AWS 2021: Modular Groups
Problem Set 4

Lecturer: Lori Watson
Written by: Tyler Genao, Hyun Jong Kim, Zonia Menendez and Sam Mundy (Assistants)

1 Definitions and Notations

1. Recall that we have an *extended upper half plane* $\mathcal{H}^*$, or $\mathbb{H}^*$, via adding a projective line to $\mathcal{H}$,

$$\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

   Here, we can regard our elements of $\mathcal{H} \subseteq \mathcal{H}^*$ as column vectors $\begin{bmatrix} \tau \\ 1 \end{bmatrix}$. We regard elements of $\mathbb{Q} \cup \{\infty\}$ as equivalence classes of column vectors: a rational number $a/b \in \mathbb{Q}$ is regarded as $\begin{bmatrix} a \\ b \end{bmatrix}$, and is equivalent to $\begin{bmatrix} ra \\ rb \end{bmatrix}$ for all $r \in \mathbb{Q}^\times$. We also set $\infty := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

2. Via matrix multiplication, we have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}^*$ which extends the usual action on $\mathcal{H}$: for $\gamma := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathcal{H}^*$, we set

$$\gamma \cdot \begin{bmatrix} x \\ y \end{bmatrix} := \frac{ax + by}{cx + dy}.$$

3. For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, we also have that Γ acts on $\mathcal{H}^*$. The orbits of $\mathbb{P}(\mathbb{Q})$ under Γ are called the *cusps* of Γ.

4. Let X and Y be Riemann surfaces and $f : X \to Y$ a nonconstant holomorphic map.

   Fix $x \in X$, and set $y = f(x)$. If u and t are local parameters[1] at x and y, respectively, which map x and y to the origin, then in some neighborhood of x we can express f in the form

$$t(f(z)) = a_e u(z)^e + a_{\epsilon+1} u(z)^{c+1} + \cdots, \quad a_\epsilon \neq 0$$

   for some positive integer e. This integer is independent of the choice of u and t. It is called the *ramification index* of the covering map f at x. If $e > 1$, then x is said to be a *ramified point* of f, and that y *ramifies* in X under f.

The following definitions concern a generalization of modular groups, called *Fuchsian groups.* They will be used in Problems 5, 6, 10 and 19.

5. A *Fuchsian group* is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. In particular, $\mathrm{SL}_2(\mathbb{Z})$ and all of its subgroups are Fuchsian groups.

[1] In particular, for some open subsets $U, U' \subset Y$, one has that $u : U \to \mathbb{C}$ and $t : U' \to \mathbb{C}$ are maps which are homeomorphic onto their images, and the transition maps $u \circ t^{-1} : t(U \cap U') \to u(U \cap U')$ and $t \circ u^{-1} : u(U \cap U') \to t(U \cap U')$ are both holomorphic maps.

6. A non-scalar element of α of $\mathrm{GL}_2^+(\mathbb{R})$ is called *elliptic, parabolic,* or *hyperbolic* when it satisfies

$$\mathrm{tr}(\alpha)^2 < 4\det(\alpha), \quad \mathrm{tr}(\alpha)^2 = 4\det(\alpha), \quad \text{or} \quad \mathrm{tr}(\alpha)^2 > 4\det(\alpha)$$

respectively.

7. A Fuchsian group Γ acts on $\mathcal{H} \cup \mathbb{R} \cup \{\infty\}$ via linear fractional transformations. One can show that an element $\alpha \in \Gamma$ is:
   - elliptic if and only if α has fixed points z_0 and $\overline{z}_0$ for some $z_0 \in \mathcal{H}$;
   - parabolic if and only if α has a unique fixed point on $\mathbb{R} \cup \{\infty\}$;
   - hyperbolic if and only if α has two distinct fixed points on $\mathbb{R} \cup \{\infty\}$.

8. Fix a Fuchsian group Γ, and let $z \in \mathcal{H} \cup \mathbb{R} \cup \{\infty\}$. We call z an *elliptic point*, *parabolic point*, or *hyperbolic point* of Γ if there is some elliptic/parabolic/hyperbolic element of Γ fixing z, respectively.

9. Fix a Fuchsian group Γ.
   - Let P_Γ denote the set of parabolic points of Γ. Elements of P_Γ are sometimes called *cusps* of Γ.
   - The space $\mathcal{H}^*$ denotes $\mathcal{H} \cup P_\Gamma$.
   - The space $X(\Gamma)$ denotes the quotient space $\Gamma\backslash\mathcal{H}^*$.

10. Fix a Fuchsian group Γ, and let $\pi : \mathcal{H}^* \to \Gamma\backslash\mathcal{H}^* = X(\Gamma)$ be the quotient map. A point $a \in X(\Gamma)$ is called an *elliptic point* or a *cusp*, respectively, when there is a lift $z \in \mathcal{H}^*$ of a that is either an elliptic point or a cusp for Γ. When a is neither an elliptic point nor a cusp, it is called an *ordinary point*.

2 Introductory Problems

Problem 1. Determine the stabilizers of i, ζ_3 and ∞ under $\mathrm{SL}_2(\mathbb{Z})$, where $\zeta_3 := \frac{-1+\sqrt{-3}}{2}$.

Problem 2.

a. Prove that $\mathrm{SL}_2(\mathbb{Z})$ has exactly one cusp.

b. Show that any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ has finitely many cusps.

Problem 3. $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ properly discontinuously. In other words, for any two points x, y of $\mathcal{H}$, there exist neighborhoods U and V of x and y, respectively, such that $\#\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma U \cap V \neq \emptyset\} < \infty$. Convince yourself that this is the case.

Problem 4.

1. Show that $\mathbb{C}$ is a Riemann surface.
2. At what points is the map $\mathbb{C} \to \mathbb{C}, z \mapsto z^2$ ramified?

Problem 5. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$ be a non-scalar element. Show that the listed definitions for α to be elliptic/parabolic/hyperbolic are indeed equivalent.

Problem 6. Let Γ be a Fuchsian group and $\alpha \in \Gamma$ a non-scalar element.

1. Show that if α is an elliptic/parabolic/hyperbolic element of Γ, then for any $\gamma \in \Gamma, \gamma\alpha\gamma^{-1}$ is also an elliptic/parabolic/hyperbolic element, respectively.
2. How do the fixed points of α and $\gamma\alpha\gamma^{-1}$ compare?

Problem 7. Show that homothetic lattices have equal j-invariants.

Problem 8. The j-function has a Laurent series expansion in terms of $q := e^{2\pi i\tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864229970q^3 + 20245856256q^4 + 333202640600q^5 + \dots$$

By the theory of complex multiplication, one has for imaginary quadratic $\tau \in \mathcal{H}$ that $j(\tau)$ is an algebraic integer. Assuming that $j(\frac{1+\sqrt{-163}}{2}) \in \mathbb{Z}$, use this j-function expansion to show that $e^{\pi\sqrt{163}}$ is very close to an integer.

3 Intermediate Problems

Problem 9 (Diamond & Shurman, Exercise 3.1.4)**.** Show that for a prime $p \in \mathbb{Z}^+$, $\Gamma_0(p)$ has exactly two cusps.

Problem 10.

a. Show that every elliptic element of $\mathrm{SL}_2(\mathbb{Z})$ is of order dividing 4 or 6.

b. What elements of $\mathrm{SL}_2(\mathbb{Z})$ represent the conjugacy classes of elliptic elements?

c. What are the elliptic points of $\mathrm{SL}_2(\mathbb{Z})$?

Problem 11 (Miyake, Lemma 1.7.1)**.** Let G be a topological group acting continuously on X. Assume that for any two points x, y of X, there exist neighborhoods U of x and V of y such that $gU \cap V = \emptyset$ for all $g \in G$ satisfying $x \neq y$. Show that $G\backslash X$ is a Hausdorff space.

Problem 12.

1. Show that the projective line $\mathbb{CP}^1 := \mathbb{P}^1(\mathbb{C})$ is a Riemann surface.
2. There is a map $\mathbb{CP}^1 \to \mathbb{CP}^1$ given by $[s : t] \mapsto [s^2 : t^2]$. Where is this map ramified, and what ramification indices does it have at those points?
3. Do the same for the map $\mathbb{CP}^1 \to \mathbb{CP}^1$ given by $[s : t] \mapsto [s^2(s-t) : t^3]$.

Problem 13 (Cyclic isogenies)**.** Let $\mathbb{C}/\Lambda$ be a complex elliptic curve. An isogeny $\varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is called *cyclic* if its kernel $\{z + \Lambda_1 \in \mathbb{C}/\Lambda_1 : z \in \Lambda_2\}$ is a cyclic subgroup of $\mathbb{C}/\Lambda_1$.

a. Show that a cyclic subgroup $C \subseteq \mathbb{C}/\Lambda$ induces a cyclic isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/C_0$ with kernel C for some superlattice[2] C_0 of Λ.

b. Show that any isogeny $\varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ factors as a multiplication-by-n map followed by a cyclic isogeny.

The following four exercises are related to (complex) elliptic curves with complex multiplication, see Problem 11 of Problem Set 3.

Problem 14. Recall that an *order* $\mathcal{O}$ of a number field K is a subring of the ring of integers $\mathcal{O}_K$ of equal $\mathbb{Z}$-rank. Equivalently, $\mathcal{O}$ is a subring of $\mathcal{O}_K$ with its own $\mathbb{Z}$-basis of algebraic integers. One has that the index $[\mathcal{O}_K : \mathcal{O}] < \infty$.

a. Show that an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with squarefree $d \in \mathbb{Z}^+$ has the form

$$\mathcal{O} = [1, f\omega_K]$$

where

$$\omega_K := \begin{cases} \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \pmod 4 \\ \sqrt{-d} & \text{if } d \equiv 1, 2 \pmod 4 \end{cases}$$

and $f = [\mathcal{O}_K : \mathcal{O}]$.

b. Show that for each integer $f \in \mathbb{Z}^+$, the lattice $\mathcal{O}_f := [1, f\omega_K]$ is an order of K with index f in $\mathcal{O}_K$.

Problem 15. Let $\mathbb{C}/\Lambda$ be a complex elliptic curve with CM. Then its endomorphism ring $\mathcal{O} := \mathrm{End}(\mathbb{C}/\Lambda)$ is an order in an imaginary quadratic number field K.

For an endomorphism $\alpha \in \mathrm{End}(\mathbb{C}/\Lambda)$, we write $(\mathbb{C}/\Lambda)[\alpha]$ for its kernel $\ker \phi_\alpha = \alpha^{-1}\Lambda/\Lambda$. We call this the *$\alpha$-torsion subgroup* of $\mathbb{C}/\Lambda$.

Let us assume the following fact: as $\mathcal{O}$-modules, we have for $\alpha \in \mathrm{End}(\mathbb{C}/\Lambda)$ that

$$(\mathbb{C}/\Lambda)[\alpha] \cong_{\mathcal{O}} \mathcal{O}/\alpha\mathcal{O}.$$

Then show that the degree of an endomorphism $\alpha \in \mathrm{End}(\mathbb{C}/\Lambda)$ is the absolute value of its field-theoretic norm, $\deg(\phi_\alpha) = |\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)|$.

[2] A *superlattice* of Λ is less fun than it sounds: it is just a lattice which contains Λ. Compare this word to sublattice.

Problem 16. Show that for two isogenous complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$, $\mathbb{C}/\Lambda_1$ has CM iff $\mathbb{C}/\Lambda_2$ has CM.

Problem 17.

a. Show that if a lattice $\Lambda \subseteq \mathbb{C}$ is homothetic to its complex conjugate $\overline{\Lambda}$, then $j(\Lambda) \in \mathbb{R}$. (In fact, this is if and only if.)

b. Show that if $\mathcal{O}$ is an order in an imaginary quadratic number field, then $j(\mathcal{O}) \in \mathbb{R}$.

c. Conclude that for any imaginary quadratic order $\mathcal{O}$, there is some complex elliptic curve $\mathbb{C}/\Lambda$ with CM by $\mathcal{O}$ and whose j-invariant is a real number. (*Hint:* assume that Problem 11.c on Problem Set 3 works if we replace $\mathcal{O}_K$ with $\mathcal{O}$.)

4 Advanced Problems

Problem 18. Let $f : X \to Y$ be a nonconstant holomorphic map of compact Riemann surfaces.

a. Show that f is surjective.

b. Show that f has finite fibers: that is, for all $y \in Y$ one has $\#f^{-1}(y) < \infty$.

Note that there is analogous statement in algebraic geometry: any nonconstant morphism $\phi : C_1 \to C_2$ of projective algebraic curves is surjective and has finite fibers.

Problem 19. This problem will construct a Fuchsian group which has no cusps.

a. Consider the following real 2 by 2 matrices:

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \beta = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}, \qquad \gamma = \frac{1}{2}(1 + \alpha + \beta + \alpha\beta).$$

(In the definition of γ, the element 1 is being used to denote the identity matrix.) Show that

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$$

is a (noncommutative but unital) subring of the ring $M_2(\mathbb{R})$ of 2 by 2 real matrices. This is a *quaternion algebra*, as the elements α and β satisfy

$$\alpha^2 = -1, \qquad \beta^2 = 3, \qquad \alpha\beta = -\beta\alpha.$$

b. Consider the *conjugation* on $\mathcal{O}$ given for any element of the form

$$a = a_0 + a_1\alpha + a_2\beta + a_3\alpha\beta \in \mathcal{O}$$

by

$$\bar{a} = a_0 - a_1\alpha - a_2\beta - a_3\alpha\beta.$$

Show that conjugation $a \mapsto \bar{a}$ defines a ring automorphism of $\mathcal{O}$.

c. For any $a \in \mathcal{O}$, show that

$$a + \bar{a} = \mathrm{tr}(a), \qquad a\bar{a} = \det(a).$$

Here, tr and det are the usual trace and determinant operations on matrices.

d. Let

$$\mathcal{O}_1 = \{a \in \mathcal{O} : a\bar{a} = 1\}.$$

Show that $\mathcal{O}_1$ is a Fuchsian group with no cusps. (*Hint:* Write a as in part b., and write down the condition that a would satisfy if it were parabolic explicitly in a_0, a_1, a_2, a_3. Then do a "descent" procedure by looking modulo 3.)

One can use this problem to show that $\mathcal{O}_1 \backslash \mathcal{H}$ is a compact Riemann surface.