Lecture 2

Stabilizers + a correction

We begin with a correction for the statement of Proposition 9(B) in the notes for the previous lecture (with my thanks to the student who pointed out the error). The statement should read

Prop. 9(B): If $\tau, \gamma\tau \in \mathcal{F}$ with $\tau \neq \gamma\tau$, then either $|\mathrm{Re}(\tau)| = 1/2$ and $\gamma\tau = \tau \mp 1$, or $|\tau| = 1$ and $\gamma\tau = -1/\tau$. This statement and the accompanying proof will be updated in the Lecture 1 notes.

The proof of Prop. 9(B) points to the possibility that $\tau \in \mathcal{F}$ can be fixed by some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma \neq \pm I_2$ when $\tau = i, \omega$ or $-\bar{\omega}$. Indeed, we have the following proposition:

Proposition 1 *Let $\tau \in \mathcal{F}$ and let $stab_\tau = \{\gamma \in SL_2(\mathbb{Z}) : \gamma\tau = \tau\}$ be the stabilizer of τ. Then*

$$stab_\tau = \begin{cases} \langle S \rangle & \text{if } \tau = i \\ \langle ST \rangle & \text{if } \tau = \omega \\ \langle TS \rangle & \text{if } \tau = -\bar{\omega} \\ \langle -I_2 \rangle & \text{otherwise} \end{cases}$$

For the proof, please see the corrected Lecture 1 notes.

We next turn our attention to congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, beginning with the subgroups $\Gamma(N)$.

The principal congruence subgroup of level N

The principal subgroup of level N, denoted $\Gamma(N)$ is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

that is, the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $a \equiv d \equiv 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$.

We have seen $\Gamma(N)$ for one N already: since every integer is congruent to $0, 1 \pmod{1}$, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. For every $N \in \mathbb{Z}^+$, $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$. This is a consequence of the next claim.

Claim 2 *The map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N}$ is a group homomorphism.*

By definition, $\Gamma(N)$ is the kernel of this group homomorphism, thus it is normal.

Other congruence subgroups

Definition 3 *A subgroup* Γ *of* $SL_2(\mathbb{Z})$ *is a congruence subgroup if* $\Gamma(N) \subset \Gamma$ *for some* $N \in \mathbb{Z}^+$*. The least such* N *for which this occurs is the level of* Γ*.*

Among the most important congruence subgroups are $\Gamma_1(N)$ and $\Gamma_0(N)$.

Definition 4 *For* $N \in \mathbb{Z}^+$*,*

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where the $*$ *indicates that there are no conditions on* b *modulo* N*.*

Definition 5 *For* $N \in \mathbb{Z}^+$*,*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

where again the $*$ *indicates that there are no conditions on* a, b, d *modulo* N*.*

One can check that

Claim 6 *For all* $N \in \mathbb{Z}^+$*,*

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$$

As a special case of the claim above, note that since $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, we have $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1) = \Gamma_1(1) = \Gamma_0(1)$. For other N, however $\Gamma(N)$ is a proper subgroup of $\Gamma_1(N)$. In particular, for $N > 1$ we have $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N) \setminus \Gamma(N)$.

What about the containment $\Gamma_1(N) \subseteq \Gamma_0(N)$? For most values of $N > 1$, we will have $-I_2 \in \Gamma_0(N)$, but $-I_2 \notin \Gamma_1(N)$. There is an exception.

Proposition 7 $\Gamma_0(2) = \Gamma_1(2)$.

Proof: Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(2)$. Then c is even and ad must be odd. Therefore both a and b are mod, so $a \equiv d \equiv 1 \pmod{2}$ and $c \equiv 0 \pmod{2}$, so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(2)$. $\square$

We will later translate these containments $\Gamma_1(N) \subseteq \Gamma_0(N)$ into maps between their associated modular curves. As noted in the introduction to the first lecture, the curves associated to $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$ parameterize isomorphism classes of ellitpic curves with some torsion data. In the case of $\Gamma(N)$, the corresponding modular curves parameterize isomorphism classes of elliptic curves with full level N structure (i.e., an isomorphism from the group of N-torsion points of the elliptic curve to the group $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$). Noncuspidal points on the projective modular curve associated to $\Gamma_1(N)$ correspond to isomorphism classes of elliptic curves with a point of order N. Noncuspidal points on the projective modular curve associated to $\Gamma_0(N)$ correspond to isomorphism classes of elliptic curves with a cyclic subgroup of order N - equivalently, a cyclic N isogeny. Since $\Gamma_0(2) = \Gamma_1(2)$, these last two statements indicate that the data of an elliptic curve with a point of order 2 is the same as the data of an elliptic curve with a cyclic 2-isogeny.

$\Gamma(N), \Gamma_1(N), \Gamma_0(N)$ will be our focus in these lectures, by they are not the only congruence subgroups.

Example 8 *Let Γ be a congruence subgroup with $\Gamma(N) \subseteq \Gamma$. Since $\Gamma(N)$ is normal, $\alpha\Gamma(N)\alpha^{-1}$ again contains $\Gamma(N)$.*

Example 9 *Let M, N be integers with $M|N$. $\Gamma_1(M,N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N) : b \equiv 0 \pmod{M}\}$ is a congruence subgroup ($\Gamma(M) \subseteq \Gamma_1(M,N)$.*

There are other discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ that are of interest to mathematicians; within $\mathrm{SL}_2(\mathbb{Z})$, in addition to having congruence subgroups, there are finite index subgroups besides congruence subgroups.

Claim 10 *For any congruence subgroup Γ, $[SL_2(\mathbb{Z}) : \Gamma] < \infty$*

To see a proof that there are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which are not congruence subgroups, see Keith Conrad's notes at `https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf`. Interestingly, though there are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which are not congruence subgroups (in fact, "most" finite index subgroups are not), for $\mathrm{SL}_n(\mathbb{Z})$ with $n > 2$, every finite index subgroup is a congruence subgroup.

Elements of $\Gamma\backslash\mathcal{H}$

As before, we would like to identify a subset of $\mathcal{H}$ with which we can (nearly) identify the points of the set $\Gamma\backslash\mathcal{H}$. The subset we identify may not be connected as a subset of $\mathcal{H}$. As a result, it may be more difficult to imagine that the quotient space is connected, but we should keep in mind though the next proof will allow us to (nearly) identify the points of the set $\Gamma\backslash\mathcal{H}$, there is more work to be done to understand the topology.

Definition 11 *For a congruence subgroup Γ,*

$$Y(\Gamma) = \Gamma\backslash\mathcal{H}.$$

For $\Gamma = \Gamma(N)$ we write $Y(\Gamma) = Y(N)$. For $\Gamma = \Gamma_1(N)$, we write $Y(\Gamma) = Y_1(N)$. For $\Gamma = \Gamma_1(N)$, we write $Y(\Gamma) = Y_0(N)$.

In Lecture 1, we showed that there is a surjection

$$\pi : \mathcal{F} \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} = Y(1)$$

$$\tau \mapsto \mathrm{SL}_2(\mathbb{Z})\tau.$$

(That π is a surjection is Proposition 9(A).) We will use this result to prove the following.

Proposition 12 *Let* Γ *be a finite index subgroup of* $SL_2(\mathbb{Z})$*, and choose elements* $\gamma_1, \dots, \gamma_m$ *such that*

$$SL_2(\mathbb{Z}) = \bigcup_{k=1}^{m} \{\pm I_2\}\Gamma\gamma_k.$$

Then

$$\bigcup_{k=1}^{m} \gamma_k \mathcal{F}$$

surjects to $Y(\Gamma)$*.*

Proof: Let $\Gamma\tau \in Y(\Gamma)$, and let $\tau \in \Gamma\tau$ be an element of the orbit. By Prop. 9(A) of Lecture 1, there is $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau' \in \mathcal{F}$ such that $\tau = \gamma'\tau'$. There is also some $\gamma \in \Gamma$ and some k such that $\gamma' = \pm\gamma\gamma_k$, so $\tau = \gamma\gamma_k\tau' = \gamma(\gamma_k\tau') \in \Gamma\tau$.