

0.1 有限群

定义 0.1 (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 0.2 (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 0.1 (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. \square

命题 0.2

令 (G, \cdot) 是一个群, 任取 $x \in G$. 则

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

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) 就能立即得到结论. \square

定义 0.3 (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 0.3

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

证明 记

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

由命题 0.2 可知 f 是一个群同态. 注意到 $\text{im } f = \langle x \rangle$, 即 $\langle x \rangle$ 是 f 的同态像. 从而由命题??可知, $\langle x \rangle = \text{im } f < G$. \square

定义 0.4 (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 0.4

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 $x^{-1} \in \langle S \rangle$. \square

定义 0.5 (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**.

注 我们一般用 C_n 表示 n 阶循环群.

笔记 有限循环群与无限循环群示意图如下:

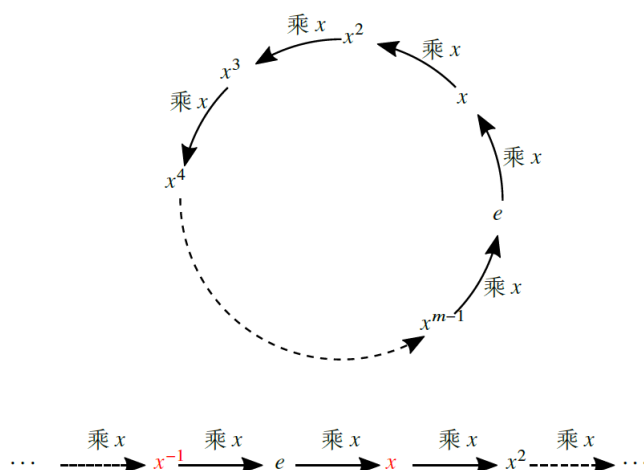


图 1: 有限循环群和无限循环群

命题 0.5

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 0.3 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 $H \supset \langle x \rangle$. \square

命题 0.6

设 $G = \langle x \rangle$ 是有限循环群, 并且 $|x| = n$, 则 $G = \{e, x, x^2, \dots, x^{n-1}\}$, 并且 $\{e, x, x^2, \dots, x^{n-1}\}$ 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 $q \in \mathbb{Z}$, $0 \leq r \leq n-1$, 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 $0 \leq m' < m \leq n-1$, 使得 $x^m = x^{m'}$, 则 $x^{m-m'} = e$ 。其中 $1 \leq m-m' \leq n-1 < n$, 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, $G = \{e, x, x^2, \dots, x^{n-1}\}$, 其中枚举法中的这些元素是两两不同的。 □

命题 0.7

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

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

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

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

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 0.8

设 $G = \langle x \rangle$ 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 0.9

所有的无限循环群是彼此同构的。进而所有的无限循环群 $\langle x \rangle (|x| = \infty)$ 都同构于整数加群 $(\mathbb{Z}, +)$ 。

◆

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

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

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

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

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。 \square

命题 0.10

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

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

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

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

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

命题 0.11

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 $\phi(n)$ 。 \clubsuit

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 0.10 可知, $\gcd(m, n) = \frac{n}{|x^m|} = 1$ 。

若 $\gcd(m, n) = 1$, 则由命题 0.10 可知, $|x^m| = \frac{n}{\gcd(n, m)} = n$ 。从而

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

又由命题 0.6 可知 $G = \{e, x, \dots, x^{n-1}\}$ 。于是

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

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

定义 0.6 (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)。 \clubsuit

定义 0.7 (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 $|H| = \infty$ 。 \clubsuit

定义 0.8 (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 0.1

令 G 是一个有限群, $H < G$ 是一个子群, $a \in G$. 令

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

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

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

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

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

故 g 是 f 的逆映射. 因此 f 是双射. □

命题 0.12

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 0.9 (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

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

商集 $H \backslash G$ 定义为

$$H \backslash G = \{Ha : a \in G\}.$$

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

$$[G : H] = |G/H|. \quad \clubsuit$$

定理 0.1

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

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

证明 一方面, 设 $x \in G$, 取 $a = x$, 则 $x = xe = ae \in xH$. 另一方面, 由命题 0.12 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**

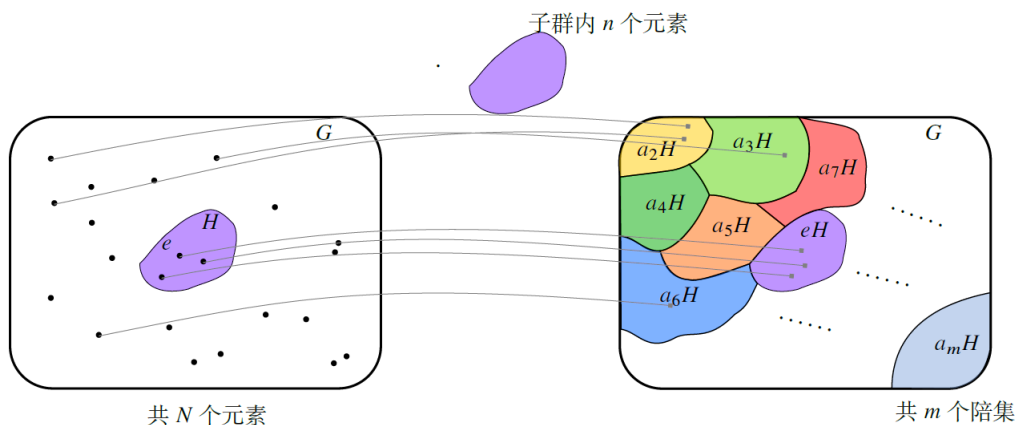


图 2: 左陪集示意图

定理 0.2 (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 $[G : H] = \frac{|G|}{|H|}$. 特别地,

$$|H| \mid |G|.$$



证明 由定理 0.1 可知 $G = \bigsqcup_{i=1}^{[G:H]} a_i H$, 从而

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

又由引理 0.1 可知 $|a_i H_i| = |H|$. 故

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

□

例题 0.1 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 0.2

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 $aHxb = aHyb$, 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 $hx = a^{-1}ahxb b^{-1} = a^{-1}ah'yb b^{-1} = h'y \in Hy$. 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 $xh = a^{-1}axhb b^{-1} = a^{-1}ah'yb b^{-1} = h'y \in Hy$. 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. \square


引理 0.3

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 0.12** 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 0.2** 可知 $xH = yH \iff y^{-1}xH = H \iff H = x^{-1}yH$, 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 $x = ye \in yH$. 从而 $xH \cap yH \neq \emptyset$. 于是由 **命题 0.12** 可知 $xH = yH$. 故 $xH = yH \iff x \in yH$. 同理可证 $xH = yH \iff y \in xH$. \square

推论 0.1

(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 0.2** 可知

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

又由引理 0.3 可知

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

故

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

(2) 由引理 0.3 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 0.3 可知 $a_1H = a_2H$.

□

命题 0.13

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 $I = \{1, 2, \dots, [G : H]\}$, $J = \{1, 2, \dots, [H : K]\}$. 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 0.1 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 0.1 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 0.1(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 0.2 可得

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

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 0.9 可知

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

□

定义 0.10 (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 0.14

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 $|HK| = \frac{|H||K|}{|H \cap K|}$ 。

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 0.3 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 0.3, 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

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

□

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。