Number Theory II

D-MATH Prof. Dr. Emmanuel Kowalski

Solutions: Exercise Sheet 1

1. Let

$$\mathbf{D} = \{ z \in \mathbf{C} \mid |z| < 1 \}$$

be the unit disc in \mathbf{C} .

Prove that the maps

$$f: \mathbf{H} \to \mathbf{D}, \qquad g: \mathbf{D} \to \mathbf{H}$$

defined by

$$f(z) = \frac{z-i}{z+i},$$
 $g(w) = i\frac{w+1}{1-w}$

are indeed well-defined and are reciprocal conformal equivalences (i.e., they are reciprocal bijective holomorphic maps).

Solution:

First we will show that the maps are well-defined. Let $z \in \mathbf{H}$ be arbitrary and write z = x + yi with $x, y \in \mathbf{R}$. Calculate

$$\begin{split} f(z) &= \frac{x+i(y-1)}{x+i(y+1)} = \frac{x^2+y^2-1}{x^2+(y+1)^2} + i\frac{x(y-1)-x(y+1)}{x^2+(y+1)^2} \\ &= \frac{x^2+y^2-1}{x^2+(y+1)^2} - i\frac{2x}{x^2+(y+1)^2}. \end{split}$$

Since y > 0, we have that 2(y + 1) > 2 and $(y + 1)^2 + y^2 - 1 > 0$, so that

$$(x^{2} + (y+1)^{2} - (x^{2} + y^{2} - 1)) \cdot (x^{2} + (y+1)^{2} + (x^{2} + y^{2} - 1)) > 4x^{2}.$$

This is equivalent to

$$(x^{2} + (y+1)^{2})^{2} > (x^{2} + y^{2} - 1)^{2} + 4x^{2},$$

from which we obtain

$$|f(z)| = \frac{(x^2 + y^2 - 1)^2 + 4x^2}{(x^2 + (y+1)^2)^2} < 1,$$

and $f(z) \in \mathbf{D}$.

Let $\omega = x + yi \in \mathbf{D}$, with $x, y \in \mathbf{R}$, be arbitrary. Then

$$g(\omega) = \frac{(x+1)i - y}{(1-x) - yi}$$
$$= \frac{(1-x^2) - y^2}{(1-x)^2 + y^2}i + R,$$

for some $R \in \mathbf{R}$. We need to show that $\frac{(1-x^2)-y^2}{(1-x)^2+y^2} > 0$. This is true if and only if $1-x^2-y^2 > 0$, which follows for all $x + yi \in \mathbf{D}$, as $x^2 + y^2 < 1$.

Next, we will show that the maps are bijections. Let $z \in \mathbf{H}$ and $\omega \in \mathbf{D}$ be arbitrary. Then

$$g \circ f(z) = g\left(\frac{z-i}{z+i}\right) = i\frac{\frac{z-i+z+i}{z+i}}{\frac{z+i-(z-i)}{z+i}} = i\frac{2z}{2i} = z.$$

and

$$f \circ g(\omega) = f\left(\frac{\omega i + i}{1 - \omega}\right) = \frac{\frac{\omega i + i - i + \omega i}{1 - \omega}}{\frac{\omega i + i + i - \omega i}{1 - \omega}} = \frac{2\omega i}{2i} = \omega.$$

Hence f and g are reciprocal bijections. Moreover, since z + i is never zero on the upper-half plane **H**, we have that the derivative f'(z) exists for all $z \in \mathbf{H}$ and f is holomorphic.

2. a) Let K be a field. Show that the subgroup G of $SL_2(K)$ generated by the matrices of the form

$$u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad v(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},$$

for $x \in K$ contains the matrices

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

for $a \in K^{\times}$. (Hint: consider a product u(b)v(c)u(d)v(e) and specialize b, c, d and e.) Solution:

Let $a \in K^{\times}$ be arbitrary. Then

$$u(-a)v(a^{-1}-1)u(1)v(-1+a) = \begin{pmatrix} 1 & -a \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ a^{-1}-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ a-1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} a & -a \\ a^{-1}-1 & 1 \end{pmatrix} \begin{pmatrix} a & 1 \\ a-1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} a \\ & a^{-1} \end{pmatrix}.$$

b) Deduce that $G = SL_2(K)$. (Hint: use linear algebra to reduce to the previous question.)

Solution:

Clearly G is a subgroup of $SL_2(K)$, so we only have to show the other inclusion. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(K)$. We will have a couple of cases.

First, assume that c = 0. Then ad = 1, so that $d = a^{-1}$ (and especially $a \neq 0$), and we can write

$$\begin{pmatrix} a & b \\ & d \end{pmatrix} = \begin{pmatrix} a \\ & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a} \\ & 1 \end{pmatrix} \in G.$$
(1)

From now on we can assume that $c \neq 0$. If b = 0, we can similarly write

$$\begin{pmatrix} a \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ a^{-1} \end{pmatrix} \begin{pmatrix} 1 \\ ac \\ 1 \end{pmatrix} \in G.$$
(2)

Assume $b \neq 0$ and $c \neq 0$. Note that

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} \in G.$$

If a = 0, we have $c = b^{-1}$. Note that

$$\begin{pmatrix} b \\ -b^{-1} & d \end{pmatrix} = \begin{pmatrix} b \\ d & b^{-1} \end{pmatrix} \begin{pmatrix} -1 \\ 1 & \end{pmatrix},$$

which is contained in G by part (2). Finally, if $a \neq 0$ as well, we have

$$\begin{pmatrix} a & b \\ & d \end{pmatrix} \begin{pmatrix} a^{-1} & -b \\ & a \end{pmatrix} = \begin{pmatrix} 1 \\ ca^{-1} & 1 \end{pmatrix},$$

which is in G by part (1). Hence $SL_2(K)$ is contained in G and we are done.

c) Let p be a prime number. Show that $SL_2(\mathbf{F}_p)$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Solution:

By part b) we have that $SL_2(\mathbf{F}_p)$ is generated by matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

for $x, y \in \mathbf{F}_p$. Let $r' \in \mathbf{F}_p$ be arbitrary. We can write $r' = r + p\mathbf{Z}$, for $r \in (0, 1, \dots, p-1)$. Then we have in $\mathrm{SL}_2(\mathbf{F}_p)$

$$\begin{pmatrix} 1 & r' \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^r$$

and similarly

$$\begin{pmatrix} 1 \\ r' & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 & 1 \end{pmatrix}^r.$$

Thus the two matrices $\begin{pmatrix} 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ generate $SL_2(\mathbf{F}_p)$.

d) Show that for any prime number p, the map $SL_2(\mathbf{Z}) \to SL_2(\mathbf{F}_p)$ defined by reduction modulo p is a surjective homomorphism. Solution: Let $A = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in SL_2(\mathbf{F}_p)$ be arbitrary. There exists $r_1 \in \mathbf{Z}$ such that $r_1\overline{a} + \overline{c} = \overline{c}_1$ is a unit in \mathbf{F}_p . Then

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}^{r_1} \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c}_1 & \overline{d}_1 \end{pmatrix},$$

for some $\overline{d_1} \in \mathbf{F}_p$. There also exists $r_2 \in \mathbf{Z}$ such that

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^{r_2} \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}^{r_1} \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{b}_2 \\ \overline{c}_1 & \overline{d}_1 \end{pmatrix},$$

for $\overline{b}_2 \in \mathbf{F}_p$. Let $c_1, b_2 \in \mathbf{Z}$ such that $\overline{c}_1 \equiv c_1 \pmod{p}$ and $\overline{b}_2 \equiv b_2 \pmod{p}$. Then

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^{-b_2} \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}^{-c_1} \begin{pmatrix} \overline{1} & \overline{b}_2 \\ \overline{c}_1 & \overline{d}_1 \end{pmatrix} = \begin{pmatrix} \overline{1} & \\ & \overline{1} \end{pmatrix},$$

so that the matrix

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}^{-r_1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}^{-r_2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}^{c_1} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}^{b_2}$$

gets mapped reduction modulo p to the matrix A.

Alternative solution: Since $SL_2(\mathbf{F}_p)$ is generated by the matrices $\begin{pmatrix} 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 \end{pmatrix}$ from part c), and since these are in the image of the reduction map, the latter must be surjective.

e) For any positive integer $q \ge 1$, prove that the subgroups

$$\Gamma_{0}(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_{2}(\mathbf{Z}) \mid c \equiv 0 \mod q \right\},$$

$$\Gamma_{1}(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_{2}(\mathbf{Z}) \mid c \equiv 0 \mod q, \ a, d \equiv 1 \mod q \right\}$$

$$\Gamma(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_{2}(\mathbf{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod q \right\},$$

have finite index in $SL_2(\mathbf{Z})$. Compute this index when q is a prime number. (Hint: compute the size of $SL_2(\mathbf{F}_p)$.)

Solution:

First, let q = p be a prime number. We will denote $\pi_p : \operatorname{SL}_2(\mathbf{Z}) \to \operatorname{SL}_2(\mathbf{F}_p)$ the reduction modulo p map from the previous exercise. Then the group $\Gamma(p)$ is precisely the kernel of π_p . Since $\operatorname{SL}_2(\mathbf{Z})/\Gamma(p) \to \operatorname{SL}_2(\mathbf{F}_p)$ is injective and $\operatorname{SL}_2(\mathbf{F}_p)$ is finite, we have that the index $[\operatorname{SL}_2(\mathbf{Z}) : \Gamma(p)]$ is finite. Since we have the inclusions

$$\Gamma(p) \subseteq \Gamma_1(p) \subseteq \Gamma_0(p) \subseteq \mathrm{SL}_2(\mathbf{Z}),$$

we have that the subgroups $\Gamma_1(p)$ and $\Gamma_0(p)$ have finite index in $SL_2(\mathbf{Z})$ as well.

Next we will compute the index of these subgroups. From the isomorphism above we have that $[\operatorname{SL}_2(\mathbf{F}_p) : \Gamma(q)] = |\operatorname{SL}_2(\mathbf{F}_p)|$. Recall that the group $\operatorname{SL}_2(\mathbf{F}_p)$ is the kernel of the determinant homomorphism $\operatorname{GL}_2(\mathbf{F}_p) \to \mathbf{F}_q^{\times}$. The first column of the matrix can be any nonzero vector in \mathbf{F}_p^2 , which leaves us with $p^2 - 1$ choices (all vectors except the zero vector). Then the second column must be linearly independent from the first, which excludes all scalar multiples of the first column. Hence we exclude p different vectors, and are left with $p^2 - p$ possible choices, so that

$$|\operatorname{GL}_2(\mathbf{F}_p)| = (p^2 - 1)(p^2 - p).$$

Hence

$$[\operatorname{SL}_2(\mathbf{Z}):\Gamma(p)] = |\operatorname{SL}_2(\mathbf{F}_p)| = \frac{|\operatorname{GL}_2(\mathbf{F}_p)|}{|\mathbf{F}_p^{\times}|} = \frac{(p^2 - 1)(p^2 - p)}{p - 1} = p(p^2 - 1).$$

Next we will compute the index $[\Gamma_1(p) : \Gamma(p)]$. Consider the surjective homomorphism $\rho_1 : \Gamma_1(p) \to \mathbf{F}_p$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b$. Note that ρ_1 is a homomorphism since

$$\varrho_1\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\right) = \varrho_1\left(\begin{pmatrix}aa'+bc'&bd'+ab'\\ca'+dc'ⅆ'+cb'\end{pmatrix}\right) \\
= ab'+bd' \\
= b+b'+(a-1)b'+(d-1)b \equiv b+b' \pmod{p}$$

Since $\ker(\varrho_1) = \Gamma(p)$, we obtain that $[\Gamma_1(p) : \Gamma(p)] = p$. Hence

$$[\operatorname{SL}_2(\mathbf{Z}):\Gamma_1(p)] = \frac{[\operatorname{SL}_2(\mathbf{Z}):\Gamma(p)]}{[\Gamma_1(p):\Gamma(p)]} = p^2 - 1.$$

Finally we can turn to the group $\Gamma_0(p)$. Consider the surjective homomorphism $\rho_0: \Gamma_0(p) \to \mathbf{F}_p^{\times}$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d$. Note that ρ_0 is a homomorphism since

$$\varrho_0\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\right) = \varrho_0\left(\begin{pmatrix}aa'+bc'&bd'+ab'\\ca'+dc'ⅆ'+cb'\end{pmatrix}\right)$$
$$= dd'+cb' \equiv dd' \pmod{p}$$

Since $\ker(\varrho_0) = \Gamma_1(p)$, we obtain that $[\Gamma_0(p) : \Gamma_1(p)] = p - 1$. Hence

$$[\mathrm{SL}_{2}(\mathbf{Z}):\Gamma_{0}(p)] = \frac{[\mathrm{SL}_{2}(\mathbf{Z}):\Gamma_{1}(p)]}{[\Gamma_{0}(p):\Gamma_{1}(p)]} = p + 1.$$

For general integers q this is solved similarly. We can write $q = \prod_i p_i^{n_i}$, where p_i are distinct prime numbers and $n_i \in \mathbf{N}$. Then there exists a homomorphism

$$\phi_q : \operatorname{SL}_2(\mathbf{Z}) \to \prod_i \operatorname{SL}_2(\mathbf{Z}/p_i^{n_i}\mathbf{Z}),$$

from the reduction mod $p_i^{n_i}$, for all *i*. By the Chinese remainder theorem, for a positive integer *a* we have that *a* (mod *q*) is isomorphic to *a* (mod $p_i^{n_i}$) for all *i*. Hence

$$\Gamma(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}_2(\mathbf{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 \\ & 1 \end{pmatrix} \pmod{p_i^{n_i}}, \forall i \right\}.$$

Then $\Gamma(q)$ is the kernel of the homomorphism ϕ_q and the quotient $\operatorname{SL}_2(\mathbf{Z})/\Gamma(q)$ is isomorphic to a subgroup of $\prod_i \operatorname{SL}_2(\mathbf{Z}/p_i^{n_i}\mathbf{Z})$, so it is finite. Again from the inclusions $\Gamma(q) \subseteq \Gamma_1(q) \subseteq \Gamma_0(q)$ we obtain that the other subgroups have finite index as well.

- **3.** Let G be a group and let X be a set of which G acts on the left, where the action of $g \in G$ on $x \in X$ is denoted $g \cdot x$. We denote by $\mathcal{C}(X)$ the space of all functions $f: X \to \mathbb{C}$.
 - a) Show that G acts on the right on $\mathcal{C}(X)$ by

$$(f \cdot g)(x) = f(g \cdot x)$$

for $f \in \mathcal{C}(X)$, $g \in G$ and $x \in X$. Solution:

Let $f \in \mathcal{C}(X)$ be arbitrary. Then for every $x \in X$ and the identity element $e \in G$ we have

$$(f \cdot e)(x) = f(e \cdot x) = f(x)$$

Let $h \in G$ be arbitrary as well. Then

$$\begin{aligned} (f \cdot (gh))(x) &= ((f \cdot g) \cdot h)(x) \\ &= (f \cdot g)(h \cdot x) \\ &= f(g \cdot (h \cdot x)) = f((gh) \cdot x) \end{aligned}$$

b) Let $\alpha \colon G \times X \to \mathbf{C}^{\times}$ be a function. Show that defining

$$(f \bullet g)(x) = \alpha(g, x) f(g \cdot x)$$

(for $f \in \mathcal{C}(X)$, $g \in G$ and $x \in X$) defines an action of G on $\mathcal{C}(X)$ if and only if

$$\alpha(gh, x) = \alpha(h, x)\alpha(g, h \cdot x) \tag{3}$$

for all $(g,h) \in G^2$ and $x \in X$.

Solution:

Let $x \in X$ be arbitrary. Let $e \in G$ be the identity element and $g, h \in G$ arbitrary. Then

$$\begin{split} (f \bullet e)(x) &= \alpha(e, x) f(x) = f(x) \iff 1 = \alpha(e, x) \\ \iff \alpha(e, x) = \alpha(e, x) \alpha(e, x) \\ \iff \alpha(e^2, x) = \alpha(e, x) \alpha(e, e \cdot x), \end{split}$$

so (e, x) satisfies equation (3). We further have

$$\begin{aligned} \alpha(gh, x)f((gh) \cdot x) &= (f \bullet (gh))(x) \\ &= ((f \bullet g) \bullet h)(x) \\ &= \alpha(h, x)(f \bullet g)(h \cdot x) \\ &= \alpha(h, x)\alpha(g, h \cdot x)f((gh) \cdot x), \end{aligned}$$

which holds if and only if $\alpha(gh, x) = \alpha(h, x)\alpha(g, h \cdot x)$.

c) Let $\gamma \colon X \to \mathbf{C}^{\times}$ be any function. Show that

$$\alpha(g, x) = \frac{\gamma(g \cdot x)}{\gamma(x)}$$

defines a function with the property of Question b). Solution:

Let $g, h \in G$ and $x \in X$ be arbitrary. Then

$$\alpha(gh,x) = \frac{\gamma((gh) \cdot x)}{\gamma(x)} = \frac{\gamma(h \cdot x)}{\gamma(x)} \cdot \frac{\gamma(g \cdot (h \cdot x))}{\gamma(h \cdot x)} = \alpha(h,x)\alpha(g,h \cdot x),$$

so equation (3) is satisfied and by part b) we are done.

4. Let G be a group acting transitively on a non-empty set X. Let $\alpha: G \times X \to \mathbf{C}^{\times}$ be a function satisfying the relation (3) of the previous exercise. We denote again by • the corresponding action of G on $\mathcal{C}(X)$. We also denote by $\mathcal{C}(G)$ the space of functions on G.

Let *H* be a subgroup of *G*. We denote by V_H the space of $f \in \mathcal{C}(X)$ such that $f \bullet h = f$ for all $h \in H$.

a) Let $x_0 \in X$ be fixed. Let λ be the linear map

$$\lambda: V_H \to \mathcal{C}(G)$$

defined by

$$\lambda(f)(g) = f(g \cdot x_0)\alpha(g, x_0)$$

Show that λ is injective.

Solution:

We have that $f \in \mathcal{C}(X)$ is contained in the kernel of λ if and only if $\lambda(f)$ maps all elements of G to 1, i.e. $\lambda(f)(g) = 1$ for all $g \in G$. In other words, this means that $f(g \cdot x_0)\alpha(g, x_0) = 1$ for all $g \in G$. But then $f(x_0)\alpha(e, x_0) = 1$, for $e \in G$ the identity element, and since $\alpha(e, x_0) = 1$ (by Question b)) we have $f(x_0) = 1$. Since this holds for any $x_0 \in X$, it holds for all elements in X, and f is the trivial morphism. Hence the kernel of λ is just the identity and the map above is injective. b) Show that for all $f \in V_H$, the function $\tilde{f} = \lambda(f)$ satisfies

$$\widetilde{f}(hg) = \widetilde{f}(g) \tag{4}$$

for all $h \in H$ and $g \in G$. Solution: Let $f \in V_H$, $g \in G$ and $h \in H$ be arbitrary. Then

$$\begin{split} \tilde{f}(hg) &= \lambda(f)(hg) \\ &= f((hg) \cdot x_0) \alpha(hg, x_0) \\ &= f(h \cdot (g \cdot x_0)) \alpha(g, x_0) \alpha(h, g \cdot x_0) \\ &= (f \bullet h)(g \cdot x_0) \alpha(g, x_0) \\ &= f(g \cdot x_0) \alpha(g, x_0) \\ &= \lambda(f)(g) = \tilde{f}(g). \end{split}$$

c) Let K be the stabilizer of x_0 in G. Show that the map $\chi \colon K \to \mathbf{C}^{\times}$ defined by $\chi(k) = \alpha(k, x_0)$ is a group homomorphism. Solution:

Let $e \in G$ be the identity, and $g, h \in K$ arbitrary. By Question b) we have

$$\chi(e) = \alpha(e, x_0) = 1.$$

We further have

$$\chi(gh) = \alpha(gh, x_0) = \alpha(h, x_0)\alpha(g, h \cdot x_0) = \alpha(h, x_0)\alpha(g, x_0) = \chi(g)\chi(h),$$

so that χ is a group homomorphism.

d) Show that for all $f \in V_H$, the function $\tilde{f} = \lambda(f)$ also satisfies

$$\widetilde{f}(gk) = \chi(k)\widetilde{f}(g) \tag{5}$$

for all $k \in K$ and $g \in G$. Solution: Let $f \in V_H$, $k \in K$ and $g \in G$ be arbitrary. Then

$$\begin{split} \tilde{f}(gk) &= \lambda(f)(gh) \\ &= f((gk) \cdot x_0) \alpha(gk, x_0) \\ &= f(g \cdot x_0) \alpha(k, x_0) \alpha(g, k \cdot x_0) \\ &= \alpha(k, x_0) \cdot f(g \cdot x_0) \alpha(g, x_0) \\ &= \chi(k) \tilde{f}(g). \end{split}$$

e) Show that the image of λ is the set of functions $\tilde{f}: G \to \mathbb{C}$ such that (4) and (5) are valid for all $g \in G$, $h \in H$ and $k \in K$. (Hint: given a function \tilde{f} which satisfies those conditions, define explicitly a function f so that $\lambda(f) = \tilde{f}$.) Solution:

Let \tilde{f} be a function which satisfies those conditions. For $g \in G, x \in X$ we define

$$f(g \cdot x) := \frac{f(g)}{\alpha(g, x)}.$$

We will show that $\lambda(f) = \tilde{f}$. First, we need to show that f is well-defined. Let $h \in H$ be arbitrary. Then

$$(f \bullet h)(x) = \alpha(h, x)f(h \cdot x)$$

= $\alpha(h, x)\tilde{f}(h)\alpha(h, x)^{-1}$
= $\tilde{f}(h) = \tilde{f}(h \cdot e)$
= $\tilde{f}(e) = f(x),$

so that $f \in V_H$. Hence we are left to show that $\lambda(f) = \tilde{f}$. This is the case if and only if for all $g \in G$ we have

$$\lambda(f)(g) = f(g),$$

which holds since

$$f(g \cdot x_0)\alpha(g, x_0) = \frac{f(g)}{\alpha(g, x_0)}\alpha(g, x_0) = \tilde{f}(g).$$

- 5. Let $G = SL_2(\mathbf{R}), X = \mathbf{H}$ and consider the action of G on X by Möbius transformations.
 - a) Show that for any integer $k \in \mathbf{Z}$, we can define

$$\alpha\left(\begin{pmatrix}a&b\\c&d\end{pmatrix},z\right) = (cz+d)^k$$

to have an example of the situation of the two previous exercises. In what way is this related to modular forms?

Solution:

Recall that the action of G on X by Möbius transformations is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

for $z \in \mathbf{H}$.

Let $k \in \mathbf{Z}$ be arbitrary. Let $g = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $h = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$ be matrices. Then

$$\begin{aligned} \alpha(gh, x) &= \left((a_2c_1 + c_2d_1)z + b_2c_1 + d_1d_2 \right)^k \\ &= (c_2z + d_2)^k \left(\frac{(c_1a_2 + c_2d_1)z + c_1b_2 + d_1d_2}{c_2z + d_2} \right)^k \\ &= (c_2z + d_2)^k \left(c_1 \left(\frac{a_2z + b_2}{c_2z + d_2} + d_1 \right) \right)^k \\ &= \alpha(h, x)\alpha(g, h \cdot x). \end{aligned}$$

Hence α satisfies equation (3). In the context of modular forms, the function α is precisely the automorphy factor, and a weakly modular function of weight k and level 1 is a meromorphic function $f: \mathbf{H} \to \mathbf{C}$ such that for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

for all $z \in \mathbf{H}$.

b) Show that if $k \neq 0$, this function α is not of the form given by Question c) of Exercise 3.

Solution:

Let k > 0 be an integer. Assume that there is a function $\gamma: X \to \mathbf{C}^{\times}$ such that

$$\alpha(g,z) = \frac{\gamma(g \cdot z)}{\gamma(z)},$$

for all $g \in \text{SL}_2(\mathbf{R})$ and $z \in \mathbf{H}$. Then for all g in the stabilizer $\text{Stab}_{\text{SL}_2(\mathbf{R})}(z)$ we have that $\alpha(g, z) = \frac{\gamma(z)}{\gamma(z)} = 1$, for some $z \in \mathbf{H}$.

Consider $\frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \operatorname{Stab}_{\operatorname{SL}_2(\mathbf{R})}(i)$. Note that

$$\frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot i = \frac{i-1}{i+1} = \frac{(i-1)^2}{-2} = i.$$

Then we would have that

$$\alpha \left(\frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, i\right) = \left(\frac{1+i}{2}\right)^k = 1,$$

which implies that

$$\left(\frac{1+i}{\sqrt{2}}\right)^k = e^{\frac{2\pi i}{8}k} = 2^{\frac{k}{2}},$$

which is never true for any k > 0.