LOCAL ARITHMETIC OF CURVES AND JACOBIANS

1. Lecture 1: Curves and Jacobians

Let k be a field. When talking about geometric objects over k, following [Poo17], we make the conventions that:

- An *algebraic variety* over k is a finite type, separated k-scheme,
- A *curve* over k is an algebraic variety all of whose irreducible components have dimension 1,
- An algebraic variety is said to be *nice* if it's smooth, projective and geometrically integral.

For nice varieties line bundles and linear equivalence classes of divisors coincide, and we will pass between the two without comment.

In this course we will predominantly be interested in the arithmetic of nice curves and abelian varieties, over finite extensions of $\mathbb{Q}_p$ for a prime p, though much of the motivation comes from (the aim of) understanding these objects over number fields.

1.1. Examples of nice curves.

We begin by reviewing the curves which will form our basic examples throughout the course.

Example 1.1 (Projective line)**.** The most basic example is the projective line

$$\mathbb{P}^1_k = \mathrm{Proj}\,(k[x,y])\,.$$

It has genus 0.

Example 1.2 (Elliptic curves)**.** An elliptic curve is a genus 1 curve with a specified k-point O. If we assume $\mathrm{char}(k) \neq 2,3$, then any elliptic curve E has a *Weierstrass equation* of the shape

$$E : y^2 = x^3 + ax + b,\ a, b \in k$$

such that the *discriminant* $\Delta_E = -16(4a^3 + 27b^2)$ is $\neq 0$ (this is equivalent to the equation being smooth). Strictly speaking this equation defines an affine curve, and we should instead consider the projective curve

$$\{y^2z - x^3 - axz^2 - bz^3 = 0\} \subseteq \mathbb{P}^2_k$$

which contains an additional point at infinity (which we can force to correspond to the specified point O).

Example 1.3 (Hyperelliptic curves)**.** A hyperelliptic curve is a nice curve C of genus at least 2, equipped with a degree 2 (finite separable) morphism to $\mathbb{P}^1_k$. Assuming $\mathrm{char}(k) \neq 2$, C can be defined by an equation of the shape

$$C : y^2 = f(x)$$

where $f(x)$ is a squarefree polynomial and the morphism is given by projecting onto the x-coordinate. If $\deg(f) \in \{2g+1, 2g+2\}$ then C has genus g (use Riemann–Hurwitz for the map to $\mathbb{P}^1$). Again, as with the previous example, this is a smooth affine curve. The associated nice curve consists of the two affine curves

$$U_1 : y^2 = f(x)$$

and

$$U_2 : z^2 = w^{2g+2} f(1/w)$$

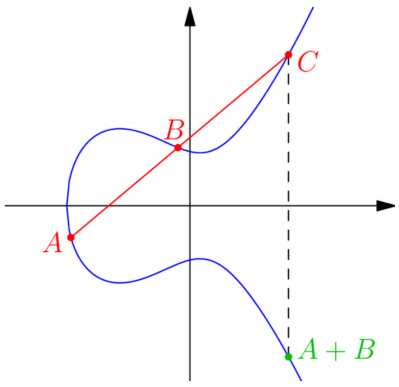
glued over $\{x \neq 0\}$ and $\{w \neq 0\}$ along the isomorphism $x = 1/w$ and $y = z/w^{g+1}$. We call the points on $U_2 \setminus U_1$ the *points at infinity*. There are two such points (possibly defined only over a quadratic extension of k) if $\deg(f)$ is even, and one point if $\deg(f)$ is odd.

Remark 1.4. If $k = \bar{k}$ then the examples above cover all curves of genus 0,1 and 2. To cover genus 3 we additionally need to include smooth plane quartics, i.e. smooth curves defined by the vanishing of a degree 4 homogeneous polynomial in 3 variables. See e.g. [Har77, Chapter IV], especially the discussion surrounding Remark 5.5.1, for a discussion of the classification of curves of small genus.

1.2. **Abelian varieties.** Milne's two articles in [CS86] are a good reference for the material in the remainder of this lecture.

Let E/k be an elliptic curve, specified point $O \in E(k)$. Then the set $E(k)$ of k-points of E has a natural (abelian) group structure with identity O, which can be seen in the following two ways:

- Pick a Weierstrass equation for E with O the point at infinity. Then the group structure on $E(k)$ is described by the *chord–tangent process*



- More abstractly, one shows via Riemann–Roch that the map

$$P \mapsto (P) - (O) \in \mathrm{Div}^0(E/k)/\text{lin. eq.} = \mathrm{Pic}^0(E/k)$$

  is a bijection from $E(k)$ to $\mathrm{Pic}^0(E/k)$ with O mapping to 0. We can then pull back the group structure on $\mathrm{Pic}^0(E/k)$ to $E(k)$.

These two ways are equivalent and turn out to give E the structure of an *abelian variety*.

Definition 1.5. An *abelian variety* over k is a nice group variety (i.e. a nice variety equipped with a group structure where the group operations are given by morphisms).

Remark 1.6. We have:

- The group structure is automatically abelian (this follows from projectivity).
- Any proper, connected, geometrically reduced group variety is in fact automatically smooth and projective, whence an abelian variety.
- All one dimensional abelian varieties are elliptic curves (and, of course, conversely).
- Over $\mathbb{C}$, any abelian variety of dimension g is (as a complex Lie group) isomorphic to $\mathbb{C}^g/\Lambda$ for some lattice $\mathbb{Z}^{2g} \cong \Lambda \subseteq \mathbb{C}^g$.

1.3. **Torsion points on abelian varieties.** Lots of current work in number theory is concerned with understanding as well as possible the group of rational points of abelian varieties over fields of arithmetic interest (e.g. number fields and their completions). Particularly accessible is the subgroup consisting of points of finite order. The following describes what the torsion points on an abelian variety look like over an algebraically closed field. Over $\mathbb{C}$ this follows from the last bullet point of the remark above.

Theorem 1.7. *Let k be a field and A/k an abelian variety of dimension g. Then for each $n \geq 1$ coprime to the characteristic of k we have*

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

It's often helpful to put all the torsion points (or all prime power torsion points for a fixed prime) together into an object called the *Tate module*.

Definition 1.8 (Tate module)**.** Let k be a field, A/k an abelian variety, and l a prime number different from the characteristic of k. We define the l-adic Tate module $T_l(A)$ of A to be the inverse limit

$$T_l(A) = \lim_{\leftarrow} A(\bar{k})[l^n].$$

As an abelian group this is abstractly isomoprhic to $\mathbb{Z}_l^{2g}$.

Remark 1.9. For n coprime to the characteristic of k, it turns out that all n-torsion points are contained in $A(k^{\mathrm{sep}})$. In particular, the absolute Galois group G_k of k acts naturally on these points. In this way we get a $\mathbb{Z}_l$-linear action of G_k on the l-adic Tate module $T_l(A)$, hence a $\mathbb{Q}_l$-linear action on

$$V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

We refer to this as the *l-adic Galois representation associated to A*.

1.4. **Abelian varieties over number fields.** For this subsection we work over a number field K. Let A/K be an abelian variety. The first starting point for understanding the group $A(K)$ is the Mordell–Weil theorem.

Theorem 1.10 (Mordell–Weil theorem)**.** *Let K be a number field and A/K an abelian variety. Then $A(K)$ is a finitely generated abelian group. Thus*

$$A(K) \cong A(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$$

where $A(K)_{\mathrm{tors}}$ is a finite abelian group and $r \geq 0$ an integer. We call this integer r the rank *of A/K, denoted* $\mathrm{rk}(A/K)$.

The rank of an abelian variety is one of its most important invariants. It is, conjecturally, related via the Birch and Swinnerton–Dyer conjecture (see Maistret's course for more on this) to another important invariant: the L-function $L(A/K, s)$.

Definition 1.11 (The L-function of an abelian variety)**.** Let A/K be an abelian variety of dimension g. For each nonarchimedean place v of K and prime l with $v \nmid l$, we define the *local L-polynomial*

$$L_v(A, T) = \det\left(1 - \mathrm{Frob}_v^{-1} T | (V_l(A)^\vee)^{I_v}\right)$$

where here I_v denotes the inertia group at v, Frob_v is the (arithmetic) Frobenius at v, and $V_l(A)^\vee$ is the dual of $V_l(A)$.

It's a general fact (which follows from the Weil conjectures and the existence of the Néron model) that $L_v(A, T)$ is a polynomial with integer coefficients and is independent of the choice of l. Writing q_v for the size of the residue field at v, one defines the L-*function* of A/k to be the function of a complex variable s given by

$$L(A/K, s) = \prod_{v \nmid \infty \text{ place of } k} L_v(A, q_v^{-s})^{-1}.$$

Remark 1.12. The L-function of any abelian variety can be shown to converge for $\mathrm{Re}(s) > 3/2$ and conjecturally has analytic continuation to the whole of $\mathbb{C}$ satisfying a functional equation $s \leftrightarrow 2 - s$. This is known for all elliptic curves over $\mathbb{Q}$ by work of Wiles, Taylor–Wiles, and Breuil–Conrad–Diamon–Taylor. More recently there has been much work towards this conjecture for elliptic curves over more general fields (totally real or CM) and for abelian surfaces over totally real fields. In particular, we now know analytic continuation for the L-function associated to an elliptic curve over totally real quadratic and cubic fields. oreover, we know meromorphic continuation for the L-function of an elliptic curve over all CM fields, and for the L-function of an abelian surface over totally real fields. See [FLHS15], [DNS19], [ACC$^+$18], [BCGP18] and the references therein.

Example 1.13. Let E/K be an elliptic curve and v a nonarchimedean place of K of norm q_v. Let $\bar{E}/k_v$ be the reduction of a minimal Weierstrass equation at v, where k_v is the residue field of v. If E has good reduction at v then

$$L_v(E, T) = 1 - a_v T + q_v T^2$$

where $a_v = q_v + 1 - |\bar{E}(k_v)|$. For the places of bad reduction of E we have

$$L_v(E, T) = \begin{cases} 1 - T & E \text{ split mult at } v, \\ 1 + T & E \text{ non-split mult at } v, \\ 1 & E \text{ additive at } v. \end{cases}$$

1.5. **Jacobians.** The theory of curves and abelian varieties meets in *Jacobians*, which are one of the main sources of examples of abelian varieties.

Definition 1.14 (Approximate definition)**.** Let C be a nice curve of genus g. Then one can naturally associate to C a g-dimensional abelian variety $\mathrm{Jac}(C)$, the *Jacobian* of C, such that (as abelian groups) for any field extension K/k,

$$\mathrm{Jac}(C)(K) = \mathrm{Pic}^0\left(C/K^{\mathrm{sep}}\right)^{\mathrm{Gal}(K^{\mathrm{sep}}/K)}$$

functorially.

Remark 1.15. More precisely, it's a theorem that the functor from k-schemes to abelian groups

$$T \mapsto \mathrm{Pic}^0\left(C_{T_{k^{\mathrm{sep}}}}\right)^{\mathrm{Gal}(k^{\mathrm{sep}}/k)}$$

is representable by an abelian variety over k. This representing object is the Jacobian of C.

Remark 1.16. Since $\mathbb{P}^1_k$ has genus 0 its Jacobian should be zero, which is reflected in the isomorphism $\deg : \mathrm{Pic}(\mathbb{P}^1_k) \xrightarrow{\sim} \mathbb{Z}$. Moreover, for an elliptic curve E, the Riemann–Roch argument shows that E is its own Jacobian.

Remark 1.17. Let C be a nice curve of genus ≥ 2 with a k-point O. Then the Riemann–Roch argument generalises to give a closed immersion $C \to \mathrm{Jac}(C)$ (induced by $P \mapsto (P) - (O)$) called the *Abel–Jacobi map*. If k is a number field one of the main ways to understand the set $C(k)$ of rational points on C is to attempt to understand the image of $C(k)$ inside its Jacobian.

Remark 1.18. Even when the equation defining a curve is quite simple, the equations defining the Jacobian can be very complicated. For example, Flynn shows in [Fly90] that the Jacobian of a general genus 2 curve $y^2 = f(x)$ where $f(x)$ has degree 6, is given by the vanishing of 72 quadratic forms in $\mathbb{P}^{15}_k$ (over a field k with $\mathrm{char}(k) \neq 2, 3, 5$). Consequently, one of our aims for this course is to describe how to compute certain invariants of Jacobians by working with the underlying curves.

Remark 1.19. We have a canonical isomorphism

$$T_l(\mathrm{Jac}(C)) \cong \mathrm{Hom}_{\mathbb{Z}_l}\left(H^1_{\text{ét}}(C_{\bar{k}}, \mathbb{Z}_l), \mathbb{Z}_l\right)$$

compatible with the Galois actions. Thus understanding the Tate module of the Jacobian of C is the same as understanding the first étale cohomology group of C.

1.6. **The dual abelian variety.** One of the main things which distinguishes Jacobians from general abelian varieties is that they are canonically *principally polarised*. To explain what this means we need to introduce the dual of an abelian variety.

Definition 1.20 (Approximate definition)**.** Let A/k be an abelian variety. Then there is another abelian variety, $A^\vee/k$, of the same dimension of A, and such that, for any extension K/k,

$$A^\vee(K) = \mathrm{Pic}^0\left(A/K\right)$$

functorially.[1] Again, this can be made precise in a way analagously to Remark 1.15.

Again, the Riemann–Roch argument shows that an elliptic curve is canonically isomorphic to its dual. The relavance of the dual abelian variety for arithmetic is that a lot of natural pairings (the Weil pairing, local duality pairings, the Cassels–Tate pairing,...) naturally take place not between an abelian variety and itself, as is the case for elliptic curves, but between an abelian variety and its dual. However, abelian varieties are closely related to their duals via the notion of a polarisation.

Definition 1.21. Let $\mathcal{L}$ be a line bundle on an abelian variety A/k and $x \in A(k)$. Writing τ_x for the 'translation-by-x' morphism, the line bundle

$$\tau_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

is algebraically equivalent to zero. This construction gives a map $A(k) \to A^\vee(k)$,

$$x \longmapsto \tau_x^*\mathcal{L} \otimes \mathcal{L}^{-1}.$$

In fact, this can be ramped up to give a homomorphism of abelian varieties

$$\phi_{\mathcal{L}} : A \longrightarrow A^\vee.$$

In general, any homomorphism $A \to A^\vee$ which arises via this construction after base-extension to $\bar{k}$ is called a *polarisation*. A polarisation is called *principal* if it's an isomorphism.

Remark 1.22. One can show that a polarisation is an *isogeny* (finite kernel in this context) if and only if the line bundle $\mathcal{L}$ is ample. Since all abelian varieties are projective they come endowed with at least one (very) ample line bundle, and are thus always isogeneous to their duals. This has a number of consequences for their arithmetic. For example, over a number field an abelian variety has the same rank and L-function as its dual.

Proposition 1.23. *Let C/k be a nice curve. Then $J = \mathrm{Jac}(C/k)$ is canonically principally polarised.*

Sketch of proof. We'll first do this over $\bar{k}$. Pick an initial point $O \in C(\bar{k})$. For any n, we have a morphism (defined over $\bar{k}$) $C^n \to J$ induced by

$$(P_1, ..., P_n) \mapsto \sum_{i=1}^{n} (P_i) - n(O).$$

It turns out that when $n = g-1$ the image is an effective divisor on J, and hence yields a line bundle Θ on J called the *Theta bundle*. The resulting polarisation $\phi_\Theta : J \to J^\vee$ can be shown to be principal, and does not, in fact, depend on the choice of initial point O. Using this latter fact, one can additionally show that the morphism ϕ_Θ (although not Θ in general) is defined over k. □

[1] Here $\mathrm{Pic}^0(A/K)$ is the subgroup of $\mathrm{Pic}(A/K)$ consisting of line bundles algebraically equivalent to 0. We do not need to pass to a larger extension and take galois invariants here since, unlike for curves, every abelian variety has at least one k-point.

2. Exercises for lecture 1

2.1. Let k be an algebraically closed field of characteristic different from 2, and let $C : y^2 = f(x)$ be a hyperelliptic curve over k of genus $g \geq 2$. Suppose that $f(x)$ has odd degree $2g+1$ and denote by $\mathcal{R}$ the set of roots of $f(x)$.

(i) Show that the ramification points of the x-coordinate map $\phi : C \to \mathbb{P}^1$ are the points $P_r = (r, 0)$ for $r \in \mathcal{R}$, along with the unique point O at infinity.

(ii) Show that each of the degree 0 divisors

$$\{(P_r) - (O) \ \mid \ r \in \mathcal{R}\}$$

are 2-torsion points in the Jacobian of C.

(iii) Show that, for k now not necessarily algebraically closed, as a G_k-module, the 2-torsion subgroup of the Jacobian of C is isomorphic to

$$\mathbb{F}_2[\mathcal{R}]/\Sigma$$

where $\mathbb{F}_2[\mathcal{R}]$ denotes the permuation module on $\mathcal{R}$ with $\mathbb{F}_2$-coefficients, and Σ is the formal sum of the elements of $\mathcal{R}$.

(iv) What is the analagous description in the case where $f(x)$ has even degree?

2.2. Let k be an algebraically closed field of characteristic different from 2, and let $C : y^2 = f(x)$ be a hyperelliptic curve over k of genus 2 (so that f has degree 5 or 6). Denote by ι the *hyperelliptic involution* sending a point $P = (x, y)$ to $(x, -y)$.

(i) Show that the class of the canonical divisor K_C is represented by the divisor $P + \iota(P)$ for any point P on C (hint: consider the degree 2 map to $\mathbb{P}^1$ and use Riemann–Hurwitz).

(ii) Show that the map sending $\{P_1, P_2\}$ to the divisor $(P_1) + (P_2) - (O) - (\iota(O))$ (for O any point at infinity) is a surjection from the set of unordered pairs of points on C, to the set degree 0 divisors on C modulo linear equivalence. Show that the inverse image of any degree 0 divisor class other than 0 consists of a unique pair. What is the inverse image of the 0 class? (Note that for a general (say perfect) field k this gives a description of $\mathrm{Jac}(C)(\bar{k})$ as a G_k-set.)

(iii)* How would one go about adding two points $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$ of $\mathrm{Jac}(C)$ via this identification?

3. Models of curves and abelian varieties

In order to understand the behaviour of curves and abelian varieties over number fields it's natural to first try to understand them over completions of number fields. In particular the L-function, for example, is defined only using the abelian variety over all completions. Thus we now move from arbitrary fields to a fixed finite extension K of $\mathbb{Q}_p$ for a prime p (of course, there is also a lot of interesting stuff going on over the real numbers and the complex numbers, but we will not persue this further). Let $\mathcal{O}_K$ denote the ring of integers of K, and k the residue field. Our general philosophy is to study curves and Jacobians over K by reducing, as much as possible, to questions over the finite field k. This can often reduce questions to a finite computation, whilst from a theoretical point of view the Weil conjectures give a huge tool to draw on. The key method for moving from K to its residue field is given by the theory of models. Roughly, the idea is that one wants to 'reduce modulo p' but before one can do this the equations defining the variety in question need to have coefficients in $\mathcal{O}_K$. Of course, there are many changes of variables over K which achieve this and we need to single out ones which are particularly useful.

3.1. Motivation: elliptic curves. Let p be a prime taken, for simplicity, not equal to $2, 3$ and let

$$E/\mathbb{Q}_p : y^2 = x^3 + ax + b$$

be an elliptic curve. After a change of variable of the form $(x, y) \mapsto (u^2x, u^3y)$ for $u \in \mathbb{Q}_p^\times$ we can assume that $a, b \in \mathbb{Z}_p$ and that $\mathrm{ord}_p(\Delta_E)$ is minimal amongst all such equations. We call this the *minimal Weierstrass equation* for E. The reduction modulo p,

$$\bar{E}/\mathbb{F}_p : y^2 = x^3 + \bar{a}x + \bar{b},$$

is well defined (up to isomorphism over $\mathbb{F}_p$) and falls into one of three cases:

- $\bar{E}/\mathbb{F}_p$ is an elliptic curve. This happens if and only if $\mathrm{ord}_p(\Delta_E) = 0$ and is referred to as *good reduction*.
- $\bar{E}/\mathbb{F}_p$ has a node. This happens if the polynomial $x^3 + ax + b \pmod p$ has a unique double root and is referred to as *multiplicative reduction*.
- $\bar{E}/\mathbb{F}_p$ has a cusp. This happens if the polynomial $x^3 + ax + b \pmod p$ has a triple root and is referred to as *additive reduction*.

Moreover, the subset of non-singular points on $\bar{E}$ have a natural group structure.

Remark 3.1. If E has good reduction then it does so over any extension of $\mathbb{Q}_p$ also, and the same is true of multiplicative reduction. On the other hand, additive reduction becomes either good or multiplicative after a finite extension. In fact, as $p \neq 2$, any ramified quadratic extension of the splitting field of $x^3 + ax + b$ suffices.

For general curves $C/\mathbb{Q}_p$ we have a similar picture to the one above, but we need some more involved theory to describe it.

3.2. Models of curves. As before, let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ its ring of integers and k its residue field. Fix a nice curve C/K.

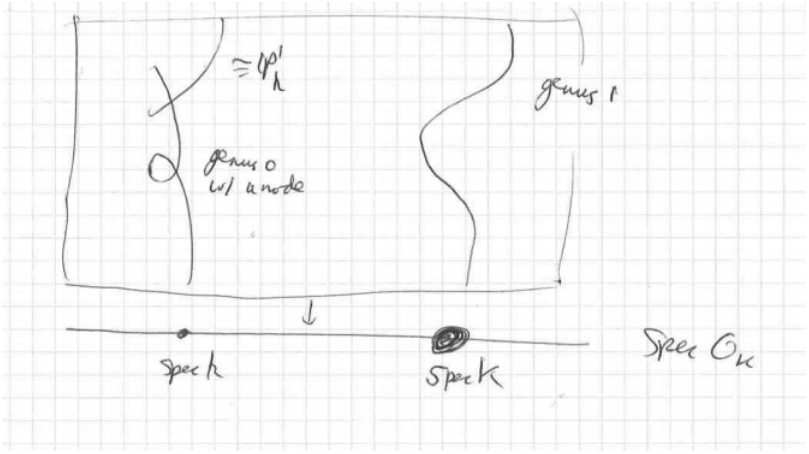
Definition 3.2. A *model* of C is a scheme $\mathcal{C}/\mathcal{O}_K$, finite type, flat and proper[2] over $\mathcal{O}_K$, and equipped with a specified isomorphism

$$\mathcal{C} \times_{\mathcal{O}_K} K \xrightarrow{\sim} C$$

of schemes over K. We refer to $\mathcal{C} \times_{\mathcal{O}_K} K$ as the *generic fibre* of $\mathcal{C}$, and define its *special fibre* to be the k-scheme

$$\overline{\mathcal{C}} = \mathcal{C} \times_{\mathcal{O}_K} k.$$

The picture is as follows (genera added to illustrate how arithmetic genus is presrved when passing to the special fibre):



Example 3.3. Let $E/\mathbb{Q}_p$ be an elliptic curve say with minimal Weierstrass equation $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}_p$. Then we can consider the scheme

$$\mathcal{E} : \{y^2z - x^3 - axz^2 - bz^3 = 0\} \subseteq \mathbb{P}^2_{\mathbb{Z}_p}$$

which is a model of E. Its special fibre is the curve $\bar{E}$ above (along with the usual point at infinity). We will refer to this as the *minimal Weierstrass model*.

For elliptic curves the minimal Weierstrass model gives a 'best' model of E over $\mathbb{Z}_p$. In some sense, it's the model which gives the special fibre the best chance of being an elliptic curve over $\mathbb{F}_p$. In general, we want to find an equation free method for specifying a 'best' or a least 'not that bad' model of a curve.

There are, broadly, two ways to go:

- Insist that the scheme $\mathcal{C}/\mathcal{O}_K$ is regular ('smooth as a surface').

[2]Roughly, flatness ensures that the resulting reduction retains information about C (such as being connected, having dimension 1, having arithmetic genus equal to the genus of C) and properness ensures projectivity of the reduction and the existence of a reduction map on points.

- Ask that the special fibre be 'not too bad'. The usual thing to ask for is that it be 'semistable' (the analogue of the special fibres of good or multiplicative elliptic curves).

The first of these is always possible and in fact there is a minimal such model (assuming that C has genus at least 1), the *minimal regular model*[3]. This is a fundamental object however the special fibres of these models can still be quite complicated. By contrast, semistable curves (to be discussed shortly) are all quite simple, however it is not always the case that a given curve has a semistable model. That said, one can always find one over a finite extension of K in which case there is a minimal such (now assuming that C has genus at least 2). Moreover, when such a model can be found the minimal regular model has semistable special fibre also. We will focus on semistable curves, as they are easier to work with and are all that is needed for many problems. However, there are still cases when one needs to work with a regular model instead and computing (with) these models is an important topic which we will not discuss further.

The best possible situation, which is an instance of both cases above, is when the special fibre is in fact a nice curve. Indeed, nice curves are in particular semistable and when the special fibre is a nice curve the structure map $\mathcal{C} \to \mathrm{Spec}\mathcal{O}_K$ is smooth whence $\mathcal{C}$ is regular.

Definition 3.4. We say that C has *good reduction* if there is a model $\mathcal{C}$ of C whose special fibre is a nice curve over k.

Example 3.5. Note that:

- If E is an elliptic curve then this is consistent with what we had previously (at least, if an elliptic curve has good reduction in the first sense, then it also has good reduction in the second; the converse is also true but not immediately obvious).
- Suppose $C : y^2 = f(x)$ is a hyperelliptic curve over $\mathbb{Q}_p$, $p \neq 2$, and suppose that $f(x) \in \mathbb{Z}_p[x]$ is such that $\mathrm{ord}_p(\Delta(f)) = 0$ where $\Delta(f)$ is the discriminant of $f(x)$. Then we may glue the affine schemes

$$\mathcal{U}_1 = \mathrm{Spec}\mathbb{Z}_p[x, y]/(y^2 - f(x))$$

and

$$\mathcal{U}_2 = \mathrm{Spec}\mathbb{Z}_p[w, z]/(z^2 - w^{2g+2} f(1/w))$$

along $x = 1/w$ and $y = w^{g+1}z$ over the open subsets $x \neq 0$ and $x \neq 0$ respectively. The resulting scheme is a model of C whose special fibre is the nice hyperelliptic curve given by the equation $y^2 = \bar{f}(x)$, where $\bar{f}(x)$ is the reduction of $f(x)$ modulo p.

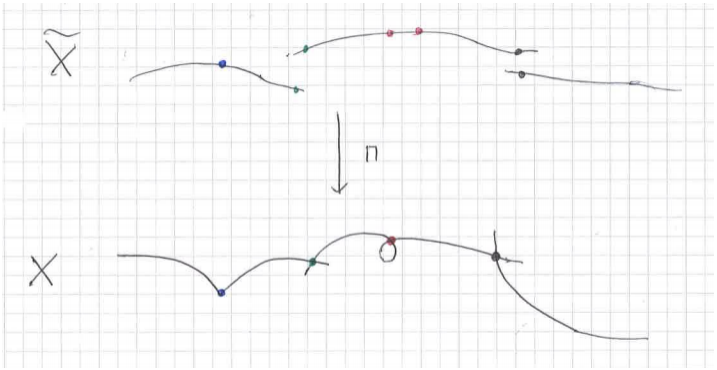
[3]Formally, we say a regular model $\mathcal{C}$ for C is *minimal* if for every other regular model $\mathcal{C}'$ for C, the map between their generic fibres corresponding to the identity on C extends to a morphism $\mathcal{C}' \to \mathcal{C}$. One can show that there always exists a regular model of C that is minimal in this sense, which is necessarily unique. This is the *minimal regular model* of C.

Remark 3.6. One can show that if C has genus at least 1 and $\mathcal{C}$ and $\mathcal{C}'$ are models of C with good reduction, then (as follows from the existence of the minimal regular model) $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic over $\mathbb{Z}_p$.

3.3. The structure of singular curves. The aim of this subsection is to motivate and define semistable curves, and study their properties. To begin with suppose $k = \bar{k}$ and let X be a projective, reduced, connected curve (possibly singular and with multiple irreducible components). Denote by X_{sing} the set of singular points of X.

Definition 3.7. The *normalisation* of X, $\tilde{X}$, is the disjoint union of the normalisations of the individual components (and is thus a disjoint union of nice curves). It comes with a natural morphism $\pi : \tilde{X} \to X$ which is an isomorphism away from X_{sing}.

The picture is as follows:



Remark 3.8. Locally in some affine $U = \text{Spec}(A) \subseteq X$, the irreducible components which intersect U correspond to the minimal prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_r$ of A. Then $\tilde{U} = \pi^{-1}(U)$ is

$$\text{Spec}\left(\prod_{i=1}^{r} \widetilde{A/\mathfrak{p}_i}\right),$$

where $\widetilde{A/\mathfrak{p}_i}$ is the integral closure of $A/\mathfrak{p}_i$ in its field of fractions. The morphism π is given by the natural inclusion of A into the direct product.

To measure 'how singular' X is, we measure the difference between X and its normalisation $\tilde{X}$. This is done by considering the short exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \pi_*\mathcal{O}_{\tilde{X}} \longrightarrow \mathcal{S} \longrightarrow 0 \tag{3.9}$$

with $\mathcal{S}$ defined by the sequence. Since π is an isomorphism away from X_{sing} it's a skyscraper sheaf supported on X_{sing}.

Definition 3.10. For $x \in X$ a closed point, we define

$$\delta_x := \dim_k \mathcal{S}_x = \dim_k \widetilde{\mathcal{O}_{X,x}}/\mathcal{O}_{X,x}$$

where here $\widetilde{\mathcal{O}_{X,x}}$ is the product of the normalisations of $\mathcal{O}_{X,x}/\mathfrak{p}_i$ where the $\mathfrak{p}_i$ are the minimal prime ideals of $\mathcal{O}_{X,x}$; they correspond to the irreducible components of X

passing through x. We note that x is smooth if and only if $\delta_x = 0$. We also define $m_x := \#\pi^{-1}(x)$. We say that x is a *ordinary double point*, or a *node*, if $m_x = 2$ and $\delta_x = 1$.

Remark 3.11. One can show that $x \in X$ is an ordinary double point if and only if the completed local ring at x is isomorphic to $k[[u, v]]/(uv)$. That is, the completed local ring is isomorphic to the completed local ring at the origin of the curve given by the two coordinate axes in $\mathbb{A}^2$. This is the picture of what an ordinary double point looks like to have in mind.

Example 3.12 (Plane curves)**.** Let X be an affine plane curve given by an equation $\{f(x, y) = 0\} \subseteq \mathbb{A}^2$ and suppose that $(0, 0) \in X$. Then we can write

$$f(x, y) = a_1x + a_2y + b_1x^2 + b_2xy + b_3y^2 + ...$$

Then $(0, 0)$ is a singular point of X if and only if $a_1 = 0 = a_2$, and an ordinary double point if and only if the discriminant

$$b_2^2 - 4b_1bb_3$$

of the quadratic term is non-zero.

Remark 3.13. The structure of a singular point is a local property so if $x \in X$ has an open neighbourhood isomorphic to an open neighbourhood of a plane curve then we can still use the above example.

Definition 3.14. We say that X is *semistable* if (it is reduced and) all its singular points are ordinary double points. If k is no longer assumed algebraically closed, we say that a curve X/k is *semistable* if X if $X_{\bar{k}}$ is semistable.

Example 3.15. If $E/\mathbb{Q}_p$ is an elliptic curve, and $\bar{E}/\mathbb{F}_p$ is the reduction of its minimal Weierstrass equation, then the example above shows that $\bar{E}$ is semistable if and only if E has good or multiplicative reduction.

Example 3.16. Let $C : y^2 = f(x)$ be a possibly singular 'hyperelliptic' curve over k where $\deg(f) > 2$ and $\mathrm{char}(k) \neq 2$. Then C is semistable if and only if $f(x)$ has no roots of multiplicity higher than 2.

A slight refinement of the notion of a semistable curve is a stable curve.

Definition 3.17 (Stable curves)**.** If $k = \bar{k}$, we say that X is *stable* if it is semistable and if X has arithmetic genus at least 2, and any irreducible component of X isomorphic to $\mathbb{P}^1_k$ intersects the other irreducible components in a least 3 points. For general k, we say that X is stable if $X_{\bar{k}}$ is.

Remark 3.18. Equivalently, a semistable curve over an algebraically closed field is stable if and only if its automorphism group is finite.

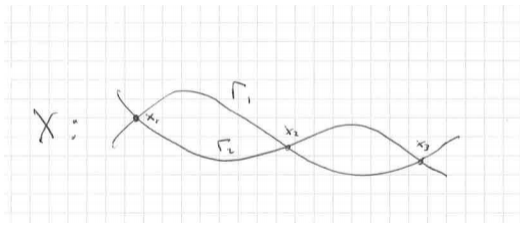
3.4. The dual graph of a semistable curve. A useful invariant of a semistable curve (as we will see later) is its dual graph, which is defined as follows.

Definition 3.19 (Dual graph)**.** Let $k = \bar{k}$ and X be a semistable curve over k. We define the *dual graph* of X to be the graph whose vertices are the irreducible components of X, and such that vertices v_1 and v_2 (where $v_1 = v_2$ is allowed) are joined by one edge for each singular point lying on both of the corresponding irreducible components. Note that loops and multiple edges are allowed.

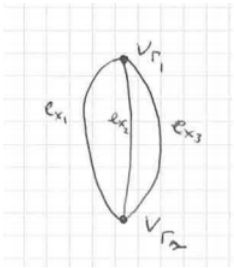
Example 3.20. Suppose $\mathrm{char}(k) \neq 2$ and consider the singular hyperelliptic curve

$$y^2 = x^2(x-1)^2(x+1)^2.$$

This consists of two irreducible components intersecting in 3 (ordinary double) points.



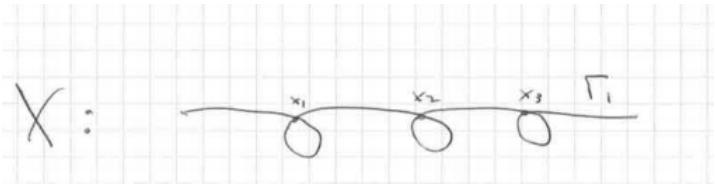
Its dual graph is the 'banana graph':



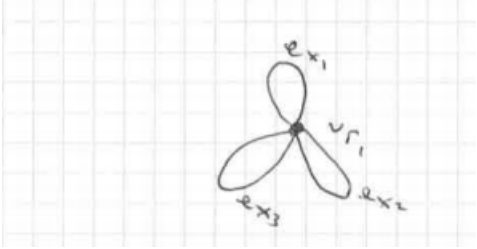
Example 3.21. Suppose now that $\mathrm{char}(k) \neq 2, 3$ and consider the singular hyperelliptic curve

$$y^2 = x^2(x-1)^2(x+1)^2(x-2).$$

Now this consists of one irreducible component with 3 nodes on it.



Its dual graph is:



3.5. Semistable models. We now return to the case where K is a finite extension of $\mathbb{Q}_p$ and C/K is a nice curve. We say C has *semistable reduction* over K if there is a model $\mathcal{C}/\mathcal{O}_K$ for C whose special fibre is a semistable curve over the residue field k. We call such a model a *semistable model* for C. If additionally the special fibre of $\mathcal{C}$ is stable we call this a *stable model*.

Whilst it's not true that all curves admit semistable models (cf. elliptic curves with additive reduction) the power of the theory of semistable models lies in the following deep result of Deligne–Mumford.

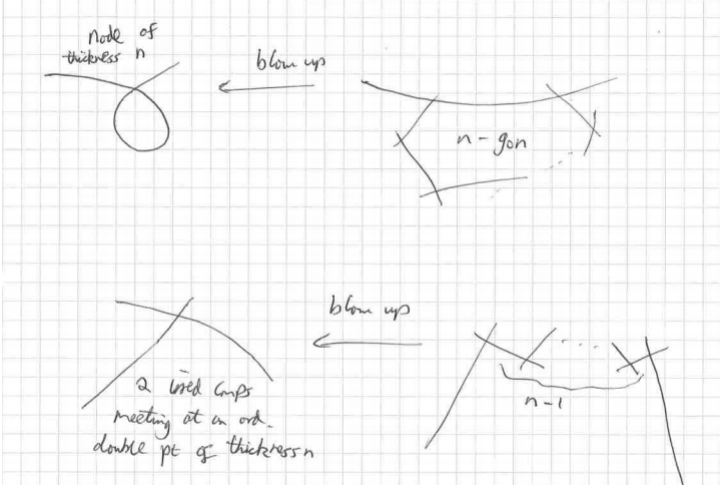
Theorem 3.22 (Semistable reduction theorem)**.** *Let C/K be a nice curve. Then there is a finite extension L/K such that C has semistable reduction over K.*

A slight refinement which follows fairly quickly from this is:

Proposition 3.23. *Let C/K be a nice curve of genus at least 2 and L/K any finite extension where C has semistable reduction. Then C has a stable model $\mathcal{C}$ over $\mathcal{O}_L$ which is unique up to $\mathcal{O}_L$-isomorphism. Moreover, if F/L is a further finite extension, then $\mathcal{C} \times_{\mathcal{O}_L} \mathcal{O}_F$ is the stable model of C over F.*

In particular, we can talk about *the* stable reduction of C.

3.6. Relationship between the stable model and the minimal regular model. In general, if (K is a finite extension of $\mathbb{Q}_p$ and) C/K is a semistable curve, its minimal regular model is readily obtained from its stable model by some simple blow ups. To explain this, let $\mathcal{C}/\mathcal{O}_K$ be the stable model of C. If a closed point $x \in \mathcal{C}$ is non-regular then it is necessarily a singular point of the special fibre, and hence corresponds to an ordinary double point on the special fibre $\bar{\mathcal{C}}$. If we assume that both x and the two points lying over x in the normalisation of $\bar{\mathcal{C}}$ are defined over k, it follows formally from the fact that the completed local ring at $x \in \bar{\mathcal{C}}$ is isomorphic to $k[[u,v]]/(uv)$, that the completed local ring at $x \in \mathcal{C}$ is isomorphic to $\mathcal{O}_K[[u,v]]/(uv-c)$ for some $c \in \mathcal{O}_K$ of valuation ≥ 1. The valuation of c, say n, is called the *thickness* of the ordinary double point. One sees that x is a regular point of $\mathcal{C}$ if and only if $n = 1$. When $n > 1$ one can repeatedly blow up at x to resolve the singularity. If this is done minimally, the result is given by replacing x by a chain of $n-1$ copies of the projective line, each intersecting transversally. See [Liu02, Corollary 10.3.25] and the surrounding discussion for more details. The picture is as follows:



In general, the condition that x and the points over it in the normalisation be defined over k is always satisfied after finite extension of k. If one then follows the above procedure at every ordinary double point of $\bar{\mathcal{C}}$ this yields the minimal regular model of C/K. Since the minimal regular model commutes with unramified extension, we can always make an unramified extension of K to make this true. As a corollary we find:

Corollary 3.24. *If C/K has semistable reduction its minimal regular model is a semistable model for C.*

4. Exercises for lecture 2

4.1. Justify Example 3.12: let X be an affine plane curve over an algebraically closed field k, given by an equation $\{f(x,y)=0\} \subseteq \mathbb{A}^2$ and suppose that $(0,0) \in X$. Write

$$f(x,y) = a_1x + a_2y + b_1x^2 + b_2xy + b_3y^2 + ...$$

Show that $(0,0)$ is a singular point of X if and only if $a_1 = 0 = a_2$. Supposing $(0,0)$ is singular, compute the completed local ring at $(0,0)$ in the case that the discriminant

$$b_2^2 - 4b_1b_3$$

of the quadratic term is non-zero, and deduce that $(0,0)$ is an ordinary double point.

4.2. Let k be an algebraically closed field. The *aritmetic genus* $p_a(X)$ of a (projective, reduced, connected) curve X/k is defined to be the k-dimension of $H^1(X, \mathcal{O}_X)$. Show that if X is semistable then

$$p_a(X) = \#\text{edges of } \mathcal{G} - \#\text{vertices of } \mathcal{G} + 1 + \sum_{\Gamma \text{ irred comp of } X} g(\tilde{\Gamma})$$

where $\mathcal{G}$ is the dual graph of X, and $g(\tilde{\Gamma})$ denotes the genus of the normalisation of Γ.

(One can rewrite the sum #edges of $\mathcal{G}$ − #vertices of $\mathcal{G}$ + 1 as the rank of the first homology group $H_1(\mathcal{G}, \mathbb{Z})$ of $\mathcal{G}$.)

4.3. Let p be odd and $C/\mathbb{Q}_p : y^2 = f(x)$ be a hyperelliptic curve where $f(x)$ is monic and has coefficients in $\mathbb{Z}_p$. Suppose that the discriminant of $f(x)$ has p-adic valuation 1. Show that the scheme over $\mathbb{Z}_p$ given by glueing the usual charts

$$\text{Spec } \mathbb{Z}_p[x,y]/(y^2 - f(x))$$

and

$$\text{Spec } \mathbb{Z}_p[w,z]/(z^2 - w^{2g+2}f(1/w))$$

via $x = 1/w$ and $y = w^{g+1}z$ gives both a regular[4] and semistable model of C (in particular, this is the minimal regular model of C).

[4]By definition, a scheme X is regular if for each $x \in X$ the local ring $\mathcal{O}_{X,x}$ at x is regular, i.e. if its dimension is equal to the $\mathcal{O}_{X,x}/\mathfrak{m}_x$-dimension of $\mathfrak{m}_x/\mathfrak{m}_x^2$, where $\mathfrak{m}_x$ is the maximal ideal of $\mathcal{O}_{X,x}$. To check regularity it suffices to check this for x a closed point.

5. Lecture 3: Semistable models of hyperelliptic curves and Néron models of abelian varieties

5.1. Semistable models of hyperelliptic curves: introduction. Again, K is a finite extension of $\mathbb{Q}_p$, ring of integers $\mathcal{O}_K$, residue field k. The aim of this lecture is to give some examples of computing the (potential) stable reduction of curves. Our examples will come from hyperelliptic curves over finite extensions of $\mathbb{Q}_p$ with p odd. We will just state the results rather than giving proofs, but the idea is as follows. By definition a hyperelliptic curve comes equipped with a degree 2 morphism $\phi : C \to \mathbb{P}^1_K$. Let B be the branch locus of this morphism, i.e. the points of $\mathbb{P}^1_K$ above which this map ramifies. If C is given by an equation $y^2 = f(x)$ then the map ϕ is projection to the x coordinate and B is the collection of roots of $f(x)$, along with the point at infinity if $f(x)$ has odd degree. The scheme $\mathbb{P}^1_{\mathcal{O}_K}$ gives a regular proper semistable model of $\mathbb{P}^1_K$. Taking the closure of B in $\mathbb{P}^1_{\mathcal{O}_K}$ gives a divisor on $\mathbb{P}^1_{\mathcal{O}_K}$. The idea is to blow up at closed points on the special fibre of $\mathbb{P}^1_{\mathcal{O}_K}$ to gradually improve this divisor. At any stage of this process we may take the normalisation of the resulting model of $\mathbb{P}^1_K$ in $K(C)$. This will give a model of C and, if the new divisor is sufficiently nice, will be regular/semistable/stable (of course, the last two will in general need an extension of K).

This approach works more generally to produce (potential) stable models of cyclic covers of the projective line (for residue characteristic different from the degree of the cover) and has been described algorithmically for superelliptic curves by Bouw–Wewers in [BW17]. See https://pypi.org/project/mclf/ for a sage implementation in certain cases. The particular framework described below is set out in [DDMM18], although we make several simplyfying assumptions.

5.2. Setup. Take p to be odd. Let π_K be a uniformiser for K and denote by $v : K^\times \to \mathbb{Z}$ the normalised valuation. Let $C : y^2 = f(x)$ be a hyperelliptic curve over K of genus $g \geq 2$, so that $f(x)$ is a squarefree polynomial of degree at least 5. We will describe the stable model of C (possibly over an extension of K) by describing both the dual graph, and the normalisation of each irreducible component, of its special fibre. The answer will be in terms of the combinatorial data set out below.

5.3. Clusters. Denote by $\mathcal{R}$ the set of roots of $f(x)$, and c_f the leading coefficient of $f(x)$, so that C has equation

$$C : y^2 = c_f \prod_{r \in \mathcal{R}} (x - r).$$

Assumption 5.1. We assume:

(1) The set of roots $\mathcal{R}$ is contained in K. If this is not the case we simply replace K by a finite extension for which this does hold.
(2) We assume that $|\mathcal{R}| = 2g + 1$. Given (1) this can be achieved by a change of variables sending a point $(r, 0)$ (r a root of $f(x)$) to infinity.

Definition 5.2. A *cluster* is a nonempty subset of $\mathcal{R}$ cut out by a disc. That is, a nonempty subset of the form

$$\mathfrak{s} = \{r \in \mathcal{R} \mid v(r-z) \geq n\}$$

for some $z \in K$ and $n \in \mathbb{Z}$ (note that if we wish we can without loss of generality take z to be a root of $f(x)$). If $\mathfrak{s}$ is a cluster of size at least 2 then amongst all such pairs (z,n) 'cutting out' $\mathfrak{s}$, the maximal n is called the *depth* of $\mathfrak{s}$, denoted $d_{\mathfrak{s}}$.

Note that $\mathcal{R}$ and each singleton $\{r\}$ for $r \in \mathcal{R}$ are clusters.

Example 5.3. Consider the hyperelliptic curve over $\mathbb{Q}_p$ with equation

$$C : y^2 = x(x-p)(x-p^3)(x+p^3)(x-1)(x-1-p^2)(x-1+p^2).$$

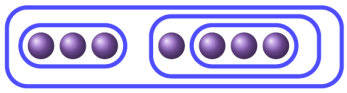
Then

$$\mathcal{R} = \{1, 1+p^2, 1-p^2, p, 0, p^3, -p^3\}.$$

The clusters of size at least 2 are

$$\mathcal{R},\ \{1, 1+p^2, 1-p^2\},\ \{p, 0, p^3, -p^3\},\ \text{and}\ \{0, p^3, -p^3\}.$$

Their depths are 0, 2, 1 and 3 respectively. It's convenient to represent this in the *cluster picture* shown below



Assumption 5.4. We make one last simplifying assumption on C.

- Assume that there is no cluster of size $2g$.

This can also always be satisfied after a suitable change of variables (potentially after an appropriate additional field extension), but will not go into this. At any rate, it only serves to eliminate special cases in the forthcoming statement.

Notation 5.5. We also introduce the following terminology:

- if $\mathfrak{s}' \subsetneq \mathfrak{s}$ is a maximal subcluster we say that $\mathfrak{s}'$ is a *child* of $\mathfrak{s}$ and that $\mathfrak{s}$ is the *parent* of $\mathfrak{s}'$. We denote this as $\mathfrak{s}' < \mathfrak{s}$ and write $\mathfrak{s} = P(\mathfrak{s}')$.
- a cluster $\mathfrak{s}$ is called a *twin* if $|\mathfrak{s}| = 2$.
- a cluster $\mathfrak{s}$ is *odd* if $|\mathfrak{s}|$ is odd, *even* if $|\mathfrak{s}|$ is even, and *übereven* if each child of $\mathfrak{s}$ is even.

A convenient way of representing the information encoded in the clusters is in the following finite tree.

Definition 5.6 (The tree $\mathcal{T}_C$)**.** Let $\mathcal{T}_C$ be the finite tree with

- one vertex $v_{\mathfrak{s}}$ for each cluster of size at least 3, coloured yellow if $\mathfrak{s}$ is übereven and blue otherwise,
- an edge from $v_{\mathfrak{s}}$ to $v_{P(\mathfrak{s})}$ for each cluster $\mathfrak{s} \neq \mathcal{R}$, coloured blue if $\mathfrak{s}$ is odd, and coloured yellow if $\mathfrak{s}$ is even.

5.4. The stable model. In the situation of the previous subsection the following proposition describes the (special fibre of the) stable model of C.

Proposition 5.7. *We have:*

(i) *The curve C/K is semistable if and only if, for each cluster $\mathfrak{s}$ of size at least 3, the quantity*

$$\nu_{\mathfrak{s}} = v(c_f) + |\mathfrak{s}|d_{\mathfrak{s}} + \sum_{r \notin \mathfrak{s}} v(z_{\mathfrak{s}} - r)$$

is even, where here $z_{\mathfrak{s}}$ is any element of $\mathfrak{s}$.

Suppose now that C/K is semistable.

(ii) *Let $\mathcal{G}_C$ be the graph given by (in order)*
- *taking two disjoint copies of $\mathcal{T}_C$ and glueing them along their common blue parts,*
- *for each twin $\mathfrak{s}$, adding a loop to the unique vertex of $\mathcal{G}_C$ over $v_{P(\mathfrak{s})}$ if $P(\mathfrak{s})$ is not übereven, and adding an edge joining the two vertices of $\mathcal{G}_C$ over $v_{P(\mathfrak{s})}$ if $P(\mathfrak{s})$ is übereven.*

Then the special fibre of the stable model of C has dual graph $\mathcal{G}_C$.

(iii) *The normalisation of the component $\Gamma_{\mathfrak{s}}$ corresponding to a vertex $v_{\mathfrak{s}}$ of $\mathcal{G}_C$ is the hyperelliptic curve over k with equation*

$$\Gamma_{\mathfrak{s}} : y^2 = c_{\mathfrak{s}} \prod_{\text{odd } \mathfrak{o} < \mathfrak{s}} (x - \mathrm{red}_{\mathfrak{s}}(\mathfrak{o}))$$

where $c_{\mathfrak{s}} \in k^\times$ is given by

$$c_{\mathfrak{s}} = \frac{c_f}{\pi^{v(c_f)}} \prod_{r \notin \mathfrak{s}} \frac{z_{\mathfrak{s}} - r}{\pi^{v(z_{\mathfrak{s}} - r)}} \pmod{\pi_K}$$

for $z_{\mathfrak{s}}$ any element of $\mathfrak{s}$, and

$$\mathrm{red}_{\mathfrak{s}}(\mathfrak{o}) = \frac{z_{\mathfrak{o}} - z_{\mathfrak{s}}}{\pi^{d_{\mathfrak{s}}}} \pmod{\pi_K}$$

for $z_{\mathfrak{o}}$ any element of $\mathfrak{o}$.

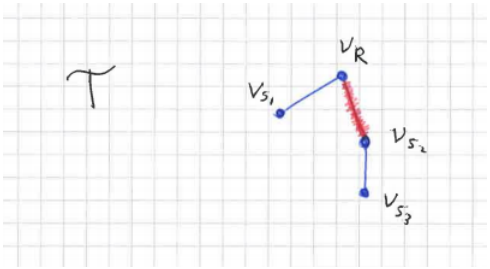
Remark 5.8. The condition that $\nu_{\mathfrak{s}}$ be even for all clusters $\mathfrak{s}$ of size at least 3 is automatically satisfied if K is replaced by a ramified quadratic extension of K.

Remark 5.9. If $\mathfrak{s}$ is an übereven cluster then there are two vertices in $\mathcal{G}_C$ lying over the vertex $v_{\mathfrak{s}}$ of $\mathcal{T}_C$. Correspondingly, the equation for $\Gamma_{\mathfrak{s}}$ defines two disjoint projective lines.

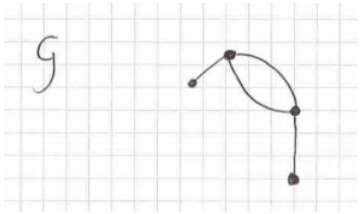
Example 5.10. Returning to Example 5.3 write the clusters as

$$\mathcal{R},\ \mathfrak{s}_1 = \{1, 1+p^2, 1-p^2\},\ \mathfrak{s}_2 = \{p, 0, p^3, -p^3\},\ \text{and } \mathfrak{s}_3 = \{0, p^3, -p^3\}.$$

We compute $\nu_{\mathcal{R}} = 0$, $\nu_{\mathfrak{s}_1} = 3 \cdot 2 + 0 = 6$, $\nu_{\mathfrak{s}_2} = 4 \cdot 1 = 4$ and $\nu_{\mathfrak{s}_3} = 3 \cdot 3 + 1 = 10$ so that $C/\mathbb{Q}_p$ is semistable. The graph $\mathcal{T}_C$ is shown below (with yellow replaced by red due to my lack of a yellow pen):



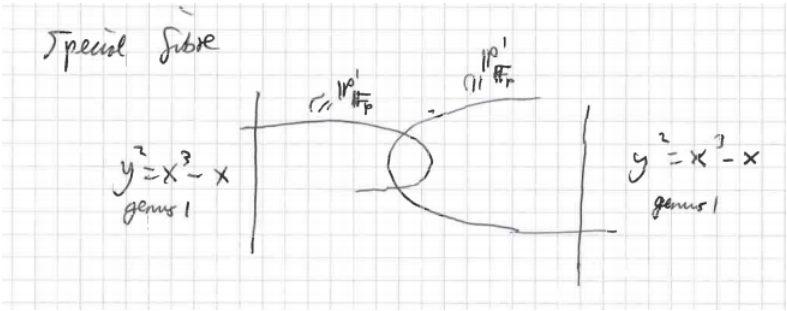
Taking the double cover ramified over the blue part gives the graph $\mathcal{G}_C$ as shown:



Note that the geometric genus of the hyperelliptic curve $\Gamma_{\mathfrak{s}}$ of Proposition 5.7 is the number $g(\mathfrak{s})$ defined by

$$\#\{\text{odd children of } \mathfrak{s}\} \in \{2g(\mathfrak{s})+2, 2g(\mathfrak{s})+1\}.$$

In particular the components corresponding to $\mathcal{R}$ and $\mathfrak{s}_2$ are necessarily isomorphic to $\mathbb{P}^1$. One easily computes from Proposition 5.7 (iii) that the two remaining components are both given by the equation $y^2 = x^3 - x$ and have genus 1. The final picture is as follows:



5.5. The minimal regular model of a semistable hyperelliptic curve. In the contex of Proposition 5.7 we can additionally describe the thickness of each node in terms of the clusters and hence describe the minimal regular model of a semistable hyperelliptic curve C/K.

Lemma 5.11. *Let $\mathcal{G}_C$ be as in Proposition 5.7 and let e be an edge of $\mathcal{G}_C$ corresponding to clusters $\mathfrak{s} < P(\mathfrak{s})$, where $\mathfrak{s}$ has size at least 2. Writing $\delta_{\mathfrak{s}} = d_{P(\mathfrak{s})} - d_{\mathfrak{s}}$ the thickness*

of the corresponding node is

$$n(e) := \begin{cases} \delta_{\mathfrak{s}}/2 & e \text{ came from a blue edge,} \\ \delta_{\mathfrak{s}} & e \text{ came from a yellow edge,} \\ 2\delta_{\mathfrak{s}} & \mathfrak{s} \text{ a twin.} \end{cases}$$

In particular, the dual graph of the minimal regular model of C is obtained from $\mathcal{G}_C$ by replacing each edge e by a path of length $n(e)$.

Remark 5.12. The condition for semistability in Proposition 5.7 (i) forces $\delta_{\mathfrak{s}}/2 \in \mathbb{Z}$ in the first of the three cases above.

Example 5.13. Returning to Example 5.3 we find that each node has thickness 1, so that the stable model and minimal regular model coincide.

5.6. The Néron model of an abelian variety. We now change tack completely and move on from models of curves to models of abelian varieties. It turns out that for an abelian variety there is always a canonical 'best model', the Néron model. As usual, let K be a finite extension of $\mathbb{Q}_p$ (for p arbitrary now). The standard reference for Néron models is the book [BLR90].

Theorem 5.14. *Let A/K be an abelian variety. Then there exists a smooth*[5]*, separated, finite type group scheme $\mathcal{A}/\mathcal{O}_K$ with generic fibre A, satisfying the universal property (the* Néron mapping property*):*

for each smooth $\mathcal{O}_K$-scheme $\mathcal{Y}$, any K-morphism $\mathcal{Y}_K \to A$ extends uniquely to an $\mathcal{O}_K$-morphism $\mathcal{Y} \to \mathcal{A}$. We call $\mathcal{A}$ the Néron model *of A.*

Example 5.15. Let E/K be an elliptic curve with good reduction. Then the minimal Weierstrass equation for E gives the Néron model of E.

Remark 5.16. Note that, unlike for curves, we have dropped properness in favour of smoothness, although the Néron mapping property forces a weak version of the valuative criterion for properness. In fact, the Néron model is proper if and only if its special fibre is an abelian variety over k.

Definition 5.17. The *reduction* of an abelian variety over K is the group variety $\mathcal{A}_k = \mathcal{A} \times_{\mathcal{O}_K} k$ over k. If this is an abelian variety then we say that A/K has *good reduction.* The *identity component* of the Néron model, denoted $\mathcal{A}^0$, is the open subscheme whose special fibre is the connected component of the identity $(\mathcal{A}_k)^0$ of $\mathcal{A}_k$ (i.e. remove the closed subset consisting of the union of the (finitely many) components of the special fibre not containing the identity element).

Remark 5.18. Note that the Néron mapping property gives $A(K) = \mathcal{A}(\mathcal{O}_K)$ giving us a reduction homomorphism $A(K) \to \mathcal{A}_k(k)$. We write $A_0(K)$ for the points reducing to $\mathcal{A}_k^0(k)$. The group $A(K)/A_0(K)$ is finite and we define the *Tamagawa number* $c(A/K)$

[5]We take as our definition that a morphism $f : Y \to Z$ is *smooth* if it is flat and if each fibre $Y \times_Z k(z)$ $(z \in Z)$ is geometrically regular.

to be its order. Alternatively, if one defines $\Phi := \mathcal{A}_k/\mathcal{A}_k^0$ (a finite etale group scheme over k) then one has

$$c(A/K) = \Phi(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}.$$

5.7. Neron models of Jacobians. Often, one can use the existence of the Néron model as a black box, and prove everything via the universal property. However, from a computational viewpoint this is not that satisfactory. For Jacobians however the situation is quite good since it turns out that the models of curves we have been working with are quite closely related to the Néron model of the Jacobian of their generic fibre. A precise result is as follows.

Theorem 5.19. *Let C/K be a nice curve. Suppose that either*

- *$\mathcal{C}/\mathcal{O}_K$ is a semistable model of C,*

or

- *$\mathcal{C}/\mathcal{O}_K$ is a regular model for C and the greatest common divisor of the multiplicities of the irreducible components of the special fibre of $\mathcal{C}$ is 1.*

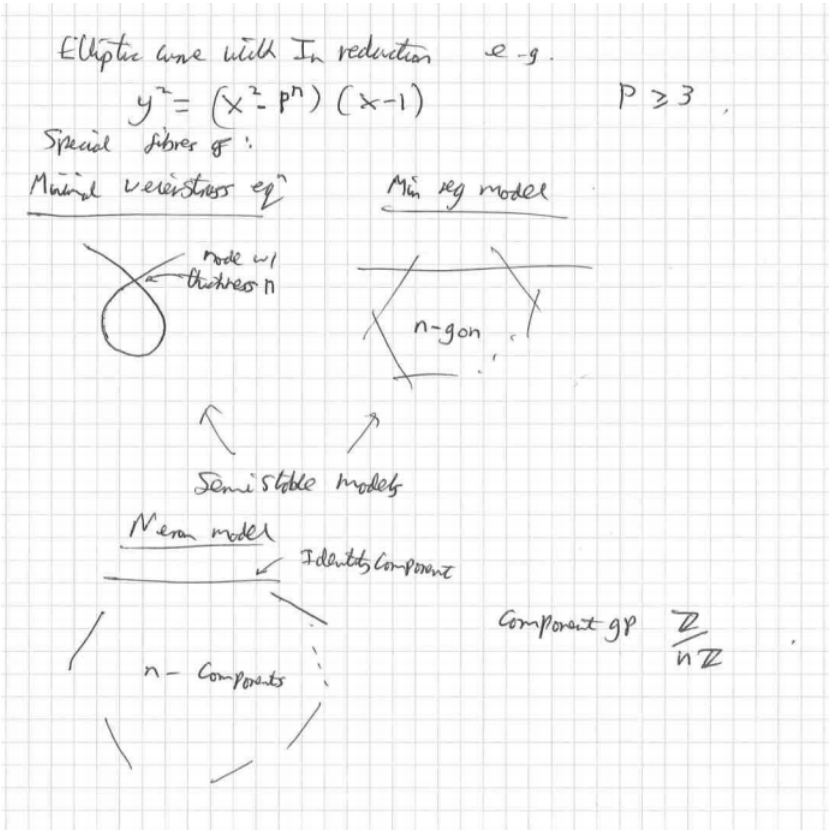
Then $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_K}$ is canonically isomorphic to the identity component of the Neron model of the Jacobian of C. (The map is by extending the one on the generic fibre).

Proof. The first part is [BLR90, Theorem 9.5.4 (b)] whilst op. cit. Corollary 9.7.2 is the second part. □

Corollary 5.20. *Let C/K be a nice curve and let $\mathcal{C}/\mathcal{O}_K$ be a model satisfying one of the two cases in Theorem 5.19. Then the special fibre of the identity component of the Néron model of the Jacobian of C is $\mathrm{Pic}^0_{\mathcal{C}_k/k}$. In particular, if C has good reduction and $\mathcal{C}$ is a model for C with nice special fibre, then the special fibre of the Néron model of the Jacobian of C is the Jacobian of the special fibre of $\mathcal{C}$.*

Remark 5.21. The component group, and hence Tamagawa number, can be understood via [BLR90, Theorem 9.6.1] but this needs a regular model.

5.8. Néron models of elliptic curves. We close this section by discussing the situation for elliptic curves. Either by showing that it satisfies the Néron mapping property, or from Raynaud's theorem, it follows that the Néron model of an elliptic curve is the smooth part of its minimal regular model. In particular it follows e.g. from Tate's algorithm that the identity component of the Neron model is the smooth part of the minimal Weierstrass model. We have the following picture for an elliptic curve with type I_n reduction:


Elliptic curve with I_n reduction e.g.
$y^2 = (x^2 - p^n)(x-1)$
$p \geq 3$.
Special fibres of:
Minimal weierstrass eq^n
Min reg model
node w/ tangents
n-gon
Semistable models
Neron model
Identity Component
n - Components
Component gp $\frac{\mathbb{Z}}{n\mathbb{Z}}$

6. Exercises for Lecture 3

6.1. Let $p > 3$ be a prime and $C/\mathbb{Q}_p$ the hyperelliptic curve

$$C : y^2 = x(x-p)(x-2p)(x-3p)(x-1)(x-1+p)(x-2).$$

Show that $C/\mathbb{Q}_p$ has semistable reduction, compute the dual graph of its special fibre, and the normalisations of each of the components.

6.2. Find a curve $C/\mathbb{Q}_5$ which has semistable reduction, and such that the special fibre of its stable model consists of two elliptic curves meeting at a single point.

6.3. Let K be a finite extension of $\mathbb{Q}_p$, ring of integers $\mathcal{O}_K$, residue field k. Let C/K be a semistable curve, $\mathcal{C}/\mathcal{O}_K$ its minimal regular model, and $\mathcal{G}$ the dual graph of (the base change to $\bar{k}$ of the special fibre of) $\mathcal{C}$. Let L/K be a field extension of ramification degree e, and let $\mathcal{C}'$ and $\mathcal{G}'$ denote the corresponding objects over L. Show that $\mathcal{G}'$ is obtained from $\mathcal{G}$ by replacing each edge with a path of length e.

7. Lecture 4: Describing the Tate module of Jacobians

Let K be a finite extension of $\mathbb{Q}_p$ and C/K a nice curve. Our aim is to understand the l-adic Tate module of $\mathrm{Jac}(C)$ for $l \neq p$. We consider the case where C/K is semistable, although the general case can be deduced from this by keeping careful track of the action of the Galois group of some (Galois) extension over which C attains semistable reduction. Note that by the semistable reduction theorem, for general C this still describes the restriction of the Tate module to a finite index subgroup of G_K.

7.1. Semistable abelian varieties. As well as a notion of semistability for curves there is a corresponding notion of semistability for abelian varieties.

Definition 7.1 (Semistable abelian varieties)**.** Let A/K be an abelian variety and $\mathcal{A}/\mathcal{O}_K$ its Néron model. We say that A has *semistable reduction* over K if the special fibre $A_{\bar{k}}$ of $\mathcal{A}$ is an extension of an abelian variety by a torus. In the special case where $A_{\bar{k}}$ is an abelian variety we say that A has *good reduction*.

Example 7.2. An elliptic curve is semistable precisely when it has good or multiplicative reduction.

Remark 7.3. For the Jacobian $\mathrm{Jac}(C)$ of a nice curve of genus at least 2, one can show that $\mathrm{Jac}(C)$ is semistable if and only if C is. We'll (almost) see how to prove the implication 'C semistable $\Rightarrow$ $\mathrm{Jac}(C)$ semistable' later in this lecture (see Remark 7.15).

Remark 7.4. As for elliptic curves, the Néron–Ogg–Shafarevich criterion states that A has good reduction if and only if $T_l(A)$ is unramified for some l different from the residue characteristic of K. Similarly, one can show that A has semistable reduction if and only if the inertia group I_K acts unipotently on $T_l(A)$.

Remark 7.5. Even when A/K is semistable the Néron model still does not commte with ramified base change (consider an elliptic curve with multiplicative reduction - the order of its component group gets multiplied by the ramification degree) but it is true at least that when A/K is semistable then the identity component of the Néron model commutes with base change. For Jacobians of curves this follows from the corresponding fact for the stable model, along with Theorem 5.19.

7.2. The Tate module of an abelian variety.

7.2.1. *Abelian varieties with good reduction.* Let A/K be an abelian variety with good reduction and let $\mathcal{A}/\mathcal{O}_K$ be its Néron model. Then its special fibre $\bar{\mathcal{A}}$ is an abelian variety over k of dimension g also. For any $l \neq \mathrm{char}(k)$ we have

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

On the other hand (since Néron models commute with unramified base change) we have a reduction map

$$A(K^{\mathrm{nr}})[l^n] \to \bar{\mathcal{A}}[l^n]$$

which is surjective by Hensel's lemma. Simply by counting we deduce that $A[l^n] \subseteq A(K^{\mathrm{nr}})$ (i.e. all l-power torsion in unramified) and that reduction gives an isomorphism $A[l^n] \cong \bar{\mathcal{A}}[l^n]$. In particular, $T_l(A)$ is unramified and we have a canonical isomorphism

$$T_l(A) \cong T_l(\bar{\mathcal{A}}) \tag{7.6}$$

which is equivariant for the action of $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \mathrm{Gal}(\bar{k}/k)$.

In particular, if $A = \mathrm{Jac}(C)$ is the Jacobian of a nice curve C, and C has good reduction (in general this is strictly stronger than $\mathrm{Jac}(C)$ having good reduction) then we have a canonical isomorphism

$$T_l(\mathrm{Jac}(C)) \cong T_l(\mathrm{Jac}(\bar{\mathcal{C}})) \tag{7.7}$$

equivariant for the action of $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \mathrm{Gal}(\bar{k}/k)$, where here $\mathcal{C}$ is the model of C realising the good reduction. This means that the local L-polynomial of $\mathrm{Jac}(C)$ is completely determined by the action of Frobenius on $H^1_{\mathrm{et}}(\bar{\mathcal{C}}_{\bar{k}}, \mathbb{Z}_l)$, and this may be understood by the Weil conjectures in terms of the number of points on $\bar{\mathcal{C}}$ over finite extensions of k. See Andrew Sutherland's course for more on this.

Remark 7.8. An alternative viewpoint of (7.7) is that it follows as a special case of the smooth and proper base change theorems in étale cohomology applied to the scheme $\mathcal{C}/\mathcal{O}_K$ (which is smooth and proper over $\mathcal{O}_K$ under our good reduction assumption).

7.2.2. *Semistable abelian varieties.* We now move on to the case where A/K has semistable but not necessarily good reduction. It turns out, though it is harder to prove, that the analogue of (7.6) is that there is a $\mathrm{Gal}(K^{\mathrm{nr}}/K) = \mathrm{Gal}(\bar{k}/k)$ equivariant isomorphism

$$T_l(A)^{I_K} \cong T_l(\bar{\mathcal{A}}^0) \tag{7.9}$$

where here I_K denotes the inertia group of K. In fact, this holds in general without the assumption that A/K is semistable though we will not persue that further.

7.3. The Picard group of semistable curves. In light of (7.9), we want to describe $T_l(\bar{\mathcal{A}}^0)$ in the case that $A = \mathrm{Jac}(C)$ is the Jacobian of a nice curve C/K. Supposing that C/K is semistable, by Theorem 5.19 we have $T_l(\bar{\mathcal{A}}^0) = T_l(\mathrm{Pic}^0(\bar{\mathcal{C}}))$ where $\mathcal{C}/\mathcal{O}_K$ is the stable model of C. It is this group which we now describe. We begin by describing the Picard group of an arbitrary semistable curve X over an algebraically closed field.

It will be convenient to begin with a slight refinement of the definition of the dual graph.

Definition 7.10 (Dual graph, take two)**.** As usual, let $\pi : \tilde{X} \to X$ be the normalisation morphism and write

- S = set of singular (ordinary double) points of X,
- T = set of connected components of $\tilde{X}$,
- R = $\pi^{-1}(\mathcal{S})$; this comes with two canonical maps
  - $\phi : R \to S$, $P \mapsto \pi(x)$,
  - $\psi : R \to R$, $P \mapsto$ component of $\tilde{X}$ on which x lies.

The dual graph $\mathcal{G}$ of X has vertex set T and edge set S. R is thought of as the set of edge endpoints, and the maps ϕ and ψ specify adjacency. Note that a graph automorphism of $\mathcal{G}$ (which we allow to permute multiple edges and swap edge endpoints) is precisely the data of bijections $R \to R$, $S \to S$ and $T \to T$ that commute with ϕ and ψ.

The following proposition reduces understanding the Tate module $T_l\mathrm{Pic}^0(X)$ associated to a semistable curve, to understanding the Tate module of the Jacobians of the normalisations of its irreducible components, along with the (co)homology group of its dual graph.

Proposition 7.11. *Let X be a semistable curve over $k = \bar{k}$ and $\mathcal{G}$ its dual graph. Then for each prime $l \neq \mathrm{char}(k)$ we have an exact sequence*

$$0 \longrightarrow H^1(\mathcal{G}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_l(1) \longrightarrow T_l\mathrm{Pic}^0(X) \longrightarrow \prod_{\Gamma \in \mathcal{J}} T_l(\mathrm{Jac}(\Gamma)) \longrightarrow 0$$

where $H^1(\mathcal{G}, \mathbb{Z})$ denotes the first singular cohomology group[6] of the graph $\mathcal{G}$.

Proof (sketch). We consider (3.9) where we replace the structure sheaf with the invertible elements of the structure sheaf. Thus we obtain

$$0 \longrightarrow \mathcal{O}_X^\times \longrightarrow \pi_*(\mathcal{O}_{\tilde{X}}^\times) \longrightarrow \mathcal{F} \longrightarrow 0$$

where again $\mathcal{F}$ is defined by the sequence and is a skyscraper sheaf supported on X_{sing}. The associated sequence for cohomology gives

$$0 \longrightarrow \mathcal{O}_X^\times(X) \longrightarrow \mathcal{O}_{\tilde{X}}^\times(X) \longrightarrow \mathcal{F}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \prod_{\Gamma \in T} \mathrm{Pic}(\Gamma) \longrightarrow 0.$$

Now $\mathcal{O}_X^\times(X) = k^\times$ since X is proper and connected, whilst $\mathcal{O}_{\tilde{X}}^\times(X) = (k^\times)^S$ (functions from S to $k^\times$), and the map $\mathcal{O}_X^\times(X) \longrightarrow \mathcal{O}_{\tilde{X}}^\times(X)$ sends an element of $k^\times$ to the constant function with this value. On the other hand, $\mathcal{F}(X) = \oplus_{x \in S} \mathcal{F}_x$ and using the fact that each element of S is an ordinary double point we find that

$$\mathcal{F}(X) = \mathrm{coker}\left((k^\times)^S \xrightarrow{\phi^*} (k^\times)^R\right)$$

where ϕ^* is pullback of functions. Bringing the above discussion together, and restricting to degree 0 line bundles, we have an exact sequence

$$0 \longrightarrow k^\times \xrightarrow{\Delta} (k^\times)^T \xrightarrow{\psi^*} \frac{(k^\times)^R}{\phi^*\left((k^\times)^S\right)} \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \prod_{\Gamma \in T} \mathrm{Jac}(\Gamma)(k) \longrightarrow 0 \tag{7.12}$$

where Δ is the diagonal embedding.

On the other hand, if we write $\mathcal{G} = U \cup V$ where U is the union of open edges and V is the union of small open neighbourhoods of the vertices then Mayer–Vietoris gives

$$0 \longrightarrow H_1(\mathcal{G}, \mathbb{Z}) \longrightarrow \mathbb{Z}^R \xrightarrow{(\phi,\psi)} \mathbb{Z}^S \oplus \mathbb{Z}^T \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{7.13}$$

[6]We view the graph $\mathcal{G}$ as a topological space in the obvious way, by thinking of each edge as an interval on the real line.

since $H_0(U) = \mathbb{Z}^S$, $H_0(V) = \mathbb{Z}^T$, $H_0(U \cap V) = \mathbb{Z}^R$ and all higher homology groups vanish. Applying $\mathrm{Hom}\,(-, \mathbb{Z}_l(1))$ to this sequence, and comparing the result with the sequence of Tate modules obtained from (7.12), gives the result. □

Remark 7.14. If each component of X has arithmetic genus 0, as is the case for the curves of Examples 3.20 and 3.21, then the proposition gives a canonical isomorphism

$$H^1(\mathcal{G}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_l(1) \cong T_l \mathrm{Pic}^0(X).$$

Remark 7.15. The exact sequence (7.12) describes $\mathrm{Pic}^0(X)$ on the level of k-points. However, one can ramp this argument up to give a description of the identity component of the relative Picard functor $\mathrm{Pic}^0_{X/k}$ as an algebraic group. In fact, this shows that $\mathrm{Pic}^0_{X/k}$ is an extension of an abelian variety, namely $\prod_{\Gamma \in \mathcal{I}} \mathrm{Jac}(\Gamma)$, by a torus of dimension equal to the rank of $H_1(\mathcal{G}, \mathbb{Z})$. In particular, this shows that the Jacobian of a semistable curve over a local field has semistable reduction.

7.4. Computation of local factors of L-functions. Now return to the case where K is a finite extension of $\mathbb{Q}_p$, l a prime $\neq p$, and C/K a nice curve with semistable reduction, and denote by J its Jacobian. Fixing a semistable model $\mathcal{C}/\mathcal{O}_K$ for C, and let $\mathcal{G}$ be the dual graph of $\mathcal{C}_{\bar{k}}$. We get as a corollary of the above discussion (the G_k-action on $\mathcal{G}$ coming from the actions on the sets S, T and R above, and Γ denotes an irreducible component of $\mathcal{C}_{\bar{k}}$ and $\widetilde{\Gamma}$ its normalisation):

Corollary 7.16. *Denoting $\tilde{C}_{\bar{k}}$ the normalisation of $\mathcal{C}_{\bar{k}}$, we have a short exact sequence of G_k-modules*

$$0 \longrightarrow H^1(\mathcal{G}, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_l(1) \longrightarrow T_l(J)^{I_K} \longrightarrow \bigoplus_{G_k-\text{orbs of cmps } \Gamma} \mathrm{Ind}_{\mathrm{Stab}(\Gamma)}^{G_k} T_l(\mathrm{Jac}(\widetilde{\Gamma})) \longrightarrow 0.$$

Recall that the local L-polynomial of J/K defined as

$$L(J/K, T) = \det\left(1 - \mathrm{Frob}_K^{-1} T \mid ((V_l J)^\vee)^{I_K}\right).$$

Corollary 7.17. *We have*

$$L(J/K, T) = \det\left(1 - \mathrm{Frob}_K^{-1} T \;\middle|\; H_1(\mathcal{G}, \mathbb{Q}_l) \oplus \bigoplus_{G_k-\text{orbs of cmps } \Gamma} \mathrm{Ind}_{\mathrm{Stab}(\Gamma)}^{G_k} T_l(\mathrm{Jac}(\widetilde{\Gamma}))\right).$$

Proof. The Weil pairing $T_l \times T_l \to \mathbb{Z}_l(1)$ gives

$$T_l(J)^\vee \cong T_l(J)(-1)$$

where the (-1) denotes a Tate twist. Since $\mathbb{Z}_l(1)$ is unramified we can take inertia invariants to find

$$T_l(J)^\vee \cong T_l(J)^{I_K}(-1).$$

It just remains to twist the statement of the above corollary by -1, $\otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and note that

- characteristic polynomials depend only on the semisimplification of a representation
- $H^1(\mathcal{G}, \mathbb{Q}_l)$ and $H_1(\mathcal{G}, \mathbb{Q}_l)$ are isomorphic representations.

□

Example 7.18. As a (very) special case of the above, take an elliptic curve E over K with multiplicative reduction. Take as our semistable model the minimal Weierstrass model, so that its special fibre is a nodal cubic curve. In particular, the Jacobian of the normalisation of the special fibre is (the Jacobian of $\mathbb{P}^1$) 0, and $H_1(\mathcal{G}, \mathbb{Q}_l)$ is isomorphic to $\mathbb{Q}_l$ with G_k acting trivially if E has split multiplicative reduction, and with Frob acting as multiplication by -1 in the case of non-split reduction. Applying the corollary we find

$$L(E,T) = \begin{cases} 1-T & E \text{ has split multiplicative reduction} \\ 1+T & E \text{ has non-split multiplicative reduction.} \end{cases}.$$

8. Exercises for lecture 4

8.1. Let $C/\mathbb{Q}$ be the genus 3 hyperelliptic curve

$$C : y^2 = x\left(x^2 - 2x - 8\right)\left(x^4 - 16x^2 + 100\right).$$

Compute the local factor of the L-function of the Jacobian of C over $\mathbb{Q}_3$.

Hint: for a 'singular hyperelliptic curve' $X : y^2 = f_1(x)f_2(x)^2$ over a field k, where $f_1(x)$ and $f_2(x)$ are coprime square free polynomials, the normalisation $\tilde{X}$ of X is the the curve

$$\tilde{X} : y^2 = f_1(x)$$

and the normalisation map $\pi : \tilde{X} \to X$ is given by

$$\pi(x, y) = (x, yf_2(x)).$$

8.2. For an elliptic curve E having split multiplicative reduction over a local field K, a result of Tate gives an isomorphism

$$E(\bar{K}) \cong \bar{K}^\times / q^{\mathbb{Z}},$$

equivariant for the natural G_K-actions on each side, where $q \in K$ is an element of valuation ≥ 1. Use this to give another proof that the local factor of the L-function of E/K is

$$L(E/K, T) = \begin{cases} 1 - T & E \text{ has split multiplicative reduction} \\ 1 + T & E \text{ has non-split multiplicative reduction.} \end{cases}$$

References

[ACC+18] P. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B. Le Hung, J. Newton, S. Scholze, R. Taylor, and J. Thorne, *Potential automorphy over cm fields*, Preprint **arXiv:1812.09999** (2018).

[BCGP18] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Abelian surfaces over totally realy fields are potentially modular*, Preprint **arXiv:1812.09269** (2018).

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[BW17] Irene I. Bouw and Stefan Wewers, *Computing L-functions and semistable reduction of superelliptic curves*, Glasg. Math. J. **59** (2017), no. 1, 77–108. MR3576328

[CS86] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR861969

[DDMM18] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan, *Local arithmetic of curves and jacobians*, Preprint **arXiv:1808.02936** (2018).

[DNS19] M. Derickx, F. Najman, and S. Siksek, *Elliptic curves over totally real cubic fields are modular*, Preprint **arXiv:1901.03436** (2019).

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206. MR3359051

[Fly90] Eugene Victor Flynn, *The Jacobian and formal group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), no. 3, 425–441. MR1041476

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. MR1917232 (2003g:14001)

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254

School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow, G12 8QQ.

Email address: adam.morgan@glasgow.ac.uk