Notes on
MATH 678
(Modular Forms)

September 22, 2023

Faye Jackson

Contents

I. Introduction and Motivation

Goals:

- Goals of the book: To explain the statement of the modularity theorem.
  - The book introduces many things: modular forms, elliptic curves, modular curves. These are all relevant to modern mathematics, and so are their generalizations, that is: automorphic forms/representations, abelian varieties, Shimura varieties.
  - The first is the $\mathrm{SL}_2(\mathbb{R})$ version, and the rest are the general G versions.
- Our Goal: Be able to think about these things both in specific and in general.

II. The Basics

II.1. Modular Forms

Definition II.1.1

The modular group is $\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1, a, b, c, d \in \mathbb{Z} \right\}$.

Exercise II.1.1

This group is generated by

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

We'll also think often of the upper half-plane $\mathcal{H} \subseteq \widehat{\mathbb{C}}$, which is the set $\{a + bi \mid b > 0\}$.

We know $\mathrm{SL}_2(\mathbb{R})$ acts on $\widehat{\mathbb{C}}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

Then $\mathcal{H} = \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}_2(\mathbb{R})$.

Definition II.1.2

Let $k \in \mathbb{Z}$. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is called weaklymodular of weight k provided that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Example II.1.2

If in weight zero, this is $\mathrm{SL}_2(\mathbb{Z})$-invariant. Then $f : (\mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}_2(\mathbb{R})) / \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{Z}$.

Example II.1.3

Consider $\mathrm{d}\tau$. Then for $f(\tau)\,\mathrm{d}\tau$ to be invariant we need f to be weight two, as $\mathrm{d}(\gamma(\tau)) = (c + d\tau)^{-2}\,\mathrm{d}\tau$.

Definition II.1.3

A modular form $f : \mathcal{C} \to \mathbb{C}$ of weight k is

- weakly modular of weight k.

- holomorphic on $\mathcal{H}$.
- holomorphic at ∞.

Let D be the complex unit disk, $D' = D \setminus \{0\}$. Then $\tau \mapsto e^{2\pi i\tau}$ takes $\mathcal{H} \to D'$ and is $\mathbb{Z}$-periodic. Because $f(\tau) = f(\tau+1)$ for any weakly modular form, we know f factors through the map $\mathcal{H} \to D'$ as some $g : D' \to \mathbb{C}$. Saying f is holomorphic at ∞ is equivalent to saying that it extends holomorphically to D.

We reserve the letter $q = e^{2\pi i\tau}$. We know $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for $q \in D'$. Holomorphic at ∞ can also be understood as $a_n = 0$ for $n < 0$. Thus we have a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n.$$

Set $M_k(\mathrm{SL}_2(\mathbb{Z}))$ to be the weight k modular forms, then

Exercise II.1.4

Try this:

$$M(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_k M_k(\mathrm{SL}_2(\mathbb{Z})).$$

Actual Example: "Weight k Eisenstein series" for $k > 2$ even.

$$G_k(\tau) = \sum_{(c,d)}{}' \frac{1}{(c\tau + d)^k}.$$

where $\sum'_{(c,d)}$ means

$$\sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}}.$$

Exercise II.1.5

G_k is weakly modular of weight k.

Strategy: Write it out and then use that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on the index set.

For holomorphicity use the fact that

$$\sum_{d\in\mathbb{Z}} \frac{1}{\tau + d} = \pi\cot(\pi\tau) = \pi i - 2\pi i \sum_{m\geq 0} q^m.$$

differentiating $k-1$ times gives

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau + d)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m\geq 1} m^{k-1} q^m.$$

Then we have

$$\begin{aligned}\sum_{(c,d)}{}' \frac{1}{(c\tau + d)^k} &= \sum_{d>0} \frac{1}{d^k} + 2\sum_{c=1}^{\infty}\left(\sum_{d\in\mathbb{Z}} \frac{1}{(c\tau + d)^k}\right) \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\end{aligned}$$

Remark II.1.1

There are no odd weight modular forms over $\mathrm{SL}_2(\mathbb{Z})$. Namely, $-I \in \mathrm{SL}_2(\mathbb{Z})$ gives $f(\tau) = f(\tau)(-1)^k$, thus k must be even.

Last time we used the example of the Eisenstein series $G_k(\tau)$ for $k > 2$ even. The q-expansion is

$$G_k(\tau) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Definition II.1.4

A modular form $f : \mathcal{H} \to \mathbb{C}$ is called a cuspform if $a_0(f) = 0$ in $\sum a_n(f) q^n$. We collect these as

$$S(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_k S_k(\mathrm{SL}_2(\mathbb{Z})).$$

Example II.1.6

$(60G_4)^3 - 27(140G_6)^2 =: \Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ is a cuspform (using that we're a graded ring). In fact, it is nonzero! Check the degree 1 term of the q-expansion.

II.2. Congruence subgroups

Definition II.2.1

Define

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\} = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})).$$

In fact $\Gamma(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$. We say $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if there exists $\Gamma(N) \subseteq \Gamma$.

Example II.2.1

We will often consider the congruence subgroups

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

Exercise II.2.2

$[\Gamma_1(N) : \Gamma(N)] = N$ and $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$, using the first isomorphism theorem to translate into $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Notation: For $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f : \mathcal{H} \to \mathbb{C}$, we define

$$[\gamma]_k : f \mapsto f[\gamma]_k$$

via

$$(f[\gamma]_k)(\tau) := (c\tau + d)^{-k} f(\gamma(\tau)).$$

For $f : \mathcal{H} \to \mathbb{C}$ we want to factor it through a map $\mathcal{H} \to D'$.

Note that $\Gamma(N) \subseteq \Gamma$ for some N, so $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$.If $h \in \mathbb{Z}_{>0}$ be the minimal so that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. This implies that $f(\tau + h) = f(\tau)$.

Now define $\mathcal{H} \to D' : \tau \mapsto e^{2\pi i \tau / h}$, so that f factors through $\mathcal{H}$. We get $g : D' \to \mathbb{C}$. This allows us to define f being holomorphic at ∞.

Pick $\alpha \in \mathrm{SL}_2(\mathbb{Z}), s \in \mathbb{Q}, \alpha(\infty)$. Given f, Γ-weakly modular, f is holomorphic at s if $f[\alpha]_k$ is holomorphic at ∞. Crunching the numbers gives that $f[\alpha]_k$ is weakly $\alpha^{-1}\Gamma\alpha$-modular (which is also a congruence subgroup) to make this work.

Definition II.2.2

We call $f : \mathcal{H} \to \mathbb{C}$ modular of weight k with level Γ

(1) f is holomorphic on $\mathcal{H}$.
(2) f is weight k, Γ-invariant, so $f[\gamma]_k = f$ for $\gamma \in \Gamma$.
(3) $f[\alpha]_k$ is holomorphic at ∞, for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ (suffices to take finitely many α because $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite, the q-series changes by a root of unity).
(4) f is called a cuspform if $a_0 = 0$ for $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

II.3. **Elliptic Curves as Complex Tori**

Definition II.3.1

$\Gamma = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subseteq \mathbb{C}$ such that ω_1, ω_2 are a basis of $\mathbb{C}$ over $\mathbb{R}$.

We can assume $\gamma_1/\omega_2 \in \mathcal{H}$.

Exercise II.3.1

Lattices $\Lambda = \Lambda'$ if and only if there exist matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ such that

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

Definition II.3.2

A complex torus is $\mathbb{C}/\Lambda$ as a complex manifold. The complex structure depends on Λ. There is an inherited group structure via addition.

Observation: If $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is non-constant and holomorphic, then it is surjective.

Proof. Look at im f, which is closed (compactness),connected, and open (by the open mapping theorem).

Definition II.3.3

An <u>isogeny</u> is a holomorphic homomorphism $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ which is nonconstant.

Example II.3.2

$[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, where $z \mapsto Nz$.

Exercise II.3.3

$\mathbb{C}/\Lambda =: E$, and $E[N] := \ker[N]$. Describe $E[N]$ as a group.

It is fairly clear that $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, by subdividing the lattice points in $\Lambda = \langle \omega_1, \omega_2 \rangle$.

Fact: Any isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is of the form $z + \Lambda \mapsto mz + \Lambda'$, $m \in \mathbb{C} \setminus \{0\}$.

Proposition II.3.1

Isogeny is an equivalence relation on complex tori.

Proof. The only nontrivial portion is showing symmetry. Take an isogeny $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, take $\varphi(z + \Lambda) = mz + \Lambda'$. This implies $m\Lambda \subseteq \Lambda'$. There exist naturals n_1, n_2 such that $\{n_1\omega_1', n_2\omega_2'\}$ is a basis of $m\Lambda$, where ω_1', ω_2' is a basis of Λ'.

Then $n_1 n_2 \Lambda' \subseteq m\Lambda$. Thus $n_1 n_2/m\Lambda' \subseteq \Lambda$.

We then define $\widehat{\varphi} : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ by $\widehat{\varphi}(z + \Lambda') = n_1 n_2 z/m + \Lambda$.

Also $\widehat{\varphi} \circ \varphi = [n_1 n_2] = [\deg \varphi]$. Note $\deg[N] = N^2$.

Consider the self-isogenies, we know that $\mathbb{Z} \subseteq \operatorname{Isog}(E, E)$.

Complex Multiplication curves are those such that $\mathbb{Z} \subsetneq \operatorname{Isog}(E, E)$, and in this case we will have that $\operatorname{Isog}(E, E) \subseteq \mathcal{O}_K$, where K is a quadratic imaginary number field.

II.4. Modular Curves

These are Moduli spaces of elliptic curves.

Definition II.4.1

If $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, then $Y(\Gamma) = \mathcal{H}/\Gamma$, which we call the modular curve for Γ.

Exercise II.4.1

For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then elliptic curves up to isomorphism are in bijection with $Y(\Gamma)$.

Namely $\tau \in \mathcal{H} \mapsto \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$

Example II.4.2

$\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ are congruence subgroups, and

$Y_0(N) \cong \{(E, C) \mid E \text{ is an elliptic curve}, C \subseteq E[N], E \text{ cyclic of order } N\}/\sim$

$Y_1(N) \cong \{(E, Q) \mid Q \text{ is a point of order } N\}/\sim .Y(N) \qquad \cong \{(E, (P, Q)) \mid P, Q \text{ generate } E[N], \langle P, Q\rangle$

where $\langle P, Q\rangle$ is the Weil pairing (see book/homework). There are of course maps $Y_1(N) \to Y_0(N) \to Y(N) \to Y(\mathrm{SL}_2(\mathbb{Z}))$.

We have a map $\Delta : \mathcal{H} \to \mathbb{C}$ called the modular discriminant defined by $\Delta = g_2^3 - 27g_3^3, g_2 = 60G_4, g_3 = 140G_6$. We also may consider

$$j : \mathcal{H} \to \mathbb{C}$$
$$j = \frac{1728 g_2^3}{\Delta}$$

which is weight zero and holomorphic on $\mathcal{H}$ but not at ∞. We can actually think of j as $j : \{E\}/\sim \to \mathbb{C}$ which is an invariant on elliptic curves, called the j-invariant. The modularity theorem will concern

- Elliptic curves E where $j(E) \in \mathbb{Q}$
- CM elliptic curves imply $j(E)$ is algebraic.

As some examples, $j(i) = 1728, j(\mu_3) = 0$, $\mu_N := e^{2\pi i/N}$. We also can consider moonshine theory–concerning the coefficients of j and the monster group.

Modular curves can be viewed as Riemann surfaces

- Give $Y(\gamma)$ a manifold structure
- Compactify $Y(\Gamma) \subseteq X(\Gamma)$.

We have a map $\pi : \mathcal{H} \to Y(\Gamma)$, and we give $Y(\Gamma)$ the quotient topology. How do we show $Y(\Gamma)$ is Hausdorff?

Proposition II.4.1

If $\tau_1, \tau_2 \in \mathcal{H}$, then there exists neighborhoods U_i containing τ_i such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma(U_1) \cap U_2 \neq \emptyset$ implies $\gamma(\tau_1) = \tau_2$.

Proof. Choose any U_1', U_2' containing τ_1, τ_2 with compact closure. First we need a claim.

Claim

$\gamma(U_1') \cap U_2' \neq \emptyset$ for finitely many $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Well we know $\mathcal{H} = \mathrm{SL}_2(\mathbb{R}) / \mathrm{SO}_2(\mathbb{R})$. Take a section $S : x + yi \mapsto \frac{1}{\sqrt{y}}\left[\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right]$. Then

$$e_1, e_2 \in \mathcal{H}, \gamma(e_1) = e_2 \iff \gamma \in S(e_1)\, \mathrm{SO}_2(\mathbb{R}) S(e_2)^{-1}.$$

If we let e_1, e_2 range over $\overline{U}_1, \overline{U}_2$, then γ lies in a compact subset of $\mathrm{SL}_2(\mathbb{R})$

Thus the number of such γ is finite since $\mathrm{SL}_2(\mathbb{Z})$ is discrete. F is the finite set of such γ, for each $\gamma \in F$, choose disjoint $U_{1,\gamma}, U_{2,\gamma}$ containing $\gamma(\tau_1), \tau_2$ respectively. Then

$$U_1 = U_1' \cap \bigcap_\gamma \gamma^{-1}(U_{1,\gamma}) \qquad\qquad U_2 = U_2' \cap \bigcap_\gamma U_{2,\gamma}$$

Corollary II.4.2

$Y(\Gamma)$ is Hausdorff

We now want to construct charts, tha tis for each $\pi(\tau) \in Y(\Gamma)$, we want $\widetilde{U} \subseteq Y(\Gamma)$, a homeomorphism $\varphi : \widetilde{U} \to V \subseteq \mathbb{C}$ onto V open, and we want holomorphic transition maps.

The $Y(\Gamma)$ are in fact "ramified covers." If τ is only fided by $\Gamma \cap \{\pm I\}$ then take a small neighborhood U of τ, then $\pi : U \to \widetilde{U}$ is a homeomorphism.

Definition II.4.2

Let Γ be a congruence subgroup. We say τ is elliptic in Γ if $\mathrm{Stab}_\Gamma(\tau) \supsetneq \{\pm I\}$.

Fact: For each τ, Γ_τ is finite cyclic (of order 1,2,3,4,6).

Definition II.4.3

$h_\tau = |\Gamma_\tau / (\Gamma \cap \{\pm I\})|$

We may then choose $U \subseteq \mathcal{H}$ such that $\gamma(U) \cap U \neq \emptyset$ implies $\gamma \in \Gamma_\tau$. We also know elliptic points are discrete. Then $U \xrightarrow{\psi = \rho \circ \delta} \widehat{\mathbb{C}}$ where $\rho(z) = z^{h_\tau}$, and

$$\delta : z \mapsto \begin{bmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{bmatrix} z$$

where $\delta(\tau) = 0, \delta(\overline{\tau}) = \infty$. This will induce a map $\varphi : \pi(U) \to \widehat{\mathbb{C}}$ giving us a chart.

Look at Elliptic points. Suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ fixes $\tau \in \mathcal{H}$ and $c \neq 0$, this implies

$$c\tau^2 + (d-a)\tau - b = 0$$

and $ad - bc = 1$, so this implies $(d-a)^2 + 4bc < 0$, so $(d+a)^2 < 4$ which holds if and only if $|a+d| < 2$. Thus

$$\mathrm{char}(\gamma) = x^2 - (a+d)x + 1 = x^2 + 1 \text{ or } x^2 \pm x + 1.$$

Thus if $\gamma \neq \pm I$ and γ fixes some τ then one of

$$\mathrm{ord}(\gamma) = 3 \qquad \mathrm{ord}(\gamma) = 4 \qquad \mathrm{ord}(\gamma) = 6.$$

In these cases respectively we have

$$\gamma \sim \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}^{\pm 1} \qquad \gamma \sim \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\pm 1} \qquad \gamma \sim \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}^{\pm 1}.$$

In the case $\mathrm{ord}(\gamma) = 6$, we can take the action of $\mathbb{Z}[\gamma]$ on $\mathbb{Z}^2$ making it into a $\mathbb{Z}[\gamma]$-module. We see that $\mathbb{Z}[\gamma]$ is a PID, so

$$\mathbb{Z}^2 = (\mathbb{Z}[\gamma])^r \oplus \bigoplus_I \mathbb{Z}[\gamma]/I$$

But there's no torsion, and $\mathbb{Z}[\gamma]$ has $\mathbb{Z}$-dimension two, since γ is a 6-th root of unity, and so its minimal polynomial has degree two, and $\mathbb{Z}[\gamma] \cong \mathbb{Z}[X]/\text{minpoly}$. This gives a map $\varphi : \mathbb{Z}[\gamma] \to \mathbb{Z}^2$ which is an isomorphism. Call $u = \varphi(1), v = \varphi(\gamma)$.

Then

$$\gamma[u, v] = [v, -u + v] = [u, v] \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

$$\gamma[v, u] = [v, u] \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}^{-1}$$

One of $[u, v]$ or $[v, u]$ has determinant one, and move it over.

Proposition II.4.3
$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \Gamma_i$, $\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \in \Gamma_{\mu_3}$ and nothing else. That is the elliptic points $Y(1) = Y(\mathrm{SL}_2(\mathbb{Z}))$ are $\{\pi(i), \pi(\mu_3)\}$ where μ_3 is a third root of unity.

Corollary II.4.4
Elliptic points of $Y(\Gamma)$ are Γ-orbits in $\mathrm{SL}_2(\mathbb{Z})i$, $\mathrm{SL}_2(\mathbb{Z})\mu_3$.

II.5. **Cusps**

Fact: $\mathrm{Stab}_\infty = \pm\left[\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right]$, for $m \in \mathbb{Z}$.

Define $\mathcal{H}^\star = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. We'll define $X(\Gamma) = \mathcal{H}^\star/\Gamma$.

Exercise II.5.1

There are finitely many images of $\mathbb{Q} \cup \{\infty\}$. There is only one orbit for $\mathrm{SL}_2(\mathbb{Z})$, as the action is

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{m}{n} = \frac{am+bn}{cm+dn}.$$

But then $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$, and so we can only split this orbit into finitely many pieces.

Definition II.5.1

We call the finitely points in $X(\Gamma) \setminus Y(\Gamma)$ the cusps

We can take a topology on $\mathcal{H}^\star$ coming from the Riemann sphere, but then all of our cusps will be close together!!! This is awful! Instead, take a topology generated by

- Opens in $\mathcal{H}$
- $N_m \cup \{\infty\}$ where $N_m = \{\tau \in \mathcal{H} \mid \mathrm{im}(\tau) > m\}$.
- All $\mathrm{SL}_2(\mathbb{Z})$ orbits of $N_m \cup \{\infty\}$.

We then give $X(\Gamma)$ the quotient topology

Proposition II.5.1

$X(\Gamma)$ is Hausdorff, compact, and connected.

Proof. For Hausdorff, there's three cases, two points in $\mathcal{H}$, a cusp and a point in $\mathcal{H}$, and then two cusps. For the first case, it's a simple proof using the properties of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$. For s, τ a cusp and a point, prove $\mathrm{Im}(\gamma(\tau)) \le \max(\mathrm{Im}(\tau), \mathrm{Im}(1/\tau))$.

Consider s_1, s_2 and $\alpha_i(\infty) = s_i$. Then $U_i = \alpha_i(N_2 \cup \{\infty\})$. If $\pi(U_1) \cap \pi(U_2) \neq \emptyset$, then

$$\gamma\alpha_1(\tau_1) = \alpha_2(\tau_2).$$

This will imply $\alpha_2^{-1}\gamma\alpha_1 : \tau_1 \mapsto \tau_2$. Claim: τ_1, τ_2 are translates of each other. This follows since they lie in the same $\mathrm{SL}_2(\mathbb{Z})$ orbit and they have "large" imaginary part. A messy computation yields that

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}(\tau)}{(d + c\,\mathrm{Re}(\tau))^2 + c^2(\mathrm{Im}(\tau))^2}$$

which is clearly less than 2 if $c \neq 0$, since $c \in \mathbb{Z}$. Thus τ_1, τ_2 are translates.

This will show $\alpha_2^{-1}\gamma\alpha_1$ fixes infinity, showing $s_1 \sim s_2$ in $X(\Gamma)$.

To show compactness it suffices to show this for a fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$. Namely

$$D^\star = D \cup \infty \qquad\qquad D = \{\tau \in \mathcal{H} \mid |\Re\tau| \le 1/2, |\tau| \ge 1\}$$

as $X(\Gamma)$ will be a finite union of these with some gluings. Well if we have an open cover, we can assume one contains one of the $N_m \cup \{\infty\}$, but then $D \setminus N_m$ is clearly compact.

It turns out that $X(\Gamma)$ is a compact manifold. We must understand charts of the cusps. We now consider

$$h_{s,\Gamma} = |\mathrm{SL}_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s| < \infty$$

Choose $\delta(s) = \infty, \delta \in \mathrm{SL}_2(\mathbb{Z})$ We then define $U_s = \delta^{-1}(N_2 \cup \{\infty\}), \psi : \rho \circ \delta$ where $\rho : z \mapsto e^{2\pi i z/h_s}$. One must check that the map ψ factors through the projection $U_s \xrightarrow{\pi} \pi(U_s)$.

Recall that $X(\Gamma)$ is a compact manifold

Theorem II.5.2 (Modularity)

For E an elliptic curve such that $j(E) \in \mathbb{Q}$ there exists an N and a surjective map $X_0(N) \twoheadrightarrow E$ of compact Riemann surfaces.

Goal: Compute the genus of $X(\Gamma)$. Recall from the theory of compact riemann surfaces that

- If $f : X \to Y$ is a nonconstant map of compact riemann surfaces, then it is surjective.
- For all $y \in Y$, $f^{-1}(\{y\})$ is discrete, which implies $\left|f^{-1}(y)\right| < \infty$.
- Away from finitely many points of Y, $\left|f^{-1}(y)\right| = d$ is constant and we call this constant d the degree of f. We call those points where $\left|f^{-1}(y)\right| \neq d$ the ramification points. Consider $z \mapsto z^n$ as an example.
- For all $x \in X$, there exists some number e_x such that $\sum_{x \in f^{-1}(y)} e_x = d$, and we should think of e_x as the multiplicity or ramification number.

Important formula in this setting

Theorem II.5.3 (Riemann-Hurwitz Formula)

If $f : X \to Y$ is a nonconstant map of compact connected Riemann surfaces then

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X} (e_x - 1)$$

where d is the degree of f, g_X, g_Y are the genuses of X, Y, and e_x ramification number at $x \in X$.

Proof Idea. Triangulate Y and generically you have d triangles in X for each triangle you start with, but we have to accoutn for ramification points.

In our case, we have $f : X(\Gamma) \to X(1)$, and $X(1)$ is a sphere, and so it is zero. Thus our formula simplifies to

$$2g - 2 = -2d + \sum_{x \in X} (e_x - 1).$$

The ramification points will be elliptic points and cusps.

<u>Elliptic Points</u>: If $\langle \gamma \rangle = \mathrm{SL}_2(\mathbb{Z})_\tau$ fixing τ, then $|\langle \gamma \rangle| = 4, 6$ and we have to worry about $i, \mu_3 = e^{2\pi i/3}$. Then

$$h_\tau = [\{\pm I\}\Gamma_T : \{\pm I\}] \in \{2, 3\}.$$

Let $\tau \in U \subseteq \mathcal{H}$ which is a coordinate chart and $\pi : \mathcal{H}^\star \to X(1), \pi_\Gamma : \mathcal{H}^\star \to X(\Gamma)$. Then we're looking at

$$\begin{tikzcd}
U \arrow[r, "\mathrm{Id}"] \arrow[d, "\pi_\Gamma"] \arrow[dd, dashed, bend right=60, "q \mapsto q^{h_\Gamma}"'] & U \arrow[d, "\pi"] \arrow[dd, dashed, bend left=60, "q \mapsto q^{h}"] \\
\pi_\Gamma(U) \arrow[r, "f"] \arrow[d, "\varphi_\Gamma"] & \pi(U) \arrow[d, "\varphi"] \\
V_\Gamma \arrow[r, "f_{\mathrm{loc}}"] & V
\end{tikzcd}$$

$$q \mapsto q^{h/h_\Gamma}$$

We know $h/h_\Gamma \in \{1,2,3\}$. The interesting case is when τ is elliptic for $\mathrm{SL}_2(\mathbb{Z})$ but NOT Γ. Then this determines the ramification number.

Cusps: We have $z \mapsto e^{2\pi i z/h_\Gamma}$ where $h_\Gamma = |\mathrm{SL}_2(\mathbb{Z})_\infty| \,/\, |\{\pm I\}\Gamma_s|$. Then the ramificatio number is

$$e_x = \frac{h_\Gamma}{h} = h_\Gamma.$$

Say τ is elliptic, and consider $F_\tau = f^{-1}(\tau)$, and $\mathcal{E}_h$ is the number of elliptic points in F_τ for Γ, and n is the number of other points. Then

$$|F_\tau| = \mathcal{E}_h + n \qquad\qquad d = \sum_{x \in F_\tau} e_x = hn + \mathcal{E}_h.$$

We then see that

$$\sum_{x \in F_\tau} e_x - 1 = (h-1)n = \frac{h-1}{h}(d - \mathcal{E}_h).$$

For cusps, notice that

$$\sum_{x \in F_\infty} e_x - 1 = d - \mathcal{E}_\infty.$$

Therefore

$$\begin{aligned} 2g - 2 &= -2d + d - \mathcal{E}_\infty + \frac{1}{2}(d - \mathcal{E}_i) + \frac{2}{3}(d - \mathcal{E}_{\mu_3}) \\ &= \frac{1}{6}d - \mathcal{E}_\infty - \frac{1}{2}\mathcal{E}_i - \frac{2}{3}\mathcal{E}_{\mu_3} \\ g &= 1 + \frac{d}{12} - \frac{\mathcal{E}_\infty}{2} - \frac{\mathcal{E}_i}{4} - \frac{\mathcal{E}_{\mu_3}}{6}. \end{aligned}$$

Generally this computation is hard. Why is it important?

Idea:

Modular forms of weight $k \rightsquigarrow$ meromorphic Γ-invariant differentials on $\mathcal{H}$, $H^0(X(\Gamma), \Omega^{\otimes k})$.

The right hand side is computable using the Riemann-Roch theorem if you have seen it.

Definition II.5.2

A function $f : \mathcal{H} \to \widehat{\mathbb{C}}$ is an automorphic function of weight k and level Γ if

(1) f is meromorphic on $\mathcal{H}$.

(2) f is weight k, Γ-invariant

(3) $f[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

This is not an automorphic form if you have heard of that! We call these $\mathcal{A}_k(\Gamma)$, and we note that $\mathcal{A}_0(\Gamma)$ consists of the meromorphic functions on $X(\Gamma)$, as the function must descend. Let $\mathbb{C}(X)$ denote the meromorphic functions to $\mathbb{C}$ from X.

Definition II.5.3

For X a compact riemann surface, $f \in \mathbb{C}(X)$,

$$\operatorname{div} f = \sum_X n_x[x].$$

We define the degree of $D \in \mathrm{Div}(X) = \mathbb{Z}X$ as

$$\deg D = \deg \sum_X n_x[x] = \sum_X n_x.$$

Fact: If X if a compact Riemann surface then

- If $f : X \to \mathbb{C}$ is holomorphic on X, then f is constant.
- $\mathbb{C}(\widehat{\mathbb{C}}) = \mathbb{C}(t)$.
- For f on the Riemann sphere, $\deg \operatorname{div} f = 0$.

Proposition II.5.4

$\mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}(j)$.

Recall that $j : \mathcal{H} \to \widehat{\mathbb{C}}$ is given by $j := \frac{1728 g_2^3}{\Delta}$

Proof. Suppose $f \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$. Then f has zeroes $z_1, \ldots, z_n$ and poles $p_1, \ldots, p_m$ in a fundamnetal domain for $\mathcal{H}$ (which we can think of as $X(1) \setminus \{\infty\}$). We can define

$$g(\tau) = \frac{\prod_i j(\tau) - j(z_i)}{\prod_j j(\tau) - j(p_i)}.$$

Then g has the same zeroes and poles as f in $\mathcal{H}$, because j is holomorphic on $\mathcal{H}$ with a pole at ∞. This implies f/g is holomorphic on $\mathcal{H}$, so it must be holomorphic on $X(1)$ as it will have the same behavior at ∞. Thus it will be constant!

Exercise II.5.2

If $\mathcal{A}_k(\Gamma)$ is nonempty containing some f, then

$$\mathcal{A}_k(\Gamma) = \mathbb{C}(X(\Gamma))f.$$

Furthermore $j' \in \mathcal{A}_2(\Gamma)$, hence $\mathcal{A}_k(\Gamma)$ for k even is nonempty.

Goal: Define $\operatorname{div}(f)$ for $f \in \mathcal{A}_k(\Gamma)$. We'll do this in cases

- Suppose $\tau \in \mathcal{H}$ with $\pi(\tau) \in X(\Gamma)$ is not a cusp. Note that $\tau \mapsto (c\tau + d)^k$ has no 0s or poles on $\mathcal{H}$ and

$$f(\gamma\tau) = \underbrace{j(\gamma, \tau)}_{(c\tau+d)^k} f(\tau).$$

  The local coordinates at τ are of the form $q = (t - \tau)^h$ fr some h.

  For $f(t) = a_m(t - \tau)^m$, then define $v_{\pi(\tau)}(f) = m/h$. In particular $v_{\pi(\tau)}(f) \in \frac{1}{3}\mathbb{Z} \cup \frac{1}{2}\mathbb{Z}$. When $k = 0$, we have that f is an actual function on $X(\Gamma)$ so $m/h \in \mathbb{Z}$.

Suppose $\pi(\tau)$ is a cusp. We can focus on $\tau = \infty$ because it's similar elsewhere (transform to ∞)

Local coordinates are $q_h = e^{2\pi i \tau/h}$, where h is defined as the smallest positive integer satisfying

$$\{\pm I\}\Gamma_\infty = \{\pm I\}\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle$$

To define "f meromorphic at ∞," we leveraged periodicity of f, we have $f(\tau + h) = (\pm 1)^k f(\tau)$. When it's $f(\tau + h) = f(\tau)$ we call the cusp <u>regular</u>, and otherwise it's <u>irregular</u>. Define $\hbar = h$ in the first case and $\hbar = 2h$ in the second case (aka the period).

Example II.5.3

$1/2$ is irregular for $\Gamma = \Gamma_1(4)$, which is the only example for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$.

Let $h' = 2h$, then f is h'-periodic, and $f(\tau) = g(q_{h'})$ close to ∞. We define

$$v_{\pi(\infty)}(f) = \frac{m}{2}$$

where

$$g(q_{h'}) = \sum_{n=m}^{\infty} a_n q_{h'}^n.$$

In the regular case, $v_{\pi(\infty)}(f) = v_\infty(f)$ and in the irregular case $v_{\pi(\infty)}(f) = \frac{v_\infty(f)}{2}$.

III. Differentials

Intuition: If f is weight k Γ-invariant, k is even, then $f(\tau)(\mathrm{d}\tau)^{k/2}$ is honest to god Γ-invariant. Thus we should think of f as sort of differentials on the modular curve.

The Next Goal: Define these differentials appropriately

Definition III.0.1

For $V \subseteq \mathbb{C}$ open we define

$$\Omega^{\otimes n}(V) := \{f(q)(\mathrm{d}q)^n \mid f \text{ is meromorphic on } V\}$$

with $(\mathrm{d}q)^{n+m} := (\mathrm{d}q)^n(\mathrm{d}q)^m$. Then

$$\Omega(V) := \bigoplus_{n\in\mathbb{N}_0} \Omega^{\otimes n}(V)$$

is a graded ring of differentials

Suppose we have a holomorphic map $\varphi : V_1 \to V_2$, then we define the pullback

$$\varphi^* : \Omega^{\otimes n}(V_2) \to \Omega^{\otimes n}(V_1)$$
$$\varphi^*(f(q_2)(\mathrm{d}q_2)^n) := f(\varphi(q_1))(\varphi'(q_1))^n(\mathrm{d}q_1)^n.$$

Exercise III.0.1

$(\varphi^*)^{-1} = (\varphi^{-1})^*$.

Definition III.0.2

For $U \subseteq X$ open, where X is a Riemann Surface, $\Omega^{\otimes}(U)$ is defined via the charts $\varphi_j : U_j \to V_j \subseteq \mathbb{C}$. Namely, we have $\omega \in \Omega^{\otimes n}(U)$ is a $(\omega_j) \in \prod_J \Omega^{\otimes n} V_j$ such that for

$$V_{j,k} := \varphi_j(U_j \cap U_k) \qquad \varphi_{j,k} = \varphi_k \circ \varphi_j^{-1} : V_{j,k} \to V_{k,j}$$

such that

$$\omega_j\big|_{V_{j,k}} = \varphi_{j,k}^*\left(\omega\big|_{V_{k,j}}\right).$$

It is fairly simple then to define pullback everywhere.

We then have $\pi : \mathcal{H} \to X(\Gamma)$ then $\pi^* : \Omega^{\otimes n}(X(\Gamma)) \to \Omega^{\otimes n}(\mathcal{H})$.

But wait! The differential that is pulled back must then be Γ invariant. This will give us

$$\begin{aligned}\pi^*\omega = f(\tau)(\mathrm{d}\tau)^n &= \gamma^*(f(\tau)(\mathrm{d}\tau)^n) \\ &= f(\gamma\tau)(j(\gamma,\tau))^{-2n}(\mathrm{d}\tau)^n.\end{aligned}$$

Thus $f(\gamma\tau) = j(\gamma,\tau)^{2n} f(\tau)$, so $f \in \mathcal{A}_{2n}(\Gamma)$. This gives us an honest to god map

$$\Omega^{\otimes n}(X(\Gamma)) \to \mathcal{A}_{2n}(\Gamma).$$

Theorem III.0.1

This is a bijection.

Proof. Map in the other direction is an absolute shitshow. Take $f \in \mathcal{A}_{2n}(\Gamma)$, and call $k = 2n$. Work locally to construct $\omega(f) \in \Omega^{\otimes n}(X(\Gamma))$. We'll do this for the non-cusp points, but we won't check the gluing condition. Oops!

For $\tau \in U \subseteq H$ we constructed a map $\psi : U \xrightarrow{\rho\circ\delta} V$, and we showed this factors through as $\varphi : \pi(U) \to V$.

We'll instead construct "$\omega(f)$" in V so that it pulls back to the right thing in U, and then we'll pull it back to $\pi(U)$ via φ. We have $\delta \in \mathrm{GL}_2(\mathbb{C}), \alpha \coloneqq \delta^{-1}$. So the first step is to take $\lambda \coloneqq \alpha^*(f(\tau)(\mathrm{d}\tau)^n)$.

We define an extension of the $f[\gamma]_k$ formula as

$$f[\alpha]_k = (\det\alpha)^{k/2} j(\alpha,\tau)^{-k} f(\alpha(\tau)).$$

We in fact have $\alpha'(\tau) = \frac{\det\alpha}{(j(\alpha,\tau))^2}$. One may then check that

$$\lambda = (f[\alpha]_k)(z)(\mathrm{d}z)^n.$$

In contrast, ρ is not invertible, so the same trick does not work. Instead, we just have to think hard... If we have a non-elliptic point though, $\rho = \mathrm{Id}$ and we're done. Otherwise we should consider that λ is $\delta\Gamma\delta^{-1}$-invariant.

Lets defdine $\rho_h : z \mapsto \mu_h z$ where $\mu_h = e^{2\pi i/h}$. We have that $\rho_h^*(\lambda) = \lambda$ by invariance. But then this implies

$$\mu_h^n z^n (f[\alpha]_k)(\mu_h z) = z^n (f[\alpha]_k)(z).$$

Then $z^n f[\alpha]_k(z)$ is invariant under rotation by h, so it is equal to $g(z^h)$. We may then consider

$$\omega = \frac{g(q)(\mathrm{d}q)^n}{(h\,\mathrm{d}q)^n}.$$

In fact $\rho^*(\omega) = \lambda$ as desired.

The map $\mathcal{A}_{k=2n}(\Gamma) \to \Omega^{\otimes n}(X(\Gamma))$ gives us a way to define the order of vanishing of a differential $\omega \in \Omega^{\otimes n}(X(\Gamma))$. On a cusp we write this as

$$v_0(\omega_j) = v_0\left(\frac{g_j(q)}{(hq)^{k/2}}\right)$$

where $z^n f[\alpha]_{2n}(z) = g_j(z^h)$. This is precisely

$$v_{\pi(\tau)}(f) - \frac{k}{2}\left(1 - \frac{1}{h}\right).$$

If we're at a cusp, we have a different type of function g_j with

$$v_0(\omega_j) = v_0\left(\frac{g_j(q)}{\left(\frac{2\pi i q}{h}\right)^{k/2}}\right) = v_{\pi(\rho)}(f) - \frac{k}{2}.$$

Unlike the order of vanishing of f (which can be non-integral), the order of vanishing of ω_j is always integer (as it's just the order of vanishing of some function.

Exercise III.0.2

Show that

$$S_2(\Gamma) \leftrightarrow \Omega^{\otimes 1}_{\text{hol}}(X(\Gamma)).$$

III.1. **Computing Dimensions**

What we want from this is the dimensions of $\mathcal{M}_{-k}(\Gamma), S_k(\Gamma) \subseteq \mathcal{A}_k(\Gamma)$. We will use the Riemann-Roch formula.

Recall III.1.1

For X a compact Riemann surface we defined

$$\operatorname{Div}(X) = \{\sum_{x \in X} n_x[x] \mid n_x = 0, \text{ all but finitely many } x, n_x \in \mathbb{Z}\}$$

and

$$\deg(D) = \sum n_x \qquad\qquad D \geq D', n_x \geq n'_x.$$

We also define $\operatorname{Div}^0(X) = \deg^{-1}(\{0\})$. Then we have a map

$$\operatorname{div} : \mathbb{C}(X) \to \operatorname{Div}^0(X) \subseteq \operatorname{Div}(X),$$

whose image is called the principal divisors. Abel's Theorem says that

$$\operatorname{Div}^0(X)/\operatorname{div}(\mathbb{C}(X)) \cong \mathbb{C}^g/\Gamma_g$$

We also have

$$L(D) = \{f \in \mathbb{C}(X) \mid f = 0 \text{ or } \operatorname{div}(f) + D \geq 0\}.$$

And here we have

- $L(D)$ is a vector space.
- $\dim L(D) =: \ell(D)$.
- $\operatorname{div} : \Omega(X) \to \operatorname{Div}(X)$ is given by $\omega \mapsto v_0(f_x)$ where locally at x, $\omega = f_x(q)(\mathrm{d}q)^n$.
- If $\lambda \in \Omega^1(X)$, then $\operatorname{div}(\lambda)$ is a canonical divisor, since everything in $\Omega^1(X)$ is equivalent up to principal divisors.

Theorem III.1.1 (Riemann-Roch)

Let X be a compact Riemann surface, then

$$\ell(D) = \deg D - g + 1 + \ell(\operatorname{div}(\lambda) - D)$$

where λ is the canonical divisor.

Corollary III.1.2

We have that

(1) $\ell(\operatorname{div}(\lambda)) = g$.

(2) $\deg(\operatorname{div}(\lambda)) = 2g - 2$.

(3) $\deg(D) < 0$ implies $\ell(D) = 0$.

(4) $\deg(D) > 2g - 2$ implies $\ell(D) = \deg(D) - g + 1$.

We know that

$$\Omega^1(X(\Gamma)) \cong \mathbb{C}(X(\Gamma))\lambda$$
$$\Omega^1_{\text{hol}}(X(\Gamma)) \to L(\lambda)$$
$$f_0\lambda \mapsto f_0$$

as the left and right hand sides both correspond to $\operatorname{div}(f_0) + \operatorname{div}(\lambda) \geq 0$. the upshot of this by the corollary above is $\dim S_2(\Gamma) = g$.

Now we'll derive dimensions for k even. Our orders of vanishing for forms have rationals in them, and we can get around this with flooring and previous work...

Namely, recall that for $f \in \mathcal{A}_k(\Gamma)$, $f \neq 0$, we know $\mathcal{A}_k(\Gamma) = \mathbb{C}\left(X(\Gamma)\right) f$. Then we see that

$$\mathcal{M}_k(\Gamma) = \{f_0 f \mid f_0 f = 0 \text{ or } \operatorname{div}(f_0 f) \geq 0\} \cong L(\lfloor \operatorname{div}(f) \rfloor).$$

We should now study $\lfloor \operatorname{div}(f) \rfloor$. Well, f corresponds to some $\omega(f) \in \Omega^{\otimes k/2}(X(\Gamma))$. Well we know that

$$\deg \omega(f) = \operatorname{div}(\lambda) \cdot \frac{k}{2} = (2g-2)\frac{k}{2} = k(g-1).$$

We may then compute that

$$\lfloor \operatorname{div}(f) \rfloor = \operatorname{div}(\omega) + \sum_i \left\lfloor \frac{k}{4} \right\rfloor x_{2,i} + \sum_i \left\lfloor \frac{k}{3} \right\rfloor x_{3,i} + \sum_i \frac{k}{2} x_i,$$

where $x_{2,i}, x_{3,i}$ are elliptic points and x_i are cusps. We then know that $\deg \lfloor \operatorname{div}(f) \rfloor > 2g - 2$ for $k \geq 2$. Thus for $k \geq 2$ we see that

$$\dim(\mathcal{M}_k(\Gamma)) = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \mathcal{E}_2 + \left\lfloor \frac{k}{3} \right\rfloor \mathcal{E}_3 + \frac{k}{2} \cdot \mathcal{E}_\infty.$$

For cusp forms we have a similar argument yielding for $k \geq 4$ that

$$S_k(\Gamma) = L\left(\left\lfloor \operatorname{div}(f) - \sum_i x_i \right\rfloor\right)$$
$$\dim S_k(\Gamma) = \dim(\mathcal{M}_k(\Gamma)) - \mathcal{E}_\infty.$$

We also know from previous work that

$$\dim S_2(\Gamma) = g.$$

We know that $\mathcal{M}_0(\Gamma) = \mathbb{C}$, and $S_0(\Gamma) = 0$. The book shows $\mathcal{M}_k(\Gamma) = 0$ for $k < 0$.

Proof Idea. If $f \in \mathcal{M}_k(\Gamma)$, then we'd have $\frac{f^{12}}{\Delta^k} \in S_0(\Gamma)$...

Application: For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, let k be even, then

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) \qquad = S_k(\mathrm{SL}_2(\mathbb{Z})) \oplus \mathbb{C}E_k \qquad (k < 4)$$

$$\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 \pmod 12 \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise} \end{cases}.$$

In fact this implies that $\mathcal{M}(\mathrm{SL}_2(\mathbb{C})) = \mathbb{C}[E_4, E_6]$ and $S(\mathrm{SL}_2(\mathbb{Z})) = \Delta \cdot \mathbb{C}[E_4, E_6]$.

How should we run this for k odd? When $-I \notin \Gamma$, it is in fact still true that

$$\dim(\mathcal{M}_k(\Gamma)) = \ell(\lfloor \mathrm{div}(f) \rfloor)$$

since this doesn't use differentials (since there will still be a nonzero f, need to check). There exists an $\omega \in \Omega^k(X(\Gamma))$ that pulls back to $f(\tau)^2 (\mathrm{d}\tau)^k$. In fact we can compute $\lfloor \mathrm{div}(f) \rfloor$ in terms of ω, to give the formula

$$\ell(\lfloor \mathrm{div}(f) \rfloor) = (k-1)(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \mathcal{E}_{3^+} + \frac{k}{2}\mathcal{E}_\infty^{reg} + \frac{k-1}{2}\mathcal{E}_\infty^{irr}. \qquad (k \geq 3)$$

IV. Eisenstein Series

For now, define $\mathcal{E}_k(\Gamma) := \mathcal{M}_k(\Gamma)/S_k(\Gamma)$ as the eisenstein space, eventually we'll make $\mathcal{E}_k(\Gamma)$ as a subspace of $\mathcal{M}_k(\Gamma)$, but that comes later.

Goal is to study $\mathcal{E}_k(\Gamma(N)), \mathcal{E}_k(\Gamma_1(N)), \mathcal{E}_k(\Gamma_0(N))$.

Recall IV.0.1

For $k \geq 4$ even we defined $G_k(\tau) = \sum'_{(c,d) \in \mathbb{Z}^2} \frac{1}{(c\tau + d)^k}$. We then define $E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)}$.

Then

$$E_k(\tau) = \frac{1}{2} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ \gcd(c,d) = 1}} \frac{1}{(c\tau + d)^k}.$$

The book defines

$$P_+ := \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\} \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

Recall the structure of SL_2 given as

$$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \qquad T = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \qquad U = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

We will also have

$$E_k(\tau) = \frac{1}{2} \sum_{\gamma \in P_+ \backslash \mathrm{SL}_2(\mathbb{Z})} j(\gamma, \tau)^{-k}.$$

Exercise IV.0.2

Check the above!

The adeles $\mathbb{A}$ are $\prod_p' \mathbb{Q}_p \times \mathbb{R}$ where for almost all p we have the p-coordinate lies in $\mathbb{Z}_p$ (what $\prod'$ means). Modular forms will later be related to automorphic representations $\mathrm{SL}_2(\mathbb{A})$.

We have by combining our earlier dimension formulas for $M_k(\Gamma(N))$ and $S_k(\Gamma(N))$.

$$\mathcal{E}_k(\gamma) = \begin{cases} \mathcal{E}_\infty & \text{if } k \geq 4 \text{ even} \\ \mathcal{E}_\infty^{reg} & \text{if } k \geq 3 \text{ odd } -I \notin \Gamma \\ \mathcal{E}_\infty - 1 & \text{if } k = 2 \\ \mathcal{E}_\infty^{reg}/2 & \text{if } k = 1, -I \notin \Gamma 1 \qquad\qquad \text{if } k = 0 \\ 0 & \text{if } k < 0, k > 0 \text{ odd } -I \in \Gamma. \end{cases}$$

Consider $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N. Let

$$\delta = \begin{pmatrix} a & b \\ c_v & d_v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

where $(c_v, d_v) = \overline{v}$, then $\epsilon_N = 1/2$ if $N = 1, 2$ and 1 otherwise. Then we can consider

$$E_k^{\overline{v}}(\tau) = \epsilon_N \sum_{\gamma \in (P_+ \cap \Gamma(N)) \backslash \Gamma(N)\delta} j(\gamma, \tau)^{-k}$$

Proposition IV.0.1

For all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $E_k^{\overline{v}}[\alpha]_k(\tau) = E_k^{\overline{v}\gamma}(\tau)$

Corollary IV.0.2

$E_k^{\overline{v}}(\tau)$ is weight k $\Gamma(N)$ invariant, since then we essentially have $\overline{v} = \overline{v}\gamma$.

Proof. Ignore ϵ_N for convenience

$$E_k^{\overline{v}}[\gamma]_k(\tau) = j(\gamma, \tau)^{-k} \sum_{\gamma'} j(\gamma', \gamma(\tau))^{-k}.$$

Recall that $j(\gamma, \tau) j(\gamma', \gamma(\tau)) = j(\gamma'\gamma, \tau)$. Then

$$E_k^{\overline{v}}[\gamma]_k(\tau) = \sum_{\gamma'} j(\gamma'\gamma, \tau) = \sum_{\gamma'' \in (P_+ \cap \Gamma(N)) \backslash \Gamma(N)\delta\gamma} j(\gamma'', \tau) = E_k^{\overline{v}\gamma}(\tau).$$

One can prove holomorphicity of these things. But doing so is painful.

FACT: $E_k^{\overline{v}}(\tau)$ is weight k, $\Gamma(N)$ modular form for $k \geq 3$. We may also define for $\Gamma(N) \subseteq \Gamma$ the form

$$E_{k,\Gamma}^{\overline{v}}(\tau) = \sum_{\gamma_j \in \Gamma(N) \backslash \Gamma} E_k^{\overline{v}}[\gamma_j](\tau) \in \mathcal{M}_k(\Gamma).$$

For $N > 2$ and k even, one may calculate that $E_k\overline{v}$ is nonvanishing at $-d_v/c_v$ and vanishes at all other cusps.

Hence if we pick $\overline{v}$ which represents each cusp of $\Gamma(N)$, then $\{E_k^{\overline{v}}\}$ are linearly independent. The size of this is exactly the number of cusps $\mathcal{E}_\infty$!!! Wait this means it's a basis.

IV.1. Dirichlet Characters

Definition IV.1.1

A dirichlet character is a group homomorphism $\chi : G_N := (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

The dirichlet characters themselves form a group $\chi_1\chi_2(m) = \chi_1(m)\chi_2(m)$. We'll call this $\widehat{G}_N$. Then $\widehat{G}_N \cong G_N$ in a non-canonical way.

We have

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong \prod_{\substack{p^k \mid N \\ p^{k+1} \nmid N}} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$$

and the right hand side is cyclic for $p \neq 2$, and

$$(\mathbb{Z}/2^k\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/2\mathbb{Z}\right)^{k-2}.$$

Lifting: If $d \mid N$, then there is a map $G_N \twoheadrightarrow G_d$, and so there is a map $\widehat{G}_d \hookrightarrow \widehat{G}_N$.

Definition IV.1.2

We define the conductor of $\chi \in \widehat{G}_N$ to be the smallest d so that χ comes from $\widehat{G}_d$. We denote this by $\mathrm{Cond}(\chi)$. If $\mathrm{Cond}(\chi) = N$, then χ is called primitive.

Given $\chi \in \widehat{G}_N$, we may extend to $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ by sending everything not in $(\mathbb{Z}/N\mathbb{Z})^\times$ to zero. Likewise we get a map $\chi : \mathbb{Z} \to \mathbb{C}$ by sending $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$.

Something that shows up a lot is a sum of the form $g(\chi) = \sum\limits_{n=0}^{N-1} \chi(n)\mu_N^n$ where $\mu_N = e^{2\pi i N}$. One can thinkof this as a Fourier transform if we squint our eyes a bit (sums to integrals and such).

Application: We remember how $\Gamma_1(N)$ lies in $\Gamma_0(N)$ as

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}_{\bmod N} \qquad\qquad \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}_{\bmod N}$$

and so $\Gamma_0(N)/\Gamma_1(N)$ is in fact $(\mathbb{Z}/N\mathbb{Z})^\times$. We define

$$M_k(N, \chi) := \{f \in M_k(\Gamma_1(N)) \mid f[\gamma]_k = \chi(d_\gamma)f, \gamma \in \Gamma_0(N)\}.$$

We call these modular forms of weight k of level N with Nebentypus character χ. Then $M_k(N, 1) = M_k(\Gamma_0(N))$.

Fact:

$$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(N, \chi).$$

Why? Finite dimensional representation theory! Look at the action of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ on the left hand side, which is a finite dimensional complex vector space. The irreducible representations are those things acting by χ, and so we take the "eigenspaces" of these to get the break up. Note the eigenspaces will often have multiplicity and not be irreducible themselves.

Recall orthogonality from representation theory as well, that is for fixed χ we have

$$\sum_{n\in G_N}\chi(n)=\begin{cases}\phi(N) & \text{if } \chi=1\\ 0 & \text{otherwise}\end{cases}$$

where ϕ is Euler's totient function, and for fixed n we have

$$\sum_{\chi\in\widehat{G}_N}\chi(n)=\begin{cases}\phi(N) & \text{if } n=1\\ 0 & \text{otherwise}\end{cases}.$$

This is the general fact from group theory that

$$\frac{1}{\phi(N)}\sum_{n\in G_N}\chi_1(n)\overline{\chi_2(n)}=\begin{cases}1 & \text{if } \chi_1=\chi_2\\ 0 & \text{otherwise}\end{cases}.$$

We may also consider that, via the decomposition introduced before, we have

$$\mathcal{E}_k(\Gamma_1(N))=\bigoplus_{\chi}\mathcal{E}_k(N,\chi).$$

Also, we may consider the unnormalized Eistenstein series with $\overline{v}\in(\mathbb{Z}/N\mathbb{Z})^2$ of order N, for $k\geq 3$,

$$G_k^{\overline{v}}(\tau)=\sideset{}{'}\sum_{(c,d)\equiv\overline{v}}\frac{1}{(c\tau+d)^k}.$$

Idea: $G_k^{\overline{v}}\in\mathcal{E}_k(\Gamma_0(N))$, so we can get something in $\mathcal{E}_k(\Gamma_1(N))$ by averaging over a finite set of coset representatives. This may be zero, you have to be careful! But thankfully it's not super hard to compute the Fourier expansions with some effort.

Take u,v with $uv=N$, $\psi\in\widehat{G}_u,\varphi\in\widehat{G}_v$, with φ primitive and $\varphi\psi(-1)=(-1)^k$. Then we may define

$$G_k^{\psi\varphi}(\tau)\coloneqq\sum_{c=0}^{u-1}\sum_{d=0}^{v-1}\sum_{e=0}^{u-1}\psi(d)\overline{\varphi(d)}G_k^{\overline{(cv,d+ev)}}(\tau).$$

For $\gamma\in\Gamma_1(N)$ we have

$$G_k^{\psi\varphi}[\gamma]_k=\psi\varphi(d_\gamma)G_k^{\psi\varphi}.$$

Thus $G_k^{\psi\varphi}\in M_k(N,\psi\varphi)$.

We can normalize this to $E_k^{\psi\varphi}(\tau)$. The idea then is to define for $t\in\mathbb{N}$

$$E_k^{\psi,\varphi,t}\coloneqq E_k^{\psi\varphi}(t\tau).$$

This won't always yield a modular form, but if $tuv\mid N$ then it is.

Theorem IV.1.1

$\{E_k^{\psi,\varphi,t}\}$ is a basis for $\mathcal{E}_k(\Gamma_1(N))$. If we impose $\psi\varphi=\chi$, then this is a basis for $\mathcal{E}_k(N,\chi)$.

The steps to proving something like this

- Prove everything converges (not much harder than standard Eisenstein series)
- Prove everything transforms properly (by construction essentially)

- Prove things are holomorphic (get weird zeta functions when writing down Fourier Expansion Hard!)
- Prove things are linearly independent by looking at Fourier series.

Suppose $N > 0$, $\overline{v}$ as before, k is any integer, $\epsilon_N = 1/2$ if $N = 1, 2$ and 1 otherwise, then

$$E_k^{\overline{v}}(\tau, s) = \epsilon_N \sideset{}{'}\sum_{\substack{(c,d)\equiv v \\ \gcd(c,d)=1}} \frac{\operatorname{Im}(\tau)^s}{(c\tau+d)^k \left|c\tau+d\right|^{2s}}.$$

Fact, this converges absolutely and uniformly for

$$\{s \mid \operatorname{Re}(k+2s) > 2\}.$$

If $k \geq 3$, this converges for $s = 0$. We can check this has the right transformation properties, and then there is at most one meromorphic continuation to the complex plane!!! One can find it, and $s = 0$ is not a pole for $N = 1, 2$.

IV.2. Interlude on L-functions/ζ-functions

Definition IV.2.1

We say $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ lies in the Selberg-class of functions if it converges absolutely for $\operatorname{Re}(s) > 1$ and

(1) Analyticity: there is a meromorphic continuation, and the only possible pole is at $s = 1$.

(2) Ramanujan: $a_1 = 1$, $a_n \ll_\varepsilon n^\varepsilon$ for all $\varepsilon > 0$.

(3) Functional Equation: There should be a γ factor so that if $\Phi(s) \coloneqq \gamma(s) f(s)$ then

$$\Phi(s) = \overline{\Phi(1-\overline{s})}.$$

(4) Euler Product: We should be able to write f as

$$f(s) = \prod_{p \text{ prime}} f_p(s)$$

where $f_p(s) = \exp\left(\sum_{n=1}^\infty \frac{b_{p^n}}{p^{ns}}\right)$

The primary example is the Riemann ζ-function. Here we have

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

and

$$\Phi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Natural Constructions:

$$\begin{tikzcd} \text{Galois Reps} \arrow[r] & L\text{-functions} & \text{Automorphic Forms} \arrow[l] \\ & \text{Algebraic Varieties} \arrow[u] & \end{tikzcd}$$

For modular forms–namely eigenforms in a later sense–we have for $f = \sum_{n=0}^{\infty} a_n q^n$ then

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

will lie in the Selberg class.

Another important example is Artin L-functions. Take $\rho \in \mathrm{Rep}(\mathrm{Gal}(K/\mathbb{Q}))$ where $K/\mathbb{Q}$ is a finite Galois extension. Then there is an L-function

$$L(\rho, s) = \text{ramified primes} \times \prod_{\mathfrak{p}} \left(\mathrm{char}(\rho(\mathrm{Frob}(\mathfrak{p})))(N(\mathfrak{p})^{-1})\right)^{-1},$$

where char is the characteristic polynomial, and $N(\mathfrak{p})$ is the norm.

If $L = \mathbb{Q}$ and ρ is trivial, then this is just the Riemann zeta function. Then for ρ_{reg} the canonical representation for $K/\mathbb{Q}$ we have

$$L(\rho_{\mathrm{reg}}, s) = \prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(p)^{-s}}.$$

For $K = \mathbb{Q}(\mu_N)$ with $\mu_N = e^{2\pi i/N}$, we have $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^{\times}$, and the Galois representations ar e Dirichlet characters χ, and it turns out you get

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

These are called Dirichlet L-functions.

Conjecture IV.2.1 (Artin)

$L(\rho, s)$ is analytic if $\rho \neq 1$.

The abelian case is ok. If the group is solvable it's also ok.

For going from algebraic varieties to L-functions, it has to do with counting the number of points of a variety X over $\mathbb{F}_p$.

Meromorphic Continuation and the Functional Equation

Warmup: The Γ function is defined as

$$\Gamma(s) := \int_{t=0}^{\infty} e^{-t} t^s \frac{\mathrm{d}t}{t}$$

for $s \in \mathbb{C}$, $\mathrm{Re}(s) > 0$. One may check that $\Gamma(s+1) = s\Gamma(s)$. This allows us to extend Γ to $\mathrm{Re}(s) \leq 0$. Because

$$\Gamma(s) = \frac{\Gamma(s+1)}{s},$$

so this is defined for $\mathrm{Re}(s) > -1$ besides when $s = 0$, and then keep playing the game.

There is a generalization of this idea

Definition IV.2.2

Let $f : \mathbb{R}^+ \to \mathbb{C}$. We define the Mellin transform of f to be

$$\mathfrak{M}f(s) = \int_{t=0}^{\infty} f(t) t^s \frac{\mathrm{d}t}{t}$$

Then if $f(t) = e^{-t}$ we have $\mathfrak{M}f(s) = \Gamma(s)$. We can define

$$\Theta(it) \coloneqq \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}$$
$$\sum_{n=1}^{\infty} e^{-\pi n^2 t} = \frac{1}{2}(\Theta(it) - 1).$$

Taking the Mellin transform

$$\int_{t=0}^{\infty} \sum_{n=1}^{\infty} e^{-\pi n^2 t} t^s \frac{\mathrm{d}t}{t} = \frac{1}{2}\int_{t=0}^{\infty} (\theta(it) - 1) t^s \frac{\mathrm{d}t}{t}.$$

The left hand side has excellent convergence properties, so we may exchange the integral and the sum, which gives us for $\mathfrak{M}f$ on the left hand side

$$\mathfrak{M}f(s) = \sum_{n=1}^{\infty} (\pi n^2)^{-s}\Gamma(s) = \pi^{-s}\Gamma(s)\zeta(2s).$$

Then we may define $\mathfrak{M}f(s/2) =: \Phi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Splitting off the $0, 1$ portion of this

$$\frac{1}{2}\int_{t=0}^{1} (\Theta(it) - 1) t^{s/2} \frac{\mathrm{d}t}{t} = \frac{1}{2}\int_{0}^{1} \Theta(it) t^{s/2} \frac{\mathrm{d}t}{t}.$$

We also have a formula $\Theta(i/t) = t^{1/2}\Theta(it)$. Thus via a change of variables

$$\begin{aligned}
&\left[\frac{1}{2}\int_{t=1}^{\infty} \Theta(i/t) t^{-s/2} \frac{\mathrm{d}t}{t}\right] - \frac{1}{s} \\
&= \left[\frac{1}{2}\int_{t=1}^{\infty} \Theta(it) t^{1-s/2} \frac{\mathrm{d}t}{t}\right] - \frac{1}{s} \\
&= \left[\frac{1}{2}\int_{t=1}^{0} (\Theta(it) - 1) t^{1-s/2} \frac{\mathrm{d}t}{t}\right] - \frac{1}{s} - \frac{1}{1-s}.
\end{aligned}$$

One should then recombine things and show things are invariant under $s \mapsto 1 - s$.

V. Hecke Operators

V.1. Definitions and Computations

Call $\mathrm{GL}_2(\mathbb{Q})^+ \subseteq \mathrm{GL}_2(\mathbb{Q})$ the subgroup of positive determinant matrices. If we have $\Gamma_1, \Gamma_2 \in \mathrm{SL}_2(\mathbb{Z}), \alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ we'll define an operator

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2).$$

Reminder: Double cosets are a little weird.

Exercise V.1.1

Suppose G is finite, H_1, H_2 are subgroups. Compute $|H_1\alpha H_2|$ in temrs of cardinalities of subgroups of G. We have

$$|H_1\alpha H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap \alpha H_2 \alpha^{-1}|}.$$

For $\beta \in \mathrm{GL}_2(\mathbb{Q})^+$ we define

$$f[\beta]_k(\tau) := (\det \beta)^{k-1} j(\beta, \tau)^{-k} f(\beta(\tau)).$$

Now we see that

$$\Gamma_1 \alpha \Gamma_2 = \coprod_j \Gamma_1 \beta_j$$

for some $\beta_j \in \alpha\Gamma_2$, and we then define

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k.$$

We need to know: there are finitely many β_j, this doesn't depend on β_j, and this actually takes modular forms of weight k level Γ_1 to weight k level Γ_2 forms.

Fact: $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup.

Lemma V.1.1

We have that

$$\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 \backslash \Gamma_2 \to \Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2,$$

and the left hand side is finite, so we only need finitely many β_j.

To show this gives a map as claimed, first check it's well-defined (does not depend on choice of β_j), then we take

$$f[\Gamma_1\alpha\Gamma_2]_k[\gamma_2]_k = \sum_j f[\beta_j]_k[\gamma_2]_k = \sum_j f[\beta_j']_k = f[\Gamma_1\alpha\Gamma_2]_k.$$

None of this effects holomorphicity on $\mathcal{H}$, but we need to check holomorphicity at the cusps. Recall this was $f[\gamma]_k$ is holomorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The necessary lemma is

Lemma V.1.2

If $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and $\alpha\gamma = \gamma'$ then

$$\alpha = r \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

for $r \in \mathbb{Q}^+$. And this will not change holomorphicity at ∞.

This same proof will also show that if f is a cuspform then $f[\Gamma_1\alpha\Gamma_2]_k$ is a cuspform.

Example V.1.2

If $\Gamma_1 \supseteq \Gamma_2$ and $\alpha = 1$ then we get the embedding $M_k(\Gamma_1) \hookrightarrow M_k(\Gamma_2)$.

If $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$ then

$$f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k$$

and gives an isomorphism $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.

If $\Gamma_1 \subseteq \Gamma_2$, $\{\gamma_{2,j}\}$ represents $\Gamma_1 \backslash \Gamma_3$

$$f[\Gamma_1 \alpha \Gamma_2]_k = \sum_j f[\gamma_{2,j}]_k$$

Then

$$\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$$
$$\Gamma_3' = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$$

gives

$$\begin{tikzcd} \Gamma_3 \arrow[r, "\sim"] \arrow[d] & \Gamma_3' \arrow[d] \\ \Gamma_2 & \Gamma_1 \arrow[l, dashed] \end{tikzcd}$$

Then as moduli spaces

$$\begin{tikzcd} X_3 \arrow[r, "\sim"] \arrow[d] & X_3' \arrow[d] \\ X_2 & X_1 \arrow[l, dashed] \end{tikzcd}$$

Then we have

$$[\Gamma_1 \alpha \Gamma_2]_k : \mathrm{Div}(X_2) \to \mathrm{Div}(X_1)$$

given by

$$\begin{aligned} x \mapsto \sum_{y \in \pi_2^{-1}(x)} e_y y \mapsto e_y \alpha y \alpha^{-1} \\ \mapsto \sum_y e_y \pi_1(\alpha y \alpha^{-1}). \end{aligned}$$

Special Cases: $\Gamma_0(N), \Gamma_1(N)$, that is

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \qquad \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \mod N$$

Given $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have a Diamond operator

$$\langle d \rangle = [\Gamma_1(N)\alpha\Gamma_1(N)]_k$$

where

$$\alpha \mapsto \begin{pmatrix} * & * \\ 0 & d \end{pmatrix}$$

where $\mapsto$ here is the reduction mod N. In particular since $\Gamma_1(N)$ is a normal subgroup of $\Gamma_1(N)$ we have

$$\langle d \rangle f = f[\alpha]_k$$

and in fact

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d) f \text{ for all } d\}.$$

The next is $\alpha = \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]$ where p is prime with

$$T_p \coloneqq [\Gamma_1(N)\alpha\Gamma_1(N)]_k.$$

Exercise V.1.3

$T_p, \langle d \rangle$ commute.

Proof. Note first that

$$\begin{aligned} \alpha^{-1}\Gamma_1 \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_1 \alpha &= \Gamma_1 \alpha^{-1} \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \alpha \Gamma_1 \\ &= \Gamma_1 \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_1. \end{aligned}$$

The second equality above requires a check. Then we know this is

$$\alpha^{-1} \coprod_j \Gamma_1 \beta_j \alpha = \coprod_j \Gamma_1 \alpha^{-1} \beta_j \alpha =: \coprod_j \Gamma_1 \beta_j'.$$

Then we can compute

$$T_p \langle d \rangle f = \sum_j f[\alpha]_k [\beta_j]_k = \sum_j f[\beta_j']_k [\alpha]_k = \langle d \rangle T_p f.$$

Last time we defined the Hecke operators $\langle d \rangle$, T_p. For convenience let N be fixed and write Γ_1 for $\Gamma_1(N)$.

Proposition V.1.3

For $f \in \mathcal{M}_k(\Gamma_1)$, write the Fourier expansion as $f(\tau) = \sum a_n(f) q^n$ where $q = e^{2\pi i \tau}$. Then we may write the Fourier expansion of $T_p f$ explicitly

$$(T_p f)(\tau) = a_{np}(f) q^n + 1_N(p) p^{k-1} a_n(\langle p \rangle f) q^{np}.$$

where 1_N is the trivial character of N evaluated at p. In particular if $f \in \mathcal{M}_k(N, \chi)$ we have

$$(T_p f)(\tau) = a_{np}(f) q^n + 1_N(p) p^{k-1} \chi(f) a_n(f) q^{np}.$$

Proof. A group theory exercise yields if $p \nmid N$ then

$$\Gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1 = \coprod_{j=0}^{p-1} \Gamma_1 \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$$

and if $p \mid N$ then

$$\Gamma_1 \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1 = \Gamma_1 \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \coprod \coprod_{j=0}^{p-1} \Gamma_1 \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix},$$

where $mp - nN = 1$.

We'll only do the $p \mid N$ cosets first. Here we have

$$\begin{aligned}(T_p f)(\tau) &= \sum_{j=0}^{p-1} f\left[\begin{pmatrix}1 & j\\ 0 & p\end{pmatrix}\right]_k \\ &= \sum_{j=0}^{p-1} p^{k-1}p^{-k} f\left(\frac{\tau+j}{p}\right) \\ &= \sum_{j=0}^{p-1}\sum_{n=0}^{\infty} \frac{a_n(f)}{p} e^{2\pi i n(\tau+j)/p} \\ &= \sum_{j=0}^{p-1}\sum_{n=0}^{\infty} \frac{a_n(f)}{p} \mu_p^{nj} q_p^n\end{aligned}$$

where $\mu_p = e^{2\pi i/p}, q_p = e^{2\pi i\tau/p}$. We have that

$$\sum_{j=0}^{p-1} \mu_p^{nj} = \begin{cases} p & \text{if } p \mid n \\ 0 & \text{if } p \nmid n\end{cases}.$$

Thus this becomes

$$(T_p f)(\tau) = \sum_n a_{pn} q^n.$$

For the $p \nmid N$ case we take

$$f\left[\begin{pmatrix}m & n\\ N & p\end{pmatrix}\begin{pmatrix}p & 1\\ 0 & 1\end{pmatrix}\right]_k = (\langle p\rangle f)\begin{bmatrix}p & 0\\ 0 & 1\end{bmatrix}_k(\tau).$$

This is

$$\sum_n p^{k-1} a_n(\langle p\rangle f) e^{2\pi i n p\tau} = \sum_n p^{k-1} a_n(\langle p\rangle f) q^{np}.$$

Proposition V.1.4

If $d, r \in (\mathbb{Z}/N\mathbb{Z})^\times$ and p, q are prime the

- $\langle d\rangle T_p = T_p\langle d\rangle$.
- $\langle d\rangle\langle r\rangle = \langle r\rangle\langle d\rangle$.
- $T_pT_q = T_qT_p$.

Now we may define $\langle n\rangle, T_n$ by

$$\begin{aligned}\langle n\rangle &= \begin{cases}\langle n\rangle & \text{if } (n,N)=1 \\ 0 & \text{if } (n,N)\neq 1\end{cases} \\ T_n &= \sum_{\substack{ad=n\\ a\mid d}} \langle a\rangle \left[\Gamma_1 \begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\Gamma_1\right]_k\end{aligned}$$

$$T_{p^2} = \left[\Gamma_1\begin{pmatrix}1 & 0\\ 0 & p^2\end{pmatrix}\Gamma_1\right]_k + \langle p\rangle T_1.$$

One may check this satisfies the recursion

$$T_{p^r} = T_p T_p^{r-1} - p^{k-1}\langle p\rangle T_{p^{r-2}}.$$

Then we can define $T_n = \prod_i T_{p_i^{r_i}}$ where $n = \prod p_i^{r_i}$. Then

$$(T_n f)(\tau) = \sum_n a_m(T_n f) q^m$$
$$a_m(T_n f) = \sum_{d|(m,n)} d^{k-1} a_{mn/d^2}(\langle d\rangle f).$$

V.2. **Peterson Inner Product**

Let $\tau = x + iy$, and write $\mathrm{d}\nu = \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$, which is the "hyperbolic measure" on $\mathcal{H}$. One can prove that $\mathrm{d}\nu$ is actually $\mathrm{GL}_2^+(\mathbb{R})$-invariant. This lets us integrate over $\mathcal{H}^*$.

Recall we have the fundamental domain

$$D^* = \{\tau \in \mathcal{H} \mid |\mathrm{Re}(\tau)| \le 1/2, |\tau| \ge 1\} \cup \{\infty\}.$$

We want to integrate on D^*. One may check that if $\varphi : \mathcal{H} \to \mathbb{C}$ is bounded and continuous then

$$\int_{D^*} \varphi(\alpha(\tau))\,\mathrm{d}\nu(\tau)$$

converges, where $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Take $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and write $\mathrm{SL}_2(\mathbb{Z}) = \coprod_j \{\pm I\}\Gamma\alpha_j$. If φ is Γ-invariant then the following will not depend on the choice of α_j,

$$\sum_j \int_{D^*} \varphi(\alpha_j(\tau))\,\mathrm{d}\nu(\tau) =: \int_{X(\Gamma)} \varphi(\tau)\,\mathrm{d}\nu(\tau).$$

We may then define

$$V_\Gamma := \int_{X(\Gamma)} \mathrm{d}\nu(\tau)$$

Definition V.2.1

We define the <u>Peterson inner product</u> of $f, g \in S_k(\Gamma)$ to be

$$\langle f, g\rangle := \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k\,\mathrm{d}\nu(\tau).$$

We normalize by the volume so that the inner product remains the same over $\Gamma_1 \subseteq \Gamma_2$. It takes some work but we must check $\varphi(\tau) := f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$ is Γ-invariant.

Remark V.2.1

We only need 1 of $f, g \in S_k(\Gamma)$ to be bounded.

Exercise V.2.1

We can see that

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{j(\gamma,\tau)\overline{j(\gamma,\tau)}}$$

$$\begin{aligned}\varphi(\gamma(\tau)) &= f(\gamma(\tau))\overline{g(\gamma(\tau))}\operatorname{Im}(\gamma(\tau))^k \operatorname{Im}(\gamma(\tau))^k \\ &= f[\gamma]_k j(\gamma,\tau)^k \overline{g[\gamma]_k j(\gamma,\tau)}^k \operatorname{Im}(\gamma(\tau))^k \\ &= f(\tau)g(\tau)\operatorname{Im}(\tau)^k = \varphi(\tau).\end{aligned}$$

Want: $M_k(\Gamma_1(N))$ has an orthonormal basis of eigenvectors under $\{T_n, \langle n\rangle \mid (n,N)=1\}$. We want to apply the spectral theorem, and we need $T_n, \langle n\rangle$ are normal.

Recall V.2.2

The adjoint is defined by $\langle Tf, g\rangle = \langle f, T^*g\rangle$ we take T is normal provided that $TT^* = T^*T$.

One can get a simultaneous orthonormal basis of eigenvectors using that these operators commute and some linear algebra.

Here's a fact: For any Γ, let $\alpha' = \det(\alpha)\alpha^{-1}$. Then

$$\langle f[\Gamma\alpha\Gamma]_k, g\rangle = \langle f, g[\Gamma\alpha'\Gamma]_k\rangle.$$

This implies that

$$\langle p\rangle^* = \langle p^{-1}\rangle.$$

As the relevant matrix is represented as $\left(\begin{smallmatrix} n & s \\ N & 0 \ p\end{smallmatrix}\right)$ of determinant 1 and its inverse can be represented by a similar matrix with p^{-1} in the bottom right. Then for T_p^* w ehave

$$\begin{aligned}\alpha &= \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\\ \alpha' &= p\begin{pmatrix}1 & 0\\ 0p^{-1} & \end{pmatrix} = \begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & n\\ N & mp\end{pmatrix}^{-1}\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\begin{pmatrix}p & n\\ N & m\end{pmatrix}.\end{aligned}$$

The left hand side is in $\Gamma_1(m)$ and the right hand side is in Γ_0. Thus we have something like

$$\Gamma_1\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1\begin{pmatrix}p & n\\ N & m\end{pmatrix}.$$

Thus $T_p^* = \langle p\rangle^{-1}Tp$.

V.3. **Oldforms and Newforms**

Last time we defined the Peterson inner product on $S_k(\Gamma)$. We then showed $S_k(\Gamma_1(N))$ has an orthonormal eigenbasis under $\{T_n, \langle n\rangle \mid (n,N)=1\}$.

We'll work on the non-coprime case as well! We want to talk about modular forms "coming from lower level."

- If $M \mid N$ we have a trivial inclusion $S_k(\Gamma_1(M)) \hookrightarrow S_k(\Gamma_1(N))$ because $\Gamma_1(M) \supseteq \Gamma_1(N)$.
- Now suppose $d \mid N/M$, and let $\alpha_d = \left[\begin{smallmatrix} d & 0\\ 0 & 1\end{smallmatrix}\right]$ (the action is $\alpha_d\tau = d\tau$). Then if $f \in S_k(\Gamma_1(M))$ then $f[\alpha_d]_k \in S_k(\Gamma_1(dM)) \subseteq S_k(\Gamma_1(N))$.

Proof. Fix $\gamma \in \Gamma_1(\delta M)$. Then we compute that

$$\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \delta^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b\delta \\ c\delta^{-1} & d \end{pmatrix}.$$

Thus since c contains a factor of δ we have this conjugate lies in $\Gamma_1(M)$.

Thus for each $d \mid N$ we may define

$$\begin{aligned} \iota_d : S_k(\Gamma_1(Nd^{-1}))^2 &\to S_k(\Gamma_1(N)) \\ (f, g) &\mapsto f + g[\alpha_d]_k. \end{aligned}$$

Definition V.3.1

We call the oldforms

$$S_k(\Gamma_1(N))^{\text{old}} := \operatorname{span}(\operatorname{im}(\iota_p) : p \mid N \text{ prime}).$$

We define the newforms $S_k(\Gamma_1(N))^{\text{old}}$ as the orthogonal complement of the oldforms under the Peterson inner product.

Proposition V.3.1

For all $n \in \mathbb{Z}_{>0}$, these spaces are stable under $\{T_n, \langle n \rangle\}$.

Proof. Let $p \mid N$. Case 1 is to take $(d, N) = 1$. Let $T = \langle d \rangle$ or $T = T_{p'}$ for $p' \neq p$. Then we can consider the diagram

$$\begin{tikzcd} S_k(\Gamma_1(Np^{-1}))^2 \arrow[r, "\left[\begin{smallmatrix} T & 0 \\ 0 & T \end{smallmatrix}\right]"] \arrow[d, "\iota_p"'] & S_k(\Gamma_1(Np^{-1}))^2 \arrow[d, "\iota_p"] \\ S_k(\Gamma_1(N)) \arrow[r, "T"'] & S_k(\Gamma_1(N)) \end{tikzcd}$$

Showing this commutes is shows that the oldforms remain oldforms. For $T = \langle d \rangle_N$, we can show $\langle d \rangle_N = \langle d \rangle_{Np^{-1}} = [\alpha_p] \langle d \rangle_N [\alpha_p]^{-1}$. For the other case one must check $T_{p', Np^{-1}} = T_{p', N}$. Checking the compatibility with $[\alpha_p]$ is frankly awful. We check Dirichlet character by Dirichlet character. That is we check for $g \in S_k(Np^{-1}, \chi)$ that we have

$$(T_{p', Np^{-1}} g)[\alpha_p] = T_{p', N}(g[\alpha_p]).$$

We can check this at the level of Fourier series.

The one thing we haven't checked is T_p, as all other operators are zero or combinations of these via multiplication (and recursion for say T_{p^2}. We do the same thing with a different matrix. Namely

$$\begin{tikzcd} S_k(\Gamma_1(Np^{-1}))^2 \arrow[r, "\left[\begin{smallmatrix} T_p & p^{k-1} \\ \langle p \rangle & 0 \end{smallmatrix}\right]^I"] \arrow[d, "\iota_p"'] & S_k(\Gamma_1(Np^{-1}))^2 \arrow[d, "\iota_p"] \\ S_k(\Gamma_1(N)) \arrow[r, "T_p"'] & S_k(\Gamma_1(N)) \end{tikzcd}$$

Proof for newforms is to show oldforms are invariant under $\langle n\rangle^*, T_n^*$. The only interesting case is $T_n, (n, N) >$ 1¿ THEn we have $T_n^* = \omega T_n \omega^{-1}$, where $\omega = \left[\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right]_k$.

We then need to suffer through the computation that

$$\iota_p \circ \begin{bmatrix} 0 & p^{k-2}\omega \\ \omega & 0 \end{bmatrix} = \omega \circ \iota_p.$$

Corollary V.3.2

$S_k(\Gamma_1(N))^{\text{old,new}}$ each have an orthonormal basis under $\{T_n, \langle n\rangle \mid (n, N) = 1\}$.

Consider $L_d : d^{1-k}[\alpha_d]_k$. Then on Fourier series this acts very simply

$$\sum_{n=1}^{\infty} a_n q^n \mapsto \sum_{n=1}^{\infty} a_n q^{dn}.$$

Thus if $f \in L_d$, then $a_n(f) = 0$ for $d \nmid n$. Then to have $f \in \operatorname{span}(\operatorname{im} L_p \mid p \mid N)$ we must have $a_n(f) = 0$ for all $(n, N) = 1$.

Theorem V.3.3 (Main lemma, Atkin-Lehmer)

The converse is true. That is if $a_n(f) = 0$ for all $(n, N) = 1$ then $f \in \operatorname{span}(\operatorname{im} L_p \mid p \mid N)$.

Proof of 1st Reduction. Define

$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \mod N \right\}$$

Fact: $\alpha_N \Gamma_1(N) \alpha_N^{-1} = \Gamma^1(N)$.

We can consider a map

$$L^M = M^{k-1}[\alpha_M^{-1}] : S_k(\Gamma_1(M)) \to S_k(\Gamma^1(N))$$

which sends $\sum a_n q^n$ to $\sum a_n q_m^n$ where $q_M = e^{2\pi i \tau / M}$. Then in fact the following diagram commutes where $N = dM$,

$$\begin{array}{ccc} S_k(\Gamma_1(M)) & \xrightarrow{L_d} & S_k(\Gamma_1(N)) \\ \\ S_k(\Gamma^1(M)) & \underset{\text{Incl}}{\hookrightarrow} & S_k(\Gamma^1(N)) \end{array}$$

by computing via Fourier series

$$\begin{array}{ccc} \sum a_n q^n & \xrightarrow{\quad L_d \quad} & \sum a_n q^{dn} \\ \\ \sum a_n q^{n/M} & \underset{\text{Incl}}{\hookrightarrow} & \sum a_n q^{n/M} = \sum a_n q^{dn/N}. \end{array}$$

Thus the main lemma amounts to saying that if $f \in S_k(\Gamma^1(N))$, $f = \sum_n a_n(f) q_N^n$ with $a_n(f) = 0$ for all $(n, N) = 1$ then

$$f \in \sum_p S_k(\Gamma^1(Np^{-1})) \subseteq S_k(\Gamma^1(N)).$$

Proof of Second Reduction, projections. We work in $\Gamma(N)$. For $d \mid N$ define

$$\Gamma_d = \Gamma_1(N) \cap \Gamma^0(Nd^{-1}).$$

Fact: $\Gamma(N)\backslash\Gamma_d$ has representatives

$$\left\{ \begin{pmatrix} 1 & bN/d \\ 0 & 1 \end{pmatrix} \mid 0 \leq b \leq d \right\}.$$

We'll define the following

$$\begin{aligned} \pi_d : S_k(\Gamma(N)) &\to S_k(\Gamma_d) \subseteq S_k(\Gamma(N)) \\ f &\mapsto \frac{1}{d} \sum_{b=0}^{d-1} f\left[\begin{smallmatrix} 1 & bN/d \\ 0 & 1 \end{smallmatrix}\right]_k \\ \sum_{n=1}^{\infty} a_n q_N^n &\mapsto \sum_{n, d \mid n} a_n q_N^n. \end{aligned}$$

We then can define

$$\pi = \prod_{p \mid N} (\operatorname{Id} - \pi_p).$$

This kills everything that's not coprime to N. Thus the condition for the Main Lemma is that $f \in S_k(\Gamma^1(N)) \cap \ker(\pi)$. We can then apply some linear algebra

$$\ker \pi = \ker \left(\prod_{p \mid N} (\operatorname{Id} - \pi_p) \right) = \sum_{p \mid N} \ker(\operatorname{Id} - \pi_p) = \sum_{p \mid N} \operatorname{im}(\pi_p).$$

But wait we know that $\operatorname{im}(\pi_p) = S_k(\Gamma_p)$. Thus for our reduction we need to show that

$$S_k(\Gamma^1(N)) \cap \sum_{p \mid N} S_k(\Gamma_1(N)) \cap \Gamma^0(Np^{-1}) = \sum_{p \mid N} S_k(\Gamma^1(Np^{-1})).$$

The $\supseteq$ inclusion is true from previous discussion.

Proof. We know $G = \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $S_k(\Gamma(N))$. We want to think of the spaces above as various fixed points of G. Write $G = \prod_i G_i = \prod_i \operatorname{SL}_2(\mathbb{Z}/p_i^{e_i})$ where $N = \prod_i p_i^{e_i}$. We then define H_i as

$$H_i \coloneqq \Gamma^1(p_i^{e_i}) / \Gamma(p_i^{e_i})$$

and $H = \prod H_i$. Define

$$K_i = \frac{\Gamma_1(p_i^{e_i}) \cap \Gamma^0(p_i^{e_i - 1})}{\Gamma(p_i^{e_i}}$$

Fact:

$$\langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1}) \rangle = \Gamma^1(p^{e-1}).$$

The third reduction becomes

$$S_k(\Gamma(N)) \cap \sum_{i=1}^{n} S_k(\Gamma(N))^{K_i} = \sum_{i=1}^{n} S_k(\Gamma(N)).$$

Now were looking at G acting on $S_k(\Gamma(N))$, we know that

Definition V.3.2

We say $f \in \mathcal{M}_k(\Gamma_1(N))$ is an eigenform if it is an eigenvector for all $\langle n \rangle, T_n$.

We say it is normalized if $a_1(f)$. A newform is an eigenform in $S_k(\Gamma_1(N))^{\text{new}}$.

The eigenvalues for diamond operators $\langle n \rangle$ will just be $\chi(n)$ where $f \in \mathcal{M}_k(N, \chi)$. What about for T_n? Recall the formula is

$$a_m(T_n f) = \sum_{d \mid (m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f).$$

Setting $m = 1$ yields

$$a_1(T_n f) = \chi(1) a_n(f) = a_n(f).$$

thus the eigenvalue is $a_n(f)/a_1(f)$.

Proposition V.3.4

For $f \in S_k(\Gamma_1(N))^{\text{new}}$, an eigenvector for $\{\langle n \rangle, T_n \mid (n, N) = 1\}$ is an eigenform.

Proof. All we have to check are the T_n.

Claim

For $f \in S_k(\Gamma_1(N))^{\text{new}}$, we have $a_1(f) \neq 0$.

If not, then we know for $(n, N) = 1$, we have

$$a_n(f) = a_1(T_n f) = c_n a_1(f) = 0.$$

The main lemma then would tell us $f \in S_k(\Gamma_1(N))^{\text{old}}$ because $a_n(f) \neq 0$ whenever f is a newform and $(n, N) = 1$.

Without loss of generality, assume $a_1(f) = 1$. Let $m \in \mathbb{Z}^+$, and consider $g_m = T_m f - a_m(f) f$. Then g_m is still an eigenform away from N (that is for $T_n, (n, N) = 1$). Furthermore $a_1(g_m) = 0$. Thus g_m is an oldform and a newform. Thus $g_m = 0$, so $T_m f = a_m(f) f$.

Corollary V.3.5 (Multiplicity 1)

If f, f' have the same T_m eigenvalues then $f' = cf$.

Proof. The eigenvalues are the coefficients upon normalization!

Theorem V.3.6

We have

$$B_k(N) \coloneqq \{f(n\tau) \mid f \text{ is a newform of level } M, nM \mid N\}$$

is a basis for $S_k(\Gamma_1(N))$.

Proof. We look at

$$S_k\left(\Gamma_1(N)\right) = S_k(\Gamma_1)^{\text{new}} \oplus \sum_{p \mid N} \iota_p(S_k(\Gamma_1(Np^{-1})))^2.$$

Spanning happens via induction.

Linear independence. Choose minimal linear combination

$$\sum_{i,j} c_{i,j} f_i(n_{i,j}\tau) = 0$$

where $f_i \in S_k(M_i, \chi_j)$. We can in fact require that all the χ_i lift to the same χ. Namely we can do this by applying $\langle d\rangle - \widetilde{\chi}_i(d)$ for some d with $\widetilde{\chi}_i(d) \neq \widetilde{\chi}_j(d)$ to get a nontrivial relation with fewer terms.

By applying $T_p - a_p(f_i)$ we can require all fourier coefficients away from N to agree, as otherwise we'd have a nontrivial relation with fewer terms.

Strong Multiplicity One implies the f_i must be the same, and then we're actually done.

Proposition V.3.7

Let $f \in \mathcal{M}_k(N, \chi)$. Then f is a normalized eigenform if and only if the Fourier coefficients satisfy

(1) $a_1(f) = 1$

(2) $a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \chi(p)p^{k-1}a_{p^{r-2}}(f)$.

(3) $a_{mn}(f) = a_m(f)a_n(f)$ for m, n coprime.

Proof. The forward direction is a bunch of computation. For the converse, we need to show

$$a_m(T_p f) = a_p(f)a_m(f)$$

for all p, m. If $p \nmid M$ then

$$a_m(T_p f) = a_{pm}(f) = a_p(f)a_m(f).$$

If $p \mid m$, write $m = p^r m'$ for $p \nmid m'$, then

$$a_m(T_p f) = a_{p^{r+1}m'}(f) + \chi(p)p^{k-1}a_{m'p^{r-1}}(f)$$

via the formula. Then

$$\begin{aligned} a_m(T_p f) &= a_{m'}(f)\left[a_{p^{r+1}}(f) + \chi(p)p^{k-1}a_{p^{r-1}}(f)\right] \\ &= a_{m'}(f)a_p(f)a_{p^r}(f). \\ &= a_p(f)a_m(f). \end{aligned}$$

Fact: $E_k^{\psi,\varphi}$ satisfy this. You just write down the Fourier coefficients...

V.4. **Connection with L-functions**

Let $f \in \mathcal{M}_k(\Gamma_1(\mathbb{N}))$. We may define for a complex variable $s \in \mathbb{C}$

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}.$$

The convergence of $L(s, f)$ in a half place will be given by estimating the Fourier coefficients. Namely it converges if $\mathrm{Re}(s) > k$, and if it is a cuspform then it converges if $\mathrm{Re}(s) > \frac{k}{2} + 1$.

Theorem V.4.1

The following are equivalent

- f is a normalized eigenform
- We have a product as

$$L(s, f) = \prod_p \left(1 - a_p p^{-s} + \chi(p) p^{k-1-2s}\right)^{-1}.$$

Proof. Being a normalized eigenform is equivalent to conditions (1),(2),(3) from before.

Exercise V.4.1

Let

$$X = \sum_{r=0}^{\infty} \frac{a_{p^r}}{p^{rs}},$$

then X is the p-part of the Euler product.

Idea: Plug in condition (2) for $r \geq 2$, and find an equation X must satisfy. Doing this in reverse shows relation (2) if we have the Euler product.

Taking $s \to +\infty$ yields $L(s, f) = 1$ if and only if $a_1(f) = 1$.

Fact: Let g be a function on prime powers. Then

$$\prod_p \sum_{r=0} g(p^r) = \sum_{n=1}^{\infty} \prod_{p^r || n} g(p^r).$$

Assuming (1),(2),(3) We then write

$$\begin{aligned}
L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} &= \sum_{n=1}^{\infty} \left(\prod_{p^r | a_{p^n}} n^{-s} \right) \\
&= \sum_{n=1}^{\infty} \prod_{p^r | n} \frac{a_{p^r}}{p^{rs}} \\
&= \prod_p \sum_{r=0}^{\infty} \frac{a_{p^r}}{p^{rs}} \\
&= \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}.
\end{aligned}$$

Running the equalities backwards gives essentially the converse.

Now we'll look at functional equations. Let $f = \sum a_n q^n \in S_k(\Gamma_1(\mathbb{N}))$. Recall that the Mellin transform of some function ϕ is defined to be

$$\psi(s) = \int_{t=0}^{\infty} \phi(it) t^s \frac{\mathrm{d}t}{t}.$$

Proposition V.4.2

The Mellin transform of $f = \sum a_n q^n$ is $\frac{1}{(2\pi)^s}\Gamma(s)L(s,f)$.

Well we see that

$$\begin{aligned} g(s) &= \int_{t=0}^{\infty} \sum_n a_n e^{-2\pi n t} t^s \frac{\mathrm{d}t}{t} \\ &= \sum_n a_n \int_{t=0}^{\infty} e^{-2\pi n t} t^s \frac{\mathrm{d}t}{t} \\ &= \sum_n \frac{a_n}{(2\pi)^s n^s} \Gamma(s) \\ &= \frac{1}{(2\pi)^s} \Gamma(s) L(s,f). \end{aligned}$$

via change of variables.

Definition V.4.1

Let $\Gamma_N = \frac{N^{s/2}}{(2\pi)^s}\Gamma(s)L(s,f)$. Then define the operator W_N as

$$f \mapsto i^k N^{1-k/2} f \left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right]_k.$$

This is in fact an involution and so has eigenvalues ± 1.

Theorem V.4.3

If $f \in S_k(\Gamma_1(N))^{\pm}$ (eigenspaces for W_N) then $\Gamma_N(s) = \pm\Gamma_N(k-s)$.

This implies that $L(s,f)$ has an analytic continuation just as for the Riemann zeta function.

VI. Jacobians and Abelian Varieties

Let X be a Compact Riemann Surface

If the genus $g = 1$ (warmup), then $X = \mathbb{C}/\Lambda$ for some lattice Λ. Pick a differential $\mathrm{d}x$ on X. Then we can look at

$$\begin{aligned} X &\to \{\text{path integrals on } X \text{ starting at } 0\}/\{\text{integrals over loops}\} \\ z + \Lambda &\mapsto \int_0^{z+\Lambda} \mathrm{d}x/\text{integrals over loops}. \end{aligned}$$

Any loop will be a combination of the two fundamental loops $0 \to \omega_1$ and $0 \to \omega_2$, where $\Lambda = \mathbb{Z}\langle \omega_1, \omega_2 \rangle$.

This is an isomorphism of groups so long as the differential is translation invariant. We want to generalize this to $g > 1$.

Let $\gamma : [0,1] \to X$ be some path. Fix $\omega \in \Omega^1_{\text{hol}}(X)$, that is a 1-form on charts which agrees on intersections. We can check $\int_\gamma \omega$ makes sense.

Let γ, γ' have the same endpoints. Then $\int_\gamma \omega$ and $\int_{\gamma'} \omega$ differ by an integral over a loop. If X is genus g then it looks like a sphere with g-many handles coming off of it.

Let $A_1, \ldots, A_g$ be the longitudinal loops at 0 and $B_1, \ldots, B_g$ be the latitudinal loops about these g handles. Fact: for any loop α at 0, there exists unique integers m_i, n_i so that

$$\int_\alpha \omega = \sum_i \left(m_i \int_{A_i} \omega + n_i \int_{B_i} \omega \right).$$

Definition VI.0.1

Let $H_1(X, \mathbb{Z})$ be the $\mathbb{Z}$-linear combinations of A_i, B_i (this is the integral homology of X. This gives us a map

$$H_1(X, \mathbb{Z}) \hookrightarrow \Omega^1_{\text{hol}}(X)^* = \operatorname{Hom}_{\mathbb{C}}(\Omega^1_{\text{hol}}(X), \mathbb{C}).$$

Fact: $\Omega^1_{\text{hol}}(X)^* \cong H_1(X, \mathbb{Z}) \otimes \mathbb{R} =: H_1(X, \mathbb{R})$.

We define

Definition VI.0.2

The Jacobian of X, denoted $\operatorname{Jac}(X)$ is

$$\Omega^1_{\text{hol}}(X)/H_1(X, \mathbb{Z}).$$

There is a map $X \hookrightarrow \operatorname{Jac}(X)$.

VI.1. **Connection to Divisors**

Now we're gonna look at the connection to divisors

$$\operatorname{Div}^0(X) = \left\{ \sum_{x \in X} n_x[x] \mid n_x = 0 \text{ for almost all } x, \sum_x n_x = 0 \right\}$$
$$\operatorname{Div}^\ell(X) = \left\{ \delta \in \operatorname{Div}^0(X) \mid \delta = \operatorname{div}(f), f \in \mathbb{C}(X) \right\}.$$

Definition VI.1.1

We call the Picard group of X

$$\operatorname{Pic}^0(X) = \operatorname{Div}^0(X)/\operatorname{Div}^\ell(X).$$

In genus $g = 0$, we have $\operatorname{Pic}^0(X) = \{0\}$, because we can just manufacture a rational function for any divisor.

If $g > 0$, fix a basepoint x_0. The map

$$X \hookrightarrow \operatorname{Pic}^0(X)$$
$$x \mapsto [x] - [x_0].$$

This is in fact an embedding!

Theorem VI.1.1 (Abel)

We have that $\operatorname{Pic}^0(X) \xrightarrow{\sim} \operatorname{Jac}(X)$, the map here is given by $\sum_x n_x[x] = \sum_x n_x \int_{x_0}^x$.

Theorem VI.1.2 (Modularity)

Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then there exists an N such that there is a map

$$J_0(N) \twoheadrightarrow E,$$

which is a holomorphic group homomorphism of complex tori, where $J_0(N) \coloneqq \mathrm{Jac}(X_0(N))$.

This automatically gives a map $X_0(N) \to E$, and one can argue it is still surjective. This version of Modularity turns out to be equivalent to the old one.

We also have a nice description of $\Omega^1_{\mathrm{hol}}(X(\Gamma))$, namely

$$\Omega^1_{\mathrm{hol}}(X(\Gamma)) = S_2(\Gamma).$$

We want to look at maps of Jacobians. Namely given X, Y compact riemann surfaces and a map $h : X \to Y$ we want to produce maps

$$h_J : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$$
$$h^J : \mathrm{Jac}(X) \leftarrow \mathrm{Jac}(Y)$$

We obviously have a map

$$h^* : \mathbb{C}(Y) \to \mathbb{C}(X)$$
$$g \mapsto g \circ h.$$

Then in fact $v_x(h^* g) = e_x v_{h(x)} g$ where e_x is the ramification number of h at x.

Recall that $\omega \in \Omega^1_{\mathrm{hol}}(Y)$. Then in charts this is $\omega = (\omega_i)$, where $\omega_i = f_i(q)\,\mathrm{d}q$. This induces a pushforward map as we know how to act on $f_i(q) \in \mathbb{C}(Y)$.

$$h^* : \Omega^1_{\mathrm{hol}}(Y) \to \Omega^1_{\mathrm{hol}}(X)$$
$$h_* : \Omega^1_{\mathrm{hol}}(X)^* \to \Omega^1_{\mathrm{hol}}(Y)^*$$

Let γ be a path in X, then $h(\gamma)$ is a path in Y, and it turns out for $\lambda \in \Omega^1_{\mathrm{hol}}(Y)$ we have

$$\int_\gamma h^*\lambda = \int_{h\circ\gamma} \lambda,$$

which is just a change of variables.

This then induces a map

$$h_J : \mathrm{Jac}(X) \to \mathrm{Jac}(Y).$$

Explicitly, we have

$$h_J\left(\sum_x n_x \int_{x_0}^{x}\right) \bullet = \sum_x n_x \int_{h(x_0)}^{h(x)} \bullet = \sum_x n_x \int_{x_0}^{x} h^*(\bullet).$$

where $\bullet \in \Omega^1_{\text{hol}}(Y)$. We now turn to the Picard group. We can define a norm map

$$\begin{aligned} \operatorname{norm}_h &: \mathbb{C}(X) \to \mathbb{C}(Y) \\ (\operatorname{norm}_h f)(y) &= \prod_{x \in h^{-1}(y)} f(x)^{e_x}. \end{aligned}$$

Then we have

$$v_y(\operatorname{norm}_h f) = \sum_{x \in h^{-1}(y)} v_x(f).$$

Then we can look at

$$\operatorname{div}(\operatorname{norm}_h f) = \sum_y \sum_{x \in h^{-1}(y)} v_x(f)[y] = \sum_x v_x(f)[h(x)].$$

This lets us predict that

$$\begin{aligned} h_D &: \operatorname{Div}(X) \to \operatorname{Div}(Y) \\ h_D\left(\sum_x n_x[x]\right) &\mapsto \sum_x n_x[h(x)] \end{aligned}$$

so then

$$h_D(\operatorname{div}(f)) = \operatorname{div}(\operatorname{norm}_h f).$$

We then get a map

$$\begin{aligned} h_P &: \operatorname{Pic}^0(X) \to \operatorname{Pic}^0(Y) \\ h_P([d]) &= [h_D(d)]. \end{aligned}$$

There is then a diagram of the form

$$\begin{tikzcd} \operatorname{Pic}^0(X) \arrow[r, "h_P"] \arrow[d, "\sim"'] & \operatorname{Pic}^0(Y) \arrow[d, "\sim"] \\ \operatorname{Jac}(X) \arrow[r, "h_J"'] & \operatorname{Jac}(Y). \end{tikzcd}$$

Recall VI.1.1

We have that

$$\begin{aligned} \operatorname{Jac}(X) &= \Omega^1_{\text{hol}}(X)^*/H_1(X,\mathbb{Z}) \\ \operatorname{Pic}^0(X) &= \operatorname{Div}^0(X)/\operatorname{Div}^\ell(X). \end{aligned}$$

and a theorem of Abel says that

$$\begin{aligned} \operatorname{Pic}^0(X) &\xrightarrow{\sim} \operatorname{Jac}(X) \\ \sum n_x x &\mapsto \sum_x n_x \int_{x_0}^x \cdot \end{aligned}$$

> We had defined pushforwards
>
> $$h_P : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$$
>
> $$h_J : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$$
>
> where $h : X \to Y$ is a map of compact Riemann Surfaces. The first was a norm map, and the second was pullback of differentials.

We now want the pullbacks. Let $h : X \to Y$, and let $X' = X - \mathcal{E}$, $Y' = Y - h(\mathcal{E})$ where we've cut out the ramified points (those with multiplicity). Then $h : X' \to Y'$ is a d-fold cover for some d.

To define the pullbacks we define the pushforwards of differentials

$$\mathrm{tr}_h : \Omega^1_{\mathrm{hol}}(X) \to \Omega^1_{\mathrm{hol}}(Y).$$

Let $y \in Y'$. Take a small $y \in U \subseteq Y'$ so that $h_i^{-1} : U \to U_i$ is defined (since this is a covering map). Then we define for $\omega \in \Omega^1_{\mathrm{hol}}(X)$ to be

$$(\mathrm{tr}_h \omega)\big|_U = \sum_{i=1}^{d} (h_i^{-1})^*(\omega\big|_U).$$

One must check this is well-defined on Y' and that it extends holomorphically to Y.

Dually, we get

$$\mathrm{tr}_h^* : \Omega^1_{\mathrm{hol}}(Y)^* \to \Omega^1_{\mathrm{hol}}(X)^*.$$

We need to pullback loops as well. Given a path δ in Y' and a basepoint $x \in h^{-1}(\delta(0)) \subseteq X'$, there is a unique path γ lying in X' which lifts δ and satisfies $\gamma(0) = x$. This gives d lifts total.

What if δ is in Y but only endpoints can be in $h(\mathcal{E})$? Then for each x, there are e_x many lifts γ which begin at x. There are then d lifts total.

If δ is a loop in Y', then $\gamma(1) \in h^{-1}(\delta(0))$ for any lift γ. Thus we can take the concatenation of all the lifts of δ. This will give us some collection of loops in cycles!

In other words, fixing $y_0 \in Y'$, then $\pi_1(y_0, Y')$ acts on $h^{-1}(y_0)$, and this is called the monodromy action.

Reverse change of variables

$$\int_{\delta \in Y'} (h^{-1})^* \omega = \int_{h^{-1} \circ \delta} \omega$$

for $\omega \in \Omega^1_{\mathrm{hol}}(X)$. Hence

$$\int_\delta \mathrm{tr}_h \omega = \sum_{\text{all lifts } \gamma} \int_\gamma \omega,$$

for δ lying in Y'. One can extend this formula to δ in Y, not just Y'.

Thus tr_h^* descends to

$$h^J : \mathrm{Jac}(Y) \to \mathrm{Jac}(X).$$

In fact, for $\lambda \in \Omega_{\mathrm{hol}}(Y)$ we have

$$(\mathrm{tr}_h \circ h^*)(\lambda) = \deg(h)\lambda.$$

As a consequence we have the fact that

$$h_J \circ h^J = [\deg h].$$

This is similar to the fact that we had for elliptic curves and isogenies!

Corollary VI.1.3

We have that

$$h_*(H_1(X, \mathbb{Z})) \subseteq H_1(Y, \mathbb{Z})$$

is of finite index.

What about for Picard Groups? For $h : X \to Y$, we have

$$h^* : \mathbb{C}(Y) \to \mathbb{C}(X)$$

and

$$\operatorname{div}(h^* g) = \sum_x e_x v_{h(x)}(g)[x] = \sum_y v_y(g) \sum_{x \in h^{-1}(y)} e_x[x].$$

This suggests we should define

$$h^D\left(\sum_y n_y[y]\right) = \sum_y n_y \sum_{x \in h^{-1}(y)} e_x[x].$$

This in fact gives you

$$h^P : \operatorname{Pic}^0(Y) \to \operatorname{Pic}^0(X).$$

These maps actually commute with the Abel-Jacobi isomorphism $\operatorname{Pic}^0(-) \to \operatorname{Jac}(-)$!

VI.2. **Jacobians and Hecke Operators**

Suppose $\Gamma_1, \Gamma_2 \subseteq \mathrm{SL}_2(\mathbb{Z})$ are congruence subgroups. Then suppose $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Then we can define

$$\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 \qquad\qquad \Gamma_3' = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}.$$

Then for the modular curves, we have a picture

$$\begin{tikzcd} X_3 \arrow[r, "\overset{\alpha}{\sim}"] \arrow[d, "\pi_2"'] & X_3' \arrow[d, "\pi_1"] \\ X_2 & X_1. \end{tikzcd}$$

We'll then define

$$[\Gamma_1\alpha\Gamma_2]_2 : \operatorname{Div}(X_2) \to \operatorname{Div}(X_1)$$

which is given by $(\pi_1)_D \circ \alpha_D \circ (\pi_2)^D$. Now let $\gamma_{2,j}$ be representatives of the quotient $\Gamma_3\backslash\Gamma_2$. Then recall that with $\beta_j \coloneqq \alpha\gamma_{2,j}$ we have

$$\Gamma_1\alpha\Gamma_2 = \bigsqcup_j \Gamma_1\beta_j.$$

Upshot:

$$[\Gamma_1 \alpha \Gamma_2]^2 : \mathrm{Pic}^0(X_2) \to \mathrm{Pic}^0(X_1).$$

We can compute for $\Gamma_2\tau \in X_2$, that we get

$$\begin{tikzcd}
\{\Gamma_3 \gamma_{2,j}\tau\} \arrow[r, mapsto, "\alpha"] & \{\Gamma_3' \beta_j \tau\} \arrow[d, mapsto, "\pi_1"] \\
\Gamma_2 \tau \arrow[u, mapsto, "\pi_2^{-1}"] & \{\Gamma_1 \beta_j \tau\}.
\end{tikzcd}$$

Explicitly, then the map is given by

$$[\Gamma_1 \alpha \Gamma_2]^2 \left(\sum_\tau n_\tau \Gamma_2 \tau\right) = \sum_\tau n_\tau \sum_j \Gamma_1 \beta_j \tau.$$

Remember that we had an isomorphism

$$w : S_2(\Gamma) \xrightarrow{\sim} \Omega^1_{\mathrm{hol}}(X(\Gamma)).$$

Then we must have

$$\mathrm{Jac}(X(\Gamma)) = S_2(\Gamma)^* / H_1(X(\Gamma), \mathbb{Z}).$$

We have defined a double coset operator

$$[\Gamma_1 \alpha \Gamma_2]_2 : S_2(\Gamma_1) \to S_2(\Gamma_2),$$

which induces a map

$$[\Gamma_1 \alpha \Gamma_2]_2^* : S_2(\Gamma_2)^* \to S_2(\Gamma_1)^*.$$

A priori this is not the same as $[\Gamma_1 \alpha \Gamma_2]^2$. But in fact these maps are the same!!!

Claim

Maps are the same. Essentially tr_{π_2} is defined on local patches which will be given by $\gamma_{2,j} \ldots$

Looking at $J_1(N) = \mathrm{Jac}(X(\Gamma_1(N)))$,

Proposition VI.2.1

Let $T = T_p, \langle d \rangle$. Then T acts on $J_1(N)$ by definition.

Easy consequence$T_p : S_2(\Gamma_1(N))^* \to S_2(\Gamma_1(N))^*$ descends to $J_1(N)$, and hence acts on $H_1(X_1, \mathbb{Z})$.

Then if $f = \mathrm{char}\, T_p$ has integer coefficients, then $f(T_p) = 0$ on $H_1(X_1, \mathbb{Z})$. Then $f(T_p) = 0$ on $S_2(\Gamma_1(N))^*$ hence $S_2(\Gamma_1(N))$.

Therefore the eigenvalues of T_p are algebraic integers. Then $a_p(f)$ are algebraic integers, so $a_n(f)$ is algebraic integer.

Definition VI.2.1

Consider the Hecke algebra over $\mathbb{Z}$ is defined as

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle \mid n \in \mathbb{Z}^+\}],$$

as operators on $S_2(\Gamma_1(N))$ (so there will be relations, ex. T_{p^3} is related to T_{p^2}, T_p).

There is an evaluation map (and it is a homomorphism) for each normalized eigenform $f \in S_2(\Gamma_1(N))$ given by

$$\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$$
$$Tf = \lambda_f(T)f.$$

Call $H_1 = H_1(X(\Gamma), \mathbb{Z})$, which is a finitely generated $\mathbb{Z}$-module. Then $\mathrm{End}(H_1)$ is a finitely generated $\mathbb{Z}$-module, and we know

$$\mathbb{T}_{\mathbb{Z}} \hookrightarrow \mathrm{End}(H_1)$$

from last time.

Likewise $\mathrm{im}(\lambda_f) = \mathbb{Z}[\{a_n(f)\}] \subseteq \mathbb{C}$. We may define $K_f = \mathbb{Q}(\{a_n(f)\})$. THen

$$|\mathrm{Hom}(K_f, \mathbb{C})| = [K_f : \mathbb{Q}].$$

If we have $\sigma \in \mathrm{Hom}(K_f, \mathbb{C})$ then we can take f to f^σ by mapping each coefficient in the Fourier series. Why the hell is this still a modular form?

Theorem VI.2.2

If $f \in S_2(N, \chi)$ and $\sigma \in \mathrm{Hom}(K_f, \mathbb{C})$, then $f \in S_2(N, \chi^\sigma)$. Furthermore, if f is a newform, then so is f^σ.

The rest of the class will be spent on proving this.

Recall VI.2.1 (Nakayama's Lemma, Commutative Algebra)

Suppose A is a commutative ring, $J \subseteq A$ is an ideal contained in all maximal ideals, and M is a finitely generated A-module. Then, if $M = JM$, we have that $M = \{0\}$.

Fix a basis $\varphi_1, \dots, \varphi_{2g}$ of $H_1(X_1(N), \mathbb{Z})$ over $\mathbb{Z}$. Let $V = H_1(X_1(N), \mathbb{Z})_{\mathbb{C}}$. Now $\mathbb{T}_{\mathbb{Z}}$ acts on V, which is a complex vector space by its action on the basis (i.e., formally weirdly enough). Suppose $v \in V$ is a λ-eigenvector of $\mathbb{T}_{\mathbb{Z}}$, where $\lambda : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$ is a homomorphism. Then if $\sigma \in \mathrm{Aut}(\mathbb{C})$ then v^σ is a λ^σ-eigenvector.

To proceed, we need to show the space of eigenvalues for V is the same as the space of eigenvalues for S_2. We'll construct a complement of $S_2^* \subseteq V$. We'll call the complement $\overline{S_2^*}$, and we'll study the eigenvalues of each piece of $V = S_2^* \oplus \overline{S_2^*}$.

Recall VI.2.2

Consider the operator $W_N = \left[\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right]_2$, and recall that $W_N T = T^* W_N$ for any Hecke operator T (where T^* is the adjoint for the Peterson inner product).

Define for each $g \in S_2$ a map

$$\psi_g : S_2 \to \mathbb{C}$$
$$h \mapsto \langle W_N g, h \rangle.$$

If we collect these into $\{\psi_g\} =: \overline{S_2^*}$, then $\overline{S_2^*}$ is a vector space and $g \mapsto \psi_g$ provides an isomorphism of vector spaces $S_2 \to \overline{S_2^*}$.

We actually need that they're isomorphic as a $\mathbb{T}_{\mathbb{Z}}$-module. This is fairly easy, and comes from the W_N factor.

Exercise VI.2.3

Verify that $S_2 \xrightarrow{\sim} \overline{S_2^*}$ as $\mathbb{T}_\mathbb{Z}$-modules.

Claim

$\mathbb{T}_\mathbb{Z}$-eigenvalues on S_2 and S_2^* are the same.

Proof. Let f be a normalized eigenform. Then take $\lambda_f : \mathbb{T}_\mathbb{Z} \to \mathbb{C}$, and let $J_f \coloneqq \ker(\lambda_f)$. We will show $J_f S_2 \neq S_2$ using Nakayama. We know that J_f is a prime ideal (being a kernel), but we don't know J_f is contained in every maximal ideal. The idea is to localize $\mathbb{T}_\mathbb{Z}$ at J_f, and then show we didn't kill everything by localizing.

Now we can look at

$$S_2^*[J_f] \coloneqq \{\varphi \in S_2^* \mid \varphi \circ T = 0, \forall T \in J_f\}.$$

Then we have a short exact sequence

$$0 \longrightarrow J_f S_2 \longrightarrow S_2 \longrightarrow S_2/J_f S_2 \longrightarrow 0,$$

which upon dualizing gives

$$0 \longleftarrow (J_f S_2)^* \longleftarrow S_2^* \longleftarrow (S_2/J_f S_2)^* \longleftarrow 0,$$

This implies that

$$S_2^* \supseteq (S_2/J_f S_2)^* \cong S_2^*[J_f].$$

We should show that the eigenvalue on the right hand side coming from f is the same as that on S_2.

Let $T \in \mathbb{T}_\mathbb{Z}$. Then for $\varphi \in S_2^*[J_f]$ we have

$$T \cdot \varphi = \varphi \cdot T = \varphi \circ [T - \lambda_f(T)\,\mathrm{Id}] + \lambda_f(T)\varphi.$$

The left hand side lies in J_f, so this becomes $T \cdot \varphi = \lambda_f(T)\varphi$. Perfect! This shows that if λ_f is an eigenvalue of S_2 then it is also an eigenvalue of S_2^* (and dualizing yields the converse).

Thus S_2 and $S_2^* \oplus \overline{S_2^*}$ have the same eigenvalues. Now we want to show that V and $S_2^* \oplus \overline{S_2^*}$ are isomorphic as $\mathbb{T}_\mathbb{Z}$-modules via

$$(z_1\varphi_1, \ldots, z_{2g}\varphi_{2g}) \mapsto \left(\sum_j z_j\varphi_j, \sum_j z_j\overline{\varphi}_j\right).$$

There is a short claim that this is well-defined, i.e. that the RHS lies in $\overline{S_2^*}$... this is an exercise.

It's injective as if $\sum_j z_j\varphi_j = 0$ and $\sum_j z_j\overline{\varphi}_j = 0$, then conjugating we get $\sum_j \overline{z}_j\varphi_j = 0$. This allows us to say $\sum \mathrm{Re}(z_j)\varphi_j = 0, \sum \mathrm{Im}(z_j)\varphi_j = 0$. But wait! As a real vector space the φ_j are all linearly independent, so $\mathrm{Re}(z_j) = 0, \mathrm{Im}(z_j) = 0$. Perfect! Then the $z_j = 0$.

Then they're complex vector spaces of the same dimension so they are isomorphic.

Why does this matter? Well take some $f \in S_2$ which is a normalized eigenform. So $\lambda_f : \mathbb{T}_\mathbb{Z} \to \mathbb{C}$ is an eigenvalue for S_2, so it is for V, and then λ_f^σ is an eigenvalue for V, but then it is an eigenvalue for S_2 by the above. So there is a $g \in S_2$ with eigenvalue λ_f^σ. Normalizing, we see the Fourier coefficients of g must be $\sigma(a_f(n))$ as Hecke operators can extract the Fourier coefficients.

This can similarly show $f \in S_2(N, \chi)$ maps to $f^\sigma \in S_2(N, \chi^\sigma)$, since diamond operators give the eigenvalue depending on χ for these. Showing f^σ is a newform if f is... should not be too hard

Corollary VI.2.3

$S_2(\Gamma_1)$ has a basis with $\mathbb{Q}$ Fourier coefficients.

Proof. Suppose f is a newform of level $m \mid N$ with field K. Let $\{\alpha_1, \ldots, \alpha_d\}$ be a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Let $\sigma_1, \ldots, \sigma_d$ be embeddings $K_f \hookrightarrow \mathbb{C}$. Then consider the matrix $A = \left(\alpha_i^{\sigma_j}\right)$. Now we can look at

$$F = \begin{pmatrix} f^{\sigma_1} \\ \vdots \\ f^{\sigma_d} \end{pmatrix}$$

$$g = Af$$

$$g_i = \sum_j \alpha_i^{\sigma_j} f^{\sigma_j}$$

Notice thenthat $g_i^\sigma = g_i$ for any σ. Then we need A is invertible (fact from algebraic number theory). Then

$$\operatorname{span}(g_i) = \operatorname{span}(f^{\sigma_i}).$$

The proof then proceeds by some basic induction, working newform by newform.

VI.3. Abelian Varieties and Modularity

Fix $f \in S_2(\Gamma_1(N))$ a newform of level N, then $\lambda_f : \mathbb{T}_\mathbb{Z} \to \mathbb{C}$ was defined last time as an evaluation map (for the eigenvalue), $I_f = \ker \lambda_f$, and we now define

$$A_f := J_1(N)/I_f J_1(N).$$

Note I_f, A_f only depend on the Galois orbit of f (in the sense discussed last time).

Well we know $\mathbb{T}_\mathbb{Z}/I_f$ acts on A_f, and we can look at this as a diagram

$$\begin{tikzcd} J_1(N) \arrow[r, "T_p"] \arrow[d] & J_1(N) \arrow[d] \\ A_f \arrow[r, "a_p"'] & A_f. \end{tikzcd}$$

Namely we have that

$$(a_p \cdot \varphi)(f^\sigma) = \varphi(a_p(f^\sigma) f^\sigma)$$

for $\varphi \in A_f$, and $a_p(f^\sigma)$ is the p-th Fourier coefficient of f^σ. We wish to study A_f. We say $f_1 \sim f_2$ if there is a Galois action σ for which $f_1 = f_2^\sigma$. The equivalence class of f is denoted $[f]$. We now define

$$V_f := \operatorname{span}(\{g \in [f]\}) \subseteq S_2(N).$$

We have since the galois orbits are linearly independent (easy check) that

$$\dim V_f = [K_f : \mathbb{Q}].$$

Now define

$$\Lambda_f = H_1(X(N), \mathbb{Z})\big|_{V_f} \subseteq V_f^*.$$

> **Proposition VI.3.1**
> $A_f \cong V_f^*/\Lambda_f$. Furthermore, this right hand side is a complex torus of dimension $[K_f : \mathbb{C}]$.

Proof. Condense notation as $S_2 = S_2(\Gamma_1(N)), H_1 = H_1(X_1(N), \mathbb{Z})$. Then by definition

$$\begin{aligned} A_f &= \frac{J_1(N)}{I_f J_1(N)} = \frac{S_2^*/H_1}{I_f(S_2^*/H_1)} \\ &\cong \frac{S_2^*}{I_f S_2^* + H_1} \cong \frac{S_2^*/I_f S_2^*}{\text{image of } H_1 \text{ in } S_2^*/I_f S_2^*}. \end{aligned}$$

Last time we had that this (on top) is the dual of the annihilator, $S_2[I_f]^*$

$$A_f \cong \frac{S_2[I_f]^*}{H_1\big|_{S_2[I_f]}}.$$

We will show that $V_f = S_2[I_f]$, and then the result follows. We will also show Λ_f is actually a lattice.

(1) We know $V_f \subseteq S_2[I_f]$. We need to know this is an equality. The strategy is just to compute the dimension of $S_2[I_f]$. Well

$$\dim(S_2[I_f]) = \dim(S_2[I_f]^*) = \dim(S_2^*/I_f S_2^*).$$

Then we have a pairing

$$\begin{aligned} \mathbb{T}_{\mathbb{C}} \times S_2 &\to \mathbb{C} \\ (T, g) &\mapsto a_1(Tg). \end{aligned}$$

Then we get $\mathbb{T}_{\mathbb{C}} \to S_2^*$. We claim the pairing is bilinear, non-degenerate.

- Bilinearity is easy.
- If $g \in S_2$, and $(T, g) = 0$ for all $\mathbb{T}_{\mathbb{C}}$, then $(T_n, g) = a_1(T_n g) = a_n(g)$, so $g = 0$.
- If $T \in \mathbb{T}_{\mathbb{C}}$ and $(T, g) = 0$ for all $g \in S_2$. But then we see that

$$a_n(Tg) = a_1(T_n T g) = a_1(T T_n g) = 0.$$

  Thus $Tg = 0$ for all g, so $T = 0$.

This shows an isomorphism $\mathbb{T}_{\mathbb{C}} \to S_2^*$. Thus

$$\dim(S_2[I_f]) = \dim(S_2^*/I_f S_2^*) = \dim(\mathbb{T}_{\mathbb{C}}/I_f \mathbb{T}_{\mathbb{C}}).$$

And in fact, since $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C}$ surjects onto $\mathbb{T}_{\mathbb{C}}$ we have

$$\dim(\mathbb{T}_{\mathbb{C}}/I_f \mathbb{T}_{\mathbb{C}}) \leq \dim\left(\frac{\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C}}{I_f \otimes \mathbb{C}}\right) = \dim\left(\frac{\mathbb{T}_{\mathbb{Z}}}{I_f} \otimes \mathbb{C}\right) = \operatorname{rank}(\mathbb{T}_{\mathbb{Z}}/I_f)$$

The second to last equality follows because $\mathbb{C}$ is free over $\mathbb{Z}$, and $\mathbb{Z}$ is a PID, so tensor product by $\mathbb{C}$ is exact. We finally claim

$$\operatorname{rank}(\mathbb{T}_{\mathbb{Z}}/I_f) = [K_f : \mathbb{Q}].$$

because $\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$ provides an isomorphism of $\mathbb{T}_{\mathbb{Z}}/I_f$ with the $\mathbb{Z}$-module generated by the coefficients of f in $\mathbb{C}$.

This in fact gives equality of the dimensions so $V_f = S_2[I_f]$. Further we get a nice fact that

$$\frac{\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C}}{I_f \otimes \mathbb{C}} \to \frac{\mathbb{T}_{\mathbb{C}}}{I_f \mathbb{T}_{\mathbb{C}}}$$

is an isomorphism!

(2) Showing that Λ_f is a lattice is a big computation like this that we will not do.

Clarification for people

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}\{T_n, \langle n\rangle\} \subseteq \mathrm{End}(S_2(\Gamma_1(N)))$$
$$\mathbb{T}_{\mathbb{C}} = \mathbb{C}\{T_n, \langle n\rangle\} \subseteq \mathrm{End}(S_2(\Gamma_1(N))),$$

but in fact $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C} \neq \mathbb{T}_{\mathbb{C}}$. Not actually true... but one can imagine T_2 scales by 3, and T_3 scales by $\sqrt{2}$ and everything else is zero. Then we would have $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C} \cong \mathbb{Z}^2 \otimes \mathbb{C} = \mathbb{C}^2$, and $\mathbb{T}_{\mathbb{C}} \cong \mathbb{C}$.

We do have a surjection

$$\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{C} \twoheadrightarrow \mathbb{T}_{\mathbb{C}}$$

as mentioned in the proof above.

Then $J_1(N)/I_f J_1(N) = A_f \cong V_f^*/\Lambda_f$ is a torus as desired.

Theorem VI.3.2

There is an isogeny (surjective homomorphism with finite kernel)

$$J_1(N) \to \bigoplus_{f,\ \text{level } N_f} A_f^{m_f}$$

where m_f is the number of divisors of N/N_f.

Proof. Must use the basis for $S_2(\Gamma_1(N))$. These were $f(n\tau)$ were f is a newform of some level and $n \mid N/N_f$. We rewrite the basis of $S_2(\Gamma_1(N))$ as

$$B_2(N) = \coprod_{[f]} \coprod_{n \mid N/N_f} \coprod_{\sigma} \{f^\sigma(n\tau)\}$$

We then define a map

$$\Psi_{f,n} : S_2(\Gamma_1(N))^* \to V_f^*$$
$$\varphi \mapsto \psi$$

such that

$$\psi\left(\sum_{j=1}^{d} z_j f^{\sigma_j}(\tau)\right) = \sum_{j=1}^{d} z_j n\varphi(f^{\sigma_j}(n\tau)).$$

We then claim that

Claim

$\Psi_{f,n}$ takes $H_1(X_1(N), \mathbb{Z})$ to $\Lambda_f = H_1(X_1(N_f), \mathbb{Z})\big|_{V_f}$.

Let $\varphi = \int_\alpha$, where α is a loop. Then

$$\psi(f^\sigma(\tau)) = n \int_\alpha f^\sigma(n\tau)\, \mathrm{d}\tau = \int_{\widetilde{\alpha}} f^\sigma(\tau)\, \mathrm{d}\tau.$$

where $\widetilde{\alpha} = n\alpha$. One can show that $\widetilde{\alpha}$ is a lift of a loop in $X_1(N_f)$.

We then obtain

$$\Psi = \prod_{f,n} \psi_{f,n} : S_2(\Gamma_1(N))^* \to \bigoplus_{f,n} V_f^* = \bigoplus_f (V_f^*)^{m_f}.$$

By the claim, this descends to a map

$$\overline{\Psi} : J_1(N) \to \bigoplus_f A_f^{m_f}.$$

We now must show $\overline{\psi}$ is an isogeny. We'll start with surjectivity. If φ is the dual vector of $f^\sigma(n\tau)$ then $\psi_{f,n}(\varphi)$ sends $f^\sigma(\tau)$ to n and everything else to 0, and $\psi_{g,n}(\varphi)$ is zero.

This makes up the basis that we'd like to have! To prove the finite kernel property, we need to show the image of H_1 in Λ_f under $\psi_{f,n}$ has the same rank as Λ_f.

This is a computation that is not too difficult.

This will allow us to state the modularity theorem in better terms, namely the surjection $J_1(N) \twoheadrightarrow E$ of the modularity theorem will be a specific map $AF_{\twoheadrightarrow}E$ for a specific newform!

Note: We've done everything for $\Gamma_1(N)$, we could do everything for $\Gamma_0(N)$. Note $X_1(N)$ surjects onto $X_0(N)$, and so indeed what we've done is precisely stronger. If we define

$$A'_f = J_0(N_f)/I_f J_0(N_f) \cong (V'_f)^*/\Lambda'_f,$$

and we get a map

$$J_0(N) \to \bigoplus_f (A'_f)^{m_f}.$$

The modularity theorem is then stated as

Theorem VI.3.3 (Modularity Theorem)

If E is an elliptic curve with $j(E) \in \mathbb{Q}$ then there exists an N and $f \in S_2(\Gamma_0(N))$ with a surjection $A'_f \twoheadrightarrow E$.

VII. The Land of Algebraic Geometry

VII.1. Complex Tori as Elliptic Curves

Recall VII.1.1

A complex torus is $\mathbb{C}/\Lambda$ where Λ is a lattice with $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Goal is to relate this to a cubic curve.

A meromorphic function is a holomorphic map $f : \mathbb{C}/\Lambda \to \widehat{\mathbb{C}}$. Put another way, this is a meromorphic Λ-periodic map $\mathbb{C} \to \mathbb{C}$ (or holomorphic $\mathbb{C} \to \widehat{\mathbb{C}}$).

The Weierstrass $\wp_\Lambda$ function is given by

$$\wp_\Lambda(z) \coloneqq \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

, where $z \in \mathbb{C} \setminus \Lambda$ and $\sum'$ means to exclude $\frac{1}{0}$.

The summand is $\sim \frac{z}{\omega^3}$, which can be used to show $\wp_\Lambda(z)$ converges absolutely and uniformly on all compact subsets away from Λ. Thus $\wp_\Lambda$ is holomorphic at all points $\mathbb{C} \setminus \Lambda$.

We can of course compute for $z \in \mathbb{C} \setminus \Lambda$ that

$$\wp'_\Lambda(z) = -2 \sum_{\omega\in\Lambda} \frac{1}{(z-w)^3}.$$

It is clear that $\wp'_\Lambda(z)$ is in fact Λ-periodic.

Exercise VII.1.2 (1.4.2)

Show that $\wp_\Lambda(z)$ must in fact be periodic.

Fact: The field of all meromorphic functions on $\mathbb{C}/\Lambda$ is given by $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ (that is rational expressions in $\wp_\Lambda, \wp'_\Lambda$).

Recall VII.1.3

We have the Eisenstein series

$$G_k(\tau) \coloneqq \sum_{c,d\in\mathbb{Z}}{}' \frac{1}{(c\tau+d)^k},$$

which is sum of reciprocals of k-th powers over a lattice $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.

This can generalize to a function of a lattice

$$G_k(\Lambda) \coloneqq \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^k}.$$

Usually we will take $k > 2$ to guarantee good convergence properties. Also if k is odd $G_k(\Lambda) \equiv 0$, so we'll restrict to k even.

There is then an identity for every $m \in \mathbb{C}^\times$,

$$G_k(m\Lambda) = m^{-k} G_k(\Lambda).$$

Theorem VII.1.1 (1.4.1)

The Laurent expansion of $\wp_\Lambda$ at $z = 0$ (i.e., on a tiny punctured disk about $z = 0$) is given by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{n=2\\ n \text{ even}}}^{\infty} (n+1) G_{n+2}(\Lambda) z^n.$$

Furthermore, we have the following relation

$$(\wp_\Lambda'(z))^2 = 4(\wp_\Lambda(z))^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda),$$

where $g_2(\Lambda) := 60G_4(\Lambda)$ and $g_3(\Lambda) := 140G_6(\Lambda)$.

Proof. For the first piece, recall

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sideset{}{'}\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

We see that

$$\begin{aligned}\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right)\\ &= \frac{1}{\omega^2}\left(\left(1 + \frac{z}{\omega} + \frac{z^2}{\omega^2} + \cdots\right)^2 - 1\right),\end{aligned}$$

since $z/\omega < 1$ for z sufficiently small and $\omega \in \Lambda$ nonzero (here using that Λ is discrete). In fact, upon simplifying, we see that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}.$$

We now have that

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + \sideset{}{'}\sum_{\omega\in\Lambda}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.\\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}\left(\sideset{}{'}\sum_{\omega\in\Lambda}\frac{1}{\omega^{n+2}}\right)(n+1)z^n,\end{aligned}$$

which is exactly what we want.

For the second part, we write

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + O(z^6)\\ \wp_\Lambda'(z) &= -\frac{2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + O(z^5).\end{aligned}$$

Both $(\wp_\Lambda'(z))^2$ and $4(\wp_\Lambda(z))^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$ look like

$$\frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + O(z^2).$$

Thus the difference of these two is a holomorphic function with value 0 at 0. Furthermore it is Λ-periodic, so by complex analysis (i.e., Liousville's theorem) it must be constant.

Proposition VII.1.2

The cubic equation

$$4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

has distinct roots. This is equivalent to $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$ (the discriminant), and equivalently this means the curve $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ is nonsingular.

Proof. In 1.4.1, not difficult to prove (just compute with an explicit lattice).

This is a cubic equation coming from a lattice on $\mathbb{C}$. This is our relation to elliptic curves! It gives us a map

$$\begin{aligned} \mathbb{C} \setminus \Lambda &\to \left\{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\right\} \\ z &\mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)). \end{aligned}$$

If we mod out by the lattice, this is a bijection (this is a simple computation). How does this compare to the torus $\mathbb{C}/\Lambda$? Well we're missing a point! By mapping Λ/Λ to some point at ∞, we get a bijection

$$\mathbb{C}/\Lambda \to \text{an "elliptic curve" } E_\Lambda.$$

We should see how the group law on the torus translates to E_Λ! We'll say zero is the point at ∞ as $\mathcal{O}_{E_\Lambda}$.

Then in fact "colinear points sum to zero" (this is not obvious but it is a computation). Namely if $z_1, z_2, z_3 \in E_\Lambda$ lie on the same line then $z_1 + z_2 + z_3 = \mathcal{O}$. When $z_1 = z_2$, we should take a line tangent to z_1! It turns out that $P = (x, y)$ gives $-P = (x, -y)$.

We actually have every elliptic curve $y^2 = 4x^3 - a_2x - a_3$ where $a_2^3 - 27a_3^2 \neq 0$ comes from a lattice. One can actually very explicitly write it down!

How should we consider isomorphisms of elliptic curves? Well consider $m \in \mathbb{C}^\times$, then

$$(x, y) \mapsto (m^{-2}x, m^{-3}y)$$

maps

$$\{y^2 = 4x^3 - a_2x - a_3\} \xrightarrow{\sim} \{y^2 = 4x^3 - m^{-4}a_2x - m^{-6}a_3\}.$$

This map comes from an isomorphism of tori, namely $z + \Lambda \mapsto mz + m\Lambda$.

Corollary VII.1.3

The discriminant function $\Delta : \mathcal{H} \to \mathbb{C}$, which we recall is

$$\Delta(\tau) = (g_2(\tau))^3 - 27(g_2(\tau))^2$$

is in fact never zero.

Proof. Up to some multiple, $\Delta(\tau)$ is in fact the discriminant of an elliptic curve E_{Λ_τ} (which is nonsingular).

VII.2. Elliptic curves as algebraic curves

This is section 7.1 in the book. Let k be a field of characteristic 0 and let $\overline{k}$ be the algebraic closure.

Definition VII.2.1

A Weierstrass equation over k is

$$y^2 = 4x^3 - a_2 x - a_3$$

for $a_2, a_3 \in k$. The discriminant is $\Delta = a_2^3 - 27a_3^2 \in k$. If $\Delta \neq 0$, then we define the j-invariant to be $j = \frac{1728a_2^3}{\Delta} \in k$. We call

$$E(x, y) = y^2 - 4x^3 + a_2 x + a_3.$$

Definition VII.2.2

If we have a Weierstrass equation with $\Delta \neq 0$, we say E is nonsingular and we call

$$\mathcal{E} = \{(x, y) \in \overline{k}^2 \mid E(x, y) = 0\} \cup \{\infty\},$$

an elliptic curve over k, which we can think of as a variety which is a subset of the projective plane $\mathbb{P}^2(\overline{k})$.

If L/k is any extension we write $\mathcal{E}(L)$ for $\mathcal{E} \cap \mathbb{P}^2(L^2)$.

Let L/k be Galois and $\mathcal{E}/k$ to be an elliptic curve over k. Furthermore let $\sigma \in \mathrm{Gal}(L/k)$, and for $x \in L$ write $x^\sigma \coloneqq \sigma(x)$. Then since $E(x, y) \in k[x, y]$ we have

$$E(x^\sigma, y^\sigma) = E(x, y)^\sigma$$

for $x, y \in L$. Thus there is a group action $\mathrm{Gal}(L/k)$ on $\mathcal{E}(L)$.

This actually can give you representations of a Galois group for certain curves/points on those curves. There is a group law on $\mathcal{E}$ where $P + Q + R = \mathcal{O}_\mathcal{E}$ if and only if $P, Q, R \in \mathcal{E}$ are colinear (over k). This also gives a group structure on $\mathcal{E}(L)$ for any $k \subseteq L \subseteq \overline{k}$. Namely we can just write down an equation for the point $P + Q$ and it's an equation over k.

Thus $\mathrm{Gal}(L/k)$ is acting on a group! It acts in a nice way, $\sigma \in \mathrm{Gal}(L/k)$ gives a group homomorphism $\mathcal{E}(L) \to \mathcal{E}(L)$, since the equation for $P + Q$ is an equation over k (and hence is carried over nicely by σ).

Theorem VII.2.1 (Bezout's Theorem)

If C_1, C_2 are two curves in x, y of degree d_1, d_2 then they meet in $d_1 d_2$ points in $\mathbb{P}^2(\overline{k})$, where we count with multiplicity.

Suppose $k = \mathbb{Q}$, so $\mathcal{E}/\mathbb{Q}$ is an elliptic curve. What can we say about the structure of $\mathcal{E}(\mathbb{Q})$. This is an abelian group. But what is it? It turns out $\mathcal{E}(\mathbb{Q})$ is finitely generated, and this result is called Mordell's Theorem. It is quite difficult to prove

Author's Note: I may include notes about the Mordell-Weil Theorem as an appendix from a UVA (Ono's) REU mini-course

The rank of $\mathcal{E}(\mathbb{Q})$ is often called the rank of an elliptic curve.

Recall VII.2.1

If k is a field of characteristic zero then the elliptic curve $\mathcal{E} \subseteq \overline{k}^2$ is the solutions to

$$E(x, y) = y^2 - 4x^3 + g_2 x + g_3,$$

> where $\Delta = g_2^3 - 27g_3^2 \neq 0$ (aka the curve is nonsingular, aka not all formal partial derivatives vanish at some P).

Why do we require that if $(x, y) \in \mathcal{E}$ with $D_1E(x, y) = 0$, $D_2E(x, y) = 0$. $D_2E(x, y) = 2y$, so if this is zero $y = 0$.

Factor $y^2 = 4(x - x_1)(x - x_2)(x - x_3)$. Then $E(x, y) = 0$ when $x = x_1, x_2, x_3$ since $y = 0$, but then this gives that $D_1E(x, y)$ vanishing implies there is a non-distinct root, so then $\Delta = 0$. The converse is similar.

Note: from our discussion last time, if a tangent line through P goes through ∞, then P is a 2-torsion point since $P + P + \infty = \infty$, $P = -P$. If the coefficients lie in some field k then we can write down the equation of the addition in this group structure as rational functions with coefficients in k.

> **Remark VII.2.1**
>
> We can think of an ellitpic curve $E[x, y] = \mathcal{E}$ as a functor from k-algebras to groups
>
> $$\mathcal{E} : R \mapsto \mathcal{E}(R) \subseteq R \times R.$$

Torsion! We will have that $E[N] \coloneqq \mathcal{E}(\overline{k})[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, where $\mathcal{E}(L)[N] = \{x \in \mathcal{E}(L) \mid Nx = \infty\}$. Last time, we saw that if L/K is Galois then $\mathrm{Gal}(L/k)$ acts on $\mathcal{E}(L)$, and this gives an action on N-torsion as $\mathrm{Gal}(L/k)$ acting on $\mathcal{E}(L)[N]$:

$$\rho : \mathrm{Gal}(L/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

To see that $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

VII.3. **Algebraic Curves and Function Fields**

Let $I = \langle \varphi_1, \ldots, \varphi_r \rangle \subseteq \overline{k}[x_1, \ldots, x_n]$. Now consider

$$V \coloneqq \{p \in \overline{k}^n \mid \varphi(p) = 0 \text{ for all } \varphi \in I\},$$

We then know that I is prime, so the coordinate ring $\overline{k}[V] = \overline{k}[x_1, \ldots, x_n]/I$ is an integral domain, and we can consider its field of fractions $\overline{k}(V)$. If $\overline{k}(V)$ is a finite dimensional extension of $\overline{k}(t)$, then we say V is an <u>affine algebraic curve</u>.

If $[D_j\varphi_i(p)]$ is rank $n - 1$ for each $p \in V$, then we say that V is nonsingular. This is nice, but we really want to homogenize. Say if φ_1 was $x_1 + x_2^2$ we would take it to $x_0x_1 + x_2^2$. Under this replacement if V' is the corresponding subset of $\overline{k}^{n+1}$ then $x \in V'$ implies $\lambda x \in V'$ for any $\lambda \in \overline{k}$.

We would then define $\mathbb{P}^r(\overline{k})$ to be the quotient of $\overline{k}^{r+1}$ by the action of scaling by an element of $\overline{k}$. This is <u>projective r-space over $\overline{k}$</u>. We can then consider

$$\begin{aligned}
I_{\text{hom}} &= \langle \varphi_{i,\text{hom}} \rangle \subseteq \overline{k}[x_0, \ldots, x_r] \\
V_{\text{hom}} &= \{\underbrace{[p_0 : \cdots : p_r]}_{p} \in \mathbb{P}^r(\overline{k}) \mid \varphi(p) = 0 \text{ for all } \varphi \in I_{\text{hom}}\}.
\end{aligned}$$

This will make V_{hom} compact which will be nice! V_{hom} is then called a <u>projective algebraic curve</u>.

Definition VII.3.1

We'll define the tangent space $T_p(C)$ (C is an affine algebraic curve) to be

$$T_p(C) \coloneqq \{v \in \overline{k}^n \mid [D_j\varphi_i(p)]v = 0\}.$$

We'll also consider $\mathfrak{m}_p \subseteq \overline{k}[C]$, which is the maximal ideal at p, to be

$$\mathfrak{m}_p \coloneqq \{f \in \overline{k}[C] \mid f(p) = 0\}.$$

Then $\mathfrak{m}_p/\mathfrak{m}_p^2$ is called the cotangent space at p.

Lemma VII.3.1

$\mathfrak{m}_p/\mathfrak{m}_p^2$ is naturally dual to T_pC as a vector space.

Proof. We must construct a perfect pairing

$$\mathfrak{m}_p/\mathfrak{m}_p^2 \times T_pC \to \overline{k}.$$

This will take $(f, v) \mapsto \nabla f(p) \cdot v$.

We must check this is well-defined. If $f \in \mathfrak{m}_p^2$ then $f = \sum g_i h_i$, where $g_i(p), h_i(p) = 0$, then

$$\nabla f(p) = \sum g_i(p) \cdot \nabla h_i(p) + \nabla g_i(p) \cdot h_i(p) = 0.$$

Furthermore, this is the coordinate ring, so if $\varphi \in I$, we see

$$\nabla \varphi \cdot v = 0,$$

since $\nabla \varphi_i \cdot v = 0$ for all φ_i. Linearity is clear. To show this is a perfect pairing, suppose $v \in T_pC$ and $(f, v) = 0$ for all f. Then $\nabla x_i(p) \cdot V = 0$, so $v = 0$.

To see the other direction, if $\nabla f \cdot v = 0$ then all the first-order partials vanish at p, and we can write f as...

Local Rings. Consider the localization $\overline{k}[C]_p \coloneqq \{f/g \in \overline{k}(C) \mid g(p) \neq 0\}$, then $M_p = \mathfrak{m}_p\overline{k}[C]_p$ is the unique maximal ideal, and

$$M_p/M_p^2 \cong \mathfrak{m}_p/\mathfrak{m}_p^2,$$

Theorem VII.3.2

$\overline{k}[C]_p$ is a discrete valuation ring

Proof. First we show M_p is principal. Take $t \in M_p$ generating M_p/M_p^2. Now consider $N = \langle t \rangle$. We want to show M_t/N is zero. Thus by Nakayama's Lemma we can show $M_p \cdot M_p/N = M_p/N$. We see that

$$M_p \cdot \frac{M_p}{N} = \frac{M_p^2 + N}{N} = \frac{M_p}{N}.$$

Can write any $f \in \overline{k}[C]_p$ as $t^e v$, then we define the valuation as $v_p(f) = e$. We also let $v_p(0) = \infty$.

More generally, for $f/g \in \overline{k}(C)$ we let

$$v_p(f/g) = v_p(f) - v_p(g)$$

This gives $v_p : \overline{k}(C) \to \mathbb{Z} \cup \{\infty\}$.

Note: Each $f/g \in \overline{k}(C)$ gives a map

$$\begin{aligned} C &\to \mathbb{P}^1(\overline{k}) \\ p &\mapsto \begin{cases} 0 & \text{if } v_p(f/g) > 0 \\ \infty & \text{if } v_p(f/g) < 0 \\ \frac{f(p)}{g(p)} & \text{if } v_p(f/g) = 0 \end{cases} . \end{aligned}$$

Exercise VII.3.1

Let $E(x,y) : y^2 = 4x^3 - 4x$. We want to compute $v_{(0,0)}\left(\frac{x}{y}\right)$.

Theorem VII.3.3

There's an equivalence of categories between projective nonsingular curves with non-constant maps and finite extensions of $k(t)$.

This is given by $C \leftrightarrow k(C)$, and is contravariant.

Proof Sketch. There is an equivalence

$$\text{varieties}/k \leftrightarrow \mathbb{K}/k$$

where the left hand side is dominant rational maps (dense image defined on an open).

This can be upgraded to curves$/k$ with finite extensions $\mathbb{K}$ of $k(t)$ by de-singularizing and compactitying (nontrivial, but reasonable).

For divisors, we can look at $h : C \to C'$ over k, then $h : \overline{k}(C') \to \overline{k}(C)$. Then $\deg h = [\overline{k}(C) : \overline{k}(C')]$.

We then have for $Q \in C'$ that

$$\sum_{p \in h^{-1}(Q)} e_p(h) = \deg h$$

where $e_p(h) = v_p(t' \circ h)$, where t' is a uniformizer at $h(p)$.

We can define $\mathrm{Div}, \mathrm{Div}^0, \mathrm{Div}^\ell, \mathrm{Pic}^0$ as before, and we get for each $h : C \to C'$ a pushforward and pullback

$$h_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C') h^* : \mathrm{Pic}^0(C') \to \mathrm{Pic}^0(C)$$

We have h_* sends $[p]$ to $[h(p)]$ and h^* sends $[Q]$ to $\sum_{p \in h^{-1}(Q)} e_p(h)[p]$. Then $h_* \circ h^* = [\deg h]$.

Theorem VII.3.4

If $\mathcal{E}$ is an elliptic curve, then the map $\mathrm{Div}(\mathcal{E}) \to \mathcal{E}$ induces an isomorphism

$$\mathrm{Pic}^0(\mathcal{E}) \xrightarrow{\sim} \mathcal{E}.$$

Proof. Map is a homomorphism, and restriction to $\mathrm{Div}^0(\mathcal{E})$ si surjective as $[p] - [0] \mapsto p$.

We want to show the kernel is Div^ℓ. The Lemma is

Lemma VII.3.5 (1) $p \neq q$ if and only if $[p] - [q]$ is not principal.

(2) $[p] - [0] + [Q] - [0] \equiv [P + Q] - [0]$ modulo Div^ℓ.

Suppose $[p] - [q]$ is principal, that is $[p] - [q] = \mathrm{div}(f)$. Then $f : \mathcal{E} \twoheadrightarrow \mathbb{P}^1(k)$ with p being sent to 0, q being sent to ∞.

The genus tells us this is a big problem, becasue $\mathbb{P}^1(k)$ has genus zero, and $\mathcal{E}$ has genus one. For the second part write $f(x, y) = ax + by + c$ in $k(\mathcal{E})$. Then

$$\mathrm{div}(f) = [P] + [Q] + [R] - 3[0].$$

Likewise the line through $R, -R$ has divisor $[R] - [0] + [-R] - [0]$. Thus

$$[P] + [Q] - 3[0] + 2[0] - [-R] \in \mathrm{Div}^\ell .$$

Then we have

$$[P] + [Q] - [P + Q] - [0] \in \mathrm{Div}^\ell .$$

Then $[P] + [Q] \equiv [P + Q] + [0]$, which is equivalent to what we wanted.

Now suppose we have $\sum_p [n_p]p = 0$ (that is the divisor $\sum_p n_p[p]$ goes to 0). By (1) this is true if and only if $\left(\sum_p n_p[p]\right) - [0]$ is principal.

By (2) this is if and only if $\left(\sum_p n_p([p] - [0])\right)$ is principal. By (1) this becomes $\sum n_p[p] \in \mathrm{Div}^\ell$. This is what we wanted!

Corollary VII.3.6

$\sum n_p[p]$ is principal if and only if $\sum n_p = 0$ and $\sum [n_p]p = 0$.

Weil Pairing! We'll look at

$$\mu_N = \{x \in \overline{k} \mid x^N = 1\},$$

while this might look like $\mathbb{Z}/N\mathbb{Z}$, it carries a nontrivial Galois action to keep track of. The Weil pairing is a map

$$e_N : \mathcal{E}[N] \times \mathcal{E}[N] \to \mu_N.$$

Let $P, Q \in \mathcal{E}[N]$ Then $N[Q] - N[0] \in \mathrm{Div}^\ell$ from our corollary. Say this is $\mathrm{div}(f)$. We now want to compute $\mathrm{div}(f \circ [N])$, which is

$$\sum_{R:[N]R=Q} N[R] - \sum_{S:[N]S=0} N[S].$$

We then fix $Q' \in \mathcal{E}[N^2]$ such that $[N]Q' = Q$. Then

$$\mathrm{div}(f \circ [N]) = N \sum_{S \in \mathcal{E}[N]} [Q' + S] - [S],$$

which we're supposed to see is principal, without the N! This is because $\mathcal{E}[N]$ has N^2 points. We then have this as $\mathrm{div}(g)$ and $\mathrm{div}(f \circ [N]) = \mathrm{div}(g^N)$.

For all $x \in E$, we have

$$g(x+p)^N = f([N]x + [N]P) = f([N]x) = g(x)^N,$$

Hence $\frac{g(x+P)}{g(x)} \in \mu_N$ and is constant. Thus we define

$$e_n(P,Q) = \frac{g(x+P)}{g(x)}.$$

Theorem VII.3.7

This map is bilinear in a multiplicative sense, i.e.

$$e_N(aP, cQ) = e_N(P,Q)^{ac}.$$

It's also alternating $e_N(Q,Q) = 1$. This implies that it's skew-symmetric.

Furthermore it's non-degenerate. Even more incredibly it is Galois equivariant $e_N(P,Q)^\sigma = e_N(P^\sigma, Q^\sigma)$. Finally, it is isomorphism invariant.

A lot of these are not that hard to check.

Corollary VII.3.8

We have $e_n(P', Q') = e_n(P,Q)^{\det\gamma}$ if

$$\begin{bmatrix} P' \\ Q' \end{bmatrix} = \gamma \begin{bmatrix} P \\ Q \end{bmatrix}.$$

Now we're going to look at function fields of modular curves. Recall that $\mathbb{C}(X(1)) = \mathbb{C}(j)$. We would like to compute $\mathbb{C}(X(N)), \mathbb{C}(X_1(N)), \mathbb{C}(X_0(N))$.

Take $v \in \mathbb{Z}^2$ with $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ nonzero. We write

$$f_0^{\overline{v}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp\left(\frac{cv\tau + dv}{N}\right),$$

and one can check this is weight 0 and $\Gamma(N)$-invariant, and it is meromorphic on the upper half plane and the cusps.

We define

$$\begin{aligned} f_0 &\coloneqq \sum_{d=0}^{N-1} f_0^{\overline{(0,d)}} \\ f_1 &\coloneqq f_0^{\overline{(0,1)}} \\ f_{(1,0)} &\coloneqq f_0^{\overline{(1,0)}} \\ j_N(\tau) &\coloneqq j(N\tau). \end{aligned}$$

Then we have the following proposition

Proposition VII.3.9

We have

$$\mathbb{C}(X(N)) = \mathbb{C}(j, f_{1,0}, f_1)$$

$$\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1)$$
$$\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N).$$

Moreover, $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is galois with group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$

We'll talk about this more next time. Of course we get a tower of Galois extensions of all of these.

Recall VII.3.2

$\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is Galois with group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I$.

How to check? We have a map $\theta : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X(N)))$ via $\mathrm{SL}_2(\mathbb{Z})$ acting via conjugation on $\Gamma(N)$ (giving us $\mathrm{SL}_2(\mathbb{Z})$ acting on functions). This is our hammer, and we've used it before (recall $f[\alpha]$).

It is easy to check that $\ker\theta = \pm I \cdot \Gamma(N)$. Then $\ker\theta = \pm I\Gamma(N)$. Then $\theta(\mathrm{SL}_2(\mathbb{Z}))$ in fact fixes $\mathbb{C}(X(1))$. Thus this gives a map into the Automorphism group. By Galois Theory, the fixed field will be some field extension, and it is not hard to show the fixed field is in fact $\mathbb{C}(X(1))$, which tells us everything we need.

Unrelated Note: If you want to know something about Weil groups, there's stuff from Tate from the Corvallis Conference with a nice note called Number Theory Background.

Recall that for Λ_τ given as $\mathbb{Z}\cdot 1 \oplus \tau\mathbb{Z}$, we have a map

$$\begin{aligned} \mathbb{C}/\Lambda_\tau &\to E_\tau \\ z &\mapsto (\wp_\tau(z), \wp_\tau'(z)), \end{aligned}$$

and the Elliptic Curve is as

$$E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

Recall that $f_0^{\overline{v}} = \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau\left(\frac{cv\tau+dv}{N}\right)$. One should think of this is the X-coordinate of some N-torsion

Suppose $j(\tau) \notin \{0, 1728\}$. This implies that $g_2(\tau), g_3(\tau)$. We then define

$$\begin{aligned} \mathbb{C}/\Lambda_\tau &\to \mathbb{C}^2 \cup \{\infty\} \\ z &\mapsto \left(\frac{g_2(\tau)}{g_3(\tau)}\wp_\tau, \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2}\rho_\tau'\right) \end{aligned}$$

this takes the torus to another elliptic curve $Ej(\tau)$ with equation

$$Ej(\tau) : y^2 = 4x^3 - \frac{(g_2(\tau))^3}{(g_3(\tau))^2}x - \frac{(g_2(\tau))^3}{(g_3(\tau))^2}.$$

This is an admissible change of variables from E_τ. Now $f_0^{\overline{v}}$ are x-coordinates of $E_{j(\tau)}[N]$. Moreover, if we let $v = (1,0), (0,1)$, this gives points P_τ, Q_τ which are a basis for the N-torsion.

We can rewrite the equations as

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j-1728}\right)x - \left(\frac{27j}{j-1728}\right).$$

We'll call this a "universal elliptic curve" over $X(1)$. There are two ways to think about this. We could say it's an ellitpic curve over $\mathbb{C}(X(1)) = \mathbb{C}(j)$, or we can think of it as

$$\begin{tikzcd} E_c \arrow[r] \arrow[d] & E_j \arrow[d] \\ \operatorname{Spec}\mathbb{C} \arrow[r, "c"'] & X(1)_{\mathrm{alg}} \end{tikzcd}$$

where we view $X(1)_{\mathrm{alg}}$ as the algebraic curve with function field $\mathbb{C}(X(1))$. We can enhance this elliptic curve as (E_j, P_τ, Q_τ), and this will live over $X(N)$.

Digression: There will be some functor $\mathcal{M} : \text{Schemes} \to \text{Sets}$ which is called a "moduli functor." In some sense this is

$$S \mapsto \{\text{"objects" over } S\},$$

where the objects could be interesting (say elliptic curves over S). The functor is called "representable" by some scheme M if

$$\mathcal{M}(S) \simeq \operatorname{Hom}(S, M),$$

with naturality in S. If this is true there's an incredible trick one can do. What if you let $S = M$. Then

$$\mathcal{M}(M) = \operatorname{Hom}(M, M).$$

This has a canonical element Id_M, which gives a *canonical* object over M. We'll call this $M_{\mathrm{univ}} \to M$. Messing with the Yoneda lemma tells us for any $S \to M$ we have

$$\begin{tikzcd} S \times_M M_{\mathrm{univ}} \arrow[r] \arrow[d] & M_{\mathrm{univ}} \arrow[d] \\ S \arrow[r] & M. \end{tikzcd}$$

This is what is called a "fine moduli space." It turns out $X(1)_{\mathrm{alg}}$ is NOT a "fine moduli space." There's some issue with it really being a compactification of $Y(1)$.

But even worse, we've thrown out $0, 1728$, which are the elliptic points. So our universal elliptic curve is just a close approximation of this.

Then $\mathbb{C}(X(N)) = \mathbb{C}(j, X(E_j[N]))$ over $\mathbb{C}(j)$. We can also adjoin the y-coordinates

$$\left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2} \wp'_\tau\left(\frac{c_v\tau + d_v}{N}\right).$$

One can show the Galois group of $\mathbb{C}(j, E_j[N])$ over $\mathbb{C}(j)$ is $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, making it an extension of $\mathbb{C}(j, X(E_j[N]))$.

Now lets look at this over $\mathbb{Q}$. The coefficients of E_j live in $\mathbb{Q}(j)$. Hence we get something like

$$\mathbb{Q}(j) \subseteq \mathbb{Q}(j, E_j[N]),$$

and this is still Galois. But the Galois group will be larger. The key is the roots of unity

$$\mu_N = \{z \in \overline{\mathbb{Q}} \mid z^N = 1\}.$$

We set

$$H_{\mathbb{Q}} = \operatorname{Gal}(\mathbb{Q}(\mu_N, j, E_j[N])/\mathbb{Q}(j)).$$

We have a map $H_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Where does it come from? Well $H_{\mathbb{Q}}$ acts on $E_j[N] \cong (\mathbb{Z}/N\mathbb{Z})^2 \subseteq \overline{\mathbb{Q}(j)}$.

Lemma VII.3.10

Take $\sigma \in H_{\mathbb{Q}}$, then for $\mu \in \mu_N$ we have

$$\sigma(\mu) = \mu^{\det(\rho(\sigma))}.$$

Proof. Use results from last time, since the Weil pairing is surjective we win.

Now if $\sigma \in H_{\mathbb{Q}}$ fixes $E_j[N]$ then $\sigma \in \ker(\rho)$, so $\sigma \in \ker(\det(\rho))$, so σ fixes μ_N. This implies $\mu_N \subseteq \mathbb{Q}(j, E_j[N])$. Another way to do this is the Weil pairing has an algebraic formula with coefficients in $\mathbb{Q}(j)$ and is surjective.

And also $\rho_\star = \rho\big|_{H_{\mathbb{Q}(\mu_N)}} : H_{\mathbb{Q}(\mu_N)} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $H_{\mathbb{Q}(\mu_N)} \subseteq H_{\mathbb{Q}}$ fixes the roots of unity. The original ρ is injective since if you fix $E_j[N]$ then you fix all of $\mathbb{Q}(\mu_N, j, E_j[N]) = \mathbb{Q}(j, E_j[N])$.

But then $\rho_\star$ injects into $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Well Galois Theory says we can take the situation over complex numbers

$$\begin{tikzcd}
\mathbb{C}(j, E_j[N]) \arrow[d, dash, "\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})"'] & \mathbb{Q}(j, E_j[N]) \arrow[d, dash] \\
\mathbb{C}(j) & \mathbb{C}(j) \cap \mathbb{Q}(j, E_j[N]) \arrow[d, dash] \\
& \mathbb{Q}(j)
\end{tikzcd}.$$

This implies $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ injects into $H_{\mathbb{Q}(\mu_N)}$. Therefore $H_{\mathbb{Q}(\mu_N)} \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Thus $H_{\mathbb{Q}} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, via some basic group theory.

We can then look at Modular Curves as Algebraic Curves. In particular, we have all these function fields

$$\begin{tikzcd}
\mathbb{Q}(j, E_j[N]) \arrow[r, squiggly, dash] \arrow[d, dash] & X(N)_{\mathrm{alg}} \arrow[d, dash] \\
\mathbb{Q}(j, F_1) \arrow[r, squiggly, dash] \arrow[d, dash] & X_1(N)_{\mathrm{alg}} \arrow[d, dash] \\
\mathbb{Q}(j, F_0) \arrow[r, squiggly, dash] \arrow[d, dash] & X_0(N)_{\mathrm{alg}} \arrow[d, dash] \\
\mathbb{Q}(j) \arrow[r, squiggly, dash] & X(1)_{\mathrm{alg}}
\end{tikzcd}$$

where $\mathbb{Q}(j, E_j[N])$ is Galois over $\mathbb{Q}(j), \mathbb{Q}(j, F_0), \mathbb{Q}(j, F_1)$. Thus these correspond to projective nonsingular curves. This is what we define as the algebraic version on the right hand side.

This allows us to formula algebraic versions of modularity. $X_0(N)_{\mathrm{alg}} \to E$ and $J_0(N)_{\mathrm{alg}} \to E$ which is a homomorphism.

And as discussed previously if $f \in S_2(\Gamma_0(N))$ then we want to look at a homomorphism $A'_{f,\mathrm{alg}} \to E$.

Last time: function fields of modular curves. Now, how can we make sense of isogenies $E \to E'$ algebraically and of Hecke operators?

For Hecke operators we already have $[\Gamma_1 \alpha \Gamma_2] : \mathrm{Div}(X_2) \to \mathrm{Div}(X_1)$. For $\Gamma_1(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ with (E, Q) an elliptic curve and Q its n-torsion we have

$$\begin{aligned} T_p &: \mathrm{Div}(X_1) \to \mathrm{Div}(X_1) \\ T_p[E, Q] &= \sum_C [E/C, Q + C] \end{aligned}$$

where C is a subgroup of order p and $C \cap \langle Q \rangle = \{0\}$.

Now for elliptic curves over arbitrary fields

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

One cannot do a standard change of variables in arbitrary characteristic (namely $2, 3$). But one can define Δ, j. For $j \neq 0, 1728$ we can look at the curve

$$y^2 + xy = x^3 - \left(\frac{36}{j - 1728}\right) x - \frac{1}{j - 1728}.$$

It is still true that $E \hookrightarrow \mathbb{P}^2(\overline{k})$ and this forms an abelain group. The Group equations are defined over $k_{\text{prime}}(\{a_i\})$, where k_{prime} is $\mathbb{F}_p, \mathbb{Q}$ depending on the characteristic of k.

Theorem VII.3.11

The N-torsion for $N = \prod_p p^{e_p}$ can be described as

$$E[N] = \prod_p E[p^{e_p}],$$

Furthermore

- $E[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^2$ if $\mathrm{char}(k) \neq p$.
- $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for every e, or $E[p^e] \cong 0$ for every e provided that $\mathrm{char}(k) = p$. The first is called the ordinary case and the second is called the supersingular case.

The point, $E[p^e]$ is a finite affine scheme over k. Thus this is still $\mathrm{Spec}(A)$ for some k-algebra A, where $\dim_k A = p^{2e}$. The problem is how many points we have on the scheme.

Consider μ_p, well this is $\mathrm{Spec}\left(k[x]/(x^p - 1)\right)$. In characteristic p this is $k[x]/(x-1)^p$. So then there's only one point on μ_p, this spectrum. This is exactly the sort of thing that is happening in general.

In the ordinary case, we have

$$E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$$

as a scheme.

We also need to study singular Weierstrass curves. That is when $\Delta = 0$. Suppose P is singular. We can change coordinates so that $P = (0, 0)$. We then get

$$C(x, y) = y^2 + a_1 xy - x^3 - a_2 x^2.$$

If $\mathrm{char}(k) \neq 2$, this can be simplfied to

$$C(x, y) = y^2 - x^3 - a_2' x^2.$$

Check from these equations that $(0, 0)$ is the only singular point.

Then write $E(x, y) = (y - m_1x)(y - m_2x) - x^3$. There are two cases

- If $m_1 \neq m_2$, then there are two tangent directions and this is called a nodal singularity. In this case we can get a group structure on the points where you're nonsingular and this is isomorphic to $\overline{k}^\times$. Thus this is often called the multiplicative case.
- If $m_1 = m_2$, then we call this a cusp and the group is $\overline{k}$ additively, and this is called the additive case.

Now we'll look at more algebraic properties of curves in arbitrary characteristic.

Question: Finite fields, Galois groups?

Recall VII.3.3

For every p^n, there is a unique field $\mathbb{F}_{p^n}$, which is a degree n extension of $\mathbb{F}_p$ with Galois group $\mathbb{Z}/n\mathbb{Z}$. Furthermore it is generated by the Frobenius map $x \mapsto x^p$.

We have $\mathbb{F}_{p^n}$ embeds in $\mathbb{F}_{p^m}$ if and only if $n \mid m$. Also $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \widehat{\mathbb{Z}}$, the inverse limit of all the $\mathbb{Z}/n\mathbb{Z}$.

We get $\sigma_p : \mathbb{P}^n(\overline{\mathbb{F}}_p) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$ given by

$$[x_0 : \cdots : x_n] = [x_0^p : \cdots : x_n^p].$$

Suppose we have a curve C with an embedding $C \hookrightarrow \mathbb{P}^n(\overline{\mathbb{F}}_p)$ cut out by equations $\varphi_1, \ldots, \varphi_k$. We can then define

$$C^{\sigma_p} : \varphi_1^{\sigma_p}, \ldots, \varphi_k^{\sigma_p},$$

where $\varphi_i^{\sigma_p}$ tells us to act on the coefficients of φ_i via σ_p. Then σ_p gives a map $C \to C^{\sigma_p}$, since 0 is fixed by σ_p and σ_p is a Galois automorphism. Essentially for any field map $\varphi^\sigma(\sigma(x)) = \sigma(\varphi(x))$.

This should then induce a map of function fields!

Example VII.3.4

Conisder

$$\sigma_p : \mathbb{P}^1(\overline{\mathbb{F}}_p) \to \mathbb{P}^1(\overline{\mathbb{F}}_p)$$

This then gives us

$$\begin{aligned} \overline{\mathbb{F}}_p(t) &\leftarrow \overline{\mathbb{F}}_p(t) \\ t^p &\leftarrow\!\shortmid t, \end{aligned}$$

and we can consider $\overline{\mathbb{F}}_p(t^p) = \overline{\mathbb{F}}_p(s)$. Then $t^p = s$, and the minimal polynomial is $x^p - s = x^p - t^p = (x-t)^p$. Furthermore, this map above is a bijection, but we *really* should not think of it as an isomorphism.

Then $\mathbb{F}_p(t)/\mathbb{F}_p(s)$ is an inseperable extension (separable extension is when the minimal polynomial has no repeated roots).

For any algebraic extension $k \subseteq K$, we can factor this as

$$k \hookrightarrow k^{\text{sep}} \to K,$$

where the first is separable, and the second is purely inseperable. Thus if we have $h : C \to C'$, we get a factoring as follows

$$C \hookrightarrow C_{\text{sep}} \to C',$$

where the first is inseparable and looks like σ_p^e, and the second is separable. Thus we get a factorization $h = h_{\text{sep}} \circ \sigma_p^e$.

Then $\deg(h) = \deg[K(C) : K(C')]$. Then $\deg(h) = \deg(h)_{\text{sep}} \deg(h)_{\text{inseparable}}$. It is still true that

$$\sum_{P \in h^{-1}(Q)} e_P(h) = \deg h,$$

where the ramification inseparable piece is ramified *everywhere* which is quite strange. In particular one thing that will be true is if $\varphi : E \to E'$, then

$$\deg(\varphi)_{\text{sep}} = |\ker \varphi| .$$

Example VII.3.5

The isogeny $[p] : E \to E$. The kernel is the p-torsion. Fact: $\deg[p] = p^2$ always. But the p-torsion may be smaller than p^2! This is because the inseperable piece is taking over.

We'll have $\deg[p]_{\text{sep}} = p$ in the ordinary case and $\deg[p]_{\text{sep}} = 1$ in the supersingular case.

Why do we care about this? Well if we have an elliptic curve with coefficients over $\mathbb{Z}$, we can reduce all the coefficents modulo p to get a curve over $\mathbb{F}_p$. This is called the reduction at p of this elliptic curve.

It turns out, sometimes when you reduce a nonsingular elliptic curve E over $\mathbb{Z}$ then sometimes it can become singular in the reduction. Here we'll fix $E/\mathbb{Q}$ and define

$$v_p(E) = \min(v_p(\Delta(E)) : E' \sim E),$$

where E' has integral coefficients via a change of coordinates from E. We also define

$$\Delta(E)_{\min} = \prod_p p^{v_p(E)}.$$

Fact: $\Delta(E)_{\min}$ can be achieved via a change of coordinates with a Weierstrass curve. We call such an integral curve achieving the minimal discriminant a "minimal Weierstrass model." From now on assume E is given in this form.

We then may reduce E to E_p. There are two reduction types

1) Good reduction, we get a nonsingular elliptic curve
   a) Ordinary $|E_p[p]| = p$.
   b) Supersingular $|E_p[p]| = 1$.
2) Bad reduction, there are many subtypes
   a) Multiplicative, $m_1 \neq m_2$.
      i) Split, $m_1, m_2 \in \mathbb{F}_p$
      ii) Nonsplit, $m_1, m_2 \notin \mathbb{F}_p$, in fact $m_1, m_2 \in \mathbb{F}_{p^2}$.
   b) Additive, $m_1 = m_2$.

HW: find an example of each reduction type, due next Tuesday.

Algebraic Conductor. This will be $N_E = \prod_p p^{f_p}$ where

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if multiplicative reduction} \\ 2 & \text{if additive reduction } p \neq 2,3 \\ 2+\delta_p & \text{if additive reduction } p \in \{2,3\} \end{cases}.$$

δ_p is something we'll look at later. We can be assured from the book that δ_p is no more than 6. Recall in the modularity theorem we wanted a map $X_0(N) \to E$. It turns out the N we need is N_E.

Last time: Reduction of $E/\mathbb{Q}$. The groups one gets in each case

- Good reduction: an elliptic curve
- Multiplicative split: $\mathbb{G}_m : R \mapsto \mathbb{G}_m(R) = R^\times$
- Multiplicative non-split, $U(1)$, the 1-units in $\mathbb{F}_{p^2}$ with $x^{p+1} = 1$. What would the points of a general R be for R an algebra over $\mathbb{F}_{p^2}$.
- Additive case, $\mathbb{G}_a : R \mapsto R^+$ (viewed as an additive group).

We want to understand reductions over $\overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$). Let $\overline{\mathbb{Z}}$ be the algebraic integers.

If we have a maximal ideal $\subseteq \overline{\mathbb{Z}}$ then $\cap \mathbb{Z} = p\mathbb{Z}$ for some p prime.

We can think of

$$\overline{\mathbb{Q}} = \bigcup_{K/\mathbb{Q} \text{ finite alg}} K.$$

For each K we have $\mathcal{O}_K$ the ring of integers of K, and play this same game (here $\overline{\mathbb{Z}} \cap K = \mathcal{O}_K$).

We can consider what $p\mathcal{O}_K$ is for p a prime. Then

$$p\mathcal{O}_K = \prod_{j=1}^{g_K} {}^{e_j}_{K,j},$$

where ${}_{K,j}$ are prime ideals in $\mathcal{O}_K$ and $e_i \in \mathbb{N}$. These will be maximal, so $\mathcal{O}_K/{}_{K,j}$ is a field (a finite extension of $\mathbb{F}_p$). It is customary to say

$$f_i = [\mathcal{O}_K/{}_{K,j} : \mathbb{F}_p].$$

Then we actually have

$$[K : \mathbb{Q}] = \sum_{j=1}^{g_K} e_j f_j.$$

An alternate way to view this, we have a map $\mathbb{Z} \to \mathcal{O}_K$ and so a map $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}$, and this is counting the degree at $p\mathbb{Z}$ in two different ways (degree defined appropriately)

> **Remark VII.3.1**
>
> Neukirch "Algebraic Number Theory" and also Cassels and Frohlich are good references for algebraic number theory.

If we have then $\subseteq \overline{\mathbb{Z}}$ then we can write it as

$$= \bigcup_{K/\mathbb{Q}} {}_K$$

such that for K'/K we have $\mathfrak{p}_{K'} \cap \mathcal{O}_K = {}_K$. Then in fact

$$\overline{\mathbb{Z}}_{(\overline{\mathfrak{p}})} = \{x/y \mid y \notin \overline{\mathfrak{p}}\}$$

$$\overline{\mathbb{Z}}_{(\overline{\mathfrak{p}})}/\overline{\mathfrak{p}} = \overline{\mathbb{Z}}/\overline{\mathfrak{p}} = \overline{\mathbb{F}_p}.$$

Lemma VII.3.12

If we have $\subseteq \overline{\mathbb{Z}}$ a maximal ideal and $\alpha \in \overline{\mathbb{Q}}$ then α or $1/\alpha$ lies in $\overline{\mathbb{Z}}_{()}$.

Proof. Fix α. Then $\alpha \in K/\mathbb{Q}$ for some finite extension $K/\mathbb{Q}$. Thus it suffices to show α or $1/\alpha$ lies in $\mathcal{O}_{K_{(_K)}}$. This is in fact easy since $\mathcal{O}_{K_{(_K)}}$ is a discrete valuation ring.

For the unitiated (including the current writer of the notes, check back with the future writer),this is a valuation map from the ring to $\mathbb{Z} \cup \{\infty\}$. Then $v_{_K} = -v_{_K}(1/\alpha)$. Furthermore $v_{_K}^{-1}(\mathbb{Z}_{\geq 0}) = \mathcal{O}_{K_{(_K)}}$, so one of these lies in the set.

Example VII.3.6

$K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}$ and p a prime. Then we write

$$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{a'p^k}{b'p^j}\right) = k - j,$$

where $a = a'p^k, b = b'p^j$ where $p \nmid a', b'$. The points in $\mathbb{Z}_{(p)}$ are exactly those points with nonnegative valuation.

Suppose we have an elliptic curve $E/\overline{\mathbb{Q}}$. Transform the Weierstrass equation so that we have something $\overline{\mathbb{Z}}$-integral. We know $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Z}}$. So we can assume the coefficients of E lie in $\overline{\mathbb{Z}}_{()}$.

Reduce via map $\overline{\mathbb{Z}}_{()} \to \overline{\mathbb{F}}_p$ to get Weierstrass equation. We can then make sense of ordinary, supersingular, multiplicative, and additive cases.

Potentially: Isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ are much bigger than those over $\mathbb{Q}$. In fact this happens. Thus when we think about reduction, the situation is slightly different.

Fact: So long as $p \neq 2$ we can change coordinates to the form

$$E : y^2 = x(x-1)(x-\lambda)$$

where $\lambda \notin \{0, 1\}$ and $\lambda \in \overline{\mathbb{Z}}_{()}$. Then one can check that additive reduction is not possible for an equation of this type. The same is true for $p = 2$, but this is not quite the right form.

Definition VII.3.2

A -minimal Weierstrass equation is one with only good or multiplicative reduction over .

Proposition VII.3.13

Reduction type is well defined on $\overline{\mathbb{Q}}$-isomorphism classes. That is the reduction type cannot move between good and multiplcative for minimal models like the above.

Proof. There is the number Δ, and there's another number c_4, associated to the elliptic curves. We in fact have

$$\text{additive reduction} \iff \Delta = 0, c_4 = 0 \mod$$

If we do a change of variables, then $u^{12}\Delta' = \Delta$ and $u^4 c_4' = c_4$ for some u (in terms of the change of coordinates).

The case we're frightened of–$\Delta' \in \overline{\mathbb{Z}}_{()}^{\times}$ but $\Delta \in \overline{\mathbb{Z}}$.

If this is the case then $u^{12}, u^4 \in \overline{\mathbb{Z}}_{()}$. Then c_4 will also lie this ideal, which will give us additive reduction (which is impossible with minimal models).

Proposition VII.3.14

$E/\overline{\mathbb{Q}}$ has good reduction at if and only if $j[E] \in \overline{\mathbb{Z}}_{()}$.

Proof. Remember that the j invariant is $j = c_4^3/\Delta$.

Reducing Points. There is a reduction map

$$\begin{aligned} \mathbb{P}^n(\overline{\mathbb{Q}}) &\to \mathbb{P}^n(\overline{\mathbb{F}}_p) \\ [x_0, \ldots, x_n] &\mapsto [\widetilde{x}_1, \ldots, \widetilde{x}_n]. \end{aligned}$$

Technical point, we have to scale $x_0, \ldots, x_n$ so that one of them does not lie in $\overline{\mathbb{Z}}$ and all of them lie in $\overline{\mathbb{Z}}_{()}$.

Hence $E \subseteq \mathbb{P}^2(\overline{\mathbb{Q}})$ can be reduced on points. We want to understand reduction of $E[N]$.

Theorem VII.3.15

We get a map $E[N] \to \widetilde{E}[N]$ that is surjective.

Proof. Getting the map is clear–equations for N-torsion are algebraic and we can just reduce. When $p \nmid 6N$, then $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ or $E[p^n] = 0$. The second obviously works and the first we'll get an isomorphism if we have injectivity...then we stare at the map.

Proposition VII.3.16

Say $E/\overline{\mathbb{Q}}$ has good reduction at p. Say $C \subseteq E$ is a cyclic subgroup of order p. Then

- E/C has good reduction
- $E, E/C$ have the same reduction type, ordinary versus supersingular.

Proof of second piece. Say $\varphi : E \to E/C = E'$ is the isogeny. Then $\psi : E' \to E$ can be given as the dual isogeny.

We know $\psi \circ \varphi = [p]_E$ and $\varphi \circ \psi = [p]_{E'}$. Then if we look at the reduced isogenies

$$\begin{aligned} \widetilde{\varphi} \circ \widetilde{\psi} \circ \widetilde{\varphi} &= \widetilde{\varphi} \circ [p]_{\widetilde{E}'} \\ &= [p]_{\widetilde{E}} \circ \widetilde{\varphi}. \end{aligned}$$

This in fact tells us that

$$\deg_{\text{sep}}[p]_{\widetilde{E}} = \deg_{\text{sep}}[p]_{\widetilde{E}'}.$$

Reduction for more general Curves. Specifically, we want modular curves.

Definition VII.3.3

Suppose C is a nonsingular affine curve over $\mathbb{Q}$ cut out by equations $\varphi_1, \ldots, \varphi_m \in \mathbb{Z}_{(p)}[X_1, \ldots, X_n]$. We'll say C has good reduction at p provided that

(1) $I = \langle \varphi_1, \ldots, \varphi_m \rangle \subseteq \mathbb{Z}_{(p)}[X_1, \ldots, X_N]$ is prime

(2) $\widetilde{I} = \langle \widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_m \rangle \subseteq \mathbb{F}_p[X_1, \ldots, X_N]$ defines a nonsingular affine algebraic curve.

What is Condition 1 doing? Lets see what it rules out

Non-Example VII.3.7

Let $I = \langle p(py-1), (y-x^2)(py-1) \rangle$. Inside $\mathbb{Q}$ we have $I_{\mathbb{Q}} \subseteq \mathbb{Q}[x, y]$ just defines the curve $y = 1/p$. However this is not prime in $\mathbb{Z}_{(p)}[x, y]$ since we cannot scale by $1/p$.

The reduction is $\widetilde{I} \subseteq \mathbb{F}_p[x, y]$ is $y = x^2$.

For elliptic curves Condition 1 is automatic, as Weierstrass equations are very simple.

For projective curves we'll homogenize the affine case.

Definition VII.3.4

Suppose we have some $I_{(0)} \subseteq \mathbb{Z}_{(p)}[X_1, \ldots, X_n]$ prime with homogenization $I \subseteq \mathbb{Z}_{(p)}[X_0, \ldots, X_n]$.

Say this gives a projective curve C_{hom}. We say C_{hom} has good reduction at p if for all i either C_i (unhomogenizing at x_i) has good reduction at p or $\widetilde{I}_{(i)} = \mathbb{F}_p[X_1, \ldots, \widehat{X}_i, \ldots, X_N]$ (empty reduction).

We can let $\widetilde{C}_{\text{hom}}$ be the reduced curve given by $(\widetilde{I}_{(0)})_{\text{hom}}$.

Note: Some commutative algebra tells us that if $I_{(0)}$ is prime, I is prime, and this implies $I_{(i)}$ is prime.

Recalling that $\mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$ gives us a map on points for reducing projective curves.

Theorem VII.3.17

If C is nonsingular, projective, of good reduction at p, then the reduction map $C \to \widetilde{C}$ is surjective.

Fact we won't state: You can also reduce morphisms! The idea is to reduce the algebraic equations defining the maps, which gives you something rational, and then extend by nonsingularity.

One would really like to have a commutative diagram

$$\begin{tikzcd} C \arrow[r, "h"] \arrow[d] & C' \arrow[d] \\ \widetilde{C} \arrow[r, "\widetilde{h}"'] & \widetilde{C}' \end{tikzcd}$$

But in fact this only holds if $g(C') > 0$.

Theorem VII.3.18

If $g(C') > 0$ and $h : C \to C'$ over $\mathbb{Q}$ where these have good reduction then

$$\begin{tikzcd} C \arrow[r, "h"] \arrow[d] & C' \arrow[d] \\ \widetilde{C} \arrow[r, dashed, "\widetilde{h}"'] & \widetilde{C}' \end{tikzcd} \quad \text{and this } \widetilde{h} \text{ is unique.}$$

Something that could go wrong when reducing maps. Look at

$$h : \mathbb{P}^1 \to \mathbb{P}^1$$
$$[x : y] \mapsto [px : y].$$

Then $\widetilde{h}$ doesn't quite make sense, as it maps $[1 : 0]$ to $[0 : 0]$ (which is not in $\mathbb{P}^1_p$

Corollary VII.3.19

Suppose C, C' are nonsingular and projective with good reduction at p and $g(C') > 0$.

(a) If h is surjective, then $\widetilde{h}$ is surjective.
(b) If $k : C' \to C''$ and $g(C'') > 0$ then $\widetilde{k \circ h} = \widetilde{k} \circ \widetilde{h}$.
(c) h is an isomorphism implies $\widetilde{h}$ is an isomorphism.

Theorem VII.3.20

The map $\mathrm{Div}^0(C) \to \mathrm{Div}^0(\widetilde{C})$ where $p \mapsto \widetilde{p}$ is well-defined, and furthermore

$$\mathrm{Div}^\ell(C) \to \mathrm{Div}^\ell(\widetilde{(C)}).$$

However, it is not necessasarily true that the reduction of the divisor of a function is the divisor of the reduction of the function.

This then induces a map

$$\mathrm{Pic}^0(C) \to \mathrm{Pic}^0(\widetilde{C}).$$

Theorem VII.3.21

Theorem VII.3.18 is true for $E/\overline{\mathbb{Q}}$, h an isogeny.

Fix ideals $p \subseteq \mathbb{Z}$ and $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$, and $p \nmid N$.

Recall VII.3.8

$E/\overline{Q}$ has good reduction if and only if $j(E) \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$.

Definition VII.3.5

Consider the set

$$S_1(N,)'_{\text{good}} = \{(E, Q) \in S_1(N) \mid E \text{ has good reduction at } \text{ and } j(\widetilde{E}) \neq 0, 1728\}.$$

We also define

$$\widetilde{S}_1(N) = \{(E, Q) \mid E/\overline{\mathbb{F}}_p, Q \in E[N]\}$$

We also define

$$\widetilde{S}_1(N)' = \{(E, Q) \in \widetilde{S}_1(N) \mid j(E) \neq 0, 1728\}.$$

We also have a surjection $S_1(N)'_{\text{good}} \twoheadrightarrow \widetilde{S}_1(N)'$.

Consider the modular curve $X_1(N)$. We had a universal elliptic curve E_j living over this. The function field was x-coordinates of torsion on this curve. We can also consider $\widetilde{E}_j$,

$$\widetilde{E}_j : y^2 + xy = x^3 - \left(\frac{36}{j-1728}\right)x - \frac{1}{j-1728}.$$

Fix $Q \in \widetilde{E}_j[N]$ of order N. Let $\varphi_{1,N} \in \mathbb{F}_p(j)[X]$ be the minimal polynomial of $x(Q)$.

We can then define

Definition VII.3.6

$\mathbb{K}_1^p(N) = \mathbb{F}_p(j)[X]/\varphi_{1,N}(X)$.

This is our candidate function field. It is easy to show this is a function field. Thus there exists a nonsingular projective curve corresponding to this, and we must ask if that is the same as $\widetilde{X}_1(N)$ (which as of now we don't even know if that has good reduction!).

Theorem VII.3.22 (Igusa)

For the modular curve $X_1(N)$,

- $X_1(N)$ has good reduction at p.
- $\mathbb{F}_p(\widetilde{X_1(N)}) \xrightarrow{\sim} \mathbb{K}_1^p(N)$.
- There is a commutative diagram

$$\begin{tikzcd} S_1(N)'_{\text{good}} \arrow[r, "\psi"] \arrow[d] & X_1(N) \arrow[d] \\ \widetilde{S}_1(N)' \arrow[r, "\widetilde{\psi}"] & \widetilde{X_1(N)} \end{tikzcd}$$

Corollary VII.3.23

There is a commutative diagram

$$\begin{tikzcd} \operatorname{Div}^0(S_1(N)'_{\text{good}}) \arrow[r] \arrow[d] & \operatorname{Pic}^0(X_1(N)) \arrow[d] \\ \operatorname{Div}^0(\widetilde{S}_1(N)') \arrow[r] & \operatorname{Pic}^0(\widetilde{X_1(N)}) \end{tikzcd}$$

VII.4. **Eichler-Shimura Relation**

Idea: Compute $\widetilde{T}_p : \operatorname{Pic}^0(\widetilde{X}_1(N)) \to \operatorname{Pic}^0(\widetilde{X}_1(N))$.

Warmup: Consider the diamond operator $\langle d\rangle$, We have $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. The quotient is $(\mathbb{Z}/N\mathbb{Z})^\times$ and we pick a d here. We pick a matrix

$$\begin{bmatrix} a & 0 \\ c & \delta \end{bmatrix} \in \Gamma_0(N)$$

reducing to d. We can think of conjugation by this matrix acting on $\Gamma_0(N)$, and we can think of it as a double coset operator as well. We then get a map

$$\langle d\rangle : X_1(N) \to X_1(N)$$
$$\langle d\rangle_* : \operatorname{Pic}^0(X_1(N)) \to \operatorname{Pic}^0(X_1(N)).$$

Since this comes from an actual honest to god map of curves, we're actually fine.

General double coset operators. Let Γ_1, Γ_2 be congruence subgroups and

$$\Gamma_3 = \Gamma_1 \cap g^{-1}\Gamma_2 g$$
$$\Gamma_3' = g\Gamma_1 g^{-1} \cap \Gamma_2.$$

There are then maps

$$\begin{tikzcd} X_3 \arrow[r, leftrightarrow] \arrow[d] & X_3' \arrow[d] \\ X_1 & X_2. \end{tikzcd}$$

In the T_p case, $\Gamma_1, \Gamma_2 = \Gamma_1(N)$. Then

$$\Gamma_{1,0}(N,p) = \Gamma_1(N) \cap \Gamma_0(Np).$$

Then one gets maps

$$\begin{tikzcd} & X_{1,0}(N,p) \arrow[dl] \arrow[dr] & \\ X_1(N) & & X_1(N) \end{tikzcd}$$

The problem is $X_{1,0}(N,p)$ does not have good reduction at p. The reduction somehow looks like 2 copies of $\widetilde{X_1(N)}$ glued at the supersingular points.

The books says in fact we can sort of reduce this diagram, but we have to wrestle with $X_{1,0}(N,p)$ having singular reduction.

Assuming $\widetilde{T}_p$ is well-defined, we compute it.

> **Recall VII.4.1**
>
> Eigenvalues of T_p are coefficients of forms. We would like to do point counts for the reduced modular curves.
>
> We have $a_p(f)$ is the coefficent in the modular curve, and we'd like to relate that to $a_p(\widetilde{E})$ (a point count of $\overline{\mathbb{F}_p}^2$ points on $\widetilde{E}$).

We should also recall what the Hecke operator does on the moduli problem

> **Recall VII.4.2**
>
> We have that
>
> $$T_p : \mathrm{Div}^0(S_1(N)) \to \mathrm{Div}^0(S_1(N))$$
> $$T_p[E,Q] = \sum_C [E/C, Q + C],$$
>
> where the sum is over all $C \subseteq E$ of order p with $C \cap \langle Q \rangle = 0$. In our case this second condition is vacuous since $p \nmid N$, and Q has order N.
>
> Also recall that if E has ordinary reduction at p, then so does E/C. Thus we can split this computation into an ordinary and supersingular computation.

Let $E/\overline{\mathbb{Q}}$ have ordinary reduction at , and let

$$C_0 = \ker(E[p] \twoheadrightarrow \widetilde{E}[p]).$$

And of course $|C_0| = p$.

Lemma VII.4.1

We need to know what the reduction looks like, well

$$[\widetilde{E/C}, \widetilde{Q+C}] = \begin{cases} [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] & \text{if } C = C_0 \\ (\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}) & \text{if } C \neq C_0 \end{cases}.$$

Proof when $C = C_0$. Let $E' = E/C, Q' = Q + C = \varphi(Q)$, where $\varphi : E \to E'$. Let $\psi : E' \to E$ be the dual isogeny.

Consider the diagram

$$\begin{tikzcd} E'[p] \arrow[r, "\psi"] \arrow[d] & E[p] \arrow[d] \\ \widetilde{E'[p]} \arrow[r, "\widetilde{\psi}"'] & \widetilde{E}[p] \end{tikzcd}$$

We know this commutes, so then we have the following steps

- $\psi(E'[p]) \subseteq E[p]$ as order p.
- $\psi(E'[p]) \subseteq C$, and this implies $\psi(E'[p]) = C$.
- $\widetilde{E'[p]} \subseteq \ker \widetilde{\psi}$.
- $\ker(\widetilde{\psi}) = \widetilde{E'[p]}$

Upshot: compute the degrees of everything in sight.

$$\deg[p]_{\widetilde{E'}} = p^2 \qquad \deg(\widetilde{\varphi}) = p \qquad \deg(\widetilde{\psi}) = p.$$

Hence,

$$\begin{aligned} \deg_{\text{sep}}[p]_{\widetilde{E'}} &= p & \deg_{\text{insep}}[p]_{\widetilde{E'}} &= p \\ \deg_{\text{sep}} \widetilde{\psi} &= p & \deg_{\text{insep}} \widetilde{\psi} &= 1 \\ \deg_{\text{sep}} \widetilde{\varphi} &= 1 & \deg_{\text{insep}} \widetilde{\varphi} &= p. \end{aligned}$$

This implies that $\widetilde{\varphi} = \iota \circ \sigma_p$, where ι is an isomorphims and σ_p is the Frobenius map. With $\iota : \widetilde{E}^{\sigma_p} \to \widetilde{E}$.

This is a field extensions sort of argument (splitting into separable/inseparable). Then ι induces an equivalence

$$\iota : [\widetilde{E'}, \widetilde{Q'}] \leftrightarrow [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}].$$

The other computation is similar.

Where we we?

Recall VII.4.3

We had an elliptic curve $E/\overline{\mathbb{Q}}$ with ordinary reduction at , $Q \in E$ a point of order N, and $C_0 = \ker(E[p] \to \widetilde{E}[p])$, with $p \nmid N$.

Lemma VII.4.2

If $C \subseteq E$, $|E| = p$, then

$$[\widetilde{E/C}, \widetilde{Q+C}] = \begin{cases} [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] & \text{if } C = C_0 \\ (\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}) & \text{if } C \neq C_0 \end{cases}.$$

where σ_p is the Frobenius map.

We did the proof when $C = C_0$ last time! The proof for $C \neq C_0$ is similar.

Fact: $E[p]$ has $p+1$ subgroups of order p (this is $(\mathbb{Z}/p\mathbb{Z})^2$, which we can view as a vector space). We had the reduction of the diamond operator, which when $(d, N) = 1$ had the form

$$\begin{aligned} \langle\widetilde{d}\rangle : \widetilde{S_1(N)} &\to \widetilde{S_1(N)} \\ [E, Q] &\mapsto [E, [d]Q]. \end{aligned}$$

We should have something like

$$\begin{aligned} T_p[E, Q] &= \sum_C [E/C, Q + C] \\ \widetilde{T}_p[\widetilde{E}, \widetilde{Q}] &= \sum_C [\widetilde{E/C}, \widetilde{Q+C}] \\ &= (\sigma_p + p\langle\widetilde{p}\rangle\sigma_p^{-1})[\widetilde{E}, \widetilde{Q}]. \end{aligned}$$

This is all in the case of ordinary reduction. In the supersingular case, we can take the same setup as before. This ends up showing that

$$[\widetilde{E/C}, \widetilde{Q+C}] = [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] = [\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}].$$

This implies the same formula is true, but there's some collapsing so it is less interesting in some sense.

In general we have that

$$\begin{tikzcd} S_1(N)'_{\text{good}} \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}(S_1(N)'_{\text{good}}) \arrow[d] \\ \widetilde{S_1(N)}' \arrow[r, "\sigma_p + p\langle\widetilde{p}\rangle\sigma_p^{-1}"'] & \mathrm{Div}(\widetilde{S_1(N)}'). \end{tikzcd}$$

We define a map $\sigma = \sigma_{p_*} + \langle\widetilde{\sigma}\rangle\sigma_p^*$ from $\mathrm{Pic}^0(\widetilde{X}_1)$ to itself.

It turns out $\mathrm{Div}^0(\widetilde{S}_1')$ to this picard group is surjective.

Theorem VII.4.3 (Eichler-Shimura)

We have a commutative diagram

$$\begin{tikzcd} \mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\ \mathrm{Pic}^0(\widetilde{X_1(N)}) \arrow[r, "\sigma_{p*} + \langle\widetilde{p}\rangle_* \sigma_p^*"'] & \mathrm{Pic}^0(\widetilde{X_1(N)}) \end{tikzcd}$$

There is also an $X_0(N)$ version.

$$\begin{array}{ccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X_0(N)}) & \xrightarrow[\sigma_{p_\star}+\sigma_p^*]{} & \mathrm{Pic}^0(\widetilde{X_0(N)}) \end{array}$$

Definition VII.4.1

We let $a_p(E) = p + 1 - \left|\widetilde{E}(\mathbb{F}_p)\right|$ when E has good reduction at p.

There is in fact a Lefschetz formula

$$\widetilde{E}(\mathbb{F}_p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}(H^i_{\text{et}}(E, \mathbb{Q}_p)).$$

This gives a good reason to care about $a_p(E)$. In H^0 we'll have a contribution of 1, and in H^2 we'll have a contribution of p. In H^1 we'll have what's called a Tate Module, and we're computing the trace of frobenius on this Galois representation.

Theorem VII.4.4

Supposing E has good reduction, $a_p(E) = 0$ if and only if E has supersingular reduction at p.

Supposing E has bad reduction, we define,

$$a_p(E) = \begin{cases} 1 & \text{if } E \text{ split} \\ -1 & \text{if } E \text{ nonsplit} \\ 0 & \text{if } E \text{ additive} \end{cases},$$

and this will fit into the general theory.

Proposition VII.4.5

$E/\mathbb{Q}$ has good reduction at p, then

$$[a_p(E)] = \sigma_{p_*}\sigma_p^*$$

on $\mathrm{Pic}^0(E)$.

We know $\widetilde{E}[\mathbb{F}_p] = \ker(\sigma_p - \mathrm{Id})$, $h_* \circ h^* = \deg(h)$, and so

$$\left|\widetilde{E}[\mathbb{F}_p]\right| = \deg(\sigma_p - 1) = (\sigma_p - 1)_*(\sigma_p - 1)^*.$$

If we FOIL this we get

$$\sigma_{p_*}\sigma_p^* + 1_*1^* - (\sigma_{p_*} + \sigma_p^*).$$

The modularity theorem can now be restated as

Theorem VII.4.6 (Modularity)

If $E/\mathbb{Q}$ is an elliptic curve and the conductor is N_E. Then there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$ for each prime p.

(Before: $X_0(N_E) \twoheadrightarrow E$).

Theorem VII.4.7

Let $E/\mathbb{Q}$ be a curve, with N_E a conductor, $\alpha : X_0(N) \twoheadrightarrow E$.

Then in fact there is an $f \in S_2(\Gamma_0(M_F))$ with $M_F \mid N$ so that $a_p(f) = a_p(E)$ for all $p \nmid N_E N$.

Proof. Recall that $S_2(\Gamma_0(N))$ has a basis $\bigcup_f \bigcup_{n|N} \bigcup_\sigma f^\sigma(n\tau)$ where f is a newform.

This told us we had an isogeny

$$\mathrm{Pic}^0(X_0(N)) \twoheadrightarrow \bigoplus_{f,n} A'_{f,\mathbb{C}},$$

and we can consider the dual isogeny, and then write down

$$\oplus_{f,n} A'_{f,\mathbb{C}} \xrightarrow{\prod_{f,n} a_p(f) - a_p(E)} \oplus_{f,n} A'_{f,\mathbb{C}}$$

$$\mathrm{Pic}^0(X_0(N), \mathscr{C}) \xrightarrow[T_p - a_p(E)]{} \mathrm{Pic}^0(X_0(N), \mathbb{C}) \xrightarrow{\alpha_*} \mathrm{Pic}^0(E_\mathbb{C}).$$

We now have some facts

- If $a_p(f) \neq a_p(E)$ then the top map $\oplus_n A'_{f,\mathbb{C}}$ (should be believable, it's nonzero)
- The square commutes.
- The composition of bottom maps is 0.

If for some p, $a_p(f) \neq a_p(E)$, then the image of $\oplus_n (A'_f)_\mathbb{C}$ lies in $\ker \alpha_*$. Now suppose for each f, there is a p such that $a_p(f) \neq a_p(E)$. This implies that the image of $\oplus_{f,n} A'_{f,\mathbb{C}} \subseteq \ker(\alpha_*)$.

But this is bad because the map above $\oplus_{f,n} A'_{f,\mathbb{C}} \to \mathrm{Pic}^0(X_0(N), \mathbb{C})$ is surjective. This would imply $\mathrm{Pic}^0(E_\mathbb{C})$ is trivial!!!

But this isn't true, so there is a p with $a_p(f) \neq a_p(E)$.

Remark VII.4.1

If f is as in Theorem VII.4.7 then $f/\mathbb{Q}$. Why? Well $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$a_p(f^\sigma) = a_p(f)^\sigma$$

for almost all primes $a_p(f) = a_p(E) =\in \mathbb{Z}$ so $a_p(f) = a_p(f^\sigma)$. Strong Multiplicity one would then imply that $f = f^\sigma$

How do we relate the versions of modularity. Well we look for a map

$$X_\mathbb{Q}\text{-Mod} \to a_p - \text{-Mod}.$$

Well recall we had $\dim A'_f = [K_f : \mathbb{Q}]$ but since $f/\mathbb{Q}$ in the situation above, A'_f is an elliptic curve (abelian variety of dimension one).

Have: $X_0(N) \to \mathrm{Pic}^0(X_0(N)) \to A'_f$. Then we can apply Theorem VII.4.7 to this setup. Then there's a g with $a_p(g) = a_p(A'_f)$ (except at divisions), and you end up with $g = f$ in the proof. Why? Well the idea is the $a_p(f) - a_p(E)$ portion above, and applying strong multiplicity one.

Thus $a_p(f) = a_p(A'_f)$ for almost all p, when $f/\mathbb{Q}$.

Theorem VII.4.8 (Carayol)

$a_p(f) = a_p(A'_f)$ for all p.

We then have $A'_f \twoheadrightarrow E$. Then it turns out $A'_f \cong E$ and $a_p(f) = a_p(A'_f) = a_p(E)$ for all p.

VII.5. Some L-function stuff

Recall for a newform f we defined $L(s,f) := \sum_{n=1}^{\infty} a_n(f)n^{-s}$. We were able to show that

$$L(s,f) = \prod_p \left(1 - a_p(f)p^{-s} + 1_N(p)p^{1-2s}\right)^{-1}$$

where $1_N(p)$ detects if $p \mid N$ where f has level N. We can also define

$$t_{p^e} = p^e + 1 - \left|\widetilde{E}(\mathbb{F}_{p^e})\right|$$

Then we can define a local zeta function

$$Z_p(X,E) = \prod_{e=1}^{\infty} \exp\left(\frac{t_{p^e}(E)}{e}x^e\right).$$

One can show

$$Z_p(p^{-s},E) = (1 - a_p(E)p^{-s} + 1_E(p)p^{1-2s})^{-1},$$

where 1_E is 1 if good reduction and 0 if bad reduction. This clearly depends on reduction type, and,

$$Z_p(p^{-s},E) = \begin{cases} (1 - a_p(E)p^{-s} + p^{1-2s})^{-1} & \text{if good} \\ (1-p^{-s})^{-1} & \text{if split} \\ (1+p^{-s})^{-1} & \text{if non-split} \\ 1 & \text{if additive} \end{cases}.$$

Define

$$L(s,E) = \prod_p (1 - a_p(E)p^{-s} + 1_E(p)p^{1-2s}) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}.$$

Formally defined,$a_1(E), A_p(E) = p + 1 - |E(\mathbb{F}_p)|$. Furthermore

$$a_{p^e}(f) = a_p(E)a_{p^{e-1}}(E) - 1_E(p)pa_{p^{e-2}}(E).$$

Furthermore if $(m,n) = 1$ then $a_{mn}(E) = a_m(E)a_n(E)$.

Theorem VII.5.1 (Modularity)

$L(s,f) = L(s,E)$. As a consequence $L(s,E)$ has a functional equation and an analytic continuation.

Conjecture VII.5.2 (Birch-Swinnerton-Dyer)

$\operatorname{ord}_{s=1} L(s,E) = \operatorname{rank}(E/\mathbb{Q}) = r$ which is determined by $E(\mathbb{Q}) = \mathbb{Z}^r \oplus T$.

Then $L(s,E)$ converges when $\operatorname{Re}(s) > 2$. The functional equation determines $\operatorname{Re}(s) < 0$.

Definition VII.5.1

Let $K/\mathbb{Q}$ be an imaginary quadratic extension. An order $\mathcal{O} \subseteq \mathcal{O}_K$, $\operatorname{rank}_{\mathbb{Z}}(\mathcal{O}) = [K : \mathbb{Q}] = 2$.

In this simple case the orders are $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ where $n \in \mathbb{Z}_{\geq 1}$.

Definition VII.5.2 (Heegner Point)

A Heegner point in $X_0(N)$ relative to K is a pair (E, C) such that $E, E/C$ have complex multiplication by the same order $\mathcal{O}$.

Then these will look like

$$\begin{aligned} x_n &:= (E = \mathbb{C}/\mathcal{O}_n, E' = E/C = \mathbb{C}/\mathcal{N}_n^{-1}) \\ &\mathcal{N} \subseteq \mathcal{O}_K, \mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n. \end{aligned}$$

with $\mathcal{O}_K/N \cong \mathbb{Z}/N\mathbb{Z}$, where inverse is taken with respect to the notion of fractional ideal.

The Heegner Hypothesis is that each $p \mid N$ splits in K, which implies there exist Heegner points in $X_0(N)$ for all $\mathcal{O}_N$. It turns out $x_n \in X_0(N)(H_n)$ where H_n is a ring class field of $\mathcal{O}_n$.

This is a generalization of the Hilbertclass field, with Galois group $(\mathcal{O}_n/n\mathcal{O}_K)^\times/(\mathbb{Z}/N\mathbb{Z})^\times$.

Consider $E/\mathbb{Q}$ by modularity $X_0(N) \xrightarrow{\alpha} E$. Then we can consider the image this Heegner point $x_n \mapsto y_n \in E(H_n)$. We can then consider

$$\begin{aligned} \mathrm{tr}_n : E(H_{np}) &\to E(H_n) \\ z &\mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z). \end{aligned}$$

Theorem VII.5.3

$\mathrm{tr}_n(y_{np}) = a_p(E) y_n$.

Proof. We'll use Eichler-Shimura. We'll need the version where the composition

$$\mathrm{Pic}^0(X_0(N)) \xrightarrow{T_p - a_p(E)} \mathrm{Pic}^0(X_0(N)) \xrightarrow{\alpha} E$$

is zero. We might as well work in the picard group then! So we can look at

$$\begin{aligned} \mathrm{tr}_n(y_{np}) &= \mathrm{tr}(\alpha(x_{np})) = \alpha(\mathrm{tr}(x_{np})) \\ &= \alpha(T_p(x_n) = a_p(E)\alpha(x_n) = a_p(E) y_n. \end{aligned}$$

Exercise VII.5.1

Why is $\mathrm{tr}(x_{np}) = T_p(x_n)$? Idea: look at what we did for Hecke operators and Galois actions in the $X_1(N)$ moduli problem, and adapt a similar formula for $X_0(N)$.

Also probably understand H_n better than I do (can't wait to learn class field theory one day).

Define

$$y_K := \mathrm{tr}_{H_1/K}(y_1) \in E(K).$$

We need to say something about its height.

Definition VII.5.3

If $p \in E(K)$, we define the naive height as

$$h(p) \coloneqq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v, \mathbb{Q}_v] \cdot \log \max(|x|_v, |y|_v, |z|_v),$$

where M_K is all the places (absolute values in K)

We can also define the Neron-Tate Height

$$\widehat{h}_n(p) = \lim_{n\to\infty} \frac{h([2^n]p)}{4^n}.$$

This allows us to define a height pairing

$$\begin{aligned} \langle , \rangle : E(K) \times E(K) &\to \mathbb{R} \\ \langle P, Q \rangle &\coloneqq \frac{1}{2}\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q). \end{aligned}$$

It turns out that $\langle P, P \rangle = 0$ if and only if P is torsion.

Theorem VII.5.4 (Gross-Zagier)

If $E/\mathbb{Q}$ is an elliptic curve, K is an imaginary quadratic field satisfying the Heegner Hypothesis. Then

$$L'(1, E_K) = c_{E,K} \cdot \langle y_K, y_K \rangle,$$

for some special number $c_{E,K}$ which is not terrible to write down.

Now write the analytic rank as $\mathrm{rk}_{an} = \mathrm{ord}_{s=1} L(s, E)$. The algebraic rank as $\mathrm{rk}_{alg} = \mathrm{rk}(E)$.

Corollary VII.5.5

$\mathrm{rk}_{an}(E_K) = 1$ then $\mathrm{rk}_{alg}(E_K) \geq 1$.

Theorem VII.5.6 (Kolyvagin)

If $\mathrm{ord}(y_k) = \infty$, then $\mathrm{rk}_{alg}(E_K) = 1$.

This actually tells us that if $\mathrm{rk}_{an}(E_K) = 1$ implies $\mathrm{rk}_{alg}(E_K) = 1$.

VIII. Galois Representations

We skip 9.1, and check there fore definitions

Definition VIII.0.1

Let ℓ be a prime. The ring of ℓ-adic integers is

$$\mathbb{Z}_\ell \coloneqq \lim_{\leftarrow} \mathbb{Z}/\ell^n\mathbb{Z}$$

along $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$.

Explicitly, $a \in \mathbb{Z}_\ell$ si a sequence $a = (a_1, a_2, \ldots)$ with $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $a_{n+1} \equiv a_n \pmod{\ell}^n$.

Note $\mathbb{Z}_\ell$ is an integral domain and the natural map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}_\ell \\ a &\mapsto (a + \ell\mathbb{Z}, a + \ell^2\mathbb{Z}, \ldots) \end{aligned}$$

is injective. This inclusion induces

$$\mathbb{Z}/\ell^n\mathbb{Z} \cong \mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$$

for every n. Then $\mathbb{Z}_\ell$ is profinite because $\mathbb{Z}/\ell^n\mathbb{Z}$ is finite for all n.

The group of units $\mathbb{Z}_\ell^\times$ is

$$\begin{aligned}\mathbb{Z}_\ell^\times &= \{(a_1, a_2, \ldots) \mid a_i \in (\mathbb{Z}/\ell^i\mathbb{Z})^\times\} \\ &= (a_1, a_2, \ldots) \mid a_1 \not\equiv 0\}.\end{aligned}$$

Also $\mathbb{Z}_\ell$ has a unique maximal ideal $\ell\mathbb{Z}_\ell$. Furthermore, it comes equipped with a topology with basis given by the sets

$$U_x(n) \coloneqq x + \ell^n\mathbb{Z}_\ell,$$

where $n \in \mathbb{Z}^+$.

Definition VIII.0.2

The field $\mathbb{Q}_\ell$ is the fraction field of $\mathbb{Z}_\ell$.

$\mathbb{Q}_\ell$ has a topology given in the same way. The basis is

$$U_x(n) = x + \ell^n\mathbb{Z}_\ell$$

for $x \in \mathbb{Q}_\ell, n \in \mathbb{Z}^+$. For any $d > 0$, $\mathbb{Q}_\ell^d$ is a topological $\mathbb{Q}_\ell$-vector space with the product topology. The group $\mathrm{GL}_d(\mathbb{Q}_\ell)$ inherits the subspace topology from $\mathbb{Q}_\ell^{d^2}$. Under this topology, matrix multiplication and inversion are continuous (i.e. $\mathrm{GL}_d(\mathbb{Q}_\ell)$ is a topological group).

Now let K be a number field ($K \subseteq \overline{\mathbb{Q}}, [K : \mathbb{Q}] < \infty$) with ring of integers $\mathcal{O}_K$. If λ is a prime in $\mathcal{O}_K$ over ℓ, then we can play the same game:

$$\mathcal{O}_{K,\lambda} = \lim_{\leftarrow_n} \mathcal{O}_K/\lambda^n\mathcal{O}_K,$$

and similarly define $K_\lambda = \mathrm{Frac}(\mathcal{O}_{k,\lambda})$. Then we have

$$\mathbb{Q}_\ell \hookrightarrow, \mathbb{Z}_\ell \hookrightarrow \mathcal{O}_{K,\lambda}, K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda \mid \ell} K_\lambda,$$

with the proof in the book.

Galois Representations:

- Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$.
- Define $G_{\mathbb{Q}} = \mathrm{Aut}(\overline{\mathbb{Q}})$.
- We want to study representations of $G_{\mathbb{Q}}$ on $\mathbb{Q}_\ell$-vector spaces.
- Recall that

$$\overline{\mathbb{Q}} = \bigcup_{\substack{K/\mathbb{Q} \\ [K:\mathbb{Q}]<\infty \\ K \text{ Galois}}} K.$$

Then for any $\sigma \in G_{\mathbb{Q}}$ and any $K/\mathbb{Q}$ Galois of finite degree, we have $\sigma\big|_K \in \mathrm{Gal}(K/\mathbb{Q})$. This defines a compatible system of surjections

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}),$$

compatible in the sense that if $K' \subseteq K$ we have a commutative diagram

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, two heads] \arrow[dr, two heads] & \mathrm{Gal}(K/\mathbb{Q}) \arrow[d, two heads] \\ & \mathrm{Gal}(K'/\mathbb{Q}) \end{tikzcd}$$

So really we have that

$$G_{\mathbb{Q}} = \varprojlim_{\substack{K/\mathbb{Q} \\ \text{fin. Galois}}} \mathrm{Gal}(K/\mathbb{Q}).$$

This has a natural topology

Definition VIII.0.3

The Krull topology on $G_{\mathbb{Q}}$ has basis sets

$$U_\sigma(K) = \{\sigma\tau \mid \tau\big|_K = \mathrm{Id}_K\}.$$

Let's discuss some important elements of $G_{\mathbb{Q}}$. Fix a prime p, $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p.

Definition VIII.0.4

The decomposition group of $\mathfrak{p}$ is

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \mid \mathfrak{p}^\sigma = \sigma\}.$$

We then have a surjective map $D_{\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ given by

$$\sigma \mapsto (x + \mathfrak{p} \mapsto x^\sigma + \mathfrak{p}).$$

Definition VIII.0.5

An absolute Frobenius over p is any preimage $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ of the Frobenius map $\sigma_p \in G_{\mathbb{F}_p}$, where $\sigma_p(x) = x^p$.

This is well-defined up to $I_{\mathfrak{p}} := \ker(D_{\mathfrak{p}} \to G_{\mathbb{F}_p})$, which we call the inertia group of $\mathfrak{p}$.

Explicitly,

$$I_{\mathfrak{p}} := \{\sigma \in D_{\mathfrak{p}} \mid x^\sigma \equiv x \pmod{\mathfrak{p}},\ \text{for all } x \in \overline{\mathbb{Z}}\}.$$

Theorem VIII.0.1

Fix a finite set of primes $S \subseteq \mathbb{Z}$. For each prime $\mathfrak{p}$ lying over $p \notin S$, choose an absolute Frobenius $\mathrm{Frob}_{\mathfrak{p}}$. Then the set

$$\{\mathrm{Frob}_{\mathfrak{p}} \mid p \notin S\}$$

is dense for the Krull topology.

Proof. We use Tchebotarov Density Theorem (stated below) to prove this theorem.

take $U_\sigma(K)$ for some $\sigma \in G_{\mathbb{Q}}$ and K some number field. We want to show $\mathrm{Frob}_{\mathfrak{p}} \in U_\sigma(K)$.

Consider $\sigma\big|_L \in \mathrm{Gal}(K/\mathbb{Q})$. By Tchebotarov, σ is a Frobenius for some $\mathfrak{p}_K$. Lift $\mathfrak{p}_K$ to $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$. Then $\mathrm{Frob}_{\mathfrak{p}} \in U_\sigma(K)$.

Theorem VIII.0.2 (Tchebotarov Density Theorem 9.1.2 in [DS05])

Let K be a Galois number field. Then every element of $\mathrm{Gal}(K/\mathbb{Q})$ is a Frobenius for $\mathfrak{p}$ for infinitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

Here we mean $x^\sigma \equiv x \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_K$.

Definition VIII.0.6

Let $d > 0$. A d-dimensional Galois representation is a continuous homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(L)$$

for L a finite extension of $\mathbb{Q}_\ell$.

Remark VIII.0.1

$L = K_\lambda$ for some λ, K works. If ρ, ρ' are two Galois representations then we say $\rho \sim \rho'$ if there exists some $g \in \mathrm{GL}_d(L)$ so that

$$\rho'(\sigma) = g^{-1}\rho(\sigma)g$$

for all $\sigma \in G_{\mathbb{Q}}$. One can think of this as a commutative diagram.

Example VIII.0.1

Fix $n > 0$, let μ_{ℓ^n} be a primitive ℓ^n-th root of unity (say $e^{2\pi i/\ell^n}$). Then $\mathbb{Q}(\mu_{\ell^n})$ is a Galois number field of degree $\phi(\ell^n)$ over $\mathbb{Q}$, and we have a canonical isomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) &\xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^\times \\ (\mu_{\ell^n} \overset{\sigma}{\mapsto} \mu_{\ell^n}^a) &\mapsto a \pmod{\ell^n}. \end{aligned}$$

If we define

$$\mathbb{Q}(\mu_{\ell^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{\ell^n})$$

then

$$G_{\mathbb{Q},\ell} \coloneqq \mathrm{Aut}(\mathbb{Q}(\mu_{\ell^\infty})) \xrightarrow{s} \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times.$$

The inclusion $\mathbb{Q}(\mu_\ell^\infty) \subseteq \overline{\mathbb{Q}}$ induces $G_{\mathbb{Q}} \twoheadrightarrow G_{\mathbb{Q},\ell}$ by restriction.

Then we have a representaiton

$$G_{\mathbb{Q}} \twoheadrightarrow G_{\mathbb{Q},\ell} \xrightarrow{\sim} \mathbb{Z}_\ell^\times \hookrightarrow \mathbb{Q}_\ell^\times = \mathrm{GL}_1(\mathbb{Q}_\ell).$$

This is a Galois representation (check continuity). This is called the ℓ-adic cyclotomic character χ_ℓ.

Claim

χ_ℓ is continuous.

Proof. Since χ_ℓ is a group homomorphism, it suffices to show that $\chi_\ell^{-1}(U_1(n))$ is open (aka look at neighborhoods of identity). Explicitly we see that

$$\begin{aligned}\chi_\ell^{-1}(U_1(n)) &= \{\sigma \mid \chi_\ell(\sigma) \in 1 + \ell^n\mathbb{Z}_\ell\} \\ &= \{\sigma \in G_{\mathbb{Q}} \mid \sigma\big|_{\mathbb{Q}(\mu_{\ell^n})} = \mathrm{Id}\}.\end{aligned}$$

But this is simply $U_{\mathrm{Id}}(\mathbb{Q}(\mu_{\ell^n}))$ which is open.

Exercise VIII.0.2

Compute that $\chi_\ell(\mathrm{Frob}_{\mathfrak{p}}) = p$. In [DS05] This is 9.3.6.

We want to think more generally about $\rho(\mathrm{Frob}_{\mathfrak{p}})$

Problem: $\mathrm{Frob}_{\mathfrak{p}}$ is only well-defined up to inertia.

Definition VIII.0.7

Let ρ be a Galois representaton and p a prime. Then ρ is unramified at p if $I_{\mathfrak{p}} \subseteq \ker\rho$ for any $\rho \subseteq \overline{\mathbb{Z}}$ lying over p.

Example VIII.0.3

χ_ℓ is unramified at p since p is unramified in $\mathbb{Q}(\mu_{\ell^n})$, so $I_{\mathfrak{p}}$ acts trivially on $\mathbb{Q}(\mu_{\ell^n})$.

We can give an equivalent definition of Galois representation

Definition VIII.0.8

Let $d > 0$. A d-dimensional Galois representation is a d-dimensional topological vector space V over L, where $[L : \mathbb{Q}_\ell] < \infty$ that is also a $G_{\mathbb{Q}}$-module such that the map

$$\begin{aligned} V \times G_{\mathbb{Q}} &\to V \\ (v, \sigma) &\mapsto v^\sigma \end{aligned}$$

is continuous.

Remark VIII.0.2

We say $V \sim V'$ if there exists a continuous $G_{\mathbb{Q}}$-module isomorphism $V \to V'$ of L-vector spaces.

We can realize χ_ℓ in this way. Define

$$C = \mathrm{Spec}(\mathbb{Q}[x, y]/(xy - 1))$$

This is a curve, and for any $\mathbb{Q}$-algebra R, the R-points of C are $C(R) = \{(a, b) \in R^2 \mid ab = 1\}$. This is isomorphic to $R^\times$.

Thus C has the structure of a "$\mathbb{Q}$-group scheme." For $n \in \mathbb{Z}^+$, define

$$C[\ell^n] = \{a \in C(\overline{\mathbb{Q}}) \mid a^{\ell^n} - 1 = 0\} \subseteq \overline{\mathbb{Q}}^\times.$$

Then we have an isomorphism

$$\begin{aligned} C[\ell^n] &\xrightarrow{\sim} \mathbb{Z}/\ell^n\mathbb{Z} \\ \mu_{\ell^n}^a &\mapsto a. \end{aligned}$$

Furthermore $\mathrm{Aut}(C[\ell^n]) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ in the natural way.

Definition VIII.0.9

The ℓ-adic Tate module of C is

$$T_\ell(C) = \varprojlim_n C[\ell^n].$$

We have an induced isomorphism ψ from $T_\ell(C)$ to $\mathbb{Z}_\ell$. $T_\ell(C)$ carries an action of $G_{\mathbb{Q},\ell}$ because $\mathrm{Aut}(C[\ell^n]) = \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$ as $C[\ell^n] = \mathbb{Q}(\mu_{\ell^n})$.

We can also define

$$V_\ell(C) \coloneqq T_\ell(C) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We get

$$V_\ell(C) \times G_{\mathbb{Q}} \to V_\ell(C)$$

which is compatible with our previous construction.

References

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.