群的直积

- 设 G_1, G_2 为群, 则 G_1 与 G_2 (作为集合) 的乘积 $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ 在运算

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

下构成群. 因为结合律显然. 单位元为 $e = (e_1, e_2)$, 其中 e_1 是群 G_1 的单位元, e_2 是群 G_2 的单位元. 元素 (g_1, g_2) 的逆是 (g_1^{-1}, g_2^{-1}). 群 G 称为 G_1 与 G_2 的直积.

- 显然交换群的直积仍为交换群, 且有限群直积的阶等于群的阶的乘积. 若 $H_1 \leq (\trianglelefteq) G_1$, $H_2 \leq (\trianglelefteq) G_2$, 则显然有 $H_1 \times H_2 \leq (\trianglelefteq) G_1 \times G_2$. 特别地, $G_1 \times G_2$ 有正规子群 $\{e_1\} \times G_2$ 和 $G_1 \times \{e_2\}$.
- 容易验证 $G_1 \times G_2 \cong G_2 \times G_1$ ($(g_1, g_2) \mapsto (g_2, g_1)$ 是一个同构映射), 又 $i_1(a) = (a, e_2)$, $i_2(b) = (e_1, b)$ 分别为 G_1, G_2 到 $G_1 \times G_2$ 的单同态, $p_1(a, b) = a$, $p_2(a, b) = b$ 分别为 $G_1 \times G_2$ 到 G_1, G_2 的满同态. 故

$$G_1 \cong i_1(G_1) = \mathrm{Ker} p_2 = G_1 \times \{e_2\},$$
$$G_2 \cong i_2(G_2) = \mathrm{Ker} p_1 = \{e_1\} \times G_2.$$

- 设群 $B \cong C$, 则对任意群 A 有 $A \times B \cong A \times C$. 反之是否成立?

循环群的直积

- 类似地, 也可以定义任意 n 个群的直积, 且也有如上类似性质. 例如域 F 上的 n 维向量空间 F^n 的加法群就是 n 个 F 的加法群的直积.
- 定理: 若正整数 m 与 n 互素, 则 m 阶循环群与 n 阶循环群的直积为 mn 阶循环群.
- 证明: 设 $G_1 = \langle a \rangle$ 为 m 阶循环群, $G_2 = \langle b \rangle$ 为 n 阶循环群, 则 (a, e_2) 和 (e_1, b) 在群 $G_1 \times G_2$ 中的阶依然为 m 和 n. 由于元素 (a, e_2) 和 (e_1, b) 可交换, 阶又互素, 所以 $(a, b) = (a, e_2)(e_1, b)$ 在群 $G_1 \times G_2$ 中的阶为 mn, 从而 $G_1 \times G_2$ 为循环群.
- 上面的定理中若 m 与 n 不互素, 设 $\ell = \mathrm{lcm}(m, n)$, 则 $\ell < mn$. 又对任意 $(g_1, g_2) \in G_1 \times G_2$, 有 $(g_1, g_2)^\ell = (g_1^\ell, g_2^\ell) = (e_1, e_2)$, 这表明 $G_1 \times G_2$ 中无 mn 阶元, 从而 $G_1 \times G_2$ 不是循环群, 即两个阶数不互素的循环群的直积不再是循环群.
- 一般地, 设 $G = G_1 \times G_2$, $g_1 \in G_1$, $g_2 \in G_2$, 则 $o(g_1, g_2) = \mathrm{lcm}(o(g_1), o(g_2))$. 此结论也可推广到任意 n 个群的直积.
- 练习: 设 G_1 和 G_2 都是非单位循环群, 若 G_1 和 G_2 中至少有一个为无限循环群, 则 $G_1 \times G_2$ 不是循环群.

中国剩余定理

- 定理 (中国剩余定理): 设正整数 m 与 n 互素, a, b 是任意整数, 则同余方程组

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$$

有整数解. 进一步地, 若 x 和 y 都是解, 则有 $x \equiv y \pmod{mn}$.

- 证明: 考虑整数模 m 和模 n 的加法群 $\mathbb{Z}_m$ 和 $\mathbb{Z}_n$, 它们分别为 m 阶和 n 阶循环群, 由于 m 与 n 互素, $\mathbb{Z}_m \times \mathbb{Z}_n$ 为 mn 阶循环群且 $(1_m, 1_n)$ 是其生成元. 对任意整数 a 和 b, $(a \pmod{m}, b \pmod{n}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, 所以存在整数 x 使得

$$(a \pmod{m}, b \pmod{n}) = x(1_m, 1_n) = (x \pmod{m}, x \pmod{n}),$$

即有 $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$. 进一步地, 若 x 和 y 都是解, 则有 $x(1_m, 1_n) = (a \pmod{m}, b \pmod{n}) = y(1_m, 1_n)$, 从而 $x \equiv y \pmod{mn}$.

- 如何求上述同余方程组的解? 由于 m 与 n 互素, 存在整数 u, v 使得 $um + vn = 1$, 令 $x = avn + bum$ 即可.

群直积的子群

- 若 $H_1 \leq (\trianglelefteq) G_1$, $H_2 \leq (\trianglelefteq) G_2$, 则有 $H_1 \times H_2 \leq (\trianglelefteq) G_1 \times G_2$. 反之如何?
- 定理: 设有限群 G_1 和 G_2 的阶互素, 则 $G_1 \times G_2$ 的子群一定为 $H_1 \times H_2$, 其中 $H_1 \leq G_1$, $H_2 \leq G_2$.
- 证明: 设 $K \leq G_1 \times G_2$. 由于 $p_1(a,b) = a$, $p_2(a,b) = b$ 分别为 $G_1 \times G_2$ 到 G_1 和到 G_2 的满同态, 令 $H_1 = p_1(K)$, $H_2 = p_2(K)$, 则显然有 $H_1 \leq G_1$, $H_2 \leq G_2$, 下面证明 $K = H_1 \times H_2$.
- 事实上, 对于 $(a,b) \in K$, 由定义 $a \in H_1$, $b \in H_2$, 所以 $(a,b) \in H_1 \times H_2$, 故 $K \subseteq H_1 \times H_2$. 另一方面, 对于 $a \in H_1$, 由定义存在某个 $c \in G_2$ 使得 $(a,c) \in K$. 设 $m = o(a)$, $n = o(c)$, 由于 G_1 和 G_2 的阶互素, 由 Lagrange 定理有 m 与 n 互素. 利用中国剩余定理, 存在整数 r 满足 $r \equiv 1 \pmod{m}$ 和 $r \equiv 0 \pmod{n}$. 故有 $a^r = a^1 = a$ 和 $c^r = c^0 = e_2$, 由此得到 $(a, e_2) = (a,c)^r \in K$. 同理可以证明对于 $b \in H_2$, $(e_1, b) \in K$. 从而对任意 $a \in H_1$, $b \in H_2$ 有 $(a,b) = (a,e_2)(e_1,b) \in K$, 故 $H_1 \times H_2 \subseteq K$.
- 问如上定理中若有限群 G_1 和 G_2 的阶不互素, 则结论如何?

(内) 直积

- 定理: 设 G 为群, H, K 为 G 的两个子群, 且满足: (i) $G = HK$, (ii) $H \cap K = \{e\}$, (iii) H 中每个元素与 K 中每个元素可交换, 则 $G \cong H \times K$.
- 证明: 构作映射 $\sigma : H \times K \to G$ 为 $\sigma(h, k) = hk$, 对任意 $h \in H$, $k \in K$. 由 (i) 知 σ 为满射. 若 $\sigma(h_1, k_1) = \sigma(h_2, k_2)$, 即 $h_1k_1 = h_2k_2$, 从而 $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, 由 (ii) 知 $h_1 = h_2$, $k_1 = k_2$, 故 σ 为单射. 进一步地, $\sigma((h_1, k_1)(h_2, k_2))) = \sigma(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2)$, 由 (iii) 知 $h_2k_1 = k_1h_2$, 故 $\sigma((h_1, k_1)(h_2, k_2))) = (h_1h_2)(k_1k_2)$ $= (h_1k_1)(h_2k_2) = \sigma(h_1, k_1)\sigma(h_2, k_2)$, 即 σ 保持运算, 故 σ 为同构.
- 注: (1) 定理的条件 (i) 和 (ii) 保证 G 中每个元素可唯一地表成 H 与 K 中的元素的乘积. (2) 定理的条件 (i) 和 (iii) 保证 H 和 K 都是 G 的正规子群. (3) 定理的条件 (iii) 也可以换成 H 和 K 都是 G 的正规子群. (4) 在上面定理中, 也称群 G 为它的子群 H 和 K 的 (内) 直积, 习惯上也记为 $G = H \times K$. (5) 类似地, 也可得到一个群是它的多个子群 (内) 直积的条件.

素数平方阶群和整数模 n 的乘法群

- 定理: 设 p 为素数, G 为 p^2 阶群, 则 G 或为循环群或为两个 p 阶循环群的直积. 故 p^2 阶群一定交换.
- 证明: G 中非单位元的阶为 p^2 或者 p. 若 G 中有 p^2 阶元, 则它为循环群. 若 G 中无 p^2 阶元, 则 G 中每个非单位元的阶均为 p. 由于 p-群的中心非单位, 可从 $Z(G)$ 中选取一个非单位元 a, 则 $\langle a\rangle$ 为 p 阶循环群, 还可以从 $G\backslash\langle a\rangle$ 中选取一个非单位元 b, 同样 $\langle b\rangle$ 也是 p 阶循环群. 由于 $b\notin\langle a\rangle$, $\langle a\rangle\cap\langle b\rangle=\{e\}$, 从而 $|\langle a\rangle\langle b\rangle|=p^2$, 因此 $G=\langle a\rangle\langle b\rangle$. 又 $a\in Z(G)$, 因此 $\langle a\rangle$ 中每个元素与 $\langle b\rangle$ 中每个元素可交换. 从而 $G\cong\langle a\rangle\times\langle b\rangle$ 为两个 p 阶循环群的直积.
- 设正整数 s 与 t 互素, 则易知 $U(st)\cong U(s)\times U(t)$. (事实上, $x\mapsto(x\ (\mathrm{mod}\, s), x\ (\mathrm{mod}\, t))$ 是 $U(st)$ 到 $U(s)\times U(t)$ 的同构映射.)
- 设 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ 为 n 的素因子分解式, 则

$$U(n)\cong U(p_1^{e_1})\times U(p_2^{e_2})\times\cdots\times U(p_k^{e_k}).$$

- Gauss 证明了: $U(2)\cong\{1\}$, $U(4)\cong\mathbb{Z}_2$, 当 $m\geq 3$ 时有 $U(2^m)\cong\mathbb{Z}_2\times\mathbb{Z}_{2^{m-2}}$, 对任意奇素数 p 和任意正整数 m 有 $U(p^m)\cong\mathbb{Z}_{\phi(p^m)}$, 其中 $\phi(p^m)=p^m-p^{m-1}$.

群在群上的同构作用

- 群 G 在集合 M 上的作用即群 G 到 M 上的全变换群 S_M 的同态.
- 设 H, K 是两个群, H 的自同构群 $\mathrm{Aut}(H)$ 是 S_H 的一个子群. 称群同态 $\varphi : K \to \mathrm{Aut}(H)$ 为群 K 在群 H 上的一个同构作用. (这自然是 K 在集合 H 上的一个群作用)
- 例:
  (1) 对任意 $y \in K$, 定义 $\varphi(y) = I_H$, 即 H 的恒等自同构, 则显然 $\varphi : K \to \mathrm{Aut}(H)$ 为群同态, 称其为 K 在 H 上的平凡同构作用.
  (2) 设 F 为域, F 在加法下构成群, F 的非零元集 F^* 在乘法下构成群. 对任意 $t \in F^*$, $\varphi_t : F \to F$ 定义为 $\varphi_t(x) = tx$ 是加法群 F 的自同构. 容易验证 $\varphi : F^* \to \mathrm{Aut}(F)$, 其中 $\varphi(t) = \varphi_t$, 为群同态, 这便得到一个域 F 的乘法群 F^* 在域 F 的加法群上的同构作用.
  (3) 设 G 为群, $H \trianglelefteq G$, $K \leq G$. 对任意 $y \in K$, $\varphi_y : x \mapsto yxy^{-1}$ 是群 H 的自同构, 从而 $\varphi : y \mapsto \varphi_y$ 是 K 到 $\mathrm{Aut}(H)$ 的同态, 即 φ 是 K 在 H 上的一个同构作用. 称为 K 在 H 上的共轭作用.
  (4) 对任意群 H, 设 $K \leq \mathrm{Aut}(H)$, 则包含映射 $i : K \to \mathrm{Aut}(H)$ $(i(y) = y, \forall y \in K)$ 显然是一个同构作用.

半直积

- 设 H, K 是两个群, φ 是 K 在 H 上的同构作用, 并对任意 $y \in K$, 记 $\varphi_y = \varphi(y) \in \mathrm{Aut}(H)$. 在集合 $H \times K$ 上定义运算如下, 对 $(x, y), (u, v) \in H \times K$,

$$(x, y)(u, v) = (x\varphi_y(u), yv).$$

  容易验证 $H \times K$ 在如上运算下构成一个群, 称为群 H 和 K (关于 φ) 的半直积, 记为 $H \rtimes_\varphi K$.
- 结合律直接验证. 群 $H \rtimes_\varphi K$ 的单位元为 (e_H, e_K), $(x, y)^{-1} = (\varphi_{y^{-1}}(x^{-1}), y^{-1})$.
- 若 φ 是 K 在 H 上的平凡同构作用, 则 $H \rtimes_\varphi K$ 恰为直积 $H \times K$.
- 若 φ 不是 K 在 H 上的平凡同构作用, 则 $H \rtimes_\varphi K$ 一定是非交换群 (不论 H, K 是否交换). 事实上, 因为 φ 非平凡, 存在 $y \in K$ 和 $x \in H$ 使得 $\varphi_y(x) \neq x$. 从而

$$(x, e_K)(e_H, y) = (x, y) \neq (\varphi_y(x), y) = (e_H, y)(x, e_K).$$

- 例: 设 $H = \langle x \rangle$ 为 n 阶循环群, $K = \langle a \rangle$ 为 2 阶循环群, $\varphi_a : x \mapsto x^{-1}$. 则半直积 $H \rtimes_\varphi K$ 恰为二面体群 D_n.

半直积

- 例: 设 $H = \mathbb{Z}_3 = \{0, 1, 2\}$ 为 3 阶循环群 (运算写成加法), $\mathrm{Aut}(\mathbb{Z}_3) \cong U(3)$ 为 2 阶群, 其非单位元为负自同构 $\theta : x \mapsto -x$. 设 $K = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ 为 4 阶循环群 (运算也写成加法), 其生成元为 1. 所以从 $\mathbb{Z}_4$ 出发的群同态 φ 被 $\varphi(1) = \varphi_1$ 所唯一确定. 定义 $\varphi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3)$ 为 $\varphi_1 = \theta$, 即 $\varphi_0 = \varphi_1^0, \varphi_2 = \varphi_1^2$ 为恒等自同构而 $\varphi_1, \varphi_3 = \varphi_1^3$ 为负自同构 θ, 或对于 $n \in \mathbb{Z}_4$, $\varphi_n(x) = (-1)^n x$. 由此得到的半直积 $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ 为 12 阶非交换群, 其中的运算为

$$(x, n)(y, m) = (x + (-1)^n y, n + m).$$

- 交错群 A_4 和二面体群 D_6 都是 12 阶非交换群, $A_4 \ncong D_6$, 因为 A_4 中无 6 阶元而 D_6 中有 6 阶元. 而如上得到的 $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ 既不同构于 A_4, 也不同构于 D_6. 事实上, A_4 和 D_6 中都没有 4 阶元, 而 $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ 中有 4 阶元 $(1, 1)$.
- 现在我们已有三个互不同构的 12 阶非交换群: A_4, D_6 和 $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$.
- $i_H : x \mapsto (x, e_K)$ 和 $i_K : y \mapsto (e_H, y)$ 分别是 H 和 K 到 $H \rtimes_\varphi K$ 的单同态, 所以 $H \times \{e_K\}$ 和 $\{e_H\} \times K$ 都是 $H \rtimes_\varphi K$ 的子群, 且 $H \cong H \times \{e_K\}$, $K \cong \{e_H\} \times K$.

半直积

- $p_K : (x, y) \mapsto y$ 是 K 到 $H \rtimes_\varphi K$ 的满同态, $\mathrm{Ker} p_K = H \times \{e_K\}$, 从而 $H \times \{e_K\} \trianglelefteq H \rtimes_\varphi K$, 也可以说 H 是 $H \rtimes_\varphi K$ 的一个正规子群. 但是若 φ 非平凡, 则 $p_H : H \rtimes_\varphi K \to H$ 定义为 $p_H(x, y) = x$, 不是群同态, 所以 K 看作是 $\{e_H\} \times K$ 不是 $H \rtimes_\varphi K$ 的正规子群.
- 交 $H \cap K$ (即 $(H \times \{e_K\}) \cap (\{e_H\} \times K)$) 是单位元群.
- 定理: 设 G 为群, H, K 为 G 的两个子群, 且满足: (i) $G = HK$, (ii) $H \cap K = \{e\}$, (iii) $H \trianglelefteq G$, 则 $G \cong H \rtimes_\varphi K$, 其中 φ 是 K 在 H 上的共轭作用, 即对任意 $y \in K$, $x \in H$, $\varphi_y(x) = yxy^{-1}$.
- 证明: 构作映射 $\sigma : H \times K \to G$ 为 $\sigma(h, k) = hk$, 对任意 $h \in H$, $k \in K$. 由 (i) 知 σ 为满射. 若 $\sigma(h_1, k_1) = \sigma(h_2, k_2)$, 即 $h_1 k_1 = h_2 k_2$, 从而 $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$, 由 (ii) 知 $h_1 = h_2$, $k_1 = k_2$, 故 σ 为单射. 进一步地,

$$\sigma((h_1, k_1)(h_2, k_2))) = \sigma(h_1 \varphi_{k_1}(h_2), k_1 k_2) = \sigma(h_1 k_1 h_2 k_1^{-1}, k_1 k_2)$$
$$= h_1 k_1 h_2 k_1^{-1} k_1 k_2 = h_1 k_1 h_2 k_2 = \sigma(h_1, k_1)\sigma(h_2, k_2),$$

  即 σ 保持运算, 故 σ 为同构.
- 例: 当 $n \geq 3$ 时, 由如上定理可得 $S_n = A_n \rtimes \langle (12) \rangle$.

作业

- P27: 44, 45. P57: 9. P58: 22.

1. 设 G_1 和 G_2 为有限群, 若 $G_1 \times G_2$ 为循环群, 证明 G_1 和 G_2 都是循环群且阶互素.
2. 设 G_1 和 G_2 都是非单位循环群, 若 G_1 和 G_2 中至少有一个为无限循环群, 则 $G_1 \times G_2$ 不是循环群.
3. 设 $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$, 证明 $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ 且 $(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.
4. 设 H, K, L 都是 G 的正规子群, 满足 $G = HKL = \{abc \mid a \in H, b \in K, c \in L\}$ 和 $H \cap (KL) = K \cap (HL) = L \cap (HK) = \{e\}$, 证明 $G \cong H \times K \times L$.
5. 设 H, K 是有限群 G 的正规子群满足 $G = HK$ 且 H 与 K 的阶互素, 证明 G 的任意子群 L 可以写成 $L = (H \cap L)(K \cap L)$.
6. 设群 G_1 和 G_2 都是非单位元群, 若 $G_1 \times G_2$ 的每个子群一定为 $H_1 \times H_2$, 其中 $H_1 \leq G_1$, $H_2 \leq G_2$. 则 G_1 和 G_2 中每个元素的阶都有限并且对任意 $a \in G_1$ 和 $b \in G_2$, $o(a)$ 与 $o(b)$ 互素.
7. 设 n 为奇数, 证明 $D_{2n} \cong D_n \times \mathbb{Z}_2$.

Sylow 定理

- 设 G 为 n 阶群, 由 Lagrange 定理得知 G 的子群的阶为 n 的因子. 反之, 对于 n 的因子 d, G 是否一定有 d 阶子群? 一般说来不一定有, 例如 A_4 无 6 阶子群.
- 下面设 p 是 n 的一个素因子, 记 $n = p^r m$, 其中 $p \nmid m$ (称 p^r 为 n 的 p 部分而 m 为 n 的非 p 部分, 也称 n 的 p-adic 阶为 r), 则 G 中是否有 p 阶元? 对于 $1 \leq k \leq r$, G 是否有 p^k 阶子群? 下面的 Sylow 定理就肯定地回答了这些问题.
- 注: Sylow 为挪威数学家, 生于 1832 年, 曾获数学竞赛奖. 成年后一直任中学数学教师, 作为业余爱好研究群结构并在克里斯蒂安尼亚大学 (现奥斯陆大学) 上课, Sophus Lie (李群李代数的发现者) 曾是他班上的学生. Sylow 定理发表后, 他一举成名, 但他拒绝了任大学教授的邀请, 直到退休后才在 Sophus Lie 的坚持下接受了大学的教授职位. Sylow 还花了 8 年时间与 Sophus Lie 一起编辑 Abel 的数学全集.
- 为了证明如下的 Sylow 定理, 首先介绍一个初等数论的基本结论.

组合数的 p 部分

- 引理：设 p 是一个素数，$n = p^r m$，$p \nmid m$，则对于任意 $0 \le k \le r$ 有

$$p^{r-k} \Big\| \binom{n}{p^k},$$

即 $\binom{n}{p^k}$ 的 p 部分为 p^{r-k}（或 $\binom{n}{p^k}$ 的 p-adic 阶为 $r-k$）.

- 证明思路：根据

$$\binom{n}{p^k} = \frac{n!}{(n-p^k)! \cdot p^k!}$$

以及 $n!$ 的 p 部分 p^s 的幂指数 s 的计算公式

$$s = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

可证. 也可以通过比较

$$\binom{n}{p^k} = \frac{n(n-1)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots 1}$$

分子分母中的对应因子 $n-j$ 和 p^k-j，$1 \le j \le p^k-1$，的 p 部分得到证明.

Sylow 定理

- 定理 (Sylow 第一定理)：设群 G 的阶为 $n = p^r m$, 其中 p 为素数且 $p \nmid m$, $r > 0$, 那么对于满足 $1 \leq k \leq r$ 的任一 k, G 一定有 p^k 阶的子群.
- 证明: 设 Ω 是 G 的所有 p^k 元子集构成的集合. 这时 Ω 的元素可表示为

$$A = \{a_1, a_2, \cdots, a_{p^k}\}.$$

对于 $g \in G$, 我们定义

$$gA = \{ga_1, ga_2, \cdots, ga_{p^k}\},$$

则 $(g, A) \mapsto gA$ 是群 G 在 Ω 上的一个作用 (G 在 Ω 上的左乘作用). 所以

$$\Omega = \bigcup_{i=1}^{t} O_{A_i},$$

这里 O_{A_i}, $1 \leq i \leq t$, 是群作用的所有互不相同的轨道. 故

$$|\Omega| = \sum_{i=1}^{t} |O_{A_i}|.$$

Sylow 定理

- 有引理我们得到

$$p^{r-k+1} \nmid |\Omega| = \binom{n}{p^k}.$$

因此至少有一条轨道 O_{A_j} 满足 $p^{r-k+1} \nmid |O_{A_j}|$. 可以证明 G_{A_j} 就是 G 的一个 p^k 阶子群. 事实上, 根据轨道-稳定子定理有

$$|G| = |O_{A_j}| \cdot |G_{A_j}|$$

$$|G_{A_j}| = p^k q \geq p^k. \tag{1}$$

- 另一方面, 对于 $g \in G_{A_j}$, 由 $gA_j = A_j$ 得到对于 $a \in A_j$, 有 $ga \in A_j$, 所以右陪集 $G_{A_j}a = \{ga : \ g \in G_{A_j}\} \subseteq A_j$, 故

$$|G_{A_j}| = |G_{A_j} \cdot a| \leq |A_j| = p^k. \tag{2}$$

由 (1) 和 (2) 我们得到 $|G_{A_j}| = p^k$.

- 推论: (1) Cauchy 定理: 若素数 p 整除有限群 G 的阶, 则 G 中一定有 p 阶元.
(2) G 的 p^r 阶子群存在, 称这样的子群为 G 的 Sylow p-子群.

Sylow 定理

- 定理 (Sylow 第二定理)：设 K 为有限群 G 的子群，其阶可被素数 p 整除，P 是 G 的一个 Sylow p-子群，则存在 P 的某个共轭子群 $P' = aPa^{-1}$ 使得 $P' \cap K$ 是 K 的 Sylow p-子群.
- 证明：考虑 K 在 G 关于 P 的左商集 $X = (G/P)_l = \{aP \mid a \in G\}$ 上的左乘作用，即对 $g \in K$，定义 $g \circ (aP) = (ga)P$. 由于 $p \nmid |X|$，故存在 $x = aP \in X$，使得包含 x 的轨道 O_x 满足 $p \nmid |O_x|$. 而在此作用下 x 的稳定子群是 $K_x = aPa^{-1} \cap K$，故 K_x 为 $P' = aPa^{-1}$ 的子群，从而 $|K_x|$ 为 p 的方幂. 再由 $|O_x| \cdot |K_x| = |K|$ 和 $p \nmid |O_x|$ 知 $|K_x|$ 恰为 $|K|$ 的 p 部分，即 K_x 是 K 的 Sylow p-子群.
- 推论：(1) 有限群 G 的任意 p-子群一定为 G 的某个 Sylow p-子群的子群. (2) 有限群 G 的任意两个 Sylow p-子群一定共轭，从而 G 的 Sylow p-子群正规当且仅当其 Sylow p-子群只有一个.
- 证明：(1) 设 K 为 p-群，则 K 的 Sylow p-子群是其自身，即 $P' \cap K = K$，故 $K \leq P'$. (2) 特别地，若 K 也是 G 的 Sylow p-子群，由 $|K| = |P'|$ 知 $K = P' = aPa^{-1}$.

Sylow 定理

- 定理 (Sylow 第三定理)：设群 G 的阶为 $n = p^r m$, 其中 p 为素数且 $p \nmid m$, $r > 0$, 记 n_p 为 G 的 Sylow p-子群个数, 则

$$n_p \mid m, \quad \text{且} \quad n_p \equiv 1 \pmod{p}.$$

- 证明: 设 P 是 G 的一个 Sylow p-子群, 记 G 的所有 Sylow p-子群组成的集合为 $X = \{aPa^{-1} \mid a \in G\}$, 显然 $|X| = n_p$. 考虑 P 在此集合 X 上的共轭作用, 即对 $g \in P$, 定义 $g \circ (aPa^{-1}) = g(aPa^{-1})g^{-1} = (ga)P(ga)^{-1}$. 此作用每个轨道的长度都是 $|P|$ 的因子, 从而为 p 的方幂. 显然此作用下包含 P 的轨道为 $\{P\}$. 反之对任一包含一个元素的轨道 $\{P_i\}$, 即对任意 $g \in P$, 都有 $gP_ig^{-1} = P_i$, 则有 $P \leq N_G(P_i)$, 即 P 也是 $N_G(P_i)$ 的一个 Sylow p-子群. 又 P_i 是 $N_G(P_i)$ 的正规 Sylow p-子群, 从而 $P_i = P$, 这就证出只有一个轨道包含 1 个元素. 而此作用的其它轨道长度被 p 整除, 所以 $n_p \equiv 1 \pmod{p}$. 进一步地, P 的共轭子群个数为 $[G : N_G(P)]$, 所以 $n_p \mid |G| = p^r m$. 由于 n_p 与 p 互素, 所以 $n_p \mid m$.
- 注：类似地可以证明对于任意正整数 $k \leq r$, G 的 p^k 阶子群的个数模 p 余 1.

Sylow 定理的应用

- 命题：设 p, q 为素数，则 pq 和 p^2q 阶群都不是单群.
- 证明：$p = q$ 时的情形显然，下面设 $p \neq q$. 设 G 为 pq 阶群，不妨设 $q > p$，则由 $n_q \mid p$ 且 $n_q \equiv 1 \pmod{q}$ 知 $n_q = 1$，于是 G 的 Sylow q-子群唯一，从而正规.
- 设 G 为 p^2q 阶群. 若 $p > q$，则如上推理可得 $n_p = 1$，G 不是单群. 若 $p < q$，则 $n_q = 1$ 或 p^2. 若 $n_q = p^2$，则 G 有 p^2 个 q 阶群，这时 G 中的 q 阶元个数为 $p^2(q-1)$，故 G 中其它阶的元素 (包括单位元) 有 p^2 个，这时 $N_p = 1$.
- 注：著名的 Burnside p^aq^b 定理是说对于不同素数 p, q, a, b 为正整数，则 p^aq^b 阶群都是可解群，从而不是单群.
- 命题：设 p 为奇素数，则 $2p$ 阶群或为循环群，或为二面体群.
- 证明思路：设 G 为 $2p$ 阶群，G 的 Sylow p-子群 P 为循环群且正规，可得 G 的右陪集分解为 $G = \langle a \rangle \cup \langle a \rangle b$. 若 $o(ab) = 2p$，则 G 循环. 若 $o(ab) = 2$，则有 $bab = a^{-1}$，这时 G 为二面体群 D_p. 再证 ab 的阶不能为 p. (若 $o(ab) = p$，因为 $\langle a \rangle \trianglelefteq G$，而 $\langle a \rangle b$ 在群 $G/\langle a \rangle$ 中的阶为 2，则 $\langle a \rangle = \langle a \rangle (ab)^p = (\langle a \rangle ab)^p = (\langle a \rangle b)^p = \langle a \rangle b$，矛盾.)

Sylow 定理的应用

- 定理：最小有限非交换单群同构于交错群 A_5.
- 命题：若有限群 G 的阶 < 60, 则 G 不是非交换单群.
- 证明：我们已知素数阶群为循环群, 这是交换单群. 素数幂次 (次数 ≥ 2) 阶群不是单群 (考虑群的中心). pq, p^2q 阶群 (p, q 为不相同的素数) 不是单群. $2m$ 阶群 (m 为奇数) 不是单群. 故只需考虑 $n = |G| = 24, 36, 40, 48, 56$ 的情形.
- (a): $n = 24 = 2^3 \cdot 3$, 则 $n_2 = 1$ 或 3. 若 $n_2 = 3$, 则 G 在这三个 G 的 Sylow 2-子群上的共轭作用诱导了群同态 $\rho : G \to S_3$. 显然 $\mathrm{Ker}\rho$ 为 G 的非平凡正规子群, (显然 ρ 非单. 若 $\mathrm{Ker}\rho = G$, 则对任意 $g \in G$ 和 G 的一个 Sylow 2-子群 P 有 $gPg^{-1} = P$, 与 G 的 Sylow 2-子群不唯一矛盾) 故 G 非单. 同理可得 $n = 48$ 的情形.
- (b): $n = 36 = 2^2 \cdot 3^2$, 则 $n_3 = 1$ 或 4. 若 $n_3 = 4$, 则 G 在这四个 G 的 Sylow 3-子群上的共轭作用诱导了群同态 $\rho : G \to S_4$. 易证 $\mathrm{Ker}\rho$ 为 G 的非平凡正规子群, 故 G 非单.
- (c): $n = 40 = 2^3 \cdot 5$, 则 $n_5 = 1$, G 非单.
- (d): $n = 56 = 2^3 \cdot 7$, 则 $n_7 = 1$ 或 8. 若 $n_7 = 8$, 则 G 中的 7 阶元个数为 $8(7-1) = 48$, 故 G 其它阶元素只有 8 个, 故 $n_2 = 1$, G 非单.

Sylow 定理的应用

- 命题: 设 G 是 60 阶单群, 则 $G \cong A_5$.
- 证明: (a) 首先证明 G 无指数为 $2 \leq m \leq 4$ 的子群. 事实上, 如果 $[G:H]=m$, 则 G 在 H 的左陪集上的左乘作用诱导非平凡同态 $\rho: G \to S_m$. 若 $m \leq 4$, 则 $\mathrm{Ker}\rho$ 为 G 的非平凡正规子群.
- (b) G 有指数为 5 的子群 H. 事实上, 考虑 G 的 Sylow 2-子群, 则 $n_2 = 5$ 或者 15. (若 $n_2 = 3$, 则 G 的一个 Sylow 2-子群的正规化子为指数为 3 的子群) 如果 $n_2 = 5$, 则可取 H 为 G 的一个 Sylow 2-子群的正规化子. 若 $n_2 = 15$, 则 $n_3 = 10$ 且 $n_5 = 6$. 这时 G 中 5 阶元和 3 阶元共有 $20 + 24 = 44$ 个, 故必存在 G 的两个 Sylow 2-子群 P_1, P_2 使得 $P_1 \cap P_2 \neq \{e\}$. 记 $P_1 \cap P_2 = \{e, x\}$, $H = \langle P_1, P_2 \rangle$. 由于 P_1, P_2 均为交换群, $\langle x \rangle \trianglelefteq H$, 所以 $H \neq G$. 又 $4 \mid |H| \mid 60$ 和 $|H| > 4$ 得到 $|H| = 12$ 或 20, 再利用上面的 (a), 可得 $|H| = 12$, 即为 G 的指数为 5 的子群.
- (c) 考察 G 在 H 的左陪集上的左乘作用诱导非平凡同态 $\rho: G \to S_5$. 故 $\mathrm{Ker}\rho = \{e\}$, 即 ρ 为单同态, 因此 $G \cong M \leq S_5$. 由于 $[S_5 : M] = 2$, 所以 $M \trianglelefteq S_5$, 从而 $M \cap A_5 \trianglelefteq A_5$, 又 $M \cap A_5 \neq \{e\}$ (否则 $|MA_5| = |M||A_5| = 60^2 > 120 = |S_5|$, 矛盾), 故 $M = A_5$.

pq 阶群

- 例: 设 $p < q$ 为素数, 确定所有的 pq 阶群.
- 阶: 设 G 为 pq 阶群. 由 Sylow 定理和 $p < q$ 得到 G 的 Sylow q-子群 $Q \trianglelefteq G$, 设 P 是 G 的一个 Sylow p-子群. 由于 P, Q 的阶都是素数, 所以它们都是循环群. 又显然 $Q \cap P = \{e\}$, 所以 $|QP| = |Q||P|/|Q \cap P| = pq = |G|$, 所以 $G = QP$. 从而 G 是 Q 和 P 的一个半直积, 即 $G \cong Q \rtimes_\varphi P$. (注意现在我们不知道群 G, 所以也不知道 P 在 Q 上的共轭作用 φ 到底是什么. 下面我们来确定 φ)
- Q 是 q 阶循环群, 所以 $\mathrm{Aut}(Q) = U(q)$ 为 $q-1$ 阶循环群. $\varphi : P \to \mathrm{Aut}(Q)$ 是群同态, 对于任意 $y \in P$, $o(y) \mid p$, 所以 $o(\varphi_y) \mid o(y) \mid p$, 又 $o(\varphi_y) \mid q-1$, 所以 $o(\varphi_y) \mid \gcd(p, q-1)$.
- 若 $p \nmid (q-1)$, 则对于任意 $y \in P$, $o(\varphi_y) = 1$, 即 φ_y 为 Q 的恒等自同构, φ 是平凡的同构作用, 所以 $G \cong Q \times P$. 又 Q, P 为阶数互素的循环群, 所以 G 为循环群. (若素数 $p < q$ 满足 $p \nmid (q-1)$, 则 pq 阶群一定为循环群. 例如 $2021 = 43 \cdot 47$ 阶群一定循环.)
- 下面设 $p \mid (q-1)$. 若作用 φ 平凡, 则 G 为循环群. 那么这时是否存在 P 在 Q 上的非平凡同构作用?

pq 阶群

- 由于 P 是 p 阶群, 设 $P = \langle a \rangle$. 则同态 $\varphi : P \to \mathrm{Aut}(Q)$ 被 φ_a 所唯一确定. 若 $o(\varphi_a) = 1$, 则 φ 平凡, 所以下面设 $o(\varphi_a) = p$. 因为 $p \mid (q-1)$, $\mathrm{Aut}(Q) = U(q)$ 有唯一的 p 阶循环子群 $\langle \alpha \rangle$. 从而 $\varphi_a \in \langle \alpha \rangle$, 即 $\varphi_a = \alpha^j$ 对某个 $1 \leq j \leq p-1$. 不妨取 $\varphi_a = \alpha$, 则对任意 $a^i \in P$, 有 $\varphi_{a^i} = \alpha^i$, 我们得到一个 P 在 Q 上的非平凡同构作用 φ, 由此有 $G \cong Q \rtimes_\varphi P$ 为 pq 阶非交换群.
- 进一步地, 对任意 P 在 Q 上的非平凡同构作用 ψ, 存在 $1 \leq m \leq p-1$ 使得 $\psi_a = \alpha^m$, 即 $\psi_a = \varphi_a^m$, 所以对于任意 $y = a^i \in P$,

$$\psi_y = \psi_{a^i} = \psi_a^i = (\varphi_a^m)^i = \varphi_a^{mi} = \varphi_{a^{mi}} = \varphi_{(a^i)^m} = \varphi_{y^m} = \varphi_y^m.$$

  定义 $\pi : Q \rtimes_\psi P \to Q \rtimes_\varphi P$ 为 $(x, y) \mapsto (x, y^m)$. 因为 $y \mapsto y^m$ 是循环群 P 的自同构, 所以 π 为双射, 还容易验证 π 保持运算, 从而 $Q \rtimes_\psi P \cong Q \rtimes_\varphi P$. 这表明由 P 在 Q 上的非平凡同构作用得到的 pq 阶群唯一.
- 对任意素数 $p < q$, 若 $p \nmid (q-1)$, 则 pq 阶群只有一个 (pq 阶循环群); 若 $p \mid (q-1)$, 则有 2 个 pq 阶群.

- 下面给出 π 保持运算的证明, 为了区分, 记 $Q \rtimes_\psi P$ 中的运算为 $\circ_\psi$, $Q \rtimes_\varphi P$ 中的运算为 $\circ_\varphi$. 对任意 $(x, y), (u, v) \in Q \rtimes_\psi P$,

$$\begin{aligned}\pi((x, y) \circ_\psi (u, v)) &= \pi(x\psi_y(u), yv) = (x\psi_y(u), (yv)^m) \\ &= (x\varphi_{y^m}(u), y^m v^m) = (x, y^m) \circ_\varphi (u, v^m) = \pi(x, y) \circ_\varphi \pi(u, v).\end{aligned}$$

- q 为素数, 所以 $\mathbb{Z}_q$ 为 q 元域, 其乘法群 $\mathbb{Z}_q^*$ 为 $q-1$ 阶循环群. 若 $p \mid (q-1)$, $\mathbb{Z}_q^*$ 有唯一的 p 阶子群 H. 考虑 $\mathbb{Z}_q$ 上的仿射群 $\mathrm{Aff}(\mathbb{Z}_q)$, 令

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in H, b \in \mathbb{Z}_q \right\},$$

则容易验证 $G \leq \mathrm{Aff}(\mathbb{Z}_q)$. 对于 $g \in H$ 且 $g \neq 1$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$$

不交换, 所以 G 为 pq 阶非交换群.

- 对任意素数 $p < q$, 若 $p \mid (q-1)$, 则 pq 阶群或为循环群或为如上定义的群 G.

何时 n 阶群一定循环?

- 我们知道素数阶群一定循环. 对于素数 $p < q$, 若 $p \nmid (q-1)$, 则 pq 阶群一定循环. 设 $n \geq 2$ 为正整数, 则 n 满足什么条件才能使 n 阶群一定循环?
- 首先若 n 有一个素因子 p 使得 $p^2 \mid n$, 则 n 阶群 $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{\frac{n}{p^2}}$ 不是循环群, 因为它有非循环子群 $\mathbb{Z}_p \times \mathbb{Z}_p$. 所以如果 n 阶群一定循环, 则 n 没有平方因子. 另外如果 n 有两个素因子 $p < q$ 满足 $p \mid (q-1)$, 设 G 是非交换的 pq 阶群 (上面已经构作出了), 则 n 阶群 $G \times \mathbb{Z}_{\frac{n}{pq}}$ 不交换, 从而也不是循环群. 所以如果 n 阶群一定循环, 则 n 不能有素因子 $p < q$ 使得 $p \mid (q-1)$.
- 设 $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ 为 n 的素因子分解式, 其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数, $e_i \geq 1$, $1 \leq i \leq k$. 则

$$\phi(n) = p_1^{e_1-1} p_2^{e_2-1} \cdots p_k^{e_k-1} (p_1-1)(p_2-1) \cdots (p_k-1).$$

  所以若 n 没有平方因子且 n 不存在素因子 $p < q$ 使得 $p \mid (q-1)$, 则一定有 $\gcd(n, \phi(n)) = 1$.
- 这样我们得到 n 阶群一定循环的一个必要条件是 $\gcd(n, \phi(n)) = 1$.

255 阶群

- 实际上 $\gcd(n, \phi(n)) = 1$ 也是 n 阶群一定循环的一个充分条件, 即设 n 为正整数, 则 n 阶群一定循环的充要条件为 $\gcd(n, \phi(n)) = 1$.
- 例: 设 $n = 255$. 容易计算出 $\phi(255) = 128$, 由 $\gcd(255, \phi(255)) = 1$ 知 255 阶群一定循环. 下面给出一个简单证明.
- 设 G 为 255 阶群. 由于 $255 = 3 \cdot 5 \cdot 17$, 容易得到 G 的 Sylow 17-子群唯一, 设 H 为 G 的 Sylow 17-子群, 故 H 为 17 阶循环群且 $H \trianglelefteq G$.
- 对 H 利用 N/C 定理, 由于 $H \trianglelefteq G$, 所以 $N_G(H) = G$, 从而 $G/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的一个子群, 故有 $|G/C_G(H)| \mid 255$ 和 $|G/C_G(H)| \mid 16$, (因为 $|\mathrm{Aut}(H)| = 16$) 由此得到 $|G/C_G(H)| = 1$, 故 $C_G(H) = G$, 这便得到 $H \leq Z(G)$. 从而 $|G/Z(G)| \mid 15$, (因为 $G/Z(G) \cong (G/H)/(Z(G)/H)$) 即 $|G/Z(G)| = 1, 3, 5$ 或者 15. 故 $G/Z(G)$ 为循环群, 由 G/Z 定理得到 G 交换.
- 所以, G 的 Sylow 3-子群和 Sylow 5-子群都是正规子群, 从而唯一. 设 K 为 G 的 Sylow 3-子群, L 为 G 的 Sylow 5-子群, 容易验证得到 $G = KLH$ 且 $K \cap LH = L \cap KH = H \cap KL = \{e\}$, 所以 $G \cong K \times L \times H$. 注意到 K, L, H 为阶数彼此互素的循环群, 从而 G 为循环群.

作业

- P64: 5, 6. P65: 12, 19, 20, 21.

1. 求 S_5 的 Sylow 5-子群的个数, 并写出一个这样的子群.
2. 设 $N \trianglelefteq G$ 且 N 为 p-群, 证明 G 的所有 Sylow p-子群都包含 N.
3. 设 $N \trianglelefteq G$, P 是 G 的一个 Sylow p-子群, 证明 $N \cap P$ 是 N 的 Sylow p-子群且 PN/N 是 G/N 的 Sylow p-子群.
4. 设 H 是 G 的一个 Sylow p-子群, $K = N_G(H)$, $L = N_G(K)$, 证明 $K = L$.
5. 设 K 是 G 的一个 Sylow p-子群, $K \not\trianglelefteq G$, 证明存在 G 的子群 H 使得 $H \cap K$ 不是 H 的 Sylow p-子群.
6. 证明 72 和 180 阶群不是单群.
7. 设 $p < q < r$ 为素数. 证明: pqr 阶群有唯一的 r 阶子群.
8. 证明 $D_n \leq S_n$ 并且 $D_n \leq A_n$ 当且仅当 $n \equiv 1 \pmod 4$. 进一步地, 设 p 为素数且 $p \equiv 3 \pmod 4$, 证明: A_p 无 $2p$ 阶子群.

有限交换群的结构

- 下面证明有限交换群是循环群的直积, 且分解是唯一的.
- 设 G 为 n 阶交换群, $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ 为 n 的标准分解式, 其中 $p_1, p_2, \ldots, p_s$ 为互不相同的素数, $e_i \geq 1$, $1 \leq i \leq s$.
- 对任意 $1 \leq i \leq s$, 设 P_i 为 G 的 Sylow p_i-子群, (因为 G 交换, 所以其 Sylow 子群正规, 从而 G 的 Sylow 子群唯一), 记 $\widetilde{P}_i = P_1 \cdots P_{i-1} P_{i+1} \cdots P_s$. 由交换性知 $P_1 P_2 \cdots P_s$ 和 $\widetilde{P}_i$ 都是 G 的子群, 再利用 $\left|P_i \cap \widetilde{P}_i\right| = 1$ 和对 s 的归纳知 $\left|\widetilde{P}_i\right| = n/p_i^{e_i}$ 和 $\left|P_1 P_2 \cdots P_s\right| = n$. 所以

$$G \cong P_1 \times P_2 \times \cdots \times P_s,$$

  即任一有限交换群是其 Sylow 子群的直积.
- 注: Lagrange 定理的逆对有限交换群成立, 即设 G 为 n 阶交换群, d 为正整数且 $d \mid n$, 则 G 有 d 阶子群.
- 所以我们只需讨论有限交换 p-群. 我们用两种方法证明如下定理.
- 定理: 设 A 是有限交换 p-群, a 是 A 中一个最高阶元素, 则存在 $B \leq A$ 使得 $A \cong \langle a \rangle \times B$.

有限交换群的结构

- 引理: 设 A 是有限交换 p-群, 则 A 循环当且仅当 A 只有一个 p 阶子群.
- 证明: 必要性显然. 下证充分性, 对 $|A|$ 做归纳. 设 A 只有一个 p 阶子群 P, 考虑映射 $\eta : a \mapsto a^p$, 这是群 A 的一个自同态. 对任意 $x \in P$, $x^p = e$, 所以 $P \leq \mathrm{Ker}\eta$, 反之对任意 $b \in \mathrm{Ker}\eta$, 若 $b \neq e$, 则 $o(b) = p$, 从而 $\langle b \rangle = P$, 即 $b \in P$, 故 $\mathrm{Ker}\eta \leq P$. 所以 $\mathrm{Ker}\eta = P$. 由同态基本定理有 $A/P \cong \eta(A)$. 如果 $\eta(A) = \{e\}$, 则 $A = P$ 为循环群. 若 $\eta(A) \neq \{e\}$, 则有 $P \leq \eta(A)$. 由归纳假设, $\eta(A)$ 循环, 设 $\eta(A) = \langle g \rangle$, 再设 a 是在 η 下 g 的一个原像, 即 $\eta(a) = a^p = g$, 于是 $|A|/p = |\eta(A)| = o(g) = o(a)/p$, 所以 $o(a) = |A|$, 故 $A = \langle a \rangle$.
- 对 $|A|$ 做归纳下面证明前面定理. 记 $o(a) = p^r$. 若 $o(a) = |A|$, 则 $A = \langle a \rangle$, 取 $B = \{e\}$ 即可. 若 A 非循环, 可取一个不含于 $\langle a \rangle$ 的 p 阶子群 P, 作 $\overline{A} = A/P$. 注意到 $o(aP) \mid o(a)$ 且若 $o(aP) < o(a)$ 可推出 $P = \langle a^{p^{r-1}} \rangle \leq \langle a \rangle$, 从而 $o(aP) = o(a)$, 故 aP 为 $\overline{A}$ 中最高阶元素. 由归纳假设, 存在 $\overline{B} \leq \overline{A}$ 使得 $\overline{A} \cong \langle aP \rangle \times \overline{B}$. 令 $\overline{B} = B/P$, 则 $B \geq P$ 且 $A = \langle a \rangle B$. 进一步地, 由 $\langle aP \rangle \cap \overline{B} = \{P\}$ 得到 $\langle a \rangle \cap B \leq P$, 由 $P \nleq \langle a \rangle$ 可得 $\langle a \rangle \cap B = \{e\}$. 所以 $A \cong \langle a \rangle \times B$.

有限交换群的结构

- 定理: 设 A 是有限交换 p-群, a 是 A 中一个最高阶元素, 则存在 $B \leq A$ 使得 $A \cong \langle a \rangle \times B$.
- 证明: 设 $o(a) = p^r$, $r \geq 1$, 且设 B 是满足 $\langle a \rangle \cap B = \{e\}$ 的 A 的最大子群 (注意这样的 B 一定存在). 下证一定有 $A = \langle a \rangle B$.
- 若否, 则存在 $x \in A \backslash \langle a \rangle B$. 设 $o(x) = p^s$, 则显然有 $1 \leq s \leq r$ 且 $x^{p^s} = e \in \langle a \rangle B$. 取 k 为满足 $x^{p^k} \in \langle a \rangle B$ 的最小正整数, 令 $y = x^{p^{k-1}}$, 则有 $y \notin \langle a \rangle B$ 但是 $y^p \in \langle a \rangle B$. 记 $y^p = a^m z$, 其中 m 为整数, $z \in B$. 若 $p \nmid m$, 则 $o(a^m) = p^r$, 从而 $(a^m)^{p^{r-1}} \neq e$. 由

$$e = y^{p^r} = (y^p)^{p^{r-1}} = (a^m)^{p^{r-1}} z^{p^{r-1}}$$

  得到 $(a^m)^{p^{r-1}} = z^{-p^{r-1}} \in \langle a \rangle \cap B$, 与 $\langle a \rangle \cap B = \{e\}$ 矛盾, 所以 $p \mid m$.
- 设 $m = pt$, 令 $w = ya^{-t}$, 则有 $w^p = z \in B$. 由于 $y \notin \langle a \rangle B$ 但是 $a^{-t} \in \langle a \rangle B$, 所以 $w \notin \langle a \rangle B$, 进而 $w \notin B$.
- 由 $w \notin B$ 得到 $\langle w \rangle B \supsetneq B$, 由 B 的选取有 $\langle a \rangle \cap \langle w \rangle B \neq \{e\}$. 故存在整数 ℓ 和 $u \in B$ 使得 $e \neq w^\ell u \in \langle a \rangle$. 若 $p \mid \ell$, 则 w^ℓ 为 w^p 的方幂, 故 $w^\ell \in B$, 从而 $w^\ell u \in \langle a \rangle \cap B = \{e\}$, 矛盾. 所以 $p \nmid \ell$.

有限交换群的结构

- 由于 $p \nmid \ell$, 即 p 与 ℓ 互素, 故存在整数 i 和 j 使得 $i\ell + jp = 1$. 所以
$$w = w^{i\ell+jp} = (w^{\ell}u)^{i}u^{-i}(w^{p})^{j} \in \langle a\rangle B,$$
与 $w \notin \langle a\rangle B$ 矛盾.
- 因为 $\langle a\rangle \cap B = \{e\}$ 和 $A = \langle a\rangle B$, 所以 $A \cong \langle a\rangle \times B$. 定理证毕.
- 设 A 是有限交换 p-群. 不妨设 $A \neq \{e\}$, 设 A 中元素阶的最大值为 p^{m_1} (即 $exp(A) = p^{m_1}$), 选取 A 中一个阶为 p^{m_1} 的元素 a_1, 则有 $B_1 \leq A$ 使得 $A \cong \langle a_1\rangle \times B_1$. 若 $B_1 = \{e\}$, 则 $A \cong \langle a_1\rangle$.
- 若 $B_1 \neq \{e\}$, 设 B_1 中元素阶的最大值为 p^{m_2}, 则有 $m_1 \geq m_2$. 选取 B_1 中一个阶为 p^{m_2} 的元素 a_2, 则有 $B_2 \leq B_1$ 使得 $B_1 \cong \langle a_2\rangle \times B_2$. 由此得到 $A \cong \langle a_1\rangle \times \langle a_2\rangle \times B_2$. 若 $B_2 = \{e\}$, 则 $A \cong \langle a_1\rangle \times \langle a_2\rangle$.
- 若 $B_2 \neq \{e\}$, 设 B_2 中元素阶的最大值为 p^{m_3}, 则有 $m_1 \geq m_2 \geq m_3$. 选取 B_2 中一个阶为 p^{m_3} 的元素 a_3, 则有 $B_3 \leq B_2$ 使得 $B_2 \cong \langle a_3\rangle \times B_3$. 由此得到 $A \cong \langle a_1\rangle \times \langle a_2\rangle \times \langle a_3\rangle \times B_3$.
- 继续这一过程, 我们可得到子群序列 $B_1, B_2, B_3, \cdots$. 对于 $i \geq 1$, B_{i+1} 的阶是 B_i 的阶的真因子, 所以一定存在某个正整数 t 使得 $B_t = \{e\}$. 这样我们得到 $A \cong \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_t\rangle$.

有限交换群的结构

- 定理：有限交换 p-群 A 可以分解为循环子群的直积

$$A \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_t \rangle,$$

并且直积因子的个数 t 以及它们的阶 $p^{m_1}, p^{m_2}, \cdots, p^{m_t}$ (不妨设 $m_1 \geq m_2 \geq \cdots \geq m_t$) 由群 A 唯一决定.

- 证明：前面已有分解性. 下面证明唯一性, 对 $|A|$ 做归纳. 若 $|A| = p$, 则 A 分解的唯一性显然. 设 $|A| > p$, 考虑 A 的自同态 $\eta : a \mapsto a^p$, 容易验证, 若 $A \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_t \rangle$, 则有

$$\mathrm{Ker}\eta \cong \langle a_1^{p^{m_1-1}} \rangle \times \langle a_2^{p^{m_2-1}} \rangle \times \cdots \times \langle a_t^{p^{m_t-1}} \rangle$$

和

$$\eta(A) \cong \langle a_1^p \rangle \times \langle a_2^p \rangle \times \cdots \times \langle a_t^p \rangle.$$

所以 $|\mathrm{Ker}\eta| = p^t$ 是 A 唯一确定的子群 $\mathrm{Ker}\eta$ 的阶, 得到 t 的不变性. 对 η 的像利用归纳假设得到 $a_1^p, a_2^p, \cdots, a_t^p$ 的阶 $p^{m_1-1}, p^{m_2-1}, \cdots, p^{m_t-1}$ 被 $\eta(A)$, 从而也被 A 唯一决定, 因此 $p^{m_1}, p^{m_2}, \cdots, p^{m_t}$ 由群 A 唯一决定.

有限交换群的结构

- 定理：设 G 为 n 阶交换群，$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ 为 n 的素因子分解，其中 $p_1, p_2, \ldots, p_s$ 为互不相同的素数，$e_i \geq 1$，$1 \leq i \leq s$. 则

$$G \cong \times_{i=1}^{s} \left(\mathbb{Z}_{p_i^{\ell_{i1}}} \times \mathbb{Z}_{p_i^{\ell_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{\ell_{ik_i}}} \right),$$

  其中 ℓ_{ij} 为正整数且满足对任意 $1 \leq i \leq s$，有 $\ell_{i1} \geq \ell_{i2} \geq \cdots \geq \ell_{ik_i}$ 和 $\sum_{j=1}^{k_i} \ell_{ij} = e_i$. 多重集合 $\{p_1^{\ell_{11}}, \cdots, p_1^{\ell_{1k_1}}, \cdots, p_s^{\ell_{s1}}, \cdots, p_s^{\ell_{sk_s}}\}$ 由群 G 唯一确定，称其为 G 的初等因子. 这里 $\mathbb{Z}_m$ 为 m 阶循环群.
- 推论：有限交换群被它的初等因子唯一确定，即设 G_1 与 G_2 都是 n 阶交换群，则 $G_1 \cong G_2$ 当且仅当它们有相同的初等因子.
- 对每个 i，$1 \leq i \leq s$，由于 $\sum_{j=1}^{k_i} \ell_{ij} = e_i$ 且 $\ell_{i1} \geq \ell_{i2} \geq \cdots \geq \ell_{ik_i}$，所以 $\ell_{i1}, \ell_{i2}, \cdots, \ell_{ik_i}$ 的个数恰为 e_i 的分拆数 $p(e_i)$. 从而 $p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ 阶交换群的个数 (即初等因子个数) 为 $p(e_1)p(e_2)\cdots p(e_s)$.
- 例：$3969 = 7^2 \cdot 3^4$. 2 的分拆为 2 和 $1+1$，所以 $p(2) = 2$. 4 的分拆为 4，$3+1$，$2+2$，$2+1+1$，和 $1+1+1+1$，所以 $p(4) = 5$. 从而 3969 阶交换群的个数为 10. (一般地，设 $p \neq q$ 为素数，则 $p^2 q^4$ 阶交换群的个数是 10.)

有限交换群的结构

- 设 $k = \max\{k_1, k_2, \ldots, k_s\}$, 令

$$\begin{aligned} d_k &= p_1^{\ell_{11}} p_2^{\ell_{21}} \cdots p_s^{\ell_{s1}}, \\ d_{k-1} &= p_1^{\ell_{12}} p_2^{\ell_{22}} \cdots p_s^{\ell_{s2}}, \\ \cdots & \quad \cdots \\ d_1 &= p_1^{\ell_{1k}} p_2^{\ell_{2k}} \cdots p_s^{\ell_{sk}}, \end{aligned}$$

  其中约定 $\ell_{ij} = 0$ 若 $j > k_i$.

- 由于

$$\mathbb{Z}_{p_1^{\ell_{1j_1}}} \times \mathbb{Z}_{p_2^{\ell_{2j_2}}} \times \cdots \times \mathbb{Z}_{p_s^{\ell_{sj_s}}} \cong \mathbb{Z}_{p_1^{\ell_{1j_1}} p_2^{\ell_{2j_2}} \cdots p_s^{\ell_{sj_s}}},$$

  我们可得下面这个有限交换群的结构定理.

- 定理: 设 G 为 n 阶交换群, 则

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k},$$

  其中 d_i, $1 \leq i \leq k$ 为正整数且满足 $d_1 \mid d_2 \mid \cdots \mid d_k$ 和 $d_1 d_2 \cdots d_k = n$. 多重集合 $\{d_1, d_2, \cdots, d_k\}$ 由群 G 唯一确定, 称其为 G 的不变因子.

有限交换群的结构

- 推论：设 G_1 与 G_2 都是 n 阶交换群，则 $G_1 \cong G_2$ 当且仅当它们有相同的不变因子.
- 例：$1500 = 2^2 \cdot 3 \cdot 5^3$，$p(2) = 2$，$p(1) = 1$，$p(3) = 3$，所以 1500 阶交换群有 6 个. 进一步地，1500 阶交换群的初等因子有如下可能：$\{2^2, 3, 5^3\}$，$\{2, 2, 3, 5^3\}$，$\{2^2, 3, 5^2, 5\}$，$\{2, 2, 3, 5^2, 5\}$，$\{2^2, 3, 5, 5, 5\}$，$\{2, 2, 3, 5, 5, 5\}$，由此互不同构的 6 个 1500 阶交换群分别为：$\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^3}$ (或 $\mathbb{Z}_{1500}$)，$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^3}$ (或 $\mathbb{Z}_2 \times \mathbb{Z}_{750}$)，$\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$ (或 $\mathbb{Z}_5 \times \mathbb{Z}_{300}$)，$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5$ (或 $\mathbb{Z}_{10} \times \mathbb{Z}_{150}$)，$\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ (或 $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{60}$)，和 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ (或 $\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{30}$).
- 设 G 是有限生成的交换群，定义 $G_t = \{a \in G \mid o(a) \text{ 有限}\}$ 为 G 中所有阶有限的元素构成的集合，则 G_t 为 G 的有限子群. 且有 $G \cong \mathbb{Z}^r \times G_t$，其中 r 由 G 唯一确定，称为 G 的秩. 又 G_t 可唯一地分解为有限循环群的直积，由此可得有限生成交换群的结构定理.

作业

1. 证明 Lagarange 定理的逆对有限交换群成立.
2. 设 G 为有限交换 p-群, n 为正整数且 $p \nmid n$. 证明对任意 $a \in G$, 方程 $x^n = a$ 在群 G 中有解.
3. 给出 360 阶交换群的所有可能的初等因子组和不变因子组, 并写出所有互不同构的 360 阶交换群.
4. 给出所有的 16 阶交换群, 并分别给出其中恰有 2 个 2 阶元, 3 个 2 阶元, 和 4 个 2 阶元的群.
5. 证明 $175 = 5^2 \cdot 7$ 阶群和 $20449 = 11^2 \cdot 13^2$ 阶群一定交换, 并写出所有互不同构的 175 阶和 20449 阶群.
6. 设 A, B, C 均为有限交换群且 $A \times B \cong A \times C$, 证明 $B \cong C$.
7. 设 p 为素数, 求群 $\mathbb{Z}_p \times \mathbb{Z}_p$ 的自同构群 $\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$.
8. 设 $m \geq n$ 为正整数, p 为素数, 求群 $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$ 的各阶循环子群的个数. 进一步地, 求该群的所有子群的个数 (选作).
9. 证明有限生成交换群是有限群当且仅当它的一组生成元均为有限阶元素.
10. 分类所有的 75 阶群. 证明交换的 75 阶群有 2 个, 非交换的 75 阶群唯一.

换位子

- 设 G 为群, $a, b \in G$, 定义 $[a, b] = aba^{-1}b^{-1}$, 并称之为 a 和 b 的换位子 (commutator). 显然 a 与 b 可交换当且仅当 $[a, b] = e$.
- 对任意 $a, b, c \in G$ 和任意群同态 $\sigma : G \to H$, 有 $[a, b]^{-1} = [b, a]$, $c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}]$, 和 $\sigma([a, b]) = [\sigma(a), \sigma(b)]$, 所以换位子的逆、共轭以及同态像还是换位子.
- 显然交换群中的换位子只有单位元 e, 但通常说来, 很难判断非交换群中的元素是否为换位子.
- 例: 考察对称群 S_n, 其中 $n \geq 3$. 由于符号函数 $\mathrm{sgn} : S_n \to \{\pm 1\}$ 为群同态, 而群 $\{\pm 1\}$ 为交换群, 所以对任意 $\sigma, \tau \in S_n$,

$$\mathrm{sgn}([\sigma, \tau]) = [\mathrm{sgn}(\sigma), \mathrm{sgn}(\tau)] = 1,$$

  故 S_n 中的换位子一定是偶置换.
- 令 $\sigma = (123)$, $\tau = (12) \in S_n$, 则

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = (123)(12)(132)(12) = (132),$$

  即 3-轮换 (132) 为换位子. 又 S_n 中的 3-轮换彼此共轭 (它们有相同的型), 所以 S_n 中每个 3-轮换都是换位子.

换位子群

- 注意到换位子的乘积不一定为换位子, 所以群 G 的所有换位子组成的集合不必是 G 的子群.
- 群 G 的所有换位子生成的子群称为 G 的换位子群, 或者导群, 记作 $[G,G]$ 或者 G', 即 $G' = \langle aba^{-1}b^{-1} \mid a,b \in G \rangle$. 显然 G 为交换群当且仅当 $G' = \{e\}$, 因此, 从某种意义上讲, G' 是 G 的非交换性的一种度量, G' 越大, G 离交换性越远.
- 例: 对于 $n \geq 3$, 由于 A_n 可以由 3-轮换生成, 而 3-轮换又都是 S_n 中的换位子, 所以 $A_n \leq S_n'$. 又每个换位子都是偶置换, 所以 $S_n' \leq A_n$. 由此我们求出 $S_n' = A_n$.
- 由于换位子的共轭还是换位子, 所以 $G' \trianglelefteq G$.
- 命题: 设 $\sigma : G \to H$ 为群同态, 则 $\sigma(G)$ 交换当且仅当 $G' \leq \mathrm{Ker}\sigma$.
- 证明: 记 $K = \mathrm{Ker}\sigma$. $\sigma(G) \cong G/K$ 交换当且仅当对任意 $a,b \in G$, $[aK,bK] = [a,b]K = K$, 即 $[a,b] \in K$, 这等价于 $G' \leq K$.
- 定理: 设 $N \trianglelefteq G$, 则 G/N 是交换群当且仅当 $G' \leq N$. 特别地, G/G' 交换.
- 证明: 考虑自然同态 $\pi : G \to G/N$ 即可. 这时 $\mathrm{Ker}\pi = N$ 而 $\pi(G) = G/N$.

可解群

- 递归地定义群 G 的 n 级导群 $G^{(n)}$ 如下: $G^{(1)} = G'$, 对 $n > 1$, $G^{(n)} = (G^{(n-1)})'$.
- 命题: 设 $\sigma : G \to H$ 为群同态, 则对任意正整数 n 有 $\sigma(G)^{(n)} = \sigma(G^{(n)})$.
- 证明: 对 n 做归纳. 由于对任意 $a, b \in G$, $\sigma([a, b]) = [\sigma(a), \sigma(b)]$, 所以 $\sigma(G)' = \sigma(G')$, 即命题对 $n = 1$ 时成立. 对于 $n \geq 2$, 设命题对 $n - 1$ 成立, 即 $\sigma(G)^{(n-1)} = \sigma(G^{(n-1)})$, 则

$$\sigma(G)^{(n)} = (\sigma(G)^{(n-1)})' = \sigma(G^{(n-1)})' = \sigma((G^{(n-1)})') = \sigma(G^{(n)}).$$

  由归纳法原理, 命题得证.
- 定义: 设 G 为群, 如果存在某个正整数 n 使得 $G^{(n)} = \{e\}$, 则称 G 为可解群.
- 显然交换群都可解, 而非交换单群不可解. (G 为非交换单群, 则必有 $G' = G$)
- 命题: 可解群的子群和商群仍为可解群.
- 证明: 若 G 可解, 存在正整数 n 使得 $G^{(n)} = \{e\}$. 对任意 $H \leq G$, 有 $H^{(n)} \leq G^{(n)}$, 所以 $H^{(n)} = \{e\}$, 即 H 也可解.

可解群

- 对于 $N \trianglelefteq G$, 记 $\pi : G \to G/N$ 为自然同态, 则有
$$\pi(G)^{(n)} = \pi(G^{(n)}) = \pi(\{e\}) = \{\overline{e}\},$$
所以 $G/N = \pi(G)$ 可解.
- 命题: 设 $N \trianglelefteq G$, 若 N 和 G/N 均可解, 则 G 可解.
- 证明: 由 G/N 可解, 存在正整数 n 使得 $(G/N)^{(n)} = \{\overline{e}\}$. 利用自然同态 $\pi : G \to G/N$ 可得到 $(G/N)^{(n)} = \pi(G)^{(n)} = \pi(G^{(n)})$, 即 $\pi(G^{(n)}) = \{\overline{e}\}$, 所以 $G^{(n)} \subseteq \mathrm{Ker}\pi = N$. 再由 N 可解, 存在正整数 m 使得 $N^{(m)} = \{e\}$. 于是
$$G^{(n+m)} = (G^{(n)})^{(m)} \subseteq N^{(m)} = \{e\},$$
所以 G 为可解群.
- 命题: 有限 p-群可解.
- 证明: 设 $|G| = p^n$, 对 n 做归纳. $n = 1$ 时结论显然. 设 $n > 1$ 且结论对 $< n$ 成立, 来考察 n 的情形. 令 $N = Z(G)$, 则 $N \trianglelefteq G$. 若 $N = G$, 则 G 交换, 结论成立. 若 $N \neq G$, 因为 $N \neq \{e\}$, 设 $|N| = p^m$, 则 $1 \leq m < n$, 这时 $|G/N| = p^{n-m}$. 由归纳假设, N 和 G/N 都可解, 故 G 可解.

可解群

- Burnside 定理：设 p, q 是素数, a, b 是正整数, 则 $p^a q^b$ 阶群可解.
- 注: 该定理是 Burnside 在 20 世纪初利用群的特征标证明的, 证明非常简洁, 是有限群表示理论中的著名结论. 但它的纯群论方法 (不利用群特征标) 的证明是在 50 多年后才给出的, 还很繁琐. 参见 I. Martin Isaacs 所著 "Finite Group Theory" 一书第 7 章的 7D.
- 命题: 设 G 为群, 则 G 是可解群的充分必要条件是存在 G 的子群列 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{e\}$, 使得对任意 $0 \leq i \leq s-1$, G_i/G_{i+1} 都是交换群. (满足如上性质的 G 的子群列称为 G 的一个可解群列)
- 证明: 必要性: 取 $G_i = G^{(i)}$ 即可. 充分性：用归纳法证明 $G^{(i)} \leq G_i$, $1 \leq i \leq s$. 因为 G/G_1 交换, 所以 $G' \leq G_1$, 即 $i = 1$ 时结论正确. 现在设 $G^{(i)} \leq G_i$, 对任意 $1 \leq i < s$. 同样由于 G_i/G_{i+1} 是交换群, 所以 $G_i' \leq G_{i+1}$, 而由归纳假设 $G^{(i)} \leq G_i$, 故 $G^{(i+1)} = (G^{(i)})' \leq G_i' \leq G_{i+1}$, 这就完成了归纳法证明. 于是 $G^{(s)} \leq G_s = \{e\}$, 即 $G^{(s)} = \{e\}$, 从而 G 为可解群.
- 例: 对称群 S_2 是交换群, 故可解. S_3 有一个可解群列 $S_3 \trianglerighteq A_3 \trianglerighteq \{(1)\}$, 所以 S_3 可解. 类似地, 由 $S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq \{(1)\}$ 知 S_4 为可解群. 对于 $n \geq 5$, S_n 不可解.

作业

- Feit-Thompson 定理：奇阶群可解.
- P58: 17, 19. P65: 14, 15, 17, 18.

1. 设 G 为群, $H \leq G$ 且 $G' \subseteq H$, 证明 $H \trianglelefteq G$.
2. 群 G 的子群 H 称为是特征子群若对任意 $\alpha \in \mathrm{Aut}(G)$ 有 $\alpha(H) = H$. 证明 G' 是 G 的特征子群.
3. 求二面体群 D_n 的换位子群.
4. 证明对任意正整数 n 有 $G^{(n)} \trianglelefteq G$.
5. 设 H, K 都是有限可解群, 证明 H, K 的半直积 $H \rtimes_\varphi K$ 也是可解群.
6. 设 G 是群, $N \trianglelefteq G$ 且 $N \neq G$, 称 N 是 G 的极大正规子群如果对任意 $H \trianglelefteq G$ 和 $N \subseteq H \subseteq G$, 一定有 $H = N$ 或者 $H = G$.
   (1) 设 $N \trianglelefteq G$, 证明 N 是 G 的极大正规子群当且仅当 G/N 是单群.
   (2) 设 G 是有限群, $G \neq \{e\}$, 证明 G 有极大正规子群.
   (3) 设 G 是有限群, 证明 G 可解当且仅当存在 G 的子群列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{e\},$$

使得对任意 $0 \leq i \leq s-1$, G_i/G_{i+1} 都是素数阶循环群.

自由群

- 自由群可以认为是其元素之间没有任何关系的群, 因此任一群都可以看成自由群的同态像.
- 设 X 为一个非空集合, $X^{-1} = \{x^{-1} \mid x \in X\}$, $S = X \cup X^{-1}$. 由 S 中的元素组成的有限序列 $w = a_1 a_2 \cdots a_n$ $(a_i \in S, 1 \leq i \leq n)$ 称为 S 上的一个字. 允许空集合组成的字, 称为空字, 记为 $\varnothing$.
- 字 w 称为既约字 (或简化字), 如果 w 中没有形如 $a^{-1}a$ $(a \in S$, 对 $x \in X, (x^{-1})^{-1} = x)$ 的字串.
- 任一字都可以通过削去其中的字串 $a^{-1}a$ 简化成既约字. 例如: xx^{-1} 可以简化为 $\varnothing$, 而

$$w = x^{-1}xyy^{-1}x^{-1}yz \to x^{-1}x(yy^{-1})x^{-1}yz \to x^{-1}(xx^{-1})yz \to x^{-1}yz.$$

一个字可以有不同的简化方式, 例如上面的字 w 可以简化如下:

$$w = x^{-1}xyy^{-1}x^{-1}yz \to (x^{-1}x)yy^{-1}x^{-1}yz \to (yy^{-1})x^{-1}yz \to x^{-1}yz.$$

- 命题: 对任一字 w, w 有唯一的既约形式.
- 证明: 对字 w 的长度 n 做归纳.

- 若 $n = 1$, 则 w 显然是既约的, 结论成立.
- 设 $n > 1$, 并设结论对长度小于 n 的字成立. 下面设 w 为长度为 n 的字, 若 w 本身既约, 则已证.
- 若 w 不是既约的, 则 w 一定形如 $w = \cdots a^{-1}a \cdots$, 为得到 w 的既约形式, 我们必须消去其中的 $a^{-1}a$. 设 w_0 是 w 的一个既约形式. 如果在得到 w_0 的某一步消去 w 中的符号对 $a^{-1}a$, 我们可以在第一步就消去这一对而其它步骤不变, 则 w 仍然化为 w_0. 若对 $a^{-1}a$ 不是同时消去, 由于要得到既约形式, 故其中 a^{-1} 或 a 一定在某一步被消去, 则该步之前必为

$$\cdots a(a^{-1}a)\cdots \quad \text{或} \quad \cdots(a^{-1}a)a^{-1}\cdots$$

的形式, 此时消去 aa^{-1} 与消去 $a^{-1}a$ 效果是一样的, 从而我们总可以在第一步就消去 $a^{-1}a$, 并且消去后得到的字的长度为 $n-2$. 由归纳假设可得唯一的既约形式.
- 用 W 表示 S 上的字组成的集合, 对于 $w, w' \in W$, 定义 $w \sim w'$, 若 w 与 w' 有相同的既约形式. 容易验证 $\sim$ 是集合 W 上的一个等价关系且保持字的连写性质.

自由群

- 什么是字的连写？对于 $u, v \in W$, uv 就是把字 u 和 v 按先 u 后 v 连写在一起所得到的字. $\sim$ 保持连写性质即若 $w \sim w'$ 且 $u \sim u'$, 则 $wu \sim w'u'$. 事实上, 设 w_0 是 w 和 w' 的既约形式, u_0 是 u 和 u' 的既约形式, 则 wu 经简化可得 w_0u_0 (不一定是既约的), 同时 $w'u'$ 经简化也可得 w_0u_0, 故 $wu \sim w'u'$.
- 用 $\overline{w}$ 表示如上等价关系下包含字 w 的等价类. 记 $F(X) = \{\overline{w} \mid w \in W\}$ 为 W 在该等价关系下的商集, 即 $\sim$ 的等价类集合. 在其中定义乘法 $\overline{w_1} \cdot \overline{w_2} = \overline{w_1 w_2}$, 则 $F(X)$ 成为一个群, 称为 X 上的自由群, 而 X 称为自由群 $F(X)$ 的自由生成元集.
- $F(X)$ 中的结合律显然. $\overline{\varnothing}$ 为单位元. 对于 $w = a_1 a_2 \cdots a_n \in W$, $a_i \in S$, $1 \leq i \leq n$, 定义 $w^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$, 则 $\overline{w}^{-1} = \overline{w^{-1}}$.
- 定理 (自由群的泛性质): 设 G 为群, X 为集合, $f : X \to G$ 为映射, 则 f 可以扩充为群同态 $\varphi : F(X) \to G$ 使得 $f = \varphi i$, 这里 $i : X \to F(X)$ 为自然的包含映射. 进一步地, 满足如上性质的群同态是唯一的.

- 证明: 容易验证如下定义的 φ 为延拓 f 的群同态. 对 $w = a_1 \cdots a_n$, $a_i \in X \cup X^{-1}$, 定义 $\varphi(\overline{w}) = \varphi(a_1) \cdots \varphi(a_n)$, 其中

$$\varphi(a_i) = \begin{cases} f(a_i), & \text{若 } a_i \in X, \\ f(a_i^{-1})^{-1}, & \text{若 } a_i \in X^{-1}. \end{cases}$$

  进一步地, 若 $\psi : F(X) \to G$ 也是延拓 f 的群同态且 $f = \psi i$, 则对任意 $a \in X$, 有 $\psi(\overline{a}) = \psi(i(a)) = f(a)$. 故对任意 $\overline{w} \in F(X)$, 设 $w = a_1 \cdots a_n$, 其中 $a_i \in X \cup X^{-1}$. 若 $a_i \in X^{-1}$, 则 $a_i^{-1} \in X$ 且 $a_i = (a_i^{-1})^{-1}$, 由 ψ 为同态有

  $\psi(\overline{a_i}) = \psi\left(\overline{a_i^{-1}}^{-1}\right) = \psi\left(\overline{a_i^{-1}}\right)^{-1} = f(a_i^{-1})^{-1}$. 从而

  $\psi(\overline{w}) = \psi(\overline{a_1} \cdots \overline{a_n}) = \psi(\overline{a_1}) \cdots \psi(\overline{a_n}) = \varphi(\overline{w})$, 即 $\psi = \varphi$.
- 在如上定理条件中取 $X \subseteq G$, 如果 $\langle X \rangle = G$, 则 φ 为满同态, 即 G 为 $F(X)$ 的商群. 特别地, (1) 取 $X = G$, 得到 G 是自由群的商群. (2) 若 X 有限, 即 G 为有限生成群, 则 G 是有限生成自由群的商群.
- 定理: 每个群都是自由群的商群, 每个有限生成群都是有限生成自由群的商群.

群的表现

- 定义：若群 $G = F(X)/N$, 则群 G 的表现 (presentation) 记为 $\langle X \mid r = e, \text{ 其中 } r \in N\rangle$. 特别地, 如果 $R = \{r_1, r_2, \ldots, r_t\} \subseteq N$ 且包含 R 的最小正规子群为 N (注意这并不是 $N = \langle R\rangle$), 则 G 的表现为

$$G = \langle X \mid r_1 = r_2 = \cdots = r_t = e\rangle.$$

  X 中的元素称为 G 的生成元, N (或 R) 中的元素构成生成元的生成关系 (或定义关系). G 也是由生成元集 X 和定义关系集 R 决定的群.
- 例如: n 阶循环群为 $\langle a\rangle/\langle a^n\rangle$, 从而可以表现为 $\langle a \mid a^n = e\rangle$.
- Dyck 定理: 设 $G = \langle a_1, a_2, \cdots, a_n \mid r_1 = r_2 = \cdots = r_t = e\rangle$, $H = \langle a_1, a_2, \cdots, a_n \mid r_1 = r_2 = \cdots = r_t = r_{t+1} = \cdots = r_{t+k} = e\rangle$, 则 H 是 G 的同态像.
- 设 $X = \{a_1, a_2, \cdots, a_n\}$, $F(X)$ 的包含 $\{r_1, \cdots, r_t\}$ 的最小正规子群为 K, 包含 $\{r_1, \cdots, r_t, \cdots, r_{t+k}\}$ 的最小正规子群为 N, 则有 $K \trianglelefteq N$, $G \cong F(X)/K$, $H \cong F(X)/N$. 由 $(F(X)/K)/(N/K) \cong F(X)/N$ 得到 H 是 G 的同态像.

二面体群 D_n 的表现

- 首先二面体群 D_n 有生成元 a (绕中心旋转 $\frac{2\pi}{n}$ 角度) 和 b (对某一固定对称轴的反射), 且满足 $a^n = b^2 = (ab)^2 = e$. 令 $X = \{a, b\}$, 则 $X \hookrightarrow D_n$ 诱导了满同态 $\varphi : F(X) \to D_n$. 令 $N = \mathrm{Ker}\varphi$, 则 $a^n, b^2, (ab)^2 \in N$. 令 K 是包含 $a^n, b^2, (ab)^2$ 的 $F(X)$ 的正规子群, 则 $K \leq N$. 由第三同构定理有

$$(F(X)/K)/(N/K) \cong F(X)/N \cong D_n,$$

所以 $|F(X)/K| = |D_n||N/K| \geq 2n$. 另一方面, $F(X)/K$ 中的元素均可写为 $a^i b^j$ $(0 \leq i \leq n-1, 0 \leq j \leq 1)$ 的形式, 故 $|F(X)/K| \leq 2n$. 因此 $|F(X)/K| = 2n$ 且 $K = N$, 故

$$D_n = \langle a, b \mid a^n = b^2 = (ab)^2 = e \rangle.$$

- 例如, $\langle a \mid a^4 = a^6 = e \rangle$ 为 2 阶循环群 $(= \langle a \mid a^2 = e \rangle)$, $S_3 = \langle a, b \mid a^2 = b^3 = (ab)^2 = e \rangle$. 无限循环群 $\mathbb{Z}$ 为由一个元素生成的自由群 $\langle a \rangle$, 而 $\mathbb{Z} \times \mathbb{Z} = \langle a, b \mid aba^{-1}b^{-1} = e \rangle$. n 个 $\mathbb{Z}$ 的直积称为秩为 n 的自由交换群.

四元数群

- 由 Dyck 定理可得若有限群 G 和 H 有相同的生成元集并且 H 满足 G 的定义关系, 则 H 为 G 的同态像. 进一步地, 若还有 $|H| \geq |G|$, 则 $H \cong G$.
- 例: 考察群 $G = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle$. 设 $X = \{a, b\}$, N 是由 $b^{-2}a^2$ 和 $(ab)^{-2}a^2$ 生成的正规子群, 则 $G \cong F(X)/N$. 但这个群的结构到底如何? 我们需要把 G 中元素写成 a, b 组成的字且满足 $a^2 = b^2 = (ab)^2$. 令 $H = \langle b \rangle$, $S = \{H, aH\}$. 容易知道 S 在左乘 a 和 b 下封闭, 事实上, $baH = aH$, $aaH = H$. 所以 $G = H \cup aH$. 由 $b^2 = (ab)^2$ 得到 $b = aba$, 所以由 $a^2 = b^2 = (aba)^2 = ab^4a$ 得知 $b^4 = e$, 所以 G 最多含有 8 个元素 $e, b, b^2, b^3, a, ab, ab^2, ab^3$. (当然它们可能相同, 例如 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 就满足这个定义关系而只有 4 个元素) 下面考虑由复矩阵

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{和} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

生成的群 K, 它满足 $A^2 = B^2 = (AB)^2$ 且至少有 8 个元素 A^iB^j, $i = 0, 1$, $j = 0, 1, 2, 3$, 故 G 为 8 阶群. 此群称为四元数群, 记为 Q.

8 阶群的分类

- 定理：在同构的意义下，只有下面 5 个 8 阶群：$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, 二面体群 D_4 和四元数群 Q. (Cayley, 1859)
- 证明：设 G 为 8 阶群. 若 G 交换，则 G 同构于 $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, 或 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
- 下面设 G 不交换. 这时 G 中一定有 4 阶元，设 a 为一个 4 阶元，$b \in G \backslash \langle a \rangle$，则 $G = \langle a \rangle \cup \langle a \rangle b = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. 考虑元素 b^2，显然 b^2 不等于 b, ab, a^2b, a^3b，由 a, b 不交换得到 $b^2 \neq a, a^3$，所以有 $b^2 = e$ 或 a^2. 若 $b^2 = e$，因为 $\langle a \rangle$ 正规，$bab^{-1} \in \langle a \rangle$，又 bab^{-1} 与 a 有相同的阶，故 $bab^{-1} = a$ 或者 $bab^{-1} = a^{-1}$，前者得出 G 交换，矛盾，所以 $bab^{-1} = a^{-1}$，又 $b^2 = e$，我们得到 $(ab)^2 = e$，这时

$$G = \langle a, b \mid a^4 = b^2 = (ab)^2 = e \rangle \cong D_4.$$

若 $b^2 = a^2$，同样由 $bab^{-1} = a^{-1}$ 得到 $(ab)^2 = a^2$，这时

$$G = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle \cong Q.$$

作业

- 设 X 为 r 元集合, 称

$$\mathbb{Z}(X) = F(X)/F(X)' = \langle X \mid xyx^{-1}y^{-1} = e,\ \forall x, y \in X \rangle$$

为有限生成自由交换群, 其中 $r = |X|$ 称为它的秩. 显然这时 $\mathbb{Z}(X)$ 为 r 个无限循环群 $\mathbb{Z}$ 的直积, 记为 $\mathbb{Z}^r$.

- P71: 1, 2, 3, 4.

1. 证明四元数群 Q 的每个子群都是正规子群. (这样的群称为 Hamilton 群).
2. 求群 $G = \langle a, b \mid a^3 = b^9 = e,\ a^{-1}ba = b^{-1} \rangle$ 的阶, 并确定群 G.
3. 求群 $G = \langle a, b \mid ab^2 = b^3a,\ ba^3 = a^2b \rangle$ 的阶, 并确定群 G.
4. 求群 $G = \langle a, b \mid a^6 = e,\ a^3 = b^2,\ b^{-1}ab = a^{-1} \rangle$ 的阶.
5. 设 $G = \langle a, b, c \mid a^2 = b^2 = c^2 = e, ac = ca, (ab)^3 = (bc)^3 = e \rangle$, 证明 $G \cong S_4$.
6. 确定所有的 12 阶群.