抽象代数学不懂笔记

过于抽象

作者：杨毅涵
组织：南开大学数学科学学院
时间：October 13, 2024
邮箱：matyyh@163.com

游荡的孤高的灵魂不需要羁绊之地———— 比企谷八幡

目录

第 1 章 群

1.1 群同态

定理 1.1 (群同态基本定理)

设 $f: G \to G'$ 是群的满同态，则 $G/\mathrm{Ker}\, f \simeq G'$.

证明 为了方便书写，我们记 $N = \mathrm{Ker}\, f$.

首先我们定义映射 $\varphi: G/N \to G'$ 为

$$\varphi(gN) = f(g)$$

为了验证这确实是一个映射，我们只需要证明对于同一个陪集的不同的代表元 g, h，我们有 $f(g) = f(h)$，而这是因为若 g, h 属于同一个陪集，则有 $g^{-1}h \in N$，从而

$$e_{\in G'} = f(g^{-1}h) = f(g)^{-1}f(h)$$

所以有 $f(g) = f(h)$.

那么由 f 是满同态，容易证明 φ 是满射，进一步，为了证明同构，我们需要证明单射.

若 $\varphi(gN) = \varphi(hN)$，则 $f(g) = f(h)$，从而导致 $g^{-1}h \in N$，故 $gN = hN$，从而 φ 是单射，从而是双射.

最后，由 f 是同态，我们知道

$$\varphi(gN \cdot hN) = \varphi(ghN) = f(gh) = f(g)f(h) = \varphi(gN)\varphi(hN)$$

所以 φ 是同态，又因为 φ 是双射，所以 φ 是群同构，也即

$$G/N \simeq G'$$

□

笔记 如果 $f: G \to G'$ 不是满同态，我们可以取出 $\mathrm{Im}\, f$，从而自然地有 $f: G \to \mathrm{Im}\, f$ 是满同态，所以我们有

$$G/\mathrm{Ker}\, f \simeq \mathrm{Im}\, f$$

从中也可以发现“满同态”并不是一个本质的性质，我们很容易通过取出同态像把一个不是满的同态变成满的.

笔记 通过这个定理，我们在遇到一个从 G 到 H 的满同态时，可以在同构的意义下把 H 看做是 G 的一个商群，而这个同构关系的精细程度，取决于同态核的大小.

同样的，当遇到一个G 的一个商群 G/N 的时候，我们可以通过自然同态将 G/N 看做是同态像，从而我们知道要找出一个群 G 的所有同态像，就相当于找出 G 的所有商群，也就相当于找出 G 的所有正规子群.

笔记 令 π 是自然映射，从而我们有以下交换图，其中 $f = \varphi \circ \pi$.

$$\begin{tikzcd}
G \arrow[rr, bend left, "f"] \arrow[dr, "\pi"'] & & H \\
& G/\mathrm{Ker} f \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

命题 1.1

设群同态 $f: G \to H$，我们有

(1) 任取 $K < G$，有 $f(K) < H$.

(2) 任取 $L < H$，有 $f^{-1}(L) < G$，且 $\mathrm{Ker}\, f < f^{-1}(L)$.

命题 1.2

设群同态 $f: G \to H$，我们有

(1) 任取 $M \lhd H$，有 $f^{-1}(M) \lhd G$.

(2) 若 f 为满同态，任取 $K \lhd G$，有 $f(K) \lhd H$.

定理 1.2 (群的同态定理)

设 f 是群 G 到群 G' 的满同态，令 $N = \mathrm{Ker}\, f$，则

(1) f 建立了 G 中包含 N 的子群与 G' 中子群之间的双射.

(2) f 建立了 G 中包含 N 的正规子群与 G' 中正规子群之间的双射.

(3) 如果 $H \lhd G, N \subseteq H$，则有 $G/H \simeq G'/f(H)$.

证明 (1) 首先，对 G 中任意包含 N 的子群 K，我们有 $f(K) < G'$，从而我们得到了一个从G 中任意包含 N 的子群到 G' 中子群的映射

$$K \longmapsto f(K)$$

下面我们证明这是双射：对于任何 G' 的子群 H，由命题 1.1 我们知道 $f^{-1}(H) < G$ 且包含 N，并且有 $f(f^{-1}(H)) = H$，从而这是满射.

此外若 H_1, H_2 是 G 中两个包含 N 的子群且 $f(H_1) = f(H_2)$，我们知道对任意的 $h_1 \in H_1$，存在 $h_2 \in H_2$ 使得 $f(h_1) = f(h_2)$，也即 $h_1 h_2^{-1} \in N \subseteq H_2$，故我们知道 $h_1 = h_1 h_2^{-1} h_2 \in H_2$，从而 $H_1 \subseteq H_2$，同理有 $H_2 \subseteq H_1$，故 $H_1 = H_2$，故单射，故双射.

(2) 设 H 为 G 中任一包含 N 的正规子群，对任意 $h' = f(h) \in f(H), g' = f(g) \in G'$，我们有 $ghg^{-1} \in H$，从而

$$g'h'g'^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}) \in f(H)$$

故 $f(H)$ 为 G' 的正规子群.

反之若 $f(H)$ 是 G' 的正规子群，则知道 $f(gHg^{-1}) = f(H)$，因为 $N \subseteq H, N \subseteq gHg^{-1}$，又由于 (1) 中证明了单射，从而 $gHg^{-1} = H$，故 H 是 G 的正规子群.

(3) 令 π 是 G' 关于 $f(H)$ 的自然映射，考虑如下交换图

$$\begin{tikzcd} G \arrow[rr, bend left, "\pi\circ f"] \arrow[dr, "f"'] & & G'/f(H) \\ & G' \arrow[ur, "\pi"'] & \end{tikzcd}$$

我们考虑 $\mathrm{Ker}\,(\pi\circ f)$，有

$$\mathrm{Ker}\,(\pi\circ f)=f^{-1}(\mathrm{Ker}\,\pi)=f^{-1}(\pi^{-1}(e_{\in G'}f(H)))=f^{-1}(f(H))=H$$

从而由群同态基本定理，我们有

$$G/H=G/\mathrm{Ker}\,(\pi\circ f)=G'/f(H)$$

□

笔记 (3) 中的证明方法我们将经常用到：通常为了证明一个商群 G/N 与某个群 H 同构，我们经常构造 G 到 H 的满同态，然后证明这个同态的核是 N，利用群同态基本定理就可以得到这个同构.

推论 1.1

设 G 是群，$N\lhd G$，有自然同态

$$\pi: G\to G/N$$

(1) π 建立了 G 中包含 N 的子群与 G/N 的子群之间的双射.

(2) π 建立了 G 中包含 N 的正规子群与 G/N 的正规子群之间的双射.

(3) 若 $N\subseteq H, H\lhd G$，则 $G/H\simeq(G/N)/(H/N)$.

笔记 由于同态像就可以看做是商群，所以用商群和自然同态的语言在叙述上不失一般性.

定理 1.3

设 G 是群，$N\lhd G$，$\pi: G\to G/N$ 是自然同态，对于 $H<G$，我们有

(1) HN 是 G 中包含 N 的子群.

(2) $HN=\pi^{-1}(\pi(H))$.

(3) $(H\cap N)\lhd H$，且 $\mathrm{Ker}\,(\pi|_H)=H\cap N$.

(4) $HN/N\simeq H/(H\cap N)$

证明 (1) 由于 $N=eN\subseteq HN$，显然.

(2) 我们有

$$\begin{aligned}\pi(HN) &= \{hnN|h\in H, n\in N\}\\ &= \{hN|h\in H\}\\ &= \pi(H)\end{aligned}$$

从而我们知道 $HN\subseteq\pi^{-1}(\pi(H))$，另一方面，我们任取 $a\in\pi^{-1}(\pi(H))$，存在 $b\in H$ 使得

$\pi(a)=\pi(b)$，所以

$$\pi(b^{-1}a)=\pi(b)^{-1}\pi(a)=e_{\in G/N}$$

故 $b^{-1}a\in N$，所以我们有

$$a=bb^{-1}a=b(b^{-1}a)\in HN$$

故 $\pi^{-1}(\pi(H))\subseteq HN$，从而 $HN=\pi^{-1}(\pi(H))$.

(3) 显然有 $(H\cap N)<H$，又对于任意 $h\in H,n\in H\cap N$，因为 $N\lhd G$，有 $hnh^{-1}\in N$，又 $n\in H\cap N$，故存在 $h_0\in H$ 使得 $n=h_0$，从而 $hnh^{-1}=hh_0h^{-1}\in H$，故 $hnh^{-1}\in H\cap N$，从而得证 $H\cap N$ 是 H 的正规子群.

又因为 $\operatorname{Ker}(\pi|_H)\subseteq\operatorname{Ker}\pi=N$，$\operatorname{Ker}(\pi|_H)\subseteq H$，从而 $\operatorname{Ker}(\pi|_H)\subseteq H\cap N$，另一方面，我们任取 $n\in H\cap N$，有 $\pi|_H(n)=N=e_{\in G/N}$，从而 $H\cap N\subseteq\operatorname{Ker}(\pi|_H)$，故有

$$\operatorname{Ker}(\pi|_H)=H\cap N$$

(4) 我们已知 $\pi(H)=\pi(HN)=HN/N$，所以有满同态：

$$\pi|_H:H\to HN/N$$

所以由同态基本定理我们知道

$$H/\operatorname{Ker}(\pi|_H)\simeq HN/N$$

又知道 $\operatorname{Ker}(\pi|_H)=H\cap N$，从而我们知道

$$H/(H\cap N)\simeq HN/N$$

$\square$

笔记 这个定理的另一个形式可以写成：设 G 和 H 为两个群，存在群同态 $\varphi:G\to H$，任取 $K<G$，有

(1) $\varphi(K)=\varphi(K\operatorname{Ker}\varphi)$.

(2) $K\operatorname{Ker}\varphi=\varphi^{-1}(\varphi(K))$.

笔记 这个定理还有一个名字叫做钻石定理，因为可以将涉及的群的关系表为如下形式：

$$\begin{tikzcd}
 & HN & \\
H \arrow[ur] & & N \arrow[ul, "\triangleright" description] \\
 & H\cap N \arrow[ul, "\triangleright" description] \arrow[ur] &
\end{tikzcd}$$

1.2 循环群

定理 1.4

循环群的任一子群必是循环群.

证明 设 $G_1 < G = \langle a \rangle$，令 $k = \min\{m \in \mathbb{N} | a^m \in G_1\}$，我们下面证明 $G_1 = \langle a^k \rangle$.

显然有 $\langle a^k \rangle \subseteq G_1$，另一方面，对任意的 $a^m \in G_1$，要证 $a^m \in \langle a^k \rangle$，只要证明 $k \mid m$，做带余除法，我们假设 $m = qk + r$，其中 $0 \leq r \leq k-1$，则我们知道

$$a^r = a^{m-qk} = a^m \cdot (a^k)^{-q} \in G_1$$

从而我们知道若 $r \neq 0$，则与 k 的取法的最小性矛盾，从而我们知道 $r = 0$ 也即 $k \mid m$，从而 $G_1 \subseteq \langle a^k \rangle$，所以我们知道

$$G_1 = \langle a^k \rangle < \langle a \rangle = G$$

□

推论 1.2

$\{\mathbb{Z};+\}$ 的子群必然形如 $m\mathbb{Z}(m \in \mathbb{N})$

定理 1.5

设群 $G = \langle a \rangle$，若群 G 是无限阶的，则 G 与 $\{\mathbb{Z};+\}$ 同构；若 G 是有限阶的，则 G 与 $\{Z_m;+\}$ 同构.

证明 令

$$\begin{aligned} \varphi : \{Z;+\} &\longrightarrow G \\ n &\longmapsto a^n \end{aligned}$$

对 $\forall n_1, n_2 \in \{\mathbb{Z};+\}$，有

$$\varphi(n_1+n_2) = a^{n_1+n_2} = a^{n_1} \cdot a^{n_2} = \varphi(n_1)\varphi(n_2)$$

于是 φ 是同态，且容易验证为满同态，根据同态基本定理有

$$\{\mathbb{Z};+\}/\operatorname{Ker}\varphi \simeq G$$

其中

$$\operatorname{Ker}\varphi = \begin{cases} \{0\} & \Longrightarrow \{\mathbb{Z};+\} \simeq G \\ m\mathbb{Z} & \Longrightarrow \{\mathbb{Z}_m;+\} \simeq G \end{cases}$$

□

推论 1.3

两个循环群同构 $\Longleftrightarrow$ 它们有相同的阶.

定理 1.6

设 G 是 m 阶循环群，m_1 是 m 的一个正整数因子，则存在唯一的 $G_1 < G$ 使得 $|G_1| = m_1$.

证明 不妨设 $G = \{\mathbb{Z}_m; +\} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$，则

$$\langle\overline{\frac{m}{m_1}}\rangle = \{\overline{0}, \overline{\frac{m}{m_1}}, \overline{2\frac{m}{m_1}}, \cdots, \overline{(m_1-1)\frac{m}{m_1}}\}$$

是 G 的 m_1 阶子群，则存在性得证.

下面证明唯一性：若 H 是 G 的 m_1 阶子群，设 $H = \langle\overline{h}\rangle = \{\overline{0}, \overline{h}, \overline{2h}, \cdots, \overline{(m_1-1)h}\}$，且我们有

$$\overline{m_1 h} = \overline{0}$$

从而我们知道 $m \mid m_1 h$，也即存在 $k \in \mathbb{N}$ 使得 $m_1 h = km$，从而 $h = k\dfrac{m}{m_1}$.

若 $\gcd(k, m_1) = d > 1$，则我们知道存在 $i \neq j, 0 \leq i, j \leq m_1 - 1$，使得

$$\frac{m_1}{d} \mid i - j$$

从而有 $\overline{ih - jh} = \overline{(i-j)\dfrac{k}{d}\dfrac{m}{\frac{m_1}{d}}} = \overline{\dfrac{i-j}{\frac{m_1}{d}}\dfrac{k}{d}m} = \overline{0}$，从而导致 $\overline{ih} = \overline{jh}$，与 H 的阶为 m_1 矛盾，从而我们知道 $\gcd(k, m_1) = 1$，从而对任意 $0 \leq i \neq j \leq m_1 - 1$，有

$$\frac{(i-j)k}{m_1} \notin \mathbb{Z}$$

从而 $\overline{ih} \neq \overline{jh}$，有 H 的阶为 m_1，又因为对于任意的 i，存在 j 使得 $kj \equiv i (\mathrm{mod} m_1)$，从而有

$$\overline{jh} = \overline{kj\frac{m}{m_1}} = \overline{(lm_1 + i)\frac{m}{m_1}} = \overline{i\frac{m}{m_1}}$$

所以我们知道 $H = \langle\overline{h}\rangle = \langle\overline{\dfrac{m}{m_1}}\rangle$，唯一性得证. □

笔记 m 阶循环群的生成元的阶也是 m.

笔记 由此我们会考虑这样一个性质是否描述了循环群的本质，也就是如果一个阶为 m 的群，对 m 的每个正整数因子 m_1，都存在 G 的唯一的一个 m_1 阶子群，则 G 是循环群，也即上面的定理实际上是循环群的充分必要条件.

定理 1.7

$|G| = m$，则

$$G\text{是循环群} \iff \text{对}m\text{的每个正整数因子}m_1\text{，都存在}G\text{的唯一的一个}m_1\text{阶子群}$$

命题 1.3

有限群 G 的任一元 a 的阶也是有限的，且是 $|G|$ 的因子.

证明 设 a 的阶为 m，则

$$\langle a\rangle = \{a^0, a^1, \cdots, a^{m-1}\} < G$$

从而根据 Lagrange 定理得证. □

例 1.1 若 G 是循环群，$N \lhd G$，证明 G/N 也是循环群.

证明 设 $G = \langle a \rangle$，则我们断言有

$$G/N = \langle aN \rangle$$

这是因为对 $\forall b \in G,\ b = a^m$，则我们有 $bN = a^m N = (aN)^m$，从而得证. □

笔记 想证明一个群是循环群，实际上就是去寻找生成元.

1.3 变换群与置换群

定义 1.1

A 的全体可逆变换在复合运算下构成的群称之为 **A 的全变换群**，记为 $\{S_A; \cdot\}$，S_A 的子群称之为**变换群**.

$|A| = n$ 时，S_n 的子群称之为**置换群**. ♣

定理 1.8 (Caylay 定理)

任何一个群都与一个变换群(对称群 S_G 的子群)同构. ♡

证明 设 G 是一个群，$\forall a \in G$，令 $\varphi_a : G \longrightarrow G$，$\varphi_a(g) = ag, \forall g \in G$，容易证明 φ 单射且满射，从而我们知道 $\varphi_a \in S_G$.

令 $T = \{\varphi_a \mid a \in G\} \subseteq S_G$，由于

$$\varphi_a \cdot (\varphi_b)^{-1} = \varphi_a \varphi_{b^{-1}} = \varphi_{ab^{-1}} \in T$$

从而我们知道 $T < S_G$，再令 $f : G \longrightarrow T$，$f(a) = \varphi_a, \forall a \in G$，我们有

$$f(ab) = \varphi_{ab} = \varphi_a \varphi_b = f(a)f(b)$$

从而 f 是群同态，又容易证明 f 单射且满射，从而 f 是群同构，所以有 $G \simeq T < S_G$. □

推论 1.4

任一有限群都与一个置换群同构. ♡

命题 1.4

S_n 中两个不相交的轮换是可交换的. ♠

定理 1.9

S_n 中的任何元素 σ 都可以表为 S_n 中一些不相交的轮换的乘积，且在不计次序的情况下表法唯一. ♡

证明 任取 $a \in \{1, 2, \cdots, n\}$，考虑

$$a (= \sigma^0(a)), \sigma^1(a), \sigma^2(a), \cdots$$

不妨设第一次与前面元素有重复的为 $\sigma^m(a)$，且设于 $\sigma^k(a)$ 重复，下面说明 $k=0$，若不然，则

$$\sigma^{m-1}(a)=\sigma^{-1}(\sigma^m(a))=\sigma^{-1}(\sigma^k(a))=\sigma^{k-1}(a)$$

与 m 的取法矛盾，从而知道 $k=0$.

我们知道 $\sigma_1=(a,\sigma(a),\cdots,\sigma^{m-1}(a))$ 在 $\{a,\sigma(a),\cdots,\sigma^{m-1}(a)\}$ 上作用于 σ 相同.

再取 $b\in\{1,2,\cdots,n\}-\{a,\sigma(a),\cdots,\sigma^{m-1}(a)\}$，按照上面的方法再作轮换

$$\sigma_2=(b,\sigma(b),\cdots,\sigma^{l-1}(b))$$

则 σ 与 σ_2 在 $\{b,\sigma(b),\cdots,\sigma^{l-1}(b)\}$ 作用相同，且由于 σ 是单射，知道 σ_1 与 σ_2 不相交，继续这样下去，我们知道必在有限次后将 $\{1,2,\cdots,n\}$ 用完，从而得到有限个不相交的轮换 $\sigma_1,\sigma_2,\cdots,\sigma_s$ 使得

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s$$

注意任一文字所在的轮换是唯一的，所以如果不计次序，表法唯一. □

命题 1.5

任一置换都可以表示为对换的乘积，且对换个数的奇偶性是不变的. ♠

证明 设 V 是数域 $\mathbb{P}$ 上的 n 维线性空间，$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$ 为其一组基，对任意 $\sigma\in S_n$，定义 V 上的线性变换 π_σ 满足

$$\pi_\sigma(\varepsilon_i)=\varepsilon_{\sigma_i}$$

这样我们得到一个映射：

$$\pi:S_n\longrightarrow \mathrm{GL}(V),\quad \sigma\mapsto\pi_\sigma$$

容易验证这是一个单同态，再对取行列式的映射复合得到群同态：

$$\det\circ\pi:S_n\longrightarrow\mathbb{P}^*,\quad \sigma\mapsto\det(\pi_\sigma)$$

我们知道在映射 $\det\circ\pi$ 之下任何对换的像为 -1，故我们知道当一个 n 元置换表位对换乘积的时候，对换个数的奇偶性不变. □

定义 1.2

上面群同态 $\det\circ\pi$ 的核 A_n 为全体偶置换构成的群，也被称为 n **元交错群**. ♣

命题 1.6

关于交错群，我们有以下性质：

1. 当 $n\geq 2$ 时，有 $|A_n|=\dfrac{n!}{2}$
2. $A_n\lhd S_n$

♠

一些交错群 容易看出 A_1,A_2 是平凡群，A_3 是 3 阶循环群，而 A_4 是 12 阶群，可以验证

$$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}\simeq\text{Klein Group}$$

是 A_4 的正规子群，实际上这也是唯一的非平凡正规子群.

定理 1.10

当 $n \geq 5$ 时，A_n 是单群.

1.4 群作用

定义 1.3

设群 G 在非空集合 X 上有一个**作用**，任取 $x \in X$，我们记

$$G.x := \{a.x \in X \mid a \in G\}$$

并称该集合为 x 在 G 作用下的轨道，也称之为过 x 的 **G-轨道**.

命题 1.7

设群 G 在非空集合 X 上有一个作用，任取 $x, y \in X$，以下两个叙述等价：

(1) x 和 y 属于同一个 G-轨道.

(2) $G.x = G.y$.

推论 1.5

设群 G 在非空集合 X 上有一个作用，则任取 $x, y \in X$，有

- 或者 $G.x = G.y$.
- 或者 $G.x \cap G.y = \emptyset$.

定义 1.4

G 在 X 上作用，任取 $x \in X$，考虑集合

$$G_x = \{a \in G \mid a.x = x\}$$

我们称 G_x 为 x 的**稳定化子(迷向子群)**. 如果有 $G_x = G$，我们称 x 为 G-作用的**不动点**，我们记所有不动点的集合为：

$$\mathrm{Fix}(G) := \{x \in X \mid G_x = G\}$$

命题 1.8

设群 G 作用在非空集合 X 上，任取 $x \in X$，对任意 $y \in G.x$，存在 $a \in G$，满足

$$G_y = aG_x a^{-1}$$

命题 1.9

设群 G 作用在非空集合 X 上，任取 $x \in X$，任取 $a \in G$，记 $y = a.x$，则

$$G_{x,y} = aG_x$$

推论 1.6

沿用上面记号，存在双射：

$$\begin{aligned}\Phi\colon G.x &\to \{aG_x \mid a \in G\}\\ a.x &\mapsto aG_x\end{aligned}$$

定义 1.5

设群 G 分别作用在非空集合 X 和非空集合 Y 上，设存在双射

$$f\colon X \to Y$$

满足任取 $x \in X$，$a \in G$，有

$$a.f(x) = f(a.x)$$

那么我们称 G 在 X 上的作用和在 Y 上作用等价.

注 即下面的交换图对任何 $a \in G$ 都成立：

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "a"'] & Y \arrow[d, "a"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

我们考虑 G 在轨道 $Y = G.x \subset X$ 上的作用.

命题 1.10

设存在群 G 作用在非空集合 X 上，任取 $x \in X$，则 G 在 G/G_x 上的作用与 G 在 $G.x$ 上的作用等价.

证明 考虑上面提到的双射 $\Phi : G/G_x \to G.x$，则我们有

$$a.\Phi(hG_x) = a.h.x = (ah).x = \Phi(ahG_x) = \Phi(a.hG_x)$$

□

注 即如下交换图：

$$\begin{tikzcd} G/G_x \arrow[r, "\Phi"] \arrow[d, "a"'] & G.x \arrow[d, "a"] \\ G/G_x \arrow[r, "\Phi"'] & G.x \end{tikzcd}$$

注 如果群 G 在 X 上有一个作用，则这个作用可以诱导一个 G 在一些 G-轨道的并集上的作用.

定义 1.6
我们记下面的集合为所有 G-轨道的空间.

$$X/G := \{G.x \mid x \in X\}$$

♣

由于 $G.x$ 与 G/G_x 之间存在双射，从而我们有下面这个关于轨道大小的公式.

推论 1.7
沿用上面记号，我们有

$$|G.x| = |G/G_x| = [G:G_x] = \frac{|G|}{|G_x|}$$

♡

再考虑 X 关于 G-轨道的分解，我们可以进一步描述 X 的大小.

推论 1.8
我们有

$$|X| = \sum_{G.x\in X/G} |G.x| = \sum_{G.x\in X/G} \frac{|G|}{|G_x|}$$

♡

注 由于 G-作用的不动点通常会包含特殊信息，我们也会将上式写为

$$|X| = |\mathrm{Fix}(G)| + \sum_{G.x\in X/G, |G.x|>1} \frac{|G|}{|G_x|}$$

推论 1.9
设群 G 作用在非空集合 X 上，若存在素数 p，使得 $|G| = p^l$，其中 l 为非零自然数，则

$$|X| \equiv |\mathrm{Fix}(G)| \mod p$$

♡

证明 对于 G_x，若存在 $|G_x| = |G|$，即 $x \in \mathrm{Fix}(G)$，也即 $|G.x| = 1$，故如对于任何满足 $|G.x| > 1$ 的 x，有 $p \mid \frac{|G|}{|G_x|}$，所以我们有

$$|X| = |\mathrm{Fix}(G)| + \sum_{G.x\in X/G, |G.x|>1} \frac{|G|}{|G_x|} \equiv |\mathrm{Fix}(G)| \mod p$$

□

定义 1.7
设群 G 作用在非空集合 X 上. 任取 $a \in G$，若对 $x \in X$，有 $a.x = x$，我们称 x 为 a 的一个不动点. 我们记 a 的不动点集为

$$X^a := \{x \in X \mid a.x = x\}$$

♣

定理 1.11 (Burnside 引理)

设有限群 G 作用在一个有限非空集合 X 上，则

$$|X/G| = \frac{1}{|G|}\sum_{a\in G}|X^a|$$

证明 我们考虑 $G\times X$ 的子集：

$$D = \{(a,x)\in G\times X \mid a.x = x\}$$

则有

$$\sum_{a\in G}|X^a| = |D|$$

另一方面，也有

$$\sum_{x\in X}|G_x| = |D|$$

任取 $x\in X$，我们可以将 G 分解为一些子集的不交并：

$$G = \bigcup_{y\in G.x}\{a\in G \mid a.x = y\}$$

这个实际上就是 G 关于 G_x 的左陪集分解，轨道 $G.x$ 中每个元素对应一个 G_x 的左陪集. 注意到任取 $a\in G$，我们有

$$|G_x| = |aG_x|$$

因此

$$|G_x| = \frac{|G|}{|G.x|}$$

综合以上信息，我们有

$$\sum_{a\in G}|X^a| = |D| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G.x|} = |G|\sum_{G.x\in X/G}\sum_{y\in G.x}\frac{1}{|G.x|} = |G|\sum_{G.x\in X/G}1$$

因此，我们有

$$|X/G| = \frac{1}{|G|}\sum_{a\in G}|X^a|$$

□

1.5 群在自身上的共轭作用

定义 1.8

我们可以定义共轭作用，任取群 G，任取 $a\in G$，我们可以定义以下映射：

$$\begin{aligned}\mathrm{Ad}_a\colon G &\to G\\ b &\mapsto aba^{-1}\end{aligned}$$

注意到共轭作用不仅仅是双射，而且是 G 的群同构. 从而我们得到 G 到 $\mathrm{Aut}(G)$ 的同态映射：

$$\begin{aligned} \mathrm{Ad}\colon G &\to \mathrm{Aut}(G) \\ a &\mapsto \mathrm{Ad}_a \end{aligned}$$

所以我们有 $\mathrm{Inn}(G) := \{\mathrm{Ad}_a \mid a \in G\} = \mathrm{Ad}(G)$.

任取 $a \in \mathrm{Ker\,Ad}$，我们有 $\mathrm{Ad}_a = \mathrm{id} \in \mathrm{Aut}(G)$，即任取 $b \in G$，有

$$aba^{-1} = \mathrm{Ad}_a(b) = \mathrm{id}(b) = b$$

因此等价的，我们任取 $b \in G$，有

$$ab = ba$$

故我们知道

$$a \in Z(G) := \{c \in G \mid \forall b \in G, cb = bc\}$$

另一方面，任取 $a \in Z(G)$，我们考虑伴随作用的定义可以直接验证，任取 $b \in G$，

$$\mathrm{Ad}_a(b) = aba^{-1} = baa^{-1} = b$$

因此，$a \in \mathrm{Ker\,Ad}$，故实际上给出了以下结论：

命题 1.11

任给群 G，我们有 $\mathrm{Ker\,Ad} = Z(G)$.

命题 1.12

设 G 为一个群，以下关系给出 G 上元素的等价关系：

- 任取 $a, b \in G$，我们定义 $a \sim b$ 当且仅当 a 和 b 共轭.

证明 逐条验证性质即可. □

定义 1.9

设 G 为一个群，任取 $a \in G$，我们称以下集合为 a 的**共轭类**.

$$[a] := \{b \in G \mid a \sim b\}$$

命题 1.13

考虑群 G 在 G 上的共轭作用，任取 $a \in G$，则 a 的轨道为 a 的共轭类:

$$G.a = \mathrm{Ad}(G)(a) = [a]$$

命题 1.14

考虑群 G 在 G 上的共轭作用，任取 $a, b \in G$，以下两个叙述等价：

(1) $ab = ba$.

(2) $b \in G_a$.

定义 1.10

设 G 为一个群，任取 $a \in G$，集合

$$Z_G(a) := \{b \in G \mid ab = ba\}$$

为 a 在 G 的**中心化子(centralizer)**.

笔记 容易证明 $Z_G(a)$ 为 G 的一个子群.

推论 1.10

考虑 G 在 G 上的共轭作用，任取 $a \in G$，则 a 的稳定子群和 a 在 G 的中心化子相同：

$$G_a = Z_G(a)$$

考虑到 $|G.a| = |G/G_a|$，我们有下面的结论：

命题 1.15

设 G 为一个有限群，任取 $a \in G$，我们有

$$|[a]| = [G\colon Z_G(a)]$$

定义 1.11

设 G 为一个群，任取 G 的非空子集 S，我们称以下集合为

$$Z_G(S) := \{b \in G \mid \forall a \in S, ab = ba\}$$

集合 S 在 G 中的**中心化子**.

命题 1.16

设 G 为一个群，任取 G 的非空子集 S，则 S 的中心化子 $Z_G(S)$ 为 G 的一个子群.

定义 1.12

设 G 为一个群，任取 G 的一个非空子集 S，我们称集合

$$N_G(S) := \{a \in G \mid \mathrm{Ad}_a(S) = S\}$$

为 S 的**正规化子**.

注 从定义我们看出来，如果 G 在 G 上面的作用是由共轭给出的，则有 $N_G(S) = G_S$.

命题 1.17

设 G 为群，任取 G 的子群 H，我们有 $H \lhd N_G(H)$.

定义 1.13

我们记 G 中所有共轭类的集合为：

$$[G] := \{[a] \mid a \in G\}$$

定理 1.12 (类方程)

设 G 是一个有限群，记 $Z(G)$ 为 G 的中心，我们有

$$|G| = |Z(G)| + \sum_{[a]\in[G],|[a]|>1} [G\colon N_G(a)]$$

注 注意到求和第二部分中的每一项 $N_G(a)$ 的选取是依赖于共轭类 $[a]$ 中代表元 a 的选取，如果我们选择另一个代表元 $b \in [a]$，因此有 $c \in G$，使得

$$b = cac^{-1}$$

因此 $N_G(b) = cN_G(a)c^{-1}$，因此我们有

$$[G\colon N_G(a)] = [G\colon N_G(b)]$$

因此这个数值不依赖与代表元的选取.

推论 1.11

设 G 为一个阶为 p^l 的群，其中 p 为素数，l 为非零自然数，则 G 的中心非平凡，即

$$Z(G) \neq \{e\}$$

证明 由类方程：

$$|G| = |Z(G)| + \sum_{[a]\in[G],|[a]|>1} [G\colon N_G(a)]$$

我们注意到 $p \mid |G|$，且对任意 $|[a]| > 1$，我们有 $p \mid [G\colon N_G(a)]$，因此

$$p \mid |Z(G)|$$

由于 $e \in Z(G)$，从而我们知道 $|Z(G)| = kp$，其中 k 为非零自然数. □

推论 1.12

设 G 为一个阶为 p^2 的群，其中 p 为素数，则 G 为交换群.

证明 由 Cor 1.11 知 $Z_G \neq \{e\}$，由于 $Z(G)$ 为 G 的子群，因此 $|Z(G)| = p$ 或 p^2.

若 $|Z(G)| = p^2$，则 G 为交换群.

若 $|Z(G)| = p$，我们知道 $Z(G)$ 为 p 阶循环群，设 $a \in Z(G)$ 为 $Z(G)$ 的生成元，注意到 $Z(G) \lhd G$，我们有商群

$$G/Z(G)$$

由于

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = p$$

我们知道 $G/Z(G)$ 是 p 阶循环群，设 $b \in G$ 满足 $bZ(G)$ 为 $G/Z(G)$ 的生成元，考虑 G 关于 $Z(G)$ 的左陪集分解，我们有

$$G = \bigcup_{i=0}^{p-1} b^i Z(G)$$

因此 G 中所有元素都可以写成 b^ia^j 的形式，其中 $i,j\in\mathbb{Z}$.

任取 b^ia^j 与 b^sa^t，我们考虑

$$(b^ia^j)(b^sa^t)=b^i(a^jb^s)a^t=b^{i+s}a^{j+s}=b^s(b^ia^t)a^j=(b^sa^t)(b^ia^j)$$

因此 G 是交换群，即 $G=Z(G)$，这与 $|Z(G)|=p$ 矛盾，因此 $|Z(G)=p^2|$，即 G 为交换群. □

注 事实上，若 G 的阶为 p^2，其中 p 为素数，则

$$G\cong\mathbb{Z}_{p^2}\quad \text{或者}\quad \mathbb{Z}_p\times\mathbb{Z}_p$$

1.6 Sylow 定理

定理 1.13 (Cauchy 定理)

设 $|G|=n$，任取素数 $p\mid n$，我们可以在 G 中找到一个 p 阶子群.

证明 我们考虑以下集合

$$X=\left\{(a_1,\cdots,a_p)\in\underbrace{G\times\cdots\times G}_{p\text{ times}}\mid a_1\cdots a_p=e\in G\right\}$$

我们注意到对称群 S_p 中的 p 轮换 $\sigma=(12\cdots p)$ 生成的子群

$$H=\langle\sigma\rangle$$

可以作用在 X 上，有

$$f\colon H\times X\to X,\quad \left(\sigma^k,(a_1,\cdots,a_p)\right)\mapsto\left(a_{\sigma^k(1)},\cdots,a_{\sigma^k(p)}\right)$$

我们有

$$|X|=|\mathrm{Fix}(H)|+\sum_{H.x\in X/H,|H.x|>1}\frac{|H|}{|H_x|}$$

注意到对于右式第二部分 $|H|=p$，由于 $H_x<H,H_x\neq H$，因此我们有 $H_x=\{e\}$，即

$$|X|=|\mathrm{Fix}(H)|+\sum_{H.x\in X/H,|H.x|>1}p$$

另一方面，我们知道只要取定 X 中的前 $p-1$ 个分量，第 n 个分量被唯一确定，故

$$|X|=|G|^{p-1}$$

所以我们有

$$p\mid|\mathrm{Fix}(H)|$$

再研究 $\mathrm{Fix}(H)$ 中的元素，我们有对于任意 k，有

$$(a_1,\cdots,a_p)=\left(a_{\sigma^k(1)},\cdots,a_{\sigma^k(p)}\right)$$

也就是存在 $a\in G$，使得 $a_1=\cdots=a_p=a$，即 $a^p=e$，由于 $|\mathrm{Fix}(H)|>1$，知道存在

$a \neq e$，使得 $a^p = e$，则我们知道 p 阶子群

$$\langle a \rangle < G$$

□

定理 1.14 (Sylow 第一定理)

$|G| = p^\ell m$，其中 p 为素数，满足 $(p, m) = 1$，则任取 $0 \leq k \leq l$，G 中有 p^k 阶子群.

证明 我们使用归纳法对 $|G|$ 的阶数进行归纳：设 G 的阶为 $n = p^l m$，其中 $l \in \mathbb{N}$，p, m 为非零自然数，p 是素数，$(p, m) = 1$，则任取 $0 \leq k \leq l$，G 中有 p^k 阶子群.

(1) $|G| = 1$，显然.

(2) 下面假设结论对 $1 \leq |G| < n$ 都成立，我们考虑 $|G| = n$ 的情形. 若 $l = 0$，显然，下面设 $l \geq k > 0$，我们按照 $|Z(G)|$ 是否可以被 p 整除来分类：

(i) 若 $p \mid |Z(G)|$，由 Cauchy 定理，知 $Z(G)$ 有一个 p 阶子群 P，由于 $P < Z(G)$，则我们有 $P \lhd G$，考虑 G/P，这是一个阶小于 G 的群，由归纳假设我们知道结论对于 G/P 成立，记 $\overline{H}$ 为 G/P 的一个 p^{k-1} 阶子群，令 π 为自然同态

$$\pi \colon G \to G/P$$

我们考虑 $H < G$，满足

$$H = \pi^{-1}(\overline{H})$$

因此 $P < H$，且 $H/P = \overline{H}$，因此我们有

$$|H| = [H \colon P]|P| = p^k$$

结论成立.

(ii) 如果 $p \nmid |Z(G)|$，我们考虑

$$|G| = |Z(G)| + \sum_{[a] \in [G], |[a]| > 1} [G \colon N_G(a)]$$

由于 $p \mid G$ 且 $p \nmid |Z(G)|$，因此存在 $[a] \in [G]$，满足 $|[a]| > 1$ 且

$$p \nmid [G \colon N_G(a)] = \frac{|G|}{|N_G(a)|}$$

因此 $p^l \mid |N_G(a)|$，由归纳假设我们知道存在 $N_G(a)$ 的 p^k 阶子群，从而存在 G 的 p^k 阶子群.

(3) 由归纳原理知道成立.

□

定义 1.14

G 为一个群，设 G 的阶为 $n = p^l m$，其中 p 为素数，满足 $(p, m) = 1$，则

- 若 $\{e\} \neq H < G$，满足 $|H| = p^k$，则称 H 为 G 的一个 **p-子群**.
- 若 $\{e\} \neq H < G$，满足 $|H| = p^l$，则称 H 为 G 的一个 **Sylow p-子群**.

注 Sylow 第一定理保证了上面定义的子群总是存在的.

引理 1.1

设 G 为一个群，设 G 的阶为 $n = p^l m$，其中 p 为素数，满足 $(p, m) = 1$，设 P 是 G 的一个 Sylow p-子群. 任取 $a \in G$，如果 $o(a) \mid p^l$，且 $aPa^{-1} = p$，则 $a \in P$.

证明 设 $a \in G$，满足 $o(a) \mid p^l$，我们记 $H = \langle a \rangle$，若 $aPa^{-1} = P$，我们考虑 a 和 P 生成的子群 K，注意到

$$K = \left\{a^j b \mid j \in \mathbb{Z}, b \in P\right\} = HP$$

于是我们知道

$$|K| = |HP| = \frac{|H||P|}{|H \cap P|} = p^l \frac{|H|}{|H \cap P|}$$

由于 $|H| \mid p^l$，所以我们知道如果 $H \neq H \cap P$，则

$$p^{l+1} \mid |K| \mid |G|$$

与 $v_p(|G|) = l$ 矛盾，因此 $H = H \cap P$，即 $H \subset P$，即 $a \in P$. □

引理 1.2

设 G 为一个群，设 G 的阶为 $n = p^l m$，其中 p 为素数，满足 $(p, m) = 1$，设 P 是 G 的一个 Sylow p-子群，H 为 G 的一个 p-子群，则有

$$H \cap P = H \cap N_G(P) (=: N_H(P))$$

证明 注意到 $P < N_G(P)$，因此我们有

$$H \cap P \subset H \cap N_G(P)$$

下面我们证明另一个方向的包含关系，任取 $a \in H$，由于 H 为 p-子群，则 $o(a) \mid |H| \mid p^l$，因此若 $a \in N_G(P)$，则由前面的引理我们知道 $a \in P$，因此我们有

$$H \cap N_G(P) \subset H \cap P$$

综上我们有

$$H \cap N_G(P) = H \cap P$$

□

定理 1.15 (Sylow 第二定理)

$|G| = p^\ell m$，其中 p 为素数，满足 $(p, m) = 1$，则有

- 任意 G 的 p-子群都是 G 的某个 Sylow p-子群的子群.
- G 的任意两个 Sylow p-子群互相共轭，即若 H_1 和 H_2 都是 G 的 Sylow p-子群，则存在 $a \in G$，满足

$$H_2 = aH_1a^{-1}$$

证明 由 Sylow 第一定理，我们知道 G 中有 Sylow p-子群，设 $P < G$ 为一个 Sylow p-子群，

我们记

$$[P] = \{P_1, \cdots, P_s\}$$

为 P 在共轭作用下的轨道，任取 $H < G$，满足 $|H| = p^k$，其中 $0 \leq k \leq l$.

我们考虑 H 在 $[P]$ 上的共轭作用，并记 $[P]$ 的轨道分解为

$$[P] = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_t$$

在对 $[P]$ 的元素做一个重排之后，我们设对任意 $1 \leq i \leq t$，由 $P_i \in \mathcal{O}_i$，我们知道下面的等式成立

$$|\mathcal{O}_i| = [H\colon N_H(P_i)] = [H\colon\ (H \cap N_G(P_i))] = [H\colon H \cap P_i]$$

因此我们有以下两个结论：

(i) 若 $|\mathcal{O}_i| = 1$，则

$$H = H \cap P_i$$

因此我们有 $H < P_i$.

(ii) 若 $|\mathcal{O}_i| > 1$，由于

$$|\mathcal{O}_i| \mid |H| \mid p^l$$

因此 $p \mid |\mathcal{O}_i|$. 我们假设 H 不被包含在任意的 P_i 中，则对任意 $i = 1, \cdots, t$，都有

$$p \mid |\mathcal{O}_i|$$

因此

$$p \mid \sum_{i=1}^{t} |\mathcal{O}_i| = |[P]|$$

另一方面，我们考虑

$$|[P]| = [G\colon N_G(P)]$$

由于 $P < N_G(P)$，因此

$$p \nmid |[P]|$$

矛盾，因此存在 P_i 使得 $|O_i| = 1$，即 $H < P_i$.

于是第一个论断证毕，下面我们考虑第二个论断：取 H 为 G 的任意一个 Sylow p-子群，设 P 为任意的一个 Sylow p-子群，考虑所有与 P 共轭的子群构成的集合.

重复以上讨论，我们知道存在一个与 P 共轭的 Sylow p-子群 P' 使得

$$H < P', \quad |H| = |P'|$$

所以我们有 $P' = H$，结论得证. □

注 考虑不同的群作用，我们可以得到不同的证明，如教材中的证明是利用了 H 在 G/P 上的左平移作用.

定理 1.16 (Sylow 第三定理)
$|G| = p^\ell m$，其中 p 为素数，满足 $(p,m)=1$，则 G 中 Sylow p-子群的个数 n_p 满足以下条件

$$n_p \equiv 1 \mod p$$

♡

证明 设 P 为 G 的一个 Sylow p-子群，我们记

$$[P] := \{P_1 = P, P_2, \cdots, P_s\}$$

为所有 Sylow p-子群的集合. 我们考虑 P 在 $[P]$ 上的共轭作用，我们记 $[P]$ 的轨道分解如下：

$$[P] = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_t$$

不妨设对任意 $1 \le i \le t \le s$，$\mathcal{O}_i$ 为 P_i 的轨道，因此 O_1 为 P 的轨道，所以我们有 $|\mathcal{O}_1| = 1$.

任取 $i > 1$，我们有

$$|\mathcal{O}_i| = [P : P \cap P_i] > 1$$

因此

$$p \mid |\mathcal{O}_i|$$

综上所述有

$$(n_p =)|[P]| \equiv |\mathcal{O}_1| = 1 \mod p$$

□

推论 1.13
$|G| = p^\ell m$，其中 p 为素数，满足 $(p,m)=1$，设 P 为 G 的一个 Sylow p-子群，沿用上面的记号，有以下两个叙述等价

- $P \lhd G$
- $n_p = 1$

♡

注 条件如上，我们设 G 的 Sylow p-子群的个数为 n_p，则满足

- $n_p \mid m$
- $n_p \equiv 1 \mod p$

第一个是因为

$$n_p = |[P]| = |G.P| = |G/G_P| = \frac{|G|}{|N_G P|} \mid m$$

1.7 群的直积

我们在 $H \times K$ 上定义一个二元运算：

$$\cdot: (H \times K) \times (H \times K) \to H \times K, \quad ((a,x),(b,y)) \mapsto (ab, xy)$$

容易验证 $H \times K$ 构成一个群.

定义 1.15

任取群 H 和 K，我们称群 $H \times K$ 为 H 和 K 的**(外)直积**，记作 $H \otimes_e K$[a](区别于集合的笛卡尔积).

[a]下标是为了说明是外直积，external，与后面的内直积 internal 区分

考虑到群 H 和 K，我们记 $G = H \otimes_e K$，通过考虑第一个分量和第二个分量，我们可以构造群 H 和 K 到 G 的单射：

$$j_H: H \to G, \quad a \mapsto (a, e_K)$$
$$j_K: K \to K, \quad x \mapsto (e_H, x)$$

我们容易验证 j_H 与 j_K 是单同态，我们记

$$N_H = \mathrm{Im}\,(j_H), \quad N_K = \mathrm{Im}\,(j_K)$$

命题 1.18

我们沿用上述记号，有以下结论

- $N \cong N_H$ 且 $K \cong N_K$.
- 任取 $a \in H$ 和 $x \in K$，我们有
$$(a, e_K)(e_H, x) = (e_H, x)(a, e_K)$$
- $N_H \lhd G$ 且 $N_K \lhd G$.
- $N_H \cap N_K = \{(e_H, e_K)\}$.
- $G = N_H N_K$.

定义 1.16

设 G 为一个群，N_1, N_2 为 G 的两个子群，假设 N_1, N_2 满足以下条件：

- $N_1 \lhd G$ 且 $N_2 \lhd G$
- $N_1 \cap N_2 = \{e\}$
- $G = N_1 N_2$

我们称 G 为 N_1 和 N_2 的**(内)直积**. 我们记作 $G = N_1 \otimes_i N_2$.

下面我们证明内直积的两个正规子群元素是可以交换的.

命题 1.19

设 G 为一个群，N_1, N_2 为 G 的两个正规子群，满足 $G = N_1 \otimes_i N_2$，则任取 $a \in N_1, x \in N_2$，我们有

$$ax = xa$$

证明 由于 N_2 为正规子群，所以我们有

$$axa^{-1} = y \in N_2$$

即

$$ax = ya = x(x^{-1}y)a$$

同理由于 N_1 是正规子群，所以有

$$x^{-1}ax = b \in N_1$$

即

$$ax = xb = x(ba^{-1})a$$

所以有

$$x^{-1}y = ba^{-1} \in N_1 \cap N_2 = \{e\}$$

即

$$x = y, a = b \Longrightarrow ax = ya = xa$$

□

注 注意到 N_1, N_2 也可以定义外直积，上面这个命题告诉我们这两个群的外直积与内直积是同构的.

命题 1.20

设 G 为一个群，设 N_1 和 N_2 为 G 的两个正规子群，满足 $G = N_1 \otimes_i N_2$，则映射

$$\varphi\colon N_1 \otimes_e N_2 \to N_1 \otimes_i N_2, \quad (a, x) \mapsto ax$$

是一个群同构.

证明 首先证明是一个群同态：

$$\varphi((a,x)(b,y)) = \varphi((ab, xy)) = (ab)(xy) = a(bx)y = (ax)(by) = \varphi((a,x))\varphi((b,y))$$

下面证明这是一个单射，任取 $a, b \in N_1$ 和 $x, y \in N_2$，则

$$\varphi((a,x)) = ax = by = \varphi((b,y)) \Leftrightarrow N_1 \ni b^{-1}a = yx^{-1} \in N_2 \Leftrightarrow a = b, x = y$$

再证明是满射，这是因为任取 $ax \in N_1N_2$，总存在 $(a, x) \in N_1 \otimes N_2$，使得

$$\varphi(a, x) = ax$$

综上我们知道是同构. □

定义 1.17 (群的扩张)

设群 G，A, B，若有 $N \lhd G$，其中

$$A \cong N, \quad B \cong G/N$$

则称 G 是 B 过 A 的扩张，其中 N 称为扩张核.

定义 1.18 (短正合序列)

短正合序列为

$$\{1\} \xrightarrow{i} A \xrightarrow{\lambda} G \xrightarrow{\mu} B \xrightarrow{0} \{1\}$$

其中 $\mathrm{Im}\ i = \mathrm{Ker}\ \lambda$，$\mathrm{Im}\ \lambda = \mathrm{Ker}\ \mu$，$\mathrm{Im}\ \mu = \mathrm{Ker}\ 0$.

实际上本质为 λ 单射，μ 满射.

$$A \xrightarrow{\lambda(\text{单})} G \xrightarrow{\mu(\text{满})} B$$

其中 $\mathrm{Im}\ \lambda = \mathrm{Ker}\ \mu$.

命题 1.21

下面两个命题是等价的：

(a) G 是 B 过 A 的扩张.

(b) 存在短正合序列

$$\{1\} \xrightarrow{i} A \xrightarrow{\lambda} G \xrightarrow{\mu} B \xrightarrow{0} \{1\}$$

证明

(a) $\Longleftrightarrow$ (b):

$$\begin{tikzcd}
 & (A \cong)N(\lhd G) & & G/N(\cong B) \arrow[d, "h"] & \\
\{1\} \arrow[r] & A \arrow[u, "f=\lambda"] \arrow[r, "\lambda"] & G \arrow[ur, "\pi"] \arrow[r, "\mu=h\circ\pi"] & B \arrow[r] & \{1\}
\end{tikzcd}$$

交换图道尽一切. □

命题 1.22

G 是 B 过 A 的扩张，$G \cong G'$，则 G' 也是 B 过 A 的扩张.

证明

$$\begin{tikzcd}
A \arrow[r, "\lambda(\text{单})"] \arrow[dr, "f\circ\lambda"'] & G \arrow[r, "\mu(\text{满})"] \arrow[d, "f"] & B \\
 & G' \arrow[ur, "\mu\circ f^{-1}"'] &
\end{tikzcd}$$

道尽一切. □

命题 1.23

若 G 跟 G' 都是 B 过 A 的扩张，且有同态映射 f 使得下图交换，则 f 是同构映射.

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\lambda"] \arrow[d, "id"'] & G \arrow[r, "\mu"] \arrow[d, "f"] & B \arrow[r] \arrow[d, "id"] & 1 \\
1 \arrow[r] & A \arrow[r, "\lambda'"] & G' \arrow[r, "\mu'"] & B \arrow[r] & 1
\end{tikzcd}$$

证明 先证明 f 是单射：由于交换，若 $f(x)=e$，则

$$\mu(x)=id(\mu(x))=\mu'(f(x))=\mu'(e)=e$$

从而 $x\in \mathrm{Ker}\,\mu=\mathrm{Im}\,\lambda$，即存在 $y\in A$，使得 $x=\lambda(y)$，再由交换得到

$$e=f(x)=f(\lambda(y))=\lambda'(y)$$

由于 λ' 是单同态，所以 $y=e$，从而 $x=\lambda(y)=\lambda(e)=e$，故 f 是单同态.

再证明 f 是满射：对于 $x'\in G$，有 $\mu'(x')\in B=\mu(G)$，从而 $\mu'(x')=\mu(x)$，$x\in G$，再由交换图有

$$\mu'(x')=\mu(x)=\mu'(f(x))$$

从而我们有

$$\mu'(x'f(x)^{-1})=e$$

这告诉我们

$$x'f(x)^{-1}\in \mathrm{Ker}\,\mu'=\mathrm{Im}\,\lambda'=\mathrm{Im}\,f\circ\lambda\subseteq \mathrm{Im}\,f$$

所以 $x'\in \mathrm{Im}\,f\cdot f(x)=\mathrm{Im}\,f$，从而 f 是满射. □

定义 1.19 (等价扩张)

称上面命题中满足条件的 G 和 G' 是 B 过 A 的等价扩张.

定义 1.20

设 G 是群 B 过 A 的扩张，N 是扩张核，若有 $H<G$，使得 $G=HN$，其中 $H\cap N=\{e\}$，则称此扩张为非本质扩张，并说 G 是 N 与 H 的半直积，记为

$$G=H\ltimes N$$

若还有 $H\lhd G$，则称此扩张为平凡扩张，并说 G 是 N 与 H 的内直积，记为 $G=H\otimes N$.

注 对于非本质扩张，有 $B\cong H$，这是因为

$$B\cong G/N=HN/N\cong H/(H\cap N)=H/\{e\}=H$$

定理 1.17

设 A, B 是群 G 的子群，则

(a) $G = AB$，$A \cap B = \{e\} \iff \forall g \in G$，有 $g = ab$，其中 $a \in A, b \in B$，且分解是唯一的.

(b) 若 $G = AB$，$A \cap B = \{e\}$，且 A, B 都是 G 的正规子群 $\iff \forall a \in A, b \in B$ 有 $ab = ba$ 且此时 $G = A \otimes B = B \otimes A$.

证明 (a) 分解的存在性由 $G = AB$ 立刻得到，若有

$$g = a_1b_1 = a_2b_2$$

我们有

$$a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{e\}$$

从而 $a_1b_1 = a_2b_2$，故唯一性得证.

反之若 $g = ab$ 分解唯一，告诉我们 $A \cap B$ 只能是 $\{e\}$，否则表示不唯一，故得证.

(2) 若 A, B 都是正规子群，则

$$aba^{-1} \in B, b^{-1} \in B \Longrightarrow b^{-1}aba^{-1} \in B$$

同理有

$$b^{-1}ab \in A, a^{-1} \in A \Longrightarrow b^{-1}aba^{-1} \in A$$

所以我们有

$$b^{-1}aba^{-1} \in A \cap B = \{e\}$$

所以有

$$ab = ba$$

反过来，若 $ab = ba$，则对任意 $g = ab \in G$，$x \in A$，有

$$gxg^{-1} = abxb^{-1}a^{-1} = axbb^{-1}a^{-1} = axa^{-1} \in A$$

故 A 是正规子群，同理 B 是正规子群，即 G 为平凡扩张，即 $G = A \otimes B = B \otimes A$. □

注 $G = A \otimes_i B$ 立刻得到 G 是 B 过 A 的平凡扩张，反之不一定对(需要加条件).

命题 1.24

设 A 为 r 阶循环群，B 为 s 阶循环群，则 $A \otimes_e B$ 为 rs 阶循环群 $\iff (r, s) = 1$.

定理 1.18

设 A, B 是两个群，则一定存在 B 过 A 的扩张 G，且在同构意义下 G 是唯一的.

证明 令 $G = A \otimes_e B$，容易验证是平凡扩张.

下设 G_1 也是 B 过 A 的平凡扩张，则有

$$A_1 \lhd G_1, B_1 \lhd G_1, G_1 = A_1B_1, A_1 \cap B_1 = \{e\}$$

且

$$A \cong A_1, B \cong G/A_1 \cong B_1$$

下证 $G \cong G_1$.

我们记 $f_1 \colon A \to A_1$ 与 $f_2 \colon B \to B_1$ 都是同构，令

$$f \colon G \to G_1, \quad (a, b) \mapsto f_1(a) \cdot f_2(a)$$

满射我们容易得到，下证单射：假设有

$$g_1(\in G_1) = f_1(a)f_2(b) = f_1(a')f_2(b')$$

由定理 1.17 我们知道分解是唯一的，从而 $f_1(a) = f_1(a')$，$f_2(b) = f_2(b')$. 由于 f_1, f_2 都是同构，所以我们知道 f 单射，从而 f 是双射.

容易验证 f 是同态，故我们知道 G 与 G_1 同构. □

命题 1.25

设 p, q 为素数，$p < q$ 且 $p \mid q - 1$，则 pq 阶群是一个循环群. ♠

证明 由 *Sylow* 定理我们知道存在 p 阶子群 P，q 阶子群 Q.

可以证明子群唯一，从而 $P \lhd G, Q \lhd G$，又 $PQ < G$，和

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$$

我们知道 $G = PQ$，所以 $G = P \otimes_i Q \cong P \otimes_e Q$，由命题 1.24 我们知道为循环群. □

证明 另证：由于 G 中元素的阶只能为 $1, p, q, pq$，而 1 阶元只有一个，p 阶元有 $p - 1$ 个，q 阶元有 $q - 1$，故

$$1 + (p - 1) + (q - 1) < pq$$

从而知道存在 pq 阶元. □

1.8 可解群与幂零群

定义 1.21 (换位子与换位子群)

设 $g_1, g_2 \in G$，则称

$$[g_1, g_2] := g_1^{-1} g_2^{-1} g_1 g_2$$

为 g_1, g_2 的换位子[a].

设 $H < G, K < G$，则称

$$[H, K] := \langle \{[h, k] \mid h \in H, k \in K\} \rangle$$

为 H 与 K 的换位子群.

[a]即 $g_2 g_1 [g_1, g_2] = g_1 g_2$. ♣

注 (1) $[g_2,g_1]=[g_1,g_2]^{-1}$.

(2) $[K,H]=[H,K]$.

命题 1.26

设 α 为 G 到 G_1 的同态，则

(a) $\forall g\in G$，有 $\alpha([g_1,g_2])=[\alpha(g_1),\alpha(g_2)]$.

(b) 设 $H<G,K<G$，有 $\alpha([H,K])=[\alpha(H),\alpha(K)]$.

引理 1.3

设 H,K 是群 G 的子群，则有

(a) $[H,K]=\{1\}\iff H\subseteq Z_G(K)$.

(b) $[H,K]\subseteq K\iff H\subseteq N_G(K)$.

(c) 若 $H\lhd G,K\lhd G$，则 $[H,K]\lhd G$，且 $[H,K]\subseteq H\cap K$.

(d) 若 $H_1<H,K_1<K$，则 $[H_1,K_1]<[H,K]$.

推论 1.14

(a) G 是交换群 $\iff[G,G]=\{1\}$.[a]

(b) $K\lhd G\Rightarrow[K,K]\lhd G$.

(c) $[G,G]\lhd G$，$G^{(1)}\lhd G$.

[a] $[G,G]=G^{(1)},[G^{(1)},G^{(1)}]=G^{(2)}$.

定义 1.22

群 G 中的子群序列：

$$G=G_1\supset G_2\supset\cdots\supset G_t\subset G_{t+1}=\{1\}$$

若满足 $G_i\lhd G_{i-1}$，则称为 G 的**次正规群列**，若还有 $G_i\lhd G$，则称为 G 的**正规群列**. G_{i-1}/G_i 称为次正规群列的**因子**，称

$$G_1/G_2,G_2/G_3,\cdots,G_t/G_{t+1}$$

为**因子列**，称 t 为**长度**.

若 $G_1,G_2,\cdots,G_{t+1}$ 出现在另一个次正规群列中，则称这个新的次正规群列为已有次正规群列的**加细**.

注 正规子群的正规子群不一定是正规子群!

定义 1.23

设 G 是群，G 中的三类子群分别定义为：

(a) $G^{(h)}$ 定义为：$G^{(0)}=G,G^{(h)}=[G^{(h-1)},G^{(h-1)}]$.

(b) $\Gamma_1(G)=G,\Gamma_k(G)=[G,\Gamma_{k-1}(G)]$.

(c) $C_0(G)=\{1\},C_k(G)/C_{k-1}(G)=Z(G/C_{k-1}(G))$.

称以下三个群列：

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots$$

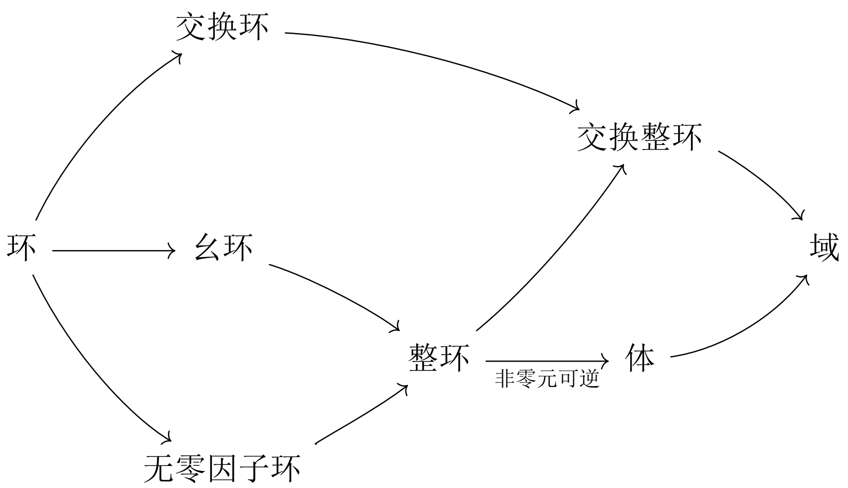
$$G = \Gamma_1(G) \supset \Gamma_2(G) \supset \cdots$$

$$C_0(G) \subset C_1(G) \subset C_2(G) \subset \cdots$$

为 G 的导出列，降中心列，升中心列.

注 $C_0(G) = \{1\}, C_1(G) = Z(G)$，后面可以考虑群同态基本定理来观察.

第 2 章 环



2.1 环的基本概念

定义 2.1

设 $\mathcal{R}$ 是一个非空集合，如果在 $\mathcal{R}$ 中有两种二元运算，且满足下面的条件：

(1) $\mathcal{R}$ 对于“加法”成为交换群，即 $\{\mathcal{R};+\}$ 为交换群；

(2) $\mathcal{R}$ 对于“乘法”成为半群，即 $\{\mathcal{R};\cdot\}$ 为半群；

(3) $\mathcal{R}$ 对于“乘法”与“加法”满足结合律：

$$a(b+c)=ab+ac,\quad (a+b)c=ac+bc,\quad \forall a,b,c\in\mathcal{R}$$

则称 $\mathcal{R}$ 是一个环，有时为了更加清楚，也说 $\{\mathcal{R};+;\cdot\}$ 为一个环.

笔记 如果一个环对于乘法也有幺元，则称该环为**幺环**，如果一个环对于乘法交换，则称该环为**交换环**.

定义 2.2

设 $\mathcal{R}$ 为一个环，$a,b\in\mathcal{R}$，且 $a\neq 0,b\neq 0$，若 $ab=0$，则称 a 为 $\mathcal{R}$ 中的一个**左零因子**，b 为 $\mathcal{R}$ 中的一个**右零因子**，都简称为**零因子**.

如果在环 $\mathcal{R}$ 中，由 $ax=ay$，$a\neq 0$，可以推出 $x=y$，则称 $\mathcal{R}$ 满足**左消去律**；如果由 $xa=ya$，$a\neq 0$ 可以推出 $x=y$，则称 $\mathcal{R}$ 满足**右消去律**.

命题 2.1

一个环 $\mathcal{R}$ 没有零因子的充分必要条件是 $\mathcal{R}$ 满足左右消去律.

证明 $\Longrightarrow$: 若 $\mathcal{R}$ 没有零因子，若 $ax=ay$，且 $a\neq 0$，则 $a(x-y)=0$，如果 $x\neq y$，则

$x-y\neq 0$ 与 $\mathcal{R}$ 没有零因子矛盾，故 $x=y$，因此 $\mathcal{R}$ 满足左消去律，同理可证满足右消去律.

$\Longleftarrow$: 设 $\mathcal{R}$ 满足左右消去律，则若 $ax=0$，$a\neq 0$，则 $ax=a0$，由左消去律可以得到 $x=0$，这说明 $\mathcal{R}$ 没有右零因子，同理可证没有左零因子. $\square$