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:

$$
\begin{equation*}
\mathrm{SL}_{2}(\mathbb{Z}) \cong\left\langle s, u: s^{2}=u^{3}, s^{4}=u^{6}=1\right\rangle \tag{1}
\end{equation*}
$$

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 $\omega_{1}, \omega_{2}$ comprise a framing of a lattice $\Lambda$ 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 $\left[\omega_{1}, \omega_{2}\right]$. The framing is positive if $\operatorname{Im}\left(\omega_{2} / \omega_{1}\right)>0$. This is the condition that the angle $\theta$ from $\omega_{1}$ to $\omega_{2}$ satisfies $0<\theta<\pi$. If $\left[\omega_{1}, \omega_{2}\right]$ is not positive, then $\left[\omega_{1},-\omega_{2}\right]$ and $\left[\omega_{2}, \omega_{1}\right]$ are both positive framings of the lattice.

We consider two lattices $\Lambda$ and $\Lambda^{\prime}$ 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 $\Lambda^{\prime}=u \Lambda$. Similarly, two framed lattices are equivalent if one can be obtained from the other by a rotation and dilation:

$$
\left[u \omega_{1}, u \omega_{2}\right] \sim\left[\omega_{1}, \omega_{2}\right] .
$$

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 $\operatorname{Im}(\tau)>0$.

[^0]This implies that one can identify the set of equivalence classes of positively framed lattices with the upper half plane

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

(ii) Define

$$
\binom{\omega_{2}^{\prime}}{\omega_{1}^{\prime}}=\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right)\binom{\omega_{2}}{\omega_{1}}
$$

Show that

$$
\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right):\left[\omega_{1}, \omega_{2}\right] \mapsto\left[\omega_{1}^{\prime}, \omega_{2}^{\prime}\right]
$$

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

$$
\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right): \tau \mapsto \frac{a \tau+b}{c \tau+d}
$$

(iii) Let

$$
S=\left(\begin{array}{cc}
0 & -1 \\
1 & 0
\end{array}\right), T=\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right) \text { and } U=S T
$$

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

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

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 $\rho^{2}$.
(v) Let

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

Show that $\tau \in F$ if and only if 1 is a shortest vector in $\mathbb{Z} \oplus \mathbb{Z} \tau$ and $\tau$ is a shortest vector in $\mathbb{Z} \oplus \mathbb{Z} \tau$ that is not a multiple of 1 .
(vi) Show that
$F^{o}:=F-(\{\tau: \operatorname{Re}(\tau)=-1 / 2\} \cup\{\tau:|\tau|=1$ and $\operatorname{Re}(\tau)<0\})$
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 $\Lambda$ 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 $\omega_{1}, \omega_{2}$ of a lattice, the output is the pair of vectors $\omega_{1}^{\prime}, \omega_{2}^{\prime}$, where

- if $\omega_{2}$ is shorter than $\omega_{1}$, then $\omega_{1}^{\prime}=\omega_{2}$ and $\omega_{2}^{\prime}=-\omega_{1}$;
- if $\omega_{1}$ is shorter than $\omega_{2}$ and if $\omega_{2} \pm \omega_{1}$ is shorter than $\omega_{2}$, then $\omega_{1}^{\prime}=\omega_{1}$ and $\omega_{2}^{\prime}=\omega_{2} \pm \omega_{1}$;
- 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 an 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 $\rho$ to $\rho^{2}$.) Write this as the union of two "half edges": the arc from $\rho^{2}$ to $i$, and the arc from $i$ to $\rho$. Call these $A$ and $B$. Note that $S$ interchanges $A$ and $B$.
(x) Let $\Gamma$ 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 $\Gamma$ 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 $\rho$. Show that each vertex in the orbit of $i$ has degree 2 and each vertex in the orbit of $\rho$ has degree 3 .
(xii) Show that the stabilizer of each vertex lies in the normal subgroup of $\mathrm{SL}_{2}(\mathbb{Z})$ generated by $S^{2}$ and $U^{3}$.

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 $\Gamma$ and that $G$ is generated by the images $\bar{S}$ and $\bar{U}$ of $S$ and $U$ in $G$. The next step is to prove that

$$
\begin{equation*}
G \cong\left\langle\bar{S}, \bar{U}: \bar{S}^{2}=\bar{U}^{3}=1\right\rangle \tag{2}
\end{equation*}
$$

(xiii) Each word $w=g_{1} g_{2} \ldots g_{m}$ in $\bar{S}$ and $\bar{U}$ corresponds to the edge path ${ }^{2}$

$$
A, g_{1}(A), g_{1} g_{2}(A), \ldots, g_{1} g_{2} \ldots g_{m}(A)
$$

Note that the path corresponding to the word $w$ in $\bar{S}$ and $\bar{U}$ 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 $\Gamma$ 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.)
$(\mathrm{xv})$ 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

$$
d s^{2}=\frac{d x^{2}+d y^{2}}{y^{2}}
$$

where $\tau=x+i y$. 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".

[^1](c) Modular forms are very important in both analytic and algebraic number theory. They are "analytic functions" $f: \mathfrak{h} \rightarrow \mathbb{C}$ that satisfy certain conditions, the main one being that there is an $m \geq 0$ such that
$$
f((a \tau+b) /(c \tau+d))=(c \tau+d)^{m} f(\tau)
$$

for all $\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$ in $\mathrm{SL}_{2}(\mathbb{Z})$.


[^0]:    ${ }^{1} \mathrm{~A}$ bad pun.

[^1]:    ${ }^{2}$ 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.

