群的直积

定义 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 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 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 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 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

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

即

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

于是 $x' \in f(G) f(x) \subset f(G)$. $\square$

注. *1 的证明中，用了两次扩张的充要条件，即定理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 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 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 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 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 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 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 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 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. $\square$

定理 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

$$|(a, b)| = \left[|a|, |b|\right].$$

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