# 群同态, 类方程

请在 10 月 23 日课前提交纸质作业.

1. (5 分) 证明或证伪以下命题:

   (1) 单同态 $\varphi : G \to G$ 一定是自同构.

   (2) 满同态 $\varphi : G \to G$ 一定是自同构.

2. (5 分) 对任意群 $G$, 定义 $\operatorname{Aut} G$ 是所有 $G$ 的自同构 (automorphism), 定义 $\operatorname{Inn} G$ 为所有 $G$ 的内自同构 (inner automorphism).

$$\operatorname{Aut} G := \{\text{同构 } \sigma : G \to G\},$$
$$\operatorname{Inn} G := \{\phi_g : h \mapsto ghg^{-1} | g \in G\},$$

   证明, $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

3. (10 分) 如果 $p = 2p' + 1$, 其中 $p, p'$ 都是素数, 那么 $p$ 被称作"安全素数". 考虑两个安全素数 $p = 2p' + 1, q = 2q' + 1$, 其中 $p, p', q, q'$ 两两不同且均大于 2. 记 $n = pq$.

   证明: $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_n$.

   提示: 可以考虑如下三个映射, $\pi_1 : \mathbb{Z}_n^* \to \mathbb{Z}_{n^2}^*$, $\pi_2 : \mathbb{Z}_n \to \mathbb{Z}_{n^2}^*$ 和 $\pi : \mathbb{Z}_n^* \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}^*$

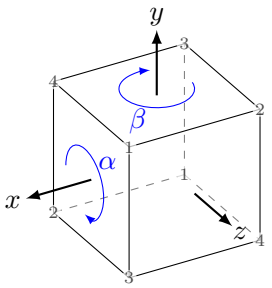
$$\pi_1(a) = a^n, \qquad \pi_2(t) = (1+n)^t, \qquad \pi(a,t) = a^n(1+n)^t.$$

4. (10 分) 给定一个正方体, 按照某种特定方式对它整体旋转 (即特殊正交变换, 可以保角度的旋转, 但没有镜面操作) 的时候, 它会与原来的正方体重合, 尽管点和面可能换了位置. 以正方体的中心为原点, 沿着正方体的边建立 $x$ 轴 (左右方向)、$y$ 轴 (上下方向) 和 $z$ 轴 (前后方向), 正方体的"基本旋转"恰好就是顺时针沿着 $x$ 轴或 $y$ 轴转九十度, 记为 $\alpha, \beta$. 可以证明, 保持正方体占位不变的旋转都是由这两种旋转生成的, 因此正方体的旋转构成了一个群, 记为 $R$.

   (1) 证明: $R \cong \mathrm{Sym}(4)$, 因此 $\mathrm{Sym}(4)$ 可以被视为正方体的旋转群.

   提示: 对正方体的顶点编号 $1, 2, 3, 4$, 并且对径点编上相同的号, 这样一来, 每一个面的顶点都恰好具有四个编号, 考虑底面的编号, 给出 $\alpha, \beta$ 所对应的 $\mathrm{Sym}(4)$ 中的元素, 证明他们生成了 $\mathrm{Sym}(4)$.

   (2) 写出 $\mathrm{Sym}(4)$ 的类方程 (class equation), 并解释它的几何意义 (即每个共轭类对应的旋转类型).



5. (10 分) 设 $N \trianglelefteq G$, $|N| = n$, $[G : N] = m$. 这里记号 $[G : N]$ 表示 $G$ 中 $N$ 的左陪集的数目, 被称作指数 (index).

   (1) 设 $g \in G$ 且 $\gcd(\mathrm{order}(g), m) = 1$. 证明 $g \in N$.

   (2) 设 $m$ 和 $n$ 互素. 证明, $N$ 是 $G$ 的唯一的大小为 $n$ 的正规子群.

6. (10 分) 设 $G$ 是一个 15 阶群.

   (1) 证明 $G$ 有阶分别为 3 和 5 的正规子群.

   (2) 证明 $G$ 是循环群.

   提示: 需要使用 Sylow 第三定理: 若 $|G| = p^k m$ ($p$ 为素数, $m > 0$, $\gcd(p, m) = 1$), 记 Sylow $p$-子群的数目为 $n_p$, 那么 $n_p \mid m$ 且 $n_p \equiv 1 \pmod{p}$.