清华大学 2025-2026 秋季学期，群与 Galois 理论，作业 4

请用 A4 大小的纸张**正反面**用钢笔，签字笔或者圆珠笔书写，并注明自己的姓名、年级（书院或系）和作业的**总页数**。除定理公式所涉及的人名之外，请使用**中文**。本次作业请扫描并上传至网络学堂，具体截止日期请查阅网络学堂，逾期视作零分。

A. 最少的生成元个数

G 是群，如果存在有限个 $x_1, \cdots, x_n$，使得 $G = \langle x_1, \cdots, x_n \rangle$，我们就称 G 是**有限生成的**。以上最小可能的 n 被称作是 G 的**最少的生成元个数**，记作 $\min_{\mathrm{gen}}(G)$。我们规定 $\min_{\mathrm{gen}}(\{1\}) = 0$。

A1) 证明，$\min_{\mathrm{gen}}(G) = 1$ 等价于 G 是非平凡的循环群。

A2) 假设 $n \geqslant 3$。证明，$\min_{\mathrm{gen}}(\mathfrak{S}_n) = 2$。

A3) p 是素数，r 是自然数，$G = \left(\mathbb{Z}/p\mathbb{Z}\right)^r = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{r\text{ 个}}$。证明，$\min_{\mathrm{gen}}(G) = r$。

（提示：将 G 视为 $\mathbb{Z}/p\mathbb{Z}$-线性空间）

A4) G 是有限生成群，假设有**满的**群同态 $\varphi : G \longrightarrow G'$。证明，$G'$ 是有限生成群并且

$$\min_{\mathrm{gen}}(G') \leqslant \min_{\mathrm{gen}}(G).$$

A5) G 是群，$H \lhd G$ 是正规子群。证明，如果 H 和 G/H 是有限生成的，那么，G 也是并且

$$\min_{\mathrm{gen}}(G) \leqslant \min_{\mathrm{gen}}\left(G/H\right) + \min_{\mathrm{gen}}(H).$$

A6) 对于群 $A = \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$，其中，$s \in \mathbb{Z}_{\geqslant 1}, d_1, \cdots, d_s \in \mathbb{Z}_{\geqslant 2}$，使得 $d_s \mid d_1, d_{s-1} \mid d_{s-2}, \cdots, d_2 \mid d_1$。证明，$\min_{\mathrm{gen}}(A) = s$。

A7) 对于群 $A = \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r\text{ 个}}$。证明，$\min_{\mathrm{gen}}(A) = r$。据此证明，如果 $\mathbb{Z}^r \simeq \mathbb{Z}^{r'}$，那么，$r = r'$。

A8)（子群生成元个数可以更多）对任意的 $n \geqslant 3$，给出如下的例子：G 是群，$H < G$ 是子群，$\min_{\mathrm{gen}}(G) = 2$ 而 $\min_{\mathrm{gen}}(H) = n$。

A9)（有限生成群的子群未必有限生成）令 $G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle < \mathbf{GL}(2; \mathbb{Q})$ 是由两个元素生成的群。证明，$H = \left\{ \begin{pmatrix} 1 & \frac{m}{2^k} \\ 0 & 1 \end{pmatrix} \middle| k \in \mathbb{Z}_{\geqslant 0}, m \in \mathbb{Z} \right\}$ 是 G 的子群并且不是有限生成的。

A10)（有限生成交换群子群的生成元个数）G 是有限生成交换群，$H < G$ 是子群。证明，

$$\min_{\mathrm{gen}}(H) \leqslant \min_{\mathrm{gen}}(G).$$

（提示：找一个 $g \in G$，使得 $\min_{\mathrm{gen}}\left(G/\langle g \rangle\right) < \min_{\mathrm{gen}}(G)$）

A11) $r \geqslant 1$，A 是 $\mathbb{Z}^r$ 的子群。证明，存在 $r' \leqslant r$，使得 $A \simeq \mathbb{Z}^{r'}$。

B. 阶为 p^3 的群有 5 个，$p \neq 2$

假设 p 是奇素数。用 $\mathbb{F}_p$ 表示 p 个元素的有限域，用 $\mathbb{Z}/p\mathbb{Z}$ 表示其加法群。

B1) 在同构意义下，写下所有阶为 2^3 的群和阶为 p^2 的群。

B2) 我们在课上用对角线均为 1 的上三角矩阵给出了 $\mathbf{GL}(2;\mathbb{F}_p)$ 一个 Sylow 子群。计算 $\mathbf{GL}(2;\mathbb{F}_p)$ 中 Sylow p-子群的个数。

B3) 给定两个非平凡的群同态 $\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbf{GL}(2;\mathbb{F}_p)$ 和 $\varphi' : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbf{GL}(2;\mathbb{F}_p)$。对任意的整数 k，令 $\varphi_k(x) = \varphi(kx)$，其中，$x \in \mathbb{Z}/p\mathbb{Z}$。证明，存在 $A \in \mathbf{GL}(2;\mathbb{F}_p)$ 和 $k = 1, 2, \cdots, p-1$，使得对任意的 $x \in \mathbb{Z}/p\mathbb{Z}$，有

$$\varphi'(x) = A \cdot \varphi_k(x) \cdot A^{-1}.$$

B4) 在同构的意义下，可能的半直积 $\left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\right) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ 恰有两个。进一步证明，其中恰有一个是非交换群并且其中心同构于 $\mathbb{Z}/p\mathbb{Z}$。

B5) G 是群，$|G| = p^3$。假设 G 不是循环群并且存在 $g \in G$ 使得 $\mathrm{ord}(g) = p^2$。证明，$\langle g \rangle \lhd G$。

B6) 证明，在同构的意义下，上一个小问题中的群恰好两个。

B7) 在同构意义下，写下所有阶为 p^3 的群。

I do not believe there is anything useful which men can know with exactitude that they cannot know by arithmetic and algebra.

——— Nicolas Malebranche
