TOPICS IN NUMBER THEORY - EXERCISE SHEET II

École Polytechnique Fédérale de Lausanne

Exercise 1 **(Action of the modular group on the upper-half plane)**

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$ be the modular group and let $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ be the upper-half plane. Recall that Γ acts on $\mathbb{H}$ by Möbius transformations. Let also

$$D = \{z \in \mathbb{H}, |\Re(z)| < 1/2, |z| > 1\}$$

be the usual fundamental domain for the modular group Γ.

Prove that if $z, z' \in \overline{D}$, $z \neq z'$, are such that there exists $A \in \Gamma$ satisfying $z' = A \cdot z$, then either, $\Re(z) = \pm 1/2$ and $z' = z \mp 1$, or $|z| = 1$ and $z' = -1/z$.

Let $\rho = e^{2\pi i/3}$. For $z \in \overline{D}$, let

$$S(z) = \{A \in \Gamma, A \cdot z = z\}$$

be the stabilizer of z under the action of Γ. Prove that if $z \in \overline{D} \setminus \{i, \rho, -\rho^2\}$ then $S(z) = \{I_2\}$.

Let T and S be the elements of Γ respectively defined by their action on $z \in \mathbb{H}$ by $T \cdot z = z + 1$ and $S \cdot z = -1/z$. Prove that $S(i) = \{I_2, S\}$, $S(\rho) = \{I_2, ST, (ST)^2\}$ and $S(-\rho^2) = \{I_2, TS, (TS)^2\}$.

Exercise 2 **(On class numbers of positive definite quadratic forms)**

Let $D < 0$ be an integer such that $D = 0 \pmod 4$, or $D = 1 \pmod 4$. Let $\mathfrak{Q}_D$ be the set of quadratic forms

$$Q(x, y) = Ax^2 + Bxy + Cy^2$$

with coefficients $A, B, C \in \mathbb{Z}$ satisfying $B^2 - 4AC = D$, $A > 0$ and $\gcd(A, B, C) = 1$.

For $\gamma \in \Gamma$ and $Q \in \mathfrak{Q}_D$, we define

$$(\gamma \cdot Q)(x, y) = Q(ax + by, cx + dy),$$

where

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Prove that this defines an action of the modular group Γ on $\mathfrak{Q}_D$.

The number of equivalence classes under this action is called the class number of D and is denoted by $h(D)$. The goal of this exercise is to show that $h(D)$ is finite.

Steps. — (I) Prove that there is a bijection between $\mathfrak{Q}_D$ and the set

$$\left\{ \frac{-B+i\sqrt{-D}}{2A}, A, B, C \in \mathbb{Z}, B^2-4AC = D, A > 0, \gcd(A,B,C) = 1 \right\}.$$

(II) For $Q \in \mathfrak{Q}_D$, we set

$$z_Q = \frac{-B+i\sqrt{-D}}{2A}.$$

For $\gamma \in \Gamma$ and $Q \in \mathfrak{Q}_D$, check that

$$z_{\gamma \cdot Q} = \gamma^{-1} \cdot z_Q.$$

(III) Show that in each equivalence class of the action of Γ on $\mathfrak{Q}_D$, there is a unique representative whose coefficients satisfy $-A < B \leq A < C$ or $0 \leq B \leq A = C$.

(IV) Conclude.

***Exercise 3* (On the space of modular forms).** — *For $k \in \mathbb{Z}$, prove that the set of modular forms of weight $2k$ is a vector space over $\mathbb{C}$.*

Prove also that if f is a modular form of weight $2k$ and g is a modular form of weight 2ℓ then fg is a modular form of weight $2k+2\ell$.

***Exercise 4* (Elliptic functions).** — *A discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$ is called a lattice.*

An elliptic function relative to a lattice Λ is a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ which satisfies $f(z+\omega) = f(z)$ for any $z \in \mathbb{C}$ and any $\omega \in \Lambda$. All along this exercise, we let $\Lambda \subset \mathbb{C}$ be a lattice, and f be an elliptic function relative to Λ.

Prove that if f has no poles then f is constant. Prove also that if f has no zeros then f is constant.

For $z \in \mathbb{C}$, we let $\mathrm{res}_z(f)$ be the residue of f at z. Show that

$$\sum_{z \in \mathbb{C}/\Lambda} \mathrm{res}_z(f) = 0.$$

For $z_0 \in \mathbb{C}$, we let $v_{z_0}(f)$ be the order of f at z_0, that is the integer $n \in \mathbb{Z}$ such that the function $f(z)(z-z_0)^{-n}$ is holomorphic and non-zero at z_0. Show that

$$\sum_{z \in \mathbb{C}/\Lambda} v_z(f) = 0.$$

The order $\mathrm{ord}(f)$ *of f is defined by*

$$\mathrm{ord}(f) = \sum_{\substack{z \in \mathbb{C}/\Lambda \\ v_z(f) > 0}} v_z(f).$$

Show that if f is non-constant then we have

$$\mathrm{ord}(f) \geq 2.$$

Exercise 5 **(On the Weierstrass function).** — *For $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$, we define the Weierstrass $\wp_\tau$-function by*

$$\wp_\tau(z) = \frac{1}{z^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \left(\frac{1}{(z-(m\tau+n))^2} - \frac{1}{(m\tau+n)^2} \right),$$

and, for $k \geq 2$, we define the Eisenstein series $G_{2k}(\tau)$ by

$$G_{2k}(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^{2k}}.$$

All along this exercise, we view $\tau \in \mathbb{H}$ as being fixed and $z \in \mathbb{C}$ as being a variable.

Check that, for $k \geq 2$, the Eisenstein series G_{2k} converges absolutely.

Prove that the series defining the Weierstrass $\wp_\tau$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \smallsetminus \langle 1, \tau \rangle$, where

$$\langle 1, \tau \rangle = \mathbb{Z} + \tau\mathbb{Z}.$$

Prove also that it defines a meromorphic function on $\mathbb{C}$, having a double pole with residue 0 at each point of $\langle 1, \tau \rangle$, and no other pole.

Show that the Weierstrass $\wp_\tau$-function is an even elliptic function.

Prove that there is a neighborhood U of the origin such that for any $z \in U \smallsetminus \{0\}$, we have

$$\wp_\tau(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\tau) z^{2k}.$$

Finally, prove that, for any $z \in \mathbb{C} \smallsetminus \langle 1, \tau \rangle$, we have

$$\wp_\tau'(z)^2 = 4\wp_\tau(z)^3 - 60G_4(\tau)\wp_\tau(z) - 140G_6(\tau).$$

Exercise 6 **(Non-vanishing of the Discriminant on the upper-half plane)**

For $\tau \in \mathbb{H}$, we define the Discriminant $\Delta(\tau)$ by

$$\Delta(\tau) = 60^3 G_4(\tau)^3 - 27 \cdot 140^2 G_6(\tau)^2.$$

The goal of this exercise is to prove that, for $\tau \in \mathbb{H}$, we have

$$\Delta(\tau) \neq 0,$$

without using the fact that $\Delta(\tau)$ is a modular form.

Steps. —

(I) Check that $\Delta(\tau)$ is the discriminant of the polynomial

$$4X^3 - 60G_4(\tau)X - 140G_6(\tau).$$

(II) Let $\omega_1 = 1$, $\omega_2 = \tau$ and $\omega_3 = 1 + \tau$. Prove that

$$\wp_\tau'\left(\frac{\omega_i}{2}\right) = 0,$$

for $i \in \{1, 2, 3\}$.

(III) Prove that

$$\wp_\tau\left(\frac{\omega_i}{2}\right) \neq \wp_\tau\left(\frac{\omega_j}{2}\right),$$

for $i, j \in \{1, 2, 3\}$, $i \neq j$.

(IV) Conclude using Exercise 5.

To go further. — *For $\tau \in \mathbb{H}$, let E_τ be the elliptic curve defined over $\mathbb{C}$ by the Weierstrass equation*

$$y^2 = 4x^3 - 60G_4(\tau)x - 140G_6(\tau).$$

One can show that the map $\Psi : \mathbb{C}/\langle 1, \tau\rangle \to E_\tau(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ defined by

$$\Psi(z) = (\wp_\tau(z) : \wp'_\tau(z) : 1),$$

is an isomorphism of Riemann surfaces and also a group homomorphism.

To go further. — *One can prove that, for $\tau \in \mathbb{H}$, we have the Jacobi product formula*

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

where $q = e^{2\pi i\tau}$, from which we immediately deduce that $\Delta(\tau) \neq 0$.

***Exercise 7* (On the modular invariant)**. — *For $\tau \in \mathbb{H}$, we define the modular invariant $j(\tau)$ by*

$$j(\tau) = 12^3 \frac{60^3 G_4(\tau)^3}{\Delta(\tau)}.$$

Prove that a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular function of weight 0 if and only if it is a rational function of j.

***Exercise 8* (Modular forms in terms of their zeros)**

Let f be a non-zero modular form and let $z_1, \ldots, z_N$ be the zeros of f belonging to $\overline{D} \smallsetminus \{i, \rho, -\rho^2\}$ (possibly with repetitions). Prove that there exists a constant $\lambda \in \mathbb{C} \smallsetminus \{0\}$ such that, for $\tau \in \mathbb{H}$, we have

$$f(\tau) = \lambda G_4(\tau)^{v_\rho(f)} G_6(\tau)^{v_i(f)} \Delta(\tau)^{v_\infty(f)+N} \prod_{\ell=1}^{N} (j(\tau) - j(z_\ell)),$$

where $v_\rho(f)$, $v_i(f)$ and $v_\infty(f)$ respectively denote the orders of vanishing of f at ρ, i and ∞.

Pierre Le Boudec - *Spring 2016*

École Polytechnique Fédérale de Lausanne