Elliptic Curves

Lectures by David Holmes
Typeset by Steve Alberts
First revision by David Holmes

September 2, 2015

Abstract

These are notes from a first course on elliptic curves at Leiden university in spring 2015. They are aimed at advanced batchelor/beginning master students. We do not assume any backgound in algebraic geometry. We define varieties via functors points, but only on the category of fields. This makes several things simpler, but is not ideal in all respects - for example, defining morphisms of varieties as functors doesn't give what one wants.

The main result of the course is a proof of the Mordell-Weil theorem for elliptic curves over $\mathbb{Q}$ with rational 2-torsion, via Selmer groups. Our proof of this is fairly complete, except that at one point we have to assume more algebraic geometry to show that non-constant maps of curves are surjective (but this can just be taken as a black box).

Not everything from the lectures has been typeset, in particular some examples and basic definitions are omitted. The handwritten notes on the course website are complete, but then you have to read my handwriting!

Comments and corrections are very welcome, please email them to David.

Contents

1 Motivation and introduction

[not typed yet]

2 Basic Definitions

Definition 2.1 (Affine & Projective Space)**.** Let k be a field and $n \geq 0$ an integer. The affine n-space $\mathbb{A}_k^n$ is the functor

$$\mathbf{Fld}_k \to \mathbf{Set}$$

$$K \mapsto K^n$$

A morphism of field extension $K/k \to L/k$ naturally gives rise to a map of sets $K^n \to L^n$. The projective space $\mathbb{P}_k^n$ is the functor

$$\mathbf{Fld}_k \to \mathbf{Set}$$

$$K \mapsto \mathbb{P}^n(K)$$

where

$$\mathbb{P}^n(K) := (K^{n+1} \backslash \{0\}) / \sim$$

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow \exists \lambda \in K^* : (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$$

The morphisms are again sent to the obvious maps of sets, though here one has to verify that these maps are well-defined.

Definition 2.2 (Affine patches)**.** For every $0 \leq i \leq n$ there exists a natural transformation

$$\varphi_i : \mathbb{A}_k^n \to \mathbb{P}_k^n$$

defined by

$$\varphi_i(K) : \mathbb{A}_k^n(K) \to \mathbb{P}_k^n(K), (x_1, \ldots, x_n) \mapsto (x_1 : \ldots : x_{i-1} : 0 : x_i : \ldots : x_n)$$

Definition 2.3 (Affine Varieties)**.** Let k be a field, $n \geq 0$ an integer and $I \triangleleft k[X_1, \ldots, X_n]$ an ideal. An affine variety is a subfunctor of the form

$$V_I^A : \mathbf{Fld}_k \to \mathbf{Set}, K \mapsto \{(x_1, \ldots, x_n) \in K^n | \forall f \in I : f(x_1, \ldots, x_n) = 0\}$$

of $\mathbb{A}_k^n$.

It is important to remember that this functor is a subfunctor of affine space, *not* just an abstract functor.

Definition 2.4 (Homogenous ideal)**.** A homogeneous ideal is an ideal $I \triangleleft k[X_0, \ldots, X_n]$ which can be generated by homogeneous polynomials $f_1, \ldots, f_r$, i.e. polynomials such that every monomial has the same degree.

Note that if f is homogeneous of degree $\deg(f_i)$ then

$$f_i(\lambda(x_0, \ldots, x_n)) = \lambda^{\deg(f_i)} f_i(x_0, \ldots, x_n)$$

for all $(x_0, \ldots, x_n) \in k^{n+1}$ and $\lambda \in k$, and moreover if k is infinite then this condition is actually equivalent to being homogeneous.

Definition 2.5 (Projective varieties)**.** A projective variety is a subfunctor of $\mathbb{P}^n_k$ of the form

$$V_I^P : \mathbf{Fld}_k \to \mathbf{Set}$$

$$K \mapsto \{(x_0 : \ldots : x_n) \in \mathbb{P}^n_k(K) | \forall f \in I \text{ homogeneous} : f(x_0, \ldots, x_n) = 0\}$$

Here I is a homogeneous ideal of $k[X_0, \ldots, X_n]$.

It is important to remember that this functor is a subfunctor of projective space, *not* just an abstract functor.

A projective variety gives us affine varieties by composition with the affine patches φ_i. This we call the *affine restrictions* of the projective variety.

Definition 2.6 (Hypersurface)**.** An affine (projective) variety is an affine (projective) hypersurface if it can be written as $V^A_{(f)}$ ($V^P_{(f)}$) for some (homogeneous) $f \neq 0$.

Instead of $V^A_{(f)}$ we just write V^A_f, and similarly for projective.

Definition 2.7 (Empty variety)**.** ...

Definition 2.8 (Smooth)**.** An affine hypersurface $V^A_I \subset \mathbb{A}^n_k$ is called smooth if there exists a polynomial f such that $V^A_f = V^A_I$ and such that, writing

$$J = \left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \right),$$

we have $V^A_J = \varnothing$.

A projective variety is called smooth if each of its affine restrictions is smooth.

Theorem 2.9 (Hilbert's Nullstellensatz)**.** Let k be a field, $n \geq 0$ and K an algebraically closed field containing k. Let $I, J \triangleleft k[X_1, \ldots, X_n]$, then we have

$$V^A_I(K) = V^A_J(K) \Leftrightarrow \sqrt{I} = \sqrt{J}$$

[insert definition of radical]

Proof. Omitted.

□

Corollary 2.10. Let k, n, K, I, J as in theorem 2.9. Then the following are equivalent.

1. $V^A_I = \varnothing$
2. $I = (1)$
3. $V^A_I(K) = \varnothing$

Proof. The implications $2 \Rightarrow 1 \Rightarrow 3$ are easy. The implication $3 \Rightarrow 2$ follows from Hilbert's Nullstellensatz, since $\sqrt{I} = (1) \implies I = (1)$.

□

Corollary 2.11 (Criterium for smoothness)**.** If $f \in k[X_1, \ldots, X_n]$ is irreducible, then V_f^A is smooth if and only if

$$\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) = (1)$$

Proof. When

$$J := \left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) = (1)$$

then from the previous definition we find that $V_J^A = \varnothing$, so we find that V_f^A is smooth.
Now we assume that V_f^A is smooth, then there exists some $g \in k[X_1, ..., X_n]$ such that $V_f^A = V_g^A$ and

$$J = \left(g, \frac{\partial g}{\partial X_1}, \ldots, \frac{\partial g}{\partial X_n}\right) = (1)$$

From 2.9 we obtain that $\sqrt{(f)} = \sqrt{(g)}$, so $g = uf^m$ for some $m \geq 1$ and $u \in k^*$. We get

$$(1) = \left(g, \frac{\partial g}{\partial X_1}, \ldots, \frac{\partial g}{\partial X_n}\right) = \left(f^m, \frac{\partial f^m}{\partial X_1}, \ldots, \frac{\partial f^m}{\partial X_n}\right) = f^{m-1}\left(f, m\frac{\partial f}{\partial X_1}, \ldots, m\frac{\partial f}{\partial X_n}\right)$$

If $m = 1$, then we are done. On the other hand, if $m > 1$ then $f \in k^*$, and we are also done. □

Definition 2.12 (Plane curve)**.** A plane curve C is a hypersurface in $\mathbb{P}^2$. An equation for C is a polynomial f satisfying $C = V_f^P$ and $(f) = \sqrt{(f)}$.

Definition 2.13 (Elliptic Curve)**.** An elliptic curve over k is a pair of a smooth plane curve E and the point $O := (0 : 1 : 0) \in E(k)$, such that E can be written as V_f^P for

$$f = Y^2Z - (X^3 + aX^2Z + bXZ^2 + cZ^3)$$

with $a, b, c \in k$.

Of course, including the point $(0 : 1 : 0)$ is redundant, but this makes things more consistent with the literature.

Lemma 2.14. The curve V_f^P given by

$$f = Y^2 - X^3 - aX^2 - bX + c$$

is smooth (i.e. V_f^P is an elliptic curve) if and only if

$$\Delta(f) = 16(-4a^3c + a^2b + 18abc - 4b^3 - 27c^2) \neq 0$$

Proof. Homework exercise.

□

3 Intersections of plane curves

Definition 3.1 (Naive intersection)**.** Let $V, W \subset \mathbb{P}^n_k$ be subfunctors, then the naive intersection is the functor

$$V \cap W : \mathbf{Fld}_k \to \mathbf{Set}, K \mapsto V(K) \cap W(K)$$

Definition 3.2 (Meeting properly)**.** Let C, D be plane curves. We say C and D meet properly if $(C \cap D)(K)$ is finite for every field K containing k.

[pictures, examples]

For the composition law $*$ on $E(K)$ which we will define, we will need for lines to intersect with an elliptic curve exactly 3 times, which is why we are looking for another definition of intersection.

Definition 3.3 (Local ring)**.** Let k be a field, K an extension of k and $p = (x_p, y_p) \in \mathbb{A}^2_k(K)$. The local ring $\mathcal{O}_p$ is the localisation of $R := k[X, Y]$ at the maximal ideal $I = (X - x_p, Y - y_p)$:

$$\mathcal{O}_p = k[X, Y]_{(X-x_p, Y-y_p)} = \{(f, g) \in R \times (R \backslash I)\} / \sim$$

Here $(f_1, g_1) \sim (f_2, g_2)$ if and only if there exists an $s \in R \backslash I$ such that

$$s(f_1 g_2 - f_2 g_1) = 0$$

[motivation: think about fractions]

Definition 3.4. Let $f, g \in k[X, Y]$ be irreducible, such that $(f) \neq (g)$. We let $p \in \mathbb{A}^2_k(\overline{k})$ such that $f(p) = g(p) = 0$. We define

$$\iota_p(f, g) := \dim_{\overline{k}} \mathcal{O}_p / (f_p, g_p)$$

Here f_p and g_p are the images of f and g in the localisation of $k[X, Y]$.

Lemma 3.5. $\iota_p(f, g)$ is finite.

The proof of this lemma in the lectures had a gap. The version below corrects this, but assumes a bit of extra commutative algebra. Next time I teach this course I must tidy this all up!

Proof. First we want to have that $(f_p) \neq (g_p)$, so assume $(f_p) = (g_p)$. Then $f_p = g_p h$ for some $h \in \mathcal{O}_p^*$. From the definition of f_p and g_p we get that $f = gh$ for this h, so since f, g are irreducible, we must have $h \in k^*$, otherwise we would have a factorisation. We obtain $(f) = (g)$, which contradicts the assumption.

We will prove something a little more general: let k be a field, and R a finitely generated k-algebra which is local and of dimension 0. Then R is finitely generated as k-module.

Firstly, the Nullstellenzats tells us (OK, need a stronger form!) that the field $l := R/\mathfrak{m}$ is a finite extension of k (we only need the case where k is algebraically closed so $l = k$). So we are done if we can show that some power of $\mathfrak{m}$ is zero. But $\mathfrak{m}$ is finitely generated as an ideal (since R is noetherian), and every element of $\mathfrak{m}$ is nilpotent (since R has dimension 0), so this is clear.

□

[insert proof that number does not depend on chart - easy]

Definition 3.6 (Intersection number)**.** For curves C, D in $\mathbb{P}^2_k$ which meet properly, we define

$$\iota(C, D) := \sum_{p \in (C \cap D)(\overline{k})} \iota_p(C, D)$$

Definition 3.7 (Degree)**.** The degree $\deg(C)$ of a curve C is the degree of an equation for C.

Theorem 3.8 (Bezout)**.** Let k be a field and $C, D \subset \mathbb{P}^2_k$ two curves which meet properly. Then we have

$$\iota(C, D) = \deg(C) \cdot \deg(D)$$

Proof. We only proof this theorem for when $\deg(C) = 1$. Since we can always translate the curves to different coordinates, we may assume without loss of generality that C is given by the equation $x = 0$ and $(0 : 1 : 0) \notin D(k)$. We let g be such that D is given by $g = 0$, so then $x \nmid g$. By our assumption every point of $(C \cap D)(\overline{k})$ is contained in the affine patch

$$\varphi_2 : \mathbb{A}^2 \to \mathbb{P}^2, (x, y) \mapsto (x : y : 1)$$

The degree of g is equal to the degree of the polynomial $g(0, y, 1) \in k[y]$. A calculation will now yield that $\iota(C, D)$ equals the number of roots of g in $\overline{k}$ with multiplicities. We obtain that $\iota(C, D) = \deg(C) \deg(D)$.

□

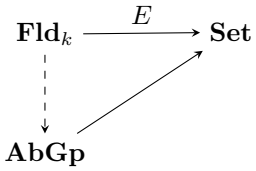
4 Group Law

Let k be a field and C, D two plain curves. We write

$$C \cdot D := \sum_{p \in (C \cap D)(\overline{k})} \iota_p(C, D)[p]$$

We write $[p]$ for elements of the free abelian group generated by $\mathbb{P}^2(\overline{k})$. The expression $C \cdot D$ is a formal sum.

A group law on an elliptic curve E is a factorisation of E. It will be a functor $\mathbf{Fld}_k \to \mathbf{AbGp}$ making the following diagram commute



Here the functor $\mathbf{AbGp} \to \mathbf{Set}$ is the forgetful functor.

Now let E be an elliptic curve over a field k, and let K be a field extension of k. Let $p, q \in E(K)$. For the composition law, we want to draw a line through p and q and look at the third point of intersection of this line with $E(K)$. Because of Bezout's theorem, this point always exists. More precisely:

Lemma 4.1. Let L be the line through p and q, then we can write

$$E \cdot L = [p] + [q] + [r]$$

for a unique $r \in E(K)$.

The non-obvious part of this lemma is that if $p, q \in E(K)$, then $r \in E(K)$. This is an exercise. The rest follows directly from Bezout. If $p = q$, then we should replace L with the tangent line to $E(K)$ through p.

Definition 4.2 (Composition law)**.** For $p, q \in E(K)$, write $L \cdot E = [p] + [q] + [r]$. We definie $p * q = r$.

This operation doesn't define a group law, since it isn't even associative.

Definition 4.3 (Group law)**.** We define $p + q := O * (p * q)$.

Proposition 4.4. The operation $+$ defines an abelian group law on an elliptic curve with neutral element $O = (0 : 1 : 0)$.

Proof. The operation is abelian since $*$ is. We want

$$p + O = p$$

We draw the line L through p and O and find a third point r. We draw the line through r and O, which is L. So the third point we find here is p. We define $-p := p * (O * O)$. We need to show this is in fact the inverse of p, so we compute

$$p + (-p) = O * (p * (p * (O * O)))$$

Let $s := O * O$, and $r = O * p$. Then we have

$$p + (-p) = O * (p * (p * s)) = O * s = O$$

Associativity is a real pain, not nice.

□

4.1 Formulae for group law

Proposition 4.5 (Inversion formula)**.** Let $p \in E(K)$, say $p = (x_p : y_p : 1)$. Then $-p = (x_p : -y_p : 1)$.

Proof. We computed $-p = p * (O * O)$. The tangent line to $E(K)$ through O is the line given by $Z = 0$. The only point in the naive intersection of this line with E is O, so we obtain $O * O = O$. The line given by $X - x_p Z = 0$ gives a naive intersection containing the points O, p and $(x_p : -y_p : 1)$. If $y_p \neq 0$, Bezout's theorem gives that $p * O = (x_p : -y_p : 1)$, so we are done. If $y = 0$, we can compute that $\iota_p(E, X - x_p Z = 0) = 2$ and so we get the same result. So

$$-p = (x_p : -y_p : 1)$$

□

Addition formulae

Let $E : Y^2 = X^3 + aX^2 + bX + c$ be an elliptic curve and $p_1 = (x_1 : y_1 : 1), p_2 = (x_2 : y_2 : 1)$ points on $E(K)$. Write $p_1 * p_2 = (x_3 : y_3 : 1)$. If $p_2 \neq -p_1$ then we have

$$p_1 + p_2 = (x_3 : -y_3 : 1)$$

We can compute x_3 and y_3. Suppose $p_1 \neq p_2$, then we have

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 + y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_1$$

If $p_1 = p_2$, then we obtain

$$x_3 = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c}$$

These formulae can be derived from drawing lines and computing the intersections. They could also be used to define the group law, but this isn't very illuminating.

4.2 Points of order 2 & 3

We write $E(K)[n]$ for the n-torsion points of $E(K)$.

Let E be given by

$$Y^2 = f(X) = X^3 + aX^2 + bX + c$$

4.2.1 2-torsion points

The 2-torsion points are easy to find, since for these points we have $p = -p$. Hence if $p = (x_p : y_p : 1)$, we get $y_p = -y_p = 0$ by proposition 4.5. So the 2-torsion points of $E(\overline{k})$ are the roots of $X^3 + aX^2 + bX + c$ and O. Since E is smooth, these roots are all different and hence $E(\overline{k})[2]$ is isomorphic to V_4.

4.2.2 3-torsion points

The 3-torsion points are a little bit more complicated. Suppose $3p = 0$, for $p = (x_p : y_p : 1)$. Then $2p = -p$, so $x_{2p} = x_{-p} = x_p$. So we get

$$3p = 0 \Leftrightarrow x_{2p} = x_p$$

We let

$$\psi(X) = 3X^4 + 4aX^3 + 6bX^2 + 12c + (4ac - b^2)$$

The formulae for the group law then yield that $3p = 0$ if and only if x_p is a root of ψ. We can write $\psi = 2f \cdot f'' - f'^2$ and so $\psi' = 2f \cdot f''' = 12f$. If ψ would have a double root, then this would be a root of ψ and ψ'. But if $12 \neq 0$, this would be a root of f and f', which because E is smooth is not possible. **Case $12 = 0$ is an exercise**. So there are four different roots of ψ in $\overline{k}$, hence there are four possible values for x_p. Since p isn't a 2-torsion points, this gives a total of eight possibilities for $(x_p : y_p : 1)$. Hence $E(\overline{k})[3]$ contains 9 elements.

Theorem 4.6. Let k be an algebraically closed field, E an elliptic curve over k and p a prime number. If p is a unit in k, then for all $r \geq 1$ we have

$$E(k)[p^r] \cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z}$$

If p isn't a unit, then either

$$E(k)[p] \cong \mathbb{Z}/p\mathbb{Z}$$

or $E(k)[p] = 0$.

Proof. Omitted.

□

4.3 Elliptic curves over finite fields

Let $\mathbb{F}_q$ be the field with $q = p^n$ elements for some prime p and $n \geq 1$. Let E be an elliptic curve over $\mathbb{F}_q$. Since we can view $E(\mathbb{F}_q)\backslash\{O\}$ as a subset of $\mathbb{A}^2(\mathbb{F}_q)$, we know that $E(\mathbb{F}_q)$ contains at most $q^2 + 1$ elements.

We can find better bounds by noticing that there are only q possible x-coordinates for points in $E(\mathbb{F}_q)$. If we fix the last coordinate, this gives us at most $2q$ non-zero points in $E(\mathbb{F}_q)$, since every x-coordinate yields at most 2 possibilities for the y-coordinate. This gives that $E(\mathbb{F}_q)$ has at most $2q + 1$ elements. The following theorem gives an even better bound.

Theorem 4.7 (Hasse,Weil)**.**

$$|\#E(k) - q - 1| \leq 2\sqrt{q}$$

Proof. Omitted. □

5 Reduction modulo p

Definition 5.1. Let $x \in \mathbb{Q}^*$ and p a prime number. We can write $x = p^r \frac{a}{b}$ for r, a, b with $p \nmid ab$, and this r is unique. We write $\mathrm{ord}_p(x) := r$. We also define $\mathrm{ord}_p(0) = \infty$.

Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve over $\mathbb{Q}$. Then

$$\Delta(E) = 2(4a^3 + 27b^2)$$

is the discriminant of E. Let p be a prime number. If $\mathrm{ord}_p(a), \mathrm{ord}_p(b) \geq 0$, then we can reduce these numbers modulo p, this gives $\overline{a}, \overline{b} \in \mathbb{F}_p$. We want to define a curve

$$\overline{E} : Y^2 = X^3 + \overline{a}X + \overline{b}$$

over $\mathbb{F}_p$. We want this to be an elliptic curve as well.

Definition 5.2 (Good primes)**.** Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve over $\mathbb{Q}$. We call p a prime of good reduction, or a good prime, if $\mathrm{ord}_p(a), \mathrm{ord}_p(b) \geq 0$ and $\mathrm{ord}_p(\Delta(E)) = 0$.

This definition states for which primes the reduced curve is an elliptic curve.

We can also reduce points.

There is a reduction homomorphism.

$$\mathrm{red} : E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$

for all good primes p. For $(x : y : z) \in E(\mathbb{Q})$, we choose a representative (x, y, z) such that $\mathrm{ord}_p(x), \mathrm{ord}_p(y), \mathrm{ord}_p(z) \geq 0$ and $\mathrm{ord}_p(x) \mathrm{ord}_p(y) \mathrm{ord}_p(z) = 0$. Exercise: this is always possible. So we get a point $(\overline{x}, \overline{y}, \overline{z})$, and we define $\mathrm{red}(x : y : z) := (\overline{x} : \overline{y} : \overline{z})$. One can verify that $\mathrm{red}(x : y : z) \in \overline{E}(\mathbb{F}_p)$ and that this definition is independent of the choice of representatives (exercise).

Proposition 5.3. The reduction map is a homomorphism of groups.

Proof. Follows from writing out the formulae for the group law, which hold for curves over any field.

□

5.1 Discrete Valuation Rings

Definition 5.4 (Discrete valuation)**.** Let K be a field. A discrete valuation on K is a function

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

satisfying

1. $v(xy) = v(x) + v(y)$
2. $v(x + y) \geq \min\{v(x), v(y)\}$

3. $v(x) = \infty \Leftrightarrow x = 0$

A valuation is called trivial if $v(K) = \{0, \infty\}$ and called normalised if v is surjective.

An example of a discrete valuation is the map $\text{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ we saw earlier.

Definition 5.5 (Integers of a field)**.** Let K be a field with a discrete valuation v. We define the subring $\mathcal{O}_K$ of K by

$$\mathcal{O}_K = \mathcal{O}_{K,v} := \{x \in K : v(x) \geq 0\}$$

This ring is called the ring of integers.

Definition 5.6 (Discrete Valuation Ring)**.** Let R be a domain with fraction field K. We call R a discrete valuation ring if there exists a non-trivial discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ such that $R = \mathcal{O}_{K,v}$.

Proposition 5.7. Let R be a DVR with fraction field K. Then there exists a unique normalised discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ satisfying $R = \mathcal{O}_{K,v}$.

Proof. Exercise.

□

For a discrete valuation ring R, with normalised valuation v, there exists a unique maximal ideal given by

$$\mathcal{M} := \{x \in R | v(x) > 0\}$$

Definition 5.8 (Residue field)**.** The residue field of a discrete valuation ring R is the quotient $R/\mathcal{M}$, where $\mathcal{M}$ is the unique maximal ideal of R.

Lemma 5.9. Let $\pi \in R$ be a uniformiser of v, i.e. an element satisfying $v(\pi) = 1$. Then $\mathcal{M} = \pi R$.

Proof. Suppose $x \in \mathcal{M}$, then $v(x) > 0$, so we have $v(\pi^{-1}x) = v(\pi^{-1}) + v(x) = v(x) - 1 \geq 0$. So $\pi^{-1}x \in R$, hence $x \in \pi R$. If $x \in \pi R$, then we have $v(\pi^{-1}x) \geq 0$ since $\pi^{-1}x \in R$. Hence we get

$$v(x) = v(\pi) + v(\pi^{-1}x) \geq 1 > 0$$

We conclude $\mathcal{M} = \pi R$. □

5.2 Reduction over DVRs

Let R be a discrete valuation ring, K the fraction field of R and v the unique normalised valuation on K satisfying $\mathcal{O}_{K,v} = R$. Let E be an elliptic curve over K given by

$$E : Y^2 = X^3 + aX^2 + bX + c =: f(X)$$

We want to reduce this curve to k and we do this by doing the same we did for reducing curves over $\mathbb{Q}$. Suppose $v(a), v(b), v(c) \geq 0$ and $v(\Delta(E)) = 0$. We have a quotient map

$$R \to R/\mathcal{M} =: k$$

We define

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$$

The condition $v(a), v(b), v(c) \geq 0$ gives us that $\overline{a}, \overline{b}, \overline{c}$ are elements of k. The restriction $v(\Delta(E)) = 0$ gives that $\Delta(E)$ is a unit in k, and is thus non-zero. Hence $\overline{E}$ is an elliptic curve over k.

Just as before, we define a reduction map by choosing a representative (x_p, y_p, z_p) for $p \in E(K)$, such that $x_p, y_p, z_p \in R$ and $v(x_p)v(y_p)v(z_p) = 0$, then taking the images of x_p, y_p and z_p under the quotient map from R to $R/\mathcal{M}$.

Proposition 5.10. The reduction map

$$\text{red} : E(K) \to \overline{E}(k)$$

is a group homomorphism.

Proof. As before. □

This generalises reduction modulo p.

6 p-adic Numbers

Warning: throughout this section, we are a bit careless with 0 - we do not always spell it out as a special case, even when we should.

Definition 6.1 (p-adic norm)**.** Let p be a prime number and $x \in \mathbb{Q}$. We define the p-adic norm on $\mathbb{Q}$ by

$$|x|_p := p^{-\operatorname{ord}_p(x)}$$

Proposition 6.2. The function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ is a norm for all primes p and it satisfies $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in \mathbb{Q}$. Inequality holds if and only if $x = y$.

Proof. Exercise.

□

Definition 6.3 (Field of p-adic numbers)**.** We define $\mathbb{Q}_p$ as the completion of the metric space $(\mathbb{Q}, |\cdot|_p)$, i.e.

$$\mathbb{Q}_p = \frac{\{\text{Cauchy sequences in } (\mathbb{Q}, |\cdot|_p)\}}{\{\text{null-sequences}\}}$$

This is an extension field of $\mathbb{Q}$.

Proposition 6.4. Let (a_n) be a Cauchy sequence in $(\mathbb{Q}, |\cdot|_p)$ which doesn't converge to 0. Then there is an N such that $|a_n|_p = |a_m|_p$ for all $n, m \geq N$.

Proof. Since (a_n) is Cauchy we have

$$\forall \varepsilon > 0 : \exists N : \forall n, m \geq N : |a_m - a_n|_p < \varepsilon$$

Because (a_n) doesn't converge to 0 we also have

$$\exists \varepsilon > 0 : \forall N : \exists n \geq N : |a_m|_p \geq \varepsilon$$

Let $\varepsilon > 0$ be satisfying the second formula. Let N be satisfying the first formula. Let $n \geq N$ be as in the second formula. Then for all $m \geq n$ we have

$$|a_m|_p = |a_m - a_n + a_n|_p = \max\{|a_m - a_n|_p, |a_n|_p\}$$

Because $n, m \geq N$, we have that $|a_m - a_n|_p < \varepsilon$, while n is such that $|a_n|_p \geq \varepsilon$. So $|a_m|_p = |a_n|_p$.

□

Corollary 6.5. We can define the absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ by setting $|0|_p = 0$ and

$$|(a_n)|_p := \lim_{n\to\infty} |a_n|_p$$

Check this is an absolute value, and that it's image in $\mathbb{R}$ is the same as the image of $\mathbb{Q}$.

6.1 Discrete valuation on $\mathbb{Q}_p$

We can find a discrete valuation ord_p on $\mathbb{Q}_p$ by reversing the steps we took to get from ord_p to $|\cdot|_p$. We define

$$\mathrm{ord}_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}, x \mapsto -\log_p(|x|_p)$$

We write $\mathbb{Z}_p$ for the discrete valuation ring:

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p | \, \mathrm{ord}_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

Since $v(p) = -\log_p\left(\frac{1}{p}\right) = 1$, we find by lemma 5.9 that the maximal ideal $\mathcal{M}_p$ is equal to $p\mathbb{Z}_p$.

Proposition 6.6. The residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{F}_p$.

Proof. Let $\alpha \in \mathbb{Z}_p$ and (a_n) a Cauchy sequence representing α. Then since $\mathrm{ord}_p(\alpha) \geq 0$ there is an N such that for all $n \geq N$ we have $\mathrm{ord}_p(a_n) \geq 0$. Choose the minimal N with this property. Choose M to be the minimal index such that for all $n, m \geq M$ we have $|a_n - a_m|_p < 1$. Then $\mathrm{ord}_p(a_n - a_m) > 0$. Write $a_n = \frac{b_n}{c_n}$ for b_n, c_n coprime. Then p is no divisor of c_n when $n > N$. Let $\overline{b_n}$ be the image of b_n in $\mathbb{F}_p$. Choose $r > \max\{M, N\}$ and define

$$\varphi : \mathbb{Z}_p \to \mathbb{F}_p, \alpha \frac{\overline{b_r}}{\overline{c_r}}$$

It is possible to show this is a well-defined map, independent of any choice. Restricted to $\mathbb{Z}$ this is the canonical map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, so φ is surjective. The kernel are precisely the elements for which $\overline{b_r}$ vanishes, i.e. the elements $x \in \mathbb{Z}_p$ with $\mathrm{ord}_p(x) > 0$. So $\ker(\varphi) = p\mathbb{Z}_p$, so $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

□

In a similar way we can prove

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

6.2 Expansions of p-adic numbers

Proposition 6.7 (Expansion in $\mathbb{Z}_p$)**.** Let $\alpha \in \mathbb{Z}_p$. Then there are unique $a_0, a_1, \ldots \in \{0, \ldots, p-1\}$ such that

$$\alpha = \sum_{i=0}^{\infty} a_i p^i$$

We have $a_0 = 0 \Leftrightarrow \alpha \in p\mathbb{Z}_p$.

Proof. Let φ be the isomorphism $\mathbb{Z}_p/p\mathbb{Z}_p \to \mathbb{F}_p$ as before. Let $0 \leq a_0 \leq p-1$ such that $\varphi(\alpha) = \overline{a_0}$. Because φ is injective, we have

$$\alpha \in p\mathbb{Z}_p \Leftrightarrow \overline{a_0} = 0 \Leftrightarrow a_0 \in p\mathbb{Z} \Leftrightarrow a_0 = 0$$

Now we have

$$\varphi(\alpha - a_0) = \varphi(\alpha) - \varphi(a_0) = 0$$

following the definition of φ. So we find $\alpha - a_0 \in p\mathbb{Z}_p$. Let $\alpha_1 \in \mathbb{Z}_p$ such that $\alpha - a_0 = p\alpha_1$, choose a_1 such that $\varphi(\alpha_1) = \overline{a_1}$ and choose α_{i+1} such that $\alpha_i - a_i = p\alpha_{i+1}$. Then we get a series $\sum_{i=0}^{\infty} a_i p^i$ satisfying

$$\left|\alpha - \sum_{i=0}^{N} a_i p^i\right|_p = \left|\alpha - a_0 - \sum_{i=1}^{N} a_i p^i\right|_p = \left|p\alpha_1 - \sum_{i=1}^{N} a_i p^i\right|_p = |a_N p^N - a_N p^N|_p$$

This converges to 0 as $N \to \infty$, so the series converges to α. Finally, suppose that $\sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i$. Then we have $a_0 = \varphi(\alpha) = b_0$, so the first terms are equal. Inductively we can thus show that $a_i = b_i$ for all i.

□

Corollary 6.8 (Expansion in $\mathbb{Q}_p$)**.** Let $\alpha \in \mathbb{Q}_p$. Then there are unique $a_i \in \{0, \ldots, p-1\}$ such that

$$\alpha = \sum_{i=\mathrm{ord}_p(\alpha)}^{\infty} a_i p^i$$

Proof. This follows directly from the expansions of $\mathbb{Z}_p$. Write $\alpha = p^{\mathrm{ord}_p(\alpha)} p^{-\mathrm{ord}_p(\alpha)} \alpha$ and then expand $p^{-\mathrm{ord}_p(\alpha)}\alpha \in \mathbb{Z}_p$. Multiplication with $p^{\mathrm{ord}_p(\alpha)}$ gives the expansion for α.

□

6.3 Hasse principal

Let C be a variety over $\mathbb{Q}$. We can view $\mathbb{Q}$ as a subfield of both $\mathbb{Q}_p$ and $\mathbb{R}$, so $C(\mathbb{Q}) \neq \varnothing$ implies $C(\mathbb{Q}_p) \neq \varnothing \neq C(\mathbb{R})$. We say a variety satisfies the Hasse principal if the other implication holds.

Definition 6.9 (Hasse principal)**.** Let $C \subset \mathbb{P}^2_{\mathbb{Q}}$ a smooth curve. We say C satisfies the Hasse principal if

$$C(\mathbb{Q}) \neq \varnothing \Leftrightarrow C(\mathbb{R}) \neq \varnothing \text{ and for all primes } p : C(\mathbb{Q}_p) \neq \varnothing$$

Theorem 6.10 (Legendre)**.** Every smooth degree 2 curve over $\mathbb{Q}$ satisfies the Hasse principal.

Proposition 6.11 (Selmer)**.** The curve C in $\mathbb{P}^2_{\mathbb{Q}}$ given by $3X^3 + 4Y^3 + 5Z^3$ satisfies $C(\mathbb{R}) \neq \varnothing \neq C(\mathbb{Q}_p)$, while $C(\mathbb{Q}) = \varnothing$.

Lemma 6.12. Let $\{f_1, \ldots, f_r\} \subset \mathbb{Z}_p[X_1, \ldots, X_k]$, then we have

$$\exists \bar{\alpha} \in \mathbb{Z}_p^k : \forall i f_i(\bar{\alpha}) = 0 \Leftrightarrow \forall n > 0 : \exists \bar{x} \in \mathbb{Z}/p^n\mathbb{Z} : \forall i f_i(\bar{x}) = 0$$

Proof. From left to right is easy: view $\mathbb{Z}/p^n\mathbb{Z}$ as $\mathbb{Z}_p/p^n\mathbb{Z}_p$, then a common root of $f_1, \ldots, f_r$ in $\mathbb{Z}_p$ yields a common root in $\mathbb{Z}_p/p^n\mathbb{Z}_p$.

So suppose for every n we have such a common root. Define

$$S(n) := \{(x_1, \ldots, x_k) \in (\mathbb{Z}/p^n\mathbb{Z})^k : \forall i : f_i(x_1, \ldots, x_k) = 0\}$$

This is non-empty for every n, so the set

$$\bigcup_{n>0} S(n)$$

is infinite. Choose $x_1 \in S(1)$ such that the set

$$\left\{ y \in \bigcup_{m>1} S(m) | y \equiv x_1 (\mathrm{mod} p) \right\}$$

is infinite. We choose x_{i+1} such that the set

$$\left\{ y \in \bigcup_{m>i+1} S(m) | y \equiv x_{i+1} (\mathrm{mod} p^{i+1}) \right\}$$

is infinite and $x_{i+1} \equiv x_i \bmod p^i$. With the aid of the axiom of choice, we get a sequence (x_i) with $x_n \in (\mathbb{Z}/p^n\mathbb{Z})^k$. We can choose lifts to $\mathbb{Z}_p$, say $\widetilde{x_i}$. By construction, this gives a Cauchy sequence in $\mathbb{Z}_p$ and so it has a limit $x \in (\mathbb{Z}_p)^k$. Since polynomials define continuous maps in the p-adic topology [exercise!], we obtain

$$f_i(x) = f_i(\lim_{i\to\infty} \widetilde{x_i}) = \lim_{i\to\infty} f(\widetilde{x_i}) = 0$$

□

If desired, one could remove all the choices in the previous proof.

6.4 Hensel's lemma

Theorem 6.13 (Hensel's Lemma)**.** Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $\alpha \in \mathbb{Z}_p^n$ such that there exists an $m \geq 0$ satisfying

- $f(\alpha) \equiv 0 \bmod p^{2m+1}$
- $\exists i : \frac{\partial f}{\partial x_i}|_\alpha \not\equiv 0 \bmod p^{m+1}$

Then there exists a $b \in \mathbb{Z}_p^n$ such that $b \equiv \alpha \bmod p^{m+1}$ and $f(b) = 0$.

Hensels lemma says that, given enough smoothness, an approximate root of a polynomial is enough to find a root in $\mathbb{Z}_p$.

Proof. First we look for a $\beta \in \mathbb{Z}_p^n$ satisfying $\beta \equiv \alpha \bmod p^{m+1}$ and $f(\beta) \equiv 0 \bmod p^{2m+2}$. For this we write

$$\beta_i = \alpha_i + h_i p^{m+1}$$

We look for this $h_i \in \mathbb{Z}_p$. We use Taylor expansion around a:

$$f(\beta_1, ..., \beta_n) = f(\alpha_1, ..., \alpha_n) + \sum_{j=1}^{n} \left(\frac{\partial f}{\partial x_j} \right) |_\alpha h_j p^{m+1} + O(p^{2m+2})$$

So we are looking for an h_i such that this is divisible by p^{2m+2}.

There exists a unique $k \leq m$ such that p^k divides $\left(\frac{\partial f}{\partial x_j} \right) |_\alpha$ for all j, and such that there exists a j such that p^{k+1} does not divide $\left(\frac{\partial f}{\partial x_j} \right) |_\alpha$. We can find some H_j such that

$$\frac{f(a_1, \ldots, a_n)}{p^{2m+1}} + \sum_{j=1}^{n} \left(\frac{\partial f}{\partial x_j} \right) |_\alpha \frac{1}{p^k} H_j = 0 \bmod p$$

Since the j^{th} partial derivative is now a unit in $\mathbb{Z}_p$, we can find H_j by solving for H_j. Now we set $h_j := p^{m-k} H_j$. We can now verify that β does what we want.

So this gives us if α satisfies $f(\alpha) \equiv 0 \bmod p^{2m+r}$ for some $r \geq 1$, we can find a β with $\beta \equiv \alpha \bmod p^{m+r}$ and $f(\beta) \equiv 0 \bmod p^{2m+r+1}$.

Now we let $\beta := \alpha_{2m+2} \in \mathbb{Z}_p^n$. Because $\alpha_{2m+2} \equiv \alpha \bmod p^{m+1}$, there still exists a j such that

$$\left(\frac{\partial f}{\partial x_j} \right) |_{\alpha_{2m+2}} \not\equiv 0 \bmod p^{m+1}$$

Now we end up with a sequence $\alpha_{2m+3}, \alpha_{2m+4}, \ldots$ which is Cauchy in $\mathbb{Z}_p^n$. Since f is continuous, we have for $b := \lim_{r \to \infty} \alpha_{2m+r}$

$$f(b) = \lim_{r \to \infty} f(\alpha_{2m+r}) = 0$$

□

Definition 6.14. A discrete valuation ring R is called Hensellian if the statement in Hensels lemma holds for R.

So Hensels lemma can be reformulated as '$\mathbb{Z}_p$ is Hensellian'.

7 Elliptic curves over $\mathbb{Q}_p$

Fix an elliptic curve E over $\mathbb{Q}_p$ given by

$$E : Y^2 = X^3 + aX + b$$

with $a, b \in \mathbb{Z}_p$ and $\mathrm{ord}_p(\Delta) = 0$. Recall that we have a reduction homomorphism

$$\mathrm{red} : E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p)$$

Proposition 7.1. The reduction map red is surjective.

Proof. Since red is a group homomorphism, we already know that $(0 : 1 : 0) \in \mathrm{red}(E(\mathbb{Q}_p))$, so let $(x_0 : y_0 : 1) \in \overline{E}(\mathbb{F}_p)$. Let $x_0', y_0' \in \mathbb{Z}_p$ such that $x_0' \equiv x_0 \bmod p$ and $y_0' \equiv y_0 \bmod p$. Let

$$F(X, Y) := Y^2 - (X^3 + aX + b)$$

Then we have $F(x_0', y_0') \equiv 0 \bmod p$. Because $\overline{E}$ is smooth, either

$$\frac{\partial F}{\partial X}(x_0', y_0') \not\equiv 0 \bmod p$$

or

$$\frac{\partial F}{\partial Y}(x_0', y_0') \not\equiv 0 \bmod p$$

Hensels lemma gives an $(x_1, y_1) \in \mathbb{Z}_p^2$ such that $F(x_1, y_1) = 0$, $x_1 \equiv x_0' \bmod p$ and $y_1 \equiv y_0' \bmod p$. We find that $(x_1 : y_1 : 1) \in E(\mathbb{Q}_p)$ and $\mathrm{red}(x_1 : y_1 : 1) = (x_0 : y_0 : 1)$.

□

7.1 Filtrations

Notation 7.2. We let $E^0(\mathbb{Q}_p) := E(\mathbb{Q}_p)$ and

$$E^1(\mathbb{Q}_p) := \ker(E(\mathbb{Q}_p) \xrightarrow{\mathrm{red}} \overline{E}(\mathbb{F}_p))$$

Next we want to define a chain

$$E^0(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset E^2(\mathbb{Q}_p) \supset ...$$

Proposition 7.3. For $p \in E^0(\mathbb{Q}_p)$, the following are equivalent:

1. $p \in E^1(\mathbb{Q}_p)$
2. we can write $p = (x : y : z)$ with $\mathrm{ord}_p(x) > 0$, $\mathrm{ord}_p(y) = 0$ and $\mathrm{ord}_p(z) > 0$.

Proof. $2 \Rightarrow 1$: Because p divides x and z but not y, we find immediately that $\mathrm{red}(p) = 0$.

$1 \Rightarrow 2$: If $\mathrm{red}(p) = 0$, then we have $\mathrm{red}(p) = (\bar{x} : \bar{y} : \bar{z})$ with $x, z \in p\mathbb{Z}_p$ and $y \notin p\mathbb{Z}_p$. The claim follows.

□

Definition 7.4. For $n \geq 2$, let

$$E^n(\mathbb{Q}_p) := \{(x : y : z) \in E^1(\mathbb{Q}_p) | \operatorname{ord}_p(x) - \operatorname{ord}_p(y) \geq n\}$$

This restriction is independent of the chosen representative for $(x : y : z)$, it's saying that $\frac{x}{y}$ should be an element of $p^n\mathbb{Z}_p$.

Theorem 7.5. 1. The set $E^n(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$ for all n and the map

$$E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p, Q \mapsto p^{-n}\frac{x(Q)}{y(Q)}$$

is an isomorphism of groups.

2. We have

$$\bigcap_n E^n(\mathbb{Q}_p) = \{0\}$$

Proof. 1. We use induction. If $n = 1$, we already have that $E^n(\mathbb{Q}_p)$ is a subgroup by definition. Since red is surjective, we also get the isomorphism. Now suppose $n > 1$ and we know the statement holds for any $m < n$. Suppose $Q = (x : y : 1) \in E^1(\mathbb{Q}_p)$. Because $\operatorname{red}(Q) = 0$, we have $y \notin \mathbb{Z}_p$: the last coordinate of $\operatorname{red}(Q)$ is 0, so if $\operatorname{ord}_p(y) \geq 0$, then only the first coordinate of $\operatorname{red}(Q)$ could be non-zero, which is impossible. similar for x. So write $x = p^{-m_1}x_0, y = p^{-m_2}y_0$ for $m_1, m_2 > 0$ and $x_0, y_0 \in \mathbb{Z}_p^*$. Since $Q \in E(\mathbb{Q}_p)$, we have

$$p^{-2m_2}y_0^2 = p^{-3m_1}x_0^3 + ap^{-m_1}x_0 + b$$

By taking the ord_p of both sides, we find $2m_2 = 3m_1$. Let $n := m_2 - m_1 \geq 1$, then $m_1 = 2n$ and $m_2 = 3n$. Since we have $\operatorname{ord}_p(x) = \operatorname{ord}_p(z) - 2n$ and $\operatorname{ord}_p(y) = \operatorname{ord}_p(z) - 3n$, because $\operatorname{ord}_p(x) - \operatorname{ord}_p(y) = n$, we can write $Q = (p^n x_0 : y_0 : p^{3n}z_0)$ for $y_0 \in \mathbb{Z}_p^*$ and $x_0, z_0 \in \mathbb{Z}_p$. Since $Q \in E(\mathbb{Q}_p)$ we have

$$p^{3n}y_0^2z_0 = p^{3n}x_0^3 + ap^{7n}x_0z_0^2 + bp^{9n}z_0^3$$

The point $\overline{Q_0} = (\overline{x_0} : \overline{y_0} : \overline{z_0})$ is a point on the non-smooth curve given by

$$E_0 : y^2z = x^3$$

over $\mathbb{F}_p$. Despite its non-smoothness, we can still make $E_0(\mathbb{F}_p)\backslash\{(0 : 0 : 1)\}$ into an abelian group by using the formulae for the group law on elliptic curves. We can use this to verify that the map

$$\phi : E^n(\mathbb{Q}_p) \to E_0(\mathbb{F}_p)\backslash\{(0 : 0 : 1)\}, Q \mapsto \overline{Q_0}$$

is a surjective group homomorphism. The map

$$E_0(\mathbb{F}_p)\backslash\{(0 : 0 : 1)\} \to \mathbb{F}_p, (x : y : z) \mapsto \frac{x}{y}$$

is an isomorphism of groups [exercise], so finally the map

$$E^n(\mathbb{Q}_p) \to \mathbb{F}_p, (x : y : z) \mapsto p^{-n}\frac{x}{y}$$

is a surjective group homomorphism with kernel $E^{n+1}(\mathbb{Q}_p)$. In particular, $E^{n+1}(\mathbb{Q}_p)$ is a subgroup of $E^n(\mathbb{Q}_p)$.

2. Suppose $Q = (x_Q : y_Q : z_Q) \in \bigcap_n E^n(\mathbb{Q}_p)$. Then for all n we have $\mathrm{ord}_p(x_Q) - \mathrm{ord}_p(y_Q) \geq n$. This can only be true if $x_Q = 0$, while $y_Q \neq 0$. Suppose $z_Q \neq 0$, then since $Q \in E(\mathbb{Q}_p)$ it would have to satisfy $y_Q^2 = bz_Q^2$. Since $\mathrm{ord}_p(b) = 0$, this gives $\mathrm{ord}_p(y_Q) = \mathrm{ord}_p(z_Q)$, and thus $\mathrm{red}(Q) \neq 0$, a contradiction. So we obtain $Q = (0 : 1 : 0)$.

□

Corollary 7.6. Let $m \in \mathbb{Z}_{>0}$ such that $p \nmid m$. Then the map

$$[m] : E^1(\mathbb{Q}_p) \to E^1(\mathbb{Q}_p), Q \mapsto mQ$$

is a bijection.

Proof. Injective: note that this map is a group homomorphism, so suppose $mQ = 0$ for some $Q \in E^1(\mathbb{Q}_p)$. If $Q \neq 0$, then $Q \in E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p)$ for $n = \mathrm{ord}_p(x_Q) - \mathrm{ord}_p(y_Q)$ and it is non-zero in that quotient. Then the image of Q in $\mathbb{F}_p$ is non-zero so since $p \nmid m$, we find that the image of mQ is non-zero. This is a contradiction, so $Q = 0$ and $[m]$ is injective.

Surjective: let $Q \in E^1(\mathbb{Q}_p)$ be arbitrary. Since $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p)$ is isomorphic to $\mathbb{F}_p$ and $m \not\equiv 0 \bmod p$, we can find an $R_1 \in E^1(\mathbb{Q}_p)$ such that $mR_1 \equiv Q \bmod E^2(\mathbb{Q}_p)$. similarly we can find $R_i \in E^i(\mathbb{Q}_p)$ such that $Q - mR_{i-1} \equiv mR_i \bmod E^{i+1}(\mathbb{Q}_p)$. We get a sequence $R_1, R_2, \ldots$ such that $R_i \in E^i(\mathbb{Q}_p)$ and $Q - m\sum_{j=1}^{i} R_i \in E^{i+1}(\mathbb{Q}_p)$. We now want to find a convergent subsequence. We give

$$\mathbb{Z}_p^* \times \mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p^* \times \mathbb{Z}_p \times \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p^* \times \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p^*$$

product topologies and we get maps ψ_0, ψ_1, ψ_2 defined by

$$\psi_0 : \mathbb{Z}_p^* \times \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{P}^2(\mathbb{Q}_p), (x, y, z) \mapsto (x : y : z)$$

(similar for ψ_1, ψ_2). Then the union of the images is the entire $\mathbb{P}^2(\mathbb{Q}_p)$, so $\mathbb{P}^2(\mathbb{Q}_p)$ becomes a compact topological space [see homework]. Let $S_i = \sum_{j=1}^{i} R_i$, then infinitely many S_i are in the image of at least one of the ψ_i, say ψ_0. Compactness implies existence of a convergent subsequence $(\tilde{S}_i)$ of (S_i). Let $S := \lim_{i\to\infty} \tilde{S}_i$. Let $R := \psi_0(S)$. Because R is a limit of elements in $E(\mathbb{Q}_p)$, which is closed in $\mathbb{P}^2(\mathbb{Q}_p)$, we have that $R \in E(\mathbb{Q}_p)$. The reduction map is continuous so $E^1(\mathbb{Q}_p)$ is closed in $E(\mathbb{Q}_p)$, hence $R \in E^1(\mathbb{Q}_p)$. Similarly we can show that $E^n(\mathbb{Q}_p)$ is closed in $E(\mathbb{Q}_p)$ for all n. Let $T_i := Q - m\tilde{S}_i$, then the sequence of T_i converges to $T := Q - mR$. Because all $E^i(\mathbb{Q}_p)$ are closed, they all contain T, hence $T = 0$. So $Q = mR$ and we find that $[m]$ is surjective.

□

8 Torsion points

Corollary 8.1. Let E be an elliptic curve over $\mathbb{Q}$ given by

$$E : Y^2 = X^3 + aX + b$$

and p a good prime. Let

$$E(\mathbb{Q})_{p'-\text{tors}} = \{x \in E(\mathbb{Q}) : \exists m \in \mathbb{Z}_{\geq 1} : p \nmid m, mx = 0\}$$

Then the map

$$\text{red} : E(\mathbb{Q})_{p'-\text{tors}} \to \overline{E}(\mathbb{F}_p)$$

is injective.

Proof. First note that $E(\mathbb{Q})_{p'-\text{tors}}$ is a subgroup of $E(\mathbb{Q})$. Suppose $Q \in E(\mathbb{Q})_{p'-\text{tors}}$ satisfies $\text{red}(Q) = 0$. Then there is some $m \nmid p$ such that $mQ = 0$. Let $\varphi : E(\mathbb{Q}) \to E(\mathbb{Q}_p)$ be an inclusion, then $\text{red}(\varphi(Q)) = 0$, so $\varphi(Q) \in E^1(\mathbb{Q}_p)$. So we get

$$m\varphi(Q) = \varphi(mQ) = \varphi(0) = 0$$

From corollary 7.6 we obtain that $\varphi(Q) = 0$, so since φ is injective, we find $Q = 0$.

□

Corollary 8.2. The torsion group $E(\mathbb{Q})_{\text{tors}}$ is finite.

Proof. Let $p_1 \neq p_2$ be two good primes for E. Then we have a map

$$E(\mathbb{Q})_{p_1'-\text{tors}} \times E(\mathbb{Q})_{p_2'-\text{tors}} \to E(\mathbb{Q})_{\text{tors}}, (x, y) \mapsto x + y$$

Because $p_1 \neq p_2$, this is a surjective group homomorphism. The previous corollary implies that the two groups on the left are finite, so $E(\mathbb{Q})_{\text{tors}}$ must be finite as well.

□

Theorem 8.3. The map $\text{red} : E(\mathbb{Q})_{\text{tors}} \to \overline{E}(\mathbb{F}_p)$ is injective.

Proof. Omitted, not really hard but long and messy.

□

Theorem 8.4. If $Q = (x : y : 1) \in E(\mathbb{Q})_{\text{tors}}$ then we have $x \in \mathbb{Z}, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 | \Delta$.

Proof. Omitted, long, messy, not really hard.

□

The previous two theorems don't generalise well to general number fields, they are just true for $\mathbb{Q}$.

Theorem 8.5 (Mazur)**.** If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups: $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $m \in \{1, ..., 10\} \cup \{12\}$ and $n \in \{2, 4, 6, 8\}$. All these groups occur.

Proof. A very long way beyond this course.

□

9 Galois Cohomology

9.1 Finite Groups

Definition 9.1 (Action)**.** Let G be a finite group and M an abelian group. An action of G on M is a group homomorphism $G \to \mathrm{Aut}(M)$.

Proposition 9.2. An action of G on M is equivalent to a map of sets $G \times M \to M$ satisfying

(M1) For all $g \in G, m, m' \in M$ we have $g(m' + m) = gm + gm'$.

(M2) For all $g, g' \in G, m \in M$ we have $(gg')m = g(g'm)$.

(M3) For all $m \in M$ we have $1m = m$.

Proof. Exercise. □

Definition 9.3 (G-modules)**.** A G-module is an abelian group M equipped with a G-action.

Definition 9.4 (Morphisms)**.** A morphism of G-modules M_1, M_2 is a morphism of groups $f : M_1 \to M_2$ satisfying $f(gm) = gf(m)$ for all $m \in M_1$.

Proposition 9.5. Let $f : M_1 \to M_2$ be a morphism of G-modules. Then $\ker(f), \mathrm{im}(f)$ and $\mathrm{coker}(f)$ are G-modules in a natural way. The canonical maps are morphisms of G-modules.

Proof. For $\ker(f)$ and $\mathrm{im}(f)$ the G-action is a restriction of the action on M_1. So we need to show that for $g \in G$ and $m \in \ker(f)$, we have $gm \in \ker(f)$. This is true since $f(gm) = gf(m) = g \cdot 0 = 0$. If $m \in \mathrm{im}(f)$ there is an $m' \in M_1$ such that $f(m') = m$, so we have $f(gm') = gf(m') = gm$. The canonical maps are morphisms by definition.

If $\overline{m} \in \mathrm{coker}(f)$, define $g\overline{m} := \overline{gm}$. Suppose m' is another representative for $\overline{m}$, then there is an $m'' \in \mathrm{im}(f)$ with $m' = m + m''$. We get $gm' = gm + gm''$, so since $gm'' \in \mathrm{im}(f)$ this action is well-defined. The natural projection again is a morphism by definition.

□

Definition 9.6. A sequence

$$A_1 \to A_2 \to A_3 \to \cdots$$

of G-modules is called exact if it is an exact sequence of abelian groups.

Definition 9.7. If M is a G-module, the set of G-invariants is defined by

$$M^G := \{m \in M : \forall g \in G : gm = m\}$$

Proposition 9.8. If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules then the sequence

$$0 \to A^G \to B^G \to C^G$$

is also exact.

Proof. Let $f : A \to B$ and $h : B \to C$ be the maps in the sequence. Injectivity of f is obvious. First we need to show that the restrictions of f and g map in to the right codomain. So let $a \in A^G$, then for all $g \in G$ we have $gf(a) = f(ga) = f(a)$, hence $f(A^G) \subset B^G$. The same argument holds for h. We also have $f(A^G) \subset f(A) = \ker(h)$. Hence for all $b \in f(A^G)$ we have $h(b) = 0$. We also have

$$\ker(h|_{B^G}) = \ker(h) \cap B^G \subset \ker(h) = \mathrm{im}(f)$$

So for every $b \in \ker(h|_{B^G})$ there is an $a \in A$ such that $f(a) = b$. For all $g \in G$ we have

$$b = gb = gf(a) = f(ga)$$

so since f is injective we obtain $ga = a$. So the sequence is exact.

□

Definition 9.9 (Crossed homomorphism)**.** Let M be a G-module. A map of sets $f : G \to M$ is called a crossed homomorphism if

$$f(gh) = f(g) + gf(h)$$

holds for every $g, h \in G$. We call f a principal crossed homomorphism if there exists an $m \in M$ such that $f(g) = gm - m$ for all $g \in G$.

Notation 9.10. Write $\mathrm{CH}(G, M)$ for the set of crossed homomorphisms $G \to M$ and $\mathrm{PCH}(G, M)$ for the set of principal crossed homomorphisms.

Proposition 9.11. Let M be a G-module.

1. The set $\mathrm{CH}(G, M)$ forms a group under addition.
2. $\mathrm{PCH}(G, M) \subset \mathrm{CH}(G, M)$
3. The set $\mathrm{PCH}(G, M)$ is a subgroup of $\mathrm{CH}(G, M)$.

Proof.

1. Suppose $f_1, f_2 \in \mathrm{CH}(G, M)$. Then for all $g, h \in G$ we have

$$(f_1 + f_2)(gh) = f_1(gh) + f_2(gh) = f_1(g) + f_2(g) + gf_1(h) + gf_2(h)$$

$$= (f_1 + f_2)(g) + g(f_1 + f_2)(h)$$

So $\mathrm{CH}(G, M)$ is closed under addition, so it's a group.

2. If $f \in \mathrm{PCH}(G, M)$, then for all $g, h \,\mathrm{im}\, G$ we have

$$f(gh) = ghm - m = ghm - gm + gm - m = gm - m + g(hm - m) = f(g) + gf(h)$$

Hence $\mathrm{PCH}(G, M) \subset \mathrm{CH}(G, M)$.

3. Choose $m = 0$ to find that $0 \in \mathrm{PCH}(G, M)$. If $f_1, f_2 \in \mathrm{PCH}(G, M)$, then there are m, m' such that

   $$(f_1 + f_2)(g) = f_1(g) + f_2(g) = gm - m + gm' - m' = g(m + m') - (m + m')$$

   for all $g \in G$, so $f_1 + f_2 \in \mathrm{PCH}(G, M)$. Finally, note that negations of principal crossed homomorphisms are again principal.

□

Definition 9.12 (Cohomology)**.** For G a finite group and M a G-module, we define the following cohomology groups:

$$H^0(G, M) := M^G$$

$$H^1(G, M) := \frac{\mathrm{CH}(G, M)}{\mathrm{PCH}(G, M)}$$

Note that if the G-action on M is trivial, then $\mathrm{PCH}(G, M) = 0$ and $\mathrm{CH}(G, M) = \mathrm{Hom}(G, M)$. In this case we then have $H^1(G, M) = \mathrm{Hom}(G, M)$.

If $f : A \to B$ is a morphism of G-modules, we obtain a group homomorphism

$$H^1(G, A) \to H^1(G, B), [h] \mapsto [f \circ h]$$

Proposition 9.13. Let $0 \xrightarrow{i} A \to B \xrightarrow{\pi} C \to 0$ be a short exact sequence of G-modules. There is a natural group homomorphism $\delta : H^0(G, C) \to H^1(G, A)$.

Proof. Let $c \in C^G$, then there is a $b \in B$ such that $\pi(b) = c$. Choose such a b. Consider $gb - b \in B$ for some $g \in G$, then we have $\pi(gb - b) = g\pi(b) - \pi(b) = gc - c = 0$, since $c \in C^G$. Let $a \in A$ be the unique element such that $i(a) = gb - b$ and define $\delta_b(c)(g) := a$. Then $\delta_b(c)$ is a map $G \to A$. We want that $\delta : H^0(G, C) \to H^1(G, A), c \mapsto [\delta_b(c)]$ is a well-defined homomorphism of groups. Let $b' \in B$ such that $\pi(b') = c$, then $\pi(b' - b) = 0$. So there is an $a' \in A$ such that $b' - b = i(a')$, so $b' = b + i(a')$. Then we have

$$gb' - b = g(b + i(a')) - (b + i(a')) = gb - b + gi(a') - (a')$$

So $\delta_b(c) - \delta_{b'}(c) \in \mathrm{PCH}(G, A)$, so δ is well-defined. Exercise: it is a group homomorphism.

□

Theorem 9.14. In the setting of the previous proposition, we have a long exact sequence of cohomology:

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

Proof. Exercise. □

9.2 Hilbert 90

Theorem 9.15 (Dedekind)**.** Let F be a field and G a group. Every finite set $\{\chi_1, ..., \chi_n\} \subset \mathrm{Hom}(G, F^*)$ is linearly independent over F.

Proof. Omitted, not hard.

□

Theorem 9.16 (Hilbert 90)**.** Let L be a finite Galois extension of a field K and $G = \mathrm{Gal}(L/K)$. Then $H^1(G, L^*) = 0$.

Proof. Let $f \in \mathrm{CH}(G, L^*)$. We want to show that there exists a $\gamma \in L^*$ such that $f(g) = \frac{g\gamma}{\gamma}$ for all $g \in G$. For all $g, h \in G$ we have $f(gh) = f(g)gf(h)$ since f is a crossed homomorphism. The maps $\chi_g : L^* \to L^*, l \mapsto gl$ are homomorphisms of groups, so according to Dedekinds theorem they are linearly independent. Since all the $f(g)$ are non-zero, the map

$$L^* \to L, l \mapsto \sum_{g \in G} f(g)\chi_g(l)$$

is non-zero. So there exists an $\alpha \in L$ such that

$$\beta := \sum_{g \in G} f(g)\chi(\alpha) \neq 0$$

Then for all $g \in G$ we get

$$g\beta = \sum_{h \in G} gf(h)g(h\alpha) = \sum_{h \in G} f(g)^{-1}f(gh)(gh)\alpha$$

$$= f(g)^{-1} \sum_{h \in G} f(gh)(gh)\alpha = f(g)^{-1} \sum_{h \in G} f(h)h\alpha = f(g)^{-1}\beta$$

We find $f(g) = \frac{\beta}{g\beta}$, so $\gamma := \beta^{-1}$ gives that f is principal.

□

Theorem 9.17. If G has order m, then for every G-module M we have

$$mH^1(G, M) = 0$$

Proof. Omitted, roughly three pages to prove.

□

9.3 Inflation & Restriction

Definition 9.18 (Restriction map)**.** Let $H \subset G$ a subgroup and M a G-module. The map

$$\mathrm{CH}(G, M) \to \mathrm{CH}(H, M), f \mapsto f|_H$$

is a morphism of groups which maps $\mathrm{PCH}(G, M)$ into $\mathrm{PCH}(H, M)$. This yields a map

$$\mathrm{Res} : H^1(G, M) \to H^1(H, M), [f] \mapsto [f|_H]$$

Proposition 9.19. Let $H \triangleleft G$ be a normal subgroup and M a G-module. Then M^H is naturally a G/H-module.

Proof. The action of G/H on M^H will be defined by $gHm := gm$. We need to show this is well-defined, so suppose $g_1H = g_2H$, then $g_2^{-1}g_1 \in H$, so $g_2^{-1}g_1m = m$. Hence we have $g_1m = g_2m$ for all $m \in M^H$. So this action is well-defined. □

Definition 9.20 (Inflation map)**.** Let $H \triangleleft G$ a normal subgroup and M a G-module. Then the composition

$$G \xrightarrow{\pi} G/H \xrightarrow{f} M^H \xrightarrow{i} H$$

yields the inflation morphism

$$\mathrm{Inf} : H^1(G/H, M^H) \to H^1(G, M), [f] \mapsto [i \circ f \circ \pi]$$

Here π is the quotient map and i the inclusion.

Theorem 9.21 (Inflation-Restriction exact sequence)**.** The sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)$$

is exact.

Proof. See homework. □

9.4 Galois Cohomology

Definition 9.22 (Perfect fields)**.** A field k is called perfect if every algebraic extension is separable.

We fix a perfect field K and an algebraic closure $\overline{K}$ of K. We let $G := \mathrm{Gal}(\overline{K}/K)$.

Definition 9.23 (Krull topology)**.** We call a subset $U \subset G$ open if and only if for every $u \in U$ there exists a subgroup $H \subset G$ such that $uH \subset U$ and $[\overline{K}^H : K] < \infty$. The topology defined by these opens is called the Krull topology.

Proposition 9.24. A subgroup $H \subset G$ is open if and only if $[\overline{K}^H : K]$ is finite.

Proof. If H is a subgroup of G for which $[\overline{K}^H : K]$ is finite, then we have $uH \subset H$ for all $u \in H$, so H is open. So suppose H is an open subgroup of G. Then for all $h \in H$ there is an H' satisfying the conditions of the definition. In particular there exists a subgroup H' such that $H' \subset H$, so $\overline{K}^H \subset \overline{K}^{H'}$. We find $[\overline{K}^H : K] \leq [\overline{K}^{H'} : K] < \infty$.

□

Proposition 9.25. Every open subgroup of G is closed.

Proof. Every open subgroup of G is the complement of the union of non-trivial cosets. Suppose H is an open subgroup, and gH is a non-trivial coset. Then for any $u \in gH$ we have that $u = gh$ for some $h \in H$, so $uH = ghH = gH \subset gH$. So since H is open, we obtain that gH is also open. So $G \backslash H$ is open, and thus every open subgroup of G is closed.

□

Definition 9.26 (Krull topology 2)**.** We can embed G in the product

$$\prod_{\substack{K \subset L \subset \overline{K} \\ [L:K] < \infty}} \mathrm{Gal}(L/K)$$

By giving $\mathrm{Gal}(L/K)$ the discrete topology and G the subset topology of this product, we also obtain the Krull topology on G. Since $\mathrm{Gal}(L/K)$ are all finite, they are compact, the product is compact according to Tychonov.

Proposition 9.27. The two definitions of the Krull topology are equivalent.

Proof. Exercise.

□

Corollary 9.28. The Krull topology turns G into a compact topological space.

Proof. Exercise.

□

Theorem 9.29 (Galois correspondence)**.** There is an inclusion reversing bijection

$$\{\text{closed subgroups } H \subset G\} \to \{K \subset L \subset \overline{K}\}$$

$$H \mapsto \overline{K}^H$$

The inverse is given by $L \mapsto \mathrm{Gal}(L/K)$. Open subgroups are corresponding to finite extensions of K.

Proof. Omitted. □

Proposition 9.30. Every closed subgroup is an intersection of open subgroups.

Proof. Exercise. □

Definition 9.31 (Discrete modules)**.** A G-module M is called discrete if the map

$$G \times M \to M, (g, m) \mapsto gm$$

is continuous when M is equipped with the discrete topology.

Notation 9.32. Let M be a discrete G-module. We write $\mathrm{CH}(G, M)$ for the set of *continuous* crossed homomorphisms $G \to M$ and $\mathrm{PCH}(G, M)$ for the set of continuous crossed homomorphisms.

Proposition 9.33. A crossed homomorphism $f : G \to M$ is continuous if and only if there exists an open normal subgroup $N \triangleleft G$ such that f is the inflation of a crossed homomorphism $G/N \to M^N$.

Proof. Homework exercise.

□

Proposition 9.34. Every principal crossed homomorphism is continuous.

Proof. Exercise.

□

Definition 9.35 (Galois Cohomology)**.** We define the cohomology groups

$$H^0(G, M) = M^G$$

$$H^1(G, M) := \frac{\mathrm{CH}(G, M)}{\mathrm{PCH}(G, M)}$$

This definition looks identical to the one we had before, but note that the crossed homomorphisms here have to be continuous.

Proposition 9.36. We can obtain $H^1(G, M)$ by taking the direct limit over open normal subgroups of G:

$$H^1(G, M) = \lim_H H^1(G/H, M^H)$$

So $H^1(G, M)$ is torsion.

Proof. Homework exercise.

□

Corollary 9.37.

$$H^1(G, \overline{K}^*) = \lim_{L/K \text{finite inside} \overline{K}} H^1(\mathrm{Gal}(L/K), L^*) = 0$$

Proof. Exercise.

□

Definition 9.38. For L a field an $n \geq 1$ we write

$$\mu_n(L) := \{\zeta \in L^* : \zeta^n = 1\}$$

Let k be a perfect field, then we get a short exact sequence

$$1 \to \mu_n(\overline{k}) \to \overline{k}^* \xrightarrow{x \mapsto x^n} \overline{k}^* \to 1$$

This yields a long exact sequence in cohomology:

$$1 \to \mu_n(k) \to k^* \xrightarrow{x \mapsto x^n} k^* \to H^1(G, \mu_n(\overline{k})) \to H^1(G, \overline{k}^*) = 0$$

The map $x \mapsto x^n$ in the long sequence is no longer surjective. The kernel of the map $k^* \to H^1(G, \mu_n(\overline{k}))$ contains precisely the $x \in k^*$ for which $X^n - x$ has a root in k. Since this map is surjective, we get the following proposition.

Proposition 9.39.

$$H^1(G, \mu_n(\overline{k})) \cong k^*/(k^*)^n$$

9.5 Change of base field

Notation 9.40. For the coming part we write

$$H^i(K, E) := H^i(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$$

for E an elliptic curve over the field K.

Let E be an elliptic curve over $\mathbb{Q}$, $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$ and $\overline{\mathbb{Q}_p}$ an algebraic closure of $\mathbb{Q}_p$. The canonical embedding $\mathbb{Q} \to \mathbb{Q}_p$ can be extended to a non-unique embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$. This induces a restriction map

$$\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

This map is even continuous. By composing various maps we get a map

$$H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_p, E)$$

which is independent of the choice of the embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$.

10 Proof of weak Mordell-Weil Theorem

Theorem 10.1 (Weak Mordell-Weil Theorem)**.** For $n \geq 1$ and E an elliptic curve over $\mathbb{Q}$, the quotient $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite.

We will spend the remainder of this chapter on proving this theorem. First let E be an elliptic curve over a perfect field k and let $\overline{k}$ be an algebraic closure. For $n \geq 1$ we can define functors $[n] : E \to E$, by setting

$$[n](L) : E(L) \to E(L), p \mapsto np$$

The kernel of $[n](L)$ is exactly $E(L)[n]$. Earlier we have proven for $n \in \{2, 3\}$ that

$$E(\overline{k})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

if $n \in k^*$, otherwise $E(\overline{k})[n] \cong \mathbb{Z}/n\mathbb{Z}$ or $E(\overline{k})[n] = 0$. The statement actually holds for any $n \in k^*$, however we certainly won't need more than what we have proven.

Theorem 10.2. The map $[n](\overline{k}) : E(\overline{k}) \to E(\overline{k})$ is surjective.

Proof. Many ways to prove, all use some non-trivial ingredient. Ours will be algebraic geometry. Ignore this proof if it doesn't make sense.

First, $ker[n]$ is finite and $E(\bar{K})$ is infinite, so $[n]$ is non-constant. The curve E is projective hence proper, hence $[n]$ is proper, so the image of $[n]$ is closed. The curve E is connected, so the image of $[n]$ is connected. Hence the image of $[n]$ is a closed, connected subscheme and is not finite, so it must be the whole of E. □

This theorem yields a short exact sequence of G-modules, where $G - \mathrm{Gal}(\overline{k}/k)$.

$$0 \to E(\overline{k})[n] \to E(\overline{k}) \xrightarrow{[n]} E(\overline{k}) \to 0$$

This then gives a long exact sequence in cohomology.

$$0 \to E(k)[n] \to E(k) \xrightarrow{[n]} E(k) \to H^1(k, E(\overline{k})[n]) \to H^1(k, E) \xrightarrow{[n]} H^1(k, E)$$

From this we then derive a short exact sequence

$$0 \to E(k)/nE(k) \to H^1(k, E[n]) \to H^1(k, E)[n] \to 0$$

We get such sequences for $\mathbb{Q}$ and $\mathbb{Q}_p$ for any p, so we get the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \longrightarrow & H^1(\mathbb{Q}_p, E[n]) & \longrightarrow & H^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0 \end{array}$$

Lemma 10.3. The previous diagram commutes.

Proof. Exercise in unravelling the definitions. □

Notation 10.4. Write $\mathbb{R} := \mathbb{Q}_\infty$, then define

$$\Omega_{\mathbb{Q}} := \{2, 3, \ldots\} \cup \{\infty\}$$

The commutative diagram above exists for every $p \in \Omega_{\mathbb{Q}}$. So we can define the following groups.

Definition 10.5 (Selmer Groups)**.** The n^{th} Selmer group is defined by

$$S^{(n)}(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E[n]) \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)\right)$$

The commutative diagram we saw earlier gives us that $S^{(n)}(E/\mathbb{Q})$ will contain the image of $E(\mathbb{Q})/nE(\mathbb{Q})$. We will later show that the Selmer groups are finite, proving the Weak Mordell-Weil theorem.

Definition 10.6 (Tate-Shafarevich groups)**.** The Tate-Shafarevich group is defined to be

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)\right)$$

Lemma 10.7. For every pair of morphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

in an abelian category we have a canonical long exact sequence

$$0 \to \ker(\alpha) \to \ker(\beta \circ \alpha) \xrightarrow{\alpha} \ker(\beta) \to \operatorname{coker}(\alpha) \xrightarrow{\beta} \operatorname{coker}(\beta \circ \alpha) \to \operatorname{coker}(\beta) \to 0$$

Proof. Exercise.

□

Corollary 10.8. There is a short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0$$

Proof. Apply the previous lemma to the sequence

$$H^1(\mathbb{Q}, E[n]) \to H^1(\mathbb{Q}, E)[n] \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)[n]$$

□

10.1 Extensions of $\mathbb{Q}_p$

Sadly this is all a bit sketchey, for reasons of time.

Let p be a fixed prime number, and K a finite field extension of $\mathbb{Q}_p$.

Definition 10.9 (Integral closure)**.** The integral closure of $\mathbb{Z}_p$ in K is the ring

$$\mathcal{O}_K := \{x \in K : \exists f \in \mathbb{Z}_p[X] : f(x) = 0\}$$

We call $\mathcal{O}_K$ the ring of integers of K, so $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$.

Fact 10.10. The ring $\mathcal{O}_K$ is a discrete valuation ring.

We write $\nu : K \to \mathbb{Z}$ for the normalised valuation and π for a uniformiser.

In general the composite map $\mathbb{Q}_p \hookrightarrow K \xrightarrow{\nu} \mathbb{Z}$ is not the normalised valuation on $\mathbb{Q}_p$.

Theorem 10.11. For $K/\mathbb{Q}_p$ there exists a unique $e \in \mathbb{Z}_{\geq 1}$ such that

$$\begin{array}{ccc} K & \xrightarrow{\nu} & \mathbb{Z} \\ \uparrow & & \uparrow{\scriptstyle \cdot e} \\ \mathbb{Q}_p & \xrightarrow[\mathrm{ord}_p]{} & \mathbb{Z} \end{array}$$

commutes.

Definition 10.12 (Ramification index)**.** The e of theorem 10.11 is called the ramification index of K over $\mathbb{Q}_p$. If $e = 1$, we say K is unramified over $\mathbb{Q}_p$.

Fact 10.13. The ring of integers $\mathcal{O}_K$ satisfies Hensel's lemma.

Proposition 10.14. Let $f \in \mathbb{F}_p[t]$ be irreducible and let

$$k := \mathbb{F}_p[t]/f$$

Choose a lift $\tilde{f}$ of f to $\mathbb{Z}_p$, i.e. $\tilde{f} \in \mathbb{Z}_p[t]$ getting mapped to f under the identification $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Let

$$K := \mathbb{Q}_p[t]/\tilde{f}$$

Then the residue field of $\mathcal{O}_K$ is canonically isomorphic to k.

Proof. Omitted.

□

10.2 Elliptic curves over extensions of $\mathbb{Q}_p$

Let $K/\mathbb{Q}_p$ be an unramified extension. Then p is a uniformiser in K, since it is one in $\mathbb{Q}_p$. Let E/K be an EC and assume p is a good prime. We define filtrations as in 7.2 and 7.4. By the same proof as we used for 7.1 we find

$$E(K)/E^1(K) \cong \overline{E}(k)$$

where k is the residue field of K and by the proof of 7.5 we find

$$E^n(K)/E^{n+1}(K) \cong k$$

for $n \geq 1$. The same proof as 7.6 yields that if $p \nmid m$, then

$$[m] : E^1(K) \to E^1(K), p \mapsto mp$$

is a bijection.

Lemma 10.15. Let E/K be an elliptic curve with good reduction and m and integer such that $p \nmid m$. Let $Q \in E(K)$, then the following are equivalent:

1. There exists a $\widetilde{Q} \in E(K)$ such that $m\widetilde{Q} = Q$.
2. There exists a $Q_0 \in \overline{E}(k)$ such that $mQ_0 = \mathrm{red}(Q)$.

Proof. The map $\mathrm{red} : E(K) \to \overline{E}(k)$ is a group homomorphism, so 1 implies 2. Suppose there exists a Q_0 as in 2. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \xrightarrow{\mathrm{red}} & \overline{E}(k) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \\ 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \xrightarrow{\mathrm{red}} & \overline{E}(k) & \longrightarrow & 0 \end{array}$$

By definition of E^1, the rows are exact, and the diagram commutes too. The map $E^1(K) \to E^1(K)$ is an isomorphism. We choose a $P \in E(K)$ with $\mathrm{red}(P) = Q_0$, then we have $\mathrm{red}(Q - mP) = 0$. By exactness there exists an $R \in E^1(K)$ such that $Q - mP = R$. So there exists an $R' \in E^1(K)$ such that $mR' = R$, so $Q - mP = mR'$. We find $Q = m(R' + P)$.

□

Corollary 10.16. Let $E/\mathbb{Q}_p$ be an EC of good reduction and let n be such that $p \nmid n$. Let $Q \in E(\mathbb{Q}_p)$, then there exists a finite unramified extension K of $\mathbb{Q}_p$ such that $Q \in n \cdot E(K)$.

Proof. Since $[n] : \overline{E}(\overline{\mathbb{F}_p}) \to \overline{E}(\overline{\mathbb{F}_p})$ is surjective there is an $R \in \overline{E}(\overline{\mathbb{F}_p})$ with $nR = \mathrm{red}(Q)$. Because R is defined by finitely many coëfficiënts, namely 3, there exists a finite extension k of $\mathbb{F}_p$ such that $R \in \overline{E}(k)$. Write $k = \mathbb{F}_p[t]/f$ for some polynomial f, then by proposition 10.14 there is an unramified finite extension K of $\mathbb{Q}_p$ such that k is the residue field of $\mathcal{O}_K$. So we have the following commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\text{red}} & \overline{E}(k) \\ \uparrow & & \uparrow \\ E(\mathbb{Q}_p) & \xrightarrow{\text{red}} & \overline{E}(\mathbb{F}_p) \end{array}$$

So there is an $R \in \overline{E}(k)$ with $nR = \text{red}(Q)$, so by lemma 10.15 there is an $\widetilde{R} \in E(K)$ such that $n\widetilde{R} = Q$. So $Q \in n \cdot E(K)$.

□

Now we get back to the Selmer groups, to show that these are finite. We have

$$S^{(n)}(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[n]) \to H^1(\mathbb{Q}_p, E[n]) \to H^1(K, E[n])$$

where the arrows are all induced by the change of base field. The first inclusion follows from the definition of the Selmer groups. We can now formulate the following proposition.

Proposition 10.17. Let E be an elliptic curve over $\mathbb{Q}$, given by $Y^2 = X^3 + aX + b$ for $a, b \in \mathbb{Z}$. Let Δ_E be the discriminant of E and T the set of primes dividing $2n\Delta_E$. Then for any $\gamma \in S^{(n)}(E/\mathbb{Q})$ and $p \in \Omega_{\mathbb{Q}} \backslash T$ there exists a finite unramified extension K of $\mathbb{Q}_p$ such that γ maps to zero in $H^1(K, E[n])$.

Proof. Let γ_p be the image of γ in $H^1(\mathbb{Q}_p, E[n])$. Recall the diagram we used to define $S^{(n)}(E/\mathbb{Q})$, then there follows that there exists a $Q \in E(\mathbb{Q}_p)$ which gets mapped to γ_p, by exactness. Since $p \nmid 2\Delta$, we have that E has good reduction at p. Since $p \nmid n$, we can use the previous corollary to obtain a finite unramified extension K of $\mathbb{Q}_p$ such that $Q \in nE(K)$. So Q we get that γ_p maps to 0 in $H^1(K, E[n])$ and thus γ does too.

□

We finally move on to prove that the Selmer groups are finite. We make a few assumptions to get rid of some technical difficulties. Firstly, we will assume $E(\mathbb{Q})[2] = E(\overline{\mathbb{Q}})[2]$. So if E is given by $Y^2 = f(X)$, we will have that f has three roots in $\mathbb{Q}$. We will only show $S^{(2)}(E/\mathbb{Q})$ is finite, since this is enough for our purposes. It will show $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

We let $E/\mathbb{Q}$ be an elliptic curve with coefficients in $\mathbb{Z}$ and $\#E(\mathbb{Q})[2] = 4$. We have

$$E(\overline{\mathbb{Q}})[2] = E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2 \cong (\mu_2)^2$$

as $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Here μ_2 is as in definition 9.38 So we get

$$H^1(\mathbb{Q}, E[2]) = H^1(\mathbb{Q}, (\mu_2)^2)$$

Lemma 10.18. We have $H^1(\mathbb{Q}, (\mu_2)^2) = (H^1(\mathbb{Q}, \mu_2))^2$.

Proof. Exercise. □

So as in 9.39 we get $H^1(\mathbb{Q}, (\mu_2)^2) \cong (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$. Since $S^{(2)}(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[2])$, we can embed $S^{(2)}(E/\mathbb{Q})$ in $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$.

Definition 10.19. Let T be the set of primes dividing $2\Delta_E$. We let

$$\widetilde{S}^2(E/\mathbb{Q}) := \left\{ \left((-1)^{\varepsilon(\infty)} \prod_p p^{\varepsilon(p)}, (-1)^{\varepsilon'(\infty)} \prod_p p^{\varepsilon'(p)} \right) \right\} \subset (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$$

Here $\varepsilon(p), \varepsilon'(p) \in \{0,1\}$ and $\varepsilon(p) = \varepsilon'(p) = 0$ if $p \notin T$.

Proposition 10.20. The set $\widetilde{S}^2(E/\mathbb{Q})$ is finite.

Proof. Since T is finite, the are only finitely many combinations of $\varepsilon, \varepsilon'$.

□

The following theorem finally proves the weak Mordell-Weill theorem.

Theorem 10.21. We have $S^{(2)}(E/\mathbb{Q}) \subset \widetilde{S}^2(E/\mathbb{Q})$.

Proof. Let $\gamma \in S^{(2)}(E/\mathbb{Q})$ correspond to

$$\left((-1)^{\varepsilon(\infty)} \prod_p p^{\varepsilon(p)}, (-1)^{\varepsilon'(\infty)} \prod_p p^{\varepsilon'(p)} \right) \in (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$$

with $\varepsilon(p), \varepsilon'(p) \in \{0,1\}$. Let $p_0 \notin T$ be a prime. We want to show $\varepsilon(p_0) = \varepsilon'(p_0) = 0$. By proposition 10.17 there exists a finite unramified extension K of $\mathbb{Q}_{p_0}$ such that γ gets mapped to 0 in $H^1(K, E[2])$. Since $E(\overline{K})[2] = E(\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$, we get $H^1(K, E[2]) \cong \left(K^*/(K^*)^2\right)^2$, and the canonical map $H^1(\mathbb{Q}, E[2]) \to H^1(K, E[2])$ is given by

$$(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2 \to \left(K^*/(K^*)^2\right)^2, q(\mathbb{Q}^*)^2 \mapsto q(K^*)^2$$

We get a commutative diagram

$$\begin{array}{ccccc} H^1(\mathbb{Q}, E[2]) & \xrightarrow{\sim} & \left(\mathbb{Q}^*/(\mathbb{Q}^*)^2\right)^2 & \xrightarrow{(\mathrm{ord}_{p_0})^2} & (\mathbb{Z}/2\mathbb{Z})^2 \\ \downarrow & & \downarrow & & \downarrow \\ H^1(K, E[2]) & \xrightarrow{\sim} & \left(K^*/(K^*)^2\right)^2 & \xrightarrow{(\mathrm{ord}_{p_0})^2} & (\mathbb{Z}/2\mathbb{Z})^2 \end{array}$$

Where the map $(\mathbb{Z}/2\mathbb{Z})^2 \to (\mathbb{Z}/2\mathbb{Z})^2$ is the identity (commutativity follows because K is unramified over $\mathbb{Q}_p$). Now we have $(\mathrm{ord}_{p_0})^2(\gamma) = (\varepsilon(p_0), \varepsilon'(p_0))$, so since γ is mapped to 0 in $H^1(K, E[2])$, by commutativity we obtain $\varepsilon(p_0) = \varepsilon'(p_0) = 0$.

□

Since $S^{(2)}(E/\mathbb{Q})$ is finite, we obtain that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. This concludes the proof of the weak Mordell Weil theorem.

11 Heights

For the last part of the proof of the Mordell Weil theorem, we will use heights.

Definition 11.1 (Primitive representative)**.** Let $n \geq 0$ and let $p \in \mathbb{P}^n(\mathbb{Q})$. A primitive representative for p is an element $(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}$ with $p = (a_0 : \ldots : a_n)$ and $\gcd(a_0, \ldots, a_n) = 1$.

Definition 11.2 (Height)**.** The height of $p \in \mathbb{P}^n(\mathbb{Q})$ is

$$H(p) := \max_{0 \leq i \leq n} |a_i|$$

for a primitive representative $(a_0, ..., a_n)$. The logarithmic height of p is $h(p) = \log(H(p))$.

Note the height is independent of the choice of representative.

Remark 11.3. For any B the sets $\{p \in \mathbb{P}^n(\mathbb{Q}) : H(p) \leq B\}$ and $\{p \in \mathbb{P}^n(\mathbb{Q}) : h(p) \leq B\}$ are finite.

For $x \in \mathbb{Q}$ we can write $h(x) = h(x : 1)$. So for $p = (x_p : y_p : 1) \in E(\mathbb{Q})$ for an elliptic curve E over $\mathbb{Q}$, we can define $h(p) = h(x_p)$. We will show that $h(2p)$ is approximately $4h(p)$, so that h is an approximate quadratic form.

Definition 11.4 (Resultants)**.** Let $f, g \in \mathbb{Z}[X]$, with $f = f_m X^m + \cdots + f_0$ and $g = g_n X^n + \cdots + g_0$, with $f_m, g_n \neq 0$. The resultant of f and g is given by

$$\mathrm{Res}(f,g) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & f_m & \cdots & f_1 & f_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 \\ g_n & g_{n-1} & \cdots & g_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_n & \cdots & g_1 & g_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

This is the determinant of an $m + n$ by $m + n$ matrix.

It is true (but not obvious) that

$$\mathrm{Res}(f,g) = f_m^n g_n^m \prod_{\substack{p,q \in \overline{\mathbb{Q}} \\ f(p)=g(q)=0}} (p - q).$$

We will not use this.

Definition 11.5 (Reciprocal polynomial)**.** We write $\mathrm{recip}(f) = f_0 X^m + \cdots + f_m$.

Proposition 11.6.

1. If $m = n$, then $\mathrm{Res}(\mathrm{recip}(f), \mathrm{recip}(g)) = \pm \mathrm{Res}(f, g)$.
2. There exist $a, b \in \mathbb{Z}[X]$ such that $\deg(a) < n, \deg(b) < m$ satisfying

$$\mathrm{Res}(f,g) = af + bg$$

3. If $\mathrm{Res}(f,g)=0$, then $\deg(\gcd(f,g))>0$.

Proof. 1. The resultant of the reciprocal polynomials is obtained by switching some rows and columns. 'Hence' $\mathrm{Res}(\mathrm{recip}(f),\mathrm{recip}(g)) = \pm\,\mathrm{Res}(f,g)$.

2. Let $C_1,...,C_{m+n}$ be the columns of the matrix we used to define the resultant, say M. Then

$$C := \begin{pmatrix} x^{m-1}f \\ x^{m-2}f \\ \vdots \\ f \\ x^{n-1}g \\ \vdots \\ g \end{pmatrix} = x^{m+n-1}c_1 + \cdots + c_{m+n}$$

We find that $\mathrm{Res}(f,g)$ equals the degree 0 part of $\det(C_1,\ldots,C_{m+n-1},C)$. So the result follows from writing out this determinant.

3. If $\mathrm{Res}(f,g)=0$, we write $\mathrm{Res}(f,g) = fa+gb = 0$ using the second part of the proposition. Let $\alpha\in\overline{\mathbb{Q}}$ be such that $f(\alpha)=0$, then $g(\alpha)=0$ or $b(\alpha)=0$. If $g(\alpha)=0$, then $(X-\alpha)$ is a degree 1 divisor of f and g, so we're done. If $b(\alpha)=0$, we repeat the process, since $0 = a\frac{f}{X-\alpha} + \frac{b}{X-\alpha}g$. So we can choose a root $\beta\neq\alpha$ of f, and since $\deg(b)<\deg(f)$, this will eventually give us a common root of f and g.

□

Proposition 11.7. Let $F,G\in\mathbb{Q}[X,Y]$ be homogeneous polynomials of the same degree $m>0$, such that $V_F^P\cap V_G^P=\varnothing$. We let

$$\varphi:\mathbb{P}^1(\mathbb{Q})\to\mathbb{P}^1(\mathbb{Q}),(x:y)\mapsto(F(x,y):G(x,y))$$

This is a well-defined map. There exists some $B\in\mathbb{R}$ such that for all $p\in\mathbb{P}^1(\mathbb{Q})$ we have

$$|h(\varphi(p)) - mh(p)| \le B$$

Proof. We can assume without loss of generality that the coefficients of F,G are in $\mathbb{Z}$. Let $p\in\mathbb{P}^1(\mathbb{Q})$ with primitive representative (a,b). Then for all $c\in\mathbb{Z}$ we have

$$|ca^ib^{m-i}| \le |c|\max(|a|^m,|b|^m)$$

We set $c := (m+1)\max\{\text{coëfficiënts of } F,G\}$. Then we get

$$|F(a,b)|,|G(a,b)| \le c\max(|a|,|b|)^m$$

We then have

$$H(\varphi(p)) \le \max(|F(a,b)|,|G(a,b)|) \le c\max(|a|,|b|)^m = cH(p)^m$$

So $h(\varphi(p)) \le mh(p)+\log(c)$.

The other inequality is harder. Since $V_F^P \cap V_G^P = \varnothing$, we have that $F\left(\frac{X}{Y},1\right), G\left(\frac{X}{Y},1\right) \in \mathbb{Z}\left[\frac{X}{Y}\right]$ have no common root in $\overline{\mathbb{Q}}$, so $R := \operatorname{Res}\left(F\left(\frac{X}{Y},1\right), G\left(\frac{X}{Y},1\right)\right) \neq 0$, following from the previous proposition. Let $u, v \in \mathbb{Z}\left[\frac{X}{Y}\right]$ of degree at most $m-1$, such that $R = u\left(\frac{X}{Y}\right) F\left(\frac{X}{Y},1\right) + v\left(\frac{X}{Y}\right) G\left(\frac{X}{Y},1\right)$. Note that $Y^m F\left(\frac{X}{Y},1\right) = F(X,Y)$, since F is homogeneous of degree m, and the same holds for G. Since $\deg(u) \leq m-1$, we get $U(X,Y) := Y^{m-1} u\left(\frac{X}{Y}\right) \in \mathbb{Z}[X,Y]$, and the same holds for $V(X,Y) := Y^{m-1} v\left(\frac{X}{Y}\right)$. So we get

$$Y^{2m-1} R = U(X,Y)F(X,Y) + V(X,Y)G(X,Y)$$

Swapping the roles of X, Y we find that there exist U', V' such that

$$X^{2m-1} R = U'(X,Y)F(X,Y) + V'(X,Y)G(X,Y)$$

Substituting $X = a, Y = b$, this gives

$$U(a,b)F(a,b) + V(a,b)G(a,b) = b^{2m-1} R$$

$$U'(a,b)F(a,b) + V'(a,b)G(a,b) = a^{2m-1} R$$

So since $\gcd(a,b) = 1$ we have that $\gcd(F(a,b), G(a,b))$ divides R. From the argument we used earlier in the proof we also get there exists a c' such that

$$|U(a,b)|, |U'(a,b)|, |V(a,b)|, |V'(a,b)| \leq c' \max(|a|,|b|)^{m-1}$$

So we obtain

$$2\max(|a|,|b|)^{m-1} \max(|F(a,b)|, |G(a,b)|) \geq R|a|^{2m-1}$$

$$2\max(|a|,|b|)^{m-1} \max(|F(a,b)|, |G(a,b)|) \geq R|b|^{2m-1}$$

Using that $\gcd(F(a,b), G(a,b))$ divides R, we get

$$H(\varphi(p)) \geq \frac{1}{R} \max(|F(a,b)|, |G(a,b)|) \geq \frac{1}{2c'} H(p)^m$$

Taking logarithms yields the inequality.

□

Definition 11.8 (Veronese map)**.** Define

$$\mathcal{V} : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{Q})$$

$$((a:b),(c:d)) \mapsto (ac : ad + bc : bd)$$

It is an exercise to show this is well-defined.

Proposition 11.9. For all $p, q \in \mathbb{P}^1(\mathbb{Q})$ we have

$$\frac{1}{2} \leq \frac{H(\mathcal{V}(p,q))}{H(p)H(q)} \leq 2$$

Proof. Homework exercise.

□

11.1 Heights on Elliptic curves

Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve over $\mathbb{Q}$. For $p \in E(\mathbb{Q})$ we let $H(p) := H(x(p) : z(p))$ if $p \neq (0 : 1 : 0)$, and $H(0 : 1 : 0) = 1$. Again, $h(p) = \log(H(p))$.

Lemma 11.10. For all $b \in \mathbb{R}$, we have that $\{p \in E(\mathbb{Q}) : h(p) \leq B\}$ is finite.

Proof. Easy exercise.

□

Proposition 11.11. There exists a constant A such that for all $p \in E(\mathbb{Q})$ we have

$$|h(2p) - 4h(p)| \leq A$$

Proof. We assume $p \neq (0 : 1 : 0)$, in that case the expression $|h(2p) - 4h(p)|$ is simple. So write $p = (x : y : z), 2p = (x_2 : y_2 : z_2)$. Let $F, G \in \mathbb{Q}[X, Z]$ be homogeneous of degree 4 such that

$$F(X, 1) = (3X^2 + a)^2 - 8X(X^3 + aX + b)$$

$$G(X, 1) = 4(X^3 + aX + b)$$

Then we obtain from the formulae of the group law that $\frac{x_2}{z_2} = \frac{F(x,z)}{G(x,z)}$. Smoothness of E yields that $V_F^P \cap V_G^P = \varnothing$, so proposition 11.7 gives us the result.

□

Proposition 11.12. There exists at most one function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ satisfying

1. $\hat{h}(p) - h(p)$ is bounded on $E(\mathbb{Q})$.
2. $\hat{h}(2p) = 4\hat{h}(p)$

Proof. Suppose that for all $p \in E(\mathbb{Q})$ we have $|\hat{h}(p) - h(p)| \leq B$. Then given a $p \in E(\mathbb{Q})$ we have

$$|\hat{h}(2^n p) - h(2^n p)| \leq B$$

so

$$\left|\hat{h}(p) - \frac{h(2^n p)}{4^n}\right| \leq \frac{B}{4^n}$$

Hence we get that $\frac{h(2^n p)}{4^n}$ converges to $\hat{h}(p)$ as $n \to \infty$, so since there can be at most one limit, we obtain that $\hat{h}$ is unique.

□

Lemma 11.13. There exists a constant A such that for all $p \in E(\mathbb{Q})$ and for all $N \geq M \geq 0$ we have

$$\left|\frac{h(2^N p)}{4^N} - \frac{h(2^M p)}{4^M}\right| \leq \frac{A}{3 \cdot 4^M}$$

Proof. From 11.11 we have that there exists an A such that for all $p \in E(\mathbb{Q})$ we have

$$|h(2p) - 4h(p)| < A$$

Let $N \geq M \geq 0$ and $p \in E(\mathbb{Q})$, then we have

$$\left| \frac{h(2^N p)}{4^N} - \frac{h(2^M p)}{4^M} \right| \leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} |h(2^{n+1}p) - 4h(2^n p)| \leq \sum_{n=M}^{N-1} \frac{A}{4^{n+1}}$$

Since

$$\sum_{n=M}^{N-1} \frac{1}{4^{n+1}} \leq 4^{-M} \sum_{n=0}^{\infty} \frac{1}{4^n} = \frac{1}{3 \cdot 4^M}$$

we obtain that

$$\left| \frac{h(2^N p)}{4^N} - \frac{h(2^M p)}{4^M} \right| \leq \frac{A}{3 \cdot 4^M}$$

which is what we wanted to show.

□

Corollary 11.14. For all $p \in E(\mathbb{Q})$, the sequence $\left(\frac{h(2^n p)}{4^n} \right)_n$ is Cauchy in $\mathbb{R}$.

Definition 11.15 (Canonical/Néron-Tate height)**.** Given $p \in E(\mathbb{Q})$, we define

$$\hat{h}(p) := \lim_{n \to \infty} \frac{h(2^n p)}{4^n}$$

This is called the canonical or Néron-Tate height of p.

Theorem 11.16. The function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ satisfies:

1. $\hat{h}(p) - h(p)$ is bounded on $E(\mathbb{Q})$;
2. $\hat{h}(2p) = 4\hat{h}(p)$;
3. For all $c \in \mathbb{R}$ the set $\{p \in E(\mathbb{Q}) : \hat{h}(p) \leq c\}$ is finite;
4. For all $p \in E(\mathbb{Q})$, we have that $\hat{h}(p) \geq 0$ and $\hat{h}(p) = 0$ if and only if $p \in E(\mathbb{Q})_{\text{tors}}$.

Proof.

1. Apply lemma 11.13 to $M = 0$, then we obtain

   $$\left| \frac{h(2^N p)}{4^N} - h(p) \right| \leq \frac{A}{3}$$

   for all $N \geq 0$. By letting $N \to \infty$, we get the result.

2. Straightforward:

   $$\hat{h}(2p) = \lim_{n \to \infty} \frac{h(2^{n+1}p)}{4^n} = 4 \lim_{n \to \infty} \frac{h(2^{n+1}p)}{4^{n+1}} = 4\hat{h}(p)$$

3. Use part 1 of this theorem, then let B be such that $|\hat{h}(p) - h(p)| \leq B$ for all p. Then

$$\{p \in E(\mathbb{Q}) : \hat{h}(p) \leq c\} = \{p \in E(\mathbb{Q}) : h(p) \leq B + c\}$$

is finite.

4. Since $H(p) \geq 1$, we have that $h(p) \geq 0$ and thus $\hat{h}(p) \geq 0$. If $p \in E(\mathbb{Q})_{\text{tors}}$ then $S := \{2^n p : n \geq 0\}$ is finite, so $\hat{h}$ is bounded on S. Let D be such that $\hat{h}(p) \leq D$ for all $p \in S$, then

$$\hat{h}(p) = \frac{\hat{h}(2^n p)}{4^n} \leq \frac{D}{4^n}$$

for all n. So $\hat{h}(p) = 0$. If $p \notin E(\mathbb{Q})_{\text{tors}}$, suppose $\hat{h}(p) = 0$. Then for all $n \geq 0$ we have $\hat{h}(2^n p) = 0$. So $\hat{h}$ vanishes on the infinite set $\{2^n p : n \geq 0\}$, which is contradicting part 3 of this theorem.

□

Definition 11.17 (Quadratic form)**.** Let M be an abelian group and k a field. Let $2 \in k^*$. A function $f : M \to k$ is called a quadratic form if for all $x, y \in M$

1. $f(2x) = 4f(x)$
2. $B(x, y) := f(x + y) - f(x) - f(y)$ is bi-additive.

Note that $B(x, y) = B(y, x)$ and $f(x) = \frac{1}{2}B(x, x)$ since 2 is a unit.

Proposition 11.18. Let M, k as in the previous definition. Suppose $f : M \to k$ satisfies the parallelogram law

$$f(x + y) + f(x - y) = 2f(x) + 2f(y)$$

for all $x, y \in M$. Then f is a quadratic form.

Proof. Plugging in $x = y = 0$ yields $f(0) = 0$. Plugging in $x = y$ then gives us $f(2x) = 4f(x)$. We just need to show that $B(x, y)$ is bi-additive. By symmetry, we just need to show $B(x + y, z) = B(x, z) + B(y, z)$, i.e.

$$f(x+y+z)-f(x+y)-f(z)-f(x+z)+f(x)+f(z)-f(y+z)+f(y)+f(z) = 0$$

From the parallelogram law we can derive the following four identities:

$$f(x + y + z) + f(x + y - z) - 2f(x + y) - 2f(z) = 0$$

$$f(x + y - z) + f(x - y + z) - 2f(x) - 2f(y - z) = 0$$

$$f(x + y + z) + f(x - y + z) - 2f(x + z) - 2f(y) = 0$$

$$2f(y + z) + 2f(y - z) - 4f(y) - 4f(z) = 0$$

The alternating sum of these four identities gives the required identity.

□

Lemma 11.19. There exists a $C \in \mathbb{R}$ such that for all $p_1, p_2 \in E(\mathbb{Q})$ we have

$$H(p_1 + p_2)H(p_1 - p_2) \leq CH(p_1)^2 H(p_2)^2$$

Proof. Let $p_3 = p_1 + p_2$ and $p_4 = p_1 - p_2$, write $p_i = (x_i : y_i : z_i)$ for primitive representatives (x_i, y_i, z_i). The addition formula yields

$$(x_3x_4 : x_3z_4 + x_4z_3 : z_3z_4) = (w_0 : w_1 : w_2)$$

where

$$w_0 = x_1^2x_2^2 - 2ax_1x_2z_1z_2 - 4b(x_1z_1z_2^2 + x_2z_1^2z_2) + a^2z_1^2z_2^2$$
$$w_1 = 2(x_1x_2 + az_1z_2)(x_1z_2 + x_2z_1) + 4bz_1^4z_2^4$$
$$w_2 = (x_2z_1 - x_1z_2)^2$$

From the inequality 11.9 we obtain $H(w_0 : w_1 : w_2) \geq \frac{1}{2}H(p_1 + p_2)H(p_3 - p_4)$. From a similiar argument as we gave while proving 11.7, there exists a $C > 0$ such that

$$H(w_0 : w_1 : w_2) \leq CH(p_1)^2 H(p_2)^2$$

Combining the two inequalities yields the result.

□

Lemma 11.20. The canonical height $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is a quadratic form.

Proof. Because of proposition 11.18, we can show that $\hat{h}$ satisfies the parallelogram law to get the result. By taking logarithms in the previous lemma, we get for all P, Q

$$h(P + Q) + h(P - Q) \leq 2h(P) + 2h(Q) + B$$

for some constant B. By replacing P by 2^nP, Q by 2^nQ, dividing by 4^n and then take the limit $n \to \infty$, we obtain

$$\hat{h}(P + Q) + \hat{h}(P - Q) \leq 2\hat{h}(P) + 2\hat{h}(Q)$$

Now let $P' = P + Q$ and $Q' = P - Q$, then

$$2\hat{h}(P') + 2\hat{h}(Q') \leq 4\hat{h}(P) + 4\hat{h}(Q) = \hat{h}(2P) + \hat{h}(2Q) = \hat{h}(P' + Q') + \hat{h}(P' - Q')$$

Hence $\hat{h}$ satisfies the parallelogram law, so it is a quadratic form.

□

12 Proof of the Mordell Weil Theorem

Theorem 12.1 (Mordell-Weil)**.** Let E over $\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group.

Proof. Let $p_1, ..., p_n$ be coset representations for $E(\mathbb{Q})/2E(\mathbb{Q})$ (finite by Weak Mordell-Weil). Let $C := \max_i \hat{h}(p_i)$. Set

$$S := \{p \in E(\mathbb{Q}) : \hat{h}(p) \leq C\}$$

This is a finite set. Claim: S generates $E(\mathbb{Q})$. Suppose that $E(\mathbb{Q})\backslash\langle S\rangle \neq \varnothing$. Then let $Q \in E(\mathbb{Q})\backslash\langle S\rangle$ be of minimal height. There exist $1 \leq i \leq n$ and $R \in E(\mathbb{Q})$ such that

$$Q = p_i + 2R$$

since $E(\mathbb{Q})$ is a union of cosets. Then $R \notin \langle S\rangle$, since otherwise we would have $Q \in \langle S\rangle$. Hence we have $\hat{h}(R) \geq \hat{h}(Q)$. We obtain

$$2C \geq 2\hat{h}(p_i) = \hat{h}(p_i + Q) + \hat{h}(p_i - Q) - 2\hat{h}(Q) = \hat{h}(p_i + Q) + \hat{h}(-2R) - 2\hat{h}(Q)$$

$$= \hat{h}(p_i + Q) + 4\hat{h}(R) - 2\hat{h}(Q) \geq 0 + 4\hat{h}(R) - 2\hat{h}(Q) \geq 2\hat{h}(Q)$$

The last inequality follows because Q is of minmimal height. This is a contradiction, since $Q \notin S$. Hence we find that S generates $E(\mathbb{Q})$.

□

13 Factoring integers using elliptic curves

Not typeset yet.