MATHEMATICS 332: ALGEBRA — EXERCISES USING MODULES OVER A PID

Reading and Exercises:

The special linear group over the integers is

$$\mathrm{SL}_2(\mathbb{Z}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \}.$$

The complex upper half plane is

$$\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\,(\tau) > 0\}.$$

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the set $\mathcal{H}$ by fractional linear transformations,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \tau \longmapsto \frac{a\tau + b}{c\tau + d}\,.$$

Suppose that a point $\tau \in \mathcal{H}$ is an *elliptic point*, meaning that it is fixed by a nontrivial transformation $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. Thus $a\tau + b = c\tau^2 + d\tau$; solving for τ with the quadratic equation ($c = 0$ is impossible since $\tau \notin \mathbb{Q}$) and remembering that $\tau \in \mathcal{H}$ shows that $|a + d| < 2$ (exercise). Thus the characteristic polynomial of γ is $x^2 + 1$ or $x^2 \pm x + 1$. Since γ satisfies its characteristic polynomial, one of $\gamma^4 = I$, $\gamma^3 = I$, $\gamma^6 = I$ holds, and γ has order 1, 2, 3, 4, or 6 as a matrix. Orders 1 and 2 give the identity transformation (exercise). So the following proposition describes all nontrivial fixing transformations.

Proposition. *Let* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(a) *If* γ *has order 3 then* γ *is conjugate to* $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]^{\pm 1}$ *in* $\mathrm{SL}_2(\mathbb{Z})$.
(b) *If* γ *has order 4 then* γ *is conjugate to* $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^{\pm 1}$ *in* $\mathrm{SL}_2(\mathbb{Z})$.
(c) *If* γ *has order 6 then* γ *is conjugate to* $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]^{\pm 1}$ *in* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. (c) Since $\gamma^6 = I$ the lattice $L = \mathbb{Z}^2$ of integral column vectors is a module over the ring $\mathbb{Z}[\zeta_6]$ where $\zeta_6 = e^{2\pi i/6}$: the scalar-by-vector product $(a + b\zeta_6) \cdot v$ for $a, b \in \mathbb{Z}$ and $v \in L$ is defined to be the matrix-by-vector product $(aI + b\gamma)v$. (In fact we are viewing L as a 2-dimensional representation of the cyclic group of order 6 generated by ζ_6, the action of the group on L extended to the group algebra $\mathbb{Z}[\zeta_6]$.)

The ring $\mathbb{Z}[\zeta_6]$ is known to be a principal ideal domain and L is finitely generated over it. The structure theorem for finitely generated modules over a principal ideal domain therefore says that L is $\mathbb{Z}[\zeta_6]$-isomorphic to a sum $\bigoplus_k \mathbb{Z}[\zeta_6]/I_k$ where the I_k are ideals. As an abelian group, L is free of rank 2. Every nonzero ideal I_k of $\mathbb{Z}[\zeta_6]$ has rank 2 as an abelian group, making the quotient $\mathbb{Z}[\zeta_6]/I_k$ a torsion group, so no such terms appear in the sum. Only one free summand appears, for otherwise the sum would be too big as an abelian group. Thus there is a $\mathbb{Z}[\zeta_6]$-module isomorphism $\phi_\gamma : \mathbb{Z}[\zeta_6] \longrightarrow L$.

Let $u = \phi_\gamma(1)$ and $v = \phi_\gamma(\zeta_6)$ and let $[u \ \ v]$ denote the matrix with columns u and v. Then $L = \mathbb{Z}u + \mathbb{Z}v$ so $\det[u \ \ v] \in \{\pm 1\}$ (exercise). Compute that $\gamma u = \zeta_6 \cdot$

$\phi_\gamma(1) = \phi_\gamma(\zeta_6) = v$, and similarly $\gamma v = \zeta_6 \cdot \phi_\gamma(\zeta_6) = \phi_\gamma(\zeta_6^2) = \phi_\gamma(-1+\zeta_6) = -u+v$. Thus

$$\gamma[u \;\; v] = [v \;\; -u+v] = [u \;\; v] \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right], \text{ so } \gamma = [u \;\; v] \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] [u \;\; v]^{-1},$$

and

$$\gamma[v \;\; u] = [-u+v \;\; v] = [v \;\; u] \left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right], \text{ so } \gamma = [v \;\; u] \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]^{-1} [v \;\; u]^{-1}.$$

One of $[u \;\; v]$, $[v \;\; u]$ is in $\mathrm{SL}_2(\mathbb{Z})$, proving (c). Parts (a) and (b) are similar (exercise). □

Now we can understand elliptic points and their isotropy (stabilizing) subgroups.

Corollary. *The elliptic points for* $\mathrm{SL}_2(\mathbb{Z})$ *are* $\mathrm{SL}_2(\mathbb{Z})i$ *and* $\mathrm{SL}_2(\mathbb{Z})\zeta_3$ *where* $\zeta_3 = e^{2\pi i/3}$. *The modular curve* $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ *has two elliptic points. The isotropy subgroups of* i *and* ζ_3 *are*

$$\mathrm{SL}_2(\mathbb{Z})_i = \langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \rangle \quad \textit{and} \quad \mathrm{SL}_2(\mathbb{Z})_{\zeta_3} = \langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \rangle.$$

For each elliptic point τ *of* $\mathrm{SL}_2(\mathbb{Z})$ *the isotropy subgroup* $\mathrm{SL}_2(\mathbb{Z})_\tau$ *is finite cyclic.*

Proof. The fixed points in $\mathcal{H}$ of the matrices in the proposition are i and ζ_3. The first statement follows (exercise). The second statement follows since i and ζ_3 are not equivalent under $\mathrm{SL}_2(\mathbb{Z})$. The third statement can be verified directly (exercise), and the fourth statement follows since all other isotropy subgroups of order greater than 2 are conjugates of $\mathrm{SL}_2(\mathbb{Z})_i$ and $\mathrm{SL}_2(\mathbb{Z})_{\zeta_3}$. See the guided exercise below for a more conceptual proof of the fourth statement. □

Exercise 1. If the nontrivial transformation $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ fixes $\tau \in \mathcal{H}$, show that $|a+d| < 2$.

Exercise 2. Show that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ has order 2 then $\gamma = -I$. (One way to do this by thinking about the minimal polynomial of γ, the polynomial $X^2 - 1$, and the characteristic polynomial of γ; another way is to use the Jordan form of γ.)

Exercise 3. (a) In the proof of the proposition, why does the condition $L = \mathbb{Z}u + \mathbb{Z}v$ imply $\det[u \;\; v] = \pm 1$?

(b) Prove the other two parts of the proposition. (Hints are available from the instructor.)

Exercise 4. (a) Complete the proof of the corollary. (Hints are available from the instructor.)

(b) Give a more conceptual proof of the fourth statement of the corollary as follows: The isotropy subgroup of i in $\mathrm{SL}_2(\mathbb{R})$ is the special orthogonal group $\mathrm{SO}(2)$, and it follows (you may take this as given for now) that $\mathcal{H} \cong \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2)$. Here the right side is a quotient *space*, not a quotient group. Show that an element $s(\tau)$ of $\mathrm{SL}_2(\mathbb{R})$ moves τ to i and the isotropy subgroup of τ correspondingly conjugates to a discrete subgroup of $\mathrm{SO}(2)$. But since $\mathrm{SO}(2)$ is the rotations of the circle, any such subgroup is cyclic.