Contents

Elliptic curves over function fields
Douglas Ulmer 213

Elliptic curves over function fields 215
Introduction 215

Lecture 0. Background on curves and function fields 217
1. Terminology 217
2. Function fields and curves 217
3. Zeta functions 218
4. Cohomology 219
5. Jacobians 219
6. Tate's theorem on homomorphisms of abelian varieties 221

Lecture 1. Elliptic curves over function fields 223
1. Elliptic curves 223
2. Frobenius 224
3. The Hasse invariant 225
4. Endomorphisms 226
5. The Mordell-Weil-Lang-Néron theorem 226
6. The constant case 227
7. Torsion 228
8. Local invariants 230
9. The L-function 231
10. The basic BSD conjecture 232
11. The Tate-Shafarevich group 232
12. Statements of the main results 233
13. The rest of the course 234

Lecture 2. Surfaces and the Tate conjecture 237
1. Motivation 237
2. Surfaces 237
3. Divisors and the Néron-Severi group 238
4. The Picard scheme 239
5. Intersection numbers and numerical equivalence 239
6. Cycle classes and homological equivalence 240
7. Comparison of equivalence relations on divisors 241
8. Examples 241
9. Tate's conjectures T_1 and T_2 243
10. T_1 and the Brauer group 244

11. The descent property of T_1 246
12. Tate's theorem on products 246
13. Products of curves and DPC 247

Lecture 3. Elliptic curves and elliptic surfaces 249
1. Curves and surfaces 249
2. The bundle ω and the height of $\mathcal{E}$ 252
3. Examples 252
4. $\mathcal{E}$ and the classification of surfaces 254
5. Points and divisors, Shioda-Tate 255
6. L-functions and Zeta-functions 256
7. The Tate-Shafarevich and Brauer groups 257
8. The main classical results 258
9. Domination by a product of curves 259
10. Four monomials 259
11. Berger's construction 260

Lecture 4. Unbounded ranks in towers 263
1. Grothendieck's analysis of L-functions 263
2. The case of an elliptic curve 266
3. Large analytic ranks in towers 267
4. Large algebraic ranks 270

Lecture 5. More applications of products of curves 273
1. More on Berger's construction 273
2. A rank formula 274
3. First examples 275
4. Explicit points 276
5. Another example 277
6. Further developments 277

Bibliography 279

Elliptic curves over function fields

Douglas Ulmer

IAS/Park City Mathematics Series
Volume XX, XXXX

Elliptic curves over function fields

Douglas Ulmer

Introduction

These are the notes from a course of five lectures at the 2009 Park City Math Institute. The focus is on *elliptic curves* over function fields over *finite fields*. In the first three lectures, we explain the main classical results (mainly due to Tate) on the Birch and Swinnerton-Dyer conjecture in this context and its connection to the Tate conjecture about divisors on surfaces. This is preceded by a "Lecture 0" on background material. In the remaining two lectures, we discuss more recent developments on elliptic curves of large rank and constructions of explicit points in high rank situations.

A great deal of this material generalizes naturally to the context of curves and Jacobians of *any genus* over function fields over *arbitrary ground fields*. These generalizations were discussed in a course of 12 lectures at the CRM in Barcelona in February, 2010, and will be written up as a companion to these notes, see [Ulm11]. Unfortunately, theorems on unbounded ranks over function fields are currently known only in the context of finite ground fields.

Finally, we mention here that very interesting theorems of Gross-Zagier type exist also in the function field context. These would be the subject of another series of lectures and we will not say anything more about them in these notes.

It is a pleasure to thank the organizers of the 2009 PCMI for the invitation to speak, the students for their interest, enthusiasm, and stimulating questions, and the "elder statesmen"—Bryan Birch, Dick Gross, John Tate, and Yuri Zarhin—for their remarks and encouragement. Thanks also to Keith Conrad for bringing the fascinating historical articles of Roquette [Roq06] to my attention. Last but not least, thanks are due as well to Lisa Berger, Tommy Occhipinti, Karl Rubin, Alice Silverberg, Yuri Zarhin, and an anonymous referee for their suggestions and TEXnical advice.

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332
E-mail address: douglas.ulmer@math.gatech.edu

LECTURE 0

Background on curves and function fields

This "Lecture 0" covers definitions and notations that are probably familiar to many readers and that were reviewed very quickly during the PCMI lectures. Readers are invited to skip it and refer back as necessary.

1. Terminology

Throughout, we use the language of schemes. This is necessary to be on firm ground when dealing with some of the more subtle aspects involving non-perfect ground fields and possibly non-reduced group schemes. However, the instances where we use any hard results from this theory are isolated and students should be able to follow readily the main lines of discussion, perhaps with the assistance of a friendly algebraic geometer.

Throughout, a *variety* over a field F is a separated, reduced scheme of finite type over $\operatorname{Spec} F$. A *curve* is a variety purely of dimension 1 and a *surface* is a variety purely of dimension 2.

2. Function fields and curves

Throughout, p will be a prime number and $\mathbb{F}_q$ will denote the field with q elements with q a power of p. We write $\mathcal{C}$ for a smooth, projective, and absolutely irreducible curve of genus g over $\mathbb{F}_q$ and we write $K = \mathbb{F}_q(\mathcal{C})$ for the function field of $\mathcal{C}$ over $\mathbb{F}_q$. The most important example is when $\mathcal{C} = \mathbb{P}^1$, the projective line, in which case $K = \mathbb{F}_q(\mathcal{C}) = \mathbb{F}_q(t)$ is the field of rational functions in a variable t over $\mathbb{F}_q$.

We write v for a closed point of $\mathcal{C}$, or equivalently for an equivalence class of valuations of K. For each such v we write $\mathcal{O}_{(v)}$ for the local ring at v (the ring of rational functions on $\mathcal{C}$ regular at v), $\mathfrak{m}_v \subset \mathcal{O}_{(v)}$ for the maximal ideal (those functions vanishing at v), and $\kappa_v = \mathcal{O}_{(v)}/\mathfrak{m}_v$ for the residue field at v. The extension $\kappa_v/\mathbb{F}_q$ is finite and we set $\deg(v) = [\kappa_v : \mathbb{F}_q]$ and $q_v = q^{\deg(v)}$ so that $\kappa_v \cong \mathbb{F}_{q_v}$.

For example, in the case where $\mathcal{C} = \mathbb{P}^1$, the "finite" places of $\mathcal{C}$ correspond bijectively to monic irreducible polynomials $f \in \mathbb{F}_q[t]$. If v corresponds to f, then $\mathcal{O}_{(v)}$ is the set of ratios g/h where $g, h \in \mathbb{F}_q[t]$ and f does not divide h. The maximal ideal $\mathfrak{m}_v$ consists of ratios g/h where f does divide g, and the degree of v is the degree of f as a polynomial in t. There is one more place of K, the "infinite" place $v = \infty$. The local ring consists of ratios g/h with $g, h \in \mathbb{F}_q[t]$ and $\deg(g) \leq \deg(h)$. The maximal ideal consists of ratios g/h where $\deg(g) < \deg(h)$ and the degree of $v = \infty$ is 1. The finite and infinite places of $\mathbb{P}^1$ give all closed points of $\mathbb{P}^1$.

We write K^{sep} for a separable closure of K and let $G_K = \operatorname{Gal}(K^{sep}/K)$. We write $\overline{\mathbb{F}}_q$ for the algebraic closure of $\mathbb{F}_q$ in K^{sep}. For each place v of K we have the decomposition group D_v (defined only up to conjugacy), its normal subgroup the inertia group $I_v \subset D_v$, and Fr_v the (geometric) Frobenius at v, a canonical generator

of the quotient $D_v/I_v \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ that acts as $x \mapsto x^{q_v^{-1}}$ on the residue field at a place w dividing v in a finite extension $F \subset K^{sep}$ unramified over v.

General references for this section and the next are [Gol03], [Ros02], and [Sti09].

3. Zeta functions

Let $\mathcal{X}$ be a variety over the finite field $\mathbb{F}_q$. Extending the notation of the previous section, if x is a closed point of $\mathcal{X}$, we write κ_x for the residue field at x, q_x for its cardinality, and $\deg(x)$ for $[\kappa_x : \mathbb{F}_q]$.

We define the Z and ζ functions of $\mathcal{X}$ via Euler products:

$$Z(\mathcal{X}, T) = \prod_x \left(1 - T^{\deg(x)}\right)^{-1}$$

and

$$\zeta(\mathcal{X}, s) = Z(\mathcal{X}, q^{-s}) = \prod_x \left(1 - q_x^{-s}\right)^{-1}$$

where the products are over the closed points of $\mathcal{X}$. It is a standard exercise to show that

$$Z(\mathcal{X}, T) = \exp\left(\sum_{n \geq 1} N_n \frac{T^n}{n}\right)$$

where N_n is the number of $\mathbb{F}_{q^n}$-valued points of $\mathcal{X}$. It follows from a crude estimate for the number of $\mathbb{F}_{q^n}$ points of $\mathcal{X}$ that the Euler product defining $\zeta(\mathcal{X}, s)$ converges in the half plane $\mathrm{Re}(s) > \dim \mathcal{X}$.

If $\mathcal{X}$ is smooth and projective, then it is known that $Z(\mathcal{X}, T)$ is a rational function of the form

$$\frac{\prod_{i=0}^{\dim \mathcal{X} - 1} P_{2i+1}(T)}{\prod_{i=0}^{\dim \mathcal{X}} P_{2i}(T)}$$

where $P_0(T) = (1 - T)$, $P_{2\dim \mathcal{X}}(T) = (1 - q^{\dim \mathcal{X}} T)$, and for all $0 \leq i \leq 2 \dim \mathcal{X}$ $P_i(T)$ is a polynomial with integer coefficients and constant term 1. We denote the inverse roots of P_i by α_{ij} so that

$$P_i(T) = \prod_j (1 - \alpha_{ij} T)$$

The inverse roots α_{ij} of $P_i(T)$ are algebraic integers that have absolute value $q^{i/2}$ in every complex embedding. (We say that they are *Weil numbers of size* $q^{i/2}$.) It follows that $\zeta(\mathcal{X}, s)$ has a meromorphic continuation to the whole s plane, with poles on the lines $\mathrm{Re}\, s \in \{0, \ldots, \dim \mathcal{X}\}$ and zeroes on the lines $\mathrm{Re}\, s \in \{1/2, \ldots, \dim \mathcal{X} - 1/2\}$. This is the analogue of the Riemann hypothesis for $\zeta(\mathcal{X}, s)$.

It is also known that the set of inverse roots of $P_i(T)$ (with multiplicities) is stable under $\alpha_{ij} \mapsto q^i/\alpha_{ij}$ and that for $i \leq \dim \mathcal{X}$, $P_{2d-i}(T) = P_i(q^{d-i}T)$. Thus $\zeta(\mathcal{X}, s)$ satisfies a functional equation when s is replaced by $\dim \mathcal{X} - s$.

In the case where $\mathcal{X}$ is a curve, $P_1(T)$ has degree $2g$ (g = the genus of $\mathcal{C}$) and has the form

$$P_1(T) = 1 + \cdots + q^g T^{2g} = \prod_{j=1}^{2g} (1 - \alpha_{1j} T).$$

Thus $\zeta(\mathcal{C}, s)$ has simple poles for $s \in \frac{2\pi i}{\log q}\mathbb{Z}$ and $s \in 1 + \frac{2\pi i}{\log q}\mathbb{Z}$ and its zeroes lie on the line $\mathrm{Re}\, s = 1/2$.

For a fascinating history of the early work on zeta functions and the Riemann hypothesis for curves over finite fields, see [Roq06] and parts I and II of that work.

4. Cohomology

Assume that $\mathcal{X}$ is a smooth projective variety over $k = \mathbb{F}_q$. We write $\overline{\mathcal{X}}$ for $\mathcal{X} \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Note that $G_k = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $\overline{\mathcal{X}}$ via the factor $\overline{\mathbb{F}}_q$.

Choose a prime $\ell \neq p$. We have ℓ-adic cohomology groups $H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ which are finite-dimensional $\mathbb{Q}_\ell$-vector spaces and which vanish unless $0 \leq i \leq 2 \dim \mathcal{X}$.

Functoriality in $\overline{\mathcal{X}}$ gives a continuous action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Since the geometric Frobenius ($\mathrm{Fr}_q(a) = a^{q^{-1}}$) is a topological generator of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, the characteristic polynomial of Fr_q on $H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ determines the eigenvalues of the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$; in fancier language, it determines the action up to semi-simplification.

An important result (inspired by [Wei49] and proven in great generality in [SGA5]) says that the factors P_i of $Z(\mathcal{X}, t)$ are characteristic polynomials of Frobenius:

$$P_i(T) = \det(1 - T \,\mathrm{Fr}_q \,|H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell)). \tag{4.1}$$

From this point of view, the functional equation and Riemann hypothesis for $Z(\mathcal{X}, T)$ are statements about duality and purity.

To discuss the connections, we need more notation. Let $\mathbb{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}(\overline{\mathbb{F}}_q)$ and $\mathbb{Q}_\ell(1) = \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, so that $\mathbb{Q}_\ell(1)$ is a one-dimensional $\mathbb{Q}_\ell$-vector space on which $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts via the ℓ-adic cyclotomic character. More generally, for $n > 0$ set $\mathbb{Q}_\ell(n) = \mathbb{Q}_\ell(1)^{\otimes n}$ (n-th tensor power) and $\mathbb{Q}_\ell(-n) = \mathrm{Hom}(\mathbb{Q}_\ell(n), \mathbb{Q}_\ell)$, so that for all n, $\mathbb{Q}_\ell(n)$ is a one-dimensional $\mathbb{Q}_\ell$-vector space on which $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts via the nth power of the ℓ-adic cyclotomic character.

We have $H^0(\overline{\mathcal{X}}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ (with trivial Galois action) and $H^{2\dim \mathcal{X}}(\overline{\mathcal{X}}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(\dim \mathcal{X})$. The functional equation follows from the fact that we have a canonical non-degenerate, Galois equivariant pairing

$$H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell) \times H^{2\dim \mathcal{X} - i}(\overline{\mathcal{X}}, \mathbb{Q}_\ell) \to H^{2\dim \mathcal{X}}(\overline{\mathcal{X}}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(\dim \mathcal{X}).$$

Indeed, the non-degeneracy of this pairing implies that if α is an eigenvalue of Fr_q on $H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$, then $q^{\dim \mathcal{X}}/\alpha$ is an eigenvalue of Fr_q on $H^{2\dim \mathcal{X} - i}(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$.

The Riemann hypothesis in this context is the statement that the eigenvalues of Fr_q on $H^i(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ are algebraic integers with absolute value $q^{i/2}$ in every complex embedding.

See [SGA4$\frac{1}{2}$] or [Mil80] for an overview of étale cohomology and its connections with the Weil conjectures.

5. Jacobians

5.1. Picard and Albanese properties

We briefly review two (dual) universal properties of the Jacobian of a curve that we will need. See [Mil86b] for more details.

We assume throughout that the curve $\mathcal{C}$ has an $\mathbb{F}_q$-rational point x, i.e., a closed point with residue field $\mathbb{F}_q$. If T is another connected variety over $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point t, a *divisorial correspondence* between (C, x) and (T, t) is an invertible sheaf $\mathcal{L}$ on $C \times_{\mathbb{F}_q} T$ such that $\mathcal{L}|_{C \times t}$ and $\mathcal{L}|_{x \times T}$ are trivial. Two divisorial correspondences are equal when they are isomorphic as invertible sheaves. Note

that the set of divisorial correspondences between $(\mathcal{C}, x)$ and (T, t) forms a group under tensor product and is thus a subgroup of $\mathrm{Pic}(\mathcal{C} \times T)$. We write

$$\mathrm{DivCorr}((\mathcal{C}, x), (T, t)) \subset \mathrm{Pic}(\mathcal{C} \times T)$$

for this subgroup. One may think of a divisorial correspondence as giving a family of invertible sheaves on C: $s \mapsto \mathcal{L}|_{C \times s}$.

Let $J = J_{\mathcal{C}}$ be the Jacobian of $\mathcal{C}$ and write 0 for its identity element. Then J is a g-dimensional abelian variety over $\mathbb{F}_q$ and it carries the "universal divisorial correspondence with C." More precisely, there is a divisorial correspondence $\mathcal{M}$ between (C, x) and $(J, 0)$ such that if S is another connected variety over $\mathbb{F}_q$ with $\mathbb{F}_q$-rational point s and $\mathcal{L}$ is a divisorial correspondence between (C, x) and (S, s), then there is a unique morphism $\phi : S \to J$ sending s to 0 such that $\mathcal{L} = \phi^* \mathcal{M}$. (Of course $\mathcal{M}$ depends on the choice of base point x, but we omit this from the notation.)

It follows that there is a canonical morphism, the Abel-Jacobi morphism, $AJ : \mathcal{C} \to J$ sending x to 0. Intuitively, this corresponds to the family of invertible sheaves parameterized by $\mathcal{C}$ that sends $y \in \mathcal{C}$ to $\mathcal{O}_{\mathcal{C}}(y - x)$. More precisely, let $\Delta \subset \mathcal{C} \times C$ be the diagonal, let

$$D = \Delta - x \times \mathcal{C} - \mathcal{C} \times x,$$

and let $\mathcal{L} = \mathcal{O}_{\mathcal{C} \times \mathcal{C}}(D)$ which is a divisorial correspondence between (C, x) and itself. The universal property above then yields the morphism $AJ : \mathcal{C} \to J$. It is known that AJ is a closed immersion and that its image generates J as an algebraic group.

The second universal property enjoyed by J (or rather by AJ) is the Albanese property: it is universal for maps to abelian varieties. More precisely, if A is an abelian variety and $\phi : \mathcal{C} \to A$ is a morphism sending x to 0, then there is a unique homomorphism of abelian varieties $\psi : J \to A$ such that $\phi = \psi \circ AJ$.

Combining the two universal properties gives a useful connection between correspondences and homomorphisms: Suppose $\mathcal{C}$ and $\mathcal{D}$ are curves over $\mathbb{F}_q$ with rational points $x \in \mathcal{C}$ and $y \in \mathcal{D}$. Then we have an isomorphism

$$\mathrm{DivCorr}((\mathcal{C}, x), (\mathcal{D}, y)) \cong \mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}}). \tag{5.1.1}$$

Intuitively, given a divisorial correspondence on $\mathcal{C} \times \mathcal{D}$, we get a family of invertible sheaves on $\mathcal{D}$ parameterized by $\mathcal{C}$ and thus a morphism $\mathcal{C} \to J_{\mathcal{D}}$. The Albanese property then gives a homomorphism $J_{\mathcal{C}} \to J_{\mathcal{D}}$. We leave the precise version as an exercise, or see [Mil86b, 6.3]. We will use this isomorphism later to understand the Néron-Severi group of a product of curves.

5.2. The Tate module

Let A be an abelian variety of dimension g over $\mathbb{F}_q$, for example the Jacobian of a curve of genus g. (See [Mil86a] for a brief introduction to abelian varieties and [Mum08] for a much more complete treatment.) Choose a prime $\ell \neq p$. Let $A[\ell^n]$ be the set of $\overline{\mathbb{F}}_q$ points of A of order dividing ℓ^n. It is a group isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ with a linear action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. We form the inverse limit

$$T_\ell A = \varprojlim_n A[\ell^n]$$

where the transition maps are given by multiplication by ℓ. Let $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, a $2g$-dimensional $\mathbb{Q}_\ell$-vector space with a linear action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. It is often called the *Tate module* of A.

According to Roquette, what we now call the Tate module seems to have first been used in print by Deuring [Deu40] as a substitute for homology in his work on correspondences on curves. It appears already in a letter of Hasse from 1935, see [Roq06, p. 36].

The following proposition is the modern interpretation of the connection between homology and torsion points.

Proposition 5.2.1. *Let A be an abelian variety over a field k and let ℓ be a prime not equal to the characteristic of k. Let $V_\ell A$ be the Tate module of A and $(V_\ell A)^*$ its dual as a $G_k = \mathrm{Gal}(k^{sep}/k)$-module.*

- *There is a canonical isomorphism of G_k-modules*
$$(V_\ell A)^* \cong H^1(A \times \overline{k}, \mathbb{Q}_\ell).$$
- *If A is the Jacobian of a curve $\mathcal{C}$ over k, then*
$$H^1(A \times \overline{k}, \mathbb{Q}_\ell) \cong H^1(\mathcal{C} \times \overline{k}, \mathbb{Q}_\ell).$$

For a proof of part 1, see [Mil86a, 15.1] and for part 2, see [Mil86b, 9.6].

Exercises 5.2.2. These exercises are meant to make the Proposition more plausible.

(1) Show that if $A(\mathbb{C})$ is a complex torus $\mathbb{C}^g/\Lambda$, then the singular homology $H_1(A(\mathbb{C}), \mathbb{Q}_\ell)$ is canonically isomorphic to $V_\ell A(\mathbb{C})$. (Hint: Use the universal coefficient theorem to show that $H_1(A(\mathbb{C}), \mathbb{Z}/\ell^n\mathbb{Z}) \cong \Lambda/\ell^n\Lambda$.)

(2) (Advanced) Let $\mathcal{C}$ be a smooth projective curve over an algebraically closed field k. Let ℓ be a prime not equal to the characteristic of k. Use geometric class field theory (as in [Ser88]) to show that unramified Galois covers $\mathcal{C}' \to \mathcal{C}$ equipped with an isomorphism $\mathrm{Gal}(\mathcal{C}'/\mathcal{C}) \cong \mathbb{Z}/\ell\mathbb{Z}$ are in bijection with elements of $\mathrm{Hom}(J_{\mathcal{C}}[\ell], \mathbb{Z}/\ell\mathbb{Z})$. (Make a convention to deal with the trivial homomorphism.) This suggests that $H^1(\mathcal{C}, \mathbb{Z}/\ell\mathbb{Z})$ "should be" $\mathrm{Hom}(J_{\mathcal{C}}[\ell], \mathbb{Z}/\ell\mathbb{Z})$ and $H_1(C, \mathbb{Z}/\ell\mathbb{Z})$ "should be" $J_{\mathcal{C}}[\ell]$. The reason we only have "should be" rather than a theorem is that a non-trivial Galois cover $\mathcal{C}' \to \mathcal{C}$ is never locally constant in the Zariski topology. This is a prime motivation for introducing the étale topology.

6. Tate's theorem on homomorphisms of abelian varieties

As usual, let k be a finite field and let A and B be two abelian varieties over k. Choose a prime ℓ not equal to the characteristic of k and form the Tate modules $V_\ell A$ and $V_\ell B$. Any homomorphism of abelian varieties $\phi : A \to B$ induces a homomorphism of Tate modules $\phi_* : V_\ell A \to V_\ell B$ and this homomorphism commutes with the action of $G_k = \mathrm{Gal}(\overline{k}/k)$ on the Tate modules. We get an induced homomorphism $\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}_\ell \to \mathrm{Hom}_{G_k}(V_\ell A, V_\ell B)$. Tate's famous result [Tat66a] asserts that this is an isomorphism:

Theorem 6.1. *The map $\phi \mapsto \phi_*$ induces an isomorphism of $\mathbb{Q}_\ell$-vector spaces:*
$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}_\ell \tilde{\to} \mathrm{Hom}_{G_k}(V_\ell A, V_\ell B).$$

We also mention [Zar08] which gives a different proof and a strengthening with finite coefficients.

We will use Tate's theorem in Theorem 12.1 of Lecture 2 to understand the divisors on a product of curves in terms of homomorphisms between their Jacobians.

LECTURE 1

Elliptic curves over function fields

In this lecture we discuss the basic facts about elliptic curves over function fields over finite fields. We assume the reader has some familiarity with elliptic curves over global fields such as $\mathbb{Q}$ or number fields, as explained, e.g., in [Sil09], and we will focus on aspects specific to characteristic p. The lecture ends with statements of the main results known about the conjecture of Birch and Swinnerton-Dyer in this context.

1. Elliptic curves

1.1. Definitions

We write $k = \mathbb{F}_q$ for the finite field of cardinality q and characteristic p and we let K be the function field of a smooth, projective, absolutely irreducible curve $\mathcal{C}$ over k.

An *elliptic curve* over K is a smooth, projective, absolutely irreducible curve of genus 1 over K equipped with a K-rational point O that will serve as the origin of the group law.

All the basic geometric facts, e.g., of [Sil09, Ch. III and App. A], continue to hold in the context of function fields. We review a few of them to establish notation, but will not enter into full details.

Using the Riemann-Roch theorem, an elliptic curve E over K can always be presented as a projective plane cubic curve defined by a Weierstrass equation, i.e., by an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1.1}$$

where $a_1, \dots, a_6 \in K$. The origin O is the point at infinity $[0 : 1 : 0]$. We often give the equation in affine form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1.2}$$

where $x = X/Z$ and $y = Y/Z$.

The quantities $b_2, \dots, b_8, c_4, c_6, \Delta, j$ are defined by the usual formulas ([Sil09, III.1] or [Del75]). Since E is smooth, by the following exercise $\Delta \neq 0$.

Remark/Exercises 1.1.3. The word "smooth" in the definition of an elliptic curve means that the morphism $E \to \operatorname{Spec} K$ is smooth. Smoothness of a morphism can be tested via the Jacobian criterion (see, e.g., [Har77, III.10.4] or [Liu02, 4.3.3]). Show that the projective plane cubic (1.1.1) is smooth if and only if $\Delta \neq 0$. Because the ground field K is not perfect, smoothness is strictly stronger than the requirement that E be regular, i.e., that its local rings be regular local rings (cf. [Liu02, 4.2.2]). For example, show that the projective cubic defined by $Y^2Z = X^3 - tZ^3$ over $K = \mathbb{F}_p(t)$ with $p = 2$ or 3 is a regular scheme, but is not smooth over K.

Definitions 1.1.4. Let E be an elliptic curve over K.

(1) We say E is *constant* if there is an elliptic curve E_0 defined over k such that $E \cong E_0 \times_k K$. Equivalently, E is constant if it can be defined by a Weierstrass cubic (1.1.1) where the $a_i \in k$.
(2) We say E is *isotrivial* if there exists a finite extension K' of K such that E becomes constant over K'. Note that a constant curve is isotrivial.
(3) We say E is *non-isotrivial* if it is not isotrivial. We say E is *non-constant* if it is not constant.

Remark/Exercises 1.1.5. Show that E is isotrivial if and only if $j(E) \in k$. Suppose that E is isotrivial, so that E becomes constant over a finite extension K' and let k' be the field of constants of K' (the algebraic closure of k in K'). *A priori*, the definition of isotrivial says that there is an elliptic curve E_0 over k' such that $E \times_K K' \cong E_0 \times_{k'} K'$. Show that we may take K' to have field of constants k and E_0 to be defined over k. Show also that we may take K' to be separable and of degree dividing 24 over K.

Exercise 1.1.6. For any elliptic curve E over K, the functor on K-algebras $L \mapsto \mathrm{Aut}_L(E \times L)$ is represented by a group scheme $\underline{\mathrm{Aut}}(E)$. (Concretely, this means there is a group scheme $\underline{\mathrm{Aut}}(E)$ such that for any K-algebra L, $\mathrm{Aut}_L(E \times L)$ is $\underline{\mathrm{Aut}}(E)(L)$, the group of L-valued points of $\underline{\mathrm{Aut}}(E)$.) Show that $\underline{\mathrm{Aut}}(E)$ is an étale group scheme. Equivalently, show that any element of $\mathrm{Aut}_{\overline{K}}(E)$ is defined over a separable extension of K. (This is closely related to the previous exercise.)

1.2. Examples

Let $K = \mathbb{F}_p(t)$ with $p > 3$ and define elliptic curves

$$\begin{aligned} E_1 &: \quad y^2 = x^3 + 1 \\ E_2 &: \quad y^2 = x^3 + t^6 \\ E_3 &: \quad y^2 = x^3 + t \\ E_4 &: \quad y^2 = x^3 + x + t. \end{aligned}$$

Then $E_1 \cong E_2$ over K and both are constant, E_3 is isotrivial and non-constant, whereas E_4 is non-isotrivial.

For more examples, let $K = \mathbb{F}_p(t)$ (with p restricted as indicated) and define

$$\begin{aligned} (p \neq 3) \qquad & E_5 : \quad y^2 + ty = x^3 \\ (p \neq 2) \qquad & E_6 : \quad y^2 = x^3 + tx \\ (p \text{ arbitrary}) \qquad & E_7 : \quad y^2 + xy + ty = x^3 \\ (p \text{ arbitrary}) \qquad & E_8 : \quad y^2 + xy = x^3 + tx \\ (p \text{ arbitrary}) \qquad & E_9 : \quad y^2 + xy = x^3 + t. \end{aligned}$$

Then E_5 and E_6 are isotrivial and non-constant whereas E_7, E_8, and E_9 are non-isotrivial.

2. Frobenius

If X is a scheme of characteristic p, we define the *absolute Frobenius* morphism $\mathrm{Fr}_X : X \to X$ as usual: It is the identity on the underlying topological space and

raises functions to the p-th power. When $X = \operatorname{Spec} K$, Fr_X is just the map of schemes induced by the ring homomorphism $K \to K$, $a \mapsto a^p$.

Suppose as usual that K is a function field and let E be an elliptic curve over K. Define a new elliptic curve $E^{(p)}$ over K by the fiber product diagram:

$$\begin{array}{ccc} E^{(p)} = \operatorname{Spec} K \times_{\operatorname{Spec} K} E & \longrightarrow & E \\ \downarrow & & \downarrow \\ \operatorname{Spec} K & \xrightarrow{\mathrm{Fr}} & \operatorname{Spec} K \end{array}$$

More concretely, if E is presented as a Weierstrass cubic as in equation (1.1.2), then $E^{(p)}$ is given by the equation with a_i replaced by a_i^p. The universal property of the fiber product gives a canonical morphism $\mathrm{Fr}_{E/K}$, the *relative Frobenius*:

$$\begin{array}{ccccc} E & \xrightarrow{\mathrm{Fr}_{E/K}} & E^{(p)} & \longrightarrow & E \\ & \searrow & \downarrow & & \downarrow \\ & & \operatorname{Spec} K & \xrightarrow{\mathrm{Fr}} & \operatorname{Spec} K \end{array}$$

By definition $\mathrm{Fr}_{E/K}$ is a morphism over K. In terms of Weierstrass equations for E and $E^{(p)}$ as above, it is just the map $(x, y) \mapsto (x^p, y^p)$.

It is evident that $\mathrm{Fr}_{E/K}$ is an isogeny, i.e., a surjective homomorphism of elliptic curves, and that its degree is p. We define $V = V_{E/K}$ to be the dual isogeny, so that $V_{E/K} \circ \mathrm{Fr}_{E/K} = [p]$, multiplication by p on E.

Note that $j(E^{(p)}) = j(E)^p$ so that if E is non-isotrivial, E and $E^{(p)}$ are not isomorphic. Thus, using Frobenius and its iterates, we see that there are infinitely many non-isomorphic elliptic curves isogenous to any non-isotrivial E. This is in marked contrast to the situation over number fields (cf. [Fal86]).

Lemma 2.1. *Let E be an elliptic curve over K. Then $j(E)$ is a p-th power in K if and only if there exists an elliptic curve E' over K such that $E \cong E'^{(p)}$.*

Proof. We sketch a fancy argument and pose as an exercise a more down-to-earth proof. Obviously if there is an E' with $E \cong E'^{(p)}$, then $j(E) = j(E'^{(p)}) = j(E')^p \in K^p$. Conversely, suppose $j(E) \in K^p$ and choose an elliptic curve E'' such that $j(E'')^p = j(E)$. It follows that $E''^{(p)}$ is isomorphic to E over a finite separable extension of K. In other words, E is the twist of $E''^{(p)}$ by a cocycle in $H^1(G_K, \operatorname{Aut}_{K^{sep}}(E''^{(p)}))$. But there is a canonical isomorphism $\operatorname{Aut}_{K^{sep}}(E''^{(p)}) \cong \operatorname{Aut}_{K^{sep}}(E'')$ and twisting E'' by the corresponding element of

$$H^1(G_K, \operatorname{Aut}_{K^{sep}}(E'')) \cong H^1(G_K, \operatorname{Aut}_{K^{sep}}(E''^{(p)}))$$

we obtain an elliptic curve E' with $E'^{(p)} \cong E$. □

Exercise 2.2. Use explicit equations, as in [Sil09, Appendix A], to prove the lemma.

3. The Hasse invariant

Let F be a field of characteristic p and E an elliptic curve over F. Let $\mathcal{O}_E$ be the sheaf of regular functions on E and let Ω^1_E be the sheaf of Kähler differentials on E. The coherent cohomology group $H^1(E, \mathcal{O}_E)$ is a one-dimensional F-vector

space and is Serre dual to the space of invariant differentials $H^0(E, \Omega^1_E)$. Choose a non-zero differential $\omega \in H^0(E, \Omega^1_E)$ and let η be the dual element of $H^1(E, \mathcal{O}_E)$. The absolute Frobenius Fr_E induces a (p-linear) homomorphism:

$$\mathrm{Fr}_E^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E).$$

We define an element $A = A(E, \omega)$ of F by requiring that $\mathrm{Fr}_E^*(\eta) = A(E, \omega)\eta$. This is the *Hasse invariant* of E. It has weight $p-1$ in the sense that $A(E, \lambda^{-1}\omega) = \lambda^{p-1}A(E, \omega)$ for all $\lambda \in F^\times$.

Suppose E is given by a Weierstrass equation (1.1.2) and $\omega = dx/(2y+a_1x+a_3)$. If $p = 2$, then $A(E, \omega) = a_1$. If $p > 2$, choose an equation with $a_1 = a_3 = 0$. Then $A(E, \omega) =$ the coefficient of x^{p-1} in $(x^3 + a_2x^2 + a_4x + a_6)^{(p-1)/2}$. These assertions follow from [KM85, 12.4] where several other calculations of A are also presented.

Recall that E/K is *ordinary* if the group of p-torsion points $E(\overline{K})[p] \neq 0$ and *supersingular* otherwise. It is known that E is supersingular if and only if $A(E, \omega) = 0$ (e.g., [KM85, 12.3.6 and 12.4]) and in this case $j(E) \in \mathbb{F}_{p^2}$ (e.g., [KM85, proof of 2.9.4]). (Alternatively, one may apply [Sil09, V.3.1] to E over $\overline{K}$.) In particular, if E is supersingular, then it must also be isotrivial.

4. Endomorphisms

The classification of endomorphism rings in [Sil09, III.9] goes over verbatim to the function field case: $\mathrm{End}_{\overline{K}}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic number field, or an order in a quaternion algebra over $\mathbb{Q}$ ramified exactly at ∞ and p. The quaternionic case occurs if and only if E is supersingular, and the imaginary quadratic case occurs if and only if $j(E)$ is in $\overline{\mathbb{F}}_p$ and E is not supersingular ([Sil09, V.3.1 and Exer. V.5.8]).

In particular, if E is non-isotrivial, then $\mathrm{End}_{\overline{K}}(E) = \mathrm{End}_K(E) = \mathbb{Z}$.

5. The Mordell-Weil-Lang-Néron theorem

We write $E(K)$ for the group of K-rational points of E and we call $E(K)$ the Mordell-Weil group of E over K. Lang and Néron (independently) generalized the classical Mordell-Weil theorem to the function field context:

Theorem 5.1. *Assume that $K = \mathbb{F}_q(\mathbb{C})$ is the function field of a curve over a finite field and let E be an elliptic curve over K. Then $E(K)$ is a finitely generated abelian group.*

(The theorems of Lang and Néron apply much more generally to any abelian variety A over a field K that is finitely generated over its "constant field" k, but one has to take care of the "constant part" of A. See [Ulm11] for details.)

We will not give a detailed proof of the MWLN theorem here, but will mention two strategies. One is to follow the method of proof of the Mordell-Weil (MW) theorem over a number field. Choose a prime number $\ell \neq p$. By an argument very similar to that in [Sil09, Ch. VIII] one can show that $E(K)/\ell E(K)$ is finite (the "weak Mordell-Weil theorem") by embedding it in a Selmer group and showing that the Selmer group is finite by using the two fundamental finiteness results of algebraic number theory (finiteness of the class group and finite generation of the unit group) applied to Dedekind domains in K. One can then introduce a theory of heights exactly as in [Sil09] and show that the MW theorem follows from the weak MW theorem and finiteness properties of heights. See the original paper of Lang

and Néron [LN59] for the full details. A complete treatment in modern language has been given by Conrad [Con06].

One interesting twist in the function field setting comes if one takes $\ell = p$ above. It is still true that the Selmer group for p is finite, but one needs to use the local restrictions at all places; the maximal abelian extension of exponent p unramified outside a finite but non-empty set of places is not finite and so one needs some control on ramification at every place. See [Ulm91] for a detailed account of p-descent in characteristic p.

A second strategy of proof, about which we will say more in Lecture 3, involves relating the Mordell-Weil group of E to the Néron-Severi group of a closely related surface $\mathcal{E}$. In fact, finite generation of the Néron-Severi group (known as the "theorem of the base") is equivalent to the Lang-Néron theorem. A direct proof of the theorem of the base was given by Kleiman in [SGA6, XIII]. See also [Mil80, V.3.25].

6. The constant case

It is worth pausing in the general development to look at the case of a constant curve E. Recall that K is the function field $k(\mathcal{C})$ of the curve $\mathcal{C}$ over $k = \mathbb{F}_q$. Suppose E_0 is an elliptic curve over k and let $E = E_0 \times_k K$.

Proposition 6.1. *We have a canonical isomorphism*

$$E(K) \cong \mathrm{Mor}_k(\mathcal{C}, E_0)$$

where Mor_k *denotes morphisms of varieties over* k (=*morphisms of* k*-schemes*). *Under this isomorphism,* $E(K)_{tor}$ *corresponds to the subset of constant morphisms.*

Proof. By definition, $E(K)$ is the set of K-morphisms

$$\mathrm{Spec}\, K \to E = E_0 \times_k K.$$

By the universal property of the fiber product, these are in bijection with k-morphisms $\mathrm{Spec}\, K \to E_0$. Since $\mathcal{C}$ is a smooth curve, any k-morphism $\mathrm{Spec}\, K \to E_0$ extends uniquely to a k-morphism $\mathcal{C} \to E_0$. This establishes a map $E(K) \to \mathrm{Mor}_k(\mathcal{C}, E_0)$. If $\eta : \mathrm{Spec}\, K \to \mathcal{C}$ denotes the canonical inclusion, composition with η ($\phi \mapsto \phi \circ \eta$) induces a map $\mathrm{Mor}_k(\mathcal{C}, E_0) \to E(K)$ inverse to the map above. This establishes the desired bijection and this bijection is obviously compatible with the group structures.

Since k is finite, it is clear that a constant morphism goes over to a torsion point. Conversely, if $P \in E(K)$ is torsion, say of order n, then the image of the corresponding $\phi : \mathcal{C} \to E_0$ must lie in the set of n-torsion points of E_0, a discrete set, and this implies that ϕ is constant. □

For example, if K is rational (i.e., $\mathcal{C} = \mathbb{P}^1$ so that $K = k(t)$), then $E(K) = E_0(k)$.

Corollary 6.2. *Let* $J_{\mathcal{C}}$ *be the Jacobian of* $\mathcal{C}$. *We have canonical isomorphisms*

$$E(K)/E(K)_{tor} \cong \mathrm{Hom}_{k-av}(J_{\mathcal{C}}, E_0) \cong \mathrm{Hom}_{k-av}(E_0, J_{\mathcal{C}}).$$

Proof. The Albanese property of the Jacobian of $\mathcal{C}$ (Subsection 5.1 of Lecture 0) gives a surjective homomorphism

$$\mathrm{Mor}_k(\mathcal{C}, E_0) \to \mathrm{Hom}_{k-av}(J_{\mathcal{C}}, E_0).$$

This homomorphism sends non-constant (and therefore surjective) morphisms to non-constant (surjective) homomorphisms, so its kernel consists exactly of the constant morphisms. The second isomorphism in the statement of the corollary follows from the fact that Jacobians are self-dual. □

By Poincaré complete reducibility [Mil86a, 12.1], $J_{\mathcal{C}}$ is isogenous to a product of simple abelian varieties. Suppose $J_{\mathcal{C}}$ is isogenous to $E_0^m \times A$ and A admits no non-zero morphisms to E_0. We say that "E_0 appears in $J_{\mathcal{C}}$ with multiplicity m." Then it is clear from the corollary that $E(K)/E(K)_{tor} \cong \mathrm{End}_k(E_0)^m$ and so the rank of $E(K)$ is m, $2m$, or $4m$.

Tate and Shafarevich used these ideas to exhibit isotrivial elliptic curves over $F = \mathbb{F}_p(t)$ of arbitrarily large rank. Indeed, using Tate's theorem on isogenies of abelian varieties over finite fields (reviewed in Section 6 of Lecture 0) and a calculation of zeta functions in terms of Gauss sums, they were able to produce a hyperelliptic curve $\mathcal{C}$ over $\mathbb{F}_p$ whose Jacobian is isogenous to $E_0^m \times A$ where E_0 is a supersingular elliptic curve and the multiplicity m is as large as desired. If $K = \mathbb{F}_p(\mathcal{C})$, E is the constant curve $E = E_0 \times F$, and E' is the twist of E by the quadratic extension K/F, then $\mathrm{Rank}\, E'(F) = \mathrm{Rank}\, E(K)$ and so $E'(F)$ has large rank by the analysis above. See the original article [TS67] for more details and a series of articles by Elkies (starting with [Elk94]) for a beautiful application to the construction of lattices with high packing densities.

7. Torsion

An immediate corollary of the MWLN theorem is that $E(K)_{tor}$ is finite. In fact, $E(K)_{tor}$ is isomorphic to a group of the form

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

where m divides n and p does not divide m. (See for example [Sil09, Ch. 3].) One can also see using the theory of modular curves that every such group appears for a suitable K and E.

In another direction, one can give uniform bounds on torsion that depend only on crude invariants of the field K.

Indeed, in the constant case, $E(K)_{tor} \cong E_0(\mathbb{F}_q)$ which has order bounded by $(q^{1/2}+1)^2$. In the isotrivial case, there is a finite extension K' with the same field of constants $k = \mathbb{F}_q$ over which E becomes constant. Thus $E(K)_{tor} \subset E(L)_{tor}$ again has cardinality bounded by $(q^{1/2}+1)^2$.

We now turn to the non-isotrivial case.

Proposition 7.1. *Assume that E is non-isotrivial and let $g_{\mathcal{C}}$ be the genus of $\mathcal{C}$. Then there is a finite (and effectively calculable) list of groups—depending only on $g_{\mathcal{C}}$ and p—such that for any non-isotrivial elliptic curve E over K, $E(K)_{tor}$ appears on the list.*

Proof. (Sketch) First consider the prime-to-p torsion subgroup of $E(K)$. It has the form $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ where $m|n$ and $p \not| \, m$. There is a modular curve $X(m,n)$, irreducible and defined over $\mathbb{F}_p(\mu_m)$, that is a coarse moduli space for elliptic curves with subgroups isomorphic to G. We get a morphism $\mathcal{C} \to X(m,n)$ which is non-constant (because E is non-isotrivial) and therefore surjective. The Riemann-Hurwitz formula then implies that $g_{\mathcal{C}} \geq g_{X(m,n)}$. But the genus of $X(m,n)$ goes to infinity with n. Indeed, $g_{X(m,n)} \geq g_{X(1,n)}$ and standard

genus formulae ([Miy06, 4.2]) together with crude estimation show that the latter is bounded below by

$$1 + \frac{n^2}{24\zeta(2)} - \frac{n \log_2 n}{4}.$$

This shows that for a fixed value of $g_{\mathcal{C}}$, only finitely many groups G as above can appear as $E(K)_{tor}$.

The argument for p-torsion is similar, except that ones uses the Igusa curves $Ig(p^n)$ (cf. [KM85, Ch. 12]). If $E(K)$ has a point of order p^n, we get a non-constant morphism $\mathcal{C} \to Ig(p^n)$ and the genus of $Ig(p^n)$ is asymptotic to $p^{2n}/48$ [Igu68, p. 96]. □

This proposition seems to have been rediscovered repeatedly over the years. The first reference I know of is [Lev68].

Since the genus of a function field is an analogue of the discriminant (more precisely q^{2g-2} is an analogue of the absolute value of the discriminant of a number field), the proposition is an analogue of bounding $E(K)_{tor}$ in terms of the discriminant of a number field K. One could ask for a strengthening where torsion is bounded by "gonality", i.e., by the smallest degree of a non-constant map $\mathcal{C} \to \mathbb{P}^1$. This would be an analogue of bounding $E(K)_{tor}$ in terms of the degree of a number field K, as in the theorems of Mazur, Kamienny, and Merel [Mer96]. This is indeed possible and can be proven by mimicking the proof of the proposition, replacing bounds on the genus of the modular curve with bounds on its gonality. See [Poo07] for the best results currently known on gonality of modular curves.

Exercise 7.2. Compute the optimal list mentioned in the proposition for $g = 0$. (This is rather involved.) Note that the optimal list in fact depends on p. Indeed, $\mathbb{Z}/11\mathbb{Z}$ is on the list if and only if $p = 11$.

One can be very explicit about p-torsion:

Proposition 7.3. *Suppose that E is a non-isotrivial elliptic curve over K. Then $E(K)$ has a point of order p if and only if $j(E) \in K^p$ and $A(E, \omega)$ is a $(p-1)$st power in $K^\times$.*

Note that whether $A(E, \omega)$ is a $(p-1)$st power is independent of the choice of the differential ω.

Proof. Let $E \xrightarrow{\mathrm{Fr}} E^{(p)} \xrightarrow{V} E$ be the standard factorization of multiplication by p into Frobenius and Verschiebung. Recall (e.g., [Ulm91, 2.1]) that $A(E, \omega)$ is a $(p-1)$st power in K if and only if $\ker \mathrm{Fr} \cong \mu_p$ if and only if $\ker V \cong \mathbb{Z}/p\mathbb{Z}$ if and only if there is a non-trivial p-torsion point in $E^{(p)}(K)$.

Now suppose that $P \in E(K)$ is a non-trivial p-torsion point. Then $\mathrm{Fr}(P)$ is a non-trivial p-torsion point in $E^{(p)}(K)$ and so $A(E, \omega)$ is a $(p-1)$st power in K. Let E' be the quotient of E by the cyclic subgroup generated by P: $E' = E/\langle P \rangle$. Since $\langle P \rangle$ is in the kernel of multiplication by p, we have a factorization of multiplication by p:

$$[p] : E \to E' \to E.$$

Since $E \to E'$ is étale of degree p and $[p]$ is inseparable of degree p^2, we have that $E' \to E$ is purely inseparable of degree p. But an elliptic curve in characteristic p has a unique inseparable isogeny of degree p (namely the quotient by the unique

connected subgroup of order p, the kernel of Frobenius) so we have an identification $E = E'^{(p)}$. By 2.1, $j(E) \in K^p$.

Conversely, suppose $A(E,\omega)$ is a $(p-1)$st power and $j(E) \in K^p$. Let E' be the elliptic curve such that $E'^{(p)} \cong E$. Given a differential ω on E, there is a differential ω' on E' such that $A(E,\omega) = A(E',\omega')^p$ (as can be seen for example by using Weierstrass equations). It follows that $A(E',\omega')$ is also a $(p-1)$st power in K. Thus we have a non-trivial point of order p in $E'^{(p)}(K) = E(K)$. □

Part of the proposition generalizes trivially by iteration: if $E(K)$ has a point of order p^n, then $j(E) \in K^{p^n}$. A full characterization of p^n torsion seems harder—the condition that $A(E,\omega)$ be a $(p-1)$st power is closely related to the equations defining the Igusa curve $Ig(p)$ ([KM85, 12.8]), but we do not have such explicit equations for $Ig(p^n)$ when $n > 1$.

8. Local invariants

Let E be an elliptic curve over K and let v be a place of K. A model (1.1.2) for E with coefficients in the valuation ring $\mathcal{O}_{(v)}$ is said to be *integral at* v. The valuation of the discriminant Δ of an integral model is a non-negative integer and so there are models where this valuation takes its minimum value. Such models are *minimal integral models at* v.

Choose a model for E that is minimal integral at v:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\overline{a}_i \in \kappa(v)$ be the reductions of the coefficients and let E_v be the plane cubic

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6 \tag{8.1}$$

over the residue field κ_v. It is not hard to check using Weierstrass equations that the isomorphism type of the reduced cubic (8.1) is independent of the choice of minimal model.

If the discriminant of a minimal integral model at v has valuation zero, i.e., is a unit at v, then the reduced equation defines an elliptic curve over κ_v. If the minimal valuation is positive, then the reduced curve is singular. We distinguish three cases according to the geometry of the reduced curve.

Definition 8.2.

(1) If E_v is a smooth cubic, we say E has *good reduction at* v.
(2) If E_v is a nodal cubic, we say E has *multiplicative reduction at* v. If the tangent lines at the node are rational over $\kappa(v)$ we say the reduction is *split multiplicative* and if they are rational only over a quadratic extension, we say the reduction is *non-split multiplicative*.
(3) If E_v is a cuspidal cubic, we say E has *additive reduction*.

Define an integer a_v as follows:

$$a_v = \begin{cases} q_v + 1 - \#E_v(\kappa_v) & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has split multiplicative reduction at } v \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } v \\ 0 & \text{if } E \text{ has additive reduction at } v \end{cases} \tag{8.3}$$

Exercise 8.4. To make this definition less *ad hoc*, note that in the good reduction case, the numerator of the ζ-function of the reduced curve is $1 - a_v q_v^{-s} + q_v^{1-2s}$. Show that in the bad reduction cases, the ζ-function of the reduced curve is

$$\frac{1 - a_v q_v^{-s}}{(1 - q_v^{-s})(1 - q_v^{1-s})}.$$

In the good reduction case, the results about zeta functions and étale cohomology reviewed in Lecture 0, Sections 3 and 4 imply the "Hasse bound": $|a_v| \leq 2\sqrt{q_v}$.

There are two more refined invariants in the bad reduction cases: the Néron model and the conductor. The local exponent of the conductor at v, denoted n_v is defined as

$$n_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has multiplicative reduction at } v \\ 2 + \delta_v & \text{if } E \text{ has additive reduction at } v \end{cases} \tag{8.5}$$

Here δ_v is a non-negative integer that is 0 when $p > 3$ and is ≥ 0 when $p = 2$ or 3. We refer to [Tat75] for a definition and an algorithm to compute δ_v.

The (global) conductor of E is defined to be the divisor $\mathfrak{n} = \sum_v n_v[v]$. Its degree is $\deg \mathfrak{n} = \sum_v n_v \deg v$.

The Néron model will be discussed in Lecture 3 below.

Exercise 8.6. Mimic [Sil09, Ch. VII] to define a filtration on the points of E over a completion K_v of K. Show that the prime-to-p part of $E(K)_{tor}$ maps injectively into $E(K_v)/E(K_v)_1$. Relate $E(K_v)/E(K_v)_1$ to the special fiber of the Néron model of E at v. As in the classical case, this gives an excellent way to bound the prime-to-p part of $E(K)_{tor}$.

9. The L-function

We define the L-function of E/K as an Euler product:

$$L(E,T) = \prod_{\text{good } v} \left(1 - a_v T^{\deg v} + q_v T^{2\deg v}\right)^{-1} \prod_{\text{bad } v} \left(1 - a_v T^{\deg v}\right)^{-1} \tag{9.1}$$

and

$$L(E,s) = L(E, q^{-s}).$$

(Here T is a formal indeterminant and s is a complex number. Unfortunately, there is no standard reasonable parallel of the notations Z and ζ to distinguish the function of T and the function of s.) Because of the Hasse bound on the size of a_v, the product converges absolutely in the region $\operatorname{Re} s > 3/2$, and as we will see below, it has a meromorphic continuation to all s.

When E is constant it is elementary to calculate $L(E,s)$ in terms of the zeta-functions of E_0 and $\mathcal{C}$.

Exercise 9.2. Suppose that $E = E_0 \times_k K$. Write the ζ-functions of E_0 and $\mathcal{C}$ as rational functions:

$$\zeta(E_0, s) = \frac{\prod_{i=1}^{2}(1 - \alpha_i q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

and

$$\zeta(\mathcal{C}, s) = \frac{\prod_{j=1}^{2g_C}(1 - \beta_j q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}.$$

Prove that

$$L(E,s) = \frac{\prod_{i,j}(1-\alpha_i\beta_j q^{-s})}{\prod_{i=1}^{2}(1-\alpha_i q^{-s})\prod_{i=1}^{2}(1-\alpha_i q^{1-s})}.$$

Thus $L(E,s)$ is a rational function in q^{-s} of degree $4g_{\mathcal{C}}-4$, it extends to a meromorphic function of s, and it satisfies a functional equation for $s \leftrightarrow 2-s$. Its poles lie on the lines $\operatorname{Re} s = 1/2$ and $\operatorname{Re} s = 3/2$ and its zeroes lie on the line $\operatorname{Re} s = 1$.

Although the proofs are much less elementary, these facts extend to the non-constant case as well:

Theorem 9.3. *Suppose the E is a non-constant elliptic curve over K. Let $\mathfrak{n}$ be the conductor of E. Then $L(E,s)$ is a polynomial in q^{-s} of degree $N = 4g_{\mathcal{C}} - 4 + \deg \mathfrak{n}$, it satisfies a functional equation for $s \leftrightarrow 2-s$, and its zeroes lie on the line $\operatorname{Re} s = 1$. More precisely,*

$$L(E,s) = \prod_{i=1}^{N}(1-\alpha_i q^{-s})$$

where each α_i is an algebraic integer of absolute value q in every complex embedding. The collection of α_i (with multiplicities) is invariant under $\alpha_i \mapsto q^2/\alpha_i$.

The theorem is a combination of results of Grothendieck, Deligne, and others. We will sketch a proof of it in Lecture 4.

Note that in all cases $L(E,s)$ is holomorphic at $s=1$. In the non-constant case, its order of vanishing at $s=1$ is bounded above by N and it equals N if and only if $L(E,s) = (1-q^{1-s})^N$.

10. The basic BSD conjecture

This remarkable conjecture connects the analytic behavior of the function $L(E,s)$, constructed from local data, to the Mordell-Weil group, a global invariant.

Conjecture 10.1 (Birch and Swinnerton-Dyer)**.**

$$\operatorname{Rank} E(K) = \operatorname{ord}_{s=1} L(E,s)$$

The original conjecture was stated only for elliptic curves over $\mathbb{Q}$ [BSD65] but it is easily seen to make sense for abelian varieties over global fields. There is very strong evidence in favor of it, especially for elliptic curves over $\mathbb{Q}$ and abelian varieties over function fields. See [Gro10, Lecture 3, §4] for a summary of the best theoretical evidence in the number field case. We will discuss what is known for elliptic curves in the function field case later in this course. See Section 12 for statements of the main results and [Ulm11] for a discussion of the case of higher dimensional abelian varieties over function fields.

11. The Tate-Shafarevich group

We define the Tate-Shafarevich group of E over K as

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right).$$

Here the cohomology groups can be taken to be Galois cohomology groups:

$$H^1(K,E) = H^1(G_K, E(K^{sep}))$$

and similarly for $H^1(K_v, E)$; or they can be taken as étale or flat cohomology groups of $\operatorname{Spec} K$ with coefficients in the sheaf associated to E. The flat cohomology definition is essential for proving finer results on p-torsion in $Ш(E/K)$.

Exercise 11.1. Show that the group $H^1(K, E)$ (and therefore $Ш(E/K)$) is torsion. Hint: Show that given a class $c \in H^1(K, E)$, there is a finite Galois extension L/K such that c vanishes in $H^1(L, E)$.

The refined BSD conjecture relates the leading coefficient of $L(E, s)$ at $s = 1$ to invariants of E including heights, Tamagawa numbers, and the order of $Ш(E/K)$. In particular, the conjecture that $Ш(E/K)$ is finite is included in the refined BSD conjecture. We will not discuss that conjecture in these lectures, so we refer to [Gro10] and [Ulm11] for more details.

12. Statements of the main results

Much is known about the BSD conjecture over function fields. We start with general results.

Theorem 12.1. *Let E be an elliptic curve over a function field K. Then we have:*

1. $\operatorname{Rank} E(K) \leq \operatorname{ord}_{s=1} L(E, s)$.
2. *The following are equivalent:*
   - $\operatorname{Rank} E(K) = \operatorname{ord}_{s=1} L(E, s)$
   - *$Ш(E/K)$ is finite*
   - *for any one prime number ℓ ($\ell = p$ is allowed), the ℓ-primary part $Ш(E/K)_{\ell^\infty}$ is finite.*
3. *If K'/K is a finite extension and if the BSD conjecture holds for E over K', then it holds for E over K.*

The theorem was proven by Tate [Tat66b] and Milne [Mil75] and we will sketch a proof in Lecture 3. When the equivalent conditions of Item 2 hold, it turns out that the refined BSD conjecture automatically follows. (This is also due to Tate and Milne and will be discussed in detail in [Ulm11].)

We now state several special cases where the conjecture is known to be true. As will be seen in the sequel, they all ultimately reduce either to Tate's theorem on isogenies of abelian varieties over finite fields (Theorem 6.1 of Lecture 0) or to a theorem of Artin and Swinnerton-Dyer on $K3$ surfaces [ASD73].

Theorem 12.2. *If E is an isotrivial elliptic curve over a function field K, then the BSD conjecture holds for E.*

Recall that a constant curve is also isotrivial.

To state the next result, we make an *ad hoc* definition. If E is an elliptic curve over $K = \mathbb{F}_q(t)$ we define the *height* h of E to be the smallest non-negative integer such that E can be defined by a Weierstrass equation (1.1.1) where the a_i are all polynomials and $\deg(a_i) \leq hi$. For example, the curves E_1 and E_2 in Subsection 1.2 have height $h = 0$ and the other curves $E_3, \dots E_9$ there all have height $h = 1$. See Section 4 of Lecture 3 below for a more general definition.

Theorem 12.3. *Suppose that $K = k(t)$ and that E is an elliptic curve over K of height $h \leq 2$. Then the BSD conjecture holds for E.*

Note that this case overlaps the preceding one since an elliptic curve over $k(t)$ is constant if and only if its height is zero (cf. Proposition 4.1 in Lecture 3).

The following case is essentially due to Shioda [Shi86]. To state it, consider a polynomial f in three variables with coefficients in k which is the sum of exactly 4 non-zero monomials, say

$$f = \sum_{i=1}^{4} c_i \prod_{j=1}^{3} x_j^{e_{ij}}$$

where the $c_i \in k$ are non-zero. Set $e_{i4} = 1 - \sum_{j=1}^{3} e_{ij}$ and let A be the 4×4 integer matrix $A = (e_{ij})$. If $\det A \neq 0 \pmod p$, we say that f *satisfies Shioda's condition*. Note that the condition is independent of the order of the variables x_j.

Theorem 12.4. *Suppose that $K = k(t)$ and that E is an elliptic curve over K. Suppose that E is birational to a plane curve $V(f) \subset \mathbb{A}^2_K$ where f is a polynomial in $k[t, x, y] \subset K[x, y]$ which is the sum of exactly 4 non-zero monomials and which satisfies Shioda's condition. Then the BSD conjecture holds for E.*

For example, the theorem applies to the curves E_4, E_7, E_8, and E_9 of Subsection 1.2 over $K = \mathbb{F}_q(t)$ for any prime power q. It applies more generally to these curves when t is replaced by t^d for any d prime to p. Note that when d is large, the height of the curve is also large, and so we get cases of BSD not covered by Theorem 12.3.

Finally we state another more recent and ultimately much more flexible special case due to Lisa Berger [Ber08].

Theorem 12.5. *Suppose that $K = k(t)$ and that E is an elliptic curve over K. Suppose that E is birational to a plane curve of the form*

$$f(x) = t^d g(y)$$

where f and g are rational functions of one variable and d is prime to p. Then the BSD conjecture holds for E.

Here one should clear denominators to interpret the equation $f = t^d g$ (or work in a Zariski open subset of the plane). For example, if $f(x) = x(x-1)$ and $g(y) = y^2/(1-y)$ then we have the plane curve over $K = k(t)$ defined by

$$x(x-1)(1-y) = t^d y^2$$

which turns out to be birational to

$$y^2 + xy + t^d y = x^3 + t^d x^2.$$

13. The rest of the course

The remainder of these lectures will be devoted to sketching the proofs of most of the main results and applying them to construct elliptic curves of large rank over function fields.

More precisely, in Lecture 2 we will review facts about surfaces and the Tate conjecture on divisors. This is a close relative of the BSD conjecture.

In Lecture 3 we will explain the relationship between the BSD and Tate conjectures and use it to prove the part of Theorem 12.1 related to $\ell \neq p$ as well as most of the other theorems stated in the previous section.

In Lecture 4 we will recall a general result on vanishing of L-functions in towers and combine it with the results above to obtain many elliptic curves of arbitrarily large rank.

In Lecture 5, we will give other applications of these ideas to ranks of elliptic curves and explicit points.

LECTURE 2

Surfaces and the Tate conjecture

1. Motivation

Consider an elliptic curve E/K and suppose that $K = k(t)$ and that we choose an equation for E as in Lecture 1, equation (1.1.2) where the a_i are in $k[t]$. Then (1.1.2), viewed in $K[x, y]$, defines an affine open subset of an elliptic curve E. But if we view it as an equation in $k[t, x, y]$, it defines an affine surface with a projection to the affine t line. The generic fiber of this projection is the affine curve just mentioned.

With a little more work (discussed in the next lecture), for any E over $K = k(\mathcal{C})$ we can define a smooth projective surface $\mathcal{E}$ over k with a morphism $\pi : \mathcal{E} \to \mathcal{C}$ whose generic fiber is E. Obviously there will be close connection between the arithmetic of $\mathcal{E}$ and that of E. Although $\mathcal{E}$ has higher dimension than E, it is defined over the finite field k and as a result we have better control over its arithmetic. Pursuing this line of inquiry leads to the main theorems stated at the end of the previous section.

In this lecture, we discuss the relevant facts and conjectures about surfaces over finite fields. In the next lecture we will look carefully at the connections between $\mathcal{E}$ and E and deduce the main classical theorems.

There are many excellent references for the general theory of surfaces, including [Bea96], [BHPV04], and [Bǎd01]. We generally refer to [Bǎd01] below since it works throughout over a field of arbitrary characteristic.

2. Surfaces

Let $k = \mathbb{F}_q$ be a finite field of characteristic p. As always, by a surface over k we mean a purely 2-dimensional, separated, reduced scheme of finite type over k. Such a scheme is automatically quasi-projective and is projective if and only if it is complete [Bǎd01, 1.28]. Since k is perfect, a surface $\mathcal{X}$ is a regular scheme if and only if $\mathcal{X} \to \operatorname{Spec} k$ is a smooth morphism (e.g., [Liu02, 4.3.3, Exer. 3.24]). We sloppily say that "$\mathcal{X}$ is smooth" if these conditions hold. Resolution of singularities is known for surfaces: For any surface $\mathcal{X}$, there is a proper birational morphism $\tilde{\mathcal{X}} \to \mathcal{X}$ with $\tilde{\mathcal{X}}$ smooth. (We may even take this morphism to be a composition of normalizations and blow ups at closed points [Lip78]. See also [Art86] for a nice exposition.) Therefore, every surface is birational to a smooth projective surface. In the cases of interest to us, this can be made very explicit in an elementary manner.

Throughout we assume that $\mathcal{X}$ is a smooth, projective, absolutely irreducible surface over k and we assume that $\mathcal{X}(k)$ is non-empty, i.e., $\mathcal{X}$ has a k-rational point.

3. Divisors and the Néron-Severi group

We give a lightning review of divisors and equivalence relations on divisors. See, for example, [Har77, V.1] for more details.

3.1. Divisor classes

A (Weil) *divisor* is a finite formal $\mathbb{Z}$-linear combination of reduced, closed, codimension 1 subvarieties of $\mathcal{X}$:

$$D = \sum a_Z Z.$$

In other words, the set of divisors is the free abelian group on the reduced, closed, codimension 1 subvarieties on $\mathcal{X}$.

If Z is a reduced, closed subvariety of $\mathcal{X}$ of codimension 1, there is an associated valuation

$$\mathrm{ord}_Z : k(\mathcal{X})^\times \to \mathcal{Z}$$

that sends a rational function to its order of zero or pole along Z.

A rational function f on $\mathcal{X}$ has a divisor:

$$\mathrm{Div}(f) = \sum_Z \mathrm{ord}_Z(f) Z.$$

A divisor D is said to be *linearly equivalent to zero* if there is a rational function f such that $\mathrm{Div}(f) = D$. Two divisors D and D' are linearly equivalent if their difference $D - D'$ is linearly equivalent to zero.

The group of divisors modulo those linear equivalent to zero is the *divisor class group* $DivCl(\mathcal{X})$. It is a fundamental invariant of $\mathcal{X}$.

3.2. The Picard group

Let $\mathrm{Pic}(\mathcal{X})$ be the Picard group of $\mathcal{X}$, i.e., the group of isomorphism classes of invertible sheaves on $\mathcal{X}$ with group law given by the tensor product. There is a cohomological calculation of $\mathrm{Pic}(\mathcal{X})$:

$$\mathrm{Pic}(\mathcal{X}) \cong H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}^\times).$$

The map sending a divisor D to the invertible sheaf $\mathcal{O}_{\mathcal{X}}(D)$ induces an isomorphism $DivCl(\mathcal{X}) \tilde{\to} \mathrm{Pic}(\mathcal{X})$.

3.3. The Néron-Severi group

As usual, we write $\overline{\mathcal{X}}$ for $\mathcal{X} \times_k \overline{k}$. We first introduce the notion of algebraic equivalence for divisors on $\overline{\mathcal{X}}$. Intuitively, two divisors D and D' are algebraically equivalent if they lie in a family parameterized by a connected variety (which we may take to be a smooth curve). More precisely, if T is a smooth curve over $\overline{k}$ and $\mathcal{D} \subset \mathcal{X} \times_{\overline{k}} T$ is a divisor that is flat over T, then we get a family of divisors on $\mathcal{X}$ parameterized by T: $t \in T$ corresponds to $\mathcal{X} \times \{t\} \cap \mathcal{D}$. Two divisors D_1 and D_2 on $\mathcal{X}$ are algebraically equivalent if they lie in such a family, i.e., if there is a curve T and a divisor $\mathcal{D}$ as above and two points t_1 and $t_2 \in T(\overline{k})$ such that $D_i = \mathcal{X} \times_{\overline{k}} \{t_i\} \cap \mathcal{D}$. (*A priori*, to ensure transitivity of this relation we should use chains of equivalences (see [Har77, Exer. V.1.7]) but see [Ful84, 10.3.2] for an argument that shows the definition works as is.) Note that linear equivalence is algebraic equivalence where T is restricted to be $\mathbb{P}^1$ ([Har77, Exer. V.1.7]) and so algebraic equivalence is weaker than linear equivalence.

The group of divisors on $\overline{\mathcal{X}}$ modulo those algebraically equivalent to zero is the *Néron-Severi* group $\mathrm{NS}(\overline{\mathcal{X}})$. A classical (and difficult) theorem, the "theorem of

the base," says that $\mathrm{NS}(\overline{\mathcal{X}})$ is finitely generated. See [LN59] and [SGA6, XIII.5.1] for proofs and Lecture 3 below for more discussion. See also [Con06] for a modern discussion of the results in [LN59].

Since linear equivalence is weaker than algebraic equivalence, $\mathrm{NS}(\overline{\mathcal{X}})$ is a quotient of $\mathrm{Pic}(\overline{\mathcal{X}})$.

We define $\mathrm{NS}(\mathcal{X})$ to be the image of $\mathrm{Div}(\mathcal{X})$ in $\mathrm{NS}(\overline{\mathcal{X}})$ or equivalently the image of $\mathrm{Pic}(\mathcal{X})$ in $\mathrm{NS}(\overline{\mathcal{X}})$. Thus $\mathrm{NS}(\mathcal{X})$ is again a finitely generated abelian group. As we will see, it is of arithmetical nature.

Exercise 3.3.1. Let $G_k = \mathrm{Gal}(\overline{k}/k)$. Show that $\mathrm{NS}(\mathcal{X})$ is the group of invariants $\mathrm{NS}(\overline{\mathcal{X}})^{G_k}$. You will need to use that k is a finite field.

4. The Picard scheme

We define $\mathrm{Pic}^0(\mathcal{X})$ as the kernel of the surjection $\mathrm{Pic}(\mathcal{X}) \to \mathrm{NS}(\mathcal{X})$. In order to understand this group better, we will introduce more structure on the Picard group. The main fact we need to know is that the group $\mathrm{Pic}^0(\mathcal{X} \times \overline{k})$ is the set of points on an abelian variety and is therefore a divisible group. (I.e., for every class $c \in \mathrm{Pic}^0(\mathcal{X} \times \overline{k})$ and every positive integer n, there is a class c' such that $n\,c' = c$.) Readers willing to accept this assertion can skip the rest of this section.

The Picard group $\mathrm{Pic}(\mathcal{X})$ is the set of k-points of a group scheme. More precisely, under our hypotheses on $\mathcal{X}$ there is a group scheme called the *Picard scheme* and denoted $\underline{\mathrm{Pic}}_{\mathcal{X}/k}$ which is locally of finite type over k and represents the relative Picard functor. This means that if $T \to S = \operatorname{Spec} k$ is a morphism of schemes and $\pi_T : \mathcal{X}_T := \mathcal{X} \times_{\operatorname{Spec} k} T \to T$ is the base change then

$$\underline{\mathrm{Pic}}_{\mathcal{X}/k}(T) = \frac{\mathrm{Pic}(\mathcal{X}_T)}{\pi_T^* \mathrm{Pic}(T)}.$$

Here the left hand side is the group of T-valued points of $\underline{\mathrm{Pic}}_{\mathcal{X}/k}$. See [Kle05] for a thorough and detailed overview of the Picard scheme, and in particular [Kle05, 9.4.8] for the proof that there is a scheme representing the relative Picard functor as above.

We write $\underline{\mathrm{Pic}}^0_{\mathcal{X}/k}$ for the connected component of $\underline{\mathrm{Pic}}_{\mathcal{X}/k}$ containing the identity. Under our hypotheses, $\underline{\mathrm{Pic}}^0_{\mathcal{X}/k}$ is a geometrically irreducible projective group scheme over k [Kle05, 9.5.3, 9.5.4]. It may be non-reduced. (See examples in [Igu55] and [Ser58] and a full analysis of this phenomenon in [Mum66].) We let $\mathrm{PicVar}_{\mathcal{X}/k} = \left(\underline{\mathrm{Pic}}^0_{\mathcal{X}/k}\right)_{red}$, the *Picard variety* of $\mathcal{X}$ over k, which is an abelian variety over k.

If k' is a field extension of k, we have

$$\mathrm{Pic}^0(\mathcal{X}_{k'}) = \underline{\mathrm{Pic}}^0_{\mathcal{X}/k}(k') = \mathrm{PicVar}_{\mathcal{X}/k}(k')$$

so that $\mathrm{Pic}^0(\mathcal{X}_{k'})$ is the set of points of an abelian variety.

By [Kle05, 9.5.10], $\underline{\mathrm{Pic}}^0_{\mathcal{X}/k}(k) = \mathrm{Pic}^0(\mathcal{X})$, in other words, the class of a divisor in $\underline{\mathrm{Pic}}(\mathcal{X})$ lies in $\underline{\mathrm{Pic}}^0(\mathcal{X})$ if and only if the divisor is algebraically equivalent to 0.

5. Intersection numbers and numerical equivalence

There is an intersection pairing on the Néron-Severi group:

$$\mathrm{NS}(\mathcal{X}) \times \mathrm{NS}(\mathcal{X}) \to \mathbb{Z}$$

which is bilinear and symmetric. If D and D' are divisors, we write $D.D'$ for their intersection pairing.

There are two approaches to defining the pairing. In the first approach, one shows that given two divisors, there are divisors in the same classes in $\mathrm{NS}(\mathcal{X})$ (or even the same classes in $\mathrm{Pic}(\mathcal{X})$) that meet transversally. Then the intersection number is literally the number of points of intersection. The work in this approach is to prove a moving lemma and then show that the resulting pairing is well defined. See [Har77, V.1] for the details.

In the second approach, one uses coherent cohomology. If $\mathcal{L}$ is an invertible sheaf on $\mathcal{X}$, let

$$\chi(\mathcal{L}) = \sum_{i=0}^{2} (-1)^i \dim_k H^i(\mathcal{X}, \mathcal{L})$$

be the coherent Euler characteristic of $\mathcal{L}$. Then define

$$D.D' = \chi(\mathcal{O}_\mathcal{X}) - \chi(\mathcal{O}_\mathcal{X}(-D)) - \chi(\mathcal{O}_\mathcal{X}(-D')) + \chi(\mathcal{O}_\mathcal{X}(-D-D')).$$

One checks that if C is a smooth irreducible curve on $\mathcal{X}$, then $C.D = \deg \mathcal{O}_\mathcal{X}(D)|_C$ and that if C and C' are two distinct irreducible curves on $\mathcal{X}$ meeting transversally, then $C.C'$ is the sum of local intersection multiplicities. See [Bea96, I.1-7] for details. (Nowhere is it used in this part of [Bea96] that the ground field is $\mathbb{C}$.)

Two divisors D and D' are said to be *numerically equivalent* if $D.D'' = D'.D''$ for all divisors D''. If $\mathrm{Num}(\mathcal{X})$ denotes the group of divisors in $\mathcal{X}$ up to numerical equivalence, then we have surjections

$$\mathrm{Pic}(\mathcal{X}) \twoheadrightarrow \mathrm{NS}(\mathcal{X}) \twoheadrightarrow \mathrm{Num}(\mathcal{X})$$

and so $\mathrm{Num}(\mathcal{X})$ is a finitely generated group. It is clear from the definition that $\mathrm{Num}(\mathcal{X})$ is torsion-free and so we can insert $\mathrm{NS}(\mathcal{X})/tor$ (Néron-Severi modulo torsion) into this chain:

$$\mathrm{Pic}(\mathcal{X}) \twoheadrightarrow \mathrm{NS}(\mathcal{X}) \twoheadrightarrow \mathrm{NS}(\mathcal{X})/tor \twoheadrightarrow \mathrm{Num}(\mathcal{X}).$$

6. Cycle classes and homological equivalence

There is a general theory of cycle classes in ℓ-adic cohomology, see for example [SGA4$\frac{1}{2}$, [Cycle]]. In the case of divisors, things are much simpler and we can construct a cycle class map from the Kummer sequence.

Indeed, consider the short exact sequence of sheaves on $\overline{\mathcal{X}}$ for the étale topology:

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \to 0.$$

(The sheaves μ_{ℓ^n} and $\mathbb{G}_m$ are perfectly reasonable sheaves in the Zariski topology on $\mathcal{X}$, but the arrow in the right is not surjective in that context. We need to use the étale topology or a finer one.) Taking cohomology, we get a homomorphism

$$Pic(\overline{\mathcal{X}})/\ell^n = H^1(\overline{\mathcal{X}}, \mathbb{G}_m)/\ell^n \to H^2(\overline{\mathcal{X}}, \mu_{\ell^n}).$$

Since $\mathrm{Pic}^0(\overline{\mathcal{X}})$ is a divisible group, we have $\mathrm{NS}(\overline{\mathcal{X}})/\ell^n = \mathrm{Pic}(\overline{\mathcal{X}})/\ell^n$ and so taking an inverse limit gives an injection

$$\mathrm{NS}(\overline{\mathcal{X}}) \otimes \mathbb{Z}_\ell \to H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1)).$$

Composing with the natural homomorphism $\mathrm{NS}(\mathcal{X}) \to \mathrm{NS}(\overline{\mathcal{X}})$ gives our cycle class map

$$\mathrm{NS}(\mathcal{X}) \to \mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell \to H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1)). \tag{6.1}$$

We declare two divisors to be (ℓ-)*homologically equivalent* if their classes in $H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))$ are equal. (We will see below that this notion is independent of ℓ.) The group of divisors modulo homological equivalence will (temporarily) be denoted $\mathrm{Homol}(\mathcal{X})$. It will turn out to be a finitely generated free abelian group.

The intersection pairing on $NS(\mathcal{X})$ corresponds under the cycle class map to the cup product on cohomology. This means that a divisor that is homologically equivalent to zero is also numerically equivalent to zero. Thus we have a chain of surjections:

$$\mathrm{Pic}(\mathcal{X}) \twoheadrightarrow \mathrm{NS}(\mathcal{X}) \twoheadrightarrow \mathrm{NS}(\mathcal{X})/tor \twoheadrightarrow \mathrm{Homol}(\mathcal{X}) \twoheadrightarrow \mathrm{Num}(\mathcal{X}).$$

7. Comparison of equivalence relations on divisors

A theorem of Matsusaka [Mat57] asserts that the surjection

$$\mathrm{NS}(\mathcal{X})/tor \twoheadrightarrow \mathrm{Num}(\mathcal{X})$$

is in fact an isomorphism. Thus

$$\mathrm{NS}(\mathcal{X})/tor \cong \mathrm{Homol}(\mathcal{X}) \cong \mathrm{Num}(\mathcal{X})$$

and these groups are finitely generated, free abelian groups. Since $\mathrm{NS}(\mathcal{X})$ is finitely generated, $\mathrm{NS}(\mathcal{X})_{tor}$ is finite.

In all of the examples we will consider, $\mathrm{NS}(\mathcal{X})$ is torsion free. (In fact, for an elliptic surface with a section, the surjection $\mathrm{NS}(\mathcal{X}) \to \mathrm{Num}(\mathcal{X})$ is always an isomorphism, see [SS09, Theorem 6.5].) So to understand $\mathrm{Pic}(\mathcal{X})$ we have only to consider the finitely generated free abelian group $\mathrm{NS}(\mathcal{X})$ and the group $\mathrm{Pic}^0(\mathcal{X})$, which is (the set of points of) an abelian variety.

Exercise 7.1. In the case of a surface $\mathcal{X}$ over the complex numbers, use the cohomology of the exponential sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_{\mathcal{X}} \xrightarrow{\exp} \mathcal{O}_{\mathcal{X}}^\times \to 0$$

to analyze the structure of $\mathrm{Pic}(\mathcal{X})$.

8. Examples

8.1. $\mathbb{P}^2$

It is well known (e.g., [Har77, II.6.4]) that two curves on $\mathbb{P}^2$ are linearly equivalent if and only if they have the same degree. It follows that $\mathrm{Pic}(\mathbb{P}^2) = \mathrm{NS}(\mathbb{P}^2) \cong \mathbb{Z}$.

8.2. $\mathbb{P}^1 \times \mathbb{P}^1$

By [Har77, II.6.6.1], two curves on $\mathbb{P}^1 \times \mathbb{P}^1$ are linearly equivalent if and only if they have the same bi-degree. It follows that $\mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) = \mathrm{NS}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z}^2$.

8.3. Abelian varieties

If $\mathcal{X}$ is an abelian variety (of any dimension g), then $\mathrm{Pic}^0(\mathcal{X})$ is the dual abelian variety and $\mathrm{NS}(\mathcal{X})$ is a finitely generated free abelian group of rank between 1 and $4g^2$. See [Mum08] for details.

8.4. Products of curves

Suppose that $\mathcal{C}$ and $\mathcal{D}$ are smooth projective curves over k with k-rational points $x \in \mathcal{C}$ and $y \in \mathcal{D}$. By definition (see Subsection 5.1 of Lecture 0), the group of divisorial correspondences between $(\mathcal{C}, x)$ and $(\mathcal{D}, y)$ is a subgroup of $\mathrm{Pic}(\mathcal{C} \times \mathcal{D})$ and it is clear that

$$\begin{aligned}\mathrm{Pic}(\mathcal{C} \times \mathcal{D}) &\cong \mathrm{Pic}(\mathcal{C}) \times \mathrm{Pic}(\mathcal{D}) \times \mathrm{DivCorr}\left((\mathcal{C}, x), (\mathcal{D}, y)\right) \\ &\cong \mathrm{Pic}^0(\mathcal{C}) \times \mathrm{Pic}^0(\mathcal{D}) \times \mathbb{Z}^2 \times \mathrm{DivCorr}\left((\mathcal{C}, x), (\mathcal{D}, y)\right).\end{aligned}$$

Moreover, as we saw in Lecture 0,

$$\mathrm{DivCorr}\left((\mathcal{C}, x), (\mathcal{D}, y)\right) \cong \mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}})$$

is a discrete group. It follows that

$$\mathrm{Pic}^0(\mathcal{C} \times \mathcal{D}) \cong \mathrm{Pic}^0(\mathcal{C}) \times \mathrm{Pic}^0(\mathcal{D}) \tag{8.4.1}$$

and

$$\mathrm{NS}(\mathcal{C} \times \mathcal{D}) \cong \mathbb{Z}^2 \times \mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}}). \tag{8.4.2}$$

This last isomorphism will be important for a new approach to elliptic curves of high rank over function fields discussed in Lecture 5.

8.5. Blow ups

Let $\mathcal{X}$ be a smooth projective surface over k and let $\pi : \mathcal{Y} \to \mathcal{X}$ be the blow up of $\mathcal{X}$ at a closed point $x \in \mathcal{X}$ so that $E = \pi^{-1}(x)$ is a rational curve on $\mathcal{Y}$. Then we have canonical isomorphisms

$$\mathrm{Pic}(\mathcal{Y}) \cong \mathrm{Pic}(\mathcal{X}) \oplus \mathbb{Z} \quad \text{and} \quad \mathrm{NS}(\mathcal{Y}) \cong \mathrm{NS}(\mathcal{X}) \oplus \mathbb{Z}$$

where in both groups the factor $\mathbb{Z}$ is generated by the class of E. See [Har77, V.3.2].

8.6. Fibrations

Let $\mathcal{X}$ be a smooth projective surface over k, $\mathcal{C}$ a smooth projective curve over k, and $\pi : \mathcal{X} \to \mathcal{C}$ a non-constant morphism. Assume that the induced extension of function fields $k(\mathcal{C}) \hookrightarrow k(\mathcal{X})$ is separable and $k(\mathcal{C})$ is algebraically closed in $k(\mathcal{X})$. Then for every closed point $y \in \mathcal{C}$, the fiber $\pi^{-1}(y)$ is connected, and it is irreducible for almost all y. Write F for the class in $\mathrm{NS}(\mathcal{X})$ of the fiber over a k-rational point y of $\mathcal{C}$. (This exists because we assumed that $\mathcal{X}$ has a k-rational point.) We write $\langle F \rangle$ for the subgroup of $\mathrm{NS}(\mathcal{X})$ generated by F.

It is clear from the definition of $\mathrm{NS}(\mathcal{X})$ that if y' is another closed point of $\mathcal{C}$, then the class in $\mathrm{NS}(\mathcal{X})$ of $\pi^{-1}(y')$ is equal to $(\deg y')F$.

Now suppose that $z \in \mathcal{C}$ is a closed point such that $\pi^{-1}(z)$ is reducible, say

$$\pi^{-1}(z) = \sum_{i=1}^{f_z} n_i Z_i$$

where the Z_i are the irreducible components of $\pi^{-1}(z)$ and the n_i are their multiplicities in the fiber. Then a consideration of intersection multiplicities (see for example [Sil94, III.8]) shows that for any integers m_i,

$$\sum_i m_i Z_i \in \langle F \rangle \subset \mathrm{NS}(\mathcal{X})$$

if and only if there is a rational number α such that $m_i = \alpha n_i$ for all i. More precisely, the intersection pairing restricted to the part of $\mathrm{NS}(\mathcal{X})$ generated by the

classes of the Z_i is negative semi-definite, with a one-dimensional kernel spanned by integral divisors that are rational multiples of the whole fiber. It follows that the subgroup of $\mathrm{NS}(\mathcal{X})/\langle F\rangle$ generated by the classes of the Z_i has rank $f_z - 1$. It is free of this rank if the gcd of the multiplicities n_i is 1.

It also follows that if D is a divisor supported on a fiber of π and D' is another divisor supported on other fibers, then $D = D'$ in $\mathrm{NS}(\mathcal{X})/\langle F\rangle$ if and only if $D = D' = 0$ in $\mathrm{NS}(\mathcal{X})/\langle F\rangle$.

Define $L^2\,\mathrm{NS}(\mathcal{X})$ to be the subgroup of $\mathrm{NS}(\mathcal{X})$ generated by all components of all fibers of π over closed points of $\mathcal{C}$. By the above, it is the direct sum of the $\langle F\rangle$ and the subgroups of $\mathrm{NS}(\mathcal{X})/\langle F\rangle$ generated by the components of the various fibers. Thus we obtain the following computation of the rank of $L^2\,\mathrm{NS}(\mathcal{X})$.

Proposition 8.6.1. *For a closed point y of $\mathcal{C}$, let f_y denote the number of irreducible components in the fiber $\pi^{-1}(y)$. Then the rank of $L^2\,\mathrm{NS}(\mathcal{X})$ is*

$$1 + \sum_y (f_y - 1).$$

If for all y the greatest common divisor of the multiplicities of the components in the fiber of π over y is 1, then $L^2\,\mathrm{NS}(\mathcal{X})$ is torsion-free.

9. Tate's conjectures T_1 and T_2

Tate's conjecture T_1 for $\mathcal{X}$ (which we denote $T_1(\mathcal{X})$) characterizes the image of the cycle class map:

Conjecture 9.1 ($T_1(\mathcal{X})$)**.** *For any prime $\ell \neq p$, the cycle class map induces an isomorphism*

$$\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Q}_\ell \to H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k}$$

We will see below that $T_1(\mathcal{X})$ is equivalent to the apparently stronger integral statement that the cycle class induces an isomorphism

$$\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell \to H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))^{G_k}$$

We will also see that $T_1(\mathcal{X})$ is independent of ℓ which is why we have omitted ℓ from the notation.

Since G_k is generated topologically by Fr_q, we have

$$H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k} = H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{Fr_q=1} = H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)^{Fr_q=q}.$$

The injectivity of the cycle class map implies that

$$\mathrm{Rank}\,\mathrm{NS}(\mathcal{X}) \leq \dim_{\mathbb{Q}_\ell} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)^{Fr_q=q}$$

and $T_1(\mathcal{X})$ is the statement that these two dimensions are equal.

The second Tate conjecture relates the zeta-function to divisors. Recall that $\zeta(\mathcal{X}, s)$ denotes the zeta function of $\mathcal{X}$, defined in Lecture 0, Section 3.

Conjecture 9.2 ($T_2(\mathcal{X})$)**.** *We have*

$$\mathrm{Rank}\,\mathrm{NS}(\mathcal{X}) = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s)$$

Note that by the Riemann hypothesis, the poles of $\zeta(\mathcal{X}, s)$ at $s = 1$ come from $P_2(\mathcal{X}, q^{-s})$. More precisely, using the cohomological formula (4.1) of Lecture 0 for P_2, we have that the order of pole of $\zeta(\mathcal{X}, s)$ at $s = 1$ is equal to the multiplicity of q as an eigenvalue of Fr_q on $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$.

Thus we have a string of inequalities

$$\operatorname{Rank} \mathrm{NS}(\mathcal{X}) \leq \dim_{\mathbb{Q}_\ell} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)^{Fr_q = q} \leq -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s). \tag{9.3}$$

Conjecture $T_1(\mathcal{X})$ is that the first inequality is an equality and conjecture $T_2(\mathcal{X})$ is that the leftmost and rightmost integers are equal. It follows trivially that $T_2(\mathcal{X})$ implies $T_1(\mathcal{X})$. Tate proved the reverse implication.

Proposition 9.4. *The conjectures $T_1(\mathcal{X})$ and $T_2(\mathcal{X})$ are equivalent. In particular, $T_1(\mathcal{X})$ is independent of ℓ.*

Proof. First note that the intersection pairing on $\mathrm{NS}(\mathcal{X})$ is non-degenerate, so we get an isomorphism

$$\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}(\mathrm{NS}(\mathcal{X}), \mathbb{Q}_\ell).$$

On the other hand, the cup product on $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))$ is also non-degenerate (by Poincaré duality), so we have

$$H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1)) \cong \mathrm{Hom}(H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1)), \mathbb{Q}_\ell).$$

If we use a superscript G_k to denote invariants and a subscript G_k to denote coinvariants, then we have a natural homomorphism

$$H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k} \to H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))_{G_k}$$

which is an isomorphism if and only if the subspace of $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))$ where Fr_q acts by 1 is equal to the whole of the generalized eigenspace for the eigenvalue 1. As we have seen above, this holds if and only if we have

$$\dim_{\mathbb{Q}_\ell} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)^{Fr_q = q} = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s).$$

Now consider the diagram

$$\begin{array}{ccccc} \mathrm{NS}(\mathcal{X}) \otimes \mathbb{Q}_\ell & & = & & \mathrm{Hom}(\mathrm{NS}(\mathcal{X}), \mathbb{Q}_\ell) \\ \downarrow h & & & & \uparrow h^* \\ H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k} & \xrightarrow{f} & H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))_{G_k} & = & \mathrm{Hom}(H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k}, \mathbb{Q}_\ell). \end{array}$$

The lower right arrow is an isomorphism by elementary linear algebra. The maps h and h^* are the cycle map and its transpose and they are isomorphisms if and only if $T_1(\mathcal{X})$ holds. One checks that the diagram commutes ([Tat66b, p. 24] or [Mil75, Lemma 5.3]) and so $T_1(\mathcal{X})$ implies that f is an isomorphism. Thus $T_1(\mathcal{X})$ implies $T_2(\mathcal{X})$. □

We remark that the equality of $\dim_{\mathbb{Q}_\ell} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)^{Fr_q = q}$ and $-\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s)$ would follow from the semi-simplicity of Fr_q acting on $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ (or even from its semisimplicity on the $Fr_q = q$ generalized eigenspace). This is a separate "standard" conjecture (see for example [Tat94]); it does not seem to imply $T_1(\mathcal{X})$.

10. T_1 and the Brauer group

We define the (cohomological) Brauer group $\mathrm{Br}(\mathcal{X})$ by

$$\mathrm{Br}(\mathcal{X}) = H^2(\mathcal{X}, \mathbb{G}_m) = H^2(\mathcal{X}, \mathcal{O}_{\mathcal{X}}^\times)$$

(with respect to the étale or finer topologies). Because $\mathcal{X}$ is a smooth proper surface over a finite field, the cohomological Brauer group is isomorphic to the usual Brauer group (defined in terms of Azumaya algebras) and it is known to be a torsion group.

(See [Mil80, IV.2] and also three fascinating articles by Grothendieck collected in [Gro68].) Artin and Tate conjectured in [Tat66b] that $\mathrm{Br}(\mathcal{X})$ is finite.

Similarly, define

$$\mathrm{Br}(\overline{\mathcal{X}}) = H^2(\overline{\mathcal{X}}, \mathbb{G}_m) = H^2(\overline{\mathcal{X}}, \mathcal{O}_{\overline{\mathcal{X}}}^\times).$$

This group is torsion but need not be finite.

Taking the cohomology of the exact sequence

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \to 0$$

as in Section 6, we have an exact sequence

$$0 \to \mathrm{NS}(\overline{\mathcal{X}})/\ell^n \to H^2(\overline{\mathcal{X}}, \mu_{\ell^n}) \to \mathrm{Br}(\overline{\mathcal{X}})_{\ell^n} \to 0. \tag{10.1}$$

Taking G_k-invariants and then the inverse limit over powers of ℓ, we obtain an exact sequence

$$0 \to \mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell \to H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))^{G_k} \to T_\ell \,\mathrm{Br}(\mathcal{X}) \to 0.$$

Since $\mathrm{Br}(\mathcal{X})_\ell$ is finite, $T_\ell \,\mathrm{Br}(\mathcal{X})$ is zero if and only if the ℓ-primary part of $\mathrm{Br}(\mathcal{X})$ is finite. It follows that the ℓ part of the Brauer group is finite if and only if $T_1(\mathcal{X})$ for ℓ holds if and only if the integral version of $T_1(\mathcal{X})$ for ℓ holds. In particular, since $T_1(\mathcal{X})$ is independent of ℓ, if $\mathrm{Br}(\mathcal{X})[\ell^\infty]$ is finite for one ℓ, then $\mathrm{Br}(\mathcal{X})[\ell^\infty]$ is finite for all $\ell \neq p$. It is even true, although more difficult to prove, that $T_1(\mathcal{X})$ is equivalent to the finiteness of $\mathrm{Br}(\mathcal{X})$.

Theorem 10.2. *$T_1(\mathcal{X})$ holds if and only if $\mathrm{Br}(\mathcal{X})$ is finite if and only if there is an ℓ ($\ell = p$ allowed) such that the ℓ-primary part of $\mathrm{Br}(\mathcal{X})$ is finite.*

Proof. We sketch the proof of the prime-to-p part of this assertion following [Tat66b] and refer to [Mil75] for the full proof. We already noted that the ℓ-primary part of $\mathrm{Br}(\mathcal{X})$ is finite for one $\ell \neq p$ if and only if $T_1(\mathcal{X})$ holds. To see that almost all ℓ-primary parts vanish, we consider the following diagram, which is an integral version of the diagram in the proof of Proposition 9.4:

$$\begin{array}{ccccc}
\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell & \xrightarrow{e} & \mathrm{Hom}(\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell, \mathbb{Z}_\ell) & = & \mathrm{Hom}(\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \\
\downarrow{\scriptstyle h} & & & & \uparrow{\scriptstyle g^*} \\
H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))^{G_k} & \xrightarrow{f} & H^2(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))_{G_k} & = & \mathrm{Hom}(H^2(\overline{\mathcal{X}}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1))^{G_k}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)
\end{array}$$

Here e is induced by the intersection form, h is the cycle class map, f is induced by the identity map of $H^1(\overline{\mathcal{X}}, \mathbb{Z}_\ell(1))$ and g^* is the transpose of a map

$$g : \mathrm{NS}(\mathcal{X}) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to H^2(\overline{\mathcal{X}}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1))$$

obtained by taking the direct limit over powers of ℓ of the first map in equation (10.1).

We say that a homomorphism $\phi : A \to B$ of $\mathbb{Z}_\ell$-modules is a *quasi-isomorphism* if it has a finite kernel and cokernel. In this case, we define

$$z(\phi) = \frac{\#\ker(\phi)}{\#\,\mathrm{coker}(\phi)}.$$

It is easy to check that if $\phi_3 = \phi_2\phi_1$ (composition) and if two of the maps ϕ_1, ϕ_2, ϕ_3 are quasi-isomorphisms, then so is the third and we have $z(\phi_3) = z(\phi_2)z(\phi_1)$.

In the diagram above, if we assume $T_1(\mathcal{X})$, then h is an isomorphism. The map e is induced from the intersection pairing and is a quasi-isomorphism and

$z(e)$ is (the ℓ part of) the order of the torsion subgroup of $\mathrm{NS}(\mathcal{X})$ divided by (the ℓ part of) discriminant of the intersection form. We saw above that under the assumption of $T_1(\mathcal{X})$, the map f is a quasi-isomorphism and it turns out that $z(f)$ is essentially (the ℓ part of) the leading term of the zeta function $\zeta(\mathcal{X}, s)$ at $s = 1$. In particular, under $T_1(\mathcal{X})$, e, f, and h are isomorphisms for almost all ℓ. The same must therefore be true of g^*. By taking G_k-invariants and a direct limit over powers of ℓ in equation (10.1), one finds that $z(g^*)$ is equal to the order of $\mathrm{Br}(\mathcal{X})[\ell^\infty]$ and so this group is trivial for almost all ℓ. This completes our sketch of the proof of the theorem. □

The sketch above has all the main ideas needed to prove that the prime-to-p part of the Artin-Tate conjecture on the leading coefficient of the zeta function at $s = 1$ follows from the Tate conjecture $T_1(\mathcal{X})$. The p-part is formally similar although more delicate. To handle it, Milne replaces the group in the lower right of the diagram with the larger group $\mathrm{Hom}(H^2(\mathcal{X}, (\mathbb{Q}_p/\mathbb{Z}_p)(1)), \mathbb{Q}_p/\mathbb{Z}_p)$. The z invariants of the maps to and from this group turn out to have more p-adic content that is related to the term $q^\alpha(\mathcal{X})$ in the Artin-Tate leading coefficient conjecture. We refer to [Mil75] for the full details and to [Ulm11] for a discussion of several related points, including the case $p = 2$ (excluded in Milne's article, but now provable due to improved p-adic cohomology) and higher dimensional abelian varieties.

11. The descent property of T_1

If $\tilde{\mathcal{X}} \to \mathcal{X}$ is the blow up of $\mathcal{X}$ at a closed point, then $T_1(\tilde{\mathcal{X}})$ is equivalent to $T_1(\mathcal{X})$. Indeed, under blowing up both the rank of $\mathrm{NS}(\cdot)$ and the dimension of $H^2(\cdot, \mathbb{Q}_\ell(1))^{G_k}$ increase by one. (See Example 8.5 above.) In fact:

Proposition 11.1. *$T_1(\mathcal{X})$ is invariant under birational isomorphism. More generally, if $\mathcal{X} \to \mathcal{Y}$ is a dominant rational map, then $T_1(\mathcal{X})$ implies $T_1(\mathcal{Y})$.*

Proof. We give simple proof of the case where $\mathcal{X}$ and $\mathcal{Y}$ are surfaces. See [Tat94] for the general case.

First, we may assume $\mathcal{X} \dashrightarrow \mathcal{Y}$ is a morphism. Indeed, let $\tilde{\mathcal{X}} \to \mathcal{X}$ be a blow up resolving the indeterminacy of $\mathcal{X} \dashrightarrow \mathcal{Y}$, i.e., so that the composition $\tilde{\mathcal{X}} \to \mathcal{X} \dashrightarrow \mathcal{Y}$ is a morphism. As we have seen above $\mathcal{T}_1(\mathcal{X})$ implies $T_1(\tilde{\mathcal{X}})$ so we may replace $\mathcal{X}$ with $\tilde{\mathcal{X}}$ and show that $T_1(\mathcal{Y})$ holds.

So now suppose that $\pi : \mathcal{X} \to \mathcal{Y}$ is a dominant morphism. Since the dimensions of $\mathcal{X}$ and $\mathcal{Y}$ are equal, π must be generically finite, say of degree d. But then the push forward and pull-back maps on cycles present $\mathrm{NS}(\mathcal{Y}) \otimes \mathbb{Q}_\ell$ as a direct factor of $NS(\mathcal{X}) \otimes \mathbb{Q}_\ell$; they also present $H^2(\overline{\mathcal{Y}}, \mathbb{Q}_\ell(1))$ as a direct factor of $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))$. The cycle class maps and Galois actions are compatible with these decompositions and since by assumption $NS(\mathcal{X}) \otimes \mathbb{Q}_\ell \tilde{\to} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k}$, we must also have $NS(\mathcal{Y}) \otimes \mathbb{Q}_\ell \tilde{\to} H^2(\overline{\mathcal{Y}}, \mathbb{Q}_\ell(1))^{G_k}$, i.e., $T_1(\mathcal{Y})$. □

Note that the dominant rational map $\mathcal{X} \dashrightarrow \mathcal{Y}$ could be a ground field extension, or even a purely inseparable morphism.

12. Tate's theorem on products

In this section we sketch how T_1 for products of curves follows from Tate's theorem on endomorphisms of abelian varieties over finite fields.

Theorem 12.1 (Tate)**.** *Let $\mathcal{C}$ and $\mathcal{D}$ be curves over k and set $\mathcal{X} = \mathcal{C} \times_k \mathcal{D}$. Then $T_1(\mathcal{X})$ holds.*

Proof. Extending k if necessary, we may assume that $\mathcal{C}$ and $\mathcal{D}$ both have rational points. Fix rational base points x and y (which we will mostly omit from the notation below). Recall from Subsection 8.4 that

$$\mathrm{NS}(\mathcal{C} \times \mathcal{D}) \cong \mathbb{Z}^2 \times \mathrm{DivCorr}(\mathcal{C}, \mathcal{D}) \cong \mathbb{Z}^2 \times \mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}}).$$

By the Künneth formula,

$$\begin{aligned} H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell) &\cong \big(H^2(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^0(\overline{\mathcal{D}}, \mathbb{Q}_\ell)\big) \oplus \big(H^0(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^2(\overline{\mathcal{D}}, \mathbb{Q}_\ell)\big) \\ &\qquad \oplus \big(H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)\big) \\ &\cong \mathbb{Q}_\ell(-1) \oplus \mathbb{Q}_\ell(-1) \oplus \big(H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)\big) \end{aligned}$$

Twisting by $\mathbb{Q}_\ell(1)$ and taking invariants, we have

$$H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k} = {\mathbb{Q}_\ell}^2 \oplus \big(H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)(1)\big)^{G_k}.$$

Under the cycle class map, the factor $\mathbb{Z}^2$ of $\mathrm{NS}(\mathcal{X})$ (corresponding to $\mathcal{C} \times \{y\}$ and $\{x\} \times \mathcal{D}$) spans the factor ${\mathbb{Q}_\ell}^2$ of $H^2(\overline{\mathcal{X}}, \mathbb{Q}_\ell(1))^{G_k}$ (corresponding to $H^2 \otimes H^0$ and $H^0 \otimes H^2$ in the Kunneth decomposition). Thus what we have to show is that the cycle class map induces an isomorphism

$$\mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}}) \otimes \mathbb{Q}_\ell \tilde{\to} \big(H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)(1)\big)^{G_k}$$

But $H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)(1) \cong H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)^* \cong V_\ell(J_{\mathcal{D}})$ and $H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \cong V_\ell(J_{\mathcal{C}})^*$ ($* = \mathbb{Q}_\ell$-linear dual). Thus

$$\big(H^1(\overline{\mathcal{C}}, \mathbb{Q}_\ell) \otimes H^1(\overline{\mathcal{D}}, \mathbb{Q}_\ell)(1)\big)^{G_k} \cong (V_\ell(J_{\mathcal{C}})^* \otimes V_\ell(J_{\mathcal{D}}))^{G_k} \cong \mathrm{Hom}_{G_k}(V_\ell(J_{\mathcal{C}}), V_\ell(J_{\mathcal{D}})).$$

Thus the needed isomorphism is

$$\mathrm{Hom}(J_{\mathcal{C}}, J_{\mathcal{D}}) \otimes \mathbb{Q}_\ell \tilde{\to} \mathrm{Hom}_{G_k}(V_\ell(J_{\mathcal{C}}), V_\ell(J_{\mathcal{D}}))$$

and this is exactly the statement of Tate's theorem (Lecture 0, Theorem 6.1). This completes the proof of the theorem. □

Remarks 12.2.

(1) A variation of the argument above, using Picard and Albanese varieties, shows that T_1 for a product $\mathcal{X} \times \mathcal{Y}$ of varieties of any dimension follows from T_1 for the factors.
(2) It is worth noting that Tate's conjecture T_1 (and the proof of it for products of curves) only characterizes the image of in ℓ-adic cohomology of $\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_\ell$, not the image of $\mathrm{NS}(\mathcal{X})$ itself. This should be contrasted with the Lefschetz $(1,1)$ theorem, which characterizes the image of $\mathrm{NS}(\mathcal{X})$ in deRham cohomology when the ground field is $\mathbb{C}$.

13. Products of curves and DPC

Assembling the various parts of this lecture gives the main result:

Proposition 13.1. *Let $\mathcal{X}$ be a smooth, projective surface over k. If there is a dominant rational map*

$$\mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathcal{X}$$

from a product of curves to $\mathcal{X}$, then the Tate conjectures $T_1(\mathcal{X})$ and $T_2(\mathcal{X})$ hold.

Indeed, by Theorem 12.1, we have $T_1(\mathcal{C} \times \mathcal{D})$ and then by Proposition 11.1 we deduce $T_1(\mathcal{X})$. By Proposition 9.4, $T_2(\mathcal{X})$ follows as well.

We say that "$\mathcal{X}$ is dominated by a product of curves (DPC)." The question of which varieties are dominated by products of curves has been studied by Schoen [Sch96]. In particular, over any field there are surfaces that are not dominated by products of curves. Nevertheless, as we will see below, the collection of DPC surfaces is sufficiently rich to give some striking results on the Birch and Swinnerton-Dyer conjecture.

LECTURE 3

Elliptic curves and elliptic surfaces

We keep our standard notations throughout this lecture: p is a prime, $k = \mathbb{F}_q$ is the finite field of characteristic p with q elements, $\mathcal{C}$ is a smooth, projective, absolutely irreducible curve over k, $K = k(\mathcal{C})$ is the function field of $\mathcal{C}$, and E is an elliptic curve over K.

1. Curves and surfaces

In this section we will construct an elliptic surface $\mathcal{E} \to \mathcal{C}$ canonically associated to an elliptic curve E/K. More precisely, we give a constructive proof of the following result:

Proposition 1.1. *Given an elliptic curve E/K, there exists a surface $\mathcal{E}$ over k and a morphism $\pi : \mathcal{E} \to \mathcal{C}$ with the following properties: $\mathcal{E}$ is smooth, absolutely irreducible, and projective over k, π is surjective and relatively minimal, and the generic fiber of π is isomorphic to E. The surface $\mathcal{E}$ and the morphism π are uniquely determined up to isomorphism by these requirements.*

Here "the generic fiber of π" means $\mathcal{E}_K$, the fiber product:

$$\begin{array}{ccc} \mathcal{E}_K := \eta \times_{\mathcal{C}} \mathcal{E} & \longrightarrow & \mathcal{E} \\ \downarrow & & \downarrow \pi \\ \eta = \operatorname{Spec} K & \longrightarrow & \mathcal{C} \end{array}$$

"Relatively minimal" means that if $\mathcal{E}'$ is another smooth, absolutely irreducible, projective surface over k with a surjective morphism $\pi' : \mathcal{E}' \to \mathcal{C}$, then any birational morphism $\mathcal{E} \to \mathcal{E}'$ commuting with π and π' is an isomorphism. Relative minimality is equivalent to the condition that there are no rational curves of self-intersection -1 in the fibers of π (i.e., to the non-existence of curves in fibers that can be blown down).

Remarks 1.2. The requirements on $\mathcal{E}$ and π imply that π is flat and projective and that all geometric fibers of π are connected. These properties of π will be evident from the explicit construction below. It follows that $\pi_* \mathcal{O}_{\mathcal{E}} \cong \mathcal{O}_{\mathcal{C}}$ and more generally that π is "cohomologically flat in dimension zero," meaning that for every morphism $T \to C$ the base change

$$\pi_T : \mathcal{E}_T = \mathcal{E} \times_{\mathcal{C}} T \to T$$

satisfies $\pi_{T*} \mathcal{O}_{\mathcal{E}_T} = \mathcal{O}_T$.

Uniqueness in Proposition 1.1 follows from general results on minimal models, in particular [Lic68, Thm. 4.4]. See [Chi86] and [Liu02, 9.3] for other expositions.

We first give a detailed construction of a (possibly singular) "Weierstrass surface" $\mathcal{W} \to \mathcal{C}$ and then resolve singularities to obtain $\mathcal{E} \to \mathcal{C}$.

More precisely, the proposition follows from the following two results.

Proposition 1.3. *Given an elliptic curve E/K, there exists a surface $\mathcal{W}$ over k and a morphism $\pi_0 : \mathcal{W} \to \mathcal{C}$ with the following properties: $\mathcal{W}$ is normal, absolutely irreducible, and projective over k, π_0 is surjective, each of its fibers is isomorphic to an irreducible plane cubic, and its generic fiber is isomorphic to E.*

This proposition is elementary, but does not seem to be explained in detail in the literature, so we give a proof below.

Proposition 1.4. *There is an explicit sequence of blow ups (along closed points and curves in $\mathcal{W}$) yielding a proper birational morphism $\sigma : \mathcal{E} \to \mathcal{W}$ where the surface $\mathcal{E}$ and the composed morphism $\pi = \pi_0 \circ \sigma : \mathcal{E} \to \mathcal{W} \to \mathcal{C}$ have the properties mentioned in Proposition 1.1.*

Proof of Proposition 1.3. Choose a Weierstrass equation for E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.5}$$

where the a_i are in $K = k(\mathcal{C})$. Recall that we have defined the notion of a minimal integral model at a place v of K: the a_i should be integral at v and the valuation at v of Δ should be minimal subject to the integrality of the a_i. Clearly, there is a non-empty Zariski open subset $U \subset \mathcal{C}$ such that for every closed point $v \in U$, the model (1.5) is a minimal integral model.

Let $\mathcal{W}_1$ be the closed subset of $\mathbb{P}^2_U := \mathbb{P}^2_k \times_k U$ defined by the vanishing of

$$Y^2Z + a_1XYZ + a_3YZ^2 - \big(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\big) \tag{1.6}$$

where X, Y, Z are the standard homogeneous coordinates on $\mathbb{P}^2_k$. Then $\mathcal{W}_1$ is geometrically irreducible and there is an obvious projection $\pi_1 : \mathcal{W}_1 \to U$ (the restriction to $\mathcal{W}_1$ of the projection $\mathbb{P}^2_U \to U$). The fiber of π_1 over a closed point v of U is the plane cubic

$$Y^2Z + a_1(v)XYZ + a_3(v)YZ^2 = X^3 + a_2(v)X^2Z + a_4(v)XZ^2 + a_6(v)Z^3$$

over the residue field κ_v at v. The generic point η of $\mathcal{C}$ lies in U and the fiber of π_1 at η is E/K.

There are finitely many points in $\mathcal{C} \setminus U$ and we must extend the model $\mathcal{W}_1 \to U$ over each of these points. Choose one of them, call it w, and choose a model of E that is integral and minimal at w. In other words, choose a model of E

$$y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6 \tag{1.7}$$

where the $a'_i \in K$ are integral at w and the valuation at w of the discriminant Δ is minimal. The new coordinates are related to the old by a transformation

$$(x, y) = (u^2x' + r, u^3y' + su^2x' + t) \tag{1.8}$$

with $u \in K^\times$ and $r, s, t \in K$. Let U' be a Zariski open subset of $\mathcal{C}$ containing w on which all of the a'_i are integral and the model (1.7) is minimal. Let $\mathcal{W}'$ be the geometrically irreducible closed subset of $\mathbb{P}^1_{U'}$ defined by the vanishing of

$$Y'^2Z' + a'_1X'Y'Z' + a'_3Y'Z'^2 - \big(X'^3 + a'_2X'^2Z' + a'_4X'Z'^2 + a'_6Z'3\big)$$

with its obvious projection $\pi' : \mathcal{W}' \to U'$. On the open set $V = U \cap U'$, u is a unit and the change of coordinates (1.8), or rather its projective version

$$(X, Y, Z) = (u^2X' + rZ, u^3Y' + su^2X' + tZ', Z')$$

defines an isomorphism between $\pi_1^{-1}(V)$ and $\pi'^{-1}(V)$ compatible with the projections. Glueing $\mathcal{W}_1$ and $\mathcal{W}'$ along this isomorphism yields a new surface $\mathcal{W}_2$ equipped with a projection $\pi_2 : \mathcal{W}_2 \to U_2$ where $U_2 = U \cup U'$. Note that U_2 is strictly larger than U. Moreover π_2 is surjective, its geometric fibers are irreducible projective plane cubics, and its generic fiber is E.

We now iterate this construction finitely many times to extend the original model over all of $\mathcal{C}$. We arrive at a surface $\mathcal{W}$ equipped with a proper, surjective morphism $\pi : \mathcal{W} \to \mathcal{C}$ whose geometric fibers are irreducible plane cubics and whose generic fiber is E. Since $\mathcal{C}$ is projective over k, so is $\mathcal{W}$. Since $\mathcal{W}$ is obtained by glueing reduced, geometrically irreducible surfaces along open subsets, it is also reduced and geometrically irreducible. Since it has only isolated singular points, by Serre's criterion it is normal.

This completes the proof of Proposition 1.3. □

Note that the closure in $\mathcal{W}$ of the identity element of E is a divisor on $\mathcal{W}$ which maps isomorphically to the base curve $\mathcal{C}$. We write $s_0 : \mathcal{C} \to \mathcal{W}$ for the inverse morphism. This is the *zero section* of π_0. In terms of the coordinates on $\mathcal{W}_1$ used in the proof above, it is just the map $t \mapsto ([0, 1, 0], t)$.

Discussion of Proposition 1.4. The algorithm mentioned in the Proposition is the subject of Tate's famous paper [Tat75]. His article does not mention blowing up, but the steps of the algorithm nevertheless give the recipe for the blow ups needed. The actual process of blowing up is explained in detail in [Sil94, IV.9] so we will not give the details here. Rather, we explain why there is a simple algorithm, following [Con05].

First note that the surface $\mathcal{W}$ is reduced and irreducible and so has no embedded components. Also, it has isolated singularities. (They are contained in the set of singular points of fibers of π_0.) By Serre's criterion, $\mathcal{W}$ is thus normal. Moreover, and this is the key point, its singularities are *rational double points*. (See [Art86] for the definition and basic properties of rational singularities and [Bǎd01, Chapters 3 and 4] for many more details. See [Con05, Section 8] for the fact that the singularities of a minimal Weierstrass model are rational.) This implies that the blow up of $\mathcal{W}$ at one of its singular points is again normal (so has isolated singularities) and again has at worst rational double points. An algorithm to desingularize is then simply to blow up at a singular point and iterate until the resulting surface is smooth. Given the explicit nature of the equations defining $\mathcal{W}$, finding the singular points and carrying out the blow ups is straightforward.

In fact, Tate's algorithm also calls for blowing up along certain curves. (This happens at steps 6 and 7.) This has the effect of dealing with several singular points at the same time, so is more efficient, but it is not essential to the success of the algorithm.

This completes our discussion of Proposition 1.4. See below for a detailed example covering a case not treated explicitly in [Sil94]. □

Conrad's article [Con05] also gives a coordinate-free treatment of integral minimal models of elliptic curves.

It is worth remarking that Tate's algorithm and the possible structures of the bad fibers are essentially the same in characteristic p as in mixed characteristic. On the other hand, for non-perfect residue fields k of characteristic $p \leq 3$, there are more possibilities for the bad fibers, in both equal and mixed characteristics—see [Szy04].

The zero section of $\mathcal{W}$ lifts uniquely to a section which we again denote by $s_0 : \mathcal{C} \to \mathcal{E}$.

2. The bundle ω and the height of $\mathcal{E}$

We construct an invertible sheaf on $\mathcal{C}$ as follows, using the notation of the proof of Proposition 1.1. Take the trivial invertible sheaf $\mathcal{O}_U$ on U with its generating section 1_U. At each stage of the construction, extend this sheaf by glueing $\mathcal{O}_U$ and $\mathcal{O}_{U'}$ over $U \cap U'$ by identifying 1_U and $u^{-1}1_{U'}$ where u is the function appearing in the change of coordinates (1.8).

The resulting invertible sheaf ω has several other descriptions. For example, the sheaf of relative differentials $\Omega^1_{\mathcal{E}/\mathcal{C}}$ is invertible on the locus of $\mathcal{E}$ where $\pi : \mathcal{E} \to \mathcal{C}$ is smooth (in particular in a neighborhood of the zero section) and, more or less directly from the definition, ω can be identified with $s_0^*(\Omega^1_{\mathcal{E}/\mathcal{C}})$. Using relative duality theory, ω can also be identified with the inverse of $R^1\pi_*\mathcal{O}_\mathcal{E}$. Finally, since $\mathcal{W}$ as only rational singularities, ω is also isomorphic to $R^1\pi_{0*}\mathcal{O}_\mathcal{W}$

One may identify the coefficients a_i of the Weierstrass equation locally defining $\mathcal{W}$ with sections of ω^i. Using this point of view, $\mathcal{W}$ can be identified with a closed subvariety of a certain $\mathbb{P}^2$-bundle over $\mathcal{C}$. Namely, let V be the locally free $\mathcal{O}_\mathcal{C}$ module of rank three

$$V = \omega^2 \oplus \omega^3 \oplus \mathcal{O}_\mathcal{C} \tag{2.1}$$

(where the exponents denote tensor powers). If $\mathbb{P}V$ denotes the projectivization of V over $\mathcal{C}$, a $\mathbb{P}^2$ bundle over $\mathcal{C}$, then $\mathcal{W}$ is naturally the closed subset of $\mathbb{P}E$ defined locally by the vanishing of Weierstrass equations as in (1.6).

Exercises 2.2. Verify the identifications and assertions in this section. In the case where $\mathcal{C} = \mathbb{P}^1$, so $K = k(t)$, check that $\omega = \mathcal{O}_{\mathbb{P}^1}(h)$ where h is the smallest positive integer such that E has a model (1.5) where the a_i are in $k[t]$ and $\deg a_i \leq hi$.

Exercises 2.3. Check that c_4, c_6, and Δ define *canonical* sections of ω^4, ω^6, and ω^{12} respectively, independent of the choice of equation for E. If $p = 2$ or 3, check that b_2 defines a canonical section of ω^2 and that $c_4 = b_2^2$ and $c_6 = -b_2^3$. If $p = 2$, check that a_1 defines a canonical section of ω and that $b_2 = a_1^2$. Note that since positive powers of ω have non-zero sections, the degree of ω is non-negative.

Definition 2.4. The *height* of $\mathcal{E}$, denoted h, is defined by $h = \deg(\omega)$, the degree of ω as an invertible sheaf on $\mathcal{C}$.

Note that if E/K is constant (in the sense of Lecture 1) then the height of the corresponding $\mathcal{E}$ is 0.

3. Examples

The case when $\mathcal{C} = \mathbb{P}^1$ is particularly simple. First of all, one may choose a model (1.5) that is integral and minimal simultaneously at every finite v, i.e., for every $v \in \mathbb{A}^1_k$. Indeed, start with any model and change coordinates so that the

a_i are in $k[t]$. If w is a finite place where this model is not minimal, it is possible (because $k[t]$ is a PID) to choose a change of coordinates

$$(x, y) = (u^2x' + r, u^3y' + su^2x' + t)$$

where $r, s, t, u \in k[t][1/w]$ and u a unit yielding a model that is minimal at w. Such a change of coordinates does not change the minimality at any other finite place. Thus after finitely many steps, we have a model integral and minimal at all finite places. (This argument would apply for any K and any Dedekind domain $R \subset K$ which is a PID, yielding a model with the $a_i \in R$ that is minimal at all $v \in \operatorname{Spec} R$.)

Focusing attention at $t = \infty$, there is a change of coordinates (1.8) with $u = t^{-h}$ yielding a model integral and minimal at ∞. (Here h is minimal so that $\deg(a_i) \leq hi$.) So the bundle $\omega = \mathcal{O}(h) = \mathcal{O}(h\infty)$.

As a very concrete example, consider the curve

$$y^2 = x(x + 1)(x + t^d)$$

over $\mathbb{F}_p(t)$ where $p > 2$ and d is not divisible by p. Since $\Delta = 16t^{2d}(t^d - 1)^2$, this model is integral and minimal at all non-zero finite places. It is also minimal at zero as one may see by noting that c_4 and c_6 are units at 0. At infinity, the change of coordinates

$$(x, y) = (t^{2h}x', t^{3h}y')$$

with $h = \lceil d/2 \rceil$ yields a minimal integral model. Thus $\omega = \mathcal{O}(h)$.

Working with Tate's algorithm shows that E has I_2 reduction at the d-th roots of unity, I_{2d} reduction at $t = 0$, and either I^*_{2d} or I_{2d} reduction at infinity depending on whether d is odd or even.

Since the case of I_n reduction is not treated explicitly in [Sil94], we give more details on the blow ups needed to resolve the singularity over $t = 0$. In terms of the coordinates on $\mathcal{W}_1$ used in the proof of Proposition 1.4 we can consider the affine surface defined by

$$x^3 + (t^d + 1)x^2 + t^dx - y^2 = 0$$

which is an open neighborhood of the singularity at $x = y = t = 0$. If $d = 1$, then the tangent cone is the irreducible plane conic defined by $x^2 + tx - y^2 = 0$. The singular point thus blows up into a smooth rational curve and it is easy to check that the resulting surface is smooth in a neighborhood of the fiber $t = 0$. Now assume that $d > 1$. Then the tangent cone is the reducible conic $x^2 - y^2 = 0$ and so the singular point blows up into two rational curves meeting at one point. More precisely, the blow up is covered by three affine patches. In one of them, the surface upstairs is

$$tx_1^3 + (t^d + 1)x_1^2 + t^{d-1}x_1 - y_1^2 = 0$$

and the morphism is $x = tx_1$, $y = ty_1$. The exceptional divisor is the reducible curve $t = x_1^2 - y_1^2 = 0$ and the point of intersection of the components $t = x_1 = y_1 = 0$ is again a double point. Considering the other charts shows that there are no other singular points in a neighborhood of $t = 0$ and that the exceptional divisor meets the original fiber over $t = 0$ in two points. We now iterate this process $d-1$ times, introducing two new components at each stage. After $d-1$ blow ups, the interesting part of our surface is given by

$$t^{d-1}x_{d-1}^3 + (t^d + 1)x_{d-1}^2 + tx_{d-1} - y_{d-1}^2 = 0.$$

At this last stage, blowing up introduces one more component meeting the two components introduced in the preceding step at one point each. The (interesting part of the) surface is now

$$t^d x_d^3 + (t^d + 1)x_d^2 + x_d - y_d^2 = 0$$

which is regular in a neighborhood of $t = 0$. Thus we see that the fiber over $t = 0$ in $\mathcal{E}$ is a chain of $2d$ rational curves, i.e., a fiber of type I_{2d}.

The resolution of the singularities over points with $t^d = 1$ is similar but simpler because only one blow up is required. At $t = \infty$, if d is even then the situation is very similar to that over $t = 0$ and the reduction is again of type I_{2d}. If d is odd, the reduction is of type I_{2d}^*. We omit the details in this case since it is treated fully in [Sil94].

Exercise 3.1. In the table in Tate's algorithm paper [Tat75] (and the slightly more precise version in [Sil09, p. 448]), the last three rows have restrictions on p. Give examples showing that these restrictions are all necessary for the discriminant and conductor statements, and for the statement about j in the I_n^*, $p = 2$ case. Show that the other assertions about the j-invariant are correct for all p.

4. $\mathcal{E}$ and the classification of surfaces

It is sometimes useful to know how $\mathcal{E}$ fits into the Enriques-Kodaira classification of surfaces. In this section only, we replace k with $\overline{k}$ and write $\mathcal{E}$ for what elsewhere is denoted $\overline{\mathcal{E}}$.

Recall that the height of $\mathcal{E}$ is defined as $h = \deg \omega$.

Proposition 4.1. *$\omega \cong \mathcal{O}_\mathcal{C}$ if and only if E is constant. If $h = \deg(\omega) = 0$, then E is isotrivial.*

Proof. It is obvious that if E is constant, then $\omega \cong \mathcal{O}_\mathcal{C}$. Conversely, suppose $\omega \cong \mathcal{O}_\mathcal{C}$. Then the construction of $\pi_0 : \mathcal{W} \to \mathcal{C}$ in Proposition 1.3 yields an irreducible closed subset of $\mathbb{P}^2_\mathcal{C}$ (because the $\mathbb{P}^2$-bundle $\mathbb{P}V$ in (2.1) is trivial):

$$\mathcal{W} \subset \mathbb{P}^2_\mathcal{C} = \mathbb{P}^2_k \times_k \mathcal{C}.$$

Let $\sigma : \mathcal{W} \to \mathbb{P}^2_k$ be the restriction of the projection $\mathbb{P}^2_C \to \mathbb{P}^2_k$. Then σ is not surjective (since most points in the line at infinity $Z = 0$ are not in the image) and so its image has dimension < 2. Considering the restriction of σ to a fiber of π_0 shows that the image of σ is in fact an elliptic curve E_0 and then it is obvious from dimension considerations that

$$\mathcal{W} = \pi_0^{-1}(\pi_0(\mathcal{W})) = E_0 \times \mathcal{C}.$$

It follows that E, the generic fiber of π_0, is isomorphic to $E_0 \times \operatorname{Spec} K$, i.e., that E is constant.

Now assume that $h = 0$. Then Δ is a non-zero global section of the invertible sheaf ω^{12} on $\mathcal{C}$ of degree 0. Thus ω^{12} is trivial. It follows that there is a finite unramified cover of $\mathcal{C}$ over which ω becomes trivial and so by the first part, E becomes constant over a finite extension, i.e., E is isotrivial. □

Note that E being isotrivial does not imply that $h = 0$.

Exercise 4.2. Give an example of a non-constant E of height zero. Hint: Consider the quotient of a product of elliptic curves by a suitable free action of a group of order two.

Proposition 4.3. *The canonical bundle of $\mathcal{E}$ is $\Omega^2_{\mathcal{E}} \cong \pi^* \left(\Omega^1_C \otimes \omega\right)$.*

Here we are using that $\mathcal{E} \to \mathcal{C}$ has a section and therefore no multiple fibers. The proof, which we omit, proceeds by considering $R^1\pi_*\mathcal{O}_{\mathcal{E}}$ and using relative duality. See for example [Băd01, 7.15].

We now consider several cases:

If $2g_{\mathcal{C}} - 2 + h > 0$, then it follows from the Proposition that the dimension of $H^0(\mathcal{E}, (\Omega^2)^{\otimes^n})$ grows linearly with n, so $\mathcal{E}$ has Kodaira dimension 1.

If $2g_{\mathbb{C}} - 2 + h = 0$, then the Kodaira dimension of $\mathcal{E}$ is zero and there are two possibilities: (1) $g_{\mathcal{C}} = 1$ and $h = 0$; or (2) $g_{\mathcal{C}} = 0$ and $h = 2$. In the first case, there is an unramified cover of $\mathcal{C}$ over which $\mathcal{E}$ becomes constant and so $\mathcal{E}$ is the quotient of a product of two elliptic curves. These surfaces are sometimes called "bi-elliptic." In the second case, $\Omega^2_{\mathcal{E}} = \mathcal{O}_{\mathcal{E}}$ and $H^1(\mathcal{E}, \mathcal{O}_{\mathcal{E}}) = H^0(\mathcal{C}, \omega^{-1}) = 0$ and so $\mathcal{E}$ is a K3 surface.

If $2g_{\mathcal{C}} - 2 + h < 0$, then the Kodaira dimension of $\mathcal{E}$ is $-\infty$ and there are again two possibilities: (1) $g_{\mathcal{C}} = 0$ and $h = 1$, in which case $\mathcal{E}$ is a rational surface by Castelnuovo's criterion; or (2) $g_{\mathcal{C}} = 0$ and $h = 0$, in which case E is constant and $\mathcal{E}$ is a ruled surface $E_0 \times \mathcal{C} = E_0 \times \mathbb{P}^1$.

5. Points and divisors, Shioda-Tate

If D is an irreducible curve on $\mathcal{E}$, then its generic fiber

$$D.E := D \times_{\mathcal{C}} E$$

is either empty or is a closed point of E. The former occurs if and only if D is supported in a fiber of π. In the latter case, the residue degree of $D.E$ is equal to the generic degree of $D \to \mathcal{C}$. Extending by linearity, we get homomorphism

$$\operatorname{Div}(\mathcal{E}) \to \operatorname{Div}(E)$$

whose kernel consists of divisors supported in the fibers of π.

There is a set-theoretic splitting of this homomorphism, induced by the map sending a closed point of E to its scheme-theoretic closure in $\mathcal{E}$. However, this is not in general a group homomorphism.

Let $L^1 \operatorname{Div}(\mathcal{E})$ be the subgroup of divisors D such that the degree of $D.E$ is zero and let $L^2 \operatorname{Div}(\mathcal{E})$ be subgroup such that $D.E = 0$. We write $L^i \operatorname{Pic}(\mathcal{E})$ and $L^i \operatorname{NS}(\mathcal{E})$ $(i = 1, 2)$ for the images of $L^i(\mathcal{E})$ in $\operatorname{Pic}(\mathcal{E})$ and $\operatorname{NS}(\mathcal{E})$ respectively.

The Shioda-Tate theorem relates the Néron-Severi group of $\mathcal{E}$ to the Mordell-Weil group of E:

Theorem 5.1. *If $\mathcal{E} \to \mathcal{C}$ is non-constant, $D \mapsto D.E$ induces an isomorphism*

$$\frac{L^1 \operatorname{NS}(\mathcal{E})}{L^2 \operatorname{NS}(\mathcal{E})} \cong E(K)$$

If $\mathcal{E} \to \mathcal{C}$ is constant, we have

$$\frac{L^1 \operatorname{NS}(\mathcal{E})}{L^2 \operatorname{NS}(\mathcal{E})} \cong E(K)/E(k)$$

This theorem seems to have been known to the ancients (Lang, Néron, Weil, ...) and was stated explicitly in [Tat66b] and in papers of Shioda. A detailed proof in a more general context is given in [Shi99]. Note however that in [Shi99] the ground field is assumed to be algebraically closed. See [Ulm11] for the small modifications needed to treat finite k.

It is obvious that $NS(\mathcal{E})/L^1NS(\mathcal{E})$ is infinite cyclic. We saw in Example 8.6 of Lecture 2 that $L^2NS(\mathcal{E})$ is free abelian of rank $1+\sum_v(f_v-1)$. So as a corollary of the theorem, we have the following rank formula, known as the Shioda-Tate formula:

$$\text{Rank}\, E(K) = \text{Rank}\, NS(\mathcal{E}) - 2 - \sum_v (f_v - 1) \tag{5.2}$$

For more on the geometry of elliptic surfaces and elliptic curves over function fields, with an emphasis on rational and K3 surfaces, I recommend [SS09].

6. L-functions and Zeta-functions

We are going to relate the L-function of E and the zeta function of $\mathcal{E}$. We note that from the definition, $Z(\mathcal{E},T)$ depends only on the underlying set of closed points of $\mathcal{E}$ and we may partition this set using the map π.

We have

$$\begin{aligned} Z(\mathcal{E},T) &= \prod_{\text{closed } x\in\mathcal{E}} \left(1-T^{\deg(x)}\right)^{-1} \\ &= \prod_{\text{closed } y\in\mathcal{C}} \prod_{x\in\pi^{-1}(y)} \left(1-T^{\deg(x)}\right)^{-1} \\ &= \prod_{\text{closed } y\in\mathcal{C}} Z(\pi^{-1}(y), T^{\deg(y)}) \end{aligned}$$

For y such that $\pi^{-1}(y)$ is a smooth elliptic curve, we know that

$$Z(\pi^{-1}(y),T) = \frac{(1-a_yT+q_yT^2)}{(1-T)(1-q_yT)}$$

and the numerator here is the factor that enters into the definition of $L(E,T)$.

To complete the calculation, we need an analysis of the contribution of the bad fibers. We consider the fiber $\pi^{-1}(y)$ as a scheme of finite type over the residue field κ_y, the field of q_y elements. As such, it has irreducible components. Its "geometric components" are the components of the base change to $\overline{\kappa}_y$; these are defined over some finite extension of κ_y.

For certain reduction types (I_n, I_n^* ($n\geq 0$), IV and IV^*) it may happen that all the geometric components are defined over κ_y, in which case we say the reduction is "split", or it may happen that some geometric components are only defined over a quadratic extension of κ_y, in which case we say the reduction is "non-split." This agrees with the standard usage in the case of I_n reduction and may be non-standard in the other cases.

Proposition 6.1. *The zeta function of the a singular fiber of π has the form*

$$\begin{aligned} Z(\pi^{-1}(y),T) &= \frac{(1-T)^a(1+T)^b}{(1-q_yT)^f(1+q_yT)^g} \\ &= \frac{1}{(1-T)(1-q_yT)}\frac{(1-T)^{a+1}(1+T)^b}{(1-q_yT)^{f-1}(1+q_yT)^g} \end{aligned}$$

where the integers a, b, f, and g are determined by the reduction type at y and are given in the following table:

	a	b	f	g
split I_n	0	0	n	0
non-split I_n, *n odd*	-1	1	$(n+1)/2$	$(n-1)/2$
non-split I_n, *n even*	-1	1	$n/2+1$	$(n-2)/2$
split I_n^*	-1	0	$5+n$	0
non-split I_n^*	-1	0	$4+n$	1
II	-1	0	1	0
II^*	-1	0	9	0
III	-1	0	2	0
III^*	-1	0	8	0
split IV	-1	0	3	0
non-split IV	-1	0	2	1
split IV^*	-1	0	7	0
non-split IV^*	-1	0	3	4

Exercise 6.2. Use an elementary point-counting argument to verify the proposition. In particular, check that the number of components of $\pi^{-1}(y)$ that are rational over κ_y is f and that the order of pole at $T = q_y^{-1}$ of

$$Z(\pi^{-1}(y), T)(1-T)(1-q_yT)$$

is $f-1$.

Using the Proposition and the definition of the L-function (in Lecture 1, equation (9.1)) we find that

$$L(E,T) = \frac{Z(\mathcal{C},T)Z(\mathcal{C},qT)}{Z(\mathcal{E},T)} \prod_{\text{bad } v} \frac{(1-T)^{a_v+1}(1+T)^{b_v}}{(1-q_vT^{\deg(v)})^{f_v-1}(1+q_vT^{\deg(v)})^{g_v}} \tag{6.3}$$

where a_v, b_v, f_v and g_v are the invariants defined in the Proposition at the place v. Using the Weil conjectures (see Section 3 of Lecture 0), we see that the orders of $L(E,s)$ and $\zeta(\mathcal{E},s)$ at $s=1$ are related as follows:

$$\operatorname{ord}_{s=1} L(E,s) = -\operatorname{ord}_{s=1}\zeta(\mathcal{E},s) - 2 - \sum_v (f_v - 1). \tag{6.4}$$

Remark 6.5. This simple approach to evaluating the order of zero of the L-function does not yield the important fact that $L(E,T)$ is a polynomial in T when E is non-constant, nor does it yield the Riemann hypothesis for $L(E,T)$.

For a slightly more sophisticated (and less explicit) comparison of ζ-functions and L-functions in a more general context, see [Gor79].

7. The Tate-Shafarevich and Brauer groups

The last relationship between E and $\mathcal{E}$ we need concerns the Tate-Shafarevich and Brauer groups.

Theorem 7.1. *Suppose that E is an elliptic curve over $K = k(\mathcal{C})$ and $\mathcal{E} \to \mathcal{C}$ is the associated elliptic surface as in Proposition 1.1. Then there is a canonical isomorphism*

$$\operatorname{Br}(\mathcal{E}) \cong Ш(E/K).$$

The proof of this result, which is somewhat involved, is given in [Gro68, Section 4]. The main idea is simple enough: one computes $\mathrm{Br}(\mathcal{E}) = H^2(\mathcal{E}, \mathbb{G}_m)$ using the morphism $\pi : \mathcal{E} \to \mathcal{C}$ and a spectral sequence. Using that the Brauer group of a smooth, complete curve over a finite field vanishes, one finds that the main term is $H^1(\mathcal{C}, R^1\pi_*\mathbb{G}_m)$. Since $R^1\pi_*\mathbb{G}_m$ is the sheaf associated to the relative Picard group, it is closely related to the sheaf on $\mathcal{C}$ represented by the Néron model of E. This provides a connection with the Tate-Shafarevich group which leads to the theorem.

See [Ulm11] for more details about this and the closely related connection between $H^2(\overline{\mathcal{E}}, \mathbb{Z}_\ell(1))^{G_k}$ and the ℓ-Selmer group of E.

8. The main classical results

We are now in a position to prove the theorems of Section 12 of Lecture 1. For convenience, we restate Theorem 12.1 and a related result.

Theorem 8.1. *Suppose that E is an elliptic curve over $K = k(\mathcal{C})$ and $\mathcal{E} \to \mathcal{C}$ is the associated elliptic surface as in Proposition 1.1.*

(1) *BSD holds for E if and only if T_2 holds for $\mathcal{E}$.*
(2) $\mathrm{Rank}\, E(K) \leq \mathrm{ord}_{s=1}\, L(E, s)$.
(3) *The following are equivalent:*
   - $\mathrm{Rank}\, E(K) = \mathrm{ord}_{s=1}\, L(E, s)$
   - *$Ш(E/K)$ is finite*
   - *for any one prime number ℓ ($\ell = p$ is allowed), the ℓ-primary part $Ш(E/K)_{\ell^\infty}$ is finite.*
(4) *If K'/K is a finite extension and if the BSD conjecture holds for E over K', then it holds for E over K.*

Proof. Comparing (5.2) and (6.4), we have that

$$\mathrm{Rank}\, E(K) - \mathrm{ord}_{s=1}\, L(E, s) = \mathrm{Rank}\, NS(\mathcal{E}) + \mathrm{ord}_{s=1}\, \zeta(\mathcal{E}, s).$$

Since BSD is the assertion that the left hand side is zero and T_2 is the assertion that the right hand side is zero, these conjectures are equivalent.

By Theorem 9.3 of Lecture 2, the right hand side is ≤ 0 and therefore so is the left. This gives the inequality $\mathrm{Rank}\, E(K) \leq \mathrm{ord}_{s=1}\, L(E, s)$.

The statements about $Ш(E/K)$ follow from Theorem 7.1 ($Ш(E/K) \cong \mathrm{Br}(\mathcal{E})$), the equivalence of BSD and $T_2(\mathcal{E})$, and Theorem 10.2 of Lecture 2.

The last point follows from the equivalence of BSD and $T_2(\mathcal{E})$ and Proposition 11.1 of Lecture 2. □

Proofs of Theorems 12.2 and 12.3 of Lecture 1. Theorem 12.2 of Lecture 1 concerns isotrivial elliptic curves. By the last point of Theorem 8.1 above, it suffices to show that BSD holds for constant curves. But if E is constant, then $\mathcal{E}$ is a product of curves, so the Tate conjecture for $\mathcal{E}$ follows from Theorem 12.1 of Lecture 2. The first point of Theorem 8.1 above then gives BSD for E.

Theorem 12.3 of Lecture 1 concerns elliptic curves over $k(t)$ of low height. By the discussion in Section 4, if $E/k(t)$ has height ≤ 2 then $\mathcal{E}$ is a rational or K3 surface. (Strictly speaking, this is true only over a finite extension of k, but the last point of Theorem 8.1 allows us to make this extension without loss of generality.) But $T_2(\mathcal{X})$ for a rational surface follows from Proposition 13.1 of Lecture 2. For E

such that $\mathcal{E}$ is a K3 surfaces, Artin and Swinnerton-Dyer proved the finiteness of $Ш(E/K)$ (and therefore BSD) in [ASD73]. □

9. Domination by a product of curves

Combining part 1 of Theorem 8.1 with Proposition 13.1 of Lecture 2, we have the following.

Theorem 9.1. *Let E be an elliptic curve over K with associated surface $\mathcal{E}$. If $\mathcal{E}$ is dominated by a product of curves, then BSD holds for E.*

Theorem 12.4 ("four monomials") and Berger's theorem 11.1 are both corollaries of Theorem 9.1, as we will explain in the remainder of this lecture.

10. Four monomials

We recall Shioda's conditions. Suppose that $f \in R = k[x_1, x_2, x_3]$ is the sum of exactly four non-zero monomials:

$$f = \sum_{i=1}^{4} c_i \prod_{j=1}^{3} x_j^{e_{ij}}$$

where $c_i \in k$ and the e_{ij} are non-negative integers. Let $e_{i4} = 1 - \sum_{j=1}^{3} e_{ij}$ and form the 4×4 matrix $A = (e_{ij})$. Assuming that $\det(A) \neq 0$ (in $\mathbb{Z}$), let δ be the smallest positive integer such that there is a 4×4 integer matrix B with $AB = \delta I_{4\times 4}$. We say that *$f$ satisfies Shioda's 4-monomial condition* if $\delta \neq 0$ in k, i.e., if $p \nmid \delta$. The following exercise shows that this is equivalent to the definition in Lecture 1.

Exercises 10.1. Show that a prime ℓ divides δ if and only if it divides $\det(A)$. Show that if we change the definition of e_{i4} to $e_{i4} = d - \sum_{j=1}^{3} e_{ij}$ for some other non-zero integer d and define δ_d using the new $A = (e_{ij})$, then δ_1 divides δ_d for all d. I.e., $d = 1$ is the optimal choice to minimize δ.

Exercise 10.2. With c_i and e_{ij} as above, show that the system of equations

$$\prod_{j=1}^{4} d_j^{e_{ij}} = c_i^{-1} \qquad i = 1, \dots, 4$$

has a solution with $d_j \in \overline{\mathbb{F}}_q$, $j = 1, \dots, 4$.

Proof of Theorem 12.4 of Lecture 1. Briefly, the hypotheses imply that the associated elliptic surface $\mathcal{E} \to \mathbb{P}^1$ is dominated by a Fermat surface (of degree δ) and thus by a product of Fermat curves (of degree δ). Thus Theorem 9.1 implies that BSD holds for E.

In more detail, note that $\mathcal{E}$ is birational to the affine surface $V(f) \subset \mathbb{A}^3_k$. So it will suffice to show that $V(f)$ is dominated by a product of curves. To that end, it will be convenient to identify $k[t, x, y]$ and $R = k[x_1, x_2, x_3]$ by sending $t \mapsto x_1$, $x \mapsto x_2$ and $y \mapsto x_3$, so that f becomes

$$f = \sum_{i=1}^{4} c_i \prod_{j=1}^{3} x_j^{e_{ij}}.$$

Exercise 10.2 implies that, after extending k if necessary, we may change coordinates ($x_j \mapsto d_j x_j$) so that the coefficients c_i are all 1. Then the matrix A defines rational a map ϕ from $V(f)$ to the Fermat surface of degree 1

$$F_1^2 = \{y_1 + y_2 + y_3 + y_4 = 0\} \subset \mathbb{P}^3_k,$$

namely $\phi^*(y_i) = \prod_{j=1}^4 x_j^{e_{ij}}$. Similarly, the matrix B defines a rational map ψ from the Fermat surface of degree δ

$$F_\delta^2 = \{z_1^\delta + z_2^\delta + z_3^\delta + z_4^\delta = 0\} \subset \mathbb{P}^3_k$$

to $V(f)$, namely $\psi^*(x_i) = \prod_{j=1}^4 z_j^{B_{ij}}$. The composition of these maps is the standard projection from F_δ^2 to F_1^2, namely $y_i \mapsto z_i^\delta$ and so both maps are dominant.

Finally, Shioda and Katsura [SK79] showed that F_δ^2 is dominated by the product of Fermat curves $F_\delta^1 \times F_\delta^1$. Thus, after extending k, $\mathcal{E}$ is dominated by a product of curves and Theorem 9.1 finishes the proof. □

As we will explain below, this Theorem can be combined with results on analytic ranks to give examples of elliptic curves over $\mathbb{F}_p(t)$ with arbitrarily large Mordell-Weil rank. (In fact, similar ideas can be used to produce Jacobians of every dimension with large rank. For this, see [Ulm07] and also [Ulm11].)

Unfortunately, Theorem 12.4 is very rigid—as one sees in the proof, varying the coefficients in the 4-nomial f does not vary the isomorphism class of $\mathcal{E}$ over $\overline{\mathbb{F}}_q$ and so we get only finitely many non-isomorphic elliptic curves over $\overline{\mathbb{F}}_p(t)$. Berger's construction, explained in the next subsection, was motivated by a desire to overcome this rigidity and give *families* of examples of curves where one knows the BSD conjecture.

11. Berger's construction

Berger gave a much more flexible construction of surfaces that are dominated by a product of curves in a tower. More precisely, we note that if $\mathcal{E} \to \mathbb{P}^1$ is an elliptic surface and $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is the morphism with $\phi^*(t) = u^d$ (corresponding to the field extension $k(u)/k(t)$ with $u^d = t$), then it is not in general the case that the base changed surface

$$\begin{array}{ccc} \mathcal{E}' = \mathcal{E} \times \mathbb{P}^1_k & \longrightarrow & \mathbb{P}^1_k \\ \downarrow & & \downarrow \\ \mathbb{P}^1_k & \xrightarrow{\phi} & \mathbb{P}^1_k \end{array}$$

is dominated by a product of curves. Berger's construction gives a rich class of curves for which DPC *does* hold in every layer of a tower of coverings. We restate Theorem 12.5 from Lecture 1 in a slightly different (but visibly equivalent) form.

Theorem 11.1. *Let E be an elliptic curve over $K = k(t)$ and assume that there are rational functions $f(x)$ and $g(y)$ on $\mathbb{P}^1_k$ such that E is birational to the curve $V(f(x) - tg(y)) \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$. Then the BSD conjecture holds for E over the field $k(u) = k(t^{1/d})$ for all d prime to p.*

Proof. Clearing denominators we may interpret $f(x) - tg(y)$ as defining a hypersurface $\mathcal{X}$ in the affine space $\mathbb{A}^3$ with coordinates x, y, and t and it is clear that the elliptic surface $\mathcal{E} \to \mathbb{P}^1$ associated to E is birationally isomorphic to $\mathcal{X}$.

On the other hand, $\mathcal{X}$ is visibly birational to $\mathbb{P}^1 \times \mathbb{P}^1$ since we may eliminate t. Thus $\mathcal{X}$ and $\mathcal{E}$ are dominated by a product of curves. This checks the case $d = 1$.

For larger d, note that the elliptic surface $\mathcal{E}_d \to \mathbb{P}^1$ associated to $E/k(u)$ is birational to the hypersurface $\mathcal{X}_d$ in $\mathbb{A}^3_k$ defined by $f(x) - u^d g(y)$. Berger showed by a fundamental group argument, generalizing [Sch96], that $\mathcal{X}_d$ is dominated by a product of curves, more precisely, by a product of covers of $\mathbb{P}^1$. (For her argument to be correct, π_1 should be replaced by the prime-to-p fundamental group $\pi_1^{p'}$ throughout.) This was later made more explicit in [Ulm09a], where it was observed that $\mathcal{X}_d$ is dominated by a product of two explicit covers of $\mathbb{P}^1$.

More precisely, let $\mathcal{C}_d$ and $\mathcal{D}_d$ be the covers of $\mathbb{P}^1_k$ defined by $z^d = f(x)$ and $w^d = g(y)$. Then there is a rational map from $\mathcal{C}_d \times \mathcal{D}_d$ to the hypersurface $\mathcal{X}_d$, namely

$$(x, z, y, w) \mapsto (x, y, u = z/w).$$

This is clearly dominant and so $\mathcal{X}_d$ and $\mathcal{E}$ are dominated by products of curves.

Applying Theorem 9.1 finishes the proof. □

Note that there is a great deal of flexibility in the choice of data for Berger's construction. As an example, take $f(x) = x(x-a)/(x-1)$ and $g(y) = y(y-1)$ where $a \in \mathbb{F}_q$ is a parameter. Then if $a \neq 1$, the curve $f(x) = tg(y)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ has genus 1 and a rational point. A simple calculation shows that it is birational to the Weierstrass cubic

$$y^2 + txy - ty = x^3 - tax^2 + t^2 ax.$$

Theorem 11.1 implies that this curve satisfies the BSD conjecture over $\mathbb{F}_{q^n}(t^{1/d})$ for all n and all d prime to p. Varying q and a we get infinitely many curves for which BSD holds at every layer of a tower.

We will give more examples and discuss further applications of the idea behind Berger's construction in Lectures 4 and 5.

LECTURE 4

Unbounded ranks in towers

In order to prove results on analytic ranks in towers, we need a more sophisticated approach to L-functions. In this lecture we explain Grothendieck's approach to L-functions over function fields and then use it and a new linear algebra lemma to find elliptic curves with unbounded analytic and algebraic ranks in towers of function fields.

1. Grothendieck's analysis of L-functions

1.1. Galois representations

As usual, we let $K = k(\mathcal{C})$ be the function field of a curve over a finite field k and $G_K = \mathrm{Gal}(K^{sep}/K)$ its Galois group. As in Lecture 0, Section 2, we write D_v, I_v, and Fr_v for the decomposition group, inertia group, and (geometric) Frobenius at a place v of K.

We fix a prime $\ell \neq p$ and consider a representation

$$\rho : G_K \to \mathrm{GL}(V) \cong \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell) \tag{1.1.1}$$

on a finite-dimensional $\overline{\mathbb{Q}}_\ell$ vector space. We make several standing assumptions about ρ.

First, we always assume ρ is continuous and unramified away from a finite set of places of K. By a compactness argument (see [KS99, 9.0.7]) , it is possible to define ρ over a finite extension L of $\mathbb{Q}_\ell$, i.e., there is a representation

$$\rho' : G_K \to \mathrm{GL}_n(L)$$

isomorphic to ρ over $\overline{\mathbb{Q}}_\ell$. Nothing we say will depend on the field of definition of ρ and we will generally not distinguish between ρ and isomorphic representations defined over subfields of $\overline{\mathbb{Q}}_\ell$.

We also always assume that ρ is pure of integral weight w, i.e., for all v where ρ is unramified, the eigenvalues of $\rho(\mathrm{Fr}_v)$ are Weil numbers of size $q_v^{w/2}$.

Finally, we sometimes assume that ρ is "symplectically self-dual of weight w." This means that on the space V where ρ acts, there is an G_K-equivariant, alternating pairing with values in $\overline{\mathbb{Q}}_\ell(-w)$.

1.2. Conductors

The Artin conductor of ρ is a divisor on $\mathcal{C}$ (a formal sum of places of K) and is a measure of its ramification. We write $\mathrm{Cond}(\rho) = \mathfrak{n} = \sum_v n_v[v]$. To define the local coefficients, fix a place v of K and let $G_i \subset I_v$ be the higher ramification groups at v (in the lower numbering). Then define

$$n_v = \sum_{i=0}^{\infty} \frac{1}{[G_0 : G_i]} \dim V/V^{G_i}.$$

Here V^{G_i} denotes the subspace of V invariant under G_i. It is clear that $n_v = 0$ if and only if ρ is unramified at v. If ρ is tamely ramified at v (i.e., G_1 acts trivially), then $n_v = \dim V/V^{G_0} = \dim V/V^{I_v}$. In general, the first term of the sum above is the *tame conductor* and the rest of the sum is the *Swan conductor*. We refer to [Mil80, V.2] and also [Ser77, §19] for an alternative definition and more discussion about the conductor, including the fact that the local coefficients n_v are integers.

1.3. L-functions

Let us fix an isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ so that we may regard eigenvalues of Frobenius on ℓ-adic representations as complex numbers. Having done this, a representation (1.1.1) gives rise to an L-function, defined as an Euler product:

$$L(\rho, T) = \prod_v \det\left(1 - T \operatorname{Fr}_v | V^{I_v}\right) \tag{1.3.1}$$

and $L(\rho, s) = L(\rho, q^{-s})$. The product is over the places of K, the exponent I_v denotes the subspace of elements invariant under the inertia group I_v, and Fr_v is a Frobenius element at v.

Because of our assumption that ρ is pure of weight w, the product defining $L(\rho, s)$ converges absolutely and defines a holomorphic function in the region $\operatorname{Re} s > w/2 + 1$.

It is clear from the definition that if ρ and σ are Galois representations then $L(\rho \oplus \sigma, s) = L(\rho, s)L(\sigma, s)$ and $L(\rho(n), s) = L(\rho, s - n)$.

It is also clear that $L(\rho_{triv}, s) = \zeta(\mathcal{C}, s)$. and so $L(\rho_{triv}(n), s) = \zeta(\mathcal{C}, s - n)$.

Exercise 1.3.2. Prove that if ρ factors through $G_K \to G_k$, so that Fr_v goes to $\alpha^{\deg v}$, then

$$L(\rho, T) = Z(\mathcal{C}, \alpha T)$$

is a twisted version of the zeta function of $\mathcal{C}$. Compare with Exercise 9.2 of Lecture 1. Note that a representation factors through $G_K \to G_k$ if and only if it is trivial on $G_{\overline{k}K}$, so this exercise fills in the missing cases in the following theorem.

Theorem 1.3.3. *Suppose that ρ is a representation of G_K (satisfying the standing hypotheses of Subsection 1.1) that contains no copies of the trivial representation when restricted to $G_{\overline{k}K}$. Then there is a canonically defined $\overline{\mathbb{Q}}_\ell$-vector space $H(\rho)$ with continuous G_k action such that*

$$L(\rho, s) = \det\left(1 - q^{-s} \operatorname{Fr}_q | H(\rho)\right).$$

The dimension of $H(\rho)$ is $\deg(\rho)(2g_{\mathcal{C}} - 2) + \deg \mathfrak{n}$ where $\mathfrak{n}$ is the conductor of ρ.

Proof. (Sketch) The representation $\rho : G_K \to \mathrm{GL}(V)$ gives rise to a constructible sheaf $\mathcal{F}_\rho$ on $\mathcal{C}$. In outline: ρ is essentially the same thing as a lisse sheaf $\mathcal{F}_U$ on the open subset $j : U \hookrightarrow \mathcal{C}$ over which ρ is unramified. We defined $\mathcal{F}_\rho$ as the push-forward $j_*\mathcal{F}_U$. For each closed point v of $\mathcal{C}$, the stalk of ρ at v is V^{I_v}.

Let $H^i(\overline{\mathcal{C}}, \mathcal{F})$ be the étale cohomology groups of $\mathcal{F}$. They are finite dimensional $\overline{\mathbb{Q}}_\ell$ vector spaces and give continuous representations of G_k.

The Grothendieck-Lefschetz fixed point formula says that for each finite extension $\mathbb{F}_{q^n}$ of $k \cong \mathbb{F}_q$, we have

$$\sum_{x \in \mathcal{C}(\mathbb{F}_{q^n})} \operatorname{Tr}(Fr_x | \mathcal{F}_x) = \sum_{i=0}^{2} (-1)^i \operatorname{Tr}\left(Fr_{q^n} | H^i(\overline{\mathcal{C}}, \mathcal{F})\right).$$

On the left hand side, the sum is over points of $\mathcal{C}$ with values in $\mathbb{F}_{q^n}$ and the summand is the trace of the action of the Frobenius at x on the stalk of $\mathcal{F}$ at a geometric point over x.

Multiplying both sides by T^n/n, summing over $n \geq 1$, and exponentiating, one finds that

$$L(\rho, T) = \prod_{i=0}^{2} \det\left(1 - T \operatorname{Fr}_q | H^i(\overline{\mathcal{C}}, \mathcal{F})\right)^{(-1)^{i+1}}.$$

Now $H^0(\overline{\mathcal{C}}, \mathcal{F})$ and $H^2(\overline{\mathcal{C}}, \mathcal{F})$ are isomorphic respectively to the invariants and coinvariants of V under $G_{\overline{k}K}$ and so under our hypotheses on ρ, $H^i(\overline{\mathcal{C}}, \mathcal{F})$ vanishes for $i = 0, 2$. Thus we have

$$L(\rho, s) = \det\left(1 - q^{-s} \operatorname{Fr}_q | H(\rho)\right)$$

where $H(\rho) = H^1(\overline{\mathcal{C}}, \mathcal{F})$.

The dimension formula comes from an Euler characteristic formula proven by Raynaud and sometimes called the Grothendieck-Ogg-Shafarevich formula. It says

$$\sum_{i=0}^{2} (-1)^i \dim H^i(\overline{\mathcal{C}}, \mathcal{F}) = \deg(\rho)(2 - 2g_{\mathcal{C}}) - \deg(\operatorname{Cond}(\rho)).$$

Since H^0 and H^2 vanish, this gives the desired dimension formula. □

Obviously we have omitted many details. I recommend [Mil80, V.1 and V.2] as a compact and readable source for several of the key points, including passing from ℓ-torsion sheaves to ℓ-adic sheaves, the conductor, and the Grothendieck-Ogg-Shafarevich formula. See [Mil80, VI.13] for the Grothendieck-Lefschetz trace formula.

Remark/Exercise 1.3.4. If we are willing to use a virtual representation of G_k in place of a usual representation, then the Theorem has a more elegant restatement which avoids singling out representations that are trivial when restricted to $G_{\overline{k}K}$. State and prove this generalization.

Exercise 1.3.5. Check that we have the Artin formalism formula: if F/K is a finite separable extension and ρ is a representation of G_F, then

$$L(\rho, s) = L(\operatorname{Ind}_{G_F}^{G_K} \rho, s).$$

Note that the left hand side is an Euler product on F with almost all factors of some degree, say N, whereas the right hand side is an Euler product on K, with almost all factors of degree $N[F : K]$. The equality can be taken to be an equality of Euler products, where that on the left is grouped according to the places of K.

1.4. Functional equation and Riemann hypothesis

Theorem 1.3.3 shows that the L-function of ρ has an analytic continuation to the entire s plane (meromorphic if we allow ρ to have trivial factors over $\overline{k}K$). In this section we deduce other good analytic properties of $L(\rho, s)$.

Theorem 1.4.1. *Suppose (in addition to the standing hypotheses) that ρ is symplectically self-dual of weight w. Then $L(\rho, s)$ satisfies a functional equation*

$$L(\rho, w + 1 - s) = \pm q^{N(s-(w+1)/2)} L(\rho, s)$$

where $N = (2g_{\mathcal{C}} - 2)\deg(\rho) + \deg(\operatorname{Cond}(\rho))$. The zeroes of ρ lie on the line $\operatorname{Re} s = (w + 1)/2$.

PROOF. (Sketch) We use the notation of the proof of Theorem 1.3.3. The functional equation comes from a symmetric pairing

$$H(\rho) \times H(\rho) \to H^2(\overline{\mathcal{C}}, \overline{\mathbb{Q}}_\ell(-w)) \cong \overline{\mathbb{Q}}_\ell(-w-1).$$

(Symmetric because ρ is skew-symmetric and $H = H^1$.) That there is such a pairing is not as straightforward as it looks, because we defined the sheaf $\mathcal{F}$ as a push forward $j_*\mathcal{F}_U$ where $j : U \hookrightarrow \mathcal{C}$ is a non-empty open set over which ρ is unramified and $\mathcal{F}_U$ is the lisse sheaf on U corresponding to ρ. It is well-known that j^* identifies $H^1(\overline{\mathcal{C}}, \mathcal{F})$ with the image of the "forget supports" map

$$H^1_c(\overline{U}, \mathcal{F}_U) \to H^1(\overline{U}, \mathcal{F}_U)$$

from compactly supported cohomology to usual cohomology. (This is often stated, but the only proof I know of in the literature is [Ulm05, 7.1.6].) The cup product

$$H^1_c(\overline{U}, \mathcal{F}_U) \times H^1(\overline{U}, \mathcal{F}^*_U) \to H^2_c(\overline{U}, \overline{\mathbb{Q}}_\ell) \cong \overline{\mathbb{Q}}_\ell(-1)$$

then induces a pairing on $H^1(\overline{\mathcal{C}}, \mathcal{F})$ via the above identification. Poincaré duality shows that the pairing is non-degenerate and so $H(\rho)$ is orthogonally self-dual of weight $w+1$.

The location of the zeroes is related to the eigenvalues of Frobenius on $H(\rho) = H^1(\overline{\mathcal{C}}, \mathcal{F})$ and these are Weil numbers of size q^{w+1} by Deligne's purity theorem [Del80]. I recommend the Arizona Winter School 2000 lectures of Katz (published as [Kat01]) for a streamlined proof of Deligne's theorem in the generality needed here. □

2. The case of an elliptic curve

Next, we apply the results of the previous section to elliptic curves. Throughout, E will be an elliptic curve over a function field $K = k(\mathcal{C})$ over a finite field k of characteristic p.

2.1. The Tate module

We consider the Tate module of E. More precisely, fix a prime $\ell \neq p$ and let

$$T_\ell E = \varprojlim_n E(\overline{K})[\ell^n] \quad \text{and} \quad V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let ρ_E be the representation of G_K on the dual vector space $V_\ell^* = \mathrm{Hom}(V_\ell E, \mathbb{Q}_\ell) \cong H^1(\overline{E}, \mathbb{Q}_\ell)$. Then ρ_E is two-dimensional and continuous and (by the criterion of Ogg-Néron-Shafarevich, see [ST68, Thm. 1]) it is unramified outside the (finite) set of places where E has bad reduction.

At every place v of K where E has good reduction, we have

$$\det(1 - \rho(\mathrm{Fr}_v)T) = 1 - a_v T + q_v T^2$$

where a_v is defined as in (8.3) by $\#E_v(\kappa_v) = 1 - a_v + q_v$. This follows from the smooth base change theorem [Mil80, VI.4] and the cohomological description of the zeta function of the reduction, as in Section 4 of Lecture 0. Thus ρ is pure of weight $w = 1$.

The Weil pairing induces an alternating, G_k-equivariant pairing $V_\ell E \times V_\ell E \to \mathbb{Q}_\ell(-1)$ and so ρ is symplectically self-dual of weight 1.

If E is constant, then ρ_E factors through $G_K \to G_k$ and since G_k is abelian, ρ_E is the direct sum of two characters. More precisely, if $E \cong E_0 \times_k K$ and

$1 - aT + qT^2 = (1 - \alpha_1 T)(1 - \alpha_2 T)$ is the numerator of the Z-function of E_0, then ρ_E is the sum of the two characters that send Fr_v to $\alpha_i^{\deg v}$.

If E is non-isotrivial, then ρ_E restricted to $G_{\overline{k}K}$ has no trivial subrepresentations. One way to see this is to use a slight generalization of the MWLN theorem, according to which $E(\overline{k}K)$ is finitely generated (when E is non-isotrivial). Thus its ℓ-power torsion is finite and this certainly precludes a trivial subrepresentation in $\rho|_{G_{\overline{k}K}}$. In fact, by a theorem of Igusa [Igu59], $\rho|_{G_{\overline{k}K}}$ is contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ so is certainly irreducible, even absolutely irreducible.

Exercise 2.1.1. Show that if E is isotrivial but not constant, then ρ_E restricted to $G_{\overline{k}K}$ has no trivial subrepresentation. Hint: E is a twist of a contant curve $E' = E_0 \times_k K$. Relate the action of G_K on the Tate module of E to its action on that of E' and show that there exists an element $\sigma \in G_{\overline{k}K}$ that acts on $V_\ell E$ via a non-trivial automorphism of E. But a non-trivial automorphism has only finitely many fixed points.

We can summarize this discussion as follows.

Proposition 2.1.2. *Let ρ be the action of G_K on the Tate module $V_\ell E$ of E. Then ρ is continuous, unramified outside a finite set of places of K, and is pure and symplectically self-dual of weight 1. If E is non-constant, then $\rho|_{G_{\overline{k}K}}$ has no trivial subrepresentations.*

The conductor of ρ_E as defined in the previous section is equal to the conductor of E as mentioned in Section 8 of Lecture 1. This was proven by Ogg in [Ogg67].

2.2. The L-function

Applying the results of the previous section, we get a very satisfactory analysis of the L-function of E. Since we know everything about the constant case by an elementary analysis (cf. exercise 9.2 of Lecture 1), we restrict to the non-constant case.

Theorem 2.2.1. *Let E be a non-constant elliptic curve over $K = k(\mathcal{C})$ and let q be the cardinality of k. Let $\mathfrak{n}$ be the conductor of E. Then $L(E, s)$ is a polynomial in q^{-s} of degree $N = 4g_{\mathcal{C}} - 4 + \deg(\mathfrak{n})$. Its inverse roots are Weil numbers of size q and it satisfies a functional equation*

$$L(E, 2 - s) = \pm q^{N(s-1)} L(E, s).$$

Combining the Theorem with Theorem 12.1, we obtain the following.

Corollary 2.2.2. *The rank of $E(K)$ is bounded above by $N = 4g_{\mathcal{C}} - 4 + \deg(\mathfrak{n})$. If equality holds, then $L(E, s) = (1 - q^{1-s})^N$.*

The sign in the functional equation can be computed as a product of local factors. This can be seen via the connection with automorphic forms (a connection which is outside the scope of these lectures) or, because we are in the function field situation, directly via cohomological techniques. See [Lau84] for the latter.

3. Large analytic ranks in towers

3.1. Statement of the theorem

We give a general context in which one obtains large analytic ranks by passing to layers of a suitable tower of function fields.

As usual, let p be a prime and q a power of p. Let $K = \mathbb{F}_q(t)$, for each d not divisible by p, set $F_d = \mathbb{F}_q(t^{1/d}) \cong \mathbb{F}_q(u)$, and $K_d = \mathbb{F}_q(\mu_d)(t^{1/d}) \cong \mathbb{F}_q(\mu_d)(u)$.

Suppose that E is an elliptic curve over K. Let $\mathfrak{n}$ be the conductor of E and let

$$\mathfrak{n}' = \mathfrak{n} - \dim(V_\ell E/V_\ell E^{I_0})[0] - \dim(V_\ell E/V_\ell E^{I_\infty})[\infty].$$

This is the conductor of E except that we have removed the tame part at $t = 0$ and $t = \infty$.

Theorem 3.1.1. *Let E be an elliptic curve over K and define $\mathfrak{n}'$ as above. Suppose that $\deg \mathfrak{n}'$ is odd. Then the analytic rank of E over F_d (and K_d) is unbounded as d varies. More precisely, there exists a constant c depending only on E such that if d has the form $d = q^n + 1$, then*

$$\operatorname{ord}_{s=1} L(E/F_d, s) \geq \frac{d}{2n} - c = \frac{q^n + 1}{2n} - c.$$

and

$$\operatorname{ord}_{s=1} L(E/K_d, s) \geq d - c = q^n + 1 - c$$

This theorem is proven in detail in [Ulm07, §2-4]. We will sketch the main lines of the argument below.

3.2. A linear algebra lemma

Our analytic rank results ultimately come from the following odd-looking result of linear algebra.

Proposition 3.2.1. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i \in \mathbb{Z}/a\mathbb{Z}$ such that $V = \oplus_{i \in \mathbb{Z}/a\mathbb{Z}} W_i$. Let $\phi : V \to V$ be an invertible linear transformation such that $\phi(W_i) = W_{i+1}$ for all $i \in \mathbb{Z}/a\mathbb{Z}$. Suppose that V admits a non-degenerate, ϕ-invariant symmetric bilinear form $\langle , \rangle$. Suppose that a is even and $\langle , \rangle$ induces an isomorphism $W_{a/2} \cong W_0^*$ (the dual vector space of W_0). Suppose also that $N = \dim W_0$ is odd. Then the polynomial $1 - T^a$ divides $\det(1 - \phi T | V)$.*

We omit the proof of this proposition, since it is not hard and it appears in two forms in the literature already. Namely, embedded in [Ulm05, 7.1.11ff] is a matrix-language proof of the proposition, and a coordinate-free proof is given in [Ulm07, §2].

3.3. Sketch of the proof of Theorem 3.1.1

For simplicity, we assume that E is non-isotrivial. (If $p > 3$ and E is isotrivial, then the theorem is vacuous because all of the local conductor exponents n_v are even.) Let ρ be the representation of G_K on $V = H^1(\overline{E}, \mathbb{Q}_\ell) = (V_\ell E)^*$ and let ρ_d be the restriction of ρ to G_{F_d}. Then by Grothendieck's analysis, we have

$$L(E/F_d, s) = \det\left(1 - \operatorname{Fr}_q q^{-s} | H(\rho_d)\right).$$

Here $H(\rho_d)$ is an H^1 on the rational curve whose function field is $F_d = \overline{\mathbb{F}}_q(u) = \overline{\mathbb{F}}_q(t^{1/d})$.

The projection formula in cohomology (a parallel of the Artin formalism 1.3.5) implies that

$$H(\rho_d) \cong H(\operatorname{Ind}_{G_{F_d}}^{G_K} \rho) \cong H(\rho \otimes \operatorname{Ind}_{G_{F_d}}^{G_K} \mathbf{1})$$

where $\mathbf{1}$ denotes the trivial representation. Since the cohomology H is computed on $\overline{\mathbb{P}}^1_u$ (the $\mathbb{P}^1$ with coordinate u, with scalars extended to $\overline{\mathbb{F}}_q$) and $\overline{\mathbb{P}}^1_u \to \overline{\mathbb{P}}^1_t$ is Galois with group μ_d, we have

$$H(\rho_d) \cong \bigoplus_{j=0}^{d-1} H(\rho \otimes \chi^j)$$

where χ is a character of $\mathrm{Gal}(\overline{\mathbb{F}}_q(u)/\overline{\mathbb{F}}_q(t))$ of order exactly d.

Now the decomposition displayed above is not preserved by Frobenius. Indeed Fr_q sends $H(\rho \otimes \chi^j)$ to $H(\rho \otimes \chi^{qj})$. Thus we let $o \subset \mathbb{Z}/d\mathbb{Z}$ denote an orbit for multiplication by q and we regroup:

$$H(\rho_d) \cong \bigoplus_{o \subset \mathbb{Z}/d\mathbb{Z}} \left(\bigoplus_{j \in o} H(\rho \otimes \chi^j) \right).$$

We write V_o for the summand indexed by an orbit $o \subset \mathbb{Z}/d\mathbb{Z}$ in the last display and a_o for the cardinality of o. As we will see presently, the hypotheses of the theorem imply that Proposition 3.2.1 applies to most of the V_o and for each one where it does, we get a zero of the L-function. Before we do that, there is one small technical point to take care of: The linear algebra proposition requires that V be literally self-dual (not self-dual with a weight) and it implies that 1 is an eigenvalue of ϕ on V. To get the eigenvalue q that we need, we should twist ρ by $-1/2$ (which is legitimate once we have fixed choice of square root of q) so that it has weight 0, apply the lemma, and twist back to get the desired zero. We leave the details of these points to the reader.

Assuming we have made the twist just mentioned, we need to check which V_o are self-dual. Since ρ is self-dual, Poincaré duality gives a non-degenerate pairing on $H(\rho_d)$ which puts $H(\rho \otimes \chi^j)$ in duality with $H(\rho \otimes \chi^{-j})$. Thus if $d = q^n + 1$ for some $n > 0$, then all of the orbits o will yield a self-dual V_o. Possibly two of these orbits have odd order (those through 0 and $d/2$, which have order 1) and all of the other have a_o even. Moreover, for the orbits of even order, setting $W_{o,i} = H(\rho \otimes \chi^{q^i j_o})$ for some fixed $j_o \in o$, we have

$$V_o \cong \bigoplus_{i=0}^{a_o - 1} W_{o,i}$$

with $W_{o,i}$ and $W_{o,i+a_0/2}$ in duality.

The last point that we need is that $W_{o,i}$ should be odd-dimensional. The hypothesis on $\mathfrak{n}'$ implies that for all characters χ^j of sufficiently high order (depending only on E), the conductor of $\rho \otimes \chi^j$ is odd. The Grothendieck-Ogg-Shafarevich dimension formula (mentioned at the end of the proof of Theorem 1.3.3) then implies that for all orbits o consisting of characters of high order, $H(\rho \otimes \chi^{j_o})$ has odd dimension.

The linear algebra proposition 3.2.1 now implies that for $d = q^n + 1$ and for most orbits $o \subset \mathbb{Z}/d\mathbb{Z}$, 1 is an eigenvalue of Fr_q on V_o (and q is an eigenvalue of Fr_q on the corresponding factor of $H(\rho_d)$). Since each of these orbits has size $\leq 2n$, there is a constant c such that the number of "good" orbits is $\geq d/2n$. Thus

$$\mathrm{ord}_{s=1} L(E/F_d, s) \geq \frac{d}{2n} - c$$

for a constant c depending only on E.

To get the assertions over K_d, note that in passing from F_d to K_d, each factor $(1 - q^{a_o}T^{a_o})$ of $L(E/F_d, T)$ becomes $(1 - qT)^{a_o}$ and so

$$\mathrm{ord}_{s=1} L(E/K_d, s) \geq d - c$$

for another c independent of E.

This completes our discussion of Theorem 3.1.1. We refer to [Ulm07, §2-4] for more details. □

3.4. Examples

It is easy to see that the hypotheses in Theorem 3.1.1 are not very restrictive and that high analytic ranks are in a sense ubiquitous. The following rephrasing of the condition in the theorem should make this clear.

Exercise 3.4.1. Prove that if $p > 3$ and E is an elliptic curve over K, then Theorem 3.1.1 guarantees that E has unbounded analytic rank in the tower F_d if the number of geometric points of $\mathbb{P}^1_{\mathbb{F}_q}$ over which E has multiplicative reduction is odd.

Corollary 3.4.2. *Let p be any prime number, $K = \mathbb{F}_p(t)$, and let E be one of the curves E_7, E_8, or E_9 defined in Subsection 1.2 of Lecture 1. Then*

$$\mathrm{ord}_{s=1} L(E/\mathbb{F}_p(t^{1/d}), s)$$

is unbounded as d varies through integers prime to p

Proof. If $p > 3$, then one sees immediately by considering the discriminant and j-invariant that E has one finite, non-zero place of multiplicative reduction and is tame at 0 and ∞, thus it satisfies the hypotheses of Theorem 3.1.1. If $p = 2$ or 3, one checks using Tate's algorithm that E has good reduction at all finite non-zero places and is tame at zero, but the wild part of the conductor at ∞ is odd and so the theorem again applies. □

For another example, take the Legendre curve

$$y^2 = x(x - 1)(x - t)$$

over $\mathbb{F}_p(t)$, $p > 2$. It is tame at 0 and ∞ and has exactly one finite, non-zero place of multiplicative reduction.

4. Large algebraic ranks

4.1. Examples via the four-monomial theorem

Noting that the curves E_7, E_8, and E_9 are defined by equations involving exactly four monomials, we get a very nice result on algebraic ranks.

Theorem 4.1.1. *Let p be any prime number, $K = \mathbb{F}_p(t)$, and let E be one of the curves E_7, E_8, or E_9 defined in Subsection 1.2 of Lecture 1. Then for all d prime to p and all powers q of p, the Birch and Swinnerton-Dyer conjecture holds for E over $K_d = \mathbb{F}_q(t^{1/d})$. Moreover, the rank of $E(\mathbb{F}_p(t^{1/d}))$ is unbounded as d varies.*

Proof. This follows immediately from Corollary 3.4.2 and Theorem 12.4 of Lecture 1 as soon as we note that E/K_d is defined by an equation satisfying Shioda's conditions. □

Similar ideas can be used to show that for every prime p and every genus $g > 0$, there is an explicit hyperelliptic curve C over $\mathbb{F}_p(t)$ such that the Jacobian of C satisfies BSD over $\mathbb{F}_q(t^{1/d})$ for all q and d and has unbounded rank in the tower $\mathbb{F}_p(t^{1/d})$. This is the main theorem of [Ulm07].

4.2. Examples via Berger's construction

As we pointed out in Lecture 3, the Shioda 4-monomial construction is rigid—varying the coefficients does not lead to families that vary geometrically. Berger's thesis developed a new construction with parameters that leads to families of curves for which the BSD conjecture holds in a tower of fields. This together with the analytic ranks result 3.1.1 gives examples of families of elliptic curves with unbounded ranks.

To make this concrete, we quote the first example with parameters from [Ber08] that, together with the analytic rank construction 3.1.1, gives rise to unbounded analytic and algebraic ranks.

Theorem 4.2.1 (Berger)**.** *Let $k = \mathbb{F}_q$ be a finite field of characteristic p and let $a \in \mathbb{F}_q$ with $a \neq 0, 1, 2$. Let E be the elliptic curve over $K = \mathbb{F}_q(t)$ defined by*

$$y^2 + a(t-1)xy + a(t^2-t)y = x^3 + (2a+1)tx^2 + a(a+2)t^2x + a^2t^3.$$

Then for all d prime to p the BSD conjecture holds for E over $\mathbb{F}_q(t^{1/d})$. Moreover, for every q and a as above, the rank of $E(\mathbb{F}_q(t^{1/d}))$ is unbounded as d varies.

Proof. This is an instance of Berger's construction (Theorem 11.1 of Lecture 3). Indeed, let $f(x) = x(x-a)/(x-1)$ and $g(y) = y(y-a)/(y-1)$. Then $V(f - tg) \subset \mathbb{P}^1_K \times \mathbb{P}^1_K$ is birational to E, which is a smooth elliptic curve for all $a \neq 0, 1$. Berger's Theorem 11.1 of Lecture 3 shows that E satisfies BSD over the fields $\mathbb{F}_q(t^{1/d})$.

The discriminant of E is

$$\Delta = a^2(a-1)^4t^4(t-1)^2\left(a^2t^2 - (2a^2 - 16a + 16)t + a^2\right).$$

Assume first that $p > 3$. One checks that Δ is relatively prime to c_4 so that the zeroes of Δ are places of multiplicative reduction. Since the discriminant (in t) of the quadratic factor $a^2t^2 - (2a^2 - 16a + 16)t + a^2$ is $-64(a-1)(a-2)^2$ we see that there are three finite, non-zero geometric points of multiplicative reduction. Since $p > 3$, the reduction at 0 and ∞ is tame and so $\mathfrak{n}'$ (defined as in Subsection 3.1 of Lecture 4) has degree 3. Thus by Theorem 3.1.1 of Lecture 4, E has unbounded analytic ranks in the tower $\mathbb{F}_q(t^{1/d})$ and thus also unbounded algebraic ranks by the previous paragraph on BSD.

If $p = 2$ or 3, one needs to use Tate's algorithm to compute $\mathfrak{n}'$, which again turns out to have degree 3. We leave the details of this computation as a pleasant exercise for the reader. □

LECTURE 5

More applications of products of curves

In the last part of Lecture 4, we chose special curves E and used a domination $\mathcal{C}\times\mathcal{D}\dashrightarrow\mathcal{E}$ of the associated surface to deduce the Tate conjecture for $\mathcal{E}$ and thus the BSD conjecture for E. This yields an *a priori* equality of analytic and algebraic ranks. We then used other, cohomological, methods (namely the analytic ranks theorem) to compute the analytic rank.

It turns out to be possible to use domination by a product of curves and geometry to prove directly results about algebraic ranks and explicit points. We sketch some of these applications in this lecture.

1. More on Berger's construction

Let k be a field (not necessarily finite), $K = k(t)$, and $K_d = k(t^{1/d}) = k(u)$. Recall that in Berger's construction we start with rational curves $\mathcal{C} = \mathbb{P}^1_k$ and $\mathcal{D} = \mathbb{P}^1_k$ and rational functions $f(x)$ on $\mathcal{C}$ and $g(y)$ on $\mathcal{D}$. We get a curve in $\mathbb{P}^1_K \times \mathbb{P}^1_K$ defined by $f(x) - tg(y) = 0$ and we let E be the smooth proper model over K of this curve. (Some hypotheses are required for this to exist, but they are weaker than our standing hypotheses below.) The genus of E was computed by Berger in [Ber08, Theorem 3.1]. All the examples we consider will be of genus 1 and will have a K-rational point.

We establish more notation to state a precise result. Let us assume for simplicity all the zeroes and poles of f and g are k-rational. Write

$$\text{(1.1)}\qquad \operatorname{div}(f) = \sum_{i=1}^{k} a_i P_i - \sum_{i'=1}^{k'} a'_{i'} P'_{i'} \quad \text{and} \quad \operatorname{div}(g) = \sum_{j=1}^{\ell} b_j Q_j - \sum_{j'=1}^{\ell'} b'_{j'} Q'_{j'}$$

with $a_i, a'_{i'}, b_i, b'_{j'}$ positive integers and P_i, $P'_{i'}$, Q_j, and $Q'_{j'}$ distinct k-rational points. Let

$$m = \sum_{i=1}^{k} a_i = \sum_{i'=1}^{k'} a'_{i'} \quad \text{and} \quad n = \sum_{j=1}^{\ell} b_j = \sum_{j'=1}^{\ell'} b'_{j'}.$$

As standing hypotheses, we assume that: (i) all the multiplicities a_i, $a'_{i'}$, b_j, and $b'_{j'}$ are prime to the characteristic of k; and (ii) $\gcd(a_1 \ldots, a_k, a'_1, \ldots, a'_{k'}) = \gcd(b_1 \ldots, b_\ell, b'_1, \ldots, b'_{\ell'}) = 1$.

Under these hypotheses, Berger computes that the genus of E is

$$\text{(1.2)}\qquad g_E = (m-1)(n-1) - \sum_{i,j} \delta(a_i, b_j) - \sum_{i',j'} \delta(a'_{i'}, b'_{j'})$$

where $\delta(a,b) = (ab - a - b + \gcd(a,b))/2$.

From now on we assume that we have chosen the data f and g so that E has genus 1. Two typical cases are where f and g are quadratic rational functions with

simple zeroes and poles, or where f and g are cubic polynomials. There is always a K-rational point on E; for example, we may take a point where x and y are zeroes of f and g.

Let $\mathcal{E}_d \to \mathbb{P}^1$ be the elliptic surface over k attached to E/K_d. It is clear that $\mathcal{E}_d$ is birational to the closed subset of $\mathbb{P}^1_k \times \mathbb{P}^1_k \times \mathbb{P}^1_k$ (with coordinates x, y, u) defined by the vanishing of $f(x) - u^d g(y)$. We saw in Section 11 of Lecture 3 that $\mathcal{E}$ is dominated by a product of curves and we would now like to make this more precise.

Recall that we defined covers $\mathcal{C}_d \to \mathcal{C} = \mathbb{P}^1$ and $\mathcal{D}_d \to \mathcal{D} = \mathbb{P}^1$ by the equations $z^d = f(x)$ and $w^d = g(y)$. Note that there is an action of μ_d, the d-th roots of unity, on $\mathcal{C}_d$ and on $\mathcal{D}_d$.

Proposition 1.3. *The surface $\mathcal{E}_d$ is birationally isomorphic to the quotient surface $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$ where μ_d acts diagonally.*

Proof. We have already noted that $\mathcal{E}_d$ is birational to the zero set $\mathcal{X}$ of $f(x) - u^d g(y)$ in $\mathbb{P}^1_k \times \mathbb{P}^1_k \times \mathbb{P}^1_k$. Define a rational map from $\mathcal{C}_d \times \mathcal{D}_d$ to $\mathcal{X}$ by sending (x, z, y, w) to $(x, y, u = z/w)$. It is clear that this map factors through the quotient $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$. Since the map is generically of degree d, it induces a birational isomorphism between $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$ and $\mathcal{X}$. Thus $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$ is birationally isomorphic to $\mathcal{E}_d$. □

In the next section we will explain how this birational isomorphism can be used to compute the Néron-Severi group of $\mathcal{E}_d$ and the Mordell-Weil group $E(K_d)$.

2. A rank formula

We keep the notation and hypotheses of the preceding subsection. Consider the base $\mathbb{P}^1_k$, the one corresponding to K, with coordinate t. For each geometric point x of this $\mathbb{P}^1_k$, let f_x be the number of components in the fiber of $\mathcal{E} \to \mathbb{P}^1$ over x. For almost all x, $f_x = 1$ and its value at any point can be computed using Tate's algorithm.

Define two constants c_1 and c_2 by the formulae

$$c_1 = \sum_{x \neq 0, \infty} (f_x - 1)$$

and

$$c_2 = (k-1)(\ell - 1) + (k' - 1)(\ell' - 1).$$

Here the sum is over geometric points of $\mathbb{P}^1_k$ except $t = 0$ and $t = \infty$ and k, k', ℓ, and ℓ' are the numbers of distinct zeroes and poles of f and g (cf. equation (1.1)). Note that c_1 and c_2 depend only on the data defining E/K, not on d.

Theorem 2.1. *Suppose that k is algebraically closed and that d is relatively prime to all of the multiplicities a_i, $a'_{i'}$, b_j, and $b'_{j'}$ and to the characteristic of k. Then we have*

$$\operatorname{Rank} E(K_d) = \operatorname{Rank} \operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} - c_1 d + c_2.$$

Here $\operatorname{Hom}(\cdots)^{\mu_d}$ signifies the homomorphisms commuting with the actions of μ_d on the two Jacobians induced by its action on the curves.

Sketch of Proof. In brief, we use the birational isomorphism

$$(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d \dashrightarrow \mathcal{E}_d$$

to compute the rank of the Néron-Severi group of $\mathcal{E}_d$ and then use the Shioda-Tate formula to compute the rank of $E(K_d)$.

More precisely, we saw in Lecture 2, Subsection 8.4 that the Néron-Severi group of the product $\mathcal{C}_d \times \mathcal{D}_d$ is isomorphic to $\mathbb{Z}^2 \times \operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})$. It follows easily that the Néron-Severi group of the quotient $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$ is isomorphic to $\mathbb{Z}^2 \times \operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d}$.

One then keeps careful track of the blow-ups needed to pass from $(\mathcal{C}_d \times \mathcal{D}_d)/\mu_d$ to $\mathcal{E}_d$. The effect of blow-ups on Néron-Severi is quite simple and was noted in Subsection 8.5 of Lecture 2. This is the main source of the term c_2 in the formula.

Finally, one computes the rank of $E(K_d)$ using the Shioda-Tate formula, as in Section 5 of Lecture 3. This step is the main source of the term $c_1 d$.

The hypothesis that k is algebraically closed is not essential for any of the above, but it avoids rationality questions that would greatly complicate the formula.

For full details on the proof of this theorem (in a more general context) see [Ulm09a, Section 6]. □

3. First examples

One of the first examples is already quite interesting. We give a brief sketch and refer to [Ulm09a] for more details.

With notation as in Section 1, we take $f(x) = x(x-1)$ and $g(y) = y^2/(1-y)$. The genus formula (1.2) shows that E has genus 1. In fact, the change of coordinates $x = -y/(x+t)$, $y = -x/t$ brings it into the Weierstrass form

$$y^2 + xy + ty = x^3 + tx^2.$$

We remark in passing that if the characteristic of k is not 2, E has multiplicative reduction at $t = 1/16$ and good reduction elsewhere away from 0 and ∞. Thus by the analytic rank result of Lecture 2, when k is finite, say $k = \mathbb{F}_p$ and $p > 3$, we expect E to have unbounded analytic rank in the tower $\mathbb{F}_p(t^{1/d})$. (In fact a more careful analysis gives the same conclusion for every p.)

Now assume that k is algebraically closed. To compute the constant c_1, one checks that (for k of any characteristic) E has exactly one irreducible component over each geometric point of $\mathbb{P}^1_k$. Thus $c_1 = 0$. It is immediate from the definition that $c_2 = 0$. Thus our rank formula yields

$$\operatorname{Rank} E(K_d) = \operatorname{Rank} \operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d}.$$

Next we note that there is an isomorphism $\phi : \mathcal{C}_d \to \mathcal{D}_d$ sending (x, z) to $(y = 1/x, w = 1/z)$. This isomorphism *anti-commutes* with the μ_d action: Let ζ_d be a primitive d-th root of unity and write $[\zeta_d]$ for its action on curves or Jacobians. Then $\phi \circ [\zeta_d] = [\zeta_d^{-1}] \circ \phi$. Using ϕ to identify $\mathcal{C}_d$ and $\mathcal{D}_d$, our rank formula becomes

$$\operatorname{Rank} E(K_d) = \operatorname{Rank} \operatorname{End}(J_{\mathcal{C}_d})^{anti-\mu_d}$$

where "$\operatorname{End}(\cdots)^{anti-\mu_d}$" denotes those endomorphisms anti-commuting with μ_d in the sense above.

Suppose that k has characteristic zero. Then a consideration of the (faithful) action of $\operatorname{End}(J_{\mathcal{C}_d})$ on the differentials $H^0(J_{\mathcal{C}_d}, \Omega^1)$ shows that $\operatorname{End}(J_{\mathcal{C}_d})^{anti-\mu_d} = 0$ for all d (see [Ulm09a, 7.6]). We conclude that for k of characteristic zero, the rank of $E(K_d)$ is zero for all d.

Now assume that k has characteristic p (and is algebraically closed). If we take d of the form $p^f + 1$ then we get many elements of $\mathrm{End}(J_{\mathcal{C}_d})^{anti-\mu_d}$. Namely, we consider the Frobenius Fr_{p^f} and compute that

$$\mathrm{Fr}_{p^f} \circ [\zeta_d] = [\zeta_d^{p^f}] \circ \mathrm{Fr}_{p^f} = [\zeta_d^{-1}] \circ \mathrm{Fr}_{p^f} .$$

The same computation shows that $\mathrm{Fr}_{p^f} \circ [\zeta_d^i]$ anticommutes with μ_d for all i. It turns out that there are two relations among these endomorphism in $\mathrm{End}(J_{\mathcal{C}_d})$ if $p > 2$ and just one relation if $p = 2$ (see [Ulm09a, 7.8-7.10]). Thus we find that, for d of the special form $d = p^f + 1$,

$$\mathrm{Rank}\, E(\overline{\mathbb{F}}_p(t^{1/d})) = \begin{cases} d-2 & \text{if } p > 2 \\ d-1 & \text{if } p = 2. \end{cases}$$

The reader may enjoy checking that this is in exact agreement with what the analytic rank result (Theorem 3.1.1 of Lecture 4) predicts.

Somewhat surprisingly, there are *more* values of d for which we get high ranks. A natural question is to identify all pairs (p, d) such that $E(\overline{\mathbb{F}}_p(t^{1/d})$ has "new" rank, i.e, points of infinite order not coming from smaller values of d. The exact set of pairs (p, d) for which we get high rank is mysterious. There are "systematic" cases (such as $(p, p^f + 1)$, as above, or $(p, 2(p-1))$) and other cases that may be sporadic. This is the subject of ongoing research so we will not go into more detail, except to note that the example in Section 5 below is relevant to this question.

4. Explicit points

The main ingredients in the rank formula of Section 2 are the calculation of the Néron-Severi group of a product of curves in terms of homomorphisms of Jacobians and the Shioda-Tate formula. Tracing through the proof leads to a homomorphism

$$\mathrm{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d} \cong \mathrm{DivCorr}(\mathcal{C}_d, \mathcal{D}_d) \to L^1\,\mathrm{NS}(\mathcal{E}_d) \to \frac{L^1\,\mathrm{NS}(\mathcal{E}_d)}{L^2\,\mathrm{NS}(\mathcal{E}_d)} \cong E(K_d).$$

For elements of $\mathrm{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d}$ where we can find an explicit representation in $\mathrm{DivCorr}(\mathcal{C}_d, \mathcal{D}_d)$, the geometry of Berger's construction leads to explicit points in $E(K_d)$. This applies notably to the endomorphisms $\mathrm{Fr}_{p^f} \circ [\zeta_d^i]$ appearing in the analysis of the first example above. Indeed, these endomorphisms are represented in $\mathrm{DivCorr}(\mathcal{C}_d, \mathcal{D}_d)$ by the graphs of Frobenius composed with the automorphisms $[\zeta_d^i]$ of $\mathcal{C}_d$.

Tracing through the geometry leads to remarkable explicit expressions for points in $E(K_d)$. The details of the calculation are presented in [Ulm09a, §8] so we will just state the results here, and only in the case $p > 2$.

Theorem 4.1. *Let $p > 2$, $k = \overline{\mathbb{F}}_p$ and $K = k(t)$. Let E be the elliptic curve*

$$y^2 + xy + ty = x^3 + tx^2$$

over K. Let $q = p^f$, $d = q + 1$, $K_d = k(t^{1/d})$, and

$$P(u) = \left(\frac{u^q(u^q - u)}{(1+4u)^q}, \frac{u^{2q}(1 + 2u + 2u^q)}{2(1+4u)^{(3q-1)/2}} - \frac{u^{2q}}{2(1+4u)^{q-1}} \right).$$

Then the points $P_i = P(\zeta_d^i t^{1/d})$ for $i = 0, \ldots, d-1$ lie in $E(K_d)$ and they generate a finite index subgroup of $E(K_d)$, which has rank $d-2$. The relations among them are that $\sum_{i=0}^{d-1} P_i$ and $\sum_{i=0}^{d-1} (-1)^i P_i$ are torsion.

It is elementary to check that the points lie in $E(K_d)$. To check their independence and the relations by elementary means, one may compute the height pairing on the lattice they generate. It turns out to be a scaling of the direct sum of two copies of the $A^*_{(d-2)/2}$ lattice. Since we know from the previous section that $E(K_d)$ has rank $d-2$, the explicit points generate a subgroup of finite index. As another check that they have finite index, we could compute the conductor of E—it turns out to have degree $d+2$—and apply Corollary 2.2.2 of Lecture 4. All this is explained in detail in [Ulm09a, §8].

5. Another example

We keep the notation and hypotheses of Sections 1 and 2. For another example, assume that $k = \overline{\mathbb{F}}_p$ with $p > 2$. Let $f(x) = x/(x^2-1)$ and $g(y) = y(y-1)$. The curve $f(x) - tg(y) = 0$ has genus 1 and the change of coordinates $x = (x'+t)/(x'-t)$, $y = -y'/2tx'$ brings it into the Weierstrass form

$$y'^2 + 2tx'y' = x'^3 - t^2x'.$$

This curve, call it E, has multiplicative reduction of type I_1 at the places dividing t^2+4, good reduction at other finite, non-zero places, and tame reduction at $t = 0$ and $t = \infty$. We find that the constants c_1 and c_2 are both zero and that

$$\operatorname{Rank} E(\overline{\mathbb{F}}_p(t^{1/d})) = \operatorname{Rank} \operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d}.$$

Recall that the curves $\mathcal{C}_d$ and $\mathcal{D}_d$ are defined by the equations

$$z^d = f(x) = \frac{x}{x^2-1} \quad \text{and} \quad w^d = g(y) = y(y-1).$$

Consider the morphism $\phi : \mathcal{C}_d \to \mathcal{D}_d$ defined by $\phi^*(y) = 1/(1-x^2)$ and $\phi^*(w) = z^2$. It is obviously not constant and so induces a surjective homomorphism $\phi_* : J_{\mathcal{C}_d} \to J_{\mathcal{D}_d}$.

The homomorphism ϕ_* clearly does not commute with the action of μ_d. Indeed, if ζ_d denotes a primitive d-th root of unity and $[\zeta_d]$ its action on one of the Jacobians, we have $\phi_* \circ [\zeta_d] = [\zeta_d^2] \circ \phi_*$. (This formula already holds at the level of the curves $\mathcal{C}_d$ and $\mathcal{D}_d$.)

Now let us assume that d has the form $d = 2p^f - 1$ and consider the map $\phi \circ \operatorname{Fr}_{p^f} : \mathcal{C}_d \to \mathcal{D}_d$. Then we find that

$$(\phi \circ \operatorname{Fr}_{p^f})_* \circ [\zeta_d] = [\zeta_d^{2p^f}] \circ (\phi \circ \operatorname{Fr}_{p^f})_* = [\zeta_d] \circ (\phi \circ \operatorname{Fr}_{p^f})_*$$

in $\operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})$, in other words that $(\phi \circ \operatorname{Fr}_{p^f})_*$ commutes with the μ_d action. Similarly $([\zeta_d^i] \circ \phi \circ \operatorname{Fr}_{p^f})_*$ commutes with the μ_d action for all i.

Further analysis of the homomorphisms $([\zeta_d^i] \circ \phi \circ \operatorname{Fr}_{p^f})_*$ in $\operatorname{Hom}(J_{\mathcal{C}_d}, J_{\mathcal{D}_d})^{\mu_d}$ (along the lines of [Ulm09a, 7.8]) shows that they are almost independent; more precisely, they generate a subgroup of rank $d-1$. Thus we find (for d of the form $d = 2p^f - 1$) that the rank of $E(k(t^{1/d}))$ is at least $d-1$.

The reader may find it a pleasant exercise to write down explicit points in this situation, along the lines of the discussion in Section 4 and [Ulm09a, §8].

6. Further developments

There have been further developments in the area of rational points on curves and Jacobians over function fields. To close, we mention three of them.

In the examples of Sections 3 and 5, the set of d that are "interesting," i.e., for which we get high rank over K_d, depends very much on p, the characteristic of k. In his thesis (University of Arizona, 2010), Tommy Occhipinti gives, for every p, remarkable examples of elliptic curves E over $\mathbb{F}_p(t)$ such that for *all* d prime to p we have

$$\operatorname{Rank} E(\overline{\mathbb{F}}_p(t^{1/d})) \geq d.$$

The curves come from Berger's construction where f and g are generic degree two rational functions. The rank inequality comes from the rank formula in Theorem 2.1 and the Honda-Tate theory of isogeny classes of abelian varieties over finite fields.

In the opposite direction, the author and Zarhin have given examples of curves of every genus over $\mathbb{C}(t)$ such that their Jacobians have bounded rank in the tower of fields $\mathbb{C}(t^{1/\ell^n})$ where ℓ is a prime. See [UZ10].

Finally, after some encouragement by Dick Gross at PCMI, the author produced explicit points on the Legendre curve over the fields $\mathbb{F}_p(\mu_d)(t^{1/d})$ where d has the form p^f+1 and proved in a completely elementary way that they give Mordell-Weil groups of unbounded rank. In fact, this construction is considerably easier than that of Tate and Shafarevich [TS67] and could have been found in the 1960s. See [Ulm09b].

It appears that this territory is rather fertile and that there is much still to be discovered about high ranks and explicit points on curves and Jacobians over function fields. Happy hunting!

Bibliography

[Art86] M. Artin, *Lipman's proof of resolution of singularities for surfaces*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 267–287. ↑237, 251

[ASD73] M. Artin and H. P. F. Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on K3 surfaces*, Invent. Math. **20** (1973), 249–266. ↑233, 259

[Băd01] L. Bădescu, *Algebraic surfaces*, Universitext, Springer-Verlag, New York, 2001. Translated from the 1981 Romanian original by Vladimir Maşek and revised by the author. ↑237, 251, 255

[BHPV04] W. P. Barth, K. Hulek, C. A. M. Peters, and A. Van de Ven, *Compact complex surfaces*, Second, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 4, Springer-Verlag, Berlin, 2004. ↑237

[Bea96] A. Beauville, *Complex algebraic surfaces*, Second, London Mathematical Society Student Texts, vol. 34, Cambridge University Press, Cambridge, 1996. Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid. ↑237, 240

[Ber08] L. Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*, J. Number Theory **128** (2008), 3013–3030. ↑234, 271, 273

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. ↑232

[Chi86] T. Chinburg, *Minimal models for curves over Dedekind rings*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 309–326. ↑249

[Con05] B. Conrad, *Minimal models for elliptic curves* (2005). Preprint. ↑251

[Con06] B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*, Enseign. Math. (2) **52** (2006), 37–108. ↑227, 239

[Del75] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 53–73. Lecture Notes in Math., Vol. 476. ↑223

[Del80] P. Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. ↑266

[Deu40] M. Deuring, *Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper. II*, J. Reine Angew. Math. **183** (1940), 25–36. ↑221

[Elk94] N. D. Elkies, *Mordell-Weil lattices in characteristic* 2. *I. Construction and first properties*, Internat. Math. Res. Notices (1994), 343 ff., approx. 18 pp. (electronic). ↑228

[Fal86] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **7**3 (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. ↑225

[Ful84] W. Fulton, *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 2, Springer-Verlag, Berlin, 1984. ↑238

[Gol03] D. M. Goldschmidt, *Algebraic functions and projective curves*, Graduate Texts in Mathematics, vol. 215, Springer-Verlag, New York, 2003. ↑218

[Gor79] W. J. Gordon, *Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer*, Compositio Math. **38** (1979), 163–199. ↑257

[Gro10] B. Gross, *Lectures on the conjecture of Birch and Swinnerton-Dyer* (2010). Notes from a course at the 2009 Park City Mathematics Institute. ↑232, 233

[Gro68] A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, 1968, pp. 88–188. ↑245, 258

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. ↑223, 238, 240, 241, 242

[Igu55] J-I. Igusa, *On some problems in abstract algebraic geometry*, Proc. Nat. Acad. Sci. U. S. A. **41** (1955), 964–967. ↑239

[Igu59] J-I. Igusa, *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959), 453–476. ↑267

[Igu68] J-I. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan **20** (1968), 96–106. ↑229

[Kat01] N. M. Katz, *L-functions and monodromy: four lectures on Weil II*, Adv. Math. **160** (2001), 81–132. ↑266

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. ↑226, 229, 230

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. ↑263

[Kle05] S. L. Kleiman, *The Picard scheme*, Fundamental algebraic geometry, 2005, pp. 235–321. ↑239

[LN59] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81** (1959), 95–118. ↑227, 239

[Lau84] G. Laumon, *Les constantes des équations fonctionnelles des fonctions L sur un corps global de caractéristique positive*, C. R. Acad. Sci. Paris Sér. I Math. **298** (1984), 181–184. ↑267

[Lev68] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462. ↑229

[Lic68] S. Lichtenbaum, *Curves over discrete valuation rings*, Amer. J. Math. **90** (1968), 380–405. ↑249

[Lip78] J. Lipman, *Desingularization of two-dimensional schemes*, Ann. Math. (2) **107** (1978), 151–207. ↑237

[Liu02] Q. 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. ↑223, 237, 249

[Mat57] T. Matsusaka, *The criteria for algebraic equivalence and the torsion group*, Amer. J. Math. **79** (1957), 53–66. ↑241

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449. ↑229

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), 517–533. ↑233, 244, 245, 246

[Mil80] J. S. Milne, *Etale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. ↑219, 227, 245, 264, 265, 266

[Mil86a] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 103–150. ↑220, 221, 228

[Mil86b] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212. ↑219, 220, 221

[Miy06] T. Miyake, *Modular forms*, English, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda. ↑229

[Mum66] D. Mumford, *Lectures on curves on an algebraic surface*, With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59, Princeton University Press, Princeton, N.J., 1966. ↑239

[Mum08] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. ↑220, 241

[Ogg67] A. P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), 1–21. ↑267

[Poo07] B. Poonen, *Gonality of modular curves in characteristic p*, Math. Res. Lett. **14** (2007), 691–701. ↑229

[Roq06] P. Roquette, *The Riemann hypothesis in characteristic p, its origin and development. III. The elliptic case*, Mitt. Math. Ges. Hamburg **25** (2006), 103–176. ↑215, 219, 221

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. ↑218

[Sch96] C. Schoen, *Varieties dominated by product varieties*, Internat. J. Math. **7** (1996), 541–571. ↑248, 261

[SS09] M. Schütt and T. Shioda, *Elliptic surfaces* (2009). Preprint. ↑241, 256

[SGA4$\frac{1}{2}$] *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. ↑219, 240

[SGA5] *Cohomologie l-adique et fonctions L*, Lecture Notes in Mathematics, Vol. 589, Springer-Verlag, Berlin, 1977. Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie. ↑219

[SGA6] *Théorie des intersections et théorème de Riemann-Roch*, Lecture Notes in Mathematics, Vol. 225, Springer-Verlag, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6), Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre. ↑227, 239

[Ser58] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium internacional de topología algebraica International symposium on algebraic topology, 1958, pp. 24–53. ↑239

[Ser77] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. ↑264

[Ser88] J.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. Translated from the French. ↑221

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. ↑266

[Shi86] T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), 415–432. ↑234

[Shi99] T. Shioda, *Mordell-Weil lattices for higher genus fibration over a curve*, New trends in algebraic geometry (Warwick, 1996), 1999, pp. 359–373. ↑255

[SK79] T. Shioda and T. Katsura, *On Fermat varieties*, Tôhoku Math. J. (2) **31** (1979), 97–115. ↑260

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑242, 251, 253, 254

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. ↑223, 225, 226, 228, 231, 254

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, Second edition, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. ↑218

[Szy04] M. Szydlo, *Elliptic fibers over non-perfect residue fields*, J. Number Theory **104** (2004), 75–99. ↑252

[Tat66a] J. T. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. ↑221

[Tat66b] J. T. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire bourbaki, vol. 9, 1966, pp. Exp. No. 306, 415–440. ↑233, 244, 245, 255

[Tat75] J. T. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, iv (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. ↑231, 251, 254

[Tat94] J. T. Tate, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991), 1994, pp. 71–83. ↑244, 246

[TS67] J. T. Tate and I. R. Shafarevich, *The rank of elliptic curves*, Soviet Math. Dokl. **8** (1967), 917–920. ↑228, 278

[Ulm91] D. Ulmer, *p-descent in characteristic p*, Duke Math. J. **62** (1991), 237–265. ↑227, 229

[Ulm05] D. Ulmer, *Geometric non-vanishing*, Invent. Math. **159** (2005), 133–186. ↑266, 268

[Ulm07] D. Ulmer, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), 379–408. ↑260, 268, 270, 271

[Ulm09a] D. Ulmer, *On Mordell-Weil groups of Jacobians over function fields* (2009). Preprint. ↑261, 275, 276, 277

[Ulm09b] D. Ulmer, *Explicit points on the Legendre curve* (2009). Preprint. ↑278

[Ulm11] D. Ulmer, *Curves and Jacobians over function fields* (2011). Notes from a course at the CRM, Barcelona. In preparation. ↑215, 226, 232, 233, 246, 255, 258, 260

[UZ10] D. Ulmer and Y. G. Zarhin, *Ranks of Jacobians in towers of function fields*, Math. Res. Lett. **17** (2010), 637–645. ↑278

[Wei49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. ↑219

[Zar08] Y. G. Zarhin, *Homomorphisms of abelian varieties over finite fields*, Higher-dimensional geometry over finite fields, 2008, pp. 315–343. ↑221