0.1 半群、幺半群和群

定义 0.1 (二元运算)

如果 G 是一个非空集合, 每个函数 $G\times G\to G$ 叫作 G 上的一个**二元运算**. 对 (a,b) 在一个二元运算之下的象有许多常用的记号:ab(乘法记号),$a+b$(加法记号),$a\cdot b$,$a\times b$ 等等. ♣

注 为方便起见, 我们在本章中一般采用乘法记号, 并且把 ab 叫作 a 和 b 的**积**. 一个集合上可以有许多个不同的二元运算 (例如在 $\mathbb{Z}$ 上由 $(a,b)\longmapsto a+b$ 和 $(a,b)\longmapsto ab$ 分别给出**通常的加法**和**乘法运算**).

定义 0.2 (半群和交换半群)

设 G 是一个非空集合, 如果 G 上满足

(i) 结合律:$a(bc)=(ab)c$(对所有 $a,b,c\in G$) 的一个二元运算, 便称 G 是一个**半群**.

如果一个半群 G 包含有一个

(ii)**(双侧) 幺元素** $e\in G$, 使得 $ae=ea=a$(对所有 $a\in G$), 便称 G 是一个**幺半群**.

如果幺半群 G 满足

(iii) 对于每个 $a\in G$ 均存在 **(双侧) 逆元素** $a^{-1}\in G$, 使得 $a^{-1}a=aa^{-1}=e$, 便称 G 是一个**群**.

如果半群 G 的二元运算满足

(iv) 交换律:$ab=ba$(对所有 $a,b\in G$), 便称 G 为**交换半群**或者 **Abel 半群**. ♣

注 如果 G 是幺半群而其上的二元运算写成乘法, 则 G 的幺元素永远写成 e. 如果二元运算写成加法, 则 $a+b(a,b\in G)$ 叫做 a 与 b 的和, 并且幺元素写成 0. 这时又如果 G 是群, 则 $a\in G$ 的逆元素表示成 $-a$. 我们以 $a-b$ 表示 $a+(-b)$.Abel 群常常写成加法形式.

例题 0.1 $(M_n(\mathbb{R}),\cdot)$ 是一个含幺 (乘法) 半群.

证明 $\forall A,B,C\in(M_n(\mathbb{R}),\cdot)$, 则不妨设 $A=(a_{ij})_{n\times n},B=(b_{ij})_{n\times n},C=(c_{ij})_{n\times n}$. 再设 $A\cdot B=(d_{ij})_{n\times n},B\cdot C=(e_{ij})_{n\times n},(A\cdot B)\cdot C=(f_{ij})_{n\times n},A\cdot(B\cdot C)=(g_{ij})_{n\times n}$. 于是

$$d_{ij}=\sum_{k=1}^{n}a_{ik}b_{kl},e_{ij}=\sum_{k=1}^{n}b_{ik}c_{kl}.$$

其中 $i,j=1,2,\cdots,n$.

从而

$$f_{ij}=\sum_{l=1}^{n}d_{il}c_{lj}=\sum_{l=1}^{n}\left(\sum_{k=1}^{n}a_{ik}b_{kl}\right)\cdot c_{lj}=\sum_{l=1}^{n}\sum_{k=1}^{n}a_{ik}b_{kl}c_{lj},$$

$$g_{ij}=\sum_{k=1}^{n}a_{ik}e_{kj}=\sum_{k=1}^{n}a_{ik}\cdot\left(\sum_{l=1}^{n}b_{kl}c_{lj}\right)=\sum_{k=1}^{n}\sum_{l=1}^{n}a_{ik}b_{kl}c_{lj}.$$

由二重求和号的可交换性, 可知 $f_{ij}=g_{ij},\forall i,j\in\{1,2,\cdots,n\}$. 故 $(A\cdot B)\cdot C=A\cdot(B\cdot C)$.

记 $I_n=\begin{pmatrix}1&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}\in M_n(\mathbb{R})$, 于是 $\forall X\in M_n(\mathbb{R})$, 则不妨设 $X=(x_{ij})_{n\times n},I_n=(\delta_{ij})_{n\times n}$. 其中 $\delta_{ij}=\begin{cases}1,\text{当}i=j\text{时},\\0,\text{当}i\neq j\text{时},\end{cases}$. 再设 $I_n\cdot X=(x'_{ij})_{n\times n},X\cdot I_n=(x''_{ij})_{n\times n}$, 于是由矩阵乘法的定义可知

$$x'_{ij}=\sum_{k=1}^{n}x_{ik}\delta_{kj}=x_{ij}\delta_{jj}=x_{ij}.$$

$$x''_{ij}=\sum_{k=1}^{n}\delta_{ik}x_{kj}=\delta_{ii}x_{ij}=x_{ij}.$$

故 $x'_{ij}=x''_{ij}=x_{ij},\forall i,j\in\{1,2,\cdots,n\}$. 从而 $X=I_n\cdot X=X\cdot I_n$. 因此 I_n 是 $(M_n(\mathbb{R}),\cdot)$ 的单位元. 综上所述,$(M_n(\mathbb{R}),\cdot)$ 是一个含幺 (乘法) 半群. □

例题 0.2 常见的群

1. 我们称只有一个元素的群为**平凡群**, 记作 e. 其中的二元运算是 $e\cdot e=e$.
2. 常见的加法群有 $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ 等. 这些加法群分别称为整数加群、有理数加群、实数加群、复数加群.
3. 常见的乘法群有 $(\mathbb{Q}^\times,+),(\mathbb{R}^\times,+),(\mathbb{C}^\times,+)$ 等, 其中 $\mathbb{Q}^\times=\mathbb{Q}\backslash 0$, 类似地定义其余两个集合. 这些乘法群分别称为有理数乘群、实数乘群、复数称群.
4. 在向量空间中,n 维欧式空间对加法构成群即 $(\mathbb{R}^n,+)$. 类似地 $(\mathbb{C}^n,+),(\mathbb{Q}^n,+),(\mathbb{Z}^n,+)$ 也是群. 对于这些群, 单位元都是零向量, 加法逆元则是对每个坐标取相反数, 如 $(x_1,\cdots,x_n)$ 的加法逆元是 $(-x_1,\cdots,-x_n)$.
5. 所有的 $m\times n$ 矩阵也对加法构成群, 单位元都是零矩阵, 加法逆元则是对每一项取相反数. 对于 $n\times n$ 的实矩阵加法群, 我们记作 $(M(n,\mathbb{R}),+)$, 类似地我们将 $n\times n$ 的复矩阵加法群记作 $(M(n,\mathbb{C}),+)$.

证明 证明都是显然的. □

定义 0.3 (阶)

势 $|G|$ 叫作群 G 的**阶**. 如果 $|G|$ 是有限的或者是无限的, 则群 G 也分别叫做**有限的**或者**无限的**, 也分别叫做**有限群**或者**无限群**. ♣

定理 0.1

(1) 如果 G 是幺半群, 则幺元素 e 是唯一的.

(2) 如果 G 是群, 则

(i) $c\in G$ 并且 $cc=c\Rightarrow c=e$;

(ii) 对于所有的 $a,b,c\in G,ab=ac\Rightarrow b=c$, 同样地 $ba=ca\Rightarrow b=c$(左消去律和右消去律);

(iii) 对于每个 $a\in G$, 逆元素 a^{-1} 是唯一的;

(iv) 对于每个 $a\in G,(a^{-1})^{-1}=a$;

(v) 对于 $a,b\in G,(ab)^{-1}=b^{-1}a^{-1}$;

(vi) 对于 $a,b\in G$, 方程 $ax=b$ 和 $ya=b$ 均在 G 中有唯一解:$x=a^{-1}b,y=ba^{-1}$. ♡

证明 (1) 若 e' 也是 (双侧) 幺元素, 则 $e'=e'e=e$. 下证 (2).

(i) $cc=c\Rightarrow c^{-1}(cc)=c^{-1}c\Rightarrow(c^{-1}c)c=c^{-1}c\Rightarrow ec=e\Rightarrow c=e$.

(ii) $ab=ac\Rightarrow a^{-1}(ab)=a^{-1}(ac)\Rightarrow(a^{-1}a)b=(a^{-1}a)c\Rightarrow eb=ec\Rightarrow b=c$.

$ba=ca\Rightarrow(ba)a^{-1}=(ca)a^{-1}\Rightarrow b(a^{-1}a)=c(a^{-1}a)\Rightarrow be=ce\Rightarrow b=c$.

(iii) 若 a' 也为 a 的逆元素, 则 $a^{-1}a=e=a'a$, 于是由 (ii) 可得 $a^{-1}=a'$.

(iv) 由 (双侧) 逆元素的定义立得.

(v) $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=(ae)a^{-1}=aa^{-1}=e$. 同理 $(b^{-1}a^{-1})(ab)=e$. 再根据 (iii) 可知 $(ab)^{-1}=b^{-1}a^{-1}$.

(vi) 将 $x=a^{-1}b$ 代入方程 $ax=b$ 可得 $ax=a\left(a^{-1}b\right)=\left(aa^{-1}\right)b=eb=b$, 故 $x=a^{-1}b$ 是方程 $ax=b$ 的解. 若 $x=c$ 也是 $ax=b$ 的解, 则 $ac=b\Rightarrow a^{-1}(ac)=a^{-1}b=\left(aa^{-1}\right)c=a^{-1}b\Rightarrow ec=a^{-1}b\Rightarrow c=a^{-1}b$. 故 $x=a^{-1}b$ 是方程 $ax=b$ 的唯一解. 类似可证 $y=ba^{-1}$ 是方程 $ya=b$ 的唯一解.

□

命题 0.1

设 G 是半群, 则 G 是群的充要条件是下面两条件成立:

(i) 存在一个元素 $e\in G$, 使得对所有 $a\in G$ 均有 $ea=a$(左幺元素);

(ii) 对于每个 $a \in G$, 均存在一个元素 $a^{-1} \in G$, 使得 $a^{-1}a = e$(左逆).

注 如果改成“右幺元素”和“右逆”, 则类似的结果也成立.

证明 ($\Rightarrow$): 显然.

($\Leftarrow$): 先证若 $c \in G$ 且 $cc = c$, 则 $c = e$. 由 (i)(ii) 可知 $c^{-1}(cc) = c^{-1}c = e \Rightarrow (c^{-1}c)c = e \Rightarrow e = ec$, 从而再由 (i) 可得 $c = e$.

由于 $e \in G$, 从而 $G \neq \varnothing$. 如果 $a \in G$, 由 (ii) 可知 $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = a(ea^{-1}) = aa^{-1}$, 从而由上述结论可知 $aa^{-1} = e$. 因此 a^{-1} 是 a 的双侧逆. 由于对每个 $a \in G$ 均有 $ae = (aa^{-1}a) = (aa^{-1})a = ea = a$, 从而 e 为双侧幺元素. 因此 G 是群. □

命题 0.2

设 G 是半群, 则 G 是群的充要条件是对于所有 $a, b \in G$, 方程 $ax = b$ 和 $ya = b$ 在 G 中均可解.

证明 ($\Rightarrow$): 由定理 0.1(iv)立得.

($\Leftarrow$): 对 $\forall a \in G$, 取 $b = a$, 由 $ya = b$ 可解, 故存在 $e \in G$, 使得对 $\forall a \in G$ 均有 $ea = a$. 对 $\forall a \in G$, 取 $b = e$, 由 $ya = b$ 可解, 故对每个 $a \in G$, 都存在一个元素 $a^{-1} \in G$, 使得 $a^{-1}a = e$. 因此由命题 0.1可知 G 是群. □

例题 0.3 整数集合 $\mathbb{Z}$, 有理数集合 $\mathbb{Q}$ 和实数集合 $\mathbb{R}$ 对于通常加法都是无限 Abel 群. 对于通常的乘法都是幺半群但不是群 (0 没有逆). 但是 $\mathbb{Q}$ 和 $\mathbb{R}$ 的非零元素集合对于乘法分别形成无限 Abel 群. 偶整数集合对于乘法形成半群但不是幺半群.

定理 0.2

假设 $R(\sim)$ 是幺半群 G 上的一个等价关系, 并且对所有 $a_i, b_i \in G$, 由 $a_1 \sim a_2, b_1 \sim b_2$ 可以导出 $a_1b_1 \sim a_2b_2$. 则 G 的所有 R 等价类组成的集合 G/R 对于二元运算 $(\bar{a})(\bar{b}) = \overline{ab}$ 是幺半群. 其中 $\bar{x}$ 表示 $x \in G$ 的等价类.

幺半群 G 上满足此定理中条件的等价关系称作 G 上的一个**同余关系**.

如果 G 为 Abel 群, 则 G/R 也为 Abel 群.

证明 如果 $\bar{a}_1 = \bar{a}_2$ 并且 $\bar{b}_1 = \bar{b}_2 (a_i, b_i \in G)$, 由引论中第 4 节的 (20) 式有 $a_1 \sim a_2$ 和 $b_1 \sim b_2$. 由假设有 $a_1b_1 \sim a_2b_2$, 从而再由 (20) 式 $\overline{a_1b_1} = \overline{a_2b_2}$. 因此可以定义 G/R 中的二元运算 (即与等价类代表元的选取无关). 这个二元运算是满足结合律的, 因为 $\bar{a}(\bar{b}\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{(ab)}\bar{c} = (\bar{a}\bar{b})\bar{c}$. 又由于 $(\bar{a})(\bar{e}) = \overline{ae} = \bar{a} = \overline{ea} = (\bar{e})(\bar{a})$, 从而 $\bar{e}$ 是幺元素, 于是 G/R 为幺半群. 如果 G 为群, 则 $\bar{a} \in G/R$ 显然有逆元素 $\overline{a^{-1}}$, 因此 G/R 也是群. 类似地,G 的交换性导致 G/R 的交换性. □

例题 0.4 假设 m 是固定的整数. 根据引论的定理 6.8 可知模 m 同余是加法群 $\boldsymbol{Z}$ 上的同余关系. 以 $\boldsymbol{Z}_m$ 表示 $\boldsymbol{Z}$ 在模 m 同余之下的等价类集合. 由定理 0.2(采用加法记号) 知 $\boldsymbol{Z}_m$ 是 Abel 群, 其加法由 $\bar{a} + \bar{b} = \overline{a+b}$ 给出 $(a, b \in \boldsymbol{Z})$. 引论中定理 6.8 的证明表明 $\boldsymbol{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$, 从而 $\boldsymbol{Z}_m$ 对于加法是 m 阶有限群, 叫作是**模 m 整数 (加法) 群**. 类似地, 由于 $\boldsymbol{Z}$ 对于乘法是交换幺半群, 而模 m 同余对于乘法也是同余关系 (引论的定理 6.8), 从而 $\boldsymbol{Z}_m$ 对于由 $(\bar{a})(\bar{b}) = \overline{ab} (a, b \in \boldsymbol{Z})$ 给出的乘法是交换幺半群. 验证对于所有 $\bar{a}, \bar{b}, \bar{c} \in \boldsymbol{Z}_m$:

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}, (\bar{a} + \bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c} (\text{分配律})$$

进而, 如果 p 为素数, 则 $\boldsymbol{Z}_p$ 的非零元素形成 $p-1$ 阶乘法群.

注 习惯上我们仍把 $\boldsymbol{Z}_m$ 中元素表示成 $0, 1, \ldots, m-1$, 而不写成 $\bar{0}, \bar{1}, \ldots, \overline{m-1}$. 这种有些混淆的记号在课文中不会引起困难, 所以在方便的时候我们就使用它.

证明

□

例题 0.5 有理数加法群 $\boldsymbol{Q}$ 上的下列关系是同余关系:

$$a \sim b \Longleftrightarrow a - b \in \boldsymbol{Z}$$

由定理 0.2, 等价类集合 (表示成 $\boldsymbol{Q}/\boldsymbol{Z}$) 对于由 $\bar{a} + \bar{b} = \overline{a+b}$ 给出的加法是 (无限)Abel 群.$\boldsymbol{Q}/\boldsymbol{Z}$ 叫作**模 1 有理数群**.

证明

□

定义 0.4 (有意义乘积和标准 n 元乘积)

设 G 是一个半群, $\{a_1, a_2, \cdots\}$ 是 G 中任意一个元素序列,

(i) 我们归纳地定义 $a_1, \ldots, a_n$(以这种排列次序) 的一个**有意义乘积**[a]: 如果 $n = 1$, 则唯一的有意义乘积为 a_1. 如果 $n > 1$, 则有意义乘积定义为形如 $(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ 的任何一个乘积, 其中 $m < n$, 并且 $(a_1 \cdots a_m)$ 和 $(a_{m+1} \cdots a_n)$ 分别是 m 元和 $n - m$ 元的有意义乘积.

(ii) 我们如下归纳定义 $a_1, \cdots, a_n$ 的**标准 n 元乘积**[b] $\prod_{i=1}^{n} a_i$:

$$\prod_{i=1}^{1} a_i = a_1, \text{而当} n > 1 \text{时}, \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n.$$

[a] 为了证明这个定义的良定义性, 需要逆归定理的更强的形式见 Burrill, C. ; W, Foundations of Real Numbers. New York: McGraw-Hill, Inc, 1967.,57 页

[b] 由逆归定理可以推出对每个 $n \in \boldsymbol{N}^*$,G 中任意 n 个元素的标准 n 元乘积对应 G 中的唯一元素 (它显然是一个有意义乘积), 因此这个定义是良定义的

♣

注 注意当 $n \geqslant 3$ 时, 可能存在 $a_1, \ldots, a_n$ 的许多个有意义乘积.

定理 0.3 (广义结合律)

如果 G 是半群而 $a_1, \ldots, a_n \in G$, 则 $a_1, \ldots, a_n$ 以此排列次序的任意两个有意义乘积均彼此相等.

♡

注 根据这个定理, 我们可以将 $a_1, \ldots, a_n \in G(G$ 为半群) 的任何有意义乘积写成 $a_1 a_2 \ldots a_n$, 即不加任何括号也不会有任何混淆.

证明 我们归纳证明: 对于每个 n, 任意一个有意义乘积 $a_1 \ldots a_n$ 均等于标准 n 元乘积 $\prod_{i=1}^{n} a_i$. 对于 $n = 1, 2$ 这显然是对的. 如果 $n > 2$, 由定义 $(a_1 \ldots a_n) = (a_1 \ldots a_m)(a_{m+1} \ldots a_n)$, 其中 $m < n$. 从而根据归纳假设和结合性便有:

$$\begin{aligned}(a_1 \ldots a_n) = (a_1 \ldots a_m)(a_{m+1} \ldots a_n) &= \left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m} a_{m+i}\right) \\ &= \left(\prod_{i=1}^{m} a_i\right)\left(\left(\prod_{i=1}^{n-m-1} a_{m+i}\right) a_n\right) = \left(\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m-1} a_{m+i}\right)\right) a_n \\ &= \left(\prod_{i=1}^{n-1} a_i\right) a_n = \prod_{i=1}^{n} a_i.\end{aligned}$$

□

定理 0.4 (广义交换律)

如果 G 为交换半群而 $a_1, \ldots, a_n \in G$, 则对于 $1, 2, \ldots, n$ 的任意一个置换 $i_1, \ldots i_n$, 均有

$$a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}.$$

♡

证明

□

定义 0.5 (方幂)

假设 G 为半群,$a \in G$,$n \in \boldsymbol{N}^*$. 元素 $a^n \in G$ 定义为标准 n 元乘积 $\prod_{i=1}^{n} a_i$, 其中 $a_i = a (1 \leqslant i \leqslant n)$. 如果 G 是幺半群, 则 a^0 定义为幺元素 e. 如果 G 是群, 则对于每个 $n \in \boldsymbol{N}^*$,a^{-n} 定义为 $(a^{-1})^n \in G$.

♣

注 根据定义和广义结合律,$a^1=a,a^2=aa,a^3=(aa)a=aaa,\ldots,a^n=a^{n-1}a=aa\ldots a(n\text{ 个因子})$.

注意当 $m\neq n$ 时可能会有 $a^m=a^n$(例如在 $\boldsymbol{C}$ 中,$-1=i^2=i^6$).

加法记号 如果 G 中的二元运算写成加法, 我们便用 na 代替 a^n. 因此 $0a=0,1a=a,na=(n-1)a+a$, 如此等等.

定理 0.5

如果 G 是群 [半群, 幺半群], 而 $a\in G$, 则对所有 $m,n\in\boldsymbol{Z}[\boldsymbol{N}^*,\boldsymbol{N}]$, 均有

(i) $a^ma^n=a^{m+n}$(加法记号:$ma+na=(m+n)a$);

(ii) $(a^m)^n=a^{mn}$(加法记号:$n(ma)=nma$).

♡

证明 显然对每个 $n\in\boldsymbol{N}$ 均有 $(a^n)^{-1}=(a^{-1})^n$, 并且对每个 $n\in\boldsymbol{Z}$ 均有 $(a^{-1})^n=((a^{-1})^{-1})^{-n}=a^{-n}$.

(i) 对于 $m>0$ 和 $n>0$ 是对的, 因为标准 n 元乘积和标准 m 元乘积相乘是一个有意义乘积, 根据广义结合律, 它等于标准 $(m+n)$ 元乘积. 将 a,m,n 改为 $a^{-1},-m,-n$ 并且利用上述推理就可得到 $m<0$ 和 $n<0$ 的情形. 情形 $m=0$ 或者 $n=0$ 是平凡的. 而情形 $m\geqslant 0,n<0$ 和 $m<0,n\geqslant 0$ 可以分别对 m 和 n 作归纳法.

(ii) 对于 $m=0$ 是显然的. 当 $m>0,n\in\boldsymbol{Z}$ 时, 可以对 m 归纳证得. 然后用此结果证明 $m<0$ 和 $n\in\boldsymbol{Z}$ 的情形.

□