Arithmetic of curves

Daniel Miller and David Zywina

Fall 2013

Contents

1 Introduction

1.1 Disclaimer

These notes originated in a course "Topics in algebra: the arithmetic of curves" taught by David Zywina at Cornell University. However, a significant amount of material (including, no doubt, many errors) has been added since then, so they are far from an exact reflection of what he covered in class. Moreover, the

notation has been changed in many places (sometimes significantly) as has the order in which material is covered. Most significantly, the tone of these notes differs drastically from the perspective Zywina took in class, with the notes being much more cohomological and scheme-theoretic than Zywina's generally elementary (and pedagogically correct) approach. Any errors in these notes are entirely the fault of the former author.

The original computations were done using the commercial computer algebra system Magma. For these notes, everything has been reworked into Sage, an open-source alternative designed for for number theorists. Nearly all of the Sage code used is contained (using the LaTeX package `sagetex`) in the source code for this document, which may be found at https://github.com/dkmiller/arith-curve.

1.2 Notation and conventions

Following Bourbaki, we write $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}\ldots$ for the natural numbers, integers, rationals.... In this work, $0 \notin \mathbf{N}$.

Following Poonen, a *nice variety* over a field k is a smooth, projective, geometrically integral variety over k.

If k is a field, k^s (resp. $\bar{k}$) denotes its separable (resp. algebraic) closure. We will write $G_k = \mathrm{Gal}(k^s/k)$ for the *absolute Galois group* of k.

Let X be a scheme over a finite field $\mathbf{F}_q$. The *Frobenius of* X is the morphism $\mathrm{Fr}_X = \mathrm{Fr}_{X,q} : X \to X$ that is the identity on the underlying topological space, and $x \mapsto x^q$ on the structure sheaf. The Frobenius in $G_{\mathbf{F}_q} = \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$ is the *arithmetic* Frobenius, given by $x \mapsto x^q$ on $\overline{\mathbf{F}_q}$. We will write fr_q for the arithmetic Frobenius.

If v is a finite place of a global field k, then k_v denotes the completion of k with respect to v. Most of our notation here is standard, with the possible exception of $\kappa_v = \mathfrak{o}_v/\mathfrak{p}_v$ for the residue field of v.

If k is a global field and v is a finite place of k, fr_v denotes the arithmetic Frobenius associated to v. We will sometimes take fr_v to be a single (non-canonical) element of G_k, or the elements' entire conjugacy class. This should not cause any confusion.

If E is a module over a ring A and $x \in E$, then we will write E/x instead of $E/(A \cdot x)$. In particular, for $a \in A$, A/a is the quotient of A by the ideal generated by A.

All abelian groups are tacitly taken to modules over $\mathbf{Z}$, so the previous convention applies. Even if an abelian group G is written multiplicatively, G/n will be used to denote $G/(G^n)$. We write ${}_nG$ for the group $\{g \in G : n \cdot G = 0\}$.

The end of an example is marked by a triangle $\triangleright$. Following Bourbaki, we mark sections and paragraphs covering especially advanced material with a

star $\star$.

1.3 Motivation: plane curves

Fir a non-constant polynomial $f(x, y) \in \mathbf{Q}[x, y]$. Assume f is geometrically irreducible, that is, irreducible as an element of the ring $\overline{\mathbf{Q}}[x, y]$. We can define the curve C over $\mathbf{Q}$ determined by the equation $f(x, y) = 0$. For now, we will think of C in terms of its functor of points. To any $\mathbf{Q}$-algebra A, we set $C(A) = \{(a, b) \in A^2 : f(a, b) = 0\}$. As a scheme, $C = \operatorname{Spec}(\mathbf{Q}[x, y]/f)$. Some big questions are:

1. Is $C(\mathbf{Q}) = \varnothing$?
2. Is $C(\mathbf{Q})$ finite?
3. Can we compute $C(\mathbf{Q})$?

At the present, we have no way of answering any of these questions algorithmically for general curves.

Example 1.3.1. Let $f = x^2 + y^2 - 1$, i.e. C is the circle. It is well-known that

$$C(\mathbf{Q}) = \left\{ \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) : t \in \mathbf{Q} \right\} \cup \{(-1, 0)\}.$$

This can be proved in the usual manner by choosing the point $(-1, 0)$ in C, and then drawing lines with rational slopes through $(-1, 0)$. As a Riemann surface, $C(\mathbf{C})$ is a sphere with two points removed. ▷

Example 1.3.2. Let $f = x^2 + y^2 + 1$. Then $C(\mathbf{R}) = \varnothing$, hence $C(\mathbf{Q}) = \varnothing$. But as a Riemann surface, $C(\mathbf{C})$ is the same sphere with two points removed. Thus the geometry of C does not necessarily determine $C(\mathbf{Q})$. ▷

Example 1.3.3. Let $f = x^4 + y^4 - 1$. Then it is a theorem of Fermat that $C(\mathbf{Q}) = \{(\pm 1, 0), (0, \pm 1)\}$. It is a (much harder) theorem of Wiles that if C_n is the curve given by $f = x^n + y^n - 1$ for $n \geqslant 3$, then $C_n(\mathbf{Q}) = \{(\pm 1, 0), (0, \pm 1)\}$. In fact, this is the celebrated "Fermat's Last Theorem," proved in [Wil95]. ▷

Example 1.3.4 (Stoll)**.** Consider

$$C : y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

This is a curve of genus 2, i.e. $C(\mathbf{C})$ is a punctured two-holed torus. It turns out that $\#C(\mathbf{Q}) \geqslant 642$ [Sto09, §6]. However, by a theorem of Faltings, $\#C(\mathbf{Q})$ is finite. This example exhibits the largest known number of rational points of a genus two curve over $\mathbf{Q}$. If we take $C : y^2 = f(x)$ with $f \in \mathbf{Q}[x]$ a "random" sextic polynomial, then the expectation is that $C(\mathbf{Q}) = \varnothing$. ▷

It is natural to ask whether for each $g \geqslant 2$ there exists a number B_g such that whenever a curve C over $\mathbf{Q}$ has genus g, we have $\#C(\mathbf{Q}) \leqslant B_g$. This is not even known for $g = 2$.

Example 1.3.5. Let $C : y^2 = x^3 + 875x$. Note that $C(\mathbf{Q})$ has the obvious point $(0, 0)$, and one can do a bit of work to show that this is the only point. ▷

Example 1.3.6. Let $C : y^2 = x^3 + 877x$. Then $C(\mathbf{Q})$ once again contains $(0, 0)$. A computer search showed that $(0, 0)$ is the only point on C of height $\leqslant 1000000$. For now, the *height* of a solution is just the largest absolute value of the numerator / denominator of a solution written in reduced fractions. But other methods lead us to expect many more solutions (infinitely many, in fact). Let E be the projective curve over $\mathbf{Q}$ obtained by adjoining a point O to C. As a Riemann surface, $E(\mathbf{C})$ is just a torus.

We can give E the structure of an *abelian variety* over $\mathbf{Q}$. That is, we can give E the structure of a commutative algebraic group (the multiplication operation $m : E \times E \to E$ is given by regular functions), with O being the identity. Later, we will think of E as being identified with its jacobian $\mathrm{Jac}(E)$ via the choice of a single point $O \in E(\mathbf{Q})$. Since E is a commutative algebraic group, $E(\mathbf{Q})$ is an abelian group (with identity O). It is a theorem of Mordell that $E(\mathbf{Q})$ is finitely generated. We know the structure of such groups: $E(\mathbf{Q}) \simeq A \times \mathbf{Z}^r$, where A is finite, and $r = \operatorname{rk} E$ is the *(algebraic) rank* of E.

In general, the group A is (conjecturally) computable. In our case, $A = \mathbf{Z}/2$. It is much harder to compute the algebraic rank of E. The Birch and Swinnerton-Dyer conjecture says that r agrees with the order of vanishing r' of a certain holomorphic function $L(E, s)$ at $s = 1$. Sometimes, r' can be computed. In our example, a computation shows that $r' = 1$, so we should expect $E(\mathbf{Q}) \simeq \mathbf{Z}/2 \times \mathbf{Z}$. In particular, $E(\mathbf{Q})$ should be infinite. One can show (using other methods) that $E(\mathbf{Q}) = \langle (0, 0), (x_0, y_0) \rangle$, where

$$x_0 = \frac{37549452812716219310550406994209279234620 1}{62159877768715054254632207806972380441 00}.$$

For details, see [BC84]. One method to construct such large solutions for a rank one elliptic curve uses Heegner points. ▷

In general, we will take a curve C over $\mathbf{Q}$, consider its jacobian J, and study $J(\mathbf{Q})$. This will be a group, and its structure heavily influences $C(\mathbf{Q})$. For example, we could study how the rank of $J(\mathbf{Q})$ affects $C(\mathbf{Q})$. In the case that $C = E$ is an elliptic curve, $\mathrm{Jac}(E) = E$, so studying the curve and studying its jacobian is the same thing. The "average rank of an elliptic curve" is not known, nor is there a general consensus on what is should be. Some expect the rank of a random curve to be 0 or 1, both with probability $\frac{1}{2}$. Others suppose

that elliptic curves over $\mathbf{Q}$ have rank 2 with nonzero probability as well. It was proven recently (see [BS10a, §1]) that

$$\limsup_{X\to\infty} \frac{1}{4X^2} \sum_{\substack{|a|,|b|\leqslant X \\ 4a^3+27b^2\neq 0}} \mathrm{rk}(E_{a,b}) \leqslant \frac{7}{6},$$

where $E_{a,b}$ is the elliptic curve over $\mathbf{Q}$ defined by $y^2 = x^3 + ax + b$.

It is natural to ask whether there is a global bound for $\mathrm{rk}\, E(\mathbf{Q})$ as E ranges over all elliptic curves over $\mathbf{Q}$. It is known that there are curves with rank at least 28, but their exact ranks are not known [Duj]. The largest known rank is 19.

Our assumption that $f(x, y)$ is irreducible is not a serious one. For example, if $f = y^2 - x^2$, then we can factor f as $(x + y)(x - y)$, and then treat the solutions to $x+y = 0$ and $x-y = 0$ separately. Another example is $f = x^2+y^2$, which only factors over $\mathbf{Q}(i)$ as $(y + ix)(y - ix)$. We know that the rational points lie in the intersection of the two components over $\mathbf{Q}(i)$. In general, a curve over $\mathbf{Q}$ will be the union of finitely many geometrically irreducible components, each of which is defined over some finite extension of $\mathbf{Q}$. Also, the assumption that $f \in \mathbf{Q}[x, y]$ is not serious, as every curve is birational to a plane curve.

Let C be a curve over $\mathbf{Q}$. Then $C(\mathbf{C}) \smallsetminus \{\text{singular points}\}$ is a compact Riemann surface with points removed, i.e. it is a torus with g handles with finitely many points removed. Call this g the *genus* of C. The following result was originally known as the *Mordell Conjecture*.

Theorem 1.3.7 (Faltings)**.** *If C is a curve over $\mathbf{Q}$ with $g \geqslant 2$, then $C(\mathbf{Q})$ is finite.*

For curves of genus $g < 2$, $\#C(\mathbf{Q})$ can be infinite. In Faltings' theorem, $\mathbf{Q}$ can be replaced by any field finitely generated over $\mathbf{Q}$.

Now let C be a smooth projective curve of genus g over $\mathbf{F}_p$. We are interested in $\#C(\mathbf{F}_{p^n})$, which is obviously computable for each n. Define the *zeta function* of C to be the formal power series

$$Z(C, t) = \exp\left(\sum_{n\geqslant 1} \#C(\mathbf{F}_{p^n}) \frac{t^n}{n}\right).$$

Theorem 1.3.8 (Weil)**.** *If C is a smooth projective curve of genus g over $\mathbf{F}_p$, then*

$$Z(C, t) = \frac{P(C, t)}{(1 - t)(1 - pt)},$$

where $P(C, t) \in \mathbf{Z}[t]$ has degree $2g$. Moreover, if we write $P(C, t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, then for each i, we have $|\alpha_i| = p^{1/2}$.

The second statement in the theorem is called the *Riemann hypothesis* for C. It can be used to obtain explicit bounds on the size of $C(\mathbf{F}_{p^n})$ as $n \to \infty$. For example, we can compute

$$\begin{aligned}\sum_{n>0} \#C(\mathbf{F}_{p^n})\frac{t^n}{n} &= \log Z(C,t)\\ &= -\log(1-t) - \log(1-pt) + \sum_i \log(1-\alpha_t t)\\ &= \sum_{n>0}\left(p^n + 1 - \sum_{i=1}^{2g}\alpha_i^n\right)\frac{t^n}{n}.\end{aligned}$$

Therefore, $\#C(\mathbf{F}_{p^n}) = p^n + 1 - \sum_{i=1}^{2g}\alpha_i^n$. It follows easily that $|\#C(\mathbf{F}_{p^n}) - (p^n+1)| \leqslant 2gp^{n/2}$. This is equivalent to the bound

$$p^n - 2gp^{n/2} + 1 \leqslant \#C(\mathbf{F}_{p^n}) \leqslant p^n + 2gp^{n/2} + 1.$$

In particular, setting $n = g = 1$, we obtain $\#C(\mathbf{F}_p) \geqslant (p^{1/2}-1)^2 > 0$, hence $C(\mathbf{F}_p) \neq \varnothing$.

2 Jacobians and abelian varieties

At first, we will work over $\mathbf{C}$ and treat curves as Riemann surfaces. By [Har77, I.6.12] and [Jos06, 5.8.7], the category of smooth projective curves over $\mathbf{C}$ is equivalent to the category of compact connected Riemann surfaces, so we are not losing any information here. Let's start with some general definitions.

Definition 2.0.1. *A* variety *over a field k is a separated scheme of finite type over* $\operatorname{Spec}(k)$*. We call a variety X over k* nice *if it is smooth, projective, and geometrically integral.*

Recall that a k-scheme X is *geometrically integral* if $X_{\bar{k}} = X \times_k \operatorname{Spec}(\bar{k})$ is integral. A *curve* is a variety of dimension one. If we are interested in $C(k)$ for general curves, it is sufficient to consider nice curves. If X is a variety, we can consider its functor of points $h_X : \mathsf{Alg}_k \to \mathsf{Set}$ which assigns to a k-algebra A the set $X(A)$ of "A-valued points." This extends to a functor $h_X : \mathsf{Sch}_k^\circ \to \mathsf{Set}$ which is defined by $h_X(Y) = \hom_k(Y, X)$.

Earlier, for $f \in \mathbf{Q}[x,y]$ and C defined by the equation $f = 0$, we defined $C(A) = \{(a,b) \in A^2 : f(a,b) = 0\}$ for any $\mathbf{Q}$-algebra A. Note that

$$\begin{aligned}C(A) &= \{(a,b) \in A^2 : f(a,b) = 0\}\\ &= \hom_{\mathsf{Alg}_{\mathbf{Q}}}(\mathbf{Q}[x,y]/f, A)\\ &= \hom_{\mathsf{Sch}_k}\left(\operatorname{Spec} A, \operatorname{Spec}(\mathbf{Q}[x,y]/f)\right),\end{aligned}$$

so this agrees with our general definition. By the Yoneda Lemma, the functor h_X determines X up to unique isomorphism.

2.1 Jacobians over C

For the rest of this section, let C be a nice curve over $\mathbf{C}$. Set $X = C(\mathbf{C})$; this is a compact connected Riemann surface. So topologically, X is a many-handled torus. Let $\Lambda = \mathrm{H}_1(X, \mathbf{Z})$, the first singular homology group of X, which can be identified with $\pi_1(X)^{\mathrm{ab}}$. We will regard elements of Λ as equivalence classes $[\gamma]$ for $\gamma \in \pi_1(X)$.

It is a theorem of algebraic topology that $\Lambda \simeq \mathbf{Z}^{2g}$ for some $g \geqslant 0$; we will call g the *genus* of X (and also of C). Let K be the field of *meromorphic* functions on X, i.e. functions which are locally quotients of nonzero holomorphic functions. For $f \in K$, at any point $x \in X$, we can write f in local coordinates as $z^n(a_0 + a_1 z + \cdots)$ where $a_0 \neq 0$ and $n \in \mathbf{Z}$. We call $n = \mathrm{ord}_x(f)$ the *order of vanishing* of f at x. The *degree* of f is the sum $\deg(f) = \sum_{x \in X} \mathrm{ord}_x(f)$. If f is holomorphic instead of just meromorphic, then $\deg(f) = 0$ because f is constant, but the converse fails.

We can identify K with the function field of C, i.e. the set of rational maps $C \to \mathbf{A}^1$. Certainly rational maps yield meromorphic functions, and it is a basic theorem of Riemann surface theory that meromorphic functions are in fact algebraic. Moreover, if C is nice, then C can be recovered from K. To do this, pick some $x \in K \smallsetminus \mathbf{C}$. If we let A be the integral closure of $\mathbf{C}[x]$ in K, then $\mathrm{Spec}(A)$ will be a smooth affine curve. Pick some embedding of $\mathrm{Spec}(A)$ into projective space; the closure of its image will be a projective curve C' (possibly with singularities) with function field K. We can resolve the singularities of C' to obtain a smooth projective curve C'' with function field K. By [Har77, I.6.12], this induces an anti-equivalence between the category of extensions $K/\mathbf{C}$ of transcendence degree one and the category of nice curves over $\mathbf{C}$ with surjective morphisms.

One might ask whether the singular homology $\mathrm{H}_1(X, \mathbf{Z})$ can be defined "algebraically." Essentially, the answer is no – that is, there is no known algebraic definition for $\mathrm{H}_1(X, \mathbf{Z})$ that gives the "right" answers. On the other hand, $\mathrm{H}_1(X, \mathbf{Q})$ is naturally isomorphic to the dual of the algebraic de Rham cohomology $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q})$, and $\mathrm{H}_1(X, \mathbf{Z}_\ell)$ is naturally isomorphic to the dual of the ℓ-adic cohomology $\mathrm{H}^1_{\mathrm{et}}(X, \mathbf{Z}_\ell)$. Both of these isomorphisms are hard theorems – the first due to Grothendieck [Gro66], the second originally due to Artin, and proved in [Del77, I 4.6.3].

With C as before, let $V = \Omega^1(X) = \mathrm{H}^0(X, \Omega^1) = \mathrm{H}^1_{\mathrm{dR}}(X)$ be the first analytic de Rham cohomology of C. This is a complex vector space of dimension g, so we get a non-topological definition of g. We can consider Ω^1 as the sheaf of

(algebraic) differentials, and $g = \dim_{\mathbf{C}} \mathrm{H}^0(X, \Omega^1)$, giving us a purely algebraic definition of g. There is a natural pairing $\mathrm{H}_1(X, \mathbf{Z}) \otimes \mathrm{H}^1_{\mathrm{dR}}(X) \to \mathbf{C}$, defined by

$$[\gamma] \otimes \omega \mapsto \int_\gamma \omega.$$

This pairing is nondegenerate, and $\mathbf{C}$-linear in the second component. It induces an injection $\Phi : \Lambda \hookrightarrow V^\vee$.

Definition 2.1.1 (analytic)**.** *The* Jacobian *of* X *is* $\mathrm{Jac}(X) = V^\vee/\Phi(\Lambda)$.

Is is known that $\Phi(\Lambda)$ is a *lattice* in $V^\vee$, i.e. it is discrete and $V^\vee/\Phi(\Lambda)$ is compact. There is the *Abel-Jacobi map* $j : X \to \mathrm{Jac}(X)$ defined as follows. Fix $x_0 \in X$; we send $x \in X$ to $\omega \mapsto \int_{[x_0,x]} \omega$, where $[x_0, x]$ denotes any path from x_0 to x. A different choice of $[x_0, x]$ will differ by a closed loop, i.e. an element of $\mathrm{H}_1(X, \mathbf{Z})$. So $j : X \to \mathrm{Jac}(X)$ is well-defined. Note that $\mathrm{Jac}(X)$ is a compact complex Lie group.

After choosing a basis for $V^\vee$, we have $\mathrm{Jac}(X) \simeq \mathbf{C}^g/L$, where $L \simeq \mathbf{Z}^{2g}$. As a real Lie group, $\mathrm{Jac}\, X$ is isomorphic to $(S^1)^{2g}$. We care about $\mathrm{Jac}(X)$ because, despite its analytic definition, it is in fact a projective variety.

Theorem 2.1.2. *For* X *a compact Riemann surface,* $\mathrm{Jac}(X)$ *is algebraic, i.e. there exists a variety* J *defined over* $\mathbf{C}$ *such that* $J(\mathbf{C}) \simeq \mathrm{Jac}(X)$ *as complex manifolds. Moreover, the group operation on* $\mathrm{Jac}(X)$ *is algebraic, i.e. there is a morphism* $m : J \times_{\mathbf{C}} J \to J$ *such that* $J(\mathbf{C}) \times J(\mathbf{C}) \to J(\mathbf{C})$ *corresponds to the addition law on* $\mathrm{Jac}(X)$.

Proof. See [Mila, I.18]. Essentially, X is the analytification of a curve C, and one proves that $\mathrm{Jac}(X)$ (defined analytically) is isomorphic as a complex manifold to the analytification of $\mathrm{Jac}(C)$ (defined algebraically). □

Let $\mathrm{Div}(X)$ be the free abelian group generated by the points of X. There is a map $\deg : \mathrm{Div}(X) \to \mathbf{Z}$, defined by $\sum n_x \cdot x \mapsto \sum n_x$. We define $\mathrm{Div}^\circ(X)$ by the short exact sequence

$$0 \longrightarrow \mathrm{Div}^\circ(X) \longrightarrow \mathrm{Div}(X) \longrightarrow \mathbf{Z} \longrightarrow 0.$$

There is also a map $\mathrm{div} : K^\times \to \mathrm{Div}(X)$, where $\mathrm{div}(f) = \sum_x \mathrm{ord}_x(f) \cdot x$. It is a basic fact that $\deg(\mathrm{div}(f)) = 0$, so we can define the *Picard group* of X to be $\mathrm{Pic}(X) = \mathrm{Div}\, X/\,\mathrm{div}(K^\times)$ and $\mathrm{Pic}^\circ(X) = \mathrm{Div}^\circ(X)/\,\mathrm{div}(K^\times)$.

Let $\mathscr{M}$ be the sheaf of meromorphic functions on X. It is not hard to show that $\mathrm{Div}(X) = \mathrm{H}^0(X, \mathscr{M}^\times/\mathscr{O}^\times)$ and $\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathscr{O}^\times)$. Indeed, the first equality is often taken to be a definition as in [Har77, III.6], and the second is

a straightforward exercise in Čech cohomology. An example where the Picard group is easily determined is $\mathrm{Pic}^\circ(\mathbf{P}^1) = 0$.

The Abel-Jacobi map $j : X \to \mathrm{Jac}\, X$ extends naturally to a homomorphism $j : \mathrm{Div}^\circ(X) \to \mathrm{Jac}(X)$.

Theorem 2.1.3 (Jacobi)**.** *The map $j : \mathrm{Div}^\circ(X) \to \mathrm{Jac}(X)$ is surjective.*

Theorem 2.1.4 (Abel)**.** *The kernel of $j : \mathrm{Div}^\circ(X) \to \mathrm{Jac}(X)$ is $\mathrm{div}(K^\times)$.*

It follows that j induces an isomorphism $j : \mathrm{Pic}^\circ(X) \xrightarrow{\sim} \mathrm{Jac}(X)$. Note that $\mathrm{Pic}^\circ(X)$ parameterizes invertible sheaves (line bundles) on X of degree zero.

Note that in general, $\mathbf{C}^g/L$ for some lattice L need not be algebraic if $g > 1$. In the future, we'll try to define $\mathrm{Jac}(C)$ for a curve C over any field. The variety $\mathrm{Jac}(C)$ will be a nice variety, i.e. smooth, projective and geometrically integral. We will use this to give an "algebraic definition of $\mathrm{H}_1(X, \mathbf{Z}/n)$."

2.2 Abelian varieties over arbitrary fields

Recall that a variety X/k is *nice* if it is smooth, projective, and geometrically integral.

Definition 2.2.1. *Let k be a field. An* abelian variety *over k is a nice group variety over k.*

In other words, there are morphisms $m : A \times A \to A$, $i : A \to A$, $e : \mathrm{Spec}(k) \to A$ such that the induced maps $m_* : h_A \times h_A \to h_A$ etc. turn h_A into a group-valued functor. In particular, $A(X)$ is an "honest group" for each k-scheme X.

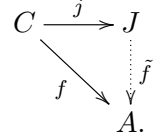
Example 2.2.2. The general linear group $\mathrm{GL}(n)$ is a group variety, but not nice (at least, not in the technical sense) because it is not projective. More generally, no linear algebraic group is an abelian variety, for the same reason. ▷

Note that abelian varieties are not required to be commutative, but this is in fact the case. This is easy to see over $\mathbf{C}$. If A is an abelian variety over $\mathbf{C}$, then $G = A(\mathbf{C})$ is a compact connected complex Lie group. Let $\mathfrak{g}$ be its Lie algebra, and consider the composite map $f : G \xrightarrow{\mathrm{ad}} \mathrm{GL}(\mathfrak{g}) \hookrightarrow \mathrm{End}(\mathfrak{g})$, where $\mathrm{ad} : G \to \mathrm{GL}(\mathfrak{g})$ is the adjoint representation. After picking a basis for $\mathrm{End}(\mathfrak{g})$, the components of f are entire holomorphic functions on a compact complex manifold, hence locally constant. Since G is connected, f is constant, i.e. the adjoint representation of G is trivial. But $\ker(\mathrm{ad}) = Z(G)$, so G is commutative. The case A/k for arbitrary k of characteristic zero follows from the Lefschetz principle, or one can just prove commutativity directly using a "rigidity principle" for maps on projective varieties [Mila, I.1.4].

2.3 Albanese varieties

We'd like to describe the jacobian J of a nice curve C over k with $C(k) \neq \varnothing$. It will be an abelian variety over k of dimension g, the genus of C. So far we've only defined the genus of a curve C/k with $k \subset \mathbf{C}$. For an arbitrary field k and a curve C/k, set $g(C) = h^0(C_{\bar{k}}, \Omega^1) = h^1(\mathscr{O}_C)$. In general, if $\mathscr{F}$ is some sheaf on a scheme X over k, we write $h^i(X, \mathscr{F})$ or $h^i(\mathscr{F})$ for $\dim_k \mathrm{H}^i(X, \mathscr{F})$.

Definition 2.3.1 (Albanese)**.** *Let C/k be a curve with fixed $x_0 \in C(k)$. The* jacobian *of C is an abelian variety $J = \mathrm{Jac}(C)$ with a morphism $j : C \to J$ taking x_0 to 0, such that for any morphism $f : C \to A$ to an abelian variety A with $f(x_0) = 0$, there is a unique $\tilde{f} : J \to A$ making the following diagram commute:*



Since (J, j) is the solution of a universal problem, it is unique up to unique isomorphism. Our definition can be made much more concise. Let AbV_k be the category of abelian varieties over k, and let $\mathsf{Var}_{k,*}$ be the category of "nice pointed varieties" over k, i.e. nice varieties X/k with chosen $x \in X(k)$. Forgetting the group structure gives an inclusion functor $\iota : \mathsf{AbV}_k \to \mathsf{Var}_{k,*}$. Our definition of $\mathrm{Jac}(C)$ can be rephrased as saying that $j : C \to \mathrm{Jac}(C)$ induces a natural isomorphism

$$\hom_{\mathsf{Var}_{k,*}}(C, \iota A) \simeq \hom_{\mathsf{AbVar}_k}(\mathrm{Jac}\, C, A).$$

It turns out that for any nice pointed variety X, there is an abelian variety $A = \mathrm{Alb}(X)$, the *Albanese variety* of X, with a morphism $j : X \to \mathrm{Alb}(X)$ that induces a similar natural isomorphism (with $\mathrm{Alb}(X)$ in place of $\mathrm{Jac}\, C$). So taking jacobian may be seen as the left-adjoint to the forgetful functor from abelian varieties to pointed varieties. For a proof that $\mathrm{Alb}(X)$ exists, see [Moc12, A.11].

In general, the map $X \to \mathrm{Alb}(X)$ need not be an embedding. For example, if C is a curve of genus 0, then $\mathrm{Alb}(X) = 0$ by [Mila, I.3.9]. On the other hand, if the genus $g \geqslant 1$, then $C \to J$ is an embedding. The map $C(\bar{k}) \to \mathrm{Pic}^\circ(C_{\bar{k}})$ sends a point x to the divisor $[x] - [x_0]$. If $[x] - [x_0] = [y] - [x_0]$ in $\mathrm{Pic}^\circ(C_{\bar{k}})$, then $[x] - [y] = \mathrm{div}(f)$ for some rational map $f : C \to \mathbf{P}^1$. If $x \neq y$, then f would have a unique simple zero and poll, which would imply that f is birational. But this is impossible, so $x \neq y$ implies $j(x) \neq j(y)$.

If $C(k) = \varnothing$, we can still define $J = \mathrm{Jac}(C)$. It will be a k-variety with a morphism $j : C \times C \to J$ such that $j(\Delta) = 0$. We require that for any abelian

variety A over k with $f : C \times C \to A$ such that $f(\Delta) = 0$, there is a unique lift $\tilde{f} : J \to A$ of f. The map j should be thought of "$(x, y) \mapsto j(x) - j(y)$," even though an embedding $C \to J$ may not be defined over k.

2.4 Picard schemes

Another approach to defining $J = \mathrm{Jac}(C)$ involves the Picard group. Recall that over $\mathbf{C}$, we proved that $J(\mathbf{C}) \simeq \mathrm{Pic}^\circ(C)$. One might hope that J satisfies $J(L) = \mathrm{Pic}^\circ(C_L)$ for all field extensions L/k. This works if $C(k) \neq \varnothing$, but not otherwise. For, if $J(k^s) = \mathrm{Pic}^\circ(C_{k^s})$, then we would have $\mathrm{Pic}^\circ(C) = J(k) = J(k^s)^{G_k} = \mathrm{Pic}^\circ(C_{k^s})^{G_k}$. But this does not always hold.

For a curve C over k, we will define an abelian variety $\mathrm{Pic}^\circ(C)$ in terms of its functor of points. To do this, we need to define Picard groups for arbitrary schemes. For any scheme X, the *Picard group* of X is $\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathscr{O}_X^\times)$. It is straightforward to show (using Čech cohomology) that $\mathrm{Pic}(X)$ is isomorphic to the group of isomorphism classes of invertible sheaves on X, with group operation induced by tensor product: $[\mathscr{L}] + [\mathscr{L}'] = [\mathscr{L} \otimes \mathscr{L}']$.

Let C be a nice curve. If $D = \sum D_x \cdot x$ is a divisor on C, the *degree* of D is $\deg D = \sum D_x \in \mathbf{Z}$. Since C is smooth, Cartier divisors are Weil divisors, so deg induces a well-defined map $\mathrm{Pic}(C) \to \mathbf{Z}$. For T an arbitrary scheme, define $\mathrm{Pic}^\circ(C \times T)$ to be the subset of $\mathrm{Pic}(C \times T)$ consisting of invertible sheaves $\mathscr{L}$ with $\deg(\mathscr{L}_t) = 0$ for all $t \in T$. That is, the following sequence is exact

$$0 \longrightarrow \mathrm{Pic}^\circ(C \times T) \longrightarrow \mathrm{Pic}(C \times T) \longrightarrow \prod_{t \in T} \mathbf{Z},$$

where the last map is $c \mapsto (\deg(c_t))_{t \in T}$. Now we define the functor $\mathrm{Pic}^\circ_C : \mathsf{Sch}^\circ_k \to \mathsf{Ab}$ by sending T to $\mathrm{Pic}^\circ(C \times_k T)/\mathrm{Pic}(T)$.

Theorem 2.4.1. *If C is a nice curve over k with $C(k) \neq \varnothing$, then Pic°_C is represented by $\mathrm{Jac}(C)$.*

Proof. By [Moc12, A.6], Pic°_C and $\mathrm{Alb}(C)$ are canonically dual. By [BG06, 8.10.22], jacobians of curves are self-dual, so the result follows from the duality theory of abelian varieties mentioned later. □

In general, we might have $C(k) = \varnothing$. We will have $J(L) = \mathrm{Pic}^\circ(C_{L'})^{\mathrm{Gal}(L'/L)}$ where L'/L is any separable extension with $C(L') \neq \varnothing$. Let $J = \mathrm{Jac}(C)$ and $j : C \to J$ be the standard embedding. Let $C^g = C \times \cdots \times C$ (g-fold product), and consider the map $f : C^g \to J$, $f(x_1, \ldots, x_g) = j(x_1) + \cdots + j(x_g)$. The symmetric group S_g acts on C^g, and f is S_g-equivariant. The quotient $\mathrm{Sym}^g(C) = C^g/S_g$ exists, and has a (birational) map $\mathrm{Sym}^g(C) \to J$. Weil defined a "rational group law" on $\mathrm{Sym}^g(C)$ using the Riemann-Roch Theorem,

and then showed that this induces an "honest group law" on a nice variety birational to $\mathrm{Sym}^g(C)$. For more details on Weil's construction (and proofs), see [Mila, III.7].

Now suppose X is an arbitrary scheme. Recall that $\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathscr{O}_X^\times)$; this classifies invertible sheaves on X, where the group operation on sheaves is $\otimes$. If X is integral, $\mathrm{Pic}(X)$ is easy to describe via the following result. (Remember that Cartier divisors on a curve are just Weil divisors.)

Theorem 2.4.2. *Let X be an integral scheme. Then $\mathrm{Pic}(X)$ is naturally isomorphic to the class group $\mathrm{Cl}(X)$ of Cartier divisors on X.*

Proof. Let $\mathscr{M}$ be the sheaf of rational functions on X. By definition, the group of Cartier divisors on X is $\mathrm{Div}(X) = \mathrm{H}^0(X, \mathscr{M}^\times/\mathscr{O}^\times)$. The short exact sequence

$$1 \to \mathscr{O}^\times \to \mathscr{M}^\times \to \mathscr{M}^\times/\mathscr{O}^\times \to 1,$$

induces a long exact sequence in sheaf cohomology:

$$0 \to \mathrm{H}^0(\mathscr{O}^\times) \to \mathrm{H}^0(\mathscr{M}^\times) \to \mathrm{Div}(X) \to \mathrm{Pic}(X) \to \mathrm{H}^1(\mathscr{M}^\times) \to \cdots.$$

If X is integral, the sheaf $\mathscr{M}^\times$ is flasque, so $\mathrm{H}^1(\mathscr{M}^\times) = 0$. It follows that $\mathrm{Cl}(X) = \mathrm{Div}(X)/\mathrm{H}^0(\mathscr{M}^\times) \xrightarrow{\sim} \mathrm{Pic}(X)$. □

⋆ For X/k an arbitrary scheme, consider the functor $\mathrm{Pic}_X : \mathsf{Sch}_k^\circ \to \mathsf{Ab}$ given by $\mathrm{Pic}_X(T) = \mathrm{Pic}(X \times_k T)/\mathrm{Pic}(T)$. This is not in general representable. However, if X is a nice k-variety, then the fppf-sheafification of Pic_X is representable [Kle05, 4.1.38]. Even better, if $X(k) \neq \varnothing$, then Pic_X is representable [Kle05, 2.5]. We will also denote the representing scheme by Pic_X, and we call Pic_X the *Picard scheme* of X. It is not a variety, but it is a disjoint union of ind-varieties [Kle05, 4.8]. More precisely, choose a very ample line bundle $\mathscr{L}$ on X. If $\mathscr{F}$ is any coherent sheaf on X, write $\mathscr{F}(n) = \mathscr{F} \otimes \mathscr{L}^{\otimes n}$. Recall that the *Euler characteristic* of $\mathscr{F}$ is $\chi(\mathscr{F}) = \sum (-1)^i h^i(\mathscr{F})$. By [Gro61, 2.5.3], there is a (unique) polynomial $\phi \in \mathbf{Q}[t]$ such that $\chi(\mathscr{F}(n)) = \phi(n)$ for all $n \in \mathbf{Z}$; set $h_{\mathscr{L}}(\mathscr{F}) = \phi$. We call ϕ the *Hilbert polynomial* of $\mathscr{F}$.

If $X(k) \neq \varnothing$, we can define for $x \in X(k)$ the modified Picard functor

$$\mathrm{Pic}_{X,x}(T) = \{(\mathscr{L}, i) : \mathscr{L} \in \mathrm{Pic}(X_T)\ ,\ i : x_T^*\mathscr{L} \xrightarrow{\sim} \mathscr{O}_T\}/\sim .$$

There is an obvious map $\mathrm{Pic}(X_T) \to \mathrm{Pic}_{X/x}(T)$ given by $\mathscr{L} \mapsto \mathscr{L} \otimes (x \circ f)_T^* \mathscr{L}^{-1}$, where $f : X \to \mathrm{Spec}(k)$ denotes the structure morphism. It is a good exercise to prove that this induces an isomorphism $\mathrm{Pic}_X \xrightarrow{\sim} \mathrm{Pic}_{X,x}$.

For $\phi \in \mathbf{Q}[t]$, denote by Pic_X^ϕ the functor which assigns to a scheme T the subset of $\mathrm{Pic}_X(T)$ consisting of invertible sheaves $\mathscr{F}$ on $X \times T$ with $h_{\mathscr{L}}(\mathscr{F}_t) = \phi$ for all $t \in T$. By [Kle05, 6.20], Pic_X^ϕ is a clopen subscheme of Pic_X, and Pic_X

is covered by the Pic^{ϕ}_X. Moreover, the Pic^{ϕ}_X are varieties. We can do even better. If we let Pic^d_X send T to the subset of $\mathrm{Pic}_X(T)$ consisting of invertible sheaves $\mathscr{F}$ with $\deg h_{\mathscr{L}}(\mathscr{F}_t) = d$ for all $t \in T$, then the Pic^d_X form a cover of Pic_X by clopen subvarieties. Just as the genus of a curve is the dimension of its jacobian, there is a natural isomorphism $\mathrm{H}^1(\mathscr{O}_X) \simeq \mathrm{Lie}(\mathrm{Pic}_X)$, from which we deduce $\dim(\mathrm{Pic}_X) = h^1(\mathscr{O}_X)$ when X is nice [Kle05, 5.11]. ⋆

Unlike the case when X is a curve, it is not always true that $\mathrm{Pic}_X(\bar{k})/\mathrm{Pic}^{\circ}_X(\bar{k}) =$ **Z**. In general, we set $\mathrm{NS}(X) = \mathrm{Pic}_X(\bar{k})/\mathrm{Pic}^{\circ}_X(\bar{k})$, and call $\mathrm{NS}(X)$ the *Néron-Severi group* of X. Suppose $X = A$ is already an abelian variety over k. Then we have

$$\mathrm{Pic}^{\circ}_A(\bar{k}) = \left\{c \in \mathrm{Pic}(A_{\bar{k}}) : t_a^* c = c \text{ for all } a \in A(\bar{k})\right\}$$

where $t_a : A_{\bar{k}} \to A_{\bar{k}}$ is translation by a. See [Mila, I.8.4] for a partial proof.

For an abelian variety A over k, the *dual* of A is defined to be $A^\vee = \mathrm{Pic}^{\circ}_A$. Each $c \in \mathrm{Pic}(A)$ gives a map $\varphi_c : A \to A^\vee$. At the level of points, it is defined as $a \mapsto t_a^* c - c$, where if $c = [\mathscr{L}]$, the class $t_a^* c - c \in A^\vee(\bar{k}) = \mathrm{Pic}^\circ(A)$ is represented by $[t_a^*\mathscr{L} \otimes \mathscr{L}^{-1}]$. It turns out that $A^{\vee\vee} \simeq A$, so calling $A^\vee$ the dual of A is rather natural. The map $\varphi_c : A \to A^\vee$ is a homomorphism of abelian varieties. If c is ample (i.e. the map from A to some projective space induced by $n \cdot c$ for $n \gg 0$ is an embedding) then φ_c is an *isogeny*, where

Definition 2.4.3. *A homomorphism $\varphi : A \to B$ is an* isogeny *if it is surjective with finite kernel.*

It is not at all obvious, but "A is isogenous to B" is an equivalence relation on abelian varieties. The relation is clearly reflexive and transitive. To see that it is symmetric, suppose we have an isogeny $\varphi : A \to B$. For any ample $c \in \mathrm{Pic}(A^\vee)$, $d \in \mathrm{Pic}(B)$, the composite

$$B \xrightarrow{\varphi_d} B^\vee \xrightarrow{\varphi^\vee} A^\vee \xrightarrow{\varphi_c} A^{\vee\vee} \xrightarrow{\sim} A$$

is an isogeny.

Definition 2.4.4. *Let A be an abelian variety. A* polarization *of A is an isogeny of the form $\varphi_c : A \to A^\vee$ for some ample $c \in \mathrm{Pic}(A)$.*

The duality theory of abelian varieties is very rich. A good place to start is Chapter VII of [vdGM13].

2.5 Recovering a curve from its jacobian

Let k be a field, C/k a nice curve, and $J = \mathrm{Jac}(C)$ its jacobian. What does (the arithmetic of) J tell us about (the arithmetic of) C? In particular, can

we recover C from J? In general, J does not determine C. For example, if $g = g(C) = 0$, then $J = 0$. However, there are (non-algebraically closed) fields k for which there are nice curves C over k with $g(C) = 0$ (hence $\operatorname{Jac} C = 0 = \operatorname{Jac} \mathbf{P}^1$), but $C \not\simeq \mathbf{P}^1_k$. There are more difficult examples when the genus $g > 0$.

Suppose we add some data. Assume $g \geqslant 2$ and $C(k) \neq \varnothing$. This gives us a map $j : C \to J$ determined by $x \mapsto 0$ for some distinguished $x \in C(k)$. Consider $\theta = j(C) + \cdots + j(C)$, where there are $g - 1$ terms in the sum. It turns out that θ is an irreducible ample divisor of J, called the *theta-divisor*. Thus θ induces a polarization $\varphi_\theta : J \to J^\vee$.

Theorem 2.5.1 (Torelli)**.** *If C, C' are nice curves over a field k with $(J, \theta) \simeq (J', \theta')$, then $C \simeq C'$ over k.*

Proof. See [Mila, III.13] for a rather unenlightening proof. □

It is known that $\varphi_\theta : J \to J^\vee$ is actually an isomorphism. We call a polarization $A \to A^\vee$ *principal* if it is an isomorphism. The famous *Schottky problem* asks what pairs (A, c), with c inducing a principal polarization, come from jacobians.

⋆ This question has an easy partial answer if we are willing to use heavy machinery. Consider the functor $\mathcal{M}_g$ which sends a scheme S to the set of isomorphism classes of curves of genus g over S. The functor $\mathcal{M}_g$ is unfortunately not representable (there is no *fine* moduli spaces for curves), but it is nearly so (there is a *coarse* moduli space). That is, there is a scheme (a variety, actually) M_g together with a natural transformation $\mathcal{M}_g \to h_{M_g}$ such that $\mathcal{M}_g(L) \to h_{M_g}(L)$ is a bijection whenever L is an algebraically closed field, and such that $\mathcal{M}_g \to h_{M_g}$ is initial among all morphisms from $\mathcal{M}_g$ to representable functors. For a proof, see [DFK94, 5]. Along the same lines, we can let $\mathcal{A}_g$ be the functor which assigns to a scheme S the set of isomorphism classes of principally polarized abelian schemes of dimension g over S. The functor $\mathcal{A}_g$ has a coarse moduli space A_g.

The operation "take jacobian with its canonical polarization" induces a natural transformation $j : \mathcal{M}_g \to \mathcal{A}_g$, and Torelli's theorem can be rephrased as saying that j is injective. Shottky's question asks what the image of j is. To see that it cannot be all of $\mathcal{A}_g$, simply note that $\dim(M_g) = 3g - 3$, while $\dim(A_g) = \frac{g(g+1)}{2}$. For $g > 3$, A_g has greater dimension than M_g, so $j : M_g(\bar{\mathbf{Q}}) \to A_g(\bar{\mathbf{Q}})$ cannot possibly be surjective. On the other hand, for $g \leqslant 3$, all principally polarized abelian varieties are jacobians (possibly after a change of the polarization). ⋆

One might hope that all abelian varieties are at least isogenous to jacobians. While this is true for dimension $d \leqslant 3$, it is not true in general. In fact, for

all $d > 3$, there exists an abelian variety of dimension d over $\overline{\mathbf{Q}}$ which is not isogenous to a jacobian. This was proven recently in [Tsi12]

Example 2.5.2 (group law on elliptic curves)**.** Let k be field of characteristic not 2 or 3. Let E be an elliptic curve of the form $y^2 = x^3 + ax + b$ with $4a^3 + 27b^2 \neq 0$. That is, E is the subset of $\mathbf{P}^2_k$ given by

$$x_1^2 x_2 - x_0^3 - a x_0 x_2^2 - b x_2^3.$$

The choice of $O = (0 : 1 : 0) \in E(k)$ induces an embedding $j : E \to \mathrm{Jac}(E)$ which is an isomorphism by the Riemann-Roch theorem. We would like to relate the induced group operation on E with the classical definition using chords and tangents.

Let $P, Q \in E(\bar{k})$. If we assume $P, Q \neq O$, then we can write $P = (P_0 : P_1 : 1)$, $Q = (Q_0 : Q_1 : 1)$. Assume $P_0 \neq Q_0$. Then there is an obvious rational function (canonical up to scale), whose zero-set is a line containing both P and Q. Indeed, we put

$$\ell_{P,Q}(x_0 : x_1 : x_2) = \frac{Q_1 - P_1}{Q_0 - P_0} \cdot \frac{x_0}{x_2} - \frac{x_1}{x_2} + \frac{P_1 Q_0 - P_0 Q_1}{Q_0 - P_0}.$$

The function $\ell_{P,Q}$ has P, Q and a third point R as simple zeros, and one can verify directly that $\mathrm{div}(\ell_{P,Q}) = P + Q + R - 3O = (P - O) + (Q - O) + (R - O)$. Recall that $(\mathrm{Jac}\, E)(\bar{k}) = \mathrm{Pic}^\circ(E_{\bar{k}})$, and the map $j : E \to \mathrm{Jac}(E)$ corresponds to $P \mapsto P - O$. Thus $j(P) + j(Q) + j(R) = \mathrm{div}(\ell_{P,Q}) = 0$ in $\mathrm{Pic}^\circ(E_{\bar{k}})$, i.e. $j(P) + j(Q) = -j(R)$.

It is well-known that R can be written as a rational function of P and Q, so the chord-tangent law defines a rational map $m : E \times E \to E$ with $j(m(P)) + j(m(Q)) = m(j(P), j(Q))$. It follows that m is defined everywhere. ▷

3 The Mordell-Weil theorem

3.1 Statement and generalizations

The goal of this section is to give an essentially complete proof of the *Mordell-Weil theorem*. Throughout the section, k will denote a field, often a *number field* (finite field extension of $\mathbf{Q}$). Important examples are the *quadratic fields* $k = \mathbf{Q}(\sqrt{d})$ and *cyclotomic fields* $\mathbf{Q}(\zeta_n)$.

Theorem 3.1.1 (Mordell-Weil)**.** *Let A be an abelian variety over a number field k. Then the abelian group $A(k)$ is finitely generated.*

This is clearly false if $k = \mathbf{C}$ and $A \neq 0$, for then $A(\mathbf{C})$ is a complex Lie group, hence uncountable. In fact, whenever k is a local field, $A(k)$ is a Lie group

over k, hence uncountable. The Mordell-Weil theorem does holds whenever k is finitely generated over its prime field. In this case, basic algebra shows that $A(k) = A(k)_{\text{tors}} \oplus \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_r$, where the x_i are linearly independent over $\mathbf{Z}$. We call $\operatorname{rk} A = r$ the *rank* of A. Mordell proved the theorem for A an elliptic curve over $\mathbf{Q}$, demonstrating an assertion of Poincaré.

Example 3.1.2. Let $E \subset \mathbf{P}^2_{\mathbf{Q}}$ be the projective closure of the affine curve defined by $y = x^3 + 2x + 3$, with $O = (0 : 1 : 0)$ the point at infinity. The curve has a group law such that $a + b + c = 0$ if and only if a, b, c are colinear. Alternatively, let $J = \operatorname{Jac} E$, The point $O \in E(\mathbf{Q})$ induces an embedding $E \hookrightarrow J$ sending O to 0. This is an isomorphism, and we can use it to transfer the group structure of J to E. The curve E has an obvious rational point $(-1, 0)$ of order two. Another rational points is $(3, 6)$. Their sum is $\left(\frac{1}{4}, -\frac{15}{16}\right)$. One can show that $E(\mathbf{Q}) = \langle(-1, 0)\rangle \oplus \langle(3, 6)\rangle$, where $(-1, 0)$ has order two and $(3, 6)$ has infinite order. So $E(\mathbf{Q}) = \mathbf{Z}/2 \oplus \mathbf{Z}$. ▷

Example 3.1.3. Let $E/\mathbf{Q}$ be the projective closure of $y^2 + y = x^3 + x^2 - 2x$. We claim that $E(\mathbf{Q}) = \langle(0, 0), (1, 0)\rangle \simeq \mathbf{Z}^{\oplus 2}$. As an exercise, try to find ten more points in $E(\mathbf{Q})$. ▷

A result that motivated Weil is the following conjecture of Mordell (now a theorem of Faltings).

Theorem 3.1.4 (Faltings)**.** *If C is a nice curve over a number field k with genus $g \geqslant 2$, then $C(k)$ is finite.*

Mordell's conjecture fails if $g \leqslant 1$. For $g = 0$, $\mathbf{P}^1$ has lots of rational points, and we have seen examples of elliptic curves with infinitely many rational points. Here is a heuristic. Assume $C(k) \neq \varnothing$ and consider the canonical embedding $C \hookrightarrow J$. We have $C(k) = C \cap J(k)$. The set C has positive codimension in J, and $J(k)$ is a finitely generated abelian group. So $C(k)$ is the intersection of two "sparse" subsets of J. One would expect this forces $C(k)$ to be small. This heuristic is validated by the following theorem, originally known as the *Mordell-Lang conjecture*.

Theorem 3.1.5 (Faltings)**.** *Let A be an abelian variety over an algebraically closed field k of characteristic zero, and let Γ be a finitely generated subgroup of $A(k)$. If $X \subset A$ is a subvariety, then there is a finite set $S \subset \Gamma$ and a finite set $\{B_s : s \in S\}$ of abelian subvarieties of A such that*

$$X(k) \cap \Gamma = \bigcup_{s \in S} (s + B_s(k) \cap \Gamma)\,.$$

Proof. See [McQ95] for a proof in the case $k = \mathbf{C}$. The general case follows by the Lefschetz principle. McQuillan actually proves the theorem for a broader class of group varieties than abelian varieties. □

Corollary 3.1.6. *Let A be an abelian variety over $\mathbf{C}$, and let C be a nice curve in A of genus $g \geqslant 2$. Let Γ be a finitely generated subgroup of $A(\mathbf{C})$. Then $C(\mathbf{C}) \cap \Gamma$ is finite.*

Proof. Since C has genus $g \geqslant 2$, it cannot contain a nontrivial abelian variety. Thus each $B_s = 0$, so the theorem yields $C(\mathbf{C}) \cap \Gamma = S$ for some finite set $S \subset \Gamma$. □

There is a relative version of the Mordell-Lang conjecture known as the *Lang-Néron theorem*. Let K/k be a *regular* field extension, that is, $\bar{k} \cap K = k$ and K/k is separable. If A is an abelian variety defined over K, then there is an abelian variety $\mathrm{tr}_{K/k}(A)$ defined over k together which a morphism $\tau : \mathrm{tr}_{K/k}(A)_K \to A$ that is initial among abelian varieties B/k with morphisms $B_K \to A$. One calls $\mathrm{tr}_{K/k}(A)$ the *K/k-trace of A*. Intuitively, $\mathrm{tr}_{K/k}(A)$ is the smallest abelian subvariety of A defined over k. A proof of the following theorem can be found in [Con06].

Theorem 3.1.7 (Lang-Néron)**.** *Let K/k be a finitely generated regular extension, and let A be an abelian variety over K. Then the group $A(K)/\mathrm{tr}_{K/k}(A)(k)$ is finitely generated.*

This implies the Mordell-Weil theorem for finitely generated fields. If K is a finitely generated field, let k be the algebraic closure of the prime field of K within K. Then K/k is regular, and by the usual Mordell-Weil theorem, $\mathrm{tr}_{K/k}(A)(k)$ is finitely generated, so $A(K)$ has a finitely generated subgroup with finitely generated quotient. It follows that $A(K)$ is finitely generated.

3.2 Plan of the proof

Let A be an abelian variety over a number field k. Our proof has three parts:

1. Construct a "height function" $|\cdot| : A(k) \to \mathbf{R}_{\geqslant 0}$ with good properties.
2. Prove the weak Mordell-Weil theorem: $A(k)/n$ is finite for all $n \geqslant 2$.
3. Show that 1 and 2 formally imply the full Mordell-Weil theorem.

We will prove 3 here, spend the next several sections on 2, and finally construct a good height function in 3.11. For the sake of space, write $A(k)/n$ instead of $A(k)/nA(k)$, and ${}_nA(k)$ instead of $\{x \in A(k) : n \cdot x = 0\}$.

Lemma 3.2.1. *Let A be an abelian group with a function $|\cdot| : A \to \mathbf{R}_{\geqslant 0}$ such that for some $n \geqslant 2$,*

- *for all $c > 0$, the set $B_c = \{x \in A : |x| \leqslant c\}$ is finite*

- $|x-y| \leqslant |x| + |y|$ *and* $|nx| = n|x|$ *for all* $x, y \in A$, $n \in \mathbf{N}$
- *the group* A/n *is finite*

Then A *is finitely generated.*

Proof. Let $\{a_i\}$ be a (finite) set of coset representatives for A/n. Let $c = 2\sup\{|a_i|\}$. We claim that A is generated by the finite set B_c. This will be shown "by descent." Fix $n \geqslant 2$ and let $x_1 \in A$. By our assumptions, we can write $x_1 = y_{i_1} + nx_2$ with $y_{i_1} \in \{a_i\}$, and one see that

$$|x_2| = \frac{1}{n}|x_1 - y_{i_1}| \leqslant \frac{|x_1| + |y_{i_1}|}{n} \leqslant \frac{1}{n}|x_1| + \frac{c}{2n}.$$

Setting $x_{r+1} = y_{i_r} + nx_r$ with $y_{i_r} \in \{a_i\}$, we can continue this process, obtaining the inequality

$$|x_{r+1}| \leqslant \frac{1}{n}|x_r| + \frac{c}{2n} \leqslant \frac{1}{n^r}|x_1| + \frac{1}{2}\left(\frac{1}{n} + \cdots + \frac{1}{n^r}\right)c \leqslant \frac{|x_1|}{n^r} + \frac{c}{2}.$$

For $r \gg 0$, the quantity on the right is less than c. Thus x_1 is in the subgroup of A generated by B_c and $\{a_i\}$. Since $|a_i| \leqslant c$ for each i, we have $A = \langle B_c \rangle$. □

To prove the weak Mordell-Weil theorem, we will use group cohomology extensively. For some motivation, let A be an abelian variety over a field k of characteristic zero. Let ${}_nA$ be the kernel of $\cdot n : A(\bar{k}) \to A(\bar{k})$. We can take G_k-invariants of ${}_nA$, resulting in an exact sequence:

$$0 \longrightarrow ({}_nA)^{G_k} \longrightarrow A(k) \xrightarrow{n} A(k).$$

We are interested in continuing this exact sequence to the right, i.e. in constructing a long exact sequence

$$0 \longrightarrow ({}_nA)^{G_k} \longrightarrow A(k) \xrightarrow{n} A(k) \xrightarrow{\delta} \mathrm{H}^1(G_k, {}_nA) \longrightarrow \mathrm{H}^1(G_k, A(\bar{k})) \longrightarrow \mathrm{H}^1(G_k, A(\bar{k})) \longrightarrow \cdots$$

This fits into a general framework of derived functors, but we will mostly just use the concrete definition of $\mathrm{H}^1(G_k, -)$ using cocycles and coboundaries.

Here is a very brief explanation of the construction of $|\cdot|$. For simplicity, we assume k is a number field. There is a height function on $\mathbf{P}^n(\bar{k})$ defined by

$$h(x_0 : \cdots : x_n) = \frac{1}{[L : \mathbf{Q}]} \sum_v \log \sup\{|x_i|_v\},$$

where L/k is some extension containing the x_i and $|\cdot|_v$ is the normalized absolute value associated with v. For a very ample divisor c on A, we get an embedding $\varphi_c : A \to \mathbf{P}^n$, and thus a height function $h_c : A(\bar{k}) \to \mathbf{R}_{\geqslant 0}$. As it stands, this is not uniquely defined, but there is a unique way of adjusting h_c by a bounded function on $A(\bar{k})$ to get a function $\widehat{h}_c : A(\bar{k}) \to \mathbf{R}$ such that

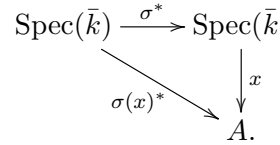
$$(x, y) \mapsto \langle x, y\rangle_c = \frac{1}{2}\left(\widehat{h}_c(x+y) - \widehat{h}_c(x) - \widehat{h}_c(y)\right)$$

is bilinear. One calls $\widehat{h}_c$ the *Néron-Tate height* associated with c. The function $|\cdot|$ in the proof can be taken to be $|\cdot|_c = \widehat{h}_c^{1/2}$ for any very ample even divisor c.

This proof of the Mordell-Weil theorem is very nearly effective. Given a set of generators for $A(k)/n$, it gives an algorithm for finding a set of generators for $A(k)$. Moreover, one can choose any integer n. Most people use $n = 2$ when doing computations.

3.3 Group cohomology

Let k be a number field, $\bar{k}$ an algebraic closure of k, and $G_k = \mathrm{Gal}(\bar{k}/k)$ the *absolute Galois group* of k. This is a *profinite group* (compact, totally connected and Hausdorff) with a basis of neighborhoods of 1 being the groups $G_L = \mathrm{Gal}(\bar{k}/L)$ where L ranges over the finite extensions of k. Let A be an abelian variety over k of dimension $d \geqslant 1$. There is no harm in thinking of $k = \mathbf{Q}$ and A as an elliptic curve. The abelian group $A(\bar{k})$ naturally has a continuous G_k-action. One way to see this is to embed A into some huge projective space and let G_k act on each coordinate. A more high-brow way to see this is to note that $A(\bar{k}) = \hom(\mathrm{Spec}(\bar{k}), A)$, so if $\sigma \in G_k$, $\in A(\bar{k})$, the point $\sigma(x)$ is the composite



The homomorphism $A \xrightarrow{n} A$ that sends x to $n \cdot x$ is an isogeny. Let ${}_nA$ be the n-torsion subgroup of $A(\bar{k})$, i.e.

$${}_nA = \{x \in A(\bar{k}) : n \cdot x = 0\}.$$

If k were a field of positive characteristic p and $p \mid n$, it would be better to think of $A[n]$ as the scheme $A \times_A 0$ via $n : A \to A$. In any case, there is an exact sequence

$$0 \longrightarrow {}_nA \longrightarrow A(\bar{k}) \xrightarrow{n} A(\bar{k}) \longrightarrow 0.$$

Recall that if G is an arbitrary group acting on some abelian group M, we define the module of *G-invariants* of M by

$$M^G = \{m \in M : \sigma m = m \text{ for all } \sigma \in G\}.$$

Taking G_k-invariants of the above short exact sequence, we get an exact sequence

$$0 \longrightarrow ({}_nA)^{G_k} \longrightarrow A(k) \xrightarrow{n} A(k).$$

We don't usually have exactness on the right because the functor $(-)^{G_k}$ is not right-exact. For example, if k is a number field, the n-th power map $(-)^n : \bar{k}^\times \to \bar{k}^\times$ is surjective, but $(-)^n : (\bar{k}^\times)^{G_k} = k^\times \to k^\times$ is not.

$\star$ We can define $\mathrm{H}^\bullet(G_k, {}_nA)$ using the formalism of derived functors. Consider the category G_k-Mod of (discrete) abelian groups with continuous G_k-action. This is an abelian category with enough injectives. The functor $\Gamma = (-)^{G_k} : G_k\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is left-exact, so we can define the group cohomology as the derived functors of Γ, i.e. $\mathrm{H}^\bullet(G_k, -) = \mathsf{R}^\bullet\Gamma$. In particular, $\mathrm{H}^0(G_k, M) = M^{G_k}$ for any discrete G_k-module M. $\star$

Choose $x \in A(k)$. Then $x = n \cdot y$ for some $y \in A(\bar{k})$. Take $\sigma \in G_k$. Then $x = \sigma x$, so $\sigma(n \cdot y) = n \cdot \sigma(y)$. Then $n \cdot (\sigma y - y) = n \cdot \sigma y - n \cdot y = 0$, so $\sigma y - y \in {}_nA$. Thus we have a map (*not* usually a homomorphism) $\varphi : G_k \to {}_nA$, $\sigma \mapsto \sigma y - y$. Take $\sigma, \tau \in G_k$. Then one computes

$$\begin{aligned}\varphi(\sigma\tau) &= \sigma\tau(y) - y \\ &= \sigma(\tau y - y) + \sigma y - y \\ &= \sigma\varphi(\tau) + \varphi(\sigma).\end{aligned}$$

So φ is a homomorphism precisely when the action of G_k on ${}_nA$ is trivial. Moreover, there is a number field L/k such that $G_L \subset G_k$ fixes y. In particular, $\varphi(G_L) = 0$, so the map $\varphi : G_k \to {}_nA$ is continuous. Suppose we choose some y' distinct from y with $x = n \cdot y'$. We could define $\varphi' : G_k \to {}_nA$ by $\sigma \mapsto \sigma y' - y'$. Since $n(y - y') = 0$, we have $y' - y \in {}_nA$, hence $y' = y + \alpha$ for some $\alpha \in {}_nA$. We now have

$$\begin{aligned}\varphi'(\sigma) &= \sigma y' - y' \\ &= \sigma(y + \alpha) - (y + \alpha) \\ &= \sigma y - y + \sigma\alpha - \alpha \\ &= \varphi(\sigma) + \sigma\alpha - \alpha.\end{aligned}$$

Maps $G_k \to {}_nA$ of the form $\sigma \mapsto \sigma\alpha - \alpha$ will be called *coboundaries*.

Suppose we have another point $x' \in A(k)$. Choose a y' with $x' = ny'$. Then $x + x' = n(y + y')$, and the point $x + x'$ gives rise to a map $G_k \to {}_nA$, $\sigma \mapsto \sigma(y + y') - (y + y')$; this map is just $\varphi + \varphi'$, where $\varphi' : \sigma \mapsto \sigma y' - y$.

Definition 3.3.1. *Let G be a profinite group, M a discrete G-module. The group $Z^1(G,M)$ of* 1-cocycles *consists of continuous maps $\varphi : G \to M$ such that $\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma)$. The group $B^1(G,M)$ of* 1-coboundaries *consists of continuous maps $\varphi : G \to M$ of the form $\sigma \mapsto \sigma\alpha - \alpha$ for some $\alpha \in M$. The* first cohomology of G with coefficients in M *is*

$$\mathrm{H}^1(G,M) = Z^1(G,M)/B^1(G,M).$$

One can prove using a canonical projective resolution of M that this agrees with the derived functor definition. It is not hard to check directly that if $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence of G_k-modules, then there is a natural exact sequence:

$$0 \longrightarrow M'^G \xrightarrow{f} M^G \xrightarrow{g} M''^G \xrightarrow{\delta} \mathrm{H}^1(G,M') \longrightarrow \mathrm{H}^1(G,M) \longrightarrow \mathrm{H}^1(G,M'') \longrightarrow \cdots$$

where $\delta(x)$ is defined as follows. Choose a lift $\tilde{x}$ in M of x, and let $\delta(x)(\sigma) = f^{-1}(\sigma\tilde{x} - \tilde{x})$. One can check that this is a cocycle, and that choosing a different $\tilde{x}$ changes $\delta(x)(\sigma)$ by a coboundary.

$\star$ If G is a discrete group, then the cohomology $\mathrm{H}^\bullet(G,M)$ can be interpreted as an Ext-group. It is easy to see that the category of G-module is equivalent to the category of $\mathbf{Z}[G]$-modules, and that $M^G \simeq \hom_{\mathbf{Z}[G]}(\mathbf{Z}, G)$. It follows that $\mathrm{H}^\bullet(G,M) \simeq \mathrm{Ext}^\bullet_{\mathbf{Z}[G]}(\mathbf{Z}, M)$. If G is a profinite group, then $\mathbf{Z}[G]$ is the wrong ring to use. Instead, one considers the *completed group ring*

$$\mathbf{Z}[\![G]\!] = \varprojlim_{\substack{N \lhd G \\ N \text{ open}}} \mathbf{Z}[G/N]$$

where we give each $\mathbf{Z}[G/N]$ the discrete topology and $\mathbf{Z}[\![G]\!]$ the inverse limit topology. The category of discrete G-modules with continuous action is equivalent to the category of discrete $\mathbf{Z}[\![G]\!]$-modules with continuous action, $M^G \simeq \hom_{\mathbf{Z}[\![G]\!]}(\mathbf{Z}, M)$, whence $\mathrm{H}^\bullet(G,M) \simeq \mathrm{Ext}^\bullet_{\mathbf{Z}[\![G]\!]}(\mathbf{Z}, M)$.

In the case that $G = G_k$, one can interpret the groups $\mathrm{H}^\bullet(G,M)$ as a special case of étale cohomology. Recall that a morphism $f : X \to S$ of schemes is *étale* if it is flat and unramified. The *étale site* of S, denoted $S_{\text{ét}}$, is the full subcategory of Sch_S consisting of $X \to S$ that are étale. A collection $\{f_i : U_i \to X\}$ in $S_{\text{ét}}$ is a *cover* if the images of the f_i cover X. With this notion of a cover, $S_{\text{ét}}$ is a (subcanonical) site, so we can talk about sheaves and cohomology on $S_{\text{ét}}$. The main example is: $\star$

Example 3.3.2 ($\star$)**.** Let k be a field, and write $k_{\text{ét}}$ for $\operatorname{Spec}(k)_{\text{ét}}$. Then the objects of $k_{\text{ét}}$ are all of the form $\operatorname{Spec}(L_1) \sqcup \cdots \sqcup \operatorname{Spec}(L_n) \to \operatorname{Spec}(k)$ for a finite family of separable field extensions $L_1, \dots, L_n$ of k. One can check that the category $\operatorname{Sh}(k_{\text{ét}})$ of abelian sheaves on $k_{\text{ét}}$ is equivalent to the category of discrete G_k-modules, via the functor $\mathscr{F} \mapsto \mathscr{F}_{\bar{k}} = \varinjlim_{L/k} \mathscr{F}(\operatorname{Spec} L)$, where L ranves over all finite Galois extensions of k. If M is a G_k-module, then there is a corresponding étale sheaf $\widetilde{M}$, determined by $\widetilde{M}(\operatorname{Spec} L) = M^{G_L}$. Since $M^G \simeq \mathrm{H}^0(k_{\text{ét}}, \widetilde{M})$, we obtain that $\mathrm{H}^\bullet(G_k, M) \simeq \mathrm{H}^\bullet(k_{\text{ét}}, \widetilde{M})$. For more details, see [Del77, I 2.4]. ▷

In our case, from the long exact sequence associated to $0 \to {}_nA \to A(\bar{k}) \xrightarrow{n} A(\bar{k}) \to 0$ yields a short exact sequence

$$0 \longrightarrow A(k)/n \xrightarrow{\delta} \mathrm{H}^1\left(G_k, {}_nA\right) \longrightarrow {}_n\mathrm{H}^1\left(G_k, A(\bar{k})\right) \longrightarrow 0.$$

We will try to prove that $A(k)/n$ is finite by embedding it into a group we know is finite. Unfortunately $\mathrm{H}^1(G_k, {}_nA)$ is infinite, so we cannot just use the above exact sequence to show that $A(k)/n$ is finite.

In general, suppose G is a (commutative) group scheme over k. For example, G could be the multiplicative group $\mathbf{G}_m$, or an abelian variety A. If G is any commutative group scheme over k, we will use ${}_nG$ to denote the fiber product $G \times_G 0$, where the map $G \to G$ is "multiply by n." This conflicts with our earlier convention that ${}_nA = {}_nA(\bar{k})$, but no confusion should arise from this. The group $G(\bar{k})$ is a G_k-module, so we can consider the cohomology groups $\mathrm{H}^\bullet\left(G_k, G(\bar{k})\right)$. We know that these are isomorphic to the étale cohomology groups $\mathrm{H}^\bullet\left(k_{\text{ét}}, \widetilde{G(\bar{k})}\right)$, and one can check quite easily that $\widetilde{G(\bar{k})}$ is just G, regarded as a sheaf on $k_{\text{ét}}$ via its functor of points. It follows that $\mathrm{H}^\bullet\left(G_k, G(\bar{k})\right) = \mathrm{H}^\bullet(k_{\text{ét}}, G)$, and we will identify the two without comment in the future.

To simplify the notation, we will often write k for $k_{\text{ét}}$, i.e. $\mathrm{H}^\bullet(k, G) = \mathrm{H}^\bullet(k_{\text{ét}}, G)$. In this context, Hilbert's *Theorem 90* says that for k a field, $\mathrm{H}^1(k, \mathbf{G}_m) = 0$. If we write $\boldsymbol{\mu}_n = {}_n\mathbf{G}_m$, then *Kummer Theory* starts with the short exact sequence $1 \to \boldsymbol{\mu}_n \to \mathbf{G}_m \xrightarrow{n} \mathbf{G}_m \to 1$ and uses Hilbert's Theorem 90 together with the long exact sequence in sheaf cohomology to derive $\mathrm{H}^1(k, \boldsymbol{\mu}_n) = k^\times/n$.

There is an alternate description of $\mathrm{H}^1(k, A)$. If G is an arbitrary commutative algebraic group over k, a *principal homogeneous space* (also called a *torsor*) for G over k is a variety X/k together with a morphism $G \times X \to X$ which, on $\bar{k}$-valued points, is a simply transitive group action. That is, if we write $g + x$ for the image of (g, x) in X, we require that

- $g + (h + x) = (g + h) + x$

- $0 + x = x$
- for all $x, y \in X(\bar{k})$, there is a unique $g \in G(\bar{k})$ such that $g + x = y$

More generally, if S is a scheme and $\mathscr{G}$ is an abelian sheaf on $S_{\text{ét}}$, a *torsor* for $\mathscr{G}$ is a sheaf of sets $\mathscr{T}$ with a group action $\mathscr{G} \times \mathscr{T} \to \mathscr{T}$ that, étale-locally on S, is isomorphic to $\mathscr{G}$ as a sheaf with left $\mathscr{G}$-action. Two torsors $\mathscr{T}, \mathscr{T}'$ are isomorphic if there is a sheaf isomorphism $\mathscr{T} \to \mathscr{T}'$ that commutes with the action of $\mathscr{G}$. One can show (see e.g. [Del77, IV 1.1]) that $\mathrm{H}^1(S_{\text{ét}}, \mathscr{G})$ is naturally isomorphic as a pointed set to the set of isomorphism classes of $\mathscr{G}$-torsors.

Thus if G is a commutative algebraic group over k, there is a natural bijection between the set of isomorphism classes of G-torsors and $\mathrm{H}^1(k, G)$. There is a non-abelian version of this. If $\mathscr{G}$ is an arbitrary sheaf of groups over $S_{\text{ét}}$, then one can still define the notion of a $\mathscr{G}$-torsor. An identical theorem holds, except that one must define the "cohomology set" $\mathrm{H}^1(S_{\text{ét}}, \mathscr{G})$. For details, see [Sko01]. There is a non-abelian version of Hilbert's Theorem 90: it says that $\mathrm{H}^1(k, \mathrm{SL}_n) = \mathrm{H}^1(k, \mathrm{GL}_n) = 0$ for all n [Ser79, X.1].

3.4 Selmer groups and weak Mordell-Weil

Recall that if G is a profinite group (e.g G_k for some field k) and M is a discrete abelian group with continuous G-action, we directly defined the first cohomology group $\mathrm{H}^1(G, M) = Z^1(G, M)/B^1(G, M)$, where

$$Z^1(G, M) = \{\varphi : G \to M \text{ continuous} : \varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma)\}.$$

and $B^1(G, M)$ consisted of all $\varphi : G \to M$ of the form $\sigma \mapsto \sigma x - x$. Note that if G acts trivially on M, then $\mathrm{H}^1(G, M) = \hom_{\text{cts}}(G, M)$. If $f : M \to M'$ is G-equivariant, then there is an obvious map $f_* : \mathrm{H}^1(G, M) \to \mathrm{H}^1(G, M')$ given by $f_*[\varphi] = [f \circ \varphi]$. Moreover, if $f : G' \to G$ is a continuous group homomorphism, then we have a map $f^* : \mathrm{H}^1(G, M) \to \mathrm{H}^1(G', M)$ given by $f^*[\varphi] = \varphi \circ f$, where we regard G' as acting on M via f.

Let k be a number field, A be an abelian variety over k, and $n \geqslant 2$. The short exact sequence $0 \to {}_nA \to A \xrightarrow{n} A \to 0$ of group schemes induces an exact sequence

$$0 \longrightarrow A(k)/n \longrightarrow \mathrm{H}^1(k, {}_nA) \longrightarrow {}_n\mathrm{H}^1(k, A) \longrightarrow 0.$$

We are trying to prove that $A(k)/n$ is finite. Since $\mathrm{H}^1(k, {}_nA)$ is always infinite, this does not follow immediately from the above exact sequence.

Example 3.4.1. Let $K = \mathbf{Q}$, and let E be the elliptic curve defined by $y^2 = (x-a)(x-b)(x-c)$ for distinct $a, b, c \in \mathbf{Q}$. Then ${}_2E(\bar{\mathbf{Q}}) = \{0, (a, 0), (b, 0), (c, 0)\}$.

Thus

$$\begin{aligned}\mathrm{H}^1(\mathbf{Q}, {}_2E) &= \hom(G_{\mathbf{Q}}, {}_2E)\\ &= \hom(G_{\mathbf{Q}}, \mathbf{Z}/2 \times \mathbf{Z}/2)\\ &= \hom(G_{\mathbf{Q}}, \mathbf{Z}/2) \times \hom(G_{\mathbf{Q}}, \mathbf{Z}/2).\end{aligned}$$

This is easily seen to be infinite (either using global class field theory, or by noting that $\mathbf{Q}$ has lots of Galois extensions of degree 2). In fact, using Kummer theory, one can show that $\mathrm{H}^1(\mathbf{Q}, {}_2E) = (\mathbf{Q}^\times/2)^{\oplus 2}$, which is $\mathbf{F}_2$-vector space of dimension $\aleph_0$. ▷

Our goal is to find a finite subgroup of $\mathrm{H}^1(k, {}_nA)$ containing $A(k)/n$. We haven't really used the fact that k is a number field yet – everything so far works for any perfect field. That changes when we start looking at completions of k.

As before, let k be a number field, and let k_v denote the completion of k at a place v. One can show that k_v will either be $\mathbf{R}$, $\mathbf{C}$, or a finite extension of some $\mathbf{Q}_p$. Choose $\overline{k_v} \supset k$; this gives a homomorphism $G_{k_v} \to G_k$, where $\sigma \mapsto \sigma|_{\bar{k}}$. It turns out that the map is injective (this is an easy corollary of Krasner's Lemma). As an example, if $k = \mathbf{Q}$, $k_v = \mathbf{R}$, then $G_{\mathbf{R}} = \{1, c\}$ where $c : \mathbf{C} \to \mathbf{C}$ is complex conjugation. The image of c in $G_{\mathbf{Q}}$ is some element of order two.

The functoriality of $\mathrm{H}^\bullet(-,-)$ applied to the injection $G_{k_v} \to G_k$ gives us a map $\mathrm{H}^1(k, {}_nA) \to \mathrm{H}^1(k_v, {}_nA)$, where we regard ${}_nA$ as a group scheme over k_v by base extension. We now have a commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(k)/n & \longrightarrow & \mathrm{H}^1(k, {}_nA) & \longrightarrow & {}_n\mathrm{H}^1(k, A) & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow & & \\
0 & \longrightarrow & \prod_v A(k_v)/n & \xrightarrow{\alpha} & \prod_v \mathrm{H}^1(k_v, {}_nA) & \longrightarrow & \prod_v {}_n\mathrm{H}^1(k_v, A) & \longrightarrow & 0.
\end{array}$$

The *n-Selmer group* of A over k is

$$\mathrm{Sel}_n(A) = \beta^{-1}(\operatorname{im}\alpha) = \ker\left(\mathrm{H}^1(k, {}_nA) \to \prod_v {}_n\mathrm{H}^1(k_v, A)\right).$$

Similarly, we define the *Tate-Shafarevich group* of A by the exact sequence

$$0 \longrightarrow Ш(A) \longrightarrow \mathrm{H}^1(k, A) \longrightarrow \prod_v \mathrm{H}^1(k_v, A).$$

Putting these two definitions together, we obtain a short exact sequence

$$0 \longrightarrow A(k)/n \longrightarrow \mathrm{Sel}_n(A) \longrightarrow {}_n Ш(A) \longrightarrow 0.$$

We will soon prove that $\mathrm{Sel}_n(A)$ is finite, hence $A(k)/n$ and ${}_n Ш(A)$ are finite.

Conjecture 3.4.2 (Tate-Shafarevich)**.** *If A is an abelian variety over a number field k, the group $Ш(A)$ is finite*

This conjecture is currently wide open. A positive answer would show that for n sufficiently large, $A(k)/n \simeq \mathrm{Sel}_n(A)$. In particular, this would imply that for $p \gg 0$, $\mathrm{rk}(A) = \dim_{\mathbf{F}_p} \mathrm{Sel}_p(A)$, where as before $\mathrm{rk}(A) = \mathrm{rk}_{\mathbf{Z}} A(k)$ is the algebraic rank of A. The Selmer groups $\mathrm{Sel}_n(A)$ are effectively computable. If $Ш(A)$ were always finite, then $A(k)$ would be computable.

3.5 Crash course in algebraic number theory

If k is a number field, we already used (without defining it) the notion of a *place* of k. In this section, we will see that k comes with a lot of extra structure which will be used later on. Let's start with places.

Definition 3.5.1. *A* local field *is a topological field that is locally compact as a topological space.*

Let k be a local field. Then the additive group of k is a locally compact group, so it has a nontrivial *Haar measure*, i.e. a translation-invariant Borel measure μ. For $\alpha \in k$, the measure $\alpha^*\mu$ defined by $\alpha^*\mu(S) = \mu(\alpha S)$ is easily seen to be translation-invariant as well. It is known that μ is unique up to scalar, so there is a real number, denoted $|\alpha|$, such that $\alpha^*\mu = |\alpha|\mu$. It turns out that $|\cdot|$ induces the topology that k already has, and that k is complete with respect to $|\cdot|$. Unfortunately, $|\cdot|$ is not always an absolute value. That is, it may not satisfy

1. $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x| \cdot |y|$,
3. $|x + y| \leqslant |x| + |y|$.

However, the only exception is $k = \mathbf{C}$, in which case $|\cdot|$ is the square of the usual absolute value. For any other local field, $|\cdot|$ is an honest absolute value, so we will speak of the "canonical absolute value" on a local field, even though it may not actually be an absolute value.

Local fields have been completely classified. If the strict triangle inequality holds, i.e. $|x + y| \leqslant \sup\{|x|, |y|\}$ for all $x, y \in k$, we say that k is *non-archimedean*. If k is not non-archimedean, we say it is *archimedean*. If k is

archimedean, one can prove that k has characteristic zero, so $\mathbf{Q} \subset k$. The absolute value on k induces one on $\mathbf{Q}$, and it is a theorem that the only archimedean absolute value on $\mathbf{Q}$ is the usual one. Thus $\mathbf{R} \subset k$. It is a general theorem that k can only be locally compact if $[k : \mathbf{R}] < \infty$, from which it follows that either $k = \mathbf{R}$ or $k = \mathbf{C}$.

If k is non-archimedean of characteristic p, then one can prove that $k = \mathbf{F}_q(\!(t)\!)$ for some finite field $\mathbf{F}_q$, where $q = p^r$. If k is non-archimedean of characteristic zero, then once again $\mathbf{Q} \subset k$. It is known (Otrowski's theorem) that the only non-archimedean absolute values on $\mathbf{Q}$ are of the form $|\cdot|_p$ for primes p, where $|x|_p = p^{-v_p(x)}$. Here $v_p : \mathbf{Q}^\times \to \mathbf{Z}$ is the unique homomorphism with $v_p(p) = 1$, $v_p(n) = 0$ for $p \nmid n$. If we write $\mathbf{Q}_p$ for the completion of $\mathbf{Q}$ with respect to $|\cdot|_p$, then k contains some $\mathbf{Q}_p$. Once again a general theorem shows that $[k : \mathbf{Q}_p] < \infty$. To summarize, local fields are one of the following:

- $\mathbf{R}$ or $\mathbf{C}$,
- $\mathbf{F}_q(\!(t)\!)$ for some prime power q,
- finite extension of $\mathbf{Q}_p$.

If k is a non-archimedean local field, we write $\mathfrak{o}_k = \{x \in k : |x| \leqslant 1\}$ and $\mathfrak{p}_k = \{x \in k : |x| < 1\}$. It turns out that $\mathfrak{o}_k$ is a complete discrete valuation ring with maximal ideal $\mathfrak{p}_k$. We denote the residue field by $\kappa_k = \mathfrak{o}_k/\mathfrak{p}_k$. When k is understood, we write $\mathfrak{o}, \mathfrak{p}, \kappa$ instead of $\mathfrak{o}_k, \mathfrak{p}_k, \kappa_k$. Choose a separable closure k^s of k. Because the field k is *henselian* ($|\cdot|$ has a unique extension to k^s), the integral closure $\mathfrak{o}_{k^s}$ of $\mathfrak{o}_k$ in k^s is a local ring (no longer noetherian) and elements of G_k preserve $|\cdot|$. The field $\mathfrak{o}_{k^s}/\mathfrak{p}_{k^s}$ is separably closed, so we get a map $G_k \to G_\kappa$, given by $\sigma \mapsto \bar{\sigma}$, where $\bar{\sigma}(\bar{x}) = \overline{\sigma x}$. The kernel is called the *inertia group* of k, and denoted I_k.

Definition 3.5.2. *A* global field *is either a finite extension of either* $\mathbf{Q}$ *or* $\mathbf{F}_p(t)$ *for some prime* p.

We call finite extensions of $\mathbf{Q}$ *number fields*, and finite extensions of $\mathbf{F}_q(t)$ *function fields*.

A *place* of a global field k is an equivalence class of embeddings $k \hookrightarrow K$, where K is a local field such that the image of k is dense. Two such embeddings are equivalent if they are (topologically) isomorphic over k. We will use the letter v to denote places of k. Traditionally, a place of k is defined to be an equivalence class of valuations – the two definitions are equivalent. Any place v induce a well-defined topology on k, and we will write k_v for the completion of k with respect to this topology. The completion k_v is local. If k_v is non-archimedean, we call v *finite*, otherwise it is *infinite*. For the remainder, let v be a finite place of k.

The absolute value on k_v induces one on k, which we will denote by $|\cdot|_v$. If v is non-archimedean (i.e. k_v is non-archimedean) then we will also use v to denote the valuation on k induced by the canonical valuation on k_v. We will write $\mathfrak{o}_v$, $\mathfrak{p}_v$, κ_v instead of $\mathfrak{o}_{k_v}\ldots$. We can choose $k_v^s \supset k^s$, in which case restriction induces a continuous homomorphism $G_{k_v} \to G_k$. This is injective by Krasner's Lemma. The image is often denoted D_v, and the image of I_{k_v} inside D_v will be written I_v. Note that D_v, as a subgroup of G_k, is only well defined up to conjugacy.

A useful fact about global fields is the *product formula*. Given the canonical absolute value $|\cdot|_v$ associated with a place, we have

$$\prod_v |x|_v = 1.$$

This property actually characterizes global fields – see [AW45]. For more details on local and global fields, see [Wei95].

Let k be a number field. Let $\mathfrak{o}_k$ be the *ring of integers* of k, that is, $\mathfrak{o}_k$ is the integral closure of $\mathbf{Z}$ in k. The ring $\mathfrak{o}_k$ is a dedekind domain. Thus if $\mathfrak{a} \subset \mathfrak{o}_k$ is a nonzero ideal, we have a factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where the $\mathfrak{p}_i \subset \mathfrak{o}_k$ are nonz-zero prime (hence maximal) ideals, and each $e_i \geqslant 1$. This factorization is unique up to reordering if we require that the $\mathfrak{p}_i$ be distinct.

For a prime $\mathfrak{p} \subset \mathfrak{o}_k$, we write (as before) $\kappa_\mathfrak{p} = \mathfrak{o}_k/\mathfrak{p}$ for the *residue field* of $\mathfrak{p}$. The field $\kappa_\mathfrak{p}$ is finite because it is finitely generated (as a ring) over its prime field. There is a unique homomorphism $v_\mathfrak{p} : k^\times \twoheadrightarrow \mathbf{Z}$ such that for $a \in \mathfrak{o}_k \smallsetminus 0$, we have $(a) = \mathfrak{p}^{v_\mathfrak{p}(a)} \cdot \mathfrak{b}$ with $(\mathfrak{b}, \mathfrak{p}) = 1$. This gives us an absolute value

$$|a|_\mathfrak{p} = \begin{cases} 0 & \text{if } a = 0 \\ (\#\kappa_\mathfrak{p})^{-v_\mathfrak{p}(a)} & \text{otherwise.} \end{cases}$$

Completing k with respect to this absolute value, we get a local field $k_\mathfrak{p}$. Our valuation (and absolute value) extend by continuity to a valuation $v_\mathfrak{p} : k_\mathfrak{p}^\times \to \mathbf{Z}$ and absolute value $|\cdot|_\mathfrak{p} : k_\mathfrak{p} \to \mathbf{R}_{\geqslant 0}$. This agrees with our previous definition of the canonical absolute value on a local field.

Let L/k be a finite extension, $\mathfrak{p} \subset \mathfrak{o}_k$ a prime ideal. The ideal $\mathfrak{p}\mathfrak{o}_L$ factors uniquely as $\mathfrak{q}_1^{e(\mathfrak{q}_1/\mathfrak{p})} \cdots \mathfrak{q}_r^{e(\mathfrak{q}_r/\mathfrak{p})}$, where the $\mathfrak{q}_i \subset \mathfrak{o}_L$ are prime. For example, if $L = \mathbf{Q}(i)$, then $2 = -i(1+i)^2$ and $5 = (1+2i)(1-2i)$. One can show that

$$\begin{aligned} 2\mathfrak{o}_L &= ((1+i)\mathfrak{o}_L)^2 \\ 3\mathfrak{o}_L &= 3\mathfrak{o}_L \\ 5\mathfrak{o}_L &= ((1+2i)\mathfrak{o}_L) \cdot ((1-2i)\mathfrak{o}_L) \end{aligned}$$

are prime factorizations in $\mathfrak{o}_L$. One says that $\mathfrak{p}$ is *unramified* in L if $e(\mathfrak{q}_i/\mathfrak{p}) = 1$ for all i. It is an easy theorem that only finitely many primes can ramify.

Now assume L/k is Galois. The action of the galois group $G = \mathrm{Gal}(L/k)$ preserves $\mathfrak{o}_L$, fixing $\mathfrak{o}_k$. This action does *not* preserve ideals in $\mathfrak{o}_L$. In fact, if $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are the primes lying above $\mathfrak{p} \subset \mathfrak{o}_k$, then G acts transitively on $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, from which we see that each $e(\mathfrak{q}_i/\mathfrak{p})$ is the same integer, denoted $e_\mathfrak{p}$. Fix $\mathfrak{q} = \mathfrak{q}_1$. The *decomposition group* of $\mathfrak{q}/\mathfrak{p}$ is

$$D(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/k) : \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

There is a canonical homomorphism $D(\mathfrak{q}/\mathfrak{p}) \to \mathrm{Gal}(\kappa_\mathfrak{q}/\kappa_\mathfrak{p})$ given by "reduce σ modulo $\mathfrak{p}$." This gives us an exact sequence

$$1 \longrightarrow I(\mathfrak{q}/\mathfrak{p}) \longrightarrow D(\mathfrak{q}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(\kappa_\mathfrak{q}/\kappa_\mathfrak{p}) \longrightarrow 1$$

(surjectivity on the right is non-trivial). So the *inertia group* of $\mathfrak{q}/\mathfrak{p}$, denoted $I(\mathfrak{q}/\mathfrak{p})$, is the subgroup of $D(\mathfrak{q}/\mathfrak{p})$ consisting of automorphisms whose action is trivial modulo $\mathfrak{q}$. Choosing $\mathfrak{q} = \mathfrak{q}_i$ for some $i \neq 1$ gives a $D(\mathfrak{q}_i/\mathfrak{p})$ that is conjugate to $D(\mathfrak{q}/\mathfrak{p})$. We will often write $D_\mathfrak{p}$ and $I_\mathfrak{p}$, keeping in mind that they are only well-defined up to conjugacy. We will use the fact that $\#I_\mathfrak{p} = e_\mathfrak{p}$, whence $\mathfrak{p}$ is unramified in L if and only if $I_\mathfrak{p} = 1$.

Choosing $\mathfrak{q}$ lying over $\mathfrak{p}$, we can complete L and k to get an extension $L_\mathfrak{q}/k_\mathfrak{p}$ of local fields. We have seen that restriction gives a map $\mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{p}) \to \mathrm{Gal}(L/k)$. It turns out that this map is an isomorphism onto the image $D(\mathfrak{q}/\mathfrak{p}) \subset \mathrm{Gal}(L/k)$. We'll write $I(L_\mathfrak{q}/k_\mathfrak{p})$ for the inverse image of $I(\mathfrak{q}/\mathfrak{p})$ in $\mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{p})$. It can be defined directly in exactly the same manner as $I(\mathfrak{q}/\mathfrak{p})$.

Passing to the algebraic closure of $k_\mathfrak{p}$, we can consider the absolute Galois group

$$G_{k_\mathfrak{p}} = \varprojlim_{L_\mathfrak{q} \supset k_\mathfrak{p}} \mathrm{Gal}(L_\mathfrak{q}/k_\mathfrak{p})$$

where $L_\mathfrak{q}$ ranges over all finite Galois extensions of $k_\mathfrak{p}$. The group $G_{k_\mathfrak{p}}$ has a distinguished subgroup $I_\mathfrak{p}$, which is the inverse limit

$$I_\mathfrak{p} = \varprojlim_{L_\mathfrak{q}/k_\mathfrak{p}} I(L_\mathfrak{q}/k_\mathfrak{p}).$$

Our exact sequence

$$1 \longrightarrow I_\mathfrak{p} \longrightarrow G_{k_\mathfrak{p}} \longrightarrow \mathrm{Gal}(\overline{\kappa_\mathfrak{p}}/\kappa_\mathfrak{p}) \simeq \hat{\mathbf{Z}} \longrightarrow 1$$

extends to a filtration of $G_{k_\mathfrak{p}}$ by normal closed subgroups whose successive quotients are abelian. Once again, recall that there is a canonical embedding $G_{k_\mathfrak{p}} \hookrightarrow G_k$ via an embedding $\bar{k} \hookrightarrow \overline{k_\mathfrak{p}}$.

3.6 Reduction of abelian varieties

Let $k_\mathfrak{p}$ be a local field. Let $\mathfrak{o}_\mathfrak{p}$ be the ring of integers of $k_\mathfrak{p}$, i.e. $\mathfrak{o}_\mathfrak{p} = \{x \in k_\mathfrak{p} : |x|_\mathfrak{p} \leqslant 1\}$. The ideal $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$ is the unique maximal ideal of $\mathfrak{o}_\mathfrak{p}$, and it turns out that $\mathfrak{p}\mathfrak{o}_\mathfrak{p} = \{x \in k_\mathfrak{p} : |x|_\mathfrak{p} < 1\}$. In an abuse of notation, we write $\mathfrak{p}$ for $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$.

Definition 3.6.1. *We say that a variety X over $k_\mathfrak{p}$ has* good reduction *if there is a smooth proper model $\mathcal{X}$ of X over $\mathfrak{o}_\mathfrak{p}$.*

In other words, we require the existence of a smooth proper scheme $\mathcal{X}$ over $\mathfrak{o}_\mathfrak{p}$ such that the following diagram is cartesian:

$$\begin{array}{ccc} X & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(\mathfrak{o}_k). \end{array}$$

We write $X_\mathfrak{p}$ for $\mathcal{X} \times_{\mathrm{Spec}(\mathfrak{o}_k)} \mathrm{Spec}(\kappa_\mathfrak{p})$, and call $X_\mathfrak{p}$ the *reduction of X modulo $\mathfrak{p}$*.

One can show that if A is an abelian variety over $k_\mathfrak{p}$ with good reduction, then $A_\mathfrak{p}$ is independent of the choice of $\mathcal{A}$, that $\mathcal{A}$ gets the structure of an abelian scheme over $\mathfrak{o}_k$, and that $A_\mathfrak{p}$ is an abelian variety over $\kappa_\mathfrak{p}$.

There is in fact a canonical model for A over $\mathfrak{o}_p$, and it exists in great generality. Let S be a connected dedekind scheme with field of fractions k. If A is an abelian variety over k, one calls a *Néron model* of A a smooth model $\mathcal{A}$ for A over S for which any morphism $X_k \to A$, where X is a smooth scheme over S, has a unique extension to a morphism $X \to \mathcal{A}$. In other words, $\mathcal{A}$ represents the functor $X \mapsto \hom_k(X_k, A)$ from smooth schemes over S to k-varieties. It is clear that $\mathcal{A}$ (if it exists) is unique up to unique isomorphism. Fortunately, it is a theorem (see [BLR90, 1.4.1]) that in our setting (S a connected dedekind scheme and A an abelian variety over k) Néron models always exist. Since the functor $X \mapsto \hom_k(X_k, A)$ that $\mathcal{A}$ represents is naturally group-valued, $\mathcal{A}$ has the structure of a commutative group scheme [BLR90, 1.2.6].

So if $S = \mathrm{Spec}(\mathfrak{o}_k)$ for a number field k and $\mathfrak{p} \subset \mathfrak{o}$ is a prime, we could have said that an abelian variety A over k has good reduction at $\mathfrak{p}$ if the Néron model $\mathcal{A}$ for $\mathfrak{o}_\mathfrak{p}$ (the localization of $\mathfrak{o}$ at $\mathfrak{p}$) is proper as an $\mathfrak{o}_\mathfrak{p}$-scheme.

Example 3.6.2. Let $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbf{Z}$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$. If $p \nmid \Delta$, then $E/\mathbf{Q}_p$ has good reduction, and $E_p/\mathbf{F}_p$ is given by the reduction of our original equation modulo p. ▷

There is a reduction map $A(k_\mathfrak{p}) \to A_\mathfrak{p}(\kappa_\mathfrak{p})$ which is a group homomorphism. It is given as the composite

$$A(k_\mathfrak{p}) = \mathcal{A}(\mathfrak{o}_\mathfrak{p}) \to \mathcal{A}(\kappa_\mathfrak{p}) = A_\mathfrak{p}(\kappa_\mathfrak{p}).$$

To see that $A(k_\mathfrak{p}) = \mathcal{A}(\mathfrak{o}_\mathfrak{p})$, think of A as being a subset of some projective space $\mathbf{P}^N$. For a point $x = (x_0 : \cdots : x_N) \in \mathbf{P}^N(k_\mathfrak{p})$, we can scale x be the denominators of the x_i to get a model $x = (x_0 : \cdots : x_N) \in \mathbf{P}^N(\mathfrak{o}_\mathfrak{p})$. We can even get a model with some $x_i \not\equiv 0 \mod \mathfrak{p}$, and the image of x in $\mathbf{P}^N(\kappa_\mathfrak{p})$ is in $A_\mathfrak{p}(\kappa_\mathfrak{p})$. By Hensel's lemma, the map $A(k_\mathfrak{p}) \to A_\mathfrak{p}(\kappa_\mathfrak{p})$ is a surjection. The kernel is a pro-p group, where p is the characteristic of $\kappa_\mathfrak{p}$. In fact, the kernel is a p-adic Lie group.

We can extend our reduction map to algebraic closures, getting a homomorphism $A(\overline{k_\mathfrak{p}}) \to A_\mathfrak{p}(\overline{\kappa_\mathfrak{p}})$, that has a pro-$p$ kernel. Choose an integer $n \geqslant 2$ with $p \nmid n$. The map ${}_nA(\overline{k_\mathfrak{p}}) \to {}_nA_\mathfrak{p}(\overline{\kappa_\mathfrak{p}})$ is an isomorphism because both groups have the same cardinality ($n^{2\dim A}$) and the kernel is pro-p. In that isomorphism both groups have a Galois action – $G_{k_\mathfrak{p}}$ on the left and $G_{\kappa_\mathfrak{p}} = \hat{\mathbf{Z}}$ on the right. The map is compatible with the Galois action, so in particular, the inertia group $I_\mathfrak{p}$ acts trivially on ${}_nA(\overline{k_\mathfrak{p}})$.

Let $A/k_\mathfrak{p}$ be an abelian variety with good reduction. Recall we had a map $\delta : A(k_\mathfrak{p})/n \hookrightarrow \mathrm{H}^1(k_\mathfrak{p}, {}_nA)$ defined as follows. For $x \in A(k_\mathfrak{p})$, choose $y \in A(\overline{k_\mathfrak{p}})$ such that $n \cdot y = x$. We define the 1-cocycle $\varphi = \delta(x)$ by $\sigma \mapsto \sigma y - y$. For $\sigma \in I_\mathfrak{p}$, the elements σy and y have the same image in $A_\mathfrak{p}(\overline{\kappa_\mathfrak{p}})$, hence $\sigma y - y \in {}_nA(\overline{k_\mathfrak{p}})$ has trivial image modulo $\mathfrak{p}$. It follows that $\sigma y - y = 0$ since it is an n-torsion point that is 0 modulo $\mathfrak{p}$. This tells us that $\varphi(\sigma) = 0$ for all $\sigma \in I_\mathfrak{p}$, i.e. $\varphi(I_\mathfrak{p}) = 0$.

Lemma 3.6.3. *Let A be an abelian variety over a number field k. With the above notation, $\varphi(I_\mathfrak{p}) = 0$ for all $\mathfrak{p} \subset \mathfrak{o}_k$ of good reduction for A.*

Let S be the finite set of primes for which A has bad reduction; we will show that the group

$$\mathrm{H}^1_S(k, {}_nA) = \left\{ [\varphi] \in \mathrm{H}^1(k, {}_nA) : \varphi(I_\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \notin S \right\}$$

is finite.

3.7 Restricted ramification

Let k be a number field, and let S be a finite set of primes of k. We defined, for a G_k-module M, the "cohomology with restricted ramification"

$$\mathrm{H}^1_S(G_k, M) = \left\{ [\varphi] \in \mathrm{H}^1(G, M) : \varphi(I_\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \notin S \right\}.$$

It is better to interpret $\mathrm{H}^1_S(G_k, M)$ in terms of Galois cohomology. First a clarification: $\varphi(I_\mathfrak{p}) = 0$ actually means that $\varphi(I_\mathfrak{p}) = 0$ for *any* choice of $I_\mathfrak{p}$. (Recall that the embeddings $G_{k_\mathfrak{p}} \hookrightarrow G_k$, and hence $I_\mathfrak{p} \hookrightarrow G_k$, are only well-defined up to conjugacy.) One easily checks that, for any $[\varphi] \in \mathrm{H}^1(G_k, M)$, the

set $\ker(\varphi) = \{\sigma : \varphi(\sigma) = 0\}$ is a subgroup of G_k. In other words, if $H \subset G_k$ denotes the (normal) subgroup generated by the $I_\mathfrak{p}$ for $\mathfrak{p} \notin S$, then

$$\mathrm{H}^1_S(G_k, M) = \ker\left(\mathrm{H}^1(G_k, M) \to \mathrm{H}^1(H, M)\right) = \mathrm{H}^1(G_k/H, M^H),$$

the second equality coming from the inflation-restriction sequence.

The normal subgroup of G_k generated by $\bigcup_{\mathfrak{p}\notin S} I_\mathfrak{p}$ is the Galois group of an extension k_S/k. One can prove that whenever L/k is a finite extension unramified away from S, then $L \subset k_S$. We write $G_{k,S} = \mathrm{Gal}(k_S/k) = G_k/G_{k_S}$, and call $G_{k,S}$ a Galois group *with restricted ramification*. In the future, if M is a G_k-module for which the action of G_k on M is unramified away from S, we will write $\mathrm{H}^1(G_{k,S}, M)$ instead of $\mathrm{H}^1_S(G_k, M)$.

$\star$ Just as one can interpret the absolute Galois group G_k as the étale fundamental group $\pi_1(\operatorname{Spec} k)$, the group $G_{k,S}$ is an étale fundamental group via the following result.

Theorem 3.7.1. *Let S be normal connected scheme with function field k. Then the group $\pi_1(S)$ is naturally isomorphic to $\mathrm{Gal}(k_S/k)$, where k_S is the composite of all finite extensions $L \subset k^s$ for which the normalization of S in L is étale over S.*

Proof. See [Sza09, 5.4.9]. □

Let S be a finite set of primes of k, and write $\mathfrak{o}_{k,S} = S^{-1}\mathfrak{o}_k$. A field extension K/k is unramified outside S precisely when the integral closure of $\mathfrak{o}_{k,S}$ inside K is étale over $\mathfrak{o}_{k,S}$. In other words, the above theorem shows that $G_{k,S} = \pi_1(\operatorname{Spec} \mathfrak{o}_{o,S})$. In proving the weak Mordell-Weil theorem, we will need following important finiteness result. $\star$

Theorem 3.7.2. *Let S be a finite set of primes of a number field k. Then $G_{k,S}$ has only finitely many open subgroups of any given index.*

Proof. This is just a rewriting of Theorem 3.7.3. □

Theorem 3.7.3 (Hermite)**.** *Let k be a number field, S a finite set of places of $\mathfrak{o}_k$. For a fixed integer $N \geqslant 1$, there is a finite extension $K \subset \bar{k}$ such that if $L \subset \bar{k}$ is an extension of k unramified outside of S with $[L : k] \leqslant N$, then $L \subset K$. Moreover, the minimal such K is Galois over k and unramified outside S.*

Proof. This follows easily from [BG06, B.2.14]. □

Hermite's theorem has a huge generalization. Call a profinite group G *small* if it has only finitely many open subgroups of any given index. If X is a connected scheme of finite type such that $X \to \operatorname{Spec}(\mathbf{Z})$ has dense image, then $\pi_1(X)$ is small [HH09, 2.8]. This is useful because of the following result.

Theorem 3.7.4. *Let G be a small group. Then $\mathrm{H}^1(G, M)$ is finite for all finite continuous G-modules M.*

Proof. Since M is finite, there is an open normal subgroup $N \subset G$ such that N acts trivially on M. Recall the *inflation-restriction exact sequence* is

$$0 \longrightarrow \mathrm{H}^1(G/N, M^N) \xrightarrow{\inf} \mathrm{H}^1(G, M) \xrightarrow{\mathrm{res}} \mathrm{H}^1(N, M),$$

where the first arrow is $[\varphi] \mapsto [\varphi \circ (G \twoheadrightarrow G/N)]$ on cocycles, and the restriction map is $[\varphi] \mapsto [\varphi|_N]$. The group $\mathrm{H}^1(G/N, M^N)$ is finite because both G/N and $M^N = M$ are finite, and $\mathrm{H}^1(N, M) = \hom_{\mathrm{cts}}(N, M)$ is finite because N is small. □

If we are willing to consider $\mathrm{H}^1(G, M)$ for M non-abelian, then the converse is true.

3.8 Torsion and weak Mordell-Weil

Let A be an abelian variety over a number field k. Recall that we are trying to show that $A(k)$ is finitely generated. We have shown that it is sufficient to prove that the quotient $A(k)/n$ is finite for some $n \geqslant 2$. Once we know that $A(k)$ is finitely generated, we can write $A(k) = A(k)_{\mathrm{tors}} \oplus \mathbf{Z} \cdot x_1 \oplus \cdots \oplus \mathbf{Z}x_r$, where each x_i is of infinite order. The algebraic rank $r = \mathrm{rk}\, A$ is very difficult to compute in general, but $A(k)_{\mathrm{tors}}$ is computable.

For all but finitely many $\mathfrak{p} \subset \mathfrak{o}$, the variety A has good reduction at $\mathfrak{p}$; choose one such prime. We have a reduction map $A(k_{\mathfrak{p}}) \to A_{\mathfrak{p}}(\kappa_{\mathfrak{p}})$, which has pro-$p$ kernel. The group $A(k)_{\mathrm{tors}}$ is contained in $A(k_{\mathfrak{p}})$, so we can think about its image in $A_{\mathfrak{p}}(\kappa_{\mathfrak{p}})$. Since $A(k)_{\mathrm{tors}}$ is finite, the kernel of $A(k)_{\mathrm{tors}} \to A_{\mathfrak{p}}(\kappa_{\mathfrak{p}})$ is a p-group. Pick another prime $\mathfrak{p}'$ of good reduction for A, with residue characteristic $\ell \neq p$. The kernel of the map $A(k)_{\mathrm{tors}} \to A_{\mathfrak{p}}(\kappa_{\mathfrak{p}}) \times A_{\mathfrak{p}'}(\kappa_{\mathfrak{p}'})$ is a p-group and a ℓ-group, hence trivial, i.e. $A(k)_{\mathrm{tors}}$ is a subgroup of $A_{\mathfrak{p}}(\kappa_{\mathfrak{p}}) \times A_{\mathfrak{p}'}(\kappa_{\mathfrak{p}'})$. Incidentally, This gives us a way to compute $A(k)_{\mathrm{tors}}$, because $A_{\mathfrak{p}}(\kappa_{\mathfrak{p}})$ and $A_{\mathfrak{p}'}(\kappa_{\mathfrak{p}'})$ are computable. Indeed, the set $X(\kappa)$ for X any projective variety over any finite field κ is computable for trivial reasons (everything involved is finite!).

Example 3.8.1. Let E be the elliptic curve over $\mathbf{Q}$ given by $y^2 = x^3 + 3$. This has descriminant $\Delta = -2^4 \cdot 3^5$, so E has good reduction away from 2 and 3. We can compute

$$\begin{aligned} E_5(\mathbf{F}_5) &= \{O, (1, \pm 2), (2, \pm 1), (3, 0)\} \\ \#E_7(\mathbf{F}_7) &= 13 \end{aligned}$$

The kernel of $E(\mathbf{Q})_{\mathrm{tors}} \to E_5(\mathbf{F}_5)$ is a 5-group, and the kernel of $E(\mathbf{Q})_{\mathrm{tors}} \to E_7(\mathbf{Q}_7)$ is a 7-group. From this, we know that $E(\mathbf{Q})_{\mathrm{tors}}$ has no points of

order 5 or 7. Thus $E(\mathbf{Q})_{\text{tors}}$ embeds into groups of oder 6 and 13, so it is the trivial group. Since $(1,2) \in E(\mathbf{Q})$ and $E(\mathbf{Q})_{\text{tors}} = 0$, we know that $E(\mathbf{Q})$ is infinite. ▷

Example 3.8.2. Let $E/\mathbf{Q}$ be the curve defined by $y^2 + y = x^3 - x^2 - 10x - 20$. One can check that E has good reduction away from 11. Easy computations yield

p	$\#E_p(\mathbf{F}_p)$
2	5
3	5
5	5
7	10
13	10

This shows us that $E(\mathbf{Q})_{\text{tors}}$ is either 0 or $\mathbf{Z}/5$. In fact, it is the latter with $E(\mathbf{Q})_{\text{tors}} = \langle (5,5) \rangle$. ▷

Let's get back to the weak Mordell-Weil theorem. Let A be an abelian variety over a number field k, and let S be the (finite) set of primes $\mathfrak{p}$ for which A has bad reduction at $\mathfrak{p}$. There are natural maps $\delta : A(k_\mathfrak{p})/n \to \mathrm{H}^1(k_\mathfrak{p}, {}_nA)$, so we get a commutative diagram with exact rows:

$$\begin{array}{ccccc} 0 & \longrightarrow & A(k)/n & \xrightarrow{\delta} & \mathrm{H}^1(k, {}_nA) \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A(k_\mathfrak{p})/n & \xrightarrow{\delta} & \mathrm{H}^1(k_\mathfrak{p}, {}_nA). \end{array}$$

Since A has good reduction outside S, the group $G_{k,S}$ defined in 3.7 acts on ${}_nA$, so we can consider the cohomology group $\mathrm{H}^1(G_{k,S}, {}_nA)$. Moreover, the n-Selmer group $\mathrm{Sel}_n(A)$ sits inside $\mathrm{H}^1(G_{k,S}, {}_nA)$, so $A(k)/n \hookrightarrow \mathrm{Sel}_n(A) \subset \mathrm{H}^1(G_{k,S}, {}_nA)$. The group $\mathrm{Sel}_n(A)$ is a "better approximation" of $A(k)/n$ than $\mathrm{H}^1(G_{k,S}, {}_nA)$, but it is $\mathrm{H}^1(G_{k,S}, {}_nA)$ that we will actually show is finite.

Theorem 3.8.3. *Let A be an abelian variety over a number field k, and let S be the set of places of k at which A has bad reduction. Then the group $\mathrm{H}^1(G_{k,S}, {}_nA)$ is finite.*

Proof. This follows immediately from three facts:

1. ${}_nA(k^s)$ is finite,
2. $G_{k,S}$ is small, and
3. Theorem 3.7.4.

Explicitly, we first choose $L = k({}_nA) \supset k$. Then L/k is unramified outside S and G_L acts trivially on ${}_nA$. Let S' denote the set of places of L lying above S. The inflation-restriction exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathrm{Gal}(L/k), {}_nA) \longrightarrow \mathrm{H}^1(G_{k,S}, {}_nA) \longrightarrow \mathrm{H}^1(G_{L,S'}, {}_nA),$$

reduces the problem to showing that $\mathrm{H}^1(G_{L,S'}, {}_nA) = \hom(G_{L,S'}, {}_nA)$ is finite. So we may as well assume ${}_nA \supset k$ in the first place, and try to prove that $\mathrm{H}^1(G_{k,S}, {}_nA) \simeq \hom(G_{k,S}, (\mathbf{Z}/n)^{\oplus 2d})$ is finite, where $d = \dim A$. For any $f : G_{k,S} \to (\mathbf{Z}/n)^{\oplus 2d}$, the image of f is the Galois group of an extension L/k unramified outside S with $[L : k] \leqslant n^{2d}$. By Hermite's Theorem, there is a fixed finite Galois extension K/k such that all $L \subset K$. Thus $\mathrm{H}^1(G_{k,S}, {}_nA) \hookrightarrow \hom(\mathrm{Gal}(K/k), \mathbf{Z}/n)^{\oplus 2d}$, a finite group. □

There is a geometric interpretation of the Tate-Shafarevich group Ш(A), defined by the exact sequence

$$0 \longrightarrow Ш(A) \longrightarrow \mathrm{H}^1(k, A) \longrightarrow \prod_v \mathrm{H}^1(k_v, A).$$

Recall that a *torsor* of A over k is a nice variety X/k with a simply transitive group action $A \times X \to X$ which is a morphism of k-varieties. In other words, we require $A(L) \times X(L) \to X(L)$ to be a simply transitive group action whenever $X(L) \neq \varnothing$. If $x \in X(L)$, we get an isomorphism $A_L \to X_L$ which is *not* generally defined over k. Two torsors are equivalent if they have compatible group actions (i.e. if they are A-equivariantly isomorphic over k). A torsor is *trivial* if it is equivalent to A with the usual left action. It turns out that a torsor X is trivial if and only if $X(k) \neq \varnothing$. There is a natural bijection

$$\{\text{torsors over } A\}/\text{equivalence} \leftrightarrow \mathrm{H}^1(k, A).$$

Example 3.8.4. Let C/k be a nice curve of genus 1. (It could be that C is not elliptic, for instance if $C(k) = \varnothing$.) Let $E = \mathrm{Jac}\, C$; this is an elliptic curve. There is an isomorphism $C \to \mathrm{Pic}^1_C$ given by $x \mapsto [x]$. The action $\mathrm{Pic}^0_C \times \mathrm{Pic}^1_C \to \mathrm{Pic}^1_C$, induced by $(D_1, D_2) \mapsto D_1 + D_2$, makes C a torsor over E. ▷

3.9 Tate-Shafarevich groups

Let k be a number field, A an abelian variety over k. Recall the Tate-Shafarevich group of A is

$$Ш(A) = \ker\left(\mathrm{H}^1(k, A) \to \prod_v \mathrm{H}^1(k_v, A)\right).$$

The *Weil-Châtelet group* of A, written $\mathrm{WC}(A)$, is the group of torsors over A modulo equivalence. As we have seen, there is a bijection $\mathrm{WC}(A) = \mathrm{H}^1(k, A)$. If k is a number field, then $\mathrm{WC}(A)$ is infinite, but if k is finite then $\mathrm{WC}(A) = 0$. We'll define the map $\mathrm{WC}(A) \to \mathrm{H}^1(k, A)$. Fix an A-torsor X. There exists some L/k with $X(L) \neq \varnothing$. Choose $x \in X(L)$, and define a cocycle $\varphi : G_k \to A(\bar{k})$ by $\sigma \mapsto \sigma x - x$, where $\sigma x - x$ is the unique point $a \in A(\bar{k})$ such that $a + x = \sigma(x)$. The image of X in $\mathrm{H}^1(k, A)$ is the cocycle φ. It isn't too hard to check that this map is well-defined. We can use this bijection to give $\mathrm{WC}(A)$ the structure of an abelian group – alternatively one can put $[S] = [T] + [U]$ if there is a A-equivariant morphism $T \times U \to S$.

This tells us that there is a natural bijection between $Ш(A)$ and the set of torsors X of A/k, such that $X(k_v) \neq \varnothing$ for all places v of k. This can be generalized. Let X/k be a nice variety. We say that X satisfies the *Hasse principle* if $X(k_v) \neq \varnothing$ for all v implies $X(k) \neq \varnothing$. So $Ш(A)$ classifies torsors over A that do not satisfy the Hasse principle. Clearly, if $X(k) \neq \varnothing$, then X satisfies the Hasse principle. Similarly, if $X(k_v) = \varnothing$ for some v, then X satisfies the Hasse principle.

Example 3.9.1 (Selmer)**.** The plane curve $C \subset \mathbf{P}^2_{\mathbf{Q}}$ given by $3x^3+4y^3+5z^3 = 0$ fails the Hasse principle. In other words, $C(\mathbf{Q}_p) \neq \varnothing$ for all p, $C(\mathbf{R}) \neq \varnothing$, but $C(\mathbf{Q}) = \varnothing$. If we let $E = \operatorname{Jac} C$, then we know that $Ш(E) \neq 0$. ▷

It turns out that the Hasse principle can be checked. That is, for a nice variety X over $\mathbf{Q}$ there is an algorithm to determine whether $X(\mathbf{Q}_v) \neq \varnothing$ for all primes. This is because X will have good reduction at all but a finite (computable!) set of primes. If X has good reduction at p with integral model $\mathcal{X}$, then $\mathcal{X}(\mathbf{F}_p) \neq \varnothing$ by the Weil conjectures. Since $\mathcal{X}$ is smooth, Hensel's lemma lets us lift an element of $\mathcal{X}(\mathbf{F}_p)$ to $\mathcal{X}(\mathbf{Z}_p) \subset X(\mathbf{Q}_p)$. For a prime p at which X has bad reduction, we can still pick an integral model $\mathcal{X}$. Either there will be an n for which $\mathcal{X}(\mathbf{Z}/p^n) = \varnothing$, in which case $X(\mathbf{Q}_p) = \varnothing$, or elements of $\mathcal{X}(\mathbf{Z}/p^n)$ for $n \gg 0$ will lift to $X(\mathbf{Z}_p)$. Checking whether $X(\mathbf{R}) = \varnothing$ is easy analysis.

If C is a nice curve of genus zero over a number field, then C satisfies the Hasse principle [Cas67, 3.4]. This is essentially the Hasse-Minkowski theorem.

Example 3.9.2 (descent)**.** Let $E/\mathbf{Q}$ be the elliptic curve defined by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ where the $e_i \in \mathbf{Z}$ are distinct. It's easy to see that ${}_2E = \{0, (e_1, 0), (e_2, 0), (e_3, 0)\} \simeq (\mathbf{Z}/2)^{\oplus 2}$. We use $\{(e_1, 0), (e_2, 0)\}$ as a $\mathbf{F}_2$-basis for ${}_2E$. We have

$$\begin{aligned} \mathrm{H}^1(\mathbf{Q}, {}_2E) &= \hom(G_{\mathbf{Q}}, {}_2E) \\ &= \hom(G_{\mathbf{Q}}, \mathbf{Z}/2)^{\oplus 2} \\ &= \left(\mathbf{Q}^\times/2\right)^{\oplus 2}. \end{aligned}$$

Here, as always, "hom" denotes the group of continuous homomorphisms, and we write $\mathbf{Q}^\times/2$ for $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$. The isomorphism $\hom(G_{\mathbf{Q}}, \mathbf{Z}/2) \simeq \mathbf{Q}^\times/2$ comes from Kummer Theory. Given a homomorphism $\varphi : G_{\mathbf{Q}} \to \mathbf{Z}/2$, the group $\ker(\varphi)$ fixes a field $k = \mathbf{Q}(\sqrt{d})$ with $d \in \mathbf{Q}^\times$. The equivalence class of d in $\mathbf{Q}^\times/2$ depends only on φ. The fact that $\varphi \mapsto d$ is a bijection is a restatement of the main theorem of Kummer Theory.

The boundary morphism in group cohomology gives us a map $\delta : E(\mathbf{Q})/2 \hookrightarrow \mathrm{H}^1(\mathbf{Q}, {}_2E)$. The composite of δ with the isomorphism $\mathrm{H}^1(\mathbf{Q}, {}_2E) \xrightarrow{\sim}) = (\mathbf{Q}^\times/2)^{\oplus 2}$ is quite explicit – we have for $P = (x_0 : x_1 : 1)$:

$$\delta(P) = \begin{cases} (1,1) & \text{if } x = 0 \\ (x_0 - e_1, x_0 - e_2) & \text{if } x_0 \notin \{e_2, e_3\} \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right) & \text{if } x_0 = e_1 \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right) & \text{if } x_0 = e_2. \end{cases}$$

Let S be the set of primes that divide $2(e_1 - e_3)(e_2 - e_3)(e_2 - e_1)$; this contains the set of primes at which E has bad reduction. We know that the group $\mathrm{H}^1(G_{\mathbf{Q},S}, {}_2E)$ is finite. Even better, one can show that it is $\mathcal{H}^{\oplus 2}$, where

$$\mathcal{H} = \left\{ b \in \mathbf{Q}^\times/2 : v_p(b) \equiv 0 \pmod 2 \text{ for } p \notin S \right\}.$$

The group $\mathcal{H}$ is generated by $S \cup \{-1\}$. This allows us to bound the rank of E. We know that $\dim_{\mathbf{F}_2}(\mathcal{H}) \leqslant \#S + 1$, so the fact that $E(\mathbf{Q})/2 \hookrightarrow \mathcal{H}^{\oplus 2}$ implies $\mathrm{rk}(E) \leqslant 2(\#S + 1)$.

We know that $E(\mathbf{Q})/2 \hookrightarrow \mathrm{Sel}_2(E) \subset \mathcal{H}^{\oplus 2}$, so we could get a better bound on $\mathrm{rk}(E)$ if we could compute the image of $\mathrm{Sel}_2(E)$ inside of $\mathcal{H}^{\oplus 2}$. Recall that there is a commutative diagram:

$$\begin{array}{ccccccccc} & & \mathrm{H}^1(G_{\mathbf{Q},S}, {}_2E) & \longrightarrow & \mathrm{H}^1(\mathbf{Q}, E) & & & & \\ & & \uparrow & & \uparrow & & & & \\ 0 & \longrightarrow & E(\mathbf{Q})/2 & \longrightarrow & \mathrm{Sel}_2(E) & \longrightarrow & {}_2Ш(E) & \longrightarrow & 0. \end{array}$$

For a pair $b = (b_1, b_2) \in \mathcal{H}^{\oplus 2}$, we get an element of $\mathrm{H}^1(\mathbf{Q}, E)$. This gives us a torsor X_b of $E/\mathbf{Q}$. Observe that $b \in \mathrm{Sel}_2(E)$ if and only if $X_b(\mathbf{Q}_p) \neq \varnothing$ for all p and $X_b(\mathbf{R}) \neq \varnothing$.

The curve X_b can be computed. We have $X_b \subset \mathbf{P}^3_{\mathbf{Q}}$, a nice curve of genus one defined by

$$\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= (e_2 - e_1) z_0^2 \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= (e_3 - e_1) z_0^2. \end{aligned}$$

▷

Example 3.9.3. Let $E/\mathbf{Q}$ be the elliptic curve $y = x^3 - x = x(x-1)(x+1)$. We'll pick $e_1 = 0$, $e_2 = 1$, $e_3 = -1$. For our curve we have $S = \{2\}$, so $\mathcal{H}$ is the subgroup of $\mathbf{Q}^\times/2$ generated by $\{-1, 2\}$. The group $\mathcal{H}^{\oplus 2}$ has representatives $\{(\pm 1, \pm 1), (\pm 2, \pm 1), (\pm 1, \pm 2), (\pm 2, \pm 2)\}$. We know that for $b = (b_1, b_2) \in (\mathbf{Q}^\times)^2$, the curve X_b is

$$b_1 z_2^2 - b_2 z_2^2 = z_0^2$$
$$b_1 z_1^2 - b_1 b_2 z_3^2 = -z_0^2.$$

Thus $X_b(\mathbf{R}) = \varnothing$ if $b_1 < 0$ and $b_2 > 0$, or if $b_1 > 0$ and $b_2 < 0$. That tells us that $\mathrm{Sel}_2(E) \subset \{(b_1, b_2) \in \mathcal{H}^{\oplus 2} : b_1 b_2 > 0\}$, a group of order eight with representatives $\{\pm(1,1), \pm(2,1), \pm(1,2), \pm(2,2)\}$.

We have

$$0 \longrightarrow E(\mathbf{Q})/2 \xrightarrow{\delta} \mathrm{Sel}_2(E) \hookrightarrow \langle -(1,1), (2,1), (1,2)\rangle.$$

Since ${}_2E \subset E(\mathbf{Q})$, this tells us that $E(\mathbf{Q})/2$ has order at least four. We have $\delta({}_2E) = \{(1,1), (-1,-2), (-1,-1), (1,2)\}$. Consider $b = (2,1)$. Then X_b is

$$2z_1^2 - z_2^2 = z_0^2$$
$$2z_1^2 - 2z_3^2 = -z_0^2.$$

This curve has real points, so we only need to check $X_b(\mathbf{Q}_2)$. As an exercise, show that $X_b(\mathbf{Z}/4) = \varnothing$, which implies $X_b(\mathbf{Q}_2) = \varnothing$, which shows that $b \notin \mathrm{Sel}_2(E)$, and thus $\#E(\mathbf{Q})/2 = 4$. Since $4 = \#({}_2E)$, we know that $\mathrm{rk}(E) = 0$. ▷

3.10 Weil heights

Recall that to prove the Mordell-Weil theorem, we needed the weak Mordell-Weil theorem and a good height function. We gave an extremely terse introduction to heights earlier – here we will do things more carefully.

The idea is as follows. Let X be a nice variety over a number field k. We want a function $H : X(k) \to \mathbf{R}$ that measures the "arithmetic complexity" of a point. For example, $\frac{1}{2}$ and $\frac{100001}{200001}$ are very close in $\mathbf{R}$, but we should think of the latter as being much more "arithmetically complex." We would want H to have properties arising from the geometry of X, and (this is very important), be such that the sets $\{x \in X(k) : |H(x)| \leqslant c\}$ are finite for all c.

Let's start with heights on projective space over $\mathbf{Q}$. Consider a point $x = (x_0 : \cdots : x_n) \in \mathbf{P}^n(\mathbf{Q})$. After scaling by a rational number, we can assume that the $x_i \in \mathbf{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. We set

$$H_{\mathbf{Q}}(x) = \sup\{|x_0|, \ldots, |a_n|\}.$$

It is easy to see that this is well defined, but it doesn't work very well over a general number field. Returning to our example, we have $H_{\mathbf{Q}}\left(\frac{1}{2}:1\right)=2$, while $H_{\mathbf{Q}}\left(\frac{100001}{200001}:1\right)=200001$, which is much larger.

Let k be a number field. Each finite place v of k is associated with a prime $\mathfrak{p}_v \subset \mathfrak{o}=\mathfrak{o}_k$. We set

$$\|a\|_v = |a|_{\mathfrak{p}_v} = \begin{cases} \#(\mathfrak{o}/\mathfrak{p}_v)^{-v_{\mathfrak{p}}(a)} & \text{if } a\neq 0\\ 0 & \text{if } a=0.\end{cases}$$

We call $\|\cdot\|_v$ the canonical absolute value associated with v. If v is a real place of k, i.e. v corresponds with $i:k\hookrightarrow \mathbf{R}$, we set $\|a\|_v=|i(a)|$. Similarly, if v is a place corresponding to an embedding $i:k\hookrightarrow\mathbf{C}$ with dense image, we set $\|a\|_v=|i(a)|^2$. Note that $\|\cdot\|_v$ is *not* an absolute value because it doesn't satisfy the triangle inequality. The following result, briefly touched on in 3.5, is known as the *product formula*.

Theorem 3.10.1. *Let k be a global field. For $a\in k^\times$, we have*

$$\prod_v \|a\|_v = 1.$$

Proof. We'll only look at $k=\mathbf{Q}$. Take $a=\pm\prod_p p^{v_p(a)}\in\mathbf{Q}^\times$. We have $\|a\|_p=p^{-v_p(a)}$ for each p, while $\|a\|_\infty=|a|$. Thus

$$\prod_v \|a\|_v = \|a\|_\infty\cdot\prod_p p^{-v_p(a)} = \prod_p p^{v_p(a)}\cdot\prod_p p^{-v_p(a)} = 1.$$

For general $k/\mathbf{Q}$, one uses the norm map $N:k\to\mathbf{Q}$ to prove the product formula for k. □

For k a general number field, we define $H_k:\mathbf{P}^n(k)\to[1,\infty)$ by

$$H_k(a_0:\cdots:a_n)=\prod_v \sup\left\{\|a_0\|_v,\dots,\|a_n\|_v\right\}.$$

If $k=\mathbf{Q}$ and the $a_i\in\mathbf{Z}$ with $\gcd(a_0,\dots,a_n)=1$, then $\max\{|a_0|_p,\dots,|a_n|_p\}=1$. Thus $H_{\mathbf{Q}}(a_0:\cdots:a_n)=\sup\{|a_0|,\dots,|a_n|\}$. The height H_k is well-defined because of the product formula. For $c\in k^\times$, we have

$$\begin{aligned}\prod_v \sup\{\|ca_0\|_v,\dots,\|ca_n\|_v\} &= \prod_v\|c\|_v\prod_v\sup\{\|a_0\|_v,\dots,\|a_n\|_v\}\\ &= 1\cdot\prod_v\sup\{\|a_0\|_v,\dots,\|a_n\|_v\},\end{aligned}$$

which implies $H_k(ca_0 : \cdots : ca_n) = H_k(a_0 : \cdots : a_n)$. It turns out that for each $c \in \mathbf{R}$, we have

$$\#\{a \in \mathbf{P}^n(k) : H_k(a) \leqslant c\} = O\left(c^{(n+1)[k:\mathbf{Q}]}\right).$$

In particular, the set on the left is finite.

The *absolute height* is a map $H : \mathbf{P}^n(\bar{\mathbf{Q}}) \to [1, \infty)$ is defined by $H(a) = H_k(a)^{[k:\mathbf{Q}]^{-1}}$ for any number field k with $a \in \mathbf{P}^n(k)$. The sets $\{x \in \mathbf{P}^n(\bar{\mathbf{Q}}) : H(a) \leqslant c\}$ can be infinite, but the sets

$$\{x \in \mathbf{P}^n(\bar{\mathbf{Q}}) : H(a) \leqslant c \text{ and } [\mathbf{Q}(x) : \mathbf{Q}] \leqslant d\}$$

are finite. The *logarithmic absolute height* is the map $h = \log H : \mathbf{P}^n(\bar{\mathbf{Q}}) \to [0, \infty)$.

Let X be a nice variety over k. We would like to define a reasonable height function on X. One way to do this is to take an embedding $\phi : X \to \mathbf{P}^n$ (probably for some very large n) and let $h_\phi : X(\bar{k}) \to [0, \infty)$ be the composite $X(k) \xrightarrow{\phi} \mathbf{P}^n(\bar{k}) \xrightarrow{h} [0, \infty)$. We can rephrase this. Let $D \in \mathrm{Div}(X)$ be a very ample divisor. A choice of a generating set for the global sections of $\mathscr{L}(D)$ gives an embedding $\phi_D : X \hookrightarrow \mathbf{P}^n$. We write h_D for the composite $X(\bar{k}) \xrightarrow{\phi_D} \mathbf{P}^n(\bar{k}) \xrightarrow{h} [0, \infty)$. Note that the notation h_D is a little bit misleading, because h_D actually depends on a choice of a generating set for $\mathscr{L}(D)$. If we chose another generating set, getting an embedding ϕ'_D of X into some projective space, then we have $h\phi_D - h\phi'_D = O(1)$, i.e. the two heights differ by a (globally) bounded function $X(\bar{k}) \to \mathbf{R}$. So if we consider h_D as an equivalence class in $\mathbf{R}^{X(\bar{k})}$, then h_D is well-defined. If $E \sim D$ is another very ample divisor, then $h_D - h_E = O(1)$, so the equivalence class of h_D only depends on the class of D in the class group of X. Finally, if $E, D \in \mathrm{Div}(X)$ are very ample, then $h_{D+E} = h_D + h_E + O(1)$. Sometimes we will write $h_{X,D}$ to emphasize the dependence of the height on X.

Theorem 3.10.2 (Weil's "height machine")**.** *Let X be a nice variety over a number field k. Then there exists a unique homomorphism $h : \mathrm{Pic}(X) \to \mathbf{R}^{X(\bar{k})}/O(1)$ such that*

1. *(Normalization). If D is very ample, then $h_D = h \circ \phi_D + O(1)$.*
2. *(Functoriality). For a morphism $\phi : X \to Y$ of nice k-varieties, we have $h_{X,\phi^* D} = h_{Y,D} \circ \phi + O(1)$ for all $D \in \mathrm{Div}(Y)$.*
3. *(Positivity). For all effective D, $h_D \geqslant O(1)$ on the complement of the base locus of D.*

Proof. The existence and uniqueness of h follows easily from the above remarks. For a proof of 2 and 3, see [BG06, 2.3]. □

3.11 Néron-Tate heights

The case we are interested in is when $X = A$ is an abelian variety over k. For $D \in \mathrm{Div}(A)$, one can show (see [Mila, I.5.4]) that $[n]^*D \sim \frac{n(n+1)}{2}D + \frac{n(n-1)}{2}[-1]^*D$. In particular, if D is symmetric (that is, $[-1]^*D = D$) then $[n]^*D \sim n^2 D$. (There are plenty of symmetric divisors: if D is arbitrary, $D + [-1]^*D$ is symmetric). By Theorem 3.10.2, if D is symmetric, we have

$$\begin{aligned} h_{A,D} \circ [n] + O(1) &= h_{A,[n]^*D} + O(1) \\ &= h_{A,n^2 D} + O(1) \\ &= n^2 h_{A,D} + O(1). \end{aligned}$$

So for all $x \in A(\bar{k})$, we have $h_{A,D}(n \cdot x) = n^2 h_{A,D}(x) + O(1)$. In other words, repeated addition gives a quadratic growth in the "complexity" of a point $x \in A(\bar{k})$.

Fix a symmetric divisor $D \in \mathrm{Div}(A)$. Define the *canonical (or Néron-Tate) height* associated to D, as a function $\widehat{h}_D : A(\bar{k}) \to \mathbf{R}$, by

$$\widehat{h}_D(a) = \lim_{n\to\infty} \frac{1}{4^n} h_D(2^n \cdot a).$$

Let's show that the limit defining $\widehat{h}_D$ exists. Our previous discussion shows that $|h_D(2 \cdot x) - 4h_D(x)| \leqslant C$ for some constant C depending only on A and D. We write this as $h_D(2 \cdot x) = 4h_D(X) + O(1)$, keeping in mind that this $O(1)$ only depends on A and D. Note that

$$\frac{h_D(2^i \cdot x)}{4^i} = \frac{h_D(2 \cdot (2^{i-1} \cdot x))}{4^i} = \frac{4h_D(2^{i-1} \cdot x) + O(1)}{4^i} = \frac{h_D(2^{i-1} \cdot x)}{4^{i-1}} + \frac{O(1)}{4^i}.$$

Thus, for any $n > m$, we have

$$\begin{aligned} \left| \frac{h_D(2^n \cdot x)}{4^n} - \frac{h_D(2^m \cdot x)}{4^m} \right| &\leqslant \sum_{i=m+1}^{n} \left| \frac{h_D(2^i \cdot x)}{4^i} - \frac{h_D(2^{i-1} \cdot x)}{4^{i-1}} \right| \\ &= \sum_{i=m+1}^{n} \left| \frac{h_D(2^{i-1} \cdot x)}{2^{i-1}} + \frac{O(1)}{4^i} - \frac{h_D(2^{i-1} \cdot x)}{2^{i-1}} \right| \\ &\leqslant \sum_{i=m+1}^{n} \frac{C}{4^i}, \end{aligned}$$

which shows that $\{4^{-n} h_D(2^n \cdot x)\}_{n=1}^{\infty}$ is a Cauchy sequence. So the limit defining $\widehat{h}_D(x)$ exists. If we set $m = 0$ and let $n \to \infty$, we see that $h_D = \widehat{h}_D + O(1)$.

If D is antisymmetric, we define $\widehat{h}_D(x) = \lim_{n\to\infty} \frac{1}{2^n} h_D(2^n \cdot x)$ The same proof shows that $\widehat{h}_D$ is well-defined. We can extend $\widehat{h}$ to a function $\widehat{h} : \mathrm{Div}(A) \to \mathbf{R}^{A(\bar{k})}$ by setting

$$\widehat{h}_D = \frac{1}{2}\left(\widehat{h}_{D+[-1]^*D} + h_{D-[-1]^*D}\right).$$

It turns out that $\widehat{h}_D$ depends only on the class of $\mathscr{L}(D)$ in $\mathrm{Pic}(A)$, so we will think of $\widehat{h}$ as a function $\widehat{h} : \mathrm{Pic}(A) \to \mathbf{R}^{A(\bar{k})}$.

For $c \in \mathrm{Pic}(A)$, the Néron-Tate height $\widehat{h}_c$ has many nice properties, for example

$$\widehat{h}_c(n \cdot x) = n^2 \widehat{h}_c(x)$$
$$\widehat{h}_c(x+y) + \widehat{h}_c(x-y) = 2\left(\widehat{h}_c(x) + \widehat{h}_c(y)\right).$$

The first is easy to show using properties of Weil heights, and the second is an easy consequence of the following lemma.

Lemma 3.11.1. *Let A be an abelian variety over a number field k, and let $c \in \mathrm{Pic}(A)$. Then the function $\langle \cdot, \cdot \rangle : A(\bar{k}) \times A(\bar{k}) \to \mathbf{R}$ defined by*

$$\langle x, y \rangle = \frac{1}{2}\left(\widehat{h}_c(x+y) - \widehat{h}_c(x) - \widehat{h}_c(y)\right)$$

is bilinear.

Proof. We are trying to prove that for $x, y, z \in A(\bar{k})$, we have

$$\widehat{h}_c(x+y+z) - \widehat{h}_c(x+y) - \widehat{h}_c(z) = \left(\widehat{h}_c(x+z) - \widehat{h}_c(x) - \widehat{h}_c(z)\right) + \left(\widehat{h}_c(y+z) - \widehat{h}_c(y) - \widehat{h}_c(z)\right).$$

This is equivalent to

$$-\widehat{h}_c(x+y+z) + \widehat{h}_c(x+y) + \widehat{h}_c(x+z) + \widehat{h}_c(y+z) - \widehat{h}_c(x) - \widehat{h}_c(y) - \widehat{h}_c(z) = 0. \quad (1)$$

Now we use the fact that for a morphism $f : A \to B$ of abelian varieties, one has $\widehat{h}_{f^*c} = \widehat{h}_c \circ f$. For a finite set S and $\sigma \subset S$, write $\pi_\sigma : A^S = \prod_S A \to A$ for the map $(x_s)_{s\in S} \mapsto \sum_{s\in\sigma} x_s$. With this, we can rewrite equation (1) as

$$\sum_{\sigma \subset \{1,2,3\}} (-1)^{|\sigma|} \widehat{h}_c \circ \pi_\sigma = 0.$$

By the functoriality of $\widehat{h}$, it is enough to show that one has

$$\sum_{\sigma \subset \{1,2,3\}} (-1)^{|\sigma|} \pi_\sigma^* = 0.$$

This is just the "theorem of the cube" (Theorem 3.11.2). □

The basic idea in this proof comes from the proofs of theorems 8.6.11 and 9.2.8 in [BG06].

Theorem 3.11.2. *Let A be an abelian variety over a field k. For any finite set S with $\#S \geqslant 3$, one has*

$$\sum_{\sigma \subset S} (-1)^{|\sigma|} \pi_\sigma^* = 0$$

as a map $\mathrm{Pic}(A) \to \mathrm{Pic}(A^S)$.

Proof. Notation is as in Lemma 3.11.1. For $\#S = 3$ this is just [vdGM13, 2.7]. The general case follows easily by induction. □

Theorem 3.11.3. *Let c be the class of a very ample line bundle. Then $\widehat{h}_c \geqslant 0$ and for all $x \in A(\bar{k})$, $\widehat{h}_c(x) = 0$ if and only if x is torsion.*

Proof. If x is torsion, then for some $n > 1$, we have $n^2 \widehat{h}_c(x) = \widehat{h}_c(nx) = \widehat{h}_c(x)$, which implies $\widehat{h}_c(x) = 0$. On the other hand, if $\widehat{h}_c(x) = 0$, then $\widehat{h}_c(n \cdot x) = 0$ for all n. The set $\{x, 2 \cdot x, 3 \cdot x, \dots\}$ is contained inside $A(L)$, where $L = k(x)$ is the finite extension of k generated by (the coordinates of) x. Thus $\mathbf{N} \cdot x \subset \{a \in A(L) : \widehat{h}_c(a) \leqslant 0\}$, which we know is a finite set. It follows that x is torsion. □

Example 3.11.4. Let $E/\mathbf{Q}$ be an elliptic curve. Then a divisor on E is just a formal sum $\sum_{x \in E} n_x \cdot x$. Of course, E has a canonical point – the origin O, so for each $n \in \mathbf{Z}$, we can consider the Néron-Tate height associated with nO. Since $\widehat{h}_{nO} = n\widehat{h}_O$, we don't lose any information by restricting ourselves to $n = 1$, but since O isn't very ample, we can only directly compute h_{nO} starting with $n = 2$.

For $n = 2$, the Riemann-Roch theorem tells us that $\ell(2O) = 2$, i.e. $\mathrm{H}^0(\mathscr{L}(2O)) = k \oplus kx$, where x is a rational function on E. For E with chosen model $y^2 = x^3 + ax + b$, x the rational function corresponds to the map $E \to \mathbf{P}^1$ given by $(x : y : 1) \mapsto (x : 1)$. Thus $h_{2O}(x : y : 1) = h_{\mathbf{Q}}(x)$.

For $n = 3$, the divisor $3O$ is actually very ample. By the Riemann-Roch theorem, $\ell(3O) = 3$, so $\mathrm{H}^0(\mathscr{L}(3O)) = k \oplus kx \oplus ky$, where $(x : y : 1) : E \to \mathbf{P}^2$ gives a Weierstrass embedding. That is, there exist a, b such that $y^2 = x^3 + ax + b$, and $\phi_{3O} : E \to \mathbf{P}^2$ induces an isomorphism between E and the zero set of $y^2 = x^3 + ax + b$ in $\mathbf{P}^2$. One has $\widehat{h}_{3O}(e) = h_{\mathbf{Q}}(x(e) : y(e) : 1) + O(1)$. ▷

Once again, let c be the class of a symmetric, very ample line bundle on an abelian variety A/k. The function

$$\langle x, y \rangle_c = \frac{1}{2} \left(\widehat{h}_c(x + y) - \widehat{h}_c(x) - \widehat{h}_c(y) \right)$$

is bilinear, and descends to $A(k)/A(k)_{\text{tors}}$. We can even tensor with $\mathbf{R}$ to get a bilinear form on $A(k)_{\mathbf{R}} = A(k) \otimes \mathbf{R}$. The form $\langle \cdot, \cdot \rangle_c$ is positive-definite on $A(k)_{\mathbf{R}}$. Thus $A(k)_{\mathbf{R}}$ with the pairing $\langle \cdot \rangle_c$ is isomorphic to $\mathbf{R}^n$ with the standard inner product, where $n = \operatorname{rk} A$. The group $A(k)/A(k)_{\text{tors}}$ is a lattice in $A(k)_{\mathbf{R}}$, and we can define the *regulator* of A with respect to c to be the square of the volume of the fundamental domain of $A(k)/A(k)_{\text{tors}}$ in $A(k)_{\mathbf{R}}$. That is,

$$\operatorname{Reg}_c(A) = \left| \det \left(\langle x_i, x_j \rangle_c \right)_{i,j} \right|$$

where $\{x_i\}$ is a $\mathbf{Z}$-basis for $A(k)/A(k)_{\text{tors}}$.

If A is an arbitrary abelian variety, there is no natural "good choice" for a canonical divisor on A. On the other hand, if $A = J = \operatorname{Jac} C$ for some nice curve C of genus g with $C(k) \neq \varnothing$, then we can use the induced embedding $j : C \to J$ to define a canonical divisor on J. Let $\Theta = j(C) + \cdots + j(C)$ be the $(g-1)$-fold sum of C in J, and consider Θ as a divisor on J. We call Θ, and the induced class θ in $\operatorname{Pic}(J)$, the *theta-divisor of* J. Note that if $J = E$ is an elliptic curve with origin O, the theta-divisor is just O. It turns out that θ is ample (see [BG06, 8.10.22]), and thus $\langle \cdot, \cdot \rangle_\theta$ is positive-semidefinite. For any $c \in \operatorname{Pic}(J)$ for which $\langle \cdot, \cdot \rangle_c$ is positive-semidefinite, set $|x|_c = \sqrt{\langle x, x \rangle_c} = \widehat{h}_c(x)^{1/2}$. The following result is very deep.

Theorem 3.11.5 (Vojta's inequality)**.** *Let C be a nice curve of genus $g \geqslant 2$ over a number field k. Let $J = \operatorname{Jac}(C)$, and let θ be the theta-divisor on J. Then there are effectively computable constants λ, λ' depending only on C and a chosen $x_0 \in C(\bar{k})$ such that for $x, y \in C \hookrightarrow J$, if $|x|_\theta \geqslant \lambda$ and $|y|_\theta \geqslant \lambda' |x|_\theta$, then*

$$\langle x, y \rangle_\theta \leqslant \frac{3}{4} |x|_\theta \cdot |y|_\theta.$$

Proof. This is hard – see [BG06, 11.9.1]. The constant $\frac{3}{4}$ is not important, as the theorem would hold for any constant in the interval $(g^{-1/2}, 1]$. □

While the following theorem is due to Faltings, our proof is far easier than the original because it rests on deep properties of height functions.

Theorem 3.11.6 (Faltings)**.** *Let C be a nice curve of genus $g \geqslant 2$ over a number field k. Then $C(k)$ is finite.*

Proof. We can assume $C(k) \neq \varnothing$, so the choice of $x_0 \in C(k)$ gives us an embedding $j : C \hookrightarrow J = \operatorname{Jac} C$ defined over k. Let $V = J(k) \otimes_{\mathbf{Z}} \mathbf{R}$. By Mordell-Weil, this is a finite-dimensional vector space, and its rank is just the (algebraic) rank of J. The induced pairing $\langle \cdot, \cdot \rangle_\theta$ on V is now a nondegenerate positive-definite bilinear form, so V is isomorphic as a Hilbert space to $\mathbf{R}^n$

with the standard dot product. Note that by basic properties of heights, S is a discrete subset of V.

For nonzero $u, v \in V$, the *angle* between u and v is the unique number $\varphi(u,v)$ in $[0,\pi]$ satisfying

$$\cos\varphi(u,v) = \frac{\langle u,v\rangle_\theta}{|u|_\theta |v|_\theta}.$$

For a nonzero v and fixed $\alpha \in (0,\pi]$, define the cone $\Gamma_{v,\alpha} = \{u \in V \smallsetminus 0 : \varphi(u,v) < \alpha\}$. This is an open subset of V that is stable under scaling by $\mathbf{R}^+$. Let S be the image of $C(k)$ in $J(k)/J(k)_{\mathrm{tors}} \hookrightarrow V$. Since $J(k)_{\mathrm{tors}}$ is finite, we only need to show that S is finite.

Let $\psi = \frac{1}{2}\cos^{-1}(\frac{3}{4})$, and for nonzero $v \in V$, let $U_v = \Gamma_{v,\psi}$. We claim that $U_v \cap S$ is finite. If it is not, then there exist $x, y \in S \cap U_v$ such that $|x|_\theta > \lambda$ and $|y|_\theta > \lambda' |x|_\theta$. By Vojta's theorem, $\cos\varphi(x,y) \leqslant \frac{3}{4}$, so $\varphi(x,y) \geqslant \cos^{-1}(\frac{3}{4})$. This forces $\varphi(x,u) \geqslant \psi$, a contradiction.

The sets $\{U_v : v \in V \smallsetminus 0\}$ form an open cover of V. Since the unit sphere $\{v \in V : |v| = 1\}$ is compact, there is a finite list $v_1, \dots, v_n \in V$ such that $V = U_{v_1} \cup \cdots \cup U_{v_n}$. Since each $U_{v_i} \cap S$ is finite, the set S is finite. □

This proof gives an effectively computable upper bound for $\#C(k)$. Indeed, since the dimension of V can be bounded above (for instance, by computing certain Selmer groups) it is possible to give an effectively computable upper bound for $\#C(k)$. On the other hand, the set $C(k)$ is not known to be effectively computable, because our proof does *not* give a bound for the heights of points in $C(k)$.

4 Curves and abelian varieties over finite fields

4.1 Motivation from complex analysis

Let's start with some motivation. Let A be an abelian variety of dimension d over $\mathbf{C}$. We have seen that $G = A(\mathbf{C})$ is a compact connected complex Lie group. Moreover, G is a *torus*, i.e. is of the form V/Λ for some complex vector space V and lattice $\Lambda \subset V$. We can realize G as a torus quite explicitly.

Let $\mathfrak{g} = \mathrm{Lie}(G)$ be the Lie algebra of G. Since G is commutative, the exponential map $\exp : \mathfrak{g} \to G$ is a group homomorphism with open image. Since G is connected, the image of $\exp : \mathfrak{g} \to G$ is all of G, and so we have an exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \mathfrak{g} \xrightarrow{\exp} G \longrightarrow 0.$$

There is a natural isomorphism $\Lambda \simeq \mathrm{H}_1(G, \mathbf{Z})$. Indeed, we can identify $\mathfrak{g}$ with the set of one-parameter subgroups of G, and such a subgroup has trivial

exponential if and only if it is of the form $\mathbf{R} \cdot \lambda$ for some $\lambda \in \Lambda$. But those are exactly the one-parameter subgroups that are also closed curves, hence $\Lambda \simeq \mathrm{H}_1(G, \mathbf{Z})$. Alternatively, we can use the pairing $\mathrm{H}_1(G, \mathbf{Z}) \times \mathfrak{g}^\vee \to \mathbf{C}$ given by $\langle \sigma, \omega \rangle = \int_\sigma \omega$ to define $\mathrm{H}_1(G, \mathbf{Z}) \to \mathfrak{g}$, and show that it is an injection with image the kernel of the exponential map.

For any $\phi \in \mathrm{End}(G)$, we have an induced map ϕ_* on $\mathrm{H}_1(G, \mathbf{Z})$. Tensoring with $\mathbf{Q}$, we this gives a representation

$$\mathrm{End}(G) \to \mathrm{End}_{\mathbf{Q}} \mathrm{H}_1(G, \mathbf{Q}) \simeq \mathrm{M}_{2d}(\mathbf{Q}).$$

This lets us take the characteristic polynomial $P_\phi \in \mathbf{Q}[t]$ of ϕ for any $\phi \in \mathrm{End}(G)$. In fact, the degree $2d$ polynomial P_ϕ is an element of $\mathbf{Z}[t]$ because ϕ fixes the lattice $\mathrm{H}_1(G, \mathbf{Z})$ inside $\mathrm{H}_1(G, \mathbf{Q})$.

Since $G = \mathfrak{g}/\Lambda$, we have ${}_nG = \frac{1}{n}\Lambda/\Lambda$, and thus there are natural isomorphisms ${}_nG \simeq \mathrm{H}_1(G, \mathbf{Z}/n)$ for all integers $n \geqslant 2$. In light of this, we will think of ${}_nG$ as a kind of algebraic avatar for $\mathrm{H}_1(G, \mathbf{Z}/n)$. Unfortunately, there is no algebraic analogue of $\mathrm{H}_1(G, \mathbf{Z})$, but there is a good substitute. Let $\widehat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n$ be the profinite completion of $\mathbf{Z}$. The isomorphisms ${}_nG \simeq \mathrm{H}_1(G, \mathbf{Z}/n)$ are compatible, so we get an isomorphism of $\widehat{\mathbf{Z}}$-modules

$$\mathrm{T}G := \varprojlim {}_nG \xrightarrow{\sim} \varprojlim \mathrm{H}_1(G, \mathbf{Z}/n) = \mathrm{H}_1(G, \widehat{\mathbf{Z}}).$$

Since $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$, we will consider $\mathrm{T}G$ only one p-part at a time. This is important because if A is an abelian variety over a field of characteristic $p > 0$, the groups ${}_{p^e}A$ are not well behaved, so the p-part of $\mathrm{T}A = \varprojlim {}_nA$ should be studied differently.

4.2 Tate modules

Let A be an abelian variety of dimension d over an algebraically closed field k. For the moment, we will think of ${}_nA$ as a scheme – namely the fiber product

$$\begin{array}{ccc} {}_nA & \longrightarrow & 0 \\ \downarrow & & \downarrow \\ A & \xrightarrow{\ n\ } & A. \end{array}$$

If n is invertible in k, then we will have ${}_nA \simeq (\mathbf{Z}/n)^{\oplus 2d}$. However, if $n = p$ and k has characteristic p, then for some $r \leqslant d$, there will be an isomorphism of group schemes

$${}_pA \simeq (\mathbf{Z}/p)^r \times \boldsymbol{\alpha}_p^{2(d-r)} \times \boldsymbol{\mu}_p^r.$$

Here $\boldsymbol{\alpha}_p(R) = \{r \in R : r^p = 0\}$ and $\boldsymbol{\mu}_p(R) = \{r \in R : r^p = 1\}$ for any $\mathbf{F}_p$-algebra R. One might hope that ${}_{p^e}A$ can be described just as easily for

$e > 1$, but this is not the case. The group schemes ${}_{p^e}A$ exhibit very complicated behavior as $e \to \infty$. Indeed, their "formal inductive limit" ${}_{p^\infty}A$, called the *Barsotti-Tate group* of A, carries quite a lot of information about A.

For the rest of this section, fix a prime ℓ that is invertible in k. The groups ${}_{\ell^n}A$ come with natural surjections ${}_{\ell^{n+1}}A \to {}_{\ell^n}A$ given by $x \mapsto \ell \cdot x$.

Definition 4.2.1. *Let A be an abelian variety. The* ℓ-adic Tate module of A *is*

$$\mathrm{T}_\ell A = \varprojlim {}_{\ell^n}A = \{(a_1, a_2, \dots) : a_n \in {}_{\ell^n}A \text{ and } \ell x_{n+1} = x_n\}.$$

The group $\mathrm{T}_\ell A$ is a free $\mathbf{Z}_\ell$-module of rank $2d$. We write $\mathrm{V}_\ell A$ for $\mathrm{T}_\ell(A) \otimes \mathbf{Q}$; this is a $\mathbf{Q}_\ell$-vector space of dimension $2d$. We have the following list of analogies:

analytic	algebraic
complex torus A	abelian variety A
$\mathrm{H}_1(A, \mathbf{Z}/n)$	${}_nA$
$\mathrm{H}_1(A, \mathbf{Z}_\ell)$	$\mathrm{T}_\ell A$
$\mathrm{H}_1(A, \mathbf{Q}_\ell)$	$\mathrm{V}_\ell A$

Two things act on $\mathrm{T}_\ell A$. The ring $\mathrm{End}(A)$ of endomorphisms of A (as an abelian variety) defined over k acts on each ${}_{\ell^n}A$, and hence on T_ℓ and V_ℓ. Also, the group $G_k = \mathrm{Gal}(\bar{k}/k)$ acts compatibly on each ${}_{\ell^n}A$, so we get a representation

$$\rho_{A,\ell} : G_k \to \mathrm{GL}(\mathrm{T}_\ell A) \simeq \mathrm{GL}(2d, \mathbf{Z}_\ell).$$

The action of $\mathrm{End}(A)$ and G_k commute, so we actually have a representation $\mathrm{End}(A)[G_k] \to \mathrm{M}_{2d}(\mathbf{Z}_\ell)$. We could also write this as $G_k \to \mathrm{Aut}_{\mathrm{End}(A) \otimes \mathbf{Z}_\ell}(\mathrm{T}_\ell A)$.

Theorem 4.2.2 (Faltings)**.** *Let A, B be abelian varieties over a finitely generated field k. Then the natural map*

$$\hom_k(A, B) \otimes \mathbf{Q}_\ell \to \hom_{\mathbf{Q}_\ell[G_k]}(\mathrm{V}_\ell A, \mathrm{V}_\ell B)$$

is an isomorphism.

It follows that the functor $\mathrm{V}_\ell : \mathsf{AbVar}_k \otimes \mathbf{Q}_\ell \to \mathsf{Rep}_{\mathbf{Q}_\ell}(G_k)$ is fully faithful.

Corollary 4.2.3. *Abelian varieties A, B over a finitely generated field k are isogeneous if and only if $\mathrm{V}_\ell A$ and $\mathrm{V}_\ell B$ are isomorphic as $\mathbf{Q}_\ell[G_k]$-modules.*

⋆ Define the "global Tate module" of A to be

$$\mathrm{T}A = \prod_p \mathrm{T}_p A.$$

This is a $\widehat{\mathbf{Z}}$-module that is isomorphic (if k has characteristic zero) to $\widehat{\mathbf{Z}}^{2d}$. It turns out that TA, as a G_k-module, has a natural interpretation in terms of

étale fundamental groups. Suppose k has characteristic zero (in characteristic $p > 0$, we have to be careful about $\mathrm{T}_p A$). If $U \to A_{\bar{k}}$ is an étale cover of $A_{\bar{k}} = A \times_k \operatorname{Spec}(\bar{k})$, then it turns out that U can be given the structure of an abelian variety in such a way that $U \to A_{\bar{k}}$ is an isogeny. We can use a polarization of $A_{\bar{k}}$ to majorize $U \to A_{\bar{k}}$ by an isogeny $A_{\bar{k}} \to A_{\bar{k}}$, which is multiplication by some integer $n \geqslant 1$. It follows that $\pi_1(A_{\bar{k}}) \simeq \mathrm{T}A$, though see [vdGM13, 10.37] for an actual proof. The standard exact sequence for fundamental groups:

$$1 \longrightarrow \pi_1(A_{\bar{k}}) \longrightarrow \pi_1(A) \longrightarrow G_k \longrightarrow 1,$$

together with a section $G_k \to \pi_1(A)$ coming from $0 \in A(k)$, induces a representation $\rho : G_k \to \operatorname{Aut}(\pi_1(A_{\bar{k}}))$. This is exactly the action of G_k on $\mathrm{T}A$, so that we get a canonical isomorphism

$$\pi_1(A) \simeq G_k \ltimes_\rho \mathrm{T}A.$$

In particular, for each prime ℓ invertible in k, we have an isomorphism $\pi_1(A)^{(\ell)} \simeq \mathrm{T}_\ell A \ltimes_{\rho_{A,\ell}} G_k$, where $(-)^{(\ell)}$ denotes taking pro-ℓ completion. $\star$

It is possible to define the ℓ-adic representation $\rho_A : G_k \to \mathrm{GL}(2d, \mathbf{Z}_\ell)$ without introducing Tate modules. This is the way that things were done "pre-Tate." Let ${}_{\ell^\infty}A = \bigcup_{n \geqslant 1} {}_{\ell^n}A$. As an abelian group, ${}_{\ell^\infty}A \simeq {}_{\ell^\infty}(\mathbf{Q}/\mathbf{Z})$, which we denote by $\mathbf{Z}(\ell^\infty)$ (such groups are called quasi-cyclic). It is easy to show that $\operatorname{End}\mathbf{Z}(\ell^\infty) \simeq \mathbf{Z}_\ell$ as topological rings, where $\operatorname{End}\mathbf{Z}(\ell^\infty)$ is given the subset topology in $\prod_{\mathbf{Z}(\ell^\infty)} \mathbf{Z}(\ell^\infty)$ and $\mathbf{Z}(\ell^\infty)$ has the discrete topology. Thus $\operatorname{Aut}_{\ell^\infty} A \simeq \mathrm{GL}(2d, \mathbf{Z}_\ell)$. The induced homomorphism $G_k \to \mathrm{GL}(2d, \mathbf{Z}_\ell)$ is continuous, and (after a change of basis) is the same as $\rho_{A,\ell}$.

4.3 Endomorphisms of abelian varieties

Let A be an abelian variety of dimension $d \geqslant 1$ over a field k, and fix a polarization $\lambda : A \to A^\vee = \mathrm{Pic}^\circ_A$.

Definition 4.3.1. *An abelian variety A is* simple *if the only abelian subvarieties of A defined over k are 0 and A.*

Note that this definition depends on k; it is possible for a simple variety to become non-simple after base change. We say A is *geometrically simple* if A_L is simple for all fields $L \supset k$ (equivalently, if $A_{\bar{k}}$ is simple).

Theorem 4.3.2 (Poincaré)**.** *If $B \subset A$ is a nontrivial abelian subvariety, then there is another abelian subvariety $C \subset A$ such that the morphism $B \times C \to A$, $(b, c) \mapsto b + c$, is an isogeny.*

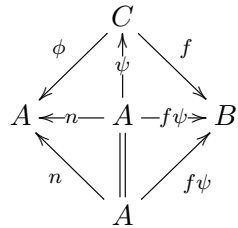
Proof. This is taken from [Mila, I.10.1]. Let $i : B \hookrightarrow A$ be the inclusion, and let $i^\vee : A^\vee \to B^\vee$ be its dual map. Let $C = \ker(i^\vee \circ \lambda)^\circ$ be the connected component of the identity in the kernel of $A \xrightarrow{\lambda} A^\vee \xrightarrow{i^\vee} B^\vee$. Since dimension is additive on exact sequences of abelian varieties, we see that $\dim C \geqslant \dim A - \dim B^\vee = \dim A - \dim B$. It turns out that $(\lambda \circ i^\vee)|_B$ is a polarization of B, so $B \cap C$ is finite, hence dimension zero. It follows that $B \times C \to A$ is an isogeny. □

There need not be a complement to B "one the nose." That is, there may not exist C such that $A \simeq B \times C$. So the category of all abelian varieties is not semisimple, but the category of "abelian varieties up to isogeny" is. The theorem of Poincaré implies that for any abelian variety A, there exist simple abelian varieties $B_1, \dots, B_r$ such that A is isogenous to $B_1 \times \cdots \times B_r$. Standard arguments show that this decomposition is unique up to ordering and isogeny.

Denote by $\mathsf{AbVar}_k^{\mathrm{iso}}$ the localisation of the category of abelian varieties over k by the collection of all isogenies. Morphisms from A to B in $\mathsf{AbVar}_k^{\mathrm{iso}}$ are (equivalence classes) of formal factorizations

$$A \xleftarrow{\phi} C \xrightarrow{f} B.$$

where ϕ is an isogeny. From [vdGM13, 5.12], there exists an integer n and an isogeny $\psi : A \to C$ such that $\phi\psi = n$. The commutative diagram:



shows that the factorization $f \circ \phi^{-1}$ is equivalent to $(f\psi) \circ n^{-1}$. It follows that $\mathsf{AbVar}_k^{\mathrm{iso}}$ is equivalent to the localisation of AbVar_k at all isogenies of the form $A \xrightarrow{n} A$. Thus

$$\hom_{\mathsf{AbVar}_k^{\mathrm{iso}}}(A, B) = \hom_{\mathsf{AbVar}_k}(A, B) \otimes \mathbf{Q}.$$

Write $\mathrm{End}(A) = \hom_{\mathsf{AbVar}_k}(A, A)$ for ring of endomorphisms of A as an abelian variety over k. If $n \circ f = 0$ for some $f : A \to A$, then the image of f is contained in the (discrete) subvariety ${}_nA \subset A$. Since $f(A)$ is irreducible, we have $f = 0$. Thus $\mathrm{End}\, A$ is torsion-free, so it embeds into the ring

$$\mathrm{End}^\circ A = \mathrm{End}_{\mathsf{AbVar}_k^{\mathrm{iso}}}(A) = \mathrm{End}(A) \otimes \mathbf{Q}.$$

Since $\mathrm{End}^\circ A$ can be defined in terms of the category $\mathsf{AbVar}_k^{\mathrm{iso}}$, it only depends on the isogeny class of A. In particular, an isogeny $f : A \to B$ induces an isomorphism $\mathrm{End}^\circ A \xrightarrow{\sim} \mathrm{End}^\circ B$. There is an obvious inclusion $\mathrm{End}^\circ(A)^\times \supset \mathrm{Aut}(A)$, and $f \in \mathrm{End}^\circ(A)^\times$ if and only if nf is an isogeny for some n.

The group $\mathrm{End}(A)$ has rank at most $(2g)^2$. Over $\mathbf{C}$, this is obvious, given the faithful action of $\mathrm{End}(A)$ on $\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z}) \simeq \mathbf{Z}^{2g}$. The general case in characteristic zero follows from the Lefschetz principle, or one can prove it directly as in [Mum08, IV.18.3].

Poincaré's reducibility theorem shows that an abelian variety A is isogenous to a product $B_1^{e_1} \times \cdots \times B_r^{e_r}$, where the B_i are simple and pairwise non-isogenous over k. A standard argument (which works in any semisimple abelian category) shows that the rings $D_i = \mathrm{End}^\circ(B_i)$ are division algebras, and moreover

$$\mathrm{End}^\circ(A) \simeq \prod_{i=1}^{r} M_{e_i}(D_i).$$

Thus the ring $\mathrm{End}^\circ(A)$ is semisimple, so we know that both the e_i and the D_i are uniquely determined by A. It follows that the decomposition type of A can be inferred from the ring $\mathrm{End}^\circ(A)$.

Example 4.3.3. If A is two-dimensional, then A is either simple or a product of elliptic curves. If A is simple, then $\mathrm{End}^\circ(A)$ is a division algebra. If A is isogenous to $E \times E'$ where E and E' are not isogenous, then $\mathrm{End}^\circ(A) \simeq \mathrm{End}^\circ(E) \times \mathrm{End}^\circ(E')$. On the other hand, if A is isogenous to $E \times E$, then $\mathrm{End}^\circ(A) \simeq \mathrm{M}_2(\mathrm{End}^\circ(E))$. ▷

4.4 Frobenius morphisms

We have remarked several times that there is no good "algebraic definition" of $\mathrm{H}_1(X, \mathbf{Q})$ for varieties X over a general field. Serre gave an example of a variety over $\overline{\mathbf{F}}_p$ which shows not only that there isn't a good definition, but that such an homology group cannot exist.

First, we need to discuss Frobenius morphisms. Let p be a prime, q a power of p, and $\mathbf{F}_q$ the field with q elements. Let X be a nice variety over $\mathbf{F}_q$. Choose an embedding $X \hookrightarrow \mathbf{P}^n_{\mathbf{F}_q}$. Write $\mathrm{Fr}_X = \mathrm{Fr}_{X,q} : X \to X$ for the map that on projective coordinates is

$$(a_0 : \cdots : a_n) \mapsto (a_0^q : \cdots : a_n^q).$$

This is well-defined because $x \mapsto x^q$ is a ring homomorphism on $\mathbf{F}_q$-algebras. So if X is the zero-set of homogeneous polynomials $f_i \in \mathbf{F}_q[x_0, \ldots, x_n]$ and $a \in X$, then

$$f_i(a_0^q : \cdots : a_n^q) = f_i(a_0 : \cdots : a_n)^q = 0,$$

so $\mathrm{Fr}_X(a) \in X$. Note that we have to raise to the q-th power rather than the p-th power because $x \mapsto x^p$ does not fix all elements of $\mathbf{F}_q$.

There is a scheme-theoretic definition of Fr_X that allows us to talk about the Frobenius on arbitrary schemes over $\mathbf{F}_q$. For a scheme X over $\mathbf{F}_q$, let $\mathrm{Fr}_X : X \to X$ be the the identity on the underlying topological space of X, with $\mathrm{Fr}_X^* : \mathscr{O}_X \to \mathscr{O}_X$ the map $x \mapsto x^q$. If X is a quasi-projective variety, it is easy to see that our two different definitions of Fr_X are equivalent.

It may seem confusing that the scheme-theoretic Frobenius is the identity on points, while our coordinate-wise definition raises elements to the q-th power. Actually, there is no contradiction. A point $x \in X$ with coordinates in $\mathbf{F}_{q^n}$ should be thought of as a map $x : \mathrm{Spec}(\mathbf{F}_{q^n}) \to X$. Raising those coordinates to the q-th power corresponds to composing x with Fr_X, or, equivalently, precomposing x with the automorphism $x \mapsto x^q$ of $\mathbf{F}_{q^n}$.

Example 4.4.1 (Serre)**.** Choose a prime $p \equiv 3 \pmod 4$. Let $E/\overline{\mathbf{F}}_p$ be the elliptic curve $y^2 = x^3 - x$. It is possible to give an explicit description of the division ring $D = \mathrm{End}^\circ(E)$. Fix $\alpha \in \mathbf{F}_{p^2}$ such that $\alpha^2 = -1$. Then $\phi : E \to E$, defined by $(x, y) \mapsto (-x, \alpha y)$, is a well-defined endomorphism. One has $\phi^2(x, y) = (x, -y)$, so $\phi^2 = -1$ in D. Write Φ for the base-change of the Frobenius morphism on the elliptic curve $y^2 = x^3 - x$ over $\mathbf{F}_p$ to $\overline{\mathbf{F}}_p$. We have

$$\Phi\phi(x, y) = (-x^p, \alpha^p y^p) = -(-x^p, \alpha^p y^p) = -\phi\Phi(x, y),$$

so $\phi\Phi = -\Phi\phi$ in D. It turns out that $\Phi^2 = -p$ (see Example 4.5.3), so D is the standard quaternion algebra with parameters $(-1, -p)$, i.e.

$$D = \mathbf{Q}\left\langle i, j, k : i^2 = -1, j^2 = -p, ij = k, ji = -k \right\rangle.$$

▷

Now we can show that "$V = \mathrm{H}_1(E, \mathbf{Q})$" cannot exist. If it did, we would expect it to be functorial in E, so there would be an action of D on V. But we would also want V to be two-dimensional over $\mathbf{Q}$. Since D is four-dimensional over $\mathbf{Q}$, this would mean that V has D-dimension $1/2$, which is nonsense. Alternatively, we would have an (injective) ring homomorphism $D \to \mathrm{End}(V) \simeq \mathrm{M}_2(\mathbf{Q})$. Since both rings have the same dimension, this would yield $D \simeq \mathrm{M}_2(\mathbf{Q})$. But $\mathrm{M}_2(\mathbf{Q})$ has zero-divisors and D does not, so this cannot be the case.

Let A and B be abelian varieties over a field k. If $f : A \to B$ is an isogeny, the *degree* of f is $[k(A) : k(B)]$ via the embedding $f^* : k(B) \to k(A)$ induced by f. Equivalently, $\deg(f)$ is the order of $\ker(f)$, considered as a group scheme. The extension $k(B)/k(A)$ is separable if and only if f is étale, if and only if $\ker(f)$ is étale over k. If f is étale, then the scheme-theoretic order of $\ker(f)$ is equal to $\#\ker(f)(\bar{k})$.

Example 4.4.2. Let $n \neq 0$, and consider the isogeny $[n] : A \to A$ that is multiplication by n. One can show that $\deg[n] = n^{2d}$, where $d = \dim A$. To see this, note that ${}_nA = \ker[n] \simeq (\mathbf{Z}/n)^{\oplus 2d}$, at least if $n \in k^\times$. ▷

Example 4.4.3. If A is defined over a finite field $\mathbf{F}_q$, let $\mathrm{Fr} = \mathrm{Fr}_A : A \to A$ be the Frobenius. With some difficulty, one can show that Fr_A is purely inseparable (i.e. $k(A)/\mathrm{Fr}^* k(A)$ is purely inseparable) of degree q^d. Alternatively, $\ker(\mathrm{Fr})(\bar{k}) = 0$, so $\ker(f)$ is "as far from étale as possible." ▷

Define a map $\deg : \mathrm{End}(A) \to \mathbf{Z}$ as follows. If f is an isogeny, let $\deg(f)$ be as above. If f is not an isogeny, set $\deg(f) = 0$. Given $f, g \in \mathrm{End}(A)$, one has $\deg(fg) = \deg(f) \cdot \deg(g)$. If one of f, g is not an isogeny this is obvious, and if they are both isogenies, this follows from the multiplicativity of the degree of field extensions. As a special case, $\deg(nf) = n^{2d} \deg(f)$. Using the multiplicativity of the degree map, we can extend it to $\deg : \mathrm{End}^\circ(A) \to \mathbf{Q}$ by $\deg(f/n) = \deg(f)/n^{2d}$. The degree map is *not* additive.

Theorem 4.4.4. *Let A be an abelian variety of dimension d. Then the map $\deg : \mathrm{End}^\circ(A) \to \mathbf{Q}$ is a homogeneous polynomial of degree $2d$.*

By this we mean the following. Choose a $\mathbf{Q}$-basis $e_1, \ldots, e_r$ of $\mathrm{End}^\circ(A)$. The theorem claims that there is a homogeneous polynomial $f \in \mathbf{Q}[x_1, \ldots, x_r]$ of degree $2d$ such that

$$\deg(c_1 e_1 + \cdots + c_r e_r) = f(c_1, \ldots, c_r).$$

It follows that for any $\alpha \in \mathrm{End}(A)$, there exists a unique polynomial $P_\alpha \in \mathbf{Q}[x]$, called the *characteristic polynomial* of α, such that $P_\alpha(n) = \deg(n - \alpha)$ for all $n \in \mathbf{Z}$. It turns out that the polynomial P_α is monic, has degree $2d$, and has integer coefficients.

Example 4.4.5. Let k be an imaginary quadratic field, $\mathfrak{o} = \mathfrak{o}_k$, and let $E = \mathbf{C}/\mathfrak{o}$. One has $\mathrm{End}(E) = \mathfrak{o}$ and $\mathrm{End}^\circ(E) = k$. It turns out that the degree map $\deg : k \to \mathbf{Q}$ is the classical norm map $\mathrm{N}_{k/\mathbf{Q}}$. More generally, let T be a complex torus, written $\mathbf{C}^d/\Lambda$. Let α be an endomorphism of T. We can lift α to a linear map $\widetilde{\alpha} : \mathbf{C}^d \to \mathbf{C}^d$. One has

$$\mathrm{End}(A) = \{\phi \in \mathrm{End}_{\mathbf{C}}(\mathbf{C}^d) : \phi(\Lambda) \subset \Lambda\}.$$

Note that $\Lambda = \mathrm{H}^1(T, \mathbf{Z})$. It is straightforward to check that

$$\deg(\alpha) = \#\ker(\alpha) = \#(\Lambda/\widetilde{\alpha}\Lambda) = \det(\widetilde{\alpha}, \mathrm{H}_1(T, \mathbf{Z})) = \det(\alpha_*, \mathrm{H}_1(T, \mathbf{Z})).$$

Since $\deg(n - \alpha) = \det(n \cdot 1 - \alpha_*, \mathrm{H}_1(T, \mathbf{Z}))$ for all n, we conclude that$P_\alpha = \det(t \cdot 1 - \alpha_*, \mathrm{H}_1(T, \mathbf{Z}))$. ▷

Recall the Tate module $\mathrm{T}_\ell A$ as in Definition 4.2.1. To make our analogy between $\mathrm{T}_\ell A$ and $\mathrm{H}_1(A, \mathbf{A}_\ell)$ precise, we have the following theorem:

Theorem 4.4.6. *There is a natural isomorphism* $\mathrm{T}_\ell A = \mathrm{H}^1(A_{\text{ét}}, \mathbf{Z}_\ell)^\vee$.

Proof. This is essentially a tautology. By [Del77, II.2.4], for lisse ℓ-adic sheaves $\mathscr{F}$ on A one has $\mathrm{H}^\bullet(A, \mathscr{F}) = \mathrm{H}^\bullet(\pi_1(A), \mathscr{F}_0)$, where $\mathscr{F}_0$ is the stalk of $\mathscr{F}$ at 0. By [vdGM13, 10.37], we know that $\pi_1(A) = \mathrm{T}(A)$. For $\mathscr{F} = \mathbf{Z}_\ell$, this gives $\mathrm{H}^1(A_{\text{ét}}, \mathbf{Z}_\ell) = \hom(\mathrm{T}A, \mathbf{Z}_\ell) = (\mathrm{T}_\ell A)^\vee$. □

Theorem 4.4.7. *Let ℓ be a prime invertible in k. For any $\alpha \in \mathrm{End}(A)$, we have $P_\alpha = \det(t \cdot 1 - \alpha_*, \mathrm{T}_\ell A)$.*

Proof. This is nontrivial. See [Mila, I.10.20]. □

Corollary 4.4.8. *For $\alpha \in \mathrm{End}^\circ(A)$, we have $P_\alpha(\alpha) = 0$.*

Proof. We use the fact [Mila, I.10.15] that the natural map

$$\mathrm{End}(A) \otimes \mathbf{Z}_\ell \to \mathrm{End}_{\mathbf{Z}_\ell}(\mathrm{T}_\ell A)$$

is injective. In $\mathrm{End}(\mathrm{T}_\ell A)$, we have $P_\alpha(\alpha) = 0$ by the Cayley-Hamilton theorem. Injectivity tells us that $P_\alpha(\alpha) = 0$ in $\mathrm{End}(A) \otimes \mathbf{Z}_\ell$, and since $\mathrm{End}(A)$ is torsion-free, we see that $P_\alpha(\alpha) = 0$ in $\mathrm{End}(A)$. □

From the theorem, we see that the characteristic polynomial of α acting on $\mathrm{T}_\ell A$ is in $\mathbf{Z}[t]$, and is independent of ℓ. This is highly non-obvious. Note that $A \mapsto \mathrm{T}_\ell A$ is a functor from abelian varieties over k to $\mathbf{Z}_\ell$-representations of G_k. If k has characteristic p and we want to assign a p-adic representation of G_k to an abelian variety, we have to work harder. Of course, $\mathrm{T}_p A$ is a $\mathbf{Z}_p$-module with a G_k-action, but there examples when $\mathrm{rk}_{\mathbf{Z}_p} \mathrm{T}_p A < 2 \dim A$. In this case, instead of studying $\mathrm{T}_p A$, (essentially the p-adic étale cohomology of A) one should study the crystalline or rigid cohomology of A. If the base field k is perfect, these yield $W(k)$-modules with the "correct" rank. For a brief survey of crystalline cohomology, see [Ill94], and for an introduction to rigid cohomology, see [LS07].

4.5 Characteristic polynomial of Frobenius

Let A be an abelian variety over $\mathbf{F}_q$, where q is a power of p. For example, A could be the jacobian of a smooth curve. Recall that there is a distinguished endomorphism $\mathrm{Fr} = \mathrm{Fr}_A$ of A, called the Frobenius of A. If we embed A into some projective space $\mathbf{P}^n$, then in coordinates we have $\mathrm{Fr}(x_0 : \cdots : x_n) = (x_0^q : \cdots : x_n^q)$. As a morphism of schemes, Fr is the identity on the underlying space of A, and is the q-th power map on $\mathscr{O}_A$. Let $d \geqslant 1$ be the dimension of A.

Recall that there is a polynomial $P_A = P_{\mathrm{Fr}_A} \in \mathbf{Z}[t]$ of degree $2d$ such that $P_A(n) = \deg(n - \mathrm{Fr}_A)$ for all integers n. Also, if ℓ is a prime not dividing q, P_A is the characteristic polynomial of Fr_* as a $\mathbf{Z}_\ell$-linear map $\mathrm{Fr}_* : \mathrm{T}_\ell A \to \mathrm{T}_\ell A$. Thus we have a map $P : \mathsf{AbVar}_{\mathbf{F}_q} \to \mathbf{Z}[t]$.

Theorem 4.5.1. *If A and B are isogenous abelian varieties over $\mathbf{F}_q$, then $P_A = P_B$.*

Proof. Let $f : A \to B$ be an isogeny. For each e, we have an exact sequence

$$0 \longrightarrow C \longrightarrow {}_{\ell^e}A \xrightarrow{f} {}_{\ell^e}A \longrightarrow 0,$$

where C is independent of e if $e \gg 1$ (since $C \subset \ker(f)$, a finite group). At the level of Tate modules, if $f_*(x) = 0$, then $f(x_i) = 0$ in ${}_{\ell^i}B$ for all i, so each $x_i \in C$. But C is a finite group, so it contains no nonzero sequences (x_i) with $\ell x_{i+1} = x_i$ for all i. Thus $x = 0$, so $f_* : \mathrm{T}_\ell A \to \mathrm{T}_\ell B$ is injective. Since $\mathrm{T}_\ell A$ and $\mathrm{T}_\ell B$ have the same rank, the map $f_* : \mathrm{V}_\ell A \to \mathrm{V}_\ell B$ is an isomorphism. (So far we have shown that $\mathrm{V}_\ell A$ is isogeny-invariant over any field.) It is easy to check that $f \circ \mathrm{Fr}_A = \mathrm{Fr}_B \circ f$. It follows that $f_* \circ (\mathrm{Fr}_A)_* = (\mathrm{Fr}_A)_* \circ f$, and from this we see that $P_A = P_B$. □

Alternatively, we could note that $\mathrm{T}_\ell : \mathsf{AbVar}_k \to \mathsf{Rep}_{\mathbf{Z}_\ell}(G_k)$ naturally descends to a functor $\mathrm{V}_\ell : \mathsf{AbVar}_k \otimes \mathbf{Q} \to \mathsf{Rep}_{\mathbf{Z}_\ell}(G_k) \otimes \mathbf{Q}$. Since $\mathsf{AbVar}_k \otimes \mathbf{Q} = \mathsf{AbVar}_k^{\mathrm{iso}}$ and $\mathsf{Rep}_{\mathbf{Z}_\ell}(G_k) \otimes \mathbf{Q} = \mathsf{Rep}_{\mathbf{Q}_\ell}(G_k)$, this gives a functor

$$\mathrm{V}_\ell : \mathsf{AbVar}_k^{\mathrm{iso}} \to \mathsf{Rep}_{\mathbf{Q}_\ell}(G_k).$$

Here and elsewhere, if $\mathcal{A}$ is an additive category, we write $\mathcal{A} \otimes \mathbf{Q}$ for the localization of $\mathcal{A}$ at the class of morphisms $n \cdot 1_A$, $n \in \mathbf{Z} \smallsetminus 0$.

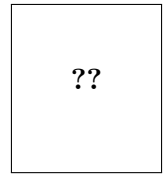
It turns out that $P_A(0) = \deg(-\mathrm{Fr}_A) = \deg(\mathrm{Fr}_A) = q^d$; this can be verified by a direct (but messy) computation. A more interesting quantity is $P_A(1) = \deg(1 - \mathrm{Fr}_A)$. Let $f = 1 - \mathrm{Fr}_A$. We claim that $f : A \to A$ is étale. Essentially, the map $df : \mathrm{Lie}(A) \to \mathrm{Lie}(A)$ is the identity, and this comes down to the fact that the differential of Frobenius is zero (morally, $\frac{d}{dx}x^q = qx^{q-1} = 0$). Thus $P_A(1) = \#\ker(f)$. Note that $f(x) = 0$ if and only if $\mathrm{Fr}_A(x) = x$, i.e. $x \in A(\mathbf{F}_q)$. So $P_A(1) = \#A(\mathbf{F}_q)$. This has a surprising consequence: the quantity $\#A(\mathbf{F}_q)$ is isogeny-invariant! This fails over number fields.

Let's specialize to elliptic curves. Let E be an elliptic curve over $\mathbf{F}_q$. We have $P_E(t) = t^2 - at + q$, for some integer $a = a(E)$. One calls a the trace of Frobenius. Indeed, $a = \mathrm{tr}(\mathrm{Fr}_{E,*}, \mathrm{T}_\ell A)$ for all $\ell \neq p$. Since $\#E(\mathbf{F}_p) = P_A(1) = 1 - a + q$, we could have defined $a = 1 + q - \#E(\mathbf{F}_q)$. Since $\#\mathbf{P}^1(\mathbf{F}_q) = q + 1$, we can think of a as an arithmetically interesting "error term" measuring how much $E(\mathbf{F}_q)$ and $\mathbf{P}^1(\mathbf{F}_q)$ differ.

Theorem 4.5.2 (Hasse bound)**.** *We have* $|a| \leqslant 2\sqrt{q}$*, i.e.*

$$|\#E(\mathbf{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

Proof. Let $n \in \mathbf{Q}$, and take $P_E(n) = n^2 - an + q = \deg(n - \pi_E) \geqslant 0$. Thus $t^2 - at + q \geqslant 0$ for all $t \in \mathbf{R}$. This implies $a^2 - 4q \leqslant 0$, hence $|a| \leqslant 2\sqrt{q}$. □



An equivalent way of formulating the Hasse bound is to claim that the complex roots of P_E have absolute value $\sqrt{q}$. Indeed, one computes

$$\left|\frac{a \pm \sqrt{a^2 - 4q}}{2}\right| = \left|\frac{a \pm \sqrt{4q - a^2}i}{2}\right| = \sqrt{\frac{a^2}{4} + \frac{4q - a^2}{4}} = \sqrt{q}.$$

If $\mathbf{F}_q$ has characteristic $\geqslant 5$, we can write E as $y^2 = x^3 + ax + b$. It follows that

$$\#E(\mathbf{F}_q) = q + 1 + \sum_{x \in \mathbf{F}_q} \left(\frac{x^3 + ax + b}{q}\right),$$

where $\left(\frac{c}{q}\right) = 0$ if $c = 0$, 1 if c is a square in $\mathbf{F}_q$, and -1 otherwise.

A special case of the Honda-Tate theorem says that for each integer a with $|a| \leqslant 2\sqrt{q}$, there is an elliptic curve E over $\mathbf{F}_q$ with $a(E) = a$. So the Hasse bound is sharp. Moreover, we will see that $a(E)$, and hence P_E, determines E up to isogeny.

Example 4.5.3. Fix a prime $p \equiv 3 \pmod 4$, and consider the elliptic curve E over $\mathbf{F}_p$ given by the equation $y^2 = x^3 - x$. Recall that $\mathrm{End}^\circ(E_{\mathbf{F}_{p^2}})$ was a quaternion algebra over $\mathbf{Q}$, of type $(-1, -p)$. We used the fact that $\mathrm{Fr}_E^2 = -p$, but didn't prove this. We know that $P_E(\mathrm{Fr}_E) = 0$, i.e. $\mathrm{Fr}_E^2 - a\mathrm{Fr}_E + p$, so all we need to do is show that $a = 0$. Since $a = p + 1 - \#E(\mathbf{F}_p)$, we just need to show that $\#E(\mathbf{F}_p) = p + 1$. The two sets

$$\{x \in \mathbf{F}_p : x^3 - x \in (\mathbf{F}_p^\times)^2\}$$
$$\{x \in \mathbf{F}_p : x^3 - x \notin (\mathbf{F}_p)^2\}$$

are bijective via $x \mapsto -x$. Call their common cardinality m. Since $\#\{x \in \mathbf{F}_p : x^3 - x = 0\} = 3$, we have $p = 2m + 3$, so $\#E(\mathbf{F}_p) = 2m + 3 + 1 = p + 1$. ▷

4.6 Zeta functions

Let A be an abelian variety over $\mathbf{F}_q$. We can consider its base extension $A_{\mathbf{F}_{q^n}}$, which is an abelian variety over $\mathbf{F}_{q^n}$. It has a characteristic polynomial $P_{A_{\mathbf{F}_{p^n}}}$. Write

$$P_A(t) = \prod_{i=1}^{2d}(x - \omega_i),$$

where the $\omega_i \in \mathbf{C}$.

Theorem 4.6.1. *We have* $P_{A_{\mathbf{F}_{q^n}}}(t) = \prod_{i=1}^{2d}(x - \omega_i^n)$.

Proof. Let $A' = A_{\mathbf{F}_{q^n}}$, and fix a prime $\ell \nmid q$. We have equality $\mathrm{V}_\ell A = \mathrm{V}_\ell A'$; write V for this vector space. The Frobenius on A induces a linear map $\mathrm{Fr}_{A,*} : V \to V$ with characteristic polynomial P_A. We have $\mathrm{Fr}_A^n = \mathrm{Fr}_{A'}^n$ as morphisms on A', so $\mathrm{Fr}_{A',*} = \mathrm{Fr}_{A,*}^n$, whence the result. □

Let's look at the case where $E/\mathbf{F}_q$ is an elliptic curve. We have $P_E(t) = t^2 - at + q$, where $a = a(E) \in \mathbf{Z}$ is the trace of Frobenius acting on $\mathrm{T}_\ell E$ for any $\ell \nmid q$. Recall that since $P_E(1) = \#E(\mathbf{F}_q)$, we get $a = q+1-\#E(\mathbf{F}_q)$. Moreover, we showed that $|a| \leqslant 2\sqrt{q}$. Equivalently, the roots of P_E have absolute value $q^{1/2}$.

Theorem 4.6.2 (Weil)**.** *Let A be an abelian variety over $\mathbf{F}_q$. Then the roots of P_A in $\mathbf{C}$ have absolute value $q^{1/2}$.*

Back to the case of elliptic curves. We can factor $P_E(t) = (t - \omega_1)(t - \omega_2)$ where $\omega_1 + \omega_2 = a$ and $\omega_1\omega_2 = q$. We know that

$$P_{E_{\mathbf{F}_{q^n}}}(t) = (x - \omega_1^n)(x - \omega_2^n) = x^2 - (\omega_1^n + \omega_2^n)t + q^n,$$

so $\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\omega_1^n + \omega_2^n)$. Recall that the *zeta function* of E is the formal power series

$$Z(E,t) = \exp\left(\sum_{n\geqslant 1} \#E(\mathbf{F}_{q^n})\frac{t^n}{n}\right).$$

We can compute:

$$\begin{aligned}\sum_{n\geqslant 1} \#E(\mathbf{F}_{q^n})\frac{t^n}{n} &= \sum \frac{(qt)^n}{n} + \sum \frac{t^n}{n} - \sum \frac{(\omega_1 t)^n}{n} - \sum \frac{(\omega_2 t)^n}{n} \\ &= -\log(1-qt) - \log(1-t) + \log(1-\omega_1 t) + \log(1-\omega_2 t) \\ &= \log\left(\frac{(1-\omega_1 t)(1-\omega_2 t)}{(1-t)(1-qt)}\right).\end{aligned}$$

It follows that

$$Z(E,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}.$$

Note that the numerator is $t^2 P_E(1/t)$.

Example 4.6.3. Let $E/\mathbf{F}_5$ be the elliptic curve $y^2 = x^3 + x + 2$. One can check directly that $E(\mathbf{F}_5) = \{0, (1, \pm 2), (4, 0)\}$. Thus $\#E(\mathbf{F}_5) = 4 = 5 + 1 - a$, so $a = 2$. It follows that $P_E(t) = t^2 - 2t + 5$ and $Z(E,t) = \frac{1-2t+5t^2}{(1-t)(1-5t)}$. In this case,

$$\sum_{n \geqslant 1} \#E(\mathbf{F}_{5^n}) t^n = t \frac{d}{dt} \log Z(E,t) = 4t + 32t^2 + 148t^3 + 640t^4 + 3044t^5 + O(t^6).$$

▷

One puts $\zeta(E,s) = Z(E, q^{-s})$. The fact that the zeros of P_E have absolute value $q^{1/2}$ implies that the zeros of $\zeta(E,s)$ have real part $\frac{1}{2}$. So the "Riemann hypothesis" for $\zeta(E,s)$ is a theorem!

4.7 Honda-Tate theory

Definition 4.7.1. *A q-*Weil number *is an algebraic integer $\omega \in \bar{\mathbf{Q}}$ such that under any embedding $\mathbf{Q}(\omega) \hookrightarrow \mathbf{C}$, the image of ω has absolute value $q^{1/2}$.*

Two q-Weil numbers ω, ω' are *conjugate* if there exists a field isomorphism $\sigma : \mathbf{Q}(\omega) \to \mathbf{Q}(\omega')$ such that $\sigma(\omega) = \omega'$, i.e. ω and ω' lie in the same $G_{\mathbf{Q}}$-orbit in $\bar{\mathbf{Q}}$. Equivalently, ω and ω' are conjugate if they have the same minimal polynomial over $\mathbf{Q}$.

It is easy to check if a given algebraic integer ω is q-Weil. Let $k = \mathbf{Q}(\omega)$, and classify embeddings $k \hookrightarrow \mathbf{C}$. The number ω is q-Weil if and only if $\omega\bar{\omega} = q$ in each such embedding.

Theorem 4.7.2 (Honda-Tate)**.** *Let A be an abelian variety over $\mathbf{F}_q$.*

1. *If A is simple, then $P_A(t) = h(t)^e$ for an irreducible polynomial $h \in \mathbf{Z}[t]$ and $e \geqslant 1$.*
2. *The map*

   {isogeny classes of simple abelian varieties over $\mathbf{F}_q$} $\to$ {conjugacy classes

   sending A to the set of roots in $\bar{\mathbf{Q}}$ of P_A, is a bijection.
3. *Fix $h \in \mathbf{Z}[t]$ the minimal polynomial of a q-Weil number. Then there exists a unique $e \geqslant 1$ such that h^e is P_A for a simple $A/\mathbf{F}_q$. In fact, it is the smallest $e \geqslant 1$ such that*

- $h(0)^e > 0$
- *for every monic* $\mathbf{Q}_p$*-irreducible factor* $g \in \mathbf{Q}_p[t]$ *of* h*, we have* $v_p(g(0)^e) \in r\mathbf{Z}$*, where* $q = p^r$*.*

The injectivity of the map is due to Tate, and the surjectivity is due to Honda.

Corollary 4.7.3. *The map*

$$\{\textit{isogeny classes of elliptic curves over } \mathbf{F}_q\} \to \{a \in \mathbf{Z} : |a| \leqslant 2\sqrt{q}\}$$

given by $E \mapsto a(E) = \mathrm{tr}(\mathrm{Fr}_E, \mathrm{T}_\ell E) = q + 1 - \#E(\mathbf{F}_q)$ *is a bijection.*

Example 4.7.4. The number $\sqrt{5}i$ is 5-Weil, with minimal polynomial $t^2 + 5$. The conditions of part 3 of the Honda-Tate theorem show that there exists an abelian variety E over $\mathbf{F}_5$ such that $P_E = t^2 + 5$. As an exercise, check that $E : y^2 = x^3 + 1$ works. ▷

Example 4.7.5. The number $\sqrt{5}$ is 5-Weil with minimal polynomial $t^2 - 5$. It is easy to check that $e = 2$, so there is a (simple) abelian variety A over $\mathbf{F}_5$ such that $P_A(t) = (t^2 - 5)^2$. One can show that $P_{A_{\mathbf{F}_{25}}}(t) = (t - 5)^4$. Since 5 is a 25-Weil number, there exists an elliptic curve E over $\mathbf{F}_{25}$ such that $P_E(t) = (t - 5)^2$. We will find that $A_{\mathbf{F}_{25}}$ is isogenous to $E \times E$. ▷

Lemma 4.7.6. *Let* A *and* B *be abelian varieties over* $\mathbf{F}_q$*. Then* $P_{A\times B} = P_A \times P_B$*.*

Proof. On $A \times B$, we have $\mathrm{Fr}_{A\times B} = \mathrm{Fr}_A \times \mathrm{Fr}_B$. Fix $\ell \nmid q$, and consider $\mathrm{V}_\ell(A \times B) = \mathrm{V}_\ell A \oplus \mathrm{V}_\ell B$. On $\mathrm{V}_\ell(A \times B)$, we have $\mathrm{Fr}_{A\times B,*} = \mathrm{Fr}_{A,*} \times \mathrm{Fr}_{B,*}$. So it comes down to showing that the characteristic polynomial of $f \oplus g$ is the product of the respective characteristic polynomials. But this is obvious. □

For any abelian variety A over $\mathbf{F}_q$, the Poincaré reducibility theorem implies A is isogenous to $\prod B_i^{n_i}$, where the B_i are simple and pairwise non-isogenous. The lemma gives $P_A = P_{\prod B_i^{n_i}} = \prod P_{B_i}^{n_i}$, where the P_{B_i} are powers of distinct irreducible polynomials. If we started with P_A, we could factor it as $P_A = \prod h_i^{m_i}$, where the h_i are distinct monic irreducible integral polyomials. For each h_i, there is a unique (and computable) $e_i \geqslant 1$ such that $h_i^{e_i} = P_{B_i}$. Thus $P_A = \prod P_{B_i}^{n_i}$, where $n_i = m_i/e_i$.

Theorem 4.7.7. *Let* A *and* B *be abelian varieties over* $\mathbf{F}_q$*. Then* A *and* B *are isogenous if and only if* $P_A = P_B$*.*

Thus, if $\mathrm{V}_\ell A$ and $\mathrm{V}_\ell B$ are isomorphic as $G_{\mathbf{F}_q}$-modules, A and B are isogenous. The converse holds under the assumption that $\mathrm{V}_\ell A$ and $\mathrm{V}_\ell B$ are semisimple (which is known, but not easy to prove).

Let A be a simple abelian variety over $\mathbf{F}_q$. Let $D = \mathrm{End}^\circ(A) = \mathrm{End}_{\mathbf{F}_q}(A) \otimes \mathbf{Q}$; this is a division algebra over $\mathbf{Q}$. Then the field $F = \mathbf{Q}(\mathrm{Fr}_A)$ is contained in the center of D.

Theorem 4.7.8. *Let A be a simple abelian variety over $\mathbf{F}_q$. Then*

1. *$D = \mathrm{End}^\circ(A)$ has center $F = \mathbf{Q}(\mathrm{Fr}_A)$*
2. *$\dim_F D = e^2$, where $P_A = h^e$ with h irreducible*
3. *$2 \dim A = e \cdot [F : \mathbf{Q}]$.*

The division algebra D can be described explicitly from Fr_A. You can give local invariants that classify it over each F_v, where v ranges over the places of F.

The previous remark merits some explanation. Let k be an arbitrary field. Let $\mathrm{Br}(k)$, be the set of isomorphism classes of division algebras with center k. The set $\mathrm{Br}(k)$ has a highly non-obvious group structure. For $D, D' \in \mathrm{Br}(k)$, there is a unique $D'' \in \mathrm{Br}(k)$ such that $D \otimes_k D' \simeq M_n(D'')$ for some n. Set $D'' = D + D'$. Under this operation, $\mathrm{Br}(k)$ is an abelian group, where the inverse of D is opposite algebra D°. It turns out (see [Ser79, X.5]) that $\mathrm{Br}(k)$ is naturally isomorphic to the Galois cohomology group $\mathrm{H}^2(G_k, (k^s)^\times) = \mathrm{H}^2(k, \mathbf{G}_m)$. If k is a nonarchimedean local field, there is a canonical isomorphism $\mathrm{Br}(k) \to \mathbf{Q}/\mathbf{Z}$, so to specify a division algebra with center k is the same as giving an element of $\mathbf{Q}/\mathbf{Z}$.

Suppose k is a number field. If v is a place of k, then the operation $D \mapsto D \otimes_k k_v$ defines a homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(k_v)$. It turns out that the image of D under this map is 0 for all but finitely many v. In fact, we have an exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

This is very deep – at the level of the main theorems of class field theory. For a proof of this (and the rest of class field theory) see [Sha92, 2.86]. In any case, to give an element of $\mathrm{Br}(k)$, it is sufficient to give an element of $\mathrm{Br}(k_{v_i}) = \mathbf{Q}/\mathbf{Z}$ for finitely many finite places $v_1, \dots, v_r$ and an element of $\mathrm{Br}(\mathbf{R}) = \mathbf{Z}/2$ for each real place of k.

Example 4.7.9. Let E be an elliptic curve over $\mathbf{F}_q$ with $P_E = x^2 + q$. Then $\mathrm{Fr}_E^2 = -q$, so $F = \mathbf{Q}(\Phi_E) \simeq \mathbf{Q}(\sqrt{-q})$. It follows that $e = 1$, so $\mathrm{End}^\circ(E) = \mathbf{Q}(\Phi_E)$. ▷

Example 4.7.10. Let E be an elliptic curve over $\mathbf{F}_q$ such that P_E is reducble. Then $P_E(t) = (t-\omega)^2$, where $\omega \in \mathbf{Z}$ with $|\omega| = q^{1/2}$. It follows that q is a square and $\omega = \pm q^{1/2}$. Then $\Phi_E = \omega \in \mathbf{Z}$, so $F = \mathbf{Q}(\Phi_E) = \mathbf{Q}$ and $e = 2$. The division ring $\mathrm{End}^\circ(E)$ is a quaternion algebra (we saw an example earlier). ▷

4.8 Curves and their jacobians

Here and elsewhere we will consider alternating sums

$$\sum (-1)^i \operatorname{tr}(f_i, H_i)$$

where $f_\bullet : H_\bullet \to H_\bullet$ is a graded linear endomorphism of a locally finite-dimensional graded vector space. We will write $\operatorname{tr}(f_\bullet, H_\bullet)$, or sometimes just $\operatorname{tr}(f, H)$, for this alternating sum.

Let's start with some motivation. Let X and Y be smooth oriented manifolds of dimension n. Let $f : X \to Y$ be a smooth map that is finite-to-one. For $x \in X$, we can choose small neighborhoods U, V of x and $y = f(x)$ such that U and V are n-balls, and for which $f : U \to V$ is injective. The relative homology $\mathrm{H}^n(U, U \smallsetminus x)$ and $\mathrm{H}^n(V, V \smallsetminus y)$ are both isomorphic to $\mathbf{Z}$ with a canonical basis coming from the orientation. With respect to these bases, f_* is multiplication by an integer, called the *degree of f at x*, and denoted $\deg_x f$.

Theorem 4.8.1 (Lefschetz)**.** *Let $f : X \to X$ be smooth with finitely many nondegenerate fixed points. Then we have*

$$\sum_{x \in X^f} \deg_x f = \operatorname{tr}(f_*, \mathrm{H}_\bullet(X, \mathbf{Q}))$$

If f is "well-behaved" around each fixed point, the local degrees are all one, so the theorem reduces to $\#\{x \in X : f(x) = x\} = \operatorname{tr}(f_*, \mathrm{H}_\bullet(X, \mathbf{Q}))$. If X is a Riemann surface, the alternating sum is

$$\operatorname{tr}(f_*, \mathrm{H}_0(X, \mathbf{Q})) - \operatorname{tr}(f_*, \mathrm{H}_1(X, \mathbf{Q})) + \operatorname{tr}(f_*, \mathrm{H}_2(X, \mathbf{Q})).$$

There is an analogue of the Lefschetz fixed point theorem for étale cohomology. Let X be a nice variety over an algebraically closed field k, and let $f : X \to X$ be an arbitrary morphism. Let ℓ be a prime invertible in k. It is proven in [Del77, IV.3.3] that one has

$$(\Gamma_f \cdot \Delta_X) = \operatorname{tr}(f^*, \mathrm{H}^\bullet(X, \mathbf{Q}_\ell)).$$

Here $(\Gamma_f \cdot \Delta)$ is the intersection number of the graph of f and the diagonal as cycles in $X \times X$. If $k = \mathbf{F}_q$ and $f = \Phi$ is the Frobenius on X, then Γ_Φ and Δ_X

intersect transversally with multiplicity one, so $(\Gamma_\Phi \cdot \Delta_X) = \#X^\Phi = \#X(\mathbf{F}_q)$. More generally (see [Del77, IV.3.7]) we have

$$\#X(\mathbf{F}_{q^n}) = \sum (-1)^i \operatorname{tr}(\Phi^{n*}, \mathrm{H}^i(X, \mathbf{Q}_\ell)).$$

If $X = C$ is a nice curve over $\mathbf{F}_q$, we can be much more concrete. The alternating sum has only three terms:

$$\#C(\mathbf{F}_{q^n}) = \operatorname{tr}(\Phi^n, \mathrm{H}^0(C, \mathbf{Q}_\ell)) - \operatorname{tr}^1(\Phi^n, \mathrm{H}^0(C, \mathbf{Q}_\ell)) + \operatorname{tr}(\Phi^n, \mathrm{H}^2(C, \mathbf{Q}_\ell))$$

One can show that the trace on $\mathrm{H}^0(C, \mathbf{Q}_\ell)$ is 1, while the trace on $\mathrm{H}^2(C, \mathbf{Q}_\ell)$ is q^n. Let J be the jacobian of C. Since $\mathrm{H}^1(C, \mathbf{Q}_\ell)^\vee \simeq \mathrm{V}_\ell J$ as $G_{\mathbf{F}_q}$-modules, we have

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - \operatorname{tr}(\Phi_*^n, \mathrm{V}_\ell J).$$

The following theorem is a straightforward consequence of the Lefschetz fixed point theorem and Theorem 4.6.1.

Theorem 4.8.2. *Let C be a nice curve over $\mathbf{F}_q$ of genus g. Let J be its jacobian, and write $P_J(t) = \prod_{i=1}^{2g}(x - \omega_i)$. Then*

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - (\omega_1^n + \cdots + \omega_{2g}^n).$$

Corollary 4.8.3. $|\#C(\mathbf{F}_{q^n}) - (q^n + 1)| \leqslant 2gq^{n/2}$.

Example 4.8.4. If C is a nice curve of genus zero over $\mathbf{F}_q$, then we know that $|\#C(\mathbf{F}_q) - (q+1)| \leqslant 0$, so $\#C(\mathbf{F}_q) = q + 1$. In particular, C has a $\mathbf{F}_q$-rational point, whence $C \simeq \mathbf{P}^1_{\mathbf{F}_q}$. ▷

Example 4.8.5. If C is a nice curve of genus one over $\mathbf{F}_q$, then we know that $\#C(\mathbf{F}_q) \geqslant q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0$. So once again C has a $\mathbf{F}_q$-rational point, hence C is an elliptic curve. ▷

It is a good exercise to find a curve C of genus $g = 2$ for which $C(\mathbf{F}_q) = \varnothing$. (**do this**)

Example 4.8.6. Let C be a nice curve of genus two over $\mathbf{F}_4$. We know that $\#C(\mathbf{F}_4) \leqslant 4 + 1 + 2 \cdot 2 \cdot \sqrt{4} = 13$. We claim that $\#C(\mathbf{F}_4) \neq 13$, i.e. the Hasse bound is not sharp. To see this, note that $\#C(\mathbf{F}_4) = 5 - (\omega_1 + \omega_2 + \omega_3 + \omega_4)$, where each ω_i has absolute value 2. Thus $\#C(\mathbf{F}_4) \leqslant 5 + (2 + 2 + 2 + 2)$, with equality if and only if each $\omega_i = -2$. If each $\omega_i = -2$, then we would have $P_J = (t + 2)^4$. This would imply

$$\#C(\mathbf{F}_{16}) = 16 + 1 - (\omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2) = 16 + 1 - (4 + 4 + 4 + 4) = 1$$

which contradicts $C(\mathbf{F}_4) \subset C(\mathbf{F}_{16})$. ▷

Example 4.8.7 (Hermite curve)**.** Let C be the curve over $\mathbf{F}_p$ defined by the equation $x^{p+1}+y^{p+1}+z^{p+1}=0$. Then $C \subset \mathbf{P}^2$ is a nice curve, and $\#C(\mathbf{F}_p) = p+1$. This is because for $(x,y,z) \in \mathbf{F}_p^3$, we have $x^{p+1}+y^{p+1}+z^{p+1} = x^2+y^2+z^2$. This is the equation of a genus zero curve. It turns out that $\#C(\mathbf{F}_{p^2}) = p^3+1$. One way to prove this is to use the fact that the map $\mathbf{F}_{p^2}^\times \to \mathbf{F}_p^\times$ given by $a \mapsto a^{p+1}$ is surjective. The curve C has degree $p+1$, so its genus is $g = \frac{(d-1)(d-2)}{2}$, which in our case is $\frac{p(p-1)}{2}$. We know that

$$p^3+1 = \#C(\mathbf{F}_{p^2}) \leqslant p^2 + 2g\sqrt{p^2} = p^3+1.$$

In particular, our bound on $\#C(\mathbf{F}_{p^2})$ is sharp in this case. The fact that $\#C(\mathbf{F}_{p^2}) = p^2+1+2\sqrt{p^2}$ tells us that $P_{J_{\mathbf{F}_{p^2}}}(t) = \prod(t-\omega_i^2)$ with each $\omega_i^2 = -p$. In other words, $P_{J_{\mathbf{F}_{p^2}}}(t) = (t+p)^{2g}$. Each $\omega_i = \pm\sqrt{p}i$, so $p+1 = \#C(\mathbf{F}_p) = (p+1) - \sum \omega_i$ tells us that half of the $\omega_i = \sqrt{p}i$, and half are $-\sqrt{p}i$. In other words,

$$P_J(t) = (t^2-\sqrt{p}i)^g(t+\sqrt{p}i)^g = (t^2+p)^g$$

Thus J is isogenous to E^g, where E is an elliptic curve over $\mathbf{F}_p$ with $a(E) = 0$. ▷

4.9 The Weil conjectures

Recall that for a curve C of genus g over $\mathbf{F}_q$, the *zeta function* of C is the formal power series

$$Z(C,t) = \exp\left(\int \sum_{n\geqslant 1} \#C(\mathbf{F}_{q^n}) t^n \frac{dt}{t}\right) = \exp\left(\sum_{n\geqslant 1} \#C(\mathbf{F}_{q^n})\frac{t^n}{n}\right).$$

By Theorem 4.8.2, there exist q-Weil numbers $\omega_1, \ldots, \omega_{2g}$ such that for all n,

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - (\omega_1^n + \cdots + \omega_{2g}^n).$$

This allows us to compute:

$$\begin{aligned} Z(C,t) &= \exp(-\log(1-qt) - \log(1-t) + \log(1-\omega_1 t) + \cdots + \log(1-\omega_{2g}t)) \\ &= \frac{(1-\omega_1 t)\cdots(1-\omega_{2g}t)}{(1-t)(1-qt)}. \end{aligned}$$

Let J be the jacobian of C. Then the numerator is the "reverse" $t^{2g}P_J(1/t)$ of $P_J(t)$. For *any* nice variety X of dimension d over $\mathbf{F}_q$, one can define $Z(X,t)$ in the same way, and one has the *Weil conjectures*. These state that

1. $Z(X,t)$ is a rational function of the form $\prod_{i=0}^{2d} P_i(X,t)^{(-1)^{i+1}}$, where the $P_i(X,t)$ are integral polynomials with $P_0(X,t) = 1-t$ and $P_{2d}(X,t) = 1-q^d t$.

2. $Z(X, 1/q^n t) = \pm q^{d\chi/2} t^\chi Z(X,t)$, where $\chi = (\Delta_X \cdot \Delta_X)$ is the Euler characteristic of X

3. Each $P_i(X,t) = \prod_j (1-\omega_j t)$, where the ω_j are q^i-Weil.

See [Wei49] for the original (and surprisingly modern) statement of the Weil conjectures. For a proof, see [Del74], or [Milb] for a proof in English. Note that our $P_i(X,t)$ are *not* the same as $P_{\mathrm{Jac}\, C}(t)$ for a curve C; $P_1(C,t)$ is the "reverse polynomial" of $P_J(t)$. Also, note that because of conjecture 3, each P_i is relatively prime to the others, i.e. in $Z(X,t) = \prod P_i(X,t)^{(-1)^{i+1}}$ there is no cancellation.

Let's relate our approach to the Weil conjectures for a curve to the general proof. The fact that

$$Z(C,t) = \frac{\det(1-\Phi^* t, \mathrm{V}_\ell J)}{(1-t)(1-qt)}$$

has a general analogue. For a graded vector space $H^\bullet$ and a graded endomorphism $f^\bullet : H^\bullet \to H^\bullet$, write

$$\det(f, H^\bullet) = \prod_i \det(f^i, H^i)^{(-1)^i}.$$

There is a general theorem (see [Del74, 1.5.4]) that

$$Z(X,t) = \frac{1}{\det(1-\Phi^* t, \mathrm{H}^\bullet(X, \mathbf{Q}_\ell))}.$$

For $X = C$ a nice curve of genus g, the map Φ^* on H^0 is the identity, and on H^2 is multiplication by q^d. For any endomorphism θ of a d-dimensional vector space V, one has

$$\det(t \cdot 1 - \theta) = t^d \det(1 - \theta t^{-1})$$

In other words, $\det(1-\theta t)$ is the "reverse" of the characteristic polynomial of θ. Thus $P_J(t)$ is the reverse of the polynomial $P_1(C,t)$, and the roots of $P_J(t)$ are q-Weil if and only for $P_1(C,t) = \prod_i (1-\omega_i t)$, the ω_i are q-Weil.

Next, we check that the functional equation holds for $Z(C,t)$. We know that $P_J(t) = \prod (t-\omega_i)$, where the ω_i are q-Weil. For each root ω of P_J, $\bar\omega$ is also a root that is q-Weil, so $\omega\bar\omega = q$, i.e. $\bar\omega = q/\omega$. It follows that the polynomials $t^{2g} P_J(q/t)$ and $P_J(t)$ have the same roots, so they are equal up to a constant (which turns out to be q^g). This yields the functional equation.

Requirement 3 in the statement of the Weil conjectures is often called the *Riemann hypothesis* for the variety. For $X = C$ a nice curve of genus g, it is easy to motivate this. Define $\zeta(C, s) = Z(X, q^{-s})$. This is a holomorphic function of s on some $\{s \in \mathbf{C} : \Re s > c\}$, and has a meromorphic continuation to the complex plane. By definition, $\zeta(C, s) = 0$ if and only if $Z(C, q^{-s}) = 0$, which happens if and only if $q^{-s} = \omega_i$ for some i. Since the ω_i are q-Weil, this tells us that $|s| = \log_q(q^{1/2}) = \frac{1}{2}$. The requirement that zeros of $\zeta(C, s)$ have absolute value $\frac{1}{2}$ is commonly called the Riemann hypothesis for C. Note that the Riemann hypothesis for curves is a theorem, unlike the (much more difficult) Riemann hypothesis for $\zeta(\mathrm{Spec}(\mathbf{Z}), s)$.

4.10 Generalizing the Weil conjectures

Proving that $Z(X, t)$ is rational is the easiest part of the Weil conjectures. Indeed, Dwork proved it before Deligne, using p-adic analytic methods. The cohomological proof is almost a triviality, following from basic properties of étale cohomology. Let X be a nice variety over $\mathbf{F}_q$, and fix a prime ℓ not dividing q. Write $\mathrm{H}(X)$ for $\mathrm{H}^\bullet(X_{\bar{\mathbf{F}}_q}, \mathbf{Q}_\ell)$. This is a graded $\mathbf{Q}_\ell$-vector space with an action of G_k. In fact, $\mathrm{H}(X)$ is a graded-commutative $\mathbf{Q}_\ell$-algebra, with multiplication the cup product. We have the following trace theorem [Del77, II.3.1].

$$\#X(\mathbf{F}_{q^n}) = \mathrm{tr}(\Phi^{*n}, \mathrm{H}(X))$$

where $\Phi = \Phi_X$ is the Frobenius of X. Now we use the following theorem from linear algebra

Theorem 4.10.1. *Let V be a finite-dimensional graded vector space over a field k of characteristic zero, and let $\theta : V \to V$ be a k-linear map. There is an equality of formal power series*

$$\sum_{n \geqslant 1} \mathrm{tr}(\theta^n, V) t^n = t \frac{d}{dt} \log \left(\frac{1}{\det(1 - \theta t)} \right).$$

Proof. See [Del77, II.3.3]. Essentially, one reduces to the case where V is concentrated in degree zero and k is algebraically closed. Then use the fact that θ can be diagonalized. □

Summing the trace formula over n gives

$$\sum_{n \geqslant 1} \#X(\mathbf{F}_{q^n}) t^n = \sum_{n \geqslant 1} \mathrm{tr}(\Phi^*, \mathrm{H}(X)).$$

We can apply Theorem 4.10.1 to conclude that

$$\sum_{n \geqslant 1} \#X(\mathbf{F}_{q^n}) t^n = t \frac{d}{dt} \log \left(\frac{1}{\det(1 - \Phi^* t, \mathrm{H}(X))} \right).$$

Applying $\exp\left(\int \frac{dt}{t}\right)$ to both sides yields the formula $Z(X,t) = \det(1 - \Phi^* t, \mathrm{H}(X))^{-1}$. So we know that $Z(X,t)$, a priori a power series over $\mathbf{Q}$, is a rational function over $\mathbf{Q}_\ell$. That is, $Z(X,t) \in \mathbf{Q}[\![t]\!] \cap \mathbf{Q}_\ell(t)$. The theory of Hankel determinants (see exercise one from §4 in [Bou90, A.IV]) shows that $Z(X,t) \in \mathbf{Q}(t)$.

This proof can be easily generalized. Let k be an arbitrary field, X a nice variety over k. Fix a prime ℓ invertible in k, and write $\mathrm{H}(X)$ for $\mathrm{H}^\bullet(X_{\bar{k}}, \mathbf{Q}_\ell)$. For a surjective morphism $f : X \to X$, let $\Gamma_f \subset X \times X$ be the graph of f, and let $\Delta_X \subset X \times X$ be the diagonal. There is the *relative zeta function of X with respect to f*:

$$Z(X, f, t) = \exp\left(\int \sum_{n \geqslant 1} (\Gamma_{f^n} \cdot \Delta_X) t^n \, \frac{dt}{t} \right).$$

One has a generalized trace formula ([dJ, ex.11] and [Del77, IV.3.3]):

$$(\Gamma_{f^n} \cdot \Delta_X) = \mathrm{tr}(f^{*n}, \mathrm{H}(X))$$

Exactly as before, it follows that $Z(X, f, t) = \det(1 - f^* t, \mathrm{H}(X))^{-1}$.

A more fruitful (but more difficult) generalization of the Weil conjectures involves the Grothendieck ring of varieties. Let $\mathsf{Var}_{\mathbf{F}_q}$ denote the category of all varieties over $\mathbf{F}_q$. Write $\mathbf{K} = K_0(\mathsf{Var}_{\mathbf{F}_q})$ for the quotient of the free abelian group on isomorphism classes of varieties over $\mathbf{F}_q$ by relations of the form $[X] = [Y] + [U]$ whenever $Y \subset X$ is a closed subvariety and $U = X \smallsetminus Y$. The ring $\mathbf{K}$ has a natural product operation induced by $[X] \cdot [Y] = [X \times Y]$. If we had started with an algebraically closed field of characteristic zero, $\mathbf{K}$ would be generated by smooth projective varieties – see [Bit04]. For a variety X over $\mathbf{F}_q$, it is a theorem that $\#X(\mathbf{F}_{q^n}) = \#\,\mathrm{Sym}^n(X)(\mathbf{F}_q)$ (see [Del77, III.2.11] for a colossal generalization). This motivates our definition of the *motivic zeta function* of X as

$$\zeta(X, t) = \sum_{n \geqslant 0} [\mathrm{Sym}^n(X)] t^n \in \Lambda(\mathbf{K}) = 1 + t\mathbf{K}[\![t]\!].$$

One can ask whether $\zeta(X,t)$ is a rational function over $\mathbf{K}$, but this turns out to be false in general.

4.11 Computing zeta functions

Let C be a nice curve of genus g over $\mathbf{F}_q$, J the jacobian of C. We have

$$P_J(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + a_{g-1} q t^{g-1} + a_{g-2} q^2 t^{g-2} + \cdots + a_t q^{g-1} t + q^g.$$

In particular, $t^{2g}P_J(1/t)$ is congruent to $1 + \cdots + a_g t^g$ modulo t^{g+1}. Thus

$$\begin{aligned} 1 + a_1 t + \cdots + a_g t^g &\equiv (1-t)(1-qt)Z(C,t) \\ &\equiv (1-t)(1-qt)\exp\left(\sum_{n\geqslant 1} \#C(\mathbf{F}_{q^n})\frac{t^n}{n}\right) \pmod{t^{g+1}} \end{aligned}$$

The values $\#C(\mathbf{F}_q), \ldots, \#C(\mathbf{F}_{q^g})$ determine $a_1, \ldots, a_g$, and hence $P_J(t)$ and $Z(C,t)$ are determined by $\#C(\mathbf{F}_{q^r})$ for $r \leqslant g$.

Example 4.11.1. Let C be the nice curve over $\mathbf{F}_p$ arising from $y^2 = x^6 - x^3 + x + 1$. (The projective closure of the zero set of this polynomial has a singularity, so we have to blow it up once.) Let J be the jacobian of C. We have

$$P_J(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + p^2$$

and

$$1 + a_1 t + a_2 t^2 \equiv (1-t)(1-pt)\exp\left(\#C(\mathbf{F}_p)t + \#C(\mathbf{F}_{p^2})\frac{t^2}{2}\right) \pmod{t^3}$$

For $p = 3$, one can compute $\#C(\mathbf{F}_3) = 7$, $\#C(\mathbf{F}_9) = 13$. Thus

$$1 + a_1 t + a_2 t^2 \equiv (1-t)(1-3t)\exp\left(7t + 13\frac{t^2}{2}\right) \equiv 1 + 3t + 6t^2 \pmod{t^3}$$

It follows that $P_J(t) = t^4 + 3t^3 + 6t^2 + 9t + 9$. This factors as $(t^2+3)(t^2+3t+3)$.

From this, we see that J is isogenous to a product of non-isogenous elliptic curves.

If $p = 5$, one can brute-force $\#C(\mathbf{F}_5) = 9$, $\#C(\mathbf{F}_{25}) = 19$. The same process yields the irreducible polynomial

$$P_J(t) = t^4 + 3t^3 + t^2 + 15t + 25.$$

Thus J is a simple abelian variety of dimension 2. As a consequence, there is no nonconstant morphism $C \to E$, where E is an elliptic curve. If there was, we would get a nonconstant morphism $J \to E$, the kernel of which would be a nontrivial abelian subvariety of J (at least after taking its connected component).

We claim that J is geometrically simple. We want $P_{\mathbf{F}_{5^n}}$ to be irreducible for all n. For, this would imply that $J_{\mathbf{F}_{5^n}}$ is simple, for each $n$and hence $J_{\bar{\mathbf{F}}_5}$ is simple. Let ω be a root of $P_J(t)$. We know that $\mathbf{Q}(\omega)/\mathbf{Q}$ is a degree-four extension. We want $\mathbf{Q}(\omega^n) = \mathbf{Q}(\omega)$. We claim that $\mathbf{Q}(\omega)$ has only the subfields $\mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}$. So if $\mathbf{Q}(\omega^n) \neq \mathbf{Q}(\omega$, then ω^n is real, i.e. $\omega^n = \pm 5^{n/2}$. This implies $\omega = \zeta\sqrt{5}$ for ζ a root of unity, whence $\zeta \in \mathbf{Q}(\omega)$. One can show that the extension $\mathbf{Q}(\omega)/\mathbf{Q}$ is not Galois, so $\zeta \in \mathbf{Q}(\sqrt{5})$, so $\zeta = \pm 1$, whence $\omega = \pm\sqrt{5}$, which cannot be the case. ▷

5 Birch and Swinnerton-Dyer conjecture

Consider an elliptic curve E over $\mathbf{Q}$. It has a model of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$ and the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. The Mordell-Weil theorem (proved in this case by Mordell) tells us that $E(\mathbf{Q})$ is finitely generated. By basic algebra, we can write $E(\mathbf{Q}) = E(\mathbf{Q})_{\mathrm{tors}} \oplus \mathbf{Z}^r$ where $E(\mathbf{Q})_{\mathrm{tors}}$ is finite, and $r = \operatorname{rk} E(\mathbf{Q})$ is the algebraic rank of E (over $\mathbf{Q}$). The group $E(\mathbf{Q})_{\mathrm{tors}}$ can be computed. One way is to look at the map $E(\mathbf{Q})_{\mathrm{tors}} \to E(\mathbf{F}_p) \times E(\mathbf{F}_{p'})$, which is injective when p and p' are distinct primes of good reduction. For example, we could choose $p \neq p'$, with both not dividing Δ.

The torsion subgroup $E(\mathbf{Q})$ is one of a finite list. In fact, there is the following deep theorem of Mazur (conjectured by Ogg).

Theorem 5.0.1. *Let E be an elliptic curve over $\mathbf{Q}$. Then $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to one of the following:*

$\mathbf{Z}/n$	*with* $n = 1, \dots, 10$ *or* $n = 12$
$\mathbf{Z}/n \oplus \mathbf{Z}/2$	*with* $n = 1, \dots, 4$

Proof. See [Maz77, III.5.1]. Essentially, Mazur classifies rational points on the modular curves $X_0(N)$. □

Each of these possibilities occur infinitely often. An analogous theorem holds over any number field. More precisely, for each integer d, there is a global bound $B(d)$ such that for any elliptic curve E over a number field k with $[k : \mathbf{Q}] = d$, one has $\#E(k)_{\mathrm{tors}} \leqslant B(d)$. This is proven in [Mer96]. For k quadratic over $\mathbf{Q}$, the possible groups $E(k)_{\mathrm{tors}}$ have been classified.

Unlike the situation with $E(\mathbf{Q})_{\mathrm{tors}}$, where everything is computable and well-understood, there is no known algorithm to compute the rank of an elliptic curve. If $Ш(E)$ is finite, then there is an algorithm, but the finiteness of $Ш(E)$ is not known in general.

The vague idea of the Birch and Swinnerton-Dyer conjecture (henceforth BSD) is as follows. Suppose $E(\mathbf{Q})$ has high rank. Then for p a prime of good reduction, we have a map $E(\mathbf{Q}) \to E(\mathbf{F}_p)$. (Scheme-theoretically, $E(\mathbf{F}_p)$ doesn't make sense. We set $E(\mathbf{F}_p) = \mathcal{E}(\mathbf{F}_p)$, where $\mathcal{E}$ is the Néron model of E over $\mathbf{Z}_{(p)}$. Since $E(\mathbf{Q}) = E(\mathbf{Z})$, we are really looking at the map $E(\mathbf{Z}) \to \mathcal{E}(\mathbf{F}_p)$.) The group $E(\mathbf{F}_p)$ has order $p + 1 - a_p(E)$, where $a_p(E) = a(\mathcal{E}_{\mathbf{F}_p})$, and $|a_p(E)| \leqslant 2\sqrt{p}$. The expectation is for $E(\mathbf{F}_p)$ to be "slightly larger" than average, given that the map $E(\mathbf{Q}) \to E(\mathbf{F}_p)$ gives us some points "for free." This effect turns out to be very subtle.

5.1 L-functions of elliptic curves

Define the function π_E on $\mathbf{R}_{\geqslant 0}$ by

$$\pi_E(x) = \prod_{p \leqslant x \text{ good}} \frac{\#E(\mathbf{F}_p)}{p}.$$

We hope that $r = \operatorname{rk} E$ can be detected from the growth of π_E. In the early 60s, Swinnerton-Dyer used a computer to get numerical data on these types of problem. He and Birch conjectured the following [BSD65, A]:

$$\lim_{x \to \infty} \frac{\log \pi_E(x)}{\log \log x} = r$$

One could also conjecture that $\pi_E(X) \sim C(\log x)^r$ as $x \to \infty$ for some constant C. The function π_E is hard to work with. Instead, we will follow standard practice in number theory and introduce an L-function.

Definition 5.1.1. *Let E be an elliptic curve over $\mathbf{Q}$ with discriminant Δ. The* partial L-function of E *is*

$$L_\Delta(E, s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}}.$$

Here, s is a complex variable, but this product does converge on the whole complex plane. Recall that if E is an elliptic curve over $\mathbf{F}_p$, the characteristic polynomial of the Frobenius Φ_E acting on $T_\ell E$ is $t^2 - a_p t + p$. The reverse of this is $\det(1 - \Phi^* t, V_\ell E) = 1 - a_p t + pt^2$. It follows that we could have defined

$$L_\Delta(E, s) = \prod_{p \nmid \Delta} \frac{1}{\det(1 - \Phi^*_{E,p} p^{-s}, \mathrm{H}^1(E_p, \mathbf{Q}_\ell))}$$

for some prime $\ell \mid \Delta$. There is a way of adding factors at the "bad primes" dividing the discriminant of E. We will come back to that later.

Lemma 5.1.2. *The product defining $L_\Delta(E, s)$ converges absolutely for all $s \in \mathbf{C}$ with $\Re s > \frac{3}{2}$. Moreover, $L_\Delta(E, s)$ is holomorphic on that region.*

Proof. The basic idea is to use the factorization $1 - a_p t + pt^2 = (1 - \omega_{p,1} t)(1 - \omega_{p,2} t)$, where $|\omega_{p,i}| = p^{1/2}$ by the Weil conjectures. We can write

$$L_\Delta(E, s) = \prod_{p \nmid \Delta} \left(1 - \frac{\omega_{p,1}}{p^{1/2}} p^{1/2-s}\right)^{-1} \left(1 - \frac{\omega_{p,2}}{p^{1/2}} p^{1/2-s}\right)^{-1}$$

Standard arguments (using only the fact that the $\omega_{p,i}$ are p-Weil) yield the result. □

Following Euler, we look at $L_\Delta(E,1)$, (which does not exist unless $L_\Delta(E,s)$ has some kind of analytic continuation, which we have not proved). At least formally (ignoring convergence) we have

$$\begin{aligned} L_\Delta(E,1) &= \prod_{p\nmid\Delta}(1-a_p(E)p^{-1}+p^{-1})^{-1} \\ &= \prod_{p\nmid\Delta}\frac{p}{p-a_p(E)+1} \\ &= \prod_{p\nmid\Delta}\frac{p}{\#E(\mathbf{F}_p)} \end{aligned}$$

This looks very similar to our definition of the function π_E. At least intuitively, larger r should lead to "quicker vanishing" at $s=1$.

Conjecture 5.1.3 (Birch and Swinnerton-Dyer)**.** *The function $L_\Delta(E,s)$ has an analytic continuation to a neighborhood of $s=1$. Moreover,*

$$\operatorname{ord}_{s=1} L_\Delta(E,s) = \operatorname{rk} E.$$

In other words, the conjecture says that $L_\Delta(E,s)\sim c(s-1)^r$ near $s=1$ for some constant c. Modern formulations of BSD include a formula for c.

Let's define the factors in $L(E,s)$ for primes $p\mid\Delta$. The following seems quite ad-hoc without motivation:

$$L_p(E,s)=\begin{cases}\dfrac{1}{1-a_pp^{-s}+p^{1-2s}} & \text{if } E \text{ has good reduction at } p\\[2ex] \dfrac{1}{1-a_pp^{-s}} & \text{if } E \text{ has bad reduction at } p\end{cases}$$

Here, $a_p=-1$ if E has split multiplicative reduction at p, $a_p=1$ if E has nonsplit multiplicative reduction, and $a_p=0$ if E has additive reduction. This terminology deserves some explanation. Fix a prime p. A *minimal model* for E at p is an equation $y^2=x^3+ax+b$, where a,b are integral over $\mathbf{Z}_{(p)}$, and such that the descriminant $\Delta=-16(4a^3+27b^2)$ has minimal p-adic valuation among such models. Let $\widetilde{E}$ be a minimal model for E. Then $\widetilde{E}$ is a scheme over $\mathbf{Z}_{(p)}$, so we can consider its reduction $\widetilde{E}_p=\widetilde{E}_{\mathbf{F}_p}$ modulo p. If E has bad reduction at p, $\widetilde{E}_p$ will be singular, but its nonsingular locus $\widetilde{E}_{p,\mathrm{ns}}$ will be a smooth group scheme over $\mathbf{F}_p$. There are three possibilities for $\widetilde{E}_{p,\mathrm{ns}}$. Either it will be the additive group $\mathbf{G}_{a,\mathbf{F}_p}$, in which case we say E has *additive reduction at p*, or it will be a one-dimensional torus (isomorphic to $\mathbf{G}_{\bar{\mathbf{F}}_p}$ after base change). In the second case we say E has *split multiplicative reduction at p* if $\widetilde{E}_{p,\mathrm{ns}}\simeq\mathbf{G}_{m,\mathbf{F}_p}$, and we say E has *nonsplit multiplicative reduction at p* if $\widetilde{E}_{p,\mathrm{ns}}\not\simeq\mathbf{G}_{m,\mathbf{F}_p}$ (it turns out that we get isomorphism after base change to a quadratic extension of $\mathbf{F}_p$). See [Sil09, III.2.5, 2.6] for a proof and details.

5.2 Conductors

Let E be an elliptic curve over $\mathbf{Q}$ with rank r. The *conductor* of E is an integer measuring the how badly E reduces over various primes. Before we can define the conductor, we need to recall some basic facts about Galois groups of local fields. Let k be a local field, L/k a finite Galois extension. Let v be a valuation on K normalized by the condition $v(\pi_L) = 1$. Let $G = \mathrm{Gal}(L/k)$. Then the *higher ramification groups* of the extension L/k are:

$$G_i = \{\sigma \in G : v(\sigma(x) - x) > i \text{ for all } x \in \mathfrak{o}_L\}.$$

For example, $G_{-1} = G$, G_0 is the inertia subgroup of L/k, and G_1 is the "wild inertia" subgroup of G. The G_i form an exhaustive descending filtration of G. For a careful study of the higher ramification groups, see [Ser79, IV].

The conductor of an elliptic curve E over $\mathbf{Q}$ is defined as a product of local data: $N = \prod_p p^{f_p}$. Each of the f_p only depend on the base change $E_{\mathbf{Q}_p}$. So, treat E is an elliptic curve over $\mathbf{Q}_p$, and choose a prime $\ell \neq p$. Let $V = E[\ell]$; this is a two-dimensional vector space over $\mathbf{F}_\ell$ with an action of $G_{\mathbf{Q}_p}$. Since $GL(V)$ is finite, the action of $G_{\mathbf{Q}_p}$ factors through a finite quotient $G = \mathrm{Gal}(L/\mathbf{Q}_p)$. We define

$$f_p(E) = \sum_{i \geqslant 0} \frac{1}{[G_0 : G_i]} \dim_{\mathbf{F}_\ell} V/V^{G_i}.$$

Note that $G_0 = I_p$, the inertia group at p, and $G_1 = P_p$, the Sylow p-subgroup of G (consisting of "wild inertia"), see [Ser79, IV] for a proof. So we can split up the sum as

$$f_p(E) = \dim_{\mathbf{F}_\ell} V/V^{I_p} + \sum_{i \geqslant 1} \frac{1}{[G_0 : G_i]} \dim_{\mathbf{F}_\ell} V/V^{G_i}.$$

The quantity $\dim V/V^{I_p}$ is called the *tame part* of f_p, sometimes written ε_p, and the rest of the sum is called the *wild part*, written δ_p. If $p \geqslant 5$, the wild part is zero and there is an easy formula for f_p:

$$f_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

See [Sil94, IV.10.2] for a proof of this. Sometimes f_p is called the *Swan conductor* of $E[\ell]$. **(mention ℓ-independence of Swan conductor)**

Theorem 5.2.1. *The function $L(E,s)$ has an analytic continuation to all of* $\mathbf{C}$. *Moreover, it satisfies a functional equation: there exists $\omega = \pm 1$ such that*

$$\Lambda(s) = \omega\Lambda(2-s)$$

where $\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$.

The constants N and ω are easily computed. They are a product of local factors, so in particular no analysis is needed to find their values.

We can give a sketch of a proof of this theorem. Expand the product formula for $L(E,s)$ to get a Dirichlet series

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

It is not immediately obvious that these $a_n = a_n(E)$ agree with our earlier definition of the $a_p = p + 1 - \#E(\mathbf{F}_p)$. It follows from an argument similar to the one Euler used to prove the product formula for $\zeta(s)$. Moreover, we have $a_n \in \mathbf{Z}$ for all n. The function $a \mapsto a_n$ is multiplicative in the number-theoretic sense: if $(m,n) = 1$, then $a_{mn} = a_m a_n$. If $n \geqslant 2$, then

$$a_{p^n} = a_p a_{p^{n-1}} - p a_{p^{n-2}}.$$

This allows us to compute a_n for any n just using the a_p. Define the Fourier series

$$f(z) = \sum_{n \geqslant 1} a_n q^n \qquad (q = e^{2\pi i z})$$

where z ranges over the upper half-plane $\mathfrak{h} = \{z \in \mathbf{C} : \Im z > 0\}$.

Theorem 5.2.2 (Fermat-Wiles)**.** *Let E be an elliptic curve over* $\mathbf{Q}$ *with conductor E. Then the function $f = f_E$ defined above is a cusp form of weight* 2 *and level N. Moreover, f is an eigenform (eigenvector for all Hecke operators).*

Proof. See [BCDT01] for a proof which relies heavily on previous work by Wiles (with help from Taylor). □

This is one version of the Taniyama-Shimura conjecture. We'll take a moment to explain everything in the theorem.

5.3 Modularity

Recall that $\mathrm{SL}(2,\mathbf{R})$ acts on $\mathfrak{h}$ via fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

There is nothing ad-hoc about this: the group scheme $\mathrm{GL}(n+1)$ acts on $\mathbf{P}^n$ in the obvious way, and our action is just a restriction of the action of $\mathrm{GL}(2,\mathbf{C})$ on $\mathbf{P}^1(\mathbf{C})$ to an action of $\mathrm{SL}(2,\mathbf{R})$ on $\mathfrak{h} \subset \mathbf{P}^1(\mathbf{C})$. The space $\Omega^1(\mathfrak{h})$ of (complex) holomorphic one-forms on $\mathfrak{h}$ consists of differentials $\eta = f(z)dz$. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbf{R})$, one easily computes

$$\gamma^*\eta = f(\gamma z)d(\gamma z) = (cz+d)^{-2} f(\gamma z)dz.$$

Let $N \geqslant 1$ be an integer, and let Γ be one of the following groups:

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}(2,\mathbf{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$
$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}(2,\mathbf{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

We say a function $f : \mathfrak{h} \to \mathbf{C}$ is a *weak modular form* of weight 2 for Γ if it is holomorphic and $f(z)\,dz$ is invariant under the action of Γ. Explicitly, for for all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, we require:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z).$$

The quotient $Y_\Gamma = \mathfrak{h}/\Gamma$ may be a non-compact orbifold, but there is a canonical way of removing the non-smooth points and compactifying (by adding finitely many "cusps") to arrive at a compact Riemann surface X_Γ. We say f is a *modular cusp form* of level N and weight two if it descends to a holomorphic differential on X_Γ. For weight-two forms, the differential $f\,dz$ automatically vanishes on the cusps of X_Γ. For details, see [DS05], or [Kna92, XI.11] for the case $\Gamma = \Gamma_0(N)$. One writes $X_0(N)$, and $X_1(N)$ for $X_{\Gamma_0(N)}$ and $X_{\Gamma_1(N)}$, and calls these *modular curves*. If we write $S_2(\Gamma)$ for the space of weight-two modular forms of level Γ, then by definition we have equality

$$S_2(\Gamma) = \mathrm{H}^0(X_\Gamma, \Omega^1).$$

Modular curves have a moduli-theoretic interpretation. There are canonical bijections [DS05, 1.5]:

$$X_0(N) \simeq \{(E,C) : E \text{ a complex torus and } C \subset E \text{ cyclic of order } N\}/\sim$$
$$X_1(N) \simeq \{(E,P) : E \text{ a complex torus and } P \in E \text{ of order } N\}/\sim .$$

This allows us to define *Hecke operators* which are correspondences on $X_0(N)$. Suppose $p \nmid N$. Then there are canonical maps

$$X_0(N) \xleftarrow{\alpha} X_0(pN) \xrightarrow{\beta} X_0(N).$$

If we think $X_0(N)$ and $X_0(pN)$ as modular spaces, these maps are easy to define. An element of $X_0(pN)$ is a pair (E, C) where C is cyclic of order pN; we may decompose C uniquely as $C_p \oplus C_N$, where C_p and C_N are cyclic of orders p and N. The map α sends (E, C) to (E, C_N) and β sends (E, C) to $(E/C_N, C/C_N)$. Write T_p for the image of $\alpha \times \beta$; this is a subvariety of $X_0(N) \times X_0(N)$. In fact, it is a correspondence, so it induces an endomorphism of $\mathrm{H}(X_0(N))$ for H any Weil cohomology theory. In particular, we have maps called *Hecke operators* (and also denoted T_p):

$$T_p : S_2(\Gamma_0(N)) = \mathrm{H}^0(X_0(N), \Omega^1) \to \mathrm{H}^0(X_0(N), \Omega^1) = S_2(\Gamma_0(N)).$$

See chapter 12 of [RS11] for a careful discussion. A cusp form $f \in S_2(\Gamma_0(N))$ is an *eigenform* if it is an eigenfunction for each T_p where $p \nmid N$.

To see how Theorem 5.2.1 follows from Theorem 5.2.2, we need to briefly introduce the Mellin transform. Recall that for a locally compact abelian group G, the *Pontryagin dual* $\widehat{G}$ of G is the group $\hom(G, S^1)$ of one-dimensional unitary representations of G, with the compact-open topology. The group $\widehat{G}$ is also locally compact. If $G = \mathbf{R}$, then $\widehat{G} = \mathbf{R}$ as well, where we interpret $s \in \mathbf{R}$ as a character of $\mathbf{R}$ via $x \mapsto e^{2\pi i s x}$. For $x \in G, y \in \widehat{G}$, write $\langle x, y \rangle$ instead of $y(x)$. The *Fourier transform* of a function $f : G \to \mathbf{C}$ is the function $\widehat{f} : \widehat{G} \to \mathbf{C}$defined by

$$\widehat{f}(y) = \int_G f(x)\overline{\langle x, y \rangle}\, dx,$$

where dx is a Haar measure on G.

The locally compact group $\mathbf{R}^\times$ (which is isomorphic to $\mathbf{R}$) has dual $i\mathbf{R}$ via $\langle x, s \rangle = x^{-s}$. A Haar measure on $\mathbf{R}^\times$ is $d^\times x = dx/x$. The *Mellin transform* of a function $f : \mathbf{R}^\times \to \mathbf{C}$ is just its Fourier transform:

$$(\mathcal{M}f)(s) = \int_{\mathbf{R}^\times} f(t)\overline{\langle t, s \rangle}\, d^\times t = \int_0^\infty f(t) t^{s-1}\, dt$$

(This is not quite the standard version of the Mellin transform, but it is the most natural in our setting.) For a modular form f of level N, we can look at what is essentially its Mellin transform:

$$\Lambda(f, s) = N^{s/2} \int_0^\infty f(it) t^{s-1}\, dt = \sum_{n \geqslant 1} a_n \int_0^\infty e^{-2\pi n t} t^{s-1}\, dt.$$

Making the substitution $u = 2\pi nt$, we get

$$\Lambda(f,s) = N^{s/2} \sum_{n \geqslant 1} \frac{a_n}{(2\pi n)^s} \int_0^\infty e^{-u} u^{s-1}\, du = N^{s/2}(2\pi)^{-s}\Gamma(s) \sum_{n \geqslant 1} \frac{a_n}{n^s}.$$

Note that if $f = f_E$ for an elliptic curve, we have $\Lambda(f,s) = \Lambda(E,s)$. By work of Hecke, the function $\Lambda(f,s)$ has an analytic continuation to all of $\mathbf{C}$ and a functional equation $\Lambda(f,s) = \pm\Lambda(f, 2-s)$. See [Kna92, VII.9.8] for a modern proof.

The function $\sum a_n n^{-s}$ (coming from a modular form f) has an analytic continuation and a functional equation by a theorem of Hecke. It follows from Theorem 5.2.2 that if E is an elliptic curve over $\mathbf{Q}$, the function $L(E,s)$ has an analytic continuation to $\mathbf{C}$ and the prescribed functional equation.

The modularity theorem has a sort of converse.

Theorem 5.3.1 (Eichler-Shimura)**.** *Let $f = \sum a_n(f) q^n$ be a newform 2 and level N with $a_1 = 1$ and $a_n \in \mathbf{Q}$ for all n. Suppose further that $T_n f = f$ for all n relatively prime to N. Then there exists an elliptic curve E_f over $\mathbf{Q}$ such that $a_n(E_f) = a_n(f)$ for all n.*

Proof. See [Kna92, XI.11] for a proof and a definition of newforms. The elliptic curve E_f can be constructed explicitly in two ways. First, the Riemann surface $X_0(N)$ actually has a canonical model (also denoted $X_0(N)$ over $\mathbf{Q}$; we denote its jacobian by $J_0(N)$. There is a subring $\mathbf{T}_N$ of $\operatorname{End} J_0(N)$ called the *Hecke algebra* which contains all of the T_n. If one puts $I_f = \{T \in \mathbf{T}_N : Tf = 0\}$, then $E_f = J_0(N)/I_f$. Complex-analytically, E is the quotient of $\mathbf{C}$ by the lattice

$$\left\{ \int_i^{\gamma \cdot i} f(z)\, dz : \gamma \in \Gamma_0(N) \right\}.$$

□

5.4 Small analytic rank

Back to BSD. Let E be an elliptic curve over $\mathbf{Q}$ with rank r, and analytic rank

$$r_{\text{an}} = \operatorname{ord}_{s=1} L(E,s)$$

By the previous discussion, $L(E,s)$ has an analytic continuation to $s = 1$, so this is well-defined. As stated earlier, a weak version of BSD is that $r = r_{\text{an}}$. From the functional equation, we get $(-1)^{r_{\text{an}}} = \omega$. The *parity conjecture* is that $r \equiv r_{\text{an}} \pmod 2$. The better variant is that $(-1)^r = \omega$. Since ω can be computed without dealing with $L(E,s)$, the parity can be approached computationally. The parity conjecture is a theorem whenever $Ш(E)$ is finite. See [Dok10] for discussion and a proof.

Theorem 5.4.1. *Let E be an elliptic curve over $\mathbf{Q}$ with $r_{\mathrm{an}} \leqslant 1$. Then $r = r_{\mathrm{an}}$ and $Ш(E)$ is finite.*

Proof. Kolyvagin [Kol88] proved the theorem if $r_{\mathrm{an}} = 0$ and E is modular (which is known over $\mathbf{Q}$). If $r_{\mathrm{an}} = 1$, this is follows from work of Gross and Zagier [GZ86]. □

One can compute $L(E, s)$ to arbitrary precision. In particular, we can look at $L(E, 1)$. It turns out that

$$L(E,1) = (1+\varepsilon)\sum_{n\geqslant 1}\frac{a_n}{n}e^{-2\pi n/\sqrt{N}}$$

If $\varepsilon = -1$, then $L(E, 1) = 0$, and it turns out that

$$L'(E,1) = 2\sum_{n\geqslant 1}\frac{a_n}{n}E_1\left(\frac{2\pi n}{\sqrt{N}}\right)$$

where

$$E_1(x) = \int_x^\infty e^{-t}\,\frac{dt}{t}.$$

Example 5.4.2. Let E be the elliptic curve $y^2 = x^3 + 875x$ over $\mathbf{Q}$. We can compute $L(E, 1) = -3.9\ldots$. In particular, $L(E, 1) \neq 0$, which implies $r_{\mathrm{an}} = 0$. The above theorem tells us that $r = 0$, so $E(\mathbf{Q}) = E(\mathbf{Q})_{\mathrm{tors}} = \{O, (0, 0)\}$. ▷

Example 5.4.3. Let E be the elliptic curve $y^2 = x^3 + 877x$ over $\mathbf{Q}$. It turns out that $L(E, 1) = 0.000\ldots$. This does *not* imply $L(E, 1) = 0$. We can compute $\omega = -1$, which means r_{an} is odd. Thus we cannot have $L(E, 1) = 0$. The BSD conjecture would imply E has rank at least one. One can compute $L'(E, 1) = 32.7\cdots \neq 0$. In particular, $r_{\mathrm{an}} \leqslant 1$, so the above theorem tells us $r = 1$. In other words, $E(\mathbf{Q}) \simeq \mathbf{Z}/2 \oplus \mathbf{Z}$, hence $E(\mathbf{Q})$ is infinite. ▷

5.5 The strong Birch and Swinnerton-Dyer conjecture

The standard version of BSD predicts the order of vanishing of the L-function $L(E, s)$ of an elliptic curve at 1 in terms of the algebraic rank of E. There is a stronger version of the conjecture that also predicts the leading term in the Laurent expansion of $L(E, s)$ at 1.

Conjecture 5.5.1 (strong BSD)**.** *Let E be an elliptic curve over $\mathbf{Q}$. Then $\mathrm{rk}(E) = r_{\mathrm{an}}(E)$, $Ш(E)$ is finite, and*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \frac{\Omega_E \operatorname{Reg}_E \#Ш(E)\prod_p c_p}{\#E(\mathbf{Q})_{\mathrm{tors}}^2}.$$

We need to explain the quantities appearing in the conjecture. First we define the *real period* Ω_E of E. Choose a minimal Weierstrass model

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

for E, with the $a_i \in \mathbf{Z}$ and $\Delta = -16(4^3 + 28b^2)$ minimal with respect to divisibility. It is not obvious that this is possible. In fact, it can only be done for elliptic curves over global fields with class number one [Sil09, VIII.8.3]. The differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

is called the *invariant differential* associated to E. It is unique up to a unit in $\mathbf{Z}$ [Sil09, VII.1.3]. We define

$$\Omega_E = \int_{E(\mathbf{R})} |\omega|,$$

where we choose the orientation of $E(\mathbf{R})$ necessary to make the integral positive. The real period of E is easily computable using a trick that takes advantage of the fast convergence of the algebro-geometric mean.

Next we define the *regulator* Reg_E of E. Our minimal model for E induces an embedding $E \hookrightarrow \mathbf{P}^2$, and we write h for the induced Weil height (see 3.10 for a general definition). We can write any $x \in E(\mathbf{Q})$ as (x_0, x_1, x_2) with the $x_i \in \mathbf{Z}$ and $\gcd(x_0, x_1, x_2) = 1$. Explicitly,

$$h(x) = \log \max\{|x_0|, |x_1|, |x_2|\}.$$

Recall that the Néron-Tate height $\widehat{h}$ associated with our embedding can be computed as

$$\widehat{h}(x) = \lim_{n\to\infty} \frac{h(2^n \cdot x)}{4^n}.$$

Using this we define a pairing on $E(\mathbf{Q})$:

$$\langle x, y\rangle = \frac{1}{2}\left(\widehat{h}(x+y) - \widehat{h}(x) - \widehat{h}(y)\right).$$

This induces a nondegenerate bilinear pairing (hence the structure of a Hilbert space) on $V = E(\mathbf{Q}) \otimes \mathbf{R}$. There is a canonical Haar measure on any Hilbert space. It is the unique Haar measure such that, given an orthonormal basis $\{v_1, \ldots, v_r\}$ of V, assigns to the fundamental domain

$$\left\{\sum_{i=1}^{r} \lambda_i v_i : 0 \leqslant \lambda_i \leqslant 1\right\}$$

the volume 1. For a lattice (discrete, cocompact subgroup) $\Lambda \subset V$, put $\mathrm{vol}(\Lambda) = \mathrm{vol}(V/\Lambda)$. Then

$$\mathrm{Reg}_E = \mathrm{vol}(E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}})^2,$$

where $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}}$ is a thought of as a lattice in $E(\mathbf{Q}) \otimes \mathbf{R}$. More explicitly, for any basis $\{x_1, \dots, x_r\}$ of $E(\mathbf{Q})$, one has

$$\mathrm{Reg}_E = \left|\det\left(\langle x_i, x_j\rangle_{i,j}\right)\right|.$$

The *Tate-Shafarevich group* of E is

$$Ш(E) = \ker\left(\mathrm{H}^1(\mathbf{Q}, E) \to \prod_v \mathrm{H}^1(\mathbf{Q}_v, E)\right)$$

where as usual we write $\mathrm{H}^1(k, A)$ for $\mathrm{H}^1(G_k, A(\bar{k}))$ when k is a field and A is a commutative group variety over k.

The c_p are *Tamagawa numbers* of E. Let $E_0(\mathbf{Q}_p)$ be the group of points in $E(\mathbf{Q}_p)$ whose reduction modulo p is is nonsingular. We define

$$c_p = [E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$$

Clearly $c_p = 1$ if E has good reduction at p. The c_p are easy to compute using Tate's algorithm.

5.6 Predicting the order of Ш

Example 5.6.1. Let E be the rational elliptic curve **??**. Using Sage, we can predict the order of $Ш(E)$. First, $\Omega_E \approx$ **??**. Next, we compute $L(E,1) \approx$ **??** $\neq 0$, so $r_{\mathrm{an}}(E) = 0$. By Theorem 5.4.1, $E(\mathbf{Q})$ and $Ш(E)$ are both finite. It follows that the regulator of E is 1. Moreover, the discriminant of E is **??**, so we only need to compute $c_3 =$ **??** and $c_{227} =$ **??**. Finally, it is possible to compute $\#E(\mathbf{Q})_{\mathrm{tors}} =$ **??**. We now know everything in the BSD formula except for the cardinality of $Ш(E)$. Solving for it, we get (conjecturally):

$$\#Ш(E) = \frac{L(E,1) \cdot \#E(\mathbf{Q})_{\mathrm{tors}}^2}{\Omega_E \cdot c_3 \cdot c_{227}} \approx \textbf{??}$$

so we could expect $Ш(E) = 9$. ▷

Example 5.6.2. Let E be the rational elliptic curve **??** (this is the quadratic twist of $y^2 = x^3 + 4x^2 - 48x + 80$ by -139). We can compute $L(E,1) \approx$ **??**, which may or may not be zero. Similarly, $L'(E,1)$ and $L''(E,1)$ appear to be zero, but $L'''(E,1) \approx$ **??** $\neq 0$. So we would guess that $r_{\mathrm{an}}(E) = 3$. We know

that $(-1)^{r_{\mathrm{an}}} = \omega = -1$, so r_{an} is odd. This tells us $L(E,1) = 0$ on the nose. One can do a "2-descent" to show that $\operatorname{rk} E = ??$ and $E(\mathbf{Q})_{\mathrm{tors}} = ??$. In fact, $E(\mathbf{Q})$ has as a basis

$$??.$$

We can now compute

$$\begin{aligned} \mathrm{Reg}_E &= ?? \\ \Omega_E &= ?? \\ \#E(\mathbf{Q})_{\mathrm{tors}} &= ?? \\ \Delta &= ?? \\ c_{37} &= ?? \\ c_{139} &= ?? \end{aligned}$$

Since $r_{\mathrm{an}} \geqslant 1$, we don't know if $Ш(E)$ is finite, but assuming BSD its order is

$$\frac{L^{(3)}(E,1)/3!}{\Omega_E \cdot \mathrm{Reg}_E \cdot c_{139}} \approx ??.$$

Recall that if $r_{\mathrm{an}} = 1$, then work of Gross-Zagier and Kolyvagin implies $r = 1$. Since $r > 1$, we have $r_{\mathrm{an}} > 1$, and since r_{an} is odd it must be 3. So $L'(E,1) = L''(E,1) = 0$. ▷

In general, if $Ш(E)$ is finite, then its cardinality must be a square. This is because there is a canonical alternating pairing $Ш(E) \times Ш(E) \to \mathbf{Q}/\mathbf{Z}$, which is nondegenerate if E is finite. See [Mil06, I.6] for a definition of this pairing in much greater generality. Note that the parity conjecture holds over $\mathbf{Q}$ by the functional equation, which is proved via the modularity theorem.

In his paper [Gol85] Goldfeld, drawing on work of Gross and Zagier, used this curve (in particular, the fact that it has analytic rank 3) to solve a very old problem of Gauss. For every $\varepsilon > 0$, there is an effectively computable constant $c > 0$ such that the class number $h(D)$ of the field $\mathbf{Q}(\sqrt{-D})$ for $D > 0$ square-free satisfies the bound

$$h(D) > c\,(\log D)^{1-\varepsilon}\,.$$

It follows that for *any* constant C, it is possible to enumerate the (finite) list of imaginary quadratic fields with class number $h \leqslant C$. For example, the only imaginary quadratic fields with class number 1 are $\mathbf{Q}(\sqrt{-D})$ for D one of

$$1, 2, 3, 7, 11, 19, 43, 67, 163.$$

5.7 Average orders of Selmer groups

For $a, b \in \mathbf{Z}$ with $4a^3 + 27b^2 \neq 0$, let $E_{a,b}$ be the rational elliptic curve $y^2 = x^3 + ax + b$. Set

$$\mathcal{E} = \{E_{a,b} : a, b \in \mathbf{Z} : 4a^3 + 27b^2 \neq 0 \text{ and } p^6 \nmid b \text{ whenever } p^4 \mid a\}.$$

Every elliptic curve over $\mathbf{Q}$ is isomorphic to a unique element of $\mathcal{E}$. We define a "naive height" on $\mathcal{E}$ by $H(E_{a,b}) = \max\{|4a^3|, 27b^2\}$. For any $x \geqslant 0$, set

$$\mathcal{E}_x = \{E \in \mathcal{E} : H(E) \leqslant x\}.$$

Given a map $\phi : \mathcal{E} \to \mathbf{R}$, we define (if the limit exists)

$$\operatorname{avg}(\phi) = \lim_{x\to\infty} \frac{\sum_{E\in\mathcal{E}_x} \phi(E)}{\#\mathcal{E}_x},$$

and let $\overline{\operatorname{avg}}(\phi)$ be the corresponding lim sup.

Theorem 5.7.1 (Bhargava-Shankar)**.** *We have* $\operatorname{avg}(\#\operatorname{Sel}_2) = 3$ *and* $\overline{\operatorname{avg}}(\#\operatorname{Sel}_3) \leqslant 4$.

Proof. See [BS10b] for a proof of the first equality, and [BS10a] for a proof of the second inequality. □

As a corollary, $\overline{\operatorname{avg}}(\mathrm{rk}) \leqslant \frac{7}{6}$. Many mathematicians (including Zywina) expect the average to be $\frac{1}{2}$. To see that the average rank is at most $\frac{7}{6}$, note that since since $E(\mathbf{Q})/3E(\mathbf{Q}) \hookrightarrow \operatorname{Sel}_3(E)$, we have $3^{\mathrm{rk}\, E} \leqslant \#\operatorname{Sel}_3(E) = 3^s$. It follows that $\mathrm{rk}\, E \leqslant s \leqslant \frac{3^s+3}{6}$, so

$$\overline{\operatorname{avg}}(\mathrm{rk}) \leqslant \frac{\overline{\operatorname{avg}}(3^s)}{6} + \frac{1}{2} \leqslant \frac{4}{6} + \frac{1}{2} = \frac{7}{6}.$$

5.8 The congruent number problem

Fix a squarefree integer $d \geqslant 1$. We say that d is a *congruent number* if there is a right triangle with rational side lengths, with area d. The requirement that n is squarefree is not significant: we can always scale the triangle by a rational number to make its area squarefree. From the well-known right triangle with sides $(3, 4, 5)$, we see that 6 is a congruent number. Our general equations are:

$$a^2 + b^2 = c^2$$
$$ab/2 = d.$$

These equations describe a curve $C_d \subset \mathbf{A}^3_{\mathbf{Q}} = \operatorname{Spec} \mathbf{Q}[a, b, c]$. The integer d is congruent precisely when $C_d(\mathbf{Q}) \neq \varnothing$. It is natural to ask whether a given

integer (for example $d = 157$) is congruent. The curve C_d is not "nice" in the technical sense, because it is not projective. Let E_d be the curve $y^2 = x^3 - d^2x$. This is birational to C_d via the map $f : C_d \xrightarrow{\sim} E_n \smallsetminus \{O, (0:0:1), (0:\pm d:1)\}$ defined by

$$(a, b, c) \mapsto \left(dbc(a+c) : d^2((a+c)^2 + b^2) : b^2c\right).$$

This map has birational inverse

$$(x : y : z) \mapsto \left(\frac{x^2 - n^2}{yz}, \frac{2nx}{y}, \frac{x^2 + n^2}{yz}\right).$$

The only obvious rational points on E_d are the origin, $(0:0:1)$ and $(0:\pm n:1)$, which comprise $E_d(\mathbf{Q})_{\text{tors}} = E_d[2]$. Thus $C_d(\mathbf{Q}) \neq \varnothing$ if and only if $\operatorname{rk} E_d > 0$. Since d is congruent if and only if C_d has rational points, we conclude that d is congruent precisely when E_d has positive rank. Assuming BSD, this occurs if and only if $L(E_d, 1) = 0$, i.e. $r_{\text{an}}(E_d) \geqslant 1$. If $L(E_d, 1) \neq 0$, which is something that can be computationally verified, then $r_{\text{an}}(E_d) = 0$, so by Theorem 5.4.1, we know that E_d has rank zero. In other words, it is easy to show that a given integer d is *not* congruent, simply by checking that $L(E_d, 1) \neq 0$.

The fact that C_d and E_d are birational gives a way of constructing many different rational triangles with area d, using the group law on E_d. For instance, in our example $d = 6$, the triple $(a, b, c) = (3, 4, 5)$ maps to the point $x = \mathbf{??}$ in $E_d(\mathbf{Q})$. One can compute $2 \cdot x = \mathbf{??}$, which corresponds to a triangle with sides $\mathbf{??}$, at least up to sign. Each multiple $n \cdot x$ gives a different triangle, with rapidly increasing complexity. We can use Sage to compute the first few:

n	(a, b, c)
2	**??**
3	**??**
4	**??**
5	**??**
6	**??**

It is possible to determine algorithmically whether any given d is congruent, but only under the assumption that BSD holds. For an integer t, let $\chi_t : G_{\mathbf{Q}} \to \{\pm 1\}$ be the Dirichlet character associated to the extension $\mathbf{Q}(\sqrt{t})/\mathbf{Q}$. We define

$$\theta_t(q) = \sum_{n > -\infty} q^{tn^2}$$

$$g(q) = q \prod_{n \geqslant 1} (1 - q^{8n})(1 - q^{16n}) = \sum_{m,n \in \mathbf{Z}} (-1)^n q^{(4m+1)^2 + 8n^2}.$$

For each t, the function θ_t is a modular form of weight $1/2$, level $4t$ and character χ_t. The function g is the unique normalized newform of level 1, weight 128 and character χ_{-2}. We can write formal expansions $\theta_2 g = \sum a(n)q^n$ and $\theta_4 g = \sum b(n)q^n$. The functions $\theta_2 g$ and $\theta_4 g$ are modular forms of weight $3/2$, level 128, and trivial (resp. χ_8) character. It turns out that the coefficients $a(n)$ and $b(n)$ have a straightforward interpretation in terms of sums of squares. Now let $E = E_1$ be the curve $y^2 = x^3 - x$, and let $\Omega = \Omega_E$ be its real period; one has

$$\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \approx \mathbf{??}.$$

Theorem 5.8.1 (Tunnell)**.** *If $d \geqslant 1$ is a squarefree integer, then*

$$L(E_d, 1) = \begin{cases} a(d)^2 \Omega d^{-1/2}/2 & \text{if } d \text{ is odd} \\ b(d/2)^2 \Omega d^{-1/2} & \text{if } d \text{ is even.} \end{cases}$$

Proof. This is Theorem 3 of [Tun83]. Tunnell uses a result of Waldspurger giving a functional equation for certain types of L-functions. □

Corollary 5.8.2. *Assume the weak BSD conjecture. Then an integer $d \geqslant 1$ is congruent if and only if $a(d) = 0$ in the case where d is odd, or $b(d/2) = 0$ in the case where d is even.*

If we define

$$\begin{aligned} A(n) &= \#\{(x, y, x) \in \mathbf{Z}^3 : x^2 + 2y^2 + 8z^2 = n\} \\ B(n) &= \#\{(x, y, z) \in \mathbf{Z}^3 : x^2 + 2y^2 + 32z^2 = n\} \\ C(n) &= \#\{(x, y, z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 8z^2 = n/2\} \\ D(n) &= \#\{(x, y, z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 32z^2 = n/2\}, \end{aligned}$$

Then for d odd, $a(d) = 0$ if and only if $A(d) = 2B(d)$, and for d even, $b(d/2) = 0$ if and only if $C(d) = 2D(d)$. These equalities are easy to check via a brute search. An easy example is $d = 2$. One has $C(2) = D(2) = 2$, so $b(1) \neq 0$. Since this implies $L(E_2, 1) \neq 0$, we can use Theorem 5.4.1, to see that $n = 2$ is not a congruent number (unconditionally).

5.9 The Sato-Tate conjecture

Let E be an elliptic curve over $\mathbf{Q}$ with conductor N. For primes p not dividing N, recall we defined $a_p(E) = p + 1 - \#E(\mathbf{F}_p)$, and proved the Hasse bound $|a_p(E)| \leqslant 2\sqrt{p}$. Thus if we define $b_p(E) = a_p(E)/2\sqrt{p}$, the numbers $b_p(E)$ lie in the interval $[-1, 1]$. It is natural to ask, for fixed E, how the $b_p(E)$ are

distributed in that interval. It is useful to set up some terminology, which we do following the appendix to Chapter 1 in [Ser68].

For a topological space, let $C_0(X)$ denote the Banach space of continuous complex-valued functions vanishing at infinity. This is the completion of the space of continuous functions with compact support. If X is locally compact, it is a theorem (one could take this as a definition of Borel measures) that the dual of $C_0(X)$ is isomorphic as a Banach space to the space of Borel measures on X. A measure μ corresponds to the functional

$$f \mapsto \int_X f \, d\mu.$$

See [Rud87, 6.19] for a proof. Given $x \in X$, write δ_x for the point mass $\int f \, d\delta_x = f(x)$. For discrete $S \subset \mathbf{R}$, we call a sequence $\{x_s\}_{s \in S}$ of points in X *equidistributed* with respect to μ if

$$\mu = \lim_{c \to \infty} \frac{1}{\#\{s \in S : s \leqslant c\}} \sum_{s \leqslant c} \delta_{x_s}$$

in the weak topology. By definition, this is the same as requiring, for each continuous f with compact support, the equality

$$\lim_{c \to \infty} \frac{1}{\#\{s \in S : s \leqslant c\}} \sum_{s \leqslant c} f(x_s) = \int_X f \, d\mu.$$

If X is a smooth oriented n-dimensional manifold, then any n-form ω induces a Borel measure via

$$f \mapsto \int_X f\omega.$$

We will often identify ω with the measure it induces. In particular, we will often abuse terminology by calling a sequence equidistributed with respect to ω.

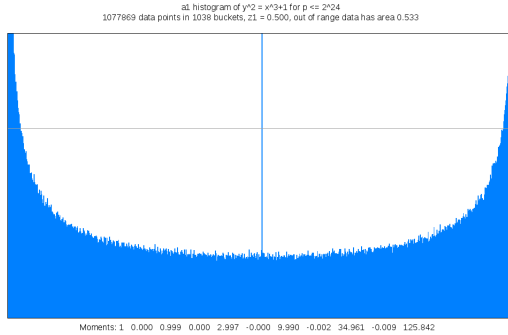
Let E be an elliptic curve over $\mathbf{Q}$. Recall that we defined $b_p(E) = a_p(E)/2\sqrt{p}$. The Sato-Tate conjecture predicts the distribution of the b_p in the interval $[-1, 1]$. If E has complex multiplication, then things were worked out quite a while ago. Let $k = \mathrm{End}^\circ(E)$; this is an imaginary quadratic field (we could write $k = \mathbf{Q}(\sqrt{-D})$ for D a positive squarefree integer). If $p \geqslant 5$ is inert in k, then $a_p(E) = 0$. The prime p is inert exactly when $-D$ is not a quadratic residue modulo p, and this happens for half of the primes.

Theorem 5.9.1 (Deuring, Hecke)**.** *Let E be an elliptic curve over $\mathbf{Q}$ with complex multiplication. Then the sequence $\{b_p(E)\}_p$ is equidistributed in $[-1, 1]$ with respect to the measure*

$$\frac{1}{2}\delta_0 + \frac{dt}{2\pi\sqrt{1 - t^2}}.$$

Proof. Do this for an arbitrary abelian variety with complex multiplication, using the associated ℓ-adic representation. □

In other words, if we restrict ourselves to primes that split in k, the $b_p(E)$ are distributed according to the following graph, corresponding to the curve $y^2 = x^3 + 1$. The image was taken from Andrew Sutherland's web page http://math.mit.edu/~drew, which has many more examples.

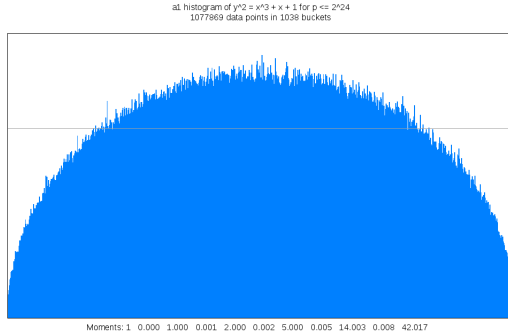


The Sato-Tate conjecture is an analogous prediction for elliptic curves without complex multiplication.

Conjecture 5.9.2 (Sato-Tate)**.** *Let E be a non-CM elliptic curve over $\mathbf{Q}$. Then the sequence $\{b_p(E)\}_p$ is equidistributed in $[-1,1]$ with respect to the measure*

$$\frac{2}{\pi}\sqrt{1-t^2}\,dt.$$

Here is the example $y^2 = x^3 + x + 1$, also taken from Sutherland's web page.



Theorem 5.9.3 (Barnet-Lamb, Geraghty, Harris, Taylor)**.** *The Sato-Tate conjecture is true.*

Proof. See [Tay08] for a proof, drawing on ideas from [BLGHT11]. □

There is a refined version of the Sato-Tate conjecture. Let $\rho = \{\rho_\ell : G_{\mathbf{Q}} \to GL(2, \mathbf{Z}_\ell)\}$ be a strictly compatible family of ℓ-adic representations in the sense of [Ser68, ch.1]. For almost all primes p, the characteristic polynomial of $\rho_\ell(\mathrm{fr}_p)$ will be of the form $t^2 - a_p t + p$. Assume ρ is *pure* in the sense that the roots $\alpha_p, \bar{\alpha}_p$ of $t^2 - a_p t + p$ are q-Weil.

Conjecture 5.9.4 (Lang-Trotter)**.** *For any integer n and imaginary quadratic field k, there are constants $C(n, \rho)$ and $C(k, \rho)$ such that*

$$\#\{p \leqslant x : \mathbf{Q}(\alpha_p) = k\} \sim C(k, \rho)\frac{\sqrt{x}}{\log x}$$
$$\#\{p \leqslant x : a_p = n\} \sim C(n, \rho)\frac{\sqrt{x}}{\log x}.$$

See the introduction to [LT76] for the original statement and some motivation.

5.10 Some computations

Let $d = 157$. We hope to show that d is congruent, i.e. that is is the area of a right triangle with rational side lengths. In other words, the curve C_d defined as the solution set to

$$a^2 + b^2 = c^2$$
$$ab/2 = d$$

has a rational point. We have seen that this is equivalent to the elliptic curve $E_d : y^2 = x^3 - d^2 x$ having positive rank.

We'll use Sage to do this. Sage can be accessed online at `http://sagenb.com/`, or just type `sage` in the command line of a computer that has Sage installed.

In Sage, the constructor `EllipticCurve`$([a_1, a_2, a_3, a_4, a_6])$ returns the elliptic curve

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The simpler constructor `EllipticCurve`$([a_4, a_6])$ returns the elliptic curve $y^2 = x^3 + a_4 x + a_6$. Sage will return an error if the curve you try to construct is singular. Since we are interested in the curve $E_{157} : y^2 = x^3 - 157^2 x$, we define

```
E = EllipticCurve([-157^2, 0])
```

If we had wanted to define an elliptic curve over a finite field $\mathbf{F}_q$, we would make sure some of the coefficients were elements of $\mathbf{F}_q$, as in `EllipticCurve([GF(5)(1) 1])`. We can compute the conductor of by `E.conductor()`; in our case E_{157} has conductor **??**. Usually one can compute the rank `E.rank()` and generators for the Mordell-Weil group `E.gens()`. In our case, these return a warning. Sage's usual algorithm was not able to determine the rank of E_{157}, and it asks you to do a two-descent. We do this:

```
E.two_descent(second_limit=13)
```

As Sage does the 2-descent, it outputs a bunch of text describing what it does (essentially a computation of $E(\mathbf{Q})/2$ and $Ш(E)[2]$). Once the 2-descent is complete, we can compute the rank to be **??** and a generator to be

??.

This corresponds to a triangle with the shorter two sides being

??.

There are a number of other things that Sage can do with elliptic curves. To make computations faster, let's try the elliptic curve

```
E = EllipticCurve([4,6])
```

described by the equation **??**. This curve has rank **??** and generator **??**. We can do computations with points on our curve:

```
P = E.gens()[0]
5*P # as an element of E(Q)
P.height() # Neron-Tate height of P
```

A lot of analytic data can be computed:

```
E.torsion_subgroup() # trivial for this curve
L = E.lseries().dokchitser() # the L-function of E
L(1) # looks like zero
L.derivative(1,2) # non-zero, so r_an<=1
E.root_number() # sign in function equation (=-1, so r_an is o
E.regulator()
E.sha().an() # predicted order assuming BSD
```

A fantastic place to learn more about Sage is its documentation page at http://www.sagemath.org/doc/.

5.11 The Sato-Tate conjecture and Haar measures

Let E be an elliptic curve over $\mathbf{Q}$. Recall we defined $b_p(E) = a_p(E)/2\sqrt{p}$. If E has CM, then the b_p are uniformly distributed in $[-1,1]$ with respect to the measure

$$\frac{1}{2}\delta_0 + \frac{dt}{2\pi\sqrt{1-t^2}},$$

and if E is not CM, then the b_p are uniformly distributed with respect to

$$\frac{2}{\pi}\sqrt{1-t^2}\,dt.$$

This has a natural reformulation which makes generalization easier. The characteristic polynomial of $\rho_{E,\ell}(\mathrm{fr}_p)$ is $t^2 - a_p t + p$. If we normalize to have roots with absolute value 1, we get $\varphi_p = t^2 - \frac{a_p}{\sqrt{p}}t + 1$. This is the characteristic polynomial of a unique conjugacy class in $\mathrm{SU}(2)$. If we write X for the space $\mathrm{SU}(2)^\natural$ of conjugacy classes in $\mathrm{SU}(2)$, then $p \mapsto \varphi_p$ can be thought of as a map $\{\text{primes}\} \to X$. Embed $\mathrm{U}(1)$ in $\mathrm{SU}(2)$ by the diagonal, and let $K = N(\mathrm{U}(1))$ be its normalizer. The group K is compact, so it has a unique normalized Haar measure.

Theorem 5.11.1. *If E is an elliptic curve with complex multiplication, then the set $\{\varphi_p(E)\} \subset \mathrm{SU}(2)^\natural$ is equidistributed with respect to the pushforward of the normalized Haar measure on $N(\mathrm{U}(1))$.*

Proof. This is a restatement of Theorem 5.9.1. To see this, note that the trace map induces an isomorphism

$$\mathrm{tr} : \mathrm{SU}(2)^\natural \xrightarrow{\sim} [-2,2].$$

The group $K = N(\mathrm{U}(1))$ has two connected components, both isomorphic to S^1:

$$K = \left\{ \begin{pmatrix} z & \\ & \bar{z} \end{pmatrix} : |z| = 1 \right\} \cup \left\{ \begin{pmatrix} & -z \\ \bar{z} & \end{pmatrix} : |z| = 1 \right\}.$$

The first connected component is mapped to $[-2,2]$ via $z \mapsto 2\Re(z)$, and the second is mapped via $z \mapsto 0$. It is easy to check that the pushforward of the Haar measure on K is exactly $\frac{1}{2}\delta_0 + \frac{dt}{2\pi\sqrt{4-t^2}}$. □

For non-CM elliptic curves, let $K = \mathrm{SU}(2)$. Then the Sato-Tate conjecture states that $\{\varphi_p\} \subset \mathrm{GL}(2,\mathbf{C})^\natural$ is uniformly distributed with respect to the pushforward of the normalized Haar measure on K. To see this, check that the pushforward by the trace of the normalized Haar measure on K to $[-2,2]$ is $\frac{1}{2\pi}\sqrt{4-t^2}dt$.

More generally, let A be a d-dimensional abelian variety over $\mathbf{Q}$, and let ℓ be a prime at which A has good reduction. For any prime p of good reduction, we have the characteristic polynomial P_{A_p} of the Frobenius at p acting on $T_\ell A$. The roots of this polynomial are p-Weil, so if we write $P_{A_p}(t) = \prod(t-\omega_i)$, then the polynomial $\varphi_p(A) = \prod\left(t - \frac{\omega_i}{\sqrt{p}}\right)$, has roots with absolute value 1. Then by [Kat88, 13.1], $\varphi_p(A)$ determines a conjugacy class in $\mathrm{SU}(2d, \mathbf{C})$. As before, we think of $\varphi(A)$ as a map $\{\text{good primes}\} \to \mathrm{GL}(2d, \mathbf{C})^\natural$.

Conjecture 5.11.2 (Serre)**.** *There exists a compact real Lie group K in $\mathrm{GL}(2d, \mathbf{C})$ such that $\{\varphi_p(A)\} \subset \mathrm{GL}(2d, \mathbf{C})^\natural$ is equidistributed with respect to the pushforward of the normalized Haar measure on K.*

There is a conjectural prediction of the group K, which we will treat in the next section.

5.12 Motives and the refined Sato-Tate conjecture

The following mostly follows Serre's original paper [Ser94], but see [Ser12] for a more elementary and explicit approach.

Let k be a field, and let X be an n-dimensional smooth variety over k. Write $\mathrm{A}(X) = \mathrm{A}^\bullet(X)$ for the Chow ring of X, consisting of algebraic cycles modulo rational equivalence. The intersection product makes $\mathrm{A}(X)$ into a commutative unital ring – for details, see [Ful98, 8.3]. There is a natural "composition" map

$$\mathrm{A}(Y \times Z) \otimes \mathrm{A}(X \times Y) \to \mathrm{A}(X \times Z), \qquad (*)$$

defined by $g \circ f = \pi_{X\times Z,*}(\pi^*_{Y\times Z} g \cdot \pi^*_{X\times Y} f)$. This satisfies all of the natural linearity and functoriality properties one would expect [Ful98, 16.1].

There is a canonical "degree map" $\deg : \mathrm{A}^n \to \mathbf{Z}$, and we say a cycle $\alpha \in \mathrm{A}^r(X)$ is *numerically equivalent to zero* if $\deg(\alpha\cdot\beta) = 0$ for all $\beta \in \mathrm{A}^{n-r}(X)$. Write $\mathrm{A}_{\mathrm{num}}(X)$ for the quotient of $\mathrm{A}(X)$ by the (graded) ideal generated by

$$\{\alpha \in \mathrm{A}(X) : \alpha \text{ is numerically equivalent to zero}\}.$$

Definition 5.12.1. *Let k be a field. A* (pure) motive over k *is a triple (X, e, r), where X is a smooth projective variety over k, $e \in \mathrm{A}_{\mathrm{num}}(X \times X)_{\mathbf{Q}}$ is an idempotent, and $r \in \mathbf{Z}$.*

See [And04, 4.1.3] for details. One defines a morphism $(X, e, r) \to (Y, f, s)$ to be an element of

$$f \cdot \mathrm{A}^{\dim X - r - s}(X \times Y)_{\mathbf{Q}} \cdot e.$$

Morphisms are composed via the "composition map" $(*)$.

With this, write $\mathsf{M}(k)$ for the category of (numerical) motives over k. Let SmProj_k be the category of smooth projective varieties over k, and let $h : \mathsf{SmProj}_k \to \mathsf{M}(k)$ be the functor $X \mapsto (X, \Delta_X, 0)$. The category $\mathsf{M}(k)$ is obviously $\mathbf{Q}$-linear, and has a Tannakian structure induced by $h(X) \otimes h(Y) = h(X \times Y)$. In fact, $\mathsf{M}(k)$ is a semisimple abelian category [Jan92]. One should think of a Weil cohomology theory as a functor $\mathrm{H} : \mathsf{M}(k) \to \mathsf{grAlg}_L$ for some field L (c.f. [And04, 4.2.5.1]).

Write $1 = \mathrm{H}(\mathbf{A}^0)$ for the trivial motive. Since every variety has a unique morphism $X \to \mathbf{A}^0$, there is a unique morphism $1 \to M$ for every motive M. The rational point $\infty \in \mathbf{P}^1$ determines a splitting of $1 \to h(\mathbf{P}^1)$, hence a direct sum decomposition $h(\mathbf{P}^1) = 1 \oplus 1(-1)$, where $1(-1)$ is the motive $(\mathbf{P}^1, [\infty] \times \mathbf{P}^1, 0)$. We define $1(r) = 1(-1)^{\otimes(-r)}$; these are called *Tate motives*. In general, put $M(r) = M \otimes 1(r)$. There is a decomposition $h(\mathbf{P}^n) = 1 \oplus \cdots \oplus 1(-n)$. If A is a d-dimensional abelian variety over k, then there is a unique decomposition $h(A) = h^0(A) \oplus \cdots \oplus h^{2d}(A)$ in $\mathsf{M}(k)$ such that $[n]$ acts as multiplication by n^i on each $h^i(A)$ [vdGM13, 13.29]. What is more, there are canonical isomorphisms $h^i(A) \simeq \bigwedge^i h^1(A)$, inducing an isomorphism $h(A) \simeq \bigwedge^\bullet h^1(A)$ (13.47, loc. cit.).

Let k be a number field, and choose an embedding $\sigma : k \hookrightarrow \mathbf{C}$. We have a Betti realization functor $\mathrm{H}_\sigma : \mathsf{M}(k) \to \mathsf{grAlg}_{\mathbf{Q}}$, assigning to a motive $M = (X, e, r)$ the vector space

$$\mathrm{H}_\sigma(M) = e^* \cdot \mathrm{H}^\bullet_{\mathrm{sing}}(X(\mathbf{C}), \mathbf{Q}) \otimes \mathrm{H}^2_{\mathrm{sing}}(\mathbf{P}^1)^{\otimes(-r)}$$

Assuming Grothendieck's standard conjectures, the functor H_σ is a *fiber functor*, so $\mathsf{M}(k)$ is equivalent to the category of representations of the (pro-reductive) *motivic Galois group*

$$G_{\mathrm{mot}}(k) = \mathrm{Aut}^\otimes(\mathrm{H}_\sigma) = \left\{ (x_M) \in \prod_{M \in \mathsf{M}(k)} \mathrm{GL}(\mathrm{H}_\sigma M) : x_M \circ f^* = f^* \circ x_N \text{ for } f : \right.$$

For a motive M, let G_M be the automorphism group of the restriction of the fiber functor to the largest Tannakian subcategory of $\mathsf{M}(k)$ containing M. There are obvious projections from $G_{\mathrm{mot}}(k)$ to the groups G_M.

Let M be a motive. There is a map $w : \mathbf{G}_m \to G_M$, induced by the grading $\mathrm{H}_\sigma M = \bigoplus \mathrm{H}^d_\sigma(M)$. The action of $a \in \mathbf{G}_M$ on the d-th piece is by a^{-d}. For example, if E is an elliptic curve without complex multiplication, then for $M = h^1(E)$, $G_M = \mathrm{GL}(2)$ and $w : \mathbf{G}_m \to \mathrm{GL}(2)$ is the inverse of the canonical injection. (**this is not correct!**)

For a motive M, there are ℓ-adic realizations $\mathrm{H}_\ell(M)$ coming from étale cohomology. After we fix a prime ℓ, the representation $\rho_{M,\ell}$ is unramified

at all but finitely many places. For those unramified places v, put $\varphi_v(M) = w(Nv^{1/2})\rho_{M,\ell}(\mathrm{fr}_v)$.

Let $T = 1(-1)$ be the Tate motive, and let $t : G_{\mathrm{mot}}(k) \to G_T$ be the canonical projection. For any motive M, let G_M^1 be the image of $\ker(t)$ under the projection $G_{\mathrm{mot}}(k) \to G_M$.

Conjecture 5.12.2 (Serre)**.** *Let M be a motive over a number field k. Let K be a maximal compact subgroup of G_M^1. The elements $\varphi_v(M)$ have eigenvalues in $\bar{\mathbf{Q}}$, and determine a unique conjugacy class (independent of ℓ) $\varphi_v(M) \in G_M^1(\mathbf{C})^\natural$. The set $\{\varphi_v(M)\} \subset G_M^1(\mathbf{C})^\natural$ is equidistributed with respect to the pushforward of the normalized Haar measure on K.*

5.13 The Bloch-Kato conjecture

Let E be an elliptic curve over $\mathbf{Q}$. Recall that the (strong) Birch and Swinnerton-Dyer conjecture is the formula

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{\mathrm{rk}\, E}} = \frac{\Omega_E \operatorname{Reg}_E \#Ш(E) \prod_p c_p}{\#E(\mathbf{Q})^2_{\mathrm{tors}}},$$

together with the claim that everything involved is well-defined and finite. For a number field k, recall that the *Dedekind zeta function* of k is the series

$$\zeta_k(s) = \sum_{\mathfrak{a}\subset \mathfrak{o}_k} \frac{1}{(N\mathfrak{a})^s},$$

where $N\mathfrak{a} = [\mathfrak{o}_k : \mathfrak{a}]$ for an ideal $\mathfrak{a}$. It is a theorem that ζ_k has an analytic continuation to $\mathbf{C} \smallsetminus 1$. The pole at $s = 1$, and we have the following analytic *class number formula.* Let r be the order of the pole of ζ_k at 1, and let r_1, r_2 be the number of real (resp. complex) places of k. Let h_k be the class number of k, d_k be the discriminant of k. Then

$$\lim_{s\to 1} \frac{\zeta_k(s)}{(s-1)^r} = \frac{2^{r_1}(2\pi)^{r_2}|d_k|^{-1/2} \operatorname{Reg}_k h_k}{\#\mu(k)}.$$

The Birch and Swinnerton-Dyer conjecture as well as the class number formula are both special cases of a very far-reaching generalization called the *Bloch-Kato conjecture.*

(add BSD for abelian varieties, brief statement of Bloch-Kato)

Follow [Lan91, III] for definition of regulator of abelian variety, general BSD.

6 Some theorems of Faltings

6.1 Background and Tate's conjecture

The goal of this section is to describe the relationships between a web of conjectures that Faltings proved in his groundbreaking paper [Fal86].

Let A be a d-dimensional abelian variety over a field k. As usual, we write $\bar{k}$ for the algebraic closure of k and $G_k = \mathrm{Gal}(\bar{k}/k)$ for the absolute Galois group of k. Fix a prime ℓ invertible in k. The groups $A[\ell^n] = \{x \in A(\bar{k}) : \ell^n x = 0\}$ are abstractly isomorphic to $(\mathbf{Z}/\ell^n)^{\oplus 2d}$, and carry a continuous action of G_k. They fit into an inverse system

$$A[\ell] \xleftarrow{\ell} A[\ell^2] \xleftarrow{\ell} A[\ell^3] \longleftarrow \cdots$$

Put

$$T_\ell A = \varprojlim A[\ell^n] = \left\{(x_n) \in \prod A[\ell^n] : \ell x_{n+1} = x_n\right\}.$$

This is the *ℓ-adic Tate module of A*. As a $\mathbf{Z}_\ell$-module, $T_\ell A \simeq \mathbf{Z}_\ell^{\oplus 2d}$. What makes $T_\ell A$ interesting is that it carries a continuous action of G_k, induced by the action of G_k on the $A[\ell^n]$. In other words, after choosing a basis of $T_\ell A$, we have a continuous representation

$$\rho_{A,\ell} : G_k \to \mathrm{GL}(2d, \mathbf{Z}_\ell).$$

The action of G_k on $T_\ell A$ factors through the smaller group $\mathrm{GSp}(2n, \mathbf{Z}_\ell)$ of symplectic simlitudes. One sees this via the *Weil pairing*. There is, for any n invertible in k, a natural perfect pairing $A[n] \times A^\vee[n] \to \mu_n$, defined at the level of schemes. For a prime ℓ invertible in k, these pairings patch together to give a perfect G_k-equivariant pairing $T_\ell A \times T_\ell A^\vee \to \mathbf{Z}_\ell(1)$. After a choice of polarization $\lambda : A \to A^\vee$, we get an (alternating) pairing $T_\ell A \times T_\ell A \to \mathbf{Z}_\ell(1)$. If ℓ is relatively prime to the degree of λ, then this pairing is perfect. In what follows, we will always assume this to be the case. For a proof of these facts in a pretty general setting, see [vdGM13, 11].

It is natural to ask how much $\rho_{A,\ell}$ "knows about" A, especially if k is a number field, or more generally, a finitely generated field.

Let X be a nice variety over a finitely generated field k. For each i, there is a canonical homomorphism

$$\mathrm{cl} : \mathrm{A}^i(X) \to \mathrm{H}^{2i}(X_{k^s}, \mathbf{Q}_\ell)(i),$$

defined in [Del77, VI 2.2.10]. One calls $\mathrm{cl}(Z)$ the cohomology class associated with a cycle Z.

Conjecture 6.1.1 (Tate)**.** *The cycle map induces an isomorphism* $\mathrm{A}^i(X) \otimes \mathbf{Z}_\ell \xrightarrow{\sim} \mathrm{H}^{2i}(X_{k^s}, \mathbf{Q}_\ell)(i)^{G_k}$.

This is essentially Conjecture 1 in [Tat65]. Often, "the Tate conjecture" means the following special case.

Conjecture 6.1.2 (Tate)**.** *Let* A, B *be abelian varieties over a finitely generated field* k*. For any prime* ℓ *invertible in* k*, the natural map*

$$\hom_k(A, B) \otimes \mathbf{Q}_\ell \to \hom_{G_k}(V_\ell A, V_\ell B)$$

is a bijection.

See the remarks after Conjecture 1 in Tate's paper, or [FWG+84, IV.1.4], for a proof that the second version of the conjecture follows from the first. Another way of stating the (second version of the) Tate conjecture is that for any finitely generated field k, the functor $V_\ell : \mathsf{AbVar}_k^{\mathrm{iso}} \to \mathsf{Rep}_{G_k}(\mathbf{Q}_\ell)$ is fully faithful.

Example 6.1.3. Let $k = \mathbf{F}_q$ be a finite field. Then G_k is naturally isomorphic to $\widehat{\mathbf{Z}}$, the profinite completion of $\mathbf{Z}$. Here $1 \in \widehat{\mathbf{Z}}$ corresponds to the *arithmetic Frobenius* $\mathrm{fr}_q \in G_{\mathbf{F}_q}$, given by $x \mapsto x^q$. Representations $\rho : G_{\mathbf{F}_q} \to \mathrm{GL}(n, \mathbf{Q}_\ell)$ are determined by $\rho(\mathrm{fr}_q)$. If such a representation is semisimple, the *Brauer-Nesbitt theorem* tells us that ρ is determined by the characteristic polynomial of $\rho(\mathrm{fr}_q)$. For an abelian variety A over $\mathbf{F}_q$, we know that the characteristic polynomial of $\rho_{A,\ell}(\mathrm{fr}_q)$ is $P_A(t) \in \mathbf{Z}[t]$, which determines A up to isogeny by Honda-Tate theory. ▷

Since we will be using characteristic polynomials quite a lot, let us state a suitably general version of the Brauer-Nesbitt theorem. Fix a field k, and for an arbitrary group G, let $K_0(G)$ denote the Grothendieck group of finite-dimensional k-representations of G. By the "characteristic polynomial" of a representation $\rho : G \to \mathrm{GL}_k(V)$, we mean the map $\chi_\rho : G \to \Lambda(k) = 1 + tk[\![t]\!]$ defined by

$$\chi_\rho(g) = \frac{1}{\det(1 - \rho(g) \cdot t, V)}.$$

Alternatively, $t\frac{d}{dt} \log \chi_\rho(g) = \sum \mathrm{tr}(\rho(g)^n)$.

Theorem 6.1.4 (Brauer-Nesbitt)**.** *If* S *spans* $k[G]$ *as a* k*-vector space, then the map* $\chi : K_0(G) \to \Lambda(k)^S$ *given by* $[\rho] \mapsto \chi_\rho$ *is an injection.*

Proof. This is Theorem 5.21 of [Egg11]. □

Corollary 6.1.5. *If* k *has characteristic zero and* $\rho_1, \rho_2 : G \to \mathrm{GL}_k(V)$ *are two semisimple representations with identical characters, then* $\rho_1 \simeq \rho_2$.

Theorem 6.1.6 (Faltings' isogeny theorem)**.** *Let A and B be abelian varieties over a number field k. For any prime ℓ, we have $\rho_{A,\ell} \simeq \rho_{B,\ell}$ as G_k-modules if and only if A and B are isogenous over k.*

From this, we see that we can fruitfully study A via $\rho_{A,\ell}$. For example, the rank of an abelian variety only depends on its isogeny class, so $\operatorname{rk} A$ only depends on $\rho_{A,\ell}$.

If k is either finite or a global field, the representation $\rho_{A,\ell}$ is semisimple, so $\rho_{A,\ell}$ is determined by the characteristic polynomial of $\rho_{A,\ell}(\mathrm{fr}_q)$. For this, one needs the *Čebotarev density theorem.*

6.2 Image of Frobenius for number fields

Fix a number field k, and a finite place v of k. Let $\mathfrak{p} \subset \mathfrak{o} = \mathfrak{o}_k$ be the corresponding maximal ideal. Let k_v be the completion of k at v. We choose $\bar{k} \subset \overline{k_v}$; this gives a map $G_{k_v} \to G_k$, defined by $\sigma \mapsto \sigma|_{\bar{k}}$. This map is only well-defined up to conjugation. By Krasner's lemma, the map is an injection. Reduction modulo $\mathfrak{p}$ gives a homomorphism $G_{k_v} \to G_{\kappa_v} = \widehat{\mathbf{Z}}$, where $\kappa_v = \mathfrak{o}_v/\mathfrak{p}$ is the residue field of $\mathfrak{p}$. This map is surjective, so we have an exact sequence (where we write D_v for the image of G_{k_v} in G_k):

$$1 \longrightarrow I_v \longrightarrow D_v \longrightarrow \widehat{\mathbf{Z}} \longrightarrow 1.$$

The group G_{κ_v} is procyclic, with generator fr_{Nv}, where as usual $Nv = \#\kappa_v$. Write fr_v for a lift of fr_{Nv} to D_v. The element $\mathrm{fr}_v \in G_k$ is only well-defined up to conjugacy and multiplication by I_v.

As before, let A be an abelian variety over k with good reduction at v. Then (by definition) there exists an abelian scheme $\mathcal{A}$ over $\mathfrak{o}_v$ whose generic fiber is A_{k_v}. The scheme $\mathcal{A}$ fits into a commutative diagram with cartesian squares:

$$\begin{array}{ccccc} A_v & \longrightarrow & \mathcal{A} & \longleftarrow & A_{k_v} \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec}(\kappa_v) & \longrightarrow & \operatorname{Spec}(\mathfrak{o}_v) & \longleftarrow & \operatorname{Spec}(k_v) \end{array}$$

We have define $A_v = \mathcal{A}_{\kappa_v}$. The property of being abelian is stable under base change, so A_v is an abelian variety over κ_v, and we have a reduction map

$$A(k_v) = \mathcal{A}(\mathfrak{o}_v) \to \mathcal{A}(\kappa_v) = A_v(\kappa_v).$$

Extending to algebraic closures, we get a map $A(\overline{k_v}) \to A_v(\overline{\kappa_v})$. This is a homomorphism with pro-p kernel. Let $\ell \nmid v$ (i.e. ℓ is relatively prime to the residue characteristic of v). At the level of torsion, we have isomorphisms

$$A(\overline{k_v})[\ell^n] \to A_v(\overline{\kappa_v})[\ell^n].$$

The map is injective because its kernel is pro-p, and it is surjective by cardinality considerations – both groups have cardinality $(\ell^n)^{2d}$). This gives us an isomorphism $A(\bar{k})[\ell^n] = A(\overline{k_v})[\ell^n] \xrightarrow{\sim} A_v(\kappa_v)[\ell^n]$. These groups have (compatible) actions of G_k, G_{k_v} and G_{κ_v}. In particular, the inertia group I_v acts trivially on $A(\bar{k})[\ell^n]$.

It follows that fr_v, *a priori* only well-defined up to conjugacy and multiplication by I_v, has a well-defined action on $A[\ell^n]$, and hence on $T_\ell A$. That is, we have the following theorem.

Theorem 6.2.1. *Let A be an abelian variety over k with good reduction at v. Then for $v \nmid \ell$, we have*

1. *$\rho_{A,\ell}$ is unramified at v (i.e. $\rho_{A,\ell}(I_v) = 1$)*
2. *$\rho_{A,\ell}(\mathrm{fr}_v)$ is well-defined up to conjugacy and has characteristic polynomial $P_{A_v}(t)$ with integer coefficients that do not depend on ℓ.*

Proof. See 4.5 for a definition of $P_{A_v}(t)$. This is Theorem 1, paired with the corollary to Theorem 3 in [ST68]. □

Recall the Čebotarev density theorem. Let k be a number field, K/k a finite Galois extension. For v unramified in K/k, there is a well-defined conjugacy class $\mathrm{fr}_v \in \mathrm{Gal}(K/k)^\natural$. Čebotarev's density theorem is essentially the Sato-Tate conjecture for the motive $h(\operatorname{Spec} K)$, i.e. it predicts equidistribution of Frobenii, in the appropriate sense.

Theorem 6.2.2 (Čebotarev)**.** *Let K/k be a finite Galois extension of number fields with Galois group G. Then $\{\mathrm{fr}_v\} \subset G^\natural$ is equidistributed with respect to the Haar measure on G.*

Proof. See [Ser68, 1.2.2] for a beautiful proof using the representation theory of compact groups. □

Recall that the statement "$\{\mathrm{fr}_v\} \subset G^\natural$ is equidistributed" means that for any conjugacy class $C \subset G$, we have

$$\lim_{x\to\infty} \frac{\{\#v : Nv \leqslant x \text{ and } \mathrm{fr}_v \in C\}}{\#\{v : Nv \leqslant x\}} = \frac{\#C}{\#G}$$

It follows that each conjugacy class in G is Frobenius for infinitely many primes.

For example, if $k = \mathbf{Q}$ and $K = \mathbf{Q}(\zeta_n)$, then $\mathrm{Gal}(K/\mathbf{Q})$ is naturally isomorphic to $(\mathbf{Z}/n)^\times$. For $p \nmid n$, the Frobenius fr_p corresponds to $p \in (\mathbf{Z}/n)^\times$. Dirichlet's theorem says that for $a \in (\mathbf{Z}/n)^\times$, there exist infinitely many p such that $p \equiv a \pmod{n}$, i.e. the Čebotarev density theorem holds for cyclotomic extensions.

Theorem 6.2.3 (Néron-Ogg-Shafarevich)**.** *Let A be an abelian variety over a number field k. Let v be a place of k, and let ℓ be a prime with $v \nmid \ell$. Then A has good reduction at v if and only if $\rho_{A,\ell}$ is unramified at v.*

Proof. This is the main theorem of [ST68]. □

6.3 L-function of an abelian variety

Let's define the L-function of an arbitrary abelian variety over a number field k. For a place v of k, choose a prime ℓ with $v \nmid \ell$. The action of fr_v on $T_\ell A$ is only well-defined up to the action of I_v, but $(T_\ell A)_{I_v} = T_\ell A/\{\sigma x - x : x \in I_v\}$ has a well-defined action of fr_v. Define

$$L_v(A,t) = \det\left(1 - \rho_{A,\ell}(\mathrm{fr}_v)\cdot t, (T_\ell A)_{I_v}\right)$$
$$L(A,s) = \prod_{v\nmid\infty} L_v\left(A, (Nv)^{-s}\right)^{-1}.$$

This is well-defined by the following theorem.

Theorem 6.3.1. *Let A be an abelian variety over a number field k. For any finite place v, the local factor $L_v(A,t)$ is an element of $\mathbf{Z}[t]$ that does not depend on ℓ.*

Proof. For v a place of good reduction, this is Theorem 6.2.1. The general case is a bit more subtle. First, note that

$$\det(1 - \rho_{A,\ell}(\mathrm{fr}_v)\cdot t, (T_\ell A)_{I_v}) = \det(1 - \rho_{A,\ell}(\mathrm{fr}_v^{-1}), ((T_\ell A)^\vee)^{I_v}).$$

The Weil pairing gives us an isomorphism $(T_\ell A)^\vee = T_\ell A(-1)$, and because the ℓ-adic cyclotomic character is unramified at $v \nmid \ell$, we get $((T_\ell A)^\vee)^{I_v} = (T_\ell A)^{I_v}(-1)$.

Let $\mathcal{A}$ be the Néron model for A over $\mathfrak{o}_v$, and let A_v be the connected component of the identity in $\mathcal{A}_{\kappa_v}$. By Lemma 2 of [ST68], there is a D_v-equivariant isomorphism $(T_\ell A)^{I_v} \to T_\ell A_v$.

Chevalley's theorem (see [Con02] for a modern proof) gives us a linear algebraic group $G \subset A_v$ such that $B = A_v/G$ is an abelian variety. In other words, we have a short exact sequence

$$1 \longrightarrow G \longrightarrow A_v \longrightarrow B \longrightarrow 0.$$

The group G splits into a product $G = T \times U$, where T is a (possibly non-split) torus and U is unipotent. The group U will be an iterated extension of copies of $\mathbf{G}_a$, so $T_\ell U = 0$.

Let $\widehat{T} = \hom_{\bar{k}}(T_{\bar{k}}, \mathbf{G}_{m,\bar{k}})$ be the group of characters of T. This has an obvious continuous G_k-action, and there is a G_k-equivariant pairing

$$T_\ell T \otimes \widehat{T} \to \mathbf{Z}_\ell(1),$$

given by $(x_n)_n \otimes \chi \mapsto (\chi(x_n))_n$. It is easy to see (by base-change to $\bar{k}$) that this pairing is nondegenerate, so we have a G_k-isomorphism $T_\ell T \simeq \widehat{T}^\vee \otimes \mathbf{Z}_\ell(1)$. We obtain

$$\det(1 - \rho_{A_v,\ell}(\mathrm{fr}_v) \cdot t) = \det(1 - \rho_{B,\ell}(\mathrm{fr}_v) \cdot t, T_\ell B) \cdot \det(1 - \mathrm{fr}_v^{-1} \cdot t, \widehat{T} \otimes \mathbf{Z}_\ell).$$

Since B does not depend on ℓ and G_k acts on $\widehat{T} \otimes \mathbf{Z}_\ell$ via its action on $\widehat{T}$, the characteristic polynomial of Frobenius is an element of $\mathbf{Z}[t]$ independent of ℓ. □

Let's check that our definition of $L(A, s)$ agrees with our previous definition in the case that $A = E$ is an elliptic curve over k. If E has good reduction at v, $(T_\ell E)_{I_v} = T_\ell E$ and there is nothing to prove. If E has bad reduction at v, then as before let E_v be the connected component of the special fiber of the Néron model at v. Recall that E has *multiplicative reduction* at v if E_v is a torus, and *additive reduction* if E_v is unipotent. Clearly

$$\mathrm{rk}_{\mathbf{Z}_\ell}(T_\ell E)^{I_p} = \begin{cases} 2 & \text{good reduction} \\ 1 & \text{mult. reduction} \\ 0 & \text{add. reduction} \end{cases}$$

If E has split multiplicative reduction at v, then the local factor $L_v(E, t)$ is the (reverse of) the characteristic polynomial of Frobenius acting on $T_\ell \mathbf{G}_m(-1) = \mathbf{Z}_\ell$. On the other hand, if E has nonsplit multiplicative reduction at v, then by [Sil09, III,2.5], E_v splits after a quadratic base-change, from which we see that fr_v acts on $\widehat{E}_v$ as -1, whence the following:

$$L_v(E, t) = \begin{cases} 1 & \text{additive reduction} \\ 1 - t & \text{split multiplicative reduction} \\ 1 + t & \text{nonsplit multiplicative reduction} \\ 1 - a_p t + p t^2 & \text{good reduction} \end{cases}$$

The function $L(A, s)$ should have an analytic continuation, functional equation, it should satisfy BSD ($\mathrm{ord}_{s=1} L(A, s) = \mathrm{rk}_{\mathbf{Z}} A(\mathbf{Q})$), and a "fancy BSD" with a precise prediction of the coefficient in Taylor series. By the Weil conjectures, the function $L(A, s)$ converges on some region $\{\Re s > c\}$.

6.4 Tate conjectures and isogenies

Much of the rest of this section follows Lang's excellent survey [Lan91] and the more technical [FWG+84]. We begin with a useful fact.

Theorem 6.4.1. *Let k be a number field and $\rho_1, \rho_2 : G_k \to \mathrm{GL}(n, \mathbf{Z}_\ell)$ continuous semisimple representations. If $\operatorname{tr}\rho_1(\mathrm{fr}_v) = \operatorname{tr}\rho_2(\mathrm{fr}_v)$ for all v in a density-one set of places, then $\rho_1 \simeq \rho_2$.*

Proof. By the Čebotarev density theorem, the set $\{\mathrm{fr}_v\} \subset G_k^\natural$ is dense. It follows that $\operatorname{tr}\rho_1 = \operatorname{tr}\rho_2$, so the conclusion follows from the Brauer-Nesbitt theorem. □

We are mainly interested in the case when $\rho_1 = \rho_{A,\ell}$ and $\rho_2 = \rho_{B,\ell}$ for A, B abelian varieties over k. The theorem tells us that if $P_{A_v} = P_{B_v}$ for almost all primes, then $\rho_{A,\ell} \simeq \rho_{B,\ell}$. A morphism $f : A \to B$ of abelian varieties induces a G_k-equivariant morphism $f_* : T_\ell A \to T_\ell B$. If f is an isogeny, then f_* is an isomorphism after tensoring with $\mathbf{Q}$. In particular, if we think of $\rho_{A,\ell}$ as a $\mathbf{Q}_\ell$-representation, then $\rho_{A,\ell} \simeq \rho_{B,\ell}$. It follows that A and B have the same bad primes.

The following theorem was conjectured by Tate, and proved when k is a finite field.

Theorem 6.4.2 (Faltings)**.** *Let k be a finitely generated field and A, B abelian varieties over k. Then*

1. *(Semisimplicity) $V_\ell A$ is a semisimple G_k-module.*
2. *(Tate conjecture) The natural map*

$$\hom(A, B) \otimes \mathbf{Z}_\ell \to \hom_{G_k}(T_\ell A, T_\ell B)$$

is an isomorphism.

Proof. See [FWG+84] for a proof when k has characteristic zero. Alternatively, see [Mila, IV.2.5] for a proof that semisimplicity and the Tate conjecture follow from Theorem 6.5.4. □

Corollary 6.4.3 (Isogeny theorem)**.** *Abelian varieties A and B over a number field k are isogenous if and only if $\rho_{A,\ell}$ and $\rho_{B,\ell}$ are isomorphic.*

Proof. We've already seen that if A and B are isogenous, then $\rho_{A,\ell} \simeq \rho_{B,\ell}$. The Tate conjecture gives us an isomorphism

$$\hom(A, B) \otimes \mathbf{Z}_\ell \xrightarrow{\sim} \hom_{G_k}(T_\ell A, T_\ell B).$$

Assuming $\rho_{A,\ell}$ and $\rho_{B,\ell}$ are isomorphic, we can choose a specific isomorphism $f : \rho_{A,\ell} \to \rho_{B,\ell}$. Since $\hom_{G_k}(T_\ell A, T_\ell B)$ is a finite rank $\mathbf{Z}_\ell$-module isomorphic to $\hom(A,B) \otimes \mathbf{Z}_\ell$, the space $\hom(A,B)$ is dense in $\hom_{G_k}(T_\ell A, T_\ell B)$. The property "$f : T_\ell A \to T_\ell B$ is an isomorphism" is open, so there exists $\varphi : A \to B$ such that φ_* is an isomorphism. We claim that φ is an isogeny. Indeed, let $C = (\ker \varphi)^\circ \subset A$. If $C \neq 0$, then $\operatorname{rk} T_\ell C > 0$. This cannot be, because $\varphi_*(T_\ell C) = 0$ and φ_* is an isomorphism. Thus $C = 0$, so $\ker \varphi$ is finite. By dimension considerations, φ is an isogeny. □

By [FWG+84, V.3.2], if $\rho_{A,\ell} \simeq \rho_{B,\ell}$, there actually exists an isogeny $f : A \to B$ with $\ell \nmid \deg f$.

Choose a finite place v of k at which A has good reduction. The polynomial $P_{A_v}(t)$ is integral, monic, and has degree $2d$. So we can write

$$P_{A_v}(t) = t^{2d} - a_v(A)t^{2d-1} + \cdots$$

where $a_v(A) = \operatorname{tr} \rho_{A,\ell}(\mathrm{fr}_v) \in \mathbf{Z}$. We have $|a_v(A)| \leqslant 2g\sqrt{Nv}$, since the roots of P_{A_v} have absolute value $\sqrt{Nv}$.

If $A = E$ is an elliptic curve over $\mathbf{Q}$, then this definition of $a_v(E)$ agrees with the the standard definition $a_p(E) = p + 1 - \#E(\mathbf{F}_p)$. If C is a nice curve over $\mathbf{Q}$ of genus g, then for $J = \operatorname{Jac} C$, we have $\#C(\mathbf{F}_p) = p + 1 - a_p(J)$.

Theorem 6.4.4. *Let A and B be abelian varieties over a number field k. Let S be a density-zero set of places of k, containing the infinite places, as well as the bad places for A and B. Then A is isogenous to B if and only if $a_v(A) = a_v(B)$ for all $v \notin S$.*

Proof. Fix a prime ℓ. If A and B are isogenous, then $\rho_{A,\ell} \simeq \rho_{B,\ell}$, so $a_v(A) = \operatorname{tr}(\rho_{A,\ell}(\mathrm{fr}_v)) = \operatorname{tr}(\rho_{B,\ell}(\mathrm{fr}_v)) = a_v(B)$ for all places $v \notin S \cup \{\ell\}$. The converse is an immediate corollary of Theorem 6.4.1. and the isogeny theorem (Corollary 6.4.3). □

This theorem is not especially useful, because it requires checking $a_v(A) = a_v(B)$ at an infinite set of places. The following lemma and its corollary give us a way of capturing the isogeny class of an abelian variety using a finite amount of data.

6.5 Finiteness theorems

Lemma 6.5.1 (Faltings)**.** *Let k be a number field, S a finite set of places, and $n \geqslant 1$ an integer. Then there is a finite set T of places, disjoint from S and depending only on (k, S, n), such that if $\rho_1, \rho_2 : G_{k,S} \to \mathrm{GL}(n, \mathbf{Z}_\ell)$ are continuous representations with $\operatorname{tr} \rho_1(\mathrm{fr}_v) = \operatorname{tr} \rho_2(\mathrm{fr}_v)$ for all $v \in T$, then $\rho_1 \simeq \rho_2$.*

Proof. Without loss of generality, we can assume S contains all places dividing ℓ. Let $d = \ell^{2n^2} = \#M_n(\mathbf{F}_\ell) \times M_n(\mathbf{F}_\ell)$. By Hermite's theorem, there are only finitely many extensions of k unramified outside S with degree $\leqslant d$. Let K/k be a Galois extension containing all these and let $G = \mathrm{Gal}(K/k)$. The Čebotarev density theorem tells us that there is a finite set T (disjoint from S) of places of k such that $G^\natural = \{\mathrm{fr}_v : v \in T\}$.

Now let ρ_1, ρ_2 be as in the statement of the lemma. Set $\rho = \rho_1 \times \rho_2 : G_{k,S} \to \mathrm{GL}(n, \mathbf{Z}_\ell) \times \mathrm{GL}(n, \mathbf{Z}_\ell)$. Let R be the $\mathbf{Z}_\ell$-subalgebra of $M_n(\mathbf{Z}_\ell) \times M_n(\mathbf{Z}_\ell)$ generated by the image of ρ. Note that R is a free $\mathbf{Z}_\ell$-module of rank at most $2n^2$. We can consider the reduction of ρ modulo ℓ, i.e. $\bar\rho : G_k \to (R/\ell)^\times$. We know that $\#(R/\ell)^\times \leqslant d$, so $\bar\rho$ factors through G as in the commutative diagram:

$$\begin{array}{ccc} G_k & \xrightarrow{\bar\rho} & (R/\ell)^\times \\ \downarrow & \nearrow & \\ G & & \end{array}$$

It follows that R/ℓ is generated (as a group) by the images of $\{\rho([\mathrm{fr}_v]) :\in T\}$. By Nakayama's lemma, R is generated as a $\mathbf{Z}_\ell$-module by $\{\rho([\mathrm{fr}_v]) : v \in T\}$.

Let $\varphi : R \to \mathbf{Z}/\ell$ be the map $(g, h) \mapsto \mathrm{tr}\, g - \mathrm{tr}\, h$. This is a homomorphism of $\mathbf{Z}_\ell$-modules. Assume $a_v(A) = a_v(B)$ for all $v \in T$. Then for $v \in T$, we have

$$\varphi(\rho(\mathrm{fr}_v)) = \mathrm{tr}\, \rho_{A,\ell}(\mathrm{fr}_v) - \mathrm{tr}\, \rho_{B,\ell}(\mathrm{fr}_v) = a_v(A) - a_v(B) = 0$$

This implies $\varphi = 0$ since φ vanishes on a set of generators of R. It follows that $\mathrm{tr}\, \rho_{A,\ell} = \mathrm{tr}\, \rho_{B,\ell}$. Since $\rho_{A,\ell}$ and $\rho_{B,\ell}$ are semisimple, this implies $\rho_{A,\ell} \simeq \rho_{B,\ell}$, and the isogeny theorem tells us that A and B are isogenous. □

Corollary 6.5.2. *Let k be a number field, S a finite set of places of k and $d \geqslant 1$ an integer. Then there is a finite set T of places of k, disjoint from S and depending only on (k, S, d), such that if A and B are d-dimensional abelian varieties with good reduction outside S, then A and B are isogenous if and only if $a_v(A) = a_v(B)$ for all $v \in T$.*

In the next section, we will prove the Mordell conjecture for number fields using Faltings proof of a finiteness result for abelian varieties.

Conjecture 6.5.3 (Shafarevich, for abelian varieties)**.** *Fix a number field k and a finite set S of places, and an integer $d \geqslant 1$. Then there are only finitely many isomorphism classes of d-dimensional abelian varieties over k with good reduction outside S.*

Since isogenous abelian varieties have the same dimension and bad primes, the conjecture breaks up into two pieces.

Theorem 6.5.4 (Finiteness I)**.** *Let A be an abelian variety over a number field k. Then there are only finitely many isomorphism classes of abelian varieties over k which are isogenous to A.*

Proof. This is a *very* brief sketch of the proof in [FWG+84, V.3], which has several parts. First, one reduces to the case of principally polarized abelian varieties with semistable reduction everywhere.

Next, one constructs the *Faltings height* $h(A)$ of an arbitrary d-dimensional abelian variety A over k as follows. Let $\mathcal{A}$ be the Néron model $\mathcal{A}$ of A over $\mathfrak{o} = \mathfrak{o}_k$, let $s : \operatorname{Spec}(\mathfrak{o}) \to \mathcal{A}$ be the identity section, and define

$$\omega_{\mathcal{A}/\mathfrak{o}} = \left(s^* \Omega^d_{\mathcal{A}/\mathfrak{o}}\right)^\vee.$$

This is a projective $\mathfrak{o}$-module of rank one. If v is an infinite place of k corresponding to $\sigma : k \hookrightarrow \mathbf{C}$, the vector space $\omega_{\mathcal{A}/\mathfrak{o}} \otimes_{\mathfrak{o},\sigma} \mathbf{C}$ has an inner product defined by

$$\langle \eta, \xi \rangle_v = \left(\frac{i}{2}\right)^d \int_{A(\mathbf{C})} \eta \wedge \bar{\xi}.$$

This inner product induces a natural norm. For any place v, put $\varepsilon_v = 1$ if v is real, and $\varepsilon_v = 2$ if v is complex. We define the Faltings height of A as $h(A) = [k : \mathbf{Q}]^{-1} \deg(\omega_{\mathcal{A}/\mathfrak{o}})$, where

$$\deg\left(\omega_{\mathcal{A}/\mathfrak{o}}\right) = \log \#(\omega_{\mathcal{A}/\mathfrak{o}}/x) - \sum_{v|\infty} \varepsilon_v \log \|x\|_v.$$

for any nonzero $x \in \omega_{\mathcal{A}/\mathfrak{o}}$. See [Mila, VI.6] for a proof that this is independent of x, and a more detailed construction of $h(A)$.

By relating the Faltings height to a natural Arakelov height on the moduli space of principally polarized abelian varieties, Faltings proved that the set

$$\{\text{semistable principally polarized } A/k \text{ with } \dim A = d \text{ and } h(A) \leqslant c\}$$

is finite for any c [FWG+84, II.4.3]. Moreover, for any A/k principally polarized with semistable reduction, there exists an integer $N \geqslant 1$ such that if $f : B \to A$ is an isogeny with $(\deg f, N) = 1$, then $h(B) = h(A)$ [FWG+84, V.3.5]. Finally, there exists a finite set $A_1, \ldots, A_n$ of abelian varieties isogenous to A such that if B is any abelian variety isogenous to A, then there is an isogeny $f : B \to A_i$ with $(N, \deg f) = 1$ [FWG+84, V.3.4]. □

There is an alternative approach to Theorem 6.5.4 due to Masser and Wüsthoz [MW93].

Theorem 6.5.5 (Finiteness II)**.** *Let $d \geqslant 1$ be an integer, k a number field and S a finite set of places of S. Then there are only finitely many isogeny classes of d-dimensional abelian varieties over k with good reduction outside S.*

Proof. Take A over k of dimension $d \geqslant 1$, with good reduction outside S. Corollary 6.5.2 gives us a finite set T of places for which the isogeny class of A is determined by $\{a_v(A) : v \in T\}$. Recall that the $a_v(A)$ are integers with absolute value $\leqslant 2g\sqrt{Nv}$. It follows that there are only finitely many possibilities for the a_v, and hence only finitely many isogeny classes of d-dimensional abelian varieties over k with good reduction outside S. □

Conjecture 6.5.6 (Shafarevich, for curves)**.** *Fix a number field k, an integer $g \geqslant 1$, and a finite set S of places of k. Then there are only finitely many nice curves over k of genus g with good reduction outside S.*

Proof. Let J be the jacobian of C. Then J is an abelian variety over k of dimension g, with good reduction outside S. There are only finitely many possibilities for J (up to isomorphism). Recall that C is determined by (J, θ). By [NN81], abelian varieties over algebraically closed fields have only finitely many isomorphism classes of principal polarizations. Thus there can be only finitely many C corresponding to J. □

6.6 Proof of the Mordell conjecture

Following Parshin [Par68], and the more expository accounts in [Lan91, IV.2] and [FWG+84, V.4], we show that the Shafarevich conjecture implies the Mordell conjecture.

Conjecture 6.6.1 (Mordell)**.** *Let C be a nice curve of genus $g \geqslant 2$ over a number field k. Then $C(k)$ is finite.*

A key ingredient is the following technical lemma.

Lemma 6.6.2. *Let C be a nice curve of genus $g \geqslant 2$ over a number field k. Then there is a finite extension k'/k and a finite set S' of places of k' satisfying the following. For every $x \in C(k)$ there is a nice curve W_k over k' with good reduction outside S', and a morphism $\varpi_x : W_x \to C_{k'}$ ramified exactly at x (with ramification index $\leqslant 2$) such that $\deg \varphi_x \leqslant 2 \cdot 4^g$.*

Proof. Assume $C(k) \neq \varnothing$, and let $j : C \hookrightarrow J = \operatorname{Jac} C$ be the embedding induced by some fixed $x \in C(k)$. The map "multiplication by two" is an étale self-covering of J; we let $\widetilde{C}$ be its pullback:

$$\begin{array}{ccc} \widetilde{C} & \longrightarrow & J \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 2} \\ C & \xrightarrow{\ j\ } & J \end{array}$$

From the Chevalley-Weil theorem [BG06, 10.3.11], we obtain a finite extension L/k such that $\varphi^{-1}(x) \subset \widetilde{C}(L)$ for all $x \in C(k)$. For any $x \in C(k)$, choose distinct $x_1, x_2 \in \widetilde{C}(L)$ such that $\varphi(x_i) = x$. There exists a divisor $D \in \operatorname{Div}(\widetilde{C})$ defined over some finite extension k'/k (which does not depend on x) such that $x_1 - x_2 + 2D = (f)$ in $\operatorname{Jac}\widetilde{C}$ for some rational function f. Let $\varphi_x : W_x \to \widetilde{C}_{k'}$ correspond to the inclusion $k'(\widetilde{C}) \hookrightarrow k'(\widetilde{C})[\sqrt{f}]$ of function fields. It's not to hard to show that W_x has the desired properties. See [Lan91, IV.2.1] for details. □

Theorem 6.6.3. *The Mordell conjecture is true.*

Proof. Let C be a nice curve of genus $g \geqslant 2$ over a number field k. Suppose that $C(k)$ is infinite. By Lemma 6.6.2, there is a finite extension k'/k and morphisms $\varphi_x : W_x \to C_{k'}$ for each $x \in C(k)$.

The genus of W_x is bounded (using Riemann-Hurwitz) since the $\deg \varphi_x$ is bounded and φ_x is only ramified only at x. The Shafarevich conjecture tells us there are only finitely many possibilities for the W_x. In particular, there exists W/k' that is isomorphic to infinitely many W_x. We have maps $W \xrightarrow{\sim} W_x \xrightarrow{\varphi_x} C_k$, unramified only at x. Choose $k' \hookrightarrow \mathbf{C}$; this gives a morphism $\varphi_x : W(\mathbf{C}) \to C(\mathbf{C})$ of compact Riemann surfaces, ramified only at x. This contradicts Theorem 6.6.4. □

Theorem 6.6.4 (de Franchis)**.** *Let X and Y be nice curves of genus $\geqslant 2$ over a field of characteristic zero. Then there are only finitely many non-constant morphisms $X \to Y$.*

Proof. The theorem was originally proved by de Franchis for Riemann surfaces. See [Lan60, p.29] for a general proof. □

References

[And04] Yves André. *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, volume 17 of *Panoramas et Synthéses*. Société Mathématique de France, Paris, 2004.

[AW45] Emil Artin and George Whaples. Axiomatic characterization of fields by the product formula for valuations. *Bull. Amer. Math. Soc.*, 51:469–492, 1945.

[BC84] A. Bremner and J. Cassels. On the equation $Y^2 = X(X^2 + p)$. *Math. Comp.*, 42(165):257–264, 1984.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[Bit04] Franziska Bittner. The universal Euler characteristic for varieties of characteristic zero. *Compos. Math.*, 140(4):1011–1032, 2004.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1990.

[Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translation from the French by P. M. Cohn and J. Howie.

[BS10a] Manjul Barghava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, 2010. `arXiv:1007.0052`.

[BS10b] Manjul Bhargava and Arul Shankar. Binary quadratic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, 2010. `arXiv:1006.1002`.

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

[Cas67] J. W. S. Cassels. Survey article—Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 42, 1967.

[Con02] Brian Conrad. A modern proof of Chevalley's theorem on algebraic groups. *J. Ramanujan Math. Soc.*, 17(1):1–18, 2002.

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

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.

[Del77] Pierre Deligne. *Cohomologie etale (SGA $4\frac{1}{2}$)*, volume 569 of *Lectures notes in mathematics*. Springer, 1977.

[DFK94] Mumford D., J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2)*. Springer-Verlag, Berlin, third edition, 1994.

[dJ] Johan de Jong. Weil cohomology theories. available at http://math.columbia.edu/~dejong/seminar/note_on_weil_cohomology.pdf.

[Dok10] Tim Dokchitser. Notes on the parity conjecture. *preprint*, 2010. arXiv:1009.5389.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Duj] A. Dujella. History of elliptic curves rank records. http://web.math.pmf.unizg.hr/~duje/tors/rankhist.html.

[Egg11] R. H. Eggermont. Generalizations of a theorem by Brauer and Nesbitt. Master's thesis, Mathematisch Instituut, Leiden, 2011.

[Fal86] Gerd Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original.

[Ful98] William Fulton. *Intersection Theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Genzgebiete. 3. Folge.* Springer-Verlag, Berlin, second edition, 1998.

[FWG+84] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Scappacher, and Ulrich Stuhler. *Rational points*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[Gro61] Alexandre Grothendieck. Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I. *Inst. Hautes Études Sci. Publ. Math.*, 11, 1961.

[Gro66] Alexandre Grothendieck. On the de Rham cohomology of algebraic varieties. *Inst. Hautes Études Sci. Publ. Math.*, 29:95–103, 1966.

[GZ86] Benedict H. Gross and Don S. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[HH09] Shinya Harada and Toshiro Hiranouchi. Smallness of fundamental groups for arithmetic schemes. *J. Number Theory*, 129(11):2707–2712, 2009.

[Ill94] Luc Illusie. Crystalline cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 43–70. Amer. Math. Soc., Providence, RI, 1994.

[Jan92] Uwe Jannsen. Motives, numerical equivalence, and semi-simplicity. *Invent. Math.*, 107(3):447–452, 1992.

[Jos06] Jürgen Jost. *Compact Riemann surfaces*. Universitext. Springer-Verlag, Berlin, third edition, 2006.

[Kat88] Nicholas Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[Kle05] Steven Kleiman. The Picard scheme. In *Fundamental algebraic geometry: Grothendieck's FGA explained*, volume 123 of *Math. Surveys Monogr.*, pages 235–321. Amer. Math. Soc., 2005.

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical notes*. Princeton University Press, Princeton, NJ, 1992.

[Kol88] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akai. Nauk SSSR Ser. math.*, 52(3):522–540, 670–671, 1988.

[Lan60] Serge Lang. Integral points on curves. *Inst. Hautes Études Sci. Publ. Math.*, 6:27–43, 1960.

[Lan91] Serge Lang. *Number Theory, III*, volume 60 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991. Diophantine geometry.

[LS07] Bernard Le Stum. *Rigid cohomology*, volume 172 of *Cambridge Tracts in Mathematics*. Cambridge Univ. Press, Cambridge, 2007.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*, volume 504 of *Lecture Notes in Mathematics,*. Springer-Verlag, Berlin, 1976.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186, 1977.

[McQ95] Michael McQuillan. Division points on semi-abelian varieties. *Invent. Math.*, 120(1):143–159, 1995.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1–3):437–449, 1996.

[Mila] J. S. Milne. Abelian varieties. available at http://www.jmilne.org/math/CourseNotes/AV.pdf.

[Milb] J. S. Milne. Lectures on étale cohomology. available at http://www.jmilne.org/math/CourseNotes/LEC.pdf.

[Mil06] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LCC, Charleston, CS, second edition, 2006.

[Moc12] Shinichi Mochizuki. Topics in absolute anabelian geometry I: generalities. *J. Math. Sci. Univ. Tokyo*, 19(2):139–242, 2012.

[Mum08] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, Bombay, 2008.

[MW93] David Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[NN81] M. S. Narasimhan and M. V. Nori. Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.*, 90(2):125–128, 1981.

[Par68] A. N. Parshin. Algebraic curves over function fields. I. *Izv. Akad. Nauk SSSR Ser. Math.*, 32:1191–1219, 1968.

[RS11] Ken Ribet and William Stein. *Lectures on modular forms and Hecke operators*. In preparation, 2011. available at http://wstein.org/books/ribet-stein/main.pdf.

[Rud87] Walter Rudin. *Real and complex analysis*. McGraw-Hill, New York, third edition, 1987.

[Ser68] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. McGill University lecture notes. W. A. Benjamin, New York, 1968.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser94] Jean-Pierre Serre. Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 377–400. Amer. Math. Soc., Providence, RI, 1994.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[Sha92] I. R. Shafarevich, editor. *Number theory. II*, volume 62 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1992. Algebraic number theory, A translation of *Number theory, 2. (Russian)*.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sko01] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[ST68] Jean-pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Sto09] M. Stoll. On the average number of rational points on curves of genus 2, 2009. `arXiv:0902.4165`.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

[Tat65] John Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, New York, 1965.

[Tay08] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. II. *Publ. Math. Inst. Hautes Études Sci.*, (108):183–239, 2008.

[Tsi12] Jacob Tsimerman. The existence of an abelian variety over $\overline{\mathbb{Q}}$ isogenous to no Jacobian. *Ann. of Math. (2)*, 176(1):637–650, 2012.

[Tun83] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

[vdGM13] Gerard van der Geer and Ben Moonen. *Abelian varieties*. In preparation, accessed in 2013. available at http://staff.science.uva.nl/~bmoonen/boek/BookAV.html.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[Wei95] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3), 1995.