《近世代数》第二次习题课 (初稿)

刘助教 2023.4.1

问题 1: $Aut(\mathbb{Z}/m\mathbb{Z})$ 的结构.

由欧阳毅等著《代数学基础》中的**定理 7.7** 知 $Aut(\mathbb{Z}/m\mathbb{Z})=(\mathbb{Z}/m\mathbb{Z})^{\times}$ 为循环群当且仅当 $m=2,4,p^a$ 或 $2p^a$, 其中 p 为奇素数且 $a\geq 1$ 以及**命题 7.5** 知 $Aut(\mathbb{Z}/2^a\mathbb{Z})=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{a-2}\mathbb{Z}, a\geq 3$. 从而若 $m=2^a p_1^{a_1}\cdots p_n^{a_n}$ 为 m 的素因子分解, 则由**定理 4.18 (4)** 知 $Aut(\mathbb{Z}/m\mathbb{Z})=Aut(\mathbb{Z}/2^a\mathbb{Z})\times Aut(\mathbb{Z}/p_1^{a_1}\mathbb{Z})\times\cdots\times Aut(\mathbb{Z}/p_n^{a_n}\mathbb{Z})$, 从而确定了 $Aut(\mathbb{Z}/m\mathbb{Z})$ 的结构.

问题 2:$SL_n(\mathbb{Z})$ 有限生成.

Way1: 思路同 $n=2$ 情形, 证明 $\{B_{ij}=I+E_{ij}|i\neq j\}$ 为其一组生成元.($SL_2(\mathbb{Z})$ 中 $S=B_{21}B_{12}^{-1}B_{21}, T=B_{12}$)

Way2: 我们先由$Lemma1$证明 $GL_n(\mathbb{Z})$ 有限生成, 再由$Lemma2$证明 $SL_n(\mathbb{Z})$ 有限生成.

$*(Lemma1)$: 任意矩阵 $A\in M_{n\times m}(\mathbb{Z})$ 总可以经过初等行列变换化为

$$\begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ & & & & O \end{pmatrix}$$

的形式, 其中 $d_1\,|d_2\,|\cdots|d_r$.

证明:to be continued.

$*(Lemma2)$: 有限生成群 G 的指数有限子群 H 是有限生成的.

证明 1: 初等证明 to be continued.

证明 2: 假设 G 由 $\{g_1,\cdots,g_n\}$ 生成, 令 F 是秩为 n 自由群且有满射群同态 $f:F\longrightarrow G$, 此时 $[F:f^{-1}(H)]=[G:H]=j$, 从而由$Lemma3$以及$Lemma4$知 $f^{-1}(H)$ 为秩是 $jn-j+1$ 的自由群. 故 $H\cong f^{-1}(H)/Ker(f)$ 为有限生成群.

$*(Lemma3)(Nielsen-Schreider)$: 自由群的子群是自由群.

$*(Lemma4)$: 若 F 是秩为 n 的自由群,H 是指数为 j 的子群, 则其秩为 $jn-j+1$.

以上两个定理的证明需要用到基本群与欧拉数, 参见 Rotman《An Introduction to the Theory of Groups》$Theorem 11.44, Theorem 11.45$.

证明: 初等变换矩阵 $\{P_{ij}=I_n-E_{ii}-E_{jj}+E_{ij}+E_{ji}|n\geq i,j\geq 1\},\{D_i(-1)=I_n-2E_{ii}|n\geq i\geq 1\}$ 以及 $\{T_{ij}(k)=I_n+kE_{ij}|n\geq i,j\geq 1,k\in\mathbb{Z}\}$ 都属于 $GL_n(\mathbb{Z})$

且由 $\{P_{ij}, D_i(-1), T_{ij}(1), T_{ij}(-1)|n \geq i, j \geq 1\}$ 生成.
对任意 $A \in GL_n(\mathbb{Z})$ 由$Lemma1$知 $A = CDE$ 其中 $C, E \in GL_n(\mathbb{Z})$,$D$ 为对角阵. 此时 $|A| = |C||D||E|$, 故 $D \in GL_n(\mathbb{Z})$ 且由 $\{D_i(-1) = I_n - 2E_{ii}|n \geq i \geq 1\}$ 生成. 综上,$GL_n(\mathbb{Z})$ 有限生成.
易知映射 $det : GL_n(\mathbb{Z}) \longrightarrow \{-1, 1\}$ 为乘法群同态且 $Ker(det) = SL_n(\mathbb{Z})$, 故 $GL_n(\mathbb{Z})/SL_n(\mathbb{Z}) \cong \{-1, 1\}$, 从而 $[GL_n(\mathbb{Z}) : SL_n(\mathbb{Z})] = 2$. 应用$Lemma2$便知 $SL_n(\mathbb{Z})$ 有限生成.

问题 3:$GL_n(\mathbb{Z})$ 只有有限多个有限子群.($SL_n(\mathbb{Z})$ 同理)
固定奇素数 p, 由于商映射 $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ 诱导的映射 $f : GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$ 为乘法群同态且 $Ker(f) = \{A \in GL_n(\mathbb{Z})|\exists B \in M_{n\times n}(\mathbb{Z}), A = I + p \cdot B\}$. 此时 $GL_n(\mathbb{Z})$ 的任意有限子群 G 都同构于 $f(G)/(Ker(f) \cap G)$, 而由$Lemma5$知若 $A \in Ker(f)$ 且 A 的阶有限, 则 $B = 0$ 即 $Ker(f) \cap G = I$, 故 $G \cong f(G)$. 再应用$Lemma6$便证.
$*(Lemma5)$: 设 p 为奇素数,X 是 n 阶整系数方阵. 如果 $I + pX \in GL_n(\mathbb{Z})$ 的阶有限, 则 X=0.
证明: 假设命题不成立, 令 m 为最小的正整数使得 $\exists X \neq 0$,$I + pX$ 的阶为 m. 若 m 不为素数, 不妨令 $m = ab$ $(a, b > 1)$. 此时 $(I + pX)^a = I + \sum_{j=1}^{a} \binom{a}{j} p^j X^j = I + pX_1$, 其中 $X_1 = \sum_{j=1}^{a} \binom{a}{j} p^{j-1} X^j$. 从而由 $(I + pX_1)^b = (I + pX)^m = I$ 以及 m 的极小性知 $X_1 = 0$, 即 $(I + pX)^a = I$ 依旧与 m 的极小性矛盾, 因此 m 为素数.
若 $I + pX = I + p^r Y$, 其中 Y 的矩阵元不全是 p 的倍数. 将 $(I + p^r Y)^m = I$ 二项式展开得到 $mp^r Y + \sum_{k=2}^{m} \binom{m}{k} p^{rk} Y^k = 0$. 由于 $p > 2, k > 1$, 和式符号内的所有数都能被比 mp^r 更大的 p 的幂整除, 产生矛盾.
$*(Lemma6)$:F_q 为 $q = p^r$(p 为素数,$r \geq 1$) 阶有限域, 则 $|GL_n(F_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.
证明: 若 $A \in GL_n(F_q)$, 令 a_i 为 A 的第 i 个列向量, 我们只需要计算有多少组有序排列的线性无关列向量 $a_1, \cdots, a_n$.
$a_1 \neq 0$ 有 $q^n - 1$ 种选择方式;a_2 不在 a_1 生成的 1 维 F_q 向量空间 $< a_1 >$ 中, 有 $q^n - q$ 种选择方式; 同理对 $n \geq i \geq 2$,a_i 不在 $a_1, a_2, \cdots, a_{i-1}$ 生成的 $i - 1$ 维 F_q 向量空间 $< a_1, a_2, \cdots, a_{i-1} >$ 中, 共有 $q^n - q^{i-1}$ 种选取方式. 综上 $|GL_n(F_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

问题 4:$SL_2(\mathbb{Z})$ 的有限子群为循环群且阶整除 4 或 6.
证明:
Step1:$SL_2(\mathbb{Z})$ 的有限阶元素的阶只能为 $1, 2, 3, 4, 6$.
对任意 $A \in SL_2(\mathbb{Z})$, 其特征多项式为 $x^2 - tr(A)x + 1$. 若 A 的阶为 n, 即 $x^n - 1$ 为其零化多项式, 此时 A 的特征值为单位根, 从而 $|tr(A)| \leq 2$ 且 $gcd(x^2 - tr(A)x + 1, x^n - 1)$ 也是 A 的零化多项式, 我们对 $tr(A)$ 分情况讨论:
$(1) : tr(A) = 2$, 此时 $gcd(x^2 - 2x + 1, x^n - 1) = x - 1$,$A$ 只能为 1 阶元 I.
$(2) : tr(A) = -2$, 此时 $gcd(x^2+2x+1, x^n-1) = x+1$ $(n\ even)$, $gcd(x^2-tr(A)x+1, x^n-1) =$

1 (n odd). 由于 $gcd(x^2+2x+1, x^n-1)$ 是 A 的零化多项式,n 只能为偶数且 $A+I=0$, 从而 A 为 2 阶元 $-I$.
(3) : $tr(A)=1$, 由于 x^2-x+1 是 $x^3+1=(x+1)(x^2-x+1)$ 的因子, 因此 $A^3=-I$ 即 $A^6=I$. 若 $A^2=I$ 则与 $A^2-A+I=0$ 矛盾, 从而 A 是 6 阶元.
(4) : $tr(A)=-1$, 此时 x^2+x+1 是 $x^3-1=(x-1)(x^2+x+1)$ 的因子, 同 (3) 中讨论知 A 为 3 阶元.
(5) : $tr(A)=0$, 此时 $A^2=-I$ 为 4 阶元.
Step2: 由拉格朗日定理知 $SL_2(\mathbb{Z})$ 的有限子群只包含有限阶元素, 因此考虑 $1,2,3,4,6$ 阶元素中的某一些所生成的子群即可.
需要一些 $SL_2(\mathbb{Z})$ 有限阶元素共轭类的知识,to be continued.

问题 5: 对任意整数 $m,n,r>1$, 存在有限群 G 以及其中的元素 a,b 满足 $ord(a)=m, ord(b)=n, ord(ab)=r$.
证明: 令 p 为不整除 $2mnr$ 的素数, 则 p 在 $\mathbb{Z}/2mnr\mathbb{Z}$ 中可逆, 记 $q=p^r(r=ord(p))$. 此时有 $2mnr|(q-1)$, 从而由 $F_q^\times$ 为 $q-1$ 阶循环群知其有元素 u,v,w 满足 $ord(u)=2m, ord(v)=2n, ord(w)=2r$.
取 $SL_2(F_q)$ 中元素

$$a=\begin{pmatrix} u & 1 \\ 0 & u^{-1} \end{pmatrix}, b=\begin{pmatrix} v & 0 \\ t & v^{-1} \end{pmatrix}$$

其中 $t=(w+w^{-1})-uv-u^{-1}v^{-1}$.
由于 a,b,ab 的特征多项式分别为 $(x-u)(x-u^{-1}),(x-v)(x-v^{-1}),(x-w)(x-w^{-1})$, 从而分别相似到对角阵 $diag(u,u^{-1}), diag(v,v^{-1}), diag(w,w^{-1})$ (由于 $u,v,w\neq 0,-1,1$. 考虑共轭类即可). 故 a,b,ab 在 $SL_2(F_q)/\{-I,+I\}$ 中的像的阶分别为 m,n,r.