群在集合上的作用（G-set）

定义 1. 一个群 G 在一个非空集 X 上的一个**作用**是指一个映射 $L: G \times X \to X$，$(g,x) \mapsto g \cdot x := L(g,x)$ 满足 $\forall x \in X, g_1, g_2 \in G$ 有 $e \cdot x = x$，$(g_1g_2)x = g_1(g_2x)$。此时，称 X 是一个**G-set**。

题 1. 记 $\mathrm{Aut}(X)$ 为集合 X 上的对称群（双射的集合）。设 X 是一个 G-set，验证：

(1) $\forall g \in G$，$L_g : X \to X$，$x \mapsto gx$ 是一个双射，从而 $L_g \in \mathrm{Aut}(X)$。

(2) $L : G \to \mathrm{Aut}(X)$，$g \mapsto L_g$ 是一个群同态。

题 2. 设 Y 是一个非空集，$\varphi : G \to \mathrm{Aut}(Y)$，$g \mapsto \varphi_g$ 是一个群同态，定义

$$G \times Y \to Y, \quad (g,y) \mapsto gy := \varphi_g(y),$$

验证：Y 是一个 G-set。

结论： 由题 1、题 2 知，G 在 X 上的一个作用等同于 G 到 $\mathrm{Aut}(X)$ 的一个群同态。

例 1. (1) 设 H 是 G 的一个子群，则 $H \times G \to G$，$(h,g) \mapsto hg$ 定义了群 H 在（集合）G 上的一个作用，称为**左乘作用**。

(2) 设 H 是 G 的一个子群，则 $H \times G \to G$，$(h,g) \mapsto hgh^{-1}$ 定义了 H 在（集合）G 上的一个作用，称为**共轭作用**。

(3) 设 H 是 G 的一个正规子群，则 $G \times H \to H$，$(g,h) \mapsto ghg^{-1}$ 定义了 G 在（集合）H 上的一个作用。

(4) 设 S_n 是 $X = \{1, \ldots, n\}$ 上的对称群。则 $S_n \times X \to X$，$(g,x) \mapsto gx := g(x)$ 构成 S_n 在 X 上的一个作用。

(5) 设 H 是 G 的一个子群，则 $G \times G/H \to G/H$，$(a, bH) \mapsto (ab)H$ 定义了 G 在（集合）G/H 上的一个作用。（私下检查。）

(6) 设 G 是一个群，令 $X = \{H \mid H \subseteq G\}$。验证：$G \times X \to X$，$(g,H) \mapsto gHg^{-1}$ 定义了 G 在集合 X 上的一个作用。

题 3. 设 X 是一个 G-set，$x \in X$。验证：(1) $G_x := \{g \in G \mid gx = x\}$ 是 G 的一个子群，称为 x 的**稳定子群**; (2) $G_{gx} = gG_xg^{-1}$，$g \in G$。

证明. 显然 $e \in G_x$，所以 $G_x \neq \emptyset$。对 $a, b \in G_x$，知

$$a^{-1}bx = a^{-1}x = a^{-1}(ax) = ex = x.$$

所以 $a^{-1}b \in G_x$。

(2) $a \in G_{gx} \iff a(gx) = gx \iff (g^{-1}ag)x = x \iff g^{-1}ag \in G_x \iff a \in gG_xg^{-1}$。所以 $G_{gx} = gG_xg^{-1}$。 □

题 4. 设 H 是群 G 的子群，考虑 G-set $X := G/H$。证明：对于 $x = gH \in G/H$, 有 $G_x = gHg^{-1}$。特别地，对 $x_0 = eH$, 有 $G_{x_0} = H$。

证明. 知 $a \in G_x \iff a(gH) = gH \iff g^{-1}ag \in H \iff a \in gHg^{-1}$。 $\square$

定义 2. 设 X 是一个 G-set。在 X 上定义关系：$x \sim y \iff \exists g \in G$ 使得 $y = gx$。易验证这是一个等价关系。(1) x 所在的等价类 $\mathcal{O}_x$ 称为 G-set X 的一个**轨道**。易知 $\mathcal{O}_x = \{gx \mid g \in G\} = Gx$。从而 X 可以分拆为一些轨道的无交并。
(2) 若存在 $x \in X$ 使 $X = \mathcal{O}_x$，即 X 只有一个轨道，则称 G 在 X 上的作用是**传递的**。

例 2. (1) G 在 G/H 上的作用是传递的; (2) $\mathrm{Aut}(X)$ 在集合 X 上的作用是传递的。

定理 1 (轨道-稳定化子定理)**.** 设 X 是一个 G-set，G_{x_0} 是 $x_0 \in X$ 的稳定子群。证明：$f : G/G_{x_0} \to \mathcal{O}_{x_0}, gG_{x_0} \mapsto gx_0$ 是一个双射。特别地，$|\mathcal{O}_{x_0}| = |G/G_{x_0}|$。

证明. 若 $g_1G_{x_0} = g_2G_{x_0}$, 则 $g_2^{-1}g_1 \in G_{x_0}$。从而 $g_2^{-1}g_1x_0 = x_0 \Rightarrow g_1x_0 = g_2x_0$。所以映射 f 是定义良好的。
f 的单性：若 $f(g_1G_{x_0}) = f(g_2G_{x_0})$, 则 $g_1x_0 = g_2x_0 \Rightarrow g_2^{-1}g_1x_0 = x_0$。从而 $g_2^{-1}g_1 \in G_{x_0} \Rightarrow g_1G_{x_0} = g_2G_{x_0}$。所以 f 是单的。
f 的满性：由于 G 在单个轨道 $\mathcal{O}_{x_0}$ 上的作用是传递的，所以 $\forall x \in \mathcal{O}_{x_0}, \exists g \in G$ 使得 $x = gx_0$。从而 $f(gG_{x_0}) = gx_0 = x$。所以 f 是满的。 $\square$

题 5. 设 X 是一个 G-set, $x_1, \ldots, x_r$ 是 X 不同轨道的代表元。则有

$$|X| = \sum_{i=1}^{r} |\mathcal{O}_{x_i}| = \sum_{i=1}^{r} G/G_{x_i}.$$

若设 $x_{s+1}, \ldots x_r$ 对应平凡的轨道，即 $|\mathcal{O}_{x_j}| = |G/G_{x_j}| = 1$, $s+1 \le j \le r$, 则不动点集 $X^G := \{x \mid gx = x, \forall g \in G\} = \{x_{s+1}, \ldots, x_r\}$ 且有

$$|X| = |X^G| + \sum_{i=1}^{s} |\mathcal{O}_{x_i}| = |X^G| + \sum_{i=1}^{s} G/G_{x_i}.$$

定义 3. (1) 元素 $a \in G$ 的**中心化子** $C_G(a)$ 定义为：

$$C_G(a) = \{g \in G \mid ga = ag\}.$$

(2) 群 G 的**中心** $Z(G)$ 定义为：

$$Z(G) = \{z \in G \mid zg = gz \ \forall g \in G\}$$

注意，$C_G(a)$ 和 $Z(G)$ 均为 G 的子群。

定理 2 (有限群的类方程)**.** 设 G 是有限群，则

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

其中 $g_1, g_2, \ldots, g_r$ 是元素个数大于 1 的共轭类的代表元。

证明. 考虑 G 在自身上的共轭作用：$g\cdot a = gag^{-1}$。知 a 所在的轨道 $\mathcal{O}_a$ 即为 a 的共轭类，a 的稳定子群 $G_a = C_G(a)$ 对应 a 的中心化子。并且 $|\mathcal{O}_a| = 1 \iff a \in Z(G)$。
取 $g_1, \ldots, g_r, a_1, \ldots, a_s$ 为 G 中不同共轭类的代表元，其中 g_i 所在共轭类中的元素个数大于 1 个，a_j 所在共轭类中的元素个数为 1 个，$i = 1, \ldots, r$，$j = 1, \ldots, s$。易知 $Z(G) = \{a_1, \ldots, a_s\}$，$|Z(G)| = s$。将 G 中的元素分轨道计数，可有

$$|G| = \sum_{j=1}^{s} |\mathcal{O}_{a_j}| + \sum_{i=1}^{s} |\mathcal{O}_{g_i}| = s + \sum_{i=1}^{r} |G/G_{g_i}| = |Z(G)| + \sum_{i=1}^{r} |G/C_G(g_i)|.$$

□

题 6. 设 p 是一个素数，G 是一个有限群且 $|G| = p^n$，其中 $n > 0$。

(1) 令 $Z(G) = \{a \in G \mid ga = ag, \forall g \in G\}$ 为 G 的中心子群。证明：$Z(G) \neq \{e\}$。

(2) 设 X 是一个 G-set，则有

$$|X| \equiv |X^G| \pmod p,$$

其中 $X^G = \{x \in X \mid g \cdot x = x \ \forall g \in G\}$ 是不动点集。

证明： (1) 考虑群 G 在自身上的共轭作用：

$$G \times G \to G, \quad (g, a) \mapsto gag^{-1}.$$

$\forall b \in G$，知 G 在 $\mathcal{O}_b \subseteq G$ 上的作用是传递的。从而 $|\mathcal{O}_b| = |G/G_b|$，其中 G_b 是 b 的稳定子群。由于 $|G| = p^n$，$|\mathcal{O}_b|$ 整除 $|G|$，所以 $|\mathcal{O}_b| = 1$ 或 $p \mid |\mathcal{O}_b|$。注意到 $|\mathcal{O}_b| = 1 \iff \mathcal{O}_b = \{b\} \iff b \in Z(G)$。
若 $Z(G) = \{e\}$，则只有一个轨道元素的个数为 1，其余轨道元素的个数均为 p 的倍数。因此，

$$p^n = |G| = 1 + mp, \quad m \in \mathbb{Z}_{>0}.$$

这是一个矛盾。故 $Z(G) \neq \{e\}$。
(2) 结合题 5 中的结论私下验证。

题 7. 如果 $|G| = p^2$，其中 p 是素数，则 G 是阿贝尔群。

证明. 由于 $|G| = p^2$，$Z(G)$ 是群 G 的子群，从而 $|Z(G)| = 1$ 或 $|Z(G)| = p$ 或 $|Z(G)| = p^2$。由题 6 知，$|Z(G)| \neq 1$。如果 $|Z(G)| = p^2$，则 $G = Z(G)$ 是阿贝尔群。如果 $|Z(G)| = p$，则 $G/Z(G)$ 的阶为 p。再利用之前习题课中的结论：一个群如果模掉它的中心后是循环群，则该群本身是阿贝尔群。 □