乘法是一个环.

当  $p$  为素数时,  $\mathbb{Z}_p$  为域.

若  $m$  是合数, 即  $m = m_1 m_2$  ( $m_i \in \mathbb{Z}, |m_i| > 1, i = 1, 2$ ), 则  $\mathbb{Z}_m$  有零因子  $\overline{m_1}, \overline{m_2}$ .

**例题 0.3** 设  $R$  是一个环. 考虑  $R^{n \times n}$  中子集

$$A = \{\alpha \mid \alpha \in R^{n \times n}, j \neq 1 \text{ 时, } \text{col}_j \alpha = 0\},$$

$$B = \{\alpha \mid \alpha \in R^{n \times n}, i \neq 1 \text{ 时, } \text{row}_i \alpha = 0\},$$

则  $A, B$  分别为  $R^{n \times n}$  的左理想与右理想. 当  $n \geq 2$  时, 一般来说,  $A, B$  都不是双边理想.