预备知识: 为防止有人不熟悉线性代数, 这里简要介绍一些基本的概念和事实, 各位同学们可以不加证明地直接使用这些结果.

对于域 K, 我们称 K 上的一个 n 阶矩阵 ($n \times n$ 矩阵) 是一个 n 行 n 列的数表, 这个数表的每一项都是 K 中的元素. 比如下面的:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

就是一个 2 阶矩阵. 对于矩阵 A, 我们通常将其表示为 $A = (a_{ij})_{1 \le i,j \le n}$, 其中 a_{ij} 是 A 中位于第 i 行第 j 列的元素. 在不会引起歧义时候, 我们有时也会省略括号外的下标, 直接记为 $A = (a_{ij})$.

我们记 $\mathrm{M}_n(K)$ 是 K 上所有 n 阶矩阵的集合. 我们在其上定义如下几种运算:

(加法) 对 $A, B \in \mathrm{M}_n(K)$, $A = (a_{ij}), B = (b_{ij})$, 我们定义 $A + B = (a_{ij} + b_{ij})$.

(乘法) 对于 $A, B \in \mathrm{M}_n(K)$, $A = (a_{ij}), B = (b_{ij})$, 我们定义 $AB = (\sum_{k=1}^{n} a_{ik} b_{kj})$.

(数乘) 对于 $A \in \mathrm{M}_n(K)$, $A = (a_{ij})$, 以及 $k \in K$, 我们定义 $kA = (k a_{ij})$.

特别地, 我们称所有元素均为 0 的矩阵为零矩阵, 并同样记作 0; 我们称只有对角线上的元素为 1, 而其它元素为 0 的矩阵为单位矩阵, 记作 I_n. 譬如说:

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

关于矩阵, 一个重要的构造是函数 $\det : \mathrm{M}_n(K) \to K$. 对 $A \in \mathrm{M}_n(K)$, 我们称 $\det(A)$ 为 A 的行列式, 它满足形式 $\det(AB) = \det(A)\det(B)$. 如果你不知道行列式的具体构造, 你可以暂时不用关心它是如何构造出来的. 你只需要知道, 对 $A \in \mathrm{M}_n(K)$, 以下几个条件是相互等价的即可:

(1) $\det(A) \neq 0$.

(2) 存在 $B \in \mathrm{M}_n(K)$, 使得 $BA = AB = I_n$.

若 A 满足以上的等价条件, 则我们称 A 是一个可逆矩阵. 此时, 使得 $BA = AB = I_n$ 的矩阵 B 是唯一的, 我们称其为 A 的逆矩阵, 记作 A^{-1}.

问题 (1): 在本系列问题中, 我们将介绍若干群的例子. 我们会给出这些群的构造, 然后由你来验证其确实构成一个群.

问题 (1.1): 对域 K, 以及 $n \in \mathbb{Z}_{\geq 1}$,请证明:$\mathrm{M}_n(K)$ 关于矩阵的加法构成一个交换群.

证明. 由 K 的加法结合律, 则 $(A+B)+C = ((a_{ij}+b_{ij})+c_{ij}) = (a_{ij}+(b_{ij}+c_{ij})) = A+(B+C)$. 由 K 的加法交换律, 则 $A+B = (a_{ij}+b_{ij}) = (b_{ij}+a_{ij}) = B+A$. 显然, $A+0 = 0+A = A$ 对所有 $A \in \mathrm{M}_n(K)$ 成立, 故 0 矩阵是矩阵加法的单位元. 注意到 $A+(-1)A = (a_{ij}+(-1)a_{ij}) = 0 = (-1)A+A$, 故 $(-1)A$ 是 A 关于矩阵加法的逆元. 综上所述, 则 $\mathrm{M}_n(K)$ 关于矩阵加法构成一个交换群. □

问题 (1.2): 我们定义:

$$\mathrm{GL}_n(K) = \left\{A \in \mathrm{M}_n(K) : A\text{是可逆矩阵}\right\},$$

请证明:$\mathrm{GL}_n(K)$ 对于矩阵的乘法构成一个群, 且当 $|K| > 2$, 则 $\mathrm{GL}_n(K)$ 是交换群当且仅当 $n = 1$.

证明. 由 $\det(AB) = \det(A)\det(B)$, 故 $A, B \in \mathrm{GL}_n(K)$ 时 $AB \in \mathrm{GL}_n(K)$, 进而 $\mathrm{GL}_n(K)$ 对矩阵乘法封闭. 注意到 $(AB)C = (\sum\limits_{k=1}^{n}\sum\limits_{l=1}^{n} a_{ik}b_{kl}c_{lj}) = A(BC)$, 故矩阵的乘法是结合的. 考虑 $I_n = (\delta_{ij})$, 其中:

$$\delta_{ij} = \begin{cases} 1 & \text{当} i = j. \\ 0 & \text{当} i \neq j. \end{cases}$$

注意到对 $A = (a_{ij})$, 有 $\sum\limits_{k=1}^{n} a_{ik}\delta_{kj} = a_{ij} = \sum\limits_{k=1}^{n} \delta_{ik}a_{kj}$, 故 $AI_n = I_nA = A$, 进而 I_n 是 $\mathrm{GL}_n(K)$ 的单位元. 此时, 则 A^{-1} 是 A 关于矩阵乘法的逆元.

当 $n = 1$, 对 $(a) \in \mathrm{M}_n(K)$, 当 $a \neq 0$, 则 $(a^{-1})(a) = (a)(a^{-1}) = (1)$ 可逆. 当 $a = 0$, 显然 (0) 不可逆. 因此, $\mathrm{GL}_1(K) = \{(a) : a \in K^\times\}$, 进而 $\mathrm{GL}_1(K)$ 同构于 $K^\times$, 故 $\mathrm{GL}_1(K)$ 是交换群. 而当 $n \geq 2$, 不失一般性, 我们只证明 $\mathrm{GL}_2(K)$ 不是交换的. 注意到:

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & an \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & n \\ 0 & 1 \end{pmatrix}$$

因此, 只需存在 $a \in K^\times$, 使得 $a \neq 1$, 则 $\mathrm{GL}_2(K)$ 不是交换群. □

问题 (1.3): 对于 $A \in \mathrm{M}_n(K)$, $A = (a_{ij})$, 若 $i > j$ 时恒有 $a_{ij} = 0$, 则我们称 A 是一个上三角矩阵. 我们定义:

$$\mathrm{B}_n(K) = \left\{A \in \mathrm{GL}_n(K) : A\text{是上三角矩阵}\right\},$$

请证明:$\mathrm{B}_n(K)$ 是 $\mathrm{GL}_n(K)$ 的子群.

证明. 不难验证, 若 $A, B \in \mathrm{B}_n(K)$, 则 $AB \in \mathrm{B}_n(K)$. 我们只证明: 若 $A \in \mathrm{B}_n(K)$, 则 $A^{-11} \in \mathrm{B}_n(K)$. 我们记 $A = (a_{ij}), A^{-1} = (b_{ij})$, 则由 $A^{-1}A = I_n$, 我们知道:

$$\begin{aligned}\delta_{ij} &= \sum_{k=1}^{n} b_{ik}a_{kj} \\ &= \sum_{k=1}^{j} b_{ik}a_{kj}\end{aligned}$$

当 $i = 1, j = 1$, 我们有:

$$b_{11}a_{11} = 1,$$

进而 $a_{11} \neq 0$, 且 $b_{11} = a_{11}^{-1}$. 下面我们归纳地证明: 对所有 $1 \leq i \leq n$, 都有 $a_{ii} \neq 0, b_{ii} = a_{ii}^{-1}$, 且当 $i > j$ 时, 有 $b_{ij} = 0$. 现设归纳假设对所有 $i < i_0$ 成立. 对 $i = i_0$, 首先考虑 $j = 1$, 则有:

$$b_{i_0 1}a_{11} = 0,$$

因此 $b_{i_0 1} = 0$. 而对 $j < i_0$, 有:

$$\sum_{k=1}^{j-1} b_{i_0 k}a_{kj} + b_{i_0 j}a_{jj} = 0,$$

对 j 进行归纳, 不妨设 b_{ik} 对所有 $1 \leq k \leq j-1$ 成立, 进而 $b_{i_0 j}a_{jj} = 0$, 故 $b_{i_0 j} = 0$. 此时, 对 $j = i_0$, 则:

$$\sum_{k=1}^{i_0-1} b_{i_0 k}a_{ki_0} + b_{i_0 i_0}a_{i_0 i_0} = 1,$$

进而 $b_{i_0 i_0}a_{i_0 i_0} = 1$, 故而归纳成立, 进而得证, □

问题 (1.4): 我们定义

$$\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) : \det(A) = 1\},$$

请证明:$\mathrm{SL}_n(K)$ 是 $\mathrm{GL}_n(K)$ 的子群.

证明. 由 $\det(AB) = \det(A)\det(B)$, 故 $A, B \in \mathrm{SL}_n(K)$ 时 $AB \in \mathrm{SL}_n(K)$. 注意到任取 $A \in \mathrm{GL}_n(K)$, 有 $\det(A) = \det(AI_n) = \det(A)\det(I_n)$, 故 $\det(I_n) = 1$, 进而 $I_n \in \mathrm{SL}_n(K)$. 此时, 由 $\det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(I_n) = 1$, 故 $\det(A^{-1}) = \det(A)^{-1}$, 进而若 $A \in \mathrm{SL}_n(K)$, 则 $A^{-1} \in \mathrm{SL}_n(K)$, 故得证. □

问题 (1.5): 我们定义:

$$\mathrm{U}_n(K) = \left\{A \in \mathrm{B}_n(K) : A\text{主对角线上的元都是}1\right\},$$

请证明:$\mathrm{U}_n(K)$ 是 $\mathrm{B}_n(K)$ 的子群.

证明. 由 (1.3) 的证明可以看出, 若 $A \in \mathrm{U}_n(K)$, 则 $A^{-1} \in \mathrm{U}_n(K)$. 其余的事实是容易验证的. □

问题 (1.6): 特别地,请证明: 存在群同构 $(K,+)\cong \mathrm{U}_2(K)$, 这里 $(K,+)$ 是 K 的加法群.

证明. 注意到:

$$\begin{pmatrix}1 & x\\ & 1\end{pmatrix}\begin{pmatrix}1 & y\\ & 1\end{pmatrix}=\begin{pmatrix}1 & x+y\\ & 1\end{pmatrix},$$

因此 $K\to \mathrm{U}_2(K), x\mapsto \begin{pmatrix}1 & x\\ & 1\end{pmatrix}$ 是保持加法的双射, 进而两者同构. □

问题 (1.7): 特别地,请证明: 对

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{M}_2(K),$$

则 A 可逆当且仅当 $ad-cb\neq 0$, 且此时:

$$A^{-1}=\frac{1}{ad-cb}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$$

提示: 事实上, 当 $n=2$ 时, $\det(A)=ad-cb$. 因此你可以首先证明 $A\mapsto ad-cb$ 满足 $\det(AB)=\det(A)\det(B)$.

证明. 对 $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, 记 $A^*=\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$, 则 $AA^*=A^*A=(ad-cb)I_2$. 故当 $ad-cb\neq 0$, 则 A 可逆. 反之, 我们记 $\det:\mathrm{M}_2(K)\to K$ 是映射 $A\mapsto ad-cb$, 注意到对 $B=\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$, 有:

$$AB=\begin{pmatrix}aa'+bc' & ab'+bd'\\ ca'+dc' & cb'+dd'\end{pmatrix},$$

因此有:

$$\begin{aligned}\det(AB)&=(aa'+bc')(cb'+dd')-(ca'+dc')(ab'+bd')\\ &=(aca'b'+ada'd'+bcb'c'+bdc'd')-(aca'b'+cda'd'+adb'c'+bdc'd')\\ &=ada'd'+bcb'c'-cda'd'-adb'c'\\ &=(ad-cb)(a'd'-c'b')\\ &=\det(A)\det(B)\end{aligned}$$

因此若 $AB=I_2$, 则 $\det(A)\det(B)=\det(I_2)=1$, 进而 $\det(A)=ad-cb\neq 0$. □

问题 (2): 本系列问题中, 我们将证明关于陪集的一些基本事实.

问题 (2.1): 对群 G, 若 H, K 是 G 的子群, 满足 $H \subset K$.请证明 下列条件等价:

(1) $[G : H] < \infty$.

(2) $[G : K], [K : H] < \infty$.

进一步地,请证明: 当上述等价条件成立, 则有 $[G : H] = [G : K][K : H]$.

证明. 我们只需证明一个事实. 即若 $\{g_i\}_{i\in I}$ 是 G/K 的一个陪集代表元系,$\{k_j\}_{j\in J}$ 是 K/H 的一个陪集代表元系, 则 $\{g_ik_j\}_{(i,j)\in I\times J}$ 是 G/H 的一个陪集代表元系. 若上述事实成立, 则 $[G : H] = |I \times J| = |I||J| = [G : K][K : H]$.

我们首先证明 g_ik_jH 是两两不同的陪集. 若 $g_ik_jH = g_{i'}k_{j'}H$, 则 $k_{j'}^{-1}g_{i'}^{-1}g_ik_j \in H$, 进而 $g_{i'}^{-1}g_i \in k_{j'}Hk_j^{-1} \subset K$, 故 $i = i'$. 进而 $k_{j'}^{-1}k_j \in H$, 则 $j = j'$. 接下来, 只需证明, 任取 $g \in G$, 存在 g_ik_j, 使得 $g \in g_ik_jH$ 即可. 由 g_i 是 G/K 代表元, 则存在 $i \in I$ 使得 $g_i^{-1}g \in K$, 进而存在 $j \in J$ 使得 $k_j^{-1}g_i^{-1}g \in H$, 故而 $g \in g_ik_jH$, 进而得证. □

问题 (2.2): 对群 G, 若 H, K 是 G 的子群, 且满足:

(1) $[G : H] = n < \infty$.

(2) $[G : K] = m < \infty$.

请证明: 若 $[G : H \cap K] < \infty$, 则 l.c.m(n, m) 整除 $[G : H \cap K]$, 这里 l.c.m(n, m) 是 n, m 的最小公倍数.

证明. 由 (2.1), 则 $[G : H][H : H \cap K] = [G : H \cap K]$, 进而 n 整除 $[G : H \cap K]$. 同理, m 整除 $[G : H \cap K]$. 进而 l.c.m(n, m) 整除 $[G : H \cap K]$. □

问题 (2.3): 在 (2.2) 的条件下,请证明 下面的映射是良定的单射:

$$H/H \cap K \to G/K$$
$$h(H \cap K) \mapsto hK$$

证明. 首先证明良定性. 若 $h(H\cap K) = h'(H\cap K)$, 则 $h'^{-1}h \in H\cap K \subset K$, 故 $hK = h'K$. 因而 $h(H \cap K) \mapsto hK$ 是良定的. 现在我们证明其是单射: 当 $hK = h'K$, 则 $h'^{-1}h \in K$, 进而 $h'^{-1}h \in H \cap K$, 故 $h(H \cap K) = h'(H \cap K)$. □

问题 (2.4): 在 (2.2) 的条件下,请证明 一定有 $[G : H \cap K] \leq mn$. 特别地, 当 mn 互素, 则 $[G : H \cap K] = mn$.

证明. 由 (2.3), 则 $[H : H \cap K] \leq [G : K] = m$, 进而 $[G : H \cap K] = [G : H][H : H \cap K] \leq nm$. □

问题 (3): 本系列问题给出了初等数论中 Wilson's 定理的一个群论证明, 以及由该证明衍生出的一些问题.

问题 (3.1): 对有限交换群 G, 若 $g_1, \ldots, g_n$ 是 G 中的全部元素, 记 $g = \prod_{i=1}^{n} g_i$ (由于 G 交换, 故而这里乘积的顺序是不重要的), 则 $g^2 = e$, 这里 e 是 G 的单位元.请证明:$g^2 = e$.

证明. 注意到 $G \mapsto G, g \mapsto g^{-1}$ 是双射, 因而 $g = \prod_{i=1}^{n} g_i^{-1}$, 故 $g^2 = \prod_{i=1}^{n} (g_i g_i^{-1}) = e$. □

问题 (3.2):: 若方程 $X^2 = e$ 在 G 中的全部解为 $a_1, \ldots, a_m$,请证明: (3.1) 中的 $g = \prod_{i=1}^{m} a_i$.

证明. 记 S 是 G 中不满足 $g^2 = e$ 的元素的集合. 注意到 $g^2 = e$ 当且仅当 $g = g^{-1}$. 因此对 $s \in S$, 一定有 $s^{-1} \neq s$, 且 $s^{-1} \in S$. 因此, 存在 $s_1, \ldots, s_l \in S$, 使得 S 中的全部元素恰好为 $s_1, s_1^{-1}, s_2, s_2^{-1}, \ldots, s_l, s_l^{-1}$. 此时 $\prod_{s \in S} s = \prod_{k=1}^{l} s_k \prod_{k=1}^{l} s_k^{-1} = e$. 故而 $g = \prod_{k=1}^{m} a_k \prod_{s \in S} s = \prod_{k=1}^{m} a_k$. □

问题 (3.3): 若方程 $X^2 = e$ 在 G 中恰有 $X = e$ 和 $X = a$ 两个解,请证明: (3.1) 中的 $g = a$.

证明. 由 (3.2) 立刻得到. □

问题 (3.4):请证明Wilson's 定理: $(p-1)! \equiv -1 \mod p$.

证明. 将 (3.3) 应用于有限交换群 $(\mathbb{Z}/p\mathbb{Z})^\times$. 注意到同余方程 $X^2 \equiv 1 \mod p$ 只有 $X = \pm 1 \mod p$ 两个解, 故而由 (3.3) 得到. □

问题 (3.5):请证明: 方程 $X^2 = e$ 在 G 中的全体解构成 G 的子群, 记作 $G[2]$.

证明. 由 G 交换, 故 $(ab)^2 = abab = aabb = a^2b^2$, 故若 $a, b \in G[2]$, 则 $ab \in G[2]$. 另一方面, 对 $a \in G[2]$, 则 $a^{-1} = a$, 故 $a^{-1} \in G[2]$, 故 $G[2]$ 构成子群. □

在下面的问题中, 你可以不加证明地用到如下事实: $G[2]$ 构成有限维 $\mathbb{F}_2$-线性空间. 即存在 $a_1, \ldots, a_d \in G[2]$, 使得 $G[2]$ 中的每一个元素都唯一形如 $\prod_{i=1}^{d} a_i^{n_i}$, 其中 $n_i \in \{0, 1\}$.

问题 (3.6):请证明: 若 $G[2]$ 非平凡, 则存在 $G[2]$ 的子群 H, 使得 $[G[2] : H] = 2$.

证明. 由问题前的事实, 当 $G[2]$ 非平凡, 则存在 $d \geq 1$, 使得 $G[2]$ 中的元素都形如 $\prod_{i=1}^{d} a_i^{n_i}$, 其中 $n_i \in \{0, 1\}$. 此时, 考虑所有形如 $\prod_{i=1}^{d-1} a_i^{n_i}$ 的元素构成的集合 H, 不难验证 H 构成 $G[2]$ 的子群, 且 $G = H \sqcup Ha_d$, 故 $[G : H] = 2$. □

问题 (3.7): 若方程 $X^2 = e$ 在 G 中只有 $X = e$ 一个解, 或该方程解的数目 > 2,请证明: (3.1) 中的 $g = e$.

证明. 当 $X^2=e$ 只有 $X=e$ 一个解, 则由 (3.2) 得到. 当解的数目 >2, 由 (3.6), 则存在 $G[2]$ 的子群 H, 使得 $[G:H]=2$, 且此时 $|H|=2^{d-1}$. 取 $y\in G[2]-H$, 则 $G[2]=H\sqcup yH$. 进而 $\prod\limits_{a\in G[2]} a=(\prod\limits_{h\in H}h)(\prod\limits_{h\in H}yh)=y^{2^{d-1}}(\prod\limits_{h\in H}h)^2=e$. □

问题 (4): 本系列问题旨在证明 $S=\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ 和 $T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ 构成 $\mathrm{SL}_2(\mathbb{Z})$ 的生成元.
问题 (4.1): 我们定义:

$$\mathrm{SL}_2(\mathbb{Z})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{R}):a,b,c,d\in\mathbb{Z}\right\},$$

请证明: $\mathrm{SL}_2(\mathbb{Z})$ 构成 $\mathrm{SL}_2(\mathbb{R})$ 的子群.

证明. 显然 $\mathrm{SL}_2(\mathbb{Z})$ 对矩阵乘法封闭. 由 (1.7), 当 $A\in\mathrm{SL}_2(\mathbb{Z})$, 则 $A^{-1}\in\mathrm{SL}_2(\mathbb{Z})$, 故而 $\mathrm{SL}_2(\mathbb{Z})$ 构成 $\mathrm{SL}_2(\mathbb{R})$ 的子群. □

问题 (4.2): 对于群 G, 若 S 是 G 的子集, 若 H 是所有包含 S 的 G 的子群中最小的一个, 则称 S 是 H 的生成元.请证明 下列条件等价:

(1) S 是 H 的生成元.

(2) 任取 $h\in H$, 则 h 形如 $s_1^{\pm1}s_2^{\pm1}\cdots s_n^{\pm1}$, 其中 $s_i\in S$.

进一步地, 我们记:

$$\langle S\rangle=\left\{g\in G:g\text{形如}s_1^{\pm1}s_2^{\pm1}\cdots s_n^{\pm1}\text{其中}s_i\in S\right\},$$

则 $\langle S\rangle$ 是 G 的子群, 且 S 构成 $\langle S\rangle$ 的生成元. 我们称 $\langle S\rangle$ 是 S 在 G 中生成的子群.

证明. 略. □

问题 (4.3): 我们记:

$$S=\begin{pmatrix}0&1\\-1&0\end{pmatrix},T=\begin{pmatrix}1&1\\0&1\end{pmatrix},$$

请证明:S,T 构成 $\mathrm{SL}_2(\mathbb{Z})$ 的生成元.
提示: 对于 $A=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$, 则 $AS=\left(\begin{smallmatrix}-b&a\\-d&c\end{smallmatrix}\right)$, $AT^n=\left(\begin{smallmatrix}a&b+na\\c&d+nc\end{smallmatrix}\right)$, 因此通过反复右乘 S,T 可以对 a,b 进行辗转相除, 使得 A 化为下三角矩阵.

证明. 对 $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$, 若 $|a|>|b|$ 则用 AS 替代 A, 不妨设 $|a|\le|b|$. 此时, 存在唯一 $n\in\mathbb{Z}$, 使得 $b=na+r$, 其中 $0\le r<|a|$. 此时 $AT^{-n}=\begin{pmatrix}a&r\\c&d-nc\end{pmatrix}$. 我们再用

S 右乘交换 a, r 的位置, 则我们可以反复进行上述过程以进行辗转相除. 最终, 我们可以将 A 化为如下的形式:

$$\begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix},$$

由 $\det(A) = 1$, 则 $a'd' = 1$. 由 a', d' 都是整数, 则 $a' = d' = 1$ 或 $a' = d' = -1$. 注意到 $S^2 = -I_2$. 若 $a' = d' = 1$, 则用 AS^2 替代 A, 不妨设 $a' = d' = -1$. 此时, 注意到:

$$SAS = \begin{pmatrix} -d' & c' \\ 0 & -a' \end{pmatrix} = \begin{pmatrix} 1 & c' \\ 0 & 1 \end{pmatrix} = T^{c'},$$

故得证. □

问题 (5): 本系列问题旨在介绍双陪集的概念, 以及双陪集相关的例子和应用.
问题 (5.1): 对集合 S, 若关系 $\sim$ 满足如下条件:

(自反性) 对 $s \in S$, 则 $s \sim s$.

(对称性) 对 $s_1, s_2 \in S$, 若 $s_1 \sim s_2$, 则 $s_2 \sim s_1$.

(传递性) 对 $s_1, s_2, s_3 \in S$, 若 $s_1 \sim s_2$, $s_2 \sim s_3$, 则 $s_1 \sim s_3$.

则我们称 $\sim$ 为 S 上的等价关系. 当 $\sim$ 是等价关系, 对 $s \in S$, 我们记 $[s] = \{s' \in S : s \sim s\}$, 称作 s 所在的等价类.请证明:

(1) 若 $\{[s_i]\}_{i\in I}$ 是 S 上等价关系 $\sim$ 的所有不同的等价类, 则有集合的无交并分解 $S = \bigsqcup_{i\in I} [s_i]$.

(2) 反之, 若 $S = \bigsqcup_{i\in I} S_i$ 是集合的无交并分解, 则存在唯一 S 上的等价关系 $\sim$, 使得每个 S_i 都是 $\sim$ 的等价类.

进一步地,请证明: 上述 (1) 和 (2) 的构造是互逆的, 进而 S 上的等价关系 1-1 对应于 S 的无交并分解.

证明. 略. □

问题 (5.2): 对于群 G, 若 H, K 是 G 的子群. 我们在 G 上定义关系 $\sim$: 对 $g, g' \in G$, 令 $g \sim g'$ 当且仅当存在 $h \in H, k \in K$, 使得 $g = hg'k$.请证明: 这个关系构成等价关系.

证明. 由 $g = ege$, 故 $g \sim g$. 当 $g \sim g'$, 则 $g = hg'k$, 进而 $g' = h^{-1}gk^{-1}$, 故 $g' \sim g$. 当 $g \sim g'$ 且 $g' \sim g''$, 则 $g = hg'k$, $g' = h'g''k'$, 故 $g = (hh')g''(k'k)$, 进而 $g \sim g''$. 故 $\sim$ 是一个等价关系. □

问题 (5.3): 在 (5.2) 的条件下,请证明: 对 $g \in G$, 则 g 所在的等价类恰为集合:

$$HgK = \{hgk : h \in H, k \in K\}.$$

我们称形如 HgK 的集合为 G 的一个 $H-K$ 双陪集, 并记 G 的所有双陪集构成的集合为 $H\backslash G/K$, 称作 G 的 $H-K$ 双陪集空间.

证明. 若 $g' \sim g$, 则 $g' = hgk$, 进而 $g' \in HgK$. 反之, 对 $g' = hgk \in HgK$, 显然 $g' \sim g$. □

问题 (5.4):请证明: 在 (5.2) 的条件下, 对 $g \in G$, 则双陪集 HgK 有如下陪集分解:

(1) 存在 K 中的元素 $\{k_i\}_{i\in I}$, 使得 $HgK = \bigsqcup_{i\in I} Hgk_i$.

(2) 存在 H 中的元素 $\{h_j\}_{j\in I}$, 使得 $HgK = \bigsqcup_{j\in J} h_j gK$.

我们记全体 Hgk_i 的集合为 $H\backslash HgK$, 记全体 $h_j gK$ 的集合为 HgK/K.

证明. 由对称性, 我们只证明 (1). 为此, 只需证明, 若 $hgk \in HgK$, 则 $H(hgk) \subset HgK$ 即可, 而这是显然的. □

问题 (5.5): 对群 G 及 $g \in G$, 若 H 是 G 的有限子群,请证明: 存在有限多个 $g_1, \ldots, g_n \in HgH$, 使得 $HgH = \bigsqcup_{i=1}^{n} Hg_i = \bigsqcup_{i=1}^{n} g_i H$.

证明. 由 H 是有限的, 则 HgH 也是有限的. 我们记 $n = \frac{|HgH|}{|H|}$. 此时, 则存在 $h_1, \ldots, h_n \in H$, 使得 $HgH = \bigsqcup_{i=1}^{n} Hgh_i$. 同时, 也存在 $h'_1, \ldots, h'_n \in H$, 使得 $HgH = \bigsqcup_{i=1}^{n} h'_i gH$. 此时, 考虑 $g_i = h'_i g h_i$, 则 $Hg_i = H(h'_i g h_i) = Hgh_i$, 而 $g_i H = (h'_i g h_i)H = h'_i gH$, 故 $g_1, \ldots, g_n$ 即为所求. □

问题 (5.6): 对群 G, 若 H 是 G 的有限子群,请证明: 一族 G 中的 $\{g_i\}_{i\in I}$, 使得 $G = \bigsqcup_{i\in I} Hg_i = \bigsqcup_{i\in I} g_i H$.

证明. 由 G 分解成双陪集的无交并, 以及 (5.5) 得到. □

问题 (5.7):请证明: 在 (5.2) 的条件下, 对 $g \in G$, 有如下事实成立:

(1) $H/(H \cap gKg^{-1}) \to HgK/K, h(H \cap gKg^{-1}) \mapsto hgK$ 是良定的双射.

(2) $(K \cap g^{-1}Hg)\backslash K \to H\backslash HgK, (K \cap g^{-1}Hg)k \mapsto Hgk$ 是良定的双射.

证明. 与 (2.3) 的证明实质相同, 故略. □

问题 (5.8): 对 $G = \mathrm{GL}_2(\mathbb{R})$, 我们记:

$$U = \mathrm{U}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : n \in \mathbb{Z} \right\},$$

则对:$g = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$, 其中 $0 \neq m \in \mathbb{Z}$,请证明:UgU 分解为 U 的左陪集的数量和分解为右陪集的数量并不相同. 因而 (5.5) 中 H 是有限群的条件是必要的.

证明. 注意到 $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & mn \\ 0 & 1 \end{pmatrix}$, 故 $gUg^{-1} = \mathrm{U}_2(m\mathbb{Z})$, $g^{-1}Ug = \mathrm{U}_2(\frac{1}{m}\mathbb{Z})$, 进而 $U/gUg^{-1} \cap U = [\mathbb{Z} : m\mathbb{Z}] = m$, 而 $g^{-1}Ug \cap U = U$, 故 $|g^{-1}Ug \cap U \backslash U| = 1$. 进而由 (5.7) 得到. □

补充说明: 这里的 (5.6) 在 $[G : H] < \infty$ 的条件下可以通过纯组合的方法证明 (Hall 定理), 此时可以放松 H 是有限群的限制 (如果你对此感兴趣, 你可以自己尝试证明). 也就是说, 只要 $|H|$ 和 $[G : H]$ 中的一者是有限的, 则我们便可以得到 (5.6) 的结论.