群论

目录

1 映射与运算 2

2 等价关系与集合分类 3

3 群的概念 5

4 子群与陪集 6

5 正规子群与商群 8

6 群的同态与同构 10

7 循环群与生成组 12

8 变换群与置换群 14

9 群作用 17

10 Sylow 子群 21

11 群的直积 24

12 可解群与幂零群 29

1 映射与运算

定义 1.1 (映射). 设集合 A，B 非空，若 A 中的任一元素都能通过某一对应法则 f 唯一地对应到 B 中的一个元素，则称 f 是从 A 到 B 的**映射**，记作 $f: A \to B$. 设 $x \in A$，则 $y \in B$，称 y 是 x 在 f 下的**像**，记作 $f(x)$；称 x 是 y 在 f 下的**原像**，记作 $f^{-1}(y)$.

定义 1.2 (单射). 设映射 $f: A \to B$，对任意 $x_1, x_2 \in A, x_1 \neq x_2$，有 $f(x_1) \neq f(x_2)$，则称 f 是**单射**.

不同元素在单射下的像也不同.

定义 1.3 (满射). 设映射 $f: A \to B$，对任意 $y \in B$，都存在原像 $f^{-1}(y)$，则称 f 是**满射**.

定义 1.4 (双射). 若映射 f 既是单射，又是满射，则称 f 是**双射**.

双射 $f: A \to B$ 是 A 中元素与 B 中元素的一一对应.

定义 1.5 (恒等映射). 设映射 $i: A \to A$，$i(x) = x$，则称 i 为**恒等映射**.

定义 1.6 (嵌入映射). 设非空集合 $A_0 \subset A$，映射 $f: A_0 \to A$，$i(x) = x$，则称 i 是嵌入映射.

嵌入映射有扩大值域的作用.

定义 1.7 (开拓与限制). 设非空集合 $A_0 \subset A$，映射 $f: A_0 \to B$，$g: A \to B$，对任意 $x \in A_0$，有 $f(x) = g(x)$，则称 g 是 f 的**开拓**，f 是 g 的**限制**.

开拓映射有扩大定义域的作用，限制映射有缩小定义域的作用.

定义 1.8 (映射的复合). 设映射 $f: A \to B$，$g: B \to C$，则定义复合映射：$g \circ f = g(f(x)) : A \to C$.

可以用交换图表示这个过程.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g\circ f"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

定义 1.9 (直积). 设非空集合 A，B，定义 A 与 B 的**直积** $A \times B = \{(a, b) \mid \forall a \in A, b \in B\}$.

定义 1.10 (代数运算). 设非空集合 A，B，D，称映射 $A \times B \to D$ 为 A 与 B 到 D 的一个**代数运算**. 即对任意 $a \in A$，$b \in B$，都有唯一的 $d \in D$ 满足 $f(a, b) = d$，记作 $a \circ b = d$.

定义 1.11 (二元运算). 设 A 为非空集合. 代数运算 $f: A \times A \to A$ 称为**二元运算**，简称**运算**.

在二元运算下，A 中的元素经过运算仍在 A 中，于是二元运算满足**封闭性**.

定义 1.12 (结合性)**.** 若在非空集合 A 上定义了一种运算“$\circ$”，对任意 $a,b,c \in A$，都有

$$(a \circ b) \circ c = a \circ (b \circ c),$$

则称运算“$\circ$”是**结合的**.

定义 1.13 (交换性)**.** 若在非空集合 A 上定义了一种运算“$\circ$”，对任意 $a,b \in A$，都有

$$a \circ b = b \circ a,$$

则称运算“$\circ$”是**交换的**.

习惯上将运算“$\circ$”称为乘法，并略去不写. 要注意这里的乘法是一种抽象的运算，与数的乘法不是一回事. 那么，结合性可以写为 $(ab)c = a(bc)$，交换性可以写为 $ab = ba$.

定义 1.14 (分配性)**.** 若在非空集合 A 上定义了两种运算“$\circ$”和“$+$”，分别称为乘法和加法，对任意 $a,b,c \in A$，若有

$$a \circ (b + c) = (a \circ b) + (a \circ c),$$

则称乘法对加法是**左分配的**，若有

$$(a + b) \circ c = (a \circ c) + (b \circ c),$$

则称乘法对加法是**右分配的**. 若乘法对加法既是左分配的，又是右分配的，则称乘法对加法是**分配的**.

与乘法类似，这里的加法也是一种抽象的运算，不能简单看作数的加法.

2 等价关系与集合分类

定义 2.1 (关系)**.** 设集合 $R \subset A \times A$，$a,b \in A$，若 $(a,b) \in R$，则称 a 和 b 有**关系** R，记作 aRb；若 $(a,b) \notin R$，则称 a 与 b 没有关系.

定义 2.2 (等价关系)**.** 若关系 R 满足

1. 反身性：$aRa,\ \forall a \in A$;
2. 对称性：aRb，则 bRa，$\forall a,b \in A$;
3. 传递性：aRb, bRc 则 aRc，$\forall a,b,c \in A$.

则称 R 为**等价关系**.

定义 2.3 (集合的分类)**.** 非空集合 A 可以分成若干不交非空子集，即 $A=\bigcup\limits_{i\in I}M_i$，$M_i\cap M_j=\varnothing$, $i\neq j$，则 $\{M_i|i\in I\}$ 称为 A 的一个**分类**或**分划**.

定理 2.1. 集合 A 的一个分类决定 A 中的一个等价关系.

证明. 设关系 R 满足

$$aRb \iff a \text{ 和 } b \text{ 在同一类},$$

则根据定义易得 R 是等价关系. □

定义 2.4 (等价类)**.** 设在集合 A 上定义了一个等价关系 R，$a\in A$，则所有与 a 有关系的元素构成一个集合 $\{b\in A\mid bRa\}$，称为 a 所在的**等价类**，记作 $\overline{a}$，a 称为这个等价类的**代表元**.

定义 2.5 (商集)**.** 设集合 A 中有等价关系 R，则以 R 为前提的所有等价类的集合 $\{\overline{a}\}$ 称为 A 对 R 的**商集**，记作 A/R.

定义 2.6 (自然映射)**.** 称从非空集合 A 到它的商集合 A/R 的映射 $\pi:A\to A/R$, $\pi(a)=\overline{a}$ 为**自然映射**.

容易验证 π 是映射，且是满射，但未必是单射，因为以 a 为代表元的等价类不一定只有 a 这一个元素，如果 $b\in\overline{a}$，那么 $\pi(a)=\pi(b)=\overline{a}$.

定理 2.2. 集合 A 中的一个等价关系决定 A 的一个分类.

证明. 对任意 $a\in A$，$\pi(a)$ 是 a 所在的等价类，于是 A 中的任何元素都有所在的等价类，这些等价类互不相交，于是构成了 A 的一个分类. □

定义 2.7 (同余关系)**.** 设集合 A 中有等价关系 R，并带有二元运算“$\circ$”，若满足

$$aRb,\ cRd\Rightarrow(a\circ b)R(c\circ d),\quad\forall a,b,c,d\in A,$$

则称 R 是**同余关系**，相应地，a 的等价类也称为 a 的**同余类**.

定理 2.3. 设“$\circ$”是 A 中的二元运算，并定义“$\overline{\circ}$”: $\overline{a}\overline{\circ}\overline{c}=\overline{a\circ c}$，则“$\overline{\circ}$”是 A 中的二元运算当且仅当 R 是同余关系.

证明. 若“$\overline{\circ}$”是二元运算，则对任意 $\overline{a},\overline{c}\in A/R$，有 $\overline{a}\mathbin{\overline{\circ}}\overline{c}\in A/R$，于是 $\overline{a\circ c}\in A/R$，设 aRb，cRd，则

$$\overline{a}\mathbin{\overline{\circ}}\overline{c}=\overline{b}\mathbin{\overline{\circ}}\overline{d}=\overline{b\circ d}=\overline{a\circ c},$$

故 $(a\circ c)R(b\circ d)$.

若 R 是同余关系，则对任意 aRb，cRd，有 $(a\circ c)R(b\circ d)$，进而 $\overline{a\circ c}=\overline{b\circ d}$，故 $\overline{a}\mathbin{\overline{\circ}}\overline{c}=\overline{b}\mathbin{\overline{\circ}}\overline{d}\in A/R$，所以“$\circ$”是二元运算. □

3 群的概念

定义 3.1 (半群)**.** 设集合 S 带有二元运算"$\circ$"，若对任意 $a,b,c\in S$，有 $(a\circ b)\circ c=a\circ(b\circ c)$，则称 $(S,\circ)$ 是**半群**.

定义 3.2 (幺半群)**.** 设半群 $(M,\circ)$，若存在 $e\in M$，对任意 $a\in M$，有 $e\circ a=a\circ e=a$，则称 $(M,\circ)$ 为**幺半群**，e 称为 $(M,\circ)$ 的**幺元**.

定义 3.3 (群)**.** 设集合 G 带有二元运算"$\circ$"，满足以下条件：

1. 对任意 $a,b,c\in G$，有 $(a\circ b)\circ c=a\circ(b\circ c)$;
2. 存在 $e\in G$，对任意 $a\in G$，有 $e\circ a=a\circ e=a$;
3. 对任意 $a\in G$，存在 $a^{-1}\in G$，使得 $a\circ a^{-1}=a^{-1}\circ a=e$,

则称 $(G,\circ)$ 是一个**群**.

注. 在不引起歧义的情况下，可以说"设 G 是一个群"，而将运算"$\circ$"看作广义上的"乘法"而省略，即"$a\circ b$"记作"ab".

注. 称"a^{-1}"为 a 的**逆元**.

定义 3.4 (交换群)**.** 若 G 中任意元素 a,b 满足 $ab=ba$，则称 G 是**交换群**或 **Abel 群**.

定理 3.1. 群 G 的幺元是唯一的.

证明. 设 $e,e'\in G$ 都是幺元，则 $e=ee'=e'$. □

定理 3.2. 群 G 的逆元是唯一的.

证明. 对任意 $a\in G$，设 $b,c\in G$ 是 a 的逆元，则 $b=b(ac)=(ba)c=c$. □

由于结合律成立，则 $a^n=\underbrace{a\circ a\circ\cdots\circ a}_{n\text{个}}$ 是良定义的. 同时有 $a^m a^n=a^{m+n}$，$(a^s)^t=a^{st}$.

定理 3.3 (消去律)**.** 设 $a,b,c\in G$，若 $ab=ac$，则 $b=c$；若 $ba=ca$，则 $b=c$.

证明. $ab=ac\Rightarrow a^{-1}ab=a^{-1}ac\Rightarrow b=c$，类似地 $ba=ca\Rightarrow baa^{-1}=caa^{-1}\Rightarrow b=c$. □

定义 3.5 (群的阶)**.** 群 G 中元素的个数称为群的**阶**，记作 $|G|$. 当 $|G|$ 有限时，称 G 为**有限群**，否则称 G 为**无限群**.

定义 3.6 (群中元素的阶)**.** 设 G 为一个群，$a\in G$，若存在正整数 k 使得 $a^k=e$，则最小的正整数 k 称为 a 的**阶**，记作 $|a|$. 即 $|a|=\min\left\{k\in\mathbb{N}^+|a^k=e\right\}$. 若不存在这样的 k，则称 a 的阶为无穷.

定理 3.4. $|a|=\infty \iff \forall m,n\in\mathbb{N}^+, m\neq n, a^m\neq a^n$.

证明. 设 $m.n.k\in\mathbb{N}^+$ 且 $m=n+k$. 则 $|a|=\infty \iff \forall k\in\mathbb{N}^+$，$a^k\neq e \iff a^{m-n}\neq e \iff a^m\neq a^n$. □

定理 3.5. 设 $|a|=d$，则 $\forall h\in\mathbb{Z}$，$a^h=e \iff d|h$.

证明. 充分性：$d|h$，则存在 $k\in\mathbb{Z}$ 使得 $h=kd$，则 $a^h=a^{kd}=(a^d)^k=e$.

必要性：设 $h=qd+r$，$0\leqslant r<d$，则 $a^{qd+r}=a^{qd}a^r=a^r=e$，则 $r=0$. □

推论 3.1. 对任意 $m,n\in\mathbb{Z}$，$a^m=a^n \iff d|m-n \iff m\equiv n \pmod d$.

定理 3.6. 设 $|a|=d$，$k\in\mathbb{N}^+$，则 $|a^k|=\dfrac{d}{(d,k)}$.

证明. 设 $|a^k|=h$，则 $a^{kh}=e$. 而 $|a|=d$，则 $d|kh$.

设 $d=d_1(d,k)$，$k=k_1(d,k)$，则 $(d_1,k_1)=1$，$d_1|k_1h$，则 $d_1|h$.

$(a^k)^{d_1}=a^{kd_1}=a^{dk_1}=e$，故 $h|d_1$. 于是 $|a^k|=h=d_1=\dfrac{d}{(d,k)}$. □

推论 3.2. $|a^k|=d \iff (d,k)=1$.

定理 3.7. 设 $a,b\in G$，$|a|=m$，$|b|=n$，$ab=ba$，$(m,n)=1$，则 $|ab|=mn$.

证明. 设 $|ab|=d$，而 $(ab)^{mn}=(a^m)^n(b^n)^m=e$，于是 $d|mn$;

又 $(ab)^{md}=a^{md}b^{md}=b^{md}=e$，故 $n|md$，而 $(m,n)=1$，于是 $n|d$. 同理 $m|d$，于是 $mn|d$，故 $mn=d$. □

4 子群与陪集

定义 4.1 (子群)**.** 设 G 是群，若非空集合 $H\subset G$ 且 H 是群，则称 H 是 G 的**子群**，记作 $H<G$.

考虑极端，G 本身和 $\{e\}$ 都是 G 的子群，称为 G 的**平凡子群**.

定理 4.1 (子群的充要条件)**.** 设 H 是群 G 的非空子集，则 $H<G$ 当且仅当对任意 $a,b\in H$，$ab^{-1}\in H$.

证明. 当 $H<G$ 时，由 H 运算的封闭性以及存在逆元即得 $ab^{-1}\in H$.

若对任意 $a,b\in H$，有 $ab^{-1}\in H$，则

对任意 $a,a\in H$，有 $e=aa^{-1}\in H$，幺元存在;

对 $e\in H$ 与任意 $b\in H$，有 $b^{-1}=eb^{-1}\in H$，逆元存在;

对任意 $a,b^{-1}\in H$，有 $ab=a(b^{-1})^{-1}\in H$，满足封闭律;

H 中的运算继承 G 中的运算，满足结合律，于是 $H<G$. □

定理 4.2. 设 H 是群 G 的非空有限子集，则 $H < G$ 当且仅当 H 对 G 的运算封闭.

证明. 必要性显然. 充分性：H 对 G 的运算封闭，故对任意 $a \in H$，$a^k \in H$，其中 k 为任意正整数. 由于 H 是有限群，于是存在正整数 $m > n$ 满足 $a^m = a^n$，故 $a^{m-n} = e \in H$. 当 $m - n = 1$ 时，$a = e$，于是 $a^{-1} = e \in H$；当 $m - n > 1$ 时，$a^{m-n-1}a = aa^{m-n-1} = e$，$a^{-1} = a^{m-n-1} \in H$，逆元存在. 封闭性满足，结合律满足，于是 $H < G$. □

定理 4.3. 若 $H_1 < G$，$H_2 < G$，则 $H_1 \cap H_2 < G$.

证明. 设 $a, b \in H_1 \cap H_2$，则由定理4.1，$ab^{-1} \in H_1$，$ab^{-1} \in H_2$，则 $ab^{-1} \in H_1 \cap H_2$，再用一次该定理，即得 $H_1 \cap H_2 < G$. □

推论 4.1. 设 I 为指标集，若对任意 $i \in I$，$H_i < G$，则 $\bigcap\limits_{i \in I} H_i < G$.

下面是一些例子.

例 4.1. 数域 F 上全体 n 阶可逆方阵关于矩阵乘法构成群，称为**一般线性群**，记作 $GL_n(F)$. 其中，行列式为 1 的 n 阶方阵关于矩阵乘法也构成群，称为**特殊线性群**，记作 $SL_n(F)$. 显然 $SL_n(F) < GL_n(F)$.

例 4.2. 给定 $m \in \mathbb{Z}$，定义集合 $m\mathbb{Z} = \{mn \mid \forall n \in \mathbb{Z}\}$，定义运算为整数加法，则 $m\mathbb{Z} < \mathbb{Z}$.

定理 4.4. $(\mathbb{Z}, +)$ 的子群都是形如 $m\mathbb{Z}$ 的.

证明. 设 $H < \mathbb{Z}$. 若 $H = \{0\}$，则 $H = 0\mathbb{Z}$.

假设 $H \neq 0$，则存在非零整数. 由于 H 是子群，若 $a \in H$，则 $-a \in H$，因此 H 中必存在正整数. 定义 $m = \min\{a \in H | a > 0\}$

任取 $n \in H$，设 $n = qm + r$，其中 $0 \leqslant r < m$. 由于 $m \in H$ 且 H 是子群，于是 $r = n - qm \in H$. 但 $0 \leqslant r < m$，而 m 是 H 中最小的正整数，因此 $r = 0$，即 $n = qm \in m\mathbb{Z}$，所以 $H \subset \mathbb{Z}$.

由于 $m \in H$，且 H 是子群，对任意整数 k，有 $km \in H$，因此 $\mathbb{Z} \subset H$. □

定义 4.2 (陪集)**.** 设 $H < G$，给定 $a \in G$，集合 $aH = \{ah | h \in H\}$ 称为以 a 为代表的**左陪集**. 类似地，集合 $Ha = \{ha | h \in H\}$ 称为以 a 为代表元的**右陪集**.

左陪集和右陪集的概念是对偶的，下面考虑左陪集的情形.

定理 4.5. 设 $H < G$，则 $aRb \iff a^{-1}b \in H$ 确定了 G 中的等价关系 R. a 所在的等价类 $\overline{a}$ 恰为以 a 为代表的左陪集 aH.

证明. 先证 R 为等价关系.

自反性：H 为子群，故 $a^{-1}a = e \in H$，即 aRa.

对称性：若 aRb，则 $a^{-1}b \in H$，$b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$，即 bRa.

传递性：若 aRb，bRc，则 $a^{-1}b \in H$，$b^{-1}c \in H$，$a^{-1}c = a^{-1}bb^{-1}c \in H$，即 aRc.

再证 $\overline{a} = aH$. 对任意 $b \in \overline{a}$，$a^{-1}b \in H$，$b = aa^{-1}b \in aH$，于是 $\overline{a} \subset aH$；对任意 $b \in aH$，存在 $h \in H$ 使得 $b = ah$. $a^{-1}b = a^{-1}ah = h \in H$，于是 $aH \subset \overline{a}$. □

由于 R 是一个等价关系，于是全体左陪集 $\{aH\}$ 为 G 的一个分类，称为**左陪集空间**. 由此可见左陪集空间是群 G 对关系 R 的商集，于是又把左陪集空间称为**左商集**，记作 G/R.

命题 4.1. 映射 $\varphi : H \to aH, h \mapsto ah$ 是双射.

证明. aH 是由 H 得到的，φ 是满射是显然的. 对任意 $h_1 \neq h_2 \in H$，$ah_1 \neq ah_2$（否则将违反消去律），故 φ 是单射. □

定义 4.3 (指数)**.** 左陪集空间中陪集的个数称为**指数**，记作 $[G : H]$.

定理 4.6 (Lagrange)**.** 设 G 为有限群，$H < G$，则

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

证明. 设 $[G : H] = n$，a_i 为每个左陪集的代表元. $G = \bigsqcup_{i=1}^{n} a_iH$，而由命题4.1，$|a_iH| = |H|$，故 $|G| = n|H| = [G : H]\,|H|$. □

推论 4.2. 设 G 是有限群，$K < H < G$，则 $[G : K] = [G : H]\,[H : K]$.

5 正规子群与商群

定义 5.1 (共轭)**.** 设 $f, h \in G$，若存在 $g \in G$，使得

$$f = ghg^{-1},$$

则称 f 和 g **共轭**.

容易验证，共轭是一个等价关系，于是决定了一个等价类，称为共轭类.

定义 5.2 (共轭类)**.** 设 G 是群，对任意 $f \in G$，与 f 共轭的元素组成的集合称为以 f 为代表元的**共轭类**.

定义 5.3 (自共轭元素)**.** 如果以 f 为代表的共轭类中的元素只有 f 一个，则称 f 是群 G 的**自共轭元素**.

性质 5.1. 一个共轭类中所有元素的阶相同.

性质 5.2. 共轭类的元素数目是群的阶的因子.

定义 5.4 (共轭子群). 若 $H < G$，$K < G$，存在 $g \in G$ 使得

$$K = gHg^{-1},$$

则称子群 H 和 K **共轭**.

定义 5.5 (元素的中心化子). 设 $a \in G$，集合 $C_G(a) = \{g \in G \mid ga = ag\}$ 是 G 的子群，称为 a 的**中心化子**.

定义 5.6 (子集的中心化子). 设 $S \subset G$，集合 $C_G(S) = \{g \in G \mid gs = sg, \forall s \in S\}$ 是 G 的子群，称为 S 的**中心化子**.

定义 5.7 (中心). $C_G(G)$ 称为 G 的**中心**.

定义 5.8 (正规化子). 设 $M \subset G$，集合 $N_G(M) = \{g \in G \mid gM = Mg\}$ 是 G 的子群，称为 M 的**正规化子**.

如果对任意 $g \in G$，子群 H 都是自共轭的，则称 H 为正规子群，即如下定义.

定义 5.9 (正规子群). 设 G 是群，$H < G$，若有

$$ghg^{-1} \in H, \ \forall\ g \in G, \ \forall\ h \in H,$$

则称 H 是 G 的**正规子群**，记作 $H \lhd G$.

例 5.1. 定义运算为矩阵乘法，$SL_n(F) \lhd GL_n(F)$.

例 5.2. 定义运算为数的加法，$m\mathbb{Z} \lhd \mathbb{Z}$.

定理 5.1. 设 $H < G$，则下列条件等价.

1. $H \lhd G$;
2. $gH = Hg, \ \forall\ g \in G$;
3. $g_1Hg_2H = g_1g_2H, \ \forall\ g_1, g_2 \in G$.

证明. $1 \to 2$: 若 $H \lhd G$，则 $gHg^{-1} = H$，故 $gH = Hg$.

$2 \to 3$: 若 $gH = Hg$，则 $g_1Hg_2H = g_1(Hg_2)H = g_1g_2H$.

$3 \to 1$: 若 $g_1Hg_2H = g_1g_2H$，则 $gHg^{-1}H = gg^{-1}H = H$，则 $gHg^{-1} = H$. □

定义 5.10 (商群)**.** 设 $H < G$，关系 R 定义为 $aRb \iff a^{-1}b \in H$，则

$$R\text{为同余关系} \iff H \lhd G,$$

商集合 G/R 对同余关系 R 导出的运算也构成一个群，称为 G 对 H 的**商群**，记为 G/H.

证明. 必要性：因为 $g^{-1}(gh) = h \in H$，故 $gR(gh)$. 又 $g^{-1}Rg^{-1}$，于是由同余关系，

$$(gg^{-1})R(ghg^{-1}),$$

即 $eR(ghg^{-1})$，$ghg^{-1} = e^{-1}ghg^{-1} \in H$，$H \lhd G$.

充分性：设任意 $a_1, a_2, b_1, b_2 \in H$，a_1Rb_1，a_2Rb_2，则

$$(a_1a_2)^{-1}(b_1b_2) = a_2^{-1}a_1^{-1}b_1b_2 = a_2{-}1a_1^{-1}b_1a_2a_2^{-1}b_2,$$

由于 $H \lhd G$，$a_1^{-1}b_1 \in H$，则 $a_2{-}1a_1^{-1}b_1a_2 \in H$，又 $a_2^{-1}b_2 \in H$，则 $(a_1a_2)^{-1}(b_1b_2) \in H$，故 R 为同余关系. □

例 5.3. 由于 $m\mathbb{Z} \lhd \mathbb{Z}$，于是有商群

$$\mathbb{Z}/m\mathbb{Z} = \left\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\right\},$$

记为 $\mathbb{Z}_m$，称为 $\mathbb{Z}$ 的**模 $\boldsymbol{m}$ 的剩余类加群**.

剩余类加群的每一个元素叫做一个剩余类. 同一剩余类中的两个元素同余，例如设 $a, b \in \overline{k}$，$k = 0, 1, \cdots, m-1$，则 $a \equiv b \pmod m$.

6 群的同态与同构

定义 6.1 (同态映射)**.** 设群 $(G_1, \circ)$, $(G_2, *)$ 之间存在映射 $f : G_1 \to G_2$，若对任意 $g_1, g_2 \in G_1$，有 $f(g_1 \circ g_2) = f(g_1) * f(g_2)$，则称 f 为**同态映射**. 符号不至于混淆时，常记作 $f(g_1g_2) = f(g_1)f(g_2)$.

如果 f 是单射，则称为**单同态**；如果 f 是满射，则称为**满同态**. 若 $f : G_1 \to G_2$ 是满同态，则称 G_1 和 G_2 是**同态的**.

定义 6.2 (同构)**.** 若同态映射 $f : G_1 \to G_2$ 是双射，则称 f 是**同构映射**，G_1 和 G_2 是**同构的**，记作 $G_1 \cong G_2$.

注. *容易验证，同构是等价关系.*

定义 6.3 (自然同态)**.** 设 $H \lhd G$，映射 $\pi : G \to G/H, g \mapsto gH$ 是同态映射，称为**自然同态**.

性质 6.1. 设同态映射 $f: G_1 \to G_2$，$g: G_2 \to G_3$，则 $gf: G_1 \to G_3$ 也是同态映射.

性质 6.2. 幺元同态到幺元，逆元同态到逆元，子群同态到子群.

定义 6.4 (核)**.** 设同态映射 $f: G_1 \to G_2$，$e_1 \in G_1$，$e_2 \in G_2$ 是幺元，G_2 的幺元 e_2 的完全原像 $\{a \in G_1 \mid f(a) = e_2\}$ 称为同态映射 f 的**核**，记作 $\ker f$.

例 6.1. 同态映射 f 是单同态当且仅当 $\ker f = \{e_1\}$.

证明. 必要性显然. 充分性：若 $\ker f = \{e_1\}$，则 $f(e_1) = e_2$，对任意 $x_1, x_2 \in G_1$，若 $f(x_1) = f(x_2)$，则 $f(x_1)\,[f(x_2)]^{-1} = f(x_1 x_2^{-1}) = e_2$，于是 $x_1 x_2^{-1} = e_1$，则 $x_1 = x_2$. □

命题 6.1. 若 $H \lhd G$，$\pi: G \to G/H$，则 $\ker \pi = H$.

命题 6.2. 设同态映射 $f: G_1 \to G_2$，则 $\ker f \lhd G_1$.

证明. 对任意 $g \in G_1$，$a \in \ker f$，

$$f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_1) = e_2,$$

于是 $gag^{-1} \in \ker f$. 由正规子群定义得 $\ker f \lhd G_1$. □

定理 6.1 (群同态基本定理)**.** 设满同态 $f: G_1 \to G_2$，则 $G_1/\ker f \cong G_2$.

证明. 记 $N = \ker f \lhd G_1$，设 $\varphi: G_1/N \to G_2,\ gN \mapsto f(g)$. 若 $g_1 N = g_2 N$，则 $g_1^{-1} g_2 \in N$，$f(g_1^{-1} g_2) = f(g_1)^{-1} f(g_2) = e_2$，于是 $f(g_1) = f(g_2)$. 这表明 g_N 在 φ 下的像是唯一的，所以 φ 是映射.

若 $f(g_1) = f(g_2)$，则 $e_2 = f(g_1)^{-1} f(g_2) = f(g_1^{-1} g_2)$，于是 $g_1^{-1} g_2 \in N$，$g_1 N = g_2 N$，因此 φ 是单射.

由于 f 是满射，因此 φ 是满射，故 φ 是双射.

对任意 $aN, bN \in G/N$，由于 f 是同态，有

$$\varphi(aNbN) = \varphi(abN) = f(ab) = f(a)f(b) = \varphi(aN)\varphi(bN).$$

因此 φ 是同构映射，故 $G_1/\ker f \cong G_2$. □

推论 6.1 (第一同构定理)**.** 设 f 是群 G 的同态，则 $G/\ker f \cong f(G)$.

定理 6.2 (第二同构定理)**.** 若 $H < G$，$N \lhd G$，则 $H \cap N \lhd H$ 且

$$H/(H \cap N) \cong HN/N.$$

证明. 令 $\varphi : H \to HN/N,\ h \mapsto hN$，显然 φ 是映射. 对任意 $hnN \in HN/N$，由于 $hnN = hN$，有

$$\varphi(h) = hN = hnN,$$

故 φ 是满射. 对任意 $h_1, h_2 \in H$，

$$\varphi(h_1h_2) = h_1h_2N = h_1Nh_2N = \varphi(h_1)\varphi(h_2),$$

故 φ 是同态. 而

$$\ker\varphi = \{h \in H \mid \varphi(h) = hN = e_2 = N\} = \{h \in H \mid h \in N\} = H \cap N,$$

由同态基本定理，有

$$H/(H \cap N) \cong HN/N.$$

□

定理 6.3 (第三同构定理)**.** 若 $H \lhd G$，$N \lhd G$，$N \subset H$，则

$$G/H \cong (G/N)/(H/N).$$

证明. 由 $H \lhd G$，$N \lhd G$ 以及 $N \subset H$，有 $N \lhd H$，且 $H/N \lhd G/N$.

设 $\pi : G \to G/N,\ g \mapsto gN$ 以及 $\psi : G/N \to (G/N)/(H/N),\ gN \mapsto (gN)(H/N)$，则 $\varphi = \psi \circ \pi : G \to (G/N)/(H/N)$ 是群同态.

由于 π，ψ 是满射，故 φ 是满射. 又

$$\ker\varphi = \{g \in G \mid \varphi(g) = H/N\},$$

$$\varphi(g) = \psi(\pi(g)) = (gN)(H/N),$$

$$(gN)(H/N) = H/N \iff gN = H/N \iff g \in H,$$

故 $\ker\varphi = G \cap H = H$，由群同态基本定理，

$$G/H \cong (G/N)/(H/N).$$

□

7 循环群与生成组

定义 7.1 (循环群)**.** 由一个元素 a 反复运算得到的群称为**循环群**，记作 $\langle a\rangle$. 这个元素称为群的**生成元**.

定理 7.1. 循环群都是交换群.

证明. 对任意 $a^m, a^n \in \langle a \rangle$，$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$. $\square$

定理 7.2. 循环群的子群仍是循环群.

证明. 设 $G_1 < \langle a \rangle$，设 $k = \min\left\{m \in \mathbb{N}^+ \mid a^m \in G_1\right\}$，则 $\langle a^k \rangle \subset G_1$.

对任意 $a^n \in G_1$，设 $n = qk + r$，则 $a^n = a^{qk}a^r \in G_1$，于是 $a^r \in G_1$，$0 \leqslant r < k$，则 $r = 0$. 于是 $a_n \in \langle a^k \rangle$，则 $G_1 \subset \langle a^k \rangle$. $\square$

定理 7.3. 设循环群 $G = \langle a \rangle$. 若 $|G| = m$，则 $G \cong (\mathbb{Z}_m, +)$；若 $|G| = \infty$，则 $G \cong (\mathbb{Z}, +)$.

证明. 设 $f : \mathbb{Z} \to G,\ n \to a^n$. 显然 f 是映射. 任意 a^n 都有 n 对应，故 f 是满射. 对任意 $m, n \in \mathbb{Z}$，

$$f(m+n) = a^{m+n} = a^m a^n = f(m)f(n),$$

故 f 是满同态. 由群同态基本定理，

$$\mathbb{Z}/\ker f \cong G.$$

而 $\ker f \lhd \mathbb{Z} = m\mathbb{Z}$，这里存在 $m \in \mathbb{N}$. 当 $m = 0$ 时，$\ker f = \{0\}$，则 $\mathbb{Z} \cong G$. 当 $m > 0$ 时，$\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \cong G$. $\square$

定理 7.4. 设 $|G| = m$，则 G 是循环群的充要条件是对每一个正整数因子 $m_1|m$，都存在唯一的 m_1 阶子群.

命题 7.1. 有限群 G 中元素的阶是 $|G|$ 的因子.

证明. 显然有限群中元素的阶有限，设 $a \in G, |a| = d$，则

$$\langle a \rangle = \left\{e, a, a^2, \cdots, a^{d-1}\right\},$$

而 $\langle a \rangle < G, |\langle a \rangle| = d$，由 Lagrange 定理得证. $\square$

命题 7.2. 素数阶群必为循环群.

证明. 设有限群 $|G| = p$，p 是素数，则由命题7.1，对任意 $g \in G$，$|g| = 1$ 或 p. 当 $|g| = 1$ 时，$g = e$. 当 $|g| = p$ 时，$|\langle g \rangle| = p = |G|$，而 $\langle g \rangle < G$，于是 $\langle g \rangle = G$，即 G 是由 g 生成的循环群. $\square$

定义 7.2 (生成的子群). 设 S 是群 G 的非空子集，包含 S 的最小子群称为 S **生成的子群**，记作 $\langle S \rangle$. 等价定义为包含 S 的所有子群的交.

定理 7.5. 设 S 是群 G 的非空子集，$S^{-1} = \left\{a^{-1} \mid a \in S\right\}$，则

$$\langle S \rangle = \left\{x_1 x_2 \cdots x_m \mid x_i \in S \cup S^{-1}\right\}$$

证明. 设 $T=\left\{x_1x_2\cdots x_m \mid x_i\in S\cup S^{-1}\right\}$. 由于 $S\subset\langle S\rangle$，$S^{-1}\subset\langle S\rangle$，于是 $S\cup S^{-1}\subset\langle S\rangle$，则 $T\subset\langle S\rangle$. 下面证明 T 是子群.

设 $x_1x_2\cdots x_n, y_1y_2\cdots y_m\in T$，则 $y_i^{-1}\in S\cup S^{-1}$，于是

$$x_1x_2\cdots x_n(y_1y_2\cdots y_m)^{-1}=x_1x_2\cdots x_ny_m^{-1}y_{m-1}^{-1}\cdots y_1^{-1}\in T.$$

故 $T<\langle S\rangle$，而 $\langle S\rangle$ 是包含 S 的最小子群，故 $T=S$. □

定义 7.3 (生成组). 若 $G=\langle S\rangle$，则称 S 为 G 的**生成组**.

定义 7.4 (有限生成群). 若存在群 G 的有限个元素的生成组，则称 G 是**有限生成群**. 若 G 还是交换群，则称为**有限生成 Abel 群**.

注意到有限群是有限生成群，但有限生成群不一定是有限群，例如 $(\mathbb{Z},+)=\langle 1\rangle$.

8 变换群与置换群

定义 8.1 (变换). 设 A 是一个集合，映射 $f:A\to A$ 称为**变换**，即集合到自身的映射.

定义 8.2 (变换群). 集合 A 上所有的可逆变换组成的集合，关于映射的复合构成群，称为集合 A 的**全变换群**，记作 S_A. 全变换群的一个子群称为 A 的一个**变换群**.

可以依定义验证 S_A 构成群. 可逆变换即双射，要求集合中的元素在变换前后是一一对应的.

定义 8.3 (对称群). 若集合 A 是含 n 个元素的有限集，S_A 也称为 n 元**对称群**，也记作 S_n. S_n 中的变换称为**置换**.

定义 8.4 (置换群). 对称群 S_n 中若干置换可以构成一个 S_n 的子群，称为**置换群**.

由定义，对称群是最大的置换群.

定理 8.1 (Cayley). 任何群都与一个变换群同构.

证明. 设 G 是群，任意 $a\in G$，定义 $\varphi_a:G\to G,\ g\mapsto ag$. g 在 φ_a 下的像 ag 是唯一的，所以 φ 是映射.

由于 $a^{-1}g\in G$，而 $\varphi_a(a^{-1}g)=g$，也就是 G 中任何元素 g 都有原像 $a^{-1}g$，所以 φ_a 是满射.

对任意 $g_1,g_2\in G$，若 $\varphi_a(g_1)=\varphi_a(g_2)$，则 $ag_1=ag_2$. 由消去律有 $g_1=g_2$，于是 φ_a 是单射. φ_a 又是满射，所以是双射，即可逆映射. 故 $\varphi_a\in S_G$.

设 $T=\{\varphi_a\mid a\in G\}$，则 $T\subset S_G$. 又因为 $(\varphi_b)^{-1}=\varphi_{b^{-1}}$，则 $\varphi_a(\varphi_b)^{-1}=\varphi_a\varphi_{b^{-1}}=\varphi_{ab^{-1}}\in T$，于是由子群的充要条件，有 $T<S_G$，则 T 是 G 的一个变换群，下面证明 $T\cong G$.

设 $f: G \to T,\ a \mapsto \varphi_a$，显然 f 是满映射. 对任意 $g_1, g_2 \in G$，若 $f(g_1) = f(g_2)$，则 $\varphi_{g_1} = \varphi_{g_2}$，$\varphi_{g_1}(e) = \varphi_{g_2}(e)$，即 $g_1 = g_2$，所以 f 是单射. 于是 f 是双射.

对任意 $a, b \in G$，$f(ab) = \varphi_{ab} = \varphi_a\varphi_b = f(a)(b)$，所以 f 是同构映射，$G \cong T$. □

推论 8.1. 任何有限群都与一个置换群同构.

下面介绍置换群相关内容. 设 $\sigma \in S_n$，设 $A = \{a_1, a_2, \cdots, a_n\}$，则置换 σ 可以表示为

$$\sigma(A) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}$$

其中，$\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_n)$ 是 $a_1, a_2, \cdots, a_n$ 的一个排列. 注意到一共有 $n!$ 种不同的排列方式，于是 $|S_n| = n!$. 特别地，若 $\mathrm{id}(a_i) = a_i, i = 1, 2, \cdots, n$，则称 id 为**恒等置换**.

定义 8.5 (轮换)**.** 设 $I_r = \{i_1, i_2, \cdots, i_r\} \subset \{a_1, a_2, \cdots, a_n\} = A$，置换 σ 满足

$$\sigma(I_r) = \begin{pmatrix} i_1 & i_2 & \cdots & i_r \\ i_2 & i_3 & \cdots & i_1 \end{pmatrix}$$

$$\sigma(A \backslash I_r) = \mathrm{id}(A \backslash I_r),$$

则称 σ 为 ***r*-轮换**，记作 $\sigma = (i_1 i_2 \cdots i_r)$. $i_1, i_2, \cdots, i_r$ 称为轮换中的**文字**，r 称为轮换的**长**.

特别地，当 $r = 2$ 时称为**对换**，$r = 1$ 时为恒等置换.

命题 8.1. r-轮换的阶为 r.

命题 8.2. $(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_1) = \cdots (i_r i_1 \cdots i_{r-1})$.

上述两个命题都是显然的.

定义 8.6. 在 S_n 中，如果若干个轮换间无共同文字，则称它们是**不相交的轮换**.

命题 8.3. 在 S_n 中不相交轮换的乘积可换.

证明. 对于两个不相交的轮换 σ_1 和 σ_2，σ_1 作用在 σ_2 作用的文字上时是恒等置换，同理 σ_2 作用在 σ_1 作用的文字上时也是恒等置换，而恒等置换与置换的乘积是可换的，于是不相交轮换的乘积可换. 对于多个不相交的轮换，以此类推即可. □

定理 8.2. S_n 中任一置换都可表为若干不相交轮换的乘积.

证明. 设 $a \in \{1, 2, \cdots, n\}$，置换 σ 作用到 a 上得到一些不同的文字.

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

假设 $\sigma^m(a)$ 与前面某一文字 $\sigma^k(a)$ 重复，那么 $k=0$，否则 $\sigma^{k-1}(a)=\sigma^{m-1}(a)$ 从而矛盾. 于是置换 σ 在 a 上的作用等同于轮换

$$\sigma_1=(a\sigma(a)\sigma^2(a)\cdots\sigma^m(a)),$$

下面考虑 $b\in\{1,2,\cdots,n\}\setminus\{a,\sigma(a),\cdots\sigma^m(a)\}$，得到轮换

$$\sigma_2=(b\sigma(b)\cdots\sigma^l(b)),$$

这里 σ_1 和 σ_2 是不相交的轮换. 以此类推，可以通过有限次操作取遍 $\{1,2,\cdots,n\}$ 中的元素. 于是任一置换可以表为若干不相交轮换的乘积. □

命题 8.4. 任一个 r-轮换都可以写成 $r-1$ 个对换的乘积.

证明. $(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)$. □

命题 8.5. 任一置换都可以表为一些对换的乘积，这些对换的表示不一定唯一，但对换个数的奇偶性不变.

证明. 由定理8.2，任一置换可以表示为若干不相交轮换的乘积，而任一轮换可以写成对换的乘积，因此任一置换都可以表为一些对换的乘积. 对换的表示不唯一，因为对任一对换的乘积，乘以 $(i_ji_k)(i_ki_j)$ 之后仍然不变. 对换的表示改变了，但对换个数的奇偶性没有变. □

对换的表示并不是置换的本质，对换个数的奇偶性才是，于是有奇置换与偶置换的概念.

定义 8.7 (奇置换与偶置换). 可以表为奇数个对换的乘积的置换称为**奇置换**，可以表为偶数个对换的乘积的置换称为**偶置换**.

下面是奇置换与偶置换的一些简单性质，这与整数的奇偶性可以类比.

性质 8.1. 两个奇置换之积是偶置换，两个偶置换之积是奇置换. 奇置换与偶置换之积是奇置换，偶置换与奇置换之积是奇置换. 置换的逆不改变置换的奇偶性.

定义 8.8 (交错群). 按照群的定义可以验证，n 元偶置换全体对置换的乘法构成群，称为 n 元**交错群**，记作 A_n.

命题 8.6. $A_n\lhd S_n$，$|A_n|=n!/2$.

证明. 对任意 $\sigma\in A_n$，$\varphi\in S_n$，$\varphi\sigma\varphi^{-1}\in A_n$，因此 $A_n\lhd S_n$. 而 A_n 中不是奇置换就是偶置换. 对任意 $\sigma\in S_n$，映射 $\sigma\to(1,2)\sigma$ 建立了一个奇置换与偶置换之间的双射，于是 $|A_n|=n!/2$. □

命题 8.7. 设置换 $\sigma=\sigma_1\sigma_2\cdots\sigma_n$ 表示为 n 个不相交的轮换的乘积，其中 σ_i 是 r_i-轮换，则 σ 的阶为 $[r_1,r_2,\cdots,r_n]$.

证明. 设 $|\sigma| = d$，$m = [r_1, r_2, \cdots, r_n]$，则通过展开即可得 $\sigma^m = \mathrm{id}$，于是 $d \mid m$.

已知 $\sigma^d = \mathrm{id}$，所以对每个 i，有 $\sigma_i^d = \mathrm{id}$. 而 σ_i 是一个 r_i-轮换，其阶为 r_i，因此 $r_i \mid d$. 所以 d 是 r_i 的公倍数，所以 $m \mid d$. □

定义 8.9 (自同构群)**.** 群 G 到自身的同构映射称为它的一个**自同构**，全体自同构组成的集合对映射的复合作成群，称为 G 的**自同构群**，记作 $\mathrm{Aut}G$.

同构映射是双射，因此 $\mathrm{Aut}G < S_G$.

定义 8.10 (内自同构群)**.** 设 G 是群，给定 $a \in G$，定义映射 $\sigma_a : G \to G,\ g \mapsto aga^{-1}$，则映射 $\sigma_a \in \mathrm{Aut}G$，称为由 a 决定的**内自同构**. 记

$$\mathrm{Inn}G = \{\sigma_a \mid a \in G\},$$

则 $\mathrm{Inn}G \lhd \mathrm{Aut}G$，称为 G 的**内自同构群**.

证明. 对任意 $g \in G$，$(\sigma_{a^{-1}})\sigma_a(g) = a^{-1}aga^{-1}a = g$. 因此 $\sigma_{a^{-1}}$ 是 σ_a 的逆映射，σ_a 是双射. 又对任意 $g_1, g_2 \in G$，

$$\sigma_a(g_1g_2) = ag_1g_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = \sigma_a(g_1)\sigma_a(g_2),$$

于是 σ_a 是同构，$\sigma_a \in \mathrm{Aut}G$.

于是 $\mathrm{Inn}G \subset \mathrm{Aut}G$. 对任意 $a, b \in G$，任意 $g \in G$，有

$$\sigma_a\sigma_b(g) = \sigma_a(bgb^{-1}) = abgb^{-1}a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g) \in \mathrm{Inn}G,$$

于是 $\mathrm{Inn}G < \mathrm{Aut}G$. 对任意 $\sigma_a \in \mathrm{Inn}G$，$\varphi \in \mathrm{Aut}G$，有

$$\varphi\sigma_a\varphi^{-1}(g) = \varphi(a\varphi^{-1}(g)a^{-1}) = \varphi(a)\varphi\varphi^{-1}(g)\varphi(a^{-1}) = \sigma_{\varphi(a)}(g) \in \mathrm{Inn}G,$$

故 $\mathrm{Inn}G \lhd \mathrm{Aut}G$. □

9 群作用

定义 9.1 (群作用)**.** 设 G 是群，X 是非空集合. 定义映射 $G \times X \to X,\ (g, x) \mapsto g \cdot x$，若满足

1. 幺元：$e \cdot x = x$;

2. 兼容性：对任意 $g_1, g_2 \in G$，$(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$,

则称映射“$\cdot$”为 G 在 X 上的一个**作用**.

群作用由公理化的定义有些抽象，下面建立群作用和置换之间的联系，也可看作是群作用的另一种定义.

定理 9.1. 设 G 是群，X 是非空集合，映射 $\varphi: G \to S_X$，$g \mapsto \varphi_g$. 则 φ 是同态当且仅当 φ 给出了一个群 G 在集合 X 上的群作用.

证明. 必要性：定义映射 $\cdot: G \times X \to X$，$(g, x) \mapsto \varphi_g(x)$，这里 $\varphi_g \in S_X$ 是同态. 下面证明"$\cdot$"是群作用.

对任意 $g \in G$，$e \in G$ 是幺元，则

$$\varphi_{ge} = \varphi_g \varphi_e = \varphi_g,$$

于是 $\varphi_e = \mathrm{id}$. 则对任意 $x \in X$，

$$e \cdot x = \varphi_e(x) = \mathrm{id}(x) = x.$$

对任意 $g_1, g_2 \in G$，有

$$(g_1 g_2) \cdot x = \varphi_{g_1} \varphi_{g_2}(x) = \varphi_{g_1}(\varphi_{g_2}(x)) = g_1 \cdot (g_2 \cdot x).$$

于是"$\cdot$"是群作用.

充分性：定义映射 $\varphi_g: X \to X$，$\varphi_g(x) \mapsto g \cdot x$，先证明 φ_g 是置换.

对任意 $x_1, x_2 \in X$，若 $\varphi_g(x_1) = \varphi_g(x_2)$，则 $g \cdot x_1 = g \cdot x_2$，用 g^{-1} 作用，得

$$g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2),$$

由兼容性公理得 $x_1 = x_2$，故 φ_g 是单射.

而 $\varphi_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = e \cdot x = x$，故对所有 $x \in X$，都存在原像 $g^{-1} \cdot x$，于是 φ_g 是满射.

因此 φ_g 是置换. 定义映射 $\varphi: G \to S_X$，$g \mapsto \varphi_g$，下面证明 φ 是同态.

对任意 $g_1, g_2 \in G$，任意 $x \in X$，有

$$\varphi_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \varphi_{g_1} \cdot (\varphi_{g_2}(x)) = \varphi_{g_1} \varphi_{g_2}(x),$$

于是 φ 是同态. □

定义 9.2 (轨道)**.** 设 G 是群，X 是非空集合. 对任意给定的 $x \in X$，称集合 $\{g \cdot x \mid \forall g \in G\}$ 为 x 的**轨道**，记作 $\mathrm{Orb}(x)$.

轨道就是在群 G 的作用下，x 所能到达的所有取值的集合.

定理 9.2. 设群 G 作用在集合 X 上. 定义关系 $xRy \iff \exists g \in G, y = g \cdot x$，则 R 是等价关系，且 x 所在的等价类是 $\mathrm{Orb}(x)$.

证明. R 是等价关系由反身性、对称性、传递性验证即可. 由 R 的定义可知 x 所在的等价类为 $\mathrm{Orb}(x)$. □

注. *由此，群 G 作用在集合 X 上，可将 X 分为若干轨道的无交并.*

定义 9.3 (稳定化子)**.** 设 G 是群，X 是非空集合. 对任意给定的 $x \in X$，集合 $\{g \mid g \cdot x = x\}$ 关于群 G 的运算构成群，称为 x 的**稳定化子**或**迷向子群**，记作 $\mathrm{Stab}(x)$.

也就是说，群 G 中有一些元素，作用在 x 上，得到的还是 x 自身. 例如 $e \in G$，$e \cdot x = x$. 下面证明 $\mathrm{Stab}(x) < G$.

证明. 已知 $\mathrm{Stab}(x) \subset G$. 对任意 $g_1, g_2 \in \mathrm{Stab}(x)$，

$$e \cdot x = (g_2^{-1} g_2) \cdot x = g_2^{-1} \cdot (g_2 \cdot x) = g_2^{-1} \cdot x = x.$$

于是

$$(g_1 g_2^{-1}) \cdot x = g_1 \cdot (g_2^{-1} \cdot x) = g_1 \cdot x = x.$$

故 $g_1 g_2^{-1} \in \mathrm{Stab}(x)$，由子群的充要条件，$\mathrm{Stab}(x) < G$. □

定义 9.4 (不动点)**.** 设群 G 作用在集合 X 上，集合 $\{x \mid g \cdot x = x, \forall g \in G\}$ 称为 X 在群 G 作用下的**不动点**.

定义 9.5 (齐性空间)**.** 若群 G 作用在集合 X 上，对任意 $x, y \in X$，都有 $g \in G$ 满足 $g \cdot x = y$，则称这个作用是**可传递**的或**可迁**的，集合 X 称为**齐性空间**.

注. *群 G 在每个轨道 $\mathrm{Orb}(x)$ 上的作用是可传递的.*

定义 9.6. 若对任意 $x \in X$，$\mathrm{Stab}(x) = e$，则称 G 的作用是**自由的**.

定义 9.7. 若对任意 $g \neq e$，存在 $x \in X$ 使得 $g \cdot x \neq x$，则称 G 的作用是**忠实的**或**有效的**.

定义 9.8. 若对任意 $g \in G$，$x \in X$，都有 $g \cdot x = x$，则称 G 的作用是**平凡的**.

定理 9.3 (轨道-稳定化子定理)**.** 设 $G/\mathrm{Stab}(x)$ 是 G 关于 $\mathrm{Stab}(x)$ 的左陪集空间，则存在双射 $\varphi : \mathrm{Orb}(x) \to G/\mathrm{Stab}(x)$. 特别地，当 G 是有限群时，有 $|G| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)|$.

证明. 设 $\varphi : \mathrm{Orb}(x) \to G/\mathrm{Stab}(x)$, $g \cdot x \mapsto g\mathrm{Stab}(x)$. 设 $g \cdot x = h \cdot x$，则 $(h^{-1}g) \cdot x = x$，于是 $h^{-1}g \in \mathrm{Stab}(x)$，$h\mathrm{Stab}(x) = g\mathrm{Stab}(x)$，所以 φ 是映射.

对于任一 $g\mathrm{Stab}(x)$，都有原像 $g \cdot x$，故 φ 是满射.

对任意 $g_1 \cdot x, g_2 \cdot x \in \mathrm{Orb}(x)$，若 $\varphi(g_1 \cdot x) = \varphi(g_2 \cdot x)$，则 $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$，$g_2^{-1} g_1 \in \mathrm{Stab}(x)$，于是 $g_2^{-1} g_1 \cdot x = x$，于是 $g_1 \cdot x = g_2 \cdot x$，$\varphi$ 是单射.

于是 φ 是双射，有 $|\mathrm{Orb}(x)| = |G\mathrm{Stab}(x)| = [G : \mathrm{Stab}(x)]$. 特别地，当 G 有限时，由 Lagrange 定理，有 $|G| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)|$. □

可以把群作用推广到集类上.

定义 9.9. 设 G 是群，$\mathcal{X}$ 是非空集类，定义映射 $G\times\mathcal{X}\to\mathcal{X}$, $(g,H)\mapsto g\cdot H$，若满足

1. 幺元：$e\cdot H=H$;

2. 兼容性：对任意 $g_1,g_2\in G$，$(g_1g_2)\cdot H=g_1\cdot(g_2\cdot H)$,

则称映射“$\cdot$”为 G 在 $\mathcal{X}$ 上的一个**作用**.

定义 9.10 (共轭作用)**.** 若群 G 作用在自身，对任意 $g,x\in G$，有

$$g\cdot x=gxg^{-1},$$

可以验证这是一个作用，称为**共轭作用**.

现在可以用群作用的语言来描述共轭类、共轭子群、中心化子以及正规化子的概念.

定义 9.11 (共轭类)**.** 设群 G 到自身有共轭作用，则对任意 $x\in G$，称 $\mathrm{Orb}(x)$ 为 x 所在的**共轭类**.

定义 9.12 (共轭子群)**.** 设 $H<G$，则称 $g\cdot H=gHg^{-1}$ 为 H 在 G 作用下的**共轭子群**.

定义 9.13 (中心化子)**.** $x\in G$ 在共轭作用下的稳定化子 $\mathrm{Stab}(x)$ 称为 x 在 G 中的**中心化子**，记作 $C_G(x)$.

定义 9.14 (中心)**.** 群 G 中所有元素的中心化子的交称为群 G 的**中心**，即与 G 中所有元素都共轭的元素组成的集合，记作 $C_G(G)$.

定义 9.15 (正规化子)**.** $H<G$ 在共轭作用下的稳定化子 $\mathrm{Stab}(H)$ 称为 H 在 G 中的**正规化子**，记作 $N_G(H)$.

定义 9.16 (类方程)**.** 由于群 G 可以划分为若干共轭类，即

$$G=\bigsqcup_{i\in I}C(x_i),$$

其中 $C(x_i)$ 为以 x_i 为代表元的共轭类. 即 $C(x_i)=\mathrm{Orb}(x_i)$. 对任意 $z\in C_G(G)$，任意 $g\in G$，都有 $z=gzg^{-1}$，即 $|C(z)|=1$. 则

$$|G|=\sum_{i\in I}|C(x_i)|=|C_G(G)|+\sum_{i\in I'}|C(x_i)|=|C_G(G)|+\sum_{i\in I'}\frac{|G|}{|C_G(x_i)|}. \tag{1}$$

其中 $C_G(G)=\{x_i\mid i\in I\backslash I'\}$. 称方程 (1) 为**类方程**.

例 9.1. 考虑对称群 S_3，$|S_3|=6$. 它的共轭类有 $\{e\}$，$\{(12),(13),(23)\}$ 以及 $\{(123),(132)\}$. 于是

$$6=1+3+2.$$

10 Sylow 子群

定义 10.1 (p-群)**.** 设 G 是有限群，p 是素数，若 $|G|=p^k, k\in\mathbb{N}^+$，则称 G 是一个 ***p*-群**.

引理 10.1. 设 p-群 G 作用在集合 X 上，若 $|X|=n$，X 中的不动点个数为 t ($t\in\mathbb{N}$)，则

(1) $t\equiv n \pmod p$;

(2) 若 $(n,p)=1$，则不动点存在.

证明. (1) 设 $X=\bigsqcup\limits_{i\in I}\mathrm{Orb}(x_i)$. x_i 为不动点当且仅当 $|\mathrm{Orb}(x_i)|=1$，于是

$$n=t+\sum_{|\mathrm{Orb}(x_i)\neq 1|}|\mathrm{Orb}(x_i)|.$$

而由轨道-稳定化子定理，$|\mathrm{Orb}(x_i)|$ 能整除 $|G|$，而 $|G|=p^k$ ($k\in\mathbb{N}^+$)，于是 p 能整除 $|\mathrm{Orb}(x_i)|$. 故 $t\equiv n \pmod p$.

(2) 若 $(n,p)=1$，则 $n\nmid p$，由 (1)，得 $t\nmid p$，则 $t\neq 0$，即存在不动点. □

引理 10.2. 在正整数中，设 p 是素数，$n=p^l m$，若 $k\leqslant l$，则 p^{l-k} 恰能整除 $\mathrm{C}_n^{p^k}$.

证明. 由组合数公式，

$$\mathrm{C}_n^{p^k}=\frac{n}{p^k}\prod_{i=1}^{p^k-1}\frac{n-i}{p^k-i},$$

而

$$\frac{n}{p^k}=p^{l-k}m\Rightarrow p^{l-k}\mid \mathrm{C}_n^{p^k},$$

设 $1\leqslant i\leqslant p^k-1$ 表示为 $i=p^t j$，其中 $(p,j)=1$，$t<k\leqslant l$. 则

$$n-i=p^t\left(p^{l-t}m-j\right),$$

$$p^k-i=p^t\left(p^{k-t}-j\right),$$

于是 $p\nmid\prod\limits_{i=1}^{p^k-1}\dfrac{n-i}{p^k-i}$，故 p^{l-k} 恰能整除 $\mathrm{C}_n^{p^k}$. □

下面若无特殊说明，默认 G 的阶为 $p^l m$，其中 p 为素数，$(p,m)=1$，$l\geqslant 1$.

定理 10.1 (Sylow 第一定理，存在性)**.** 若 $1\leqslant k\leqslant l$，则 G 存在 p^k 阶子群.

证明. 设 G 中所有 p^k 阶子集组成的集合为 $\mathcal{X}$. 则 $|\mathcal{X}|=\mathrm{C}_n^{p^k}$，这里 $n=p^l m$. 设 G 作用在 $\mathcal{X}$ 上，则有轨道分解

$$\mathcal{X}=\bigsqcup_{i\in I}\mathrm{Orb}(A_i),\quad A_i\in\mathcal{X}.$$

于是

$$|\mathcal{X}|=\sum_{i\in I}|\mathrm{Orb}(A_i)|.$$

由引理10.2，存在 $A\in\mathcal{X}$，$p^{l-k+1}\nmid|\mathrm{Orb}(A)|$. 由轨道-稳定化子定理，

$$p^{l-k+1}\nmid\frac{|G|}{|\mathrm{Stab}(A)|}\Rightarrow p^{l-k+1}\nmid\frac{p^l m}{|\mathrm{Stab}(A)|}.$$

设 $|\mathrm{Stab}(A)|=p^a b$，其中 $(a,b)=1$. 则 $p^{l-a}<p^{l-k+1}$，即 $a>k-1$，$a\geqslant k$. 于是 $p^k\mid|\mathrm{Stab}(A)|$.

由于 $\mathrm{Stab}(A)<G$，对任意 $g\in\mathrm{Stab}(A),a\in A$，定义群 $\mathrm{Stab}(A)$ 对集合 A 的作用 $g\cdot a=ga$. 由于 $\mathrm{Stab}(A)=\{g\in G\mid g\cdot a=a,\ \forall a\in A\}$，于是 $ga\in A$. 则 $\mathrm{Stab}(A)\cdot a\subset A$. 而 $\mathrm{Stab}(A)$ 到 $\mathrm{Stab}(A)\cdot a$ 之间是双射，于是 $|\mathrm{Stab}(A)|=|\mathrm{Stab}(A)\cdot a|\leqslant|A|=p^k$. 即 $\mathrm{Stab}(A)$ 是一个 p^k 阶子群. □

定义 10.2 (Sylow p-子群). 设 G 的阶是 $p^l m$，其中 p 是素数，则 G 的 p^l 阶子群称为 G 的 **Sylow p-子群**.

定理 10.2 (Sylow 第二定理，共轭性). 设 P 是 G 的一个 Sylow p-子群，H 是 P 的一个 p^k 阶子群，则 H 包含于 P 的共轭子群中. 特别地，Sylow p-子群之间互相共轭.

证明. 设 G 作用在 G/P 上，$g\cdot gP=ggP$，称为左平移作用. 将这个作用限制在 H 上，则 $h\cdot gP=hgP$. 由于 $|G/P|=m$，$(m,p)=1$，由引理10.1(2)，存在 $gP\in G/P$ 满足 $hgP=gP$. 于是 $hg\in gP$，即 $h\in gPg^{-1}$，H 包含于 P 的共轭子群中. 特别地，当 $|H|=p^l$，则 P 也包含在 H 的共轭子群中，于是 $H=gPg^{-1}$. □

定理 10.3 (Sylow 第三定理，计数定理). 设 G 的 Sylow p-子群的个数为 k，则

(1) 当且仅当 $k=1$ 时，这个 Sylow p-子群 $P\lhd G$;

(2) $k\equiv 1\pmod p$ 且 $k\mid m$.

证明. (1) 设 P 是群 G 的一个 Sylow p-子群. 若 P' 是另外一个 Sylow p-子群，则由 Sylow 第二定理，有 $P'\subset\{gPg^{-1}\mid g\in G\}$，同时有 $P\subset\{gP'g^{-1}\mid g\in G\}$. 若 $k=1$，则 $P=gPg^{-1}$，对任意 $g\in G$ 成立，于是 $P\lhd G$. 反之，若 $P\lhd G$，则 $P=gPg^{-1}$，得 $k=1$.

(2) 设 $\mathcal{X}$ 是群 G 的所有 Sylow p-子群的集合，群 $P\in\mathcal{X}$ 作用在集合 $\mathcal{X}$ 上的作用为共轭作用. 对任意 $g\in P$，

$$g\cdot P=gPg^{-1}=P,$$

因此 P 是该作用下的一个不动点. 假设 P_1 也是一个不动点，则对任意 $g\in P$，

$$gP_1g^{-1}=P_1,$$

因此 $g \in N_G(P_1)$，$P \subset N_G(P_1)$. 而 $|P| = p^l$，于是设 $|N_G(P_1)| = p^l m_1$，其中 $m_1 \mid m$. 于是 P, P_1 都是 $N_G(P_1)$ 的 Sylow p-子群，而 $P_1 \lhd N_G(P_1)$，由 (1)，得 $k = 1$，即 $P = P_1$，该作用下只有一个不动点. 由引理10.1(1)，有 $k \equiv 1 \pmod p$.

设群 G 在集合 $\mathcal{X}$ 上的作用为共轭作用. 则由 Sylow 第二定理，对任意 $P_1, P_2 \in \mathcal{X}$，存在 $g \in G$，使得

$$P_1 = g \cdot P_2 = gP_2g^{-1},$$

于是 $\mathcal{X}$ 是可传递的. 对任意 $P \in \mathcal{X}$，

$$k = |\mathcal{X}| = |\mathrm{Orb}(P)| = \frac{|G|}{|\mathrm{Stab}(P)|},$$

于是 $k \mid |G|$，即 $k \mid p^l m$. 而由于 $k \equiv 1 \pmod p$，于是 $(k, p) = 1$，则 $k \mid m$. □

下面介绍 Sylow 定理的若干应用.

定义 10.3 (单群)**.** 没有非平凡正规子群的群称为**单群**。

例 10.1. 72 阶群不是单群.

证明. 首先，$72 = 2^3 \times 3^2$，设有限群 G 的阶 $|G| = 72$，设 G 的 Sylow 2-子群的个数为 k_1，Sylow 3-子群的个数为 k_2. 由 Sylow 第三定理，k_1 可能为 $1, 3, 9$，k_2 可能为 $1, 4$.

当 $k_1 = 1$ 时，由 Sylow 第三定理 (1)，这个 8 阶的 Sylow 2-子群是 G 的正规子群. 当 $k_2 = 1$ 时，这个 9 阶的 Sylow 3 子群也是 G 的正规子群. 它们都不是平凡的.

当 $k_2 = 4$ 时，设 $X = \{P_1, P_2, P_3, P_4\}$，其中 P_i 是互不相同的 Sylow 3-子群. 设 G 作用在 X 上的作用为共轭作用. 即

$$g \cdot P_i = gP_ig^{-1},\ \forall g \in G,$$

则这个作用决定了一个同态 $\varphi : G \to S_X$.

而 $\ker\varphi \lhd G$，假设 $\ker\varphi = G$，则对任意 $g \in G$，

$$g \cdot P_i = \mathrm{id}(P_i) = P_i,$$

则 Sylow 子群之间不能互相共轭，这与 Sylow 第二定理矛盾.

假设 $\ker\varphi = \{e\}$，则由同态基本定理，

$$G/\ker\varphi \cong \varphi(G),$$

于是

$$|G/\ker\varphi| = |G/e| = |G| = |\varphi(G)| < |S_4| = 24,$$

而 $|G| = 72$，矛盾.

于是 $\ker\varphi$ 是 G 的非平凡正规子群，故 72 阶群不是单群. □

例 10.2. 56 阶群不是单群.

证明. 首先，$56 = 2^3 \times 7$，设有限群 G 的阶 $|G| = 56$，设 G 的 Sylow 2-子群的个数为 k_1，Sylow 7-子群的个数为 k_2. 由 Sylow 第三定理，k_1 可能为 $1, 7$，k_2 可能为 $1, 8$.

当 $k_1 = 1$ 时，由 Sylow 第三定理 (1)，这个 8 阶的 Sylow 2-子群是 G 的正规子群. 当 $k_2 = 1$ 时，这个 7 阶的 Sylow 7-子群也是 G 的正规子群. 它们都不是平凡的.

当 $k_1 = 7$ 且 $k_2 = 8$ 时，由于素数阶群必为循环群，于是这 8 个 Sylow 7-子群中，除幺元外的 6 个元素都是 7 阶的，且各不相同. 于是一共含有 $|G|$ 中的 $1 + 6 \times 8 = 49$ 个元素. 对任意的一个 Sylow 2-子群，除幺元外含有 7 个元素，且与 Sylow 7-子群中的元素不同. 这就有 $49 + 7 = 56$ 个元素. 而这 7 个 Sylow 2-子群元素不是完全一致的，于是 Sylow 7 子群和 Sylow 8 子群中不重复的元素个数就超过了 56，这与 $|G| = 56$ 矛盾！于是 $k_1 = 1$ 或 $k_2 = 1$，则由上述可知 56 阶群不是单群. □

例 10.3. 设 $|G| = p^l m$，$(p, m) = 1$，$p > m \neq 1$，则 G 是单群.

证明. 设 G 的 Sylow p-子群的个数为 k，由 Sylow 第三定理，k 的取值只能为 1. 而 $m > 1$，于是 G 的 Sylow p-子群是 G 的 p^l 阶真正规子群. □

注. *k 的取值只能为 1，因为当 k 取 $1 + p$ 时，$1 + p > m$ 于是不能整除. 那么其他取值更不能取到了.*

11　群的直积

定义 11.1 (群的扩张). 设 G, A, B 是群，若有 $N \lhd G$，使得 $A \cong N$，$B \cong G/N$，则称群 G 是 B 过 A 的**扩张**. 称 N 为**扩张核**.

注. *群的扩张与域的扩张完全不同，域从子域扩成扩域，而群不一定是子群，甚至不一定和子群同构.*

定义 11.2 (正合序列). 设 $G_1, G_2, \cdots, G_n$ 是群，有同态映射如下，

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} G_n$$

且满足 $f_i(G_i) = \ker f_{i+1}$，则称这个序列为**正合序列**.

注. *这里群的个数可以是有限的，也可以是无限的.*

定义 11.3 (短正合序列). 设 1 是 A 的幺元，$1'$ 是 B 的幺元，则正合序列

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

称为**短正合序列**.

注. 不难看出，λ 是单射，μ 是满射. 这是短正合序列的本质体现. 因此在书写上，可简写为

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$$

定理 11.1. 设 G, A, B 是群，则 G 是 B 过 A 的扩张当且仅当存在短正合序列

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$$

证明. 必要性：设存在 $N \lhd G$，使得 $A \cong N$，$B \cong G/N$. 设同构映射 $f : A \to N$，$h : G/N \to B$，把 f 开拓到 λ，则 λ 是单同态. 设 $\mu = h \circ \pi$，则 μ 是满同态. 于是存在短正合序列.

充分性：设存在短正合序列

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$$

则 λ 是单同态，μ 是满同态. 且

$$\lambda(A) = \ker \mu \lhd G.$$

设 $N = \ker \mu$，而 $\lambda : A \to \lambda(A)$ 是单同态，又是满射，于是 λ 是同构，$A \cong \lambda(A) = N$.

对于满同态 $\mu : G \to B$，由同态基本定理，有 $G/\ker \mu \cong B$，于是 $G/N \cong B$. 因此 G 是 B 过 A 的扩张. □

定理 11.2. 设 G, G', A, B 是群.

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

2. 若 G 和 G' 都是 B 过 A 的扩张，且存在同态 $f : G \to G'$，使下图交换，则 f 是同构映射. 称 G 和 G' 是 B 过 A 的**等价扩张**.

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

证明. 1. 由于 G 是 B 过 A 的扩张，于是有短正合序列

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1$$

设 $f : G \to G'$ 是同构，则 $f \circ \lambda : A \to G'$ 是单同态，$\mu \circ f^{-1}$ 是满同态，且 $f \circ \lambda(A) = f(\ker \mu) = \ker \mu f^{-1}$，于是 G' 是 B 过 A 的扩张.

2. 先证 f 是单射. 只需证明 $\ker f = \{e\}$，这里 e 是 G 的幺元，并设 e' 是 G' 的幺元. 设 $f(x) = e'$，下证 $x = e$.

由交换图，

$$\mu(x) = \mu' f(x) = \mu'(e') = 1,$$

于是 $x \in \ker\mu = \lambda(A)$，存在 $a \in A$ 使 $x = \lambda(a)$，即

$$e' = f(x) = f\lambda(a) = \lambda'(a),$$

又 λ 是单射，于是 $a = 1$，$x = \lambda(1) = e$.

再证 f 是满射. 对任意 $x' \in G'$，由 μ 是满射，$\mu(G) = B$，则存在 $x \in G$，使得 $\mu(x) = \mu'(x')$. 即

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

于是

$$\mu'\left(x'[f(x)]^{-1}\right) = \mu'(e') = 1,$$

即

$$x' f(x)^{-1} \in \ker\mu' = \lambda'(A) = f\lambda(A) \subset f(G),$$

于是 $x' \in f(G)f(x) \subset f(G)$. □

注. *1* 的证明中，用了两次扩张的充要条件，即定理*11.1*. 对于 $f(\ker\mu) = \ker\mu f^{-1}$，可以由核的定义以及集合的包含关系证得.

定义 11.4 (内直积)**.** 设 G 是 B 过 A 的扩张，N 为扩张核，若存在 $H < G$，使得 $H \cap N = \{e\}$ 且 $G = HN$，则称此扩张为**非本质扩张**，G 称为 N 与 H 的**半直积**，记作 $G = H \ltimes N$. 进一步，若 $H \lhd G$，则称这种扩张为**平凡扩张**，G 是 N 与 H 的**内直积**，记作 $G = H \otimes N$.

注. 对非本质扩张，有 $B \cong H$. 因为

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

例 11.1. 设 $G = (\mathbb{Z}, +)$，$A = N = 2\mathbb{Z} \lhd \mathbb{Z}$，$B = G/N = \mathbb{Z}_2$，则 G 是 B 过 A 的扩张. 由于不存在子群 $H \cong B = \mathbb{Z}_2$，于是这个扩张不是非本质扩张.

定理 11.3. 设 $A < G$，$B < G$，则

1. $G = AB$ 且 $A \cap B = \{e\}$ 当且仅当对任意 $g \in G$，存在唯一 $a \in A, b \in B$ 使得 $g = ab$.
2. 若 $G = AB$ 且 $A \cap B = \{e\}$，则 A, B 都是 G 的正规子群的充要条件为对任意 $a \in A, b \in B, ab = ba$. 此时 $G = A \otimes B$.

证明. 1. 必要性：由 $G = AB$，对任意 $g \in G$，存在 $a \in A, b \in B$ 使得 $g = ab$，假设另有 $a' \in A, b' \in B$ 使得 $g = a'b'$，则 $ab = a'b'$，$bb'^{-1} = a^{-1}a' = e$，于是 $a = a', b = b'$.

充分性：若对任意 $g \in G$，存在唯一 $a \in A, b \in B$ 使得 $g = ab$，则 $G = AB$. 若 $c \in A \cap B$，则 $c = ec = ce$，于是 $c = e$.

2. 必要性：若 $A \lhd G$，则 $bab^{-1} \in A$，于是 $a^{-1}bab^{-1} \in A$. 又 $B \lhd G$，则 $a^{-1}ba \in B$，于是 $a^{-1}bab^{-1} \in B$，故 $a^{-1}bab^{-1} \in A \cap B$. 于是 $a^{-1}bab^{-1} = e$，$ba = ab$.

充分性：若对任意 $a \in A$，$b \in B$ 有 $ab = ba$，由于 $G = AB$，对任意 $g \in G$，存在 $a \in A, b \in B$ 使得 $g = ab$，于是对任意 $a_0 \in A$，

$$ga_0g^{-1} = aba_0b^{-1}a^{-1} = aa_0bb^{-1}a^{-1} = aa_0a^{-1} \in A,$$

于是 $A \lhd G$，同理 $B \lhd G$. □

可以将内直积的概念推广到多个正规子群的情况.

定义 11.5. 设 $N_1, N_2, \cdots, N_k$ 是 G 的正规子群. 若 G 中任意元素分解为 N_i 中元素的乘积是唯一的，则称 G 是 $N_1, N_2, \cdots, N_k$ 的内直积，记作

$$G = N_1 \otimes N_2 \otimes \cdots \otimes N_k = \bigotimes_{i=1}^{k} N_i.$$

以上讨论了一个群的内直积分解，下面说明两个群的内直积总是存在且唯一.

定义 11.6 (外直积)**.** 设 A, B 是两个群，定义集合 $G = \{(a, b) \mid a \in A, b \in B\}$，定义 G 中元素的运算 $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. 则可验证 G 关于上述运算构成群，称为 A 和 B 的**外直积**，记作 $G = A \times B$.

定理 11.4. 设 A 和 B 是两个群，则一定存在 B 过 A 的平凡扩张 G，且 G 在同构意义下唯一.

证明. 设 $G = A \times B$，则 G 是群. 记 $A' = \{(a, 1') \mid a \in A\}$，$B' = \{(1, b) \mid b \in B\}$，则可证 $A' \lhd G$，$B' \lhd G$，且 $G = A'B'$，$A' \cap B' = \{(1, 1')\}$.

由内直积定义，$G = A' \otimes B' = B' \otimes A'$. 则 G 是 B' 过 A' 的平凡扩张. 容易在 A 和 A'，B 和 B' 建立同构，即 $A \to A', a \mapsto (a, 1')$，$B \to B', b \mapsto (1, b)$，故 G 是 B 过 A 的平凡扩张.

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 $A \cong A_1$，$B \cong B_1$. 下证 $G \cong G_1$.

设 $f_1 : A \to A_1, a \mapsto a_1$，$f_2 : B \to B_1, b \mapsto b_1$ 是两个同构映射. 令 $f : G \to G_1, (a, b) \mapsto f_1(a)f_2(b)$. 下证 f 是同构.

因为 f_1 和 f_2 都是满射，于是对任意 $f_1(a)$ 和 $f_2(b)$ 都有原像 a 和 b. 于是 f 是满射.

假设 $f_1(a')f_2(b') = f_1(a)f_2(b)$，由于 G_1 是平凡扩张，因此分解是唯一的. $f_1(a') = f_1(a)$，$f_2(b') = f_2(b)$. 又因为 f_1 和 f_2 是单射，于是 $a' = a, b' = b$，$(a, b) = (a', b')$.

而

$$\begin{aligned} f\left((a, b)(a', b')\right) &= f\left((aa', bb')\right) = f_1(aa')f_2(bb') = f_1(a)f_1(a')f_2(b)f_2(b') \\ &= f_1(a)f_2(b)f_1(a')f_2(b') = f\left((a, b)\right) f\left((a', b')\right), \end{aligned}$$

于是 f 是同构映射. □

注. 外直积 $G=G_1\times G_2$ 中，G_1 和 G_2 一般不是 G 的子群，但是存在某个同构关系，使得 G_1，G_2 分别和 G 的两个子群同构. 而在内直积 $G=H\otimes N$ 中，H 和 N 都是 G 的正规子群. 内直积和外直积在本质上是一致的.

注. 上述定理实际上说明了对于 $G=A\times B$，存在 $A'\lhd G$，$B'\lhd G$ 且 $A'\cong A$，$B'\cong B$，使得 $G=A'\otimes B'$.

反之，对于 $G=A\otimes B$，它和外直积的关系如下.

定理 11.5. 若 $G=A\otimes B$，则 $A\times B\cong G$.

证明. 令 $f:A\times B\to G,(a,b)\mapsto ab$，容易判断这是良定义的. 对任意 $g\in G$，都有唯一 $a\in A$，$b\in B$ 使得 $g=ab$，于是 f 是满射. 对任意 $g_1=g_2$，有 $(a_1,b_1)=(a_2,b_2)$，于是 $a_1=a_2$，$b_1=b_2$，于是 f 是单射. 又

$$f\left((a_1,b_1)(a_2,b_2)\right)=f\left((a_1a_2,b_1b_2)\right)=a_1a_2b_1b_2=a_1b_1a_2b_2=f\left((a_1,b_1)\right)f\left((a_2,b_2)\right),$$

于是 f 是同构映射. □

下面介绍外直积的若干性质.

定理 11.6. 设 $G=A\times B$，则

1. G 是有限群当且仅当 A 和 B 都是有限群，且当 G 为有限群时，有 $|G|=|A||B|$.
2. G 是交换群当且仅当 A 和 B 都是交换群.
3. $A\times B\cong B\times A$.

证明. 1. 由 Cartesian 积的性质立即可得.

2. 若 G 是交换群，对任意 $a_1,a_2\in A$，$b_1,b_2\in B$ 有 $(a_1,b_1)(a_2,b_2)=(a_2,b_2)(a_1,b_1)$，即 $(a_1a_2,b_1b_2)=(a_2a_1,b_2b_1)$，于是 $a_1a_2=a_2a_1$，$b_1b_2=b_2b_1$. 反之，若 A 和 B 都是交换群，对任意 $(a_1,b_1),(a_2,b_2)\in G$，有

$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)=(a_2a_1,b_2b_1)=(a_2,b_2)(a_1,b_1),$$

于是 G 是交换群.

3. 设映射 $f:A\times B\to B\times A,(a,b)\mapsto(b,a)$，则这是良定义的，且是双射. 而

$$f\left((a_1,b_1)(a_2,b_2)\right)=f\left((a_1a_2,b_1b_2)\right)=(b_1b_2,a_1a_2)=(b_1,a_1)(b_2,a_2)=f\left((a_1,b_1)\right)f\left((a_2,b_2)\right),$$

于是 f 是同构映射. □

定理 11.7. 设 A,B 是群，$a\in A,b\in B$ 是两个有限阶元，则对 $(a,b)\in A\times B$，有

$$|(a,b)|=[|a|,|b|].$$

证明. 设 $|a|=m$，$|b|=n$，$|(a,b)|=t$，$[|a|,|b|]=s$. 则 $(a,b)^s=(a^s,b^s)=(e_1,e_2)$，于是 $t\mid s$. 又 $(e_1,e_2)=(a,b)^t=(a^t,b^t)$，于是 $a^t=e_1$，$b^t=e_2$，于是 $m\mid t$，$n\mid t$，而 $s=[m,n]$，于是 $s\mid t$，所以 $t=s$，即 $|(a,b)|=[|a|,|b|]$. □

12 可解群与幂零群

定义 12.1 (换位子)**.** 设 $g_1, g_2 \in G$，称

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

为 g_1 和 g_2 的**换位子**.

可见，换位子的作用是换位，即 $g_2 g_1 [g_1, g_2] = g_1 g_2$. 且有

$$[g_1, g_2] [g_2, g_1] = e.$$

即 $[g_2, g_1] = [g_1, g_2]^{-1}$.

定义 12.2 (换位子群)**.** 设 $H < G$，$K < G$，称

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

为 H 和 K 的**换位子群**.

可见，$[H, K] = [K, H]$.

性质 12.1. 设 $\alpha : G \to G_1$ 是同态，则

1. 对任意 $g_1, g_2 \in G$，$\alpha([g_1, g_2]) = [\alpha(g_1), \alpha(g_2)]$.
2. 对任意 $H < G$，$K < G$，$\alpha([H, K]) = [\alpha(H), \alpha(K)]$.

引理 12.1. 设 $H < G$，$K < G$，则

1. $[H, K] = \{1\} \iff H \subset C_G(K)$;
2. $[H, K] \subset K \iff H \subset N_G(K)$;
3. 若 $H \lhd G$，$G \lhd G$，则 $[H, K] \lhd G$ 且 $[H, K] \subset H \cap K$;
4. 若 $H_1 < H$，$K_1 < K$，则 $[H_1, K_1] < [H, K]$.

推论 12.1. 设 $H < G$，$K < G$，则

1. G 是交换群当且仅当 $[G, G] = \{1\}$;
2. $K \lhd G \iff [K, K] \lhd G$;
3. $[G, G] \lhd G$.

定义 12.3 (正规列). 设群 G 的幺元为 1，它的子群 G_i 有如下排列

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

且 $G_i \lhd G_{i-1}, 2 \leqslant i \leqslant t+1$，则称这个序列为**次正规列**. 若还有 $G_i \lhd G$，则称这个序列为**正规列**. 上述序列中有 t 个包含号，所以称序列的长度为 t. 称 G_i/G_{i-1} 为次正规序列的**因子**.

定义 12.4 (因子列). 次正规序列

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

的因子

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

称为次正规序列的**因子列**.

注. *因子列没有包含关系.*

定义 12.5 (加细). 设有两个次正规序列

$$G = G_1' \supset G_2' \supset \cdots \supset G_r' \supset G_{r+1}' = \{1\},$$

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

若对任意 G_i'，都有 $G_j = G_i'$，则称后者是前者作为次正规序列的**加细**.

注. *正规序列的加细也有类似的定义. 若正规序列加细后仍是正规序列，则称后者是前者作为正规序列的加细. 但是，若正规序列加细后不再是正规序列，则把这个正规序列看作次正规序列，后者是前者作为次正规序列的加细.*

定义 12.6 (导出列). 定义 $G^{(0)} = G$，$G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right], i \geqslant 1$，称序列

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

为 G 的**导出列**.

定义 12.7 (降中心列). 定义 $\varGamma_1(G) = G$，$\varGamma_i(G) = [G, \varGamma_{i-1}(G)], i \geqslant 2$，称序列

$$G = \varGamma_1(G) \supset \varGamma_2(G) \supset \cdots$$

为 G 的**降中心列**.

定义 12.8 (升中心列). 定义 $C_0(G) = \{1\}$，$C_i(G)/C_{i-1}(G) = C(G/C_{i-1}(G)), i \geqslant 1$，称序列

$$\{1\} = C_0(G) \subset C_1(G) \subset C_2(G) \subset \cdots$$

为 G 的**升中心列**.

注. *$C_i(G)$ 是存在的，可以写成显性表达式.*

定义 12.9 (可解群，幂零群). 设 G 是群，若有 k，使 $G^{(k)} = \{1\}$，则称 G 是**可解群**. 若有 k，使 $\varGamma_k(G) = \{1\}$，则称 G 是**幂零群**.