The Modular Group $SL_2(\mathbb{Z})$ and its congruences subgroups

Topics covered : Bump's section 1.2 (The Modular Group) and Exercises 1.2.7 to 1.2.11

1. Notation

Let $\mathcal{H}$ denote the upper half place, i.e. $\{z = x + iy \in \mathbb{C} | y > 0\}$. Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of matrices $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1, a, b, c, d \in \mathbb{Z}\}$. We use the notation $\Re$ and $\Im$: $\Re(z) + i\Im(z) = x + iy = z \in \mathbb{C}$.

2. The Modular Group

2.1. Motivation. Automorphic functions for a group Γ are functions on $\Gamma\backslash\mathcal{H}$. We want to study functions that transform a bit differently under the action of discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$, called *automorphic forms*, such that the ratio of any two of them (of same weight) will yield an automorphic function.

DEFINITION 2.1. A modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ is a holomorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ such that :

$$f(\gamma(z)) = (cz + d)^k f(z), \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

plus the requirement of holomorphicity at ∞ (the Fourier coefficents $a_n = 0 \ \forall n < 0$).

2.2. $\mathrm{SL}_2(\mathbb{Z})$**...** The group $G = \mathrm{SL}_2(\mathbb{R})$ acts on the upper half plane via fractional linear transformations :

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \mapsto \gamma(z) = \frac{az + b}{cz + d}.$$

This action is not faithful since $-I$ and I have the same effect; we thus need to mod out by $\{\pm I\}$ (i.e. consider $\overline{\Gamma} := \Gamma/\Gamma \cap \{\pm 1\}$) if we require faithfulness.
In a similar fashion, $\mathrm{SL}_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$, and the subgroup of $\mathrm{SL}_2(\mathbb{C})$ fixing $\mathcal{H}$ is $\mathrm{SL}_2(\mathbb{R})$.
The action on $\mathcal{H}$ is transitive: the subgroup of upper triangular matrices act transitively:

$$\begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix} : i \mapsto x + iy.$$

The stabilizer G_i of i is the special orthogonal group

$$S0_2(\mathbb{R}) := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a^2 + b^2 = 1\}.$$

By generalities on transitive group actions, $G/G_i = \mathrm{SL}_2(\mathbb{R})/S0_2(\mathbb{R}) \cong \mathcal{H}$.

DEFINITION 2.2. The group $\Gamma(N)$ is

$$\{\mathrm{SL}_2(\mathbb{Z}) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}.$$

For example, $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$. Since $\Gamma(N) = \mathrm{Ker}(\Gamma(1) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$, $\Gamma(N)$ is a normal subgroup of finite index.

DEFINITION 2.3. A group $\Gamma \subset G$ acts discontinuously if for all compact $K_1, K_2 \subset \mathcal{H}$, $|\{\gamma \in \Gamma | K_2 \cap \gamma(K_1) \neq \emptyset\}| < \infty$.

PROPOSITION 2.4. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *acts discontinously on* $\mathcal{H}$.

PROOF. Let K_1, K_2 be two compact subsets of $\mathcal{H}$. There exists $\epsilon > 0$ such $\Im(w) > \epsilon\ \forall w \in K_2$. Fix $z = x + iy \in K_1$. Since $(c,d) \mapsto |cz+d|^2$ is a positive definite quadratic form, $\Im(\gamma(z)) = \frac{y}{|cz+d|^2} < \epsilon$ outside a big enough square $|c|, |d| < R(z)$. Because K_1 is compact, $R = max_{z\in K_1} R(z) < \infty$ and $K_2 \cap \gamma(K_1) = \emptyset$ unless $|c|, |d| < R$. This proves there are only finitely many bottom rows $(c\ d)$ of matrices $\gamma \in SL_2(\mathbb{Z})$ such that $K_2 \cap \gamma(K_1) \neq \emptyset$. It remains to show that given c, d, there are only finitely many γ with bottom row $(c\ d)$ such that $K_2 \cap \gamma(K_1) \neq \emptyset$. If γ_1 and γ_2, share a bottom row, then $\gamma_1^{-1} \circ \gamma_2$ is of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for $n \in \mathbb{Z}$; this matrix correspond to a translation $z \mapsto z + n$. For fixed γ_1, there can be only finitely such translations such that $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma_1(K_1) \cap K_2 \neq \emptyset$.

□

DEFINITION 2.5. A *fundamental domain* for Γ is an connected domain F such that

- $\forall z \in \mathcal{H}$, there exists $\gamma \in \Gamma$ such that $\gamma(z) \in \overline{F}$;
- if $z_1, z_2 \in F$ and $\gamma(z_1) = z_2$ for some $\gamma \in \Gamma$, then $z_1 = z_2$ and $\gamma = \pm I$.

PROPOSITION 2.6. *The region* $\{z \in \mathcal{H} | |z| > 1, |\Re(z)| < \frac{1}{2}\}$ *is a fundamental domain for* $\Gamma(1)$.

PROOF. Pick $z \in \mathcal{H}$, since $(c,d) \mapsto |cz+d|^2$ is a positive definite quadratic form, it has minimum value for integers c, d satisfying $(c,d) = 1$; thence $\Im(\gamma(z))$ has a maximum value for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We can find $n \in \mathbb{Z}$ such that $\gamma(z) + n$ has real part smaller or equal to $\frac{1}{2}$. In fact, $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \gamma \in \mathrm{SL}_2(\mathbb{Z})$ (with the same bottom row as γ is in $\mathrm{SL}_2(\mathbb{Z})$ and produces this effect, hence $|\Re(z)| \leq \frac{1}{2}$. This implies $|\Im(\gamma(z))| \geq 1$, otherwise we contradict maximality by taking $\gamma_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \gamma, |\Im(\gamma_1(z))| = \frac{|\Im(\gamma(z))|}{|\gamma(z)|^2}$, thus Property 1 is established.

Let $z = x + iy \in F, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $w = \gamma(z) \in F$. If $c = 0$, then $\gamma = \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for some $n \in \mathbb{Z}$, and $z, \gamma(z) \in F$ implies that $n = 0$, so $z = \gamma(z)$. Assume $c \neq 0$. Then a little geometric argument indicates that $\Im_{f\in F}(f) \geq \frac{\sqrt{3}}{2}$, also, $|cz+d| \geq cy$. These two estimates imply that :

$$\frac{\sqrt{3}}{2} < \Im(\gamma(z)) = \frac{y}{|cz+d|^2} \geq \frac{1}{c^2 y} < \frac{2}{c^2\sqrt{3}},$$

hence $c^2 < \frac{4}{3}$ and $c = \pm 1$ (0 being excluded).

Suppose $c = \pm 1$. Since γ and $-\gamma$ have the same action on $\mathcal{H}$, take without loss of generality $c = 1$. Then a little computation show that

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}.$$

Let $z_1 = z + d$, $w_1 = w - a$. Since $|\Re(z)| < \frac{1}{2}$, we have $|z_1| \geq |z| > 1$, and similarly $|w_1| > 1$, yet $w_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z_1$. Since $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is the transformation $z \mapsto -\frac{1}{z}$ and maps the circle inside out, we get a contradiction.

□

REMARK 2.7. It can be shown that every discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ has a fundamental domain.

Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Note that corresponding transformations are $z \mapsto -\frac{1}{z}$ and (resp.) $z \mapsto z+1$.

PROPOSITION 2.8. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* S *and* T.

PROOF. Clearly, $< S, T > \subseteq \mathrm{SL}_2(\mathbb{Z})$. We thus need to show equality. Since $S^2 = -I$, it is enough to compute in the projectivized groups (modulo $\{\pm I\}$). Let $\gamma \in \Gamma(1)$: we will decomposed γ in a product of S, T, T^{-1}. Note that we identify A and $-A$. Let F be the fundamental domain of $\Gamma(1)$. Then

$$\mathcal{H} = \cup_{\gamma \in \Gamma(1)} \overline{\gamma(F)},$$

such that the interior of the $\gamma(F)$ are disjoint. Hence there are $\gamma_1, \ldots, \gamma_n \in \Gamma(1)$ such that $\gamma_1(F) = F$ and $\gamma_n(F)$, and each $\gamma_k(F)$ is adjacent to $\gamma_{k+1}(F)$. Note that the adjacent domains to F are $T(F), T^{-1}(F)$ and $S(F)$. Since $\gamma_{k+1}(F)$ and $\gamma_k(F)$ are adjacent, it follows that $\gamma_k^{-1}\gamma_{k+1}(F)$ is adjacent to F, hence $\gamma_k^{-1}\gamma_{k+1}$ is T, T^{-1} or S. Since $\gamma = \prod \gamma_k^{-1}\gamma_{k+1}$, we are done. □

REMARK 2.9. The same trick to determine generators can be applied for any discrete group, once the fundamental domain has been *explicitly* given.

2.3. ... and its congruence subgroups. We can view $\mathcal{H} \subset \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \infty$, hence the topological boundary of $\mathcal{H}$ is $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \infty$.

DEFINITION 2.10. Let Γ act discontinously on $\mathcal{H}$. The *quotient space* $\Gamma \backslash \mathcal{H}$ is composed of the orbits under the action of Γ.

The quotient topology on $\Gamma \backslash \mathcal{H}$ is given by:

$$U \subset \Gamma\backslash\mathcal{H} \text{ is open iff } \pi^{-1}(U) \text{ is open, for } \pi : \mathcal{H} \longrightarrow \Gamma\backslash\mathcal{H}.$$

FACT 2.11. The space $\Gamma \backslash \mathcal{H}$ is Hausdorff (this is assured by the discontinuity of the group action on $\mathcal{H}$).

The cusps, intuitively speaking, are the points at which the *fundamental domain* of the group Γ touch the boundary of $\mathcal{H}$.

Note that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$, hence a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of finite index can only have finitely many orbits. In particular, $\mathrm{SL}_2(\mathbb{Z})$ has only one orbit (∞).

DEFINITION 2.12. An orbit of Γ in $\mathbb{P}^1(\mathbb{Q})$ is called a *cusp* .

The cusps are used to compactify $\Gamma \backslash \mathcal{H}$ (not the fundamental domain!!) by adding one point for every cusp, in order to obtain a compact Riemann surface at the end of the day.

In particular, adding ∞ to $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ will yield a compact Riemann surface of genus 0.

REMARK 2.13. When is $\Gamma\backslash\mathcal{H}^*$ a compact Riemann surface ? A *Fuchsian group of the 1st kind* is a discrete subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ (or of $\mathrm{SL}_2(\mathbb{R})/\pm 1$) such that $\Gamma\backslash\mathcal{H}^*$ is compact.

We have the following :

PROPOSITION 2.14. [**1**, Proposition 1.32] *If* $\Gamma\backslash\mathcal{H}^*$ *is compact, then the number of* Γ*-inequivalent cusps is* finite.

Two subgroups Γ and Γ' of a group G are said to be commensurable if $\Gamma \cap \Gamma'$ is of finite index in Γ and in Γ'.

PROPOSITION 2.15. [**1**, Proposition 1.31] *If* Γ, Γ' *are commensurable, then* $\Gamma\backslash\mathcal{H}^*$ *is compact iff* $\Gamma'\backslash\mathcal{H}^*$

If Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ commensurable with $\mathrm{SL}_2(\mathbb{Z})$, then $\Gamma\backslash\mathcal{H}^*$ is compact.

A possible source of confusion is that adding cusps gives a compact Riemann surface only if $\Gamma\backslash\mathcal{H}$ is of finite volume under the $\mathrm{SL}_2(\mathbb{R})$-invariant measure $\frac{1}{|y^2|}dxdy$, and it is clearly possible to take Γ small enough so the volume of $\Gamma\backslash\mathcal{H}$ is infinite.
Thus we topologize $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

If $a \in \mathcal{H}$, just pick a usual neighborhood (in the Euclidean topology). If $a = \infty$, take for a neighborhood basis $\infty \cup \{z|\Im(z) > c\}$ for $0 \leq c \in \mathbb{R}$. If $a \in \mathbb{Q}$, take for a neighborhood basis $a\cup$ the interior of a tangent circle to the real line at a. Note that a fractional linear transformation mapping a to ∞ will map the circle to a horizontal line, and vice-versa.

We give $\Gamma\backslash\mathcal{H}^*$ the quotient topology, and we obtain a manifold.

FACT 2.16. The manifold $\Gamma\backslash\mathcal{H}^*$ is Hausdorff and locally compact.

We proceed to define a complex structure on it (we shall use the nomenclature of elliptic, hyperbolic and parabolic elements and elliptic fixed point: look up Exercises 1.2.7 and 1.2.8 for more information) by giving charts around each point.

- If $a \in \mathcal{H}$ is not elliptic, the usual chart on the upper half place will do.
- If a is elliptic, then we use the transform $\phi = \frac{z-a}{z-\overline{a}}$ to map $\mathcal{H}$ to the unit disc $\mathbb{D}$.

  FACT 2.17. The group $\Gamma(N)$, for $N > 1$, does *not* contain elliptic elements.
  By Schwarz's Lemma, the stabilizer of a is mapped to the cyclic group generated by a rotation of angle $\frac{2\pi}{n}$ by conjugating with ϕ. Let w be the coordinate function on $\mathbb{D}$, then the map $z \mapsto w^n$ maps a neighborhood of $a \in \Gamma\backslash\mathcal{H}^*$ homeomorphically to a neighborhood of 0 in $\mathbb{C}$.
- If a is a cusp, we can pick $\rho \in \mathrm{SL}_2(\mathbb{Z})$ to send a to ∞. Let $\overline{\Gamma_a}$ be the stabilizer of $a \in \overline{\Gamma}$. Then $\overline{\rho\Gamma\rho^{-1}}$ is a subgroup of finite index in $\overline{\Gamma(1)}$¡ and the stabilizer of ∞ is $\overline{\rho\Gamma_a\rho^{-1}}$. Hence this is a subgroup of finite index in the stabilizer of infinity in $\mathrm{SL}_2(\mathbb{Z})$, which is generated by $z \mapsto z+1$, hence $\overline{\rho\Gamma_a\rho^{-1}}$ is generated by $z \mapsto z+n$. The map $z \mapsto e^{2\pi i\rho(z)/n}$ maps a neighborhood of $a \in \Gamma\backslash\mathcal{H}^*$ homeomorphically onto a neighborhood of 0 in $\mathbb{C}$.

This completes the description of the complex structure. The manifold $\Gamma\backslash\mathcal{H}^*$ is thus a compact Riemann surface.

3. Exercises

Exercise 1.2.7

Solution : Put γ in Jordan canonical form: the possible matrices are

$$\begin{pmatrix} \gamma & 1 \\ 0 & \gamma \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \gamma & 0 \\ 0 & \mu \end{pmatrix}, \gamma \neq \mu.$$

In the first case, if $\gamma^2 = 1$, then $\gamma = \pm 1$, and the trace is ± 2. In the second case, $\gamma\mu = 1$. If $\pm 1 \neq \gamma \in \mathbb{R}$, then $\gamma + \frac{1}{\gamma} > 2$ by the arithmetic-geometric inequality. If $\gamma \in \mathbb{C}\backslash\mathbb{R}$, then $\mu = \overline{\gamma}$ (both being roots of the same quadratic equation) and $|\gamma + \overline{\gamma}| = 2Re(\gamma) < 2$.

Note that any γ has two fixed points (with multiplicity). We will cover all cases in two strokes :

- For every $z \in \mathcal{H}$, take $\tau \in \mathrm{SL}_2(\mathbb{R})$ such that $\tau(i) = z$. Then
$$\tau \cdot SO_2(\mathbb{R})\tau^{-1} = \{\alpha \in \mathrm{SL}_2(\mathbb{R}) | \alpha(z) = z\}.$$
All elements in $S0_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a^2 + b^2 = 1\}$ have eigenvalues of norm 1, hence an element with one fixed point in $\mathcal{H}$ must of trace ± 2 or of trace small than 2.
- For $r \in \mathbb{R} \cup \infty$, look at :
$$F(r) = \{\alpha \in SL_2(\mathbb{R}) | \alpha(r) = r\},$$
$$P(r) = \{\alpha \in F(r) | \alpha \text{ parabolic or } \pm 1\}.$$
Since $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{R} \cup \infty$, there exists $\sigma \in \mathrm{SL}_2(\mathbb{R})$ so that $\sigma(\infty) = r$. But
$$F(\infty) = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} | a \in \mathbb{R}^\times, b \in \mathbb{R}\},$$
$$P(\infty) = \{\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} | h \in \mathbb{R}\},$$
thence if $\sigma \neq \pm 1$ has a fixed point in $\mathbb{R}$, its trace is greater or equal than 2.

Note that the only $\gamma \in \mathrm{SL}_2(\mathbb{R})$ of trace 2 fixing a point in $\mathcal{H}$ are $\pm I$, so the trichotomy is established.

Exercise 1.2.8 a) Note that
$$\begin{pmatrix} \gamma & 1 \\ 0 & \gamma \end{pmatrix}^n = \begin{pmatrix} \gamma^n & n\gamma^{n-1} \\ 0 & \gamma^n \end{pmatrix},$$
$$\begin{pmatrix} \gamma & 0 \\ 0 & \mu \end{pmatrix}^n = \begin{pmatrix} \gamma^n & 0 \\ 0 & \mu^n \end{pmatrix}.$$
If there is a $n \in \mathbb{N}$ such that $\gamma^n = \mu^n = 1$, then $|\gamma + \mu| < 2$, hence the element $\gamma \in \mathrm{SL}_2(\mathbb{R})$ is elliptic. If γ is elliptic, then γ^n is elliptic or ± 1; but $\{\gamma \in \Gamma | \gamma z = z\}$ is finite : take $g \in \mathrm{SL}_2(\mathbb{R})$ such that $g \cdot i = z$. Then $g^{-1}\gamma g \cdot i = i$ hence $\{\gamma \in \Gamma : \gamma z = z\} = gSO_2(\mathbb{R})g^{-1} \cap \Gamma$. Since $S0_2(\mathbb{R})$ is compact and Γ is discrete (Γ acting discontinuously), the intersection is finite.

b) Pick σ elliptic in $\mathrm{SL}_2(\mathbb{Z})$, $tr(\sigma) < 2$ hence $tr(\sigma) \in \{0, \pm 1\}$. so the characteristic polynomial is either $x^2 + 1$ or $x^2 \pm x + 1$, so $\sigma^4 = 1$ or $\sigma^6 = 1$ (i.e. $\sigma^3 = \pm 1$, but if $(\sigma)^3 = 1$ if $\sigma^3 = -1$) hence we need only look at $\sigma^4 = 1$ or $\sigma^3 = 1$. In $\overline{F}$, only i and the non-real third root of unity fit either one of these. The orbits are clearly disjoint (F is a fundamental domain).

Exercise 1.2.9

If Γ has no parabolic element, then $\mathcal{H} = \mathcal{H}^*$ and $\Gamma \backslash \mathcal{H}$ is compact .

Suppose $\Gamma \backslash \mathcal{H}$ is compact. Let $\pi : \mathcal{H} \longrightarrow \Gamma \backslash \mathcal{H}$. Suppose ∞ is a cusp. Take an infinite sequence of points $\{z_n\} \subset \mathcal{H}$ such that $\Im(z_n) \longrightarrow \infty$.

We find the proofs of the following lemmas in [**1**].

LEMMA 3.1. *For every cusp of* Γ*, there is a neighborhood* U *of* s *in* $\mathcal{H}^*$ *such that*
$$\Gamma_s = \{\sigma \in \Gamma | \sigma(U) \cap U \neq \emptyset\}.$$

LEMMA 3.2. *For every cusp* s *of* Γ*, for every compact* K *of* $\mathcal{H}$*, there is a neighborhood* U *of* s *such that* $U \cap \gamma(K) = \emptyset \forall \gamma \in \Gamma$.

Then the first lemma tells us that there is a neighborhood $U = \{z \in \mathcal{H}^8 | \Im(z) > c\}$ of ∞ such that $\Gamma_\infty = \{\gamma \in \Gamma | \gamma(U) \cap U \neq \emptyset\}$. Then $z_n \in U$ for $n >> 0$. Since no elements of Γ_∞ modifies $\Im(z)$, if two points have distinct and sufficiently large imaginary parts, then they are not Γ-equivalent. Therefore $\{\pi(z_n)\}$ contains a sequence of infinitely many distinct points of $\Gamma\backslash\mathcal{H}$. If $\Gamma\backslash\mathcal{H}$ is compact, there is a $w \in \mathcal{H}$ such that $\pi(w)$ is a limit point of $\{\pi(z_n)\}$. Let K be a compact neighborhood of w. By the second lemma, there is a neighborhood V of ∞ such that $K \cap \Gamma V = \emptyset$. Since $\pi(z_n) \in \pi(K) \cap \pi(V)$ for $n >> 0$, we get a contradiction.

Exercise 1.2.10

If $\gamma(a) = a, \gamma \in \mathrm{SL}_2(\mathbb{R})$, then a is the unique solution of a quadratic equation with rational coefficients, hence $a \in \mathbb{Q}$. The other direction follows from the definition.

Exercise 1.2.11

PROPOSITION 3.3. *An ideal class in $K = \mathbb{Q}(\epsilon)$ uniquely determines a conjugacy class in $\mathrm{GL}_2(\mathbb{Z})$ of matrices with eigenvalue γ (and determinant 1).*

PROOF.

LEMMA 3.4. *Let I be an ideal, (a_1, a_2) a $\mathbb{Z}$-basis of I. Let γ be a unit of norm 1. Then there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$A \circ (a_1, a_2)^t = \gamma(a_1, a_2)^t.$$

PROOF. If γ is a unit, then $(\gamma a_1, \gamma a_2)$ is a $\mathbb{Z}$-basis of I, hence there is a matrix $A \in \mathrm{GL}_2(\mathbb{Z})$ taking $(a_1, a_2)^t$ to $(\gamma a_1, \gamma a_2)^t$. But γ satisfies a quadratic equation, hence $\overline{\gamma}$ is also an eigenvalue, so $\gamma\overline{\gamma} = 1 = det(A)$. □

LEMMA 3.5. *Take another base (w_1, w_2) of I. Then there is a matrix $B \in \mathrm{SL}_2(\mathbb{Z})$ conjugate by $g \in \mathrm{GL}_2(\mathbb{Z})$ to A.*

PROOF. If a_1, a_2 and w_1, w_2 are bases, then there is a matrix $C \in \mathrm{GL}_2(\mathbb{Z})$ such that $C \circ (w_1, w_2)^t = (a_1, a_2)^t$. Put $B = C^{-1}AC$; thus $B \circ (w_1, w_2)^t = C^{-1}AC(w_1, w_2)^t = C^{-1}A \circ (a_1, a_2)^t = C^{-1} \circ \gamma(a_1, a_2)^t = \gamma C^{-1}(a_1, a_2)^t = \gamma(w_1, w_2)^t$. □

If w_1, w_2 is a basis of I, and J is in the same class as I, there is a constant k such that kw_1, kw_2 is a basis of J, hence by the first lemma, (kw_1, kw_2) is an eigenvector of A. We may just take w_1, w_2 to represent the whole ideal class, and all is left to prove is the converse of the second lemma : if $B = D^{-1}AD, D \in \mathrm{GL}_2(\mathbb{Z})$, then B and A correspond to the same ideal class. But $B = C^{-1}AC$ with eigenvalue γ is exactly $C^{-1}(a_1, a_2)^t$ and $C^{-1}(a_1, a_2)^t$ also has entries which are a basis of I.

□

REMARK 3.6. If we take $\mathrm{SL}_2(\mathbb{Z})$-conjugacy classes instead of $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes, we obtain the narrow class number.

Bibliography

[1] Shimura, Goro, *Introduction to the arithmetic theory of automorphic functions*. Kano Memorial Lectures, No. **1**. Publications of the Mathematical Society of Japan, No. **11**. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. xiv+267 pp.