4.5 环与域

4.5.1 环

定义15 设 $<A,\star,*>$ 是一个代数系统，若满足

（1） $<A,\star>$ 是阿贝尔群；

（2） $<A,*>$ 是一个半群；

（3） 运算 $*$ 对于运算 $\star$ 是可分配的.

称 $<A,\star,*>$ 是环。

通常称 $\star$ 为加法运算，$*$ 为乘法运算

环可简单叙述为：

（1）对加法是可换群

（2）对乘法是半群

（3）乘法对加法是可分配的

例　全体实数集 $\boldsymbol{R}$ 上定义通常的加法和乘法运算，构成的代数系统 $<\boldsymbol{R},+,\times>$ 是一个环

例　$\boldsymbol{n}$ 阶矩阵的集合 $[\boldsymbol{R}]$ 上关于矩阵的加法和乘法构成的代数系统是一个环。

定理16 设 $<A,+,\bullet>$ 是一个环，$\forall a,b,c \in A$，有

1) $a \bullet \theta = \theta \bullet a = \theta$;

2) $a \bullet (-b) = (-a) \bullet b = -(a \bullet b)$;

3) $(-a) \bullet (-b) = a \bullet b$;

4) $a \bullet (b - c) = a \bullet b - a \bullet c$;

5) $(b - c) \bullet a = b \bullet a - c \bullet a$.

其中 θ 是加法幺元，$-a$ 是 a 的加法逆元，并将 $a + (-b)$ 记为 $a - b$。

加法的幺元是乘法的零元

证明

1) $\theta \bullet a = (\theta + \theta) \bullet a = \theta \bullet a + \theta \bullet a \Rightarrow \theta \bullet a = \theta$

同理可证 $a \bullet \theta = \theta$，即 $\theta \bullet a = a \bullet \theta = \theta$

2) $a \bullet (-b) + a \bullet b = a \bullet \theta = \theta \Rightarrow a \bullet (-b) = -(a \bullet b)$

3) 由 2）即得

4) , 5) 因为环满足分配律，将减号转换为加号即得。

定义16 设 $<A,+,\bullet>$ 是环

若 $<A,\bullet>$ 是可换半群，称 $<A,+,\bullet>$ 是**交换环**。

若 $<A,\bullet>$ 是含幺半群，称 $<A,+,\bullet>$ 是**含幺环**。

例 前例中实数环是交换环，矩阵环为非交换环，但都为含幺环。

定义17 设代数系统$<A,+,\bullet>$满足：

$\forall a,b \in A$，如果$a \neq 0$，$b \neq 0$，但 $a \bullet b = 0$

则a, b 称为**零因子**。

定义17续 设代数系统 $<A,+,\bullet>$ 满足：

$\forall a,b \in A$，如果 $a \bullet b = 0 \Rightarrow a = 0$ 或 $b = 0$

称 $<A,+,\bullet>$ 无零因子。

例 $<R,+,\times>$ 是无零因子环。

定义18 设 $<A,+,\bullet>$ 是一个代数系统，若满足

（1）$<A,+>$ 是阿贝尔群；

（2）$<A,\bullet>$ 是一个可交换的独异点且无零因子，即 $\forall a,b \in A, a \neq \theta, b \neq \theta \Rightarrow a \bullet b \neq \theta$

（3）运算 $\bullet$ 对于运算 $+$ 是可分配的

称 $<A,+,\bullet>$ 是**整环**。

整环即为可换的、含幺的、无零因子环。

例 代数系统

$$<\boldsymbol{Z},+,\times>;<\boldsymbol{Q},+,\times>;<\boldsymbol{R},+,\times>$$

均为整环。

但代数系统 $<\boldsymbol{N}_4,+_4,\times_4>$ 不是整环，

因为 $\mathbf{2}\times_4\mathbf{2}=\mathbf{0}$，故 $\mathbf{2}$ 是零因子。

定理17 在整环$<A,+,\bullet>$中，条件无零因子等价于乘法消去律，即对于$c\neq\theta$，

$$c\bullet a=c\bullet b\Rightarrow a=b$$

证明 $\Rightarrow$设环中无零因子，并设$c\neq\theta$，若

$$c\bullet a=c\bullet b \Rightarrow c\bullet a-c\bullet b=c\bullet(a-b)=\theta\Rightarrow a=b$$

$\Leftarrow$设消去律成立，并设$a\neq\theta$， 若

$a\bullet b=\theta \Rightarrow a\bullet b=a\bullet\theta$ 由消去律得$b=\theta$。证毕

定义19 设$<A,+,\bullet>$是一个代数系统，若满足

（1）$<A,+>$是阿贝尔群；

（2）$<A-\{\theta\},\bullet>$是阿贝尔群；

（3）运算$\bullet$对于运算$+$是可分配的.

称$<A,+,\bullet>$是**域**。

例　代数系统

$$<Q,+,\times>,<R,+,\times>,<C,+,\times>$$

均是域。

但 $<Z,+,\times>$ 是整环不是域，因为

$<Z-\{0\},\times>$ 不是群。

域和整环之间的关系

定理18　域一定是整环。

定理19　有限整环一定是域

定义18 设 $<A,+,\bullet>$ 是一个代数系统，若满足

（1）$<A,+>$ 是阿贝尔群；

（2）$<A,\bullet>$ 是一个可交换的独异点且无零因子，即 $\forall a,b\in A, a\neq\theta, b\neq\theta \Rightarrow a\bullet b\neq\theta$

（3）运算 $\bullet$ 对于运算 $+$ 是可分配的

称 $<A,+,\bullet>$ 是**整环**。

整环即为可换的、含幺的、无零因子环。

定义19 设 $<A,+,\bullet>$ 是一个代数系统，若满足

（1）$<A,+>$ 是阿贝尔群；

（2）$<A-\{\theta\},\bullet>$ 是阿贝尔群；

（3）运算 $\bullet$ 对于运算 $+$ 是可分配的.

称 $<A,+,\bullet>$ 是**域**。

例18 设 S 为下列集合，＋和 • 为普通的加法和乘法

(1) $S=\{x \mid x=2n \wedge n \in Z\}$

(2) $S=\{x \mid x=2n+1 \wedge n \in Z\}$

(3) $S=\{x \mid x \in Z \wedge x \geq 0\}=N$

(4) $S=\{x \mid x=a+b\sqrt{3}, a, b \in Q\}$

讨论 S 对＋、• 能否构成整环？能否构成域？

解　（1）不是整环也不是域，因为乘法幺元 $1 \notin S$ 。

（2）不是整环也不是域，因为 S 不是环普通加法在 S 上不封闭。

（3）不是整环也不是域，因为 S 不是环除0以外任何正整数 x 的加法逆元 $-x \notin S$ 。

（4）是域，$\forall x_1, x_2 \in S$，有

$$x_1 = a_1 + b_1\sqrt{3},\ x_2 = a_2 + b_2\sqrt{3}$$

$$x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{3} \in S$$

$$x_1 \bullet x_2 = (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3} \in S$$

S 对+和 $\bullet$ 是封闭的， 又乘法的幺元 $1 \in S$，

可以证明 $<S,+,\bullet>$ 是整环（自己完成）。

$$\forall x \in S,\ x \neq 0,\ x = a + b\sqrt{3}$$

$$\frac{1}{x} = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} \in S$$

所以 $<S,+,\bullet>$ 是域。

内容小结

1.环的定义

2.整环和域的概念及判断

课下练习 P73 习题4.5 4,5