群同态, 类方程

参考答案

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.

   解

   (1) 反例: $\mathbb{Z}$ 上的同态 $x \mapsto 2x$.

   (2) 反例: $\mathbb{R}/\mathbb{Z}$ 上的同态 $x \mapsto 2x$.

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

   解 考虑任意 $\sigma \in \operatorname{Aut} G, \phi_g \in \operatorname{Inn} G$. 对任意 $x \in G$,

$$(\sigma\phi_g\sigma^{-1})(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \phi_{\sigma(g)}(x)$$

   也就是 $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)} \in \operatorname{Inn} G$.

   注. 商群 $\operatorname{Out} G = \operatorname{Aut} G / \operatorname{Inn} G$ 被称作 G 的外自同构群 *(outer automorphism)*.

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 $\pi : \mathbb{Z}_n^* \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}^*$

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

   解 我们给两种解法.

   解法一:

   由中国剩余定理,

$$\mathbb{Z}_{p^2q^2}^* \cong \mathbb{Z}_{p^2}^* \times \mathbb{Z}_{q^2}^*.$$

注意到 $|\mathbb{Z}_{p^2}^*| = \varphi(p^2) = p(p-1) = 2pp'$, 因此

$$\mathbb{Z}_{p^2}^* \cong \mathbb{Z}_p \times \mathbb{Z}_{p'} \times \mathbb{Z}_2 \cong \mathbb{Z}_p \times \mathbb{Z}_{2p'} \cong \mathbb{Z}_p \times \mathbb{Z}_p^*.$$

其中每一个同构都是因为有限生成 Abel 群分类定理（他们都是有限 Abel 群）. 于是,

$$\mathbb{Z}_{p^2q^2} \cong \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_p^* \times \mathbb{Z}_q^*. \tag{1}$$

根据中国剩余定理,

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q, \qquad \mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

因此, 结合 (1), 我们有

$$\mathbb{Z}_{p^2q^2} \cong \mathbb{Z}_{pq} \times \mathbb{Z}_{pq}^*.$$

解法二:

考虑提示中的 $\pi : \mathbb{Z}_n^* \times \mathbb{Z}_n \to \mathbb{Z}_{n^2}^*$, $\pi(a,t) = a^n(1+n)^t$, 容易验证这是一个同态.

$$\pi(a_1a_2, t_1+t_2) = (a_1a_2)^n(1+n)^{t_1+t_2} = a_1^n(1+n)^{t_1} \cdot a_2^n(1+n)^{t_2} = \pi(a_1,t_1)\pi(a_2,t_2).$$

(更严格地来说, 我们还应该验证 π 是良好定义的. 注意到我们的定义中隐含地把 $a \in \mathbb{Z}_n^*$ 视作了 $\mathbb{Z}_{n^2}^*$ 中的元素. 这时代表元的选取可能造成歧义, $a, a+n$ 在 $\mathbb{Z}_n^*$ 中代表相同的元素, 需要验证 $a^n, (a+n)^n$ 在 $\mathbb{Z}_{n^2}^*$ 中相同. 所幸这不难用二项式定理验证.)

其次, 我们来证明这是一个单同态. 也就是说, 对任意 $(a,t) \in \operatorname{Ker}\pi$, 我们要证明 $(a,t) = (1,0)$. 首先对 $\pi(a,t)$ 取 $\varphi(n)$ 次方, 以孤立 t.

$$1 = \pi(a,t)^{\varphi(n)} = (a^n(1+n)^t)^{\varphi(n)} = a^{\varphi(n^2)}(1+n)^{t\varphi(n)} = (1+n)^{t\varphi(n)}.$$

根据二项式定理, $(1+n)^t = 1 + nt + n^2(\dots) \equiv 1 + nt \pmod{n^2}$. 因此上式可以进一步展开为

$$1 = \pi(a,t)^{\varphi(n)} = 1 + nt\varphi(n) \ (\text{in } \mathbb{Z}_{n^2})..$$

两边都减 1 并除以 n, 得到 $t\varphi(n) = 0$ (in $\mathbb{Z}_n$). 根据条件, $\varphi(n) = 4p'q'$ 与 n 互素, 所以 $t = 0$.

现在, 已证明 $1 = \pi(a,t) = a^n$ (in $\mathbb{Z}_{n^2}$), 那么可以得出

$$1 = a^n \ (\text{in } \mathbb{Z}_{n^2}).$$

根据条件, n 与 $\varphi(n)$ 互素, 令 n^{-1} 表示 n 模 $\varphi(n)$ 的乘法逆元. 对上式两边取 n^{-1} 次方, 得到

$$1 = a^{nn^{-1}} = a \pmod{n}.$$

以上说明 π 是单同态.

最后, 因为 $\mathbb{Z}_n^* \times \mathbb{Z}_n$ 和 $\mathbb{Z}_{n^2}^*$ 的大小相同, 所以 π 是单同态就一定是同构.

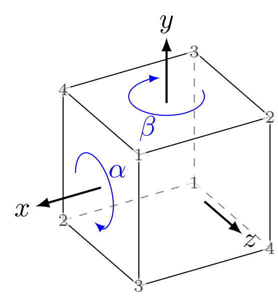
注. 计算解法二中的同构不需要知道 n 的素因数分解, 这个特性被用于构造公钥密码.

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 α, β. 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 α, β 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）.



解

(1) $\alpha = (1\ 4\ 2\ 3), \beta = (1\ 2\ 3\ 4)$，考虑 $(1\ 2) = \beta^2\alpha$, $(1\ 3) = \beta\alpha^2$, $(1\ 4) = \beta\alpha\beta$, 对于任意对换 $(a\ b) = (1\ a)(1\ b)(1\ a)$, 故 α, β 可生成 $\mathrm{Sym}(4)$ 中的所有元素.

(2) 类方程为

$$24 = 1 + 6 + 8 + 3 + 6,$$

分别对应了五个共轭类:

1. $\{\mathrm{id}\}$: 不变.
2. $\{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}$: 以两条对棱的中点的连线为轴旋转 180 度. 稳定化子 $\mathrm{Stab}((1\ 2)) = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$: 令前述旋转轴不变或翻转的变换.
3. $\{(1\,2\,3), (1\,2\,4), (1\,3\,4), (2\,3\,4), (3\,2\,1), (4\,2\,1), (4\,3\,1), (4\,3\,2)\}$: 以正方体的体对角线（对径点连线）为轴顺时针旋转 120 度或 240 度. 稳定化子 $\mathrm{Stab}((1\ 2\ 3)) = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$: 令前述旋转轴不变的变换, 只能绕相同的轴旋转.
4. $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$: 绕 $x/y/z$ 轴旋转 180 度. 稳定化子 $\mathrm{Stab}((1\ 2)(3\ 4)) = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 4\ 2\ 3), (1\ 3\ 2\ 4)\}$: 令前述旋转轴不变或翻转的变换.

5. $\{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$: 绕 $x/y/z$ 轴顺时针旋转 90 度或 270 度. 稳定化子 $\mathrm{Stab}((1\ 2\ 3\ 4)) = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$: 令前述旋转轴不变的变换, 只能绕相同的轴旋转.

注. 本题旨在说明有限群的几何意义. 实际上，正多面体的对称群都和某种群有对应关系，而他们对应的旋转类型则形成了对应的类方程.

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.

解

(1) 考虑 G 到 G/N 的典范 (canonical) 同态:

$$\pi : G \to G/N$$
$$g \mapsto gN$$

则 $\pi(g)^{\mathrm{order}(g)} = \pi\left(g^{\mathrm{order}(g)}\right) = e$, 因此 $\mathrm{order}(\pi(g)) \mid \mathrm{order}(g)$.

另一方面, $\mathrm{order}(\pi(g)) \mid |G/N| = m$, 由 $\gcd(\mathrm{order}(g), m) = 1$ 知 $\pi(g) = \bar{e}$, 即 $g \in N$.

(2) 若 G 还有另一个大小为 n 的正规子群 $N' \neq N$, 任取 $g \in N', g \notin N$, 则 $\mathrm{order}(g) \mid |N'| = n$, 又 $(n, m) = 1$, 由 (1) 知 $g \in N$, 矛盾! 因此 G 只有一个大小为 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 $n_p \equiv 1 \pmod{p}$.

解

(1) 由 Sylow 第三定理，5-Sylow 子群的个数满足 $n_5(G) \equiv 1 \pmod 5$ 且 $n_5(G) \mid 3$. 这推出 $n_5(G) = 1$. 设唯一的 5-Sylow 子群为 P，由唯一性知 P 正规。

由 Sylow 第三定理，3-Sylow 子群的个数满足 $n_3(G) \equiv 1 \pmod 3$ 且 $n_3(G) \mid 5$. 这推出 $n_3(G) = 1$. 设唯一的 3-Sylow 子群为 Q，由唯一性知 Q 正规。

(2) P, Q 分别同构于 $\mathbb{Z}_5$ 和 $\mathbb{Z}_3$, 它们的交为 $\{e\}$. 对于两个交集平凡的正规子群，它们的内直积 $PQ = QP \cong P \times Q$ 是一个有 15 个元素的子群. 因此 $G \cong P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$, 即 G 是循环群.

注. 课上讨论的 $Abel$ 群的子群的内直积。可以拓展到任意群 G 的交集平凡的正规子群 H, K. 同样有 $HK = KH \cong H \times K$. 证明可以利用自然映射 $\phi : H \times K \to HK, \phi(h, k) = hk$.