Richard Hain October 3, 2013

Math 501
Project #1

Due: Tuesday, November 5, 2013

The goal of this project is to show that $\mathrm{SL}_2(\mathbb{Z})$ has the following presentation:

$$\mathrm{SL}_2(\mathbb{Z}) \cong \langle s, u : s^2 = u^3,\ s^4 = u^6 = 1 \rangle. \tag{1}$$

You can find background material on free groups and presentations on pages 215–220 of Dummit and Foote.

Group project. This is a group[1] project. Your group can have any positive number of elements. You are welcome to seek help from us.

You are going to establish this presentation by studying the action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of equivalence classes of *positively framed lattices* in $\mathbb{C}$. There are lots of words here, so let's understand them one by one. You know what a lattice in $\mathbb{C}$ is. Two complex numbers ω_1, ω_2 comprise a framing of a lattice Λ if

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2.$$

Note that the framing determines the lattice. We'll denote this framed lattice by $[\omega_1, \omega_2]$. The framing is *positive* if $\mathrm{Im}(\omega_2/\omega_1) > 0$. This is the condition that the angle θ from ω_1 to ω_2 satisfies $0 < \theta < \pi$. If $[\omega_1, \omega_2]$ is not positive, then $[\omega_1, -\omega_2]$ and $[\omega_2, \omega_1]$ are both positive framings of the lattice.

We consider two lattices Λ and Λ' to be *equivalent* if you can obtain one from the other by a rotation and a dilatation. That is, there is a non-zero complex number u such that $\Lambda' = u\Lambda$. Similarly, two framed lattices are equivalent if one can be obtained from the other by a rotation and dilation:

$$[u\omega_1, u\omega_2] \sim [\omega_1, \omega_2].$$

The first task is to understand the set of equivalence classes of positively framed lattices in $\mathbb{C}$ and the action of $\mathrm{SL}_2(\mathbb{Z})$ on it.

(i) Show that every equivalence class of positively framed lattices contains a unique member of the form $[1, \tau]$ where $\mathrm{Im}(\tau) > 0$.

[1] A bad pun.

This implies that one can identify the set of equivalence classes of positively framed lattices with the *upper half plane*

$$\mathfrak{h} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

(ii) Define

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

Show that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : [\omega_1, \omega_2] \mapsto [\omega_1', \omega_2']$$

is an action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of equivalence classes of positively framed lattices in $\mathbb{C}$. Show that the corresponding action on $\mathfrak{h}$ is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

(iii) Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } U = ST.$$

Show that $S^2 = U^3 = -I$. Deduce that there is a homomorphism

$$\varphi : \langle s, u : s^2 = u^3,\ s^4 = u^6 = 1 \rangle \to \mathrm{SL}_2(\mathbb{Z})$$

with $S = \varphi(s)$ and $U = \varphi(u)$.

(iv) Let $\rho = e^{i\pi/3}$. Compute the stabilizers of $i \in \mathfrak{h}$ and of ρ^2.

(v) Let

$$F = \{\tau \in \mathbb{C} : |\tau| \geq 1,\ |\mathrm{Re}(\tau)| \leq 1/2\}.$$

Show that $\tau \in F$ if and only if 1 is a shortest vector in $\mathbb{Z} \oplus \mathbb{Z}\tau$ and τ is a shortest vector in $\mathbb{Z} \oplus \mathbb{Z}\tau$ that is not a multiple of 1.

(vi) Show that

$$F^o := F - \big(\{\tau : \mathrm{Re}(\tau) = -1/2\} \cup \{\tau\ : |\tau| = 1 \text{ and } \mathrm{Re}(\tau) < 0\}\big)$$

is a fundamental domain (aka, a fundamental region) for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}$. (One way to do this is to prove that a lattice Λ in $\mathbb{C}$ is generated by its shortest vector and a shortest vector that is not a multiple of the first.)

(vii) (The LLL algorithm.) Show that the following algorithm, which begins with any positive basis of a lattice, produces a positive basis of the lattice where the first basis vector is a shortest vector and the second is a shortest vector that is not a multiple of the first. Call such a basis *minimal.* The input of each step of the algorithm is a positive basis ω_1, ω_2 of a lattice, the output is the pair of vectors ω_1', ω_2', where

- if ω_2 is shorter than ω_1, then $\omega_1' = \omega_2$ and $\omega_2' = -\omega_1$;
- if ω_1 is no longer than ω_2 and if $\omega_2 \pm \omega_1$ is shorter than ω_2, then $\omega_1' = \omega_1$ and $\omega_2' = \omega_2 \pm \omega_1$;
- else STOP.

Show that the algorithm terminates and that it produces a minimal basis.

(viii) Show that if $\tau \in \mathfrak{h}$, then there is an element g of the subgroup $\langle S, T \rangle$ of $\mathrm{SL}_2(\mathbb{Z})$ such that $g\tau \in F^o$. Deduce that S and U generate $\mathrm{SL}_2(\mathbb{Z})$.

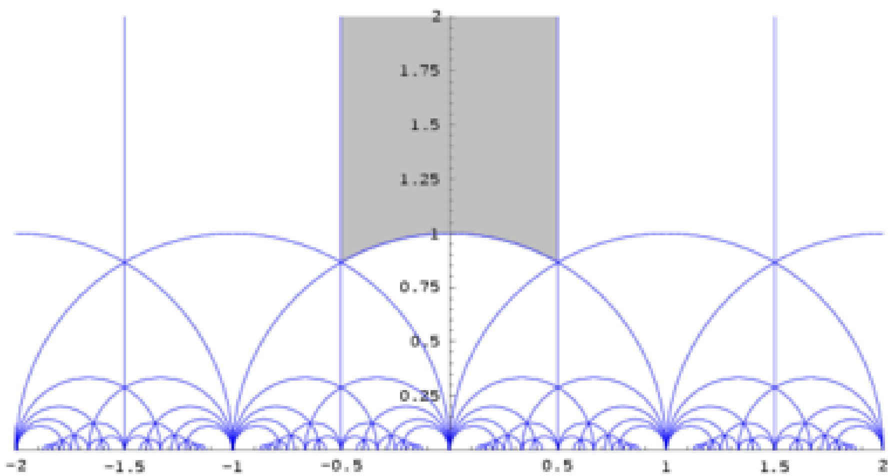

FIGURE 1. The fundamental domain and its translates

It remains to prove that the only relations between S and U are those stated above. For this, we consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on a graph.

(ix) Note that the boundary of F has 3 edges of which only one is compact. (Viz., the arc of $|\tau| = 1$ from ρ to ρ^2.) Write this as the union of two "half edges": the arc from ρ^2 to i, and the arc from i to ρ. Call these A and B. Note that S interchanges A and B.

(x) Let Γ be the graph in $\mathfrak{h}$ consisting of all translates of A and B. Show that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on the edges of Γ and that the stabilizer of each edge is $\pm I$.

(xi) Show that there are two orbits of vertices, namely the orbit of i and the orbit of ρ. Show that each vertex in the orbit of i has degree 2 and each vertex in the orbit of ρ has degree 3.

(xii) Show that the stabilizer of each vertex is generated by a conjugate of U or a conjugate of S.

Because $\pm I$ fixes everything, it is best to ignore it for the time being. To this end, set $G = \mathrm{SL}_2(\mathbb{Z})/\langle \pm I \rangle$. Note that G acts *simply* transitively on the edges of Γ and that G is generated by the images $\overline{S}$ and $\overline{U}$ of S and U in G. The next step is to prove that

$$G \cong \langle \overline{S}, \overline{U} : \overline{S}^2 = \overline{U}^3 = 1 \rangle. \tag{2}$$

(xiii) Each word $w = g_1 g_2 \dots g_m$ in $\overline{S}$ and $\overline{U}$ corresponds to the edge path[2]

$$A,\ g_1(A),\ g_1g_2(A),\ \dots,\ g_1g_2\dots g_m(A).$$

Note that the path corresponding to the word w in $\overline{S}$ and $\overline{U}$ that represents the identity is a loop that starts and ends with A.

(xiv) It is a fact (which can be proved using hyperbolic geometry) that Γ is a *tree*. That is, every pair of its vertices is joined by a unique reduced edge path.[3] Use this to prove the presentation (2) of G. (Hint available upon request.)

(xv) Deduce the presentation (1) of $\mathrm{SL}_2(\mathbb{Z})$.

Cultural Remarks:

The action of $\mathrm{SL}_2(\mathbb{Z})$ is very rich and has connections to many branches of mathematics. For example:

(a) The upper half plane is a model of the hyperbolic plane (a geometry with constant curvature -1. The metric (i.e., line element) is

$$ds^2 = \frac{dx^2 + dy^2}{y^2}$$

where $\tau = x + iy$. It is not hard to show that this line element is preserved by the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathfrak{h}$. Geodesics in $\mathfrak{h}$ are lines perpendicular to the real axis and semi-circles centered on the real axis.

(b) The quotient of $\mathfrak{h}$ by $\mathrm{SL}_2(\mathbb{Z})$ is the space that parametrizes all lattices in $\mathbb{C}$, and is also the space that parametrizes all "elliptic curves".

---

[2]An *edge path* is a sequence of edges in which two consecutive edges share a common vertex.

[3]An edge path is *reduced* if no edge occurs more than once.

(c) Modular forms are very important in both analytic and algebraic number theory. They are "analytic functions" $f : \mathfrak{h} \to \mathbb{C}$ that satisfy certain conditions, the main one being that there is an $m \geq 0$ such that

$$f\big((a\tau + b)/(c\tau + d)\big) = (c\tau + d)^m f(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$.