问题 (1): 本系列问题中, 我们将考虑 $\mathrm{SL}_2(\mathbb{R})$ 在上半平面上的作用, 以及一些相关的问题.

问题 (1.1): 我们记 $\mathcal{H} = \{x + iy \in \mathbb{C} : x \in \mathbb{R}, y > 0\}$, 称作是复平面的上半平面. 对 $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, 和 $z \in \mathcal{H}$, 我们定义 $gz = \frac{az+b}{cz+d}$. 记 $G = \mathrm{SL}_2(\mathbb{R})$, 请证明:$G \times \mathcal{H} \to \mathcal{H}, (g, z) \mapsto gz$ 给出了 G 在 $\mathcal{H}$ 上的一个群作用.

证明. 对 $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, 则:

$$\begin{aligned} g(g'z) = g(\frac{a'z + b'}{c'z + d'}) &= \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} \\ &= \frac{a(a'z + b') + b(c'z + d')}{c(a'z + b') + d(c'z + d')} \\ &= \frac{(aa' + bc')z + (ab' + bd')}{(ca' + dc')z + (cb' + dd')} \\ &= (g'g)(z). \end{aligned}$$

因而 $G \times \mathcal{H} \to \mathcal{H}, (g, z) \mapsto gz$ 是群作用. □

问题 (1.2): 请证明: G 在 $\mathcal{H}$ 上的作用是可迁的. 即固定 $z_0 \in \mathcal{H}$, 任取 $z \in \mathcal{H}$, 存在 $g \in G$ 使得 $gz = z_0$. 进一步地, 请证明: $\mathrm{Stab}_G(i) = \mathrm{SO}_2(\mathbb{R})$, 其中:

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

证明. 对 $x \in \mathbb{R}, y > 0$, 有 $\begin{pmatrix} \sqrt{y} & x\sqrt{y}^{-1} \\ 0 & \sqrt{y}^{-1} \end{pmatrix} i = \frac{\sqrt{y}i + x\sqrt{y}^{-1}}{\sqrt{y}^{-1}} = x + iy$, 故 G 的作用是可迁的. 注意到 $\frac{\cos(\theta)i+\sin(\theta)}{-\sin(\theta)i+\cos(\theta)} = \frac{e^{i(\frac{\pi}{2}-\theta)}}{e^{i(-\theta)}} = e^{i\frac{\pi}{2}} = i$, 故 $\mathrm{SO}_2(\mathbb{R}) \subset \mathrm{Stab}_G(i)$. 反之, 若 $\frac{ai+b}{ci+d} = i$, 则 $ai + b = di - c$, 故 $a = d$ 而 $b + c = 0$. 由 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, 则 $ad - cb = 1$, 进而 $a^2 + b^2 = 1$. 故存在 θ, 使得 $a = \cos(\theta), b = \sin(\theta)$, 进而 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SO}_2(\mathbb{R})$. □

问题 (1.3): 记 $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, 请证明: 对函数 $f : \mathcal{H} \to \mathbb{C}$, 以及 $k \in \mathbb{Z}_{\geq 0}$, 下列条件等价:

(1) 任取 $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, 都有 $f(\gamma z) = (cz + d)^k f(z)$ 对所有 $z \in \mathcal{H}$ 成立.

(2) 任取 $z \in \mathcal{H}$, 都有 $f(z + 1) = f(z)$ 且 $f(-\frac{1}{z}) = z^k f(z)$.

证明. 由第一次习题课的问题 (4), 我们知道 $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 和 $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 构成 $\mathrm{SL}_2(\mathbb{Z})$ 的生成元, 进而得证. □

补充说明: 对全纯函数 $f: \mathcal{H} \to \mathbb{C}$, 若 f 满足上述的 (1), 则称 f 是一个权为 k 的模形式. 因此, 本题实际上是说明, 模形式可以被 $f(z+1) = f(z)$ 和 $f(-\frac{1}{z}) = z^k f(z)$ 这两个相对简单的条件所刻画.

问题 (1.4): 我们记:$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{R}_{>0} \right\}, N = \mathrm{U}_2(\mathbb{R}), K = \mathrm{SO}_2(\mathbb{R})$, 请证明: 映射 $A \times N \times K \to \mathrm{SL}_2(\mathbb{R}), (a, n, k) \mapsto ank$ 是双射. 我们称这个分解为 $\mathrm{SL}_2(\mathbb{R})$ 的 Iwasawa 分解.

证明. 对 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, 注意到:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{c^2+d^2}} & 0 \\ 0 & \sqrt{c^2+d^2} \end{pmatrix} \begin{pmatrix} 1 & ac+bd \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{d}{\sqrt{c^2+d^2}} & \frac{-c}{\sqrt{c^2+d^2}} \\ \frac{c}{\sqrt{c^2+d^2}} & \frac{d}{\sqrt{c^2+d^2}} \end{pmatrix},$$

因此 $A \times N \times K \to \mathrm{SO}_2(\mathbb{R})$ 是满射. 下面我们证明它是单射. 若 $ank = a'n'k'$, 则我们只需证明 $a = a'$, $n = n'$ 即可. 记 $a = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, a' = \begin{pmatrix} x' & 0 \\ 0 & x'^{-1} \end{pmatrix}, n = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}, n' = \begin{pmatrix} 1 & y' \\ 0 & 1 \end{pmatrix}$, 则 $(ank)(i) = (an)(i) = a(i+y) = x^2(y+i)$, $(a'n'k')(i) = x'^2(y'+i)$. 对比实部和虚部, 则 $x^2 y = x'^2 y'$, $x^2 = x'^2$. 进而 $x = x'$ 且 $y = y'$, 故得证, □

问题 (2): 本系列问题是为不熟悉线性代数的人准备的, 在本系列问题中我们将研究 $\mathrm{M}_n(K)$ 在线性空间 $V = K^n$ 上的作用.

问题 (2.1): 对 $V = K^n$, 我们记 $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$, 因而 V 中任意元素都可以唯一写成 $v = \sum_{i=1}^{n} k_i e_i$ 的形式. 对于 $A \in \mathrm{M}_n(K)$, $A = (a_{ij})$, 我们定义 $\pi(A)(\sum_{i=1}^{n} k_i e_i) = \sum_{i=1}^{n} k_i (\sum_{j=1}^{n} a_{ji} e_j)$,请证明 如下事实成立:

(1) π 给出了 $\mathrm{M}_n(K)$ 在 V 上的一个群作用.

(2) 对 $A \in \mathrm{M}_n(K)$,$\pi(A)$ 在 V 上的作用是线性的. 即任取 $v_1, v_2 \in V$ 以及 $k_1, k_2 \in K$, 都有 $\pi(A)(k_1 v_1 + k_2 v_2) = k_1 \pi(A) v_1 + k_2 \pi(A) v_2$.

(3) $\pi(AB)v = \pi(A)(\pi(B)v)$ 对所有 $A, B \in \mathrm{M}_n(K), v \in V$ 成立.

(4) $\pi|_{\mathrm{GL}_n(K)}$ 给出了 $\mathrm{GL}_n(K)$ 在 V 上的一个群作用.

证明. 略. □

问题 (2.2): 对映射 $f: V \to V$, 若 $f(k_1 v_2 + k_2 v_2) = k_1 f(v_1) + k_2 f(v_2)$ 对所有 $v_1, v_2 \in V, k_1, k_2 \in K$ 成立, 则称 f 是一个线性映射,请证明 如下事实成立:

(1) 若 $f: V \to V$ 是线性映射, 则存在唯一 $A \in \mathrm{M}_n(K)$, 使得 $f = \pi(A)$.

(2) 若 $f: V \to V$ 是可逆的线性映射, 则存在唯一 $A \in \mathrm{GL}_n(K)$, 使得 $f = \pi(A)$, 且此时 $f^{-1} = \pi(A^{-1})$.

证明. 略. $\square$

问题 (3): 本系列问题中, 作为有限生成阿贝尔群结构定理的一个例子, 我们将研究 $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ 的结构.

问题 (3.1):请证明: 存在同构 $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

证明. 若 $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ 是同态, 记 $f(1) \equiv t \mod n$, 则 t 唯一确定了 f. 我们记 f_t 是唯一使得 $f_t(1) \equiv t \mod n$ 的同态, 则 f_t 是自同构当且仅当存在 f_s, 使得 $f_s \circ f_t = \mathrm{Id}$, 当且仅当 $f_s(f_t(1)) \equiv st \equiv 1 \mod n$, 当且仅当 $t \in (\mathbb{Z}/n\mathbb{Z})^\times$. 此时 $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), t \mod n \mapsto f_t$ 是群同构. $\square$

问题 (3.2):请证明: 当 m, n 互素, 则存在同构 $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.
提示: 利用初等数论中的中国剩余定理.

证明. 中国剩余定理说明 $(\mathbb{Z}/nm\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times, x \mod nm \mapsto (x \mod n, x \mod m)$ 是满射. 由 $\varphi(nm) = \varphi(n)\varphi(m)$, 这里 φ 是 Euler 函数, 因而 $|(Z/nm\mathbb{Z})^\times| = \varphi(nm) = |(\mathbb{Z}/n\mathbb{Z})^\times||(\mathbb{Z}/m\mathbb{Z})^\times|$, 故上述映射是同构. $\square$

问题 (3.3):请证明: 当 $n = 1$, 则 $(\mathbb{Z}/2^n\mathbb{Z})^\times$ 平凡. 当 $n = 2$, 则 $(\mathbb{Z}/2^n\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z}$. 当 $n > 2$, 请通过如下的步骤, 证明 $5 \mod 2^n$ 在 $(\mathbb{Z}/2^n\mathbb{Z})^\times$ 中的阶恰为 2^{n-2}:

(1) 请证明: 对任意的奇数 x, $x^{2^{n-2}} \equiv 1 \mod 2^n$.

(2) 请证明: 2^{n+2} 恰好整除 $5^{2^n} - 1$.

(3) 请证明: $5 \mod 2^n$ 在 $(\mathbb{Z}/2^n\mathbb{Z})^\times$ 中的阶恰为 2^{n-2}.

证明. $(\mathbb{Z}/2\mathbb{Z})^\times = \{1 \mod 2\}$, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1 \mod 4\}$. 对于 (1), 我们对 n 进行归纳. 当 $n = 3$ 时, 直接计算知, 对任意奇数 x, 都有 $x^2 \equiv 1 \mod 8$. 现在, 当 $x^{2^{n-2}} \equiv 1 \mod 2^n$, 考虑 $x^{2^{n-1}} - 1 = (x^{2^{n-2}} - 1)(x^{2^{n-2}} + 1)$, 由 x 是奇数, 则 2 整除 $(x^{2^{n-2}} + 1)$, 故 $x^{2^{n-1}} \equiv 1 \mod 2^{n+1}$. 对于 (2), 同样对 n 进行归纳. 当 $n = 0$, 显然 4 恰好整除 $5 - 1 = 4$. 因此, 只需证明 2 恰好整除 $5^{2^n} + 1$ 即可. 注意到 $5^{2^n} + 1 \equiv 2 \mod 4$, 因此 4 不整除 $5^{2^n} + 1$, 进而得到 (2). 对于 (3), 由 (1), 则 $5 \mod 2^n$ 的阶整除 2^{n-2}. 由 (2), 对 $d < n-2$ 则 2^n 不整除 $5^{2^d} - 1$, 因此 $5 \mod 2^n$ 的阶不是 2^d, 则 $5 \mod 2^n$ 的阶只能是 2^{n-2}. $\square$

问题 (3.4): 请通过以下的步骤证明, 有 $(\mathbb{Z}/2^n\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$:

(1) 请证明: $|(\mathbb{Z}/2^n\mathbb{Z})^\times| = 2^{n-1}$.

(2) 请证明: 不存在 $m \in \mathbb{Z}$, 使得 $5^m \equiv -1 \mod 2^n$.

(3) 请证明: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \to (\mathbb{Z}/2^n\mathbb{Z})^\times, (x \mod 2, y \mod 2^{n-2}) \mapsto (-1)^x 5^y \mod 2^n$ 给出了群的同构.

证明. (1) 由 $\varphi(p^n) = (p-1)p^{n-1}$ 得到. 对于 (2), 由 $5^m + 1 \equiv 2 \mod 4$, 因此 $n \geq 2$ 时不存在 m 使得 $5^m \equiv -1 \mod 2^n$. 对于 (3), (2) 说明 (3) 中的映射是双射. 由 (1), 则 $|(\mathbb{Z}/2^n\mathbb{Z})^\times| = |\mathbb{Z}/2\mathbb{Z}||\mathbb{Z}/2^{n-2}\mathbb{Z}|$, 故 (3) 中的映射是同构. □

问题 (3.5): 请将$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ 分解为若干循环群的直积.
提示: 在本问题中, 你可以直接使用如下事实: 若 p 是奇素数, 则对 $n \in \mathbb{Z}_{\geq 1}$, 模 p^n 的原根存在, 即 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 是循环群.

证明. 由 (3.2), (3.5), 以及提示, 对 $n = 2^m p_1^{n_1} \dots p_r^{n_r}$, 其中 p_i 是奇素数, 则有:

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \begin{cases} \prod_{i=1}^{r} (\mathbb{Z}/(p_i - 1)p_i^{n_i}\mathbb{Z}) & \text{当} m = 1 \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z}) \times \prod_{i=1}^{r} (\mathbb{Z}/(p_i - 1)p_i^{n_i}\mathbb{Z}) & \text{当} m > 1 \end{cases}$$

□

问题 (4): 本系列问题中, 我们将研究有限阿贝尔群的对偶群.

问题 (4.1): 对有限阿贝尔群 G, 我们记 $\widehat{G}=\mathrm{Hom}_{\mathrm{Grp}}(G,\mathbb{S}^1)$, 其中 $\mathbb{S}^1=\{z\in\mathbb{C}:|z|=1\}$. 请证明: 在 $\widehat{G}$ 上, 对 $\chi_1,\chi_2\in\widehat{G}$, 由 $(\chi_1\chi_2)(g)=\chi_1(g)\chi_2(g)$ 定义的乘法使得 $\widehat{G}$ 成为阿贝尔群.

证明. 略. $\square$

问题 (4.2): 对有限阿贝尔群 G,H, 请证明: 存在同构 $\widehat{G}\times\widehat{H}\cong\widehat{G\times H}$.

证明. 对 $\chi_G\in\widehat{G},\chi_H\in\widehat{H}$, 我们定义 $\chi_{G\times H}(g,h)=\chi_G(g)\chi_H(h)$, 则得到群同态 $\widehat{G}\times\widehat{H}\to\widehat{G\times H},(\chi_G,\chi_H)\mapsto(\chi_{G\times H})$. 注意到 $\chi_G=\chi_{G\times H}|_{G\times 1}$, 而 $\chi_H=\chi_{G\times H}|_{1\times H}$, 故上述映射是单射. 反之, 对 $\psi\in\widehat{G\times H}$, 记 $\chi_G(g)=\psi(g,1)$, $\chi_H(h)=\psi(1,h)$, 则 $\psi=\chi_{G\times H}$, 故上述映射是满射. $\square$

问题 (4.3): 请证明: 存在同构 $\widehat{\mathbb{Z}/n\mathbb{Z}}\cong\mathbb{Z}/n\mathbb{Z}$.

证明. 对同态 $f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{S}^1$, 注意到 $f(1)^n=1$, 因此 $f(1)$ 是 n-次单位根. 我们记 μ_n 是所有 n-次单位根的集合, 则 $\widehat{\mathbb{Z}/n\mathbb{Z}}=\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mu_n)$. 注意到 $\mu_n\cong\mathbb{Z}/n\mathbb{Z}$, 故 $\widehat{\mathbb{Z}/n\mathbb{Z}}\cong\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z})$. 由 (3.1) 的证明, 我们知道存在同构 $\mathbb{Z}/n\mathbb{Z}\to\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/n\mathbb{Z}),t \bmod n\mapsto f_t$. $\square$

问题 (4.4): 利用有限阿贝尔群的结构定理, 请证明: 若 G 是有限阿贝尔群, 则 $G\cong\widehat{G}$.

证明. 由 (4.2), (4.3), 以及有限阿贝尔群的结构定理立刻得到. $\square$

问题 (4.5): 对有限阿贝尔群 G, 若 H 是 G 的子群, 我们定义:

$$H^{\perp}=\left\{\chi\in\widehat{G}:\chi|_H=1\right\},$$

请证明 如下事实成立:

(1) $\widehat{G}/H^{\perp}\to\widehat{H},\chi\mapsto\chi|_H$ 是群同构.

(2) $\widehat{G/H}\to H^{\perp},\chi\mapsto\chi\circ\pi$ 是群同构, 其中 π 是自然投影 $\pi:G\to G/H$.

证明. 首先, 容易验证 $\widehat{G}/H^{\perp}\to\widehat{H}$ 是单射, 而 $\widehat{G/H}\to H^{\perp}$ 是满射, 因此 $\frac{|\widehat{G}|}{|H^{\perp}|}\leq|\widehat{H}|$, 且 $\frac{|G|}{|H|}\geq|H^{\perp}|$. 由 (4.4), 则 $|G|=|\widehat{G}|$, $|H|=\widehat{H}$, 因此 $|H^{\perp}|=\frac{|G|}{|H|}$, 进而上述两个映射都是双射, 进而是同构. $\square$

问题 (4.6): 对有限阿贝尔群 G, 请证明: 映射 $G\to\widehat{\widehat{G}},g\mapsto(\chi\mapsto\chi(g))$ 给出了群同构, 且这个同构是自然的, 即若 $f:G\to G'$ 是阿贝尔群的同态, 则有如下交换图成立:

$$\begin{tikzcd} G \arrow[r] \arrow[d, "f"] & \widehat{\widehat{G}} \arrow[d, "\widehat{\widehat{f}}"] \\ G' \arrow[r] & \widehat{\widehat{G'}} \end{tikzcd}$$

其中 $\widehat{\widehat{f}}(\theta)(\chi)=\theta(\chi\circ f)$.

证明. 显然 $G \to \widehat{\widehat{G}}$ 是单射, 因而由 $|\widehat{\widehat{G}}| = |G|$, 则其是同构. 其自然性可以通过直接地计算验证而知. $\square$

问题 (4.7): 对有限阿贝尔群 G, $\chi \in \widehat{G}$, 请证明:

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \chi = 1 \\ 0 & \chi \neq 1 \end{cases}$$

证明. 当 $\chi = 1$, 结果是显然的. 当 $\chi \neq 1$, 则存在 $g_0 \in G$, 使得 $\chi(g_0) \neq 1$, 此时 $\sum\limits_{g\in G} \chi(g) = \sum\limits_{g\in G} \chi(g_0 g) = \chi(g_0) \sum\limits_{g\in G} \chi(g)$, 则只能有 $\sum\limits_{g\in G} \chi(g) = 0$. $\square$

问题 (4.8): 对有限阿贝尔群 G, 以及函数 $f : G \to \mathbb{C}$, 我们定义 f 的 Fourier 变换 $\mathcal{F}f : \widehat{G} \to \mathbb{C}$:

$$\mathcal{F}f(\chi) = \frac{1}{\sqrt{|G|}} \sum_{g\in G} f(g)\overline{\chi(g)}.$$

请证明: 在 (4.6) 的自然同构的意义下, 有如下 Fourier 反演公式成立:

$$\mathcal{F}\mathcal{F}f(x^{-1}) = f(x).$$

证明. 此时:

$$\begin{aligned} \mathcal{F}\mathcal{F}f(x^{-1}) &= \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \sum_{g\in G} f(g)\overline{\chi(g)\chi(x^{-1})} \\ &= \frac{1}{|G|} \sum_{g\in G} f(g)\overline{\sum_{\chi\in\widehat{G}} \chi(gx^{-1})} \end{aligned}$$

将 (4.7) 运用于 $\widehat{G}$, 利用同构 $G = \widehat{\widehat{G}}$, 则我们有:

$$\sum_{\chi\in\widehat{G}} \chi(gx^{-1}) = \begin{cases} |G| & \text{当} g = x \\ 0 & \text{当} g \neq x \end{cases}$$

因此我们有 $\mathcal{F}\mathcal{F}f(x^{-1}) = f(x)$. $\square$

问题 (4.9): 对有限阿贝尔群 G, G 的子群 H, 以及函数 $f : G \to \mathbb{C}$, 请证明: 有如下 Possion 求和公式成立:

$$\frac{1}{\sqrt{|H|}} \sum_{h\in H} f(xh) = \frac{1}{\sqrt{|H^\perp|}} \sum_{\chi\in H^\perp} \mathcal{F}f(\chi)\chi(x).$$

证明. 注意到:

$$\begin{aligned} \sum_{\chi\in H^\perp} \mathcal{F}f(\chi)\chi(x) &= \frac{1}{\sqrt{|G|}} \sum_{\chi\in H^\perp} \sum_{g\in G} f(g)\chi(xg^{-1}) \\ &= \frac{1}{\sqrt{|G|}} \sum_{g\in G} f(xg) \sum_{\chi\in H^\perp} \chi(g^{-1}) \end{aligned}$$

将 (4.7) 运用于 $H^{\perp}$. 由 (4.5), 则 $\widehat{H^{\perp}} = \widehat{\widehat{G/H}} = G/H$, 因此我们有:

$$\sum_{\chi \in H^{\perp}} \chi(g^{-1}) = \begin{cases} |H^{\perp}| & \text{当} g \in H \\ 0 & \text{当} g \notin H \end{cases}$$

将上式带回, 则有:

$$\sum_{\chi \in H^{\perp}} \mathcal{F}f(\chi)\chi(x) = \frac{|H^{\perp}|}{\sqrt{|G|}} \sum_{h \in H} f(xh) = \frac{\sqrt{|H^{\perp}|}}{\sqrt{|H|}} \sum_{h \in H} f(xh).$$

□

问题 (5): 本系列问题中, 我们将研究 $\mathrm{SL}_2(K)$ 的结构. 为避免不必要的麻烦, 我们设 K 是有无穷多元素的域.

问题 (5.1): <u>请证明</u>: $\mathrm{SL}_2(K)$ 可以被形如:$n(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ 和 $n'(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ 的元素生成.

提示: 本问题改编自 2023 年丘赛代数试题, 下面的矩阵恒等式是我在丘赛之后手搓出来的, 具体构造思路我现在已经想不起来了, 各位同学有需要的话可以参考:

$$\begin{pmatrix} 1 & -\frac{a-1}{at} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \begin{pmatrix} 1 & \frac{a-1}{a^2t} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ at & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{t} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} -t & 0 \\ 0 & -\frac{1}{t} \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{t} \\ 0 & 1 \end{pmatrix}$$

证明. 由提示中第一行的恒等式 $\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$ 可被 $n(t), n'(t)$ 生成. 由提示中第二行的恒等式 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 可被 $n(t), n'(t)$ 生成. 不难验证, 形如 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}, n(t), n'(t)$ 的元素生成了 $\mathrm{SL}_2(K)$. □

问题 (5.2): <u>请证明</u> 如下的事实成立:

(1) 任取 $t \in K$, 存在 $x, y \in K$, 使得 $n(t) = xyx^{-1}y^{-1}$.

(2) 任取 $t \in K$, 存在 $x, y \in K$, 使得 $n‘(t) = xyx^{-1}y^{-1}$.

提示: 考虑 $n(t), n'(t)$ 和对角矩阵的交换化子 (称 $xyx^{-1}y^{-1}$ 是 x, y 的交换化子).

证明. 注意到:

$$\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)t \\ 0 & 1 \end{pmatrix},$$

因此 $n(t)$ 形如交换化子. 对 $n'(t)$ 也是同理的. □

问题 (5.3): 对群 G, 我们记 $[G, G]$ 是由所有形如 $gg'g^{-1}g'^{-1}$ 的元素生成的子群. <u>请证明</u>: $[\mathrm{GL}_2(K), \mathrm{GL}_2(K)] = \mathrm{SL}_2(K)$, 且 $[\mathrm{SL}_2(K), \mathrm{SL}_2(K)] = \mathrm{SL}_2(K)$.

证明. 注意到 $\mathrm{SL}_2(K) = \mathrm{Ker}(\det)$, 而 $\det(xyx^{-1}y^{-1}) = 1$, 进而 $[\mathrm{GL}_2(K), \mathrm{GL}_2(K)] \subset \mathrm{SL}_2(K)$. 由 (5.1), (5.2), 则 $[\mathrm{SL}_2(K), \mathrm{SL}_2(K)] = \mathrm{SL}_2(K)$, 进而我们有 $[\mathrm{GL}_2(K), \mathrm{GL}_2(K)] \supset [\mathrm{SL}_2(K), \mathrm{SL}_2(K)]$, 故 $[\mathrm{GL}_2(K), \mathrm{GL}_2(K)] = \mathrm{SL}_2(K)$. □

问题 (5.4):<u>请证明</u>: 若 $\chi : \mathrm{GL}_2(K) \to K^\times$ 是同态, 则存在同态 $\psi : K^\times \to K^\times$, 使得 $\chi = \psi \circ \det$.

证明. 若 $\chi : \mathrm{GL}_2(K) \to K^\times$ 是同态, 注意到 $\chi(xyx^{-1}y^{-1}) = \chi(x)\chi(y)\chi(x)^{-1}\chi(y)^{-1} = 1$, 因而 $[\mathrm{GL}_2(K), \mathrm{GL}_2(K)] \subset \mathrm{Ker}(\chi)$, 故 χ 分解经过 $\mathrm{GL}_2(K)/\mathrm{SL}_2(K)$, 注意到 $\det : \mathrm{GL}_2(K)/\mathrm{SL}_2(K) \to K^\times$ 是同构, 故得证. □

问题 (5.5):<u>请证明</u>: $H = \{\pm I_2\}$ 是 $\mathrm{SL}_2(K)$ 的正规子群, 因此 $\mathrm{SL}_2(K)$ 不是单群.

证明. 这是容易验证的. □

问题 (5.6): 如果你熟悉线性代数的话, <u>请证明</u>:$(5, 1)$ 至 (5.4) 可以推广至 $\mathrm{SL}_n(K)$.
提示: 记 E_{ij} 是只有 (i, j)-元为 1, 其余项全为 0 的矩阵, 考虑 $n_{ij}(t) = I_n + tE_{ij}(i \neq j)$, 请证明 $\mathrm{SL}_n(K)$ 可以被形如 $n_{ij}(t)$ 的元生成, 这是 (5.1) 的推广.

证明. 我们只给出证明的纲要. 同理 (5.1), 我们知道形如 $\mathrm{diag}(t_1, t_2, \cdots, t_{n-1}, \frac{1}{t_1 t_2 \ldots t_{n-1}})$ 的矩阵可以被 n_{ij} 和 n'_{ij} 生成. 同样地, 我们知道可以起到交换矩阵行或列的置换矩阵, 即 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 的对应物, 可以由 n_{ij}, n'_{ij} 生成. 因此, 同理 Gauss 消元法的过程, 则 $\mathrm{SL}_n(K)$ 中的元素可以由形如 n_{ij}, n'_{ij} 的元素生成. 对于 (5.2) 的推广, 我们同样考虑 n_{ij}, n'_{ij} 和对角矩阵的交换化子即可. 此时我们自然能够得到 (5.3) 和 (5.4) 的推广. □