10.2 子群与群的陪集分解

① 子群

定义 1： 设$<G, *>$是一个群，非空集合 $H \subseteq G$。如果 H 对于 G 的运算$*$构成群，则称 H 是 G 的子群, 记作$H \leq G$。特别，若$H \subset G$，且 H 是 G 的子群，则称 H 是 G 的真子群。记作$H < G$。

- 例如，给定整数 n，$<n\mathbb{Z}, +>$是$<\mathbb{Z}, +>$的子群。当$n \neq 1$时，$<n\mathbb{Z}, +>$是$<\mathbb{Z}, +>$的真子群。

注 1： 任何群都有子群。例如 G 和$\{e\}$都是 G 的子群，称为 G 的平凡子群。

定理 1： 设 H 是群 G 的子群，则

(1) H 的单位元 e_H 一定是 G 的单位元，即 $e_H = e_G$。

(2) 对$\forall a \in H$，a 在 H 中的逆元a'，一定是 a 在 G 中的逆元。

定理 2： 设 H 是群 G 的非空子集，则 H 构成 G 的子群的充要条件是：

(1) G 的单位元 $e \in H$;

(2) 对 $\forall a, b \in H$，有 $ab \in H$;

(3) 对 $\forall a \in H$，有$a^{-1} \in H$。

定理 3： 设 H 是群 G 的非空子集，则 H 是 G 的子群的充要条件是

$$\forall a,\ b \in \mathrm{H} \Rightarrow ab^{-1} \in \mathrm{H}。$$

定理 4： 设 H 是群 G 的非空子集。如果 H 是有限集，则 H 是 G 的子群的充要条件是

$$\forall a,\ b \in \mathrm{H} \Rightarrow ab \in \mathrm{H}。$$

定义 2： 设 G 是一个群，$a \in \mathrm{G}$。令

$$\mathrm{H} = \{a^k | k \in \mathbb{Z}\},$$

则 H 是 G 的子群，称为由 a 生成的子群，记作$\langle a \rangle$。

例如：对于群$<\mathbb{Z}, +>$，由 2 生成的子群是

$$\langle 2 \rangle = \{2^k | k \in \mathbb{Z}\} = 2\mathbb{Z}。$$

对于四元群$\mathrm{G} = \{e, a, b, c\}$，它的所有生成的子群是

$$\langle e \rangle = \{e\},\ \langle a \rangle = \{e, a\},\ \langle b \rangle = \{e, b\}, \langle c \rangle = \{e, c\}。$$

例 1： 设 G 是一个群，令

$$\mathrm{C} = \{a \in \mathrm{G} | ax = xa, \forall x \in \mathrm{G}\},$$

则 C 是 G 的子群，称为 G 的中心。

注 2： 若 G 是一个阿贝尔群，则$\mathrm{C} = \mathrm{G}$。若 G 不是一个阿贝尔群，通常情况下，$\mathrm{C} = \{\mathrm{e}\}$。

定理 5： 设 G 是一个群，H, K 是 G 的子群。证明：

⑴ $H\cap K$也是 G 的子群。

⑵ $H\cup K$是 G 的子群$\Leftrightarrow H\subseteq K$ 或 $K\subseteq H$。

定义 3： 设 H 是群 G 的子群，$a\in G$。令

$$\mathrm{H}a=\{ha|h\in\mathrm{H}\}。$$

称 Ha 是子群 H 在 G 中的右陪集，a 为 Ha 的代表元素。

例 2： 设$G=\{e,a,b,c\}$是四元群，$H=\langle a\rangle=\{e,a\}$是 G 的子群。H 在 G 中的所有右陪集是

$$\mathrm{He}=\{\mathrm{e},a\},\ \mathrm{H}a=\{a,\mathrm{e}\},\mathrm{H}b=\{b,c\},\mathrm{H}c=\{c,b\}。$$

不同的右陪集只有两个，即 H 和$\{b,c\}$。

定义 4： 设 H 是群 G 的子群，$a\in G$。令

$$a\mathrm{H}=\{ah|h\in\mathrm{H}\}。$$

称 aH 是子群 H 在 G 中的左陪集，a 为 aH 的代表元素。

例 3： 设 G 是一个群，H 是 G 的子群。$\forall a\in G$。令

$$a^{-1}\mathrm{H}a=\{a^{-1}ha|h\in\mathrm{H}\},$$

则$a^{-1}\mathrm{H}a$是 G 的子群。

定理 6： 设 G 是一个群，H 是 G 的子群。则

(1) $\mathrm{He}=\mathrm{H}$。

(2) $\forall\, a\in \mathrm{G}$，有$a\in \mathrm{H}a$。

定理 7： 设 G 是一个群，H 是 G 的子群。则$\forall\, a$，$b\in \mathrm{G}$，有

$$a\in \mathrm{H}b \Leftrightarrow ab^{-1}\in \mathrm{H} \Leftrightarrow \mathrm{H}a=\mathrm{H}b。$$

定理 8： 设 G 是一个群，H 是 G 的子群。则

(1) $\forall\, a$，$b\in \mathrm{G}$，$\mathrm{H}a=\mathrm{H}b$ 或 $\mathrm{H}a\cap \mathrm{H}b=\emptyset$。

(2) $\bigcup_{a\in \mathrm{G}} \mathrm{H}a=\mathrm{G}$。

注 3：设 G 是一个群，H 是 G 的子群。则

(1) $\mathrm{eH}=\mathrm{H}$。

(2) $\forall\, a\in \mathrm{G}$，有$a\in a\mathrm{H}$。

(3) $\forall\, a$，$b\in \mathrm{G}, a\in b\mathrm{H} \Leftrightarrow b^{-1}a\in \mathrm{H} \Leftrightarrow a\mathrm{H}=b\mathrm{H}$。

(4) $\bigcup_{a\in \mathrm{G}} a\mathrm{H}=\mathrm{G}$。

注 4： 设 G 是一个群，H 是 G 的子群。对于 $a\in \mathrm{G}$，一般没有 $a\mathrm{H}=\mathrm{H}a$。

注 5：设 H 是群 G 的子群，则对$\forall\, a$，$b\in \mathrm{G}$，有一个从$\mathrm{H}a$到$\mathrm{H}b$的双射。

定理 9： 设 G 是一个群，H 是 G 的子群。则 H 在 G 中的右陪集的个数与左陪集的个数是一样的。

定义 5： 设 H 是群 G 的子群。H 在 G 中的右陪集(左陪集)的个数称为 H 在 G 中的陪集数， 记作$[\mathrm{G}:\mathrm{H}]$。

定理 10（拉格朗日定理）： 设 G 是有限群，H 是 G 的子群。则

$$|\mathrm{G}| = |\mathrm{H}|[\mathrm{G}:\mathrm{H}]。$$

推论 1： 设 G 是 n 阶群。则$\forall\ a \in \mathrm{G}$, $|a|$是 n 的因子，且有

$$a^n = \mathrm{e}。$$

推论 2： 设 G 是素数阶的群。则$\exists\ a \in \mathrm{G}$, 使得$\mathrm{G} = \langle a \rangle$。

注 6：拉格朗日定理对分析有限群中元素的阶很有用。

注 7：拉格朗日定理(或说它的推论 1)的逆命题并不为真。即 $r|n$，但 n 阶群中不一定含有 r 阶元。例如 Klein 四元群就没有 4 阶元。

例 4： 证明 6 阶群中必含有 3 阶元。

例 5： 证明 4 阶群必是阿贝尔群。

② 正规子群

定义 6: 设 H 是群 G 的子群，如果对 $\forall a \in G$ 有 $aH = Ha$，则称 H 是 G 的正规子群（不变子群）。

- 任何群 G 都有正规子群，因为 G 的两个平凡子群，即 G 和{e}都是 G 的正规子群。
- 阿贝尔群的子群都是正规子群。

定理 11：设 H 是群 G 的一个正规子群，则以下条件满足：

(1) 对$\forall a \in G$, $aH = Ha$。

(2) 对$\forall a \in G$, $\forall h \in H$, 必存在$h' \in H$, 使 $ha = ah'$。

(3) 对$\forall a \in G$, $\forall h \in H$, 有$aha^{-1} \in H$或者$a^{-1}ha \in H$。

定理 12: 群 G 的子群 H 是正规子群的充要条件是：对 $\forall a \in G$, $\forall h \in H$, 有，$aha^{-1} \in H$(或者$a^{-1}ha \in H$)。