0.1 幺半群

定义 0.1 (代数运算/二元运算)

设 A 是一个非空集合, 若对 A 中任意两个元素 a, b, 通过某个法则 "$\cdot$", 有 A 中唯一确定的元素 c 与之对应, 则称法则 "$\cdot$" 为集合 A 上的一个**代数运算 (algebraic operation) 或二元运算**. 元素 c 是 a, b 通过运算 "$\cdot$" 作用的结果, 将此结果记为 $a \cdot b = c$. ♣

定义 0.2 (半群和交换半群)

非空集合 S 和 S 上满足结合律的二元运算 $\cdot$ 所形成的代数结构叫做**半群**. 此即

$$\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

这个半群记成 $(S, \cdot)$ 或者简记成 S, 运算 $x \cdot y$ 也常常简写成 xy. 此外, 如果半群 $(S, \cdot)$ 中的运算 "$\cdot$" 又满足交换律, 则 $(S, \cdot)$ 叫做**交换半群**. 此即

$$\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

$$\forall x, y \in S, x \cdot y = y \cdot x.$$

♣

注 像通常那样令 $x^2 = x \cdot x, x^{n+1} = x^n \cdot x (= x \cdot x^n, n \geq 1)$.

定义 0.3 (幺元素)

设 S 是半群, 元素 $e \in S$ 叫做半群 S 的**幺元素 (也叫单位元 (unit element) 或恒等元 (identity))**, 是指对每个 $x \in S, xe = ex = x$. ♣

命题 0.1 (幺元素存在必唯一)

如果半群 $(S, \cdot)$ 中有幺元素, 则幺元素一定唯一. 我们将半群 $(S, \cdot)$ 中这个唯一的幺元素 (如果存在的话) 通常记作 $\mathbf{1}_S$ **或者** $\mathbf{1}$. ♠

证明 因若 e' 也是幺元素, 则 $e' = e'e = e$. □

定义 0.4 (含幺半群和交换含幺半群)

如果半群 $(S, \cdot)$ 含有幺元素, 则 $(S, \cdot)$ 称为 **(含) 幺半群**. 此即

$$\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

$$\exists e \in S, \forall x \in S, e \cdot x = x \cdot e = x.$$

此外, 如果幺半群 $(S, \cdot)$ 中的运算 "$\cdot$" 又满足交换律, 则 $(S, \cdot)$ 叫做**交换幺半群**. 此即

$$\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

$$\exists e \in S, \forall x \in S, e \cdot x = x \cdot e = x,$$

$$\forall x, y \in S, x \cdot y = y \cdot x.$$

♣

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 $\delta_{ij}=\begin{cases}1, 当 i=j 时,\\0, 当 i\neq j 时\end{cases}$. 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. □

定义 0.5 (幺半群中多个元素的乘积)

设 $(S,\cdot)$ 是一个幺半群, 令 $x_1,\cdots,x_n\in S$, 我们递归地定义

$$x_1\cdot x_2\cdots x_n=(x_1\cdot x_2\cdots x_{n-1})\cdot x_n$$

令 $x\in S,n\in\mathbb{N}$. 若 $n>0$, 我们定义 $x^n=x\cdots x$, 而 $x^0=e$. ♣

定义 0.6 (广义结合律)

设 S 是一个非空集合, “$\cdot$” 是一个二元运算, 若对于任意有限多个元素 $x_1,x_2,\dots,x_n\in S$, 乘积 $x_1\cdot x_2\cdots x_n$ 的任何一种 “有意义的加括号方式”(即给定的乘积的顺序) 都得出相同的值. ♣

命题 0.2

设 S 是一个非空集合, “$\cdot$” 是一个满足结合律的二元运算, 令 $x_1,\cdots,x_n,y_1,\cdots,y_m\in S$, 则

$$x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_m=(x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_m)\tag{1.6}$$

♠

笔记 根据这个命题, 我们就可以得到一个半群 $(S,\cdot)$ 一定满足广义结合律, 只要 $x_1,\cdots,x_n\in S$ 的 $\cdot$ 运算顺序是固定的, 无论怎么添加括号, 我们都可以利用这个命题的结论, 将括号重排至从前往后依次乘的顺序而保持结果不变. 所以, 如果一个集合上的二元运算有结合律, 我们就可以在连续元素的乘积中不加括号, 也可以按照我们的需要随意加括号.

证明 对 m 做数学归纳. 当 $m=1$ 时, 由定义 0.5直接得到. 接下来, 假设

$$x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_k=(x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_k)$$

则由 “$\cdot$” 满足结合律, 我们有

$$\begin{aligned}&x_1\cdot x_2\cdots x_n\cdot y_1\cdot y_2\cdots y_{k+1}\\&=((x_1\cdot x_2\cdots x_n)\cdot(y_1\cdot y_2\cdots y_k))\cdot y_{k+1}\end{aligned}$$

$$= (x_1 \cdot x_2 \cdots x_n) \cdot ((y_1 \cdot y_2 \cdots y_k) \cdot y_{k+1})$$
$$= (x_1 \cdot x_2 \cdots x_n) \cdot (y_1 \cdot y_2 \cdots y_{k+1})$$

□

推论 0.1

设 S 是一个非空集合, “$\cdot$” 是一个满足结合律的二元运算, 令 $x \in S, m, n \in \mathbb{N}$, 则

$$x^{m+n} = x^m \cdot x^n$$

证明 令命题 0.2中的所有 x_i 和 y_j 都等于 x 即可得到. □

定义 0.7 (子幺半群)

令 $(S, \cdot)$ 是一个幺半群, 若 $T \subset S$, $e \in T$, 且 T 在乘法下封闭, 即

$$e \in T,$$
$$\forall x, y \in T, x \cdot y \in T.$$

则我们称 $(T, \cdot)$ 是 $(S, \cdot)$ 的一个**子幺半群**

命题 0.3 (子幺半群也是幺半群)

若 $(T, \cdot)$ 是 $(S, \cdot)$ 的一个子幺半群, 则 $(T, \cdot)$ 是个幺半群.

证明 就二元运算的定义而言, 子群第一个条件（封闭性）就满足了, 这使得我们后面的谈论是有意义的. 首先, 结合律对于 S 中元素都满足, 当然对 T 中元素也满足（T 是子集）. 接下来, 类似地,e 对于所有 S 中元素都是单位元, 固然对于 T 中元素亦是单位元. □

定义 0.8 (两个幺半群的直积)

令 $(G, \cdot_1), (G', \cdot_2)$ 是两个幺半群, 我们记 $(G \times G', *)$ 为 $(G, \cdot_1)$ 和 $(G', \cdot_2)$ 的**直积**. 满足对于 $(x, y), (x', y') \in G \times G'$, 有

$$(x, y) * (x', y') = (x \cdot_1 x', y \cdot_2 y').$$

命题 0.4 (两个幺半群的直积仍是幺半群)

若 $(G, \cdot_1), (G', \cdot_2)$ 是两个幺半群, 则它们的直积 $(G \times G', *)$ 还是一个幺半群.

证明 封闭性: 因为 G 在 $\cdot_1$ 下封闭,G' 在 $\cdot_2$ 下封闭, 而 $G \times G'$ 的元素乘积是逐坐标定义的, 则 $G \times G'$ 在 $* = (\cdot_1, \cdot_2)$ 下也是封闭的.

结合律: 同样, 逐坐标有结合律, 故整体也有结合律.

单位元: 设 e, e' 分别是 $(G, \cdot_1), (G', \cdot_2)$ 的单位元, 则不难想象,(e, e') 是直积的单位元. 对于任意 $(x, y) \in G \times G'$, 我们有 $(x, y) * (e, e') = (x \cdot_1 e, y \cdot_2 e') = (x, y)$, 另一边也是同理, 这就证明了 (e, e') 是直积的单位元. □

定义 0.9 (一族幺半群的直积)

令 $(G_i, \cdot_i)_{i \in I}$ 是一族幺半群, 其中 I 是一个指标集. 我们记它们的**直积**为 $(\prod_{i \in I} G_i, *)$. 满足对于 $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 有

$$(x_i)_{i \in I} * (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I}.$$

命题 0.5 (一族幺半群的直积仍是幺半群)

若 $(G_i,\cdot_i)_{i\in I}$ 是一族幺半群, 则它们的直积 $(\prod\limits_{i\in I} G_i,*)$ 还是一个幺半群.

证明 证明与命题 0.4同理.. 封闭性与结合律是显然的. 单位元是 $(e_i)_{i\in I}$. □

命题 0.6 (一族交换幺半群的直积仍是交换幺半群)

若 $(G_i,\cdot_i)_{i\in I}$ 是一族交换幺半群, 则它们的直积 $(\prod\limits_{i\in I} G_i,*)$ 还是一个交换幺半群.

证明 由命题 0.5可知 $(\prod\limits_{i\in I} G_i,*)$ 还是一个幺半群. 下面证明它还是交换幺半群.

由 $(G_i,\cdot_i)_{i\in I}$ 是一族交换幺半群可得, 对 $\forall (x_i)_{i\in I},(y_i)_{i\in I}\in\prod\limits_{i\in I} G_i$, 都有

$$(x_i)_{i\in I}\cdot(y_i)_{i\in I}=(x_i\cdot_i y_i)_{i\in I}=(y_i\cdot_i x_i)_{i\in I}=(y_i)_{i\in I}\cdot(x_i)_{i\in I}\,.$$

故 $(\prod\limits_{i\in I} G_i,*)$ 还是一个交换幺半群. □

定义 0.10 (幺半群同态)

假设 $(S,\cdot),(T,*)$ 是两个幺半群, 且 $f:S\to T$ 是一个映射, 我们称 f 是一个**幺半群同态**, 当 f 保持了乘法运算, 且把单位元映到了单位元. 此即

$$\forall x,y\in S, f(x\cdot y)=f(x)*f(y),$$
$$f(e)=e'.$$

其中,e 和 e' 分别是 $(S,\cdot)$ 和 $(T,*)$ 的单位元.

定义 0.11 (由子集生成的子幺半群)

设 $(S,\cdot)$ 是一个幺半群, 而 $A\subset S$ 是一个子集. 我们称 S 中所有包含了 A 的子幺半群的交集为**由 A 生成的子幺半群**, 记作 $\langle A\rangle$. 此即

$$\langle A\rangle=\bigcap\{T\subset S: T\supset A, T \text{ 是子幺半群}\}.$$

命题 0.7 (由子集生成的子幺半群是包含了这个子集的最小的子幺半群)

设 $(S,\cdot)$ 是一个幺半群, 而 $A\subset S$ 是一个子集. 则 $\langle A\rangle$ 也是一个子幺半群. 因此, 这是包含了 A 的最小的子幺半群.

注 这里说的“最小”, 指的是在包含关系下最小的, 也就是, 它包含于所有包含 A 的子幺半群.

证明 要证明 $\langle A\rangle$ 是子幺半群, 只需要证明它包含了 e, 并在乘法运算下封闭. 首先, 因为集族中每一个 T, 作为子幺半群, 都会包含 e; 因此 $\langle A\rangle$ 作为这些集合的交集也会包含 e, 这就证明了第一点. 而对于第二点, 我们首先假设 $x,y\in\langle A\rangle$, 而想要证明 $x\cdot y\in\langle A\rangle$. 注意到, 因为 $x,y\in\langle A\rangle$, 任取一个包含了 A 的子幺半群 T（集族中的集合）, 我们都有 $x,y\in T$, 于是有 $x\cdot y\in T$. 而 $x\cdot y\in T$ 对于所有这样的 T 都成立, 我们就有 $x\cdot y$ 属于它们的交集, 也就是 $\langle A\rangle$. 这样, 我们就证明了第二点. 综上, 由一个幺半群 S 的任意子集 A 生成的子幺半群都确实是一个子幺半群. □

命题 0.8

设 $(S,\cdot)$ 是一个幺半群, 且 $s\in S$, 则

$$\langle s\rangle=\{1,s,s^2,\cdots\}.$$

证明 一方面, 设 $(T,\cdot)<(S,\cdot)$ 且 $s\in T$, 则 $1\in T$. 假设 $s^n\in T$, 则

$$s^{n+1}=s\cdot s^n\in T.$$

从而由数学归纳法可知 $s^n\in T,\forall n\in\mathbb{N}_1$. 因此 $T\supset\{1,s,s^2,\cdots\}$, 故由 T 的任意性可知,$\langle s\rangle\supset\{1,s,s^2,\cdots\}$.

另一方面, 显然有 $s\in\{1,s,s^2,\cdots\}$. 因此我们只需证明 $\{1,s,s^2,\cdots\}<(S,\cdot)$ 即可. 而显然有 $1\in\{1,s,s^2,\cdots\}$, 对 $\forall s^m,s^n\in\{1,s,s^2,\cdots\}$, 由推论 0.1可得

$$s^m\cdot s^n=s^{m+n}.$$

故 $\{1,s,s^2,\cdots\}<(S,\cdot)$. 因此 $\{1,s,s^2,\cdots\}\supset\langle s\rangle$.

综上, 我们就有 $\langle s\rangle=\{1,s,s^2,\cdots\}$. □

定义 0.12 (幺半群同构)

假设 $(S,\cdot),(T,*)$ 是两个幺半群, 且 $f:S\to T$ 是一个映射, 我们称 f 是一个**幺半群同构**, 当 f 是一个双射, 且是一个同态.

$$f\text{ 是双射},$$
$$\forall x,y\in S, f(x\cdot y)=f(x)*f(y),$$
$$f(e)=e'.$$

其中,e 和 e' 分别是 $(S,\cdot)$ 和 $(T,*)$ 的单位元. ♣

注 容易验证同构是一个等价关系.

命题 0.9 (幺半群同构的逆是幺半群同态)

若 $f:(S,\cdot)\to(T,*)$ 是一个幺半群同构, 则 $f^{-1}:T\to S$ 是一个幺半群同态. 因此,f^{-1} 也是个幺半群同构. ♠

证明 令 $x',y'\in T$, 我们只需证明 $f^{-1}(x'*y')=f^{-1}(x')\cdot f^{-1}(y')$. 为了方便起见, 根据 f 是一个双射, 从而存在 $x,y\in S$, 使得 $x=f^{-1}(x'),y=f^{-1}(y')$, 并且 $f(x)=x',f(y)=y'$. 我们只需证明 $f^{-1}(x'*y')=x\cdot y$. 而由于 f 是幺半群同态, 所以 $f(x\cdot y)=f(x)*f(y)=x'*y'$. 反过来说,$f^{-1}(x'*y')=x\cdot y=f^{-1}(x')\cdot f^{-1}(y')$. 这就证明了这个命题. □