西罗定理与双陪集分解

回顾交换群的柯西定理：设 G 是一个有限交换群，p 是一个素数且 p 整除 G 的阶。则 G 中存在一个阶为 p 的元素。（在之前习题中用归纳法已证。）

定义 1. 设 G 是一个有限群，p 是一个素数且 $p \mid |G|$。记 $|G| = p^a m$，其中 $a \geq 1$ 且 $p \nmid m$。G 的阶为 p^a 的子群称为 G 的**西罗 p-子群**。

定理 1 (第一西罗定理)**.** 对于每个整除 $|G|$ 的素数幂 p^a $(a \geq 1)$，G 都存在一个阶为 p^a 的子群。特别地，G 的西罗 p-子群总存在。

证明. 我们对 $|G|$ 进行归纳证明。$|G| = p$ 时结论显然成立。现在假设定理对所有阶小于 $|G|$ 的群成立。
考虑类方程：

$$|G| = |Z(G)| + \sum [G : C_G(g_i)],$$

其中求和取遍非中心共轭类的代表元，特别地，$C_G(g_i) \neq G$。我们考虑两种情况：
情况 (i)：$p \mid |Z(G)|$。由交换群的柯西定理，$Z(G)$ 有一个阶为 p 的子群 N。由于 $N \subseteq Z(G)$，N 在 G 中正规。那么 $|G/N| = p^{a-1}m$，$m \in \mathbb{Z}_{\geq 1}$，由归纳假设，$G/N$ 有一个阶为 p^{a-1} 的子群。这个子群在商映射下的原像是 G 的一个阶为 p^a 的子群。
情况 (ii)：$p \nmid |Z(G)|$。由类方程等式，必存在某个 g_i 使得 $p \nmid [G : C_G(g_i)]$。由于 $p^a \mid |G|$，我们必有 $p^a \mid |C_G(g_i)|$。但 $C_G(g_i) \neq G$，所以由归纳假设，$C_G(g_i)$ 有一个阶为 p^a 的子群，这个子群也是 G 的子群。 □

定理 2 (第二西罗定理)**.** G 的所有西罗 p-子群都是相互共轭的。

证明. 设 $|G| = p^a m$，其中 $p \nmid m$, P, Q 是 G 的两个西罗 p-子群，即 $|P| = |Q| = p^a$。考虑 P 在 G/Q 上的左乘作用：$P \times G/Q \to G/Q$, $(h, aQ) \mapsto haQ$。将集合 G/Q 按轨道计数：

$$|G/Q| = \sum_x |\mathcal{O}_x|.$$

由于 $|G/Q| = m$ 且 $p \nmid m$，存在轨道 $\mathcal{O}_x$ 使得 $p \nmid |\mathcal{O}_x|$。设 $x = gQ$，则稳定子群

$$P_x = P_{gQ} = \{p \in P \mid pgQ = gQ\} = P \cap gQg^{-1}.$$

由轨道-稳定化子定理，$|\mathcal{O}_x| = |P|/|P_x| = |P|/|P \cap gQg^{-1}|$。由于 $p \nmid |\mathcal{O}_x|$ 且 P 是 p-群，必有 $|P|/|P \cap gQg^{-1}| = 1$，即 $P \subseteq gQg^{-1}$。但 $|P| = |gQg^{-1}| = p^n$，故 $P = gQg^{-1}$，即 P 与 Q 共轭。 □

定理 3 (第三西罗定理)**.** 设 $|G| = p^a m$，其中 $a \geq 1$ 且 $p \nmid m$。则群 G 西罗 p-子群的个数 n_p 满足：$n_p \mid m$ 且 $n_p \equiv 1 \pmod{p}$。

证明. 设 P 是 G 的一个西罗 p-子群，$X = \{gPg^{-1} : g \in G\}$ 是与 P 共轭的子群集合。由第二西罗定理知，X 事实上是 G 中所有西罗 p-子群的集合，从而 $n_p = |X|$。
(i) 考虑群 G 在集合 X 上的共轭作用，知该作用传递，且 $x = P \in X$ 处的稳定子群 $G_x = N_G(P)$。从而有

$$n_p = |X| = |\mathcal{O}_x| = |G|/|G_x| = |G|/|N_G(P)|.$$

由于 $P \subseteq N_G(P)$，从而 $|G|/N_G(P)|$ 是 $m = |G|/|P|$ 的因子, 故 $n_p \mid m$。
(ii) 再来考虑群 P 在 X 上的共轭作用。将 X 中的元素按轨道计数：$n_p = |X| = \sum_Q |\mathcal{O}_Q|$。知 $|\mathcal{O}_Q| = |P|/|P_Q|$,其中 P_Q 为 $Q \in X$ 处的稳定子群。由于 $|P| = p^a$,所以如若 $|\mathcal{O}_Q| > 1$，则有 $p \mid |\mathcal{O}_Q|$。若 $|\mathcal{O}_Q| = 1$，则有 $P_Q = P$，即 P 中的元素都满足 $gQg^{-1} = Q$。从而 $P \leq N_G(Q)$。从而 P, Q 都是 $N_G(Q)$ 的西罗 p 子群。对群 $N_G(Q)$ 利用西罗第二定理知，存在 $n \in N_G(Q)$ 使得 $P = nQn^{-1} = Q$。从而若 $|\mathcal{O}_Q| = 1$，则 $Q = P$。
因此，元素个数为 1 的轨道只有一个，其余轨道元素的个数均大于 1。从而，除 $\mathcal{O}_P$ 外，其他轨道的大小都能被 p 整除。因此，

$$n_p = |X| = \sum |\mathcal{O}_Q| \equiv 1 \pmod{p}.$$

□

双陪集分解

定义 2 (双陪集)**.** 设 G 是一个群，H, K 是 G 的两个子群。对于 $g \in G$，集合

$$HgK = \{hgk \mid h \in H, k \in K\}$$

称为 G 关于 (H, K) 的一个**双陪集** (double coset)。记 $H\backslash G/K$ 为双陪集的集合。

命题 1 (等价关系)**.** 设 G 是一个群，H, K 是 G 的两个子群。在 G 上定义关系：

$$g_1 \sim g_2 \iff \exists h \in H, k \in K \text{ 使得} g_2 = hg_1k.$$

证明：这是一个等价关系，每个等价类是一个双陪集 HgK。

命题 2 (双陪集分解)**.** 群 G 可以表示为互不相交的双陪集的并：

$$G = \bigcup_{g \in \mathcal{R}} HgK$$

其中 $\mathcal{R} \subset G$ 是**双陪集代表元**的一个集合。

命题 3 (双陪集大小公式)**.** 设 G 是有限群，则

$$|HgK| = \frac{|H| \cdot |K|}{|H \cap gKg^{-1}|}$$

证明. 考虑群 $H \times K$ 在 G 上的作用：$(h,k)\cdot x = hxk^{-1}$。元素 g 的轨道为：

$$(H\times K)\cdot g = \{hgk^{-1} \mid h\in H, k\in K\} = HgK$$

稳定子群为：

$$\mathrm{Stab}_{H\times K}(g) = \{(h,k)\in H\times K \mid hgk^{-1} = g\}$$

由 $hgk^{-1} = g$ 得 $g^{-1}hg = k$，所以

$$\mathrm{Stab}_{H\times K}(g) = \{(h, g^{-1}hg) \mid h\in H\cap gKg^{-1}\}$$

因此 $|\mathrm{Stab}_{H\times K}(g)| = |H\cap gKg^{-1}|$。由轨道-稳定化子定理：

$$|HgK| = \frac{|H\times K|}{|\mathrm{Stab}_{H\times K}(g)|} = \frac{|H|\cdot|K|}{|H\cap gKg^{-1}|}.$$

□

命题 4 (双陪集计数)**.** 对于有限群 G，有

$$|G| = \sum_{g\in\mathcal{R}} |HgK| = \sum_{g\in\mathcal{R}} \frac{|H|\cdot|K|}{|H\cap gKg^{-1}|}$$

其中 $\mathcal{R}$ 是双陪集代表元的一个集合。

西罗第二定理的另一证明. 设 $|G| = p^a m$，其中 $p\nmid m$, P, Q 是 G 的两个西罗 p-子群，即 $|P| = |Q| = p^a$。考虑群 G 关于子群 P 和 Q 的双陪集分解：

$$G = Pg_1Q \sqcup \ldots \sqcup Pg_rQ.$$

由双陪集的计数公式有

$$p^a m = |G| = |Q|\sum_{i=1}^{r} \frac{|P|}{|P\cap g_iQg_i^{-1}|} = p^a \sum_{i=1}^{r} \frac{|P|}{|P\cap g_iQg_i^{-1}|}.$$

从而 $\sum_{i=1}^{r} \frac{|P|}{|P\cap g_iQg_i^{-1}|} = m$。由于 $p\nmid m$，而每个 $\frac{|P|}{|P\cap g_iQg_i^{-1}|}$ 或为 1 或为 p 的方幂，从而必存在 i 使得 $|P| = |P\cap g_iQg_i^{-1}|$。这意味着 $P = g_iQg_i^{-1}$。从而 P 和 Q 共轭。 □