MATHEMATICS 332: ALGEBRA – MIDTERM

1. Introduction

This exam is meant to help you work with various ideas from group theory in one context.

> *As we have discussed, this exam is open instructor, and you are expected to check with me regularly on your progress, first in solving the problems and then second in expounding your solutions.*

Definition 1.1 (Modular Group)**.** *The* **modular group** *is the subgroup of* $\mathrm{SL}_2(\mathbb{R})$ *consisting of the 2-by-2 matrices having integer entries and determinant* 1*,*

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

Exercise 1. Verify that indeed $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{SL}_2(\mathbb{R})$.

---

2. Principal Congruence Subgroups

Let N be a positive integer. The *reduce mod* N map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$$

is a ring homomorphism that takes $1_{\mathbb{Z}}$ to $1_{\mathbb{Z}/N\mathbb{Z}}$. Consequently, applying the map entrywise to 2-by-2 matrices gives a group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Definition 2.1 (Principal Congruence Subgroup)**.** *Let* N *be a positive integer. The* **principal congruence subgroup of level** N *is the kernel of the entrywise reduction mod* N *map on* $\mathrm{SL}_2(\mathbb{Z})$*,*

$$\Gamma(N) = \ker\big(\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\big).$$

Thus $\Gamma(N)$ *is normal in* $\mathrm{SL}_2(\mathbb{Z})$*. Specifically,*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \right\}.$$

(*The matrix congruence is interpreted entrywise, i.e.,* $a = 1 \bmod N$ *and so on.*)

In particular $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. The next exercise shows that the entrywise reduction map $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is a surjection.

Exercise 2. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be given. Lift γ to a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{M}_2(\mathbb{Z})$. This exercise explains how to modify the lift so that its determinant is 1.

(a) Show that $\gcd(c, d, N) = 1$.

(b) Assume that $c \neq 0$. Show that $\gcd(c, d') = 1$ for some $d' = d + tN$ where $t \in \mathbb{Z}$. (If $c = 0$ then $d \neq 0$—unless $N = 1$, in which case the whole problem is

trivial—and a similar argument works, so we omit it.) Hint: Let $t = \prod_{p|c,\, p\nmid d} p$, and show that if $p \mid c$ then $d + tN \neq 0 \bmod p$.

(c) Still working with the case $c \neq 0$, show that some lift $\left[\begin{smallmatrix} a+kN & b+\ell N \\ c & d' \end{smallmatrix}\right]$ of γ lies in $\mathrm{SL}_2(\mathbb{Z})$. Thus the map surjects. (Again the $c = 0$ case is handled similarly, so we omit it. But note that the process of adjusting the lift to make its determinant equal 1 has involved all four of its entries. Since $\mathrm{SL}_2(\mathbb{Z})$ is infinite and $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite, perhaps the amount of work necessary to show that $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ surjects is surprising.)

Now that the homomorphism $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is known to surject, we have an isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Consequently the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite for all N. The next exercise is to show that specifically the index is

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

where the product is taken over all prime divisors of N.

Exercise 3. (a) Let p be a prime and let e be a positive integer. Show by induction on e that $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e}(1 - 1/p^2)$.

(b) Cite the Sun-Ze Theorem and use one more idea to show that $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p|N}(1 - 1/p^2)$, so this is also the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$.

---

3. Congruence Subgroups in General

Definition 3.1 (Congruence Subgroup, Level)**.** *Let N be a positive integer. A subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a* **congruence subgroup of level** *N if it contains the principal congruence subgroup $\Gamma(N)$. Equivalently, a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if it is the inverse image under reduction modulo N of a subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Since every $\Gamma(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, so does every congruence subgroup Γ. Besides the principal congruence subgroups, the most important congruence subgroups are the inverse images of the $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-subgroups

$$G_1 = \left\{ \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

(where "$*$" means "unspecified") and

$$G_0 = \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

Specifically, the congruence subgroups are

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N \right\}.$$

Thus for any positive integer N we have the chain of containments

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

Exercise 4. (a) Show that the map

$$g_1 : \Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto b \bmod N$$

is an epimorphism with kernel $\Gamma(N)$.

(b) Show that the map

$$g_0 : \Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto d \bmod N$$

is an epimorphism with kernel $\Gamma_1(N)$.

It follows from exercise 4(a) that

$$\Gamma(N) \lhd \Gamma_1(N), \quad \Gamma_1(N)/\Gamma(N) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}, \quad [\Gamma_1(N) : \Gamma(N)] = N.$$

And it follows from exercise 4(b) that

$$\Gamma_1(N) \lhd \Gamma_0(N), \quad \Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times, \quad [\Gamma_0(N) : \Gamma_1(N)] = \varphi(N),$$

where φ is the Euler totient function.

Exercise 4. (c) Show that in consequence of the indices in the two previous displays and of the previously-computed value of $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$, it follows that

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p),$$

the product taken over all primes dividing N.

---

4. The Theta Group as a Congruence Subgroup

Here is a sketched argument that the modular group is generated by the two matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Let Γ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by the two matrices. Note that $\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]^n \in \Gamma$ for all $n \in \mathbb{Z}$. Let $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$. The identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b' \\ c & nc + d \end{bmatrix}$$

shows that unless $c = 0$, some matrix $\alpha\gamma$ with $\gamma \in \Gamma$ has bottom row (c, d') with $|d'| \leq |c|/2$. The identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix}$$

shows that this process can be iterated until some matrix $\alpha\gamma$ with $\gamma \in \Gamma$ has bottom row $(0, *)$. Because we are working with matrices that have determinant 1, in fact the bottom row of $\alpha\gamma$ is $(0, \pm 1)$, and since $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^2 = -I$ it can be taken to be $(0, 1)$. It follows that $\alpha\gamma = \left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$ for some $n \in \mathbb{Z}$ and hence that $\alpha\gamma \in \Gamma$. Thus $\alpha \in \Gamma$, and Γ is all of $\mathrm{SL}_2(\mathbb{Z})$.

Make sure that you understand this argument. If it gives you trouble then work with me in person or via email until you get it.

Definition 4.1 (Theta Group)**.** *The* **theta group** Γ_θ *is the subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *generated by the matrices*

$$\pm\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \textit{and} \quad \pm\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}.$$

Exercise 5. This exercise shows that $\Gamma_\theta = \Gamma_0(4)$. The containment "$\subset$" holds because the four generators of Γ_θ lie in $\Gamma_0(4)$. For the other containment, let $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ be a matrix in $\Gamma_0(4)$. Similarly to the discussion above, the identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b' \\ c & nc+d \end{bmatrix}$$

shows that unless $c = 0$, some matrix $\alpha\gamma$ with $\gamma \in \Gamma_\theta$ has bottom row (c, d') with $|d'| < |c|/2$, but now the inequality is strict. Explain why the inequality is strict.

Use the identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 4n & 1 \end{bmatrix} = \begin{bmatrix} a' & b \\ c+4nd & d \end{bmatrix}$$

to show that unless $d = 0$, some matrix $\alpha\gamma$ with $\gamma \in \Gamma_\theta$ has bottom row (c', d') with $|c'| < 2|d'|$. Again explain why the inequality is strict.

Each multiplication reduces the positive integer quantity $\min\{|c|, 2|d|\}$, so the process must stop with $c = 0$ or $d = 0$. Show that in fact this means that $\alpha\gamma \in \Gamma_\theta$ for some $\gamma \in \Gamma_\theta$ and so $\alpha \in \Gamma_\theta$.