群与 Galois 理论

作业 4

陈宏泰

2024011131

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2025 年 11 月 23 日

目录

A. 最少生成元的个数

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 $\min_{\text{gen}}(G)$ 。我们规定 $\min_{\text{gen}}(\{1\}) = 0$ 。

A1)

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

证明： 若 $\min_{\text{gen}}(G) = 1$, 那么 $G = \langle x \rangle$, 其中 $x \neq 1$. 那么 $G = \{x^r \mid r \in \mathbb{Z}\}$, G 是非平凡的循环群.

若 G 是非平凡的循环群, 那么 $\exists\ x \neq 1 \in G, \text{s.t. } G = \{x^r \mid r \in \mathbb{Z}\}$, 从而 $G = \langle x \rangle$. 即 $\min_{\text{gen}}(G) = 1$. □

注： 这实在是显然的.

A2)

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

证明： 由课上内容知 $\mathfrak{S}_n = \langle (12), (12\cdots n) \rangle$. 于是 $\min_{\text{gen}}(G) \leqslant 2$.

又由 $\mathfrak{S}_n$ 非平凡的循环群, 知 $\min_{\text{gen}}(G) \neq 1$. 于是 $\min_{\text{gen}}(G) = 2$. □

A3)

p 是素数，r 是自然数，$G = (\mathbb{Z}/p\mathbb{Z})^r = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{r\text{ 个}}$ 。证明，$\min_{\text{gen}}(G) = r$ 。（提示：将 G 视为 $\mathbb{Z}/p\mathbb{Z}$ 一线性空间）

证明： 将 G 视为 $\mathbb{Z}/p\mathbb{Z}$-线性空间, 那么其维数为 r, 等价于其一组基有 r 个元素. 并且由基的定义可知, G 不可被 $r-1$ 个元素生成. 于是 $\min_{\text{gen}}(G) = r$. □

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

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

证明： 假设 $G = \langle x_1, x_2, \cdots, x_n \rangle$, 其中 $n = \min_{\text{gen}}(G)$. 由于 φ 是满同态, 于是

$$G' = \varphi(G) = \varphi\langle x_1, x_2, \cdots, x_n \rangle = \langle \varphi(x_1), \varphi(x_2), \cdots, \varphi(x_n) \rangle.$$

从而 G' 是有限生成的且 $\min_{\text{gen}}(G') \leqslant n = \min_{\text{gen}}(G)$. □

A5)

G 是群，$H \triangleleft G$ 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

$$\min_{\text{gen}}(G) \leqslant \min_{\text{gen}}(G/H) + \min_{\text{gen}}(H).$$

证明： 设 $H = \langle x_1, x_2, \cdots, x_{n_1}\rangle, G/H = \langle y_1H, y_2H, \cdots, y_{n_2}H\rangle$, 其中 $n_1 = \min_{\text{gen}}(H), n_2 = \min_{\text{gen}}(G/H)$.

于是 $\forall\ g \in G, g \in yH$, 而其中 $yH \in \langle y_1H, y_2H, \cdots, y_{n_2}H\rangle$. 从而通过适当取左陪集的代表元, 有 $\forall\ yH \in G/H$, 有 $g \in \langle y_1, y_2, \cdots, y_{n_2}\rangle$. 又由 $g \in yH$, 知 $\exists\ h \in H, \text{s.t. } g = yh$, 而 $h \in H = \langle x_1, x_2, \cdots, x_{n_1}\rangle$, 于是 $g \in \langle x_1, x_2, \cdots, x_{n_1}, y_1, y_2, \cdots, y_{n_2}\rangle$.

于是 $G \subset \langle x_1, x_2, \cdots, x_{n_1}, y_1, y_2, \cdots, y_{n_2}\rangle$, 从而 $\min_{\text{gen}}(G) \leqslant n_1 + n_2 = \min_{\text{gen}}(H) + \min_{\text{gen}}(G/H)$. □

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 $d_s \mid d_{s-1}, d_{s-1} \mid d_{s-2}, \cdots, d_2 \mid d_1$。证明，$\min_{\text{gen}}(A) = s$.

注： 有 typo: $d_s \mid d_1$ 应该为 $d_s \mid d_{s-1}$.

证明： 首先证明 $\min_{\text{gen}}(A) \leqslant s$: 取标准基

$$e_1 = (\underbrace{1, 0, \cdots, 0}_{s\text{个}}), e_2 = (0, 1, \cdots, 0), \cdots, e_s = (0, 0, \cdots, 1).$$

那么 $A = \langle e_1, e_2, \cdots, e_s\rangle$, 从而 $\min_{\text{gen}}(A) \leqslant s$.

再证明 $\min_{\text{gen}}(A) \geqslant s$: 假设 A 可以有 r 个生成元生成, 即存在 $g_1, g_2, \cdots, g_r, \text{s.t.}$

$$A = \langle g_1, g_2, \cdots, g_r\rangle.$$

由 $d_i \geqslant 2$, 知 $\exists\ p$ 为素数, s.t. $p \mid d_1$, 又 $d_s \mid d_{s-1}, d_{s-1} \mid d_{s-2}, \cdots, d_2 \mid d_1$, 从而 $p \mid d_i, \forall\ 1 \leqslant i \leqslant s$. 考虑群同态 φ:

$$A = \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^n, \quad (a_1, a_2, \cdots, a_s) \mapsto (a_1 \bmod p, a_2 \bmod p, \cdots, a_s \bmod p).$$

由于 $p \mid d_i, \forall\ 1 \leqslant i \leqslant s$, 群同态是良定义的. 又显然有 $\text{Ker}\ \varphi = pA \coloneqq \{(pa_1, pa_2, \cdots, pa_s) \mid (a_1, a_2, \cdots, a_s) \in A\}$, $\text{Im}\ \varphi = (\mathbb{Z}/p\mathbb{Z})^n$. 由第一同构定理有

$$A/pA \simeq (\mathbb{Z}/p\mathbb{Z})^n.$$

$A = \langle g_1, g_2, \cdots, g_r\rangle \Rightarrow A/pA = \langle g_1(pA), g_2(pA), \cdots, g_r(pA)\rangle$. 又由于同构, 可将 A/pA 视为 $\mathbb{F}_p$-线性空间. 由线性空间存在基, 以及基的定义可知 $r \geqslant s$, 即 $\min_{\text{gen}}(A) \geqslant s$.

综上, $\min_{\text{gen}}(A) = s$. □

A7)

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

证明： $\min_{\text{gen}}(A) = r$ 的证明思路与 A6) 完全相同.

若 $\varphi : \mathbb{Z}^r \xrightarrow{\cong} \mathbb{Z}^{r'}$, 那么取 $\mathbb{Z}^r = \langle g_1, g_2, \cdots, g_r \rangle$, 则有 $\mathbb{Z}' = \langle \varphi(g_1), \varphi(g_2), \cdots, \varphi(g_r) \rangle$. 从而 $r \geqslant r'$. 同理有 $r \leqslant r'$. 最终有 $r = r'$. □

注：生成元的构造相同. 对于素数 p 的选取是任意的.

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，$\min_{\text{gen}}(G) = 2$ 而 $\min_{\text{gen}}(H) = n$ 。

证明：直接给出置换群的例子:

考虑 $\mathfrak{S}_{2n}$, 由课上结论可知 $\mathfrak{S}_{2n} = \langle (12), (12\cdots(2n)) \rangle$. 故 $\min_{\text{gen}}(\mathfrak{S}_{2n}) = 2$. 其有子群 $H = \langle (12), (34), \cdots, (2n-1, 2n) \rangle$, 注意到 H 中的非单位元都是 2 阶的, 从而同构于 $(\mathbb{Z}/2\mathbb{Z})^n$, 由 A6) 知 $\min_{\text{gen}}(H) = \min_{\text{gen}}((\mathbb{Z}/2\mathbb{Z})^n) = n$. 从而 $G = \mathfrak{S}_n, H$ 符合条件. □

注：关于非单位元都是 2 阶的群. 可以推出此群

- 是交换群;
- 同构于 $(\mathbb{Z}/2\mathbb{Z})^n$.

前者是容易证明的, 又由于群是交换的, 可以证明其是 $\mathbb{F}_2$-线性空间, 后者得证.

最主要的是上课已经充分论证过了.

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。

证明：先证明 H 是 G 的子群:

- $H \subset G$: 计算可知:

$$A^n = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix}, \quad A^{-n} = \begin{pmatrix} 2^{-n} & 0 \\ 0 & 1 \end{pmatrix}, \quad A^n B A^{-n} = \begin{pmatrix} 1 & 2^n \\ 0 & 1 \end{pmatrix}, \text{ 其中} n \in \mathbb{Z}.$$

  故 $\begin{pmatrix} 1 & 2^n \\ 0 & 1 \end{pmatrix} \in H$, 其中 $n \in \mathbb{Z}$, 即得 $H \subset G$

- H 是 G 的子群

$$\begin{pmatrix} 1 & \frac{m}{2^k} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{n}{2^l} \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \frac{2^l m - 2^k n}{2^{k+l}} \\ 0 & 1 \end{pmatrix} \in H$$

反证法, 若 H 为有限生成的, 则存在 $S=\left\{\begin{pmatrix}1 & \frac{m_1}{2^{k_1}}\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & \frac{m_2}{2^{k_2}}\\ 0 & 1\end{pmatrix},\cdots,\begin{pmatrix}1 & \frac{m_n}{2^{k_n}}\\ 0 & 1\end{pmatrix}\right\}$, 其中 $m_i\in\mathbb{Z},k_i\in\mathbb{Z}_{\geqslant 0}$, 使得 $H=\langle S\rangle$. 而 $\langle S\rangle\simeq\langle\frac{m_1}{2^{k_1}},\frac{m_2}{2^{k_2}},\cdots\frac{m_n}{2^{k_n}}\rangle_{(\mathbb{Q},+)}$, 因为

$$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & a+b\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix},\quad a,b\in\mathbb{Q}.$$

设 $N=\max_{1\leqslant i\leqslant n}\{k_i\}+1$ 的分母的最大公倍数, 则对 H 中的任意元素形如 $\begin{pmatrix}1 & 2^{-l}\\ 0 & 1\end{pmatrix}, l>N$, $2^{-l}\notin\langle\frac{m_1}{2^{k_1}},\frac{m_2}{2^{k_2}},\cdots\frac{m_n}{2^{k_n}}\rangle_{(\mathbb{Q},+)}$, 故 $\begin{pmatrix}1 & 2^{-l}\\ 0 & 1\end{pmatrix}\notin\langle S\rangle$, 矛盾. 因此, H 不是有限生成的.

综上, 有限生成的群的子群不一定是有限生成的. □

提示：可以使用第一次作业

C5）（有限生成群之子群未必有限生成）考虑 $\mathbf{GL}(2;\mathbb{Q})$ 的子群 G ，它由两个元素生成：$G=\left\langle\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle$ 。令

$$H=\{A\in G\mid A\text{ 的对角线上的元素均为1}\}.$$

证明，H 是 G 的子群并且 H 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，

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

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

证明：若 $\min_{\text{gen}}(G)=0$, 结论平凡。若 $\min_{\text{gen}}(G)=1$, 那么由 A1) 立即得到 G 为循环群, 从而其子群 H 平凡或为循环群, 则 $\min_{\text{gen}}(H)=0$ 或 1, 结论成立.

现进行归纳, 假设对于所有 $\min_{\text{gen}}(G)<n$ 的情况结论成立, 现讨论 $\min_{\text{gen}}(G)=n$ 的情况. 设 G 的一组生成元为为 $\{g_1,g_2,\cdots g_n\}$. 不妨取 $g=g_n$, 那么 $G/\langle g\rangle$ 的一组生成元为 $\{g_1\langle g\rangle,g_2\langle g\rangle,\cdots,g_{n-1}\langle g\rangle\}$, 可知 $\min_{\text{gen}}(G/\langle g\rangle)\leqslant n-1$.

由第二同构定理, 有 $H/(\langle g\rangle\cap H)\simeq\langle g\rangle H/\langle g\rangle$. 那么可由归纳假设知

$$\min_{\text{gen}}(H/(\langle g\rangle\cap H))=\min_{\text{gen}}\langle g\rangle H/\langle g\rangle\leqslant\min_{\text{gen}}(G/\langle g\rangle)\leqslant n-1.$$

而再考虑 $\langle g\rangle\cap H$. 若 $\langle g\rangle\cap H$ 非平凡, 则由于循环群的非平凡子群都为循环群, $\langle g\rangle\cap H$ 为循环群, 从而 $\min_{\text{gen}}(\langle g\rangle\cap H)=1$, 再由 A5)

$$\min_{\text{gen}}(H)\leqslant\min_{\text{gen}}(H/(\langle g\rangle\cap H))+\min_{\text{gen}}(\langle g\rangle\cap H)\leqslant(n-1)+1=n.$$

从而

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

以上过程可用如下正合列的交换图表示.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle g\rangle & \hookrightarrow & G & \xrightarrow{\pi} & G/\langle g\rangle & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \langle g\rangle \cap H & \hookrightarrow & H & \xrightarrow{\pi} & H/(\langle g\rangle \cap H) & \longrightarrow & 1 \end{array}$$

□

A11)

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

证明： 由 A10), $\min_{\text{gen}}(A) = r' \leqslant r$. A 是有限生成的, 又由于 $\mathbb{Z}^r$ 是交换群, 故 A 也是交换群. 由有限生成群的分类定理, $A \simeq \mathbb{Z}^{r'-s} \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$, 其中 $s \geqslant 0, d_i \geqslant 2$. 若 $s \neq 0$, 则 A 中将有有限阶的非单位元, 这与 $\mathbb{Z}^r$ 中仅有单位元为有限阶矛盾. 故 $s = 0$, 即 $A \simeq \mathbb{Z}^{r'}$. □

注： 以下是一个错误的证明, 因为给出的映射是不是良定义的.

由 A10), $\min_{\text{gen}}(A) = r' \leqslant r$.

取 A 的一组生成元 $\{a_1, a_2, \cdots, a_{r'}\}$, 那么 $A = \langle a_1, a_2, \cdots, a_{r'}\rangle$. 考虑群同态 φ:

$$A \to \mathbb{Z}^r, \quad a = \sum_{i=1}^{r'} k_i a_i \mapsto (k_1, k_2, \cdots, k_{r'}),$$

这显然是满同态. 而如果 $\varphi(a) = 0$, 那么 $a = 0 \Rightarrow \text{Ker}\ \varphi = \{0\}$, 从而 φ 是单同态. 所以 φ 为同构, 有 $A \simeq \mathbb{Z}^{r'}$.

因此也可以看出验证良定义的必要性.

B. 阶为 p^3 的群有 5 个, $p \neq 2$

B1)

在同构意义下，写下所有阶为 2^3 的群和阶为 p^2 的群。

证明： 阶为 $2^3 = 8$ 的群: 循环群 $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}/ \times \mathbb{Z}/2Z$, $(\mathbb{Z}/2\mathbb{Z})^3$, 二面体群 $\mathbf{D}_4$, 四元数群 $\mathbf{Q}_8$.

阶为 p^2 的群: $\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

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。

证明： 首先进行一些抽象, 考虑群 G 和其 Sylow p-子群构成的集合 S, 那么由 Sylow 定理, 我们可以有自然的共轭作用

$$G \times S \to S, \quad (g, H) \mapsto gHg^{-1},$$

并且这个作用是传递的. 由轨道计数公式, 可知 $|S| = \frac{|G|}{|\mathrm{Stab}(H)|}$, 其中 $H \in S$. 而由于这是共轭作用, $\mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} = H\} = \mathrm{N}_G(H)$. 从而 $|S| = \frac{|G|}{|\mathrm{N}_G(H)|}$.

而 $|\mathbf{GL}(2,\mathbb{F})| = p(p-1)^2(p+1)$, 记 $\mathcal{J}_1$ 对角线均为 1 的上三角矩阵所构成的子集. 只需要计算 $\mathrm{N}_G(\mathcal{J}_1)$ 即可.

注意到 $\mathcal{J}_1$ 是循环群, 生成元是 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 故若 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{N}_G(\mathcal{J}_1)$, 那么只需要满足

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

即可, 其中 $k \in \{0, 1, \cdots, p-1\}$. 直接计算, 有

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+ck & b+kd \\ c & d \end{pmatrix}.$$

从而 $c = 0, a = kd$. 那么 $\mathrm{N}_G(\mathcal{J}_1) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, d \in \mathbb{F}_p^{\times}, b \in \mathbb{F}_p \right\}$, 阶数为 $p(p-1)^2$, 从而 $\mathbf{GL}(2;\mathbb{F}_p)$ 中 Sylow p-子群的个数为 $p+1$. □

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

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

注：这样的群同态 φ 是显然存在的. 如果认真写完这次作业能够立马构造一个.

证明：由于 φ, φ' 是非平凡的, $|\mathrm{Im}\ \varphi| = |\mathrm{Im}\ \varphi'| = p$, 从而 $\mathrm{Im}\ \varphi, \mathrm{Im}\ \varphi'$ 都是 $\mathbf{GL}(2;\mathbb{F}_p)$ 的 Sylow p-子群. 由 Sylow 定理知, $\exists A \in \mathbf{GL}(2;\mathbb{F}_p)$, s.t. $\mathrm{Im}\ \varphi' = A \cdot \mathrm{Im} \cdot \varphi\ A^{-1}$. 于是 $\forall\ x \in (\mathbb{Z}/p\mathbb{Z})^\times, \exists\ k \in (\mathbb{Z}/p\mathbb{Z})^\times$, s.t.

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

$k \neq 0$ 是由于 $\varphi'(0) = \varphi(0)$. 又由 x 可以生成 $\mathbb{Z}/p\mathbb{Z}$, 对任意 $x \in \mathbb{Z}/p\mathbb{Z}$, 都有

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

□

B4)

在同构的意义下，可能的半直积 $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{Z}/p\mathbb{Z}$ 。

证明：若 ψ 为平凡同态, $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^3$.

若 ψ 为非平凡同态, 有 $\psi^p = 1$.

先考虑 $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$, 可以构造映射 ϕ:

$$\mathbf{GL}(2;\mathbb{F}_p) \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}), A \mapsto (x \mapsto xA),$$

其中 x 为行向量. 因为

$$\phi(\mathbf{I}) = \mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}}$$
$$\phi(AB) = (x \mapsto xAB) = (x \mapsto xA)(xA \mapsto xAB) = \phi(A)\phi(B),$$

所以 ϕ 为群同态. 若 $\phi(A) = \mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}}$, $x = (1,0), (0,1)$, 即可得 $A = \mathbf{I}$, 从而 ϕ 为单射. 而 $\forall\ \varphi \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$, 其由 $\varphi((1,0)), \varphi((0,1))$ 完全决定, 故有 $\phi\left(\begin{pmatrix}\varphi((1,0))\\ \varphi((0,1))\end{pmatrix}\right) = \varphi$, ϕ 是满射. 从而 ϕ 是同构, 有 $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \simeq \mathbf{GL}(2;\mathbb{F}_p)$.

若存在另外一个满足条件的非平凡同构 ψ', 由 B3) 可知, 存在 $A \in \mathbf{GL}(2;\mathbb{F}_p)$ 和 $k = 1, 2, \cdots, p-1$ ，使得对任意的 $x \in \mathbb{Z}/p\mathbb{Z}$, s.t.

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

构造映射 π:

$$(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_{\psi'} \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z},$$
$$(x, y) \mapsto (Ax, ky).$$

首先有

$$\begin{aligned}
\pi(0) &= 0, \\
\pi((x_1, y_1)(x_2, y_2)) &= \pi((x_1 + \psi(y_1)x_2, y_1 + y_2)) \\
&= (A(x_1 + \psi'(y_1)x_2), k(y_1 + y_2)) \\
&= (Ax_1 + A\psi'(y_1)x_2, ky_1 + ky_2) \\
&= (Ax_1 + \psi_k(y_1)Ax_2, ky_1 + ky_2) \\
&= (Ax_1 + \psi(ky_1)Ax_2, ky_1 + ky_2) \\
&= (Ax_1, ky_1)(Ax_2, ky_2) \\
&= \pi((x_1, y_1))\pi((x_2, y_2)),
\end{aligned}$$

于是 π 是群同态. 若 $\pi(x, y) = (Ax, ky) = (0, 0)$, 则 $x = A^{-1} \cdot 0 = 0, y = k^{-1} \cdot 0 = 0$($A$可逆, $k \neq 0$), 于是 π 为单同态 (满射同样容易验证). 两群阶由相等, 于是 π 为双射, 从而 π 是群同构. 在同构的意义下, 当 ψ 非平凡时, $\to (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ 只有一个.

在 $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ 中任取两元素 $(x_1, y_1), (x_2, y_2)$, 有

$$\begin{aligned}
(x_1, y_1)(x_2, y_2) &= (x_1 + \psi(y_1)x_2, y_1 + y_2), \\
(x_2, y_2)(x_1, y_1) &= (x_2 + \psi(y_2)x_1, y_2 + y_1).
\end{aligned}$$

反证法: 如果其为交换群, 则 $x_1 + \psi(y_1)x_2 = x_2 + \psi(y_2)x_1 \Rightarrow (\psi(y_2) - 1)x_1 = (\psi(y_1) - 1)x_2$. 由于 x_1, x_2 是任意的, 于是有 $(\psi(y_2) - 1) = (\psi(y_1) - 1) \Rightarrow \psi(y_2) = \psi(y_1), \forall\ y_1, y_2$, 而这意味着 ψ 是平凡的, 与假设矛盾. 于是其为非交换群.

考虑群 $G = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ 在自身上的共轭作用, G 被划分为共轭类的无交并

$$G = \coprod_{k=1}^{m} \mathrm{Conj}(x_k).$$

又由于轨道计数, 以及共轭类数目为 1 的元素属于群的中心, 于是

$$|G| = \sum_{k=1}^{m} \mathrm{Conj}(x_k) = |\mathrm{Z}(G)| + \sum_{k} \mathrm{Conj}(x_k) = p^3.$$

而 $|\mathrm{Conj}(x_k)| = \frac{|G|}{C_{x_k}(G)}$, 当 $x_k \notin \mathrm{Z}(G)$ 时, 有 $p \mid |\mathrm{Conj}(x_k)|$. 于是 $p \mid |\mathrm{Z}(G)|$. 而由 Z 为 G 的真子群, 可知 $|\mathrm{Z}| \leqslant \frac{1}{2}p^3$, 从而 $|\mathrm{Z}(G)| = p$ 或者 p^2. 若 $\mathrm{Z}(G)$ 是 p^2 阶群, 那么 $|G/\mathrm{Z}(G)| = p$, 这是循环群, 从而导出 G 交换, 矛盾. 若 $\mathrm{Z}(G)$ 是 p 阶群, p 素, 从而是循环群, 从而 $\mathrm{Z}(G) \simeq \mathbb{Z}/p\mathbb{Z}$.

□

注：（交换性的一个有用判据）G 是群。证明，G 是交换群等价于 $G/\mathrm{Z}(G)$ 是循环群。

提示：同样可构造 ϕ':

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \to \mathbf{GL}\left(2; \mathbb{F}_p\right), \varphi \mapsto \begin{pmatrix} \varphi((1,0)) \\ \varphi((0,1)) \end{pmatrix}$$

但群同态的证明稍麻烦.

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，$\langle g \rangle \triangleleft G$。

证明：可知 $[G : \langle H \rangle] = p$, 由 Ore 的定理, 可知 $\langle g \rangle \triangleleft G$. □

注：（Ore 的定理）G 是有限群，p 是 $|G|$ 的最小素因子，$H < G$ 是子群。如果其指标 $[G : H] = p$ ，证明，H 是正规子群。

B6)

证明，在同构的意义下，上一个小问题中的群恰好两个。

证明：若 G 是交换群, 则 $G \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

若 G 是非交换群, 首先证明: $\exists\ a \notin G - \langle g \rangle, \text{s.t. } \mathrm{ord}(a) = p$.

反证法: 假设 $G \backslash \langle g \rangle$ 中没有 p 阶元. p-群中心 $\mathrm{Z}(G)$ 非平凡, 而 G 是非交换群, $\mathrm{Z}(G) \neq G$. 若 $\mathrm{Z}(G) = p^2$, 知 $|G/\mathrm{Z}(G)| = p$, 从而是循环群, 从而由期中复习题 (交换性的一个有用判据) 知 G 是交换群, 矛盾. 故 $\mathrm{Z}(G) = p$. $\mathrm{Z}(G)$ 中都是 p 阶元, 从而 $\mathrm{Z}(G) = \{1, g^p, g^{2p}, \cdots, g^{(p-1)p}\}$.

由 B5), $|G/\langle g \rangle| = p$, 从而是循环群. $\exists h \in G \backslash \langle g \rangle, \text{s.t. } G/\langle g \rangle = \langle h\langle g \rangle \rangle$, 于是 $h^p\langle g \rangle = \langle g \rangle \Rightarrow h^p \in \langle g \rangle$. 又 $\mathrm{ord}(h) = p^2 \Rightarrow h^{p^2} = 1, h^p \neq 1 \Rightarrow (h^p)^p = 1$, 于是 $\exists\ 1 \leqslant r \leqslant p-1, \text{s.t. } h^p = g^{rp}$.

又 $|G/\mathrm{Z}(G)| = p^2$, 从而是交换群. 于是有

$$h\mathrm{Z}(G) \cdot g\mathrm{Z}(G) = g\mathrm{Z}(G) \cdot h\mathrm{Z}(G),$$

可推出 $hgh^{-1}g^{-1} \in \mathrm{Z}(G)$, 从而 $\exists\ s \in \mathbb{Z}, \text{s.t. } hgh^{-1} = g^{1+sp}$, 从而 $\forall\ l \in \mathbb{Z}, hg^lh^{-1} = g^{l(1+sp)}$.

考虑 hg^{-r}, 由于 $hg^{-r} \notin \langle g \rangle$, 于是 $\mathrm{ord}(hg^{-r}) = p^2$. 又有

$$\begin{aligned}(hg^{-r})^p &= (hg^{-r}h^{-1})(h^2g^{-r}h^{-2}) \cdots (h^pg^{-r}h^{-p})h^p \\ &= g^{-r(1+sp)}g^{-r(1+sp)^2} \cdots g^{-r(1+sp)^p}g^{rp} \\ &= g^{r[p-\sum_{i=1}^{p}(1+sp)^i]}.\end{aligned}$$

而

$$p - \sum_{i=1}^{p}(1+sp)^i \equiv p - \sum_{i=1}^{p}(1+isp) = -\sum_{i=1}^{p} isp = -\frac{s(p-1)}{2}p^2 \equiv 0 \pmod{p^2}.$$

于是

$$(hg^{-r})^p = g^{r[p-\sum_{i=1}^{p}(1+sp)^i]} = 1,$$

而这意味着 $\mathrm{ord}(hg^{-r}) = p$, 矛盾! 于是 $\exists\ a \notin G - \langle g \rangle, \text{s.t. } \mathrm{ord}(a) = p$.

再考虑 $\langle g\rangle, \langle a\rangle$, 其中 $\langle g\rangle \triangleleft G$, 并且对于 $a^k \in \langle a\rangle$, 如果 $a^k \in \langle g\rangle$, 由 Bezout 定理, 知 $\exists\ l \in \mathbb{Z}, \text{s.t. } a^{kl} = a^1 = a \in \langle g\rangle$, 而这与 a 的取法矛盾. 于是 $\langle g\rangle \cap \langle a\rangle = \{1\}$, 又显然 $\langle g\rangle\langle a\rangle = G$, 于是

$$G \simeq \langle g\rangle \rtimes \langle a\rangle.$$

由半直积的唯一性, 这等价于说

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}.$$

其中 $\psi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ 为群同态. 而 ψ 可以由 $\psi(1)$ 完全决定. 而 $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times$, 其阶为 $p(p-1)$, 其中 p 素, 从而 $\psi(1)$ 的像要么是平凡的, 要么是 p 阶子群的生成元.

方法一: 直接考虑 $G \simeq \langle g\rangle \rtimes \langle a\rangle$. (群作用为共轭作用)

从而可以考虑 $aga^{-1} = g^k$ ，其中 $k \neq 1$ ，不然 G 是交换群。于是我们有

$$G =< a, g > \left(\mathrm{ord}(a) = p, \mathrm{ord}(g) = p^2, aga^{-1} = g^k\right)$$

而 $a^b g a^{-b} = g^{k^b}$ ，令 $b = p$ ，从而有 $g = g^{k^p}$ ，于是 $k^p = 1 \,(\mathrm{mod} p^2)$ ，结合 $k \neq 1$ ，得到 k 可生成乘法群 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 中的 p 阶子群。

我们考虑 G 的其它可能结构

$$G' =< a, g > \left(\mathrm{ord}(a) = p, \mathrm{ord}(g) = p^2, aga^{-1} = g^{k'}\right)$$

同样的有 k' 是乘法群 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 中的 p 阶子群的一个生成元，于是存在 $h, t \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ 使得 $k'^h = k, k^t = k'$ ，于得到是 $aga^{-1} = g^{k'}$ 和 $a^h g a^{-h} = g^k$ 等价。不难验证 a^h, a 都是 $\langle a\rangle$ 的一个生成元，于是有

$$G' =< a^h, g > \left(\mathrm{ord}(a) = p, \mathrm{ord}(g) = p^2, a^h g a^{-h} = g^k\right)$$

再用 $b = a^h$ 代入上式，即

$$G' =< b, g > \left(\mathrm{ord}(b) = p, \mathrm{ord}(g) = p^2, bgb^{-1} = g^k\right)$$

此时可直接验证 $G' \simeq G$ ，于是 G 不交换时只有一种群结构。

方法二: 也可考虑 $G \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$. 由上面的分析, $\psi(1)$ 的像要么是平凡的, 要么是 p 阶子群的生成元. 而 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 中 p 阶子群唯一, 于是非平凡时 ψ 在同构意义下唯一. 从而在同构意义下, 非交换群结构唯一. □

注：（交换性的一个有用判据）G 是群。证明，G 是交换群等价于 $G/\mathrm{Z}(G)$ 是循环群。

阶为 p^2 的群为交换群, 这容易验证.

B7)

在同构意义下，写下所有阶为 p^3 的群。

证明：最后只需要补充证明: 当 G 中非循环群且不存在 p^2 阶元时, $G \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$.

此时, G 中非单位元都是 p 阶元. 由 p-群中心非平凡, 可知 $\mathrm{Z}(G)$ 非平凡. 故可取 $a \in \mathrm{Z}(G)\backslash\{0\}$, 再取 $b \in G\backslash\langle a\rangle$, 则 $\langle a\rangle \cap \langle b\rangle = \{0\}$, 否则 $\exists\, k \in \mathbb{Z}$, s.t. $b^k \in \langle a\rangle$, 由 Bezout 定理, 可知 $\exists\, l \in \mathbb{Z}$, s.t. $b^{kl} = b \in \langle a\rangle$, 矛盾. 于是 $\langle a, b\rangle = \{a^i b^j \mid 0 \leqslant i, j < p\} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

再取 $c \in G\backslash\langle a, b\rangle$, 则 $\langle a\rangle \cap \langle c\rangle = \{0\}, \langle b\rangle \cap \langle c\rangle = \{0\}$, 同理可证. 于是 $G = \langle a, b, c\rangle$, 并且 $\langle a\rangle\langle b\rangle \cap \langle c\rangle = \{0\}$, 从而

$$G \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}.$$

由整个 B 题, 可知在同构意义下, 阶为 p^3 的群有 5 个:

$$\mathbb{Z}/p^3\mathbb{Z}, \mathbb{Z}/p^2 \times \mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^3, (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p^2\mathbb{Z}) \rtimes_\psi \mathbb{Z}/p\mathbb{Z},$$

其中 ψ 的作用非平凡. □