群论

参考答案

1. (10 分) 给定群 G，定义它的换位子（commutator subgroup）G' 为 $\langle aba^{-1}b^{-1} : a, b \in G\rangle$.
   (1) 证明：$G' \trianglelefteq G$.
   (2) 考虑 $N \trianglelefteq G$，证明：G/N 是 Abel 群当且仅当 $G' \leq N$.
   (3) 考虑 $\mathrm{Sym}(4)$，即 $\{1, 2, 3, 4\}$ 上的对称群，请给出一个序列：
   $$S_4 = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^n = \{1\},$$
   满足 G^i/G^{i+1}（$i = 0, \ldots, n-1$）是 Abel 群.

解

(1) G' 是 G 的子群显然，下证正规性：对于任意 $a \in G, b \in G'$, $aba^{-1}b^{-1} \in G'$，故 $aba^{-1} \in G'$，正规性得证.

(2) G/N 是 Abel 群 $\iff$ 任意 $a, b \in G, aN \cdot bN = bN \cdot aN \iff$ 任意 $a, b \in G, abN = baN \iff$ 任意 $a, b \in G$，$a^{-1}b^{-1}ab \in N \iff G' \leq N$.

(3) 考虑不断取前面一个群的换位子，$\mathrm{Sym}(4)$ 的换位子是 $\mathrm{Alt}(4)$, $\mathrm{Alt}(4)$ 的换位子是
$$\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$
这个群被称为 Klein 四元数群，记为 V，V 的换位子为 $\{1\}$.

故可以构造序列：$\mathrm{Sym}(4), \mathrm{Alt}(4), V, \{1\}$.

注. *存在上面序列的群被称为***可解群**，*$\mathrm{Sym}(n)$ 是可解群当且仅当 $n \leq 4$，特别地，$\mathrm{Sym}(5)$ 的正规子群 $\mathrm{Alt}(5)$ 是单群，因而不可解. 一个群是否可解对应了一个代数方程是否可以根式求解，这是 Galois 理论的重要内容.*

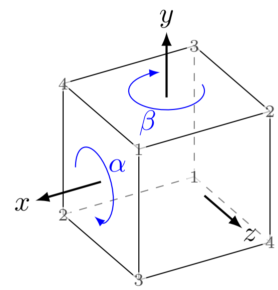
关于四元数群：我们知道，虚数单位 i 是满足 $i^2 = -1$ 的人造数. 然而，我们完全不需要限制只有一个 i 和一个 $-i$ 满足这一方程，我们还可以给出别的不同的虚数单位 $j, k, \ldots$. 但是，并不是任意个数的虚数单位都可以得到我们想要的代数系统，实际上，类似 $\mathbb{R}$ 和 $\mathbb{C}$ 的数域（即带单位元的赋范可除代数）只有四元数（三个虚数单位）和八元数（七个虚数单位）(Hurwitz 定理）. 四元数的虚数单位连同 1 构成了四元数群.

2. (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. $\{1\}$: 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.
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.
4. $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$: 绕 $x/y/z$ 轴旋转 180 度.
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.

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.

3. (10 分) 若 $N \lhd G$，考虑商群 G/N，并考虑自然映射 $\eta : G \to G/N$，$\eta(g) = gN$. 若 $K' \lhd H' \lhd G/N$. 定义

$$H = \eta^{-1}(H') = \{g \in G \mid \eta(g) \in H'\},$$
$$K = \eta^{-1}(K') = \{g \in G \mid \eta(g) \in K'\}.$$

证明:

(1) H, K 是群且 $N \triangleleft K \triangleleft H \triangleleft G$.

(2) $H/K \cong H'/K'$.

解

(1) 由于 η 是同态映射，任意 $a, b \in H, \eta(ab^{-1}) = \eta(a)\eta(b^{-1}) \in H'$，故 $ab^{-1} \in H$, 所以 H 是群，同理 K 也是群.

下证 $K \triangleleft H$. 首先，显然有 $K \leq H$. 由于 $K' \triangleleft H'$, 对任意 $k \in K, h \in H$，$\eta(hkh^{-1}) = \eta(h)\eta(k)\eta(h)^{-1} \in H'$，故 $hkh^{-1} \in H$，故 $K \triangleleft H$, 剩余部分可类似证明.

(2) 构造映射 $\phi : aK \mapsto (aN)K'$, 由于 $aK = bK \iff a^{-1}b \in K \iff a^{-1}bN \in K' \iff (aN)^{-1}bN \in K' \iff (aN)K' = (bN)K'$，故 ϕ 是良定义的且为单射，易证 ϕ 为满射，故 ϕ 为双射. 另外，对任意 $a, b \in H$，$\phi(aK \cdot bK) = \phi(abK) = (abN)K' = (aN)K' \cdot (bN)K' = \phi(aK)\phi(bK)$，故 ϕ 是同态映射. 综上所述，ϕ 是从 H/K 到 H'/K' 的同构映射，即证.

4. (10 分) 设 $N \trianglelefteq G$，$|N| = n$，$[G : N] = m$

(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:

$$\begin{aligned}\pi : G &\to G/N \\ g &\mapsto gN\end{aligned}$$

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.

5. (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) 对于 $p = 5$, 设 G 的 Sylow 5 子群为 P, 则 $|P| = 5$. 由 Sylow 第三定理, Sylow 5 子群的个数 $n_5(G) \equiv 1(\mathrm{mod} 5)$, 但又有 $n_5(G) \mid |G| = 15$, 这推出 $n_5(G) = 1$. 和它共轭的子群也是 Sylow 5 子群, 由唯一性知只能是 P 自身, 即 $P \trianglelefteq G$. 同理, G 的 Sylow 3 子群也正规, 并因此唯一.

(2) 设唯一的 Sylow 3 子群为 Q. 由于 3 阶群和 5 阶群分别同构于 $\mathbb{Z}_3$ 和 $\mathbb{Z}_5$, 它们的交为 $\{e\}$. 因此 $PQ = QP \cong P \times Q$ 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.