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 “$\cdot$” 满足结合律, 我们有

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

□

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

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

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

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

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

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

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

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

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)

设 $(G,\cdot)$ 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。 □

推论 1.2 (子群的传递性)

若 $(G,\cdot)$ 是一个群, 且 $H < G, K < H$, 则一定有 $K < G$. 因此我们可以将 $H < G, K < H$ 简记为 $K < H < G$. ♡

证明 证明是显然的. □

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 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。 □

命题 1.12 (子群的任意交仍是子群)

设 G 是一个群, $(H_i)_{i\in I}$ 是一族 G 的子群，则它们的交集仍然是 G 的子群，即

$$\bigcap_{i\in I} N_i < G.$$

♠

证明 首先, 设 e 是 G 的单位元, 则由子群对单位元封闭可知,$e \in N_i, \forall i \in I$. 从而 $e \in \bigcap_{i\in I} N_i$.

其次, 对 $\forall x, y \in \bigcap_{i\in I} N_i$, 都有 $x, y \in N_i, \forall i \in I$. 根据子群对逆元封闭可知,$y^{-1} \in N_i, \forall i \in I$. 于是再由子群对乘法封闭可知,$xy^{-1} \in N_i, \forall i \in I$. 故 $xy^{-1} \in \bigcap_{i\in I} N_i$.

综上,$\bigcap_{i\in I} N_i < G$. □

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 1.13

$(SL(n,\mathbb{R}),\cdot)$ 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 1.14

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 1.15

$\det : GL(n, \mathbb{R}) \to (\mathbb{R}^{\times}, \cdot)$ 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 $\mathrm{im}(f)$，分别为

$$\ker(f) = \{x \in G : f(x) = e'\} \subset G,$$

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

笔记 群同态的核与像示意图如下:

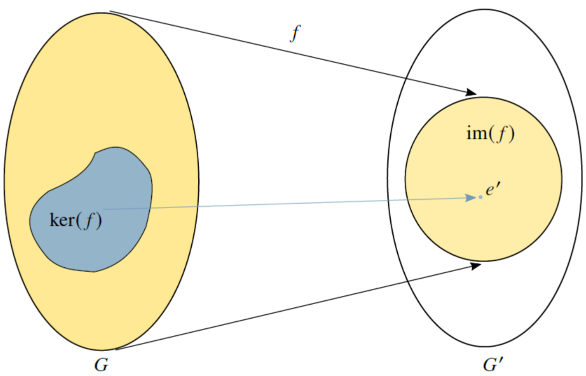

图 1.1: 群同态的核与像示意图

命题 1.16

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

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

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 $e'\in\mathrm{im}(f)$。接着，设 $y=f(x),y'=f(x')\in\mathrm{im}(f)$，只需证明 $yy'^{-1}\in\mathrm{im}(f)$。同样利用同态的性质，$yy'^{-1}=f(x)f(x')^{-1}=f(xx'^{-1})\in\mathrm{im}(f)$。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 1.15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 1.16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 1.17

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:

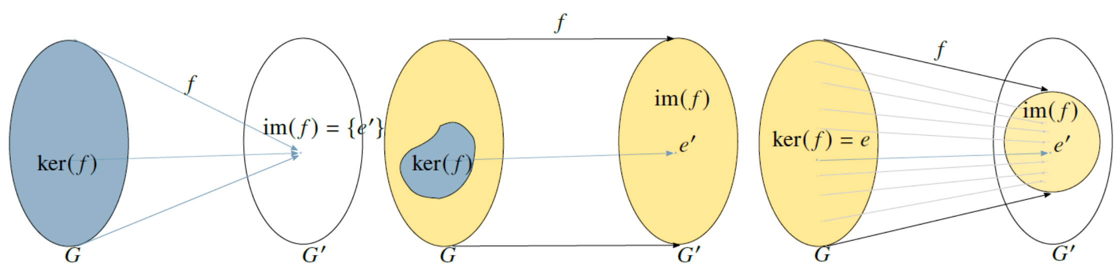

图 1.2: 平凡群, 满同态和单同态示意图

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 1.18 (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 1.19 (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 1.20 (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 1.19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 1.21 (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

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

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

□

1.3 有限群

定义 1.25 (有限群)

设 $(G,\cdot)$ 是一个群. 我们称 G 是一个**有限群**，若 G 是有限的。

定义 1.26 (元素的阶)

设 $(G,\cdot)$ 是一个群, 若 $x \in G$，则 x（在 G 中）的**阶**，记作 $|x|$，定义为那个最小的正整数 $n \in \mathbb{N}_1$，使得 $x^n = e$。若这样的 n 不存在，则记 $|x| = \infty$。

命题 1.22 (有限群的每个元素的阶必有限)

若 $(G,\cdot)$ 是有限群，且 $x \in G$，则 $|x| < \infty$。换言之，有限群的每一个元素通过自乘有限多次，都可以得到单位元。

证明 我们用反证法，假设 $|x| = \infty$，那么根据定义，对于任意的 $n \in \mathbb{N}_1$，我们都有 $x^n \neq e$。我们要说明的是，这会导致一个事实，就是所有的 $x^n (n \in \mathbb{N}_1)$ 都是不同的。假设但凡有一对 $n \neq m \in \mathbb{N}_1$ 使得 $x^n = x^m$，不失一般性我们假设 $n > m$。则通过反复的消元 (两边反复右乘 x^{-1})，我们可以得到 $x^{n-m} = e$，其中 $n - m \in \mathbb{N}_1$，而这与假设是矛盾的，因为我们假设 x 的阶是无穷的。因此，这个事实是对的——所有的 $x^n (n \in \mathbb{N}_1)$ 都是不同的, 从而 G 中有无穷多个元素, 这与 G 是有限群矛盾. 这就证明了这个命题。 □

命题 1.23

令 $(G,\cdot)$ 是一个群，任取 $x \in G$。则

$$\begin{aligned} f : (\mathbb{Z}, +) &\to (G,\cdot) \\ n &\mapsto x^n \end{aligned}$$

是一个群同态。

证明 取定 $x \in G$。令 $m, n \in \mathbb{Z}$，我们只须证明 $f(m+n) = f(m)\cdot f(n)$，也即 $x^{m+n} = x^m \cdot x^n$。于是根据命题 1.9(1)就能立即得到结论. □

定义 1.27 (由 x 生成的群)

设 $(G,\cdot)$ 是一个群，且 $x \in G$，则 $\langle x\rangle$，被称为**由 x 生成的群**，定义为

$$\langle x\rangle = \{x^n : n \in \mathbb{Z}\}.$$

命题 1.24

设 $(G,\cdot)$ 是一个群，且 $x \in G$，则 $\langle x\rangle < G$.

证明 记

$$\begin{aligned} f : (\mathbb{Z}, +) &\to (G,\cdot) \\ n &\mapsto x^n \end{aligned}$$

由命题 1.23可知 f 是一个群同态. 注意到 $\operatorname{im} f = \langle x\rangle$, 即 $\langle x\rangle$ 是 f 的同态像. 从而由命题 1.16可知,$\langle x\rangle = \operatorname{im} f < G$. □

定义 1.28 (由 S 生成的群)

设 $(G,\cdot)$ 是一个群，且 $S \subset G$。则**由 S 生成的群**，记作 $\langle S\rangle$，定义为

$$\langle S\rangle = \bigcap\{H \subset G : H \supset S, H < G\}$$

命题 1.25

令 $(G,\cdot)$ 是一个群，且 $S \subset G$，则 $\langle S\rangle < G$.

笔记 这个命题表明:G 中由 S 生成的子群，确实是包含了 S 的最小子群.

证明 在这里，我们只要证明其包含单位元，在乘法和逆元下封闭。

根据定义，$\langle S\rangle$ 是由所有包含了 S 的 G 中子群全部取交集得到的。

单位元：每个这样的子群 H 都包含单位元，故它们的交集也包含单位元。

乘法封闭性：设 $x, y \in \langle S\rangle$，任取一个包含了 S 的子群 H，则 $x, y \in H$。因为 H 是子群，故 $xy \in H$，所以由 H 的任意性可知 $xy \in \langle S\rangle$。

逆元封闭性：设 $x \in \langle S\rangle$, 任取一个包含了 S 的子群 H，则 $x \in H$。因为 H 是子群，故 $x^{-1} \in H$，所以由 H 的任意性可知 $x^{-1} \in \langle S\rangle$. □

定义 1.29 (循环群)

令 $(G,\cdot)$ 是一个群。若存在 $x \in G$，使得 $G = \langle x\rangle = \{x^n : n \in \mathbb{Z}\}$，则 G 被称为一个**循环群**，而 x 被称为 G 的一个**生成元**.

若 G 还是一个有限群, 则我们称 G 为**有限循环群**. 若 G 不是有限群, 则我们称 G 为**无限循环群**.

笔记 有限循环群与无限循环群示意图如下:

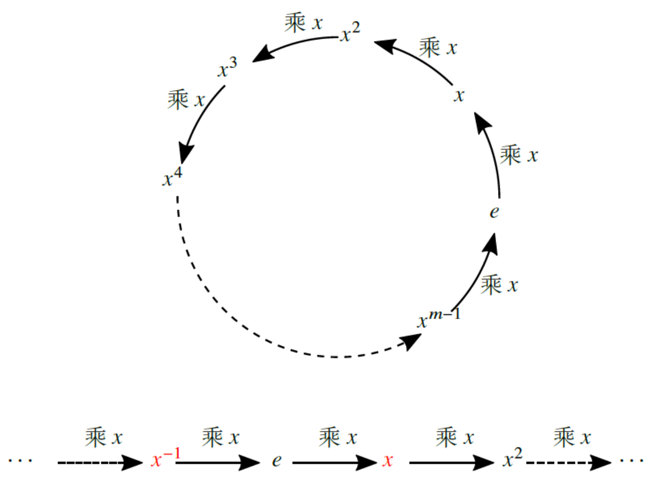

图 1.3: 有限循环群和无线循环群

命题 1.26

设 $(G,\cdot)$ 是一个群, 对 $\forall x \in G$, 都有 $\langle x\rangle = \langle\{x\}\rangle$.

笔记 这个命题表明: 由 x 生成的群就是由子集 $\{x\}$ 生成的子群.

证明 根据定义和性质，$\langle\{x\}\rangle$ 是包含了 $\{x\}$ 的最小的子群。因此要证明这个最小的子群就是 $\langle x\rangle$，我们只须证明两点。一，$\langle x\rangle$ 是个子群；二，如果一个子群 H 包含了 $\{x\}$，那么它一定要包含整个 $\langle x\rangle$。

首先, 由命题 1.24可知 $\langle x\rangle$ 是个子群。这就证明了第一点。

第二点几乎也是显然的。我们设 H 是个子群，且 $x \in H$。那么根据子群包含单位元，且有乘法和逆元的封闭

性，我们有 $e\in H$，并且递归地，对于 $\forall n\in\mathbb{N}_1$, 都有 $x^n=x\cdots x\in H$，$x^{-n}=x^{-1}\cdots x^{-1}\in H$。这就证明了 $H\supset\langle x\rangle$。
□

命题 1.27

设 $G=\langle x\rangle$ 是有限循环群, 并且 $|x|=n$，则 $G=\{e,x,x^2,\cdots,x^{n-1}\}$, 并且 $\{e,x,x^2,\cdots,x^{n-1}\}$ 中的这些元素是两两不同的。我们称这样的有限循环群的阶是 n。

证明 我们来证明两件事。第一，每一个 G 中元素都可以写成从 0 开始的前 n 项幂的形式；第二，从 0 开始的前 n 项幂是两两不同的。

我们来证明第一点。任取 G 中元素 x^m，其中 $m\in\mathbb{Z}$。根据带余除法，存在 $q\in\mathbb{Z}$，$0\le r\le n-1$, 使得 $m=qn+r$. 那么因为 $x^n=e$，所以 $x^m=x^{qn+r}=(x^n)^q\cdot x^r=x^r$，而这就属于从 0 开始的前 n 项幂。

我们来证明第二点。用反证法，假设 $0\le m'<m\le n-1$，使得 $x^m=x^{m'}$，则 $x^{m-m'}=e$。其中 $1\le m-m'\le n-1<n$，可是 $n=|x|$ 是最小的正整数 k 使 $x^k=e$，这就导致了矛盾。

综上所述，$G=\{e,x,x^2,\cdots,x^{n-1}\}$，其中枚举法中的这些元素是两两不同的。 □

命题 1.28

对于任意的 $n\in\mathbb{N}_1$，所有 n 阶的循环群都是互相同构的.

证明 设 $G=\langle x\rangle, G'=\langle y\rangle$ 都是 n 阶循环群。令

$$f:G\to G',x^m\mapsto y^m$$

则对 $\forall x^{m_1},x^{m_2}\in G$, 其中 $1\le m_1,m_2\le n-1$. 我们都有

$$f\left(x^{m_1}x^{m_2}\right)=f\left(x^{m_1+m_2}\right)=y^{m_1+m_2}=y^{m_1}y^{m_2}=f\left(x^{m_1}\right)f\left(x^{m_2}\right).$$

因此 f 是个同态映射. 此外，它是个双射，因为我们可以明确地找到其逆映射

$$f^{-1}(y^m)=x^m$$

这样，f 既是双射，也是同态，这就证明了 f 是个同构。 □

命题 1.29

令 $G=\langle x\rangle$ 是无限循环群，则 $x^n(n\in\mathbb{Z})$ 是两两不同的，且 G 只有两个生成元，分别是 x 与 x^{-1}。

笔记 显然,$(\mathbb{Z},+)$ 就是一个无限循环群, 生成元是 1 或-1.

证明 首先证明 $x^n(n\in\mathbb{Z})$ 是两两不同的。假设有两个相同，不失一般性假设 $m>n\in\mathbb{Z},x^m=x^n$，则 $x^{m-n}=e$，故 x 是有有限阶的。这就矛盾了。

接着，如果 $x^n(n\in\mathbb{Z})$ 可以生成这个群，那么 $x\in\langle x^n\rangle$，于是存在 $m\in\mathbb{Z}$ 使得 $x=(x^n)^m$，于是 $x^{nm-1}=e$。由于 x 是无限阶的，所以 $nm=1$，那么这样的 n 只能是 ±1。另外，显然 x^{-1} 也可以生成这个群。这就证明了恰好是这两个生成元。
□

命题 1.30

所有的无限循环群是彼此同构的。

笔记 这个命题告诉我们: 要研究无限循环群, 只要研究整数加群 $(\mathbb{Z},+)$ 就可以了.

证明 设 $G=\langle x\rangle, G'=\langle y\rangle$ 都是无限循环群。令

$$f:G\to G',x^m\mapsto y^m$$

则对 $\forall x^{m_1},x^{m_2}\in G$, 其中 $m_1,m_2\in\mathbb{Z}$. 我们都有

$$f\left(x^{m_1}x^{m_2}\right)=f\left(x^{m_1+m_2}\right)=y^{m_1+m_2}=y^{m_1}y^{m_2}=f\left(x^{m_1}\right)f\left(x^{m_2}\right).$$

因此 f 是个同态映射. 此外，它是个双射，因为我们可以明确地找到其逆映射

$$f^{-1}(y^m) = x^m$$

这样，f 既是双射，也是同态，这就证明了 f 是个同构。 □

命题 1.31

令 $G = \langle x \rangle$ 是一个 n 阶循环群。假设 $1 \leq m \leq n$，则 x^m 的阶为

$$|x^m| = \frac{n}{\gcd(n, m)}.$$

证明 设 $1 \leq m \leq n-1$，我们希望找到最小的正整数 k 使得 $(x^m)^k = x^{mk} = e$。由于 $|x| = n$，故这等价于 $n \mid mk$。接下来我们要利用简单的初等数论。通过同时除以 n 和 m 的最大公因数，我们得到

$$\frac{n}{\gcd(n, m)} \bigg| \frac{m}{\gcd(n, m)} \cdot k$$

而因为 $\dfrac{n}{\gcd(n, m)}$ 和 $\dfrac{m}{\gcd(n, m)}$ 是互素的，所以这个条件进一步等价于

$$\frac{n}{\gcd(n, m)} \bigg| k$$

也就是说，最小的这个正整数 k 正是 $\dfrac{n}{\gcd(n, m)}$。这就完成了证明. □

命题 1.32

令 $G = \langle x \rangle$ 是一个 n 阶循环群，则 $x^m (1 \leq m \leq n)$ 是个生成元，当且仅当

$$\gcd(m, n) = 1.$$

根据欧拉 ϕ 函数的定义，这些生成元的个数正是 $\phi(n)$。

证明 若 x^m 是一个生成元, 则由 G 是一个 n 阶循环群可知,$|x^m| = n$. 从而由命题 1.31可知,$\gcd(m, n) = \dfrac{n}{|x^m|} = 1$.

若 $\gcd(m, n) = 1$, 则由命题 1.31可知,$|x^m| = \dfrac{n}{\gcd(n, m)} = n$. 从而

$$(x^m)^n = e,\ (x^m)^{n+1} = (x^m)^n x = x, \cdots, (x^m)^{2n-1} = (x^m)^n x^{n-1} = x^{n-1}.$$

又由命题 1.27可知 $G = \{e, x, \cdots, x^{n-1}\}$. 于是

$$G = \left\{e, x, \cdots, x^{n-1}\right\} = \left\{(x^m)^n, (x^m)^{n+1}, \cdots, (x^m)^{2n-1}\right\} = \left\{(x^m)^n : n \in \mathbb{Z}\right\}.$$

因此 $G = \langle x^m \rangle$, 故 x^m 是 G 的生成元. □

定义 1.30 (群的阶)

设 $(G, \cdot)$ 是一个群, 则 G 的阶，记作 $|G|$，定义为 G 的集合大小 (元素的个数).

定义 1.31 (子群的阶)

设 $(G, \cdot)$ 是一个群,H 是 G 的子群，则 H 的阶，记作 $|H|$，定义为 H 的集合大小 (元素的个数)。若 H 是无限群则记 $|H| = \infty$。

定义 1.32 (左陪集)

设 G 是一个群，$H < G$ 是一个子群，$a \in G$。则称 aH 是 H 的一个（由 a 引出的）**左陪集**，定义为

$$aH = \{ax : x \in H\}.$$

称 aH 是 H 的一个（由 a 引出的）**右陪集**，定义为

$$Ha = \{xa : x \in H\}.$$

注 aH, Ha 一般来说不是 G 的子群.

我们只讨论左陪集的性质和结论, 右陪集的性质与左陪集类似.

引理 1.2

令 G 是一个有限群，$H < G$ 是一个子群，$a \in G$。令

$$f : H \to aH, x \mapsto ax.$$

则 f 是一个双射。特别地，$|H| = |aH|$。

笔记 这个引理表明: 陪集的大小都是一样的.

证明 证法一: 根据 f 的定义易知 f 是满射. 若 $f(h_1) = f(h_2)$，则

$$ah_1 = ah_2 \Rightarrow a^{-1}ah_1 = a^{-1}ah_2 \Rightarrow h_1 = h_2.$$

故 f 也是单射。因此 f 是双射。

证法二: 令

$$g : aH \to H, k \mapsto a^{-1}k.$$

设 $k \in aH$，则存在 $h \in H$，使得 $k = ah$。则 $g(k) = g(ah) = a^{-1}ah = h \in H$。故 g 是良定义的。注意到

$$g \circ f = \mathrm{id}_H, \quad f \circ g = \mathrm{id}_{aH}.$$

故 g 是 f 的逆映射。因此 f 是双射。 □

命题 1.33

设 G 是一个有限群，$H < G$ 是一个子群，$a, b \in G$。则左陪集 aH 和 bH 要么相等，要么无交。也就是说，我们有 $aH = bH$，或 $aH \cap bH = \emptyset$。

证明 假设 $aH \cap bH \neq \emptyset$, 则可设 $ah_1 = bh_2 \in aH \cap bH$，其中 $h_1, h_2 \in H$。我们只须证明 $aH = bH$，而根据对称性，我们只须证明 $aH \subset bH$ 即可。任取 aH 中的元素 $ah(h \in H)$，则由 $ah_1 = bh_2$ 可知,$a = bh_2h_1^{-1}$. 从而

$$ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$$

这就完成了证明. □

定义 1.33 (商集)

设 G 是一个非空集合,$H \subset G$ 是一个子集合. 则**商集** G/H 定义为

$$G/H = \{aH : a \in G\}.$$

我们把这个商集的大小 (所含元素的个数) 称为 H 在 G 中的**指数**，记为 $[G : H]$，即

$$[G : H] = |G/H|.$$

定理 1.1

设 G 是一个有限群，$H < G$ 是一个子群, 则商集 $G/H = \{aH : a \in G\}$ 就是 G 的一个分拆, 即

$$G = \bigsqcup_{i=1}^{[G:H]} a_iH = \bigsqcup_{a \in G} aH.$$

证明 一方面，设 $x \in G$，取 $a = x$，则 $x = xe = ae \in xH$. 另一方面，由由命题 1.33可知，对 $\forall aH, bH \in G/H$，都

有 aH 和 bH 要么相等，要么无交. 故商集 $G/H = \{aH : a \in G\}$ 就是 G 的一个分拆. □

笔记

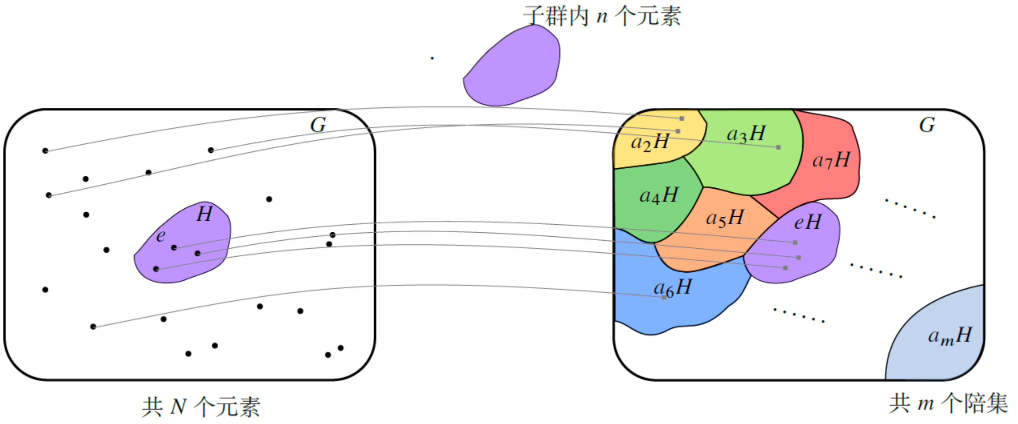

图 1.4: 左陪集示意图

定理 1.2 (Lagrange 定理)

设 G 是一个有限群，$H < G$ 是一个子群，则

$$|G| = [G : H]|H|.$$

进而 $[G : H] = \dfrac{|G|}{|H|}$. 特别地，

$$|H| \Big| |G|.$$

证明 由定理 1.1可知 $G = \bigsqcup_{i=1}^{[G:H]} a_iH$, 从而

$$|G| = \sum_{i=1}^{[G:H]} |a_iH_i|.$$

又由引理 1.2可知 $|a_iH_i| = |H|$. 故

$$|G| = [G : H]|H|.$$

□

例题 1.4 设 $(G, \cdot)$ 是一个群，若 $|G| = p$ 是素数，则不存在任何非平凡子群.

证明 设 $H < G$, 则由Lagrange 定理可知 $|H| \mid |G|$，即 $|H| \mid p$。从而 $|H| = 1$ 或 p，于是 $H = \{e\}$ 或 G。 □

引理 1.3

设 G 是一个群，$H < G$ 是一个子群,$x, y, a, b \in G$, 则

(1) $xH \subset yH \Leftrightarrow axHb \subset ayHb$.

(2) $Hx \subset Hy \Leftrightarrow aHxb \subset aHyb$.

(3) $xH \subset Hy \Leftrightarrow axHb \subset aHyb$.

进一步, 我们有

(4) $xH = yH \Leftrightarrow axHb = ayHb$.

(5) $Hx = Hy \Leftrightarrow aHxb = aHyb$.

(6) $xH = Hy \Leftrightarrow axHb = aHyb$.

证明

(4) $\Rightarrow$: 若 $xH = yH$，则要证 $axHb = ayHb$，根据对称性，只须证 $axHb \subset ayHb$。任取 $axhb \in axHb$，其中

$h \in H$，则由 $xH = yH$ 及 $xh \in xH$ 可知，存在 $h' \in H$，使得 $xh = yh'$。从而 $axhb = ayh'b \in ayHb$。故 $axHb \subset ayHb$。

$\Leftarrow$: 若 $axHb = ayHb$，则要证 $xH = yH$，根据对称性，只须证 $xH \subset yH$。任取 $xh \in xH$，其中 $h \in H$，则由 $axHb = ayHb$ 及 $axhb \in axHb$ 可知，存在 $h' \in H$，使得 $axhb = ayh'b$。从而 $xh = a^{-1}axhbb^{-1} = a^{-1}ayh'bb^{-1} = yh' \in yH$。故 $xH \subset yH$.

(5) $\Rightarrow$: 若 $Hx = Hy$，则要证 $aHxb = aHyb$，根据对称性，只须证 $aHxb \subset aHyb$. 任取 $ahxb \in aHxb$，其中 $h \in H$，则由 $Hx = Hy$ 及 $hx \in Hx$ 可知，存在 $h' \in H$，使得 $hx = h'y$。从而 $ahxb = ah'yb \in aHyb$。故 $aHxb \subset aHyb$。

$\Leftarrow$: 若 $aHbx = aHyb$，则要证 $Hx = Hy$，根据对称性，只须证 $Hx \subset Hy$。任取 $hx \in Hx$，其中 $h \in H$，则由 $aHxb = aHyb$ 及 $ahxb \in aHxb$ 可知，存在 $h' \in H$，使得 $ahxb = ah'yb$。从而 $hx = a^{-1}ahxbb^{-1} = a^{-1}ah'ybb^{-1} = h'y \in Hy$。故 $Hx \subset Hy$.

(6) $\Rightarrow$: 若 $xH = Hy$，则要证 $axHb = aHyb$，根据对称性，只须证 $axHb \subset aHyb$。任取 $axhb \in axHb$，其中 $h \in H$，则由 $xH = Hy$ 及 $xh \in xH$ 可知，存在 $h' \in H$，使得 $xh = h'y$。从而 $axhb = ah'yb \in aHyb$。故 $axHb \subset aHyb$。

$\Leftarrow$: 若 $axHb = aHyb$，则要证 $xH = Hy$，根据对称性，只须证 $xH \subset Hy$。任取 $xh \in xH$，其中 $h \in H$，则由 $axHb = aHyb$ 及 $axhb \in axHb$ 可知，存在 $h' \in H$，使得 $axhb = ah'yb$。从而 $xh = a^{-1}axhbb^{-1} = a^{-1}ah'ybb^{-1} = h'y \in Hy$。故 $xH \subset Hy$.

根据上述 (4)(5)(6) 的证明过程就能直接得到 (1)(2)(3) 的证明. □

引理 1.4

设 G 是一个群，$H < G$ 是一个子群，$x \in G$，则我们有充要条件

$$xH = H \iff x \in H.$$

一般地，对于 $x, y \in G$，我们有充要条件

$$xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H \iff x \in yH \iff y \in xH.$$

笔记 同理可知对右陪集也有相同的结论.

证明 对于 $x \in G$, 一方面，设 $xH = H$, 则 $x = xe \in xH = H$，因此 $x \in H$。

另一方面，证法一:设 $x \in H$，任取 $xh \in xH$，则根据乘法封闭性可知 $xh \in H$。故 $xH \subset H$。任取 $h \in H$，则根据乘法封闭性和逆元封闭性可知 $x^{-1}h \in H$，从而 $h = xx^{-1}h \in xH$。故 $H \subset xH$. 因此 $xH = H$.

证法二:设 $x \in H$，则 $x = xe \in xH$. 从而 $xH \cap H \neq \emptyset$. 于是由命题 1.33可知 $xH = H$.

综上, 我们就有 $xH = H \iff x \in H$.

一般地, 对于 $x, y \in G$, 由引理 1.3可知 $xH = yH \Leftrightarrow y^{-1}xH = H \Leftrightarrow H = x^{-1}yH$, 又由上述证明可知

$$y^{-1}xH = H \iff y^{-1}x \in H, x^{-1}yH = H \iff x^{-1}y \in H.$$

故 $xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H$. 下证 $xH = yH \iff x \in yH \iff y \in xH$.

一方面，设 $xH = yH$, 则 $x = xe \in xH = yH$，因此 $x \in yH$。另一方面，设 $x \in yH$，则 $x = xe \in xH$. 从而 $xH \cap yH \neq \emptyset$. 于是由命题 1.33可知 $xH = yH$. 故 $xH = yH \iff x \in yH$. 同理可证 $xH = yH \iff y \in xH$. □

推论 1.3

(1) 设 G 是一个群，$H < G$ 是一个子群，$a \in G$, 则

$$axH = aH \iff x \in H.$$

(2) 设 G 是一个群，$K < H < G, a_1, a_2 \in G, b_1, b_2 \in H$. 若 $a_1b_1K = a_2b_2K$, 则 $a_1H = a_2H$.

笔记 同理可知对右陪集也有相同的结论.

证明

(1) 由引理 1.3可知

$$axH = aH \iff xH = H.$$

又由引理 1.4可知

$$xH = H \iff x \in H.$$

故

$$axH = aH \iff x \in H.$$

(2) 由引理 1.4可知 $b_2^{-1}a_2^{-1}a_1b_1 \in K$, 从而存在 $k \in K$, 使得 $b_2^{-1}a_2^{-1}a_1b_1 = k$, 于是 $a_2^{-1}a_1 = b_2kb_1^{-1} \in H$. 再根据引理 1.4可知 $a_1H = a_2H$.

□

命题 1.34

令 $K < H < G$ 是三个有限群，则

$$[G:K] = [G:H][H:K].$$

证明 证法一:由Lagrange 定理可得

$$[G:K] = \frac{|G|}{K} = \frac{|G|}{|H|}\cdot\frac{|H|}{|K|} = [G:H][H:K].$$

证法二:设 $G/H = \{a_iH\}_{i\in I}$，$H/K = \{b_jK\}_{j\in J}$，其中 $I = \{1,2,\cdots,[G:H]\}$，$J = \{1,2,\cdots,[H:K]\}$。则 $|I| = [G:H]$，$|J| = [H:K]$。

先证明 $G/K = \{a_ib_jK\}_{i\in I,j\in J}$。因为 $G/K = \{xK : x \in G\}$，所以任取 $xK \in G/K$，都有 $x \in G$。由定理 1.1可知 $G = \bigsqcup_{i=1}^{[G:H]} a_iH$，从而存在 $i \in I$，使得 $x \in a_iH$。于是存在 $h \in H$，使得 $x = a_ih$。再由定理 1.1可知 $H = \bigsqcup_{j=1}^{[H:K]} b_jK$，因此存在 $j \in J$，使得 $h \in b_jK$。进而存在 $k \in K$，使得 $h = b_jk$。于是 $x = a_ih = a_ib_jk$。故由推论可得

$$xK = a_ib_jkK = a_ib_jK.$$

再由 xK 的任意性可知 $G/K = \{a_ib_jK\}_{i\in I,j\in J}$。

再证明 $\{a_ib_jK\}_{i\in I,j\in J}$ 两两互异 (集合中不含重复元素)。设 $a_ib_jK = a_{i'}b_{j'}K$，则由推论 1.3(2)可知，$a_iH = a_{i'}H$。又因为 $G/H = \{a_iH\}_{i\in I}$，所以 $\{a_iH\}_{i\in I}$ 两两互异，从而 $a_i = a_{i'}$。于是由引理 1.3可得

$$a_ib_jK = a_{i'}b_{j'}K \Leftrightarrow a_ib_jK = a_ib_{j'}K \Leftrightarrow a_i^{-1}a_ib_jK = a_i^{-1}a_ib_{j'}K \Leftrightarrow b_jK = b_{j'}K.$$

又因为 $H/K = \{b_jK\}_{j\in J}$，所以 $\{b_jK\}_{j\in J}$ 两两互异，因此 $b_j = b_{j'}$。故 $\{a_ib_jK\}_{i\in I,j\in J}$ 两两互异 (集合中不含重复元素)。

综上，$G/K = \bigsqcup_{i\in I}\bigsqcup_{j\in J} a_ib_jK$。因此根据定义 1.33可知

$$[G:K] = |I|\cdot|J| = [G:H][H:K].$$

□

定义 1.34 (两个子群的乘积)

设 G 是一个群, 且 $H,K < G$, 定义 H 和 K 的乘积为

$$HK = \{hk : h \in H, k \in K\}.$$

注 两个子群的乘积不一定是子群.

命题 1.35

令 $(G,\cdot)$ 是一个群。若 $H,K<G$ 是两个有限子群，则

$$|HK|=\frac{|H||K|}{|H\cap K|},\text{也即}|HK||H\cap K|=|H||K|.$$

其中 HK 未必是 G 的子群, 也不一定是群.

证明 证法一:不考虑重复性，HK 产生 $|H||K|$ 个元素，其中存在 $hk=h'k'$，$h\neq h'$，$k\neq k'$ 的情况。

现在分析产生相同乘积的 (h,k) 组合个数，对 $\forall t\in H\cap K$，都有 $hk=(ht)(t^{-1}k)$。从而一方面，对 $\forall t_1,t_2\in H\cap K$ 且 $t_1\neq t_2$，都有 $ht_i\in H$，$t_i^{-1}k\in K(i=1,2)$，$(ht_1,t_1^{-1}k)\neq(ht_2,t_2^{-1}k)$，但 $(ht_1)(t_1^{-1}k)=hk=(ht_2)(t_2^{-1}k)$。于是 HK 中产生相同乘积的不同 (h,k) 组合至少有 $|H\cap K|$ 个。

另一方面，我们有

$$\begin{aligned}hk=h'k' &\iff t=h^{-1}h'=k(k')^{-1}\in H\cap K\\ &\iff \exists t\in H\cap K\ \text{s.t.}\ h'=ht,k'=t^{-1}k.\end{aligned}$$

因此 HK 中产生相同乘积的不同 (h,k) 组合最多有 $|H\cap K|$ 个。综上，HK 中产生相同乘积的不同 (h,k) 组合恰好有 $|H\cap K|$ 个。故 $|HK|=\dfrac{|H||K|}{|H\cap K|}$。

证法二 (有待考察): 原命题等价于证明

$$\frac{|HK|}{|K|}=\frac{|H|}{|H\cap K|}.$$

因为 $H\cap K<H$，我们可以假设 $H/(H\cap K)=\{a_i(H\cap K)\}_{i\in I}$，其中 $a_i\in H(i\in I)$ 是两两不同的。我们只须证明 $HK/K=\{a_iK\}_{i\in I}$, 并且 HK/K 中的重复元对应的指标与 $H/(H\cap K)$ 相同. 再根据 $H/(H\cap K)$ 和 HK/K 的指标集相同都是 I 就能得到两个商集 $H/(H\cap K)$ 和 HK/K 所含元素的个数相等.

任取 $hkK=hK\in HK/K$，其中 $h\in H$，故存在 $i\in I$ 使得 $h\in a_i(H\cap K)$。假设 $h=a_ix$，其中 x 既在 H，也在 K。这样，$hkK=hK=a_ixK=a_iK$，因为 $x\in K$。这就证明了第一点。

接着，假设 $a_iK=a_jK$，其中 $i,j\in I$。我们只须证明 $a_i(H\cap K)=a_j(H\cap K)$。根据引理 1.4可知 $a_j^{-1}a_i\in K$，可是 $a_i=a_j\in H$，于是 $a_j^{-1}a_i\in H\cap K$。同样根据引理 1.4，我们知道 $a_i(H\cap K)=a_j(H\cap K)$。这就证明了第二点。

综上所述, 两个商集 $H/(H\cap K)$ 和 HK/K 所含元素的个数相等. 显然 H 是一个群, 于是由Lagrange 定理及商集的性质可得

$$\frac{|HK|}{|K|}\overset{?}{=\!=}[HK:K]=[H:H\cap K]=\frac{|H|}{|H\cap K|}.$$

□

注 尽管 HK 不需要成为一个群，但是 HK/K 完全可以通过 $H/(H\cap K)$ 来明确地构造出来，它们的大小相等，这就完成了这个命题的证明。