

正规子群与商群

定义 1 (共轭). 设 $f, h \in G$, 若存在 $g \in G$, 使得

$$f = ghg^{-1},$$

则称 f 和 g 共轭.

容易验证, 共轭是一个等价关系, 于是决定了一个等价类, 称为共轭类.

定义 2 (共轭类). 设 G 是群, 对任意 $f \in G$, 与 f 共轭的元素组成的集合称为以 f 为代表元的共轭类.

定义 3 (自共轭元素). 如果以 f 为代表的共轭类中的元素只有 f 一个, 则称 f 是群 G 的自共轭元素.

性质 1. 一个共轭类中所有元素的阶相同.

性质 2. 共轭类的元素数目是群的阶的因子.

定义 4 (共轭子群). 若 $H < G$, $K < G$, 存在 $g \in G$ 使得

$$K = gHg^{-1},$$

则称子群 H 和 K 共轭.

定义 5 (元素的中心化子). 设 $a \in G$, 集合 $C_G(a) = \{g \in G \mid ga = ag\}$ 是 G 的子群, 称为 a 的中心化子.

定义 6 (子集的中心化子). 设 $S \subset G$, 集合 $C_G(S) = \{g \in G \mid gs = sg, \forall s \in S\}$ 是 G 的子群, 称为 S 的中心化子.

定义 7 (正规化子). 设 $M \subset G$, 集合 $N_G(M) = \{g \in G \mid gM = Mg\}$ 是 G 的子群, 称为 M 的正规化子.

如果对任意 $g \in G$, 子群 H 都是自共轭的, 则称 H 为正规子群, 即如下定义.

定义 8 (正规子群). 设 G 是群, $H < G$, 若有

$$ghg^{-1} \in H, \forall g \in G, \forall h \in H,$$

则称 H 是 G 的正规子群, 记作 $H \triangleleft G$.

例 1. 定义运算为矩阵乘法, $SL_n(F) \triangleleft GL_n(F)$.

例 2. 定义运算为数的加法, $m\mathbb{Z} \triangleleft \mathbb{Z}$.

定理 1. 设 $H < G$, 则下列条件等价.

1. $H \triangleleft G$;
2. $gH = Hg, \forall g \in G$;
3. $g_1Hg_2H = g_1g_2H, \forall g_1, g_2 \in G$.

证明. $1 \rightarrow 2$: 若 $H \triangleleft G$, 则 $gHg^{-1} = H$, 故 $gH = Hg$.

$2 \rightarrow 3$: 若 $gH = Hg$, 则 $g_1Hg_2H = g_1(Hg_2)H = g_1g_2H$.

$3 \rightarrow 1$: 若 $g_1Hg_2H = g_1g_2H$, 则 $gHg^{-1}H = gg^{-1}H = H$, 则 $gHg^{-1} = H$. \square

定义 9 (商群). 设 $H < G$, 关系 R 定义为 $aRb \iff a^{-1}b \in H$, 则

$$R \text{ 为同余关系 } \iff H \triangleleft G,$$

商集合 G/R 对同余关系 R 导出的运算也构成一个群, 称为 G 对 H 的商群, 记为 G/H .

证明. 必要性: 因为 $g^{-1}(gh) = h \in H$, 故 $gR(gh)$. 又 $g^{-1}Rg^{-1}$, 于是由同余关系,

$$(gg^{-1})R(ghg^{-1}),$$

即 $eR(ghg^{-1})$, $ghg^{-1} = e^{-1}ghg^{-1} \in H$, $H \triangleleft G$.

充分性: 设任意 $a_1, a_2, b_1, b_2 \in H$, a_1Rb_1, a_2Rb_2 , 则

$$(a_1a_2)^{-1}(b_1b_2) = a_2^{-1}a_1^{-1}b_1b_2 = a_2^{-1}a_1^{-1}b_1a_2a_2^{-1}b_2,$$

由于 $H \triangleleft G$, $a_1^{-1}b_1 \in H$, 则 $a_2^{-1}a_1^{-1}b_1a_2 \in H$, 又 $a_2^{-1}b_2 \in H$, 则 $(a_1a_2)^{-1}(b_1b_2) \in H$, 故 R 为同余关系. \square

例 3. 由于 $m\mathbb{Z} \triangleleft \mathbb{Z}$, 于是有商群

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\},$$

记为 \mathbb{Z}_m , 称为 \mathbb{Z} 的模 m 的剩余类加群.

剩余类加群的每一个元素叫做一个剩余类. 同一剩余类中的两个元素同余, 例如设 $a, b \in \bar{k}$, $k = 0, 1, \dots, m-1$, 则 $a \equiv b \pmod{m}$.