COMPUTATIONAL ASPECTS OF SHIMURA CURVES (BUILDING BRIDGES 4, BUDAPEST)

DREW SUTHERLAND, JOHN VOIGHT; NOTES BY ALEKSANDER HORAWA

These are notes from a mini course on Computational Aspects of Shimura Curves taught by Drew Sutherland and John Voight on July 9–10, 2018. It was a part of Building Bridges: 4th EU/US Summer School on Automorphic Forms and Related Topics, July 9–14, 2018, in Budapest. They were LaTeX'ed by Aleksander Horawa (who is the only person responsible for any mistakes that may be found in them).

This version is from July 15, 2018. Check for the latest version of these notes at

http://www-personal.umich.edu/~ahorawa/index.html

If you find any typos or mistakes, please let me know at ahorawa@umich.edu.

The problem sets for the mini course are available at:

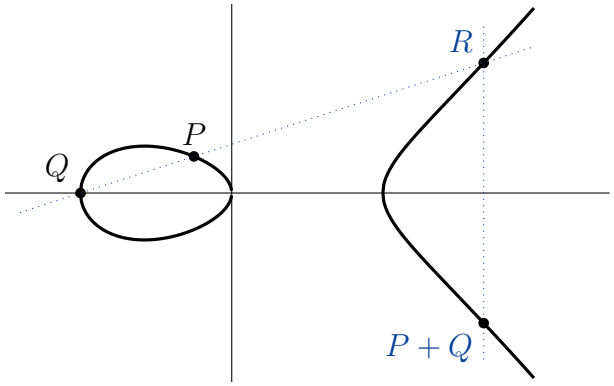
(1) https://www.math.dartmouth.edu/~jvoight/BB/BB1ex.pdf
(2) https://www.math.dartmouth.edu/~jvoight/BB/BB2ex.pdf

1. Lecture 1 (Drew Sutherland)

The first lecture will be a quick review of standard material.

Elliptic curves. There are two possible definitions of elliptic curves.

(1) Smooth projective curve over K (a perfect field) of genus one with distinguished rational point (E, O). It has a group law.



When $\mathrm{char}(K) \neq 2, 3$, we can write down the equation in the form

$$y^2 = f(x) = x^3 + a_4 x + a_6.$$

Date: July 15, 2018.

In general, the equation can be written as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$y^2 + h(x)y = h(x)$$

(2) Abelian variety of dimension 1 (projective algebraic group).

Jacobians. Let X/K be a smooth (geometrically irreducible) projective curve of genus g. We call such curves *nice*. Then there is a map

$$\{X/K \text{ nice curves}\} \overset{\text{Jac}}{\to} \{\text{abelian varieties of dimension } g \text{ over } K\}.$$

We define a *closed point* to be a $\mathrm{Gal}(\overline{K}/K)$-orbit of $X(\overline{K})$. Then

$$\mathrm{Div}(X) := \mathbb{Z}[P \mid P \text{ closed point}],$$

so a general divisor can be written as $D = \sum_P n_p P$. The *degree* of P is $\deg(P) = \#P$, and

$$\deg(D) = \sum_P n_P \deg(P).$$

The coordinate ring of X is

$$K[X] = K[x_1, \dots, x_n]/(I(X))$$

and the function field is

$$K(X) = \mathrm{Frac}(k[X]).$$

There is a one to one correspondence

$$\left\{ \begin{array}{c} \text{smooth projective curves } X \\ \text{over } K \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{function fields } K(X) \\ \text{which are finite extensions of } K(x) \end{array} \right\}.$$

For $f \in K(X)$, $\mathrm{div}(f) = \sum \mathrm{ord}_P(f)P$. Then $\deg \mathrm{div}(f) = 0$. Define

$$\mathrm{Div}^0(X) := \{D \in \mathrm{Div}(X) : \deg(D) = 0\},$$
$$\mathrm{Princ}(X) := \{\mathrm{div}\, f : f \in K(X)\},$$
$$\mathrm{Pic}^0(X) := \frac{\mathrm{Div}^0(X)}{\mathrm{Princ}(X)}.$$

If $X(K) \neq \emptyset$, then $\mathrm{Pic}^0(X) \cong \mathrm{Jac}(X)$.

The *Abel–Jacobi* map for fixed $O \in X(K)$ is

$$X \to \mathrm{Jac}(X) \cong \mathrm{Pic}^0(X)$$
$$P \mapsto [P - O].$$

If $X = E$ is an elliptic curve, this map $E \to \mathrm{Jac}(E)$ is an isomorphism. This shows the equivalence of the two definitions of an elliptic curve.

Now, suppose $K = \mathbb{Q}$ (or a number field embedded in $\mathbb{C}$). If A/K is an abelian variety of dimension g, $A(\mathbb{C})$ is a compact Lie group, isomorphic to a torus $\mathbb{C}^g/\Lambda$ for $\Lambda \cong \mathbb{Z}^{2g}$.

Definition 1.1. For a torus $X = V/\Lambda$ ($V \cong \mathbb{C}^g$, $\Lambda \cong \mathbb{Z}^{2g}$), the *dual torus* is

$$X^\vee = V^*/\Lambda^*$$

where

$$V^* = \{f : V \to \mathbb{C} : f(\alpha v) = \overline{\alpha} f(v),\ f(v_1 + v_2) = f(v_1) + f(v_2)\}$$
$$\Lambda^* = \{f \in V^* : \mathrm{Im}(f(\Lambda)) \subseteq \mathbb{Z}\}.$$

Definition 1.2. A *polarization* of X is a positive definite Hermitian form $H : V \times V \to \mathbb{C}$ such that $\mathrm{Im}\, H(\Lambda, \Lambda) \subseteq \mathbb{Z}$. It induces an *isogeny* (surjective morphisms with finite kernel)

$$\phi_H : X \to X^\vee,$$
$$v\Lambda \mapsto (w \mapsto H(v, w)\Lambda^*).$$

A *polarization* of an abelian variety A/K is an isogeny $\phi : A \to A^\vee$.

We have a one-to-one correspondence

$$\left\{ \begin{array}{c} \text{polarized abelian varieties} \\ \text{over } \mathbb{C} \end{array} \right\} \leftrightarrow \{\text{polarized tori}\}.$$

Definition 1.3. A polarization of degree 1 is a *principal polarization.*

Theorem 1.4. *Jacobians are principally polarized abelian varieties.*

The focus of this mini course is on principally polarized abelian varieties.

Endomorphism rings and algebras. Let $\mathrm{End}(A)$ be the ring of endomorphisms of A with operations defined by $(\psi + \psi)(P) = \phi(P) + \psi(P)$, $(\phi\psi)(P) = \phi(\psi(P))$. We always have $\mathbb{Z} \subseteq \mathrm{End}(A)$, since for $n \in \mathbb{Z}$ we have a map

$$[n] : A \to A$$
$$P \mapsto nP.$$

Note that $\mathrm{End}(A)$ means endomorphisms **defined over** K. There could, of course, be more endomorphisms defined over extensions of K. We write

$$\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

which is a $\mathbb{Q}$-algebra of finite dimension.

Fix a polarization $\phi : A \to A^\vee$. Then $\phi^{-1} \in \mathrm{Hom}(A^\vee, A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The *Rosati involution* is defined as

$$\alpha^\dagger := \phi^{-1} \circ \alpha^\vee \circ \phi.$$

It is positive definite: $\mathrm{Tr}_{\mathrm{End}^0(A)/\mathbb{Q}}(\alpha\alpha^\dagger) > 0$ for any $\alpha \in \mathrm{End}^0(A) \setminus \{0\}$.

Let A be a simple abelian variety (not a product of smaller dimension abelian varieties). Then $D := \mathrm{End}(A_{\overline{K}})$ is a division algebra over $\mathbb{Q}$. Let F be the center of D (which is a number field). Let $F^0 \subseteq F$ be the fixed field of the Rosati involution.

Then the degree $[D : F]$ is d^2 for some $d \in \mathbb{Z}$, $e_0 = [F : F^0] \in \{1, 2\}$, and F^0 is totally real. Let $e = [F : Q]$.

Theorem 1.5 (Albert's classification)**.** *Suppose* $\mathrm{char}(k) = 0$ *and let* $g = \dim A$*. Then there are four types of endomorphism rings of abelian varieties:*

		e_0	d	$D \otimes_{\mathbb{Q}} \mathbb{R}$	constraint
I	$D = F = F^0$	1	1	$\mathbb{R}^e$	$e \mid g$
II	$F = F^0$	1	2	$M_2(\mathbb{R})^e$	$2e \mid g$
III	$F = F^0$	1	2	$\mathbb{H}^e$	$2e \mid g$
IV	$F \neq F^0$	2	$*$	$M_d(\mathbb{C})^{e/2}$	$\frac{1}{2}ed^2 \mid g$

Example 1.6. Throughout this example, (n) means this case defines a subspace of dimension n in the moduli space.

When $g = 1$, there are two possible cases: I $\mathbb{R}$ (1), II $\mathbb{C}$ (0).

When $g = 2$, all cases are technically possible, but case III does not appear for other reasons. For the other cases, we have: I $\mathbb{R}$ (3) or $\mathbb{R}^2$ (2), II $M_2(\mathbb{R})$ (1), IV $M_2(\mathbb{C})$ (0).

Torsion subgroups. Fix an abelian variety A/K of dimension g. The *n-torsion* subgroup of A is

$$A[n] = \{P \in A(\overline{K}) : nP = 0\}.$$

When $\mathrm{char}(K) \nmid n$, $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ (which is easy to see in characteristic 0).

The *n-torsion field* $K(A[n])$ is the minimal (Galois) extension L/K such that $A[n] = A(L)[n]$.

There is a *Weil pairing* $e_n \colon A[n] \times A^\vee[n] \to \mu_n(\overline{K})$ which is bilinear, non-degenerate, skew-symmetric, and Galois-equivariant. Given a polarization, we may view this as a map $e_n \colon A[n] \times A[n] \to \mu_n(\overline{K})$.

If P is a point of order n,

$$\{Q \in A[n] : e_n(P, Q) = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^g.$$

Theorem 1.7 (Mordell–Weil)**.** *If A is an abelian variety over a number field K, then $A(K)$ is a finitely-generated abelian group. In particular, it is isomorphic to*

$$\mathbb{Z}^r \oplus \underbrace{A(K)_{\mathrm{tors}}}_{\text{finite}}.$$

Hyperelliptic curves. Suppose $\mathrm{char}(K) \neq 2$. A *hyperelliptic curve* C is a degree 2 cover $C \to \mathbb{P}^1$. It has a model $y^2 = f(x)$.[1] Note that

$$g(C) = \left\lfloor \frac{\deg(f) - 1}{2} \right\rfloor$$

and assume $g(C) \geq 2$.

The cover is given by

$$\begin{aligned} C &\to \mathbb{P}^1, \\ (x, y) &\mapsto x. \end{aligned}$$

[1] In characteristic 2, the general equation is $y^2 + h(x)y = f(x)$ with $\deg h \leq g$, $\deg f \leq 2g + 2$.

Assume that $\deg(f)$ is odd for simplicity. Then there is only one point at infinity, which we denote by ∞. We then have a *hyperelliptic involution* $P \mapsto \overline{P}$ given by $(x, y) \mapsto (x, -y)$.[2]

A divisor $D = \sum n_P P$ is *effective* if $n_P \geq 0$. We may write it as

$$D = P_1 + \cdots + P_n$$

with possible repetitions.

Definition 1.8. An effective divisor is *semi-reduced* if $P_i \neq \overline{P_j}$ for $i \neq j$. If D is semi-reduced and $\deg D \leq g$ then D is *reduced*.

Definition 1.9. An *affine divisor* has no points at infinity.

Theorem 1.10 (Mumford)**.** *Every divisor class in* $\mathrm{Pic}^0(C)$ *can be uniquely represented by* $[D - n\infty]$ *where* D *is a reduced rational affine divisor and* $n = \deg D \leq g$.

Remark 1.11. This theorem holds more generally (replacing $n\infty$ by D_∞, a divisor supported at infinity), but this is the statement we will need for $\deg(f)$ odd.

Definition 1.12 (Mumford representation)**.** Let $D = P_1 + \cdots + P_n$ be a semi-reduced affine divisor where $P_i = (x_i, y_i) \in C(\overline{K})$. Then

$$u(x) = \prod (x - x_i) \in K[x]$$

is a monic polynomial. Let $v \in K[x]$ satisfy $\deg v < \deg u$ such that $v(x_i) = y_i$ (with approporiate multiplicity).

Then the *Mumford representation* of D is $[u, v]$. The condition on u and v is $u | v^2 - f$.

Remark 1.13. The Mumford representation allows one to efficiently implement addition of divisors on a computer. This is widely used in cryptography.

Remark 1.14. In the Mumford representation $-[u, v] = [u. - v]$. Therefore, the 2-torsion points in $\mathrm{Jac}(C) \cong \mathrm{Pic}^0(C)$ have Mumford representation $[v, 0]$.

2. Lecture 2: John Voight

The main reference for this lecture and more details is John Voight's book http://quatalg.org

Recall that modular curves parameterize elliptic curves with level structure. The goal of this lecture is to describe the following analog of this:

Shimura curves parametrize abelian surfaces with potential quaternionic multiplication (PQM).

We first briefly recall the situation for elliptic curves. There is a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h} \leftrightarrow \{\text{elliptic curves over } \mathbb{C}\}/\cong$$
$$\mathrm{SL}_2(\mathbb{Z})\tau \mapsto [\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})] = [E_\tau].$$

[2]The points of a hyperellptic cruve do not form a group, so we write $\overline{P}$ instead of $-P$ as in the case of elliptic curves.

The j-invariant defines a map

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \to \mathbb{A}^1(\mathbb{C}) = \mathbb{C}$$

and in fact

$$\{j \in F\} \leftrightarrow \{\text{elliptic curves over } F\}/\cong_{\overline{F}}.$$

We can add level structure:

$$\Gamma_0(N)\backslash\mathfrak{h} \leftrightarrow \{(E, C) \mid C \leq E[N],\ C \cong \mathbb{Z}/N\mathbb{Z}\}/\cong$$
$$\Gamma_0(N)\tau \mapsto \left[\left(E_\tau, \frac{1}{N}\right)\right].$$

Here

$$\Gamma_0(N) = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N\right\} \leq \mathrm{SL}_2(\mathbb{Z}),$$
$$\Gamma_1(N) = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N\right\} \leq \mathrm{SL}_2(\mathbb{Z}).$$

Let F be a field, $\mathrm{char} F \neq 2$. A *quaternion algebra* over F

$$B = \left(\frac{a, b}{F}\right) = F \oplus Fi \oplus Fj \oplus Fij$$

with

$$i^2 = a, j^2 = b, ij = -ji.$$

Example 2.1. We have that

$$\left(\frac{1, 1}{F}\right) \cong M_2(F),\ \left(\frac{-1, -1}{\mathbb{R}}\right) \cong \mathbb{H} \neq M_2(\mathbb{R})$$

We have the *standard involution*

$$B \to B$$
$$t + xi + yj + zij = \alpha \mapsto \overline{\alpha} = t - xi - yj - zij.$$

the *reduced trace*

$$\mathrm{trd}\colon B \to F$$
$$\alpha \mapsto \alpha + \overline{\alpha},$$

and *reduced norm*

$$\mathrm{nrd}\colon B \to F$$
$$\alpha \mapsto \alpha\overline{\alpha}.$$

For a place v, over $\mathbb{Q}_v$ (which is either $\mathbb{R}$ or $\mathbb{Q}_p$), there is a unique division algebra over $\mathbb{Q}_v$, up to isomorphism.

We say that B over $\mathbb{Q}$ is *ramified* at v if $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a division algebra (otherwise, $B_v \cong M_2(\mathbb{Q}_v)$). Let

$$\mathrm{Ram}(B) = \{v \mid B \text{ is ramified at } v\}$$

and

$$\operatorname{disc}(B) = \prod_{\substack{p \in \operatorname{Ram}(B) \\ p \neq \infty}} p.$$

Theorem 2.2 (Classification)**.** *The map*

$$\{\textit{quaternion algebras over } \mathbb{Q}\}/\cong \leftrightarrow \{\textit{positive squarefree integers}\}$$
$$[B] \mapsto \operatorname{disc} B$$

is bijective. Moreover, $\#\operatorname{Ram}(B)$ *is finite and even.*

In particular, $\infty \in \operatorname{Ram}(B)$ if and only if $\#\{p \mid \operatorname{disc}(B)\}$ is odd. In this case, B is called *definite*.

Example 2.3. Consider $B = \left(\frac{-1,3}{\mathbb{Q}}\right)$. Clearly, $\operatorname{Ram}(B) \subseteq \{2, 3, \infty\}$. We check that

$$B \otimes_{\mathbb{Q}} \mathbb{R} = \left(\frac{-1,3}{\mathbb{R}}\right) \cong \left(\frac{-1,1}{\mathbb{R}}\right) \cong M_2(\mathbb{R}).$$

Hence either $\operatorname{Ram}(B) = \{2, 3\}$ or $\operatorname{Ram}(B) = \emptyset$. We see that

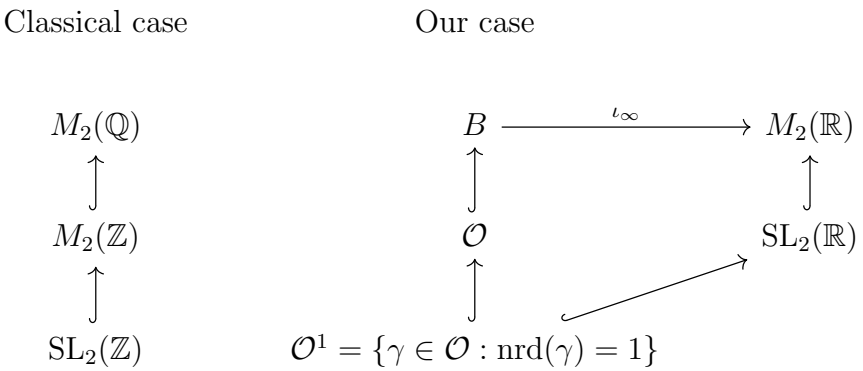
$$B \otimes_{\mathbb{Q}} \mathbb{Q}_3 \ncong M_2(\mathbb{Q}_3)$$

because $\left(\frac{-1}{3}\right) = -1$. Therefore,

$$\operatorname{Ram}(B) = \{2, 3\}$$

and so $\operatorname{disc} B = 6$. This is the quaternion algebra with the smallest discriminant (not equal to 1), so it will come up as an example a lot.

With this notation set up, we can present a more thorough overview. Let B be an indefinite quaternion algebra over $\mathbb{Q}$. We take it to be indefinite so that it embeds into $M_2(\mathbb{R})$, giving an action on $\mathcal{H}$. We do this with analogy to the classical case. The undefined terms in the diagram will be defined shortly and the details will be completed.



Then $\mathcal{O}^1$ acts on $\mathcal{H}$ via the embedding ι_∞. Recall that $E_\tau = \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$. In our case, we define $A_\tau = \mathbb{C}^2/\iota_\infty(\mathcal{O})\binom{\tau}{1}$.

Let $F = \mathbb{Q}$, $D = \operatorname{disc}(B) \in \mathbb{Z}$. Let $\mathcal{O} \subseteq B$ be an *order*: a subring, finitely-generated as a $\mathbb{Z}$-module, containing a $\mathbb{Q}$-basis of B. Equivalently, $\mathcal{O}$ is a $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of B which is closed under multiplication.

Example 2.4. Note that $M_2(\mathbb{Z}) \subseteq M_2(\mathbb{Q})$ is a maximal order. If $a, b \in \mathbb{Z} \setminus \{0\}$, then $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ is an order, but it need not be maximal.

Example 2.5 ($\operatorname{disc} B = 6$)**.** A maximal order is

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\underbrace{\left(\frac{1+i+j+ij}{2}\right)}_{k},$$

where $k^2 - k - 1 = 0$.

Let $B/\mathbb{Q}$ be indefinite. Then $\iota_\infty \colon B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$. Let $B^1 = \{\gamma \in B^\times : \operatorname{nrd}(\gamma) = 1\} = \ker \operatorname{nrd} \leq B^\times$ and define $\mathcal{O}^1 = \mathcal{O} \cap B^1$. Then $B^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ by fractional linear transformations,

Let $\Gamma^1(\mathcal{O}) = \iota_\infty(\mathcal{O}^1)/\{\pm 1\} \leq \mathrm{PSL}_2(\mathbb{R})$. It is a *Fuchsian group*, a discrete subgroup acting properly on $\mathcal{H}$. Then

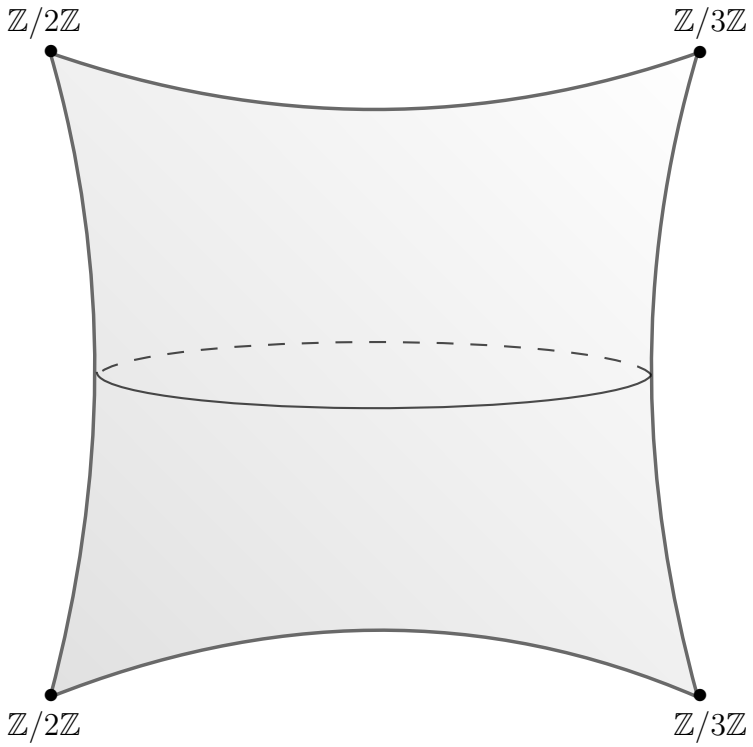
$$Y^1(\mathcal{O}) := \Gamma^1(\mathcal{O})\backslash\mathcal{H}$$

is a good complex 1-orbifold. It is compact if and only if $B \ncong M_2(\mathbb{Q})$. Otherwise:

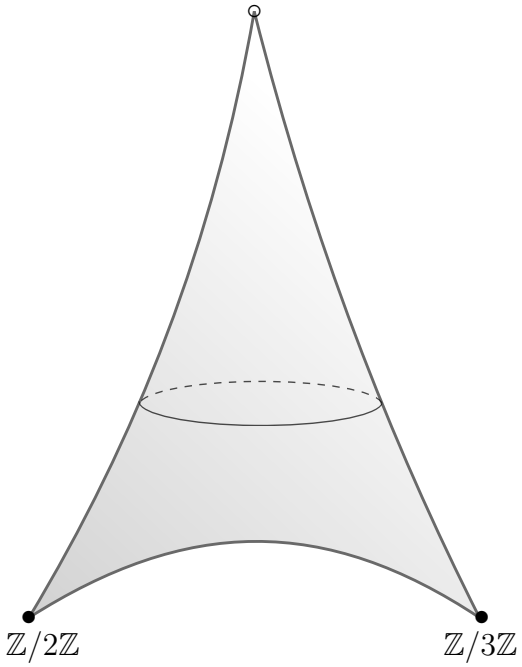
$$X^1(\mathcal{O}) := Y^1(\mathcal{O}) \cup \{\text{cusps}\}$$

is a *compactification*.

Example 2.6 ($\operatorname{disc} B = 6$)**.** We present a schematic diagram of the 1-orbifold $Y^1(\mathcal{O})$ in our recurring discriminant 6 example. The points with non-trivial stabilizers are in the four corners are we write down the stabilizer groups at these points.



For comparison, we present the corresponding diagram for the classical modular curve for $\mathrm{SL}_2(\mathbb{Z})$.



To a point $\tau \in \mathcal{H}$, we associate

$$\Lambda_\tau = \iota_\infty(\mathcal{O})\begin{pmatrix}\tau\\1\end{pmatrix} \subseteq \mathbb{C}^2,$$

which is a lattice. (Note that $\mathcal{O} \cong \mathbb{Z}^4$ as abelian groups.) Then

$$A_\tau := \mathbb{C}^2/\Lambda_\tau$$

and we have a natural map $i_\tau \colon \mathcal{O} \hookrightarrow \mathrm{End}(A_\tau)$. Then A_τ is a complex torus of dimension 2 with endomorphisms by $\mathcal{O}$.

A *principal polarization* on $\mathcal{O}$ is an element $\mu \in \mathcal{O}$ such that $\mu^2 + D = 0$, where $D = \operatorname{disc} B$. Every maximal order has a principal polarization.

Example 2.7 ($\operatorname{disc} B = 6$)**.** A principal polarization is $\mu = 3i + ij = -1 + 2i - j + 2k$. One easily checks that $\mu^2 + 6 = 0$.

The involution

$$\begin{aligned} B &\to B \\ \alpha &\mapsto \alpha^* := \mu^{-1}\overline{\alpha}\mu \end{aligned}$$

is positive ($\mathrm{Tr}(\alpha^*\alpha) > 0$ for any $\alpha \in B \setminus \{0\}$).

Example 2.8. For $M_2(\mathbb{R})$, $\alpha^* = \overline{\alpha}^T$ and we see that $\mathrm{Tr}(\alpha^*\alpha) = 2(a^2 + b^2 + c^2 + d^2) > 0$ where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$.

Then μ induces a principal polarization (and hence a Riemann form) on A_τ.

Theorem 2.9. *The map*

$$Y^1(\mathcal{O}) \leftrightarrow \left\{ \begin{array}{c} (A,\iota) \text{ principally polarized} \\ \text{complex abelian surfaces} \\ \text{with QM } \iota \text{ by } (\mathcal{O},\mu) \end{array} \right\} \Big/ \cong$$
$$\Gamma\tau \mapsto [(A_\tau, \iota_\tau)]$$

is a bijection. Here, QM by $(\mathcal{O},\mu)$ *means the diagram*

$$\begin{array}{ccc} B & \xhookrightarrow{\iota} & \mathrm{End}(A) \otimes \mathbb{Q} \\ \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle \dagger} \\ B & \xhookrightarrow{\iota} & \mathrm{End}(a) \otimes \mathbb{Q} \end{array}$$

commutes.

Theorem 2.10 (Shimura, Deligne)**.** *There exists a nice curve* $X^1_{\mathbb{Q}}$ *defined over* $\mathbb{Q}$ *and a holomorphic map*

$$\varphi\colon \mathcal{H} \to X^1_{\mathbb{Q}}(\mathbb{C})$$

that induces a biholomorphism

$$\varphi\colon \Gamma^1\backslash\mathcal{H} \to X^1_{\mathbb{Q}}(\mathbb{C}).$$

Remark 2.11. This map is the analog of the j-invariant $j\colon \mathcal{H} \to \mathbb{P}^1(\mathbb{C})$. (The curve $X^1_{\mathbb{Q}}$ is just $\mathbb{P}^1_{\mathbb{Q}}$.)

Example 2.12 ($\operatorname{disc} B = 6$, Baba–Granath)**.** The curve $X^1_{\mathbb{Q}}$ in this case is defined by the equation $x^2 + 3y^2 + z^2 = 0$ in $\mathbb{P}^2$. Note that $X^1_{\mathbb{Q}}(\mathbb{R}) = \emptyset$ in this case.

The last statement is true in more generally.

Theorem 2.13 (Ogg, Shimura)**.** *If* B *is a division algebra, there are no real points on* $X^1_{\mathbb{Q}}$.

Therefore, the study of rational points on Shimura curves is void in the global case.

3. Lecture 3 (Drew Sutherland)

Galois representations. Let A be an abelian variety of dimension g over a number field K. Then

$$A[n] \cong (\mathbb{Z}/n/Z)^{2g}.$$

We write $G_K = \mathrm{Gal}(\overline{K}/K)$. We then have a natural Galois representation

$$\rho_{A,n}\colon G_K \to \mathrm{Aut}(A[n]) \subseteq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

The image of the representation is smaller than $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$ because of the Weil pairing. More specifically, there is a basis for $A[n]$ such that

$$\rho_{A,n}(\sigma)^t \Omega \rho_{A,n}(\gamma) = \lambda\Omega \qquad \text{for } \Omega = \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix} \text{ and } \sigma(\zeta_n) = \zeta_n^\lambda.$$

This motivates the following definition.

Definition 3.1. Let R be any ring. The group of *symplectic similitudes* is

$$\mathrm{GSp}_{2g}(R) = \{M \in \mathrm{GL}_{2g}(R) : M^t \Omega M = \lambda\Omega \text{ for } \lambda \in R^x\}.$$

The *symplectic group* is the kernel of the map $M \mapsto \lambda(M)$:

$$\mathrm{Sp}_{2g}(R) = \{M \in \mathrm{GSp}_{2g}(R) : \lambda(M) = 1\}.$$

Choosing compatible bases of $A[n]$, we get a representation

$$\rho_A \colon G_K \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) = \varprojlim_n \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

where

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

We have a natural map

$$\pi_n \colon \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

and ρ_A is defined by the property $\rho_{A,n} = \pi_n \circ \rho_A$.

Then ρ_A is a continuous homomorphism of topological groups.

Remark 3.2. For $g = 1$, $\mathrm{GSp}_2 = \mathrm{GL}_2$.

Having restricted the image to GSp_{2g}, it is natural to ask when ρ_A is surjective (or has image with finite index).

Theorem 3.3 (Serre's open image theorem)**.** *For a non-PCM elliptic curve E/K, $\operatorname{Im}\rho_E$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

Therefore, for $\ell \gg 0$, $\operatorname{Im}\rho_E$ contains $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Writing

$$\rho_{A,\ell^\infty} \colon G_K \to \mathrm{GSp}(\mathbb{Z}_\ell)$$

for the analogous representation, we see that ρ_{E,ℓ^∞} is surjective (when E is an elliptic curve without PCM) for all sufficiently large ℓ.

Conjecture. There is an N_d such that for any non-PCM elliptic curve E over K of degree d, $\operatorname{im}\phi_{E,\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell > N_d$. Moreover, for $d = 1$, $N_d = 37$.

There is some numerical and theoretical reasons to conjecture that $N_1 = 37$. It is enough to consider the mod ℓ image. The possible normal subgroups are:

- Borel $\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$: this was addressed by Mazur by proving that non-CM elliptic curves do not have an ℓ-isogeny for $\ell > 37$,
- the normalizer of a split Cartan $\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\} \cong (\mathbb{F}_\ell^\times)^2$: this case was solved even for $\ell > 13$,
- the normalizer of a non-split Cartan $\cong \mathbb{F}_{\ell^2}^\times$: this is a big open problem,
- a few exceptional groups: this case is also known for $\ell > 13$.

Generalizing this to abelian varieties, Serre proved that if $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ and $\dim A$ is 2, 6, or odd, then $\operatorname{im}\rho_A$ is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

Absolute Frobenius. Let $p \in \mathbb{Z}$ and pick a prime ideal $\mathfrak{q}$ above p in $\overline{\mathbb{Z}}$. Let $\mathbb{F}_\mathfrak{q} = \overline{\mathbb{Z}}/\mathfrak{q}$. Then $\mathbb{F}_\mathfrak{q} \cong \overline{\mathbb{F}_p}$ and

$$\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}.$$

The *decompositiion group* is

$$D_\mathfrak{q} = \{\sigma \in G_\mathbb{Q} : \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Each $\sigma \in D_\mathfrak{q}$ acts on $\mathbb{F}_\mathfrak{q} = \overline{\mathbb{Z}}/\mathfrak{q}$ via $\sigma(x + \mathfrak{q}) = \sigma(x) + \mathfrak{q}$.

We get a surjective homomorphism

$$D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_p).$$

An *absolute Frobenius element* Frob_p is any preimage in $D_\mathfrak{q}$ of the Frobenius automorphism $x \mapsto x^p$. It is well-defined up to the action by the inertia subgroup

$$I_\mathfrak{q} = \{\sigma \in G_\mathbb{Q} : \sigma(x) \equiv x \mod \mathfrak{q} \text{ for all } x \in \overline{\mathbb{Z}}\}.$$

For any finite extension $L/\mathbb{Q}$, we have that $\mathrm{Frob}_p|_L = \mathrm{Frob}_{\mathfrak{q}\cap L}$ defined in the normal way.

Theorem 3.4. *If $L/\mathbb{Q}$ is a finite extension in which p is unramified, the conjugacy class of $\mathrm{Frob}_p|_L$ is uniquely determined.*

Remark 3.5. Everything above applies to number fields other than $\mathbb{Q}$: replace $\mathbb{Q}$ by K and replace p by a prime $\mathfrak{p}$ of K.

Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime of good reduction for A/K. If $\mathfrak{p}$ does not divide n, then $\mathfrak{p}$ is unramified in $K(A[n])$. Then

$$\rho_{A,n}(\mathrm{Frob}_\mathfrak{p}) = \pi_{A_\mathfrak{p}}|_{A[n]} \in \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

where $\pi_{A_\mathfrak{p}} \colon A_\mathfrak{p} \to \mathbb{A}_\mathfrak{p}$ is the Frobenius endomorphism induced by $x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}$ where $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

Therefore, the characteristic polynomial of $\rho_{A,n}(\mathrm{Frob}_\mathfrak{p})$ is the characteristic polynomial of $\pi_{A_\mathfrak{p}}$ modulo n.

Zeta functions. Let X be a smooth projective curve over $\mathbb{F}_q$. Then

$$Z_X(T) = \exp\left(\sum_{n\geq 1} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) = \frac{L(T)}{(1-T)(1-qT)}.$$

Then $L(T) \in \mathbb{Z}[T]$ has degree $2g$ and the roots α have $|\alpha| = q^{-1/2}$. Then

$$L(T) = q^g T^{2q} + a_1 q^{g-1} T^{2g-1} + \cdots + a_g T^g + a_{g-1} T^{g-1} + \cdots + a_1 T + 1$$

where

$$a_1 = -\operatorname{Tr} \pi_{\mathrm{Jac}(X)},$$

the trace of Frobenius acting on the Jacobian of X. In general, the characteristic polynomial of $\pi_X = \pi_{\mathrm{Jac}(X)}$ (acting on the Tate module) is $T^{2g}L(T^{-1})$.

A key fact is that $Z_X(T)$ is determined by $\#X(\mathbb{F}_{q^n})$ for $1 \leq n \leq g$.

For a smooth projective curve over a number field, we define the L-function via an Euler product

$$L(X, s) = \prod_\mathfrak{p} L_\mathfrak{p}(N(\mathfrak{p})^{-s})^{-1}$$

(one also needs to define $L_{\mathfrak{p}}(T)$ for primes of bad reduction).

Let A/K be a QM abelian surface with QM by $\mathcal{O}$. Let $\mathfrak{p}$ be a prime of K which is good for A. Since $\mathcal{O} \subseteq \mathrm{End}(A_{\mathfrak{p}})$ and $\pi \in \mathrm{End}(A_{\mathfrak{p}})$, $\mathrm{End}^0(A_{\mathfrak{p}})$ contains $\mathcal{O}$ and a splitting of the characteristic polynomial of π.

Albert's classification 1.5 shows that

$$\mathrm{End}^0(A_{\mathfrak{p}}) \otimes_{\mathbb{Q}} \mathbb{R} \cong \begin{cases} M_2(\mathbb{C}) & \text{ordinary reduction} \\ M_2(\mathbb{H}) & \text{supersingular reduction} \end{cases}$$

and hence

$$A_{\mathfrak{p}} \sim E^2 \quad \text{for some elliptic curve } E/\mathbb{F}_{\mathfrak{p}}$$

and $L_A(T) = L_E(T)^2$. However, for different $\mathfrak{p}$, the eliptic curve E is different.[3] Therefore, these abelian surfaces are sometimes called *fake elliptic curves*.

For $E/\mathbb{Q}$, we have that

$$\ker \rho_{E,n} = \{\sigma \in G_\sigma : \sigma|_{\mathbb{Q}(E[n])} = 1\},$$
$$\mathrm{im}\, \rho_{E,n} = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Typically, $\mathrm{im}(\rho_{E,n} = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}))$, but not always.

(1) If E has extra level n structure, for example a rational point of order n, then

$$\mathrm{im}\, \rho_{E,n} \subseteq \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

(2) If E has extra endomorphisms, $\mathrm{End}(E) = \mathcal{O}$ where $\mathcal{O}$ is an imaginary quadratic order in K, then $\mathrm{Gal}(K(E[n])/K)$ is abelian, so

$$\mathrm{im}\, \rho_{E,n} \neq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \text{ for any } n > 1.$$

Let E/K be an elliptic curve with CM by $\mathcal{O}$. Then $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2. In fact, more is true.

Lemma 3.6. *The n-torsion $E[n]$ is a free $\mathcal{O}/n\mathcal{O}$ module of rank 1.*

Proof. Fix $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ so that $E[n] \cong \frac{1}{n}\Lambda/\Lambda$ as $\mathcal{O}/n\mathcal{O}$-modules. Since $\mathbb{C}/\Lambda$ is an $\mathcal{O}$-module, $\mathcal{O}\Lambda = \Lambda$. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$, $\mathfrak{p}|n$,

$$\left(\frac{1}{n}\Lambda/\Lambda\right) \otimes_{\mathcal{O}} (\mathcal{O}/\mathfrak{p}) \cong \frac{1}{n}\Lambda/\mathfrak{p}\frac{1}{n}\Lambda.$$

We have that

$$\mathcal{O}/n\mathcal{O} \cong \prod_{\mathfrak{p}|n} \mathcal{O}/\mathfrak{p}^e,$$

so

$$E[n] \cong \prod_{\mathfrak{p}|n} \frac{1}{n}\Lambda/\mathfrak{p}^e\frac{1}{n}\Lambda.$$

Let I be the fractional $\mathcal{O}$-ideal $\frac{1}{n}\Lambda$. Then $I/\mathfrak{p}^e I$ is a free $\mathcal{O}/\mathfrak{p}^e$-module of rank 1. □

[3] This is discussed further in the exercises.

Corollary 3.7. *The image is* $\operatorname{im}\rho_E \subseteq \mathrm{GL}_1(\widehat{\mathcal{O}}) \cong \widehat{\mathcal{O}}^\times \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. *Here* $\widehat{\mathcal{O}} = \varprojlim_n \mathcal{O}/n\mathcal{O}$. *Also,*

$$\operatorname{im}\rho_{E,p} = (\mathcal{O}/p)^\times \cong \begin{cases} (\mathbb{F}_p^\times)^2 & \text{if } p \text{ is split,} \\ \mathbb{F}_{p^2}^\times & \text{if } p \text{ is inert,} \\ \mathbb{F}_p^\times & \text{if } p \text{ is ramified.} \end{cases}$$

Now, suppose that A/K is a QM abelian surface with QM by $\mathcal{O}$ (an order in a quaternion algebra).

Lemma 3.8. *The n-torsion $A[n]$ is a free $\mathcal{O}/n\mathcal{O}$-module of rank 1.*

Proof. Follow the proof of Lemma 3.6 in the CM case. Now the torus is $\mathbb{C}^2/\Lambda$ and $\mathfrak{p}|n$ is a two-sided $\mathcal{O}$-ideal. □

Corollary 3.9. *The image is* $\operatorname{im}\rho_A \subseteq \mathrm{GL}_1(\widehat{\mathcal{O}}) \cong \widehat{\mathcal{O}}^\times \subseteq \mathrm{GSp}_4(\widehat{\mathbb{Z}})$. *Also,*

$$\operatorname{im}\rho_{E,p} = (\mathcal{O}/p\mathcal{O})^\times \cong \begin{cases} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) & \text{if } p \text{ is unramified,} \\ \text{exercise} & \text{if } p \text{ is ramified.} \end{cases}$$

Suppose A/K is a QM abelian surface with a rational point P of order n. Then $A[n]$ is an $\mathcal{O}$-module so $A(K)[n]$ must contain $\mathcal{O}P$ (a cyclic $\mathcal{O}$-module). If n is coprime to $\operatorname{disc}(\mathcal{O})$, then $\mathcal{O}P \cong (\mathbb{Z}/n\mathbb{Z})^2 \subseteq A(K)[n]$.

4. Lecture 4 (John Voight)

The goal of this lecture is to work explicitly with Shimura curves.

(1) Fundamental domains.
(2) Equations using power series expansions of modular forms.

4.1. Fundamental domains.

Let $\Gamma \leq \mathrm{PSL}_2(\mathbb{R})$ be a Fuchsian group such that $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ has finite hyperbolic area.

Definition 4.1. A *fundamental domain* $\square \subseteq \mathcal{H}$ for Γ satisfies:

(1) the closure of the interior of $\square$ is $\square$,
(2) $\Gamma\square = \mathcal{H}$,
(3) $\operatorname{int}(\square) \cap \operatorname{int}(\gamma\square) = \emptyset$ for all $\gamma \in \Gamma$, $\gamma \neq 1$,
(4) $\mu(\partial\square) = 0$.

Definition 4.2. Let $z_0 \in \mathcal{H}$ be such that $\mathrm{Stab}_\Gamma(z_0) = \{1\}$. The *Dirichlet domain* for Γ at z_0 is

$$\square = \square(\Gamma; z_0) = \{z \in \mathcal{H} : \rho(z, z_0) \leq \rho(\gamma z, z_0) \text{ for all } \gamma \in \Gamma\},$$

where ρ is the hyperbolic metric.

Then

$$\square = \bigcap_{\gamma \in \Gamma} H(\gamma; z_0)$$

where

$$H(\gamma; z_0) = \{z \in \mathcal{H} : \rho(z, z_0) \leq \rho(\gamma z, z_0) = \rho(z, \gamma^{-1} z_0)\}.$$

Theorem 4.3. *The Dirichlet domain $\square(\Gamma; z_0)$ is a connected, convex, locally finite (for any $K \subseteq \mathcal{H}$ compact, $\gamma K \cap \square \neq \emptyset$ for only finitely many γ) fundamental domain for Γ with geodesic boundary.*

The isomorphism

$$\varphi \colon \mathcal{H} \xrightarrow{\sim} \mathcal{D} = \{z \in \mathbb{C} : |z| < 1\},$$
$$z \mapsto \frac{z - z_0}{z - \overline{z_0}} = w.$$

takes the action Γ on $\mathbb{H}$ to an action of $\varphi_*(\Gamma) \subseteq \mathrm{PSU}(1,1) \leq \mathrm{GL}_2(\mathbb{C})$ on $\mathcal{D}$.

For $\gamma \in \Gamma$, let $I(\gamma) = \{w \in \mathbb{C} : |cw + d| = 1\}$ if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \phi(\Gamma)$. This is the *isometric cicle*.

We need to decide whether $\rho(w, 0)$ is smaller, bigger, or the same as $\rho(\gamma w, 0)$. This is determined by whether w belongs to $\mathrm{ext}(I(\gamma))$, $I(\gamma)$, or $\mathrm{int}(I(\gamma))$, respectively. Therefore,

$$\square(\Gamma; 0) = \bigcap_{\gamma \in \Gamma \setminus \{1\}} \mathrm{cl}\,\mathrm{ext}\, I(\gamma).$$

If $\Gamma_0 := \mathrm{Stab}_\Gamma(z_0) \neq \{1\}$, then

$$\square = \bigcup_{\gamma_0 \in \Gamma_0} \gamma_0 \square',$$

where $\square'$ is the intersection $\square$ with the part of the semicircle spanned by the angle $\dfrac{2\pi}{\#\Gamma_0}$. In that case, $\square'$ is a fundamental domain for Γ.

Definition 4.4. A *side* of $\square$ is a geodesic segment of $\square \cap \gamma\square$, $\gamma \in \Gamma \setminus \{1\}$ *except* with the convention that if $L = \square \cap \gamma\square$ for $\gamma^2 = 1$, we say that γ *fixes the midpoint* by L and we doubt it.

Theorem 4.5. *The group Γ is generated by the side pairing elements*

$$\{\gamma \in \Gamma : \square \cap \gamma\square\} \neq \emptyset$$

and relations can be read off from the vertices.

Remark 4.6. There is, of course, a specific description of how the relations are *read off from the vertices*, but we omit this here.

Example 4.7 ($\mathrm{disc}\, B = 6$)**.** We go back to our main example where $\mathrm{disc}\, B = 6$. Recall that $\Gamma = \Gamma^1(\mathcal{O}) = \iota_\infty(\mathcal{O}^1)/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R})$. Here

$$\varphi(z) = w = \frac{z - i}{z + i}.$$

For $\gamma = t + xi + yj + zij \in \mathcal{O}^1$,

$$\varphi_*(\gamma) = \begin{pmatrix} t - ix & \sqrt{3}(y - iz) \\ \sqrt{3}(y + iz) & t + ix \end{pmatrix}$$

Then $I(\gamma)$ is a circle with radius $\dfrac{1}{|c|} = \dfrac{1}{\sqrt{3(y^2+z^2)}}$ and center $\dfrac{-d}{c} = \dfrac{-(t+ix)}{\sqrt{3}(y+iz)}$, unless $y^2 + z^2 = 0$ whence $\gamma \in \{\pm 1, \pm i\} = \langle i \rangle$, the stabilizer of 0.

To try to find the fundamental domain, we find circles $I(\gamma)$ with biggest radii, i.e. the smallest value of $y^2 + z^2$.

The smallest possible value would be $y^2 + z^2 = \frac{1}{4}$, but this case is ruled out by the parity condition on y and z. The next smallest possiblity is $y^2 + z^2 = \frac{1}{2}$. After a short calculation, we see that the possiblities are

$$\gamma = \pm\frac{3}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}ij,$$

$$\gamma = \pm\frac{1}{2} \pm \frac{3}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}ij.$$

This allows one to draw a picture of the fundamental domain for this group. We omit this here, however, and refer the reader to the book.

Then $\Gamma = \langle \gamma_1, \gamma_2, \gamma_3 \mid \gamma_1^2 = \gamma_2^3 = \gamma_3^3 = (\gamma_3\gamma_2\gamma_1)^2 = 1 \rangle$. One can rewrite it by setting $\gamma_4 = \gamma_3\gamma_2\gamma_1$ to get the nicer presentation:

$$\Gamma = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4 \mid \gamma_1^2 = \gamma_2^3 = \gamma_3^3 = \gamma_4^2 = \gamma_4\gamma_3\gamma_2\gamma_1 = 1 \rangle.$$

We remark that Γ is an index four subgroup of a triangle group[4]. This is also visible on the picture which can be divided into 8 triangles.

4.2. **Modular forms.** Riemann's theorem says that any Riemann surface is an algebraic curve over $\mathbb{C}$. To prove it, one needs to write down enough holomorphic functions on this Riemann surface to embed it into projective space. One way of producing them is by taking quotient of differential forms. Modular forms are functions that transform in the same way as differential forms.

Assume that $Y(\Gamma) = X(\Gamma)$ is compact, so it has no cusps.

Definition 4.8. A *modular form* of weight $k \in 2\mathbb{Z}_{\geq 0}$ for Γ is a holomorphic map $f \colon \mathcal{H} \to \mathbb{C}$ such that

$$f(\gamma z) = (cz + d)^k f(z) \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \leq \mathrm{PSL}_2(\mathbb{R}).$$

The vector space of weight k modular forms for Γ is denoted $M_k(\Gamma)$.

Since $Y(\Gamma)$ has no cusps, we do not have Fourier expansions for these modular forms. However, we may write down a regular Taylor expansion of $f(z)$ considered as a function of w

[4]Triangle groups are Fuchsian groups whose fundamental domains are obtained by reflecting a triangle along one of its sides. They are particularly easy to work with.

on the unit disc:

$$f(z) = (1-w)^k \sum_{n=0}^{\infty} b_n w^n \in M_k(\Gamma).$$

Example 4.9. The modular form

$$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \in S_2(\Gamma_0(11))$$

at $z_0 = \frac{-9+\sqrt{-7}}{2}$ (a CM point) has expansion

$$f(z) = c_0(1-w)^2(1-\Theta w + \frac{5}{2!}(\Theta w)^2 - \frac{123}{3!}(\Theta 2)^3 - \cdots)$$

where $\Theta = \frac{-4+2\sqrt{-7}}{11}\pi\Omega^2$, where $\Omega \approx 0.500491$ is the *Chowla-Selberg* period.

In general,

$$f(z) \approx f_N(z) = (1-w)^k \sum_{n=0}^{N} b_n w^n,$$

valid for $|w| \leq \rho$ to precision $\varepsilon > 0$. Here, ρ is the radius of any circle containing the fundamental domain $\square \subseteq \mathcal{D}$.

For $w \notin \square$, $|w| \leq \rho$, there is a $\gamma \in \Gamma$ such that $w' = \gamma w \in \square$. Let $z \in \mathcal{H}$ correspond to w and $z' \in \mathcal{H}'$ correspond to w'. Then

$$f_N(z') \approx f(z') = (cz+d)^k f(z) \approx (cz+d)^k f_N(z).$$

Therefore,

$$(1-w')^k \sum_{n=0}^{N} b_n (w')^n \approx (cz+d)^k (1-w)^k \sum_{n=0}^{N} b_n w^n.$$

The b_n's are unknown but the rest of the things involved here are known. For example, having picked any w, to get w', we can repeatedly apply generators of Γ to w until we reach the fundamental domain. If $\square$ is a Dirichlet domain, any of the generators obtained by Theorem 4.5 bring the elements closer to the fundamental domain.

This gives a numerical method to compute the b_n's.

When $\Gamma \leq \Delta$ and Δ is a triangle group, one can certify the output of this procedure as rigorous. Otherwise, this is an open problem.

Theorem 4.10 (Valence formula, Shimura)**.** *The dimension of the space of weight k modular forms for Γ is*

$$\dim_{\mathbb{C}} M_K(\Gamma) = \begin{cases} 1 & \text{if } k = 0 \\ g & \text{if } k = 2 \\ (k-1)(g-1) + \sum_{i=1}^{r} \left\lfloor \frac{k}{2}\left(1 - \frac{1}{e_i}\right)\right\rfloor & \text{if } k \geq 4 \end{cases}$$

where Γ has signature $(g; e_1, \ldots, e_r)$: genus g, orders of stabilizers $e_1, \ldots, e_r$, and no cusps.

Example 4.11 ($\operatorname{disc} B = 6$)**.** In this case, $\operatorname{sig}(\Gamma) = (0; 2, 2, 3, 3)$, so

$$\dim M_k(\Gamma^1) = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{if } k = 2 \\ 1 - k + 2\left\lfloor \frac{k}{4} \right\rfloor + 2\left\lfloor \frac{k}{3} \right\rfloor & \text{if } k \geq 4. \end{cases}$$

We make a table with some of the dimensions and generators[5]:

k	0	2	4	6	8	10	12	$\cdots$	24
dim	1	0	1	1	1	1	3	$\cdots$	5
generators	1	–	f_4	g_6	f_4^2	$f_4 g_6$	f_3^4, g_6^2, h_{12}	$\cdots$	$(*)$

We can *produce* 6 new function in $M_{24}(\Gamma^1)$ from the lower weights

$$f_4^7,\ f_4^3 g_6^2,\ f_4^3 h_{12},\ g_6^4,\ g_6^2 h_{12},\ h_{12}^2,$$

so they are linearly dependent! Working out the linear dependence, we obtain:

$$M(\Gamma) = \bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} \cong \frac{\mathbb{C}[x_4, x_6, x_{12}]}{(x_4^6 + 3x_6^4 + x_{12}^2)}.$$

This gives

$$Y(\Gamma) = X(\Gamma) \cong \operatorname{Proj} M(\Gamma) \subseteq \mathbb{P}(4, 6, 12) \hookrightarrow \mathbb{P}^2$$

with the embedding into $\mathbb{P}^2$ given by

$$z \mapsto \left(f_4^3(z) : g_6^2(z) : h_{12}(z)\right).$$

[5]We do not explicitly write down what f_4, g_6, h_{12} are here; they can be treated as the remaining generator in each case. They are written down in the book.