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 $AB = (\sum\limits_{k=1}^{n} a_{ik} b_{kj})$.

(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 $n \in \mathbb{Z}_{\geq 1}$,<u>请证明</u>:$\mathrm{M}_n(K)$ 关于矩阵的加法构成一个交换群.
问题 (1.2): 我们定义:

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

<u>请证明</u>:$\mathrm{GL}_n(K)$ 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 $n = 1$.
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:

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

<u>请证明</u>:$\mathrm{B}_n(K)$ 是 $\mathrm{GL}_n(K)$ 的子群.
问题 (1.4): 我们定义

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

<u>请证明</u>:$\mathrm{SL}_n(K)$ 是 $\mathrm{GL}_n(K)$ 的子群.
问题 (1.5): 我们定义:

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

<u>请证明</u>:$\mathrm{U}_n(K)$ 是 $\mathrm{B}_n(K)$ 的子群.
问题 (1.6): 特别地,<u>请证明</u>: 存在群同构 $(K, +) \cong \mathrm{U}_2(K)$, 这里 $(K, +)$ 是 K 的加法群.
问题 (1.7): 特别地,<u>请证明</u>: 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 $\det(AB) = \det(A)\det(B)$.

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 $[G : H] = [G : K][K : H]$.
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 $\mathrm{l.c.m}(n, m)$ 整除 $[G : H \cap K]$, 这里 $\mathrm{l.c.m}(n, m)$ 是 n, m 的最小公倍数.
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:

$$\begin{aligned} H/H \cap K &\to G/K \\ h(H \cap K) &\mapsto hK \end{aligned}$$

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 $[G : H \cap K] = mn$.

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:$g^2 = e$.
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 $g = \prod_{i=1}^{m} a_i$.
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 $g = a$.
问题 (3.4):请证明Wilson's 定理: $(p-1)! \equiv -1 \mod p$.
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 $G[2]$.

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 $[G[2] : H] = 2$.
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 $g = e$.

问题 (4): 本系列问题旨在证明 $S=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 和 $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 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.
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.
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 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$, 则 $AS=\begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$, $AT^n=\begin{pmatrix} a & b+na \\ c & d+nc \end{pmatrix}$, 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.

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.

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.

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.

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 $HgK = \bigsqcup\limits_{i\in I} Hgk_i$.

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

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

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 $HgH = \bigsqcup\limits_{i=1}^{n} Hg_i = \bigsqcup\limits_{i=1}^{n} g_iH$.

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 $G = \bigsqcup\limits_{i\in I} Hg_i = \bigsqcup\limits_{i\in I} g_iH$.

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.

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 $m \in \mathbb{Z}_{\geq 1}$,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.

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.