# 0.1 群的直积

**定义 0.1 (外直积)**

设 $G_1, G_2, \cdots, G_n$ 是 $n$ 个群, 构造集合 $G_1, G_2, \cdots, G_n$ 的笛卡尔积

$$G = \{(a_1, a_2, \cdots, a_n) \mid a_i \in G_i,\ i = 1, 2, \cdots, n\},$$

并在 $G$ 中定义乘法运算

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n),\ \forall (a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in G,$$

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

♣

注

(1) 如果 $e_1, e_2, \cdots, e_n$ 分别是群 $G_1, G_2, \cdots, G_n$ 的单位元, 则 $(e_1, e_2, \cdots, e_n)$ 是 $G_1 \times G_2 \times \cdots \times G_n$ 的单位元;

(2) 设 $(a_1, a_2, \cdots, a_n) \in G$, 则 $(a_1, a_2, \cdots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$;

(3) 当 $G_1, G_2, \cdots, G_n$ 都是加群时,$G_1$ 与 $G_2$ 的外直积也可记作 $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

**定理 0.1**

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是 $n$ 个群 $G_1, G_2, \cdots, G_n$ 的外直积, 则

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

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

(2) $G$ 是交换群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是交换群;

(3) $G_1 \times G_2 \times \cdots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)},\ \forall \sigma \in S_n$.

(4) 若 $a_1, a_2, \cdots, a_n$ 分别是 $G_1, G_2, \cdots, G_n$ 中的有限阶元素, 则对 $(a_1, a_2, \cdots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$, 有

$$\operatorname{ord}(a_1, a_2, \cdots, a_n) = [\operatorname{ord} a_1, \operatorname{ord} a_2, \cdots, \operatorname{ord} a_n].$$

(5) $C(G) = C(G_1) \times C(G_2) \times \cdots \times C(G_n)$.

(6) 若 $G_1, G_2, \cdots, G_n$ 分别是 $m_1, m_2, \cdots, m_n$ 阶的循环群, 则 $G$ 是循环群的充要条件是 $(m_1, m_2, \cdots, m_n) = 1$.

♡

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 $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in G$, 有

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

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

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (b_1, b_2, \cdots, b_n) \cdot (a_1, a_2, \cdots, a_n),$$

即

$$(a_1 b_1, a_2 b_2, \cdots, a_n b_n) = (b_1 a_1, b_2 a_2, \cdots, b_n a_n).$$

因此 $a_i b_i = b_i a_i,\ i = 1, 2, \cdots, n$. 从而 $G_i (i = 1, 2, \cdots, n)$ 都是交换群.

(3) 对 $\forall \sigma \in S_n$, 构造映射

$$\phi : G_1 \times G_2 \times \cdots \times G_n \longrightarrow G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)},$$

$$(a_1, a_2, \cdots, a_n) \longmapsto (a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)}), \quad \forall (a_1, a_2, \cdots, a_n) \in G_1 \times G_2 \times \cdots \times G_n,$$

因为 $\sigma$ 是双射, 所以 $\phi$ 也是双射, 且

$$\begin{aligned} &\phi((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)) \\ &= \phi(a_1 b_1, a_2 b_2, \cdots, a_n b_n) \\ &= (a_{\sigma(1)} b_{\sigma(1)}, a_{\sigma(1)} b_{\sigma(2)}, \cdots, a_{\sigma(1)} b_{\sigma(n)}) \\ &= (a_2, a_1)(b_2, b_1) = \phi(a_1, a_2) \cdot \phi(b_1, b_2). \end{aligned}$$

因此 $\phi$ 是 $G_1 \times G_2 \times \cdots \times G_n$ 到 $G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}$ 的同构映射, 即

$$G_1 \times G_2 \times \cdots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}.$$

(4) 当 $n = 1$ 时, 结论显然成立. 假设结论对 $n-1$ 成立, 现在考虑 $n$ 的情况.
设 $a_i \in G_i$, $i = 1, 2, \cdots, n$, 记 $b = (a_2, \cdots, a_n) \in G_2 \times \cdots \times G_n$,$\operatorname{ord} a_1 = m$, 则由归纳假设知

$$\operatorname{ord} b = \operatorname{ord}(a_2, \cdots, a_n) = [\operatorname{ord} a_2, \cdots, \operatorname{ord} a_n].$$

再记 $\operatorname{ord} b = n$, $s = [m, n]$,$e_1$ 为 $G_1$ 的幺元,$e_2$ 为 $G_2 \times \cdots \times G_n$ 的幺元. 则

$$(a_1, b)^s = (a_1^s, b^s) = (e_1, e_2).$$

从而 $(a_1, b)$ 的阶有限, 设其为 $t$, 则由上式得 $t \mid s$.
又因为

$$(e_1, e_2) = (a_1, b)^t = (a_1^t, b^t),$$

所以 $a_1^t = e_1$, $b^t = e_2$. 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 $s = t$, 即

$$\begin{aligned} \operatorname{ord}(a_1, a_2, \cdots, a_n) &= \operatorname{ord}(a_1, b) = [\operatorname{ord} a_1, \operatorname{ord} b] \\ &= [\operatorname{ord} a_1, [\operatorname{ord} a_2, \cdots, \operatorname{ord} a_n]] \\ &= [\operatorname{ord} a_1, \operatorname{ord} a_2, \cdots, \operatorname{ord} a_n]. \end{aligned}$$

故由数学归纳法知结论成立.

(5) 设 $a = (a_1, a_2, \cdots, a_n) \in C(G)$, 则对任意的 $x = (x_1, x_2, \cdots, x_n) \in G$, 由 $ax = xa$ 得 $a_i \in C(G_i), i = 1, 2, \cdots, n$, 因此

$$a = (a_1, a_2, \cdots, a_n) \in C(G_1) \times C(G_2) \times \cdots \times C(G_n).$$

另一方面, 设 $a = (a_1, a_2, \cdots, a_n) \in C(G_1) \times C(G_2) \times \cdots \times C(G_n)$, 则对任意的 $x = (x_1, x_2, \cdots, x_n) \in G$, 有

$$ax = (a_1 x_1, a_2 x_2, \cdots, a_n x_n) = (x_1 a_1, x_2 a_2, \cdots, x_n a_n) = xa.$$

所以 $a = (a_1, a_2, \cdots, a_n) \in C(G)$. 因此

$$C(G) = C(G_1) \times C(G_2) \times \cdots \times C(G_n).$$

(6) 设 $G_1 = \langle a_1 \rangle, G_2 = \langle a_2 \rangle, \cdots, G_n = \langle a_n \rangle$,$e_1, e_2, \cdots, e_n$ 分别为 $G_1, G_2, \cdots, G_n$ 的幺元.
**必要性**: 设 $G_1 \times G_2 \times \cdots \times G_n$ 是循环群. 若 $(m_1, m_2, \cdots, m_n) = t \neq 1$, 则由于 $\operatorname{ord} a_i = m_i$, $i = 1, 2, \cdots, n$. 而 $a_i^{\frac{m_i}{t}}$ 的阶都是 $t$, 因此由定理**??**知

$$\langle (e_1, \cdots, \underbrace{a_i^{\frac{m_i}{t}}}_{\text{第}i\text{个位置}}, \cdots, e_n) \rangle, \ i = 1, 2, \cdots, n$$

都是循环群 $G_1 \times G_2 \times \cdots \times G_n$ 中的 $n$ 个不同的 $t$ 阶子群. 而这与定理**??????**矛盾! 故 $(m_1, m_2, \cdots, m_n) = 1$.

**充分性**: 设 $(m_1, m_2, \cdots, m_n) = 1$, 则由定理 0.1(4) 和定理 0.1(1)可得

$$\begin{aligned}|\langle(a_1, a_2, \cdots, a_n)\rangle| &= \mathrm{ord}(a_1, a_2, \cdots, a_n) = [m_1, m_2, \cdots, m_n] \\ &= m_1 m_2 \cdots m_n = |G_1| \cdot |G_2| \cdots |G_n| \\ &= |G_1 \times G_2 \times \cdots \times G_n|.\end{aligned}$$

又 $\langle(a_1, a_2, \cdots, a_n)\rangle \subseteq G_1 \times G_2 \times \cdots \times G_n$, 故 $\langle(a_1, a_2, \cdots, a_n)\rangle = G_1 \times G_2 \times \cdots \times G_n$. 因此 $G_1 \times G_2 \times \cdots \times G_n$ 是循环群.

□

**定义 0.2 (换位子)**

设 $g_1, g_2$ 是群 $G$ 中的两个元素, 称

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

为 $g_1$ 与 $g_2$ 的**换位子**.

♣

**定义 0.3 (换位子群)**

若 $H, K$ 是群 $G$ 的两个子群, 称

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

为 $H$ 与 $K$ 的**换位子群**.

♣

**命题 0.1**

设 $H, K$ 是群 $G$ 的两个子群, 则

(1) $\alpha([g_1, g_2]) = [\alpha(g_1), \alpha(g_2)]$, $\quad \forall \alpha \in \mathrm{Aut}G,\ g_1, g_2 \in G$.

(2) $\alpha([H, K]) = [\alpha(H), \alpha(K)]$, $\quad \forall \alpha \in \mathrm{Aut}G$.

(3) 若 $H \lhd G$, 则 $G/H$ 为 Abel 群的充要条件是 $H \supseteq [G, G]$.

♠

证明

(1) 从换位子的定义即得.

(2) 因为 $\forall a \in H, b \in K$, 有 $\alpha(a) \in \alpha(H), \alpha(b) \in \alpha(K)$. 注意到

$$\alpha([a, b]) = \alpha(aba^{-1}b^{-1}) = \alpha(a)\alpha(b)\alpha(a)^{-1}\alpha(b)^{-1} = [\alpha(a), \alpha(b)],$$

故 $\alpha([H, K]) = [\alpha(H), \alpha(K)]$.

(3) $G/H$ 为 Abel 群, 当且仅当对 $\forall a, b \in G$, $(aH)(bH) = (bH)(aH)$, 即 $abH = baH, \forall a, b \in G$, 当且仅当 $[a, b] = a^{-1}b^{-1}ab \in H, \forall a, b \in G$, 即 $H \supseteq [G, G]$.

□

**引理 0.1**

设 $H, K$ 是群 $G$ 的子群, 则有

(1) $[H, K] = \{1\} \iff H \subseteq C_G(K)$;

(2) $[H, K] \subseteq K \iff H \subseteq N_G(K)$,
$[H, K] \subseteq H \iff K \subseteq N_G(H)$;

(3) 若 $H \lhd G, K \lhd G$, 则 $[H, K] \lhd G$ 且 $[H, K] \subseteq H \cap K$. 特别地, 由 $G \lhd G$ 知 $[G, G] \lhd G$;

(4) 当 $H_1, K_1$ 分别为 $H, K$ 的子群时有 $[H_1, K_1] \subseteq [H, K]$.

(5) 设 $H, K$ 是两个群,$N \lhd H, K$, 则

$$[H, K] \subseteq N \iff [H/N, K/N] = N \iff H/N \subseteq C(K/N).$$

♡

证明

(1) $[H,K]=\{1\}$ 当且仅当对 $\forall h\in H,k\in K$ 有

$$[h,k]=1 \iff h^{-1}k^{-1}hk=1 \iff hk=kh \iff hkh^{-1}=k,$$

即 $h\in C_G(K),\forall h\in H$, 即 $H\subseteq C_G(K)$.

(2) 先证 $[H,K]\subseteq K \iff H\subseteq N_G(K)$. 若 $[H,K]\subseteq K$, 则

$$[h,k]\in K,\quad [h^{-1},k^{-1}]\in K,\quad \forall k\in K,\ h\in H.$$

对 $\forall h\in H$, 设 $k\in K$, 则由 $[h,k]\in K$ 知存在 $k_1\in K$, 使

$$h^{-1}k^{-1}hk=k_1 \Longleftrightarrow hkk_1^{-1}=kh \Longleftrightarrow k=hkk_1^{-1}h^{-1}\in hKh^{-1},$$

故 $K\subseteq hKh^{-1}$. 再设 $hkh^{-1}\in hKh^{-1}$, 则由 $[h^{-1},k^{-1}]\in K$ 知存在 $k_2\in K$, 使

$$hkh^{-1}k^{-1}=k_1 \Longleftrightarrow hkh^{-1}=kk_1\in K,$$

故 $hKh^{-1}\subseteq K$. 因此 $hKh^{-1}=K,,\forall h\in H$. 即 $h\in N_G(K),\forall h\in H$. 故 $H\subseteq N_G(K)$.
反之, 若 $H\subseteq N_G(K)$, 对 $\forall h\in H,\ k\in K$, 有 $hKh^{-1}=K$, 从而存在 $h_1\in H,\ k_1\in K$, 使

$$k=h_1k_1h_1^{-1} \Longleftrightarrow k^{-1}=h_1k_1^{-1}h_1^{-1}.$$

于是

$$[h,k]=h^{-1}k^{-1}hk=h^{-1}h_1k_1^{-1}h_1^{-1}hk=(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}k.$$

注意到 $(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}\in hKh^{-1}$, 所以存在 $k_2\in K$, 使 $(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}=k_2$. 从而

$$[h,k]=(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}k=k_2k\in K,\ \forall k\in K,h\in H.$$

故 $[H,K]\subseteq K$.
再证 $[H,K]\subseteq H \iff K\subseteq N_G(H)$. 若 $[H,K]\subseteq H$, 则

$$[h,k]\in H,\quad [h^{-1},k^{-1}]\in H,\quad \forall k\in K,\ h\in H.$$

对 $\forall k\in K$, 设 $h\in H$, 则由 $[h,k]\in H$ 知存在 $h_1\in H$, 使

$$h^{-1}k^{-1}hk=h_1 \Longleftrightarrow hk=khh_1 \Longleftrightarrow h=khh_1k^{-1}\in kHk^{-1},$$

故 $H\subseteq kHk^{-1}$. 再设 $khk^{-1}\in kHk^{-1}$, 则由 $[h^{-1},k^{-1}]\in H$ 知存在 $h_2\in H$, 使

$$hkh^{-1}k^{-1}=h_1 \Longleftrightarrow khk^{-1}=h^{-1}h_1\in H,$$

故 $kHk^{-1}\subseteq H$. 因此 $kHk^{-1}=H,\forall k\in K$. 即 $k\in N_G(H),\forall k\in K$. 故 $K\subseteq N_G(H)$.
反之, 若 $K\subseteq N_G(H)$, 对 $\forall h\in H,\ k\in K$, 有 $kHk^{-1}=H$, 从而存在 $h_1\in H,\ k_1\in K$, 使

$$h=k_1h_1k_1^{-1}.$$

于是

$$[h,k]=h^{-1}k^{-1}hk=h^{-1}k^{-1}k_1h_1k_1^{-1}k=h^{-1}(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}.$$

注意到 $(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}\in kHk^{-1}$, 所以存在 $h_2\in H$, 使 $(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}=h_2$. 从而

$$[h,k]=h^{-1}(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}=h^{-1}h_2\in H.$$

故 $[H,K]\subseteq H$.

(3) 设 $H\lhd G,K\lhd G$, 于是对 $\forall\alpha=L_gR_{g^{-1}}\in \mathrm{Int}G$, 由命题 0.1(2)有

$$g[H,K]g^{-1}=\alpha([H,K])=[\alpha(H),\alpha(K)]=[gHg^{-1},gKg^{-1}]=[H,K],$$

即 $[H,K]\lhd G$. 由 $H\lhd G,K\lhd G$ 知

$$gHg^{-1}=H,\quad gKg^{-1}=K,\quad \forall g\in G.$$

故

$$kHk^{-1}=H,\quad \forall k\in K;$$

$$hKh^{-1} = K, \quad \forall h \in H.$$

即 $K \subseteq N_G(H)$, $H \subseteq N_G(K)$. 再由结论 (2) 知 $[H,K] \subseteq H \cap K$.

(4) 此结论是显然的.

(5) 由引理 0.1(1)知

$$[H/N, K/N] = N \Longleftrightarrow H/N \subseteq C(K/N).$$

于是对 $\forall a \in H, b \in K$, 有

$$N = [aN, bN] = (a^{-1}N)(b^{-1}N)(aN)(bN) = (a^{-1}b^{-1}ab)N = [a,b]N.$$

这也当且仅当

$$[a,b] \in N, \quad \forall a \in H, b \in K.$$

即 $[H,K] \subseteq N$.

□

**推论 0.1**

(1) 设 $G$ 是一个群,$N_1, N_2, \cdots N_k \lhd G$, 且 $N_i \cap N_j = \{1\}(i \neq j)$, 则对 $\forall i, j \in \{1,2,\cdots,k\}$, 有

$$n_i n_j = n_j n_i, \ \forall n_i \in N_i, n_j \in N_j.$$

并且

$$N_j \subseteq C(N_i), \ \forall i, j \in \{1,2,\cdots,k\}.$$

(2)

♡

证明

(1) 对 $\forall i, j \in \{1,2,\cdots,k\}$, 由引理 0.1(3)知 $[N_i, N_j] \subseteq N_i \cap N_j = \{1\}$, 故 $[N_i, N_j] = \{1\}$. 因此对 $\forall n_i \in N_i, n_j \in N_j$, 有

$$1 = [n_i, n_j] = n_i^{-1} n_j^{-1} n_i n_j \Longleftrightarrow n_i n_j = n_j n_i.$$

并且由引理 0.1(1)知

$$N_j \subseteq C(N_i), \ \forall i, j \in \{1,2,\cdots,k\}.$$

□

**定义 0.4**

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 0.5**

设 $G$ 是 $B$ 过 $A$ 的扩张, $N$ 为扩张核, $\lambda$ 是 $A$ 到 $N$ 上的同构,$\mu$ 是 $G$ 到 $B$ 上的同态且 $\mu$ 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 $\mu_1$. 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 $\mu$ 是良定义的.

**命题 0.2**

*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 $\lambda$ 是 $A$ 到 $N$ 上的同构, 以及 $\mu$ 是 $G$ 到 $B$ 上的同态且 $\mu$ 满足 $\ker \mu = N$. 则 $\lambda$ 是 $A$ 到 $G$ 的单同态,$\mu$ 是 $G$ 到 $B$ 的满同态, 并且 $G$ 是 $B$ 过 $A$ 的扩张.*

♠

证明

□

**定理 0.2**

*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**.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\lambda} & G & \xrightarrow{\mu} & B & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\ 1 & \longrightarrow & A & \xrightarrow[\lambda']{} & G' & \xrightarrow[\mu']{} & B & \longrightarrow & 1 \end{array}$$

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 0.2知 $\lambda$ 是 $A$ 到 $G$ 的单同态且 $\lambda(A) = N$. 从而 $\lambda'$ 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

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

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 $\lambda'$ 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 0.2知 $\mu$ 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

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

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 0.3**

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 $\mu\nu = \mathrm{id}_B$;

(2) 若存在 $B$ 到 $G$ 的同态 $\nu$, 使得 $\mu\nu = \mathrm{id}_B$, 则 $\nu(B) = H$ 是 $G$ 的子群,$\nu$ 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 $\nu$ 是 $B$ 到 $H$ 中的同构, 故 $\nu$ 是 $B$ 到 $G$ 中的同态. 又 $\mu\nu(b) = \mu(y) = b$, 故 $\mu\nu = \mathrm{id}_B$.

(2) 由命题**????**知 $\nu(B) = H$ 是 $G$ 的子群. 由 $\mu\nu = \mathrm{id}_B$ 知 $x = \mu\nu(x) = \mu(1) = 1, \forall x \in \ker \nu$, 即 $\ker \nu \subseteq \{1\}$, 因此 $\ker \nu = \{1\}$, 故 $\nu$ 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

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

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

对 $\forall b \in B$, 由 $\mu\nu = \mathrm{id}_B$ 知 $\mu(\nu(b)) = \mathrm{id}_B(b) = b$ 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 0.6**

设 $G$ 是一个群,$N \lhd G$,$H$ 是 $G$ 的子群, 且 $H \cap N = \{1\}$, $G = HN$, 则称 $G$ 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 $G$ 是 $N$ 与 $H$ 的**内直积**, 记为 $G = H \otimes N$.

♣

**定义 0.7**

设 $G$ 是群 $B$ 过群 $A$ 的扩张, $N$ 是扩张的核.

(1) 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**. 若 $H$ 还是 $G$ 的正规子群, 则称此扩张为**平凡扩张**.

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

♣

**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 $n \geqslant 3$. $A_n$ 是 $S_n$ 的正规子群, $\langle(12)\rangle$ 是 $S_n$ 的 2 阶子群, $\langle(12)\rangle \cap A_n = \{\mathrm{id}\}$, $S_n = \langle(12)\rangle A_n$, 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. 由命题**??**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 0.4**

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) $G$ 是 $A$ 和 $B$ 的内直积的充分必要条件是 $G$ 满足如下两个条件:

(i) $G$ 中每个元素可唯一地表为 $ab$ 的形式, 其中 $a \in A, b \in B$;

(ii) $A$ 中每个元素与 $B$ 中任意元素可交换, 即: 对任意 $a \in A, b \in B$, 有 $ab = ba$.

♡

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) 由定理**????**知条件 (i) 成立当且仅当 $A, B \lhd G$. 又由定理 0.4(1)知条件 (ii) 成立当且仅当 $G = AB, A \cap B = \{1\}$. 故 $G = A \otimes B$ 当且仅当 $G$ 同时满足条件 (i)(ii).

□

**定理 0.5**

(1) 如果群 $G$ 是正规子群 $H$ 和 $K$ 的内直积, 则 $H \times K \cong G$.

(2) 如果群 $G = G_1 \times G_2$, 则存在 $G$ 的正规子群 $G_1'$ 和 $G_2'$, 且 $G_i'$ 与 $G_i$ 同构 $(i = 1, 2)$, 使得 $G = G_1' \otimes G_2'$.

♡

注 从这个定理可以看到, 群的内外直积的概念在同构意义下是一致的, 所以有时可不对内外直积加以区分, 而统称为**群的直积**.

证明

(1) 如果群 $G$ 是正规子群 $H$ 和 $K$ 的内直积. 定义映射

$$\begin{aligned} \phi : H \times K &\longrightarrow G, \\ (h, k) &\longmapsto hk, \ \forall (h, k) \in H \times K, \end{aligned}$$

则由于 $G = HK$, 故 $\phi$ 是满射. 又由定理 0.4(2)知 $G$ 中元素为 $hk$ 形式时表法唯一, 故 $\phi$ 是单射. 又对任意的 $(h_1, k_1), (h_2, k_2) \in H \times K$, 由于 $H$ 中的元素与 $K$ 中的元素可交换, 故

$$\begin{aligned} \phi((h_1, k_1) \cdot (h_2, k_2)) &= \phi(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2) \\ &= (h_1k_1)(h_2k_2) = \phi(h_1, k_1) \cdot \phi(h_2, k_2), \end{aligned}$$

所以 $\phi$ 是同构映射, 从而 $H \times K \cong G$.

(2) 如果 $G = G_1 \times G_2$. 令

$$G_1' = \{(a_1, e_2) \mid a_1 \in G_1\}, \ G_2' = \{(e_1, a_2) \mid a_2 \in G_2\},$$

则容易验证 $G_1', G_2'$ 都是 $G$ 的子群, 且对任意的 $(a_1, a_2) \in G$,

$$(a_1, a_2) = (a_1, e_2)(e_1, a_2) \in G_1'G_2'.$$

这一表法是唯一的, 且对任意的 $(a_1, e_2) \in G_1', (e_1, a_2) \in G_2'$, 有

$$(a_1, e_2) \cdot (e_1, a_2) = (a_1, a_2) = (e_1, a_2) \cdot (a_1, e_2),$$

所以由定理 0.4(2)知 $G$ 是 $G_1'$ 与 $G_2'$ 的内直积. 而

$$\phi_1 : a_1 \longmapsto (a_1, e_2)$$

以及

$$\phi_2 : a_2 \longmapsto (e_1, a_2)$$

分别为 $G_1$ 到 $G_1'$ 和 $G_2$ 到 $G_2'$ 的同构映射.

□

**定理 0.6**

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 $G = A' \otimes B'$.

又映射 $\lambda$: $\lambda(a) = (a,1')(\forall a \in A)$ 是 $A$ 到 $G$ 的单同态, $\lambda(A) = A'$, 故 $\lambda$ 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 0.2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

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

故 $G$ 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 $\lambda_1$ 为 $A$ 到 $A_1$ 的同构, $\gamma_1$ 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 $A_1, B_1 \lhd G_1$. 从而由定理**????**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 $\lambda_1$ 是 $A$ 到 $A_1$ 的同构,$\gamma_1$ 是 $B$ 到 $B_1$ 的同构可知, 存在 $a \in A$,$b \in B$, 使

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

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 0.4(1)知 $\lambda_1(a) = \lambda_1(a')$,$\gamma_1(b) = \gamma_1(b')$. 又 $\lambda_1$ 是 $A$ 到 $A_1$ 的同构,$\gamma_1$ 是 $B$ 到 $B_1$ 的同构, 故

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

因此 $f$ 是单同态. 综上可知 $f$ 是 $G$ 到 $G_1$ 的同构.

□

**定义 0.8**

若 $N_1, N_2, \cdots, N_k$ 都是群 $G$ 的正规子群, 并且

$$G = N_1N_2\cdots N_k, \ \text{其中} N_i \cap \prod_{j=1}^{i-1} N_j = \{1\}, \ i = 1,2,\cdots,k.$$

则称 $G$ 是 $N_1, N_2, \cdots, N_k$ 的**内直积**, 记为

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

♣

注 由 $N_i \cap \prod_{j=1}^{i-1} N_j = \{1\}$, $i = 1, 2, \cdots, k$ 可推出 $N_i \cap \prod_{j \neq i} N_j = \{1\}$, $i = 1, 2, \cdots, k$.

**定理 0.7**

如果群 $G$ 是有限多个子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则 $G$ 同构于 $H_1, H_2, \cdots, H_n$ 的外直积.

♡

证明 对 $n$ 用数学归纳法. 当 $n = 2$ 时, 由定理 0.5(1)知结论成立.

假定结论对 $n-1$ 成立. 考察 $G$ 是 $n$ 个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积的情形. 令 $K = H_1 H_2 \cdots H_{n-1}$, 则由命题????知 $K$ 为 $G$ 的正规子群, 由命题????知 $H_i (i = 1, 2, \cdots, n-1)$ 为 $K$ 的正规子群. 从而由内直积的定义可得,$G$ 为 $K$ 与 $H_n$ 的内直积,$K$ 为正规子群 $H_1, H_2, \cdots, H_{n-1}$ 的内直积. 于是由定理 0.5(1)及归纳假设得

$$G \cong K \times H_n, \quad K \cong H_1 \times H_2 \times \cdots \times H_{n-1}.$$

因此

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

□

**定理 0.8**

(1) 设群 $N_1, N_2, \cdots, N_k$ 的内直积为 $G$, 即 $G = N_1 \otimes N_2 \otimes \cdots \otimes N_k$, 则对 $\forall i, j \in \{1, 2, \cdots, k\}$, 有

$$n_i n_j = n_j n_i, \ \forall n_i \in N_i, n_j \in N_j.$$

(2) 设有限群 $N_1, N_2, \cdots, N_k$ 的内直积为 $G$, 即 $G = N_1 \otimes N_2 \otimes \cdots \otimes N_k$, 则

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

(3) 设 $G$ 是一个群, 群 $N_1, N_2, \cdots, N_k \lhd G$, 则

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

(4) 设 $N_1, N_2, \cdots, N_k$ 都是群 $G$ 的正规子群, 则群 $G$ 满足

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

的充要条件是 $G$ 中任一元素可分解为 $N_i (1 \leqslant i \leqslant k)$ 中元素的积且这种分解是唯一的.

♡

证明

(1) 由内直积的定义知当 $i \neq j$ 时, 有 $N_i \cap N_j \subseteq N_i \cap \prod_{j \neq i} N_j = \{1\}$, 故利用推论 0.1(1)得, 对 $\forall i, j \in \{1, 2, \cdots, k\}$, 有

$$n_i n_j = n_j n_i, \ \forall n_i \in N_i, n_j \in N_j.$$

(2) 由内直积的定义知当 $i \neq j$ 时, 有 $N_i \cap N_j \subseteq N_i \cap \prod_{j \neq i} N_j = \{1\}$, 故利用命题??得

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

(3) 由内直积的定义和命题????立得.

(4) **必要性**: 由内直积的定义知 $G = N_1 N_2 \cdots N_k$ 且 $N_i \cap N_j = \{1\} (i \neq j)$, 则显然 $G$ 中任一元素可分解为 $N_i (1 \leqslant i \leqslant k)$ 中元素的积. 由定理 0.8(1)知, 对 $\forall i, j \in \{1, 2, \cdots, k\}$, 有

$$n_i n_j = n_j n_i, \ \forall n_i \in N_i, n_j \in N_j. \tag{1}$$

设 $g \in G$ 且

$$g = x_1x_2\cdots x_k = y_1y_2\cdots y_k, \quad x_i, y_i \in N_i(i = 1, 2, \cdots, k).$$

则由(1)式可得

$$1 = x_1x_2\cdots x_k y_k^{-1}y_{k-1}^{-1}\cdots y_1^{-1} = (x_1y_1^{-1})(x_2y_2^{-1})\cdots(x_ky_k^{-1}).$$

记 $n_i = x_iy_i^{-1} \in N_i(i = 1, 2, \cdots, k)$, 则

$$1 = n_1n_2\cdots n_k.$$

再结合(1)式可得, 对 $\forall i \in \{1, 2, \cdots, k\}$, 都有

$$n_i = \prod_{j\neq i} n_j^{-1} \in N_i \cap \prod_{j\neq i} N_j = \{1\}.$$

故 $n_i = 1$, 即 $x_i = y_i$, $i = 1, 2, \cdots, k$. 因此 $g$ 的分解唯一.

**充分性**: 由 $G$ 中任一元素可分解为 $N_i(1 \leqslant i \leqslant k)$ 中元素的积知 $G \subseteq N_1N_2\cdots N_k$. 又因为 $N_i \lhd G(i = 1, 2, \cdots, k)$, 所以 $N_1N_2\cdots N_k \subseteq G$. 故 $G = N_1N_2\cdots N_k$. 若存在 $i, j \in \{1, 2, \cdots, k\}$, 使得 $N_i \cap N_j \neq \{1\}$. 取 $n_i \in N_i \cap N_j$, 则

$$n_i = 1\cdots \underbrace{n_i}_{\text{第}i\text{个位置}}\cdots 1 = 1\cdots \underbrace{n_i}_{\text{第}j\text{个位置}}\cdots 1 \in N_1N_2\cdots N_k.$$

这与 $n_i$ 的分解唯一矛盾! 故 $N_i \cap N_j = \{1\}(i \neq j)$. 因此

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

□

**命题 0.3**

设 $G$ 为有限群,$|G| = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$,$p_1, p_2, \cdots, p_k$ 为互不相等的素数. 又每个 Sylow $p_i$ 子群 $P_i \lhd G$. 则

$$G = P_1 \otimes P_2 \otimes \cdots \otimes P_k.$$

♠

**证明** 由 Sylow 第三定理**??**知 $P_i$ 是 $G$ 中唯一的 Sylow $p_i$ 子群 $(i = 1, 2, \cdots, k)$. 由条件知 $|P_i| = p_i^{a_i}, i = 1, 2, \cdots, k$. 再由定理 0.8(2)知

$$\left|\prod_{i=1}^{k} P_i\right| = |P_1||P_2|\cdots|P_k| = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k} = |G|.$$

显然 $\prod_{i=1}^{k} P_i \subseteq G$, 故 $G = \prod_{i=1}^{k} P_i$.

由命题**??**知对 $\forall x_i \in P_i\backslash\{1\}, i = 1, 2, \cdots, k$, 都存在 $k_i \in \mathbb{N}\backslash\{0\}$, 使

$$\operatorname{ord} x_i = p_i^{k_i}, \quad i = 1, 2, \cdots, k.$$

又因为 $p_1, \cdots, p_k$ 是互不相同的素数, 所以

$$\operatorname{ord}\prod_{j\neq i} x_j = \prod_{j\neq i} p_j^{k_j} \neq p_i^{k_i} = \operatorname{ord} x_i, \quad i = 1, 2, \cdots, k.$$

因此 $P_i \cap \prod_{j\neq i} P_j = \{1\}, i = 1, 2, \cdots, k$. 从而 $P_i \cap P_j = \{1\}(i \neq j)$.

综上可知

$$G = \prod_{i=1}^{k} P_i, \quad P_i \lhd G, \quad 1 \leqslant i \leqslant k,$$

$$P_i \cap \prod_{j\neq i} P_j = \{1\}, \quad 1 \leqslant i \leqslant k,$$

故 $G = P_1 \otimes P_2 \otimes \cdots \otimes P_k$.

□