UMich Math 679 Notes

Niven Achenjang

These are my course notes for "Math 679 (A Course on Mazur's Theorem)" at University of Michigan. Each lecture will get its own 'chapter'. These notes are live-texed and so likely contain many mistakes. Furthermore, they reflect my understanding (or lack thereof) of the material as the lecture was happening, so they are far from mathematically perfect.[1] Despite this, I hope they are not flawed enough to distract from the underlying mathematics. With all that taken care of, enjoy and happy mathing.

The instructor for this class is Andrew Snowden, and the course website can be found by clicking this link. The website has notes and recordings of all the lectures, so is probably the place to go if you want to learn this stuff. If you are trying to search up some particular fact, then I guess everything is in one place here instead of spread across multiple webpages.

Contents

[1] In particular, if things seem confused/false at any point, this is me being confused, not the speaker

List of Figures

List of Tables

1 Lecture 1: Overview

1.1 Motivating the Goal

Let's start with a problem.

Problem 1.1. *Let $f \in \mathbb{Q}[x,y]$. Describe the set of points $(x,y) \in \mathbb{Q}^2$ with $f(x,y) = 0$. Equivalently, say $C/\mathbb{Q}$ is an algebraic curve. Describe $C(\mathbb{Q})$.*

This is an old problem and much is known.

Example. Say $C/\mathbb{Q}$ is an algebraic curve.

- Say it has genus $g(C) = 0$.

  Then, $C(\mathbb{Q}) = \emptyset$ or $C \cong \mathbb{P}^1$ (in which case $C(\mathbb{Q})$ is infinite)

- $g(C) = 1$

  Then, $C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q})$ is a f.g. abelian group.

- $g(C) \geq 2$

  Then, $C(\mathbb{Q})$ is always finite (Faltings' theorem) △

These are fairly qualitative descriptions of the sizes of sets of rational points. You can ask more specifically, e.g. in the case of genus $g \geq 2$, exactly how many points there can be.

Question 1.1. *How many points can a genus 2 curve have?*

Conjecture 1.2. *There exists a number N so that $\#C(\mathbb{Q}) \leq N$ for any $C/\mathbb{Q}$ genus 2.*

There's been progress on this since 2013, see e.g. this survery. This conjecture is known if you let N depend on the rank of $\mathrm{Jac}(C)$

The current[2] record is a genus 2 curve with 642 points, apparently.
Say C is genus 1 and has a point. Then, $C(\mathbb{Q}) \cong C(\mathbb{Q})_{tors} \times \mathbb{Z}^r$ and its torsion subgroup is finite.

Question 1.3. *What are the possibilities for r and for $C(\mathbb{Q})_{tors}$?*

Not a ton known about the rank (e.g. is it absolutely bounded?), but everything is known about the torsion subgroup.

Theorem 1.4 (Mazur's theorem). *$C(\mathbb{Q})_{tors}$ is isomorphic to one of*

- $\mathbb{Z}/n\mathbb{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *for* $n = 2, 4, 6, 8$

This theorem is the goal of this course.

Note 1. It seems (at least in this first recording) that the video misses a few things. Hopefully this won't continue throughout...

[2] in 2013, when this class was taught

1.2 Brief overview of proof of Mazur

Hard part: show that $\nexists N$-torsion point where N is a prime > 7.

(Step 1) Criterion to exclude N-torsion.

For this, we'll need modular curves. Start with

$$Y_1(N) = \{\text{iso. classes of pairs } (E, P) \text{ with } E \text{ an elliptic curve over } \mathbb{C} \text{ and } P \text{ a point of order } N\}$$

This has a natural topology and complex structure making it a Riemann surface and it can in fact be realized as an algebraic curve over $\mathbb{Q}$. Note that $Y_1(N)(\mathbb{Q}) = \{(E, P) : E/\mathbb{Q} \text{ and } P \in E[N](\mathbb{Q})\}$, so this first step is showing $Y_1(N)(\mathbb{Q}) = \emptyset$ if $N > 7$ is prime. We can also define

$$Y_0(N) = \{(E, G) \mid E \text{ elliptic curve and } G \subset E \text{ cyc. subgroup of order } N\}.$$

This is missing two points $0, \infty$ (cusps) and so has compactification $X_0(N) = Y_0(N) + (\text{cusps})$. These two points can be given moduli interpretations as well.

Theorem 1.5. *Let $N > 7$ be prime. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a map $f : X_0(N) \to A$ so that*

(a) *A has good reduction away from N*

(b) *$f(0) \neq f(\infty)$*

(c) *$A(\mathbb{Q})$ has rank 0*

Then, no elliptic curve $/\ \mathbb{Q}$ has a rational point of order N.

Proof Sketch. Assume we have $E/\mathbb{Q}$ with a point $P \in E(\mathbb{Q})$ of order N, and let $x \in X_0(N)(\mathbb{Q})$ be the point corresponding to $(E, \langle P \rangle)$. This x will extend to a $\mathbb{Z}[1/N]$-point of $X_0(N)$. We're gonna reduce this mod 3. Note that you can't have a point of big order on an elliptic curve mod 3 by the **Hasse bound** $(4 + 2\sqrt{3} < 8)$

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q},$$

so we have to have bad reduction at 3, i.e. x must go to one of the two cusps mod 3 (in fact, you can show it reduces to ∞). Hence, $f(x) - f(\infty)$ reduces to 0 in $A(\mathbb{F}_3)$. This is a torsion point by hypothesis **(c)**. Injectivity of the reduction map on torsion then implies that $f(x) = f(\infty) \in A(\mathbb{Q})$. Now suppose p is a prime of bad reduction for E. Then $x \mod p \in \{0, \infty\}$. Since $f(x) = f(\infty)$ and $f(0) \neq f(\infty)$, we conclude $x \mod p = \infty$. This will imply that $E[N]|_{\mathbb{Q}_p} = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$, the local Galois representation is split. Algebraic number theory implies that this decomposition holds globally $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$. One gets a contradiction from this[3] ∎

Remark 1.6. One of the most important points about is that $\operatorname{rank} A(\mathbb{Q}) = 0$. This is what let us transfer some information mod 3 (which we got by free since 3 is small) to integral information (and so to other primes p). ∘

[3] smth smth quotient by μ_N and then induct to split an ℓ-adic Tate module smth smth

(Step 2) Criterion for rank 0

Theorem 1.7. *Let $A/\mathbb{Q}$ be an abelian variety, and fix distinct primes $N \neq p$ (with N odd). Suppose*

- ***(a)*** *A has good reduction away from N*
- ***(d)*** *A has completely toric reduction at N, i.e. if you look at the Néron model, the fiber at N is a torus*
- ***(e)*** *$A[p](\overline{\mathbb{Q}})$ has Jordan-Hölder constituents 1 and χ_p (the cyclotomic character)*

Then, $A(\mathbb{Q})$ has rank 0.

Proof Sketch. Let $\mathcal{A}/\mathbb{Z}$ be the Néron model of A. If you carefully study $\mathcal{A}[p^n]$, you can show it's built from 4 basic pieces. Explicit computations with these pieces let you bound $\#\,\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}[p^n])$ independent of n. Then, $A(\mathbb{Q}) \hookrightarrow \varprojlim \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}[p^n])$ with the RHS finite, and so you win. ■

(Step 3) Complete the proof.

Let $J_0(N) := \mathrm{Jac}(X_0(N))$. Note we have a map $X_0(N) \to J_0(N)$ which is universal for maps from $X_0(N)$ to abelian varieties. Hence, A will have to be a quotient of $J_0(N)$. There's a Hecke algebra $\mathbb{T}$ which acts on $J_0(N)$. We'll define an explicit ideal $I \subset \mathbb{T}$ and use that to build A.

1.3 Plan for the class

We'll switch steps 1/2 chronologically.

- Part I: elliptic curves and abelian varities
  - theory over field (kinda quickly)
  - group schemes
  - Néron models
  - Jacobians
  - Proof of Theorem 1.7.
- Moduli of elliptic curves
  - modular curves
  - modular forms
  - Hecke operators
  - Proof of Theorem 1.5
- Proof of Mazur's theorem
  - Eisenstein ideal
  - proof of criteria

1.4 Related Results

We won't get into these in this class, but it's good to be aware of them.

1.4.1 Analogs over other number fields

Mazur's theorem is about elliptic curves over $\mathbb{Q}$. What if we replace $\mathbb{Q}$ with K? Let

$$S(d) := \{\text{primes } p : \exists \text{ell. curve } E/K \text{ which has a point of order } N, \text{ for some } [K:\mathbb{Q}] = d\}.$$

Mazur computes $S(1) = \{2, 3, 5, 7\}$ (1977). In 1992, Kamienny computed $S(2) = \{2, 3, 5, 7, 11, 13\}$. These suggest that $\#S(d) < \infty$ always.

Theorem 1.8 (Merel, 1996)**.** *$S(d)$ is finite for all $d \geq 1$. Furthermore, if $N \in S(d)$, then $N \leq d^{3d^2}$.*

The bound above is probably not optimal.

In 2003, Parent computed $S(3) = S(2)$.

1.4.2 Serre's uniformity conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. Then, $E[N](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/N\mathbb{Z})^2$ and comes equipped with a Galois action, so we have some 2-dimensional mod N representation

$$\rho_{E,N} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Theorem 1.9 (Serre, 1972)**.** *Assume E not CM. Then, there exists some number $N_0(E)$ so that $\rho_{E,N}$ is surjective for all (prime?) $N > N_0(E)$.*

Question 1.10 (Serre)**.** *Does $N_0(E)$ actually depend on E? Does there exists N_0 so that $\rho_{E,N}$ is surjective for all non-CM curves E and all $N > N_0$?*

It's believed that $N_0 = 37$ works.

If $\rho_{E,N}$ is not surjective, it's image is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are

- Borel $\begin{pmatrix} * & * \\ & * \end{pmatrix}$
- Normalizer of the split Cartan $\begin{pmatrix} * & \\ & * \end{pmatrix} \cup \begin{pmatrix} & * \\ * & \end{pmatrix}$

  (note split Cartan here is just the diagonal matrices)
- Normalizer of the non-split Cartan
- Exceptional

To prove $\rho_{E,N}$ is surjective, want to show its image is not contained in (a conjugate of?) one of these maximal subgroups.

Theorem 1.11 (Serre)**.** $\mathrm{im}(\rho_{E,N}) \not\subset$ *exceptional group for $N > 7$.*

(E non-CM and N prime).

Mazur's torsion theorem shows that $\mathrm{im}(\rho_{E,N}) \not\subset \begin{pmatrix} 1 & * \\ & * \end{pmatrix}$ for $N > 7$. This is because a rational point of order N is exactly a Galois-fixed element of the representation on the N-torsion. This is smaller than the Borel, but Mazur actually handled that case the following year. His theorem on rational isogenies shows $\mathrm{im}(\rho_{E,N}) \not\subset \begin{pmatrix} * & * \\ & * \end{pmatrix}$ for $N > 27$. Bilu-Parent (2009) showed $\mathrm{im}(\rho_{E,n}) \not\subset N(\text{split Cartan})$ for $N \gg 0$. The non-split Cartan case is still open.

2 Lecture 2: Elliptic Curves

Fix a field k.

Assumption. All curves will be smooth and projective.

Not many proofs today (reference: Silverman's book)

2.1 Review of curves

Let C/k be a curve.

Definition 2.1. A **divisor** is a formal sum $\sum_{x \in C} n_x[x]$ with $n_x \in \mathbb{Z}$ equal to 0 for all but finitely many x. The **degree** of a point is $\deg(x)[\kappa(x) : k]$. The degree of D is $\deg(D) = \sum n_x \deg(x)$. $\diamond$

This notion of degree gives a homomorphism $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ with kernel $\mathrm{Div}^0(X) := \ker(\deg)$.

Definition 2.2. If $f \in k(C)^\times$ is a nonzero rational function, we define

$$\mathrm{div}(f) := \sum_{x \in C} \nu_x(f)[x]$$

and call it a **principal divisor**. The subgroup of principal divisors is denoted $\mathrm{PDiv}(X) \subset \mathrm{Div}(X)$. $\diamond$

Fact. $\deg(\mathrm{div}(f)) = 0$, i.e. # zeros of f = # poles of f.

Definition 2.3. The **divisor class group** of C is $\mathrm{Cl}(C) = \mathrm{Div}(C)/\mathrm{PDiv}(C)$. We also set $\mathrm{Cl}^0(C) := \ker \deg$. $\diamond$

Say $f : X \to Y$ is a map of curves. We can push forward and pullback divisors. Given $D = \sum n_x[x] \in \mathrm{Div}(X)$, we define

$$f_*(D) := \sum n_x[f(x)] \in \mathrm{Div}(Y).$$

Given $D = \sum_{y \in Y} n_y[y] \in \mathrm{Div}(Y)$, we define

$$f^*(D) = \sum_{y \in Y} \sum_{f(x)=y} e(x \mid y) n_y[x]$$

with $e(x \mid y)$ the ramification index of x over y. Note that

$$f_*(f^*D) = (\deg f)D.$$

Let's discuss Riemann-Roch. Let $D \in \mathrm{Div}(X)$. Define the k-vector space

$$\mathscr{L}(D) := \{f \in k(X) : \mathrm{div}(f) \geq -D\}.$$

Example. If $x \in X$, then $\mathscr{L}([x])$ is the space of functions which are holomorphic outside x, and have at worst a simple pole at x. △

Fact. $\mathscr{L}(D) = 0$ if $\deg D < 0$.

Notation 2.4. $\ell(D) := \dim \mathscr{L}(D)$.

Theorem 2.5 (**Riemann-Roch**)**.**

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1,$$

where g is the genus of X and K is the canonical divisor of X. Furthermore, $\deg(K) = 2g - 2$.

Corollary 2.6. *If* $\deg(D) > 2g - 2$*, then* $\ell(D) = \deg D - g + 1$.

If $g = 1$, above says $\deg(D) > 0 \implies \ell(D) = \deg(D)$.

Say $f : X \to Y$ is a map of curves. This induces an extension $k(Y) \hookrightarrow k(X)$ of function fields. We let $K/k(Y)$ be the maximal intermediate extension so that $K/K(Y)$ is separable and $k(X)/K$ is totally inseparable. This factors f as

$$X \longrightarrow X' \longrightarrow Y \quad (f : X \to Y)$$

with the first map totally inseparable and the second map separable. This let's you define the separable/inseparable degrees of f.

Example. Say $X : f(x, y) = 0$ for some $f \in k[x, y]$ with $\mathrm{char}\, k = p$. Let $f^{(p)} \in k[x, y]$ be the result of raising the coefficients of f to the pth power, and let $X^{(p)} : f^{(p)}(x, y) = 0$. Thus, we get a morphism $F_p : X \to X^{(p)}$ sending $(x, y) \mapsto (x^p, y^p)$ called the **Frobenius map**. This is totally inseparable.

If $q = p^r$, can consider $F_q = F_{p^r} : X \to X^{(q)}$. △

These are the only inseparable maps. Any map $f : X \to Y$ factors as

$$X \xrightarrow[F_q]{} X^{(q)} \xrightarrow[\text{sep}]{} Y \quad (f : X \to Y)$$

where q is the inseparable degree of f.

2.2 Elliptic Curves

Definition 2.7. An **elliptic curve** is a pair $(E, 0)$ where E/k is a genus 1 curve, and $0 \in E(k)$. ◇

These have group laws. One way to see this is to show that the map

$$\begin{array}{ccc} E(k) & \longrightarrow & \mathrm{Cl}^0(E) \\ x & \longmapsto & [x] - [0] \end{array}$$

is a bijection. Transfer of structure implies that $E(k)$ is a group.

Fact. The group law on $E(k)$ is induced by an algebraic group law

$$E \times E \to E$$

on E.

We can describe an elliptic curve explicitly in terms of equations. First note $\ell([0]) = 1$ by Riemann-Roch, so it must be spanned by $1 \in \mathscr{L}([0])$. Then, $\ell(2[0]) = 2$ so it has a number function we'll call x, i.e. $1, x \in \mathscr{L}(2[0])$ linearly independent. Next, $\ell(3[0]) = 3$ so we add a function y. Now, $\ell(4[0]) = 4$ and $1, x, y, x^2 \in \mathscr{L}(4[0])$. Almost there: $\ell(5[0]) = 5$ and $1, x, y, x^2, xy \in \mathscr{L}(5[0])$. Finally, $\ell(6[0]) = 6$, but $1, x, y, x^2, xy, x^3, y^2 \in \mathscr{L}(6[0])$. So there must be some linear dependence

$$a_1y^2 + a_2x^3 + a_3xy + a_4x^2 + a_5y + a_6x + a_7 = 0.$$

Let $E' \subset \mathbb{P}^2_k$ be the curve defined by this equation. Then, $(x, y) : E \to E'$ defines a map of curves.

Proposition 2.8. *This is an isomorphism.*

Assumption. To keep equations simple, assume $\mathrm{char}(k) \neq 2, 3$.

A suitable change of variables let's one arrive at an equation of the form

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Every elliptic curve is isomorphic to one of these $E_{a,b}$'s. Which of them are isomorphic to eachother? You can set $y = u^{-3}y_1$ and $x = u^{-2}x_1$ for any $u \in k^\times$ to see that

$$E_{a,b} \cong E_{u^4a,u^6b}.$$

These are all the isomorphisms between them.

$E_{a,b}$ will define an elliptic curve iff it is smooth. To check this, one writes down the discriminant $\Delta = -16(4a^3 + 27b^2)$.

Fact. $E_{a,b}$ is an elliptic curve $\iff \Delta \neq 0$.

Hence,

$$\left\{ \begin{array}{c} \text{iso classes of} \\ \text{elliptic curves}/k \end{array} \right\} \cong \frac{\{(a, b) \in k^2 \mid \Delta \neq 0\}}{(a, b) \sim (u^4a, u^6b)}$$

Definition 2.9. The **j-invariant** of an elliptic curve is

$$j := -1728\frac{(4a)^3}{\Delta}. \qquad \diamond$$

This is an isomorphism invariant.

Theorem 2.10. *If $k = \overline{k}$, then $E \cong E' \iff j(E) = j(E')$.*

Definition 2.11. An **isogeny** is a non-constant map $f : E_1 \to E_2$ such that $f(0) = 0$. $\diamond$

Example. Multiplication by n

$$[n] : E \to E$$

is an isogeny. △

Example. Frobenius $F_q : E \to E^{(q)}$ is an isogeny. △

Fact. Isogenies are always group homomorphisms.

Notation 2.12. $\mathrm{Hom}(E_1, E_2) := \{\text{isogenies}\} \cup \{0\}$. This is a finite free $\mathbb{Z}$-module. We also write $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ which is now a ring.

Proposition 2.13. *Suppose $f : E_1 \to E_2$ is an isogeny with separable degree n and inseparable degree m.*

(a) *If $y \in E_2(\overline{k})$, then $\#f^{-1}(y) = n$.*

(b) *If $f(x) = y$, then $e(x \mid y) = m$.*

Say $f : E_1 \to E_2$ is an isogeny. Let ω_i be a nonzero holomorphic differential on E_i (unique up to scaling).

Proposition 2.14.

(a) *f separable $\iff$ $f^*(\omega_2) \neq 0$*

(b) *We can write $f^*(\omega_2) = \alpha(f)\omega_1$. This defines a homomorphism*

$$\alpha : \mathrm{Hom}(E_1, E_2) \to k.$$

(c) *If $E_1 = E_2$ and you take $\omega_1 = \omega_2$, then $\alpha : \mathrm{End}(E) \to k$ is a ring homomorphism.*

Corollary 2.15. *$[n]$ is separable $\iff$ $p \nmid n$ where $p = \mathrm{char}(k)$.*

Stay with an isogeny $f : E_1 \to E_2$.

Proposition 2.16. *There exists a **dual isogeny** $f^\vee : E_2 \to E_1$ so that*

$$\begin{array}{ccc} E_2(k) & \xrightarrow{\sim} & \mathrm{Cl}^0(E_2) \\ {\scriptstyle f^\vee}\downarrow & & \downarrow{\scriptstyle f^*} \\ E_1(k) & \xrightarrow{\sim} & \mathrm{Cl}^0(E_1) \end{array}$$

commutes.

As a consequence

(a) $f^\vee f = [\deg(f)]$

(b) $(f+g)^\vee = f^\vee + g^\vee$

Quadratic nature of deg Define $\Lambda = \mathrm{Hom}(E_1, E_2)$ and give it the pairing

$$\langle -, - \rangle : \Lambda \times \Lambda \longrightarrow \frac{1}{2}\mathbb{Z}$$

defined by

$$2\langle f, g \rangle = \deg(f+g) - \deg(f) - \deg(g).$$

One can check that

$$2\langle f, g \rangle = f^\vee g + g^\vee f$$

by using **(a)** from before. From this, one sees that $\langle -, - \rangle$ is bi-additive and that $\langle f, f \rangle = \deg(f)$. Hence, this form is positive definite and deg is a quadratic function. In particular, $\deg([n]) = n^2$.

Working over $\mathbb{C}$ Say $E/\mathbb{C}$ is an elliptic curve, i.e. a Riemann-surface of genus 1 (so topologically a torus). It's universal cover will be a map $\pi : \mathbb{C} \to E$. The kernel of this map will be

$$\Lambda = \ker \pi = \pi_1(E) = \mathrm{H}_1(E, \mathbb{Z}).$$

Thus, $\Lambda \cong \mathbb{Z}^2$ is a lattice in $\mathbb{C}$.

Conversely, if $\Lambda \subset \mathbb{C}$ is a lattice, then $E = \mathbb{C}/\Lambda$ is a Riemann surface of genus 1. One can furthermore show that it is algebraic, so this E is an elliptic curve.

Say we have two elliptic curves $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$. Then,

$$\mathrm{Hom}(E_1, E_2) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}.$$

The map corresponding to α is an isogeny $\iff \alpha \neq 0$ and is an isomorphism $\iff \alpha\Lambda_1 = \Lambda_2$.

Corollary 2.17.

$$\{\textit{isom. classes of ECs}\} \cong \{\textit{lattices in } \mathbb{C}\}_{/\textit{scaling}}.$$

If $E = \mathbb{C}/\Lambda$, we have

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

We can scale the lattice, so we may assume $\Lambda = \langle 1, \tau \rangle$ with $\tau \in \mathbb{C} \setminus \mathbb{R}$. Then the requirement is that $\alpha \in \Lambda$ and $\alpha\tau \in \Lambda$, so write $\alpha = a + b\tau$ for some $a, b \in \mathbb{Z}$. Assume $b \neq 0$ to keep things interesting (else $\alpha \in \mathbb{Z}$). Writing $\alpha\tau = c + d\tau$ with $c, d \in \mathbb{Z}$ shows that τ satisfies the quadratic equation

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

Thus, τ must be imaginary quadratic ($\impliedby b \neq 0$). Also $\alpha \in \mathbb{Q}(\tau)$, and so we see that

$$\mathrm{End}(E) = \mathbb{Z} \text{ or } \mathrm{End}(E) \text{ is an order in an imaginary quadratic field.}$$

In the second case, we say E has **complex multiplication** or **CM**.

Example. Say $\Lambda = \langle 1, i \rangle$. Then, we get $[i] : E \to E$. In terms of equations, we have $E : y^2 = x^3 + x$ and $[i] : (x, y) \mapsto (-x, iy)$. $\triangle$

Tate module + Weil pairing Say we have an elliptic curve E/k and we fix an integer n coprime to $p = \operatorname{char} k$. Then, $[n]$ is separable. Since $\deg([n]) = n^2$, we know $\#E[n](\overline{k}) = n^2$. Applying this for all $d \mid n$, one concludes that

$$E[n](\overline{k}) \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^2.$$

Example. If $k = \mathbb{C}$, then $E[n](\mathbb{C}) = \frac{1}{n}\Lambda/\Lambda$. △

Fix a prime $\ell \neq p$. The **Tate module** is

$$T_\ell E := \varprojlim E[\ell^n](\overline{k}).$$

If you want, can think of an element as a sequence $(x_0, x_1, \dots)$ where $x_0 = 0$ and $\ell x_n = x_{n-1}$. By the above discussion, $T_\ell E \cong \mathbb{Z}_\ell^2$ (if $k = \mathbb{C}$, then $T_\ell E = \Lambda \otimes \mathbb{Z}_\ell$). If $k \neq \overline{k}$, the absolute Galois group $G_k := \operatorname{Gal}(\overline{k}/k)$ will act on the Tate module, giving a representation

$$\rho : G_k \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

You can form this Tate module for any group.

Example. $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\}$ is the group with $\mathbb{G}_m(k) = k^\times$. Then, $T_\ell \mathbb{G}_m \cong \mathbb{Z}_\ell$ and again has a Galois action

$$\chi : G_k \to \mathrm{GL}_1(\mathbb{Z}_\ell) = \mathbb{Z}_\ell^\times.$$

This is the **cyclotomic character**. △

Proposition 2.18. *There exists a map*

$$e_n : E[n] \times E[n] \to \mu_n$$

satisfying

- ***(a)*** *bilinearity:* $e_n(x + y, z) = e_n(x, z)e_n(y, z)$
- ***(b)*** *alternating:* $e_n(x, x) = 0$
- ***(c)*** *non-degenerate: if* $e_n(x, y) = 0$ *for all* y*, then* $x = 0$
- ***(d)*** *Galois-equivariant:* $e_n(\sigma x, \sigma y) = \sigma e_n(x, y)$ *for* $\sigma \in G_k$
- ***(e)*** *compatibility: if* $x \in E[nm]$ *and* $y \in E[n]$*, then*

$$e_{nm}(x, y) = e_n(mx, y).$$

Thus, $\varprojlim e_{\ell^n}$ defines a pairing $T_\ell E \times T_\ell E \to T_\ell \mathbb{G}_m$.

Notation 2.19. $\mathbb{Z}_\ell(1) := T_\ell \mathbb{G}_m$. The "(1)" indicated the Galois action.

The proposition above implies that the Weil pairing defines an isomorphism

$$\bigwedge^2 (T_\ell E) \cong \mathbb{Z}_\ell(1).$$

Equivalently, $\det(\rho) = \chi$, so the Weil pairing computes the determinant of the Tate module.

Proposition 2.20. *Say we have a map $f : E_1 \to E_2$ along with $x \in E_1[n]$ and $y \in E_2[n]$. Then,*

$$e_n(f(x), y) = e_n(x, f^\vee(y)).$$

"The dual isogeny is adjoint to f w.r.t. the Weil pairing."

Proposition 2.21. *Given $f : E \to E$,*

$$\deg(f) = \det\left(f \mid T_\ell E\right).$$

Proof. Given $x, y \in T_\ell E$, we have

$$\det(f)\,\langle x, y\rangle = \langle f(x), f(y)\rangle = \langle f^\vee f(x), y\rangle = (\deg f)\,\langle x, y\rangle$$

with first equality by definition (of determinant) and the angle brackets shorthand for the Weil pairing. ■

3 Lecture 3: Abelian varieties (analytic theory)

Last time we were talking about elliptic curves, but didn't quite finish all we wanted to say, so we'll pick up where we left off.

3.1 Elliptic Curves over Finite Fields

(Reference: Silverman, Ch. V)

3.1.1 Point counting

Say $E/\mathbb{F}_q$ is an elliptic curve. The Frobenius map $F_q : E \to E^{(q)} = E$ is an endomorphism.

Remark 3.1. If $x \in E(\overline{\mathbb{F}}_q)$, then $x \in E(\mathbb{F}_q) \iff F_q x = x$, so

$$E(\mathbb{F}_q) = \ker(1 - F_q)(\mathbb{F}_q). \qquad \circ$$

Lemma 3.2. *The map $1 - F_q$ is separable, and so $\#E(\mathbb{F}_q) = \deg(1 - F_q)$.*

Proof. This is because $(1 - F_q)^* \omega = 1^*\omega - F_q^*\omega = \omega$ is nonzero, where ω is a holomorphic differential on E. ■

Recall 3.3. We defined a positive definite pairing $\langle -, -\rangle$ on $\mathrm{End}(E)$ by polarizing degree, i.e. $\langle f, f\rangle = \deg(f)$. $\odot$

We can apply Cauchy-Schwarz to this in order to see that

$$\langle 1, -F_q\rangle^2 \le \langle 1, 1\rangle\,\langle -F_q, -F_q\rangle = q,$$

so $|\langle 1, -F_q\rangle| \leq \sqrt{q}$. Recalling that

$$2\langle 1, -F_q\rangle = \deg(1 - F_q) - \deg(1) - \deg(F_q) = \#E(\mathbb{F}_q) - 1 - q,$$

we conclude

Theorem 3.4 (**Hasse bound**)**.**

$$|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}.$$

Intuition. Think of an equation $E : y^2 = x^3 + ax + b$. If you plug in a random $x \in \mathbb{F}_q$, the RHS to be a random element of $\mathbb{F}_q$ as well. Half the elements of $\mathbb{F}_q$ are squares while half are non-squares. If do get a (nonzero) square, there will be two y's solving the equation, but if you get a non-square, there will be none. Hence you expect about

$$1 + 2\left(\frac{q-1}{2}\right) + 0\left(\frac{q-1}{2}\right) = q$$

$\mathbb{F}_p$-points. The Hasse bound says this is correct within an error of about $2\sqrt{q}$.

Notation 3.5. We fix $a \in \mathbb{Z}$ so that

$$\mathbb{E}(\mathbb{F}_q) = q - a + 1,$$

i.e. $a = 2\langle 1, F_q\rangle$ (so $|a| \leq 2\sqrt{q}$).

Question 3.6 (Audience)**.** *Is there an elementary heuristic for the error term?*

Answer. It really comes from this Riemann hypothesis (which we'll state soon). That's not an elementary heuristic, but at least fits it into a bigger context. ⋆

Proposition 3.7. *$a = \mathrm{Tr}(F_q \mid T_\ell E)$ is the trace of Frobenius acting on the Tate module.*

Proof. For any 2×2 matrix A, one has $\mathrm{Tr}(a) = 1 + \det(A) - \det(1 - A)$ (exercise). If $A = F_q \mid T_\ell E$, then this reads

$$\mathrm{Tr}(F_q \mid T_\ell E) = 1 + \deg(F_q) - \deg(1 - F_q) = a$$

(last lecture [Proposition 2.21] we showed the determinant on the Tate module is the degree). ■

Definition 3.8. A **Weil number** of weight w (w.r.t. q) is an algebraic number $\alpha \in \overline{\mathbb{Q}}$ s.t. $|\alpha| = q^{w/2}$ for any embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. ◇

Theorem 3.9 (**Riemann hypothesis**)**.** *The eigenvalues of F_q on $T_\ell E$ are Weil numbers of weight* 1*.*

Proof. Let α, β be the eigenvalues under consideration. Then,

$$\alpha\beta = \det(F_q) = q \text{ and } \alpha + \beta = \mathrm{Tr}(F_q) = a,$$

so α, β both satisfy $T^2 - aT + q = 0$. Hence,

$$\alpha, \beta = \frac{a \pm \sqrt{a^2 - 4q}}{2}.$$

The Hasse bound says the discriminant is negative, so α, β are complex conjugate to each other and hence $|\alpha|^2 = |\beta|^2 = \alpha\beta = q$. ■

Definition 3.10. Let $X/\mathbb{F}_q$ be any variety. Its **zeta function** is

$$Z_X(T) = \exp\left(\sum_{r\geq 1} \#X(\mathbb{F}_{q^r})\frac{T^r}{r}\right). \qquad \diamond$$

Theorem 3.11. *If $E/\mathbb{F}_q$ is an elliptic curve, then*

$$Z_E(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Proof. $\#E(\mathbb{F}_{q^r}) = 1 + q^r - \mathrm{Tr}(F_{q^r} \mid T_\ell E)$. Since $F_{q^r} = F_q^r$, this says

$$\#E(\mathbb{F}_{q^r}) = 1 + q^r - \alpha^r - \beta^r,$$

with α, β the Eigenvalues of F_q as before. Using the identity $-\log(1-T) = \sum_{n\geq 1} T^n/n$, one now sees that

$$\sum_{r\geq 1} \#E(\mathbb{F}_{q^r})\frac{T^r}{r} = -\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T),$$

and so

$$Z_E(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}. \qquad \blacksquare$$

Remark 3.12. The numbers α, β are the roots of the Zeta function and they have absolute value $q^{1/2}$. This is why Theorem 3.9 is called the Riemann hypothesis; it's analogous to all the zeros being on the line $\mathrm{Re}(s) = \frac{1}{2}$.[4] $\circ$

Suppose $f : E_1 \to E_2$ is an isogeny over $\mathbb{F}_q$. This induces a map $T_\ell E_1 \to T_\ell E_2$ on Tate modules. This map will have no kernel and will have finite index image, so $T_\ell E_1 \otimes \mathbb{Q}_\ell \xrightarrow{\sim} T_\ell E_2 \otimes \mathbb{Q}_\ell$ as vector spaces. This isomorphism furthermore commutes with the action of Frobenius, and so these give isomorphic 2-dimensional representations of Frobenius. In particular, they have the same traces, so

Question: For $\ell \nmid \#\ker f$?

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$

Theorem 3.13 (Tate)**.** *The converse holds as well. If two Elliptic curves over $\mathbb{F}_q$ have the same number of points (over every finite extension), then they are isogenies.*

3.1.2 Ordinary/Supersingular

Consider any field k with $\mathrm{char}(k) = p$. Then, $[p]$ is not separable and has deg $= p^2$. This gives two possibilities

(a) The separable degree is p, i.e. $E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$. In this case, we say E is **ordinary**.

(b) The separable degree is 1, i.e. $E[p](\overline{k}) \cong 0$. In this case, we say E is **supersingular**.

Proposition 3.14. *If E is supersingular, then $j(E) \in \mathbb{F}_{p^2}$.*

[4] Imagine e.g. that $T = q^{-s}$ so $|T| = q^{-\mathrm{Re}(s)}$

Proof. Multiplication by p is inseparable of degree p^2, so factors as

$$E \xrightarrow[F_{p^2}]{} E^{(p^2)} \xrightarrow[f]{} E \qquad (\text{with } [p] : E \to E)$$

where f must have degree 1 and so be an isomorphism. Thus,

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2} \implies j(E) \in \mathbb{F}_{p^2}. \qquad \blacksquare$$

Corollary 3.15. *If $k = \overline{k}$, there are only finitely many s-s curves.*

(The exact number of such curves is computed in equation (15.1))

Question 3.16 (Audience)**.** *Do we know the different groups that arise as groups of rational points $E(\mathbb{F}_q)$ of elliptic curves over finite fields?*

Answer. They're very constrained. There's the Hasse bound and they have to be a product of two cyclic groups, so you should be able to say something. Unclear what the exact answer should be. $\star$

3.2 Abelian varieties

(Reference: Ch. 1 of Mumford's "Abelian Varities")

Definition 3.17. An **abelian variety** is a connected and complete (i.e. proper) group variety. $\diamond$

Example. Elliptic curves are 1-dimensional abelian varieties. $\triangle$

Proposition 3.18. *If A is an abelian variety and* $\dim A = 1$*, then $g(A) = 1$.*

Proof. If you have a group variety and a cotangent vector at the origin, you can use the group law to translate it around and form a whole vector field. This gives you a trivialization of the sheaf of 1-forms since you have a nowhere vanishing section. Thus, $\Omega^1 \cong \mathscr{O}_A$ is trivial, so $h^0(\Omega^1) = h^0(\mathscr{O}) = 1$ is the genus. $\blacksquare$

Assumption. For the rest of this lecture, we work over $\mathbb{C}$.

If A is an abelian variety, then $A(\mathbb{C})$ is a compact, connected complex Lie group.

Let X be any compact, connected complex Lie group. Let $g = \dim(X)$ and $V = \mathrm{Lie}(X) = T_eX$ with $e \in X$ the identity. Let $\exp : V \to X$ be the exponential map. Then,

(a) X is commutative.

Explanation. The adjoint map $\mathrm{Ad} : X \to \mathrm{End}(V)$ is a holomorphic map from a compact space to a vector space. By the maximum modulus principle, the map must be constant, so $\mathrm{Ad}(x) = \mathrm{Ad}(e) = \mathrm{id}$ for all $x \in X$. Hence, the conjugation action is trivial, so X is commutative.

(b) exp is a homomorphism of groups.

Explanation. This is true for all commutative Lie groups.

(c) exp is surjective

Explanation. Let $U = \mathrm{im}(\exp)$. Then U is a subgroup that is an open set (exp a local homeomorphism), so X/U is discrete + compact, i.e. a point. Hence, $X = U$.

(d) $M = \ker(\exp)$ is a lattice in V.

Explanation. exp is a local homeomorphism, so M must be discrete. exp is surjective so gives an isomorphism $V/M \xrightarrow{\sim} X$. Hence, M is cocompact.

(e) X is a torus, i.e. $\cong (S^1)^{2g}$

Explanation. It's $V/M = \mathbb{R}^{2g}/\mathbb{Z}^{2g}$.

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

(g) $\mathrm{H}^i(X, \mathbb{Z}) = \mathrm{Hom}(\bigwedge^i M, \mathbb{Z})$

Explanation. Künneth (+ induction on g?) will give an isomorphism $\bigwedge^i \mathrm{H}^1(X, \mathbb{Z}) \xrightarrow{\sim} \mathrm{H}^i(X, \mathbb{Z})$. Finally, $\mathrm{H}_1(X, \mathbb{Z}) = M$.

3.2.1 Line bundles on Complex Tori

Let $X = V/M$ be a complex torus. Let $\mathrm{Pic}(X)$ be its group of (iso classes of) line bundles. Let $\mathrm{Pic}^0(X)$ be the subgroup of line bundles which are trivial topologically. The **Néron-Sevri group** is the quotient

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X).$$

Definition 3.19. A **Riemann form** on V is a Hermitian form H whose imaginary part $E = \mathrm{im}(H)$ takes integer values on the lattice M. ◇

Warning 3.20. Some people require Riemann forms to be positive definite. •

Notation 3.21. Let $\mathcal{R}$ be the set of Riemann forms, a group under addition. Let

$$\mathcal{P} = \left\{ (H, \alpha) \;\middle|\; \begin{array}{c} H \in \mathcal{R} \text{ and } \alpha : M \to U(1) \text{ satisfying} \\ \alpha(x+iy) = e^{i\pi E(x,y)}\alpha(x)\alpha(y) \end{array} \right\},$$

and let

$$\mathcal{P}^0 := \mathrm{Hom}(M, U(1)) \subset \mathcal{P}.$$

Note that $\mathcal{P}$ is a group via

$$(H_1, \alpha_1) \cdot (H_2, \alpha_2) = (H_1 + H_2, \alpha_1\alpha_2).$$

These fit into an exact sequence

$$0 \longrightarrow \mathcal{P}^0 \longrightarrow \mathcal{P} \longrightarrow \mathcal{R} \longrightarrow 0.$$

Theorem 3.22 (**Appell-Humbert**). *There is a natural isomorphism* $\mathcal{P} \xrightarrow{\sim} \mathrm{Pic}(X)$ *inducing* $\mathcal{P}^0 \xrightarrow{\sim} \mathrm{Pic}^0(X)$ *and* $\mathcal{R} \xrightarrow{\sim} \mathrm{NS}(X)$.

Remark 3.23. We won't prove the theorem, but here are some thoughts

- Let $\pi : V \to X$ be the quotient map. If $L \in \mathrm{Pic}(X)$, the π^*L is a (trivial) line bundle on V. However, π^*L has an action by M, and L is the quotient of π^*L by its M-action.

- Say $(H, \alpha) \in \mathcal{P}$. Then, $M \curvearrowright V \times \mathbb{C}$ via

$$\lambda \cdot (v, z) = \left(v + \lambda, \alpha(\lambda) e^{\pi H(v,\lambda) + \frac{\pi}{2} H(\lambda,\lambda)} z \right).$$

  Let $L(H, \alpha)$ be the quotient bundle living on X. This is the isomorphism in the theorem.

  The hard part in proving the theorem is showing all actions look like this.

- There is a bijection between Hermitian forms H on V and alternating real forms E s.t. $E(ix, iy) = E(x, y)$. This is just a statement about complex vector spaces (nothing about lattices). The bijection is

$$E = \operatorname{im} H \text{ and } H(x, y) = E(ix, y) + iE(x, y).$$

- Given $(H, \alpha) \in \mathcal{P}$, we get $E = \operatorname{im} H$. It will be alternating and integral values on M, so it gives a map $E : \bigwedge^2 M \to \mathbb{Z}$, i.e. it is an element of

$$\operatorname{Hom}(\bigwedge^2 M, \mathbb{Z}) = \mathrm{H}^2(X, \mathbb{Z}).$$

  Under our identifications, this is $c_1(L(H, \alpha))$. Note that $L(H, \alpha)$ is topologically trivial

$$\iff c_1 = 0 \iff E = 0 \iff H = 0. \qquad \circ$$

If $x \in X$, get translation map

$$\begin{array}{rccc} t_x : & X & \longrightarrow & X \\ & y & \longmapsto & x + y. \end{array}$$

This induces an action $X \curvearrowright \operatorname{Pic}(X)$ via $x \cdot L = t_x^*(L)$.

Proposition 3.24.

$$t_x^* L(H, \alpha) = L\left(H, \alpha e^{2\pi i E(x,-)}\right)$$

Some remarks on this proposition

- The mapping $M \ni \lambda \mapsto e^{2\pi i E(x,\lambda)}$ is well-defined since E is integer valued on the lattice (so any choice of lift of x will give same result).
- Furthermore, $L(H, \alpha) \in \operatorname{Pic}(X)$ is translation-invariant iff $H = 0$ iff $L(H, \alpha) \in \operatorname{Pic}^0(X)$.
- $$t_x^* L(H, \alpha) \otimes L(H, \alpha)^\vee = L(0, e^{2\pi i E(x,-)}) \in \operatorname{Pic}^0(X).$$

  For any $L \in \operatorname{Pic}(X)$, the map $x \mapsto t^* x L \otimes L^{-1}$ defines a group homomorphism

$$\varphi_L : X \to \operatorname{Pic}^0(X).$$

What can we say about sections of these line bundles?

Definition 3.25. A **θ-function** for $(H, \alpha) \in \mathcal{P}$ is a holomorphic function $\theta : V \to \mathbb{C}$ satisfying

$$\theta(v + \lambda) = \alpha(\lambda) e^{\pi H(v,\lambda) + \frac{\pi}{2} H(\lambda,\lambda)} \theta(v) \text{ for all } v \in V, \lambda \in M. \qquad \diamond$$

Proposition 3.26. $\mathrm{H}^0(X, L(H,\alpha)) \cong \{\theta\text{-functions}\}$.

(the idea is that if you have a section of $L(H,\alpha)$, it pulls back to a section of the trivial bundle on V – i.e. a holomorphic function – which must interact with the equivariance)

Theorem 3.27 (Lefschetz)**.** *$L(H,\alpha)$ is ample $\iff$ H is positive definite.*

Corollary 3.28. *X is a projective algebraic variety (i.e. an abelian variety) $\iff$ there exists a positive definite Riemann form.*

Remark 3.29.

- X algebraic $\implies$ X projective
- If H positive definite, then $L(H,\alpha)^{\otimes 3}$ is already very ample.
- Say $E = \mathbb{C}/\langle 1, \tau\rangle$ is a 1-dimensional complex torus. Then we can define

$$H(x,y) = \frac{x\overline{y}}{|\operatorname{Im}\tau|}.$$

  This is a positive definite Riemann form, so E is algebraic. ∘

Given two complex tori X, Y, we write

$$\operatorname{Hom}(X,Y) = \{\text{holo. group homomorphisms } X \to Y\}.$$

Definition 3.30. $f \in \operatorname{Hom}(X,Y)$ is an **isogeny** if f is surjective and $\ker(f)$ is finite. It's **degree** is $\deg(f) := \#\ker(f)$. ◇

Example. $[n] : X \to X$ is an isogeny of degree n^{2g}. △

3.2.2 Dual torus

Start with $X = V/M$. Let

$$\overline{V}^* := \{\text{conj-lin maps } V \to \mathbb{C}\}$$

with lattice

$$M^\vee = \left\{ f \in \overline{V}^* : (\operatorname{im} f)(M) \subset \mathbb{Z} \right\}.$$

Define

$$X^\vee := \overline{V}^*/M^\vee.$$

Exercise. $(X^\vee)^\vee \cong X$.

Properties

- If $f : X \to Y$ is a map of tori, get dual map $f^\vee : Y^\vee \to X^\vee$.
- If f is an isogeny, then so is $f^\vee$ and $\deg f = \deg f^\vee$. In fact, more is true

  Proposition 3.31. $\ker(f)$ *is canonically (Pontryagin) dual to* $\ker(f^\vee)$

(See proof in course notes)

Application. If $X = Y$ and $f = [n]$, then $f^\vee = [n]$, and we get a canonical pairing

$$X[n] \times X^\vee[n] \longrightarrow \mathbb{Z}/n\mathbb{Z}\,(\cong \mu_n)\,,$$

the **Weil pairing**.

- There is a natural isomorphism $X^\vee = \mathrm{Pic}^0(X)$.

  Proof. Say we have $f \in \overline{V}^*$. Then we get a map

  $$\begin{array}{rccc} \alpha_f : & M & \longrightarrow & U(1) \\ & \lambda & \longmapsto & e^{2\pi i\,\mathrm{im}(f(\lambda))} \end{array}$$

  which gives an element of $\mathcal{P}^0 \cong \mathrm{Pic}(X)$. By definition, $f \mapsto \alpha_f$ descends to a map $X^\vee \to \mathrm{Pic}^0(X)$. ■

Suppose we have a Riemann form $H \in \mathcal{R}$ (H Hermitian so conjugate-linear in second slot). If H is non-degenerate, it defines an isomorphism

$$\begin{array}{ccc} V & \longrightarrow & \overline{V}^* \\ v & \longmapsto & H(v, -). \end{array}$$

This makes M to $M^\vee$, and so descends to a map of tori $\varphi_H : X \xrightarrow{\sim} X^\vee$.

Remark 3.32. If $L = L(H, \alpha)$ (for any α), then we get a commutative square

$$\begin{array}{ccc} X & \xrightarrow{\varphi_H} & X^\vee \\ {\scriptstyle =}\downarrow & & \downarrow{\scriptstyle =} \\ X & \xrightarrow{\varphi_L} & \mathrm{Pic}^0(X) \end{array}$$

with vertical maps the usual isomorphisms. ∘

Definition 3.33. A **polarization** is a map $X \to X^\vee$ of the form φ_H (or φ_L) where H is positive definite (i.e. L ample). This will necessarily be an isogeny. A **principal polarization** is one giving an isomorphism $X \xrightarrow{\sim} X^\vee$. ◇

4 Lecture 4: Abelian varieties (algebraic theory)

Last time was abelian varieties over $\mathbb{C}$. Today is the theory over general fields.

Notation 4.1. k will be a field, and A/k will be an abelian variety.

Over $\mathbb{C}$, every abelian variety was a complex torus, and this made things easy. We don't have such a uniformization over arbitrary fields, but many of the same statements are nevertheless true.

Lemma 4.2 (**Rigidity Lemma**). *Suppose X, Y, Z are varieties and X is complete. Let $f : X \times Y \to Z$ be a function so that $f|_{X\times\{y_0\}}$ is constant and $f|_{\{x_0\}\times Y}$ is constant for some $x_0 \in X$ and $y_0 \in Y$. Then, f is constant.*

Corollary 4.3. *Suppose A, B are abelian varieties, and $f : A \to B$ is a map of varieties s.t. $f(0) = 0$. Then, f is a group homomorphism.*

Proof. Consider $h : A \times A \to A$ defined by $h(x, y) = f(x + y) - f(y) - f(x)$. Then, $h(x, 0) = 0 = h(0, y)$ for all x, y, so $h = 0$ by rigidity. ■

Corollary 4.4. *Abelian varieties are commutative*

Proof. $A \to A, x \mapsto -x$ takes $0 \mapsto 0$ and so is a homomorphism. ■

Theorem 4.5 (**Theorem of the cube**). *Let X, Y, Z be varieties, X and Y complete. Fix basepoints $x_0 \in X, y_0 \in Y, z_0 \in Z$. Let L be a line bundle on $X \times Y \times Z$. Suppose that*

$$L|_{X\times Y\times z_0}, \quad L|_{X\times y_0\times Z}, \quad \text{and} \quad L|_{x_0\times Y\times Z}$$

are all trivial. Then, L is trivial.

Remark 4.6. This says that a map from $X \times Y \times Z \to B\mathbb{G}_m$ which is trivial on the three axes is itself trivial. Phrased this way it looks a bit like rigidity, except now you need 3 factors since you're mapping to a stack instead of a scheme. ∘

Question 4.7 (Audience). *Could you replace $\mathbb{G}_m$ there with GL_n?*

Answer. I don't know. ⋆

Corollary 4.8. *Let $A = AV$ (i.e. A be an abelian variety). Let $p_i : A \times A \times A \to A$ be projection onto the ith factor. Let $p_{ij} = p_i + p_j$ and $p_{123} = p_1 + p_2 + p_3$. If L is a line bundle on A, then*

$$\bigotimes_{S\subset\{1,2,3\}} (p_S^* L)^{(-1)^{1+\#S}} \simeq \mathscr{O}_A$$

is trivial.

Proof. Immediate. Notice on $A \times A \times 0$, $p_{123}^* = p_{12}^*$, $p_{12}^* L = p_1^* L$, and $p_3^* L$ is trivial. Get similar cancellation when you restrict to other axes. ■

Corollary 4.9. *Suppose we have maps $f, g, h : X \to A$ from a variety X to an AV A, and let L be a line bundle on A. Then,*

$$(f + g + h)^* L \otimes (f + g)^* L^{-1} \otimes (f + h)^* L^{-1} \otimes (g + h)^* L^{-1} \otimes f^* L \otimes g^* L \otimes h^* L$$

is trivial.

Proof. Consider $(f, g, h) : X \to A^3$ and pull back the previous corollary. ■

Problem 4.1. *Let L be a line bundle on $A = AV$. Then,*

$$[n]^*L = L^{\frac{n^2+n}{2}} \otimes ([-1]^*L)^{\frac{n^2-n}{2}}.$$

*In particular, if L is **symmetric** (i.e. $L \simeq [-1]^*L$), then $[n]^*L \simeq L^{n^2}$ and if L is **anti-symmetric** (i.e. $L^{-1} \simeq [-1]^*L$), then $[n]^*L \simeq L^n$.*

Proof. Take $f = [n]$, $g = [1]$, and $h = [-1]$. We see that

$$[n]^*L \otimes [n+1]^*L^{-1} \otimes [n-1]^*L^{-1} \otimes [n]^*L \otimes L \otimes [-1]^*L$$

is trivial, i.e.

$$[n+1]^*L = [n]^*L^2 \otimes [n-1]^*L^{-1} \otimes L \otimes [-1]^*L.$$

Now induct upwards and downwards. ■

Proposition 4.10. *$[n] : A \to A$ is an isogeny, i.e. is surjective with finite kernel.*

Proof. Choose an ample bundle L on A. We may replace L by $L \otimes [-1]L$ to assume it is symmetric and ample. Hence, $[n]^*L = L^{n^2}$ is ample. At the same time, $[n]^*L|_{A[n]}$ is trivial, so it is both trivial and ample on $A[n]$. That is, $A[n]$ is a proper variety with $\mathscr{O}_{A[n]}$ ample. This forces $\dim A[n] = 0$, so $A[n]$ is proper and quasi-finite, so finite. The image of $[n]$ will have the same dimension as A, and so $[n]$ must be surjective. ■

Abelian varieties are projective. We won't prove this.

Proposition 4.11. *$[n]$ has degree n^{2g}*

Proof. Start with a general fact:

Fact. If $f : X \to Y$ is a finite, surjective map of g-dimensional varieties and let $D_1, \ldots, D_g$ be divisors on Y. Then, we have an equality

$$(\deg f)(D_1 \cdots D_g)_Y = (f^*D_1 \cdots f^*D_g)_X$$

of intersection numbers.

Let D be a symmetric ample divisor on A. We know $[n]^*D \equiv n^2D$ (linear equivalence), so

$$(\deg[n])(D \cdots D) = \big((n^2D) \cdots (n^2D)\big) = n^{2g}(D \cdots D) \implies \deg[n] = n^{2g}.$$

Above, we are using that $(D \cdots D) \neq 0$ since this just computes the degree of the image of A under the projective map induced by D. ■

One can show that $[n]$ induces multiplication by n on the tangent space T_0A at the identity. In particular, if $\operatorname{char} k \nmid n$, this is an isomorphism of the tangent space.

Proposition 4.12. *$[n]$ separable $\iff$ n prime to $\operatorname{char} k$. So if $\operatorname{char} k \nmid n$, $\#A[n](\overline{k}) = n^{2g}$.*

An induction argument now shows that if n is prime to the characteristic, then

$$A[n](\overline{k}) \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{2g}.$$

On the other hand, $[p] : A \to A$ is not separable, so $\#A[p](\overline{k}) < p^{2g}$. In fact, $\#A[p](\overline{k}) < p^g$. We'll say more about why later.[5]

Theorem 4.13 (**Theorem of the square**). *Let L be a line bundle on A, and fix points $x, y \in A$. Then,*

$$t_{x+y}^* L \otimes L \simeq t_x^* L \otimes t_y^* L.$$

Here, t_{blah} is translation by blah.

Proof. Take $f = \mathrm{id}$, $g = x$, $h = y$ in Corollary 4.9. ■

This is essentially saying that, given L, we have a group homomorphism

$$\begin{array}{rccc} \varphi_L : & A & \longrightarrow & \mathrm{Pic}(A) \\ & x & \longmapsto & t_x^* L \otimes L^{-1}. \end{array}$$

4.1 Dual Variety

Recall 4.14. Given a complex torus $A = V/M$, the dual torus was $A^\vee = \overline{V}^*/M^\vee$. We saw that there was a bijection $A^\vee \xrightarrow{\sim} \mathrm{Pic}^0(A)$. Here, Pic^0 was the topologically trivial line bundles, but we saw these were equivalently the translation-invariant ones. ⊙

Definition 4.15. Let

$$\mathrm{Pic}^0(A) = \{L \in \mathrm{Pic}(A) : t_x^* L \cong L \text{ for all } x \in A\}.$$ ◇

Goal. We want to give $\mathrm{Pic}^0(A)$ the structure of an abelian variety $A^\vee$.

To make sense of this, we consider the following functor. For a variety T, set

$$F(T) = \left\{ \begin{array}{c} \text{isom. classes of line bundles } L \text{ on } T \times A \text{ so that} \\ \textbf{(a)} L\,|_{\{t\}\times A} \in \mathrm{Pic}^0(A)\ \forall t \in T \text{ and } \textbf{(b)} L|_{T\times\{0\}} \text{ is trivial} \end{array} \right\}.$$

Remark 4.16. $F(k) = \mathrm{Pic}^0(A)$. ○

Definition 4.17. The **dual abelian variety** is the variety $A^\vee$ representing F, if it exists. ◇

Remark 4.18. If $A^\vee$ exists, it comes with a universal bundle $\wp \in F(A^\vee)$, i.e. a line bundle on $A \times A^\vee$. This has the property, among other things, that

$$A^\vee \ni t \longmapsto \wp|_{A\times\{t\}}$$

gives a bijection $A^\vee \xrightarrow{\sim} \mathrm{Pic}^0(A)$. This is called the **Poincaré bundle**. ○

Fact. $A^\vee$ always exists.

[5] Corollary 6.24

How do you find it? Pick some ample L on A, so we get $\varphi_L : A \to \mathrm{Pic}^0(A)$. Over $\mathbb{C}$, this was an isogeny of complex tori. Over arbitrary fields, can show φ_L is surjective w/ finite kernel $K(L)$. One can endow $K(L)$ w/ a scheme structure, and then define $A^\vee = A/K(L)$.

Here's another way to think of $A^\vee$. Start with $L \in \mathrm{Pic}^0(A)$. Choose for each $x \in A$, an isomorphism $\varphi_x : t_x^* L \xrightarrow{\sim} L$. These satisfy some compatibilities:

$$\begin{array}{ccc} t_{x+y}^* L & \xrightarrow{=} & t_x^* t_y^* L \\ {\scriptstyle \varphi_{x+y}}\downarrow & & \downarrow{\scriptstyle t_x^* \varphi_y} \\ L & \xrightarrow{\varphi_x} & t_x^* L \end{array}$$

should commute. It won't in general if you pick some random φ_x. The discrepancy of its commutativity is measured by writing

$$\varphi_{x+y} = \alpha_{x,y}(t_x^* \varphi_y) \circ \varphi_y \text{ for some } \alpha_{x,y} \in \mathrm{Aut}(L) = \mathbb{G}_m.$$

These $\alpha_{x,y}$ give a 2-cocycle α (in the sense of group cohomology, with A acting trivially on $\mathbb{G}_m$). Thus, it corresponds to a central extension

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{G}(L) \longrightarrow A \longrightarrow 0$$

of A by $\mathbb{G}_m$.

Construction 4.19 (Alternate construction). Consider the maps $m, p_1, p_2 : A \times A \to A$. One can show that

$$L \in \mathrm{Pic}^0(A) \iff m^* L \cong p_1^* L \otimes p_2^* L.$$

Looking at fibers, this is giving isomorphisms $L_{x+y} \cong L_x \otimes L_y$. These induce maps $L_x \times L_y \to L_{x+y}$, i.e. a map $L \times L \to L$ lifting multiplication on A. Then, $\mathcal{G}(L) = L \setminus \{\text{zero section}\}$ with this map $L \times L \to L$ as its multiplication.

Fact. This $\mathcal{G}(L)$ is a commutative group variety.

This construction gives a map

$$\mathcal{G} : \mathrm{Pic}^0(A) \to \mathrm{Ext}^1(A, \mathbb{G}_m),$$

with Ext^1 above taken in the category of commutative group varieties.

Theorem 4.20 (Serre). *$\mathcal{G}$ above is an isomorphism of (abstract) groups.*

If you take Ext in the category of sheaves of groups, then you recover $A^\vee$.

Potentially this is in his book on algebraic groups and class fields

4.2 Mordell-Weil

Theorem 4.21 (**Mordell-Weil**). *Let A be an abelian variety over a number field K. Then, $A(K)$ is a f.g. abelian group.*

One usually proves this in two steps

(1) (**weak Mordell-Weil**) $A(K)/nA(K)$ is finite ($n \in \mathbb{Z}$)

(2) Deduce full theorem from **(1)** + theory of height functions.

We won't discuss **(2)**, but let's go over the proof of **(1)**. We'll see the same ideas later.

Proof of weak MW. Start with the **Kummer sequence**

$$0 \longrightarrow A[n](\overline{K}) \longrightarrow A(\overline{K}) \xrightarrow{n} A(\overline{K}) \longrightarrow 0.$$

This is a short exact sequence of Galois modules, so we can take cohomology to get

$$0 \longrightarrow A[n](K) \longrightarrow A(K) \xrightarrow{n} A(K) \longrightarrow \mathrm{H}^1(G_K, A[n](\overline{K})) \longrightarrow \mathrm{H}^1(G_K, A(\overline{K})) \xrightarrow{n} \mathrm{H}^1(G_K, A(\overline{K})),$$

where $G_K = \mathrm{Gal}(\overline{K}/K)$. Exactness of the above sequence mostly amounts to saying that

$$0 \longrightarrow A(K)/nA(K) \xrightarrow{\delta} \mathrm{H}^1(G_K, A[n](\overline{K})) \longrightarrow \mathrm{H}^1(G_K, A(\overline{K}))[n] \longrightarrow 0$$

is exact. To prove finiteness of $A(K)/nA(K)$, it would suffice to show that $\mathrm{H}^1(G_K, A[n](K))$ is finite, but it's not. However, there exists a finite set S of places of K such that $\mathrm{im}(\delta)$ consists of classes which are unramified away from S, i.e.

$$\mathrm{im}(\delta) \subset \mathrm{H}^1(G_{K,S}, A[n](\overline{K})),$$

where $G_{K,S}$ is the Galois group of the maximal extension of K unramified outside S. In fact, one can take S to be the set consisting of places where A has bad reduction union the set of places above n. We'll say more about this after talking about group schemes in greater generality.

Accepting the above, we only need to show that $\mathrm{H}^1(G_{K,S}, A[n](\overline{K}))$ is finite. Let L/K be a finite Galois extension s.t. G_L acts trivially on $A[n](\overline{K})$. Now, consider the **inflation-restriction sequence**

$$0 \longrightarrow \mathrm{H}^1(\mathrm{Gal}(L/K), A[n](\overline{K})) \longrightarrow \mathrm{H}^1(G_{K,S}, A[n](\overline{K})) \longrightarrow \mathrm{H}^1(G_{L,S}, A[n](\overline{K})).$$

The left group is obviously finite, so the middle group will be finite if the right one is. Note that

$$\mathrm{H}^1(G_{L,S}, A[n](\overline{K})) \cong \mathrm{Hom}(G_{L,S}, \mathbb{Z}/n\mathbb{Z}),$$

and that a map $G_{L,S} \to \mathbb{Z}/n\mathbb{Z}$ is (almost) the same thing as a $\mathbb{Z}/n\mathbb{Z}$ extension of L unramified away from S. There are only finitely many such extensions (e.g. by Hermite-Minkowski or class field theory). ■

Remember: For analyzing Galois H^1's in general, often useful to extend K to a field L whose Galois group acts trivially on the module, and then look at the inflation-restriction sequence

We'll use a similar sort of approach when we prove Theorem 1.7.

4.3 Isogeny Category

Theorem 4.22 (**Poincaré reducibility**). *Suppose A is an abelian variety and $B \subset A$ is a sub abelian variety. Then, there exists $C \subset A$ a sub abelian variety s.t. $B \times C \to A$ is an isogeny.*

Proof idea. There is a quotient map $A \to A/B$ which induces a dual map $(A/B)^\vee \to A^\vee$. Choosing any ample L on A, we get an isogeny $A^\vee \xrightarrow{\varphi_L} A$. We let C be the image of $(A/B)^\vee$ in A. ■

Definition 4.23. An abelian variety A is **simple** if its only sub AVs are 0 and A. ◇

Corollary 4.24. *Given A, there exists simple $B_1, \ldots, B_n$ and an isogeny $B_1 \times \ldots \times B_n \to A$.*

Definition 4.25. We define the category Isog whose

- objects are abelian varieties over k; and whose
- morphisms are $\mathrm{Hom}_{\mathrm{Isog}}(A, B) = \mathrm{Hom}_{\mathrm{AV}}(A, B) \otimes \mathbb{Q}$.

This is called the **isogeny category**. ◇

Remark 4.26. Can show if $f : A \to B$, there is an isogeny $g : B \to A$ s.t. $gf = [n]$ for some n. Thus, $\frac{1}{n}g$ is the inverse to f in Isog. In fact, Isog is the universal categories in which isogenies become isomorphisms. Furthermore, one can show that Isog is an abelian category, and Poincaré reducibility $\iff$ Isog is semi-simple. One gets the following consequences for free

- The decomposition of A into a product of simple AVs is unique up to isogeny
- If A is a simple Abelian variety, then $\mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$

The above are formal facts about (semi-simple) abelian categories. ◦

5 Lecture 5: Group schemes 1

(Reference: Tate's article "Finite flat group schemes" in "Modular forms and Fermat's Last Theorem")

Let E be a supersingular elliptic curve over $\mathbb{F}_p$. Then, $E[p](\overline{\mathbb{F}}_p) = 0$. However, $E[p]$ is a degree p^2 subscheme of E, so there's something there; we just can't study it via points. This is the sort of thing we'd like to understand better by studying group schemes.

Definition 5.1. Let $\mathcal{C}$ be a category with all finite products, and let $*$ be the final object (= empty product). A **group object** in $\mathcal{C}$ is a tuple (G, m, i, e) with G an object of $\mathcal{C}$ equipped with morphisms

- $m : G \times G \to G$ multiplication
- $i : G \to G$ inversion
- $e : * \to G$ identity

satisfying

- Associativity, i.e.

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathrm{id} \times m} & G \times G \\ {\scriptstyle m \times 1}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

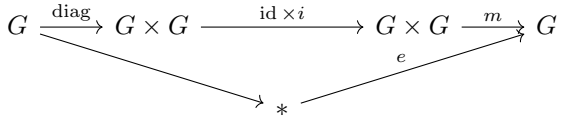
  commutes

- identity, i.e.

$$G \overset{\mathrm{id}}{\underset{=}{\rightarrow}} G \times * \xrightarrow{\mathrm{id} \times e} G \times G \xrightarrow{m} G$$

  commutes (and similarly with identity of the left)

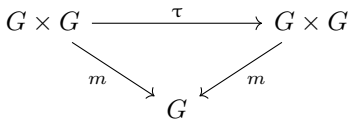
- inverse, i.e.



  commutes (and similarly with i on the left) ◇

Example. A group object in Set is a normal group. △

Definition 5.2. A group object $G \in \mathcal{C}$ is **commutative** if



commutes, where $\tau : G \times G \to G \times G$ is the morphism switching the factors. ◇

Definition 5.3. If G, H are group objects in $\mathcal{C}$, a **homomorphisms** $G \to H$ is a morphism in $\mathcal{C}$ s.t. all the diagrams you expect to commute do commute. ◇

Hence, one can form the category of group objects in $\mathcal{C}$.

One can simplify this story by using the functor of points perspective.

Notation 5.4. For $X \in \mathcal{C}$ and $T \in \mathcal{C}$, we let $h_X : \mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$ be the functor

$$h_X(T) = \mathrm{Hom}_{\mathcal{C}}(T, X).$$

Theorem 5.5 (**Yoneda Lemma**). *X is determined by h_X, i.e. $X \rightsquigarrow h_X$ gives a fully faithful embedding $\mathcal{C} \hookrightarrow \mathrm{Psh}(\mathcal{C})$.*

If G is a group object in $\mathcal{C}$, then $h_G(T)$ is naturally a group. Furthermore, if $f : T \to T'$ in $\mathcal{C}$, then $f^* : h_G(T') \to h_G(T)$ is a homomorphism. Hence, $h_G : \mathcal{C} \to \mathrm{Grp}$. The converse holds as well: if you have $G \in \mathcal{C}$ and a lift of $h_G : \mathcal{C} \to \mathrm{Set}$ to $h_G : \mathcal{C} \to \mathrm{Grp}$, then G is a group object.

Remark 5.6. This shows giving G the structure of a group object is equivalent to giving h_G the structure of a group object in the category of presheaves on $\mathcal{C}$ (i.e. category of functors $\mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$). This let's you define group objects even for categories without products. ○

5.1 (Co)kernels

Say $f : G \to H$ is a homomorphism of group objects in $\mathcal{C}$, and let 1 be the trivial group object on $\mathcal{C}$.

Definition 5.7. The **kernel** of f is the equializer of $G \underset{1}{\overset{f}{\rightrightarrows}} H$, i.e. the fiber product

$$\begin{array}{ccc} \ker f & \longrightarrow & 1 \\ \downarrow & \ulcorner & \downarrow \\ G & \xrightarrow{f} & H \end{array}.$$ ◇

Definition 5.8. The **cokernel** of f is the coequalizer of $G \underset{1}{\overset{f}{\rightrightarrows}} H$. ◇

Remark 5.9. $h_{\ker f}(T) = \ker(f : G(T) \to H(T))$. However, understanding the functor the cokernel represents is less straightforward (since the cokernel is defined in terms of maps out of it). ○

Warning 5.10. In particular, one does not have $h_{\operatorname{coker} f}(T) = \operatorname{coker}(G(T) \to H(T))$. •

5.2 Group schemes

Definition 5.11. A **group scheme** over S is a group object in the category Sch_S of schemes over S. ◇

Example. An abelian variety is a group scheme which is a proper variety. △

Assumption. Let's work over a field k.

Recall 5.12. The category of affine schemes over k is anti-equivalent to the category of k-algebras. ⊙

Hence, affine group schemes should be anti-equivalent to co-group k-algebras.

Example. Say $G = \operatorname{Spec} A$ is a group object. Then,

- multiplication $G \times G \to G \rightsquigarrow$ comultiplication $\Delta : A \to A \otimes A$
- identity $\operatorname{Spec} k \to G \rightsquigarrow$ counit $A \to k$
- inverse $G \to G \rightsquigarrow$ antipode $A \to A$

This gives A the structure of a Hopf algebra. △

Definition 5.13. A **Hopf algebra** over k is a k-vector space A with the following data:

- multiplication $m : A \otimes A \to A$
- unit $e : k \to A$
- comultiplication $\Delta : A \to A \otimes A$
- counit $\eta : A \to k$
- antipode $i : A \to A$

satisfying the expected axioms. This perspective shows that the data is symmetric w.r.t. to flipping all the arrows. ◇

Corollary 5.14. *There's an anti-equivalence of categories*

$$\left\{\begin{array}{c}\textit{affine group schemes}\\ \textit{over } k\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{commutative Hopf algebras}\\ \textit{over } k\end{array}\right\}.$$

Commutativity of a group scheme corresponds to cocommutativity of the associated Hopf algebra.

Example. Below, $T = \operatorname{Spec} R$

- **additive group** $\mathbb{G}_a = \operatorname{Spec} k[t]$ represents the functor

$$\mathbb{G}_a(T) = R$$

(with additive group law). In terms of the Hopf algebra, the comultiplication map $\Delta : k[t] \to k[t] \otimes k[t]$ sends $t \mapsto t \otimes 1 + 1 \otimes t$. Note that $t^2 \mapsto (t \otimes 1 + 1 \otimes t)^2$, *not* to $t^2 \otimes 1 + 1 \otimes t^2$

- **multiplicative group** $\mathbb{G}_m = \operatorname{Spec} k[t, t^{-1}]$ has functor of points

$$\mathbb{G}_m(T) = R^\times$$

(with multiplicative group law). Here, comultiplication is

$$\begin{array}{rccc} \Delta : & k[t,t^{-1}] & \longrightarrow & k[t,t^{-1}] \otimes_k k[t,t^{-1}] \\ & t & \longmapsto & t \otimes t. \end{array}$$

- For G an abstract group, we get the **constant group scheme** $\underline{G} = \bigsqcup_{x \in G} \operatorname{Spec} k$. Note that

$$\operatorname{Hom}(T, \underline{G}) = \operatorname{Hom}(\pi_0(T), G),$$

where $\pi_0(T)$ is the set of connected components of T. Note that $\underline{G} = \operatorname{Spec} A$ where $A = \operatorname{Map}(G, k)$. Hence, $A \otimes A = \operatorname{Map}(G \times G, k)$ and we have comultiplication $\Delta : \operatorname{Map}(G, k) \to \operatorname{Map}(G \times G, k)$ given by $(\Delta f)(x, y) = f(xy)$.

Warning 5.15. This A is different from the group algebra $k[G]$. For example, $\operatorname{Fun}(G, k)$ is always commutative, while $k[G]$ is iff G is. •

- n**th roots of unity** $\mu_n = \operatorname{Spec} k[t]/(t^n - 1)$ has functor of points

$$\mu_n(T) = \{x \in R : x^n = 1\}.$$

Note $\mu_n = \ker\left(\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m\right)$.

- Assume $\operatorname{char} k = p$. Get a group scheme $\alpha_p = \operatorname{Spec} k[t]/(t^p)$ with functor of points

$$\alpha_p(T) = \{x \in R : x^p = 0\}.$$

This is a group under addition, and $\alpha_p = \ker\left(\mathbb{G}_a \xrightarrow{F_p} \mathbb{G}_a\right)$. △

For the rest of the lecture, we'll be interested in finite (in the sense of scheme theory) group schemes.

Definition 5.16. Let G be a finite k-group scheme (i.e. its coordinate ring A is f.d. over k). It's **order** is $\#G := \dim_k(A)$. ◇

Theorem 5.17 (Grothendieck)**.** *Let G be a finite commutative k-group scheme, and let $H \subset G$ be a closed subgroup. Then,*

(1) *The (categorical) quotient G/H exists and is itself a finite (commutative) k-group scheme.*

(2) $\#(G/H) = (\#G)/(\#H)$.

(3) $h_{G/H}$ *is the quotient of* h_G *by* h_H *as sheaves on the fppf site of* k.

Remark 5.18. Cokernels existing in this category is the same as kernels existing in the category of Hopf algebras, so **(1)** above is not hard to prove. ∘

Corollary 5.19. *The category of finite commutative group schemes is abelian.*

5.3 Étale group schemes

Recall 5.20. Let A be a finite dimensional k-algebra. Then, A is **étale** over k iff it is a finite product of separable fields extensions of k. If $\operatorname{char} k = 0$, this is equivalent to A being reduced. ⊙

Suppose A is a f.d. étale k-algebra, and let k^S be the separable closure of k. Then,

$$A \otimes_k k^s = \prod_{x \in I} k^S.$$

Furthermore, there will be a Galois action $G_k \curvearrowright I$, and so we have a functor

$$\{\text{finite étale algebras}\} \xrightarrow{\Phi} \{\text{finite } G_k\text{-sets}\}.$$

One can go backwards. If I is a finite G_k-set, one can define the étale k-algebra

$$A = \left(\prod_I k^s \right)^{G_k}.$$

This gives a functor

$$\{\text{finite étale algebras}\} \xleftarrow{\Psi} \{\text{finite } G_k\text{-sets}\}$$

in the opposite direction.

Theorem 5.21. Φ, Ψ *are quasi-inverse equivalences of categories.*

Proof. Exercise. ■

Corollary 5.22. *The functor*

$$\begin{array}{ccc} \{\textit{fin ét schemes}/k\} & \longrightarrow & \{\textit{fin. } G_k\textit{-sets}\} \\ X & \longmapsto & X(k^s) \end{array}$$

is an equivalence.

Corollary 5.23. *There's an equivalence of categories*

$$\left\{ \begin{array}{c} \textit{fin ét commutative} \\ \textit{group schemes}/k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite} \\ G_k\textit{-modules} \end{array} \right\}.$$

Definition 5.24. Let $G = \operatorname{Spec} A$ be a finite commutative group scheme. A in an Artinian algebra and so $A = \prod_{i \in I} A_i$ with each A_i a local Artinian algebra. There is a unique $0 \in I$ s.t. the counit of A factors through A_0. We call $G^\circ := \operatorname{Spec} A_0 \subset G$ the **identity component** of G. ◇

Remark 5.25. G° is connected (Spec of a local ring) and has a k-point (given by counit). Hence, G° is geometrically connected, so $G^\circ \times G^\circ$ is still connected. Hence, G° will be a subgroup of G. ∘

Definition 5.26. Let $A_{\text{ét}}$ be the maximal étale subalgebra of A. Concretely, $A_{\text{ét}} = \prod_i (A_i)_{\text{ét}}$, where $(A_i)_{\text{ét}}$ is the separable closure of k in A_i. Let $G^{\text{ét}} := \operatorname{Spec}(A_{\text{ét}})$, so we have a natural map $G \to G^{\text{ét}}$. One can show that this is the universal homomorphism to an étale group scheme. In particular, $G^{\text{ét}}$ will be a quotient group of G. ⋄

Consider the tensor product $A \otimes_{A_{\text{ét}}} k$. This will be the maximal quotient of A where the idempotent defining A_0 is the identity element. Using this, one can show that $A \otimes_{A_{\text{ét}}} k \simeq A_0$. Geometrically, the sequence

$$1 \longrightarrow G^\circ \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 1$$

is exact. This is the **connected-étale sequence**.

Remark 5.27. Suppose that k is perfect (every finite extension separable). Then, $(A_i)_{\text{ét}}$ is the algebraic closure of k in A_i, and so maps isomorphically onto its residue field. So one gets an isomorphism $G_{\text{red}} \xrightarrow{\sim} G^{\text{ét}}$. Since k is perfect, the product of two reduced schemes is reduced, so G_{red} will be a subgroup. This splits the connected-étale sequence, i.e. $G \simeq G^\circ \times G^{\text{ét}}$. Furthermore, there are no nontrivial maps from an étale scheme to a connected scheme, so this splitting is unique. ∘

Example (a non-split connected-étale sequence)**.** let X be some moduli space of elliptic curves over $\mathbb{F}_p$ (e.g. $X_0(N)$). Let $\mathcal{E} \to X$ be the universal elliptic curve over X, and let $k = \mathbb{F}_p(X)$ be the function field of X. Let $E = \mathcal{E}_k$ be the generic fiber of this family, and let $G_n = E[p^n]$.

- E is not defined over $\overline{\mathbb{F}}_p$, and so E is ordinary.

  The j-invariant defines a morphism $j : X \to \mathbb{P}^1$ which is non-constant. Hence, $j \in k$ is transcendental over $\mathbb{F}_p$, but by definition $j = j(E)$. Supersingular curves are always defined over $\mathbb{F}_{p^2}$.

- Since E is ordinary, $G_n(\overline{k}) \neq 0$, so $G_n^{\text{ét}} \neq 0$.

- G_n is not reduced (since it has p-torsion), so it's not étale so $G_n^\circ \neq 0$.

- The sequence $1 \to G_n^\circ \to G_n \to G_n^{\text{ét}} \to 1$ is not split if $n \gg 0$.

  Suppose not, i.e. $G_n = G_n^\circ \times G_n^{\text{ét}}$ for all n. Take unions $G_\infty = G_\infty^\circ \times G_\infty^{\text{ét}}$. Both pieces will be p-divisible, so $\operatorname{End}(G_\infty) = \mathbb{Z}_p \oplus \mathbb{Z}_p$. It's known that the map

  $$\operatorname{End}(E) \otimes \mathbb{Z}_p \to \operatorname{End}(G_\infty)$$

  is an isomorphism, but this forces $\operatorname{rank} \operatorname{End}(E) = 2$, so E is CM. However, CM curves are defined over $\overline{\mathbb{F}}_p$,[6] a contradiction. △

Question: Why does this imply that it's not reduced?

Answer: Multiplication by p (or p^r) is not separable, so Frobenius factors through it. Hence, the kernel of Frobenius is a subgroup of G_n

We'll end with one last fact for the day: if $\operatorname{char} k \nmid \#G$, then G is étale.

Let $G = \operatorname{Spec} A$ be a finite connected (i.e. A local) commuative group scheme over k. Let $I \subset A$ be the kernel of the counit $A \to k$, so $A = k \oplus I$. Consider the projection $\pi : A \to I/I^2$.

[6] If you fix an order, there are only finitely many things CM by that order, so a Galois argument should descend you down to $\overline{\mathbb{F}}_p$

Exercise. π is a derivation.

Let $x_1, \dots, x_n \in I$ be elements projecting to a basis for I/I^2. Define $D_i : A \to A$ as the composition

$$D_i : A \xrightarrow{\Delta} A \otimes A \xrightarrow{\mathrm{id} \otimes \pi} A \otimes I/I^2 \xrightarrow{\mathrm{id} \otimes x_i^\vee} k$$

where $x_1^\vee, \dots, x_n^\vee$ give the dual basis to $x_1, \dots, x_n$.

Proposition 5.28.

(a) *If* $\operatorname{char} k = 0$, $\varphi : k[x_1, \dots, x_n] \to A$ *is an isomorphism.*

(b) *If* $\operatorname{char} k = p$ *and* $x_i^p = 0$ *for all* i, *then*

$$\varphi : k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p) \to A$$

is an isomorphism.

Proof. Nakayama ($+$ $A \simeq k \oplus I$) implies that φ is surjective. For injectivity, one uses that $\varphi \frac{\partial}{\partial x_i} = D_i \varphi$ (derivations agreeing on the generators x_j). As a consequence, the kernel of φ is stable by $\frac{\partial}{\partial x_i}$. Try to think of ideals in a polynomial ring which are stable by derivative. If $\operatorname{char} k = 0$, taking the derivative of a generator will get you something of lower degree, so the only ones are (0) and (1). If $\operatorname{char} k = p$, there's the issue that $\frac{\partial}{\partial x_i} x_i^p = 0$, but we've killed x_i^p in **(b)**. Thus, in either case, we must have $\ker \varphi = (0)$. ■

Corollary 5.29. *If* $\operatorname{char} k = 0$, *then* G *is trivial.*

Proof. A is a finite dimensional polynomial ring, so $A = k$ (i.e. $n = 0$) ■

Corollary 5.30. *If* $\operatorname{char}(k) = p$, *then* $\#G$ *is a power of* p.

Proof. Let $G_1 = \ker\left(G \xrightarrow{F_p} G^{(p)}\right)$ be the kernel of Frobenius, and let $G_2 = G/G_1$. We can apply **(b)** to G_1, so $G_1 = \operatorname{Spec} k[x_i]/(x_i^p)$ which means $\#G_1 = p^n$. Now, apply induction to G_2. ■

Theorem 5.31. *Let* $G = \operatorname{Spec} A$ *be a finite commutative* k*-group scheme. If* $\#G$ *is invertible in* k, *then* G *is étale.*

Look at the étale-connected sequence, and apply the above observations.

6 Lecture 6: Group schemes 2

Fix some base field k.

6.1 Cartier duality

Let $G = \operatorname{Spec} A$ be a finite, commutative k-group scheme. Recall that A is a commutative and cocommutative Hopf algebra. Let $A^\vee = \operatorname{Hom}_{\mathrm{Vect}_k}(A, k)$ be the k-linear dual. This is still a commutative and cocommutative Hopf algebra.

Definition 6.1. The **Cartier dual** of G is $G^\vee := \operatorname{Spec}(A^\vee)$. ◇

Note that $\#G = \#G^\vee$ and $(G^\vee)^\vee \simeq G$.

Let's describe the functor of points of $G^\vee$. Let R be a k-algebra. Then, a k-algebra map $A^\vee \to R$ is an R-algebra map $A_R^\vee \to R$ is an R-coalgebra map $R \to A_R$ is a choice of element $x \in A_R$ (the image of 1) s.t. $\Delta x = x \otimes x$ and $\eta x = 1$ (Δ the comultiplication and η the counit).

Recall 6.2. One of the axioms of a Hopf algebra says that $m(1 \otimes i)\Delta = \eta$. ⊙

Applying this to x above, we see that

$$1 = \eta(x) = m(1 \otimes i)\Delta(x) = x \cdot i(x),$$

so $x \in A_R^\times$ is a unit. Returning to our description of the functor of points of $G^\vee$, choosing this $x \in A_R^\times$ is the same as giving a map $R[t, t^{-1}] \to A_R$ of Hopf algebras over R. All in all, we have arrived at the following:

Proposition 6.3. *$G^\vee(R) = \mathrm{Hom}(G_R, (\mathbb{G}_m)_R)$, i.e. $G^\vee = \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$.*

"The R-points of $G^\vee$ are the characters of G defined over R."

Example. Say $G = \underline{\mathbb{Z}/r\mathbb{Z}}$, the constant group scheme, so $A = \prod_{i \in \mathbb{Z}/r\mathbb{Z}} k e_i$. Multiplication here is determined by $e_i e_j = \delta_{ij} e_i$ while comultiplication is given by

$$\Delta e_n = \sum_{i+j=n} e_i \otimes e_j.$$

Let $e_i^\vee$ be the dual basis of $A^\vee$. Multiplication is defined so that

$$A \xrightarrow[\Delta]{} A \otimes A \xrightarrow[e_i^\vee \otimes e_j^\vee]{} k, \qquad A \xrightarrow{e_i^\vee e_j^\vee} k$$

commutes, i.e.

$$(e_i^\vee e_j^\vee)(e_n) = (e_i^\vee \otimes e_j^\vee)(\Delta e_n) = \delta_{(i+j),n} \implies e_i^\vee e_j^\vee = e_{i+j}^\vee.$$

Similarly, comultiplication is defined so that

$$A \otimes A \xrightarrow[m]{} A \xrightarrow[e_n^\vee]{} k, \qquad A \otimes A \xrightarrow{\Delta(e_n^\vee)} k$$

commutes, i.e.

$$\Delta(e_n^\vee)(e_i \otimes e_j) = e_n^\vee(e_i e_j) = \delta_{ij}\delta_{jn} \implies \Delta e_n^\vee = e_n^\vee \otimes e_n^\vee.$$

We see from this that the map $A^\vee \to k[t]/(t^r - 1)$ sending $e_i^\vee \mapsto t^i$ is an isomorphism of Hopf algebras, i.e.

$$(\mathbb{Z}/r\mathbb{Z})^\vee \simeq \mu_r.$$

You can alternatively see this directly from the functor of points perspective. △

Example (exercise)**.** If $G = \alpha_p$, one can compute that $G^\vee = \alpha_p$ as well. △

Last time we broke group schemes into two pieces: connected (= local) and étale ones. By looking at G and $G^\vee$, we get 4 possibilities:

(the first words refers to G and the second to $G^\vee$)

- local-local

  Example. α_p △

- local-étale

  Example. μ_p △

- étale-local

  Example. $\mathbb{Z}/p\mathbb{Z}$ △

- étale-étale

  Example. $\mathbb{Z}/\ell\mathbb{Z}$ with $\ell \neq p$ △

Note above only in positive characteristic. In characteristic 0, everything is étale.

Remark 6.4. If k is perfect, one gets a splitting $G = G_{ll} \times G_{le} \times G_{el} \times G_{ee}$. ◦

6.2 Frobenius + Verschiebung

Definition 6.5. Let $G = \operatorname{Spec} A$, and let σ be the pth power map (on any ring of characteristic p). Given $\alpha \in k$ and $x \in A$, we have $\sigma(\alpha x) = \sigma(\alpha)\sigma(x)$, so σ is not quite a ring homomorphism. To fix this, we define

$$A^{(p)} := A \otimes_{k,\sigma} k,$$

so $x\alpha \otimes \beta = x \otimes \alpha^p \beta$ in $A^{(p)}$. Thus,

$$\begin{array}{rccc} F_p: & A^{(p)} & \longrightarrow & A \\ & x \otimes \alpha & \longmapsto & x^p \alpha \end{array}$$

is a k-algebra homomorphism, called **Frobenius**. Naturality implies that the induced $F_p : G \to G^{(p)}$ will be a group homomorphism. ◇

If $q = p^r$, we also have $F_q = F_p^r : G \to G^{(q)}$.

Proposition 6.6. *Let G be a finite commutative group scheme. Then,*

(1) *G is étale $\iff$ F_p is an isomorphism.*

(2) *G is connected $\iff$ $F_q = 0$ for some q.*

Proof. **(2)** First suppose $G = \operatorname{Spec} A$ is connected. Then, A is a local Artinian ring, so its maximal ideal is nilpotent. If q is big, Frobenius will map every non-unit of $A^{(q)}$ to 0, so $F_q : G \to G^{(q)}$ is the 0 morphism for $q \gg 0$. Conversely, the map $F_q : G(\overline{k}) \xrightarrow{\sim} G^{(q)}(\overline{k})$ is always an isomorphism (exercise: check this). If $F_q = 0$, then $G(\overline{k}) = 0$, so $G^{\text{ét}} = 0$, so $G = G^\circ$.

(1) If F_p is an isomorphism, then F_p is an isomorphism on G°, so $F_q = 0$ is an isomorphism on G° for $q \gg 0$, so $G^\circ = 0$. Hence, G is étale. ■

Definition 6.7. The **Verschiebung** is the Cartier dual of Frobenius $F_p : G^\vee \to (G^\vee)^{(p)}$, so it is a map $V_p : G^{(p)} \to G$. ◇

Exercise. $F_pV_p = [p] : G^{(p)} \to G^{(p)}$ and $V_pF_p = [p] : G \to G$.

6.3 Classification in height 1

Let $G = \operatorname{Spec} A$ connected, so $A = k \oplus I$ with $I = \ker \eta$ its maximal ideal. Write

$$L(G) = \operatorname{Lie}(G) = \left(I/I^2\right)^\vee.$$

Remark 6.8. For connected groups in characteristic 0, the Lie algebra remembers basically everything. Here, G is commutative so there's no bracket. Hence, it only knows the dimension, so it doesn't remember very much. ○

However, in characteristic p, there is an additional structure on the Lie algebra.

Definition 6.9. A k-linear derivation $D : A \to A$ is **invariant** if

$$\Delta D = (D \otimes 1)\Delta.$$ ◇

Given $v \in L(G)$, can build a map $A \to A$ as the composition

$$D_v : A \xrightarrow{\Delta} A \otimes A \xrightarrow{1\otimes\pi} A \otimes I/I^2 \xrightarrow{1\otimes v} A.$$

Fact. $v \mapsto D_v$ is an isomorphism $L(G) \to \{\text{invariant derivations}\}$.

Suppose $D : A \to A$ is an derivation. Then,

$$D^n(xy) = \sum_{i+j=n} \binom{n}{i} (D^i x)(D^j y).$$

If $n = p$, most of these coefficients vanish, so

$$D^p(xy) = xD^p y + yD^p x,$$

i.e. D^p is a derivation. Thus, we get a map

$$\begin{array}{rccc} F: & L(G) & \longrightarrow & L(G) \\ & D & \longmapsto & D^p. \end{array}$$

Note that $F(aD) = a^pF(D)$ when $a \in k$.

Definition 6.10. An **F-module** is a k-vector space L equipped with an additive map F satisfying $F(av) = a^pF(v)$ for all $a \in k$ and $v \in V$. ◇

Example. Say $G = \alpha_p$ so $A = k[t]/(t^p)$. An example of an invariant derivation is $D = \frac{\partial}{\partial t}$, i.e. $\Delta D = (1 \otimes D)\Delta$. Can check this just on the generator:

$$\Delta Dt = 1 \otimes 1 = (1 \otimes D)(t \otimes 1 + 1 \otimes t) = (1 \otimes D)\Delta t.$$

Furthermore, $D^p = 0$. Hence, $L(G) = k$ with $F = 0$. $\triangle$

Example. Say $G = \mu_p$ so $A = k[t]/(t^p - 1)$. Then, $D = t\frac{\partial}{\partial t}$ is an invariant derivation, and $D^p = D$ in this case (since $Dt = t$). Hence, $L(G) = k$ and F is the pth power map. $\triangle$

Warning 6.11. We see from the above examples that this extra structure let's us distinguish μ_p from α_p. However, it's not a complete invariant. For one thing, $L(G) = 0$ if G is étale. Also, a non-isomorphism of groups can induce an isomorphism on tangent spaces, e.g. $\mu_{p^2} \to \mu_p$ induces an isomorphism on $L(G)$'s. •

Definition 6.12. We say G is **height 1** if it's connected and $F_p = 0$. $\diamond$

Theorem 6.13. *$G \mapsto L(G)$ is an equivalence of categories*

$$\{\textit{height 1 group schemes}\} \longleftrightarrow \{\textit{f.d. } F\textit{-modules}\}.$$

Proof idea. We'll give the functor in the opposite direction. Say L is an F-module. Then, we set

$$A := \mathrm{Sym}^*(L)/\left(x^p - F(x) : x \in L\right).$$

This will be a f.d. k-algebra and we give it comultiplication $\Delta : A \to A \otimes A$ sending $x \mapsto x \otimes 1 + 1 \otimes x$ for all $x \in L$. Then we send $L \mapsto \mathrm{Spec}(A^\vee)$. ■

(Details in Mumford's book on Abelian varieties)

Theorem 6.14. *Assume $k = \overline{k}$ and $\operatorname{char} k = p$. Then, $L(\alpha_p)$ and $L(\mu_p)$ are the only simple objects in the category of f.d. F-modules.*

Proof. Let L be some F-module. If there is some nonzero $x \in L$ with $Fx = 0$, then $kx \subset L$ is an F-submodule isomorphic to $L(\alpha_p)$. Now suppose no such x exists. Let $e_1, \ldots, e_n$ be a k-basis of L. Write

$$F(e_i) = \sum_{i,j} C_{ij} e_j$$

and let $C = (c_{ij})_{i,j} \in M_n(k)$. Note that

$$x = \sum_{i=1}^n a_i e_i \implies Fx = \sum_{i,j=1}^n a_i^p C_{ij} e_j.$$

That is, if $x \leftrightarrow v = (a_i)$, then $Fx \leftrightarrow Cv^p$ (where v^p is take coordinate-wise pth powers). From this, we deduce $\det(C) \neq 0$ (if $Cv = 0$, the $Fx = 0$ where $x \leftrightarrow v^{1/p}$, which exists since $k = \overline{k}$). To find a copy of $L(\mu_p)$, we'll want to find an element fixed by F. Elements fixed by F correspond to v with $v = Cv^p$, i.e. $v^p = C^{-1}v$. So we want $v = (a_1, \ldots, a_n)$ so that

$$a_i^p = \sum \left(C^{-1}\right)_{ij} a_j.$$

To find such a thing, we define

$$R := k[x_i] \Big/ \left(x_i^p = \sum_j \left(C^{-1}\right)_{i,j} x_j \right),$$

so that F-fixed vectors correspond to k-points of $\operatorname{Spec} R$. Note that $\dim_k(R) = p^n$ and that $\Omega^1_{R/k} = 0$,[7] so $\operatorname{Spec} R$ is finite étale over k and has exactly p^n points over $k = \overline{k}$. Thus, $\dim_{\mathbb{F}_p}\left(L^{F=1}\right) = n = \dim_k(L)$. From this, one can check that the natural map $L^{F=1} \otimes_{\mathbb{F}_p} k \to L$ is injective (apply F to a hypothetical minimal linear dependence), which implies that $L \cong L(\mu_p)^{\oplus n}$. ■

Corollary 6.15. *Assume $k = \overline{k}$. The simple finite commutative group schemes are $\mathbb{Z}/\ell\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}, \mu_p, \alpha_p$.*

Proof. If a group scheme is simple, it is either connected or étale. If it is simple and connected, it must be height 1, and so must be μ_p or α_p. The simple étale group schemes are $\mathbb{Z}/\ell\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$.[8] ■

Corollary 6.16. *G is killed by $\#G$*

(prove by passing to algebraic closure and then inducting up from the simple case. Also, this is not the only proof of this statement).

Remark 6.17. An **F-isomodule** is an F-mod L s.t. $F : L^{(p)} \xrightarrow{\sim} L$ is an isomorphism. The above work shows we have an equivalence of categories

$$\{F\text{-isomods}\} \simeq \left\{G : G_{\overline{k}} = \mu_p^n\right\} \underset{\text{Cartier}}{\simeq} \left\{G : G_{\overline{k}} = (\mathbb{Z}/p\mathbb{Z})^n\right\} = \{G : G \text{ étale and killed by } p\} = \operatorname{Mod}_{\mathbb{F}_p[G_k]}$$

over any field k. Explicitly, this takes an F-isomodule M to $(M \otimes k^s)^{F=1}$ and takes a Galois representation V (killed by p) to $(V \otimes k^s)^{G_k}$. Fontaine generalized this to a description of the category of $\mathbb{Z}_p[G_k]$-modules. ∘

6.4 Dieudonné theory

Let k be a perfect field. Let $W = W(k)$ be the ring of Witt vectors of k.

Example. When $k = \mathbb{F}_q$, $W = \mathscr{O}_K$ is the ring of integers of the unramified extension $K/\mathbb{Q}_p$ with residue field k. In particular, $W(\mathbb{F}_p) \cong \mathbb{Z}_p$. △

The pth power map on k induces an automorphism of W which we'll call

$$\varphi : W \xrightarrow{\sim} W.$$

Definition 6.18. A **Diudonné module** is a W-module M equipped w/ additive maps F, V satisfying $F(\alpha x) = \varphi(\alpha)F(x)$, $V(\alpha x) = \varphi^{-1}(\alpha)V(x)$ and $FV = p = VF$. ◇

Theorem 6.19. *There is an equivalence of categories*

$$\left\{\begin{array}{c}\textit{finite commute } k\textit{-group schemes} \\ \textit{with } p\textit{-power order}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Dieudonné modules of} \\ \textit{finite length over } W\end{array}\right\}.$$

[7] the Jacobian matrix is given by C^{-1}, which is invertible

[8] finite étale commutative group schemes are finite G_k-modules (see Corollary 5.23). Since $k = \overline{k}$, these are finite abelian groups. All simple (finite) abelian groups are cyclic.

Apparently, this (rather, it's extension to finite, flat commutative groups over a general base) was proved by Deligne on the bus going to his year of service in the Belgian army, and the extension to the non-commutative case remains unsolved (except over fields)

At around this point, the recording becomes less useful than before

Notes from here to the end of the

We write $D(G)$ for the Dieudonné module associated to G. The functor D has several nice properties

- D is exact
- The group G is killed by p^n iff $D(G)$ is
- The order of G is equal to p^r, where r is the length of $D(G)$ as a W-module
- G is connected iff F is nilpotent on $D(G)$
- G is étale iff F is an isomorphism on $D(G)$
- $D(G^\vee)$ is naturally the dual of $D(G)$, where the dual of a Dieudonné module M is the W-module $\mathrm{Hom}_W(M, K/W)$ with F, V defined by

  $$(Ff)(x) = \varphi(f(Vx)) \text{ and } (Vf)(x) = \varphi^{-1}(f(Fx)).$$

  Above, $K = \operatorname{Frac} W$.
- If G has height 1, then $D(G)^\vee = L(G)$ (and $V = 0$).

6.5 Applications to abelian varieties

6.5.1 Duality of abelian varieties

We previously showed that if $f : X \to Y$ is an isogeny of complex tori, then $\ker f$ and $\ker(f^\vee)$ are naturally Pontryagin dual groups. This generalizes to arbitrary fields:

Proposition 6.20. *Let $f : A \to B$ be an isogeny of abelian varieties. Then, $\ker(f^\vee)$ is naturally the Cartier dual of $\ker(f)$.*

Proof. Let $G = \ker f$, and apply $\underline{\mathrm{Hom}}(-, \mathbb{G}_m)$ to the short exact sequence

$$0 \to G \to A \to B \to 0$$

of fppf sheaves. This gives

$$\underline{\mathrm{Hom}}(A, \mathbb{G}_m) \to \underline{\mathrm{Hom}}(G, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1(B, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1(A, \mathbb{G}_m).$$

There are no nontrivial maps from an abelian variety (proper) to $\mathbb{G}_m$ (affine), so the first group vanishes, and

$$\underline{\mathrm{Hom}}(G, \mathbb{G}_m) \simeq \ker\left(\underline{\mathrm{Ext}}^1(B, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1(A, \mathbb{G}_m)\right).$$

We've seen previously that $\underline{\mathrm{Hom}}(-, \mathbb{G}_m)$ is Cartier duality for finite commutative group schemes and $\underline{\mathrm{Ext}}^1(-, \mathbb{G}_m)$ is duality for abelian varieties. ∎

(A more elementary proof is given in section 15 of Mumford's "Abelian varieties")

Corollary 6.21. *Let A be an abelian variety. Then, $A[n]$ and $A^\vee[n]$ are Cartier dual. In particular, there is a canonical pairing $A[n] \times A^\vee[n] \to \mu_n$, the **Weil pairing**.*

6.5.2 p-torsion of an elliptic curve

Let E be an elliptic curve over $k = \overline{k}$ of characteristic p. Then, $G = E[p]$ is a finite commutative k-group scheme of order p^2. We will try to describe it more explicitly.

From the start, we know that G is not étale (since $\cdot p : E \to E$ is not étale, e.g. since it induces 0 on tangent spaces). We also know that G is self-Cartier dual (from the existence of the Weil pairing since E is self-dual as an abelian variety).

- Suppose that E is ordinary. Then, $G(k) \neq 0$, so $G^{\text{ét}}$ is non-zero. Thus, $G = G^0 \times G^{\text{ét}}$ with both factors having order p. By the classification of étale groups (Corollary 5.23), we conclude that $G^{\text{ét}} = \mathbb{Z}/p\mathbb{Z}$. Since G is self-dual, G^0 is necessarily the dual of $G^{\text{ét}}$, so $G^0 = \mu_p$. Thus, $G = \mu_p \times \mathbb{Z}/p\mathbb{Z}$.

- Suppose that E is supersingular, so $G(k) = 0$ which means $G^{\text{ét}} = 0$. Thus, $G = G^0$ is local, and so local-local, as it is self-dual. The only simple local-local group is α_p (e.g. by Corollary 6.15), so we must have an extension of the form

$$0 \longrightarrow \alpha_p \longrightarrow G \longrightarrow \alpha_p \longrightarrow 0.$$

  This extension cannot be split since $\alpha_p \oplus \alpha_p$ has a two-dimensional tangent space, but G has a 1-dimensional tangent space. We also cannot have $G = \alpha_{p^2}$ since this group is not self-dual (it has $V = 0$ but $F \neq 0$). Thus, we cannot have $G = \alpha_{p^2}^\vee$ either. Up to isomorphism, there are only four self-extensions of α_p (this follows from Dieudonné theory), so G must be the one we have not yet named. One can describe G as the sum of $\alpha_{p^2}, \alpha_{p^2}^\vee$ in $\text{Ext}^1(\alpha_p, \alpha_p)$, and one can also explicitly describe its Dieudonné module $D(G)$.

  Exercise (Assuming I did this computation correctly when I tried working this out myself). Show that $D(G) \simeq k \oplus k$, and one can choose bases so that $F(x, y) = (0, x^p) = V(x, y)$.

6.5.3 p-torsion of an abelian variety

Let A be an abelian variety over k, and assume k perfect of characteristic p. Write

$$A[p] = G_1 \oplus G_2 \oplus G_3 \text{ and } \#G_1 = p^r, \#G_2 = p^s, \#G_3 = p^t,$$

where G_1 is étale, G_2 is local-étale, and G_3 is local-local.

Note G_1 has to be étale-local since we're looking at p-torsion e.g. since (over $\overline{k}$) the only simple étale-étale groups are $\mathbb{Z}/\ell\mathbb{Z}$ with $\ell \neq p$ (e.g. by Corollary 6.15)

Proposition 6.22. *The numbers r, s, t are isogeny invariants.*

Proof. Decompose $A[p^n] = G_{1,n} \oplus G_{2,n} \oplus G_{3.n}$ as above. Induct over the exact sequence $0 \to A[p] \to A[p^n] \xrightarrow{p} A[p^{n-1}] \to 0$ to see that $G_{i,n}$ is a success extension of G_i's. Hence,

$$\#G_{1,n} = p^{nr}, \ \#G_{2,n} = p^{ns}, \text{ and } \#G_{3,n} = p^{nt}.$$

Now suppose $A \to A'$ is a degree d isogeny. Then, $\#\ker(G_{1,n} \to G'_{1,n}) \leq d$. For $n \gg 0$ this is only possible if $r \leq r'$. By symmetry (i.e. the existence of an isogeny $A' \to A$), we must also have $r' \leq r$, so $r = r'$. One similarly shows $s = s'$ and $t = t'$. ∎

Proposition 6.23. *We have $r = s$ and so $t = 2g - 2r$, where $g = \dim(A)$.*

Proof. By duality + isogeny-invariance, we have $r(A) = s(A^\vee) = s(A)$. ∎

Corollary 6.24. *$A[p](\overline{k}) = (\mathbb{Z}/p\mathbb{Z})^r$ with $r \leq g$.*

Proof. Since $r = s$, we have $2r = r + s \leq 2g$, so $r \leq g$. ∎

6.5.4 The Dieudonné module as a p-adic Tate module

Let A be an abelian variety of dimension g over k, a perfect field of characteristic p. Then, $T_p(A)$, the p-adic Tate module of A, has rank at most g (and possibly even 0). It is therefore much unlike the ℓ-adic Tate modules of A.

We define the Diedonné module of A, denoted $D(A)$, as the inverse limit of the $D(A[p^n])$'s. This $D(A)$ is a free W-module of rank $2g$ equipped with a semi-linear map F, and so looks more like the ℓ-adic Tate modules (note: V note needed since $VF = p$).

Suppose $k = \mathbb{F}_q$ with $q = p^r$. Let $F' = F^r$. Then, F' is a W-linear automorphism of $D(A)$, and so we get something looking even more like the ℓ-adic Tate module. One even has that the eigenvalues of F' are the same as the eigenvalues of Frobenius on the ℓ-adic Tate module.

7 Lecture 7: Raynaud's Theorem

Say $S = \operatorname{Spec} R$ is noetherian. We will consider finite *flat* commutative group schemes over S.

Assumption. If we say 'S-group scheme' in this lecture, assume we mean 'finite flat S-group scheme'.

Here are some facts about these groups (compare to theory over fields from last two lectures):

- They correspond to Hopf algebras over R which are finitely generated projective modules[9]
- The order of the group is the rank of the Hopf algebra (locally constant function on S, so simply a number if S is connected)
- Quotients work: if $H \subset G$ is closed, then G/H exists and is finite flat
- There's an equivalence of categories when S connected

$$\left\{\begin{array}{c}\text{finite étale} \\ \text{commutative } S\text{-group schemes}\end{array}\right\} \longleftrightarrow \left\{\text{finite } \pi_1^{\text{ét}}(S, \overline{s})\text{-modules}\right\},$$

  where $\overline{s}$ is a geometric point of S. This is more-or-less tautological.

  Remark 7.1. If $R = \mathscr{O}_K$ is the ring of integers of $K/\mathbb{Q}_p$, then $\pi_1^{\text{ét}} = \operatorname{Gal}(K^{un}/K)$. ∘

- If R is local + henselian, then we get a connected-étale sequence.

  If $G = \operatorname{Spec} A$, then $A = \prod A_i$ with A_i local. We let $G^0 = \operatorname{Spec}(A_j)$ be the identity component, and $G^{\text{ét}} = G/G^0$.

- Cartier duality works

Remember: The connected-étale sequence does *not* exist over arbitrary bases

[9] A finitely presented flat module over a noetherian ring is projective, see e.g. here

Our goal today is to prove Raynaud's theorem.

Setup 7.2. Let $K/\mathbb{Q}_p$ be a finite extension, let $R = \mathscr{O}_K$ with ramification index e and residue field k.

Theorem 7.3 (Raynaud)**.** *Suppose $e < p-1$. Let G, G' be finite flat commutative R-group schemes which are isomorphic over K. Then, they're isomorphic over R.*

Warning 7.4. This is false if $e \geq p-1$. For example, take $K = \mathbb{Q}_p(\mu_p)$. Then, $\mathbb{Z}/p\mathbb{Z}$ and μ_p are isomorphic over K, but not over R (e.g. since they are not isomorphic over the special fiber $\mathbb{F}_p$). •

The strategy is the reduce to the simple case, classify the simple groups, and then check the theorem holds for them by hand.

7.1 Prolongations

Definition 7.5. Let G_0/K be a group. A **prolongation** is some G/R s.t. $G_K \cong G_0$. ◇

Say $G_0 = \mathrm{Spec}(A_0)$ with A_0 a f.g. K-algebra, and say $G = \mathrm{Spec}\, A$ is a prolongation. Then, $A \subset A_0$ is an R-subalgebra. In fact,

Fact. Prolongations of G_0 correspond to R-subalgebras $A \subset A_0$ s.t.

- A is f.g. over R
- A spans A_0 over K
- A is closed under Δ

We partially order prolongations using inclusion of the corresponding R-subalgebras of A_0.

Proposition 7.6. *Any two prolongations of G_0 have both an inf and a sup.*

Proof. Say $A, A' \subset A_0$ are prolongations. Their sup is simple AA' (b/y $\supset$ obvious and AA' closed under Δ). Now, the inf exists by Cartier duality; the prolongations of G_0 are in order-reversing bijection with those of $G_0^\vee$. ■

Proposition 7.7. *If G_0 has a prolongations, then it has a maximal one G^+ and a minimal one G^-.*

Proof. Say $G_0 = \mathrm{Spec}\, A_0$ with A_0 a finite étale K-algebra, so it has some maximal order O. If A is a prolongation, then $A \subset O$. Furthermore, A, O are both lattices for A_0, so A is finite index in O. Hence, the prolongations satisfy acc which forces there to exists a maximal one. A minimal exists by Cartier duality. ■

$K/\mathbb{Q}_p$ is characteristic 0

Definition 7.8. Say G_0 satisfies **property UP** (unique prolongation) if any two prolongations are isomorphism. ◇

Raynaud's theorem says everything satisfies UP.

Remark 7.9. G_0 satisfies UP $\iff$ the natural $G^+ \to G^-$ is an isomorphism. Note this is something which can be checked after passing to an extension. ○

Say we have a short exact sequence

$$0 \longrightarrow G_0' \longrightarrow G_0 \longrightarrow G_0'' \longrightarrow 0$$

over the generic fiber. Let G be a prolongation of G_0.

Exercise. $G' :=$ the scheme-theoretic closure of G_0' in G is a prolongation of G_0'.

Then, $G'' = G/G_0'$ is a prolongation of G_0''.

Now suppose H is a second prolongation of G_0 with a map $G \to H$. Then we get maps $G' \to H'$ and $G'' \to H''$ as well. That is, we get a morphism of short eaxct sequence:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H' & \longrightarrow & H & \longrightarrow & H'' & \longrightarrow & 0 \end{array}$$

In particular, if the outer two (vertical) maps are isomorphisms, then the middle one is as well.

Proposition 7.10. *If G_0', G_0'' satisfy UP then so does G_0.*

(apply above discussion to the map $G^+ \to G^-$)

This let's us reduce to the case of simple objects.

Slogan. If you have a simple object is some abelian category, you can think of it as a module over its endomorphism ring.

Suppose G_0/K is simple. It corresponds to the Galois representation $V = G_0(\overline{K})$ which will be an irreducible representation of $G_K/\mathbb{F}_p$.

Assumption. All the group schemes today have p-power order. The other ones are étale and so simpler.

Let $\mathbb{F} := \mathrm{End}_{G_K}(V)$. This is a division algebra over $\mathbb{F}_p$ and so actually a finite extension of $\mathbb{F}_p$. Now, V is an absolutely irreducible $\mathbb{F}$-linear representation of G_K.

Assumption. Now assume $k = \overline{k}$, the residue field is algebraically closed.

In this case, G_K is like an inertia group and so splits up as

$$1 \longrightarrow I^w \longrightarrow G_K \longrightarrow I^t \longrightarrow 1$$

with I^w the wild inertia, a pro-p group, and I^t the tame inertia, an abelian group.

Fact. I^w is a pro-p group acting on a nonzero $\mathbb{F}_p$-vector space V, so it must fix a vector, i.e. $V^{I^w} \neq 0$.

Since V^{I^w} is a nonzero subrep of V (as $I^w \triangleleft G_K$), we must have $V = V^{I^w}$, i.e. V is really an irreducible representation (over $\mathbb{F}$) of the abelian group I^t. This forces $\dim_{\mathbb{F}} V = 1$.

I think the main point should be to apply Burnside's lemma and use the fact that $0 \in V$ gives an orbit of size 1

Definition 7.11. An **$\mathbb{F}$-module scheme** is a group scheme G (over K or R) equipped with a ring homomorphism $\mathbb{F} \to \mathrm{End}(G)$. It is a **Raynaud $\mathbb{F}$-module scheme** if $\#G = \#\mathbb{F}$, i.e. $\dim_{\mathbb{F}} G(\overline{K}) = 1$. $\diamond$

Above, we showed the following.

Proposition 7.12. *If $k = \overline{k}$, then any simple group over K is a Raynaud $\mathbb{F}$-module scheme (for some $\mathbb{F}$).*

Corollary 7.13. *If all Raynaud $\mathbb{F}$-module schemes over K^{un} satisfy UP, then all groups over K satisfy UP.*

7.2 $\mathbb{F}$-module schemes

Setup 7.14. Fix some finite field $\mathbb{F}$ of size $q = p^r$. Assume, there eixsts an embedding $\mathbb{F} \hookrightarrow k$.

Definition 7.15. A character $\chi : \mathbb{F}^\times \to R^\times$ is called **fundamental** if the composition

$$\mathbb{F}^\times \xrightarrow{\chi} R^\times \to k^\times$$

extends to a field homomorphism. ◇

Two facts

- Fundamental characters exist
- If χ is a fundamental character, then all other fundamental characters are of the form χ^{p^k} for some $k \in \mathbb{Z}$.

Let $\{\chi_i\}_{i\in\mathcal{I}}$ be the set of all fundamental characters, and define $i+1$ by the relation $\chi_i^p = \chi_{i+1}$. This make $\mathcal{I}$ a $\mathbb{Z}/r\mathbb{Z}$ torsor (recall $q = p^r$).

If $\mu : F^\times \to R^\times$ is any character, there exists a unique expression

$$\mu = \prod_{i\in\mathcal{I}} \chi_i^{\mu(i)} \text{ where } \mu(i) \in \mathbb{Z} \text{ and } 0 \le \mu(i) \le p-1$$

(not all $\mu(i) = 0$).

Say $G = \operatorname{Spec} A$ is an Raynaud $\mathbb{F}$-scheme over R. We want to completely understand A (e.g. write it in terms of generators and relations). To do this, we observe that $\mathbb{F}^\times$ acts on A, so we can decompose it under this action. First write $A = R \oplus I$ with I the augmentation ideal, and note $F^\times \curvearrowright I$. $\#\mathbb{F}^\times = q-1$ is invertible in R, so we can decompose I into a sum of irreducibles. Since the residue field contains an embedding of $\mathbb{F}$, all the irreducible of $F^\times$ will be 1-dimensional characters (all the characters exist over R), so

$$I = \bigoplus_\mu I_\mu \text{ where } I_\mu = \left\{x \in I : [t]x = \mu(t)x \text{ for all } t \in \mathbb{F}^\times\right\}.$$

Above, $[t] : A \to A$ is the map induced by $t \in \mathbb{F}$.

Note $G_{\overline{K}}$ is a 1-dimensional $\mathbb{F}$-module scheme over $\overline{K}$, so it has to be the constant group scheme on $\mathbb{F}$, i.e. $G_{\overline{K}} = \underline{\mathbb{F}}$. Hence, there is an isomorphism $A_{\overline{K}} \cong \operatorname{Map}(\mathbb{F}, \overline{K})$. In particular, for a character $\mu : F^\times \to \overline{K}^\times$, we'll write $\varepsilon_\mu : \mathbb{F} \to \overline{K}$ for the function extending μ by 0. Note this is an element of $A_{\overline{K}}$. Furthermore,

$$I_\mu \otimes_R \overline{K} = \overline{K}\varepsilon_\mu,$$

so I_μ is rank 1 over R for all μ. Let X_i be a generator of I_{χ_i} as an R-module (recall χ_i is a fundamental character).

Notation 7.16. For a character $\mu = \prod \chi_i^{\mu(i)}$, we define

$$X^\mu := \prod_i X_i^{\mu(i)}.$$

Note that the X_i's generate I as an R-algebra iff the X^μ's span I as an R-module.

Let $B = \mathrm{Hom}_R(A, R)$ be the Cartier dual. Note that there's an isomorphism $B_{\overline{K}} \cong \overline{K}[\mathbb{F}]$ between $B_{\overline{K}}$ and the group algebra on $\mathbb{F}$. For $t \in \mathbb{F}$, we'll write $[t] \in B_{\overline{K}}$. Let J be the augmentation ideal of B, and we decompose $J = \bigoplus_\mu J_\mu$. We can give generators after tensoring up to $\overline{K}$

- If $\mu \neq 1$, then $J_\mu \otimes_R \overline{K}$ is spanned by

$$e_\mu = \frac{1}{q-1} \sum_{t \in \mathbb{F}^\times} \mu^{-1}(t)[t].$$

- If $\mu = 1$, then $J_\mu \otimes_R \overline{K}$ is spanned by

$$-1 + \frac{1}{q-1} \sum_{t \in \mathbb{F}^\times} [t]$$

(note coefficients need to add to 0 to land in augemntation ideal)

Note $I_{\overline{K}}$ and $J_{\overline{K}}$ are dual vector spaces, and the ε_μ,e_μ's are dual bases (exercise). Write $\varepsilon_i := \varepsilon_{\chi_i}$. This generates I_{χ_i}, so we can write

$$X_i = c_i \varepsilon_i \text{ for some } c_i \in \overline{K}^\times. \tag{7.1}$$

Define

$$Y^i = c_i^{-1} e_i \text{ and } Y^\mu = \prod_i Y_i^{\mu(i)} \text{ for } \mu = \prod_i X_i^{\mu(i)}.$$

Define

$$w_\mu = \langle X^\mu, Y^\mu \rangle = \left\langle \prod_i (c_i \varepsilon_i)^{\mu(i)}, \prod_i (c_i^{-1} e_i)^{\mu(i)} \right\rangle = \langle \varepsilon^\mu, e^\mu \rangle$$

(Recall X's,Y's live in dual vector spaces).

Remark 7.17. The above expression for w_μ is independent of G. Everything involved ($A_{\overline{K}} = \mathrm{Map}(\mathbb{F}, \overline{K})$, $B_{\overline{K}} = \overline{K}[\mathbb{F}]$, $\varepsilon_i \in A_{\overline{K}}$ and $e_i \in B_{\overline{K}}$) was defined only using $\mathbb{F}$ with no reference to G. ∘

We similarly define

$$w_i = \langle X_i^p, Y_i^p \rangle = \langle \varepsilon_i^p, e_i^p \rangle,$$

another absolute constant.

Proposition 7.18.

$$w_\mu = \prod \mu(i)! \mod p$$

(in particular, $w_\mu \in R^\times$) and

$$w_i = -p \mod p^2.$$

Note that

$$\langle X^\mu, Y^\nu \rangle = \begin{cases} 0 & \text{if } \mu \neq \nu \\ w_\mu \in R^\times & \text{otherwise.} \end{cases}$$

since they live in different eigenspaces when $\mu \neq \nu$. This is telling us that we have R-dual modules I, J containing submodules span $\{X^\mu\}$,span $\{Y^\mu\}$ which are themselves R-dual! This forces $I = \text{span}\,\{X^\mu\}$ and $J = \text{span}\,\{Y^\mu\}$ since otherwise the dual of span $\{X^\mu\}$ would be a strict quotient of J, not a submodule.

Corollary 7.19. *The X_i's generate A as an R-algebra.*

One can even say more. Note $X_i^p = \delta_i X_{i+1}$ and $Y_i^p = \gamma_i Y_{i+1}$ for some $\delta_i, \gamma_i \in R$. Hence,

$$w_i = \langle X_i^p, Y_i^p \rangle = \delta_i \gamma_i \equiv -p \mod p^2 \implies v(\delta_i) \leq e.$$

This essentially proves

Theorem 7.20. *$A = R[x_i]/(x_i^p = \delta_i x_{i+1})$ for some $\delta_i \in R$ with $v(\delta_i) \leq e$ for all i.*

The converse of this will hold.

Theorem 7.21. *Suppose we are given $(\delta_i)_{i \in \mathcal{I}}$ with $\delta_i \in R$ and $v(\delta_i) \leq e$. Then, $A := R[x_i]/(x_i^p = \delta_i x_{i+1})$ has a unique Raynaud $\mathbb{F}$-module structure such that $[t]x_i = \chi_i(t)x_i$ for all $t \in \mathbb{F}^\times$.*

Proof. Choose elements $c_i \in \overline{K}^\times$ so that $\delta_i = c_i^p / c_{i+1}$ (compare with (7.1)). Define the isomorphism $A_{\overline{K}} \xrightarrow{\sim} \text{Map}(\mathbb{F}, \overline{K})$ sending $x_i \mapsto c_i \varepsilon_i$. As before, define

$$x^\mu := \prod x_i^{\mu(i)}.$$

We need to define comultiplication on A. The idea is to try and pull back comultiplication from $\text{Map}(\mathbb{F}, \overline{K})$. The hard will be to, after identifying $A \hookrightarrow A_{\overline{K}}$ with a subring, show that A is closed under this comultiplication map. This will be equivalent to showing that it's dual is closed under multiplication, so that's what we'll do.

Let $B = \text{Hom}_R(A, R)$ be the R-linear dual of A, so $B_{\overline{K}} = \overline{K}[\mathbb{F}]$ is the group algebra. Identifying $A_{\overline{K}}$ and $\text{Map}(\mathbb{F}, \overline{K})$, we have

$$x^\mu = \left(\prod c_i^{\mu(i)} \right) \varepsilon^\mu.$$

Let y_μ be the dual basis of the x^μ's. That is,

$$y_\mu = \left(\prod c_i^{-\mu(i)} \right) e_\mu.$$

We'll let $y_i = c_i^{-1} e_i$ and $y^\mu = \prod y_i^{\mu(i)} = \left(\prod c_i^{-\mu(i)} \right) e^\mu$ (note $e^\mu = w_\mu e_\mu$). These y^μ's span B an an R-module. Write $y_i^p = \gamma_i y_{i+1}$; an easy computation shows $\gamma_i \delta_i = w_i$. Note that $v(w_i) = e$ and $v(\delta_i) \leq e$, so $\gamma_i \in R$ is integral. Thus, $y_i^p \in B$. Since B is spanned by the y^μ's, which are monomials in the y_i's with exponents $< p$, one can conclude (from $y_i^p \in B$) that in fact any monomial in the y_i's lands in B, so B is an algebra (i.e. closed under multiplication). Thus, A is closed under comultiplication.

This gives a Hopf algebra structure on A. We leave uniqueness to you. ∎

This gives a nice classification. Given $\delta = (\delta_i)_{i\in\mathcal{I}}$ with $\delta_i \in R$ and $v(\delta_i) \leq e$, we get a Raynaud $\mathbb{F}$-module scheme

$$G_\delta := \operatorname{Spec}\left(\frac{R[X_i]}{(X_i^p = \delta_i X_{i+1})}\right).$$

Furthermore, all Raynaud $\mathbb{F}$-module schemes are of this form.

Exercise. Maps $f : G_\delta \to G_{\delta'}$ of $\mathbb{F}$-module schemes correspond the sequences $(a_i)_{i\in\mathcal{I}}$ (with $a_i \in R$) satisfying $a_{i+1}\delta_i = a_i^p \delta_i'$. From this, build a map of rings sending $f^*(x_i') = a_i x_i$.

Proposition 7.22. *Suppose $e < p-1$ and that we have a map $f : G_\delta \to G_{\delta'}$ of Raynaud $\mathbb{F}$-module schemes which is an isomorphism over K. Then, f is an isomorphism (over R).*

Proof. f corresponds to some $(a_i)_{i\in\mathcal{I}}$ with $a_{i+1}\delta_i = a_i^p\delta_i'$. We want to show these are all units. Pick i s.t. $v(a_i)$ is maximal. Then,

$$v(a_i) + e \geq v(a_{i+1}) + v(\delta_i) = pv(a_i) + v(\delta_i') \geq pv(a_i),$$

which forces $(p-1)v(a_i) \leq e$. This forces $v(a_i) = 0$ (since $e < p-1$ by assumption). Thus, $v(a_j) = 0$ for all $j \in \mathcal{I}$. ∎

Proposition 7.23. *Say $e < p-1$, and let G_0/K be a Raynaud $\mathbb{F}$-module scheme. Then, G_0 satisfies UP (there's at most one prolongation).*

Proof. Need to show that $G^+ \to G^-$ discussed earlier is an isomorphism. By uniqueness, G^+, G^- are necessarily $\mathbb{F}$-module schemes over R. Now this proposition follows from the previous one. ∎

This finishes the argument for Theorem 7.3.

8 Lecture 8: Elliptic curves over DVRs

(Reference: chapter VII of Silverman)

Setup 8.1. Let R be a complete dvr with field of fractions $K = \operatorname{Frac}(R)$, maximal ideal $\mathfrak{m} \subset R$, residue field $k = R/\mathfrak{m}$, and valuation $v : K^\times \to \mathbb{Z}$.

Assumption. Assume $\operatorname{char}(k) \neq 2, 3$.

Let E/K be an elliptic curve. By our characteristic assumption, we may write

$$E : y^2 = x^3 + ax + b.$$

This equation for E is not unique. If you change $(x, y) \to (u^2x, u^3y)$, then you scale $(a, b) \to (u^{-4}a, u^{-6}b)$.

Definition 8.2. We say the equation for E is **minimal** if $a, b \in R$ and $v(a) < 4$ or $v(6) < 6$. This is equivalently to saying that $a, b \in R$ and $v(\Delta)$ is minimal among all possible Weierstrass models of E. ⋄

Let $\mathcal{E}$ be the projective curve over R defined by a minimal equation. This is a called a **minimal Weierstrass model** for E, and is unique up to isomorphism.

Definition 8.3. Let $\overline{E} := \mathcal{E}_k$ be the special fiber of $\mathcal{E}$. This is a projective curve over k which will be irreducible (from the form of the Weierstrass equation), but which may not be smooth. We let $\overline{E}_{sm}$ denote the smooth locus of $\overline{E}$; this is canonically a group variety. $\diamond$

Remark 8.4. Since $\mathcal{E}$ is projective (so proper), we have $\mathcal{E}(R) = \mathcal{E}(K) = \mathcal{E}_K(K) = E(K)$. Thus, we get a reduction map

$$E(K) \to \overline{E}(k).$$

Concretely, if you have a K-point $[x : y : z]$ in projective coordinates, you can scale it so as to kill denominators, and then reduce mod $\mathfrak{m}$. $\circ$

Notation 8.5. We'll let $E_0(K) \subset E(K)$ be the points reducing into $\overline{E}_{sm}(k)$.

This $E_0(K)$ will be a subgroup of $E(K)$. Furthermore, $E_0(K) \to \overline{E}_{sm}(k)$ is a group homomorphism which is surjective by Hensel's lemma. Finally, we define

$$E_1(K) := \ker\left(E_0(K) \to \overline{E}_{sm}(k)\right).$$

8.1 Types of reduction

Write $\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$. This curve will be smooth iff

$$0 \neq \overline{\Delta} = -16\left(4\overline{a}^3 + 27\overline{b}^2\right) \iff \Delta \in R^\times.$$

In this case, we say that E has **good reduction** ($\overline{E}$ is an elliptic curve). In this case, $\mathcal{E}$ is smooth over $\operatorname{Spec} R$, and it's actually an R-group scheme.

What if $\overline{\Delta} = 0$?

- If $\overline{a} = \overline{b} = 0$, then $\overline{E} : y^2 = x^3$ has a single singular point at $(0, 0)$, a cusp.

  In this case, $\overline{E}_{sm} \cong \mathbb{G}_a$ as a group, and we see that E has **additive reduction**.

- If $\overline{a}, \overline{b} \neq 0$, then $\overline{E}$ has a single singular point at $\left(-\frac{3\overline{b}}{2\overline{a}}, 0\right)$, a node.

  In this case, $\overline{E}_{sm} \cong \mathbb{G}_m$ over $\overline{k}$ as a group. We say E has **multiplicative reduction**. If $\overline{E}_{sm} \cong \mathbb{G}_m$ over k ($\iff -\overline{b}/(2\overline{a}) = \square$ in k), we say it has **split multiplicative reduction**.

To summarize

- Good reduction $\iff \Delta \in R^\times$
- Multiplicative reduction $\iff \Delta \in \mathfrak{m}$ and $a, b \in R^\times$
- Additive reduction $\iff \Delta \in \mathfrak{m}$ and $a, b \in \mathfrak{m}$

Definition 8.6. More terminology: We say E has **bad reduction** if it has multiplicative or additive reduction. We say E has **semi-stable reduction** if it has good or multiplicative reduction ($\iff a \in R^\times$ or $b \in R^\times$). $\diamond$

Reduction type is not always preserved under field extensions.

Proposition 8.7. *Say K'/K is a finite extension. Suppose either*

(a) *K'/K is unramified; or*

(b) *E has semi-stable reduction over K*

Then, a minimal equation for E/K stays minimal over K', so the reduction type stays the same.

Proof. **(a)** Here $v' = v$ so ($v(a) < 4$ or $v(b) < 6$) $\iff$ ($v'(a) < 4$ or $v'(b) < 6$).

(b) If $v(a) = 0$ or $v(b) = 0$ (i.e. a or b is a unit), then $v'(a) = 0$ or $v'(b) = 0$, so the equation is still minimal. ■

Theorem 8.8 (**semi-stable reduction theorem**)**.** *There always exists a finite extension K'/K s.t. E has semi-stable reduction over K'.*

Proof. Start with $E : y^2 = x^3 + ax + b$. We want to make either a or b a unit, and we're allowed to make changes $(a, b) \rightsquigarrow (u^{-4}a, u^{-6}b) = (a', b')$.

- If $3v(a) \leq 2v(b)$, then take $u = a^{1/4}$ so $a' = 1$ and $b' = b/a^{3/2} \in R$. Over $K' = K(a^{1/4})$, E has semi-stable reduction.
- If $3v(a) \geq 2v(b)$, take $u = b^{1/6}$ so $b' = 1$ and $a' = a/b^{2/3} \in R$. Over $K' = K(b^{1/6})$, E has semi-stable reduction. ■

Remark 8.9. Can always take K'/K above to have degree ≤ 6 (at least away from char $= 2, 3$). This follows from the above proof. ∘

and to be separable

For K'/K sufficiently large, the reduction type of E/K' is constant and either good or multiplicative. In this first case, we say E has **potentially good reduction**. In the second, it has **potentially multiplicative reduction**.

Proposition 8.10. *E has potentially good reduction iff its j-invariant*

$$j(E) := -1728\frac{(4a^3)}{\Delta}$$

is integral.

Proof. Suppose E has semi-stable reduction. In the good case, $\Delta \in R^\times$ and $a \in R$, so $j \in R$. In the multiplicative case, $\Delta \notin R^\times$ but $a \in R^\times$, so $v(j) < 0$. ■

Example. Consider $E : y^2 = x^3 + p$ over $K = \mathbb{Q}_p$. Here, $a = 0$, $b = p$, and $\Delta = -16(27p^2)$. This has additive reduction with j-invariant $j = -1728\frac{4(0)^3}{\Delta} = 0 \in R$, so it better have potentially good reduction. Change $(x', y') = (p^{1/3}x, p^{1/2}y)$. Then, E is isomorphic to $y^2 = x^3 + 1$ over $\mathbb{Q}_p(p^{1/6})$, and this curve has good reduction. △

8.2 Reduction of torsion points

Assumption. Assume E has good reduction, i.e. $\mathcal{E}$ is a smooth, proper group scheme over R.

By the assumption, $\mathcal{E}[n]$ will be a finite, flat group scheme over R. We want to study the map

$$E[n](K) \longrightarrow \overline{E}(k)[n].$$

Proposition 8.11. *Suppose that G/R is a finite flat group scheme, and $\#G$ is invertible on R. Then,*

$$G(\overline{K}) \xrightarrow{\sim} G(\overline{k})$$

is an isomorphism of $\mathrm{Gal}(\overline{K}/K)$*-modules. In particular, $G(\overline{K})$ is an unramified Galois module.*

Proof. The map is Gal-equivariant, so it suffices to check it's a bijection. This can be checked after going to an extension of k. Since $\#G$ is invertible, G is étale, so $G \cong \underline{\mathbb{Z}/n\mathbb{Z}}$ after some extension where this proposition is clear. ■

Corollary 8.12. *If n is prime to* $\operatorname{char} k$*, then $E[n](\overline{K}) \xrightarrow{\sim} \overline{E}[n](k)$ as* Gal*-modules.*

Proposition 8.13. *Assume K is an extension of $\mathbb{Q}_p$ with ramification index $e < p-1$. Let G/R be a finite flat group scheme. Then, $G(R) \to G(k)$ is injective.*

Proof. Let $\Gamma = G(R)$, and view this as a constant group scheme $\underline{\Gamma}$ over R. We have a natural map $\underline{\Gamma} \to G$ of group schemes. Let $\overline{\Gamma}$ be the scheme theoretic image, i.e. the scheme-theoretic closure of $G(K)$ in G. The map $\Gamma \to \overline{\Gamma}$ is an isomorphism over K. Raynaud (Theorem 7.3) then implies that it is an isomorphism over R, so $\Gamma \to G$ is a closed embedding. Now we have

$$G(K) = \Gamma(R) \xrightarrow[\Gamma \text{ const}]{\sim} \Gamma(k) \hookrightarrow G(k).$$ ■

Warning 8.14. $G(R) \to G(k)$ not necessarily surjective.

Non-example. Let G be the Kummer extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p corresponding to some $a \in R^\times$. If A is an R-algebra, then

$$G(A) = \left\{ (i,z) \,\middle|\, \begin{array}{c} i \in \mathbb{Z}/p\mathbb{Z}, z \in Z \\ z^p = a^i \end{array} \right\}.$$

If R has no primitive pth root of 1, and no pth root of A, then $G(R) = 0$. If k is perfect, one has $G_k = \mathbb{Z}/p\mathbb{Z} \times \mu_p$, so $G(k) = \mathbb{Z}/p\mathbb{Z}$. Hence, $G(R) \to G(k)$ is not surjective. ▽

•

Warning 8.15. If $e \geq p-1$, $G(R) \to G(k)$ is not necessarily injective.

Non-example. Take $G = \mu_p$ and K with $K \supset \mu_p$. Then, $G(K)$ is the pth roots of unity in K, but $G(k) = 1$. ▽

•

Corollary 8.16. *Let $K/\mathbb{Q}_p$ be an extension with $e < p-1$. If E has good reduction, then*

$$E[n](K) \hookrightarrow \overline{E}[n](k).$$

8.3 Kernel of reduction map

Recall 8.17.

$$E_1(K) = \ker\left(E_0(K) \longrightarrow E_{sm}(R)\right). \qquad \odot$$

Note we're no longer assuming E has good reduction.

Remark 8.18. The points of $E_1(K)$ are $\mathfrak{m}$-adically close to the identity point of E. $\circ$

Because of this, we'll change coordinates so the identity is at the origin. Start with the projective equation

$$E : ZY^2 = X^3 + aZ^2X + bZ^3.$$

One normally takes $x = X/Z$ and $y = Y/Z$. Instead, let's use $u = X/Y$ and $v = Z/Y$. We then get the affine equation

$$E : v = \underbrace{u^3 + av^2u + bv^3}_{F(u,v)}$$

with identity point $(u, v) = (0, 0)$ at the origin. We can now iterate:

$$v = F(u, v) = F(u, F(u, v)) = \dots.$$

This turns into an (infinite) expression for v in terms of u:

$$v = \varphi(u) \text{ where } \varphi(u) = F(u, F(u, F(u, \dots))\dots) \in R[\![u]\!].$$

Proposition 8.19. *The map $\mathfrak{m} \mapsto E_1(K)$ sending $u \mapsto (u, \varphi(u))$ is a bijection of sets.*

This is not a group isomorphism, but does allow you to define a new group law on $\mathfrak{m}$ by transfer of structure. Let $\oplus : \mathfrak{m} \times \mathfrak{m} \to \mathfrak{m}$ denote the resulting addition map. One can show that

$$s \oplus t = G(s, t) \text{ for some } G \in R[\![s, t]\!].$$

Note that 0 is the identity for $\oplus$, so $G(s, 0) = s = G(0, s)$, so $G(s, t) = s + t + \dots$. This in particular implies that $\mathfrak{m}^n$ is a subgroup of $\mathfrak{m}$ under $\oplus$.

Notation 8.20. Let $E_n(K)$ denote the image of $\mathfrak{m}^n$ in $E_1(K)$.

Since $\oplus$ is normal $+$ with higher terms thrown in, one gets that

$$E_n(K)/E_{n+1}(K) \cong \mathfrak{m}^n/\mathfrak{m}^{n+1} \cong k.$$

Proposition 8.21. *$E_1(K)$ has a filtration with associated graded pieces all isomorphic to k.*

Corollary 8.22. *If k is finite of characteristic p, then $E_1(K)$ is a pro-p group.*

Corollary 8.23. *If n is prime to $p = \mathrm{char}(k)$, then the reduction map*

$$E_0[n](K) \to \overline{E}_{sm}[n](K)$$

is injective.

Theorem 8.24.

(a) *The quotient $E(K)/E_0(K)$ is finite.*

(b) *If E has split multiplicative reduction, then $E(K)/E_0(K)$ is cyclic with order $= -v(j)$.*

(c) *If E does not have split multiplicative reduction, then $\#E(K)/E_0(K) \leq 4$.*

We are not going to prove this, but will give some remarks on the proof.

Remark 8.25.

- **(a)** Follows from the existence of Néron models
- **(b)**,**(c)** follow from the classification of Néron models
- If k is finite, then **(a)** is easy since $E(K)$ is compact (using the topology coming from K) and $E_0(K)$ is an open subgroup, so the quotient is compact and discrete (i.e. finite)
- Can prove the full theorem w/o Néron models (via some casework).

  Consider the case where $v(a) = 1$ and $v(b) \geq 2$. Consider a point $P = (x, y)$. Then,

  $$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

  If P reduces to the singular locus, then $x \in \mathfrak{m}$; staring at the above expression shows that $v(x(2p)) \leq 0$. This shows $2P \in E^0(K)$, so $E(K)/E^0(K)$ is killed by 2. One can even show that the sum of any two elements in this quotient is 0, so it must be 0 or $\mathbb{Z}/2\mathbb{Z}$. ∘

8.4 Néron-Ogg-Shafarevich

Theorem 8.26 (**Néron-Ogg-Shafarevich Criterion**). *Let $\ell \neq \operatorname{char} k$ be prime. Then,*

(1) *E has good reduction $\iff$ $T_\ell E$ is unramified (i.e. inertia I_K acts trivially)*

(2) *E has semi-stable reduction $\iff$ I_K action on $T_\ell E$ is unipotent (i.e. acts by matrices $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$)*

Proof. **(1)** $T_\ell E$ is unramified $\iff$ $E[\ell^n](\overline{K})$ is unramified for all n. We have shown (Corollary 8.12) that if E has good reduction, then these are unramified. Now assume ℓ^n torsion unramified for all n. Let $d := \#E(K^{un})/E_0(K^{un})$ with K^{un} the maximal unramified extension (all ℓ-power torsion points defined over it by assumption). We claim

$$\#\left(E_0(K^{un}) \cap E[\ell^n](K^{un})\right) \geq \frac{\ell^{2n}}{d}.$$

This is simply because this group is

$$\ker\left(\underbrace{E[\ell^n](K^{un})}_{\#=\ell^{2n}} \longrightarrow \underbrace{E(K^{un})/E_0(K^{un})}_{\#=d}\right).$$

The injection $E_0(K^{un})[\ell^n] \hookrightarrow \overline{E}_{sm}(\overline{k})$ then implies that

$$\#\overline{E}_{sm}[\ell^n] \geq \ell^{2n}/d.$$

There are only a few possibilities for the group $\overline{E}_{sm}$ over $\overline{k}$. Note that

$$\#\mathbb{G}_m(\overline{k})[\ell^n] = \ell^n \text{ and } \#\mathbb{G}_a(\overline{k})[\ell^n] = 0$$

are both less that ℓ^{2n}/d (for $n \gg 0$). Thus, $\overline{E}_{sm}$ must be an elliptic curve.

(2) First say I_K acts unipotently. Then, it acts trivially on a 1-dimensional subspace, so $E[\ell^n](K^{un}) \supset \mathbb{Z}/\ell^n\mathbb{Z}$. Now do the same sort of counting argument to conclude that $\overline{E}_{sm} \neq \mathbb{G}_a$.

In the other direction, assume E has semi-stable reduction. Consider the smooth points $\mathcal{E}_{sm}$ of the minimal Weierstrass model. This is a group scheme over R, so $\mathcal{E}_{sm}[\ell^n]$ will be a flat group scheme over R (note multiplication by ℓ^n will be a flat map since this thing is smooth), but it is not necessarily finite (since $\mathcal{E}_{sm}$ not necessarily proper). Let G be the scheme theoretic closure in $\mathcal{E}_{sm}[\ell^n]$ of the $\overline{K}$-points which extend to $\overline{R}$-points.

Remark 8.27. $G \subset \mathcal{E}_{sm}[\ell^n]$ is a closed, finite, flat subgroup. Furthermore, $G_k = \overline{E}_{sm}[\ell^n]$. ∘

This G is étale (since finite, flat of ℓ-power order), so

$$E(K^{un})[\ell^n] \supset G(K^{un}) \xrightarrow{\sim} G(\overline{k}) = \overline{E}_{sm}[\ell^n](\overline{k}) \supset \mathbb{Z}/\ell^n\mathbb{Z}$$

(last containment since we're assuming semi-stable reduction). This produces a lot of unramified ℓ-power-torsion, and in particular let's us conclude that I_K fixes some vector in $T_\ell E$. Thus,

$$I_k \curvearrowright T_\ell E \text{ via } \begin{pmatrix} 1 & * \\ 0 & \alpha \end{pmatrix}$$

for some character α. Taking determinants, we see that $\alpha = \chi_\ell|_{I_K} = 1$ since the cyclotomic character is trivial on inertia. ■

9 Lecture 9: Néron models

Setup 9.1. Let R be a complete dvr with fraction field $K = \operatorname{Frac} R$, and let $\Gamma_k = \operatorname{Gal}(\overline{K}/K)$ be its absolute Galois group. Let k be the residue field of R.

9.1 Quasi-finite étale groups schemes/R

Recall 9.2. Quasi-finite means finite fibers. ⊙

Let G be a qfinite étale R-group scheme (also commutative and finite presentation?). Let $M = G(\overline{K})$. This is a Γ_K-module classifying G_K. Similarly, $M_0 = G(\overline{k})$ is a $\Gamma_k = \Gamma_K/I_K$-module classifying G_k.

Since G is étale, we get an isomorphism $G(\overline{R}) \xrightarrow{\sim} G(\overline{k})$, and so a diagram

$$\begin{array}{ccccc} G(\overline{K}) & \supset & G(\overline{R}) & \xrightarrow{\sim} & G(\overline{k}) \\ \| & & & & \| \\ M & & & & M_0 \end{array}$$

(in particular, $M_0 \subset M^{I_K}$).

Remark 9.3. Above, $\overline{R}$ is the ring of integers in $\overline{K}$. ∘

Thus, from G, we get a pair (M, M_0) with M a Γ_K-module and $M_0 \subset M^{I_K}$ a Γ_k-submodule.

Theorem 9.4. *The above assignment gives an equivalence of categories.*

Remark 9.5. Suppose $G \rightsquigarrow (M, M_0)$ and $H \rightsquigarrow (N, N_0)$ with $H \leq G$ a subgroup.

- H is closed $\iff N_0 = M_0 \cap N$
- If H is closed, then G/H is an étale quasi-finite group scheme corresponding to $(M/N, M_0/N_0)$
- If G_0/K is finite, this corresponds to some M. To specify an extension over R, just need to specify some M_0.
  - Get max extension by taking $M_0 = M^{I_K}$
  - Get min extension by taking $M_0 = 0$ (**extension of zero**)
- (M_0, M_0) corresponds to the maximal finite subgroup H in G. This has the property that $H_k = G_k$ (their special fibers agree)
- If G/R is flat, quasi-finite and killed by $n \in R^\times$, then G is étale ∘

Recall 9.6. If E is an elliptic curve with semistable reduction, then $(T_\ell E)^{I_K} \neq 0$. ⊙

Proof Sketch. We let G be the ℓ^n-torsion in the smooth part of a minimal Weierstrass model. This was a quasi-finite étale group scheme. Then we let $H \subset G$ be the maximal finite subgroup. Then, $H_k = G_k$ is the ℓ^n-torsion in an elliptic curve or in a torus, so $H(\overline{k}) \supset \mathbb{Z}/\ell^n\mathbb{Z}$. Thus,

$$\mathbb{Z}/\ell^n\mathbb{Z} \subset H(\overline{k}) \subset G(\overline{k}) \subset G(\overline{K}) = E[\ell^n](\overline{K})$$

which was what we needed to show (the existence of an inertia-invariant ℓ^n-order point). ■

9.2 Néron Models

(Reference: chapter IV of Silverman's "Advanced topics")

Let E/K be an elliptic curve with minimal Weierstrass model W/R. This W is proper, so $W(R) = E(K)$. However, it is usually singular, so W_{sm} is a smooth group scheme over R, but $W_{sm}(R) \subsetneq E(K)$. The Néron model $\mathcal{E}/R$ will be a smooth group scheme where K-points extend to R-points, i.e. $\mathcal{E}(R) = E(K)$.

These will fit into the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_0(K) & \longrightarrow & E(K) & \longrightarrow & \text{finite} & \longrightarrow & 0 \\ & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \downarrow & & \\ 0 & \longrightarrow & W_{sm}(k) & \longrightarrow & \mathcal{E}(k) & \longrightarrow & \pi_0(\mathcal{E}) & \longrightarrow & 0 \\ & & \| & & & & & & \\ & & \mathcal{E}^0(k) & & & & & & \end{array}$$

(In particular, the smooth part of the Weierstrass model is the identity component of the Néron model)

We still haven't defined the Néron model, properly.

Definition 9.7. Let C/K be a curve. A **regular model** of C is a flat, proper regular scheme $\mathcal{C}/R$ such that $\mathcal{C}_K \cong C$. Such a model $\mathcal{C}$ is a **minimal regular model** if for any regular model $\mathcal{C}'$, there exists a map $\mathcal{C}' \to \mathcal{C}$ extending the identity over K. $\diamond$

Theorem 9.8. *Minimal regular models exist and are unique.*

Remark 9.9. You can find a regular model by starting with any model, and then performing a suitable sequence of blowups and normalizations. Once you have a regular one, you get a minimal model by blowing down certain divisors (contract all (-1)-curves) $\circ$

Fact. Let E be an elliptic curve. Then, it's **Néron model** $\mathcal{E}$ is the smooth locus of its minimal regular model.

Example ($K = \mathbb{Q}_p$)**.** Let $E : y^2 = x^3 + p$. This has additive reduction (since p is not a unit). The same equation defines W, so W is smooth away from the point p given in coordinates by $(x, y) = (0, 0) \in W_k$. We claim that W is regular at p (and so regular everywhere).

Let $A = R[x, y]/(y^2 = x^3 + p)$ and let $\mathfrak{m} = (x, y, p)$, so $\operatorname{Spec} A \overset{\text{open}}{\subset} W$ with $p \in W$ corresponding the the maximal ideal $\mathfrak{m}$. Note that

$$\mathfrak{m}^2 = (x^2, xy, y^2, p^2, px, py) = \left(x^2, xy, x^3 + p, p^2, px, py\right) = \left(x^2, xy, p\right).$$

Hence, $\mathfrak{m}/\mathfrak{m}^2$ has a basis given by x, y and so is 2-dimensional. Thus, A is regular at $\mathfrak{m}$ ($\dim A_{\mathfrak{m}} = \operatorname{ht} \mathfrak{m} = \dim A = 2$).

Hence, W is a regular model. The special fiber is an irreducible curve, so there's nothing to blowdown, so W is the minimal regular model. Hence, the Néron model is $\mathcal{E} = W \setminus \{p\}$. In particular, $\mathcal{E}_k = \mathbb{G}_a$ is connected, so $E(K) = E_0(K)$. $\triangle$

Example ($K = \mathbb{Q}_p$)**.** Now look at $E : y^2 = x^3 + p^2$. This is again a minimal Weierstrass equation and W is smooth away from $p = (0, 0)$ in W_k. However, p is no longer a regular point.

Let $A = R[x, y]/(y^2 = x^3 + p^2)$ with $\mathfrak{m} = (x, y, p)$. Then,

$$\mathfrak{m}^2 = (x^2, xy, y^2, p^2, px, py) = (x^2, xy, p^2, px, py).$$

Now, $\mathfrak{m}/\mathfrak{m}^2$ has basis consisting of x, y, p, and so is 3-dimensional.

To get a regular model, we blowup the point p. Let $B \subset A[t]$ be the subring generated by tx, ty, and tp. The blowup of $\operatorname{Spec} A$ at $\mathfrak{m}$ is $\operatorname{Proj}(B)$. Let $B_1 = B[1/(tx)]^0$, $B_2 = B[1/(ty)]^0$, and $B_3 = B[1/(tp)]^0$. Then, $U_i = \operatorname{Spec} B_i$ form an affine open cover of $\operatorname{Proj}(B)$. Note that

$$B_1 = R\left[x, y, \frac{y}{x}, \frac{p}{x}\right] / \left((y/x)^2 = x + (p/x)^2, x(y/x) = y, x(p/x)\right) = R\left[x, \frac{y}{x}, \frac{p}{x}\right] \Big/ \left(\left(\frac{y}{x}\right)^2 = x + \left(\frac{p}{x}\right)^2, x\left(\frac{p}{x}\right) = p\right).$$

We can see what the special fiber is by taking $p = 0$, so

$$B_{1,k} = k\left[x, y/x, p/x\right] / ((y/x)^2 = x + (p/x)^2, x(p/x) = 0).$$

Second equations says either $x = 0$ or $(p/x) = 0$. When $x = 0$, you get $y/x = \pm(p/x)$ which is a union of two lines. When $px/ = 0$, get $x = (y/x)^2$, another line (a parabola). These three lines meet when $x = p/x = y/x = 0$, so U_1 is three copies of $\mathbb{A}^1$ meeting at a point. Pictorially, it's $*$.

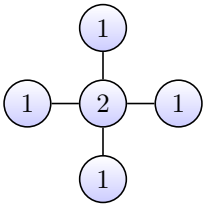
Exercise. Finish this computation.

For U_2, you get 3 lines with no intersection (2 $\mathbb{A}^1$'s, and 1 $\mathbb{G}_m$). These glue so that $U_1 \cup U_2$ is two $\mathbb{P}^1$'s meeting an $\mathbb{A}^1$ at a single point of intersection (and $U_3 \subset U_1 \cup U_2$), so the special fiber of $\operatorname{Bl}_p(W)$ is three $\mathbb{P}^1$'s meeting as in $*$. This $\operatorname{Bl}_p(W)$ is in fact the minimal regular model, so $\mathcal{E}_k$ is 3 copies of $\mathbb{G}_a$. In particular, $\pi_0(\mathcal{E}_k) = \mathbb{Z}/3\mathbb{Z}$. △

Example. If E has split multiplicative reduction and $\operatorname{val}(j(E)) = -n$, then $\mathcal{C}_k$ is n copies of $\mathbb{P}^1$ arranged in a cycle (a Néron (or standard) n-gon). If $n = 1$, $\mathcal{C}_k$ is a plane nodal curve and the minimal Weierstrass model is the minimal regular model. △

I was too lazy to add the picture here, but not too lazy to do it later on, so see Figure 2

Example. For $y^2 = x^3 + p^3$, the special fiber $\mathcal{C}_k$ is five $\mathbb{P}^1$'s meeting with dual graph the extended Dynkin diagram $\widetilde{D}_4$, i.e



(the 'central' $\mathbb{P}^1$ appears with multiplicity 2) △

If E has bad reduction, then $\mathcal{C}_k$ is made up of $\mathbb{P}^1$'s (with singularities and non-reducedness). Néron-Kodaira classified the possibilities of $\mathcal{C}_k$.

Corollary 9.10 (of classification)**.** *If E hoes not have split multiplicative reduction, then $\#\pi_0(\mathcal{E}_k) \leq 4$.*

9.3 Néron Models of Abelian Varieties

The previous discussion does not nicely generalize to higher dimensional abelian varieties. They key to get a nice generalize is to give a functorial description of Néron models.

Fact. Let $\mathcal{E}$ be the Néron model of E, and let $\mathcal{X}$ be a smooth scheme over R with $X := \mathcal{X}_K$. Then, $\operatorname{Hom}_R(\mathcal{X}, \mathcal{E}) \xrightarrow{\sim} \operatorname{Hom}_K(X, E)$.

Definition 9.11. Given a smooth scheme A/K, the **Néron model** of A is a smooth scheme $\mathcal{A}/R$ s.t.

$$\mathrm{Hom}_R(\mathcal{X}, \mathcal{A}) \xrightarrow{\sim} \mathrm{Hom}_K(X, A) \text{ for all smooth } \mathcal{X}/R.$$

This is called the **Néron mapping property**. ◇

This says that $\mathcal{A} = \eta_* A$ as sheaves on the (small) smooth site over $\mathrm{Spec}\, R$ (here, $\eta : \mathrm{Spec}\, K \hookrightarrow \mathrm{Spec}\, R$ is the generic point).

Remark 9.12.

- The Néron mapping property specifies the functor of points of $\mathcal{A}$, but only on smooth schemes. Since $\mathcal{A}$ is itself a smooth scheme, this specifies it uniquely up to isomorphism by Yoneda's lemma.
- Main theorem: $\mathcal{A}$ exists if $A = AV$.
- Important case of mapping property: $\mathcal{X} = \mathrm{Spec}\, R \implies \mathcal{A}(R) = A(K)$.
- Say K'/K is a finite extension. Let A/K be an abelian variety with Néron model $\mathcal{A}$. Let $\mathcal{A}'$ be the Néron model of $A_{K'}$. Then, $\mathcal{A} \otimes_R R'$ is a smooth scheme with generic fiber $A_{K'}$, so we get a canonical map
$$f : \mathcal{A} \otimes_R R' \longrightarrow \mathcal{A}'.$$
If K'/K is unramified, then f is an isomorphism. Similarly, if A has 'semi-stable reduction', then f is an isomorphism. In general, it won't be an iso though. In particular, $\mathcal{A}(R') \neq A(K')$ usually. ◦

Let $\mathcal{A}$ be the Néron model of A, and let $\mathcal{A}_0 := \mathcal{A}_k$ (a smooth k-group scheme). Let $\mathcal{A}_0^0$ be the identity component of $\mathcal{A}_0$.

Theorem 9.13 (Chevalley)**.** *Any smooth connected group scheme is the extension of an abelian variety by a linear group. The ground field needs to be perfect for this.*

In particular, we have

$$0 \longrightarrow L \longrightarrow \mathcal{A}_0^0 \longrightarrow B \longrightarrow 0$$

with B a k-abelian variety and L a smooth, commutative affine group scheme. We can further decompose (since L commutative)

$$0 \longrightarrow T \longrightarrow L \longrightarrow U \longrightarrow 0$$

with T a torus and U unipotent.

Definition 9.14. $\dim(T)$ is the **toric rank** of A. $\dim(U)$ is the **unipotent rank**. $\dim(B)$ probably also has a name. ◇

Definition 9.15. A has **good reduction** iff it extends to an **abelian scheme**[10] over R (i.e. $T = U = 0$). In this case, $\pi_0(\mathcal{A}_0) = 0$. A has **semistable reduction** if $U = 0$. ◇

Theorem 9.16 (**Néron-Ogg-Shafarveich**)**.** *Let $\ell \neq \mathrm{char}\, k$ be a prime. Then,*

- *A has good reduction $\iff$ $T_\ell A$ is unramified representation of Γ_K.*

  (The proof here is of the same point-counting flavor as the proof we gave in the elliptic curve case)

[10] proper, smooth group scheme with geometrically connected fibers

- *(Grothendieck) A has semi-stable reduction iff I_K acts unipotently in $T_\ell A$*

Theorem 9.17 (**Semi-stable reduction theorem**). *There exists a finite extension K'/K s.t. $A_{K'}$ has semi-stable reduction.*

Proof. Let's assume K is a finite extension of $\mathbb{Q}_p$ for simplicity. It suffices to find K'/K s.t. $I_{K'}$ acts unipotently on $T_\ell A$. We'll prove the existence of such an extension for any ℓ-adic Galois representation V.

Let I_K^w be the wild inertia group, a pro-p group. It's action on V must factor through a finite group, so can pass to a finite extension to assume that I_K^w acts trivially. Now, the **wild inertia quotient** is

See e.g. this or this

$$\Gamma_K/I_K^w = \left\langle F, \tau \,\middle|\, F\tau F^{-1} = \tau^q \right\rangle$$

where $q = \#k$, F is (a lift of) Frobenius, and τ is a generator for I^t (so F, τ generate the group topologically). From this we see that τ and τ^q are conjugate linear relations of V, so they have the same eigenvalues $\alpha_1, \ldots, \alpha_n$, i.e. $\alpha_i^q = \alpha_{\sigma(i)}$ for some $\sigma \in S_n$. Thus, $\alpha_i^{q^{n!}} = \alpha_i$, so the $\alpha_i^e = 1$ with $e = q^{n!} - 1$. Now, if K'/K has ramification degree e, then

$$\tau \text{ for } K' = (\tau \text{ for } K)^e$$

has 1 as its only eigenvalue, and so we win. ∎

10 Lecture 10: Jacobians

Goal. Associate to a curve X an abelian variety $\mathrm{Jac}(X)$.

We will first give the construction over $\mathbb{C}$.

10.1 Analytic Theory

Let X be a smooth, projective, connected curve/$\mathbb{C}$ of genus g.

Notation 10.1. Let $V = \mathrm{H}^0(X, \Omega^1)$ be its (g-dimensional) $\mathbb{C}$-vector space of global 1-forms. Let $\mathrm{H}^1_{dR}(X)$ denote its de Rham cohomology, a $2g$-dimensional $\mathbb{R}$-vector space.

Remark 10.2. Every element of V is closed as $\mathrm{d}(f(z)\mathrm{d}z) = f'(z)\mathrm{d}z \wedge \mathrm{d}z = 0$. Thus, we get a map

$$V \longrightarrow \mathrm{H}^1_{dR}(X) \otimes_{\mathbb{R}} \mathbb{C}. \qquad \circ$$

Lemma 10.3. *This map is injective*

Proof. Suppose $\omega = \mathrm{d}f$. By Cauchy-Riemann, this implies that f is holomorphic. Thus, f is constant (X projective), so $\omega = 0$. ∎

Theorem 10.4 (**Hodge decomposition for curves**). $\mathrm{H}^1_{dR}(X) \otimes_{\mathbb{R}} \mathbb{C} = V \oplus \overline{V}$

Proof. We have a natural map $V \oplus \overline{V} \to \mathrm{H}^1_{dR}(X) \otimes_{\mathbb{R}} \mathbb{C}$ which we need to show is injective. Let $J : T_x \to T_x$ be multiplication by i on the tangent space at $x \in X$. Given a 1-form ω, define $\omega^c := -i\omega J$ (recall, 1-forms eat tangent vectors). Note that V lives in the $c = 1$ eigenspace on $\mathrm{H}^1_{dR}(X) \otimes \mathbb{C}$, while $\overline{V}$ lives in the $c = -1$ eigenspace, so $V \cap \overline{V} = 0$ (inside $\mathrm{H}^1_{dR}(X) \otimes \mathbb{C}$) and we win. ■

Proposition 10.5. *Let $p : \mathrm{H}^1_{dR}(X) \otimes_{\mathbb{R}} \mathbb{C} \to V$ be the natural projection map. This induces an isomorphism*

$$\mathrm{H}^1_{dR}(X) \xrightarrow{\sim} V.$$

Proof. Say $\alpha \in \mathrm{H}^1_{dR}(X)$ and write $\alpha = \omega + \overline{\eta}$ with $\omega, \eta \in V$. Then, $\alpha = \overline{\alpha} \implies \omega = \eta$. Furthermore, $\omega = p(\alpha)$, so $\alpha = p(\alpha) + \overline{p(\alpha)}$ and we get an inverse map $V \to \mathrm{H}^1_{dR}(X)$ sending $\omega \mapsto \omega + \overline{\omega}$. ■

Proposition 10.6. *Suppose $\alpha, \beta \in \mathrm{H}^1_{dR}(X)$ are real 1-forms. Write $\omega = p(\alpha)$ and $\eta = p(\beta)$. Then,*

$$\int_X \alpha \wedge \beta = 2 \operatorname{Re} \left[\int_X \omega \wedge \overline{\eta} \right].$$

Proof sketch. Write $\alpha = \omega + \overline{\omega}$ and $\beta = \eta + \overline{\eta}$, note that $\omega \wedge \eta = 0 = \overline{\omega} \wedge \overline{\eta}$ (think: $\mathrm{d}z \wedge \mathrm{d}z$) and that $\omega \wedge \overline{\eta} = \overline{\overline{\omega} \wedge \eta}$. ■

We define a Hermitian form H on V via

$$H(\omega, \eta) = 2i \int_X \omega \wedge \overline{\eta}.$$

The factor of i above ensures that $H(\omega, \eta) = \overline{H(\eta, \omega)}$. From the previous proposition, we see that (this is why we have the factor of 2)

$$\int_X \alpha \wedge \beta = \operatorname{Im} H(p(\alpha), p(\beta)).$$

Notation 10.7. Let $L = \mathrm{H}_1(X, \mathbb{Z})$, a free $\mathbb{Z}$-module of rank $2g$.

Remark 10.8. Given $\gamma \in L$ and $\omega \in V$, we can form

$$\int_\gamma \omega \in \mathbb{C}.$$

This defines a map $i : L \to V^\vee$. ◦

Proposition 10.9. *$i(L)$ is a lattice in $V^\vee$*

Proof. Extending i to $i_{\mathbb{R}} : L \otimes \mathbb{R} \to V^\vee$. Take the dual $i^\vee_{\mathbb{R}} : V \to L^\vee_{\mathbb{R}} = \mathrm{H}^1_{dR}(X)$.[11] Chasing through identifications, this map is $\omega \mapsto \omega + \overline{\omega}$ which is known to be an isomorphism. ■

Definition 10.10. The **Jacobian** of X is

$$\operatorname{Jac}(X) := V^\vee / i(L),$$

a compact, complex torus of dimension g. ◇

[11] There's a subtly here where we've taken the real dual of the complex dual of V. To get a map $V \to \operatorname{Hom}(\operatorname{Hom}(V, \mathbb{C}), \mathbb{R})$ we send $v \in V$ to the functional $\varphi \mapsto \operatorname{Re} \varphi(v)$, where $\varphi : V \to \mathbb{C}$

We define the Hermitian form $H^\vee$ on $V^\vee$. First consider

$$\begin{array}{rccc} j: & V & \longrightarrow & V^\vee \\ & \omega & \longmapsto & H(-,\omega) \end{array}$$

(a conjugate-linear iso of $\mathbb{C}$-vector spaces). Then, define

$$H^\vee(\lambda,\mu) = H(j^{-1}(\mu), j^{-1}(\lambda)).$$

This is a positive-definite Hermitian form on $V^\vee$.

Proposition 10.11. $\operatorname{Im} \mathrm{H}^\vee(i(\gamma), i(\gamma')) = \langle \gamma, \gamma \rangle$ *is the intersection pairing on* H_1.

Proof Idea. Extend pairings to $L_\mathbb{R}$, transfer to dual $L_\mathbb{R}^* = \mathrm{H}^1_{dR}(X)$. On the left, you get $(\alpha,\beta) \mapsto \operatorname{Im} H(p(\alpha), p(\beta))$. The the right, you have $(\alpha,\beta) \mapsto \int_X \alpha \wedge \beta$. Check definitions to show that these agree. ■

Corollary 10.12. $\operatorname{Jac}(X)$ *is a principally polarized abelian variety*

Properties

- $T_0 \operatorname{Jac}(X) = V^\vee = \mathrm{H}^1(X, \mathscr{O})$ (last equality by Serre duality)
- $\mathrm{H}^0(\operatorname{Jac}(X), \Omega^1) \cong V = \mathrm{H}^0(X, \Omega^1)$
- $\mathrm{H}_1(\operatorname{Jac}(X); \mathbb{Z}) = L = \mathrm{H}_1(X; \mathbb{Z})$.

Recall 10.13. $\operatorname{Pic}(X)$ is the group of iso. classes of line bundles on X. We let $\operatorname{Pic}^0(X) \subset \operatorname{Pic}(X)$ be the subgroup of degree 0 line bundles. ⊙

Proposition 10.14. *There is a natural isomorphism* $\operatorname{Jac}(X) \xrightarrow{\sim} \operatorname{Pic}^0(X)$

Proof Sketch. Consider the exponential exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathscr{O}_X \xrightarrow{f \mapsto \exp(2\pi i f)} \mathscr{O}_X^\times \longrightarrow 0$$

of sheaves on X. Taking cohomology gives

$$0 \longrightarrow \frac{\mathrm{H}^1(X, \mathscr{O}_X)}{\mathrm{H}^1(X, \mathbb{Z})} \longrightarrow \mathrm{H}^1(X, \mathscr{O}_X^\times) \longrightarrow \mathrm{H}^2(X, \mathbb{Z}) \longrightarrow 0.$$

The middle object above is $\operatorname{Pic}(X)$ and the right map is the degree map $\deg : \operatorname{Pic}(X) \to \mathbb{Z}$. Finally, the left object is the Jacobian. ■

Remark 10.15. Fix a basepoint $x \in X$. Then, you can define the **Abel-Jacobi map** $f_x : X \to \operatorname{Jac}(X)$. Given $y \in X$, we pick a path ρ from x to y, and use this to construct

$$\begin{array}{ccc} V & \longrightarrow & \mathbb{C} \\ \omega & \longmapsto & \displaystyle\int_\rho \omega. \end{array}$$

Since there was a choice involved in picking ρ, this element of V^* is only well-defined up to the homology class of the path, i.e. up to $i(L)$. Thus, we get in this way a well defined map

$$\begin{array}{rccc} f_x: & X & \longrightarrow & \mathrm{Jac}(X) \\ & y & \longmapsto & \left[\omega \mapsto \displaystyle\int_\rho \omega\right] \end{array}$$

with $f_x(x) = 0$. This is in fact the universal map from X to an(y) abelian variety sending $x \mapsto 0$. ∘

10.2 Algebraic Theory

The description above won't work over general fields; instead, we define Jacobians in terms of their connections to line bundles.

Setup 10.16. Let k be any field, and let X/k be a smooth, connected projective curve over $k/$

Goal. We would like to give $\mathrm{Pic}^0(X)$ the structure of a variety.

To do this, we first need to figure out what we mean by a family of degree 0 line bundles (i.e. a hypothetical map $T \to \mathrm{Pic}^0$)

Definition 10.17. A **family of elements of** $\mathrm{Pic}^0(X)$ **over** T is a line bundle $\mathscr{L}$ on $X_T = X \times T$ s.t. $\mathscr{L}|_{X\times\{t\}}$ has degree 0 for all $t \in T$. We let $F(T)$ denote the set of isom classes of families / T. ⋄

This $F(T)$ is a decent first guess for the functor of points of $\mathrm{Pic}^0(X)$, but it is not correct; this functor is not representable, for at least two reasons

(1) Line bundles on T cause problems.

Suppose F is representable by some J with a universal line bundle $\mathscr{L}$ on X_J. Let L be a line bundle on some scheme T, and let $p : X_T \to T$ be the projection map. Then, $p^*(L)$ is a line bundle on X_T which is trivial on each fiber, $p^*(L)|_{X\times\{t\}} = \mathscr{O}_X$ for all $t \in T$. This is fiberwise degree 0, so $p^*(L)$ is classified by a map $f : T \to J$ (i.e. $f^*\mathscr{L} = p^*L$). Since all the fibers are trivial, f must map all of T to a single point ($f(t) \in J$ corresponds to the trivial bundle always), i.e. f is the constant map, i.e. $f^*\mathscr{L}$ must be the trivial bundle, i.e. we've reached a contradiction.

Notation 10.18. To fix this, we define

$$G(T) := F(T)/p^* \mathrm{Pic}(T).$$

This has the same k-points, and now avoids the above issue.

(2) $G(T)$ is still not representable because Pic doesn't have good descent properties (G is not a sheaf in general).

Let k'/k be a Galois extension w/ group Γ. Suppose G were a sheaf (e.g. if G were representable). We'd then get an isomorphism

$$G(k) \xrightarrow{\sim} G(k')^\Gamma.$$

Proposition 10.19. *There is an exact sequence*

$$0 \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Pic}(X_{k'})^{\Gamma} \longrightarrow \mathrm{Br}(k)$$

(have a Brauer group obstruction to $G(k) \to G(k')^{\Gamma}$ being an iso)

Proof. Let $L, L' \in \mathrm{Pic}(X)$, and assume $\exists$ isom $i : L_{k'} \xrightarrow{\sim} L'_{k'}$. This i does not have to be Galois invariant. Consider some $\sigma \in \Gamma$, and get $i^{\sigma} : L_{k'} \to L'_{k'}$. Then, i, i^{σ} differ by an automorphism. Note that $\mathrm{Aut}(L_{k'}) = (k')^{\times}$, so we may write

$$i^{\sigma} = c_{\sigma} i \text{ for some } c_{\sigma} \in (k')^{\times}.$$

This defines a 1-cocycle $c \in \mathrm{H}^1(\Gamma, (k')^{\times}) = 0$ (Hilbert 90). Thus, $c_{\sigma} = \sigma(\alpha)/\alpha$ for some $\alpha \in (k')^{\times}$ and all $\sigma \in \Gamma$. Thus, $\alpha^{-1} i$ is Γ-invariant, and so descends to an isomorphism $L \to L'$ over k. This gives injectivity on the left.

Now exactness in the middle. Say we have $L \in \mathrm{Pic}(X_{k'})^{\Gamma}$. For each $\sigma \in \Gamma$, fix an isomorphism $i_{\sigma} : L \xrightarrow{\sim} \sigma^* L$. Given, $\sigma, \tau \in \Gamma$, we can write

$$i_{\tau\sigma} = c_{\sigma,\tau} (\sigma^* i_{\tau}) \circ i_{\sigma} \text{ for some } c_{\sigma,\tau} \in (k')^{\times}.$$

One can check that these give a 2-cocycle

$$c \in \mathrm{H}^2(\Gamma, (k')^{\times}) \subset \mathrm{Br}(k) \, (= \mathrm{H}^2(k, \mathbb{G}_m)). \qquad \blacksquare$$

Example. Say X is a genus 0 curve not isomorphic to $\mathbb{P}^1$, e.g. $X^2 + Y^2 + Z^2 = 0$ over $\mathbb{R}$. Let $k' = \overline{k}$, so $X_{k'} = \mathrm{Pic}^1$ and $\mathrm{Pic}(X_{k'}) = \mathbb{Z}$. Then, $\mathrm{Pic}(X) \subset \mathrm{Pic}(X_{k'}) = \mathbb{Z}$. Note that the Galois group must act trivially on $\mathrm{Pic}(X_{k'})$; the only thing it could do is switch $\pm 1 \in \mathbb{Z}$, but only one of these corresponds to an ample line bundle. Thus, in particular, $\mathscr{O}(1) \in \mathrm{Pic}(X_{k'})^{\Gamma}$; however, it does not descend to a line bundle on X since it would then give an isomorphism $X \xrightarrow{\sim} \mathbb{P}^1_k$. $\triangle$

Example. Say $k/\mathbb{Q}_p$ a finite extension, and take $k' = \overline{k}$. Note $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$ by class field theory. In this case, $\mathrm{im}(\delta) = N^{-1}\mathbb{Z}/\mathbb{Z}$ where N is the gcd of degrees of divisors on X. $\triangle$

Remark 10.20. Neither of these give counterexamples to descent for degree 0 line bundles, but such things do exist; they're just harder to know off-hand (probably can find one by looking at genus 1 curves). $\circ$

This shows the type of things that can go wrong in representing the functor G.

Fact. If $X(k) \neq \emptyset$, then G is a sheaf.

Fix a point $x \in X(k)$ and consider the category $\mathcal{G}_x(T)$ of pairs (L, i) with L a line bundle on $X \times T$ (fiberwise degree 0), and $i : L_{\{x\} \times T} \xrightarrow{\sim} \mathscr{O}_T$ an iso. Let

$$G_x(T) := \{\text{isom classes in } \mathcal{G}_x(T)\}.$$

The isomorphism i rigidifies the category enough to kill automorphisms (automorphisms would be given by scaling, but preserving i means you better scale by 1), so $\mathcal{G}_x$ is a stack with trivial automorphism

groups. This means that G_x satisfies descent. More concretely, you can look at the cocycles from before, and use the rigidification to show they're all trivial.

Lemma 10.21. *The map $G_x \to G$ is an isomorphism.*

Proof. Say $L \in G(T)$ and let $L_0 = L|_{\{x\}\times T}$. Replace L with $L \otimes p^*(L_0^{-1})$ (this equals L in $G(T)$). This comes from $G_x(T)$, so we have surjectivity. Injectivity is similarly easy. ■

Theorem 10.22. *Suppose X has a k-point. Then, the sheaf G is representable, and the representing sheaf is denoted* $\mathrm{Jac}(X)$ *and called the* ***Jacobian*** *of X.*

Remark 10.23. If X does not have a rational point, G is not necessarily a sheaf. However, you can take its (étale- or fppf-)sheafification, and that will be representable by a scheme then called the Jacobian of X. ∘

10.2.1 Construction of $\mathrm{Jac}(X)$

References include Milne's notes or Kleiman's article, I guess

Recall we're assume X/k has a base point $x \in X(k)$. Let $X^{(r)}$ be the rth symmetric power of X, i.e. $X^{(r)} = X^r/S_r$. Then,

$$X^{(r)}(k') = \text{deg } r \text{ effective divisors on } X_{k'}.$$

Let D, D' be two effective divisors of degree $g = g(X)$. Then,

$$\ell(D + D' - g[x]) \geq 1$$

by Riemann-Roch. An appropriate semi-continuity result ensures that

$$U := \left\{(D, D') \in X^{(g)} \times X^{(g)} : \ell(D + D' - g[x]) = 1\right\}$$

is an open set. One can show that U is nonempty. Thus, if we have $(D, D') \in U$, there is a unique (up to scaling) function $f \in \mathscr{L}(D + D' - g[x])$. Note that

$$D'' := \mathrm{div}(f) + D + D' - g[x]$$

is effective of degree g, so $D'' \in X^{(g)}$. In this way, we get a map $U \to X^{(g)}$ which we think of as a rational map

$$X^{(g)} \times X^{(g)} \dashrightarrow X^{(g)}.$$

Now, Weil proved a general result saying that such a rational group law uniquely extends to an actual group law, i.e. there exists a unique group variety J with a birational group homomorphism $X^{(g)} \dashrightarrow J$. Finally, one shows that J actually represents G.

Many of the properties from the analytic theory carry over the algebraic theory.

Remark 10.24. Fix n prime to $\mathrm{char}(k)$. Get the **Kummer sequence**

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0$$

of sheaves on the étale site on $X_{\overline{k}}$. This gives rise to an isomorphism

$$\mathrm{H}^1(X_{\overline{k}}, \mu_n) \xrightarrow{\sim} \mathrm{H}^1(X_{\overline{k}}, \mathbb{G}_m)[n] = \mathrm{Pic}(X_{\overline{k}})[n] = \mathrm{Jac}(X_{\overline{k}})[n].$$

Taking an inverse limit over $n = \ell^m$ for $m \gg 0$, we conclude

$$\mathrm{H}^1(X_{\overline{k}}, \mathbb{Z}_\ell(1)) = T_\ell(\mathrm{Jac}(X)).$$

Think of this as saying $\mathrm{H}^{\text{ét}}_1(X_{\overline{k}}, \mathbb{Z}_\ell) = \mathrm{H}^{\text{ét}}_1(\mathrm{Jac}(X)_{\overline{k}}, \mathbb{Z}_\ell)$ (the seeming discrepancy with twisting here is coming from $\mathrm{H}^2_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_\ell) = \mathbb{Z}_\ell(-1)$, it sounds like). ∘

TODO: Convince yourself this makes sense

Remark 10.25. Suppose $X \to S$ is a family of smooth, geometrically connected, projective curves. Further assume it has a section, $X(S) \neq \emptyset$. Can define G as before, and it will be represented by an abelian scheme $\mathrm{Jac}(X)/S$. ∘

Example. Say R is a dvr, $K = \operatorname{Frac} R$, and X/K a curve with Jacobian $J = \mathrm{Jac}(X)$. If X extends to a smooth curve over R, then J has good reduction (The Jacobian of the extension of X will be an abelian scheme extending J). △

11 Lecture 11: Criterion for rank 0

Goal. Prove Theorem 1.7.

Theorem 11.1 (Theorem 1.7)**.** *Let $A/\mathbb{Q}$ be an abelian variety. Suppose we have distinct prime numbers $p \neq N$ with N odd, so that*

- *A has good reduction away from N*
- *A has completely toric reduction at N*
- *$A[p](\overline{\mathbb{Q}})$ has only trivial representation and cyclotomic character as its J-H constituents.*

We'll see in a bit, that this is equivalently requiring $\mathcal{A}[p]/\mathbb{Z}$ to be admissible

Then, $A(\mathbb{Q})$ has rank 0.

The proof idea is similar to that of weak Mordell-Weil.

Recall 11.2. For weak MW, we showed there's an injection $A(\mathbb{Q})/nA(\mathbb{Q}) \hookrightarrow \mathrm{H}^1(G_{\mathbb{Q}}, A[n])$ with image contained in some $\mathrm{H}^1(G_{\mathbb{Q},S}, A[n])$ which is a finite group. In general, can take

$$S = \{\text{primes of bad reduction}\} \cup \{\text{primes } \mid n\},$$

so in our case, we'll be able to take $S = \{p, N\}$. ⊙

We'll want to do even better than this. Let $\mathcal{A}$ be the Néron model of $A/\mathbb{Z}$, and let $G_n := \mathcal{A}[p^n]$, a group scheme/$\mathbb{Z}$. Then,

$$\mathrm{H}^1(G_{\mathbb{Q},S}, A[p^n]) = \mathrm{H}^1_{\text{ét}}(\operatorname{Spec} \mathbb{Z}[1/(pN)], G_n),$$

i.e. the Galois cohomology used in weak-MW is really just étale cohomology on a punctured $\operatorname{Spec} \mathbb{Z}$. Because of the ramification, we cannot use étale cohomology over all of $\operatorname{Spec} \mathbb{Z}$, but we will be able to

use fppf cohomology. That is, there will be an injection

$$A(\mathbb{Q})/p^n A(\mathbb{Q}) \hookrightarrow \mathrm{H}^1_{\mathrm{fppf}}(\operatorname{Spec}\mathbb{Z}, G_n).$$

The plan will be to show that the cardinality of the RHS is bounded, independent of n. This implies the same for the LHS which forces $\operatorname{rank} A(\mathbb{Q}) = 0$.

Remark 11.3. I didn't bother noting them in these notes, but there are quite a few places throughout the proof where we really use the fact that we're over $\mathbb{Q}$ (e.g. to freely apply Raynaud or to know $\operatorname{Pic}\mathscr{O}_{\mathbb{Q}} = 0$). Andrew drew attention to this during the lecture (and I think also in his notes online). ∘

11.1 Prelims on (pre-)admissible groups

Fix p, N for the rest of the lecture. Let's start with some definitions.

Definition 11.4.

- A group scheme $G/\mathbb{Z}[1/N]$ is **pre-admissible** if it is finite, flat, commutative, and killed by a power of p.
- A group scheme $G/\mathbb{Z}$ is **pre-admissible** if it is commutative, flat, killed by a power of p, quasi-finite, finite over $\mathbb{Z}[1/N]$, separated and of finite presentation. ◇

By Theorem 5.31, this implies that G is finite étale over $\mathbb{Z}[1/(pN)]$

Example. If A has good reduction away from N, then $\mathcal{A}[p^n]$ is pre-admissible over $\mathbb{Z}$. Here, $\mathcal{A}$ is the Néron model of the abelian variety A. △

Definition 11.5. Let $G/\mathbb{Z}[1/N]$ be pre-admissible. An **admissible filtration**

$$0 = F_0 \subset F_1 \subset \cdots \subset F_n = G$$

is an ascending filtration by closed subgroups such that F_i/F_{i-1} is $\underline{\mathbb{Z}/p\mathbb{Z}}$ or μ_p for all i. We say G is **admissible** if it has an admissible filtration. We say $G/\mathbb{Z}$ is **admissible** if it is pre-admissible and $G_{\mathbb{Z}[1/N]}$ is admissible. ◇

We define similar notions for Galois modules. We let $\Gamma_{\mathbb{Q}} := \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group.

Definition 11.6. A finite $\Gamma_{\mathbb{Q}}$-module M is **admissible** if there's a filtration

I guess M an $\mathbb{F}_p[\Gamma_{\mathbb{Q}}]$-module

$$0 = F_0 \subset \cdots \subset F_n = M$$

s.t. F_i/F_{i-1} is a 1-dimensional $\mathbb{F}_p$-vector space where $\Gamma_{\mathbb{Q}}$ acts trivially or cyclotomically. ◇

Proposition 11.7. *Let $G/\mathbb{Z}[1/N]$ be pre-admissible. Then, G is admissible $\iff$ $G(\overline{\mathbb{Q}})$ is admissible.*

Proof. First assume $G(\overline{\mathbb{Q}})$ is admissible. Let $V \subset G(\overline{\mathbb{Q}})$ be the first step of an admissible filtration, and let $H_0 \subset G_{\mathbb{Q}}$ be the subgroup corresponding to V. Let $H = \overline{H}_0 \subset G$ be its closure. Over $\mathbb{Z}[1/(Np)]$, H is finite, étale and $H(\overline{\mathbb{Q}})$ is 1-dimensional over $\mathbb{F}_p$, so H must be either μ_p or $\mathbb{Z}/p\mathbb{Z}$, depending on the Galois action on $H(\overline{\mathbb{Q}})$. All of these things – i.e. all of $H_{\mathbb{Z}[1/(pN)]}$, μ_i, $\mathbb{Z}/p\mathbb{Z}$ – extend to finite, flat groups

As in Corollary 5.23 (All group schemes in char 0 are smooth)

over $\mathbb{Z}[1/N]$. This is the situation in which Raynaud (Theorem 7.3) tells us the isomorphism extends, so $H = \mu_p$ or $H = \mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[1/N]$.[12] Now we win by induction. ■

Let's attach some invariants to admissible groups.

Definition 11.8. Let $G/\mathbb{Z}$ be admissible. We define

- $\ell(G) := \log_p(\#G_{\mathbb{Q}})$, the **length** of G (length of an admissible filtration)
- $\delta(G) := \log_p(\#G_{\mathbb{Q}}) - \log_p(\#G_{\mathbb{F}_N})$ (recall N is prime)

  If G were *finite* + flat over $\mathbb{Z}$, we'd have $\delta(G) = 0$.
- $\alpha(G) := \#\mathbb{Z}/p\mathbb{Z}$'s in an admissible filtration of $G_{\mathbb{Z}[1/N]}$.
- $h^i(G) := \log_p \# \mathrm{H}^i_{\mathrm{fppf}}(\operatorname{Spec}\mathbb{Z}, G)$ for $i = 0, 1$ ◇

Let's say a little about this flat cohomology.

Remark 11.9 (low degree fppf cohomology). Let G/S be a group scheme. A **G-torsor** is a scheme T/S w/ a simply transitive G-action, i.e. for any $x \in T(S')$ the map $G(S') \xrightarrow{\sim} T(S')$, $g \mapsto gx$ is a bijection. An **fppf G-torsor** is a G-torsor for which there exists an fppf cover $S' \to S$ so that $T(S') \neq \emptyset$. This first fppf cohomology group is simply the set of all such torsors:

$$\mathrm{H}^1_{\mathrm{fppf}}(S, G) = \{\text{isom classes of fppf } G\text{-torsors}\}.$$

Also, $\mathrm{H}^0_{\mathrm{fppf}}(S, G) = G(S)$. ○

Definition 11.10. An admissible group $G/\mathbb{Z}$ is called **elementary** if it has length 1. ◇

Example. Over $\mathbb{Z}[1/N]$, there are two elementary admissible groups, $\mathbb{Z}/p\mathbb{Z}$ and μ_p. △

Proposition 11.11 (See Theorem 9.4 and the remarks below it)**.** *Suppose H is a finite group scheme over $\mathbb{Q}_N$. The extensions of H to a pre-admissible group /$\mathbb{Z}_N$ correspond to unramified Galois submodules of $H(\overline{\mathbb{Q}}_N)$. In particular, if $H(\overline{\mathbb{Q}}_N)$ is 1-dimensional and unramified, there are two such extensions.*

Corollary 11.12. *There are 4 elementary admissible groups over $\mathbb{Z}$:*

$$\mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^\flat, \mu_p, \mu_p^\flat.$$

These have invariants as shown in Table 1.

Remark 11.13. Above, the flat sign $\flat$ denotes extension by 0. ○

Exercise. Convince yourself that the first three lines of Table 1 are correct.

Computation of the last line of Table 1. We'll need to use some facts about fppf cohomology we don't have time to prove. Write $S = \operatorname{Spec}\mathbb{Z}$.

[12] If $p = 2$, Raynaud doesn't apply, but a theorem by Fontaine does instead. Also, note here that the K is the application of Raynaud is $K = \mathbb{Q}_p$, so there is no ramification

	$\mathbb{Z}/p\mathbb{Z}$	$(\mathbb{Z}/p\mathbb{Z})^\flat$	μ_p	$\mu_p^\flat$
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	$\begin{cases} 1 & \text{if } p = 2 \\ 0 & \text{otherwise.} \end{cases}$	0
h^1	0	0	$\begin{cases} 1 & \text{if } p = 2 \\ 0 & \text{otherwise.} \end{cases}$	$\begin{cases} 1 & \text{if } p \neq 2 \text{ and } p \mid (N-1) \\ 1 & \text{if } p = 2 \text{ and } N \equiv 1 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$

Table 1: Invariants of the elementary admissible groups over $\mathbb{Z}$

First note that $\mathrm{H}^1_{\mathrm{fppf}}(S, \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^1_{\text{ét}}(S, \mathbb{Z}/p\mathbb{Z})$ since $\mathbb{Z}/p\mathbb{Z}$ is étale over S. Indeed, if T/S is an fppf torsor for $\mathbb{Z}/p\mathbb{Z}$, $\exists S' \overset{\text{ét}}{\twoheadrightarrow} S$ s.t. $T_{S'} = (\mathbb{Z}/p\mathbb{Z})_{S'}$, but then $T_{S'}$ is étale over S', so T must be étale over S (by fppf descent for properties of morphisms). Since $\mathbb{Z}/p\mathbb{Z}$ is a constant sheaf, we further have

$$\mathrm{H}^1_{\text{ét}}(S, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\pi_1^{\text{ét}}(S), \mathbb{Z}/p\mathbb{Z}),$$

but now $\pi_1^{\text{ét}}(S) = 1$ (it's the Galois group of the maximal unramified extension of $\mathbb{Q}$).

Now, observe that we have a short exact sequence

$$0 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\flat \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow 0$$

of sheaves on S. Furthermore, G above is just the pushforward of $\mathbb{Z}/p\mathbb{Z}$ along the inclusion $\operatorname{Spec} \mathbb{F}_N \hookrightarrow \operatorname{Spec} \mathbb{Z} = S$. On cohomology, we get

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^0_{\mathrm{fppf}}(S, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & \mathrm{H}^0_{\mathrm{fppf}}(S, G) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(S, (\mathbb{Z}/p\mathbb{Z})^\flat) & \longrightarrow & 0 \\ \| & & \| & & \| & & & & \| \\ \mathrm{H}^0_{\mathrm{fppf}}(S, (\mathbb{Z}/p\mathbb{Z})^\flat) & & \mathbb{Z}/p\mathbb{Z} & & \mathbb{Z}/p\mathbb{Z} & & & & \mathrm{H}^1_{\mathrm{fppf}}(S, \mathbb{Z}/p\mathbb{Z}) \end{array}$$

from which we quickly see that $\mathrm{H}^1_{\mathrm{fppf}}(S, (\mathbb{Z}/p\mathbb{Z})^\flat) = 0$.

Next up is μ_p. Start with the Kummer sequence

$$0 \longrightarrow \mu_p \longrightarrow \mathbb{G}_m \xrightarrow{p} \mathbb{G}_m \longrightarrow 0$$

(this is exact in the fppf topology even when it's not in the étale topology). Looking at cohomology, we get

$$0 \longrightarrow \mathrm{H}^0_{\mathrm{fppf}}(S, \mathbb{G}_m)/p\,\mathrm{H}^0_{\mathrm{fppf}}(S, \mathbb{G}_m) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(S, \mu_p) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(S, \mathbb{G}_m)[p] \longrightarrow 0.$$

Note that $\mathbb{G}_m(S) = \mathbb{Z}^\times = \{\pm 1\}$, so the pth power map on this group is a bijection when p odd (and trivial when p even). Furthermore, $\mathrm{H}^1_{\mathrm{fppf}}(S, \mathbb{G}_m) = \operatorname{Pic} S = 0$ since $\mathbb{Z}$ is a PID. This completes the computation.

fppf descent tells you that an fppf $\mathbb{G}_m$-torsor is the same thing as a line bundle

This just leaves $\mu_p^\flat$ for which we look at the exact sequence

$$0 \longrightarrow \mu_p^\flat \longrightarrow \mu_p \longrightarrow G \longrightarrow 0$$

where now G is the pushforward of μ_p along $\operatorname{Spec}\mathbb{F}_N \hookrightarrow \operatorname{Spec}\mathbb{Z}$. Taking cohomology gives

$$\begin{array}{ccccccc} \mathrm{H}^0_{\mathrm{fppf}}(S,\mu_p) & \longrightarrow & \mathrm{H}^0_{\mathrm{fppf}}(S,G) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p^\flat) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(S,G) \\ \| & & \| & & & & \| \\ \mu_p(\mathbb{Z}) & & \mu_p(\mathbb{F}_N) & & & & \mathrm{H}^0_{\mathrm{fppf}}(S,\mathbb{G}_m)/p\,\mathrm{H}^0_{\mathrm{fppf}}(S,\mathbb{G}_m) \end{array}$$

When p is odd, we get $\mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p^\flat) \simeq \mu_p(\mathbb{F}_N)$. When p is even, we get

$$\mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p^\flat) \simeq \ker\left(\mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p) \to \mathrm{H}^1_{\mathrm{fppf}}(S,G)\right).$$

Since $p=2$, we know $\mathrm{H}^1_{\mathrm{fppf}}(S,\mu_p) \cong \mathbb{Z}/2\mathbb{Z}$, and now we need to think about what this map is doing. Thinking through the Kummer theory, the nontrivial element of this group corresponds to the μ_2-torsor $\operatorname{Spec}\mathbb{Z}[i] \to S$ obtained by adjoining a square root of -1. The above maps on $\mathrm{H}^1_{\mathrm{fppf}}$'s is just restriction along $\operatorname{Spec}\mathbb{F}_N \hookrightarrow S$, so we want to know if $\operatorname{Spec}\mathbb{Z}[i] \times_S \mathbb{F}_N$ is the trivial torsor or not, i.e. if $\operatorname{Spec}\mathbb{F}_N[i]$ has an $\mathbb{F}_N$-point, i.e. if $\mathbb{F}_N$ has a square root of -1. This holds iff $N \equiv 1 \pmod 4$. ■

Proposition 11.14. *Let $G/\mathbb{Z}$ be admissible. Then, $h^1(G) - h^0(G) \le \delta(G) - \alpha(G)$.*

Proof. The idea is simply to induct over an admissible filtration, so we only need to show the claim behaves well in extensions. Suppose we have a short exact sequence

$$0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0.$$

This gives a long exact sequence

$$0 \to \mathrm{H}^0_{\mathrm{fppf}}(G_1) \to \mathrm{H}^0_{\mathrm{fppf}}(G_2) \to \mathrm{H}^0_{\mathrm{fppf}}(G_3) \to \mathrm{H}^1_{\mathrm{fppf}}(G_1) \to \mathrm{H}^1_{\mathrm{fppf}}(G_2) \to K \to 0$$

with $K \le \mathrm{H}^1_{\mathrm{fppf}}(G_3)$. Thus,

$$h^1(G_2) - h^0(G_2) = (h^1(G_1) - h^0(G_1)) + (\log_p(\#K) - h^0(G_3)) \le (h^1(G_1) - h^0(G_1)) + (h^1(G_3) - h^0(G_3)).$$

In other words, $h^1 - h^0$ is sub-additive in short exact sequences. On the other hand, α, δ are additive (directly from their definitions). Thus, the proposition will be true for G_2 if its true for G_1, G_3, so it suffices to check it for elementary admissible groups. Stare at Table 1. ■

11.2 Proof of Theorem 11.1

Let $\mathcal{A}$ be the Néron model of $A/\mathbb{Z}$. Let $\mathcal{A}^0$ be the connected component of the identity. Let $G_n = \mathcal{A}^\circ[p^n]$.

Remark 11.15. By assumption, A has good reduction away from N, so G_n is pre-admissible. Also by assumption, $A[p](\overline{\mathbb{Q}})$ is an admissible Galois module, so $A[p^n](\overline{\mathbb{Q}})$ is admissible also[13]. This implies that G_n is admissible. ∘

We want to bound the flat cohomology of G_n. By the last proposition of the previous section, to do this, it'll be useful to compute the invariants of G_n:

Question: Why use $\mathcal{A}^0[p^n]$ instead of $\mathcal{A}[p^n]$?

Answer: Andrew answers this. Keep reading

[13] Induction with $0 \to A[p] \to A[p^n] \xrightarrow{p} A[p^{n-1}] \to 0$

- $\ell(G_n) = 2gn$ where $g = \dim(A)$ (since $A[p^n]_{\mathbb{Q}}$ is finite (étale) or order $(p^n)^{2g}$)
- $\delta(G_n) = gn$

  $(G_n)_{\overline{\mathbb{F}}_N} = \mathcal{A}^0_{\overline{\mathbb{F}}_N}[p^n] = \mu_{p^n}^g$ with the last equality holding since we have toric reduction. Thus, $\#(G_n)_{\mathbb{F}_N} = gn$.
- $\alpha(G_n) = gn$

  First note $\alpha(G_n) = n\alpha(G_1)$. This is because α is additive and G_n is an iterated extension of G_1's. If $p \neq 2$, then $\alpha(G_1)$ is the number of $\mathbb{Z}/p\mathbb{Z}$'s in $(G_1)_{\mathbb{F}_p} = \mathcal{A}_{\mathbb{F}_p}[p]$, i.e.

$$\alpha(G_1) = \log_p \left(\#\mathcal{A}_{\mathbb{F}_p}[p]^{\text{ét}} \right).$$

  This $\mathcal{A}_{\mathbb{F}_p}[p]$ only has $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's and so $\mathcal{A}_{\mathbb{F}_p}$ is ordinary. This forces it to have the same number of $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's (think: Weil pairing), so $\alpha(G_1) = g$.

  Remark 11.16. $\mathcal{A}_{\mathbb{F}_p}[p]$ only has $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's since $G_1 = \mathcal{A}[p]$ is admissible, but we got admissibility here just from our assumption on $A[p](\overline{\mathbb{Q}})$, so (ultimately via Raynaud), we've started with some assumption on the Galois representation and concluded that this thing is ordinary mod p. ∘

Corollary 11.17 (by Proposition 11.14)**.** $h^1(G_n) - h^0(G_n) \leq 0$

We can do one better:

$$\mathrm{H}^0_{\text{fppf}}(S, G_n) = \mathcal{A}^0(\mathbb{Z})[p^n] \subset \mathcal{A}(\mathbb{Z})[p^n] = A(\mathbb{Q})[p^n].$$

Mordell-Weil tells us that $A(\mathbb{Q})$ is a f.g. abelian group, so $\#A(\mathbb{Q})[p^n]$ is bounded as $n \to \infty$. Thus,

Corollary 11.18. $h^1(G_n) \leq O(1)$ *as* $n \to \infty$.

Now, we bring in our old friend the Kummer sequence

$$0 \longrightarrow G_n \longrightarrow \mathcal{A}^0 \xrightarrow{p^n} \mathcal{A}^0 \longrightarrow 0.$$

Question 11.19. *Why is* $\mathcal{A}^0 \xrightarrow{p^n} \mathcal{A}^0$ *surjective?*

Answer. Each fiber of $\mathcal{A}^0$ is p-divisible; they are all either abelian varieties or tori. This is *not* true for $\mathcal{A}$. At N, $\mathcal{A}$ is an extension of a torus by a finite group. If that finite group has some p-part to it, then multiplication by p^n won't be surjective. ⋆

Taking cohomology of the Kummer sequence, one gets that

$$\mathrm{H}^0_{\text{fppf}}(\operatorname{Spec}\mathbb{Z}, \mathcal{A}^0) \otimes \frac{\mathbb{Z}}{p^n\mathbb{Z}} \hookrightarrow \mathrm{H}^1_{\text{fppf}}(\operatorname{Spec}\mathbb{Z}, G_n).$$

That is

$$\#\left(\mathcal{A}^0(\mathbb{Z}) \otimes \mathbb{Z}/p^n\mathbb{Z}\right) = O(1) \text{ as } n \to \infty$$

(i.e. this group has cardinality bounded independent of n).

Let C be the component group of $\mathcal{A}$ at N, so we have an exact sequence

$$0 \to \mathcal{A}^0(\mathbb{Z}) \to \mathcal{A}(\mathbb{Z}) \to C.$$

Note that C is finite and $\mathcal{A}(\mathbb{Z}) = A(\mathbb{Q})$ (by Néron mapping property), so $\mathcal{A}^0(\mathbb{Z})$ is finite index in $A(\mathbb{Q})$. Thus, $\mathcal{A}^0(\mathbb{Z})$ is finitely generated, so it must be finite ($\Longleftarrow$ $\#\mathcal{A}^0(\mathbb{Z})/p^n\mathcal{A}^0(\mathbb{Z}) = O(1)$), so $A(\mathbb{Q})$ must be finite, and we win.

12 Lecture 12: Modular curves over $\mathbb{C}$

We finished the 'first third' of the class last time. We've been talking about the arithmetic of elliptic curves/abelian varieties, but now we switch gears and start to talk about moduli of elliptic curves. We work over $\mathbb{C}$ today, but eventually want moduli spaces over $\mathbb{Z}$.

Let's start by considering the *set*

$$Y(1) = \{\text{isom classes of elliptic curves}/\mathbb{C}\}.$$

We'd like to give this the structure of an algebraic variety, but before that, let's mention some other moduli problems we'd like to be able to represent. Consider also the *sets*

$$Y_1(N) = \{\text{isom classes of pairs } (E, P) \text{ where } E \text{ an elliptic curve and } P \in E \text{ has order } N\}$$

(here, an iso $(E, P) \xrightarrow{\sim} (E', P')$ is an iso $f : E \xrightarrow{\sim} E'$ with $f(P) = P'$),

$$Y_0(N) = \{\text{isom classes of pairs } (E, G) \text{ where } E \text{ an elliptic curve and } G \subset E \text{ cyclic of order } N\},$$

and

$$Y(N) = \{\text{isom classes of triples } (E, P, Q) \text{ where } E \text{ an elliptic curve and } P, Q \in E[N] \text{ a basis}\}.$$

Note we have natural maps

$$Y(N) \longrightarrow Y_1(N) \longrightarrow Y_0(N) \longrightarrow Y(1).$$

12.1 $Y_{blah}(N)$ as a complex variety

Let's start with $Y(1)$. We know a description of it as a set. The j-invariant gives a bijection

$$j : Y(1) \xrightarrow{\sim} \mathbb{C}.$$

We would use this to give $Y(1)$ the structure of a complex variety (it looks like $\mathbb{A}^1_{\mathbb{C}}$), but this approach won't work as well for the $Y_{blah}(N)$. Instead, it's better to arrive at a complex structure via lattices.

Recall 12.1. Every elliptic curve $E/\mathbb{C}$ is of the form C/Λ with $\Lambda \subset \mathbb{C}$ a lattice. $\odot$

You can always replace Λ by $\alpha\Lambda$ with $\alpha \in \mathbb{C}^\times$, so we may assume $\Lambda = \langle 1, z\rangle$ with $z \in \mathbb{C} \setminus \mathbb{R}$. Replacing z by $-z$ if necessary, we may assume it lies in the upper half plane

$$\mathfrak{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

Notation 12.2. Given $z \in \mathfrak{H}$, we let $\Lambda_z := \langle 1, z\rangle \subset \mathbb{C}$ and $E_z := \mathbb{C}/\Lambda_z$.

Note we have a surjective map

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & Y(1) \\ \tau & \longmapsto & E_\tau. \end{array}$$

Warning 12.3. This map is not injective. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then $\langle 1, z\rangle = \langle az+b, cz+d\rangle$, so

$$(cz+d)^{-1}\,\Lambda_z = \left\langle 1, \frac{az+b}{cz+d} \right\rangle$$

and hence $E_z \simeq E_{\frac{az+b}{cz+d}}$. •

Notation 12.4. Let $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ and $z \in \mathfrak{H}$, we get

$$\gamma z := \frac{az+b}{cz+d}.$$

This defines an action $\Gamma(1) \curvearrowright \mathfrak{H}$.

Theorem 12.5. *The natural map $\mathfrak{H}/\Gamma(1) \to Y(1)$ is a bijection.*

Proof. We already have surjectivity. For injectivity, suppose $E_z \simeq E_{z'}$, i.e. $\Lambda_z = \alpha\Lambda_{z'}$ for some $\alpha \in \mathbb{C}^\times$. Then, we can write

$$1 = \alpha(cz+d) \text{ for some } c, d \in \mathbb{Z}.$$

We must have $\gcd(c,d) = 1$ since one can show $1/\gcd(c,d) \in \Lambda_z$. Now pick a, b s.t. $ad - bc = 1$, so $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Thus, $\Lambda_z = \alpha\Lambda_{z'} = \Lambda_{\gamma(z')}$. This says we can write

$$z = n\gamma(z') + m \text{ and } \gamma(z') = n'z + m' \text{ for some } n, n', m, m' \in \mathbb{Z}.$$

This implies $z = nn'z + (nm' + m)$. Taking imaginary parts, we see $nn' = 1$, so $n = n' = \pm 1$. Thus, $z = n\gamma(z') + m = \pm\gamma(z') + m$. Since $z, \gamma(z') \in \mathfrak{H}$, the sign here must be positive, so $z = \gamma(z') + m = \gamma'\gamma(z')$ where

$$\gamma' = \begin{pmatrix} 1 & m \\ & 1 \end{pmatrix}.$$ ■

Thus we've seen two descriptions $\mathbb{C} = Y(1) = \mathfrak{H}/\Gamma(1)$. Let's say a bit about these two. Pull the j-invariant back to $\mathfrak{H}$

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & j(E_z). \end{array}$$

If one writes things out explicitly, they can see that this is actually a holomorphic function on $\mathfrak{H}$ (which is invariant under $\Gamma(1)$). Alternatively, one can see that $\mathfrak{H}/\Gamma(1)$ is a punctured genus 0 curve using fundamental domains.

Fact. $\Gamma(1)$ is generated by $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ and $\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$, giving the functions $z \mapsto z+1$ and $z \mapsto -1/z$.

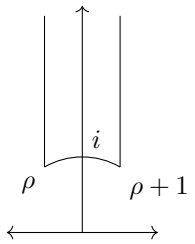


Figure 1: A fundamental domain for $\Gamma(1) \curvearrowright \mathfrak{H}$. Here, $\rho = \exp(2\pi i/3)$

Using the first of these, one can move any point $z \in \mathfrak{H}$ to one with $|\mathrm{Re}(z)| \leq \frac{1}{2}$. Then, one can use the second one to ensure $|z| > 1$. With this, one can show that

$$F := \left\{ z \in \mathfrak{H} : |z| > 1 \text{ and } -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2} \right\}$$

is a fundamental domain for $\Gamma(1) \curvearrowright \mathfrak{H}$, pictured in Figure 1. The only $\Gamma(1)$-identifications in F are between the two vertical sides (via $z \mapsto z+1$) and between the two halves of the circular arc (with positive/negative real part) via $z \mapsto -1/z$. Topologically, thinking about these boundary identifications, the two vertical sides come together to form a cylinder, and the the arc identifications let you sew up the base, so you end up with a flat plane.

Let's move on from $Y(1)$ to $Y_1(N)$. There's a surjective map

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & Y_1(N) \\ z & \longmapsto & (E_z, \frac{1}{N}) \end{array}$$

(recall $Y_1(N)$ is moduli of ECs w/ a given N-torsion point). Note that if $\gamma \in \Gamma(1)$, then $\gamma z \mapsto \left(E_{\gamma z}, \frac{cz+d}{N}\right)$. This will be the same point of $Y_1(N)$ if $N \mid c$ and $d \equiv 1 \pmod{N}$. This motivates considering the group

$$\Gamma_1(N) := \left\{ \gamma \in \Gamma(1) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Theorem 12.6. *The map $\mathfrak{H}/\Gamma_1(N) \to Y_1(N)$ is an isomorphism.*

One gets similar results for $Y_0(N)$ and $Y(N)$. Define

$$\Gamma_0(N) := \left\{ \gamma : \gamma \equiv \begin{pmatrix} * & * \\ & * \end{pmatrix} \pmod{N} \right\} \text{ and } \Gamma(N) := \{\gamma : \gamma \equiv 11 \pmod{N}\}.$$

Then, $\mathfrak{H}/\Gamma_0(N) \xrightarrow{\sim} Y_0(N)$ and $\mathfrak{H}/\Gamma(N) \xrightarrow{\sim} Y(N)$.

12.2 Y_Γ

Setup 12.7. Let $\Gamma \subset \Gamma(1)$ be any finite index subgroup. Define $Y_\Gamma := \mathfrak{H}/\Gamma$ and let $\pi : \mathfrak{H} \to Y_\Gamma$ be the quotient map.

We can give Y_Γ the structure of a complex manifold. We say a function $f : Y_\Gamma \to \mathbb{C}$ is holomorphic if

the pullback $\pi^* f : \mathfrak{H} \to \mathbb{C}$ is holomorphic.

Fact. This makes Y_Γ a Riemann surface.

Warning 12.8. This is not entirely straightforward. If $\Gamma \curvearrowright \mathfrak{H}$ has fixed points, then this causes some issues that need to be dealt with. •

There are other sorts of complications.

- Y_Γ is never compact

  To remedy this, define $\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$. The points of $\mathbb{P}^1(\mathbb{Q})$ are called **cusps**. We topologize this by saying a nbhd basis at a cusp $x \in \mathbb{P}^1(\mathbb{Q})$ consists of discs in $\mathfrak{H}$ tangent to $\mathbb{P}^1(\mathbb{R})$ at x. More precisely, a nbhd basis of ∞ is given by sets

  $$U_k := \{z : \mathrm{Im}(z) > K\} \cup \{\infty\}$$

  (and then get neighborhood bases at other cusps by translating these[14] since $\Gamma(1) \curvearrowright \mathbb{P}^1(\mathbb{Q})$ transitively).

Notation 12.9. $X_\Gamma := \mathfrak{H}^*/\Gamma$

Fact. X_Γ is a compact Riemann surface.

Note $\mathbb{P}^1(\mathbb{Q})/\Gamma$ will be a finite set, so X_Γ has finitely many cusps.

Exercise. Try and think about a moduli-theoretic interpretation of the cusps (we'll talk about this more later, but good to have it mind already).

12.3 Genera of X_Γ

We want to understand the geometry of these Riemann surfaces a little. To do that, we'll need to better understand the actions $\Gamma \curvearrowright \mathfrak{H}^*$. We start with the stabilizers

$$\Gamma(1)_z := \{\gamma \in \Gamma(1) : \gamma z = z\}.$$

Remark 12.10. Note that $-1 \in \Gamma(1)_z$ always, since

$$\begin{pmatrix} -1 & \\ & -1 \end{pmatrix} z = \frac{-z+0}{0z-1} = z. \qquad \circ$$

Let

$$\overline{\Gamma(1)} := \Gamma(1)/\{\pm 1\}.$$

Proposition 12.11. $\Gamma(1)_z \cong \mathrm{Aut}(E_z)$ *(note, no bar on the* Γ*)*

Proof. Consider some $\gamma \in \Gamma(1)_z$ and write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This defines a function $g : \Lambda_z \to \Lambda_z$ sending $g(z) = az + b$ and $g(1) = cz + d$. Since $\gamma(z) = z$, we can write $g(z) = az + b = z(cz + d)$. This means that g is actually $\mathbb{C}$-linear, and so induces an automorphism of E_z. One can reverse this reasoning to go in the other direction. ■

[14] A nbhd basis of $\gamma(\infty)$ is $\gamma(U_k)$ for $\gamma \in \Gamma(1)$

Recall 12.12. $\mathrm{Aut}(E_z) = \mathrm{End}(E_z)^\times$ is the units of an order $\mathscr{O}$ in an imaginary quadratic field. Note that

$$\mathscr{O}^\times = \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } \mathscr{O} = \mathbb{Z}[i] \\ \mathbb{Z}/6\mathbb{Z} & \text{if } \mathscr{O} = \mathbb{Z}[\rho] \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

where $\rho = e^{2\pi i/6}$. ⊙

Proposition 12.13. *Say $E/\mathbb{C}$ is an elliptic curve. Then,* $\mathrm{End}(E) = \mathbb{Z}[i] \implies E \cong E_i$.

Proof. Write $\mathbb{C}/\Lambda$ with Λ a $\mathbb{Z}[i]$-module. Since Λ is torsion-free over a Dedekind domain, it's projective. Since $\mathrm{Pic}\,\mathbb{Z}[i] = 0$, Λ must be free, so $\Lambda = \alpha\mathbb{Z}[i] = \alpha\Lambda_i$ for some α. ■

Proposition 12.14. $\mathrm{End}(E) = \mathbb{Z}[\rho] \implies E \cong E_\rho$.

(Same proof)

Proposition 12.15. *Say $z \in \mathfrak{H}$. Then,*

- $z \in \Gamma(1)i \iff \overline{\Gamma(1)}_z = \mathbb{Z}/2\mathbb{Z}$
- $z \in \Gamma(1)\rho \iff \overline{\Gamma(1)}_z = \mathbb{Z}/3\mathbb{Z}$
- $z \notin \Gamma(1)i \cup \Gamma(1)\rho \iff \overline{\Gamma(1)}_z = 0$

(up to action of $\Gamma(1)$, only two problem points, ignoring cusps).

Problem 12.1. *If z is a cusp, then $\overline{\Gamma(1)}_z \cong \mathbb{Z}$*

Proof. All cusps are conjugate, so may take $z = \infty$. Then, $z + n = z$, so $\begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} \in \Gamma(1)_z$. In general, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, then

$$\gamma(\infty) = \frac{a}{c}$$

which equals infinity $\iff c = 0$. This forces $\gamma = \begin{pmatrix} a & b \\ & a \end{pmatrix}$ with $a = \pm 1$, so $\pm\gamma$ is of the form $\begin{pmatrix} 1 & n \\ & 1 \end{pmatrix}$. ■

Now go back to some finite index subgroup $\Gamma \subset \Gamma(1)$.

Definition 12.16. A point $z \in \mathfrak{H}$ is **elliptic** for Γ if $\overline{\Gamma}_z \neq 0$ (its **order** is $\#\overline{\Gamma}_z$). ◇

Only get elliptic points of order 2 or 3. If it has order 2, then $z \in \Gamma(1)i$ and if it has order 3, then $z \in \Gamma(1)\rho$ (converses do not hold for $\Gamma \neq \Gamma(1)$).

Proposition 12.17. *Say $\Gamma \subset \Gamma'$ both finite index in $\Gamma(1)$. Get induced map*

$$f : X_\Gamma \to X_{\Gamma'}.$$

Let $z \in \mathfrak{H}$ with image $p \in X_\Gamma$. Then, the ramification index of p for f is simply $[\overline{\Gamma}'_z : \overline{\gamma}_z]$.

Proof. Choose neighborhood $U \subset \mathfrak{H}$ of z stable under $\overline{\Gamma}'_z$. Consider the diagram

$$\begin{array}{ccc} U/\overline{\Gamma}_z & \longrightarrow & X_\Gamma \\ \downarrow & & \downarrow \\ U/\overline{\Gamma}'_z & \longrightarrow & X_{\Gamma'} \end{array}$$

The horizontal maps will be local homoeomorphisms. The left vertical is visibly generically $[\overline{\Gamma}'_z : \overline{\Gamma}_z]$-to-one. ∎

Corollary 12.18 (**genus formula**). *Let $\Gamma \subset \Gamma(1)$ be an index d subgroup. Let ν_2 be the number of Γ-orbits of elliptic points of order 2, ν_3 be defined similarly, and let ν_∞ be the number of Γ-orbits of cusps. Finally, let $g = g(X_\Gamma)$ be the genus of X_Γ. Then,*

$$g = 1 + \frac{d}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Proof. $X(1) \cong \mathbb{P}^1$, so apply Riemann-Hurwitz to $f : X_\Gamma \to X(1) \cong \mathbb{P}^1$:

$$2 - 2g = 2d - \sum_{p \in X_\Gamma} (e_p - 1).$$

We only have ramification at the cusps and elliptic points. Let q_2 be the image of i in $X(1)$, let q_3 be the image of ρ in $X(1)$, and let q_∞ be the image of ∞ in $X(1)$. This gives us 3 sums to compute.

For q_2, elliptic points will be unramified (the index of the stabilizer groups is 1), while non-elliptic points over q_2 will have $e = 2$. The total number of points over q_2 (counting w/ multiplicity) is d. Thus, $\nu_2 + 2\#(\text{ram pts}) = d$, so

$$\#\text{ram pts} = \frac{d - \nu_2}{2} \implies \sum_{f(p)=q_2} (e_p - 1) = \frac{d - \nu_2}{2}.$$

A similar computation shows

$$\sum_{f(p)=q_3} (e_p - 1) = \frac{2(d - \nu_3)}{3}.$$

Over ∞, one writes

$$\sum_{f(p)=q_\infty} (e_p - 1) = \sum_{f(p)=q_\infty} e_p - \sum_{f(p)=q_\infty} 1 = d = \nu_\infty.$$

Put together, we have

$$2 - 2g = 2d - \frac{d - \nu_2}{2} - \frac{2(d - \nu_3)}{3} - (d - \nu_\infty).$$

Rearrange to win. ∎

Example (Exercise)**.** Fix N prime and take $\Gamma = \Gamma_0(N)$. In this, one gets

$$d = N+1,\ \ \nu_\infty = 2,\ \ \nu_2 = \begin{cases} 1 & \text{if } N = 2 \\ 2 & \text{if } N \equiv 1 \pmod 4 \\ 0 & \text{otherwise.} \end{cases},\ \text{and}\ \ \nu_3 = \begin{cases} 1 & \text{if } N = 3 \\ 2 & \text{if } N \equiv 1 \pmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$g(X_0(N)) = \left\lfloor \frac{N}{12} \right\rfloor + \begin{cases} -1 & \text{if } N \equiv 1 \pmod{12} \\ 1 & \text{if } N \equiv 11 \pmod{12}. \end{cases}$$

where N prime. e.g. if $N \leq 13$, then $g = 0$ unless $N = 11$ (where $g = 1$). △

Example (Exercise)**.**

$$g(X_1(N)) = 0 \iff N \leq 12 \text{ and } N \neq 11.$$

These are exactly the values of N where an elliptic curve can have an N-torsion point over $\mathbb{Q}$ (by Mazur's theorem). This is not a coincidence. △

13 Lecture 13: Modular forms

Still working over $\mathbb{C}$ today. We'll focus mostly on modular forms of level 1.

Recall 13.1.

$$\mathfrak{H}/\Gamma(1) \xrightarrow{\sim} \{\text{lattices in } \mathbb{C}\}/\text{homothety} \xrightarrow{\sim} \{\text{isom classes of ECs}\} =: Y(1) \cong \mathbb{A}^1. \qquad \odot$$

Notation 13.2. We let $\mathscr{L}$ denote the set of lattices in $\mathbb{C}$.

Recall 13.3. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, then $\Lambda_{\gamma z} = (cz+d)^{-1}\Lambda_z$. $\odot$

Definition 13.4. A **modular function** is a meromorphic function on $Y(1)$ (including at ∞). These are all just rational functions in j (since $X(1) \cong \mathbb{P}^1$). ◇

A modular form will be a function on lattices which scales predictably under homothety.

Definition 13.5. A **modular form of weight** k is a function $f : \mathscr{L} \to \mathbb{C}$ s.t.

(1) $f(\alpha\Lambda) = \alpha^{-k} f(\Lambda)$

(2) $z \mapsto f(\Lambda_z)$ is holomorphic on $\mathfrak{H}$

(3) (holomorphic at ∞) $\lim_{z\to\infty} f(z)$ exists. We call this $f(\infty)$

We let M_k denote the vector space of weight k modular forms. A **cusp form** is a modular form f with $f(\infty) = 0$. We let S_k denote the vector space of weight k cusp forms. ◇

Let's see a few perspectives on these things.

Abuse of Notation 13.6. For $z \in \mathfrak{H}$ and f a modular form, we write $f(z) := f(\Lambda_z)$. Note that, for $\gamma \in \Gamma$,

$$f(\gamma z) = f(\Lambda_{\gamma z}) = f\left((cz+d)^{-1}\Lambda_z\right) = (cz+d)^k f(z).$$

Modular interpretation of modular forms Start with the space of lattices $\mathscr{L}$. Over this, one has the trivial vector bundle $\mathbb{C} \times \mathscr{L}$. Below this, one can construct a natural family of elliptic curves $\mathcal{E} \to \mathscr{L}$ where

$$\mathscr{E} := (\mathbb{C} \times \mathscr{L})/\sim \quad \text{where } (z, \Lambda) \sim (z', \Lambda') \iff \Lambda = \Lambda' \text{ and } z \in \Lambda + z'.$$

These fit into a diagram

$$\begin{array}{ccc} \mathbb{C} \times \mathscr{L} & \longrightarrow & \mathscr{E} \\ & \searrow \quad \swarrow & \\ & \mathscr{L} & \end{array}$$

Let w be a parameter on $\mathbb{C}$. The differential $\mathrm{d}w$ on $\mathbb{C} \times \mathscr{L}$ descends to $\mathscr{E}$. If $\alpha \in \mathbb{C}^\times$, it gives a homothety $\alpha : \mathscr{L} \to \mathscr{L}$ with $\alpha^*(\mathrm{d}w) = \alpha \mathrm{d}w$, so this differential is not invariant under homothety. However, if f is a weight k modular form, then $f(\mathrm{d}w)^{\otimes k}$ will be invariant under homothety, and so you expect it to descend to the quotient.

Warning 13.7. To make this work properly, you need to work with stacks. Let $\pi : \mathscr{E} \to Y(1)$ be the universal family (viewing $Y(1)$ as a stack here). Define $\omega := \pi_* \Omega^1_{E/Y(1)}$. This is a vector bundle on $Y(1)$ whose fiber over an elliptic curve $[E] \in Y(1)$ is the space $\mathrm{H}^0(E, \Omega^1_E)$ of holomorphic 1-forms. Now, $f(\mathrm{d}w)^k$ defines a section of $\omega^{\otimes k}$ over $Y(1)$. This in fact defines a bijection (assuming you impose some condition at ∞). More on this after discussing the moduli interpretation of cusps. •

Let's try to say this more concretely. Say f is a modular form of weight k, let E be an elliptic curve, and let $\omega \in \mathrm{H}^0(E, \Omega^1)$ be nonzero. We can write $E \cong \mathbb{C}/\Lambda$, and then get two elements

$$f(\Lambda)(\mathrm{d}w)^k, \omega^k \in \mathrm{H}^0(E, \Omega^1)^{\otimes k}$$

in this 1-dimensional vector space. Thus, they must differ from each other by a scalar, i.e.

$$f(\Lambda)(\mathrm{d}w)^k = F(E, \omega)\omega^{\otimes k}.$$

This $F(-,-)$ thing has two properties

- If $(E, \omega) \cong (E', \omega')$, then $F(E, \omega) = F(E', \omega')$
- $F(E, \alpha\omega) = \alpha^{-k} F(E, \omega)$
- Some holomorphic condition

This $F(-,-)$ gives another description of sections of $\omega^{\otimes k}$.

A second interpretation of modular forms Say $f : \mathfrak{H} \to \mathbb{C}$ is a modular form, so $f(\gamma z) = (cz + d)^k f(z)$. Note that

$$\gamma^*(\mathrm{d}z) = (cz + d)^{-2} \mathrm{d}z$$

with $\mathrm{d}z$ the differential on $\mathbb{C}$. This is just an explicit computation. Thus, if f has weight $2k$, then $f(\mathrm{d}z)^k$ is invariant under $\Gamma(1)$, and so defines a meromorphic section of $(\Omega^1)^{\otimes k}$ on $X(1)$.

Proposition 13.8. *Pick $x \in \mathfrak{H}$ with image $y = \pi(x) \in X(1)$. Then,*

$$\operatorname{ord}_y(\omega) = \begin{cases} \frac{1}{2}\left(\operatorname{ord}_x(f) - k\right) & \text{if } x = i \\ \frac{1}{3}(\operatorname{ord}_x(f) - 2k) & \text{if } x = \rho \\ \operatorname{ord}_x(f) - k & \text{if } x = \infty \end{cases}$$

and $\operatorname{ord}_y(\omega) = \operatorname{ord}_x(f)$ in all other cases.

Proof when $x = i$. Say z is a local parameter on $\mathfrak{H}$ at x, and say w is one on $X(1)$ at y. The projection map $\pi : \mathfrak{H}^* \to X(1)$ is ramified with ramification index 2 at the point i. Hence, $\pi^*(w) = z^2 + \dots$. Thus, $\pi^*(\mathrm{d}w) = z\mathrm{d}z + \dots$. If $\operatorname{ord}_y(\omega) = n$, then $\omega = w^n(\mathrm{d}w)^k$. Hence,

$$f(\mathrm{d}z)^k = \pi^*\omega = z^{2n+k}(\mathrm{d}z)^k,$$

so $\operatorname{ord}_x(f) = 2n + k$. ∎

Corollary 13.9.

$$M_{2k} \cong \left\{ \text{sections } \omega \text{ of } \left(\Omega^1_{X(1)}\right)^{\otimes k} \,\middle|\, \begin{array}{c} \operatorname{ord}_{\pi(i)}(\omega) \geq -\frac{k}{2},\ \ \operatorname{ord}_{\pi(\rho)}(\omega) \geq -\frac{2k}{3},\ \ \operatorname{ord}_{\pi(\infty)}(\omega) \geq -k \\ \omega \text{ is holomorphic elsewhere} \end{array} \right\}$$

(these conditions are what's needed to ensure $\operatorname{ord}(f) \geq 0$ everywhere).

Corollary 13.10.

$$\dim M_{2k} = \left\lfloor \frac{k}{6} \right\rfloor + \varepsilon \text{ where } \varepsilon = \begin{cases} 1 & \text{if } k \not\equiv 1 \pmod 6 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $P = \pi(i)$, $Q = \pi(\rho)$, and $\infty = \pi(\infty)$. Let $n = \lfloor k/2 \rfloor$ and $m = \lfloor 2k/3 \rfloor$. The previous corollary says that

$$M_{2k} = \mathrm{H}^0\left(\mathbb{P}^1, (\Omega^1)^{\otimes k}\left(nP + mQ + k\infty\right)\right).$$

This bundle has degree

$$-2k + n + m + k = n + m - k,$$

so $\dim(M_{2k}) = 1 + n + m - k$. Now one just simplifies. ∎

Remark 13.11. The dimension of the space of cusp forms is always one less, since you add in one extra condition (vanish at ∞). ∘

Example. $\dim M_2 = 0$. $\dim M_{2k} = 1$ if $2 \leq k \leq 5$. $\dim M_{12} = 2$. Similarly, $\dim S_{2k} = 0$ for $k < 6$ while $\dim S_{12} = 1$. △

13.1 Eisenstein series and Δ

At some point, we should probably write down some modular forms.

Example. Say $\Lambda \subset \mathbb{C}$ is a lattice, and fix some even[15] $k \geq 4$. Set

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

The prime $'$ above means don't include $\lambda = 0$ in the sum. Since k is big, this will have nice convergence properties (exercise, I guess, if you want). It's clear that $G_k(\alpha\Lambda) = \alpha^{-k} G_k(\Lambda)$, so so far so good. Note that

$$G(z) = G(\Lambda_z) = \sum_{n,m}{}' \frac{1}{(nz+m)^k}.$$

This will be holomorphic in z (each term holomorphic + good convergence properties). Furthermore,

$$\lim_{z \to \infty} G(z) = \sum_{m \neq 0} \frac{1}{m^k} = 2\zeta(k).$$

Thus, G_k is a (non-cuspidal) modular form of weight k, called the **Eisenstein series of weight** k.

For $k < 12$, this gives all modular forms of weight k since we know the dimensions of the spaces of modular forms. In fact, more is true; one can show that

$$\bigoplus_{k \geq 0} M_k \cong \mathbb{Z}[G_4, G_6]$$

as (graded) rings.

One can also define the **normalized Eisenstein series of weight** k

$$E_k := \frac{1}{2\zeta(k)} G_k. \qquad \triangle$$

Remark 13.12. If $f \in M_k$, it's invariant under $z \mapsto z+1$, so it has a Fourier expansion

$$f = \sum_{n \in \mathbb{Z}} a_n q^n \text{ where } q = e^{2\pi i z}.$$

Being holomorphic at ∞ means that $a_n = 0$ for $n < 0$. Being cuspidal means $a_0 = 0$. $\circ$

Fact.

$$E_k(z) = 1 - \frac{4k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

where B_k is the kth **Bernoulli number**, defined by

$$\frac{x}{e^x - 1} = \sum_{k \geq 0} B_k \frac{x^k}{k!},$$

and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Example. Let $\Delta = E_4^3 - E_6^2$. This is a modular form of weight 12. Since we normalized our Eisenstein series, we have $\Delta(\infty) = 0$, so Δ is a cusp form. Furthermore, $\Delta \neq 0$ by looking at q-expansions

[15] If k odd, λ and $-\lambda$ cancel out below, and you just get 0

$(\Delta = q + \dots)$. This Δ is the unique (up to scaling) nonzero cusp form of weight 12. $\triangle$

Fact (Jacobi)**.** $\Delta(z) = q\prod_{n\geq 1}(1-q^n)$

13.1.1 In the modular interpretation

Recall 13.13. Every elliptic curve over $\mathbb{C}$ is isomorphic to some

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Given $u \in \mathbb{C}^\times$, there's an iso $\varphi : E_{a,b} \xrightarrow{\sim} E_{u^4a,u^6b}$ sending $\varphi(x) = u^2x$ and $\varphi(y) = u^3y$. $\odot$

Consider the differential $\omega_{a,b} \in \mathrm{H}^0(E_{a,b}, \Omega^1)$. Then,

$$\varphi^*\omega_{u^4a,u^6b} = u^{-1}\omega_{a,b}.$$

Corollary 13.14. *Given a pair (E,ω), there is a unique (a,b) s.t.*

$$(E,\omega) \cong (E_{a,b}, \omega_{a,b}).$$

This let's us define functions

$$E_4'(E,\omega) := a \text{ and } E_6'(E,\omega) := b.$$

While we're at it, let's also define $\Delta'(E,\omega) :=$ discriminant of $E_{a,b}$. Note

$$(E,\omega) \cong (E_{a,b},\omega_{a,b}) \implies (E,u\omega) = (E_{u^{-4}a,u^{-6}b}, blah),$$

so

$$E_4'(E,u\omega) = u^{-4}E_4'(E,\omega) \text{ and } E_6'(E,u\omega) = u^{-6}E_6'(E,\omega) \text{ and } \Delta'(E,u\omega) = u^{-12}\Delta'(E,\omega).$$

Thus, these are modular forms under the moduli interpretation from before.

Fact. $E_4' = E_4$, $E_6' = E_6$ and $\Delta' = \Delta$ (all up to scaling)

(Easiest way to see this is to appeal to dimension counts, I guess).

13.2 Higher Level Modular Forms

Most everything we've said carries over to an arbitrary finite index subgroup $\Gamma \subset \Gamma(1)$.

Definition 13.15. Say Γ has **level** N if $\Gamma(N) \subset \Gamma$ $\diamond$

Definition 13.16. A **modular form of weight** k **for** Γ is a function $f : \mathfrak{H} \to \mathbb{C}$ s.t.

(1) $f(\gamma z) = (cz+d)^k f(z)$ for all $\gamma \in \Gamma$

(2) f is holomorphic on $\mathcal{H}$

(3) f is holomorphic at the cusps[16]

f is a **cusp form** if it vanishes at every cusp. ◇

Notation 13.17. We let $M_k(\gamma), S_k(\Gamma)$ denote the spaces of modular/cuspidal forms of weight k for Γ.

These can be identified with sections of the Hodge bundle $\omega^{\otimes k}$ on X_Γ (w/ certain conditions at the cusps). Concretely, f defines a function $\{(E, ?, \omega)\} \to \mathbb{C}$ (with ? auxiliary data determined by Γ) satisfying certain transformation laws. Weight $2k$ modular forms will correspond to sections of $(\Omega^1_{X_\Gamma})^{\otimes k}$ w/ certain local conditions.

Proposition 13.18 (Most important case)**.** $S_2(\Gamma) \cong \mathrm{H}^0(X_\Gamma, \Omega^1)$.

(Proof: exercise)
In particular, $\dim S_2(\Gamma) = g(X_\Gamma)$.

13.3 Hecke operators

Recall 13.19. $\mathscr{L}$ denote the set of lattices on $\mathbb{C}$. ⊙

Notation 13.20. We let $\mathbb{Z}[\mathscr{L}]$ be the free abelian group on $\mathscr{L}$.

Definition 13.21. Fix an integer $n \in \mathbb{Z}_{>0}$. Let $T(n) : \mathbb{Z}[\mathscr{L}] \to \mathbb{Z}[\mathscr{L}]$ be the operator determined by

$$T(n)[\Lambda] := \sum_{[\Lambda':\Lambda]=n} [\Lambda'].$$

For $\alpha \in \mathbb{C}^\times$, we also define $H_\alpha[\Lambda] := [\alpha\Lambda]$. ◇

Proposition 13.22.

(a) *$T(nm) = T(n)T(m)$ if $(n, m) = 1$*

(b) *$T(p^{n+1}) = T(p)T(p^n) - pT(p^{n-1})H_p$*

(c) *$T(n)$ and $T(m)$ commute for any n, m*

Proof. **(a)** Say $\Lambda'' \subset \Lambda$ has index nm. By CRT, Λ/Λ'' has a unique subgroup or order n, i.e. there's a unique Λ' with $\Lambda'' \subset \Lambda' \subset \Lambda$ with Λ' index m in Λ. Thus,

$$\sum_{[\Lambda'':\Lambda]=nm} [\Lambda''] = \sum_{[\Lambda':\Lambda]=m} \sum_{[\Lambda'':\Lambda']=n} [\Lambda''].$$

This says $T(n)T(m)[\Lambda] = T(nm)[\Lambda]$.

(b) We'll only prove this when $n = 1$, i.e. we'll show $T(p)^2 = T(p^2) + pH_p$. Note

$$T(p)^2[\Lambda] - \sum_{\Lambda'' \overset{p}{\subset} \Lambda' \overset{p}{\subset} \Lambda} [\Lambda''].$$

[16] It's holomorphic at ∞ if $\lim_{z\to\infty} f(z)$ exists. For other cusp x, write $x = \gamma(\infty)$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, let $g(z) = (cz+d)^{-k} f(\gamma z)$, and then f is holomorphic at $x \iff g$ is holomorphic at ∞. If f is a modular form for Γ, then g is one for $\gamma^{-1}\Gamma\gamma$

This is equivalently

$$T(p)^2[\Lambda] = \sum_{\Lambda'' \overset{p^2}{\subset} \Lambda} \# \left\{ \begin{array}{c} \text{order } p \text{ subgroups} \\ \text{of } \Lambda/\Lambda'' \end{array} \right\} [\Lambda''].$$

There are two groups of order p^2, so

$$\#\text{such subgroups} = \begin{cases} 1 & \text{if } \Lambda/\Lambda'' \cong \mathbb{Z}/p\mathbb{Z}^2 \\ p+1 & \text{if } \Lambda/\Lambda'' \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \end{cases}$$

(note second case $\iff \Lambda'' = p\Lambda$). On the other hand,

$$T(p^2)[\Lambda] = \sum_{\Lambda'' \overset{p^2}{\subset} \Lambda} [\Lambda''].$$

From this, we see that $T(p)^2 - T(p^2) = pH_p$.

(c) By **(b)**, $T(p^n)$ is a polynomial in $T(p)$ and H_p. Hence, $T(p^n)$ and $T(p^m)$ commute. Now, by **(a)**, we win. ■

Let's now define an action of these Hecke operators on modular forms.

Definition 13.23. If f is a modular form for $\Gamma(1)$ of weight k, then

$$(T(n)f)(\Lambda) = n^{k-1} \sum_{[\Lambda':\Lambda]=n} f(\Lambda')$$

(the n^{k-1} factor just makes some things nicer later on). ◇

It's clear that $(T(n)f)(\alpha\Lambda) = \alpha^{-k}(T(n)f)(\Lambda)$. To see that these preserve the holomorphic condition, you can just explicitly compute their action on q-expansions.

Proposition 13.24. *If $f = \sum_{n\geq 0} a_n q^n$ and p is prime, then*

$$T(p)f = \sum_{n\geq 0} \left(a_{pn} + p^{k-1} a_{n/p}\right) q^n$$

(Above, $a_{n/p} = 0$ if $p \nmid n$).

(Can write a similar but uglier expression for general n)

Proof. I was too lazy to type it up... ■ TODO: Be less lazy

This gives some big commuting algebra of operators acting on a finite-dimensional space of modular forms. The utility of this is that it will enable us to find a basis of the space of *cusp* forms consisting of things which are simultaneous eigenvectors for all these $T(n)$'s.

14 Lecture 14: Modular curves over $\mathbb{Q}$

(Reference for today: Katz-Mazur 'Arithmetic Moduli of Elliptic Curves')

Let's move from modular curves over $\mathbb{C}$ to them over $\mathbb{Q}$.

Recall 14.1. We talked about $Y(1)$ as a Riemann surface whose points correspond to elliptic curves. $\odot$

To make sense of this algebraically, we should first decide what the functor of points of $Y(1)$ is. A map $S \to Y(1)$ should be a family of elliptic curves over S (equivalently, an elliptic curve over S).

Definition 14.2. An **elliptic curve**$/S$ is a proper, smooth $E \to S$ with a section $0 \in E(S)$ so that each geometric fiber is a connected, genus 1 curve. $\diamond$

Consider the functor

$$F_{\Gamma(1)}(S) := \{\text{isom classes of } E/S\}.$$

We would like $F_{\Gamma(1)}$ to be representable, and then we'd define $Y(1)$ to be its representing object.

Warning 14.3. $F_{\Gamma(1)}$ is not representable. This is e.g. because the map $F_{\Gamma(1)}(\mathbb{Q}) \to F_{\Gamma(1)}(\mathbb{C})$ is not injective (two non-isomorphic elliptic curves over $\mathbb{Q}$ can have the same j-invariant). However, if it were representable (or even just a sheaf), this would be injective. $\bullet$

Let's take a bit of a closer look of why we don't have injectivity.

Definition 14.4. We say $E, E'/k$ are **twisted forms** of each other if $E_{k^s} \cong E'_{k^s}$. $\diamond$

The existence of such things is what's obstructing representability.

Remark 14.5. Say $E, E'/k$ are twisted forms, and pick an isomorphism $\varphi : E_{k^s} \xrightarrow{\sim} E'_{k^s}$. For any $\sigma \in \mathrm{Gal}(k^s/k)$, φ^σ is another isomorphism $E_{k^s} \xrightarrow{\sim} E'_{k^s}$, so we get $\psi_\sigma := \varphi^\sigma \varphi^{-1} \in \mathrm{Aut}(E_{k^s})$. One can check that this is a cocycle and that there's a bijection

$$\{\text{isom classes of twisted forms}\} \xrightarrow{\sim} \mathrm{H}^1(\mathrm{Gal}(k^s/k), \mathrm{Aut}(E_{k^s})).$$

Hence, these twisted forms are coming from non-trivial automorphisms. $\circ$

In general with moduli problems, if the parameterized objects have non-trivial automorphism groups, you always get twisted forms and so the sheaf axiom always fails. This suggests that it might be helpful to rigidify things (e.g. add level structure so there are no nontrivial automorphisms).

Example. Say we have an elliptic curve E/k with $\mathrm{End}(E_{k^s}) = \mathbb{Z}$, so $\mathrm{Aut}(E_{k^s}) = \{\pm 1\}$ and the Galois group acts trivially on this. Hence,

$$\mathrm{H}^1(\mathrm{Gal}(k^s/k), \{\pm 1\}) = k^\times/(k^\times)^2$$

by Kummer theory. Thus, the twisted forms of E correspond to square classes in k. Explicitly, if $E : y^2 = f(x)$ and $d \in k^\times$, then the twist corresponding to d is given by $E^{(d)} : dy^2 = f(x)$. $\triangle$

Fix some integer $N \geq 2$.

Assumption. Always assume N is invertible on whatever base we're working over.

Definition 14.6. A $\Gamma(N)$**-structure** on E/S is a pair (P, Q) of $E(S)[N]$ which give a basis for the N-torsion, i.e. the map

$$(P, Q) : (\mathbb{Z}/N\mathbb{Z})^2_S \to E[N]$$

is an isomorphism of group schemes (can check this on each geometric fiber). $\diamond$

Exercise. If $N \geq 3$ and $f \in \mathrm{Aut}_S(E)$ fixing a $\Gamma(N)$-structure, then $f = \mathrm{id}$.

So elliptic curves equipped with $\Gamma(N)$-structure are rigid (when $N \geq 3$). Define

$$F_{\Gamma(N)}(S) := \{\text{isom classes of } (E, (P, Q)) \text{ over } S\}.$$

The previous exercise (+ some general facts) imply that $F_{\Gamma(N)}$ is a sheaf[17] for $N \geq 3$.

Question 14.7. *Is $F_{\Gamma(N)}$ representable?*

14.1 $F_{\Gamma(3)}$ is representable

Start with E/S with a given $\Gamma(3)$-structure (P, Q).

Riemann-Roch says we can pick a function x on E w/ a pole of order 2 along the zero section, and no other poles. This will be unique up to $x \mapsto ax + b$. You can similarly find a y w/ a pole of order 3 unique up to $y \mapsto ay + bx + c$. These x, y satisfy an equation of the form

$$y^2 + a_1xy + a_3y = h(x) \tag{14.1}$$

where h is a cubic in x. The point P is 3-torsion, so $3[P] - 3[0]$ is a principle divisor. This means it's the divisor a function with a pole of order 3 at 0 and a triple zero at P, but $1, x, y$ span the space of functions with a pole of order ≤ 3 at 0 (and no other poles), so we may assume wlog that $3[P] - 3[0] = \mathrm{div}(y)$. We can replace $x \rightsquigarrow x - x(P)$ to assume $\mathrm{val}_P(x) \geq 1$. Since P is not 2-torsion, we can't have $\mathrm{val}_p(x) = 2$ (otherwise, $\mathrm{div}(x) = 2[P] - 2[0]$), so $\mathrm{val}_P(x) = 1$. Now, looking at equation (14.1), the LHS has valuation ≥ 3 at P while the RHS has valuation ≤ 3 at P. In order for these to match, the RHS must only have an x^3 term, so we have an equation of the form

$$y^2 + a_1xy + a_3y = x^3 \text{ with } P = (0, 0).$$

The only ambiguity left in the choice of x, y is the scaling.

Now, let's make use of Q. We can write $3[Q] - 3[0] = \mathrm{div}(y - Ax - B)$.

Claim 14.8. $A \in \mathscr{O}_S^\times$

Proof. Suffices to treat the case where S is a field, and then to show that A is nonzero. Suppose $A = 0$. Then, $y - B$ vanishes to order 3 at Q, so Q is the only 0 of $y - B$. This implies that $x^3 - (B^2 + a_1xB + a_3B)$ has only one root, so it must be

$$x^3 - (B^2 + a_1xB + a_3B) = (x - x(Q))^3.$$

Comparing x^2 coefficients then shows that $x(Q) = 0$. Plugging this in shows that $y(Q) = 0$ or $y(Q) = -a_3$ which says $Q = \pm P$, a contradiction. ■

This uses 3 being invertible

Since A is a unit, replace $y \rightsquigarrow y/A^3$ and $x \mapsto x/A^2$ in order to assume $A = 1$ (Now, there's no more ambiguity in choice of x, y).

[17] Sheaf on $\mathrm{Spec}\,\mathbb{Z}[1/N]_{\mathrm{Fppf}}$

Note that we now know

$$x^3 - \big((x+B)^2 + a_1x(x+B) + a_3(x+B)\big) = (x-C)^3 \text{ where } C = x(\mathbb{Q}).$$

Comparing coefficients gives

$$3C = a_1 + 1, \quad -3C^2 = 2B + a_1B + a_3, \text{ and } C^3 = B^2 + a_3B.$$

The first two of these let's us express a_1, a_3 in terms of B, C. The last equation then gives some relation between B, C; specifically, it says $B^3 = (B+C)^3$.

Proposition 14.9. *Given E/S with $\Gamma(3)$-structure (P,Q), we have shown there exists a unique pair of functions x, y on E s.t.*

(1) $\mathrm{val}_0(x) = 2$, $\mathrm{val}_0(y) = 3$, *and x, y are regular elsewhere. Furthermore, $y^2/x^3 = 1$ at 0.*

(2) $\mathrm{val}_P(y) = 3$ *and* $\mathrm{val}_P(x) = 1$

(3) $\mathrm{val}_Q(y - x - B) = 3$ *for some $B \in \Gamma(S, \mathscr{O}_S)$.*

Furthermore, if $C = x(Q)$, then $(B+C)^3 = B^3$ and E is given by the equation

$$y^2 + a_1xy + a_3y = x^3 \text{ where } a_1 = 3C - 1 \text{ and } a_3 = -3C^2 - B - 3BC.$$

Finally, $P = (0,0)$ and $Q = (C, B+C)$.

The above is a summary of what we have done. Now, we see that we can go backwards. Given B, C, can define $(E, (P,Q))$ using the above equation. If $\Delta \in \mathscr{O}_S^\times$, this will be an elliptic curve with $\Gamma(3)$-structure.

This shows that elliptic curves with $\Gamma(3)$-structure over S are the same thing as giving B, C on S satisfying one relation and having nonzero discriminant!

Theorem 14.10. *Let*

$$R := \mathbb{Z}\left[\frac{1}{3}, B, C\right]\left[\frac{1}{\Delta}\right] \Big/ \left(B^3 = (B+C)^3\right).$$

Then, $F_{\Gamma(3)}$ is represented by $\operatorname{Spec} R$.

We'd like a similar theorem for higher N, but this approach won't work out so nicely in general. However, there's a neat trick where you use the result for $N = 3$ to get it for higher N.

14.2 $F_{\Gamma(N)}$ is representable

Proposition 14.11. *Let E/S be an elliptic curve. We'll consider a moduli problem relative to this starting data. For an S-scheme S'/S, we set*

$$G(S') := \{\Gamma(N)\text{-structures on } E_{S'}\}.$$

Then, G is represented by a finite étale scheme T/S.

Proof. Start with $T_0 := E[N] \times_S E[N]$. This represents the functor picking out two points of order N. The Weil pairing gives a map $T_0 \to (\mu_N)_S$. Inside the target, one has the subscheme $(\mu_N^{prim})_S$ of primitive roots of unity. Just take $T := T_0 \times_{(\mu_N)_S} (\mu_N^{prim})_S$; this is the closed subscheme of T_0 consisting of pairs of points with Weil pairing a primitive root of unity. Since $T \subset T_0$ is closed and T_0/S is finite étale, we conclude that T/S is finite étale as well. ■

Theorem 14.12. *Suppose that $3 \nmid N$. Then, $F_{\Gamma(3N)}$ is representable by a smooth, affine scheme $Y(3N)$ over $\mathbb{Z}[1/(3N)]$.*

Proof. Start with $T \xrightarrow{\text{fin.ét}} Y(3)$, the space of $\Gamma(N)$-structure on the universal curve over $Y(3)$. A map $S \to T$ is equivalently a map $S \to Y(3)$ along with a lift $S \to T$ of it; from this, we see that

$$\mathrm{Hom}_{\mathbb{Z}[1/(3N)]}(S,T) \cong \left\{ \begin{array}{c} \text{isom classes of } E/S \text{ with} \\ \Gamma(3)\text{-structure} + \Gamma(N)\text{-structure} \end{array} \right\}.$$

By Chinese Remainder Theorem, this is the same thing as giving a $\Gamma(3N)$-structure. Thus, we win. ■

Remark 14.13. Here's one way to think about what just happened. The Proposition 14.11 is giving a 'relative representability' result; if you already have an elliptic curve, then specifying a $\Gamma(N)$-structure is a representable task. Theorem 14.12 is now saying something like if you have something representable and something relatively representable over it, then the thing upstairs is itself representable. ∘

If $\mathcal{X}$ is a stack, X is a scheme, and $\mathcal{X} \to X$ is a morphism representable by schemes, then $\mathcal{X}$ must be a scheme (since $\mathcal{X} \simeq \mathcal{X} \times_X X$)

This only takes care of level divisible (exactly once) by 3, so we'd like to get rid of that 3. Here's how things might work: on $Y(3N)$ there's an action of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ by moving around the level 3 structure, and the quotient should be $Y(N)$.

Warning 14.14. This strategy has to fail when $N = 1$, so there must be some subtlety. •

Proposition 14.15. *Say $N \geq 4$ is prime to 3. Then, $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \curvearrowright F_{\Gamma(3N)}$ freely, and*

$$F_{\Gamma(3N)}/\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \xrightarrow{\sim} F_{\Gamma(N)}$$

as sheaves.

Proof. There's an obvious map $F_{\Gamma(3N)}/\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to F_{\Gamma(N)}$, so just need to show the action is free and that this map is a bijection. Suppose that

$$\left(E, \underbrace{(P,Q)}_{\Gamma(3)}, \underbrace{(P',Q')}_{\Gamma(N)} \right) \in F_{\Gamma(3N)}$$

is fixed by $g \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. This means there's an automorphism $f : E \xrightarrow{\sim} E$ taking (P,Q) to $g(P,Q)$ and (P',Q') to (P',Q'). Since $N \geq 4$ (in particular, it's ≥ 3) and this fixes (P',Q'), we must have $f = \mathrm{id}_E$. This then forces $g = 1$ which proves freeness.

Let's show the map of sheaves is surjective. Say we have E/S with a $\Gamma(N)$-structure. We need to extend this to a $\Gamma(3N)$-structure, but we can do so after passing to a cover. By Proposition 14.11, there exists some finite étale $T \to S$ with a universal $\Gamma(3)$ structure for E. Now, E_T has a $\Gamma(3)$-structure and

a $\Gamma(N)$-structure, so gives an element of $F_{\Gamma(3N)}(T)$ (locally) lifting the element of $F_{\Gamma(3)}(S)$ we started with.

Injectivity is clear. Any two elements of $F_{\Gamma(3N)}$ getting identified in $F_{\Gamma(N)}$ must be off by an element of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. ■

Corollary 14.16. *Suppose $N \geq 4$ and prime to 3. Then, $F_{\Gamma(N)}$ is representable by a smooth affine scheme $/\mathbb{Z}[1/(3N)]$.*

Proof. $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ acts freely on $Y(3N)$, so we define $Y(N)$ to be the quotient. This will be a smooth, affine scheme representing $F_{\Gamma(3N)}/\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) = F_{\Gamma(N)}$. ■

Warning 14.17. The argument above only works with 3 inverted since we started with $F_{\Gamma(3N)}$ even though $3 \nmid N$. We'd prefer to get $Y(N)/\mathbb{Z}[1/N]$. •

The main result is the following

Theorem 14.18. *For any $N \geq 3$, $F_{\Gamma(N)}$ is represented by a smooth affine scheme over $\mathbb{Z}[1/N]$.*

Proof Sketch. First do a base in level 2 explicitly. You can't do $\Gamma(2)$ since $Y(2)$ is genuinely not a scheme (it's not a sheaf), but you could do some modification of it or even do $\Gamma(4)$ if you wanted.[18]

Then use the same sort of tricks to get hat if $N \geq 3$ and prime to 2, then $F_{\Gamma(N)}$ is representable as a smooth affine scheme over $\mathbb{Z}[1/(2N)]$. Now, if N is prime to 6, you can glue to get the thing you want over $\mathbb{Z}[1/N]$.

You then need some more work to remove the "N prime to 6" hypothesis. ■

There are other, more abstract ways to prove this theorem that don't rely on the tricks we've been using.

14.3 Stacks

The kind of stuff we've seen works well when there are no automorphisms in the moduli problem. When there are automorphisms, the right thing to do is to use stacks. We won't say too much about these, but will say a little.

The problem with $F_{\Gamma(1)}$ is that if we have $E/k^s \in F_{\Gamma(1)}(k^s)^{\Gamma_k}$ (i.e. it's isomorphism class is Galois-invariant), then for any $\sigma \in \mathrm{Gal}(k^s/k)$, there exists an iso $\sigma^*(E) \xrightarrow{\sim} E$. The issue is that there's no required compatibility between these isomorphisms for different σ, so you can't get descent data and can't necessarily go down to the base field. When there are no automorphisms, the cocycle condition is automatic.

In general, one passes from the set of isomorphism classes to the entire category (groupoid) of objects and isomorphisms. This is the idea behind stacks.

Definition 14.19. A **stack** (on a topological space or on a site) is a rule $\mathscr{F}$ that assigns to every open U a groupoid $\mathscr{F}(U)$ and every inclusion $U' \hookrightarrow U$ s restriction function $\mathscr{F}(U) \to \mathscr{F}(U')$. We require that

[18] See here for one place with this done in detail

for $U'' \subset U' \subset U$, there's a 2-commutative diagram (so α a natural transformation of functors)

$$\begin{array}{ccc} \mathscr{F}(U) & \longrightarrow & \mathscr{F}(U') \\ & \searrow \quad \swarrow_{\alpha} & \\ & \mathscr{F}(U'') & \end{array}$$

Finally, it should satisfy some analogue of the sheaf conditions, e.g. gives a cover $U = \bigcup_{i \in I} U_i$ and objects $X_i \in \mathscr{F}(U_i)$ with isomorphisms $\varphi_{ij} : X_i|_{U_{ij}} \xrightarrow{\sim} X_j|_{U_{ij}}$ satisfying the cocycle condition $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ (over U_{ijk}), then these glue to some $X \in \mathscr{F}(U)$. $\diamond$

(Compare the above definition with the definition of a sheaf)

Example. Say G is a finite group acting on a variety X. We can try to form the quotient X/G, but this isn't always the nicest thing if G has fixed points. For example, the fibers of $X \to X/G$ don't always have cardinality $\#G$. However, there's always a nice quotient stack $[X/G]$. The stabilizers of points of X will be the automorphism groups of the corresponding point of $[X/G]$. To actually define $[X/G]$ as a stack, we'd need to specify, for each scheme Y, the groupoid of maps $Y \to [X/G]$. If one does this correctly, then they'll see (essentially by definition) that if $Y \to [X/G]$ is a map, then the fiber product $Y \times_{[X/G]} X$ is actually a scheme and is moreover a G-torsor over Y.

In fact, the groupoid of maps $Y \to [X/G]$ is, by definition, the groupoid of triples (T, f, g) where T is a scheme with G-action, $f : T \to Y$ makes T a G-torsor over Y, and $g : T \to X$ is a G-equivariant map, i.e. the groupoid of pictures

$$\begin{array}{ccc} T & \xrightarrow{g} & X \\ {\scriptstyle f}\downarrow & & \downarrow \\ Y & \longrightarrow & [X/G]. \end{array}$$

$\triangle$

Not all stacks are nice, geometric objects (compare: not all sheaves are schemes).

Definition 14.20. A **Deligne-Mumford stack** if a stack X for which there exists a scheme $\widetilde{X}$ and a map $\widetilde{X} \to X$ so that, for any map $Y \to X$ from a scheme, the fiber product

$$\begin{array}{ccc} \widetilde{X} \times_X Y & \longrightarrow & \widetilde{X} \\ \downarrow & & \downarrow \\ Y & \longrightarrow & X \end{array}$$

exists as a scheme, and the natural map $\widetilde{X} \times_X Y \to Y$ is both étale and surjective. One says that $\widetilde{X} \to X$ is an étale cover of X. $\diamond$

I'm not 100% sure this is the correct definition. I feel like usually one lets this fiber product be an algebraic space in general

We not let $\mathscr{F}_{\Gamma(1)}(S)$ be the groupoid of elliptic curves over S. Then,

$$Y(N) \to \mathscr{F}_{\Gamma(1)}$$

is an étale cover over $\mathbb{Z}[1/N]$. The point is that, given $S \to \mathscr{F}_{\Gamma(1)}$ (i.e. given an E/S), the fiber product

$$\begin{array}{ccc} T & \longrightarrow & Y(N) \\ \downarrow & \ulcorner & \downarrow \\ S & \longrightarrow & \mathscr{F}_{\Gamma(1)} \end{array}$$

is the space of $\Gamma(N)$-structures on E/S, i.e. it is the (finite, étale) scheme T from Proposition 14.11! Hence, $Y(1) := \mathscr{F}_{\Gamma(1)}$ is a DM stack.

[A mistake from two lectures ago] Recall $Y(N) = \{(E, (P, Q))\}$. Note that there is a map

$$Y(N) \twoheadrightarrow \mu_N^{prim} \text{ which sends } (E, (P, Q)) \mapsto e_N(P, Q)$$

($e_N(-,-)$ the Weil pairing). Hence, $Y(N)$ is not connected; it has one connected component for each primitive root of unity.

Two lectures ago we said $Y(N) = \mathfrak{H}/\Gamma(N)$ (over $\mathbb{C}$), but this can't be the case since the RHS is connected. What is true is that $Y(N)_\zeta = \mathfrak{H}/\Gamma(N)$ after fixing some $\zeta \in \mu_N^{prim}$.

Definition 14.21. A $\Gamma_1(N)$**-structure** on E/S is some $P \in E[N](S)$ of order N. ◇

One can define the stack $\mathscr{F}_{\Gamma_1(N)}$ of elliptic curves with $\Gamma_1(N)$ structures and similarly prove.

Proposition 14.22. *$Y_1(N) := \mathscr{F}_{\Gamma_1(N)}$ is always a smooth DM stack over $\mathbb{Z}[1/N]$. If $N \geq 4$, it's in fact a smooth, affine scheme.*

Definition 14.23. A $\Gamma_0(N)$**-structure** on E/S is a finite étale subgroup $G \subset E$ which is cyclic of order N on each fiber. ◇

Theorem 14.24. *$Y_0(N) := \mathscr{F}_{\Gamma_0(N)}$ is always a smooth DM stack over $\mathbb{Z}[1/N]$.*

These are never schemes since multiplication by -1 always gives an automorphism.

15 Lecture 15: Modular curves over $\mathbb{Z}$

Last time we discussed modular curves as schemes and then as stacks. The stack we called $Y_0(N)$ last time, we'll instead call $\mathcal{M}_0(N)$ this time.

Recall 15.1. $\mathcal{M}_0(N)$ is the stack over $\mathbb{Z}[1/N]$ which assigns to a $\mathbb{Z}[1/N]$-scheme S, the groupoid of pairs (E, G) with E/S an elliptic curve and $G \subset E$ a closed subgroup which is finite, étale over S and which is cyclic of order N in each fiber. This is the stack parameterizing elliptic curves with $\Gamma_0(N)$-structure. ⊙

$\mathcal{M}_0(N)$ is a smooth DM stack, i.e. it has an étale cover by a scheme. Explicitly, for $p \nmid N$, we define a moduli functor

$$Y(S) := \left\{ \text{isom classes of tuples } (\underbrace{E}_{\text{elliptic curve}}, \underbrace{G}_{\Gamma_0(N)\text{-structure}}, \underbrace{(P,Q)}_{\Gamma(p)\text{-structure}}) \right\}.$$

If $p > 2$, then $\Gamma(p)$-structures are rigid, so this Y will be a scheme (think, analogue of Proposition 14.11). The étale cover is then the natural map

$$Y \to \mathcal{M}_0(N)$$

forgetting the $\Gamma(p)$-structure. In fact, $\mathcal{M}_0(N) \simeq [Y/\operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})]$ (as stacks over $\mathbb{Z}[1/(pN)]$) is a quotient stack.

One can also consider the scheme quotient $Y/\operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})$ instead of the stack quotient. One can show that (over $\mathbb{Z}[1/(pN)]$) this represents the (sheafification) of the functor

$$S \longmapsto |\mathcal{M}_0(N)(S)|$$

sending S to the set of isomorphism classes of the groupoid of maps $S \to \mathcal{M}_0(N)$. Using different p's, one gets that the sheafification of $S \mapsto |\mathcal{M}_0(N)(S)|$ is represented by a scheme $M_0(N) = Y_0(N)$ over $\mathbb{Z}[1/N]$. We call $Y_0(N)$ the **coarse space**[19] of $\mathcal{M}_0(N)$.

Remark 15.2. This $Y_0(N)$ is smooth and affine ∘

The coarse space has the advantage that it's a scheme, not a stack, but it has the disadvantage that it doesn't support a universal family.

Example. When $N = 1$, the coarse space is the j-line $M_0(1) = M(1) = Y(1) = \mathbb{A}^1$. △

(Andrew mentioned that the fundamental group of $\mathcal{M}(1)$ is like the profinite completion of $\operatorname{SL}_2(\mathbb{Z})$)

15.1 Compactifying modular curves (over $\mathbb{Z}[1/N]$)

(Reference: Deligne-Rapoport article in 'Modular Functions of One Variable II')

15.1.1 Level 1

First consider the level 1 case.

Recall 15.3 (over $\mathbb{C}$)**.** Over $\mathbb{C}$, we had $Y(1) = \mathcal{H}/\Gamma(1)$ which is missing a point. To through this in, we formed $X(1) = \mathcal{H}^*/\Gamma(1)$ where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Since $\Gamma(1) \curvearrowright \mathbb{P}^1(\mathbb{Q})$ transitively, forming $X(1)$ only adds one more point to $Y(1)$. ⊙

Recall 15.4 (Valuative criterion for properness)**.** Say $X/\mathbb{C}$ is a scheme of finite presentation. Then, X is proper iff for all dvrs $A/\mathbb{C}$ with fraction field $K = \operatorname{Frac}(A)$, every K-point of X extends uniquely to an A-point. ⊙

This suggests that compactifying modular curves is related to extending elliptic curves / dvrs. This is something we know a bit about.

Recall 15.5 (Semi-stable Reduction Theorem 8.8)**.** Let A be a dvr and let $K = \operatorname{Frac}(A)$. Let E/K be an elliptic curve. Then, there exists an extension K'/K s.t. $E_{K'}$ extends over A' to an elliptic curve with semi-stable reduction (i.e. good or multiplicative reduction). ⊙

[19] Assuming I'm not mistaken, the 'coarse space' of a stack $\mathcal{X}$, if it exists, is an algebraic space X with a map $\mathcal{X} \to X$ so that $X(\overline{k}) = \left|\mathcal{X}(\overline{k})\right|$ for k any field, and $\mathcal{X} \to X$ is initial among maps from $\mathcal{X}$ to algebraic spaces. These often exist by the Keel-Mori theorem (e.g. always exist for separated DM stacks)

Question: Does the coarse space of a stack $\mathcal{X}$ always represent the sheafification of the functor $S \mapsto |\mathcal{X}(S)|$?

Answer: No, see e.g. here and/or here

Question: Is it clear that this is affine?

Answer: The map $Y \to Y(p)$ is certainly quasi-finite. I suspect it's not too hard to check that it's proper using the valuative criterion. Assuming this, Y is finite over $Y(p)$ and so affine

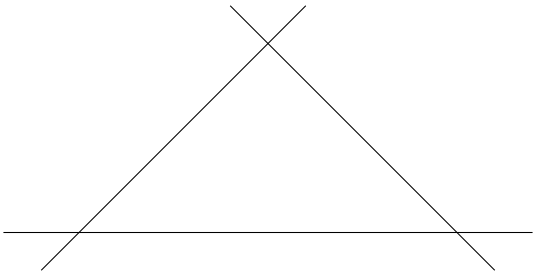


Figure 2: A picture of the standard 3-gon

So if we have an elliptic curve over with good reduction, we're happy (it extends an elliptic curve over A, an A-point of the moduli space), but if it has multiplicative reduction, then it doesn't extend to an A-point since we don't have nodal cubics in our moduli space. This suggests that the missing point should precisely be the nodal cubic.

Definition 15.6. Fix an integer $n \geq 1$. The **standard n-gon** C_n is the quotient of $\mathbb{P}^1 \times \mathbb{Z}/n\mathbb{Z}$ where $(\infty, i) = (0, i+1)$ for all $i \in \mathbb{Z}/n\mathbb{Z}$, see Figure 2. ◇

Remark 15.7. The standard n-gon only has nodal singularities. In particular, the standard 1-gon is a nodal cubic ($\mathbb{P}^1$ with $0, \infty$ identified). ○

Remark 15.8. $C_n^{sm} = \mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$ is a group, obtained by removing the nodes. Furthermore, the action of C_n^{sm} on itself extends to action on all of C_n.[20] Furtherfurthermore, $C_n^{sm}[n]$ has order n^2 and fits into a short exact sequence

$$0 \longrightarrow \mu_n \longrightarrow C_n^{sm}[n] \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

with μ_n in the identity component of C_n^{sm}. ○

Definition 15.9. A **generalized elliptic curve** over S is a tuple $(E, +, 0)$ where E/S is proper + flat (of finite presentation?), $0 \in E(S)$ (landing in the smooth locus?) and $+ : E^{sm} \times E \to E$ s.t.

(1) $+$ gives E^{sm} the structure of a group (with identity 0?) and defines an action of E^{sm} on E

(2) The geometric fibers are all either elliptic curves or n-gons. ◇

We use this to define a new moduli stack. We let $\overline{\mathcal{M}}(1)$ be the stack attaching to a scheme S, the groupoid of generalized elliptic curves $/S$ whose geometric fibers are either elliptic curves or 1-gons.

Theorem 15.10. *$\overline{\mathcal{M}}(1)$ is a proper, smooth DM stack over $\mathbb{Z}$.*

Remark 15.11. The valuative criterion for properness for DM stacks allows for finite extensions of DVRs before filling in a point. Hence, this properness statement really is Theorem 8.8. ○

Question 15.12 (Audience)**.** *What does smoothness mean for a DM stack?*

Answer. It means you have an étale cover by a smooth scheme. Alternatively, there's also a characterization in terms of an infinitesimal lifting criterion; for curves, there's no H^2 and so deformation theory tells you there's no obstruction to lifting, so you can also prove smoothness that way. ⋆

[20] The $\mathbb{G}_m$ parts fixes the singular points while the $\mathbb{Z}/n\mathbb{Z}$ parts cyclically permutes them

15.1.2 Higher Level

Definition 15.13. A $\Gamma_0(N)$**-structure for a generalized elliptic curve** E/S is a finite, flat (over S) subgroup $G \subset E^{sm}$ which is cyclic of order N. ◇

The definition of $\overline{\mathcal{M}}_0(N)$ should be related to $\Gamma_0(N)$-structures on generalized elliptic curves, but there's some subtlety...

Remark 15.14 (Cusps of $X_0(N)$). Say N is prime. The cusps of $X_0(N) = \mathfrak{H}^*/\Gamma_0(N)$ are $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$. One can show that $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{F}_N)/G$ where $G \leq \mathrm{GL}_2(\mathbb{F}_N)$ is the Borel $G = \left\{ \begin{pmatrix} * & * \\ & * \end{pmatrix} \right\}$. This acts by linear maps ($x \mapsto ax + b$), so there are 2 cusps (∞ and 0) on $X_0(N)$ (when N prime, maybe also $N > 2$). ○

Warning 15.15. The standard 1-gon has only one $\Gamma_0(N)$-structure: $\mu_N \subset C_1$. We need to add two $\mathbb{C}$-points to get the right compactification, so it won't be enough to just consider 1-gons anymore. •

We go up to N-gons: C_N has two $\Gamma_0(N)$-structures, up to isomorphism. It has $\mu_N \subset C_N^0$ and $\mathbb{Z}/N\mathbb{Z} \subset C_N$. This looks good. However, for technical reasons, you want your level structure to hit every irreducible component. Hence, the cusps should really be

$$\underbrace{\mu_N \subset C_1}_{0} \text{ and } \underbrace{\mathbb{Z}/N\mathbb{Z} \subset C_N}_{\infty}.$$

The convention below is the one Mazur uses in his paper. It sounds (see video for Lecture 18) like this convention is backwards from the standard one, so we'll later use the opposite convention for naming the cusps

We define $\overline{\mathcal{M}}_0(N)$ (for any N, prime or not) to be the stack s.t. for any scheme S, $\overline{\mathcal{M}}_0(N)(S)$ is the groupoid of (E, G) with E/S a generalized elliptic curve, and G is a $\Gamma_0(N)$-structure meeting each irreducible component in every geometric fiber.

Fact. This funny condition on G is equivalent to saying that the divisor defined by G is ample.

Theorem 15.16. *$\overline{\mathcal{M}}_0(N)$ is a proper, smooth DM stack over $\mathbb{Z}[1/N]$.*

Let's talk about maps. Suppose $N' \mid N$. Then, $\Gamma_0(N) \subset \Gamma_0(N')$ so you get a map

$$X_0(N) = \mathfrak{H}^*/\Gamma_0(N) \longrightarrow \mathfrak{H}^*/\Gamma_0(N') = X_0(N').$$

How to see this as a map $\overline{\mathcal{M}}_0(N) \to \overline{\mathcal{M}}_0(N')$?

Remark 15.17. This is easy before compactifying. If $(E, G) \in \mathcal{M}_0(N)$, there $\exists! H \subset G$ of order N', so map $(E, G) \mapsto (E, H)$. ○

Say $(E, G) \in \overline{\mathcal{M}}_0(N)$. We again have a unique $H \subset G$ of order N'. We can't make $(E, G) \mapsto (E, H)$ since we need our subgroup to meet every component of each fiber. Hence, we just contract the fibers not meeting H, i.e. we let $\overline{E}$ be E with components not meeting H contracted, and then we map $(E, G) \mapsto (\overline{E}, \text{img of } H)$.

Remark 15.18 (Algebraic construction of $\overline{E}$). Say $f : E \to S$ is the structure map. Note that, since G is ample,

$$E \simeq \mathbf{Proj}_S \left(\bigoplus_{n \geq 0} f_* \left(\mathscr{O}_E(nG) \right) \right).$$

To form the contraction, we instead take[21]

$$\overline{E} := \mathbf{Proj}_S \left(\bigoplus_{n \geq 0} f_* \mathscr{O}_E(nH) \right). \qquad \circ$$

Question: Why does this correspond to contracting the components not meeting H?

15.2 Working over $\mathbb{Z}$

We've been assuming that N is invertible so the N-torsion is étale. Now we work over $\mathbb{Z}$ (not $\mathbb{Z}[1/N]$), and so N-torsion will no longer always be étale.

Warning 15.19. Elliptic curves over $\mathbb{F}_p$ can have too little p-torsion, e.g. if $E/\mathbb{F}_p$ is supersingular, then $E(\overline{\mathbb{F}}_p)[n] = 0$. What is a $\Gamma(p)$-structure on E? $\bullet$

Answer: See e.g. Theorem 6.7/1 of 'Néron Models' by Bosch, Lutkebohmert, Raynaud. The vague

There's a solution to this problem that Drinfeld came up with, called 'Drinfeld level structures.' We won't actually talk about this; for our purposes, we only need $X_0(N)$ to be defined over $\mathbb{Z}$, so we'll do something that works in this particular case.

Assumption. Assume N is squarefree.

Definition 15.20. Let E/S be a generalized elliptic curve. A $\Gamma_0(N)$**-structure** on E is a closed subgroup $G \subset E$ which is finite, flat over S of order N. We define $\overline{\mathcal{M}}_0(N)$ where $\overline{\mathcal{M}}_0(N)(S)$ is the groupoid of (E, G) w/ G meeting each irreducible component in every fiber. $\diamond$

Theorem 15.21. *$\overline{\mathcal{M}}_0(N)$ is a proper, flat DM stack over $\mathbb{Z}$.*

Question: Is flatness easy to show?

When N is inverted, this reverts to the previous thing we were talking about. Note that it is smooth over $\mathbb{Z}[1/N]$, but not over all of $\mathbb{Z}$.

Remark 15.22. Can do this for any N, but

(1) Need to define what it means for a group scheme to be "cyclic" (e.g. should you allow $\alpha_p \times \alpha_p$, α_{p^2}, etc.?)

(2) If $p^2 \mid N$, there exists a generalized elliptic curve w/ $\Gamma_0(N)$-structure s.t. $\mu_p \subset$ Aut group. Points on DM stacks have étale automorphism groups, so $\mathcal{M}_0(N)$ won't be DM (but it will be an Artin stack) $\circ$

$\mathscr{O}_E(nH)$ is the trivial bundle when restricted to any component not meeting H, and so sends those components to $\mathbf{Proj}(\bigoplus_{n\geq 0} \mathscr{O}$ $\mathbf{Proj}\,\mathrm{Sym}^* \mathscr{O}$ = $\mathbf{Spec}\,\mathscr{O}$

Remark 15.23. Katz-Mazur worked out the theory of these Drinfeld level structures in a lot of detail in their book, but didn't really give a moduli theoretic interpretation of the compactifications. They were just working with things like $Y_0(N)$, but over all of $\mathbb{Z}$. Deligne-Rapoport did the compactified theory, but were working over $\mathbb{Z}[1/N]$. The compactified theory over $\mathbb{Z}$ was worked out by Brian Conrad. $\circ$

Remark 15.24 (properness). Say $K = \operatorname{Frac} A$ and we have E/K w/ G a $\Gamma_0(N)$-structure. May assume E has semi-stable reduction and that the points of G are defined over K. Let $\overline{E}$ be the minimal regular model, and let $\overline{G}$ be the closure of G in $\overline{E}$ (this lands in $\overline{E}^{sm}$ since $\overline{E}^{sm}$ is the Néron model and all K points extend to the Néron model). Since it's semi-stable, the special fiber of the minimal regular model will be one of these N-gons. This $\overline{G}$ may not meet all irreducible components, so contract the ones it doesn't meet. This gives the desired extension. $\circ$

[21] This footnote is an extension of the marginal comments here. I think (!) you can think of this as looking at the image of the map to projective space induced by $\mathscr{O}_E(nH)$ (for some $n \gg 0$). Hence, it will be an embedding on components meeting H (where it restricts to a very ample bundle) and constant (i.e. a contraction) on components not meeting H (where $\mathscr{O}_E(nH)$ restricts to the trivial bundle)

Question 15.25. *What's this $\overline{\mathcal{M}}_0(N)$ look like in bad characteristic?*

Suppose $p \mid N$ (N squarefree) and let $N' := N/p$ (so $p \nmid N'$). We want to look at $\overline{\mathcal{M}}_0(N)_{\mathbb{F}_p}$.

Remark 15.26. Let E/k be an elliptic curve with $k = \overline{k}$ and $\operatorname{char} k = p$.

- If E is supersingular, then $E[p]$ is an extension of α_p by α_p.[22] It only has 1 subgroup of order p, which is α_p ($= \ker(F)$, the kernel of Frobenius).
- If E is ordinary, then[23] $E[p] = \mathbb{Z}/p\mathbb{Z} \times \mu_p$ and so has exactly two subgroups of order p: $\mathbb{Z}/p\mathbb{Z}$ and μ_p ($= \ker(F)$).

In particular, there's always a canonical $\Gamma_0(p)$ structure you can put on it, given by the kernel of Frobenius. ∘

The kernel of Frobenius is always picking out the non-étale $\Gamma_0(p)$-structure, even for standard n-gons (it gives the μ_p), see I think Proposition 6.6

This suggests that there should be a map $\overline{\mathcal{M}}_0(N')_{\mathbb{F}_p} \to \overline{\mathcal{M}}_0(N)_{\mathbb{F}_p}$ (where you add the kernel of Frobenius). In fact, there are two such maps. Define

$$f, g : \overline{\mathcal{M}}_0(N')_{\mathbb{F}_p} \rightrightarrows \overline{\mathcal{M}}_0(N)_{\mathbb{F}_p}$$

as follows.

Recall 15.27. For E/S, we have the Frobenius $F : E \to E^{(p)}$ whose dual isogeny is the Verschiebung $V : E^{(p)} \to E$. ⊙

Say we have $(E, G) \in \overline{\mathcal{M}}_0(N')_{\mathbb{F}_p}$. Then we set

$$f(E, G) := (E, G, \ker(F)) \text{ and } g(E, G) := \left(E^{(p)}, V^{-1}(G)\right).$$

Let's now define

$$f', g' : \overline{\mathcal{M}}_0(N)_{\mathbb{F}_p} \rightrightarrows \overline{\mathcal{M}}_0(N')_{\mathbb{F}_p}$$

in the opposite direction. These will be

$$f(E, G, H) = (E, G) \text{ and } g(E, G, H) = (E/H, \text{image of } G \text{ in } E/H),$$

where E a generalized EC, G a $\Gamma_0(N')$-structure, and H a $\Gamma_0(p)$-structure.

One has

$$f'f = \mathrm{id} = g'g \text{ and } f'g = \mathrm{Frob} \text{ on } \overline{\mathcal{M}}_0(N')_{\overline{\mathbb{F}}_p} = g'f.$$

Remark 15.28. The picture to have in mind is that $\overline{\mathcal{M}}_0(N)_{\mathbb{F}_p}$ is two copies of $\overline{\mathcal{M}}_0(N')_{\mathbb{F}_p}$ glued along their supersingular loci (via the Frobenius map). ∘

Example. Say $N' = 1$, so $\overline{M}_0(N')_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p}$. Then, the above says $\overline{M}_0(p)_{\mathbb{F}_p}$ is just two copies of $\mathbb{P}^1$ glued along a finite set of pts (the finitely many supersingular j-invariants).

[22] "It's not α_{p^2}, not $\alpha_p \times \alpha_p$, and not the kernel of Frobenius on the second Witt scheme; it's the other extension of α_p by α_p"

[23] Get $\mathbb{Z}/p\mathbb{Z} \hookrightarrow E[p]$ since $k = \overline{k}$, and so get exact sequence $0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$ since $E[p]$ is Cartier self-dual. This sequence must split since there's also the connected-étale sequence $0 \to \mu_p \to E[p] \to \mathbb{Z}/p\mathbb{Z} \to 0$

This has the following fun consequence. $\overline{M}_0(p)_{\mathbb{F}_p}$ is a nodal curve (compare Proposition 19.7) with nodes in bijection with supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (recall a supersingular $E/\overline{\mathbb{F}}_p$ has exactly one $\Gamma_0(p)$-structure, given by $\alpha_p \hookrightarrow E[p]$). In general, given a nodal curve C, its arithmetic genus is given by the **genus formula for nodal curves**

$$p_a(C) = \sum_i g_i + \delta - \nu + 1$$

(where g_i ranges over the geometric genera of C's irreducible components, δ is the number of nodes, and ν is the number of irreducible components). In the present case, this says that

$$p_a(\overline{M}_0(p)_{\mathbb{F}_p}) = (0+0) + \delta - 2 + 1 = \delta - 1 \implies \#\text{supersingular } j\text{-invariants} = \delta = p_a(\overline{M}_0(p)_{\mathbb{F}_p}) + 1.$$

Furthermore, since $\overline{M}_0(p)$ is flat over $\mathbb{Z}$, all its fibers have the same (arithmetic) genus. Thus, the number of supersingular j-invariants over $\overline{\mathbb{F}}_p$ is one more than the genius of the classic modular curve/Riemann surface $X_0(p)$, i.e.

$$\#\text{supersingular } j\text{-invariants}/\overline{\mathbb{F}}_p = g(X_0(p)) + 1 = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 2 & \text{if } p \equiv 11 \pmod{12} \\ 1 & \text{otherwise.} \end{cases} \tag{15.1}$$

△

16 Lecture 16: Structure of the Hecke algebra

Everything today is over $\mathbb{C}$.

Recall 16.1. Say f is a modular form for $\Gamma(1)$ of weight k. We defined the Hecke operator T_n via

$$(T_n f)(\Lambda) := n^{k-1} \sum_{[\Lambda:\Lambda']=n} f(\Lambda').$$

The same formula defines $T_n f$ if f is modular for $\Gamma_0(N)$ and $(n, N) = 1$. These satisfy

- These T_n commute with each other
- If $(n, m) = 1$, then $T_{nm} = T_n T_m$
- $T_{p^{n+1}} = T_p T_{p^n} - p T_{p^{n-1}}$
- If $f = \sum_{n=1}^{\infty} a_n q^n$ and p is prime, then

$$T_p f = \sum_{n \geq 1} \left(a_{np} + p^{k-1} a_{n/p} \right) q^n.$$

In particular, $a_1(T_p f) = a_p(f)$. In general, $a_1(T_n f) = a_n(f)$ if $(n, N) = 1$. ⊙

Notation 16.2. Let $\widetilde{\mathbb{T}} := \mathbb{Z}[T_p]$ be the (formal) polynomial ring in the T_p's. Let $\mathbb{T}$ be the image of $\widetilde{\mathbb{T}}$ in $\mathrm{End}(S_2(N))$, where $S_2(N)$ is the space of weight 2 cusp forms for $\Gamma_0(N)$. We let $\mathbb{T}_{\mathbb{Q}}$ be the $\mathbb{Q}$-span of $\mathbb{T}$, and we let $\mathbb{T}_{\mathbb{C}}$ be the $\mathbb{C}$-span of $\mathbb{T}$.

(in this class, we'll mainly be interested in weight two forms)

Goal. Understand $\mathbb{T}$

16.1 Petersson inner product

Let $f, g \in S_2(N)$ be weight two cusp forms.

Recall 16.3. $f(z)\mathrm{d}z$ is invariant under $\Gamma_0(N)$. The same is true for $\overline{g(z)\mathrm{d}z}$, and so

$$f(z)\mathrm{d}z \wedge \overline{g(z)\mathrm{d}z} = 2if(z)\overline{g(z)}\mathrm{d}x\mathrm{d}y$$

is a $\Gamma_0(N)$-invariant 2-form (note $\mathrm{d}z\mathrm{d}\overline{z} = 2i\mathrm{d}x\mathrm{d}y$) ⊙

Definition 16.4. The **Petersson inner product** is

$$\langle f, g\rangle := \int_{\mathfrak{H}/\Gamma_0(N)} f(z)\overline{g(z)}\mathrm{d}x\mathrm{d}y. \qquad \diamond$$

This integral converges since f, g are cusp forms and so $\to 0$ quickly at cusps. Furthermore, $\langle -, -\rangle$ is a positive, definite Hermitian inner product on $S_2(N)$.

I think it may be enough for only one of f, g to be a cusp form

Proposition 16.5. *T_p is self-adjoint, i.e. for $f, g \in S_2(N)$*

$$\langle T_p f, g\rangle = \langle f, T_p g\rangle .$$

(One can compute this directly)

Thus, these T_p form a family of commuting, self-adjoint operators on this f.dim space, and so can be simultaneously diagonalized.

Corollary 16.6. *There exists a basis of $S_2(N)$ consisting of simultaneous eigenvectors.*

Corollary 16.7. *$\mathbb{T}_{\mathbb{C}}$ is a semi-simple $\mathbb{C}$-algebra (a product of copies of $\mathbb{C}$)*

Definition 16.8. A **Hecke eigenform** is an $f \in S_2(N)$ which is an eigenvector for all T_p's ($p \nmid N$). We say f is **normalized** if $a_1(f) = 1$. $\diamond$

Remark 16.9. If f is an eigenform, you get a homomorphism $\alpha_f : \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$ sending T_p to its eigenvalue on f, i.e. α_f determined by $T_p f = \alpha_f(T_p)f$. Such an α_f is called a **system of eigenvalues**. These give a decomposition

$$S_2(N) = \bigoplus_{\alpha} S_2(N)_\alpha \text{ where } S_2(N)_\alpha := \{f : Tf = \alpha(T)f \text{ for all } T \in \mathbb{T}\}.$$

Furthermore, $T_{\mathbb{C}} = \prod_\alpha \mathbb{C}$. ∘

Theorem 16.10 (**Multiplicity One Theorem**). *Suppose that N is prime. Let f, g be two normalized eigenforms with the same system of eigenvalues. Then, $f = g$.*

Notation 16.11. For a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ and $f : \mathfrak{H} \to \mathbb{C}$, we define

$$(f|[\gamma])(z) := (cz + d)^{-1} f(\gamma z).$$

This defines a group action (the 'slash action') of $\mathrm{SL}_2(\mathbb{R})$ on the same of functions on $\mathfrak{H}$. Furthermore, $f \in S_2(N) \iff f|[\gamma] = f$ for all $\gamma \in \Gamma_0(N)$ + the holomorphicity and vanishing conditions.

Proof. Recall $a_1(T_p f) = a_p(f)$. Hence, since f is a normalized eigenform, we see that $a_p(f)$ is the eigenvalue of T_p on f. The same is true for g, so $a_p(f) = a_p(g)$ for all $p \nmid N$. By the multiplicativity and recurrence properties of Hecke operators, this implies that $a_n(f) = a_n(g)$ for all $(n, N) = 1$. Let $h = f - g$, so $a_n(h) = 0$ unless $N \nmid n$ (recall N prime), i.e.

$$h = \sum_{n \geq 1} a_{nN}(h) q^{nN}.$$

Thus, $h(z + \frac{1}{N}) = h(z)$, so $h|[\gamma] = h$ if $\gamma \in \Gamma_0(N)$ or $\gamma = \begin{pmatrix} 1 & 1/N \\ & 1 \end{pmatrix}$. Let $\sigma := \begin{pmatrix} N & \\ & 1 \end{pmatrix}$ and set $h' := h|[\sigma^{-1}]$. Then,

$$h'|[\gamma] = h' \text{ if } \gamma \in \sigma\Gamma_0(N)\sigma^{-1} \text{ or } \gamma = \sigma \begin{pmatrix} 1 & 1/N \\ & 1 \end{pmatrix} \sigma^{-1} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}.$$

Now note that

$$\sigma\Gamma_0(N)\sigma^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv 0 \pmod{n} \right\}.$$

These together with $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ general the full $\Gamma(1)$, so $h' \in S_2(1) = 0$ which means that $h = 0$ which means that $f = g$. ∎

Remark 16.12. A stronger version of the above theorem holds. If the T_p eigenvalues of f, g agree for all but finitely many p (or even just for p in a density 1 set), then $f = g$. This is called *Strong Multiplicity One*. ∘

Warning 16.13. This theorem is false (for a silly reason) if N is not prime. Suppose $p \mid N$ and choose $f \in S_2(N/p)$. Then, both $f(z)$ and $f(pz)$ are in $S_2(N)$, and they have the same T_ℓ-eigenvalues for all $\ell \nmid N$. •

Remark 16.14. The above is the only thing that goes wrong. One can define the *old subspace*

$$S_2(N)^{old} = \mathrm{span}\left\{ f(z), f(pz) : f \in S_2(N/p), p \mid N \right\},$$

and the *new subspace* $S_2(N)^{new}$, the orthogonal complement of the old subspace. Then, multiplicity one holds on the new space. ∘

Corollary 16.15 (of Multiplicity One)**.** *For all systems α of eigenvalues,* $\dim S_2(N)_\alpha = 1$.

Corollary 16.16. *There's a bijection between homomorphisms $\mathbb{T} \to \mathbb{C}$ and normalized eigenforms.*

Corollary 16.17. *$S_2(N)$ is free of rank 1 as a $\mathbb{T}_{\mathbb{C}}$-module*

Question: How do we know every homomorphism $\mathbb{T} \to \mathbb{C}$ is realized as the eigenvalues of some eigenform?

Answer: See aside

Lemma 16.18. *Let $\chi : \mathbb{T} \to \mathbb{C}$ be a character. Then,*

$$f_\chi = \sum_{n \geq 1} \chi(T_n) q^n$$

is a weight 2 cusp form.

Proof. There is a natural pairing

$$\begin{array}{rccc} \langle -, - \rangle : & \mathbb{T} \times S_2(N) & \longrightarrow & \mathbb{C} \\ & (T, f) & \longmapsto & a_1(Tf) \end{array}$$

which we claim is perfect. Indeed, for fixed $T \in \mathbb{T}$, assume $\langle T, f \rangle = a_1(Tf) = 0$ for all $f \in S_2(N)$. Then, for any $f \in S_2(N)$ and any $m \in \mathbb{N}$, we have

$$a_m(Tf) = a_1(T_m T f) = a_1(T T_m f) = \langle T, T_m f \rangle = 0,$$

so $Tf = 0$ always, i.e. $T = 0$. Conversely, for fixed $f \in S_2(N)$, suppose $\langle T, f \rangle = a_1(Tf) = 0$ for all $T \in \mathbb{T}$. Then, $0 = \langle T_m, f \rangle = a_m(f)$ for all $m \in \mathbb{N}$, so $f = 0$. Since $\dim_{\mathbb{C}} \mathbb{T} = \dim_{\mathbb{C}} S_2(N)$ (e.g. by Corollary 16.17), we conclude that $\langle -, - \rangle$ induces an isomorphism $S_2(N) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}, \mathbb{C})$. In particular, given $\chi : \mathbb{T} \to \mathbb{C}$, there is a unique $f \in S_2(N)$ so that $\langle T, f \rangle = \chi(T)$ for all $T \in \mathbb{T}$. To finish, observe that

$$f = \sum_{n \geq 1} a_n(f) q^n = \sum_{n \geq 1} a_1(T_n f) q^n = \sum_{n \geq 1} \langle T_n, f \rangle \, q^n = \sum_{n \geq 1} \chi(T_n) q^n = f_\chi,$$

so $f_\chi = f \in S_2(N)$ as claimed. ∎

16.2 Hecke correspondences

Recall 16.19. In terms of lattices, we had defined

$$(T_p f)(\Lambda) = \sum_{[\Lambda : \Lambda'] = p} f(\Lambda').$$

If Λ corresponds to the elliptic curve E, then choosing a sublattice Λ' of index p corresponds to choosing some degree p isogeny $E' \to E$ (taking the dual, this equivalently corresponds to a degree p isogeny $E \to E'$) ⊙

Recall 16.20. $X_0(p) = \{(E, G) : G \subset E \text{ order } p\}$. An order p subgroup is the same thing as a degree p isogeny, so equivalently

$$X_0(p) = \left\{ [E \xrightarrow{\varphi} E'] : \deg \varphi = p \right\}.$$

For $p \nmid N$, we'll think (G cyclic below)

$$X_0(Np) = \left\{ (E \xrightarrow{\varphi} E', G) : \deg \varphi = p \text{ and } \#G = N \right\}. \qquad \odot$$

Consider now the diagram

$$\begin{array}{ccc} & X_0(Np) & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_2} \\ X_0(N) & & X_0(N) \end{array}$$

where

$$p_1(E \xrightarrow{\varphi} E', G) = (E, G) \text{ and } p_2(E \xrightarrow{\varphi} E', G) = (E', \varphi(G)).$$

We if start with $(E, G) \in X_0(N)$, then $p_1^{-1}(E, G) = \left\{ (E \xrightarrow{\varphi} E', G) \right\}$ is the set of degree p isogenies out of E (with the extra data of G carried along). This looks a lot like what the Hecke operator does.

The diagram above is called a **Hecke correspondence**.

Definition 16.21. A **correspondence** $f : X \dashrightarrow X$ is a diagram of the form

$$\begin{array}{ccc} & Y & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_2} \\ X & & X \end{array}$$

say with X, Y smooth projective curves and p_1, p_2 finite maps. $\diamond$

Example. Any (finite) function $f : X \to X$ can be thought of as a correspondence by taking $Y = X$, $p_1 = f$, and $p_2 = \mathrm{id}$ $\triangle$

Slogan. A correspondence is a multiple valued function ($x \mapsto p_2 p_1^{-1}(x)$)

A correspondence f induces a map $\mathrm{H}^1(X, \mathbb{Z}) \to \mathrm{H}^1(X, \mathbb{Z})$ via $(p_2)_* p_1^*$. The pushforward here is the composition

$$(p_2)_* : \mathrm{H}^1(Y, \mathbb{Z}) \simeq \mathrm{H}_1(Y, \mathbb{Z}) \xrightarrow{(p_2)_*} \mathrm{H}_1(X, \mathbb{Z}) \simeq \mathrm{H}^1(X, \mathbb{Z})$$

coming from Poincaré duality.

f also induces a map $\mathrm{H}^0(X, \Omega^1) \to \mathrm{H}^0(X, \Omega^1)$ by $(p_2)_* p_1^*$.[24]

Fact. The action of the correspondence f is compatible with the Hodge decomposition

$$\mathrm{H}^1(X, \mathbb{Z}) \otimes \mathbb{C} \simeq \mathrm{H}^0(X, \Omega^1) \oplus \overline{\mathrm{H}^0(X, \Omega^1)}.$$

f also acts on divisors. Explicitly, given $x \in X$, one has

$$f_*([x]) := \sum_{p_1(y) = x} [p_2(y)].$$

Hence, f induces a map $f_* : \mathrm{Jac}(X) \to \mathrm{Jac}(X)$ which is $f_* = (p_2^*)^\vee p_1^*$.

[24] For the pushfowards, p_2 is a local diffeomorphism so induces isos on tangent spaces, so you can get a form by taking a tangent vector downstairs, looking at its preimages up stairs, evaluating on those, and then summing the values

16.2.1 Hecke operators

Recall we have $\widetilde{\mathbb{T}} \curvearrowright \mathrm{H}^1(X_0(N), \mathbb{Z})$, we have $S_2(N) = \mathrm{H}^0(X_0(N), \Omega^1)$, and we have $\mathrm{H}^1(X_0(N), \mathbb{C}) = S_2(N) \oplus \overline{S_2(N)}$.

If $T \in \widetilde{T}$ acts by 0 on $S_2(N)$, then it acts by 0 on $\overline{S_2(N)}$ and so acts by 0 on $\mathrm{H}^1(X_0(N), \mathbb{Z})$. Thus, the image of $\widetilde{\mathbb{T}}$ in $\mathrm{End}(\mathrm{H}^1(X_0(N), \mathbb{Z}))$ is $\cong \mathbb{T}$ (its image in $\mathrm{End}(S_2(N))$).

Corollary 16.22. *$\mathbb{T}$ is a finite rank free $\mathbb{Z}$-module ($\Longleftarrow$ submodule of $\mathrm{End}(\mathrm{H}^1(X_0(N), \mathbb{Z}))$), $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes \mathbb{C}$ and $\mathbb{T}_{\mathbb{Q}} = \mathbb{T} \otimes \mathbb{Q}$.*

Corollary 16.23. *Hecke eigenvalues are always algebraic integers.*

Corollary 16.24. *$\mathbb{T}_{\mathbb{Q}}$ is a semi-simple $\mathbb{Q}$-algebra ($\Longleftarrow$ $\mathbb{T}_{\mathbb{C}}$ being semisimple), so*

$$\mathbb{T}_{\mathbb{Q}} = \prod_{i=1}^{n} K_i$$

with K_i's number fields.

Corollary 16.25. *$\mathrm{H}^1(X_0(N), \mathbb{Q}) \otimes \mathbb{C} = S_2(N) \oplus \overline{S_2(N)}$ is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 2.*

Corollary 16.26. *$\mathrm{H}^1(X_0(N), \mathbb{Q})$ is a free $\mathbb{T}_{\mathbb{Q}}$-module of rank 2.*

Note that $\mathbb{T} \subset \mathrm{End}(J_0(N))$. The decomposition $\mathbb{T}_{\mathbb{Q}} = \prod_i K_i$ gives a decomposition

$$J_0(N) \sim \prod J_0(N)_i$$

(in the isogeny category). Specifically, one will have $K_i = e_i \mathbb{T}_{\mathbb{Q}}$ with $e_i \in \mathbb{T}_{\mathbb{Q}}$ an idempotent. Pick $k \in \mathbb{Z}$ s.t. $ke_i \in \mathbb{T}$ and then set $J_0(N)_i := (ke_i)J_0(N)$ (which is independent of k, up to isogeny).

This plays nicely with cohomology, e.g. $\mathrm{H}^1(J_0(N)_i, \mathbb{Q})$ is a 2-dimensional K_i-vector space. Hence, $T_\ell(J_0(N)_i)$ is a rank 2 module over $K_i \otimes \mathbb{Q}_\ell$. If we pick a place λ of K_i over ℓ, then $T_\ell(J_0(N_i)) \otimes_{K_i} K_{i,\lambda}$ will be a 2-dimensional $K_{i,\lambda}$-vector space.

Remark 16.27. The Hecke correspondences are defined over $\mathbb{Q}$, so this $T_\ell(J_0(N_i)) \otimes_{K_i} K_{i,\lambda}$ will have a $G_{\mathbb{Q}}$-action on it. So we've associated to this K_i, a Galois representation. We'll look at this more closely next time. ∘

16.3 Atkin-Lehner involution

Definition 16.28. The **Atkin-Lehner involution** is the involution $w : X_0(N) \to X_0(N)$ taking a cyclic isogeny of degree N to its dual isogeny. In terms of cyclic subgroups, it takes $(E, G) \mapsto (E/G, E[N]/G)$. The first description makes it clear that $w^2 = \mathrm{id}$. ◇

This w induces an action on $S_2(N) = \mathrm{H}^0(X_0(N), \Omega^1)$. One can compute that this is given by

$$(wf)(z) = f\left(-\frac{1}{Nz}\right).$$

Fact. w commutes with T_p ($p \nmid N$) and so preserves eigenspaces.

Since these eigenspaces are 1-dimensional, if f is an eigenform, then $wf = \pm f$.

17 Lecture 17: Eichler-Shimura

17.1 The Proof

Today, we want to prove the Eichler-Shimura theorem.

Recall 17.1. Last time we defined Hecke correspondences $T_p : X_0(N) \dashrightarrow X_0(N)$. ⊙

Their definition makes sense over $\mathbb{Q}$ which implies that $T_p \in \mathrm{End}(J_0(N))$. Now, $J_0(N)$ extends to an abelian scheme over $\mathbb{Z}[1/N]$ (since $X_0(N)$ is smooth over $\mathbb{Z}[1/N]$), and T_p extends to an endomorphism over this base as well. Now we can reduce mod any prime away from N.

Theorem 17.2 (Eichler-Shimura Theorem). *$T_p = F + V$ on $J_0(N)_{\mathbb{F}_p}$ where F is the Frobenius and V is the Verschiebung.*

Note that this definition of T_p is kinda funny; we defined it over $\mathbb{Q}$ and then extended abstractly. We'd like to compute it via a correspondence over $\mathbb{F}_p$.

Lemma 17.3. *Let $\mathscr{O}$ be a complete dvr with $K = \mathrm{Frac}\,\mathscr{O}$ and k the residue field of $\mathscr{O}$. Let $X/\mathscr{O}$ be a smooth proper curve, and let $f, g : Y \rightrightarrows X$ be two finite, flat maps. Let $J_K = \mathrm{Jac}(X_K)$ and let $J/\mathscr{O}$ be its Néron model (so $J = \mathrm{Pic}^0_{X/\mathscr{O}}$). Let $h_K : J_K \to J_K$ be the map given by (f, g) (i.e. this pullback-pushfoward thing), and let $h : J \to J$ be its extension to J. Now say we have a divisor $D_0 \in \mathrm{Div}(X_k)$ on the special fiber of X. Let $x_0 \in J_k$ be the corresponding point. Then,*

$$h(x_0) = [g_* f^*(D_0)] \in J_k.$$

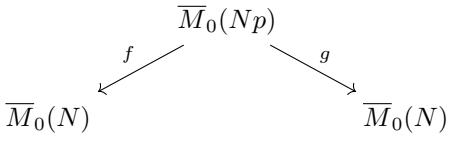
Proof. Lift D_0 to a relative divisor[25] D on $X/\mathscr{O}$ (possible since X is smooth). Let $D' = g_* f^*(D)$, another relative divisor on X. Then, D, D' define points $x, y \in J(\mathscr{O})$. By definition, $h(x)$ is the unique extension of $h_K(x_K) = [g_* f^* D_K] = y_K$, so we must have $y = h(x)$. Passing to the special fiber, we win. ■

To apply this, we'll want an integral representation of the Hecke correspondences.

Recall 17.4. $\overline{\mathcal{M}}_0(N)$ is the moduli stack of generalized elliptic curves w/ $\Gamma_0(N)$-structure, and $\overline{M}_0(N)$ is its coarse space. ⊙

There's a map of stacks $\widetilde{f} : \overline{\mathcal{M}}_0(Np) \to \overline{\mathcal{M}}_0(N)$ which forgets the level p structure, i.e. sends $(E, G) \mapsto E$ where E an EC with $\Gamma_0(N)$-structure and G is a $\Gamma_0(p)$ structure. Write $f : \overline{M}_0(Np) \to \overline{M}_0(N)$ for the induced map on coarse spaces. We can similarly define $\widetilde{g} : \overline{\mathcal{M}}_0(Np) \to \overline{\mathcal{M}}_0(N)$, $(E, G) \mapsto E/G$ as well as $g : \overline{M}_0(Np) \to \overline{M}_0(N)$. This gives a correspondence

Note that this g is simply the composition of f with the Atkin-Lehner involution at p



which, over $\mathbb{C}$, recovers the Hecke correspondence T_p from last time.

Fact. This f, g are finite + flat maps.

[25] Flat over the base and a divisor in each fiber

Corollary 17.5. *T_p is computed by $g_* f^*$ on $J_0(N)_{\mathbb{F}_p}$*

Now we can apply what we know about the structure of $\mathcal{M}_0(N)$ in characteristic p.

Recall 17.6. Define

$$\begin{array}{rccc} \widetilde{i}: & \overline{\mathcal{M}}_0(N) & \longrightarrow & \overline{\mathcal{M}}_0(Np) \\ & E & \longmapsto & (E, \ker F) \end{array}$$

and

$$\begin{array}{rccc} \widetilde{j}: & \overline{\mathcal{M}}_0(N) & \longrightarrow & \overline{\mathcal{M}}_0(Np) \\ & E & \longmapsto & (E^{(p)}, \ker V) \end{array}$$

Let i, j be the induced maps on coarse spaces.

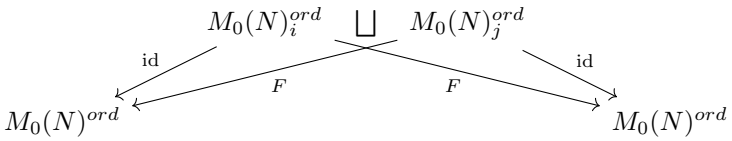
We computed before the compositions

$$fi = \mathrm{id}\,, \quad gj = \mathrm{id}\,, \quad fj = F, \quad \text{and} \quad gi = F.$$

The first two of these show that i, j are closed immersions. ⊙

Question: Why?

Let $M_0(N)^{\mathrm{ord}}$ be the open subscheme of $\overline{M}_0(N)$ representing ordinary elliptic curves. We have a map $(i, j) : M_0(N)^{\mathrm{ord}} \sqcup M_0(N)^{\mathrm{ord}} \to M_0(Np)^{\mathrm{ord}}$ which is a closed immersion and hits all the points, so is an isomorphism. Let's look at the Hecke correspondence on the ordinary locus



(the subscripts on the $M_0(N)^{ord}$'s indicate which map (i or j) they come from. The left vertical maps are $f : M_0(Np)^{ord} \to M_0(N)^{ord}$ while the right ones are $g : M_0(Np)^{ord} \to M_0(N)^{ord}$)

This is telling us that the Hecke correspondence T_p is (on the ordinary locus) a disjoint union of two correspondence, it is $T_p = (\mathrm{id}, F) + (F, \mathrm{id})$. We write $+$ instead of $\sqcup$ since it acts on divisors by addition of the two factor correspondences, i.e. if D is a divisor on $M_0(N)^{ord}$, then $T_p D = (\mathrm{id}, F)(D) + (F, \mathrm{id})(D) = F(D) + V(D)$.[26] Thus, $T_p = F + V$ holds on pts in $J_0(N)$ which are represented by divisors in the ordinary locus.

Answer: This is by cancellation theorem. fi is a closed immersion and f is separated (i.e. the diagonal of f is a closed immersion), so i must be a closed immersion too

Remark 17.7. There are only finitely many points in the supersingular locus, so any divisor is linearly equivalent to one supported in the ordinary locus! ∘

This proves Theorem 17.2!

17.2 Tate module of $J_0(N)$

Still in characteristic p.

Let $V_\ell := T_\ell(J_0(N)_{\mathbb{F}_p})[1/\ell]$ be the rational Tate module, a $\mathbb{Q}_\ell$-vector space. Since $\mathbb{T} \curvearrowright J_0(N)$, we get that V_ℓ is a $\mathbb{T}_{\mathbb{Q}_\ell}$-module which is moreover free of rank 2. The frobenius F also acts on V_ℓ, and it commutes w/ the action of $\mathbb{T}$, so can think of F as in $\mathrm{GL}_w(\mathbb{T}_{\mathbb{Q}_\ell})$. Eichler-Shimura says $T_p = F + V$, so

[26] The last equality holds since these correspondence are exactly how Frobenius and Verschiebung are defined on divisors

we get $FT_p = F^2 + p$, i.e.

$$F^2 - T_p F + p = 0.$$

Now, F is a 2×2 matrix over the ring $\mathbb{T}_{\mathbb{Q}_\ell}$ satisfying the above monic quadratic polynomial, so we'd like to conclude that $\operatorname{Tr} F = T_p$ and $\det F = p$.

Warning 17.8. This isn't automatic. For example $A = \operatorname{diag}(\lambda, \lambda) \in \mathrm{GL}_2(\mathbb{C})$ satisfies the quadratic polynomial $(A - \lambda)(A - \mu) = A^2 - (\lambda + \mu)A + \lambda\mu$ for any $\mu \in \mathbb{C}$. •

Proposition 17.9. $\operatorname{Tr}(F|V_\ell) = T_p$ *and* $\det(F|V) = p$

Proof. Let $\langle -, - \rangle : V_\ell \times V_\ell \to \mathbb{Q}_\ell(1)$ be the Weil pairing on V_ℓ. The T_q's (for $q \nmid N$) are self-adjoint w.r.t this pairing. Indeed, T_q is computed by the correspondence (f_q, g_q) and generalities tell us the adjoint is defined by (g_q, f_q). One of these looks like summing over q-isogenies out of E and the other looks like summing over q-isogenies into E, but these two sets are the same, and this is way they end up defining equal endomorphisms.

The upshot is that

$$\begin{array}{rccc} \varphi: & V_\ell & \longrightarrow & V_\ell^* \\ & x & \longmapsto & \langle -, x \rangle \end{array}$$

is an isomorphism of $\mathbb{T}_{\mathbb{Q}_\ell}$-modules. We claim that $\varphi(Fx) = V\varphi(x)$. This is because

$$\varphi(Fx)(y) = \langle y, Fx \rangle = \frac{1}{p} \langle FVy, Fx \rangle = \langle Vy, x \rangle = \varphi(x)(Vy) = (V\varphi(x))(y).$$

Hence, $\operatorname{Tr}(F|V_\ell) = \operatorname{Tr}(V|V_\ell^*) = \operatorname{Tr}(V|V_\ell)$ (last equality since the two are represented by matrices which are each others transpose). Now Eichler-Shimura says

$$T_p = F + V \implies 2T_p = \operatorname{Tr}(T_p) = 2\operatorname{Tr}(F)$$

($\operatorname{Tr}(T_p) = 2T_p$ since V_ℓ is free of rank 2 over $\mathbb{T}_{\mathbb{Q}_\ell} \ni T_p$, so T_p acts by a 2×2 scalar matrix). Now that we have this, the determinant part does follow from the polynomial $F^2 - T_p F + p = 0$. ■

(Above, important that we take trace/determinant as endomorphisms of $\mathbb{T}_{\mathbb{Q}_\ell}$-modules)

Fix a prime number N. Let $f \in S_2(N)$ be a normalized eigenform. Let $\alpha : \mathbb{T} \to \mathbb{C}$ defined by $T_p f = \alpha(T_p) f$. Since f is normalized, we have $\alpha(T_p) = a_p(f)$. Let $K = \alpha(\mathbb{T} \otimes \mathbb{Q})$, a number field; let $\mathscr{O} = \alpha(\mathbb{T})$, an order in K; and let $\mathfrak{a} := \ker \alpha \subset \mathbb{T}$, an ideal.

Notation 17.10. Set $A_f := J_0(N)/\mathfrak{a}J_0(N)$ where $\mathfrak{a}J_0(N) := \sum_{T \in \mathfrak{a}} TJ_0(N)$.

Remark 17.11. The assumption that N is prime is not needed (avoids having to worry about newform/oldform stuff). Also, the construction really only depends on $\mathfrak{a}$, not on f itself (picking f is like picking an embedding $K \hookrightarrow \mathbb{C}$). ∘

What's the dimension of A_f? First note

$$T_0(J_0(N)) = \mathrm{H}^0(X_0(N), \Omega^1) \overset{\text{over } \mathbb{C}}{=} S_2(N)$$

is (over $\mathbb{C}$) a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1. This implies that $T_0(J_0(N))$ is a free $\mathbb{T}_{\mathbb{Q}}$-module of rank 1. Thus,

$$T_0(A_f) = T_0(J_0(N))/\mathfrak{a}T_0(J_0(N))$$

is a 1-dimensional K-vector space.

Proposition 17.12. $\dim A_f = [K : \mathbb{Q}]$.

Corollary 17.13. *A_f is an elliptic curve $\iff$ $K = \mathbb{Q}$ $\iff$ Fourier coefficients of f are rational.*

Proposition 17.14. *A_f has good reduction away from N.*

This follows from the analogous statement for $J_0(N)$ (which holds since it's the Jacobian of a smooth, proper $\mathbb{Z}[1/N]$-curve).

Lemma 17.15. *Let B be an abelian variety over a dvr with good reduction, and let A be a subquotient of B. Then, A also has good reduction.*

Proof. Pick some invertible prime ℓ. Since B has good reduction, $T_\ell(B)$ is unramified (i.e. inertia acts trivially). $T_\ell(A)$ is a subquotient of $T_\ell(B)$, so $T_\ell(A)$ is also unramified. Now, Néron-Ogg-Shafarevich implies that A has good reduction. ∎

Consider

$$\mathscr{O} = \mathbb{T}/\mathfrak{a} \longrightarrow \mathrm{End}(A_f)$$

and so consider $V_\ell(A_f)$ as a $K \otimes \mathbb{Q}_\ell$-module. It will be free of rank 2.

Proposition 17.16. *Pick a prime $p \nmid \ell N$. Then, $\mathrm{Tr}(F_p|V_\ell) = a_p$ and $\det(F_p|V_\ell) = p$, where F_p is Frobenius at p, and $V_\ell = V_\ell(A_f)$.*

Proof. We've previously shown that $\mathrm{Tr}(F_p|V_\ell(J_0(N))) = T_p$. The surjection $J_0(N) \to A_f$ is compatible with the map $\mathbb{T} \to \mathbb{T}/\mathfrak{a}$, so we win as $\alpha(T_p) = a_p$. ∎

Choose an embedding $i : K \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Theorem 17.17. *There exists a unique (up to isomorphism) semi-simple representation*

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that

(1) *ρ is unramified away from $N\ell$*

(2) $\mathrm{Tr}(\rho(F_p)) = a_p(f)$

(3) $\det \rho = \chi_\ell$

Proof. (Existence) If $K = \mathbb{Q}$, we can take $V_\ell(A_f)$. In general, we take a piece of the Tate module of A_f. The choice of i determines an idempotent e of $K \otimes \mathbb{Q}_\ell$. Take ρ to be (the semi-simplification) of $e\,(V_\ell(A_f))$. We know that ρ is unramified away from $N\ell$, we know $\mathrm{Tr}(\rho(F_p)) = a_p$, and we know $\det(\rho(F_p)) = p$ for all $p \nmid N\ell$. The last of these imply $\det \rho = \chi_\ell$.

Two characters agreeing at almost all Frobenii, so get this by Chebotarev

(Uniqueness) Say ρ' also satisfies **(1)**,**(2)**,**(3)**. Then, $\mathrm{Tr}(\rho(F_p)) = a_p = \mathrm{Tr}(\rho'(F_p))$. Chebotarev tells us that the Frobenii are dense in the Galois group, so this implies that $\mathrm{Tr}(\rho(g)) = \mathrm{Tr}(\rho'(g))$ for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, ρ, ρ' are semi-simple reps w/ the same character and so $\rho \simeq \rho'$. ■

Fact. ρ is in fact absolutely irreducible.

Remark 17.18. Instead of taking our data to be a form f and an embedding of its coefficient field into $\overline{\mathbb{Q}}_\ell$, we could have just started with a homomorphism $\mathbb{T} \to \overline{\mathbb{Q}}_\ell$. For any such $\alpha : \mathbb{T} \to \overline{\mathbb{Q}}_\ell$, one gets a representation ρ_α as above. Furthermore, one has a decomposition

$$\mathrm{H}^1_{\text{ét}}(X_0(N)_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell) = \bigoplus_{\alpha:\mathbb{T}\to\overline{\mathbb{Q}}_\ell} \rho_\alpha. \qquad \circ$$

Corollary 17.19 (**Strong Multiplicity One**)**.** *Let N be prime. Choose $f, g \in S_2(N)$ normalized cusp forms (not necessarily eigenforms). Let S be a density 1 set of primes so that for all $p \in S$, f, g are eigenvectors of T_p with the same eigenvalues. Then, $f = g$.*

Proof. Let $\alpha : S \to \mathbb{C}$ be the function giving the eigenvalues. Let $V \subset S_2(N)$ be the space of h s.t. $T_p h = \alpha(p)h$ for all $p \in S$. We want to show that $\dim V = 1$. This V will have a basis consisting of normalized eigenforms for the full $\mathbb{T}$, so it's enough to show that if $h, h' \in V$ are normalized eigenforms for $\mathbb{T}$, then $h = h'$. Let $K \subset \mathbb{C}$ be generated by the coefficients of the h's, and choose an embedding $K \hookrightarrow \overline{\mathbb{Q}}_\ell$. This gives Galois representations $\rho, \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ associated to h, h'. These satisfy, among other things,

$$\mathrm{Tr}\,\rho(F_p) = a_p(h) \text{ and } \mathrm{Tr}\,\rho'(F_p) = a_p(h') \text{ for all } p \nmid N\ell.$$

Thus, $\mathrm{Tr}\,\rho(F_p) = \mathrm{Tr}\,\rho'(F_p)$ for all $p \in S$. By Chebotarev, these Frobenii are dense in the Galois group, so actually $\mathrm{Tr}\,\rho = \mathrm{Tr}\,\rho'$ everywhere. Hence, if p is any prime not dividing $N\ell$, we must have

$$a_p(h) = \mathrm{Tr}\,\rho(F_p) = \mathrm{Tr}\,\rho'(F_p) = a_p(h').$$

Choose two different ℓ's, we get $a_p(h) = a_p(h')$ for all $p \nmid N$. Now, (weak) multiplicity one implies that $h = h'$. ■

18 Lecture 18: Criterion for non-existence of torsion points

Today we want to prove Theorem 1.5.

Theorem 18.1 (Theorem 1.5)**.** *Fix a prime $N > 7$. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a map $f : X_0(N) \to A$ s.t.*

- *A has good reduction away from N.*
- *$A(\mathbb{Q})$ has rank 0.*
- *$f(0) \neq f(\infty)$.*

Then, no elliptic curve over $\mathbb{Q}$ has a rational point of order N.

After this lecture, we'll try to find some A verifying these hypothesis. The hardest one will be the second one (that $A(\mathbb{Q})$ has rank 0), but luckily we have Theorem 11.1 which gives a criterion for that. Hence, combining Theorems 18.1 + 11.1, we have (or will have by the end of the lecture)

Theorem 18.2. *Let $N > 7$ be prime. Fix a prime $p \neq N$ and suppose there is an abelian variety $A/\mathbb{Q}$ along with a map $f : X_0(N) \to A$ so that*

- *A has good reduction away from N*
- *A has completely toric reduction at N*
- *$A[p](\overline{\mathbb{Q}})$ has J-H constituents either 1 or χ_p*
- *$f(0) \neq f(\infty)$*

Then, no elliptic curve over $\mathbb{Q}$ has a point of order N.

Keep this in mind for future lectures, but today we focus on Theorem 18.1. In fact, we'll actually spend most of our time proving the below theorem instead.

Theorem 18.3. *Let A, f be an in Theorem 18.1. Suppose $E/\mathbb{Q}$ has a point of order N. Then,*

$$E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N.$$

Remark 18.4. Having a point of order $N \implies \mathbb{Z}/N\mathbb{Z} \subset E[N]$. The Weil paring then gives an extension

$$0 \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow E[N] \longrightarrow \mu_N \longrightarrow 0.$$

Theorem 18.3 then says that this extension is split. ∘

18.1 Proof of Theorem 18.1, assuming Theorem 18.3

Setup 18.5. Assume we have A, f as in Theorem 18.1.

Lemma 18.6. *$X_0(N)(\mathbb{Q})$ and $X_1(N)(\mathbb{Q})$ are finite.*

Proof. Consider the maps

$$X_1(N)(\mathbb{Q}) \to X_0(N)(\mathbb{Q}) \xrightarrow{f} A(\mathbb{Q})$$

and each of these maps have finite fibers (since $X_0(N), X_1(N)$ are curves and these maps are non-constant). $A(\mathbb{Q})$ is finite by hypothesis. ■

Lemma 18.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then,* $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$.

Proof. Let $\mathscr{O} = \mathrm{End}(E)$ and let $K = \mathscr{O} \otimes \mathbb{Q}$, so K is either $\mathbb{Q}$ or an imaginary quadric field. The natural map $\mathscr{O} \to \mathrm{End}(T_0E) = \mathbb{Q}$ is a ring homomorphism, so extends to a ring homomorphism $K \to \mathbb{Q}$, so $K = \mathbb{Q}$ and $\mathscr{O} = \mathbb{Z}$. ■

Proposition 18.8. *Theorem 18.3 $\implies$ Theorem 18.1*

Proof. Suppose $E_1/\mathbb{Q}$ is an elliptic curve with a point P_1 of order N. Then, Theorem 18.3 implies we can find $\mu_N \subset E_1$. Let $E_2 = E_1/\mu_N$, and let P_2 be the image of P_1. Now we can inductively get an infinite chain

$$E_1 \xrightarrow{N} E_2 \xrightarrow{N} E_3 \xrightarrow{N} \dots$$

of cyclic N-isogenies with order N points $P_i \in E_i$. These give points $(E_i, P_i) \in X_1(N)(\mathbb{Q})$, so finiteness implies that $E_i \cong E_j$ for some $i < j$. Let $f : E_i \to E_j$ be the isomorphism, and let $g : E_i \to E_j$ be the map appearing in the above infinite chain. Then, $f^{-1}g : E_i \to E_i$ is an isogeny of degree N^{j-i}. If $f^{-1}g = [n]$ for some integer n, then $n = N^{\frac{j-i}{2}}$ (by degree considerations), but then $(f^{-1}g)(P_i) = N^{\frac{j-i}{2}}P = 0$. However, $g(P_i) \neq 0$ and f is an isomorphism, so $f^{-1}g \neq [n]$ which implies $\mathrm{End}(E_i) \neq \mathbb{Z}$, a contradiction. ∎

18.2 Proof of Theorem 18.3

Assumption. We have a map $f : X_0(N) \to A$ where

- A has good reduction away from N
- $A(\mathbb{Q})$ has rank 0
- $f(0) \neq f(\infty)$

Suppose we have an elliptic curve $E/\mathbb{Q}$ with an N-torsion point $P \in E[N](\mathbb{Q})$.

Goal. We want to show that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$.

Let $\mathscr{E}/\mathbb{Z}$ be the Néron model of E, and extend $P \in E[N](\mathbb{Q})$ to $\mathcal{P} \in \mathscr{E}(\mathbb{Z})$.

Proposition 18.9 (Step 1)**.** *E has everywhere semistable reduction*

Proof. Suppose E has additive reduction at p.

(Case 1: $N \neq p$) The reduction map on N-torsion is injective (by Proposition 8.11), so $\mathcal{P}_{\mathbb{F}_p} \in \mathscr{E}_{\mathbb{F}_p}$ still has order N. The classification of Néron models implies that $\mathscr{E}_{\mathbb{F}_p}$ has ≤ 4 components which forces the image of $\mathcal{P}_{\mathbb{F}_p}$ in the component group is 0 (since N prime to $2, 3$), so $\mathcal{P}_{\mathbb{F}_p} \subset \mathscr{E}^0_{\mathbb{F}_p} \simeq \mathbb{G}_a$, a contradiction as $\mathbb{G}_{a,\mathbb{F}_p}$ has no non-trivial N-torsion.

(Case 2: $N = p$) Since $1 = e < N - 1$, Raynaud (theorem 7.3) will tell us that $\mathcal{P}_{\mathbb{F}_p}$ still has order N. By the same reasoning, $\mathcal{P}_{\mathbb{F}_p} \in \mathscr{E}^0_{\mathbb{F}_p} = \mathbb{G}_{a,\mathbb{F}_p}$. Now, let $K/\mathbb{Q}_p$ be such that E_K has semistable reduction. We may assume $[K : \mathbb{Q}_p] \leq 6$ (see Remark 8.9, note $p = N \notin \{2, 3\}$). Let $\mathscr{O} = \mathscr{O}_K$ and let $k = \mathscr{O}/\mathfrak{m}$ be the residue field. Let $\mathscr{E}'/\mathscr{O}$ be the Néron model of E_K. The Néron mapping property gives a map

$$f : \mathscr{E}_{\mathscr{O}} \longrightarrow \mathscr{E}'$$

which is the identity of the generic fiber. We claim that $f(\mathscr{E}^0_k) = 0$. This is because $\mathscr{E}^0_k = \mathbb{G}_a$ while $(\mathscr{E}')^0_k$ is an elliptic curve or a torus; there are no non-constant maps from $\mathbb{G}_a$ to either of these things. Let $\mathcal{P}' \in \mathscr{E}'(\mathscr{O})$ extend P. Then, $\mathcal{P}' = f(\mathcal{P})$ since these both extend P. This is a contradiction. Over k, $f(\mathcal{P})$ specializes to 0, so $\mathcal{P}'_k = 0$, contradicting injectivity on the reduction map on N-torsion (holds by Raynaud since $e(K) \leq 6 < N - 1$ as $N > 7$). ∎

Remark 18.10. The above argument can be generalized a bit. It didn't really use most of what's special about A. It's mainly just something about having an elliptic curve over an extension of $\mathbb{Q}_p$ and a point whose order is large compared to the ramification index, then the curve must be semistable. ∘

Proposition 18.11 (Step 2)**.** *Pick $p \in \{2,3\}$. Then, E has bad (so multiplicative) reduction at p, and $\mathcal{P}_{\mathbb{F}_p} \notin \mathscr{E}^0_{\mathbb{F}_p}$.*

Proof. First suppose E has good reduction. Then, $\mathcal{P}$ specializes to a point of order N in $\mathscr{E}_{\mathbb{F}_p}$. By the Hasse bound (Theorem 3.4), we know

$$\mathscr{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p} \leq 4 + 2\sqrt{3} < 8 \leq N,$$

a contradiction. Thus, E must in fact have multiplicative reduction, so $\mathscr{E}^0_{\mathbb{F}_p}$ is a 1-dimensional torus over $\mathbb{F}_p$, i.e. it's $\mathbb{G}_m$ or $T := \left(\mathrm{Res}^{\mathbb{F}_{p^2}}_{\mathbb{F}_p} \mathbb{G}_m\right)^1$, the norm 1 elements of the quadratic extension, the kernel of the norm map $\mathrm{Nm} : \mathrm{Res}^{\mathbb{F}_{p^2}}_{\mathbb{F}_p} \mathbb{G}_m \to \mathbb{G}_m$.[27] Note that $\mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^\times$ has $p-1$ elements and $T(\mathbb{F}_p) =$ norm 1 elements of $\mathbb{F}_{p^2}^\times$ has $p+1$ elements. Since $p \pm 1 \leq 4 < N$, we can't have $\mathcal{P}_{\mathbb{F}_p} \in \mathscr{E}^0_{\mathbb{F}_p}$. ■

Corollary 18.12. *$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$*

Proof. Let $G \subset E[N]$ be the group of points reducing into $\mathcal{E}^0_{\mathbb{F}_p}$, a subgroup of order N. Since N is prime (so every nonzero element of $\mathbb{Z}/N\mathbb{Z}$ has order N), Step 2 shows that $G \cap \mathbb{Z}/N\mathbb{Z} = 0$, so $E[N] = G \oplus \mathbb{Z}/N\mathbb{Z}$. The Weil pairing shows that $E[N]$ is self-Cartier dual, so we conclude that $G \simeq \mu_N$. ■

Question: Why is $\#G = N$

Proposition 18.13 (Step 3)**.** *Say $p \notin \{2,3\}$ is a prime of bad reduction for E. Then, $\mathcal{P}_{\mathbb{F}_p} \notin \mathscr{E}^0_{\mathbb{F}_p}$.*

(This is where we finally use our hypotheses)

Proof. First note

(1) $\mathcal{P}_{\mathbb{F}_p}$ has order N (if $p \neq N$, prime to N. If $p = N$, apply Raynaud, see Theorem 19.16)

(2) E has multiplicative reduction at p (Step 1)

If $p = N$, then $\#\mathscr{E}^0_{\mathbb{F}_N}(\mathbb{F}_N) = N \pm 1$ (it's a torus) which is prime to N, so $\mathcal{P}_{\mathbb{F}_N} \notin \mathscr{E}^0_{\mathbb{F}_N}$. Hence, from now on, we may assume $p \neq N$. There are three $\mathbb{Z}[1/N]$-points of $X_0(N)$ that we'll care about

(1) The cusp ∞. This is the generalized elliptic curve that's a 1-gon (so smooth locus is $\mathbb{G}_m$) with $\Gamma_0(N)$-structure $\mu_n \subset \mathbb{G}_m$.

(2) The cusp 0. This the generalized elliptic curve that's an N-gon. The smooth locus is $\mathbb{G}_m \times \mathbb{Z}/N\mathbb{Z}$ with $\Gamma_0(N)$-structure $\mathbb{Z}/N\mathbb{Z}$.

In this case, the $\Gamma_0(N)$-structure is *not* contained in the identity component.

(3) The third point is $x = (E, \mathbb{Z}/N\mathbb{Z})$ (with the $\mathbb{Z}/N\mathbb{Z}$ generated by P).

To be precise, the minimal regular model of E over $\mathbb{Z}[1/N]$ has semi-stable reduction everywhere, so it's bad fibers are n-gons. Hence, E does extend to a generalized elliptic curve and then to get a $\Gamma_0(N)$-structure, you contract all irreducible components not meeting the $\mathbb{Z}/N\mathbb{Z}$ generated by the extension of P.

Answer: G is the kernel of the map $f : E[N] \to \Phi_p$ to the component group of $\mathscr{E}_{\mathbb{F}_p}$. Since $\mathcal{E}_{\mathbb{F}_p}$ is a (the smooth locus of a) Néron n-gon, Φ_p is cyclic, so f has nontrivial kernel. Furthermore, f has nontrivial image by Step 2. Since N is prime, the claim follows

Remember: In a $\Gamma_0(N)$-structure

[27] Twisted forms of $\mathbb{G}_m$ are characterised by $\mathrm{H}^1(G_{\mathbb{F}_p}, \mathrm{Aut}\,\mathbb{G}_{m,\overline{\mathbb{F}}_p}) = \mathrm{H}^1(G_{\mathbb{F}_p}, \{\pm 1\}) = \mathrm{Hom}_{cts}(\widehat{\mathbb{Z}}, \pm 1)$ which has size 2

Let $\mathcal{A}/\mathbb{Z}[1/N]$ be the abelian scheme extending A. Then, we get $f : X_0(N) \to \mathcal{A}$ extending the f we started with, by the Néron mapping property. The reduction map

$$\mathcal{A}(\mathbb{Z}[1/N]) = A(\mathbb{Q}) = A(\mathbb{Q})_{tors} = \mathcal{A}(\mathbb{Z}[1/N])_{tors} \to \mathcal{A}(\mathbb{F}_q)$$

is injective for $q \neq 2$ (using Raynaud for q-torsion). Now, both x and $0 \in X_0(N)(\mathbb{Z}[1/N])$ have the same reduction mod 3 (Step 2 shows level structure mod 3 does not lie in identity component), so $f(x) = f(0)$ in $\mathcal{A}(\mathbb{F}_3)$. By injectivity, this implies that $f(x) = f(0) \in \mathcal{A}(\mathbb{Z}[1/N])$.

Now, suppose that $\mathcal{P}_{\mathbb{F}_p} \in \mathscr{E}^0_{\mathbb{F}_p}$. This implies that x, ∞ have the same reduction in $X_0(N)(\mathbb{F}_p)$ which implies $f(x) = f(\infty) \in \mathcal{A}(\mathbb{F}_p)$ which implies $f(x) = f(\infty)$ in $\mathcal{A}(\mathbb{Z}[1/N])$ which implies $f(0) = f(\infty)$, a contradiction. ∎

Corollary 18.14. *If p is a prime of bad reduction, then $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$.*

Now we can complete the proof of Theorem 18.3. Let $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{F}_N)$ be the representation given by $E[N]$, and let $K = \mathbb{Q}(\mu_N)$.

Lemma 18.15. *$\rho|_K$ is everywhere unramified.*

Proof. We break up into cases

($p \neq N$, E has good reduction) Then ρ unramified at p by Néron-Ogg-Shafervich.

($p = N$, E has good reduction at p) Have exact sequence of finite flat group schemes ($\mathscr{E}[N]$ finite since E has good reduction at N)

$$0 \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathscr{E}[N] \longrightarrow \mu_N \longrightarrow 0.$$

There's also the connected-étale sequence going the other way around, so this must be split. Hence, $\mathscr{E}[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$, so $\rho|_K$ is the trivial representation, and hence unramified.

(p prime of bad reduction) Steps 2 + 3 $\implies E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$, so $\rho|_K$ again trivial. ∎

Now, ρ must be of the form (recall we have an N-torsion point $P \in E[N](\mathbb{Q})$)

$$\rho = \begin{pmatrix} 1 & f_0 \\ & \chi \end{pmatrix}$$

with χ the mod N cyclotomic character and $f_0 : \Gamma \to \mathbb{F}_N$ a 1-cocycle for χ^{-1}. Let $f = f_0|_K$, so $f : \Gamma_K \to \mathbb{F}_N$ is a group homomorphism (since $\chi|_K = 1$) which is everywhere unramified. By class field theory, we can regard f as a homomorphism $\mathrm{Cl}(K) \to \mathbb{F}_N$. If we let $H = \mathrm{Cl}(K) \otimes \mathbb{Z}/N\mathbb{Z}$, then we can via f as an element of the dual space $H^* \ni f$. Now, $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{F}_N^\times$ acts on H. Now, H is an $\mathbb{F}_N$-vector space and $(N, \#\mathbb{F}_N^\times) = 1$, so we can decompose

$$H = \bigoplus_{i \in \mathbb{F}_N^\times} H^i \text{ where } H^i = \left\{x \in H : [a]x = a^i x\right\}.$$

You can do the same thing for H^*. If you write down the 1-cocycle condition for f, you can see how the Galois group acts on it, and conclude that $f \in (H^*)^1 = (H^{-1})^*$.

Theorem 18.16 (**Herbrand's theorem**). *Suppose that $j > 1$ is an odd integer. Then, $H^j \neq 0$ only if $N \mid B_{N-j}$, N divides that Bernoulli number.*

(We'll use this as a black box from algebraic number theory)

Corollary 18.17. *$H^{-1} = H^{N-2} \neq 0$ only if $N|B_2 = 1/6$, i.e. $H^{-1} = 0$.*

This forces $f = 0$, so $\rho|_K = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ is the trivial representation. Thus, ρ is really a representation of $\mathrm{Gal}(K/\mathbb{Q})$. Since $\#\,\mathrm{Gal}(K/\mathbb{Q})$ is prime to N, ρ must be semi-simple. This gives the splitting

$$E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N.$$

and so proves Theorem 18.3.

19 Lecture 19: $J_0(N)$ mod N

Goal (Course). Fix a prime $N > 7$. We want to find an abelian variety $A/\mathbb{Q}$ and a map $f : X_0(N) \to A$ s.t.

(1) A has good reduction away from N

(2) A has completely multiplicative reduction at N

(3) $A[p](\overline{\mathbb{Q}})$ only has trivial and cyclotomic Jordan-Hölder factors

(4) $f(0) \neq f(\infty)$

Such a thing would guarantee that no elliptic curve over $\mathbb{Q}$ has rational N-torsion.

The Jacobian $J_0(N) = \mathrm{Jac}(X_0(N))$ is the universal abelian variety to which $X_0(N)$ maps. Hence, such an A must be a quotient of $J_0(N)$.

Remark 19.1. For such A, condition **(1)** is free. This is because

- $X_0(N)$ has a smooth, proper model away from N
- $\implies$ $J_0(N)$ has good reduction away from N
- Good reduction passes to quotients ∘

Goal (Today). Show that **(2)** is also free. We will show

- the minimal regular model of $X_0(N)$ at N is 'nice enough'
- Deduce from this that $J_0(N)$ has completely toric reduction
- "Completely toric reduction" descends to quotients

Most of the work will be in the first step. The second will involve a theorem of Raynaud which we will employ as a black box. The third step is below

Proposition 19.2. *Let $K/\mathbb{Q}_p$ be a finite extension with $\mathscr{O} = \mathscr{O}_K$ and $k = \mathscr{O}/\mathfrak{m}$. Let A/K be an abelian variety and consider some quotient abelian variety B of A. If A has completely toric reduction, then so does B.*

Proof. Let $f : A \to B$ be the quotient map. The isogeny category is semisimple, so this map has a section (up to inverting some n), i.e. $\exists g : B \to A$ so that $fg = [n]$ for some $n > 0$. Let $\mathcal{A}, \mathcal{B}/\mathscr{O}$ be the Néron models of A, B, so f, g extend to them and we still have $fg = [n]$. On special fibers, we get $\mathcal{A}_k^0 \xrightarrow{f} \mathcal{B}_k^0$ which is surjective since $fg = [n]$ is surjective. Since $\mathcal{A}_k$ is a torus, this implies that the quotient $\mathcal{B}_k^0$ is also a torus. ■

Question: Is it a priori clear that multiplication by n is surjective on $\mathcal{B}_k^0$?

Let's now explain this theorem of Raynaud allowing us to move from the model to the Jacobian.

Definition 19.3. Let $f : X \to S$ be proper and flat. The **Picard functor** $\mathrm{Pic}_{X/S}$ is the sheafification of $S' \mapsto \mathrm{Pic}(X_{S'})$ on the fppf site of S. ◇

Theorem 19.4 (Murre)**.** *If $S = \operatorname{Spec} k$ is a field, then $\mathrm{Pic}_{X/S}$ is representable by a group scheme.*

Hence, if $S = \operatorname{Spec} k$, we can define $\mathrm{Pic}^0_{X/S}$ as the identity component of $\mathrm{Pic}_{X/S}$. In general, we define $\mathrm{Pic}^0_{X/S} \subset \mathrm{Pic}_{X/S}$ as the subsheaf whose sections land in $\mathrm{Pic}^0_{X_{\overline{s}}/s}$ for each geom pt $\overline{s} \to S$.

Now suppose $S = \operatorname{Spec} \mathscr{O}$ with $\mathscr{O}$ a dvr, $K = \operatorname{Frac} \mathscr{O}$, and $k = \mathscr{O}/\mathfrak{m}$. Further suppose that X is a curve (fibers pure of dimension 1), and let $\{X_i\}$ be the set of irreducible components of the special fiber X_k. Define

$$d_i := \text{length (local ring of generic point of } X_i) =: \textbf{multiplicity of } X_i \textbf{ in } X.$$

History. There are (at least) two algebraic geometers with the last name Raynaud. There is Michel Raynaud and there is Michèle Raynaud, and the two of them were married. I think possibly both Raynaud theorems in this class were proved by Michel, here (Lecture 7 theorem) and here (below). ⊖

Theorem 19.5 (Raynaud)**.** *Suppose that*

(1) *X_K is smooth over K*

(2) *X is regular*

(3) $\gcd(d_i) = 1$

Then, $\mathrm{Pic}^0_{X/S}$ is represented by a smooth group scheme over $\mathscr{O}$, and it is in fact isomorphic to the identity component of the Néron model of $\mathrm{Jac}(X_K)$. In particular, the identity component of the special fiber of Néron model of $\mathrm{Jac}(X_k)$ is $\mathrm{Pic}^0_{X_k/k}$.

(We will be adopting this as a black box)

So now we want to understand the minimal regular model of $X_0(N)$.

19.1 The minimal regular model of $X_0(N)$

A natural guess is that the coarse space $\overline{M}_0(N) = \left|\overline{\mathcal{M}}_0(N)\right|$ is the minimal regular model. It is a flat, proper model over $\mathbb{Z}$. Furthermore, one can show that the stack is regular over $\mathbb{Z}$. However, taking the coarse space messes with things, so this is not the minimal regular model (sounds like $\overline{M}_0(N)$ is not even regular).

Fact (see Katz-Mazur). $\overline{\mathcal{M}}_0(N)$ is regular

The approach to understand these spaces is to pass to a cover of $\overline{\mathcal{M}}_0(N)$ which is a scheme so that this stack (and its coarse space) will be recoverable as quotients by some finite group.

Setup 19.6. Fix a prime $p = N > 3$. Let $\ell > 3$ be another prime and assume $l \not\equiv 0, \pm 1 \pmod{p}$. Let $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ and note that

$$\#G = (\ell^2 - 1)(\ell^2 - \ell) = \ell(\ell - 1)^2(\ell + 1) \not\equiv 0 \pmod{p}$$

(To form an invertible matrix, pick a nonzero vector and then pick a vector that's not a multiple of the first one).

We're really only going to be caring about what happens at p, so work over $\mathbb{Z}[1/(6\ell)]$ below. There will be three spaces of interest

- $\mathcal{M}_0(p)$ and its coarse space $M_0(p) = |\mathcal{M}_0(p)|$
- $\mathcal{M}_0(p; \ell)$, the moduli space of ECs w/ $\Gamma_0(p)$ and $\Gamma(\ell)$-structures

  Since $\ell \geq 3$, the $\Gamma(\ell)$-structure rigidifies things, so this is actually a(n) (affine) scheme $M_0(p; \ell) = \mathcal{M}_0(p; \ell)$. Furthermore, $G \curvearrowright M_0(p; \ell)$ by moving around the $\Gamma(\ell)$-structure. Finally,[28]

  $$\mathcal{M}_0(p) = [M_0(p; \ell)/G] \text{ and } M_0(p) = M_0(p; \ell)/G.$$

- $M(\ell)$, the moduli scheme of ECs w/ $\Gamma(\ell)$-structure

There is a natural map $M_0(p; \ell) \to \mathcal{M}_0(p)$ which simply forgets the ℓ structure; this is the quotieht map.

Fact (see Katz-Mazur). $M_0(p; \ell)$ is regular + flat

Proposition 19.7. *$M_0(p; \ell)_{\mathbb{F}_p}$ is reduced and Cohen-Macaulay. It is also smooth away from the super-singular points, but has **ordinary nodes**[29] at the super singular points.*

Proof. $M_0(p; \ell) = \operatorname{Spec} A$ where A is a regular ring which is flat over $\mathbb{Z}[1/\ell]$ (by the fact). Note that $M_0(p; \ell)_{\mathbb{F}_p} = \operatorname{Spec} B$ where $B = A/pA$. We've killed a non-zero divisor of a regular ring, so B is CM by commutative algebra. Consider the usual maps $i, j : M(\ell) \to M_0(p; \ell)$ (i takes $\ker F$ and j takes $\ker V$) along with the usual maps $f, g : M_0(p; \ell) \to M(\ell)$. Note that i, j are closed immersions (e.g. since fi is the identity). From these, we see that

$$M_0(p; \ell)^{ord} \cong M(\ell)^{ord} \sqcup M(\ell)^{ord}$$

is smooth. Now, commutative algebra tells us that if you have a 1-dimensional thing which is generically reduced and CM, then it is reduced.

Next, we claim that intersections of images of i, j meet transversely at the supersingular points. Say $x, y \in M(\ell)$ are super-singular and $i(x) = j(y)$. Pick $v \in T_x(M(\ell))$ and $w \in T_y M(\ell)$. We want to say

[28] Note below that, since $M_0(p; \ell)$ is affine, we have $M_0(p) = \operatorname{Spec} \mathscr{O}(M_0(p; \ell))^G$

[29] i.e. the strict (go up to algebraic closure) complete local rings look like $k[\![x, y]\!]/(xy)$

they are linearly independent after being pushed to $M(p;\ell)$. Suppose we have a linear dependence

$$\alpha i_*(v) + \beta j_*(w) = 0.$$

Apply f_* and use that $fi = \mathrm{id}$ while $fj = F$ (so $(fj)_* = 0$). This implies that

$$\alpha v = 0 \implies \alpha = 0.$$

Similarly, applying g_* shows $\beta w = 0 \implies \beta = 0$.

Finally, let $z = i(x) = j(y)$. We want to show this is a node. Write $M_0(p;\ell) = \operatorname{Spec} A$ and $M(\ell) = \operatorname{Spec} C$. Let

$$a : A_z \to C_x \times C_y$$

be the ring homomorphism given by (i^*, j^*). Choose uniformizers $t \in C_x$ and $t' \in C_y$. s.t. $Ft = (t')^p$ and $Ft' = t^p$ (possible, if we work over $\overline{\mathbb{F}}_p$, since Frobenius interchanges x, y). Note that a is injective since A_z is reduced[30] (since A is) and the maps i, j hit both components at z. Let

$$u = f^*(t) - g^*(t')^p \in A_z.$$

Then,

$$i^*(u) = t - t^{p^2} \text{ and } j^*(u) = (t')^p - (t')^p = 0.$$

Similarly define $v := g^*(t') - f^*(t)^p$ and conclude that

$$a(u) = (t - t^{p^2}, 0) \text{ and } a(v) = (p, t' - (t')^{p^2})$$

(note that $a(u)$ is a uniformizer for C_x while $a(v)$ is a uniformizer for C_y). Given any $f \in$ max ideal of A_z, $a(f)$ will land in the product of the maximal ideals of C_x, C_y and so we see that we can write $a(f) = F(a(u), a(v)) = a(F(u, v))$ for some power series F. Since a is injective, $f = F(u, v)$, so we have a surjection

$$k[\![u, v]\!] \twoheadrightarrow A_z.$$

Since a is injective, we see that $uv = 0$, so we really have $k[\![u, v]\!]/(uv) \twoheadrightarrow A_z$. This must be injective or it'd kill a component, so z really is a node. ∎

We'd like to do this integrally now.

Proposition 19.8. *$M_0(p;\ell)$ is smooth over $\mathbb{Z}[1/\ell]$ away from super-singular points in characteristic p. The strict complete local ring @ a s-s pt in char p is of the form*

$$W[\![x, y]\!]/(xy - p) \text{ where } W = W(\overline{\mathbb{F}}_p)$$

is the ring of Witt vectors over $\overline{\mathbb{F}}_p$.

Proof. Let R be the strict complete local ring at a supersingular point x in characteristic p. We know that R is regular (since $M_0(p;\ell)$ is regular), flat over $\mathbb{Z}[1/\ell]$, and of dimension 2. Furthermore, $R/pR \simeq$

[30] Being reduced implies that A_z injects into the product of its quotients by minimal primes, and the minimal primes of A_z correspond to irreducible components of A passing through z

$k[\![x,y]\!]/(xy)$ by the previous proposition. By Nakayama's lemma, we get a surjective $W[\![x,y]\!] \twoheadrightarrow R$. Choose $w \in R$ so that $xy = pw$. Let $R' := W[\![x,y]\!]/(xy - pw)$ which surjects onto R. Note that, as a W-module, we have

$$R' = W \oplus \bigoplus_{i>0} Wx^i \oplus \bigoplus_{j>0} Wy^j,$$

so it is free and hence flat over W. Furthermore, $R'/p \xrightarrow{\sim} R/p$. Since R is flat over W, we conclude that $R' \xrightarrow{\sim} R$.[31] Finally, we need to show that we can take $w = 1$. We have

$$R = W[\![x,y]\!]/(xy - pw) \text{ with maximal ideal } \mathfrak{m} := (x,y,p).$$

Note that $\mathfrak{m}/\mathfrak{m}^2$ is spanned by $p, x, y \bmod pw$ (the only relation is $xy - pw$ but also $xy \in \mathfrak{m}^2$ so is 0 in the quotient). If $w \in \mathfrak{m}$, then $pw \in \mathfrak{m}^2$ which would imply $\dim \mathfrak{m}/\mathfrak{m}^2 = 3$, contradicting regularity of R ($\dim R = 2$). Thus, $w \notin \mathfrak{m}/\mathfrak{m}^2$, so $w \in R^\times$, so change $x \rightsquigarrow x/w$ to get $w = 1$. ■

Recall 19.9. $M_0(p) = M_p(p;\ell)/G = \operatorname{Spec} \mathscr{O}(M_0(p;\ell))^G$. ⊙

Since $\#G$ is prime to p, taking invariants $(-)^G$ commutes w/ tensoring $- \otimes \mathbb{F}_p$. Note that $-1 \in G$ acts trivially on $M_0(p;\ell)$ and $\overline{G} = G/\{\pm 1\}$ acts faithfully on $M_0(p;\ell)$. Let R be the strict complete local ring of $M_0(p)$ at some point x, and let S be the strict complete local ring of $M_0(p;\ell)$ at some point y above x (both x, y in char p). The points above x are permuted transitively by $\overline{G}$, with stabilizer groups $\operatorname{Aut}(x)/\{\pm 1\} =: \overline{H}$. Thinking about this, this is telling us that

$$R = S^{\overline{H}}.$$

Fact (about elliptic curves in char 3)**.** There are 3 possibilities for $\overline{H}$:

(1) If $j(x) \neq 0, 1728$, then $\overline{H} = 0$

(2) If $j(x) = 1728$, then can have $\overline{H} = \mathbb{Z}/2\mathbb{Z}$

(3) If $j(x) = 0$, can have $\overline{H} = \mathbb{Z}/3\mathbb{Z}$

Where $\overline{H} = 0$ (e.g. $j(x) \neq 0, 1728$), we get $R = S$ and we're happy.
If $\overline{H} \neq 0$, it acts nontrivially on S.

- Say $j(x) = 1728$ and $\overline{H} = \mathbb{Z}/2\mathbb{Z}$.

  Suppose x is ordinary. Then, (since we're smooth at S?) we'll have $S = W[\![x]\!]$ and $\overline{H}$ will act by $x \mapsto -x$ (if x chosen appropriately). Then, $R = W[\![x^2]\!] \cong W[\![y]\!]$ which is again smooth.

  Suppose x is supersingular. Then, $S = W[\![x,y]\!]/(xy - p)$. Choosing x, y appropriately, $\overline{H}$ acts by $x \mapsto -x, y \mapsto -y$. The invariants are generated by $X := x^2, xy = p$, and $Y := y^2$, so $R \simeq W[\![X,Y]\!]/(XY - p^2)$.

- If $j(x) = 0$ and $\overline{H} = \mathbb{Z}/3\mathbb{Z}$, get $R = W[\![x^3]\!]$ or $R = W[\![s,t]\!]/(st - p^3)$.

Theorem 19.10. *Say x is a point of $M_0(p)$ in char p with strict complete local ring R. Then,*

[31] The kernel of $R' \to R$ must be contained in $pR' = \ker(R' \to R \to R/p)$. If anything in pR' vanishes in R, then R would have p-torsion, but $R \xrightarrow{\times p} R$ is injective since R is W-flat and $W \overset{\times p}{\hookrightarrow} W$ is injective

- *If x is not supersingular, then x is a smooth point with $R \simeq W[\![x]\!]$.*
- *If x is supersingular, but $j \neq 0, 1728$, then x is a regular point with $R \simeq W[\![x,y]\!]/(xy-p)$*
- *If x is supersingular and $j = 1728$, then $R = W[\![x,y]\!]/(xy-p^2)$*
- *If x is supersingular and $j = 0$, then $R = W[\![x,y]\!]/(xy-p^3)$*

Remark 19.11. The cusps are smooth points of $X_0(p)$ ∘

These singularities are relatively mild, and can be resolved by a few blow-ups. The result is that you add a $\mathbb{P}^1$ at $j(x) = 1728$ if x is supersingular and a chain of two $\mathbb{P}^1$'s at $j(x) = 0$ if x is supersingular.

Remark 19.12. Andrew drew a picture at this point, but I'm too lazy to add a copy to these notes, so go watch the video. ∘

Proposition 19.13. *Let's say C is a curve over an algebraically closed field k. Assume*

I'm tempted to say this or something like this is proven in Liu's book

(1) *C is reduced*

(2) *all irreducible components of C are $\mathbb{P}^1$'s*

(3) *All singularities of C are simple nodes.*

Then, $\mathrm{Pic}^0_{X/k}$ is a torus

Proof Sketch. If you have a line bundle on C, you can restrict to each irreducible component. On each component (a $\mathbb{P}^1$), the line bundle looks like $\mathscr{O}(n)$. So we have an integer parameter for each irreducible component, and at the points where they meet, you have to specify an element of $\mathbb{G}_m$ identifying the two fibers.

Combinatorially, introduce the graph Γ of C whose vertices are the irreducible components and whose edges are the singular points (places where components meet). A line bundle on C gives an element of $\mathbb{Z}^{V(\Gamma)} \times \mathbb{G}_m^{E(\Gamma)}$. Conversely, an element of this will come from some line bundle. Thus, Pic^0 is a quotient of this, and so a torus.

One can say more, The map $\mathbb{Z}^{V(\Gamma)} \times \mathbb{G}_m^{E(\Gamma)} \to \mathrm{Pic}_{X/k}$ is not injective. To get the trivial bundle, it better be trivial on each component, so the integer parts have to be 0. To get a nonzero section of the associated line bundle, you need to assign a number (i.e. section of the trivial bundle) to each component in a way that respects the gluing. Pictorially, you we have a graph Γ with numbers (the $\mathbb{G}_m$ stuff) on the edges, and it represents a trivial line bundle if you can put numbers on the vertices so that each edge is the ratio of its vertices. Thinking in terms of simplicial cohomology, one can conclude that $\mathrm{Pic}^0_{X/k} = \mathrm{H}^1(\Gamma, \mathbb{G}_m)$ is a torus with character lattice $\mathrm{H}_1(\Gamma, \mathbb{Z})$. ■

This finishes the proof of

Theorem 19.14. *$J_0(N)$ has completely toric reduction at N.*

Recall 19.15 (the proof strategy)**.** The proof strategy was

- Show the minimal regular model of $X_0(N)$ has special fiber with $\mathbb{P}^1$'s glued at nodes
- A computation showed that Pic^0 is a torus
- Theorem of Raynaud implies that Pic^0 is the identity component of the special fiber of the Néron model ⊙

19.2 Fact from last time

We used this fact from last time, but didn't give a complete proof, so let's remedy that.

Theorem 19.16. *Let $K/\mathbb{Q}_p$ be a finite extension with $e < p-1$. Let $\mathscr{O} = \mathscr{O}_K$ with residue field $k = \mathscr{O}/\mathfrak{m}$. Let A be an abelian variety over K with Néron model $\mathcal{A}/\mathscr{O}$. Then,*

$$A(K)_{tors} = \mathcal{A}(\mathscr{O})_{tors} \longrightarrow \mathcal{A}(k)$$

is injective.

Proof. Let $G_0 = A(K)_{tors} \subset A$ a closed subgroup. Let G be its scheme theoretic closure in $\mathcal{A}$, so G is flat and quasi-finite. Using the Néron mapping property and the valuative criterion of properness, one can check that G is finite over $\mathscr{O}$. Now, G is a prolongation of G_0, but G_0 is a constant group scheme, so it has another prolongation: the constant one. Thus, G must be constant by Raynaud, so $G(\mathscr{O}) \hookrightarrow G(k)$ is injective (in fact, an isomorphism) since G is constant. ■

20 Lecture 20: Proof of Mazur's theorem (part 1)

In this lecture and next, we'll prove the following theorem.

Theorem 20.1 (Mazur)**.** *Let $N > 7$ be a prime $\neq 13$. Then, no elliptic curve over $\mathbb{Q}$ has a rational N-torsion point.*

The statement also holds for $N = 13$, but the proof in that case will be different (we'll see it in a couple lectures).

Recall 20.2 (Theorem 18.2)**.** It is enough to find a quotient A of $J_0(N)$ s.t. $A(\mathbb{Q})$ has rank 0 and $0 \neq \infty$ in A. Furthermore, if the J-H constituents of $A[p](\overline{\mathbb{Q}})$ are trivial and cyclotomic, then $A(\mathbb{Q})$ has rank 0. ⊙

Question 20.3. *Why exclude 13?*

Answer. $g(X_0(13)) = 0$, so its Jacobian is trivial. Recall

$$g(X_0(N)) = \left\lfloor \frac{N}{12} \right\rfloor + \begin{cases} 1 & \text{if } N \equiv -1 \pmod{12} \\ -1 & \text{if } N \equiv 1 \pmod{12} \end{cases}$$ ⋆

Assumption. For this lecture and next, N will be a prime greater than 7 and not equal to 13.

Proposition 20.4. $[0] - [\infty]$ *is a non-trivial torsion point of $J_0(N)$ of order dividing $N-1$*

Proof. The map $X_0(N) \to J_0(N)$, $x \mapsto [x] - [\infty]$ is injective. Indeed, if $[x] - [\infty] = 0 \in J_0(N)$, then $[x] - [\infty] = \operatorname{div}(f)$ for some $f : X_0(N) \to \mathbb{P}^1$, but this f would have to be degree 1 and so force $g(X_0(N)) = 0$, a contradiction. This gives non-triviality.

To see that it's torsion, recall the modular form $\Delta(z) = 4E_4^3 + 27E_6^2$, the unique cusp form of weight 12 for $\Gamma(1)$ (up to scaling). It has the property that $\Delta(z) \neq 0$ for $z \in \mathfrak{H}$ (e.g. since it's the discriminant of the corresponding elliptic curve), and that $\Delta(z) = q + \ldots$, so it vanishes to order 1 at ∞. Hence,

$\Delta(Nz)$ is a weight 12 modular form for $\Gamma_0(N)$ which also doesn't vanish on the upper half place. Now, $\Delta(z)/\Delta(Nz)$ is a $\Gamma_0(N)$-invariant function on $\mathfrak{H}$, so it descends to a meromorphic function on $X_0(N)$. Since $\Delta(z) \neq 0$ for $z \in \mathfrak{H}$, f is holomorphic and non-vanishing on $Y_0(N)$, i.e. its divisor is supported at the cusps. Looking at q-expansions, we have

$$\Delta(Nz) = q^N + \cdots \implies \frac{\Delta(z)}{\Delta(Nz)} = q^{-(N-1)} + \ldots,$$

so f must have a pole of order $(N-1)$ at $\infty \in X_0(N)$. Since $\deg \operatorname{div}(f) = 0$, we conclude that $\operatorname{div}(f) = (N-1)[0] - (N-1)[\infty]$ so $[0] - [\infty] \in J_0(N)[N-1]$. ■

Remark 20.5. Ogg showed that the order of $[0] - [\infty]$ is exactly $(N-1)/\gcd(N-1, 12)$ ∘

Remark 20.6. Mazur showed that $[0] - [\infty]$ generates the entire torsion subgroup of $J_0(N)(\mathbb{Q})$ ∘

Recall 20.7. If $\ell \neq N$ is prime, get Hecke operator T_ℓ acting on many sorts of things, including $J_0(N)$. ⊙

Proposition 20.8. $T_\ell([0] - [\infty]) = (\ell + 1)([0] - [\infty])$.

Proof sketch. Let $f, g : X_0(N\ell) \rightrightarrows X_0(N)$ be the Hecke correspondence. The space $X_0(N\ell)$ has 4 cusps, and we can identify

$$\operatorname{cusps}(X_0(N\ell)) = \operatorname{cusps}(X_0(N)) \times \operatorname{cusps}(X_0(\ell)).$$

Hence, we will denote a cups on $X_0(N\ell)$ as (x, y) with $x, y \in \{0, \infty\}$ (and x corresponding to the $X_0(N)$ part). Note that f is induced by the identity map $\mathfrak{H} \to \mathfrak{H}$, so $f(x, y) = x$. g is induced by the multiplication map $\ell : \mathfrak{H} \to \mathfrak{H}$, so also $g(x, y) = x$. The ramification index of f at $(*, 0)$ is ℓ and at $(*, \infty)$ is 1. Now, if $x \in \{0, \infty\}$ is a cusp on $X_0(N)$, then

$$f^*([x]) = \ell[(x, 0)] + [(x, \infty)] \implies g_* f^*([x]) = (\ell + 1)[x].$$ ■

Definition 20.9. We'll say an abelian variety $A/\mathbb{Q}$ satisfies **condition** JH(p) if the J-H constituents of $A[p](\overline{\mathbb{Q}})$ are trivial and cyclotomic. ◇

(Equivalently, the semisimplified reduction of $V_p(A)$ is a sum of trivials and cyclotomics, so JH(p) is an isogeny invariant condition)

20.1 Special Case

Recall 20.10. $J_0(N) = \prod A_f$ (up to isogeny) with product over Galois orbits of normalized eigenforms $f \in S_2(N)$ ⊙

Assumption. For most of today, let's assume all the f's have coefficients in $\mathbb{Q}$, so each 'Galois orbit' above is a singleton, and each A_f is an elliptic curve.

(We'll deal with the general case next lecture)

We want a quotient of $J_0(N)$ satisfying JH(p). There's a best choice (since we want to keep the cusps distinct): take A to be the product of all A_f's that satisfy JH(p) (up to isogeny). Let's be a little more careful, so we know A on the nose and not just up to isogeny.

For an eigenform $f \in S_2(N)$, let

$$\mathfrak{p}_f := \ker\left(\mathbb{T} \xrightarrow{T_\ell \mapsto a_\ell(f)} \mathbb{Z}\right).$$

Recall 20.11. $A_f = J_0(N)/\mathfrak{p}_f J_0(N)$ ⊙

Let $S = \{f \mid A_f \text{ satisfies JH}(p)\}$ and let $I := \bigcap_{f\in S} \mathfrak{p}_f$. Finally, set

$$A := J_0(N)/IJ_0(N).$$

Up to isogeny, we have $A = \prod_{f\in S} A_f$, so A satisfies JH(p). Thus,

Proposition 20.12. *$A(\mathbb{Q})$ has rank 0.*

Question 20.13. *How do we know that $A \neq 0$?*

Answer. Let p be a prime dividing the order of $[0]-[\infty]$ (so $p \mid N-1 \implies p \neq N$). Then, $J_0(N)(\mathbb{Q})$ has a p-torsion point, so $J_0(N)[p]$ must have a copy of the trivial representation in it. This copy must come from some $A_f[p]$ for some $f \in S_2(N)$. Since A_f is an elliptic curve, the Weil paring then implies that A_f satisfies JH(p),[32] so $f \in S$. ⋆

Lemma 20.14. *We have $f \in S \iff a_\ell(f) = \ell + 1 \mod p$ for all $\ell \neq N$*

Proof. Suppose $f \in S$. Then, $A_f[p]$ is $\texttt{triv} \oplus \texttt{cyc}$ (up to semisimplification). Thus, $a_\ell(f) = \mathrm{Tr}(F_\ell \mid A_f[p]) = \ell + 1 \mod p$. Conversely, if $a_\ell(f) = \ell + 1 \mod p$ for all ℓ, then the character of $A_f[p]$ is the character of $\texttt{triv} \oplus \texttt{cyc}$, so they must be the same up to semisimplification by group theory. ■

Definition 20.15. The **p-Eisenstein ideal** is the ideal $\mathfrak{a}$ of $\mathbb{T}$ generated by p and $T_\ell - (\ell+1)$ for all $\ell \neq N$. ◇

Lemma 20.16. *$\mathbb{T}_\ell/\mathfrak{a} = \mathbb{F}_p$, so $\mathfrak{a}$ is a maximal ideal.*

Proof. Take any $f \in S$. The homomorphism $\mathbb{T} \to \mathbb{T}/\mathfrak{p}_f \cong \mathbb{Z}$ takes $T_\ell \mapsto a_\ell(f)$. Hence, $T_\ell - (\ell+1) \mapsto a_\ell(f) - (\ell+1) \in (p)$, so the image of $\mathfrak{a}$ under this map is not (1), so $\mathfrak{a} \neq (1)$. Now, the quotient must be $\mathbb{F}_p$ since every T_ℓ becomes an integer (i.e. becomes $\ell+1$), and we've killed p. ■

Lemma 20.17. *$f \in S \iff$ the image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{p}_f$ is not (1) $\iff \mathfrak{p}_f \subset \mathfrak{a}$*

Proof. The image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{p}_f = \mathbb{Z}$ is the ideal generated by $a_\ell(f) - (\ell+1)$ and p, which is not the unit ideal iff $a_\ell(f) \equiv (\ell+1) \mod p$ for all p, i.e iff $f \in S$. Since $\mathfrak{a}$ is maximal, we get the last equivalence in the claim. ■

Now we can characterize our ideal I w/o reference to modular forms.

Proposition 20.18.

$$I = \bigcap_{\substack{\mathfrak{p}\subset\mathfrak{a} \\ \mathfrak{p} \text{ minimal prime}}} \mathfrak{p}$$

Proof. By definition $I = \bigcap_{f \in S} \mathfrak{p}_f$. The minimal primes of $\mathbb{T}$ are just the $\mathfrak{p}_f$'s. Finally, $\mathfrak{p}_f \subset \mathfrak{a} \iff f \in S$. ■

Question: Why?

Lemma 20.19. *The localization $I_\mathfrak{a} = 0$.*

This is because $I_\mathfrak{a}$ is the intersection of the minimal primes of $\mathbb{T}_\mathfrak{a}$, i.e. is the nilradical of $\mathbb{T}_\mathfrak{a}$, but $\mathbb{T}_\mathfrak{a}$ is reduced since $\mathbb{T}$ is.

Suppose X is a $\mathbb{T}$-module and every element is killed by a power of p. Then, the action of $\mathbb{T}$ extends to an action of its p-adic completion

$$\widehat{\mathbb{T}}_p := \varprojlim \mathbb{T}/p^n\mathbb{T}.$$

This is a complete semi-local ring, so it's the product of its localizations at maximal ideals. In particlular, $\widehat{\mathbb{T}}_\mathfrak{a} := \varprojlim \mathbb{T}/\mathfrak{a}^n$ is a direct factor of $\widehat{\mathbb{T}}_p$. Thus, $X = X_\mathfrak{a} \oplus X'$ where X' is killed by $\widehat{\mathbb{T}}_\mathfrak{a}$. Note

$$X_\mathfrak{a} = X[\mathfrak{a}^\infty] = \bigcup_{n \geq 1} X[\mathfrak{a}^n].$$

Lemma 20.20. $J_0(N)[\mathfrak{a}^\infty] \xrightarrow{\sim} A[\mathfrak{a}^\infty]$

Proof. Let $X = J_0(N)[p^\infty]$ and $Y = A[p^\infty]$, so we have a surjection $X \to Y$. The kernel of this map is $X \cap IJ_0(N) = IX$. To see this last equality, pick generators $T_1, \ldots, T_n$ of I and consider the map

$$\begin{array}{ccc} J_0(N)^n & \longrightarrow & J^0(N) \\ (X_1, \ldots, X_n) & \longmapsto & \sum T_i X_i. \end{array}$$

The image of this map is $IJ_0(N)$; since this is a map of abelian varieties, it induces a surjection on p-power torsion points. This exactly says that $X \cap IJ_0(N) = IX$. This gives an exact sequence

$$0 \longrightarrow IX \longrightarrow X \longrightarrow Y \longrightarrow 0.$$

Localize at $\mathfrak{a}$ (and note $(IX)_\mathfrak{a} = I_\mathfrak{a} X_\mathfrak{a} = 0$), to conclude that $X_\mathfrak{a} \xrightarrow{\sim} Y_\mathfrak{a}$. ■

Corollary 20.21. $[0] - [\infty] \neq 0$ *in* A.

Proof. Say $P = [0] - [\infty] \in J_0(N)$, and let Q be any nonzero p-torsion multiple of P. Since $T_\ell P = (\ell+1)P$, the same is true for Q, so $Q \in J_0(N)[\mathfrak{a}]$. The previous lemma then implies that the image of Q in A is nonzero, so $P \neq 0$ in A as well. ■

Remark 20.22. $\mathbb{T} \otimes \mathbb{Q} = \mathbb{Q} \times \mathbb{Q} \times \ldots \times \mathbb{Q}$, one fact for each eigenform f_i. Furthermore, $T \subset \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$. Explicitly, $\mathbb{T}$ is the subring of $\mathbb{Q}^n$ generated by tuples $(a_\ell(f_1), \ldots, a_\ell(f_n))$.

If there are congruences between the f_i's, then $\mathbb{T} \subsetneq \mathbb{Z}^n$. ∘

TODO: Add in picture of Spec $\mathbb{T}$ from lecture

20.2 General Case

In general, $V_p(J_0(N)) = \prod V_{f,\lambda}$ with product over pairs (f, λ) where $f \in S_2(N)$ is a normalized eigenform, and λ is a prime of the coefficient field K_f of f, above p. The ideal situation would be to take A to be

[32] $V_\ell(A_f)$ looks like $\begin{pmatrix} 1 & * \\ & \chi \end{pmatrix}$

the quotient of $J_0(N)$ s.t. V_pA is the product of those $V_{f,\lambda}$ whose semi-simple reduction is sums of trivial and cyclotomic.

Warning 20.23. This does not work. It's possible, for example that $J_0(N)$ is a simple abelian variety (e.g. all normalized eigenforms are Galois conjugate). •

I didn't really follow Andrew's description of the idea, but details in-coming next time...

Sounds like we're getting started this time. Choose p dividing the order of $[0]-[\infty]$ in $J_0(N)$. Let $\mathfrak{a} \subset \mathbb{T}$ be the ideal generated by p and $T_\ell - (\ell+1)$ for all $\ell \neq N$ as before.

Lemma 20.24. *$\mathbb{T}/\mathfrak{a} = \mathbb{F}_p$, so $\mathfrak{a}$ is maximal.*

Proof. $J_0(N)[p]$ contains copy of trivial representation, so semi-simplified reduction of some $V_{f,\lambda}$ must be triv plus cyclotomic. Hence, $a_\ell(f) = \ell + 1 \mod \lambda$, so image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{P}_f$ will be contained in λ. ■

Define

$$I = \bigcap_{\mathfrak{p}\subset\mathfrak{a} \text{ minimal prime}} \mathfrak{a} \text{ and } A := J_0(N)/IJ_0(N).$$

Proposition 20.25. *$0 \neq \infty$ in A*

(Same proof as before)

We just need $\operatorname{rank} A(\mathbb{Q}) = 0$. We will do this next time, essentially by mimicking the proof of Theorem 11.1 from before.

21 Lecture 21: Proof of Mazur's Theorem (part 2)

Last time we started proving Mazur's Theorem 20.1.

Theorem 21.1 (Theorem 20.1)**.** *Let $N > 7, \neq 13$ be prime. No elliptic curve over $\mathbb{Q}$ has a rational point of order N.*

Recall 21.2.

- We picked a prime p dividing the order of $[0]-[\infty] \in J_0(N)(\mathbb{Q})$ (so $p \mid (N-1)$).
- We defined the p-Eisenstein ideal $\mathfrak{a} \subset \mathbb{T}$, generated by p and $T_\ell - (\ell+1)$ for all $\ell \neq N$
- We set
$$I := \bigcap_{\substack{\text{minimal prime } \mathfrak{p}\subset\mathbb{T} \\ \mathfrak{p}\subset\mathfrak{a}}} \mathfrak{p} \text{ and } A := J_0(N)/IJ_0(N).$$
- To prove Theorem 21.1, it suffices to show that $\operatorname{rank} A(\mathbb{Q}) = 0$.
- Last time we treated the case where all the eigenforms of level N have $\mathbb{Q}$-coefficients. In that case, this A satisfies the JH(p) condition and we could apply Theorem 11.1. ⊙

Today we handle the general case. Theorem 11.1 won't apply, but it's proof will basically go through in the current situation. We'll show that $A(\mathbb{Q})_\mathfrak{a}$ is finite, and then an easy commutative algebra argument will show that $A(\mathbb{Q})$ is finite.

Let's recall the strategy of the proof of Theorem 11.1.

Recall 21.3. A group scheme over $\mathbb{Z}$ or $\mathbb{Z}[1/N]$ is *admissible* if

(1) It is finite + flat away from N;

(2) It is q.finite + étale away from p;

(3) There exists a filtration (over $\mathbb{Z}[1/N]$) with quotients all either $\mathbb{Z}/p\mathbb{Z}$ or μ_p

(plus some technical hypotheses) ⊙

Recall 21.4 (Proposition 11.7)**.** If $G/\mathbb{Z}$ satisfies **(1)** +**(2)** and JH(p), then it's admissible ⊙

Recall 21.5. Let $G/\mathbb{Z}$ be admissible. We defined

- $\ell(G) = \log_p(\#G)$
- $\delta(G) = \ell(G_{\mathbb{Q}}) - \ell(G_{\mathbb{F}_N})$
- $\alpha(G) = \#$ of $\mathbb{Z}/p\mathbb{Z}$'s in filtration for G (over $\mathbb{Z}[1/N]$)
- $h^i(G) = \log_p\left(\#\,\mathrm{H}^i_{\mathrm{fppf}}(\operatorname{Spec}\mathbb{Z}, G)\right)$

We proved (Proposition 11.14)

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G).$$ ⊙

Recall 21.6 (Proof Sketch of Theorem 11.1)**.** We start with an abelian variety $A/\mathbb{Q}$ with

- good reduction away from N
- completely toric reduction at N
- $A[p]$ satisfying JH(p)

Let $\mathcal{A}/\mathbb{Z}$ be the Néron model of A. Then, $\mathcal{A}[p]$ is admissible, and so $\mathcal{A}[p^n]$ is admissible for all n. We then showed that $\delta(\mathcal{A}[p^n]) \approx \alpha(\mathcal{A}[p^n])$ so the difference $h^1(\mathcal{A}[p^n]) - h^0(\mathcal{A}[p^n])$ is bounded as $n \to \infty$. The term $h^0(\mathcal{A}[p^n])$ is itself bounded (since it's $A(\mathbb{Q})[p^n]$) and so the h^1 term is itself bounded. Now, we basically (not literally) have an injection $A(\mathbb{Q}) \hookrightarrow \varprojlim \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}[p^n])$ with the RHS finite. ⊙

We want to carry out the same idea in the present setting. We'll have that $\mathcal{A}[p^n]$ localized at $\mathfrak{a}$ is admissible, and then be able to bound $\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}[\mathfrak{a}^n])$ and conclude that some $\mathfrak{a}$-part of $A^1(\mathbb{Q})$ is finite.

TODO: Make sure this is the right expression

21.1 Proving $A(\mathbb{Q})$ has rank 0

Notation 21.7. We take $N, p, \mathfrak{a}, I$ and A all as in Recall 21.2. We write d for the $\mathbb{Z}_p$-rank of $\widehat{\mathbb{T}}_{\mathfrak{a}}$, and we let e be the idempotent of $\widehat{\mathbb{T}}_p$ which projects onto $\widetilde{\mathbb{T}}_{\mathfrak{a}}$. Let let $\mathcal{A}/\mathbb{Z}$ be the Néron model of A

Proposition 21.8. *$\mathcal{A}[p^n]_{\mathfrak{a}}$ is admissible*

(This is the image of e applied to $\mathcal{A}[p^n]$)
It is enough to show that $A[p^n]_{\mathfrak{a}}$ satisfies JH(p) (by Proposition 11.7).

Lemma 21.9. *$A[p^n]_{\mathfrak{a}}$ satisfies* JH(p)

Proof. We have $A[p^n]_{\mathfrak{a}} \subset A[\mathfrak{a}^m]$ for some m. The exact sequences (below, k is the number of generators for $\mathfrak{a}$)

$$0 \longrightarrow A[\mathfrak{a}] \longrightarrow A[\mathfrak{a}^m] \longrightarrow A[\mathfrak{a}^{m-1}]^{\oplus k}$$

reduces us to the case of showing that $V := A[\mathfrak{a}](\overline{\mathbb{Q}})$ satisfies JH(p).

We know T_ℓ acts on V by $\ell+1$. By Eichler-Shimura (Theorem 17.2) we know Frobenius at $\ell \neq p, N$ satisfies

$$0 = F_\ell^2 - (\ell+1)F_\ell + \ell = (T-\ell)(T-1)$$

on V. Hence, the only generalized eigenvalues of F_ℓ on V are $1, \ell$. This suffices to prove what we want (by the below lemma). ∎

Lemma 21.10. *Let V be an $\mathbb{F}_p$-representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ s.t. the generalized eigenvalues of F_ℓ are 1 and ℓ for almost every prime ℓ. Then, the only constituents of V are* `triv`, `cyc`.

Proof. Let $W = V \oplus V^\vee(1)$ (twisting by 1 is tensoring with `cyc`). If m is the matrix of Frobenius F_ℓ on V, then the matrix of $F_\ell \curvearrowright V^\vee(1)$ is $\ell\,(m^t)^{-1}$. Consider the Jordan normal form of this (say, after passing to $\overline{\mathbb{F}}_p$) matrix: for m, you get a bunch of 1's and ℓ's on the diagonal; for $(m^t)^{-1}$ you get a bunch of 1's and (ℓ^{-1})'s; for $\ell\,(m^t)^{-1}$, all the 1's have changed to ℓ's and all the (ℓ^{-1})'s have changed to 1's. Hence,

$$\dim(V_1) = \dim(V^\vee(1)_\ell) \text{ and } \dim(V_\ell) = \dim(V^\vee(1)_1)$$

where $blah_\lambda$ is the λ-generalized eigenspace of F_ℓ on $blah$. Thus,

$$\dim(W_1) = \dim(V_1) + \dim(V^\vee(1)_1) = \dim(V_1) + \dim(V_\ell) = \dim(V)$$

and similarly $\dim(W_\ell) = \dim(V)$. In other words, the character of W is the character of $\mathtt{triv}^{\oplus \dim(V)} \oplus \mathtt{cyc}^{\oplus \dim(V)}$, so we must have $W^{ss} = \mathtt{triv}^{\oplus \dim(V)} \oplus \mathtt{cyc}^{\oplus \dim(V)}$. ∎

This proves that $\mathcal{A}[p^n]_{\mathfrak{a}}$ is admissible. Let's now compute α of it.

Lemma 21.11. *Let $G/\mathbb{Q}$ be a p-divisible group w/ action of $\widehat{\mathbb{T}}_{\mathfrak{a}}$ whose rational Tate module $V_p(G)$ is free of rank 2 over $\widehat{\mathbb{T}}_{\mathfrak{a}}[1/p]$. Then,*

$$\ell(G[p^n]) = 2nd + O(1) \text{ where } d = \mathrm{rank}_{\mathbb{Z}_p} \widehat{\mathbb{T}}_a.$$

Proof. Let $T = T_p(G)$ be the integral Tate module of G, so $\ell(G[p^n]) = \mathrm{length}(T/p^nT)$. Since $V_p(G)$ is free of rank 2, there's some finite index $T' \subset T$ which is free of rank 2 over $\widehat{\mathbb{T}}_{\mathfrak{a}}$, so

$$2nd + O(1) = \mathrm{length}(T'/p^nT') + O(1) = \mathrm{length}(T/p^nT)$$

(the $O(1)$'s in the first equality are the same). ∎

Corollary 21.12. $\alpha(\mathcal{A}[p^n]_{\mathfrak{a}}) = nd + O(1)$

Proof. To keep things simple, assume $p \neq 2$, so α is the # of $\mathbb{Z}/p\mathbb{Z}$'s in the Galois representation of $A[p^n]_{\mathfrak{a}}$. Recall the action of T_ℓ on $J_0(N)[p^n]$ is self-adjoint w.r.t the Weil paring, and so the same is true of any element of $\widehat{\mathbb{T}}_p$. Let e be the idempotent in $\widehat{\mathbb{T}}_p$ which projects onto $\widehat{\mathbb{T}}_{\mathfrak{a}}$. This is a self-adjoint

This was briefly mentioned at the start of the proof of Proposition 17.9

idempotent, and so it must be the case that $eJ_0(N)[p^n]$ and $(1-e)J_0(N)[p^n]$ are orthogonal under the Weil pairing. Since the Weil pairing is perfect, it must restrict to a perfect pairing on $eJ_0(N)[p^n]$. Last time (Lemma 20.20), we showed that

$$eJ_0(N)[p^\infty] \xrightarrow{\sim} eA[p^\infty].$$

Thus, we conclude that $A[p^n]_{\mathfrak{a}}$ is self-Cartier-dual. Since it's admissible, it must have equal numbers of $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's in it, so

$$\alpha(\mathcal{A}[p^n]_{\mathfrak{a}}) = \frac{1}{2}\ell(A[p^n]_{\mathfrak{a}}) = nd + O(1)$$

by the previous lemma applied to $G = A[p^\infty]_{\mathfrak{a}}$ (so $G[p^n] = A[p^n]_{\mathfrak{a}}$).[33] ■

Now we compute δ.

Lemma 21.13. *Say we have a p-divisible group $G/\mathbb{Q}_N$. Let $V = V_p(G)$ be its rational Tate module, and let $\mathcal{G}_n$ be the maximal q.finite étale extension of $G[p^n]$ over $\mathbb{Z}_N$. Then,*

See Remark 9.5

$$\delta(\mathcal{G}_n) = (\dim V - \dim V^I)n + O(1)$$

where $I \subset \mathrm{Gal}(\overline{\mathbb{Q}}_N/\mathbb{Q}_N)$ is the inertia subgroup.

Proof. Let $T = T_p(G)$ be the integral Tate module, so

$$\ell((\mathcal{G}_n)_{\mathbb{Q}_N}) = \mathrm{len}(T/p^nT) = n\dim(V).$$

Over the special fiber,

$$\mathcal{G}_n(\overline{\mathbb{F}}_N) = \mathcal{G}_n(\overline{\mathbb{Q}}_N)^I = (T/p^nT)^I$$

by definition of this maximal q.fin étale extension. Hence, $\ell((\mathcal{G}_n)_{\mathbb{F}_N}) = \mathrm{len}((T/p^nT)^I)$. Now consider the exact sequence

$$0 \longrightarrow T \xrightarrow{p^n} T \longrightarrow T/p^nT \longrightarrow 0.$$

Taking inertia invariants gives

$$0 \longrightarrow T^I/p^nT^I \longrightarrow (T/p^nT)^I \longrightarrow \mathrm{H}^1(I,T)[p^n] \longrightarrow 0.$$

The H^1 term above is a f.g. $\mathbb{Z}_p$-module and so its p^n-torsion is bounded. Thus,

$$\mathrm{len}((T/p^nT)^I) = \mathrm{len}(T^I/p^nT^I) + \mathrm{len}(\mathrm{H}^1(I,T)[p^n]) = n\dim(V^I) + O(1)$$

as desired. ■

We're now interested in understanding inertia invariants.

Lemma 21.14. *Say $B/\mathbb{Q}_N$ is an abelian variety with Néron model $\mathcal{B}/\mathbb{Z}_N$. Then,*

$$V_p(\mathcal{B}_{\mathbb{F}_N}) = V_p(B)^I.$$

[33] Note $V_p(G) = V_p(J_0(N))_{\mathfrak{a}}$ is free of rank 2 over $\widehat{\mathbb{T}}_{\mathfrak{a}}$

Proof. $\mathcal{B}[p^n]$ is an étale group scheme over $\mathbb{Z}_N$, so every $\overline{\mathbb{F}}_N$ points lifts to a $\mathbb{Z}_N^{un}$-point. The Néron mapping property implies that every $\mathbb{Q}_N^{un}$ point of B extends to a $\mathbb{Z}_N^{un}$-point, so

$$\mathcal{B}[p^n](\overline{\mathbb{F}}_N) = B[p^n](\mathbb{Q}_N^{un}) = B[p^n](\overline{\mathbb{Q}}_N)^I,$$

and we take the inverse limit over N. ∎

Lemma 21.15. *Let $B/\mathbb{Q}_N$ be an abelian variety with completely toric reduction. Let U be a summand of the rational Tate module $V = V_p(B)$. Then,*

$$\dim(U^I) = \frac{1}{2}\dim(U).$$

Proof. Note $\dim(V) = 2\dim(B)$. By the previous lemma, $V^I = V_p(\mathcal{B}_{\mathbb{F}_N})$. The identity component of $\mathcal{B}_{\mathbb{F}_N}$ is a torus, by assumption, so $\dim V_I = \dim \mathcal{B}_{\mathbb{F}_N} = \dim B$ (Tate module of a torus). This proves the lemma for V.

In general, note that B has semistable reduction, so Grothendieck's extension of Néron-Ogg-Shafarevich (Theorem 9.16) implies that I acts unipotently on V. In fact, there's a stronger result: for any $g \in I$, $(g-1)^2 = 0$ on V. Thus, if $U \subset V$ is any Galois-stable submodule (not necessarily a summand), then $(g-1)^2 U = 0$ for all $g \in I$, so $\dim(U^g) \geq \frac{1}{2}\dim(U)$. We'd like to extend this from a single element to the whole group. The image of I is a pro-p group[34]. The wild part is pro-N, so I^w must act trivially. Then, the action of inertia factors through the tame quotient $I^t = I/I^w$, a pro-cyclic group. If $g \in I^t$ is a generator, then $U^I = U^g$, so we conclude $\dim(U^I) \geq \frac{1}{2}\dim(U)$.

Now, if $V = U_1 \oplus U_2$, then we must have

$$\dim(V^I) = \frac{1}{2}\dim(V) \text{ and } \dim(U_i^I) \geq \frac{1}{2}\dim(U_i) \text{ for } i = 1, 2.$$

Since $V^I = U_1^I \oplus U_2^I$, the inequalities above must be equalities. ∎

Remark 21.16. If $B = J_0(N)$ (or a quotient of it), then we know $V_p(B) = \bigoplus V_{f,\lambda}$ with each piece a 2-dimensional vector space. Since $g \in I$ acts unipotently, we must have $(g-1)^2 = 0$ on each (2-dimensional) piece, so we easily get this stronger fact for the cases we care about. ∘

Remark 21.17. This lemma shows that inertia at N acts unipotently and non-trivially on $V_{f,\lambda}$. This is an instance of local-global compatibility in the Langlands program. ∘

Andrew said more about this, but I'd be lying if I said I followed completely

Proposition 21.18. $\delta(\mathcal{A}[p^n]_{\mathfrak{a}}) = nd + O(1)$

Proof. We first set up some notation. Let $\mathcal{G} = \mathcal{A}[p^\infty]$ and $\mathcal{G}_{\mathfrak{a}} = e\mathcal{G}$. Let $V = V_p(\mathcal{G}_{\mathbb{Q}})$ and $V_{\mathfrak{a}} = eV = V_p((\mathcal{A}_{\mathfrak{a}})_{\mathbb{Q}})$. Note that $\mathcal{G}[p^n]$ is the maximal étale q.finite extension of its generic fiber (e.g. by the Néron mapping property), so (Lemma 21.13)

$$\delta(\mathcal{G}[p^n]) = (\dim V - \dim V^I)n + O(1).$$

[34] V is a $\mathbb{Q}_p$-vector space and I is acting via the group of unipotent matrices. This group has a filtration whose successive quotients are $\mathbb{Q}_p$'s

This property passes to summands, so also

$$\delta(\mathcal{G}_{\mathfrak{a}}[p^n]) = (\dim V_{\mathfrak{a}} - \dim V_{\mathfrak{a}}^I)n + O(1).$$

Now, $V_{\mathfrak{a}}$ is a summand of $V_p(A)$ (or even $V_p(J_0(N))$) and A has completely toric reduction at N, so (Lemma 21.15) $\dim V_{\mathfrak{a}}^I = \frac{1}{2}\dim V_{\mathfrak{a}}$. Thus,

$$\delta(\mathcal{G}_{\mathfrak{a}}[p^n]) = \frac{1}{2}\dim(V_{\mathfrak{a}})n + O(1) = dn + O(1)$$

since $V_{\mathfrak{a}}$ is free of rank 2 over $\widehat{\mathbb{T}}_{\mathfrak{a}}$ ($\implies \dim(V_{\mathfrak{a}}) = 2d$). Finally, note that $\mathcal{G}_{\mathfrak{a}}[p^n] = \mathcal{A}[p^n]_{\mathfrak{a}}$. ■

Proposition 21.19. *$\widehat{\mathbb{T}}_{\mathfrak{a}} \otimes_{\mathbb{T}} A(\mathbb{Q})$ is finite.*

Proof. Let $\mathcal{A}^0/\mathbb{Z}$ be the identity component of the Néron model. Let $\mathcal{G}_n := \mathcal{A}^0[p^n]_{\mathfrak{a}}$. Note that α only depends on the special fiber at p (and $\mathcal{A} = \mathcal{A}^0$ away from N), so

$$\alpha(\mathcal{G}_n) = \alpha(\mathcal{A}[p^n]_{\mathfrak{a}}) = nd + O(1).$$

δ however can change, but only by the order of the component group, so

$$\delta(\mathcal{G}_n) = \delta(\mathcal{A}[p^n]_{\mathfrak{a}}) + O(1) = nd + O(1).$$

This tells us that $h^1(\mathcal{G}_n) - h^0(\mathcal{G}_n) = O(1)$, but

$$\mathrm{H}^0_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{G}_n) \subset \mathcal{A}^0(\mathbb{Z})[p^n] \subset A(\mathbb{Q})[p^n]$$

is bounded, so $h^1(\mathcal{G}_n) = O(1)$ (as $n \to \infty$). Now we do the Kummer sequence thing:

$$0 \longrightarrow \mathcal{A}^0[p^n] \longrightarrow \mathcal{A}^0 \xrightarrow{p^n} \mathcal{A}^0 \longrightarrow 0$$

(exact on the right by completely toric reduction), so we get an injection

$$\mathcal{A}^0(\mathbb{Z}) \otimes \mathbb{Z}/p^n\mathbb{Z} \hookrightarrow \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}^0[p^n]).$$

Taking inverse limits, we get

$$\mathcal{A}^0(\mathbb{Z}) \otimes \mathbb{Z}_p \hookrightarrow \varprojlim \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{A}^0[p^n]).$$

Applying e, we get

$$\mathcal{A}^0(\mathbb{Z}) \otimes_{\mathbb{T}} \widehat{\mathbb{T}}_{\mathfrak{a}} \hookrightarrow \varprojlim \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}, \mathcal{G}_n)$$

(e moves through everything since it's just taking a summand), so $\mathcal{A}^0(\mathbb{Z}) \otimes_{\mathbb{T}} \widehat{\mathbb{T}}_{\mathfrak{a}}$ is finite. We have a finite-index containment

$$\mathcal{A}^0(\mathbb{Z}) \hookrightarrow \mathcal{A}(\mathbb{Z}) = A(\mathbb{Q}),$$

and so we win. ■

We still need to deduce finiteness of $A(\mathbb{Q})$ from this.

Lemma 21.20. *Suppose that $\mathscr{O}$ is an order in a number field K, and let $\mathfrak{a} \subset \mathscr{O}$ be a maximal ideal. Let M be a f.g. $\mathscr{O}$-module s.t. the completion $\widehat{M}_{\mathfrak{a}} = M \otimes_{\mathscr{O}} \widehat{\mathscr{O}}_{\mathfrak{a}}$ is finite. Then, M is finite.*

(Proof: exercise)

Lemma 21.21. *Say M is a f.g. $(\mathbb{T}/I)$-module so that $M \otimes_{\mathbb{T}} \widehat{\mathbb{T}}_{\mathfrak{a}}$ is finite. Then, M is finite.*

Proof. Consider the map

$$\mathbb{T}/I \hookrightarrow \bigoplus_{\substack{\mathfrak{p} \subset \mathfrak{a} \subset \mathbb{T} \\ \mathfrak{p} \text{ minimal}}} \mathbb{T}/\mathfrak{p}$$

which has finite cokernel (iso after tensoring with $\mathbb{Q}$). Tensoring up to M gives

$$M \to \bigoplus_{\mathfrak{p}} M/\mathfrak{p}M$$

with finite kernel and cokernel (sum over same primes as above). Since $M \otimes_{\mathbb{T}} \widehat{\mathbb{T}}_{\mathfrak{a}}$ is finite, same is true for $M/\mathfrak{p}M$, so the previous lemma implies that $M/\mathfrak{p}M$ is finite for all $\mathfrak{p}$ in the sum. This then implies that M is finite. ∎

Corollary 21.22. *$A(\mathbb{Q})$ is finite.*

Last time we showed the two cusps map to different elements in this A, so we may conclude Mazur's theorem.

21.2 What's Left?

We've done all the hard work now, but we haven't done all the work. We need to exclude 13-torsion. We'll do this next time, following a paper of Mazur and Tate. We also have to exclude some composite orders (e.g. there could be 7-torsion, but there shouldn't be any 49-torsion).

22 Lecture 22: 13 torsion

The goal of today is to prove the following theorem

Theorem 22.1 (Mazur-Tate, this paper)**.** *No elliptic curve over $\mathbb{Q}$ has a rational point of order 13.*

(This case was missed by Mazur's method since $g(X_0(13)) = 0$)

Notation 22.2. We let $X = X_1(13)$, $J = \mathrm{Jac}(X)$, both viewed as schemes over $\mathbb{Z}[1/13]$. We let $K = \mathbb{Q}(\zeta_{13})$ (with ζ_{13} a primitive 13th root of unity), and we let K^+ be the maximal real subfield of K. Finally, we let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Note that theorem 22.1 amounts to the statement that the only rational points of X are the cusps.

22.1 Preliminaries on $X_1(13)$

Recall 22.3. $Y_1(13)$ parameterizes pairs (E, P) where E is an elliptic curve and $P \in E[13]$. ⊙

Definition 22.4. We haven't talked about $X_1(13)$ before. This parameterizes pairs (E, P) where E is a generalized elliptic curve, and P is a 13-torsion point s.t. the group generated by P meets each irreducible component of E. ◇

Fact. $g(X_1(13)) = 2$ and $g(X_0(13)) = 0$

If $g(X_1(13)) = 1$, it'd be an elliptic curve, and so there'd be more available methods for getting at its rational points. Since it's higher genus, things are a bit trickier.

Fact. $X_1(13)$ is actually a scheme, not just a stack

Recall 22.5. $X_0(13)$ has two cusps: (1-gon, μ_{13}) and (13-gon, $\mathbb{Z}/13\mathbb{Z}$). ⊙

Over each of these cusps, there are 6 points of $X_1(13)$ because a group of order 13 has 12 generators and because $(E, P) \cong (E, -P)$ (via multiplication by -1). The points over (13-gon, $\mathbb{Z}/13\mathbb{Z}$) are rational (each point is actually a rational point) while the points of (1-gon, μ_{13}) are not rational; you need a root of unity up to $\pm$, so they're defined over K^+. Summarizing

Proposition 22.6. *$X = X_1(13)$ has 12 cusps, $6/\mathbb{Q}$ and $6/K^+$.*

Note that $(\mathbb{Z}/13\mathbb{Z})^\times \curvearrowright X$ by scaling the point, i.e.

$$(\mathbb{Z}/13\mathbb{Z})^\times \ni a : (E, P) \mapsto (E, aP).$$

Since -1 acts trivially, we get an action of $\Gamma = (\mathbb{Z}/13\mathbb{Z})^\times / \{\pm 1\}$. Given $m \in (\mathbb{Z}/13\mathbb{Z})^\times$, we let $\gamma_m \in \Gamma$ denote its image.

Remark 22.7. On $X_0(N)$, there's the Atkin-Lehner involution $(E, G) \rightsquigarrow (E/G, E[N]/G)$. You might get a similar thing on $X_1(N)$, but you run into the issue that $E/\langle P \rangle$ doesn't have a natural choice of N-torsion point. However, if you fix a primitive Nth root of unity, you can take the point which has Weil pairing (with the original point) that root of unity. ◦

Given $\zeta \in \mu_{13}$ primitive and $(E, P) \in X_1(13)$, there's a point $Q \in E[13]$ so that $e_{13}(P, Q) = \zeta$. This Q is unique up to translation by P, so $(E/\langle P \rangle, \text{image of } Q)$ gives a well-defined point of $X_1(13)$.[35] This constructs a map

$$\tau_\zeta : X \to X.$$

Remark 22.8. $\tau_\zeta = \tau_{\zeta^{-1}}$ so τ_ζ makes sense for

$$\zeta \in \Gamma' := \{\text{primitive 13th roots of 1}\} / (\zeta = \zeta^{-1})$$

(Γ' just a set). ◦

We have the relations

- $\gamma_m \tau_\zeta = \tau_{\zeta^m}$
- $\tau_\zeta \gamma_m \tau_{\zeta^{-1}} = \gamma_m^{-1}$
- $\tau_\zeta^2 = 1$

[35] One has to give a different construction at the cusps

Question: Is this defined over $\mathbb{Q}$ or over $\mathbb{Q}(\mu_{13}) = K$?

Answer: It's defined over K^+, see e.g. the discussion in Kubert's paper on 'The method of mazur and tate...'

Staring at this, we see that if $\Delta = \Gamma \cup \Gamma'$, then this is a group which is isomorphic to the dihedral group of order 12. Furthermore, G acts on Δ through its action on μ_{13}, and this action is compatible w/ its action on $X_{\overline{\mathbb{Q}}}$.

22.2 Results of Ogg

Note 2. I think these are from this paper.

Proposition 22.9. *Let P_i $(1 \leq i \leq 6)$ be the rational cusps on X. For $i \neq j$, the point $[P_i] - [P_j] \in J(\mathbb{Q})$ has order 19. Furthermore, all of these generate the same cyclic subgroup of J.*

Proof sketch. For $1 \leq a \leq 6$, define the series

$$E_{2,a} = \sum_{\substack{n \equiv 0 \pmod{13} \\ m \equiv a \pmod{13}}}{}' \frac{1}{(mz+n)^2}.$$

This is a weight 2 Eisenstein series for $\Gamma_1(13)$. They are not modular forms, but the differences $\varphi_{ij} = E_{2,i} - E_{2,j}$ are modular forms of weight 2 for $\Gamma_1(13)$. This allows one to know how many zeros it has, and then to check that all the zeros of φ_{ij} lie on the cusps. Thus, $D_{ij} = \operatorname{div}(\varphi_{ij})$ is some linear combination of cusps (Ogg explicitly computes these), and

$$D_{ij} - D_{kl} = \operatorname{div}\left(\frac{\varphi_{ij}}{\varphi_{k\ell}}\right) = 0 \in J.$$

Since gives a bunch of linear relations on the cusps. Ogg writes them down and fiddles with them to conclude the proposition. ∎

Proposition 22.10. $J(\mathbb{Q})_{tors} = \mathbb{Z}/19\mathbb{Z}$

"The proof of this is pretty cool."

Proof. The only points on $X/\mathbb{F}_4$ are the 6 rational cusps. This is because no elliptic curve over $\mathbb{F}_4$ can have a point of order 13 (by the Hasse bound). This means the only other possible points could be the 6 cusps over K^+, but we know their field of definition and so can see that they are not defined over $\mathbb{F}_4$.[36] So we know $\#X(\mathbb{F}_2) = \#X(\mathbb{F}_4) = 6$. Now, we appeal to the following

Lemma 22.11. *Suppose $X/\mathbb{F}_q$ is a genus 2 curve with Jacobian $J = \operatorname{Jac}(X)$. Then,*

$$\#J(\mathbb{F}_q) = -q + \frac{1}{2}\#X(\mathbb{F}_{q^2}) + \frac{1}{2}\left(\#X(\mathbb{F}_q)\right)^2.$$

Proof idea. Use Lefschetz-fixed point. Let $V = \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ and let F be Frobenius. Then,

$$\#X(\mathbb{F}_q) = 1 + q - \operatorname{Tr}(F|V) \text{ and } \#J(\mathbb{F}_q) = \sum_{i=0}^{4} (-1)^i \operatorname{Tr}(F|\bigwedge^i V).$$

Now one uses Poincaré duality and linear algebra to work out the rest of the proof. ∎

[36] 2 is completely inert in $K = \mathbb{Q}(\zeta_{13})$ since $2 \in (\mathbb{Z}/13\mathbb{Z})^\times$ is a generator, so these cusps in char 2 should be defined over $\mathbb{F}_{2^{[K^+:\mathbb{Q}]}} = \mathbb{F}_{2^6}$ if I've not misled myself

This tells us that $\#J(\mathbb{F}_2) = 19$. Now, the map $J(\mathbb{Q})_{tors} \to J(\mathbb{F}_2)$ is injective away from 2-power torsion, so the theorem is correct up to 2-power-torsion. To deal with that, use the same strategy in char 3. Over $\mathbb{F}_3$, one has $\#X(\mathbb{F}_3) = 6$. Over $\mathbb{F}_9$, it turns out you can have an elliptic curve with a 13-torsion point, but there's only one such curve and it has an automorphism group of order 6, so the 12 generators only give 2 distinct points. Hence, $\#X(\mathbb{F}_9) = 8$ which, by the lemma, implies that $\#X(\mathbb{F}_3) = 19$ and we win. ■

Proposition 22.12. *The image of $X(\mathbb{C})$ in $J(\mathbb{C})$ (via $P \mapsto [P] - [P_6]$) meets $J(\mathbb{Q})_{tors}$ only at the 6 cusps.*

Proof idea. Suppose that $[P] - [P_6] \in J(\mathbb{Q})_{tors}$. Then, you can write $[P] - [P_6] = n([P_1] - [P_6])$ for some n (since we just computed the torsion subgroup). Thus,

$$[P] - n[P_1] + (n-1)[P_6] = \operatorname{div}(f)$$

for some function f on X. One shows that this can't happen unless $n = 1$ or something. ■

Unclear to me how to finish

Corollary 22.13. *To prove Theorem 22.1, it is enough to show that* $\operatorname{rank} J(\mathbb{Q}) = 0$.

22.3 $\operatorname{rank} J(\mathbb{Q}) = 0$

Proposition 22.14. *J is a simple abelian variety*

Proof. Suppose we have an exact sequence (in the isogeny category?)

$$0 \longrightarrow J_1 \longrightarrow J \longrightarrow J_2 \longrightarrow 0$$

with J_1, J_2 elliptic curves (since $\dim J = 2$). Since J has a $\mathbb{Q}$-point of order 19, so does J_1 or J_2 (since 19 is prime). However, an elliptic curve over $\mathbb{Q}$ can't have a rational point of order 19.[37] ■

Remark 22.15. γ_2 generates $\Gamma = (\mathbb{Z}/13\mathbb{Z})^\times / \{\pm 1\}$. ∘

Proposition 22.16. *The action of γ_2 on J satisfies $x^2 - x + 1 = 0$.*

Proof. First γ_2 satisfies $x^6 - 1 = 0$, but not $x^d - 1 = 0$ for $d < 6$ since it generates Γ (and $\#\Gamma = 6$). Furthermore, if γ_2 satisfies some polynomial, then it must satisfy some irreducible factor of that polynomial (since J is simple). Now, we factor

$$x^6 - 1 = (x-1)(x+1)(x^2 + x - 1)(x^2 - x + 1).$$

The first 3 factors all divide some $x^d - 1$ with $d < 6$, so γ_2 can only satisfy the last one. ■

The ring $\mathbb{Z}[\gamma_2]/(\gamma_2^2 - \gamma_2 + 1) \cong \mathbb{Z}[\zeta_3]$ acts on J via endomorphisms defined over $\mathbb{Q}$. Over K^+,

$$D := \frac{\mathbb{Z}[\Delta]}{(\gamma_2^2 - \gamma_2 + 1)}$$

[37] We proved this in the previous lectures. However, there's a simpler argument in this case. We know J has good reduction away from 13, so J_1, J_2 do as well. Hence, we can reduce mod 2 and apply the Hasse bound to get a contradiction.

acts on J ($\mathbb{Z}[\Delta]$ the group algebra). This thing is actually an order in a simple algebra, so $D \otimes \mathbb{Q} \cong M_2(\mathbb{Q})$. This shows that this action is faithful (it can't factor through anything) and that J is not simple over K^+ (since its endomorphism ring over K^+ contains an $M_2(\mathbb{Q})$).

Let $V = J[19](\overline{\mathbb{Q}})$, a 4-dimensional vector space over $\mathbb{F}_{19}$. Both G, Δ act on V, and they do so compatibly. The prime 19 splits in $\mathbb{Z}[\zeta_3]$ (since $19 \equiv 1 \pmod 3$), so we may write $19 = \pi\overline{\pi}$ with $\pi, \overline{\pi} \in \mathbb{Z}[\zeta_3]$ (a PID). Write

$$V_\pi := \ker(\pi \mid J) \text{ and } V_{\overline{\pi}} := \ker(\overline{\pi} \mid J)$$

so $V = V_\pi \oplus V_{\overline{\pi}}$. Both of these summands are stable by G, Γ, but they are interchanged by the τ's.

Proposition 22.17. *The Weil pairing on V induces Cartier duality between V_π and $V_{\overline{\pi}}$.*

Proof. Since the Weil paring is perfect on $V = V_\pi \oplus V_{\overline{\pi}}$, it suffices to show that each summand is self-orthogonal. Note that, for $x, y \in V$, we have

$$(\gamma_2 x, \gamma_2 y) = (x, y)$$

(by functoriality of the Weil pairing). Now, γ_2 acts on V_π via multiplication by some primitive 6th root of unity $\zeta \in \mathbb{F}_{19}$. Thus,

$$(x, y) = (\gamma_2 x, \gamma_2 y) = (\zeta x, \zeta y) = \zeta^2 (x, y) \implies (x, y) = 0$$

for $x, y \in V_\pi$. ∎

Let $V(1) \subset V$ be $J(\mathbb{Q})_{tors}$, a 1-dimensional $\mathbb{F}_{19}$-vector space. This will be stable by γ_2, so $V(1) \subset V_\pi$ or $V(1) \subset V_{\overline{\pi}}$. Assume wlog that $V(1) \subset V_{\overline{\pi}}$.

Let $V(\gamma) = \{v \in V : av = \gamma_a v \text{ for all } a \in \Gamma\}$ where we identify $\Gamma = \mathrm{Gal}(K^+/\mathbb{Q})$. Γ' interchanges $V(1), V(\gamma)$, so we must have $V(\gamma) \subset V_\pi$ and 1-dimensional.

Finally, let $V(\chi) = \mathbb{F}_{19}$ with Galois action given by the (mod 19) cyclotomic character. The dual of the inclusion $V(1) \hookrightarrow V_{\overline{\pi}}$ is a surjection $V_\pi \twoheadrightarrow V(\chi)$.

Proposition 22.18. *The sequence*

$$0 \longrightarrow V(\gamma) \longrightarrow V_\pi \longrightarrow V(\chi) \longrightarrow 0$$

is exact.

Proof. We have exactness on the left and right for free. By dimension counting, exactness in the middle just amounts to the composition being 0. The action of G on $V(\gamma)$ factors through $\mathrm{Gal}(K^+/\mathbb{Q})$ (and nothing smaller), while the action of G on $V(\chi)$ factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{1})/\mathbb{Q})$ (and nothing smaller), so $V(\gamma) \not\cong V(\chi)$. As they're both 1-dimensional, any map between them (e.g. the composite) must be 0. ∎

Now we get to the actual proof that $J(\mathbb{Q})$ has rank 0. It will be enough to show that the map $\pi : J(\mathbb{Q}) \to J(\mathbb{Q})$ is surjective. This is because $J(\mathbb{Q})$ is a f.g. module over $\mathscr{O}_{\mathbb{Q}(\zeta_3)}$ (a Dedekind domain, and even a PID) so if multiplication by the non-unit $\pi \in \mathscr{O}_{\mathbb{Q}(\zeta_3)}$ is surjective, then $J(\mathbb{Q}) = J(\mathbb{Z}[1/13])$ better be finite.

Consider the diagram

$$\begin{array}{ccccc} J(\mathbb{Z}[1/13]) & \xrightarrow{\pi} & J(\mathbb{Z}[1/13]) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Z}\left[\frac{1}{13}\right], J[\pi]\right) \\ \downarrow & & \downarrow & & \downarrow \rho \\ J(\mathbb{Q}_{13}) & \xrightarrow{\pi} & J(\mathbb{Q}_{13}) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Q}_{13}, J[\pi]\right) \end{array}$$

To show that the top π map is surjective, it suffices to show **(1)** that $\pi : J(\mathbb{Q}_{13}) \to J(\mathbb{Q}_{13})$ is surjective and **(2)** $\rho : \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Z}\left[\frac{1}{13}\right], J[\pi]\right) \to \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Q}_{13}, J[\pi]\right)$ is injective. This follows from a simple diagram chase.

Claim (1) Write $\mathcal{J}/\mathbb{Z}_{13}$ for the Néron model of J, and let

$$N := \ker\left(\mathcal{J}(\mathbb{Z}_{13}) \to \mathcal{J}(\mathbb{F}_{13})\right),$$

a pro-13 group. Consider the sequence

Compare Corollary 8.22

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & \mathcal{J}(\mathbb{Z}_{13}) & \longrightarrow & \mathcal{J}(\mathbb{F}_{13}) & \longrightarrow & 0 \\ & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\ 0 & \longrightarrow & N & \longrightarrow & \mathcal{J}(\mathbb{Z}_{13}) & \longrightarrow & \mathcal{J}(\mathbb{F}_{13}) & \longrightarrow & 0 \end{array}$$

Since $\pi \mid 19$ ($19 = \pi\overline{\pi}$) and N is pro-13 the left vertical map must be an isomorphism. Thus, by the snake lemma, the middle vertical map is surjective (keep in mind $\mathcal{J}(\mathbb{Z}_{13}) = J(\mathbb{Q}_{13})$) iff the right vertical map is. Note that $\mathcal{J}(\mathbb{F}_{13})$ is finite, so π is surjective on it iff it's injective on it. A second application of the snake lemma shows that this is the case iff the middle vertical π is injective, i.e. we only need show that

$$0 = \ker\left(\pi | \mathcal{J}(\mathbb{Z}_{13})\right) = J[\pi](\mathbb{Q}_{13}) = V_\pi^D,$$

where $D \subset G$ is the decomposition group at 13. Now, we use the exact sequence

$$0 \longrightarrow V(\gamma) \longrightarrow V_\pi \longrightarrow V(\chi) \longrightarrow 0,$$

so it's enough to show that the D-invariants of the outside guys are 0. Note that $V(\gamma)$ is a faithful representation of $\mathrm{Gal}(K^+/\mathbb{Q})$ and that 13 ramified in K^+, so the decomposition group is nontrivial there and hence $V(\gamma)^D = 0$. Similarly, $V(\chi)$ is a faithful representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q})$ and the decomposition group at 13 there is nontrivial (since $13 \not\equiv 1 \pmod{19}$), so $V(\chi)^D = 0$ as well. This proves claim **(1)**.

Claim (2) We now want to show that

$$\rho : \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Z}\left[\frac{1}{13}\right], J[\pi]\right) \to \mathrm{H}^1_{\mathrm{fppf}}\left(\mathbb{Q}_{13}, J[\pi]\right)$$

is injective.

Proposition 22.19. *There is an exact sequence of group schemes over* $\mathbb{Z}[1/13]$*:*

$$0 \longrightarrow E \longrightarrow J[\pi] \longrightarrow \mu_{19} \longrightarrow 0$$

with E *a finite, étale group scheme that becomes trivial over* $\mathbb{Z}[1/13, \zeta_{13}]$*.*

Proof. Let E be the Zariski closure of $V(\gamma)$ in $J[\pi]$. We know that $V(\gamma)|_{\mathbb{Q}(\zeta_{13})}$ is trivial, so $E|_{\mathbb{Z}[1/13,\zeta_{13}]}$ is trivial as well by Raynaud. The quotient $J[\pi]/E$ is generically $V(\chi)$ (i.e. it is that over $\mathbb{Q}$) and so we must have $J[\pi]/E = \mu_{19}$ by Raynaud again. ∎

We draw another diagram

$$\begin{array}{ccccc} \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], E) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], J[\pi]) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], \mu_{19}) \\ & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho'} \\ & & \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Q}_{13}, J[\pi]) & \longrightarrow & \mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Q}_{13}, \mu_{19}) \end{array}$$

In order to show that ρ is injective, it will suffice to show that ρ' is injective and that the top left group $\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], E) = 0$ vanishes.

Note that Kummer theory tells us that

$$\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], \mu_{19}) \simeq \operatorname{coker}\left((\mathbb{Z}[1/13])^\times \xrightarrow{(-)^{19}} (\mathbb{Z}[1/13])^\times \right) = \mathbb{Z}[1/13]^\times / \left(\mathbb{Z}[1/13]^\times\right)^{19}$$

and that

$$\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Q}_{13}, \mu_{19}) \simeq \mathbb{Q}_{13}^\times / (\mathbb{Q}_{13}^\times)^{19}.$$

The map between these two is the obvious map. Note that $\mathbb{Z}[1/13]^\times = \{\pm 13^n\}$ and that $-1 = (-1)^{19}$ is a 19th power. The map

$$\mathbb{Z}[1/13]^\times / \left(\mathbb{Z}[1/13]^\times\right)^{19} \to \mathbb{Q}_{13}^\times / (\mathbb{Q}_{13}^\times)^{19}$$

is injective since 13^n is a 19th power in $\mathbb{Z}$ iff it is in $\mathbb{Q}_{13}$.

Now we need to show that $\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], E) = 0$. Note that E is an étale group scheme, so $\mathrm{H}^1_{\mathrm{fppf}}(\mathbb{Z}[1/13], E) = \mathrm{H}^1_{\text{ét}}(\mathbb{Z}[1/13], E)$. Furthermore, E trivializes after adjoining a 13th root of unity, and one has

$$\mathrm{H}^1_{\text{ét}}(\mathbb{Z}[1/13], E) = \mathrm{H}^1_{\text{ét}}(\mathbb{Z}[1/13, \zeta_{13}], \mathbb{Z}/19\mathbb{Z})^{\mathrm{Gal}(K/\mathbb{Q})}$$

$(K = \mathbb{Q}(\zeta_{13}))$.

Let's explain the above equality. Let G be a finite, abstract group, and let $\underline{G}$ be its associated constant group scheme. Let $X \xrightarrow{\pi} Y$ be a $\underline{G}$-torsor (e.g. a Galois cover with Galois group G), so in particular $X \to Y$ is finite étale + surjective. Associated to the composition of functors

$$\mathrm{Sh}(Y) \xrightarrow[\mathrm{H}^0(X, \pi^*(-))]{} G\text{-Mod} \xrightarrow[(-)^G]{} \mathrm{Ab}, \qquad \mathrm{H}^0(Y, -) : \mathrm{Sh}(Y) \to \mathrm{Ab}$$

There's probably a shorter explanation, but this is the best I could muster

is the Grothendieck spectral sequence (group cohomology on the outside)

$$E_2^{pq} = \mathrm{H}^p(G, \mathrm{H}^q(X, \pi^*\mathscr{F})) \implies \mathrm{H}^{p+q}(Y, \mathscr{F})$$

for any $\mathscr{F} \in \mathrm{Sh}(Y)$. This gives rise to the low-degree exact sequence

$$0 \longrightarrow \mathrm{H}^1(G, \mathrm{H}^0(X, \pi^*\mathscr{F})) \longrightarrow \mathrm{H}^1(Y, \mathscr{F}) \longrightarrow \mathrm{H}^1(X, \pi^*\mathscr{F})^G \longrightarrow \mathrm{H}^2(G, \mathrm{H}^0(X, \pi^*\mathscr{F})) \longrightarrow \mathrm{H}^2(Y, \mathscr{F}).$$

Now, say that $\mathscr{F}$ is represented by a finite, flat group scheme over Y, and suppose that $\gcd(\#G, \#\mathscr{F}) = 1$. Then,

$$\mathrm{H}^1(G, \mathrm{H}^0(X, \pi^*\mathscr{F})) = 0 = \mathrm{H}^2(G, \mathrm{H}^0(X, \pi^*\mathscr{F}))$$

since you're taking group cohomology where the group and the module have coprime orders. Thus, in this case,

$$\mathrm{H}^1(Y, \mathscr{F}) \xrightarrow{\sim} \mathrm{H}^1(X, \pi^*\mathscr{F})^G$$

as desired. In the present scenario, we're in luck since $\#\operatorname{Gal}(K/\mathbb{Q}) = 12$ is coprime to $\#E = 19$.

Thus, it is enough to show that $\mathrm{H}^1_{\text{ét}}(\mathbb{Z}[1/13, \zeta_{13}], \mathbb{Z}/19\mathbb{Z}) = 0$. This group has a nice interpretation as the group of $\mathbb{Z}/19\mathbb{Z}$-torsors over $\mathbb{Z}[1/13, \zeta_{13}]$, i.e. abelian extensions $L/\mathbb{Q}(\zeta_{13})$ of degree 19 which are unramified away from the (unique) prime λ (of K) above 13.[38] This we can understand using class field theory.

Such extensions are seen by the ray class group with modulus λ. This sits into an exact sequence

$$K_\lambda^\times \longrightarrow (\text{ray class group}) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0$$

The group $K_\lambda^\times$ is prime to 19 and also $19 \nmid \#\mathrm{Cl}(K)$, so all maps (ray class group) $\to \mathbb{Z}/19\mathbb{Z}$ are trivial, and we conclude that $\mathrm{H}^1_{\text{ét}}(\mathbb{Z}[1/13, \zeta_{13}], \mathbb{Z}/19\mathbb{Z}) = 0$.

22.4 What's left?

At this point, we've ruled out all the primes we need to rule out, but there are still some composite numbers left. We still have to rule out e.g. $25, 49$ and so on. Next time we'll talk about things like that.

Note 3. There's a nice bit of discussion about the history of this stuff near the end of the lecture that I didn't bother writing down, but that's probably worth listening to.

23 Lecture 23: Finishing up

This is the last lecture. We will give an overview of how one finishes the proof of Mazur's Theorem 1.4.

Theorem 23.1 (**Mazur's Theorem**, Conjecture of Ogg)**.** *Let G be a finite group. Then, there exists an elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \simeq G$ iff*

[38] Unless I've confused myself, such torsors are in bijection with surjections $\pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{Z}[1/13, \zeta_{13}]) \twoheadrightarrow \mathbb{Z}/19\mathbb{Z}$, and this is where the description in terms of number fields comes from ($\pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{Z}[1/13, \zeta_{13}])$ is the Galois group of the maximal extension $L/\mathbb{Q}(\zeta_{13})$ unramified away from 13)

- $G = \mathbb{Z}/n\mathbb{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$*; or*
- $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *for some* $n \in \{2, 4, 6, 8\}$

So far, we have proved the following:

Theorem 23.2 (Mazur, Mazur-Tate)**.** *If $N > 7$ is prime, then no $E/\mathbb{Q}$ has a rational point of order N.*

This rules out all the primes we want to rule out, but there are some composite values we still need to take care of.

Remark 23.3. Say $E/\mathbb{Q}$ is an elliptic curve. Then, from the structure of $E(\mathbb{C})_{tors}$ and from the Mordell-Weil, we know it's a finite product of two cyclic groups, i.e.

$$E(\mathbb{Q})_{tors} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \text{ where } n \mid m.$$

By the Weil pairing, $n \in \{1, 2\}$. This is because this group has $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = E(\mathbb{C})[n]$ inside of it, and so $\mathbb{Q}$ must contain $\mu_n(\mathbb{C})$, the image of the Weil pairing. The only roots of unity in $\mathbb{Q}$ are ± 1, so $n \leq 2$. ∘

Given what we have and the above observations, we still need to

- exclude N-torsion for $N \in \{14, 15, 16, 18, 20, 21, 24, 25, 27, 35, 49\}$
- exclude $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
- show there exists elliptic curves with torsion subgroups each of the allowed G

23.1 Excluding (most of) the remaining N-torsion

For the first step, we're trying to show that there's no points on $X_1(N)$ except the cusps. This is a curve, possibly of high genus.

Slogan. A good strategy for finding the $\mathbb{Q}$-points on a curve is to find a map down to an elliptic curve.

It so happens that for any of these values, $X_0(N)$ has genus 1 and rank 0, so in those cases, we get a lot kinda easily.

Remark 23.4. All these small cases (and more) were done by Kubert before Mazur proved his theorem. ∘

Proposition 23.5. *Suppose $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 46, 49\}$. Then, no $E/\mathbb{Q}$ has a point of order N.*

Proof Sketch. In these cases, $X_0(N)$ has genus 1. Standard methods will show that $X_0(N)(\mathbb{Q})$ has rank 0.[39] Then, it's easy to compute the torsion points of $X_0(N)(\mathbb{Q})$, and this is all points. If all these points are cusps, you're done.

However, it's not always the case that all the points on $X_0(N)(\mathbb{Q})$ are cusps, so what do you do in this case? Let $x_1, \ldots, x_n$ be the non-cusp $\mathbb{Q}$-points of $X_0(N)$. Each of these x_i is represented (non-uniquely,

[39] Nowadays, this direction of BSD is known, so you can just compute the L-function and show it's nonvanishing at $s = 1$ by computing a few decimal places. You can alternatively do it by descent (the same sort of strategy as done in the 13-torsion case)

since $X_0(N)$ is a coarse space) by some (E_i, G_i) with $E_i/\mathbb{Q}$ elliptic and G_i an N-cyclic subgroup. Suppose we have some $y \in Y_1(N)(\mathbb{Q})$ corresponding to some (E, P). Then, $y \mapsto x_i$ for some i which implies that $E_{\mathbb{C}} \simeq (E_i)_{\mathbb{C}}$, i.e. E, E_i are twists of each other. Thus, one needs to show that no twisted form of these E_i's have an N-torsion point.

Since E_i admits a cyclic N-isogeny, we have an exact sequence

$$0 \longrightarrow (\mathbb{Z}/N\mathbb{Z})\,(\alpha_i) \longrightarrow E_i[N] \longrightarrow (\mathbb{Z}/N\mathbb{Z})\,(\beta_i) \longrightarrow 0$$

with $\alpha_i, \beta_i : G_{\mathbb{Q}} \to (\mathbb{Z}/N\mathbb{Z})^{\times}$ some characters.

Assumption. Suppose for simplicity that the E_i are not CM, so the only twists are quadratic twists.

Let $E_i^{(d)}$ be the dth quadratic twist of E_i. Then, we have

$$0 \longrightarrow (\mathbb{Z}/N\mathbb{Z})\,(\alpha_i\chi_d) \longrightarrow E_i^{(d)}[N] \longrightarrow (\mathbb{Z}/N\mathbb{Z})\,(\beta_i\chi_d) \longrightarrow 0,$$

and we want to know there are no Galois invariants in the N-torsion of $E_i^{(d)}$, i.e. that α_i is not a quadratic character (i.e. $\alpha_i^2 \neq 1$) and also that $\beta_i^2 \neq 1$ if the extension splits. To do this, one just computes this character α_i for each i and checks that it's not quadratic.

The CM case is a little different, but can also be handled. ■

Example ($N = 21$)**.** $X_0(N)(\mathbb{Q})$ has 4 cusps and 4 non-cusps in this case. The non-cusps correspond to the elliptic curves

$$\begin{aligned} y^2 &= x^3 + 45x - 18 \\ y^2 &= x^3 - 75x - 262 \\ y^2 &= x^3 - 1515x - 46106 \\ y^2 &= x^3 - 17235x - 870894 \end{aligned}$$

These are all 4 non-CM. One needs to check that none of their twists have 21-torsion points, e.g. one can show that $dy^2 = x^3 + 45x - 18$ never even has a 3-torsion point. △

Example ($N = 27$)**.** $X_0(N)(\mathbb{Q})$ has one non-cusp point in this case, given by

$$y^2 + y = x^3 - 30x - 5$$

which has CM by $\sqrt{-27}$. △

Fact. There exists non-cuspidal $\mathbb{Q}$-points on $X_0(N)$ (with genus 1) iff

$$N \in \{11, 14, 15, 17, 19, 21, 27\}.$$

Remark 23.6. For $N \in \{11, 14, 15\}$, $X_1(N)$ itself has genus $g = 1$. Furthermore, $X_1(N)$ is isogenous to $X_0(N)$, and so must have rank 0. Hence, you can just compute the points on it directly and see that they're all cusps. ∘

Remark 23.7. Only really need Proposition 23.5 for $N \in \{20, 21, 24, 27, 49\}$. For these values on N, the only ones with non-cuspidal $\mathbb{Q}$-points on $X_0(N)$ are $N = 21, 27$, so you really only need to do something special for the 5 curves appearing in the two earlier examples. ◦

23.2 Excluding $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\{10, 12\}\mathbb{Z}$

Lemma 23.8. *Say $E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$). Then, there exists an isogeny $E \xrightarrow{2} E'$ s.t. E' admits a cyclic isogeny of degree 4 (resp. degree 8).*

Proof. Choose $P \in E(\mathbb{Q})$ of order 2, and $Q \in E(\mathbb{Q})$ be an independent point of order 2 (resp. 4). Consider $f : E \to E_1$ killing P and $g : E \to E_2$ killing Q. Consider the dual $f^\vee : E_1 \to E$. One can show that $f^\vee(E_1[2]) \ni P$. Consider the composition $gf^\vee : E_1 \to E_2$. This is does not kill all the 2-torsion which forces it to by cyclic. ■

Question: How?

Answer: $ff^\vee : E_1 \to E_1$ is multiplication by 2, so $f^\vee(E_1[2]) \subset \ker f = \langle P \rangle$. Since $\ker f^\vee$ has order 2 and $E_1[2]$ has order 4, we must have $f^\vee(E_1[2]) = \ker f = \langle P \rangle$.

Proposition 23.9. $E(\mathbb{Q}) \not\supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Proof. By lemma, there exists a 2-isogeny $E \to E'$ s.t. E' admits a cyclic isogeny of degree 4 or 8. Making use of the extra factor of $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$, E' will in fact admit a cyclic isogeny of degree 20 or degree 24, and so E' will define a (non-cuspidal) $\mathbb{Q}$-point on $X_0(20)$ or $X_0(24)$, contradicting the work in the previous section. ■

23.3 Excluding everything left: N-torsion for $N \in \{16, 18, 25, 35\}$

We'll just make a few comments on these cases.

23.3.1 16-torsion

This was done by Lind in 1940. Kubert says this is 'easy', but the only reference seems to be Lind's 1940 thesis which is apparently not easily accessible.

Remark 23.10. In this case, $X_1(16)$ has genus 2 while $X_0(16)$ has genus 0, so you can't try mapping to an elliptic curve. There are none.[40] ◦

TODO: Try to do this yourself

23.3.2 18-torsion

In this case, $g(X_0(18)) = 0$ and $g(X_1(18)) = 2$, so again, no elliptic curve you can map to. Kubert handles this case in his paper using a Mazur-Tate type argument. He shows $J_1(18)(\mathbb{Q})_{tors} = \mathbb{Z}/21\mathbb{Z}$ meeting $X_1(18)$ only at the cusps. Hence, it suffices to show this Jacobian has rank 0.

To do this, he observes that $\gamma_5 \in (\mathbb{Z}/18\mathbb{Z})^\times$ satisfies the equation $\gamma_2^2 + \gamma_2 + 1 = 0$ on $J_1(18)$. In the ring this defines, 7 factors as $7 = \pi\overline{\pi}$. Now one does π-descent to show that $J_1(18)$ has rank 0.

23.3.3 25-torsion

Another Mazur-Tate type argument, but a little more complicated. In this case, $g(X_1(25)) = 12$ and $g(X_0(25)) = 0$. This is a high genus, so you'd like to cut it down a little. Kubert uses a quotient curve of genus $g = 4$, and then runs Mazur-Tate there.

[40] e.g. if $X_1(16)$ mapped to an elliptic curve E, then E would have conductor dividing 16, and so appear as a factor of $J_0(16)$ by the modularity theorem

23.3.4 35-torsion

$g(X_0(35)) = 3$. Note that we have an Atkin-Lehner involution for each prime factor of 35, so can consider $E = X_0(35)/w_5$. This is an elliptic curve. One shows that it has rank 0, and that all the preimages of torsion points are cusps.

Remark 23.11. Kubert does this very explicitly, writing down equations for $X_0(35)$ and for the involution w_5 and whatnot. ∘

23.4 Showing the allowable groups do occur

First suppose $4 \leq N \leq 10$ or $N = 12$. Then, $X_1(N)$ has genus 0, and it has a $\mathbb{Q}$-point (e.g. a cusp), so $X_1(N) \cong \mathbb{P}^1_{\mathbb{Q}}$. Thus, $X_1(N)(\mathbb{Q})$ is infinite, so $Y_1(N)(\mathbb{Q})$ is infinite, so you get elliptic curves w/ N-torsion (note $X_1(N)$ is a fine moduli space for these values).

When $N = 2, 3$, $X_1(N)$ is only a coarse moduli space, but that's fine since it's easy to write down curves with 2- or 3-torsion points.

Remark 23.12 (2-torsion). $E : y^2 = f(x)$ with $f(a) = 0$ for some $a \in \mathbb{Q}$. Then, $(0, a) \in E[2](\mathbb{Q})$ ∘

Remark 23.13 (3-torsion). $E : y^2 + axy + by = x^3$. Then, $(0, 0) \in E[3](\mathbb{Q})$ (recall Lecture 14) ∘

The above shows there exists elliptic curves which have N-torsion. We would like this to be the full torsion subgroup. We'll get back to this in a minute.

Remark 23.14. For $N \in \{4, 6, 8\}$, can consider the moduli space Y of E's w/ injections $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E$, and then compactify this to some curve X. In these cases, X has genus 0 and a $\mathbb{Q}$-point given by a cusp, so we get $E/\mathbb{Q}$ s.t. $E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. This X is a fine moduli space since $N \geq 4$.

For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, just pick some cubic $f(x)$ with 3 distinct rational roots, and look at $y^2 = f(x)$. ∘

This shows we can get everything we want as a subgroup. Let's see an example of how to show they can be the full torsion subgroup.

Example ($\mathbb{Z}/5\mathbb{Z}$)**.** We want to show $\exists E$ w/ $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$. By what we've done, the only problem would be if every E s.t. $E(\mathbb{Q}) \supset \mathbb{Z}/5\mathbb{Z}$ also satisfies $E(\mathbb{Q}) \supset \mathbb{Z}/10\mathbb{Z}$. That is, we're sad if

$$Y_1(1) \to Y_1(5)$$

is surjective on $\mathbb{Q}$-points. This map extends to

$$\begin{array}{ccc} X_1(10) & \xrightarrow{=} & \mathbb{P}^1 \\ \downarrow & & \downarrow{\scriptstyle 3} \\ X_1(5) & \xrightarrow{=} & \mathbb{P}^1 \end{array}$$

and no map $\mathbb{P}^1 \to \mathbb{P}^1$ of degree > 1 will be surjective on $\mathbb{Q}$-points. △

The key point to constructing the allowable subgroups is that the relevant moduli curves are genus 0. One can in fact write down what the universal families are very explicitly.

Example. The universal curve over $Y_1(4)$ is

$$E_t : y^2 + xy - ty = x^3 - tx^2 \text{ with } (0, 0) \in E_t[4]$$

where t is the parameter on $X_1(4) \cong \mathbb{P}^1$. $\triangle$

For each of the 15 allowable groups (at least the ones where the moduli problem is a scheme), you can write down the universal family.

23.5 Audience Question (showing no twists of a curve have 3-torsion)

In the example of excluding 21-torsion points, Andrew remarked that he could show that

$$y^2 = x^3 + 45x - 18$$

(and all of its quadratic twists) have no 3-torsion points.

Question 23.15 (Audience, asked much earlier in the lecture)**.** *How does one go about showing, by hand, that*

$$dy^2 = x^3 + 45x - 18$$

has no 3-torsion points for all d?

You might worry that there are infinitely many d, but it turns out to not be that bad. The trick is to consider the universal curve.

Say you have some curve like $y^2 = x^3 + ax + b$ (w/o CM), and you want to show that no quadratic twist has any 3-torsion. You can write down the universal elliptic curve with 3-torsion. There's a little catch which is that $Y_1(3)$ is a coarse space, not a fine one, but there's only one point with automorphisms: the thing that has CM by $\mathbb{Z}[\zeta_3]$. This doesn't really matter since our curve does not have CM. Hence, $Y_1(3) \setminus \{\text{this one point}\}$ is a scheme which supports a universal curve. One can write it down and make a change of variables to put it in the form

$$y^2 = x^3 + f(t)x + g(t)$$

with f a linear polynomial and g a quadratic one. If $dy^2 = x^3 + ax + b$ has a 3-torsion point, then it will be isomorphic to a member of this family. Changing $(x, y) \rightsquigarrow (x/d, y/d^2)$ shows this curve is isomorphic to

$$y^2 = x^3 + d^2ax + d^3b.$$

Now, for a, b fixed and d varying, the question is: does this curve ever appear in the family $y^2 = x^3 + f(t)x + g(t)$? That is, does there exists $u, t \in \mathbb{Q}$ such that

$$d^2a = u^4 f(t) \text{ and } d^3b = u^6 g(t)?$$

This would force

$$a^3/b^2 = f(t)^3/g(t)^2.$$

This is some explicit polynomial in t, and it turns out that for the a, b we started with, it doesn't have any solutions.

24 List of Marginal Comments

Index