第三次习题课

王沛林

Question 1. 设 G 为一个群，$Z(G), \mathrm{Inn}(G), \mathrm{Aut}(G)$ 的关系。（周三题 3 与周五题 11）

Proof. 设 σ 为如下定义的群同态

$$\begin{aligned} \sigma : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto \sigma_g : x \longmapsto gxg^{-1} \end{aligned}$$

(1)$\ker\sigma = Z(G)$，$G/Z(G) \cong \mathrm{Inn}(G)$
由定义可知 $\mathrm{im}\,\sigma = \mathrm{Inn}(G)$，考察 $\ker\sigma$

$$\begin{aligned} g \in \ker\sigma &\iff \sigma_g = id \\ &\iff gxg^{-1} = x,\ \forall x \in G \\ &\iff gx = xg,\ \forall x \in G \\ &\iff g \in Z(G) \end{aligned}$$

即 $\ker\sigma = Z(G)$，由第一同态基本定理即有 $G/Z(G) \cong \mathrm{Inn}(G)$。
(2) 若 $G/Z(G)$ 为循环群，则 G 为阿贝尔群。
不妨设 $G/Z(G) = \left\{Z(G), aZ(G), \cdots, a^{n-1}Z(G)\right\}$
则 $\forall g_1, g_2 \in G$，有 $g_1 = a^i x, g_2 = a^j y$，其中 $x, y \in Z(G)$，
有 $g_1g_2 = a^i x a^j y = a^{i+j}xy = g_2g_1$，于是 G 为阿贝尔群。
(3) 若 G 非阿贝尔群，则 $\mathrm{Aut}(G)$ 非循环群。
设则 $\mathrm{Aut}(G)$ 为循环群，由于 $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$，从而 $\mathrm{Inn}(G)$ 为循环群。
由 (1)，我们有 $G/Z(G) \cong \mathrm{Inn}(G)$，从而 $G/Z(G)$ 为循环群，由 (2)，G 为循环群，矛盾。 □

Lemma 0.1. $\forall A \in T_n(\mathbb{R})$(可逆上三角矩阵群)，$A$ 为正交矩阵当且仅当 A 为对角阵，且对角元为 ± 1。

Proof. 利用 $AA^t = I$ 即可证明。 □

Question 2. 求 $GL_n(\mathbb{R})$ 关于 $O_n(\mathbb{R})$ 的右陪集代表元。

Date: 2023 年 4 月 8 日.

Proof. 对 $\forall A \in GL_n(\mathbb{R})$，由 Gram-Schmidt 正交化，有 $A = BU$，其中 $B \in O_n(\mathbb{R}), U \in GL_n(\mathbb{R})$。右陪集代表元类应在 $T_n(\mathbb{R})$ 中找。
下证：$\forall M_1, M_2 \in T_n(\mathbb{R})$，且 $M_1 \neq M_2$，则 $M_1 M_2^{-1} \notin O_n(\mathbb{R})$ 当且仅当 M_1, M_2 主对角元大于 0。
($\Longleftarrow$) 若 $M_1 M_2^{-1} \in O_n(\mathbb{R})$。由于 M_1, M_2 主对角元大于 0，由引理只能有 $M_1 M_2^{-1} = I$，即 $M_1 = M_2$，矛盾。
($\Longrightarrow$) 若允许 M_1, M_2 对角线小于 0，取 $M_1 = 2I, M_2 = -2I$，此时 $M_1 M_2^{-1} = -I$，矛盾。
综上，$GL_n(\mathbb{R})$ 关于 $O_n(\mathbb{R})$ 的右陪集代表元为全体主对角元大于 0 的可逆上三角矩阵。 □

Question 3. 求 $GL_n(\mathbb{Z}/p^m\mathbb{Z})$ 的阶。

Proof. (1)$m = 1$ 情形。
Way 1:
考虑矩阵的列向量选择。矩阵第一列有 $p^n - 1$ 种取法，因矩阵可逆第二列不是第一列的倍数，有 $p^n - p$ 种取法，同理，第三列不为前两列的线性组合，有 $p^n - p^2$ 种取法，以此类推即可得到群的阶为 $\prod_{i=0}^{n-1}(p^n - p^i)$。
Way 2:
$(\mathbb{Z}/p\mathbb{Z})^n$ 构成线性空间，一般线性群是线性空间上的自同构群，有

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^n \cong GL_n(\mathbb{Z}/p\mathbb{Z})$$

即计算 $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^n$ 的阶即可。自同构由生成元确定，考虑自同构需要考虑 $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^n$ 的生成元。除单位元外所有元的阶为 p，第一个生成元可取除单位外的所有元，有 $p^n - 1$ 种取法，第二个要在不含第一个元生成类的元素中取，共 $p^n - p$ 种取法，依次类推，第 m 个生成元有 $p^n - p^m$ 种取法。自同构把一组生成元映到一组生成元，有

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = |\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^n| = \prod_{i=0}^{n-1}(p^n - p^i)$$

(2)$m > 1$ 情形。
考虑群同态

$$\begin{aligned} P : \mathbb{Z}/p^{m+1}\mathbb{Z} &\longrightarrow \mathbb{Z}/p^m\mathbb{Z} \\ a \mod p^{m+1} &\longmapsto a \mod p^m \end{aligned}$$

这个同态诱导一般线性群上的同态 $P^* : GL_n(\mathbb{Z}/p^{m+1}\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/p^m\mathbb{Z})$，根据第一同态基本定理，有 $|GL_n(\mathbb{Z}/p^{m+1}\mathbb{Z})| = |GL_n(\mathbb{Z}/p^m\mathbb{Z})| \cdot |\ker P^*|$。
考虑 $\ker P^*$，

$$A = (a_{ij}) \in \ker P^* \iff a_{ij} \equiv \delta_{ij} \mod p^m$$

从而每个 a_{ij} 有 p 种选择，有 $|\ker P^*| = p^{n^2}$。从而有 $|GL_n(\mathbb{Z}/p^m\mathbb{Z})| = p^{(m-1)n^2}\prod_{i=0}^{n-1}(p^n - p^i)$ □

Remark 0.2. 对于一般的有限阿贝尔群 $\mathbb{Z}/N\mathbb{Z}$，后面会学到有限阿贝尔群的结构定理，将之分解即可计算 $GL_n(\mathbb{Z}/N\mathbb{Z})$ 的阶。