抽象代数

作者: 邹文杰

组织: 无

时间:2024/10/25

版本:ElegantBook-4.5

自定义: 信息

宠辱不惊, 闲看庭前花开花落;
去留无意, 漫随天外云卷云舒.

目录

第一章 群论 I——Group Theorey I

1.1 幺半群

定义 1.1 (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 1.2 (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 1.3 (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 1.1 (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 1.4 (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 1.1 $(M_n(\mathbb{R}), \cdot)$ 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 1.5 (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 1.6 (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 $x_1,x_2,\ldots,x_n\in S$, 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 1.2

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 1.5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“·”满足结合律, 我们有

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

□

推论 1.1

令 $x\in S, m, n\in\mathbb{N}$，则

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

♡

证明 令命题 1.2中的所有 x_i 和 y_j 都等于 x 即可得到. □

定义 1.7 (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 1.3 (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 1.8 (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 1.9 (由 A 生成的子幺半群)

假设 $(S,\cdot)$ 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 1.4 ($\langle A\rangle$ 包含了 A 的最小的子幺半群)

假设 $(S,\cdot)$ 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。 □

定义 1.10 (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 1.5 (幺半群同构的逆映射一定是幺半群同态)

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。 □

1.2 群

定义 1.11

令 $(S, \cdot)$ 是一个幺半群，$x \in S$。我们称 x 是**可逆的**，当且仅当

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

其中 y 被称为 x 的**逆元**，记作 x^{-1}。 ♣

命题 1.6 (逆元存在必唯一)

令 $(S, \cdot)$ 是一个幺半群。假设 $x \in S$ 是可逆的，则其逆元唯一。也就是说，如果 $y, y' \in S$ 都是它的逆元，则 $y = y'$。 ♠

证明 假设 y, y' 都是 x 的逆元。则 $y \cdot x = e$，$x \cdot y' = e$. 从而

$$y = y \cdot e = y \cdot x \cdot y' = e \cdot y' = y'.$$

□

定义 1.12 (群)

令 $(G,\cdot)$ 是一个幺半群, 若 G 中所有元素都是可逆的, 则我们称 $(G,\cdot)$ 是一个**群**. 换言之，若 $\cdot$ 是 G 上的一个二元运算，则我们称 $(G,\cdot)$ 是个**群**，或 G 对 $\cdot$ 构成群，当这个运算满足结合律，存在单位元，且每个元素具有逆元。再进一步展开来说，同样等价地，若 $\cdot$ 是 G 上的一个二元运算，则我们称 $(G,\cdot)$ 是个**群**，当

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

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

$$\forall x\in G, \exists y\in G, x\cdot y=y\cdot x=e.$$

♣

命题 1.7

令 $(G,\cdot)$ 是一个群，令 $x\in G$，则 $(x^{-1})^{-1}=x$。

♠

证明 方便起见，我们令 $y=x^{-1}$，于是有 $x\cdot y=y\cdot x=e$。我们要证明 $y^{-1}=x$，而这就是 $y\cdot x=x\cdot y=e$，显然成立。这就证明了逆元的逆元是自身. □

命题 1.8

令 $(G,\cdot)$ 是一个群，令 $x,y\in G$，则 $(x\cdot y)^{-1}=y^{-1}\cdot x^{-1}$。

♠

证明 我们利用定义来证明。一方面，利用广义结合律，$(x\cdot y)\cdot(y^{-1}\cdot x^{-1})=e$；另一方面，同理可以得到另一边的等式 $(y^{-1}\cdot x^{-1})\cdot(x\cdot y)=e$，这就告诉我们 $(x\cdot y)^{-1}=y^{-1}\cdot x^{-1}$。 □

定义 1.13

设 $(G,\cdot)$ 是一个群，且 $x\in G$。若 $n\in\mathbb{N}_1$，我们定义 $x^{-n}=(x^{-1})^n$，另外定义 $x^0=e$。

♣

命题 1.9

设 $(G,\cdot)$ 是一个群，且 $x\in G$. 则满足

(1) $x^{-n}=(x^{-1})^n=(x^n)^{-1}, \forall n\in\mathbb{Z}$.

(2) $x^{m+n}=x^m\cdot x^n, \forall m,n\in\mathbb{Z}$.

(3) $x^{mn}=(x^m)^n=(x^n)^m, \forall m,n\in\mathbb{Z}$.

♠

证明

(1) (i) 当 $n=0$ 时, 结论显然成立.

(ii) 当 $n\in\mathbb{N}_1$ 时, 只需证明 $(x^{-1})^n=(x^n)^{-1}$ 即可. 注意到

$$x^n\cdot(x^{-1})^n=\left(\underbrace{x\cdots x}_{n\text{个}}\right)\cdot\left(\underbrace{x^{-1}\cdots x^{-1}}_{n\text{个}}\right)=e,$$

$$(x^n)^{-1}\cdot x^n=\left(\underbrace{x^{-1}\cdots x^{-1}}_{n\text{个}}\right)\cdot\left(\underbrace{x\cdots x}_{n\text{个}}\right)=e.$$

故根据逆元的定义可知结论成立.

(iii) 当 n 为负整数时, 令 $m=-n$, 则 $m\in\mathbb{N}_1$. 从而我们只需证 $x^m=(x^{-1})^{-m}=(x^{-m})^{-1}$ 即可. 根据定义 1.13可得

$$x^{-m}\cdot x^m=\left(x^{-1}\right)^m\cdot x^m=\left(\underbrace{x^{-1}\cdots x^{-1}}_{m\text{个}}\right)\cdot\left(\underbrace{x\cdots x}_{m\text{个}}\right)=e,$$

$$x^m\cdot x^{-m}=x^m\cdot\left(x^{-1}\right)^m=\left(\underbrace{x\cdots x}_{m\text{个}}\right)\cdot\left(\underbrace{x^{-1}\cdots x^{-1}}_{m\text{个}}\right)=e.$$

故根据逆元的定义可知 $x^m = (x^{-m})^{-1}$. 又由定义 1.13可知,$(x^{-1})^{-m} = \left((x^{-1})^{-1}\right)^m = x^m$. 故结论成立.

(2) 首先注意到,

(i) 如果 $m, n \in \mathbb{N}_1$，则由推论 1.1就立刻得到这个性质。若 m 或 n 是 0，利用单位元的性质也是显然的。从而我们只需证明当 m, n 至少有一个小于 0 时,$x^{m+n} = x^m \cdot x^n$. 故我们可以不失一般性，假设 $m < 0$，记 $m' = -m$，则 $x^m = x^{-m'} = (x^{-1})^{m'}$。

(ii) 若 $n < 0$，记 $n' = -n$，则同理，$x^n = (x^{-1})^{n'}$，故 $x^{m+n} = (x^{-1})^{m'+n'}$，这里 $m', n' \in \mathbb{N}_1$，于是就有

$$x^{m+n} = (x^{-1})^{m'+n'} = \left(x^{-1}\right)^{m'} \left(x^{-1}\right)^{n'} = x^m x^n,$$

因此得证了.

(iii) 若 $0 < n < m'$，则 $x^{m+n} = x^{-(m'-n)} = (x^{-1})^{m'-n}$。而 $x^m \cdot x^n = (x^{-1})^{m'} \cdot x^n$. 于是

$$\begin{aligned}
& x^{m+n} = x^m \cdot x^n \\
\Leftrightarrow\ & (x^{-1})^{m'-n} = (x^{-1})^{m'} \cdot x^n \\
\Leftrightarrow\ & \underbrace{x^{-1} \cdots x^{-1}}_{m'-n\text{个}} = \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'\text{个}}\right) \cdot x^n
\end{aligned}$$

对上式两边左乘 $x^{m'-n}$，得到

$$\begin{aligned}
x^{m+n} = x^m \cdot x^n \Leftrightarrow\ & \underbrace{x^{-1} \cdots x^{-1}}_{m'-n\text{个}} = \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'\text{个}}\right) \cdot x^n \\
\Leftrightarrow\ & x^{m'-n} \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'-n\text{个}}\right) = x^{m'-n} \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'\text{个}}\right) \cdot x^n \\
\Leftrightarrow\ & \left(\underbrace{x \cdots x}_{m'-n\text{个}}\right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'-n\text{个}}\right) = \left(\underbrace{x \cdots x}_{m'-n\text{个}}\right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'\text{个}}\right) \cdot x^n \\
\Leftrightarrow\ & e = \left(\underbrace{x^{-1} \cdots x^{-1}}_{n\text{个}}\right) \cdot x^n \Leftrightarrow e = (x^n)^{-1} \cdot x^n
\end{aligned}$$

上式最后一个等式显然成立, 故此时结论成立.

(iv) 若 $n \geq m'$, 则 $x^{m+n} = x^{n-m'}$。而 $x^m \cdot x^n = (x^{-1})^{m'} \cdot x^n$. 于是

$$\begin{aligned}
& x^{m+n} = x^m \cdot x^n \\
\Leftrightarrow\ & x^{n-m'} = (x^{-1})^{m'} \cdot x^n \\
\Leftrightarrow\ & \underbrace{x \cdots x}_{n-m'\text{个}} = \left(x^{-1}\right)^{m'} \cdot \left(\underbrace{x \cdots x}_{n\text{个}}\right)
\end{aligned}$$

对上式两边右乘 $(x^{-1})^{n-m'}$，得到

$$\begin{aligned}
x^{m+n} = x^m \cdot x^n \Leftrightarrow\ & \underbrace{x \cdots x}_{n-m'\text{个}} = \left(x^{-1}\right)^{m'} \cdot \left(\underbrace{x \cdots x}_{n\text{个}}\right) \\
\Leftrightarrow\ & \left(\underbrace{x \cdots x}_{n-m'\text{个}}\right) \cdot \left(x^{-1}\right)^{n-m'} = \left(x^{-1}\right)^{m'} \cdot \left(\underbrace{x \cdots x}_{n\text{个}}\right) \cdot \left(x^{-1}\right)^{n-m'} \\
\Leftrightarrow\ & \left(\underbrace{x \cdots x}_{n-m'\text{个}}\right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{n-m'\text{个}}\right) = \left(x^{-1}\right)^{m'} \cdot \left(\underbrace{x \cdots x}_{n\text{个}}\right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{n-m'\text{个}}\right) \\
\Leftrightarrow\ & e = \left(x^{-1}\right)^{m'} \cdot \left(\underbrace{x \cdots x}_{m'\text{个}}\right) \Leftrightarrow e = \left(x^{-1}\right)^{m'} \cdot x^{m'}
\end{aligned}$$

上式最后一个等式显然成立, 故此时结论成立.

(3) 先证 $x^{mn} = (x^m)^n$. 对 $\forall m \in \mathbb{Z}$, 固定 m, 对 n 使用数学归纳法. 当 $n = 1$ 时, 结论显然成立. 假设当 $n = k$ 时, 结论成立, 即 $x^{mk} = (x^m)^k$. 则由 (2) 的结论可得

$$x^{m(k+1)} = (x^m)^{k+1} = (x^m)^k \cdot x^m = (x^m)^{k+1}.$$

故由数学归纳法可知,$x^{mn} = (x^m)^n, \forall n \in \mathbb{Z}$. 再由 m 的任意性可知 $x^{mn} = (x^m)^n, \forall m, n \in \mathbb{Z}$. 同理可证 $x^{nm} = (x^n)^m, \forall m, n \in \mathbb{Z}$. 由于 $x^{nm} = x^{mn}, \forall m, n \in \mathbb{Z}$. 因此 $x^{mn} = (x^m)^n = (x^n)^m, \forall m, n \in \mathbb{Z}$.

□

定义 1.14 (Abel 群)

若 $(G, \cdot)$ 是一个群, 我们称它是 **Abel 群**, 或**交换群**, 当该运算满足交换律, 即

$$\forall x, y \in G, x \cdot y = y \cdot x$$

♣

例题 1.2 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. □

引理 1.1

令 $(S, \cdot)$ 是一个幺半群, 令 G 是其所有可逆元素构成的子集, 则 $(G, \cdot)$ 是个群。

♡

注 我们称呼幺半群中的可逆元素为“**单位**”，因此 G 是由所有该运算下的单位构成的集合（在这里甚至是群）。

证明 首先结合律完全继承自 S，不需要证明。而单位元是可逆的，因此 $e \in G$。剩下要证明 G 中每个元素都有（G 中的）逆元，而这几乎是显然的。假设 $x \in G$，则 x 是可逆元素，我们取 $y \in S$，使得 $x \cdot y = y \cdot x = e$（这里要注意我们只能首先保证 y 在全集 S 中）。接下来我们要证明 $y \in G$，即 y 可逆，而这是显然的，因为 x 正是它的逆。所以 $y \in G$。这样，就证明了 $(G, \cdot)$ 是个群. □

定义 1.15 (子群)

令 $(G, \cdot)$ 是一个群，且 $H \subset G$。我们称 H 是 G 的**子群**，记作 $H < G$，当其包含了单位元，在乘法和逆运算下都封闭，即

$$e \in H,$$
$$\forall x, y \in H, x \cdot y \in H,$$
$$\forall x \in H, x^{-1} \in H.$$

♣

命题 1.10 (子群也是群)

令 $(G, \cdot)$ 是一个群。若 H 是 G 的子群，则 $(H, \cdot)$ 也是个群。

♠

证明 就二元运算的良定义性而言，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，结合律肯定满足，因为它是个子集。其次，根据子群的第二个条件，$e \in H$ 是显然的。再次，我们要证明

每个 H 中元素有 H 中的逆元，而这是子群的第三个条件。 □

命题 1.11 (子群的等价条件)

$(H, \cdot)$ 是子群等价于

$$e \in H,$$
$$\forall x, y \in H, x \cdot y^{-1} \in H.$$

证明 假设 $(H, \cdot)$ 是子群。令 $x, y \in H$，利用逆元封闭性得到 $y^{-1} \in H$，再利用乘法封闭性得到 $x \cdot y^{-1} \in H$。

反过来，假设上述条件成立. 令 $x \in H$，则 $e \cdot x^{-1} = x^{-1} \in H$，这证明了逆元封闭性。接下来，令 $x, y \in H$，则利用逆元封闭性，$y^{-1} \in H$，故 $x \cdot (y^{-1})^{-1} = x \cdot y \in H$。这就证明了乘法封闭性。

综上，这的确是子群的等价条件。 □

定义 1.16 (一般线性群)

我们对于那些 $n * n$ 可逆实矩阵构成的乘法群，称为**（实数上的）n 阶一般线性群**，记作 $(GL(n, \mathbb{R}), \cdot)$。由于一个矩阵可逆当且仅当其行列式不为零，因此

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) \neq 0\}.$$

定义 1.17 (特殊线性群)

我们将由那些行列式恰好是 1 的 $n * n$ 实矩阵构成的乘法群称为 **(实数上的)n 阶特殊线性群**，记作 $(SL(n, \mathbb{R}), \cdot)$，即

$$SL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) = 1\}.$$

命题 1.12

$(SL(n, \mathbb{R}), \cdot)$ 是个群。

证明 根据定义，$SL(n, \mathbb{R})$ 首先是 $GL(n, \mathbb{R})$ 的子集，那么只要证明它是个子群即可。首先，乘法单位元单位矩阵的行列式恰好是 1（这也是为什么我们定义特殊线性群是行列式是 1 的矩阵构成的群的原因），这就证明了 $I \in SL(n, \mathbb{R})$（$I = I_n$ 指的是 n 阶单位矩阵）。另外，我们要证明 $SL(n, \mathbb{R})$ 在乘法下封闭。令 A, B 是两个行列式为 1 的 $n * n$ 实矩阵。由于行列式满足 $\det(AB) = \det(A)\det(B)$，因此 AB 的行列式也是 1，也就在特殊线性群中。这就证明了特殊线性群确实是个群。至于逆元封闭性，我们利用 $\det(A^{-1}) = \dfrac{1}{\det(A)}$。假设 $\det(A) = 1$，则 $\det(A^{-1}) = 1$，于是 $A^{-1} \in SL(n, \mathbb{R})$。综上，特殊线性群确实是个群。 □

定义 1.18 (群同态)

令 $(G, \cdot), (G', *)$ 是两个群，且 $f : G \to G'$ 是一个映射。我们称 f 是一个**群同态**，当其保持了乘法运算，即

$$\forall x, y \in G, f(x \cdot y) = f(x) * f(y).$$

命题 1.13

若 $f : (G, \cdot) \to (G', *)$ 是一个群同态，则 $f(e) = e'$，$f(x^{-1}) = f(x)^{-1}$。

笔记 也就是说，f 不仅把乘积映到乘积，而且把单位元映到单位元，把逆元映到逆元。在这个意义下，实际上 f 将所有群 G 的“信息”都保持到了 G' 上，包括单位元，乘法和逆元。至于结合律（或者更基础的封闭性），显然两边本来就有，就不必再提。

证明 首先，因为 $e \cdot e = e$，所以利用同态的性质，$f(e) = f(e \cdot e) = f(e) * f(e)$。这时，两边同时左乘 $f(e)^{-1}$，就可以各约掉一个 $f(e)$，得到 $e' = f(e)$，这就证明了 f 把单位元映到单位元。

另一方面，令 $x \in G$，则 $e' = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$。同理 $e' = f(x^{-1}) * f(x)$。于是由定义，$f(x^{-1})$ 就是 $f(x)$ 的逆元，即 $f(x^{-1}) = f(x)^{-1}$。这就证明了这个命题。 □

命题 1.14

$\det : GL(n, \mathbb{R}) \to (\mathbb{R}^{\times}, \cdot)$ 是一个乘法群同态。

证明 证明是显然的. □

定义 1.19 (群同态的核与像)

令 $f : (G, \cdot) \to (G', *)$ 是一个群同态，则我们定义 f 的**核与像**，记作 $\ker(f)$ 与 $\operatorname{im}(f)$，分别为

$$\ker(f) = \{x \in G : f(x) = e'\} \subset G,$$
$$\operatorname{im}(f) = \{y \in G' : \exists x \in G, y = f(x)\} = \{f(x) : x \in G\} \subset G'.$$

笔记 群同态的核与像示意图如下:

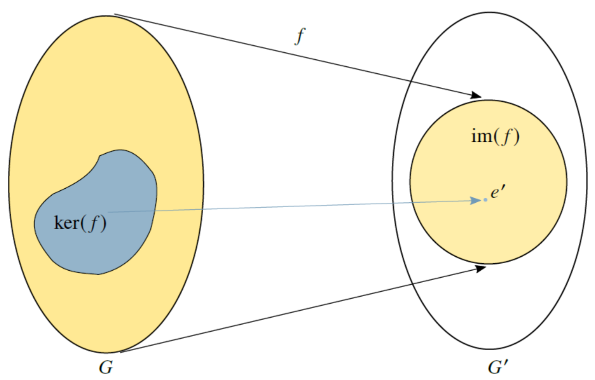

图 1.1: 群同态的核与像示意图

命题 1.15

令 $f : (G, \cdot) \to (G', *)$ 是一个群同态，则核是定义域的子群，像是陪域的子群，即

$$\ker(f) < G, \quad \operatorname{im}(f) < G'.$$

证明 先证明第一个子群关系。我们利用 $f(e) = e'$ 来说明 $e \in \ker(f)$。接着，设 $x, y \in \ker(f)$，只需证明 $xy^{-1} \in \ker(f)$。利用同态的性质，$f(xy^{-1}) = f(x)f(y)^{-1} = e'e'^{-1} = e'$，这就证明了 $xy^{-1} \in \ker(f)$。第一个子群关系得证。

再证明第二个子群关系。同样由于 $f(e) = e'$，我们有 $e' \in \operatorname{im}(f)$。接着，设 $y = f(x), y' = f(x') \in \operatorname{im}(f)$，只需证明 $yy'^{-1} \in \operatorname{im}(f)$。同样利用同态的性质，$yy'^{-1} = f(x)f(x')^{-1} = f(xx'^{-1}) \in \operatorname{im}(f)$。第二个子群关系也得证。这样我们就证完了整个命题。 □

例题 1.3 证明:$(SL(n, \mathbb{R}), \cdot) < (GL(n, \mathbb{R}), \cdot)$.

证明 由命题 1.14可知,$\det : GL(n, \mathbb{R}) \to (\mathbb{R}^{\times}, \cdot)$ 是一个乘法群同态. 注意到 $\ker(det) = (SL(n, \mathbb{R}), \cdot)$, 因此由命题 1.15可知,$(SL(n, \mathbb{R}), \cdot) = \ker(det) < (GL(n, \mathbb{R}), \cdot)$. □

定义 1.20 (满同态与单同态)

令 $f : (G, \cdot) \to (G', *)$ 是一个群同态，我们称 f 是一个**满同态**当 f 是满射，称 f 是一个**单同态**当 f 是单射。

命题 1.16

令 $f:(G,\cdot)\to(G',*)$ 是一个群同态，则 f 是一个单同态当且仅当 $\ker(f)=\{e\}$。也就是说，一个群同态是单的当且仅当核是平凡的。

证明 假设 f 是单的，那么因为 $f(e)=e'$，因此若 $f(x)=e'$，则利用单射的性质我们一定有 $x=e$，这就证明了核是平凡的。(这个方向是显然的)

另一个方向不那么显然。我们假设 $\ker(f)=\{e'\}$。假设 $x,x'\in G$，使得 $f(x)=f(x')$，我们只须证明 $x=x'$。在这里，我们同时右乘 $f(x')^{-1}$，得到 $f(x)f(x'^{-1})=f(xx'^{-1})=e'$。而因为核是平凡的，所以必须有 $xx'^{-1}=e$。接下来同时右乘 x'，我们就得到 $x=x'$。这就证明了这个命题。 □

笔记 平凡群, 满同态和单同态示意图如下:

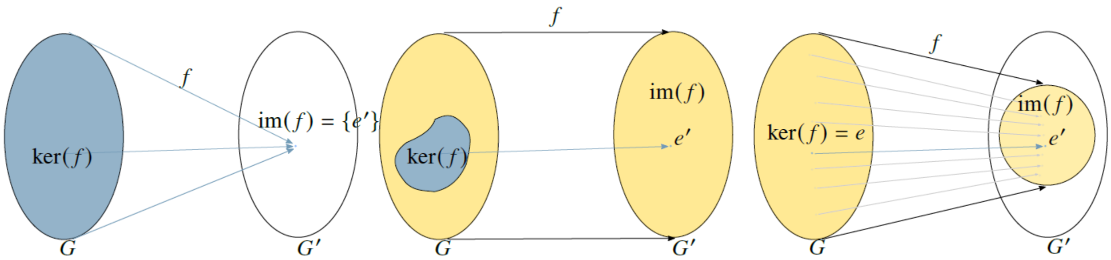

图 1.2: 平凡群, 满同态和单同态示意图

定义 1.21 (群同构)

令 $f:(G,\cdot)\to(G',*)$ 是一个映射，我们称 f 是一个**群同构**，当 f 既是一个双射，又是一个群同态。简单来说，同构就是双射的同态。

命题 1.17 (群同构的逆也是群同构)

若 $f:(G,\cdot)\to(G',*)$ 是一个群同构，则 f^{-1} 也是群同构。

证明 因为 f^{-1} 也是双射，所以我们只须证明 f^{-1} 是群同态。令 $x',y'\in G'$，设 $x'=f(x),y'=f(y)$。则 $x'*y'=f(x\cdot y)$,$x=f^{-1}(x'),y=f^{-1}(y')$, 故 $f^{-1}(x'*y')=x\cdot y=f^{-1}(x')\cdot f^{-1}(y')$。这就完成了证明。 □

定义 1.22 (两个群的直积)

令 $(G,\cdot_1),(G',\cdot_2)$ 是两个群, 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 1.18 (两个群的直积仍是群)

若 $(G,\cdot_1),(G',\cdot_2)$ 是两个群，则它们的直积 $(G\times G',*)$ 还是一个群。

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。

逆元：对于任意 $(x,y)\in G\times G'$，设 x^{-1},y^{-1} 分别是 x,y 的逆元, 则同样不难想象，(x^{-1},y^{-1}) 是 (x,y) 的逆元。

□

定义 1.23 (一族群的直积)

令 $(G_i,\cdot_i)_{i\in I}$ 是一族群，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 1.19 (一族群的直积仍是群)

若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，则它们的直积 $(\prod_{i\in I} G_i,*)$ 还是一个群。

♠

笔记 最经典的例子就是通过 n 个实数加群 $(\mathbb{R},+)$ 直积得到的 $(\mathbb{R}^n,+)$。

证明 证明与命题 1.18同理. 故我们只列出一些重点。封闭性与结合律是显然的。单位元是 $(e_i)_{i\in I}$，而 $(x_i)_{i\in I}$ 的逆元是 $(x_i^{-1})_{i\in I}$。 □

定义 1.24 (投影映射)

若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，$j\in I$ 是任意指标，我们定义映射到指标 j 的**投影映射**为

$$p_j:\prod_{i\in I} G_i\to G_j.$$

对于 $(x_i)_{i\in I}$，我们称 $p_j((x_i)_{i\in I})=x_j$ 为 $(x_i)_{i\in I}$ 的**投影**.

♣

命题 1.20 (投影映射是群同态)

若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，$j\in I$ 是任意指标，则投影映射 $p_j:\prod_{i\in I} G_i\to G_j$ 是个群同态。

♠

证明 令 $(x_i)_{i\in I},(y_i)_{i\in I}\in\prod_{i\in I} G_i$，则

$$p_j((x_i)_{i\in I})=x_j,\quad p_j((y_i)_{i\in I})=y_j$$

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

□