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) $\mathbf{Z}$ 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 $P[x_1, x_2, \cdots, x_n]$ 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 $a_{ij} = \mathrm{ent}_{ij}(\alpha)$. 由下面的两个关系:

(i) $\mathrm{ent}_{ij}(\alpha+\beta) = \mathrm{ent}_{ij}(\alpha) + \mathrm{ent}_{ij}(\beta)$;

(ii) $\mathrm{ent}_{ij}(\alpha\beta) = \sum\limits_{k=1}^{n} \mathrm{ent}_{ik}(\alpha)\mathrm{ent}_{kj}(\beta)$

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) $\forall m, n \in \mathbf{Z}, a, b \in R$,

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

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

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

(ii) $a^m \cdot a^n = a^{m+n}, (a^m)^n = a^{mn}, \forall m,n \in \mathbf{N}, a \in R$;

(iii) 若 $a,b \in R$ 且 $ab = ba$, 则 $(ab)^m = a^m b^m, \forall m \in \mathbf{N}$.

(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. **幺环:** 乘法是幺半群的环, 通常记幺元为 1.
3. **交换幺环:** 乘法是交换幺半群的环.
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:** 无零因子的幺环.
7. **体:** 非零元素集合对乘法构成群的环.
8. **域:** 交换的体, 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.

命题 0.2

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.

证明

□

例题 0.2 设 p 是一个素数. 于是 $\mathbf{Z}$ 中关系 $a \equiv b(\mathrm{mod}\ p)$ 对加法及乘法都是同余关系, 因而在 $\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$ 中有加法运算, 使 $\mathbf{Z}_p$ 为 Abel 群, 而且在 $\mathbf{Z}_p$ 中有乘法运算, 使 $\mathbf{Z}_p$ 为交换幺半群. $\mathbf{Z}_p = \{0, 1, \cdots, \overline{p-1}\}$. 又 $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}_p$ 有

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

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

证明

□

例题 0.3 设 $\mathbf{C}$ 为复数域. 考虑 $\mathbf{C}^{2\times 2}$ 中子集

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbf{C} \right\}.$$

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

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

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

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

则

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

此时有

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

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

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

由 $\boldsymbol{AB}\neq\boldsymbol{BA}$, 故 H 不是域. 称 H 为 $\mathbf{R}$ 上的**四元数体**.

证明

□

定义 0.3

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, 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 0.2

1. 一个环中任意多个理想之交还是理想.
2. 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

□

定理 0.3

设 I 为环 R 的子环. 在 R 中定义关系 "$\sim$",

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

则关系 "$\sim$" 对加法为同余关系.a 所在的等价类为 $a+I$.
关系 "$\sim$" 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, 则在商集合 $R/\sim=R/I$ 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 "$\sim$" 对 R 的加法为同余关系, 在 R/I

中有加法运算 (1) 且为 Abel 群.

现设 “$\sim$” 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 “$\sim$” 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

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

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

类似有

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

即 R/I 为半群, 加法乘法间分配律成立. 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 0.4 从定理 0.3知 $m\mathbf{Z}$ 为 $\mathbf{Z}$ 的理想, 故 $\mathbf{Z}_m=\mathbf{Z}/m\mathbf{Z}$ 对剩余类 $(\mathrm{mod}\ m)$ 的加法与乘法是一个环.

当 p 为素数时, $\mathbf{Z}_p$ 为域.

若 m 是合数, 即 $m=m_1m_2(m_i\in\mathbf{Z}, |m_i|>1, i=1,2)$, 则 $\mathbf{Z}_m$ 有零因子 $\overline{m_1}, \overline{m_2}$.

例题 0.5 设 R 是一个环. 考虑 $R^{n\times n}$ 中子集

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

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

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