第5章　代数结构

5.1　代数结构简介

【习题 5.1】

1. 试举出 4 个代数结构的例子.

解　(1) $(\mathbf{R},+)$. (2) $(\mathbf{R},+,\cdot)$. (3) $(P(X),\bigcup,\bigcap)$. (4) $(\mathbf{Z},+)$.

2. 对于表 5-1 给定的集合及其上定义的运算是否构成代数结构,在相应的位置填“√”(是)或“×”(否).

解　见表 5-1 中所填具体内容.

表　5-1

运算 / 集合	$+$	$-$	$\cdot$	$\lvert x-y\rvert$	$\lvert x\rvert$	max	min
$\mathbf{Z}$	√	√	√	√	√	√	√
$\mathbf{N}$	√	×	√	√	√	√	√
$\{x\mid 0\leqslant x\leqslant 10\}$	×	×	×	√	√	√	√
$\{x\parallel x\mid\leqslant 5\}$	×	×	×	×	√	√	√
$\{2x\mid x\in\mathbf{Z}\}$	√	√	√	√	√	√	√

3. 设$(S,*)$是半群,$a\in S$,在 S 上定义运算$\circ$如下:

$$\forall x,y\in S: x\circ y = x*a*y$$

证明:$(S,\circ)$是半群.

证　对于任意 $x,y\in S$,由于$(S,*)$是半群且 $x\circ y=x*a*y$,于是$x\circ y\in S$,即 S 关于$\circ$运算是封闭的.

又因为对于任意 $x,y,z\in S$,

$$(x\circ y)\circ z=(x*a*y)\circ z=(x*a*y)*a*z=x*a*y*a*z,$$

而 $x\circ(y\circ z)=x\circ(y*a*z)=x*a*(y*a*z)=x*a*y*a*z$,于是$(x\circ y)\circ z=x\circ(y\circ z)$,即$\circ$满足结合律,故$(S,\circ)$是半群.

4. 证明:$(\mathbf{Z}_n,\cdot_n,1)$是独异点.

证　对于任意 $x,y\in\mathbf{Z}_n$,由于 $x\cdot_n y=xy(\mathrm{mod}\ n)\in\mathbf{Z}_n$,因此 $\mathbf{Z}_n$ 关于 $\cdot_n$ 运算是封闭的.

对于任意 $x,y,z\in S$,由于$(xy)z=x(yz)$,而

$$(x\cdot_n y)\cdot_n z=(xy)(\mathrm{mod}\ n)\cdot_n z=(xy)\cdot_n z=(xy)z(\mathrm{mod}\ n),$$

且

$$x\cdot_n(y\cdot_n z)=x\cdot_n(yz)(\mathrm{mod}\ n)=x\cdot_n(yz)=x(yz)(\mathrm{mod}\ n),$$

所以,$(x\cdot_n y)\cdot_n z=x\cdot_n(y\cdot_n z)$,即 $\cdot_n$ 满足结合律.

对于任意 $x\in\mathbf{Z}_n$，显然有 $x\cdot_n 1=x(\mathrm{mod}n)=x=1\cdot_n x$，因此 $\mathbf{Z}_n$ 关于 $\cdot_n$ 运算有单位元素 1.

故($\mathbf{Z}_n$，$\cdot_n$，1)是独异点.

5. 分别给出子半群及子独异点的定义.

解 (1) 设(S，$*$)是半群，$\varnothing\neq T\subseteq S$，若($T$，$*$)是半群，只要 T 关于 $*$ 运算封闭即可，则称(T，$*$)是(S，$*$)的子半群.

(2) 设(M，$*$，e)是独异点，$\varnothing\neq N\subseteq M$，若($N$，$*$，$e$)是独异点，只要 N 关于 $*$ 运算封闭且 $e\in N$ 即可，则称(N，$*$，e)是(M，$*$，e)的子独异点.

6. 设 φ 是仅一个 2 元运算代数结构(A，$*$)到(B，$\circ$)的同态映射，则

(1) 若 $*$ 在 A 中可交换，则 $\circ$ 在 $\varphi(A)$ 中可交换.

(2) 若 $*$ 在 A 中有 0 元 θ，则 $\circ$ 在 $\varphi(A)$ 中有 0 元 $\varphi(\theta)$.

证 (1) 对于任意 $x,y\in\varphi(A)$，则存在 $a,b\in A$ 使得 $\varphi(a)=x$，$\varphi(b)=y$. 由于 $a*b=b*a$，于是 $\varphi(a*b)=\varphi(b*a)$. 因为 φ 是(A，$*$)到(B，$\circ$)的同态映射，所以 $\varphi(a)\circ\varphi(b)=\varphi(b)\circ\varphi(a)$，即 $x\circ y=y\circ x$，进而 $\circ$ 在 $\varphi(A)$ 中可交换.

(2) 对于任意 $y\in\varphi(A)$，则存在 $x\in A$ 使得 $\varphi(x)=y$. 根据已知，$x*\theta=\theta*x=\theta$，于是 $\varphi(x*\theta)=\varphi(\theta*x)=\varphi(\theta)$. 根据同态映射的定义有 $\varphi(x)\circ\varphi(\theta)=\varphi(\theta)\circ\varphi(x)=\varphi(\theta)$，即 $y\circ\varphi(\theta)=\varphi(\theta)\circ y=\varphi(\theta)$. 由 y 的任意性知，$\circ$ 在 $\varphi(A)$ 中有零元 $\varphi(\theta)$.

7. 证明：正实数集合 $\mathbf{R}^+$ 关于乘法运算 $\cdot$ 所构成的代数结构($\mathbf{R}^+$，$\cdot$)与实数集合 $\mathbf{R}$ 关于加法运算 $+$ 所构成的代数结构($\mathbf{R}$，$+$)同构.

证 令 $\varphi:\mathbf{R}^+\to\mathbf{R}$，$\varphi(x)=\ln x$，$\forall x\in\mathbf{R}^+$，则显然 $\varphi:\mathbf{R}^+\to\mathbf{R}$ 是双射. 对于任意 $x,y\in\mathbf{R}^+$，由于 $\ln(xy)=\ln x+\ln y$，即 $\varphi(x\cdot y)=\varphi(x)+\varphi(y)$，于是 φ 保持运算.

故($\mathbf{R}^+$，$\cdot$)与($\mathbf{R}$，$+$)同构.

8. 非零实数集合 $\mathbf{R}^*$ 关于乘法运算 $\cdot$ 所构成的代数结构($\mathbf{R}^*$，$\cdot$)与实数集合 $\mathbf{R}$ 关于加法运算 $+$ 所构成的代数结构($\mathbf{R}$，$+$)同构吗，为什么？

解 ($\mathbf{R}^*$，$\cdot$)与($\mathbf{R}$，$+$)不可能同构.

若 φ 是($\mathbf{R}^*$，$\cdot$)与($\mathbf{R}$，$+$)的同构映射，则因为 1 是($\mathbf{R}^*$，$\cdot$)的幺元且 0 是($\mathbf{R}$，$+$)的幺元，于是 $\varphi(1)=0$. 设 $\varphi(-1)=y$.

一方面，因为 $1\neq-1$ 且 φ 是双射，则 $y\neq0$.

另一方面，$0=\varphi(1)=\varphi((-1)\cdot(-1))=\varphi(-1)+\varphi(-1)=y+y$，于是 $y=0$，这与 $y\neq0$ 矛盾. 故($\mathbf{R}^*$，$\cdot$)与($\mathbf{R}$，$+$)不可能同构.

9. 设代数结构(A，$*$)和(B，$\circ$)中的运算都是 2 元的，在 $A\times B$ 上分别定义运算 Δ 如下：对于任意的$(x_1,y_1),(x_2,y_2)\in A\times B$，

$$(x_1,y_1)\Delta(x_2,y_2)=(x_1*x_2,y_1\circ y_2)$$

证明：($A\times B$，Δ)是代数结构，称为(A，$*$)和(B，$\circ$)中的**积代数**.

证 对于任意的$(x_1,y_1),(x_2,y_2)\in A\times B$，由于

$$(x_1,y_1)\Delta(x_2,y_2)=(x_1*x_2,y_1\circ y_2)\in A\times B$$

所以，Δ 是 $A\times B$ 上的代数运算. 因而($A\times B$，Δ)是代数结构.

5.2 群

【习题 5.2】

1. 令 $\mathbf{R}[x]$表示所有系数为实数的关于 x 的多项式组成的集合，验证 $\mathbf{R}[x]$关于多项式的加法运算构成群$(\mathbf{R}[x],+)$.

解 对于任意 $f(x),g(x)\in\mathbf{R}[x]$，显然 $f(x)+g(x)\in\mathbf{R}[x]$，即 $\mathbf{R}[x]$关于$+$运算封闭.

(1) 对于任意 $f(x),g(x),h(x)\in\mathbf{R}[x]$，由于

$$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x)),$$

即 $\mathbf{R}[x]$关于$+$是可结合的.

(2) 由于 $0\in\mathbf{R}[x]$且对于任意 $f(x)\in\mathbf{R}[x]$，有 $f(x)+0=0+f(x)=f(x)$，因此，0 是 $\mathbf{R}[x]$关于$+$的幺元.

(3) 对于任意 $f(x)\in\boldsymbol{R}[x]$，因为 $f(x)+(-f(x))=(-f(x))+f(x)=0$ 且 $-f(x)\in\mathbf{R}[x]$，所以 $-f(x)$是 $f(x)$关于$+$的逆元.

故$(\mathbf{R}[x],+)$是群.

2. 令 $\boldsymbol{M}_n(\mathbf{R})$表示元素为实数的所有 n 阶方阵组成的集合，验证 $\boldsymbol{M}_n(\mathbf{R})$关于矩阵的加法运算构成群$(\boldsymbol{M}_n(\mathbf{R}),+)$，并说明 $\boldsymbol{M}_n(\mathbf{R})$关于矩阵的乘法运算$\cdot$所作成的代数结构$(\boldsymbol{M}_n(\mathbf{R}),\cdot)$不能构成群.

解 对于任意 $\boldsymbol{A},\boldsymbol{B}\in\boldsymbol{M}_n(\mathbf{R})$，显然 $A+B\in\boldsymbol{M}_n(\mathbf{R})$，即 $\boldsymbol{M}_n(\mathbf{R})$关于$+$运算封闭.

(1) 对于任意 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in\boldsymbol{M}_n(\mathbf{R})$，由于

$$(\boldsymbol{A}+\boldsymbol{B})+\boldsymbol{C}=\boldsymbol{A}+(\boldsymbol{B}+\boldsymbol{C})$$

即 $\boldsymbol{M}_n(\mathbf{R})$关于$+$是可结合的.

(2) 由于 $\mathbf{0}\in\boldsymbol{M}_n(\mathbf{R})$且对于任意 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbf{R})$，有 $\boldsymbol{A}+\mathbf{0}=\mathbf{0}+\boldsymbol{A}=\boldsymbol{A}$，因此，$\mathbf{0}$ 是 $\boldsymbol{M}_n(\mathbf{R})$关于$+$的幺元.

(3) 对于任意 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbf{R})$，因为 $\boldsymbol{A}+(-\boldsymbol{A})=(-\boldsymbol{A})+\boldsymbol{A}=\mathbf{0}$ 且 $-\boldsymbol{A}\in\mathbf{R}[x]$，所以 $-\boldsymbol{A}$ 是 $\boldsymbol{A}$关于$+$的逆元.

故$(\boldsymbol{M}_n(\mathbf{R}),+)$是群.

由于 $\boldsymbol{E}=\mathrm{diag}(1,1,\cdots,1)=\begin{pmatrix}1&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}\in\boldsymbol{M}_n(\mathbf{R})$是 $\boldsymbol{M}_n(\mathbf{R})$关于矩阵的乘法运算$\cdot$的单位元素，而对于 n 阶零矩阵 $\mathbf{0}$，不存在任何 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbf{R})$满足 $\mathbf{0}\cdot\boldsymbol{A}=\boldsymbol{A}\cdot\mathbf{0}=\boldsymbol{E}$，即 n 阶零矩阵 $\mathbf{0}$ 关于矩阵的乘法运算$\cdot$无逆元，故$(\boldsymbol{M}_n(\mathbf{R}),\cdot)$不能构成群.

3. 设 $\mathbf{Z}_m=\{0,1,2,\cdots,m-1\}$，$+_m$ 是模 m 加法运算，$\cdot_m$是模 m 乘法运算.

(1) 证明$(\mathbf{Z}_m,+_m)$是群.

(2) 举例说明，一般情况下$(\mathbf{Z}_m,-\{0\},\cdot_m)$不是群，并推出$(\mathbf{Z}_m,-\{0\},\cdot_m)$是群的充要条件.

证 (1) 对于任意 $x,y\in\mathbf{Z}_m$，显然 $x+_m y\in\mathbf{Z}_m$，即 $\mathbf{Z}_m$ 关于$+_m$运算封闭.

对于任意 $x,y,z\in\mathbf{Z}_m$，由于

$$(x+y)+z=x+(y+z)$$

即 $\mathbf{Z}_m$ 关于 $+_m$ 是可结合的.

由于 $0\in\mathbf{Z}_m$ 且对于任意 $x\in\mathbf{Z}_m$，有 $x+_m0=0+_mx=x$，因此，0 是 $\mathbf{Z}_m$ 关于 $+_m$ 的幺元.

由于 $0\in\mathbf{Z}_m$ 是幺元，所以其关于 $+_m$ 运算的逆元为 0. 对于任意 $0\neq x\in\mathbf{Z}_m$，由于 $m-x\in\mathbf{Z}_m$ 且 $x+_m(m-x)=(m-x)+_mx=0$，于是 $m-x$ 是 $\mathbf{Z}_m$ 关于 $+_m$ 的逆元.

故 $(\mathbf{Z}_m,+_m)$ 是群.

(2) 例如 $m=6$，这时 $\mathbf{Z}_6-\{0\}=\{1,2,3,4,5\}$，因为 $2\cdot_63=0\notin\mathbf{Z}_6-\{0\}$，所以 $(\mathbf{Z}_6,-\{0\},\cdot_6)$ 不是群.

首先注意到，$\mathbf{Z}_m,-\{0\}$ 关于 $\cdot_m$ 是封闭的，满足结合律且 $1\in\mathbf{Z}_m-\{0\}$ 是 $\mathbf{Z}_m,-\{0\}$ 关于 $\cdot_m$ 的幺元.

若 m 是素数，则对于任意 $x\in\mathbf{Z}_m-\{0\}$ 有 $(x,m)=1$，即存在 $k,l\in\mathbf{Z}$ 使得 $km+lx=1$，两边模 m 得 $l(\mathrm{mod}\ m)\cdot x=1$，进而 $l(\mathrm{mod}\ m)\cdot_mx=1$. 显然，$l(\mathrm{mod}\ m)\in\mathbf{Z}_m-\{0\}$ 且是 $x\in\mathbf{Z}_m-\{0\}$ 的逆元. 因此，$(\mathbf{Z}_m,-\{0\},\cdot_m)$ 是群.

反过来，若 $(\mathbf{Z}_m,-\{0\},\cdot_m)$ 是群，而 m 不是素数，即 m 是合数，即存在 $1\leqslant x,y\leqslant m-1$ 使得 $xy=m$，这时 $x\cdot_my=0\notin\mathbf{Z}_m-\{0\}$，说明 $\mathbf{Z}_m,-\{0\}$ 关于 $\cdot_m$ 不是群，矛盾.

故 $(\mathbf{Z}_m,-\{0\},\cdot_m)$ 是群的充要条件是 m 是素数.

4. 设整数集合 $\mathbf{Z}$ 上定义 $*$ 运算如下：

$$\forall x,y\in\mathbf{Z},\quad x*y=x+y-2.$$

证明：$(\mathbf{Z},*)$ 是阿贝尔群.

解 显然，$\mathbf{Z}$ 关于 $*$ 是封闭的. 对于任意 $x,y\in\mathbf{Z}$，有 $x*y=y*x$，所以 $*$ 是可交换的.

对于任意 $x,y,z\in\mathbf{Z}$，由于 $(x*y)*z=(x+y-2)*z=(x+y-2)+z-2=x+y+z-4$，而 $x*(y*z)=x*(y+z-2)=x+(y+z-2)-2=x+y+z-4$，于是 $(x*y)*z=x*(y*z)$，即 $*$ 运算满足结合律.

对于任意 $x\in\mathbf{Z}$，因为 $x*2=x+2-2=x=2*x$，因此 2 是 $\mathbf{Z}$ 关于 $*$ 的单位元.

对于任意 $x\in\mathbf{Z}$，由于 $4-x\in\mathbf{Z}$ 且 $x*(4-x)=x+(4-x)-2=2=(4-x)*x$，于是 x 关于 $*$ 存在逆元 $4-x$.

故 $(\mathbf{Z},*)$ 是阿贝尔群.

5. 设 S 是任意非空集合，G 是所有 S 到 S 的所有双射组成的集合，则 G 关于映射的复合运算。构成群.

证 由于 G 中任意 2 个元素均为 S 上的双射，其复合仍为 S 上的双射，即 G 关于置换的复合运算。是封闭的.

根据映射的复合运算满足结合律知，G 关于置换的复合运算。也是满足结合律的.

S 上的恒等映射 I_S，它是 G 关于置换的复合运算。的单位元素.

任意的 S 上的双射，其逆映射也是 S 上的双射，所以 G 中任意元素关于置换的复合运算。均存在逆元.

于是，$(G,\circ)$ 是群.

6. 设 $(G,\cdot)$ 是群，若对于任意 $x\in G$ 都有 $x^2=e$，其中 e 为群 G 的单位元，则 $(G,\cdot)$ 是阿贝尔群.

证 根据已知条件，有 $x\cdot x=e$，其中 e 是群 $(G,\cdot)$ 的单位元素，所以 $x^{-1}=x$. 对于任

意 $x,y\in G$,一方面$(x\cdot y)^{-1}=y^{-1}\cdot x^{-1}=y\cdot x$,另一方面$(x\cdot y)^{-1}=x\cdot y$,于是 $x\cdot y=y\cdot x$,即群 G 中的运算$\cdot$是可交换的,因而$(G,\cdot)$是阿贝尔群.

7. 集合 X 的幂集 $P(X)$关于集合的对称差运算$\oplus$构成群$(P(X),\oplus)$.

证 对于任意 $A,B\in P(X)$,显然 $A\oplus B\in P(X)$,即 $P(X)$关于$\oplus$运算封闭.

对于任意 $A,B,C\in P(X)$,由于

$$(A\oplus B)\oplus C=A\oplus(B\oplus C)$$

即 $P(S)$关于$\oplus$是可结合的.

由于$\varnothing\in P(X)$且对于任意 $A\in P(X)$,有 $A\oplus\varnothing=\varnothing\oplus A=A$,因此,$\varnothing$是 $P(S)$关于$\oplus$的幺元.

对于任意 $A\in P(X)$,因为 $A\oplus A=\varnothing$,所以 A 关于$\oplus$的逆元存在.

故$(P(X),\oplus)$是群.

8. 证明:群$(G,\cdot)$只有单位元素是其唯一的幂等元素.

证 设 $x\in G$ 是幂等元素,即 $x\cdot x=x$,于是 $x\cdot x=x\cdot e$,进而 $x=e$. 显然,单位元素 e 是幂等元素,故群$(G,\cdot)$只有 e 是其唯一的幂等元素.

9. 设$(G,\cdot)$是有限群且$|G|$是偶数,则 G 中必存在元素 $x\neq e$ 满足 $x\cdot x=e$,其中 e 为 G 中的单位元.

证 对于任意 $x\in G$,因为$(x^{-1})^{-1}=x$,所以 x 和 x^{-1}在群 G 中是成对出现的. 显然 $e\cdot e=e$,即 $e=e^{-1}$. 如果对于任意 $x\neq e$ 均有 $x\cdot x\neq e$,即 $x\neq x^{-1}$,则$|G|$是奇数,与已知矛盾.

因此,G 中必存在元素 $x\neq e$ 满足 $x\cdot x=e$.

10. 设$(G,\cdot)$是有限半群,若$\cdot$运算满足消去律,则$(G,\cdot)$是群.

证 设 $G=\{g_1,g_2,\cdots,g_n\}$,对于任意 $a\in G$,考虑

$$H_1=\{a\cdot g_1,a\cdot g_2,\cdots,a\cdot g_n\}$$

由于 G 关于$\cdot$是封闭的,所以 $H_1\subseteq G$. 又因为$\cdot$满足消去律,所以 $a\cdot g_i\neq a\cdot g_j,i\neq j$. 由此可见,$H_1=G$. 因为 $a\in H_1$,必存在 $e_l\in G$ 使得 $a\cdot e_l=a$. 于是,对于任意 $x\in G$,由于 $(a\cdot e_l)\cdot x=a\cdot x$,进而 $a\cdot(e_l\cdot x)=a\cdot x$,再由消去律知 $e_l\cdot x=x$,即 $e_l\in G$ 是$(G,\cdot)$的左单位元素.

类似地,通过考虑 $H_2=\{g_1\cdot a,g_2\cdot a,\cdots,g_n\cdot a\}$知,$(G,\cdot)$存在右单位元素 $e_r\in G$. 于是$(G,\cdot)$存在单位元素 $e\in G$.

由于 $e\in H_1$,必存在 $g_i\in G$ 使得 $a\cdot g_i=e$,即 a 存在右逆元. 同样,由 $e\in H_2$,必存在 $g_j\in G$ 使得 $g_j\cdot a=e$,即 a 存在左逆元. 根据$\cdot$运算满足结合律知 $a\in G$ 存在逆元.

故$(G,\cdot)$是群.

11. 设 $G=\{f\mid f:\mathbf{R}\to\mathbf{R},\exists a,b\in\mathbf{R},a\neq0,f(x)=ax+b\}$,$G$ 上的运算为映射的复合$\circ$,则

(1) $(G,\circ)$是群.

(2) 设 $H=\{f\mid f\in G,f(x)=x+b\}$,则 $H\leqslant G$.

(3) 设 $K=\{f\mid f\in G,f(x)=ax\}$,则 $K\leqslant G$.

证 (1) 对于任意 $f,g\in G$,存在 $a,b,c,d\in\mathbf{R}$ 且 $a\neq0,c\neq0$ 使得 $f(x)=ax+b,g(x)=cx+d$,这时

$$(f\circ g)(x)=g(f(x))=g(ax+b)=c(ax+b)+d=acx+(bc+d).$$

由于 $ac\neq 0$,所以 $f\circ g\in G$,即 G 关于映射的复合运算$\circ$是封闭的.

映射的复合$\circ$满足结合律.

G 中存在恒等映射 I,I 是 G 关于映射的复合运算$\circ$的单位元.

对于任意 $f\in G$,令 $g(x)=\frac{1}{a}x+\left(-\frac{b}{a}\right)$. 显然 $g\in G$ 且

$$(f\circ g)(x)=g(f(x))=g(ax+b)=\frac{1}{a}(ax+b)+\left(-\frac{b}{a}\right)=x \quad 及$$

$$(g\circ f)(x)=f(g(x))=f\left(\frac{1}{a}x-\frac{b}{a}\right)=a\left(\frac{1}{a}x-\frac{b}{a}\right)+b=x,$$

所以 $f\circ g=g\circ f=I_G$,即 f 在 G 中关于映射的复合运算$\circ$存在逆元 g.

综上所述,$(G,\circ)$是群.

(2) 对于任意 $f,g\in H$,存在 $b,d\in R$ 使得 $f(x)=x+b$,$g(x)=x+d$,这时 $g^{-1}(x)=x-d$,进而$(f\circ g^{-1})(x)=g^{-1}(f(x))=g^{-1}(x+b)=x+(b-d)$,于是 $f\circ g^{-1}\in H$,因此 $H\leqslant G$.

(3) 对于任意 $f,g\in K$,存在 $a,c\in R$ 且 $a\neq 0,c\neq 0$ 使得 $f(x)=ax$,$g(x)=cx$,这时 $g^{-1}(x)=\frac{1}{c}x$,进而

$$(f\circ g^{-1})(x)=g^{-1}(f(x))=g^{-1}(ax)=\frac{1}{c}\cdot ax=\frac{a}{c}x,$$

于是 $f\circ g^{-1}\in K$,因此 $K\leqslant G$.

12. 设 $G=\{(x,y)\mid x,y\in\mathbf{R},x\neq 0\}$,对于任意$(x_1,y_1)\in G$ 和$(x_2,y_2)\in G$ 定义

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1x_2,x_2y_1+y_2),$$

证明

(1) $(G,\cdot)$是非阿贝尔群.

(2) 令 $H=\{(1,y)\mid y\in\mathbf{R}\}$,则 $H\leqslant G$.

证 (1)对于任意$(x_1,y_1)\in G$ 和$(x_2,y_2)\in G$,由于 $x_1x_2\neq 0$,根据定义知

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1x_2,x_2y_1+y_2)\in G,$$

即 G 关于$\cdot$运算是封闭的.

对于任意$(x_1,y_1)\in G$,$(x_2,y_2)\in G$ 和$(x_3,y_3)\in G$,一方面,

$$\begin{aligned}((x_1,y_1)\cdot(x_2,y_2))\cdot(x_3,y_3)&=(x_1x_2,x_2y_1+y_2)\cdot(x_3,y_3)\\&=(x_1x_2x_3,x_3(x_2y_1+y_2)+y_3)\\&=(x_1x_2x_3,x_3x_2y_1+x_3y_2+y_3),\end{aligned}$$

另一方面,

$$\begin{aligned}(x_1,y_1)\cdot((x_2,y_2)\cdot(x_3,y_3))&=(x_1,y_1)\cdot(x_2x_3,x_3y_2+y_3)\\&=(x_1x_2x_3,x_3x_2y_1+x_3y_2+y_3),\end{aligned}$$

于是,G 中的运算$\cdot$是可结合的.

任意$(x,y)\in G$,由于$(x,y)\cdot(1,0)=(x,y)=(1,0)\cdot(x,y)$,所以$(1,0)$是单位元.

对于任意$(x,y)\in G$,取$\left(\frac{1}{x},-\frac{y}{x}\right)\in G$,则

$$(x,y)\cdot\left(\frac{1}{x},-\frac{y}{x}\right)=\left(x\cdot\frac{1}{x},\frac{1}{x}\cdot y+\left(-\frac{y}{x}\right)\right)=(1,0),$$

$$\left(\frac{1}{x},-\frac{y}{x}\right)\cdot(x,y)=\left(x\cdot\frac{1}{x},x\cdot\left(-\frac{y}{x}\right)+y\right)=(1,0),$$

于是$(x,y)\in G$有逆元$\left(\frac{1}{x},-\frac{y}{x}\right)\in G$.

由于$(1,2)\cdot(2,3)=(2,7)\neq(2,5)=(2,3)\cdot(1,2)$,所以$G$中的运算$\cdot$是不可交换的.

综上所述,$(G,\cdot)$是非阿贝尔群.

(2) 对于任意$(1,y_1)\in H$和$(1,y_2)\in H$,由于$(1,y_2)^{-1}=(1,-y_2)$,且

$$(1,y_1)\cdot(1,y_2)^{-1}=(1,y_1)\cdot(1,-y_2)=(1,y_1-y_2)\in H,$$

于是,$H\leqslant G$.

13. 令$\varphi:\mathbf{R}\to\mathbf{R}^*$,$\varphi(x)=\mathrm{e}^x$,证明:$\varphi$是$(\mathbf{R},+)$到$(\mathbf{R}^*,\cdot)$的同态映射.

证 显然,$(\mathbf{R},+)$和$(\mathbf{R}^*,\cdot)$是群.

对于任意$x,y\in\mathbf{R}$,由于$\varphi(x+y)=\mathrm{e}^{x+y}=\mathrm{e}^x\cdot\mathrm{e}^y=\varphi(x)\cdot\varphi(y)$,所以$\varphi$是$(\mathbf{R},+)$到$(\mathbf{R}^*,\cdot)$的同态映射.

5.3 环 和 域

【习题 5.3】

1. 验证整数集合$\mathbf{Z}$关于数的加法$+$和乘法运算$\cdot$构成环.

解 (1) $(\mathbf{Z},+)$是阿贝尔群;

(2) $(\mathbf{Z},\cdot)$是半群;

(3) $\cdot$对$+$可分配:对于任意$x,y,z\in\mathbf{Z}$,有

$$x\cdot(y+z)=x\cdot y+x\cdot z$$
$$(y+z)\cdot x=y\cdot x+z\cdot x$$

所以$(\mathbf{Z},+,\cdot)$是环.

2. 设$R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\ a,b,c,d\in\mathbf{Z}\right\}$,则$R$关于矩阵的加法$+$和矩阵乘法$\cdot$构成环.

证 (1) $(R,+)$是阿贝尔群;

(2) $(R,\cdot)$是半群;

(3) 矩阵乘法$\cdot$对矩阵的加法$+$可分配:对于任意$\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in R$,有

$$\boldsymbol{A}\cdot(\boldsymbol{B}+\boldsymbol{C})=\boldsymbol{A}\cdot\boldsymbol{B}+\boldsymbol{A}\cdot\boldsymbol{C}$$
$$(\boldsymbol{B}+\boldsymbol{C})\cdot\boldsymbol{A}=\boldsymbol{B}\cdot\boldsymbol{A}+\boldsymbol{C}\cdot\boldsymbol{A}$$

所以$(R,+,\cdot)$是环.

3. 设$R=\{a+b\sqrt{3}\mid a,b\in\mathbf{Z}\}$,则$R$关于数的加法$+$和数的乘法$\cdot$构成环.

证 (1) $(R,+)$是阿贝尔群;

(2) $(R,\cdot)$是半群;

(3) 数的乘法$\cdot$对数的加法$+$可分配:对于任意$x,y,z\in R$,有

$$x\cdot(y+z)=x\cdot y+x\cdot z$$
$$(y+z)\cdot x=y\cdot x+z\cdot x$$

所以$(R,+,\cdot)$是环.

4. 设R是区间$(-\infty,+\infty)$上的所有连续函数组成的集合,对于任意$f,g\in R$,定义

$$(f+g)(x)=f(x)+g(x),(f\circ g)(x)=f(g(x)),\forall x\in(-\infty,+\infty)$$

试判断$(R,+,\circ)$是否能构成环.

解 $(R,+,\circ)$不能构成环,因为函数的复合运算$\circ$对函数的加法运算$+$不可分配,例如对于$\forall x\in(-\infty,+\infty)$,取$f(x)=x^2,g(x)=x,h(x)=2x$,它们都是$(-\infty,+\infty)$上的连续函数,但

$$(f\circ(g+h))(x)=f((g+h)(x))=f(x+2x)=f(3x)=(3x)^2=9x^2$$

而

$$\begin{aligned}(f\circ g+f\circ h)(x)&=(f\circ g)(x)+(f\circ h)(x)=f(g(x))+f(h(x))\\&=f(x)+f(2x)=x^2+(2x)^2=5x^2\end{aligned}$$

于是$f\circ(g+h)\neq f\circ g+f\circ h$.

5. 设X是集合,$P(X)$是X的幂集,证明:$P(X)$关于集合的对称差运算$\oplus$和集合的交运算$\cap$构成环$(P(X),\oplus,\cap)$.

证 (1) $(P(X),\oplus)$是阿贝尔群;

(2) $(P(X),\cap)$是半群;

(3) 集合的交运算$\cap$对集合的对称差运算$\oplus$可分配:对于任意$A,B,C\in P(X)$,有

$$A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$$

$$(B\oplus C)\cap A=(B\cap A)\oplus(C\cap A)$$

所以$(P(X),\oplus,\cap)$是环.

6. 证明:$(\mathbf{R}[x],+,\cdot)$是整环但不是除环.

证 显然,$(\mathbf{R}[x],+,\cdot)$是环.

$1\in\mathbf{R}[x]$是$(\mathbf{R}[x],+,\cdot)$的幺元,其$\cdot$是可交换的.

对于任意$f(x),g(x)\in\mathbf{R}[x]$,若$f(x)\cdot g(x)=0$,则$f(x)=0$或$g(x)=0$,即$(\mathbf{R}[x],+,\cdot)$是无零因子环.

因此,$(\mathbf{R}[x],+,\cdot)$是整环.

取$f(x)=x\neq0$,对于任意$g(x)\in\mathbf{R}[x]$,有$f(x)\cdot g(x)\neq1$,所以$f(x)$关于$\cdot$没有逆元,进而$(\mathbf{R}[x],+,\cdot)$不是除环.

7. 证明:乘法运算可交换的除环是整环.

证 设$(R,+,\cdot)$是乘法运算可交换的除环,则$(R,+,\cdot)$是含幺交换环. 下面证明:$(R,+,\cdot)$是无零因子环.

对于任意$x,y\in R$,若$x\cdot y=0$且$x\neq0$,则因为x^{-1}存在,有$x^{-1}\cdot(x\cdot y)=x^{-1}\cdot0$,即$(x^{-1}\cdot x)\cdot y=0$,亦即$1\cdot y=0$,进而$y=0$,所以$(R,+,\cdot)$是无零因子环.

8. 设$R=\{a+b\mathrm{i}\mid a,b\in\mathbf{Q}\}$,则$R$关于数的加法$+$和数的乘法$\cdot$构成除环,该环称为**高斯数环**.

证 显然,$(R,+)$是阿贝尔群,$(R,\cdot)$是半群. 由于数的乘法$\cdot$运算对数的加法$+$运算可分配,于是$(R,+,\cdot)$是环,其乘法幺元为1.

对于任意$0\neq a+b\mathrm{i}\in R,a,b\in\mathbf{Q}$,则$a$和$b$不全为0,即$a^2+b^2\neq0$. 由于$a/(a^2+b^2)-b/(a^2+b^2)\mathrm{i}\in R$且

$$(a+b\mathrm{i})\cdot(a/(a^2+b^2)-b/(a^2+b^2)\mathrm{i})=1$$

即 R 中任意非零元素关于乘法运算均有逆元. 于是,$(R,+,\cdot)$是除环.

9. 设 $R=\mathbf{Z}\times\mathbf{Z}$,定义 R 上的加法$+$运算和乘法$\cdot$运算如下:

对于任意$(x_1,y_1)\in R,(x_2,y_2)\in R$,

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2),$$

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1\cdot x_2,y_1\cdot y_2),$$

证明:$(R,+,\cdot)$是环,并求出该环的所有零因子.

证 根据已知条件知,运算$+$是 R 上的封闭运算且满足交换律和结合律,其加法幺元是$(0,0)$. 任意$(x,y)\in R$ 关于$+$的逆元为$(-x,-y)$,因此$(R,+)$是阿贝尔群.

由于$\cdot$运算是 R 上的封闭运算且满足结合律,于是$(R,\cdot)$是半群.

显然,$\cdot$ 运算是 R 上的可交换运算且对于任意$(x_1,y_1)\in R,(x_2,y_2)\in R,(x_3,y_3)\in R$,有

$$(x_1,y_1)\cdot((x_2,y_2)+(x_3,y_3))=(x_1,y_1)\cdot(x_2,y_2)+(x_1,y_1)\cdot(x_3,y_3)$$

即$\cdot$运算对$+$运算可分配.

综上所述,$(R,+,\cdot)$是环.

对于任意$(x,0)\in R(x\neq0)$及$(0,y)\in R(y\neq0)$,由于$(x,0)\cdot(0,y)=(0,0)$,所以$(x,0)\in R(x\neq0)$和$(0,y)\in R(y\neq0)$是环$(R,+,\cdot)$的所有零因子.

10. 设$(R,+,\cdot)$是含幺交换环,$x\notin R$ 是未定元,对于任意 $r\in R$,$x\cdot r=r\cdot x$. 令 $R[x]=\{f(x)\mid f(x)=a_0+a_1x+\cdots+a_nx^n,a_i\in R,i=0,1,\cdots,n-1,n\in\mathbf{N}\}$,则 $R[x]$关于多项式的加法$+$和乘法$\cdot$构成环,称$(R[x],+,\cdot)$为**环 R 上的关于 x 的一元多项式环**.

证 (1) $(R[x],+)$是阿贝尔群;

(2) $(R[x],\cdot)$是半群;

(3) 乘法$\cdot$对加法$+$可分配.

故$(R[x],+,\cdot)$是环.

11. 设$(R,+,\cdot)$是环,若 R 的乘法运算$\cdot$满足幂等性,即对于任意 $x\in R$ 有 $x\cdot x=x$,则称$(R,+,\cdot)$是**布尔环**. 证明:

(1) 对于任意 $x\in R$ 有 $x+x=0$.

(2) 布尔环是交换环.

(3) 若$|R|>2$,则$(R,+,\cdot)$不是整环.

证 (1) 对于任意 $x\in R$,考虑$(x+x)\cdot(x+x)$.

一方面$(x+x)\cdot(x+x)=x+x$,另一方面,根据分配律有

$$(x+x)\cdot(x+x)=x\cdot x+x\cdot x+x\cdot x+x\cdot x=x+x+x+x$$

于是 $x+x+x+x=x+x$,进而 $x+x=0$.

(2) 对于任意 $x\in R$,考虑$(x+y)\cdot(x+y)$.

一方面$(x+y)\cdot(x+y)=x+y$,另一方面,根据分配律有

$$(x+y)\cdot(x+y)=x\cdot x+x\cdot y+y\cdot x+y\cdot y=x+x\cdot y+y\cdot x+y$$

于是 $x+x\cdot y+y\cdot x+y=x+y$,进而 $x\cdot y+y\cdot x=0$. 由(1)知,$x\cdot y+x\cdot y=0$,因此 $x\cdot y=y\cdot x$.

(3) 若$(R,+,\cdot)$不含幺元,当然$(R,+,\cdot)$不是整环. 若$(R,+,\cdot)$含幺环,其幺元为1,由于$|R|>2$,必存在 $a\in R,a\neq0,1$. 由于 $a\cdot(a-1)=a\cdot a-a=0$,所以 a 和 $a-1$ 是环

$(R,+,\cdot)$的零因子，因此$(R,+,\cdot)$不是整环.

12. 设$(R,+,\cdot)$是环，$A=R^R$，定义 A 上的运算分别为函数的加法与乘法，即：对于任意 $f,g\in A$，$(f+g)(x)=f(x)+g(x)$，$(f\cdot g)(x)=f(x)\cdot g(x)$，$\forall x\in R$. 证明：$(A,+,\cdot)$是环.

证 (1) $(A,+)$是阿贝尔群.

由于$(R,+,\cdot)$是环，A 关于$+$运算是封闭的且 A 上的$+$运算可交换、可结合.

令 $\varphi:R\to R$，$\varphi(x)=0$，$\forall x\in R$，则 $\varphi\in A$ 且对于任意 $f\in A$ 有$(f+\varphi)(x)=f(x)+\varphi(x)=f(x)+0=f(x)$，即 $f+\varphi=f$，于是 φ 是 A 关于$+$运算的幺元.

对于任意 $f\in A$，令 $-f:R\to R$，$(-f)(x)=-f(x)$，$\forall x\in R$，则 $-f\in A$ 且有$(f+(-f))(x)=f(x)+(-f(x))=0=\varphi(x)$，即 $f+(-f)=\varphi$，于是 $-f$ 是关于$+$运算的逆元.

因此$(A,+)$是阿贝尔群.

(2) $(A,\cdot)$是半群.

由于$(R,+,\cdot)$是环，A 关于$\cdot$是封闭的且 A 上的$\cdot$运算可结合，所以$(A,\cdot)$是半群.

(3) $\cdot$对$+$可分配

对于任意 $f,g,h\in A$，

$$\begin{aligned}(f\cdot(g+h))(x)&=f(x)\cdot(g+h)(x)=f(x)\cdot(g(x)+h(x))\\&=f(x)\cdot g(x)+f(x)\cdot h(x),\\(f\cdot g+f\cdot h)(x)&=(f\cdot g)(x)+(f\cdot h)(x)\\&=f(x)\cdot g(x)+f(x)\cdot h(x),\end{aligned}$$

于是 $f\cdot(g+h)=f\cdot g+f\cdot h$.

同理可证，$(g+h)\cdot f=g\cdot f+h\cdot f$.

于是，A 上的$\cdot$运算对$+$运算可分配.

故$(A,+,\cdot)$是环.

13. 设$(R,+,\cdot)$是含幺 1 的环，对于任意 $x,y\in R$，定义

$$x\oplus y=x+y+1,\quad x\odot y=x\cdot y+x+y$$

证明：

(1) $(R,\oplus,\odot)$是含幺环.

(2) 令 $\varphi(x)=x-1$，则 φ 是环$(R,+,\cdot)$到环$(R,\oplus,\odot)$的同构映射.

证 (1) 显然，R 关于$\oplus$是封闭的且$\oplus$运算是可交换的.

对于任意 $x,y,z\in R$，有$(x\oplus y)\oplus z=(x+y+1)\oplus z=x+y+z+2$，而 $x\oplus(y\oplus z)=x\oplus(y+z+1)=x+y+z+2$，于是$(x\oplus y)\oplus z=x\oplus(y\oplus z)$，即$\oplus$满足结合律.

对于任意 $x\in R$，由于 $x\oplus(-1)=x+(-1)+1=x$，因此 -1 是 R 关于$\oplus$的单位元素.

对于任意 $x\in R$，由于 $x\oplus(-x-2)=x+(-x-2)+1=-1$，因此 $-x-2$ 是 x 关于$\oplus$的逆元素.

于是$(R,\oplus)$是阿贝尔群.

又显然 R 关于$\odot$是封闭的且对于任意 $x,y,z\in R$，有$(x\odot y)\odot z=(x\cdot y+x+y)\odot z=x\cdot y\cdot z+x\cdot z+y\cdot z+x\cdot y+x+y+z$，而 $x\odot(y\odot z)=x\odot(y\cdot z+y+z)=x\cdot y\cdot z+$