子群与陪集

定义 1 (子群)**.** 设 G 是群，若非空集合 $H \subset G$ 且 H 是群，则称 H 是 G 的**子群**，记作 $H < G$.

考虑极端，G 本身和 $\{e\}$ 都是 G 的子群，称为 G 的**平凡子群**.

定理 1 (子群的充要条件)**.** 设 H 是群 G 的非空子集，则 $H < G$ 当且仅当对任意 $a, b \in H$，$ab^{-1} \in H$.

证明. 当 $H < G$ 时，由 H 运算的封闭性以及存在逆元即得 $ab^{-1} \in H$.

若对任意 $a, b \in H$，有 $ab^{-1} \in H$，则

对任意 $a, a \in H$，有 $e = aa^{-1} \in H$，幺元存在；

对 $e \in H$ 与任意 $b \in H$，有 $b^{-1} = eb^{-1} \in H$，逆元存在；

对任意 $a, b^{-1} \in H$，有 $ab = a(b^{-1})^{-1} \in H$，满足封闭律；

H 中的运算继承 G 中的运算，满足结合律，于是 $H < G$. □

定理 2. 设 H 是群 G 的非空有限子集，则 $H < G$ 当且仅当 H 对 G 的运算封闭.

证明. 必要性显然. 充分性：H 对 G 的运算封闭，故对任意 $a \in H$，$a^k \in H$，其中 k 为任意正整数. 由于 H 是有限群，于是存在正整数 $m > n$ 满足 $a^m = a^n$，故 $a^{m-n} = e \in H$. 当 $m - n = 1$ 时，$a = e$，于是 $a^{-1} = e \in H$；当 $m - n > 1$ 时，$a^{m-n-1}a = aa^{m-n-1} = e$，$a^{-1} = a^{m-n-1} \in H$，逆元存在. 封闭性满足，结合律满足，于是 $H < G$. □

定理 3. 若 $H_1 < G$，$H_2 < G$，则 $H_1 \cap H_2 < G$.

证明. 设 $a, b \in H_1 \cap H_2$，则由定理1，$ab^{-1} \in H_1$，$ab^{-1} \in H_2$，则 $ab^{-1} \in H_1 \cap H_2$，再用一次该定理，即得 $H_1 \cap H_2 < G$. □

推论 1. 设 I 为指标集，若对任意 $i \in I$，$H_i < G$，则 $\bigcap_{i \in I} H_i < G$.

下面是一些例子.

例 1. 数域 F 上全体 n 阶可逆方阵关于矩阵乘法构成群，称为**一般线性群**，记作 $GL_n(F)$. 其中，行列式为 1 的 n 阶方阵关于矩阵乘法也构成群，称为**特殊线性群**，记作 $SL_n(F)$. 显然 $SL_n(F) < GL_n(F)$.

例 2. 给定 $m \in \mathbb{Z}$，定义集合 $m\mathbb{Z} = \{mn \mid \forall n \in \mathbb{Z}\}$，定义运算为整数加法，则 $m\mathbb{Z} < \mathbb{Z}$.

定理 4. $(\mathbb{Z}, +)$ 的子群都是形如 $m\mathbb{Z}$ 的.

证明. 设 $H < \mathbb{Z}$. 若 $H = \{0\}$，则 $H = 0\mathbb{Z}$.

假设 $H \neq 0$，则存在非零整数. 由于 H 是子群，若 $a \in H$，则 $-a \in H$，因此 H 中必存在正整数. 定义 $m = \min\{a \in H | a > 0\}$

任取 $n \in H$，设 $n = qm + r$，其中 $0 \leqslant r < m$. 由于 $m \in H$ 且 H 是子群，于是 $r = n - qm \in H$. 但 $0 \leqslant r < m$，而 m 是 H 中最小的正整数，因此 $r = 0$，即 $n = qm \in m\mathbb{Z}$，所以 $H \subset \mathbb{Z}$.

由于 $m \in H$，且 H 是子群，对任意整数 k，有 $km \in H$，因此 $\mathbb{Z} \subset H$. $\square$

定义 2 (陪集)**.** 设 $H < G$，给定 $a \in G$，集合 $aH = \{ah | h \in H\}$ 称为以 a 为代表的**左陪集**. 类似地，集合 $Ha = \{ha | h \in H\}$ 称为以 a 为代表元的**右陪集**.

左陪集和右陪集的概念是对偶的，下面考虑左陪集的情形.

定理 5. 设 $H < G$，则 $aRb \iff a^{-1}b \in H$ 确定了 G 中的等价关系 R. a 所在的等价类 $\overline{a}$ 恰为以 a 为代表的左陪集 aH.

证明. 先证 R 为等价关系.

自反性：H 为子群，故 $a^{-1}a = e \in H$，即 aRa.

对称性：若 aRb，则 $a^{-1}b \in H$，$b^{-1}a = (a^{-1}b)^{-1} \in H$，即 bRa.

传递性：若 aRb，bRc，则 $a^{-1}b \in H$，$b^{-1}c \in H$，$a^{-1}c = a^{-1}bb^{-1}c \in H$，即 aRc.

再证 $\overline{a} = aH$. 对任意 $b \in \overline{a}$，$a^{-1}b \in H$，$b = aa^{-1}b \in aH$，于是 $\overline{a} \subset aH$；对任意 $b \in aH$，存在 $h \in H$ 使得 $b = ah$. $a^{-1}b = a^{-1}ah = h \in H$，于是 $aH \subset \overline{a}$. $\square$

由于 R 是一个等价关系，于是全体左陪集 $\{aH\}$ 为 G 的一个分类，称为**左陪集空间**. 由此可见左陪集空间是群 G 对关系 R 的商集，于是又把左陪集空间称为**左商集**，记作 G/R.

命题 1. 映射 $\varphi : H \to aH, h \mapsto ah$ 是双射.

证明. aH 是由 H 得到的，φ 是满射是显然的. 对任意 $h_1 \neq h_2 \in H$，$ah_1 \neq ah_2$（否则将违反消去律），故 φ 是单射. $\square$

定义 3 (指数)**.** 左陪集空间中陪集的个数称为**指数**，记作 $[G : H]$.

定理 6 (Lagrange)**.** 设 G 为有限群，$H < G$，则

$$|G| = [G : H]\,|H|.$$

证明. 设 $[G : H] = n$，a_i 为每个左陪集的代表元. $G = \bigsqcup_{i=1}^{n} a_i H$，而由命题1，$|a_i H| = |H|$，故 $|G| = n|H| = [G : H]\,|H|$. $\square$

推论 2. 设 G 是有限群，$K < H < G$，则 $[G : K] = [G : H]\,[H : K]$.