

0.1 群的直积

定义 0.1 (外直积)

设 G_1, G_2 是两个群, 构造集合 G_1 与 G_2 的笛卡尔积

$$G = \{(a_1, a_2) \mid a_1 \in G_1, a_2 \in G_2\},$$

并在 G 中定义乘法运算

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2), \quad (a_1, a_2), (b_1, b_2) \in G,$$

则 G 关于上述定义的乘法构成群, 称为群 G_1 与 G_2 的**外直积**, 记作 $G = G_1 \times G_2$.



注

- (1) 如果 e_1, e_2 分别是群 G_1 和 G_2 的单位元, 则 (e_1, e_2) 是 $G_1 \times G_2$ 的单位元;
- (2) 设 $(a_1, a_2) \in G$, 则 $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$;
- (3) 当 G_1 和 G_2 都是加群时, G_1 与 G_2 的外直积也可记作 $G_1 \oplus G_2$.

定理 0.1

设 $G = G_1 \times G_2$ 是群 G_1 与 G_2 的外直积, 则

- (1) G 是有限群的充分必要条件是 G_1 与 G_2 都是有限群. 并且, 当 G 是有限群时, 有

$$|G| = |G_1| \cdot |G_2|;$$

- (2) G 是交换群的充分必要条件是 G_1 与 G_2 都是交换群;
- (3) $G_1 \times G_2 \cong G_2 \times G_1$.



证明

- (1) 由笛卡尔积的定义易得.
- (2) 如果 G_1 与 G_2 都是交换群, 则对任意的 $(a_1, a_2), (b_1, b_2) \in G$, 有

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2) = (b_1, b_2) \cdot (a_1, a_2),$$

所以 G 是交换群.

反之, 如果 G 是交换群, 那么对任意的 $a_1, b_1 \in G_1, a_2, b_2 \in G_2$, 有

$$(a_1, a_2) \cdot (b_1, b_2) = (b_1, b_2) \cdot (a_1, a_2),$$

即

$$(a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2).$$

因此 $a_1 b_1 = b_1 a_1, a_2 b_2 = b_2 a_2$, 从而 G_1, G_2 都是交换群.

- (3) 构造映射

$$\phi : G_1 \times G_2 \longrightarrow G_2 \times G_1,$$

$$(a_1, a_2) \longmapsto (a_2, a_1), \quad \forall (a_1, a_2) \in G_1 \times G_2,$$

则显然 ϕ 是双射, 且

$$\begin{aligned} \phi((a_1, a_2)(b_1, b_2)) &= \phi(a_1 b_1, a_2 b_2) = (a_2 b_2, a_1 b_1) \\ &= (a_2, a_1)(b_2, b_1) = \phi(a_1, a_2) \cdot \phi(b_1, b_2). \end{aligned}$$

因此, ϕ 是 $G_1 \times G_2$ 到 $G_2 \times G_1$ 的同构映射, 即

$$G_1 \times G_2 \cong G_2 \times G_1.$$



定理 0.2

设 G_1, G_2 是两个群, a 和 b 分别是 G_1 和 G_2 中的有限阶元素, 则对于 $(a, b) \in G_1 \times G_2$, 有

$$\text{ord}(a, b) = [\text{ord } a, \text{ord } b].$$



证明 设 $\text{ord } a = m, \text{ord } b = n, s = [m, n]$, 则

$$(a, b)^s = (a^s, b^s) = (e_1, e_2). \quad (1)$$

从而 (a, b) 的阶有限, 设其为 t , 则要证明 $t = s$. 由(1)式得 $t \mid s$.

又因为

$$(e_1, e_2) = (a, b)^t = (a^t, b^t),$$

所以 $a^t = e_1, b^t = e_2$. 于是 $m \mid t$, 且 $n \mid t$, 从而 t 是 m 和 n 的公倍数. 而 s 是 m 和 n 的最小公倍数, 因此 $s \mid t$. 结合以上讨论得 $s = t$.

□

定理 0.3

设 G_1 和 G_2 分别是 m 阶及 n 阶的循环群, 则 $G_1 \times G_2$ 是循环群的充要条件是 $(m, n) = 1$.



证明 设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$.

假设 $G_1 \times G_2$ 是循环群. 若 $(m, n) = t \neq 1$, 则由于 $\text{ord } a = m, \text{ord } b = n$, 而 $a^{m/t}$ 和 $b^{n/t}$ 的阶都是 t , 因此由推论??知 $\langle (a^{m/t}, e_2) \rangle$ 和 $\langle (e_1, b^{n/t}) \rangle$ 是循环群 $G_1 \times G_2$ 中的两个不同的 t 阶子群. 而这与推论??相矛盾, 所以 $(m, n) = 1$.

反之, 假设 $(m, n) = 1$, 则

$$|\langle (a, b) \rangle| = \text{ord}(a, b) = [m, n] = mn = |G_1| \cdot |G_2| = |G_1 \times G_2|,$$

又 $\langle (a, b) \rangle \subseteq G_1 \times G_2$, 故 $\langle (a, b) \rangle = G_1 \times G_2$, 因此 $G_1 \times G_2$ 是循环群.

□

定义 0.2

设 A, B, G 都是群, 若有 G 的正规子群 N 与 A 同构, 而商群 G/N 与 B 同构, 则称 G 是 B 过 A 的扩张, N 称为该扩张的核, 简称扩张核.



注 显然, 若 N 是 G 的正规子群, 则 G 是 G/N 过 N 的扩张, 扩张核为 N .

定义 0.3

设 G 是 B 过 A 的扩张, N 为扩张核, λ 是 A 到 N 上的同构, μ 是 G 到 B 上的同态且 μ 满足 $\ker \mu = N$. 1 为 A 的幺元, $1'$ 为 B 的幺元, i 是 $\{1\}$ 到 A 的映射, $i(1) = 1$. $0'$ 是 B 到 $\{1'\}$ 的映射, $0'(b) = 1' (\forall b \in B)$. 于是有群及其映射的序列 (以 $1, 1'$ 代替 $\{1\}, \{1'\}$)

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

每个映射都是群的同态映射, 并且前一映射的像恰是后一映射的核, 即

$$i(1) = \ker \lambda, \quad \lambda(A) = \ker \mu, \quad \mu(G) = \ker 0'.$$

这样的序列称为 (短) 正合序列. 以后记 (短) 正合序列时, i 与 $0'$ 省略不写, 同时也将 $1'$ 记为 1 .



注 由定理??知存在 G 到 G/N 的自然群同态 μ_1 . 由 $G/N \cong B$ 可设 G/N 到 B 的同构 f , 则 $\mu = f\mu_1$ 就是 G 到 B 的同态. 由命题??知 $\ker \mu_1 = N$, 从而

$$\mu(N) = f\mu_1(N) = f(N) = 1'.$$

故 $N \subseteq \ker \mu$. 再设 $x \in \ker \mu$, 则

$$\mu(x) = f\mu_1(x) = 1' \implies \mu_1(x) = f^{-1}(1') = N \implies x \in \ker \mu_1 = N.$$

故 $\ker \mu \subseteq N$. 综上可得 $\lambda(A) = N = \ker \mu$. 故上述定义中的同态 μ 是良定义的.

命题 0.1

若群 A, B, G 之间有 (短) 正合序列

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

即存在 G 的正规子群 N , 还存在 λ 是 A 到 N 上的同构, 以及 μ 是 G 到 B 上的同态且 μ 满足 $\ker \mu = N$. 则 λ 是 A 到 G 的单同态, μ 是 G 到 B 的满同态, 并且 G 是 B 过 A 的扩张.

证明

□

定理 0.4

设 A, B, G, G' 是群.

- (1) 若 G 是 B 过 A 的扩张, G 与 G' 同构, 则 G' 也是 B 过 A 的扩张;
- (2) 若 G, G' 都是 B 过 A 的扩张且有 G 到 G' 的同态 f , 使图 1 为交换图, 则 f 是 G 到 G' 上的同构, 这时称 G 与 G' 是 B 过 A 的等价扩张.

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \xrightarrow{\lambda} & G & \xrightarrow{\mu} & B \longrightarrow 1 \\ & & \downarrow \text{id}_A & & \downarrow f & & \downarrow \text{id}_B \\ 1 & \longrightarrow & A & \xrightarrow{\lambda'} & G' & \xrightarrow{\mu'} & B \longrightarrow 1 \end{array}$$

图 1

♥

证明

- (1) 设 A, B, G 对应的 (短) 正合序列为

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

f 是 G 到 G' 上的同构. 令 $\lambda' = f\lambda, \mu' = \mu f^{-1}$. 由命题 0.1 知 λ 是 A 到 G 的单同态且 $\lambda(A) = N$. 从而 λ' 是单同态且 $\lambda'(A) = f(\lambda(A))$ 与 A 同构. $\mu' = \mu f^{-1}$ 是 G' 到 B 上的同态, 又注意到

$$\mu'(\ker \mu') = 1' \iff \mu(f^{-1}(\ker \mu')) = 1' \iff f^{-1}(\ker \mu') = \ker \mu \iff \ker \mu' = f(\ker \mu),$$

故

$$\ker \mu' = \ker(\mu f^{-1}) = f(\ker \mu) = f(\lambda(A)) = \lambda'(A).$$

因而 G' 是 B 过 A 的扩张.

- (2) 先证 $\ker f = \{1\}$, 即 f 是单射. 若 $x \in \ker f$, 则 $\mu(x) = \mu'f(x) = \mu'(1) = 1$ 知 $x \in \ker \mu = \lambda(A)$, 因而 $\exists y \in A$, 使得 $x = \lambda(y)$. 于是 $\lambda'(y) = f(\lambda(y)) = f(x) = 1$. 由 (1) 的证明知 λ' 是单射, 故 $y = 1$, 于是 $x = \lambda(1) = 1$, 即 $\ker f = \{1\}$.

下面证 $f(G) = G'$, 即 f 是满映射. 设 $x' \in G'$, 由命题 0.1 知 μ 是 G 到 B 的满同态, 即 $\mu(G) = B$, 从而 $\exists x \in G$, 使 $\mu(x) = \mu'(x')$, 但 $\mu = \mu'f$, 故

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

因而 $(x')^{-1} f(x) \in \ker \mu' = \lambda'(A) = f(\lambda(A))$. 故 $\exists a \in A$, 使 $(x')^{-1} f(x) = f(\lambda(a)) \in f(G)$, 于是 $x' \in f(G)$, 即 f 是满映射.

□

定理 0.5

设群 G 是群 B 过群 A 的扩张, 对应的 (短) 正合序列为

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

扩张核为 $N = \lambda(A) = \ker \mu$.

- (1) 若有 G 的子群 H 满足 $G = HN, H \cap N = \{1\}$, 则 $\mu|_H$ 是 H 到 B 上的同构, 此时 $(\mu|_H)^{-1} = \nu$ 是 B 到 G 中的同态且 $\mu\nu = \text{id}_B$;
- (2) 若存在 B 到 G 的同态 ν , 使得 $\mu\nu = \text{id}_B$, 则 $\nu(B) = H$ 是 G 的子群, ν 是 B 到 $H = \nu(B)$ 上的同构且 $G = HN, H \cap N = \{1\}$.

**证明**

- (1) 由 $\ker(\mu|_H) = H \cap \ker \mu = H \cap N = \{1\}$ 知 $\mu|_H$ 是 H 到 B 的单射, 又 $\forall b \in B, \exists x \in G$, 使 $\mu(x) = b$, 而 $G = HN$, 故 $\exists y \in H, z \in N$, 使 $x = yz$. 于是 $b = \mu(x) = \mu(y)\mu(z) = \mu(y)$, 故 $\mu|_H$ 是 H 到 B 上的满映射, 于是 $\mu|_H$ 是 H 到 B 上的同构. 从而 ν 是 B 到 H 中的同构, 故 ν 是 B 到 G 中的同态. 又 $\mu\nu(b) = \mu(y) = b$, 故 $\mu\nu = \text{id}_B$.
- (2) 由命题????知 $\nu(B) = H$ 是 G 的子群. 由 $\mu\nu = \text{id}_B$ 知 $x = \mu\nu(x) = \mu(1) = 1, \forall x \in \ker \nu$, 即 $\ker \nu \subseteq \{1\}$, 因此 $\ker \nu = \{1\}$, 故 ν 是 B 到 $H = \nu(B)$ 上的同构, 若 $x \in N \cap H$, 则由 $x \in N = \ker \mu$ 知 $\mu(x) = 1$, 由 $x \in H = \nu(B)$ 知存在 $b \in B$, 使 $x = \nu(b)$. 从而

$$1 = \mu(x) = \mu\nu(b) = \text{id}_B(b) = b.$$

故 $x = \nu(b) = \nu(1) = 1$, 即 $H \cap N = \{1\}$.

对 $\forall b \in B$, 由 $\mu\nu = \text{id}_B$ 知 $\mu(\nu(b)) = \text{id}_B(b) = b$ 且 $\nu(b) \in H$, 故 $\mu|_H$ 是 H 到 B 上的满同态. 设 $x \in G$, 则 $\mu(x) \in B$. 于是 $\exists y \in H$, 使 $\mu(y) = \mu(x)$, 因而 $\mu(y^{-1}x) = 1$, 即 $z = y^{-1}x \in \ker \mu = N$ 有 $x = yz \in HN$, 故 $G = HN$. □

定义 0.4

设 G 是群 B 过群 A 的扩张, N 是扩张的核. 如果存在 G 的子群 H , 使 $H \cap N = \{1\}, G = HN$, 那么称此扩张为**非本质扩张**, 并称 G 是 N 与 H 的**半直积**, 记为 $G = H \ltimes N$.

如果 H 还是 G 的正规子群, 则称此扩张为**平凡扩张**. G 是 N 与 H 的**(内)直积**, 记为 $G = H \otimes N$.

如果 $N \subseteq C(G)$, 那么称此扩张为**中心扩张**. ♣

定理 0.6

设 G 是一个群, 则 $G = A \otimes B$ 的充要条件是 $A, B \triangleleft G$ 且 $G = AB, A \cap B = \{1\}$. ♥

证明 充分性: 由 $B \triangleleft G$ 知 G 是 G/B 过 B 的扩张, 扩张核为 B . 又 $G = AB, A \cap B = \{1\}, A \triangleleft G$, 故由定义 0.4 知 $G = A \otimes B$.

必要性: 根据内直积的定义是显然的. □

例题 0.1

1. 对整数加群 \mathbb{Z} , 它的正规子群 $2\mathbb{Z}$ 与 \mathbb{Z} 同构, 而 $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ 是 2 阶循环群, 因而 \mathbb{Z} 是 \mathbb{Z}_2 过 $2\mathbb{Z}$ 的扩张. 由于 \mathbb{Z} 的任何子群都不同构于 \mathbb{Z}_2 , 因而这个扩张不是非本质扩张.
2. 设 $n \geq 3$. A_n 是 S_n 的正规子群, $\langle(12)\rangle$ 是 S_n 的 2 阶子群, $\langle(12)\rangle \cap A_n = \{\text{id}\}, S_n = \langle(12)\rangle A_n$, 但 $\langle(12)\rangle$ 不是 S_n 的正规子群, 故 $S_n = \langle(12)\rangle \ltimes A_n$.
3. 3 阶循环群过 5 阶循环群的扩张 G 是 15 阶群. 由 4.3 节的习题 8 知这种扩张必然是平凡扩张, 即 $G = \langle a \rangle \otimes \langle b \rangle$, 其中, a, b 分别为 G 的 3 阶元素与 5 阶元素.

证明

定理 0.7

设 A, B 是 G 的子群.

- (1) $G = AB, A \cap B = \{1\}$ 当且仅当 $\forall g \in G, \exists a \in A, b \in B$, 使得 $g = ab$ 且这种表示唯一.
- (2) 若 $G = AB, A \cap B = \{1\}$, 则 A, B 都是 G 的正规子群的充分必要条件是 $ab = ba (\forall a \in A, b \in B)$, 此时 $G = A \otimes B$.

**证明**

- (1) 由 $G = AB, A \cap B = \{1\}$ 知 $\forall g \in G, \exists a \in A, b \in B$, 使 $g = ab$. 若另有 $g = a'b', a' \in A, b' \in B$, 则 $a^{-1}a' = bb'^{-1} \in A \cap B = \{1\}$, 于是 $a = a', b = b'$.

反之, 若 $\forall g \in G, \exists a \in A, b \in B$, 使 $g = ab$, 则 $G = AB$. 又若 $c \in A \cap B$, 由 $c = 1 \cdot c = c \cdot 1$ 的表示唯一可知 $c = 1$, 故 $A \cap B = \{1\}$.

- (2) 设 $A \triangleleft G, B \triangleleft G$, 于是 $a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in A \cap B = \{1\}$, 故 $ab = ba (\forall a \in A, b \in B)$.

反之, 由于 $G = AB, \forall g \in G, \exists a \in A, b \in B$, 使 $g = ab$. 又若 $a_0 \in A$, 则由 $ab = ba (\forall a \in A, b \in B)$ 有

$$ga_0g^{-1} = (ab)a_0(ab)^{-1} = aa_0a^{-1} \in A,$$

故 $A \triangleleft G$, 同样 $B \triangleleft G$, 由 **命题 0.6** 知 $G = A \otimes B$.

**定义 0.5**

设 N_1, N_2, \dots, N_k 都是群 G 的正规子群, 并且 $G = N_1N_2 \cdots N_k$, G 中任一元素可分解为 $N_i (1 \leq i \leq k)$ 中元素的积且这种分解是唯一的, 则称 G 是 N_1, N_2, \dots, N_k 的 **(内) 直积**, 记为

$$G = N_1 \otimes N_2 \otimes \cdots \otimes N_k.$$

**定理 0.8**

设 A, B 是两个群, 则一定存在 B 过 A 的平凡扩张 $G = A \times B$, 并且 G 在同构意义下唯一.



证明 在 $G = A \times B = \{(a, b) \mid a \in A, b \in B\}$ 中定义乘法

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2), \quad \forall (a_i, b_i) \in G, i = 1, 2.$$

容易验证 G 是群, 幺元为 $(1, 1')$, 其中, $1, 1'$ 分别为 A, B 的幺元. $\forall (a, b) \in G, (a, b)^{-1} = (a^{-1}, b^{-1})$, 而且

$$A' = \{(a, 1') \mid a \in A\}, \quad B' = \{(1, b) \mid b \in B\}$$

都是 G 的正规子群. 又 $G = A'B', A' \cap B' = \{(1, 1')\}$, 于是由 **命题 0.6** 知 $G = A' \otimes B'$.

又映射 $\lambda: \lambda(a) = (a, 1') (\forall a \in A)$ 是 A 到 G 的单同态, $\lambda(A) = A'$, 故 λ 是 A 到 A' 的同构. 而映射 $\mu: \mu((a, b)) = b$ 则是 G 到 B 上的同态, 并且 $\ker \mu = A' = \lambda(A), \mu|_{B'}$ 是 B' 到 B 上的同构. 即有 (短) 正合序列

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

故由 **命题 0.1** 知 G 是 B 过 A 的扩张, 扩张核为 A' . 由 $G = A' \otimes B'$ 及 $A \cong A', B \cong B'$ 知

$$G = A'B' \cong AB, \quad A \cap B \cong A' \cap B' = \{1\}.$$

又 $A' \triangleleft G$, 故由 **命题 0.1** 知 G 是 B 过 A 的平凡扩张.

设 G_1 也是 B 过 A 的平凡扩张, 于是 $G_1 = A_1 \otimes B_1$. 设 λ_1 为 A 到 A_1 的同构, γ_1 是 B 到 B_1 的同构, 令

$$f((a, b)) = \lambda_1(a)\gamma_1(b), \quad \forall a \in A, b \in B.$$

由 $G_1 = A_1 \otimes B_1$ 知 $G_1 = A_1B_1, A_1 \cap B_1 = \{1\}$ 且 $A_1, B_1 \triangleleft G_1$. 从而由 **定理 0.7(2)** 知

$$a_1b_1 = b_1a_1, \quad \forall a_1 \in A_1, b_1 \in B_1.$$

于是对 $\forall (a, b), (a', b') \in G$, 有

$$\begin{aligned} f((a, b)(a', b')) &= f((aa', bb')) = \lambda_1(aa')\gamma_1(bb') \\ &= \lambda_1(a)\lambda_1(a')\gamma_1(b)\gamma_1(b') = \lambda_1(a)\gamma_1(b)\lambda_1(a')\gamma_1(b') \\ &= f((a, b))f((a', b')). \end{aligned}$$

因此 f 是 G 到 G_1 的同态.

设 $a_1b_1 \in A_1B_1 = G_1$, 则由 λ_1 是 A 到 A_1 的同构, γ_1 是 B 到 B_1 的同构可知, 存在 $a \in A, b \in B$, 使

$$\lambda_1(a) = a_1, \gamma_1(b) = b_1 \implies f((a, b)) = \lambda_1(a)\gamma_1(b) = a_1b_1.$$

故 f 是满同态.

设 $f((a, b)) = f((a', b')) \in G_1$, 则

$$\lambda_1(a)\gamma_1(b) = f((a, b)) = f((a', b')) = \lambda_1(a')\gamma_1(b').$$

由定理 0.7(1) 知 $\lambda_1(a) = \lambda_1(a'), \gamma_1(b) = \gamma_1(b')$. 又 λ_1 是 A 到 A_1 的同构, γ_1 是 B 到 B_1 的同构, 故

$$a = a', b = b' \implies (a, b) = (a', b').$$

因此 f 是单同态. 综上所述可知 f 是 G 到 G_1 的同构.

□