Elliptic Curves
Part III Lent 2016-2017

Alexandre Daoud

May 27, 2017

Contents

1 Preliminary Definitions

1.1 Fermat's Method of Descent

Definition 1.1.1. Let $\triangle$ be a right angled triangle with legs of length a and b and hypoteneuse c with $a, b, c \in \mathbb{R}$. We say that $\triangle$ is **rational** if $a, b, c \in \mathbb{Q}$. Furthermore, we say that $\triangle$ is **primitive** if $a, b, c \in \mathbb{Z}$ are all coprime.

Lemma 1.1.2. *Every primitive triangle with legs a and b and hypoteneuse c satisfies $a = u^2 - v^2, b = 2uv$ and $c = u^2 + v^2$ for some strictly positive $u, v \in \mathbb{Z}$ such that $u > v$.*

Proof. Without loss of generality, we may assume that a is odd, b is even and c is odd. By Pythagoras' Theorem we have that

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2}\frac{c-a}{2}$$

The right hand side is a product of coprime positive integers so by the Fundamental Theorem of Arithmetic, we must have that $(c+a)/2$ and $(c-a)/2$ are squares of integers, say u^2 and v^2 respectively. Rewriting a, b and c in terms of u and v then yields the result. □

Definition 1.1.3. Let $D \in \mathbb{Q}_{>0}$. We say that D is **congruent** if there exists a rational triangle whose area is D.

Lemma 1.1.4. *Let $D \in \mathbb{Q}_{>0}$. Then D is congruent if and only if $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$ and y non-zero.*

Proof. By Lemma 1.1.2, there exists non-zero $u, v, w \in \mathbb{Q}$ such that D is congruent if and only if $Dw^2 = uv(u^2 - v^2)$. Taking $x = u/v$ and $y = w/v^2$ gives the desired result. □

Theorem 1.1.5. *1 is not a congruent number.*

Proof. By Lemma 1.1.4, it suffices to show that $w^2 = uv(u+v)(u-v)$ has no solutions for $u, v, w \in \mathbb{Z}$ with w non-zero. Without loss of generality, we may assume that u and v are coprime and $u, w > 0$. If $v < 0$ then we may replace (u, v, w) by $(-v, u, w)$. Futhermore, if u and v are of the same parity then we can replace (u, v, w) by $((u+v)/2, (u-v)/2, w/2)$.

Hence we can assume that $u, v, u+v$ and $u-v$ are positive coprime integers whose product is a square. By the Fundamental Theorem of Arithmetic, we have that $u = a^2, v = b^2, u+v = c^2$ and $u-v = d^2$ for $a, b, c, d \in \mathbb{Z}_{>0}$. Since u and v have different parity, both c and d are odd. We then have that

$$\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = u = a^2$$

This is a primitive triangle whose area is $(b/2)^2$. Let $w_1 = b/2$. By Lemma 1.1.2 we have that $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$ for some $u_1, v_1 \in \mathbb{Z}$. Hence (u_1, v_1, w) is a new solution to the original equation. However, $4w_1^2 = b^2 = v$ which divides w^2 so we have that $w_1 \leq w/2$. Continuing in this way we can construct a infinite decreasing sequence of natural numbers $\{ w_i \}$ which is a contradiction. □

Definition 1.1.6. Let K be a field such that $\operatorname{char} K \neq 2$ with algebraic closure $\overline{K}$.

1. We define an **elliptic curve** E/K to be the projective closure of a plane affine curve of the form

$$Y^2 = f(X)$$

   where $f \in K[X]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.

2. Given a field extension L/K, we define the **L-points** of E to be the set

$$E(L) = \{ (x, y) \in L^2 \mid y^2 = f(x) \} \cup \{ 0 \}$$

1.2 Remarks on Algebraic Curves

Throughout this section, we assume that K is an algebraically closed field such that $\operatorname{char} K \neq 2$.

Definition 1.2.1. Let K be a field and

$$C = \{ f(x, y) = 0 \} \subseteq \mathbb{A}_K^2$$

be a plane algebraic curve for some $f(X) \in K[X, Y]$. We say that C is **rational** if there exist some rational functions $\phi(t), \psi(t) \in K(t)$ such that the mapping

$$\begin{aligned} g : \mathbb{A}_K^1 &\to \mathbb{A}_K^2 \\ t &\mapsto (\phi(t), \psi(t)) \end{aligned}$$

is injective on $\mathbb{A}_K^1 \backslash X$ where X is a finite set and $f(\phi(t), \psi(t)) \equiv 0$.

Example 1.2.2. Any non-singular plane curve or singular cubic is rational. Any smooth plane cubic is not rational.

Definition 1.2.3. Let K be a field and $C \subseteq \mathbb{P}_K^2$ a smooth projective curve. If P is a smooth point on C and T_P is the tangent space to C at P, we say that P is an **inflection point** if the multiplicity of the intersection of C and T_P at P is greater than or equal to 3.

Proposition 1.2.4. *Let K be a field and $C \subseteq \mathbb{P}_K^2$ a smooth projective curve of degree d. If $\operatorname{char} K \nmid 2(d-1)$ then P is an inflection point of C if and only if $H(P) = 0$ where*

$$H(X_1, X_2, X_3) = \det \left(\frac{\partial^2 F}{\partial X_i \partial X_j} \right)$$

is the Hessian.

Proof. Proof Ommitted. □

Lemma 1.2.5. *Let K be a field and $C \subseteq \mathbb{P}_K^2$ a smooth projective cubic curve. Then*

1. *C has a point of inflection.*

2. *If $P \in C$ is a point of inflection then we may change coordinates such that C is given by an equation of the form*

$$Y^2Z = X(X - Z)(X - \lambda Z)$$

where $\lambda \neq 0, 1$ and $P = [0 : 1 : 0]$.

Proof.

Part 1: Recall that any two plane curves in $\mathbb{P}^2_K$ intersect. In particular, $C \cap \{ H = 0 \} \neq \varnothing$ so we must have that C contains an inflection point.

Part 2: Suppose that

$$C = \{ F(X_1, X_2, X_3) = 0 \} \subseteq \mathbb{P}^2_K$$

for some polynomial $F \in K[X_1, X_2, X_3]$. We shall change coordinates so that $P = [0 : 1 : 0]$ and $T_P C = \{ Z = 0 \}$. Since P is a point of inflection and F is a cubic polynomial, we must have that $F(t, 1, 0) = kt^3$ for some non-zero $k \in K$. Hence F cannot have terms containing the monomials X^2Y, XY^2 and Y^3. We thus see that

$$F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$$

Note that the coefficient of Y^2Z must be non-zero since otherwise P would be a singular point of C. Furthermore, the coefficient of X^3 must also be non-zero since if it were not, this would imply that $\{ Z = 0 \} \subseteq C$ which would contradict the smoothness of C. Since we can rescale X, Y and Z, C is defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Since $\operatorname{char} K \neq 2$, we can complete the square on the left hand side and so, without loss of generality, $a_1 = a_3 = 0$. We can write the right hand side of this equation as $Z^3 f(X/Z)$ for some cubic polynomial f. Since C is smooth, f has distinct roots. Without loss of generality, we may assume that they are $0, 1$ and $\lambda \neq 0, 1$ as desired.

□

Definition 1.2.6. Let K be a field and $C \subseteq \mathbb{P}^2_K$ a smooth projective curve of degree d. We define the **genus** of C to be

$$g(C) = \frac{(d-1)(d-2)}{2}$$

Proposition 1.2.7. *Let K be a field and $C \subseteq \mathbb{P}^2_K$ a smooth projective cruve. Then*

1. *C is rational if and only if $g(C) = 0$.*

2. *C is an elliptic curve if and only if $g(C) = 1$.*

Proof. Proof Ommitted. □

Definition 1.2.8. Let K be a field and $C = \{ f = 0 \}$ for some polynomial $f \in K[X_1, \ldots, X_n]$. Suppose that $K(C) = \operatorname{Frac} K[X_1, \ldots, X_n]/(f)$ is the function field of C and $P \in C$ is a smooth point. We define a discrete valuation on $K(C)$ called the **order of vanishing**

$$\operatorname{ord}_P : K(C) \to \mathbb{Z} \cup \infty$$

which takes a rational function $g \in K(C)$ and sends it to its order of vanishing at P. Note that ord_P can be negative if P is a pole of g.

Definition 1.2.9. Let K be a field and $C = \{ f = 0 \}$ an algebraic curve for some polynomial $f \in K[X_1, \ldots, X_n]$ and $P \in C$ a smooth point. We say that $t \in K(C)$ is a **uniformiser** if $\mathrm{ord}_P(t) = 1$.

Example 1.2.10. Let $C = \{ g = 0 \} \subseteq \mathbb{A}^2_K$ for some irreducible $g \in K[X, Y]$. Write $g = g_0 + g_1(X, Y) + g_2(X, Y) + \ldots$ where g_i is homogeneous of degree i. Suppose that $P = (0, 0) \in C$ is a smooth point so that $g_0 = 0$. Assume that $g_1(X, Y) = \alpha x + \beta y$ where α and β are not both zero. Then $\gamma x + \delta y$ is a uniformiser if and only if $\alpha\delta - \beta\gamma = 0$.

Example 1.2.11. Consider the curve $\{ y^2 = x(x-1)(x-\lambda) \} \subseteq \mathbb{A}^2_K$ where $\lambda \neq 0, 1$. This curve has projective closure $\{ Y^2Z = X(X-Z)(X-\lambda Z) \} \subseteq \mathbb{P}^2_K$. Let $P = [0 : 1 : 0]$. We aim to calculate $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$. Set $w = Z/Y$ and $t = X/Y$. Then the equation becomes

$$w = t(t - w)(t - \lambda w)$$

In these coordinates, P is the point $(0, 0)$ so we have that $1 = \mathrm{ord}_P(t) = \mathrm{ord}_P(t - w) = \mathrm{ord}_P(t - \lambda w)$ whence $\mathrm{ord}_P(w) = 3$. Hence, $\mathrm{ord}_P(x) = \mathrm{ord}_P(X/Z) = \mathrm{ord}_P(t/w) = 1 - 3 = -2$ and $\mathrm{ord}_P(y) = \mathrm{ord}_P(Y/Z) = \mathrm{ord}_P(1/w) = -3$.

Definition 1.2.12. Let K be a field and $C \subseteq \mathbb{P}^2_K$ a smooth projective curve. We define a **divisor** on C to be a formal sum of points of C

$$D = \sum_{P \in C} n_P P$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. We write $\mathrm{Div}(C)$ for the set of all divisors of C and we define the **degree** of D to be $\deg(D) = \sum_{P \in C} n_P$. Moreover, we say that D is **effective** and write $D \geq 0$ if $n_P \geq 0$ for all $P \in C$. Finally, if $f \in K(C)$ is a rational function, we define the **divisor over f** to be $\mathrm{Div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$.

Definition 1.2.13. Let K be a field and $C \subseteq \mathbb{P}^2_K$ be a smooth projective curve. Given $D \in \mathrm{Div}(C)$, we define the **Riemann-Roch** space of D to be

$$\mathcal{L}(D) = \{ f \in K(C)^\times \mid \mathrm{Div}(f) + D \text{ is effective } \} \cup \{ 0 \}$$

Remark. The Riemann-Roch space of a divisor D is the K-vector space of rational functions on C with poles no worse than specified by D.

Theorem 1.2.14 (Riemann-Roch for genus 1)**.** *Let K be a field, $C \subseteq \mathbb{P}^2_K$ a curve of genus 1 and D a divisor on C. Then*

$$\dim \mathcal{L}(D) = \begin{cases} \deg(D) & \text{if } \deg(D) > 0 \\ 0 \text{ or } 1 & \text{if } \deg(D) = 0 \\ 0 & \text{if } \deg(d) < 0 \end{cases}$$

Proof. Proof Omitted. □

Example 1.2.15. With notation as in Example 1.2.11, we have that $\mathcal{L}(2P) = \langle 1, x \rangle$ and $\mathcal{L}(3P) = \langle 1, x, y \rangle$.

Definition 1.2.16. Let K be a field and $V_1, V_2 \subseteq \mathbb{P}^2_K$ be projective varieties. A **rational map** between V_1 and V_2 is a (perhaps not defined everywhere) function $\phi : V_1 \to V_2$ equipped with rational functions $f_1, \cdots, f_n \in K(V_1)$ such that for all $P \in V$ where the f_i are defined we have

$$\phi(P) = [f_1(P) : \cdots : f_n(P)]$$

Definition 1.2.17. Let K be a field, $V_1, V_2 \subseteq \mathbb{P}^2_K$ projective varieties and $\phi : V_1 \to V_2$ a rational map. Given $P \in V_1$, we say that ϕ is **regular** at P if there exists a rational function $g \in K(V_1)$ such that

1. gf_i is defined at P for all i
2. $gf_i(P) \neq 0$ for some i

If ϕ is regular at all points $P \in V_1$, we say that ϕ is a **morphism** of varieties.

Remark. Recall that a projective curve is an a projective variety of dimension 1. In particular, we can define morphisms of projective curves.

Definition 1.2.18. Let $C_1, C_2 \subseteq \mathbb{P}^2_K$ be smooth projective curves and $\phi : C_1 \to C_2$ a non-constant morphism. Let

$$\begin{aligned} \phi^* : K(C_2) &\to K(C_1) \\ f &\mapsto f \circ \phi \end{aligned}$$

Then we define the **degree** of ϕ to be $\deg(\phi) = [K(C_1) : \phi^* K(C_2)]$. Furthermore, we say that ϕ is **separable** if $K(C_1)/\phi^* K(C_2)$ is a separable extension.

Definition 1.2.19. Let $C_1, C_2 \subseteq \mathbb{P}^2_K$ be smooth projective curves and $\phi : C_1 \to C_2$ a non-constant morphism. Let $P \in C_1$ and t be a uniformiser for $\phi(P)$. We define the **ramification index** of ϕ at P, denoted $e_\phi(P)$ to be the quantity

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t)$$

We say that ϕ is **unramified** at P if $e_\phi(P) = 1$ and that ϕ is unramified if it is unramified at every point $P \in C_1$.

Proposition 1.2.20. *Let $C_1, C_2 \subseteq \mathbb{P}^2_K$ be smooth projective curves and $\phi : C_1 \to C_2$ a non-constant morphism. Then for all $Q \in C_2$ we have*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

Furthermore, if ϕ is separable then $e_\phi(P) = 1$ for all but finitely many $P \in C_1$. In particular

1. *ϕ is surjective*
2. *$|\phi^{-1}(Q)| \leq \deg(\phi)$ for all but finitely many $Q \in C_2$.*

Remark. Let C_1 be an algebraic curve and $\phi : C \to \mathbb{P}^n_K$ a rational map given by $P \mapsto [f_0(P) : \cdots : f_n(P)]$ for some $f_0, \ldots, f_n \in K(C)$ not all zero. Then if C is smooth, ϕ is a morphism.

Proposition 1.2.21. *Let $C_1, C_2 \subseteq \mathbb{P}^2_K$ be smooth projective curves and $\phi : C_1 \to C_2$ a non-constant morphism. If $\deg(\phi) = 1$ then ϕ is an isomorphism.*

Proof. Proof Omitted. □

2 Elliptic Curves

2.1 Weierstrass Equations

Throughout this section, K will be a perfect field.

Definition 2.1.1. Let K be a field. An elliptic curve E over K is a smooth projective curve of genus 1, defined over K, with a specified K-rational point $\mathcal{O}_E$.

Example 2.1.2. Consider the algebraic set $\{ X^3 + pY^3 + p^2Z^3 = 0 \} \subseteq \mathbb{P}^2$ for some prime number p. Then this is not an elliptic curve over $\mathbb{Q}$ since it has no non-zero $\mathbb{Q}$-rational points. This can be shown by infinite descent. Without loss of generality, we may suppose that (a, b, c) is a non-zero integral solution to the equation. Then $a^3 + pb^3 + p^2c^3 = 0$ whence $p|a^3$ and so $p|a$. From this we have that $a = pk$ for some integer k. Then $p^3k^3 + pb^3 + p^2c^3 = 0$. It then follows that $p^2|pb^3$ whence $p|b$ and so also $b = pm$ for some integer m and we have $p^3k^3 + p^4m^3 + p^2c^3 = 0$. We again note that $p^3|p^2c^3$ and so $p|c$ and $c = pn$ for some integer n. Substituting this into the equation for the final time gives $p^3k^3 + p^4m^3 + p^5n^3 = 0$. Simplifying this, we see that (k, m, n) is a solution to the equation. But $\max\{ k, m, n \} \leq 1/p \max\{ a, b, c \}$ and so this is a smaller solution. We can repeat this process to construct an infinite sequence of tuples of integers which is clearly a contradiction and so there are no non-zero solutions.

Remark. If $D \in \mathrm{Div}(E)$ is defined over K (i.e is fixed by the action of $\mathrm{Gal}(\bar{K}/K)$) then $\mathcal{L}(D)$ has a basis in $K(E)$ and not just $\overline{K}(E)$.

Lemma 2.1.3. *Let $E \subseteq \mathbb{A}^2_K$ be a singular curve given by a Weierstrass equation*

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

for some $a_1, \ldots, a_6 \in K$. Then E is birational to $\mathbb{P}^1_K$[1].

Proof. After a linear change of coordinates, we may assume that E has a singular point at $(0, 0)$. Upon examining the partial derivatives, we see that the curve is given by the equation

$$y^2 + a_1xy = x^3 + a_2x^2$$

Then the rational map

$$\begin{aligned} E &\to \mathbb{P}^1_K \\ (x, y) &\mapsto [x : y] \end{aligned}$$

is birational since it has inverse $\mathbb{P}^1_K \to E$ given by

$$[1 : t] \to (t^2 - a_1t - a_2, t^3 - a_1t^2 - a_2t)$$

Indeed, setting $t = y/x$ and dividing through by x^2 yields $x = t^2 + a_1t - a_2$. □

Theorem 2.1.4. *Let K be a field and E/K an elliptic curve. Then E is K-isomorphic to a smooth curve in Weierstrass form via an isomorphism sending $\mathcal{O}_E$ to $[0 : 1 : 0]$.*

[1] By birational, we mean there exist rational maps in both directions which are in some sense mutually inverse.

Proof. Consider the Riemann-Roch spaces $\mathcal{L}(2\mathcal{O}_E)$ and $\mathcal{L}(3\mathcal{O}_E)$. It is easy to see that $\mathcal{L}(2\mathcal{O}_E) \subseteq \mathcal{L}(3\mathcal{O}_E)$. By the Riemann-Roch Theorem, we have that $\dim \mathcal{L}(2\mathcal{O}_E) = 2$ and $\dim \mathcal{L}(3\mathcal{O}_E) = 3$. Hence we can choose functions $x, y \in K(E)^\times$ such that $\{ 1, x \}$ is a basis for $\mathcal{L}(2\mathcal{O}_E)$ and $\{ 1, x, y \}$ is a basis for $\mathcal{L}(3\mathcal{O}_E)$. Observe that x has a pole of order 2 and y has a pole of order 3. Note that the Riemann-Roch Theorem implies that $\mathcal{L}(6\mathcal{O}_E)$ has dimension 6. However, this vector space contains the 7 elements $1, x, y, x^2, xy, x^3$ and y^2. We must therefore have a dependence relation between these 7 functions. Now, these elements without x^3 and y^2 form a basis for $\mathcal{L}(6\mathcal{O}_E)$ since they all have different order of pole at $\mathcal{O}_E$. Thus the coefficients of x^3 and y^2 are non-zero in the dependence relation. Rescaling these functions, we have

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

for some $a_i \in K$. Consider the rational map

$$\begin{aligned} \phi : E &\to E' \\ P &\mapsto [x(P) : y(P) : 1] \end{aligned}$$

Then this is a morphism of curves since E is smooth. Furthermore, $\phi(\mathcal{O}_E) = [0 : 1 : 0]$ since y has a pole of higher order at $\mathcal{O}_E$ than x. We wish to show that ϕ is an isomorphism. By Proposition 1.2.21, it suffices to show that ϕ has degree 1 and that E' is smooth. Define

$$\begin{aligned} \phi^* : K(E') &\to K(E) \\ f &\mapsto f \circ \phi \end{aligned}$$

We need to show that $[K(E) : \phi^*K(E')] = 1$. Let $Q \in E'$ be the point at infinity. By Proposition 1.2.20 we have that

$$\deg(x) = \sum_{P \in x^{-1}(Q)} e_x(P)$$

$x^{-1}(Q)$ is simply the set of all poles of x in E. But x only has one pole, namely at $\mathcal{O}_E$ and so

$$\deg(x) = e_x(\mathcal{O}_E) = \mathrm{ord}_{\mathcal{O}_E}(x^*t)$$

where t is a uniformiser for Q in $K(E')$. But a uniformiser for Q is simply given by $1/x$ and so pulling this back along x^* we have

$$\deg(x) = \mathrm{ord}_{\mathcal{O}_E}\left(\frac{1}{x}\right) = 2$$

We thus have $[K(E) : K(x)] = \deg(x) = 2$. Similarly, $[K(E) : K(y)] = \deg(y) = 3$. By the Tower Law, we have that $[K(E) : K(x, y)]$ divides both 2 and 3 whence $\deg(\phi) = [K(E) : K(x, y)] = 1$. It remains to show that E' is smooth.

Suppose, for a contradiction, that E' is singular. By Lemma 2.1.3 is birational to $\mathbb{P}^1_K$. Since $\mathbb{P}^1_K$ is smooth and E is birational to E', there exists a degree 1 map between E and $\mathbb{P}^1_K$ which must be an isomorphism. But this is a contradiction as E has genus 1 and $\mathbb{P}^1_K$ has genus 0. Hence E' must be smooth whence ϕ is an isomorphism of curves. □

Remark. A curve given by a Weierstrass equation is an elliptic curve if and only if it is smooth and $\triangle \neq 0$ where $\triangle$ is the discriminant of the Weierstrass equation.

Note that if $\mathrm{char}\, K \neq 2, 3$ then we can write the Weierstrass equation in the form $y^2 = x^3 + ax + b$ which has discriminant $\triangle = -16(4a^3 + 27b^2)$.

Proposition 2.1.5. *Let K be a field and E, E' elliptic curves over K in Weierstrass form. Then E is isomorphic to E' if and only if the Weierstrass equations are related by a substitution of the form*

$$x = u^2x' + r$$
$$y = u^3y' + u^2sx' + t$$

where $u, r, s, t \in K$ and x, y are the coordinates of E and x', y' are the coordinates of E'.

Proof. Let $\mathcal{O}_E$ be the distinguished point of E. Then $\langle 1, x\rangle = \mathcal{L}(2\mathcal{O}_E) = \langle 1, x'\rangle$ and so $x = \lambda x' + r$ for some $\lambda, r \in K$ with λ non-zero. Similarly, $\langle 1, x, y\rangle = \mathcal{L}(3\mathcal{O}_E) = \langle 1, x', y'\rangle$. Then $y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K$ such that $\mu \neq 0$. Since both E and E' sastify Weierstrass equations, it follows that $\lambda^3 = \mu^2$. Hence $\lambda = u^2$ and $\mu = u^3$ for some $u \in K^\times$. Setting $s = \sigma/u^2$ gives the desired result. □

Corollary 2.1.6. *Suppose that K is a field such that* $\operatorname{char} K \neq 2, 3$ *and suppose we are given two elliptic curves over K in Weierstrass form*

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

Then E and E' are isomorphic over K if and only if $a' = u^4c$ and $b' = u^6b$ for some $u \in K^\times$.

Definition 2.1.7. Let K be a field such that $\operatorname{char} K \neq 2, 3$ and E/K an elliptic curve with Weierstrass form $y^2 = x^3 + ax + b$. We define the **j-invariant** of E to be

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

Theorem 2.1.8. *Let K be a field such that* $\operatorname{char} K \neq 2, 3$ *and suppose we are given two elliptic curves over K in Weierstrass form*

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

If $E \cong E'$ then $j(E) = j(E')$. Furthermore, if K is algebraically closed then the converse also holds.

Proof. We only prove the forward direction. Suppose that $E \cong E'$. By Corollary 2.1.6, there exists $u \in K^\times$ such that $a' = u^4a$ and $b' = u^6b$. Then

$$j(E') = -1728\frac{(4a)^3}{-16(4a'^3 + 27b'^2)} = -1728\frac{u^{12}(4a)^3}{-16u^{12}(4a^3 + 27b^2)} = j(E)$$

□

2.2 The Group Law

Let $E \subseteq \mathbb{P}^2_K$ be an elliptic curve. By Bezout's Theorem, a line intersects the curve in at most three points. The degenerate case arises when such a line is tangent to the curve.

Definition 2.2.1. Let $E \subseteq \mathbb{P}^2_K$ be an elliptic curve and $P, Q \in E$. Let S be the third point of intersection in E of the line through P and Q. Let R be the third point of intersection in E of the line through $\mathcal{O}_E$ and S. We define the **composition** of P and Q to be $P \oplus Q = R$.

Theorem 2.2.2. *Let $E \subseteq \mathbb{P}^2_K$ be an elliptic curve. Then $(E, \oplus)$ is an abelian group.*

Proof. $\oplus$ is clearly a commutative binary operation on E. It is easy to see that $\mathcal{O}_E$ is the identity. Indeed, let $P \in E$ and let L be the line through $\mathcal{O}_E$ and P. Let Q be the third point of intersection of E and L. Then the line through $\mathcal{O}_E$ and Q is L and so $\mathcal{O}_E \oplus P = P$. To see that E has inverses with respect to $\oplus$, let $P \in E$ and L the line through $\mathcal{O}_E$ and P. Let Q be the third point of intersection of L and E. We claim that Q is the inverse of P. In other words, we need to show that $P \oplus Q = \mathcal{O}_E$. We have

$$P \oplus Q = (P \oplus \mathcal{O}_E) \oplus Q = \mathcal{O}_E$$

We postpone the proof of associativity until we have proved some important results. □

Definition 2.2.3. Let K be a field and $C \subseteq \mathbb{P}^2_K$ a smooth projective curve. We say that $D_1, D_2 \in \mathrm{Div}(C)$ are **linearly equivalent** if there exists $f \in \overline{K}(E)^\times$ such that $\mathrm{Div}(f) = D_1 - D_2$. This defines an equivalence relation on $\mathrm{Div}(C)$ and we shall write $D_1 \sim D_2$ if D_1 and D_2 are linearly equivalent and denote the equivalence class by $[D_1]$.

Furthermore, we define the **Picard group** of E to be $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$. We shall also denote $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$ where Div^0 is the collection of degree 0 divisors of E.

Proposition 2.2.4. *Let $E \subseteq \mathbb{P}^2_K$ be an elliptic curve and consider the function*

$$\begin{aligned} \phi : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [(P) - (\mathcal{O}_E)] \end{aligned}$$

Then $\phi(P \oplus Q) = \phi(P) + \phi(Q)$ and ϕ is a bijection.

Proof. Let L be the line through P and Q and S the third point of intersection of L with E. Let M be the line through $\mathcal{O}_E$ and R and R the third point of intersection of M with E so that $P \oplus Q = R$. Then

$$\begin{aligned} \mathrm{Div}\,(L/M) &= (P) + (Q) + (S) - (\mathcal{O}_E) - (S) - (R) \\ &= (P) + (Q) - ((R) + (\mathcal{O}_E)) \end{aligned}$$

and so $(P) + (Q) \sim (R) + (\mathcal{O}_E)$. We therefore have that $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.

To prove injectivity, suppose that $\phi(P) = \phi(Q)$ and assume, for a contradiction, that $P \neq Q$. Then there exists $f \in K(E)^\times$ such that $\mathrm{Div}(f) = (P) - (Q)$. We thus get a rational map

$$\begin{aligned} f : E &\to \mathbb{P}^1_K \\ R &\mapsto [f(R) : 1] \end{aligned}$$

Observe that f has degree 1 since $f^{-1}([0:1]) = \{ P \}$ and so f is an isomorphism. This implies that $E \cong \mathbb{P}^1_K$ which is a contradiction.

To prove surjectivity, fix a $[D] \in \mathrm{Pic}^0(E)$. Then $D + (\mathcal{O}_E)$ has degree 1. By the Riemann-Roch Theorem, we have that $\mathcal{L}(D + (\mathcal{O}_E)) = 1$. We may thus choose $f \in K(E)^\times$ such that $\mathrm{Div}(f) + D + (\mathcal{O}_E) \geq 0$. Since f must be a basis for this Riemann-Roch space, we have that $\deg(\mathrm{Div}(f)) = 0$. It follows that $\mathrm{Div}(f) + D + (\mathcal{O}_E)$ has degree 1 whence $\mathrm{Div}(f) + D + (\mathcal{O}_E) = (P)$ for some $P \in E$. That is to say, $D \sim (P) - (\mathcal{O}_E)$ and so $\phi(P) = [D]$. □

Remark. This proves associativity of $\oplus$ as there exists a bijective structure preserving map $(E, \oplus) \to \mathrm{Pic}^0(E)$ and the latter is a group.

Remark. We can find an explicit formula for the group law as follows. Suppose we are given an elliptic curve E in Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and let $P_0 = (x_0, y_0) \in E$. We first calculate $-P_0$. Let L be the line through P_0 and $\mathcal{O}_E$. We need to find the third point of intersection of this line. The line L is given by $x - x_0 = 0$. Substituting this into the Weierstrasas equation gives a quadratic polynomial $F(x_0, y)$ yields a quadratic polynomial with roots y_0 and y_0' where $-P = (x_0, y_0')$. In other words, $F(x_0, y) = c(y - y_0)(y - y_0')$ for some $c \in K^\times$. Equating the coefficients of y^2 yields $c = 1$. Equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$.

We now derive a formula for the addition law. To this end, fix points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$ then this is the case where $P_1 = -P_2$. If not then the line L through P_1 and P_2 has an equation of the form $y = \lambda x + \nu$ where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2 \end{cases}$$

$$\nu = \begin{cases} \frac{y_1x_2}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2 \end{cases}$$

Substituting the equation for L into the Weierstrass equation, we have a cubic polynomial $F(x, \lambda x + \nu)$ with three roots x_1, x_2 and x_3 where $P_3 = (x_3, y_3)$ is the third point of intersection of L and E. It can be shown that for three colinear points P_1, P_2, P_3 we have $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}_E$. So to find $P_1 \oplus P_2$, it suffices to apply the negation formula to P_3. Comparing coefficients again, we find that $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$ which gives us the coordinates x_3 and y_3.

Corollary 2.2.5. *Let K be a field and E/K an elliptic curve. Then $E(K)$ is an abelian group.*

Proof. This follows from the fact that $E(K)$ is a subgroup of E. □

Definition 2.2.6. Let G be a group. We say that G is a **group variety** or **algebraic group** if G is an algebraic variety such that the group operation and inversion are morphisms of varieties.

Theorem 2.2.7. *Let K be a field and E/K an elliptic curve with Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then E is a group variety.*

Proof. The inversion map is clearly rational since it is given by

$$\begin{aligned} E &\to E \\ (x, y) &\mapsto (x, -y - a_1x - a_3) \end{aligned}$$

Since E is smooth, this map is a morphism.

To show that addition is a morphism, fix $P \neq \mathbb{O}_E$ and first consider the translation map

$$\begin{aligned} \tau_P : E &\to E \\ Q &\mapsto P \oplus Q \end{aligned}$$

This is clearly rational by the formulae in the remark and so is a morphism by smoothness of E. Now note that $\oplus$ is rational and defined everywhere except possibly at points of the

form $(P,P),(P,-P),(\mathcal{O}_E,P)$ and $(P,\mathcal{O}_E)$. To prove the theorem in these cases, let Q_1 and Q_2 be arbitrary points in E. Consider the mapping

$$\phi : E \times E \xrightarrow{\tau_{Q_1}\times\tau_{Q_2}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{Q_1}^{-1}} E \xrightarrow{\tau_{Q_2}^{-1}} E$$

Since the group law is associative and commutative, ϕ agrees everywhere with $\oplus$ whenever they are both defined. Since Q_1 and Q_2 are arbitrary points, we can always find rational maps $\phi_1,\ldots,\phi_n : E\times E \to E$ such that ϕ_1 is $\oplus$, for each $(P_1,P_2)\in E\times E$, some ϕ_i is defined at (P_1,P_2) and if ϕ_i and ϕ_j are both defined at (P_1,P_2) then $\phi_i(P_1,P_2)=\phi_j(P_1,P_2)$. It thus follows that addition is defined on all of $E\times E$ and is thus a morphism. □

2.3 Elliptic Curves Over Particular Fields

Let $\Lambda = \{\, aw_1 + bw_2 \mid a,b\in\mathbb{Z}\,\}$ where $\{\, w_1,w_2\,\}$ is a basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space. Then we have a one-to-one correspondence between meromorphic functions on the Riemann surface $\mathbb{C}/\Lambda$ and Λ-invariant meromorphic functions on $\mathbb{C}$. The function field of $\mathbb{C}/\Lambda$ is generated by $\gamma(z)$ and $\gamma'(z)$ where

$$\gamma(z) = \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)$$
$$\gamma'(z) = -2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}$$

These satisfy $\gamma'(z)^2 = 4\gamma(z)^3 - g_1\gamma(z) - g_3$ for some $g_i\in\mathbb{C}$ depending on Λ. One can show that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ as Riemann surfaces and as groups where E is the elliptic curve given by the Weierstrass equation $y^2 = 4x^3 - g_1x - g_2$.

Theorem 2.3.1 (Uniformisation Theorem)**.** *Every elliptic curve over* $\mathbb{C}$ *arises this way.*

Example 2.3.2. If $K=\mathbb{R}$ then

$$E(\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{R}/\mathbb{Z} & \text{if } \triangle > 0 \\ \mathbb{R}/\mathbb{Z} & \text{if } \triangle < 0 \end{cases}$$

Example 2.3.3. If $K=\mathbb{F}_q$ then $|E(\mathbb{F}_q)-(q+1)| \le 2\sqrt{q}$.

Example 2.3.4. If $[K:\mathbb{Q}_p]<\infty$ with ring of integers $\mathcal{O}_K$ then $E(K)$ has a finite index subgroup isomorphic to $\mathcal{O}_K$.

Example 2.3.5. If $[K:\mathbb{Q}]<\infty$ then $E(K)$ is a finitely generated abelian group (Mordell-Weil Theorem).

Remark. All these isomorphisms respect the relevant topologies.

2.4 Isogenies

Throughout this section, K will be a perfect field.

Definition 2.4.1. Let K be a field and E_1 and E_2 elliptic curves over K. By an **isogeny** between E_1 and E_2, we mean a nonconstant morphism $\phi : E_1 \to E_2$ such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. We say that E_1 and E_2 are **isogenous** if there exists an isogeny between them. Furthermore, we denote by $\mathrm{Hom}(E_1,E_2)$ the collection of all isogenies between E_1 and E_2 together with the zero isogeny.

Remark. $\mathrm{Hom}(E_1, E_2)$ is a group under pointwise addition. Furthermore, the composition of any two isogenies is again an isogeny and the tower law implies that the degree is multiplicative.

Definition 2.4.2. Let K be a field and E an elliptic curve over K. We define the **multiplication by n** isogeny to be

$$\begin{aligned}[n] : E &\to E \\ P &\mapsto P \oplus \cdots \oplus P\end{aligned}$$

where the image is an n-fold sum. Furthermore, we define $[-n]$ to be $[-1] \cdot [n]$

Definition 2.4.3. Let K be a field and E an elliptic curve over K. We define the **n-torsion** subgroup of E to be $E[n] = \ker([n] : E \to E)$.

Lemma 2.4.4. *Let K be a field such that $\operatorname{char} K \neq 2$ and E an elliptic curve over K. Suppose that E has the Weierstrass form $y^2 = f(x) = (x - l_1)(x - l_2)(x - l_3)$ for some $l_i \in \overline{K}$. Then $E[2] = \{ (0,0), (l_1, 0), (l_2, 0), (l_3, 0) \} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Proof. Let $\mathcal{O}_E \neq P \in E$ with $P = (x_P, y_P)$. Then the tangent line to E at P has the equation

$$2y_P(y - y_P) = f'(x_P)(x - x_P)$$

Then $P \in E[2]$ if and only if $[2]P = \mathcal{O}_E$ if and only if $T_P E = \{ x = x_P \}$ if and only if $y_P = 0$. □

Lemma 2.4.5. *Let K be a field such that $\operatorname{char} K \neq 2$ and E an elliptic curve over K. Let $0 \neq x \in \mathbb{Z}$. Then $[x] : E \to E$ is an isogeny.*

Proof. By Theorem 2.2.7, $[x]$ is a morphism. It thus suffices to show that $[x](\mathcal{O}_E) = \mathcal{O}_E$. Equivalently, we need to show that $[x](P) \neq \mathcal{O}_E$. First suppose that $x = 2$. Then Lemma 2.4.4 implies that $[2](P) \neq \mathcal{O}_E$. Now suppose that x is odd. Lemma 2.4.4 once again implies that there exists $\mathcal{O}_E \neq T \in E[2]$. Then $[x](T) = T \neq \mathcal{O}_E$. The lemma then follows upon appealing to the multiplicative property of $[x]$. □

Remark. If $\operatorname{char} K = 2$ then we can replace the previous two lemmas with ones involving $E[3]$.

Proposition 2.4.6. *Let K be a field and $\phi : E_1 \to E_2$ an isogeny of elliptic curves over K. Then*

$$\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$$

for all $P, Q \in E_1$.

Proof. (sketch) Observe that ϕ induces a group homomorphism

$$\begin{aligned}\phi_* : \mathrm{Pic}^0(E_1) &\to \mathrm{Pic}^0(E_2) \\ \left[\sum_{P \in E_1} n_p P\right] &\mapsto \left[\sum_{p \in E_1} n_p \phi(P)\right]\end{aligned}$$

We also have group isomorphisms

$$\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$$

and so we have a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle \kappa_1} & & \downarrow{\scriptstyle \kappa_2} \\ \mathrm{Pic}^0(E_1) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E_2) \end{array}$$

whence ϕ is a group homomorphism. □

Remark. If $K = \mathbb{C}$ then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ and $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $\deg[n] = n^2$. We shall show that the former claim holds if $\mathrm{char}\, K$ does not divide n and the latter holds for all K.

Example 2.4.7. Let K be a field such that $\mathrm{char}\, K \neq 2$ and E/K an elliptic curve. Suppose that E has the Weierstrass equation

$$E : y^2 = x(x^2 + ax + b)$$

with $a, b \in K$ and $b(a^2 - 4b) \neq 0$. Suppose $T = (0, 0) \in E(K)[2]$. Fix $P = (x, y) \in E$ and let $P' = P \oplus T = (x', y')$. Using the formulae for the group law, we have

$$\begin{aligned} x' &= \left(\frac{x}{y}\right)^2 - x - a = \frac{x^2 + ax + b}{x} - x - a = \frac{b}{x} \\ y' &= -\left(\frac{y}{x}\right) x' = -\frac{b}{x^2} \end{aligned}$$

Now let

$$\begin{aligned} \xi = x + x' + a = \frac{x^2 + ax + b}{x} = \left(\frac{y}{x}\right)^2 \\ \eta = y - y' = \frac{y}{x}\left(x - \frac{b}{x}\right) \end{aligned}$$

Then

$$\begin{aligned} \eta^2 &= \left(\frac{y}{x}\right)^2 \left[\left(x + \frac{b}{x}\right)^2 - 4b\right] \\ &= \xi((\xi - a)^2 - 4b) \\ &= \xi(\xi^2 - 2a + a^2 - 4b \end{aligned}$$

Now let $E' : y^2 = x(x^2 + a' + b')$ where $a' = -2a$ and $b' = a^2 - 4b$. Then there is an isogeny

$$\begin{aligned} \phi : E &\to E' \\ (x, y) &\mapsto (\xi, \eta) \end{aligned}$$

To verify this, we need to show that $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. But this is clear as $\mathcal{O}_E$ is a pole of η of higher order than that of ξ so the image of $\mathcal{O}_E$ is the point at infinity.

Lemma 2.4.8. *Let K be a field and $\phi : E_1 \to E_2$ an isogeny of elliptic curves over K. Then there exists a morphism $\xi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that the diagram*

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle x_1} & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1_K & \xrightarrow{\xi} & \mathbb{P}^1_K \end{array}$$

commutes where x_i is the x coordinate in the Weierstrass equation of E_i. Moreover, if $\xi(t) = r(t)/s(t) \in K(t)$ with r and s coprime then $\deg \phi = \deg \xi = \max\{\deg r, \deg s\}$.

Proof. Recall from previous results that $2 = \deg x_i = [K(E_i)/K(x_i)]$ since coordinate map x_i has a pole of order 2 at $\mathcal{O}_{E_i}$. In particular, this field extension is Galois with Galois group generated by $[-1]^*$ since the inversion map leaves the x coordinate fixed. By Proposition 2.4.6 we have that $\phi \circ [-1] = [-1] \circ \phi$. Hence if $f \in K(x_2)$ then

$$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$$

$\phi^* f$ is thus fixed by the action of $\mathrm{Gal}(K(E_1)/K(x_1))$ whence $\phi^* f \in K(x_1)$. This implies that $K(x_2)$ is a subfield of $K(x_1)$. Taking $f = x_2$ gives the mapping $\xi : \mathbb{P}^1_K \to \mathbb{P}^1_K$. The tower law then implies that $\deg \phi = \deg \xi$. Now consider the field embedding

$$\begin{aligned} K(x_2) &\hookrightarrow K(x_1) \\ x_2 &\mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)} \end{aligned}$$

for some coprime $r, s \in K[X]$. We claim that the minimal polynomial of x_1 over $K(x_2)$ is $f(X) = r(X) - x_2 s(X) \in K(x_2)[X]$. x_1 is clearly a root of $f(X)$ by construction so it suffices to show that $f(X)$ is irreducible over $K(x_2)[X]$. Note that $f(X)$ is irreducible over $K[x_2, X]$. Indeed, it is a polynomial of degree 1 in x_2 so if it were to factor, one of the factors must contain only X which would mean r and s have a common factor. Appealing to Gauss' Lemma, we see that $f(X)$ is irreducible over $K(x_2)[X]$. Furthermore,

$$\deg \xi = [K(x_1) : K(x_2)] = \deg f = \max\{\deg r, \deg s\}$$

□

Example 2.4.9. From the previous example we had

$$\xi(x) = \left(\frac{y}{x}\right)^2 = \frac{x^2 + ax + b}{x}.$$

Since $b \neq 0$, the numerator and denominator are coprime and so $\deg \phi = 2$. In this case, we say that ϕ is a 2-isogeny.

Lemma 2.4.10. *Let K be a field such that* $\mathrm{char}\, K \neq 2, 3$ *and E an elliptic curve over K. Then* $\deg[2] = 4$.

Proof. Without loss of generality, we can write $E : y^2 = f(x) = x^3 + ax + b$. Let $P = (x, y) \in E$. Then

$$\begin{aligned} x(2P) &= \left(\frac{3x^2 + a}{2y}\right)^2 - 2x \\ &= \frac{(3x^2 + a)^2 - 8xf(x)}{4f(x)} \\ &= \frac{f'(x)^2 - 8xf(x)}{4f(x)} \end{aligned}$$

The numerator and denominator must be coprime else otherwise there would exist $\theta \in \overline{K}$ such that $f(\theta) = f'(\theta) = 0$. The Lemma then implies that $\deg[2] = 4$. □

Definition 2.4.11. Let G be an abelian group. A map $q : G \to \mathbb{Z}$ is said to be a **quadratic form** if

1. $q(nx) = n^2 q(x)$ for all $x \in G, n \in \mathbb{Z}$.
2. $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.

Remark. Recall that $q : G \to \mathbb{Z}$ is a quadratic form if and only if it satisfies the parallelogram law

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

for all $x, y \in G$.

Lemma 2.4.12. *Let K be a field such that $\operatorname{char} K \neq 2, 3$ and E/K an elliptic curve with Weierstrass form $y^2 = x^3 + ax + b$. Suppose that $P, Q \in E$ with $P, Q, P + Q, P - Q \neq \mathcal{O}_E$. Let $x_1, \ldots, x_4$ be the x-coordinates of these 4 points. Then there exist polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree at most 2 in x_1 and degree at most 2 in x_2 such that the ratio $(W_0 : W_1 : W_2) = (1 : x_3 + x_4 : x_3 x_4)$.*

Proof. Let $y = \lambda x + \nu$ be the line through P and Q. Then

$$\begin{aligned} f(x) - (\lambda x + \nu)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - s_1 x^2 + s_2 x - s_3 \end{aligned}$$

where s_i is the i^{th} elementary symmetric polynomial in the x_i. Comparing coefficients yields $\lambda^2 = s_1, -2\lambda\nu = s_2 - a$ and $\nu^2 = s_3 + b$. Eliminating λ and ν gives

$$F(x_1, x_2, x_3) = (s^2 - a)^2 - 4s_1(s_3 + b)$$

and so x_3 is a root of $F(x_1, x_2, X) = W_0 X^2 - W_1 X + W_2$. Repeating the calculation for the line through $P - Q$ shows that this quadratic also has a root x_4 and we get the desired ratio. □

Theorem 2.4.13. *Let K be a field and E_1 and E_2 elliptic curves over K. Then*

$$\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a quadratic form.

Proof. For the proof we assume that $\operatorname{char} K \neq 2, 3$. We first show that if $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$ then

$$\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2 \deg \phi + 2 \deg \psi$$

We may assume, without loss of generality, that $\phi, \psi, \phi + \psi, \phi - \psi \neq 0$. Indeed, those cases are either trivial or involve an easy application of Lemma 2.4.10. We first write out the mappings explicitly:

$$\begin{aligned} \phi &: (x, y) \mapsto (\xi_1(x, y), \eta_1(x, y)) \\ \psi &: (x, y) \mapsto (\xi_2(x, y), \eta_2(x, y)) \\ \phi + \psi &: (x, y) \mapsto (\xi_3(x, y), \eta_3(x, y)) \\ \phi - \psi &: (x, y) \mapsto (\xi_4(x, y), \eta_4(x, y)) \end{aligned}$$

By Lemma 2.4.12, we have that

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : F[\xi_1, \xi_2] : G[\xi_1, \xi_2])$$

where $F, G \in \mathbb{Z}[a, b][\xi_1, \xi_2]$ are some polynomials. Note that these three polynomials are have degree at most 2 in ξ_1 and degree at most 2 in ξ_2. Let $\xi_i(x) = r_i(x)/s_i(x)$ for some $r_i, s_i \in K[X]$ coprime. Then

$$(s_3s_4 : r_3s_3 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \cdots : \cdots)$$

Hence

$$\begin{aligned}
\deg(\phi + \psi) + \deg(\phi - \psi) &= \max\{\deg(r_3), \deg(s_3)\} + \max\{\deg(r_4), \deg(s_4)\} \\
&= \max\{\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4)\} \\
&\leq 2\max\{\deg(r_1)\deg(s_1)\} + 2\max\{\deg(r_2), \deg(s_2)\} \\
&= 2\deg(\phi) + 2\deg(\psi)
\end{aligned}$$

Replacing ϕ, ψ by $\phi + \psi$ and $\phi - \psi$ and using $\deg[2] = 4$ yields the reverse inequality. We have shown that the degree map satisfies the parallelogram law and is thus a quadratic form. □

Corollary 2.4.14. *Let K be a field and E/K an elliptic curve. Then $\deg([n] : E \to E) = n^2$ for all $n \in \mathbb{Z}$.*

2.5 The Invariant Differential

Throughout this section, K will be an algebraically closed field.

Definition 2.5.1. Let K be an algebraically closed field and C a smooth projective curve over K. We define the **space of differentials** over C, denoted Ω_C to be the $K(C)$-vector space generated by symbols df with $f \in K(C)$ subject to the relations

1. $d(f + g) = df + dg$
2. $d(fg) = fdg + gdf$
3. $da = 0$ for all $a \in K$

Remark. It can be shown that Ω_C is a 1-dimensional $K(C)$-vector space.

Definition 2.5.2. Let K be a field and C a smooth projective curve over K. Let $\omega \in \Omega_C$ be a non-zero differential, $P \in C$ and $t \in K(C)$ a uniformiser at P. Then $\omega = fdt$ for some $f \in K(C)^\times$. We define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$ which is independent of the choice of t. Moreover, we define $\mathrm{Div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)P$.

Definition 2.5.3. Let K be a field and C a smooth projective curve over K. We define the space of **regular differentials** to be

$$\{\, w \in \Omega_C \mid \mathrm{Div}(\omega) \geq 0 \,\}$$

Remark. $g(C) = \dim_K \{\, \omega \in \Omega_C \mid \mathrm{Div}(\omega) \geq 0 \,\}$

Lemma 2.5.4. *Let K be a field and C a smooth projective curve over K. Let $P \in C$ and $t \in K(C)^\times$ a uniformiser at P. If f is regular at P then df/dt is regular at P.*

Proof. Proof Omitted. □

Proposition 2.5.5. *Let K be a field and C a smooth projective curve over K. Suppose $f \in K(C)^\times$ such that $\operatorname{ord}_P(f) = n \neq 0$ and $\operatorname{char} K \nmid n$ then $\operatorname{ord}_P(df) = n - 1$.*

Proof. Fix a uniformiser $t \in K(C)^\times$ at P. Then we can always write $f = ut^n$ where $u \in K(C)$ satisfies $\operatorname{ord}_P(u) = 0$. Then

$$df = d(ut^n) = \left(\frac{du}{dt}t^n + nut^{n-1}\right)dt$$

By Lemma 2.5.4, du/dt is regular and so, in particular, we know that $\operatorname{ord}_P(du/dt) = 0$. Since $n \neq 0$ we have

$$\operatorname{ord}_P(df) = \operatorname{ord}_P(nut^{n-1}dt) = n - 1$$

□

Lemma 2.5.6. *Let K be a field such that $\operatorname{char} K \neq 2$ and let E/K be an elliptic curve given by the Weierstrass equation $y^2 = (x - l_1)(x - l_2)(x - l_3)$ for some $l_i \in K$. Then $\omega = dx/y$ is a differential on E with no zeroes and poles. Moreover, ω is a basis for the 1-dimensional K-vector space of regular differentials on E.*

Proof. Let $T_i = (l_i, 0)$. By Lemma 2.4.4 we have $E[2] = \{\, \mathcal{O}_E, T_1, T_2, T_3 \,\}$. Then $\operatorname{Div}(y) = T_1 + T_2 + T_3 - 3\mathcal{O}_E$.

Now suppose that $P \in E \backslash E[2]$. Then $\operatorname{ord}_P(x - x_p) = 1$ and so $\operatorname{ord}_P(x - x_P) = 1$ whence $\operatorname{ord}_P(dx) = 0$. Now if $P \in E[2]$ then $\operatorname{ord}_P(x - l_i) = 2$ and so $\operatorname{ord}_p(dx) = 1$. Finally, if $P = \mathcal{O}_E$ then $\operatorname{ord}_P(x) = -2$ and so $\operatorname{ord}_P(dx) = -3$. It then follows that $\operatorname{Div}(dx/y) = 0$ as desired. □

Definition 2.5.7. Let K be a field and $\phi : C_1 \to C_2$ a non-constant morphism between smooth projective curves over K. We define the **differential pullback** map of ϕ as

$$\begin{aligned} \phi^* : \Omega_{C_2} &\to \Omega_{C_1} \\ f dg &\mapsto (\phi^* f) d(\phi^* g) \end{aligned}$$

Theorem 2.5.8. *Let K be a field and E/K an elliptic curve over K. Let $\tau_P : E \to E$ be the translation by $P \in E$ map and $\omega = dx/y$. Then $\tau_P^*\omega = \omega$ and so ω is referred to as the **invariant differential**.*

Proof. Observe that $\operatorname{Div}(\tau_P^*\omega) = \tau_P^* \operatorname{Div}(\omega) = 0$ and so $\tau_P^*\omega$ is a regular differential. There thus exists $\lambda_P \in K^\times$ such that $\tau_P^*\omega = \lambda_P\omega$. Now consider the map

$$\begin{aligned} E &\to \mathbb{P}^1_K \\ P &\mapsto \lambda_P \end{aligned}$$

This is a morphism of smooth projective curves so it is either constant or surjective. It is clearly not surjective as its image does not contain 0 or the point at infinity. Hence $\lambda_P = \lambda$ for some $\lambda \in K^\times$ and $\tau_P^*\omega = \lambda\omega$ for all $P \in E$. Taking $P = \mathcal{O}_E$ gives $\lambda = 1$. □

Example 2.5.9. Let $K = \mathbb{C}$ so that $E(\mathbb{C}) = \mathbb{C}/\Lambda$ via $z \mapsto (\gamma(z), \gamma'(z))$. Then $dx/y = \gamma'(z)dz/\gamma'(z) = dz$ which is invariant under $z \mapsto z + a$.

Proposition 2.5.10. *Let K be a field, E/K an elliptic curve and ω the invariant differential of E. Then $\Omega_{E\times E}$ is a 2-dimensional $K(E\times E)$-vector space with basis given by $\{\, \pi_1^*\omega, \pi_2^*\omega \,\}$ where $\pi_i : E \times E \to E$ is the projection map.*

Proof. Proof Omitted □

Lemma 2.5.11. *Let K be a field and $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ for some elliptic curves E_1 and E_2 over K. If ω is the invariant differential on E_2 then $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.*

Proof. Write $E = E_2$ and consider the map

$$\begin{aligned} \mu : E \times E &\to E \\ (P, Q) &\mapsto P \oplus Q \end{aligned}$$

Then $\mu^*\omega = f\pi_1^*\omega + g\pi_2^*\omega$ for some $f, g \in K(E \times E)$. Given $Q \in E$ define the map

$$\begin{aligned} \iota_Q : E &\to E \times E \\ P &\mapsto (P, Q) \end{aligned}$$

Then

$$(\mu\iota_Q)^*\omega = (\iota_Q^* f)(\pi_1\iota_Q)^*\omega + (\iota_Q^* g)(\pi_2\iota_Q)^*\omega$$

Observe that $\pi_2\iota_Q$ is the constant map Q and so $(\pi_2\iota_Q)^*\omega = 0$. Furthermore, $(\mu\iota_Q)^* = \tau_Q^*$ and $\pi_1\iota_Q = \mathrm{id}$ and so $\tau_Q^*\omega = (\iota_Q^* f)\omega$. By Theorem 2.5.8 it follows that $\iota_Q^* f = 1$ for all $Q \in E$. This in turn implies that $f(P, Q) = 1$ for all $P, Q \in E$. Similarly, $g(P, Q) = 1$ for all $P, Q \in E$. Hence

$$\mu^*\omega = \pi_1^*\omega + \pi_2^*\omega$$

Pulling back along the map

$$\begin{aligned} E_1 &\to E \times E \\ P &\mapsto (\psi(P), \phi(P)) \end{aligned}$$

yields

$$(\psi + \phi)^*\omega = \psi^*\omega + \phi^*\omega$$

as desired. □

Proposition 2.5.12. *Let K be a field and $\phi : C_1 \to C_2$ a non-constant morphism of smooth projective curves. Then ϕ is separable if and only if $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is non-zero.*

Proof. Proof Omitted. □

Example 2.5.13. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{\, 0 \,\}$ and $n \geq 2$ an integer. Consider the map

$$\begin{aligned} \phi : \mathbb{G}_m &\to \mathbb{G}_m \\ x &\mapsto x^n \end{aligned}$$

Then $\phi^*(dx) = d(x^n) = nx^{n-1}dx$. So if $\mathrm{char}\, K \nmid n$ then ϕ is separable. Then $|\phi^{-1}(Q)| = \deg\phi$ for all but finitely many points $Q \in \mathbb{G}_m$. Since ϕ is a group homomorphism, $|\phi^{-1}(Q)| = \deg\phi$ for all $Q \in \mathbb{G}_m$ and so $|\ker\phi| = \deg\phi = n$. In other words, K contains exactly n n^{th} roots of unity.

Theorem 2.5.14. *Let K be a field and $n \in \mathbb{Z}$ such that* $\operatorname{char} K \nmid n$. *Suppose E is an elliptic curve over K. Then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.*

Proof. Let ω be the invariant differential of E. By Lemma 2.5.11 we have that $[n]^*\omega = n\omega$. Hence if $\operatorname{char} K \nmid n$, Proposition 2.5.12 implies that $[n]$ is separable. Appealing to Proposition 1.2.20 we see that $|[n]^{-1}Q| = \deg[n]$ for all but finitely many $Q \in E$. But $[n]$ is a group homomorphism and so $|[n]^{-1}Q| = \deg[n]$ for all $Q \in E$. By Corollary 2.4.14 we then have that $|E[n]| = \deg[n] = n^2$.

We thus see that $E[n]$ is a finitely generated abelian group so by the structure theorem for finitely generated abelian groups, we have that

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$$

for some integers $d_1|d_2|\ldots|d_t|n$ such that $\prod_{i=1}^{t} d_i = n^2$. Now suppose that p is a prime dividing d_1. Then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$. But $|E[p]| = p^2$ so $t = 2$ and $d_1 = d_2 = n$. Therefore, $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. □

Remark. If $\operatorname{char} K = p$ then $[p]$ is inseparable. It can be shown that either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$ (ordinary case) or $E[p^r] = 0$ for all $r \geq 1$ (supersingular case).

2.6 Elliptic Curves Over Finite Fields

Throughout this section let $\langle x, x\rangle = 2q(x)$ where $q(x)$ is a quadratic form.

Lemma 2.6.1 (Cauchy-Schwarz)**.** *Let A be an abelian group and $q : A \to \mathbb{Z}$ a positive definite quadratic form. Then for all $x, y \in A$ we have*

$$|q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}$$

Proof. Without loss of generality, we may assume that $q(x) \neq 0$. Fix $m, n \in \mathbb{Z}$. Then

$$\begin{aligned}
0 &\leq q(mx+ny) \\
&= \frac{1}{2}\langle mx+ny, mx+ny\rangle \\
&= m^2q(x) + mn\langle x, y\rangle + n^2q(y) \\
&= q(x)\left(m + \frac{\langle x, y\rangle}{2q(x)^n}\right)^2 + n^2\left(q(y) - \frac{\langle x, y\rangle^2}{4q(x)}\right)
\end{aligned}$$

Now let $m = -\langle x, y\rangle$ and $n = 2q(x)$ so that

$$\begin{aligned}
0 &\leq q(y) - \frac{\langle x, y\rangle^2}{4q(x)} \\
\langle x, y\rangle^2 &\leq 4q(x)q(y)
\end{aligned}$$

The result then follows upon taking the square root across this inequality. □

Theorem 2.6.2 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

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

Proof. Let E have a Weierstrass equation $F(x,y)=0$ with coefficients $a_1,\dots,a_6\in\mathbb{F}_q$. Note that the a_i are invariant under the Frobenius automorphism $a_i\mapsto a_i^q$. Define the Frobenius endomorphism on E by

$$\begin{aligned}\phi : E &\to E\\ (x,y)&\mapsto (x^q,y^q)\end{aligned}$$

This is a well-defined morphism of elliptic curves since applying the Frobenius automorphism across the equality $F(x,y)=0$ yields $F(x^q,y^q)=0$. This morphism clearly sends $\mathcal{O}_E$ to $\mathcal{O}_E$ and so ϕ is an isogeny of degree q. Since the Frobenius automorphism generates $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, it follows that

$$\begin{aligned}E(\mathbb{F}_q)&=\{\,P\in E\mid \phi(P)=P\,\}\\ &=\ker(1-\phi)\end{aligned}$$

Now let ω be the invariant differential of E. Note that

$$\phi^*\omega=\phi^*\left(\frac{dx}{y}\right)=\frac{dx^q}{y^q}=\frac{qx^{q-1}}{y^q}=0$$

where we have used the fact that $\operatorname{char}\mathbb{F}_q=p$. This then implies that

$$(1-\phi)^*\omega=\omega-\phi^*\omega=\omega\neq 0$$

whence $1-\phi$ is separable. Therefore,

$$|E(\mathbb{F}_q)|=|\ker(1-\phi)|=\deg(1-\phi)$$

By Theorem 2.4.13, the degree map is a positive definite quadratic form so by the Cauchy-Schwarz inequality, we have that

$$|\deg(1-\phi)-\deg\phi-\deg(1)|\leq 2\sqrt{\deg(1)\deg\phi}$$

Now, $\deg(1)=1$ and $\deg\phi=q$ by Lemma 2.4.8 and so

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

as desired. □

2.7 ζ-functions

Definition 2.7.1. Let K be a field and E/K an elliptic curve. We define the **trace** of an endomorphism of E to be

$$\begin{aligned}\mathrm{tr} : \mathrm{End}(E)&\to\mathbb{Z}\\ \psi&\mapsto\langle\psi,1\rangle\end{aligned}$$

where $\langle\psi,1\rangle=\deg(1-\psi)-\deg(\psi)-\deg 1=\deg(1+\psi)-\deg(\psi)-1$.

Lemma 2.7.2. *Let K be a field and E/K an elliptic curve. If $\psi\in\mathrm{End}(E)$ then*

$$\psi^2-[\mathrm{tr}\,\psi]\psi+[\deg\psi]=0$$

Proof. We first claim that

$$\deg([n]+\psi) = n^2 + n\,\mathrm{tr}\,\psi + \deg\psi \tag{1}$$

Since deg is a quadratic form on $\mathrm{End}(E)$ we have the bilinear form

$$\begin{aligned}\langle\cdot,\cdot\rangle : \mathrm{End}(E)\times\mathrm{End}(E) &\to \mathbb{Z}\\ (\phi,\psi) &\mapsto \deg(\phi+\psi)-\deg(\phi)-\deg(\psi)\end{aligned}$$

We thus have

$$\begin{aligned}\deg([n]+\psi) &= \langle[n],\psi\rangle + \deg([n]) + \deg(\psi)\\ &= n\,\langle 1,\psi\rangle + n^2 + \deg(\psi)\end{aligned}$$

thereby proving the claim. Clearly, $\mathrm{tr}(\phi+\psi) = \mathrm{tr}(\phi)+\mathrm{tr}(\psi)$. We next claim that $\mathrm{tr}(\phi^2) = (\mathrm{tr}\,\phi)^2 - 2\deg(\phi)$. Using the parallelogram law and the bilinearity of $\langle\cdot,\cdot\rangle$ we have

$$\begin{aligned}(\mathrm{tr}\,\phi)^2 - 2\deg(\phi) &= \langle 1,\phi\rangle^2 - 2\deg\phi\\ &= (\deg(1+\phi)-\deg(\phi)-1)^2 - 2\deg\phi\\ &= \deg(1+\phi)^2 - 2\deg\phi\deg(1+\phi) - 2\deg(1+\phi) + \deg(\phi^2) + 1\\ &= \deg(1+2\phi+\phi^2) - 2(\deg(\phi+\phi^2)+\deg(1+\phi)) + \deg(\phi^2)+1\\ &= \deg(1+2\phi+\phi^2) - \deg(1+2\phi+\phi^2) - \deg(\phi^2-1) + \deg(\phi^2)+1\\ &= \deg(\phi^2-1)+\deg(\phi^2)+1\\ &= -(\deg(1-\phi^2)-\deg(\phi^2)-1)\\ &= -\langle 1,-\phi^2\rangle\\ &= \langle 1,\phi^2\rangle\\ &= \mathrm{tr}(\phi^2)\end{aligned}$$

To prove the identity in the Lemma, it suffices to show that $\deg(\psi^2 - [\mathrm{tr}\,\psi]\psi + [\deg\psi]) = 0$. Inserting this into Equation 1 yields

$$\begin{aligned}\deg([\deg\psi]+\psi^2-[\mathrm{tr}\,\psi]\psi]) &= (\deg\psi)^2 + (\deg\psi)\,\mathrm{tr}(\psi^2-(\mathrm{tr}\,\psi)\psi)\\ &\quad + \deg(\psi^2-(\mathrm{tr}\,\psi)\psi)\\ &= (\deg\psi)^2 + (\deg\psi)(\mathrm{tr}(\psi^2)-(\mathrm{tr}\,\psi)^2)\\ &\quad + (\deg\psi)(\deg\psi-\mathrm{tr}\,\psi)\\ &= (\deg\psi)^2 + (\deg\psi)(-2\deg\psi) + (\deg\psi)((\mathrm{tr}\,\psi)^2\\ &\quad - (\mathrm{tr}\,\psi)^2 + \deg\psi)\\ &= 0\end{aligned}$$

□

Now let $E/\mathbb{F}_q$ be an elliptic curve and $\phi : E \to E$ the q-power Frobenius map. Let $a = \mathrm{tr}\,\phi = 1+\deg(\phi)-\deg(1-\phi)$ so that $|E(\mathbb{F}_q)| = q+1-a$. By Lemma 2.7.2, ϕ is a root of the polynomial $f(X) = X^2 - aX + q = 0$. Factoring this polynomial over $\mathbb{C}$ we have $(X-\alpha)(X-\beta) = 0$ for some $\alpha,\beta\in\mathbb{C}$. Hasse's Theorem then implies that $|a| \le 2\sqrt{q}$. We see that the polynomial $f(X)$ is non-negative for all X so it either has complex-conjugate roots or a double root. In either case, we see that $\alpha = \beta^*$ whence $|\alpha| = |\beta| = \sqrt{q}$.

Now let K be a number field. We have the **Dedekind ζ-function**

$$\zeta_K(s) = \sum_{\mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{N(\alpha)^s} = \prod_{\text{prime } \mathfrak{p} \lhd \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

Given a function field K (such as $\mathbb{F}_q(C)$ for some smooth projective curve $C/\mathbb{F}_q$), we similarly define

$$\zeta_K(s) = \prod_{x \in |C|} \left(1 - \frac{1}{N(x)^s}\right)^{-1}$$

where $|C|$ is the set of all closed points on C. These are given by the orbits for the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $\mathbb{C}(\overline{\mathbb{F}_q})$ and $N(x) = q^{\deg x}$ where x is the size of the orbit. We have $\zeta_K(s) = Z_C(q^{-s})$ where

$$Z_C(T) = \prod_{x \in |C|} (1 - T^{\deg x})^{-1}$$

in $\mathbb{Q}[[T]]$. Taking logs yields

$$\log Z_C(T) = \sum_{x \in |C|} \sum_{m=1}^{\infty} \frac{1}{m} T^{m \deg x}$$

using $\log(1 - X) = \sum_{n=1}^{\infty} X^n/n$. This implies that

$$T \frac{d}{dt} \log Z_C(T) = \sum_{x \in |C|} \sum_{m=1}^{\infty} \deg x T^{m \deg x}$$

Setting $n = m \deg x$ we then have

$$Z_C(T) = \exp\left(\sum_{n=1}^{\infty} \frac{|C(\mathbb{F}_{q^n})|}{n} T^n\right)$$

Theorem 2.7.3 (Dwork's Theorem for Elliptic Curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve and write $|E(\mathbb{F}_q)| = q + 1 - a$ as above. Then*

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

Proof. By Lemma 2.7.2, we have that $\phi^2 - a\phi + q = 0$ where ϕ is the q-power Frobenius map. Multiplying by ϕ^n and taking traces yields

$$\mathrm{tr}(\phi^{n+2}) + a \,\mathrm{tr}(\phi^{n+1}) + q \,\mathrm{tr}(\phi^n) = 0$$

This second order recurrence relation with initial conditions $\mathrm{tr}(1) = 2$ and $\mathrm{tr}(\phi) = a$ has solutions $\mathrm{tr}(\phi^n) = \alpha^n + \beta^n$ and so

$$\begin{aligned} E(\mathbb{F}_{q^n}) &= \deg(1 - \phi^n) \\ &= 1 + \deg(\phi^n) - \mathrm{tr}(\phi^n) \\ &= 1 + q^n - \alpha^n - \beta^n \end{aligned}$$

Hence

$$Z_E(T) = \exp\left(\sum_{n=1}^{\infty}\left(\frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{\alpha T)^n}{n} - \frac{(\beta T)^n}{n}\right)\right)$$
$$= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

□

Remark. Let s be a zero of $\zeta_K(s)$. Then $Z_E(q^{-s}) = 0$ whence $q^s = \alpha$ or $q^s = \beta$. By the previous discussion, we have that $|q^s| = \sqrt{q}$ and so $\Re(s) = 1/2$. This is an analogue of the Riemann Hypothesis.

3 Elliptic Curves over Local Fields

3.1 Formal Groups

Definition 3.1.1. Let R be a ring and $I \triangleleft R$ an ideal. We define the **I-adic** topology on R to be the one generated by the basis $\{\, r + I^n \mid r \in R, n \geq 1 \,\}$.

Definition 3.1.2. Let R be a ring and $I \triangleleft R$ an ideal. We say that a sequence (x_n) in R is **Cauchy** with respect to the I-adic topology if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that for all $m, n \geq N$ we have $x_m - x_n \in I^k$ for all $m, n \geq N$.

Definition 3.1.3. Let R be a ring and $I \triangleleft R$ an ideal. We say that R is complete with respect to I if $\bigcap_{n\geq 1} I^n = \{\, 0 \,\}$ and every Cauchy sequence in R converges with respect to I.

Example 3.1.4. $\mathbb{Z}_p$ is complete with respect to $p\mathbb{Z}_p$. $\mathbb{Z}[[t]]$ is complete with respect to (t).

Theorem 3.1.5 (Hensel's Lemma)**.** *Let R be an integral domain complete with respect to $I \triangleleft R$ and $f \in R[X]$ a polynomial. Given $s \geq 1$, suppose that $a \in R$ satisfies $F(a) \equiv 0 \pmod{I^s}$ and $F'(a) \in R^\times$. Then there exists a unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I^s}$.*

Proof. Without loss of generality, we may assume that $a = 0$ and $F'(a) = 1$. Indeed, we may simply replace $F(x)$ by $F(x + a)/F'(a)$. Consider the sequence defined by $x_0 = 0$ and $x_{n+1} = x_n - F(x_n)$. We claim that x_n is Cauchy. By induction it is clear that $x_n \equiv 0 \pmod{I^s}$ for all $n \geq 0$. Now write

$$F(X) - F(Y) = (X - Y)(1 + XG(X, Y) + YH(X, Y)$$

for some $G, H \in R[X, Y]$. We now claim that $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ for all $n \geq 0$. We prove this by induction on n. The case where $n = 0$ is clear so suppose that it holds for n. We have that $F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}}$ and so $x_n - F(x_n) \equiv x_{n-1} - F(x_{n-1}) \pmod{I^{n_s}}$ whence $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ thereby proving the claim.

(x_n) is therefore Cauchy. Since R is complete, $x_n \to b$ as $n \to \infty$ for some $b \in R$. Taking the limit in the definition of the sequence yields $b = b - F(b)$ and so $F(b) = 0$. Taking the limit in $x_n \equiv 0 \pmod{I^s}$ gives $b \equiv 0 \pmod{I^s}$. Uniqueness then follows from the expression for $F(X) - F(Y)$ and the fact that R is an integral domain. □

Example 3.1.6. Let R be a ring and $a_1, \ldots, a_6 \in R$ elements. Let E be the elliptic curve with projective Weierstrass equation $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. Conisder the affine piece $Y \neq 0$ with $t = -X/Y, w = -Z/Y$. In these coordinates, the Weierstrass equation becomes

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_rtw^2 + a_6w^3 = f(t, w)$$

We now apply Hensel's Lemma with $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ and $I = (t)$. We claim that $F(X) = X - f(t, X)$ with $s = 3$ and $a = 0$ satisfies the hypotheses of Hensel's Lemma. We have $F(a) = -f(t, 0) = -t^3 \equiv 0 \pmod{I^3}$. Furthermore, $F'(a) = 1 - a_1t - a_2t^2 \in R^\times$. Hence there exists a unique $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that $f(t, w(t)) = w(t)$ where $w(t) \equiv 0 \pmod{t^3}$. In particular, $w(t) = t^3(1 + A_1t + A_2t^2 + \ldots)$ where $A_1 = a_1, A_2 = a_1^2 + a_2, A_3 = a_1^3 + 2a_1a_2 + a_3$).

Lemma 3.1.7. *Let R be an integral domain that is complete with respect to an ideal $I \triangleleft R$. Let $a_1, \ldots, a_6 \in R$ be the Weierstrass coefficients of an elliptic curve over R. Let $K = \mathrm{Frac}(R)$ and $\overline{E}$ be the elliptic curve given by reducing the cofficients of the Weierstrass equation of E modulo I. Then*

$$\begin{aligned}\overline{E} &= \{\, (t, w) \in E(K) \mid t, w \in I \,\} \\ &= \{\, (t, w(t)) \in E(K) \mid t \in I \,\}\end{aligned}$$

is a subgroup of $E(K)$ where $w(t)$ is the power series given in the previous example.

Proof. Taking $(t, w) = (0, 0)$ shows that $\mathcal{O}_E \in \overline{E}(I)$ so it suffices to show that, given $P_1, P_2 \in \overline{E}(I)$ we have $-P_1 - P_2 \in \overline{E}(I)$. So let $t_1, t_2 \in I$. We have

$$\begin{aligned}\lambda &= \frac{w(t_2) - w(t_1)}{t_2 - t_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{t_2^n - t_1^n}{t_2 - t_1} \in I \\ \nu &= w_1 - \lambda t_1 \in I\end{aligned}$$

Substituting $w = \lambda t + \nu$ into $w = f(t, w(t))$ yields

$$\lambda t + \nu = t^3 + a_1t(\lambda t + \nu) + a_2t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3$$

The coefficient of t^3 is given by

$$A = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$$

and the coefficient of t^2 is

$$B = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu$$

We have that $A \in R^\times$ and $B \in I$ so $t^3 = -B/A - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. □

Example 3.1.8. Taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ with $I = (t)$, the Lemma implies that there exists $\iota(t) \in \mathbb{Z}[[a_1, \ldots, a_6]]$ with no constant term such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$. Taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ and $I = (t_1, t_2)$, the Lemma implies that there exists $F(t_1, t_2) \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ such that $(t_1, w(t_1)) + (t_2, w(t_2)) = F(t_1, t_2), w(F(t_1, t_2))$. In fact,

$$\begin{aligned}\iota(X) &= X - a_1X^2 - a_2^2X^3 - (a_1^3 + a_3)X^4 + \ldots \\ F(X, Y) &= X + Y - a_1XY - a_2(X^2Y + XY^2) + \ldots\end{aligned}$$

From the properties of the group law, we deduce

1. $F(X,Y) = F(Y,X)$
2. $F(X,0) = X = F(0,Y) = Y$
3. $F(X,F(Y,Z)) = F(F(X,Y),Z)$
4. $F(X,\iota(X)) = 0$

Definition 3.1.9. Let R be a ring. A **formal group** over R is a power series $F(X,Y) \in R[[X,Y]]$ such that

1. $F(X,Y) = F(Y,X)$
2. $F(X,0) = X, F(0,Y) = Y$
3. $F(F(X,Y),Z) = F(X,F(Y,Z))$

Definition 3.1.10. Let R be a ring and F and G formal groups over R. We define a **morphism** between F and G to be a power series $f \in R[[T]]$ such that $f(0) = 0$ and $f(F(X,Y)) = G(f(X),f(Y))$. We say that F and G are **isomorphic** if there exists morphisms $f : F \to G$ and $g : G \to F$ such that $f(g(T)) = g(f(T))$.

Lemma 3.1.11. *Let R be a ring and $g(X) \in R[[X]]$ such that $g(0) \in R^\times$. Then there exists $h(X) \in R[[X]]$ such that $g(h(X)) = X$.*

Proof. We claim that, given any formal power series $g(X) = \sum_{i\geq 1} a_i X^i \in R[[X]]$ such that $g(X) \equiv a_1 X \pmod{X^2}$ for some $a_1 \in R^\times$, there exists a power series $h(X) \in R[[X]]$ such that $g(h(X)) = X$. To do this, we shall inducitvely construct polynomials $h_n(X) = \sum_{i=1}^n b_i X^i$ such that $g(h(X)) \equiv \pmod{X^{n+1}}$. We then obtain the desired power series as $h = \lim_{n\to\infty} h_n(X)$ which is well-defined since $R[X]$ is X-adically complete.

Indeed, suppose that $n = 1$. Then we may set $h_1(X) = b_1 X$ with $b_1 = a^{-1}$. Then, clearly, $g(h_1(X)) \equiv X \pmod{X^2}$. Now assume that we have constructed $h_{n-1}(X)$ such that $g(h_{n-1}(X)) \equiv X \pmod{X^n}$. Then $g(h_{n-1}(X)) \equiv X + c_n X^n \pmod{X^{n+1}}$ for some $c_n \in R$. Now consider

$$h_n(X) = h_{n-1}(X) + b_n X^n$$

We have

$$h_n(X)^k = (h_{n-1}(X) + b_n X^n)^k \equiv \begin{cases} h_{n-1}^k(X) & \text{if } k > 1 \\ h_{n-1}(X) + b_n X^n & \text{if } k = 1 \end{cases} \pmod{X^{n+1}}$$

So we have

$$\begin{aligned} g(h_n(X)) = \sum_{k\geq 1} a_k h_n(X)^k = \sum_{k\geq 1} a_k (h_{n-1}(X) + b_n X^n)^k &\equiv \sum_{k\geq 1} a_k h_{n-1}^k + a b_n X^n \\ &= X + c_n X^n + a_1 b_n X^n \end{aligned}$$

So we may take $b_n = -a_1^{-1} c_n$ and we are done. □

Theorem 3.1.12. *Let R be a ring such that* $\operatorname{char} R = 0$. *Then every formal group over R is isomorphic to the formal group $\widehat{\mathbb{G}}_a$ given by the power series $G(X,Y) = X + Y$ over $R \otimes \mathbb{Q}$. In particular,*

1. *There is a unique power series*

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$$

with $a_i \in R$ such that

$$\log(F(X,Y)) = \log(X) + \log(Y)$$

For any formal group $F(X,Y)$ over R.

2. *There is a unique power series*

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$$

such that

$$\exp(\log(T)) = \log(\exp(T)) = T$$

Proof. We first prove uniqueness of the logarithm. To ease notation, denote $F_1(X,Y) = \frac{\partial}{\partial x}F(X,Y)$. Suppose $\log(T) \in R[[T]]$ exists. Denote

$$p(T) = \frac{d}{dt}\log(T) = 1 + a_2T + a_3T^2 + \dots$$

Differentiating the logarithm relation with respect to X, we have

$$p(F(X,Y))F_1(X,Y) = p(X) + 0$$

Setting $X = 0$, we have

$$p(Y)F_1(0,Y) = p(0) = 1$$

so that $p(Y) = F_1(0,Y)^{-1}$ so that $p(Y)$ is uniquely determined by F whence so is log.

We next prove existence of log. As before, set $p(T) = F_1(0,Y)^{-1} = 1 + a_2T + a_3T^2 + \dots$ for some $a_i \in R$. We define $\log(T)$ to be the formal integral of $p(T)$ with respect to T. To show that this satisfies the claimed relation, first start with the associative law

$$F(X, F(Y,Z)) = F(F(X,Y), Z)$$

And differentiate with respect to X so that

$$F_1(X, F(Y,Z)) = F_1(X,Y)F_1(F(X,Y), Z)$$

Setting $X = 0$ we have

$$\begin{aligned} F_1(0, F(Y,Z)) &= F_1(0,Y)F_1(Y,Z) \\ p(F(Y,Z))^{-1} &= p(Y)^{-1}F(Y,Z) \\ p(Y) &= p(F(Y,Z))F(Y,Z) \end{aligned}$$

Integrating this with respect to Y yields

$$log(Y) + h(Z) = log(F(Y,Z))$$

where $h(Z)$ is some integrating factor. By symmetry, we must have that $h(Z) = \log(Z)$ so we are done. The existence of the exponential series follows immediately from Lemma 3.1.11. □

Proposition 3.1.13. *Let R be a ring, complete with repsect to an ideal $I \triangleleft R$. Let $F(X,Y) \in R[[X,Y]]$ be a formal group over R. Then the binary operation*

$$\begin{aligned} \oplus_{\mathcal{F}} : I \times I &\to I \\ (x,y) &\mapsto x \oplus_{\mathcal{F}} y = F(x,y) \end{aligned}$$

makes $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ an abelian group.

Proof. Fix $x, y \in I$. Since R is complete, the power series $F(x,y)$ converge I-adically to an element of I so this binary operation is indeed closed. The rest of the abelian group axioms follow immediately from the formal group axioms. □

Corollary 3.1.14. *Let $\mathcal{F}$ be a formal group over a ring R and $n \in \mathbb{Z}$ invertible in R. Then*

1. *$[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism of formal groups.*
2. *If R is complete with respect to an ideal $I \triangleleft R$ then the induced homomorphism $[n] : \mathcal{F}(I) \to \mathcal{F}(I)$ is an isomorphism.*

Proof. Observe that $[1](T)$ is just the power series (T) and $[n+1](T) = F([n]T, T)$. By induction, it is clear that $[n]T = nT + \cdots \in R[[T]]$. Now if n is invertible in R then Lemma 3.1.11 implies that there exists an inverse for this homomorphism of formal groups. The second part then follows immediately. □

3.2 Elliptic Curves

Throughout the rest of this section, let K be a discretely valued field of characteristic 0, complete with respect to a discrete valuation $v : K^\times \to \mathbb{Z} \cup \infty$. We assume that $\mathbb{F}_K$, the residue field of K has characteristic $p > 0$ for some rational prime p and we write $\mathcal{O}_K$ for the valuation ring of K and $\mathfrak{m}_K = (\pi)$ its unique maximal ideal for some uniformiser π. Note that $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{m}_K$

We fix an elliptic curve E/K.

Definition 3.2.1. We say that a Weierstrass model $a_1, \ldots, a_6 \in L$ for E is **integral** if $a_i \in \mathcal{O}_K$ for all i. Moreover, we say that the chosen model is **minimal** if $v(\Delta_E)$ is minimal amongst all integral Weierstrass models for E.

Remark. Since the transformation $x = u^2x', y = u^3y'$ is an isomorphism of elliptic curves, every elliptic curve over K admits an integral model. Moreover, if $a_1, \ldots, a_6 \in \mathcal{O}_K$ then $\Delta \in \mathcal{O}_K$ so that $v(\Delta) \geq 0$. Since v is discrete, minimal Weierstrass models also exist for all E/K. Finally, if $\mathrm{char}(K) \neq 2, 3$ then there exist minimal equations of the form $y^2 = x^3 + ax + b$.

Lemma 3.2.2. *Suppose that E/K has an integral Weierstrass model*

$$y^2 = x^3 + ax + b$$

Let $\mathcal{O}_E \neq P = (x,y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s$ and $v(y) = -3s$ for some integer $s \geq 1$.

Proof. First suppose that $v(x) \geq 0$. Suppose, for a contradiction, that $v(y) < 0$. Applying v across the Weierstrass equation, we have

$$0 > 2v(y) = v(x^3 + ax + b) \geq \min\{3v(x), v(x)\} \geq 0$$

which is a contradiction. Hence we must have that $v(y) \geq 0$.

Now suppose that $v(x) < 0$. Then $2v(y) = 3v(x)$ so that $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$. □

Proposition 3.2.3. *Let $\widehat{E}$ be the formal group associated to E as in Example 3.1.8. Consider*

$$\begin{aligned} E_r(K) = \widehat{E}(\pi^r \mathcal{O}_K) &= \left\{ (x,y) \in E(K) \;\middle|\; -\frac{x}{y}, -\frac{1}{y} \in \pi^r \mathcal{O}_K \right\} \cup \{ 0 \} \\ &= \left\{ (x,y) \in E(K) \;\middle|\; v\left(\frac{x}{y}\right), v\left(\frac{1}{y}\right) \geq r \right\} \cup \{ 0 \} \\ &= \{ (x,y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r \} \end{aligned}$$

Then this is a subgroup of $E(K)$ and for sufficiently large r we have

$$\widehat{E}(\pi^r \mathcal{O}_K) \cong (\mathcal{O}_K, +)$$

Moreover, for all $r \geq 1$ we have

$$\frac{\widehat{E}(\pi^r \mathcal{O}_K)}{\widehat{E}(\pi^{r+1} \mathcal{O}_K)} \cong (\mathbb{F}_p, +)$$

Proof. We shall prove the Proposition for arbitrary formal groups $\mathcal{F}$ over $\mathcal{O}_K$. Let $e = v(p)$. We claim that if $r > e/(p-1)$ then

$$\log : \mathcal{F}(\pi^r \mathcal{O}_K) \to \widehat{\mathbb{G}_a}(\pi^r \mathcal{O}_K)$$

is an isomorphism with inverse given by exp. To this end, fix $x \in \pi^r \mathcal{O}_K$. We need to show that $\exp(x)$ and $\log(x)$ converge. Because we are working in a non-archimidean valued field, it suffices to show that the sequence of valuations of its terms goes to ∞. Recall that

$$\exp(T) = T + \frac{b_2}{2!} T^2 + \dots$$

for some $b_i \in \mathcal{O}_K$. We first calculate $v(n!)$:

$$v(n!) = e v_p(n!) = e \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor < e \sum_{r=1}^{\infty} \frac{n}{p^r} = en \frac{1/p}{1 - 1/p} = e \frac{n}{p-1} \leq \frac{e(n-1)}{p-1}$$

then

$$\begin{aligned} v\left(\frac{b_i x^i}{i!}\right) &\geq nr - \frac{e(i-1)}{p-1} \\ &= (i-1)\left(r - \frac{e}{p-1}\right) + r \end{aligned}$$

This is always greater than or equal to r and hence goes to ∞ as $i \to \infty$. Hence exp converges on $\mathcal{F}(\pi^r(\mathcal{O}_K))$. The same arguments show that log also converges on $\mathcal{F}(\pi^r(\mathcal{O}_K))$ so that

$$\mathcal{F}(\pi^r \mathcal{O}_K) \to \widehat{\mathbb{G}_a}(\pi^r \mathcal{O}_K) \cong (\pi^r \mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$$

To prove the second assertion, recall that $F(X,Y) = X + Y + XY + \dots$. Hence given $x, y \in \mathcal{O}_K$ we have

$$F(\pi^r x, \pi^r y) = \pi^r (x + y) \pmod{\pi^{r+1}}$$

Now define a surjective homomorphism of groups

$$\begin{aligned} \mathcal{F}(\pi^r \mathcal{O}_K) &\to \mathbb{F}_K \\ \pi^r x &\mapsto x \pmod{\pi} \end{aligned}$$

which clearly has kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$ □

Corollary 3.2.4. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a group of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Proposition 3.2.5. *Let E/K be an elliptic curve. Then the reductions modulo π of any two minimal Weierstrass equations of E define isomorphic curves over $\mathbb{F}_K$.*

Proof. Fix two minimal Weierstrass models of E with discriminants Δ_1 and Δ_2 respectively. Suppose that they are related by $[u, r, s, t]$ for some $u, r, s, t \in K$ with $u \neq 0$. Then $\Delta_1 = u^{12}\Delta_2$. But the two Weierstrass models are minimal and so we must have that $\Delta_1 = \Delta_2$ so that $u \in \mathcal{O}_K^\times$. The transformation formulae then imply that $r, s, t \in \mathcal{O}_K$ so that the Weierstrass euations for the reductions modulo π are related by the reductions of u, r, s, t. □

Definition 3.2.6. We define the **reduction** of E/K to be the curve $\widetilde{E}/\mathbb{F}_K$ given by reducing a minimal Weierstrass model of E modulo π. We say that E has **good reduction** if $\tilde{E}$ is non-singular. Otherwise we say that E has **bad reduction**.

Remark. Let E/K be an elliptic curve with integral Weierstrass model. Then we have the following situations

1. If $v(\Delta) = 0$ then E has good reduction.
2. If $0 < v(\Delta) < 12$ then E has bad reduction.
3. If $v(\Delta) \geq 12$ and the chosen model is minimal then E has bad reduction.

Definition 3.2.7. We define the **reduction map** on E to be the restriction to $E(K)$ of the map

$$\begin{aligned} \mathbb{P}^2(K) &\to \mathbb{P}^2(\mathbb{F}_K) \\ [x : y : z] &\mapsto [\overline{x} : \overline{y} : \overline{z}] \end{aligned}$$

where we choose a representative $[x : y : z]$ such that $\min\{v(x), v(y), v(z)\} = 0$. Given $P \in E(K)$, we denote by $\overline{P}$ its image in $\widetilde{E}(\mathbb{F}_K)$.

Proposition 3.2.8. *$E_1(K)$ coincides with the kernel of the reduction map.*

Proof. This is immediate from Proposition 3.2.3. □

Definition 3.2.9. Let E/K be an elliptic curve. We define the curve

$$\widetilde{E}_{\text{ns}} = \begin{cases} \widetilde{E} & \text{if } E \text{ has good reduction} \\ \widetilde{E} \setminus \{\, \text{singular point} \,\} & \text{if } E \text{ has bad reduction} \end{cases}$$

Remark. The chord-and-tangent process still produces a group law on $\widetilde{E}_{\text{ns}}$ since there is no danger of running into singular points.

Proposition 3.2.10. *Let E/K have bad reduction. Then we have one of two cases*

$$\widetilde{E}_{\mathrm{ns}}(\overline{K}) \cong \widehat{\mathbb{G}_m}(\overline{K}) \qquad \text{or} \qquad \widetilde{E}_{\mathrm{ns}}(\overline{K}) \cong \widehat{\mathbb{G}_a}(\overline{K})$$

*In the former case, we say that E has **multiplicative reduction**. In the latter case, we say that E has **additive reduction**.*

Proof. Proof omitted. □

Definition 3.2.11. Let E/K be an elliptic curve. We define

$$E_0(K) = \{\, P \in E(K) \mid \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_K) \,\}$$

Proposition 3.2.12. *$E_0(K)$ is a subgroup of $E(K)$ and reduction modulo π is a surjective group homomorphism $E_0(K) \to \widetilde{E}_{\mathrm{ns}}(K)$.*

Proof. We first check that $E_0(K)$ is indeed a group. To this end, fix $P_1, P_2 \in E_0(K)$. Let $P_3 \in E(K)$ be such that $P_1 + P_2 + P_3 = \mathcal{O}_E$. We claim that $P_3 \in E_0(K)$ so that $P_1 + P_2 = -P_3 \in E_0(K)$. By definition, P_1, P_2, P_3 all lie on a line, say $l : ax + by + cz = 0$ for some $a, b \in K$. We may assume, without loss of generality, that $\min\{v(a), v(b), v(c)\} = 0$. Reducing this line modulo π yields a line $\widetilde{l} : \widetilde{a}x + \widetilde{b}x + \widetilde{c}z = 0$. Then $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}$ all lie on $\widetilde{l}$. Now since $P_1, P_2 \in E_0(K)$, we have $\widetilde{P_1}, \widetilde{P_2} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ so that $\widetilde{P_3} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$. By definition, we then have that $P_3 \in E(K)$.

We now prove the surjectivity assertion. Suppose that E admits the Weierstrass equation $y^2 = x^3 + ax + b$. Let $f(x, y) = y^2 - x^3 - ax - b$. Fix $\widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_K) \setminus \{\, \mathcal{O}_{\widetilde{E}} \,\}$. We need to exhibit $P \in E(K)$ that maps to $\widetilde{P}$ under the reduction map. Say $\widetilde{P} = (\widetilde{x_0}, \widetilde{y_0})$ for some $x_0, y_0 \in \mathcal{O}_K$. Since $\widetilde{P}$ is nonsingular, we have one of the following cases:

$$\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\pi}$$
$$\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\pi}$$

First suppose the first case holds. Set $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. Then $g(x_0) \equiv 0 \pmod{\pi}$ and $g'(x_0) \in \mathcal{O}_X^\times$. By Hensel's Lemma, there exists $b \in \mathcal{O}_K$ such that $g(b) = 0$ and $b \equiv x_0 \pmod{\pi}$. Then $P = (b, y_0) \in E(K)$ reduces to $\widetilde{P}$ as desired. The second case is similar so it follows that the reduction map is surjective. □

Lemma 3.2.13. *If $|\mathbb{F}_K| < \infty$ then $\mathbb{P}^n(K)$ is compact with respect to the π-adic topology.*

Proof. Suppose that $|\mathbb{F}_K| < \infty$. Then each $\mathcal{O}_K/\pi^r\mathcal{O}_K$ is compact when equipped with the discrete topology. By Tychonoff's Theorem, $\prod \mathcal{O}_K/\pi^r\mathcal{O}_K$ is compact. Since $\mathcal{O}_K$ is isomorphic to $\varprojlim \mathcal{O}_K/\pi^r\mathcal{O}_K$ which is a closed subspace of $\prod \mathcal{O}_K/\pi^r\mathcal{O}_K$, it follows that $\mathcal{O}_K$ is compact. Now, $\mathbb{P}^n(K)$ is the union of compact sets

$$\{\, [a_0 : \cdots : a_{i-1} : 1 : a_{i+1}, \ldots, a_n] \mid a_j \in \mathcal{O}_K \,\}$$

so $\mathbb{P}^n(K)$ is itself compact. □

Lemma 3.2.14. *If $|\mathbb{F}_K| < \infty$ then $E_0(K)$ has finite index in $E(K)$.*

Proof. By Lemma 3.2.13, $\mathbb{P}^n(K)$ is compact. Since $E(K) \subseteq \mathbb{P}^2(K)$ is a closed subset, it follows that $(E(K), +)$ is a compact topological group. If $E_0(K) = E(K)$ then we are done so suppose that $\widetilde{E}$ has a singular point, say $(\widetilde{x_0}, \widetilde{y_0})$. Then

$$E(K) \backslash E_0(K) = \{\, (x, y) \in E(K) \mid v(x - x_0) \geq 1, v(y - y_0) \geq 1 \,\}$$

is a closed subset of $E(K)$ so that $E_0(K)$ is open. Now, the cosets of $E_0(K)$ in $E(K)$ given an open cover of $E(K)$. But $E(K)$ is compact so this open cover must have a finite subcover. But cosets are pairwise disjoint so there must be finitely many cosets to begin with. This is exactly what it means for $E_0(K)$ to have finite index in $E(K)$. □

Definition 3.2.15. We define the **Tamagawa number** of E, denoted $c_K(E)$ to be $[E(K) : E_0(K)]$.

Proposition 3.2.16. *Let E/K have split multiplicative reduction (in other words, $\widetilde{E}_{\text{ns}} \cong \mathbb{G}_m$ over K). Then $c_K(E) = v_k(\Delta)$. Otherwise, $c_K(E) \leq 4$.*

Proof. Proof omitted. □

Theorem 3.2.17. *Let $K/\mathbb{Q}_p$ be a finite extension. Then $E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$. In paticular $E(K)_{\text{tors}}$ is finite.*

Proof. For large enough r, we have that $E_r(K) \cong \mathcal{O}_K$. This is a subgroup of $E_0(K)$ which has finite index so that $E_r(K)$ necessarily has finite index in $E(K)$.

To see that $E(K)_{\text{tors}}$ is finite, first observe that $E_r(\mathcal{O}_K) \cong \mathcal{O}_K$ is torsion free. Hence $E(K)_{\text{tors}} \hookrightarrow E(K)/E_r(K)$. But the latter is finite. □

Remark. We denote by K^{ur} the union of all finite unramified extensions of the local field K.

Theorem 3.2.18. *Let $K/\mathbb{Q}_p$ be a finite extension and E/K an elliptic curve with good reduction. Suppose that $p \nmid n$. If $P \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.*

Proof. Let K_m denote the unique unramified extension of K of degree m. Then for all $m \geq 1$ we have a short exact sequence

$$0 \longrightarrow E_1(K_m) \longrightarrow E(K_m) \longrightarrow \widetilde{E}(K_m) \longrightarrow 0$$

Taking the union over all such m, we get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{\text{ur}}) & \longrightarrow & E(K^{\text{ur}}) & \longrightarrow & \widetilde{E}(\overline{\mathbb{F}}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot n} & & \downarrow{\scriptstyle \cdot n} & & \downarrow{\scriptstyle \cdot n} & & \\ 0 & \longrightarrow & E_1(K^{\text{ur}}) & \longrightarrow & E(K^{\text{ur}}) & \longrightarrow & \widetilde{E}(\overline{\mathbb{F}}) & \longrightarrow & 0 \end{array}$$

where $\overline{\mathbb{F}}$ is the residue field of K^{ur}. By Corollary 3.1.14, the first vertical map is an isomorphism since n is invertible in $\mathcal{O}_K$. Since $[n] : \widetilde{E}(\overline{\mathbb{F}}) \to \widetilde{E}(\overline{\mathbb{F}})$ is a non-constant isogeny, it is surjective. Applying the Snake Lemma then gives us an exact sequence

$$0 \longrightarrow E(K^{\text{ur}})[n] \longrightarrow \widetilde{E}(\overline{\mathbb{F}})[n] \longrightarrow 0$$

so that $E(K^{\mathrm{ur}})[n] \cong \widetilde{E}(\overline{\mathbb{F}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E(K^{\mathrm{ur}})/nE(K^{\mathrm{ur}}) = 0$. But we also have that $E(\overline{K})[n] = (\mathbb{Z}/n\mathbb{Z})^2$ so, in fact, $E(K^{\mathrm{ur}})[n] = E(\overline{K})[n]$.

Now, by the above discussion, given $P \in E(K)$, there exists a $Q \in E(K^{\mathrm{ur}})$ such that $nQ = P$. Then

$$\begin{aligned}[n]^{-1}P &= \{\, Q + T \mid T \in E(\overline{K})[n] \,\} \\ &= \{\, Q + T \mid T \in E(K^{\mathrm{ur}})[n] \,\}\end{aligned}$$

Hence $[n]^{-1}P \subseteq E(K^{\mathrm{ur}})$ so that $K([n]^{-1}P)$ is unramified as claimed. □

4 The Torsion Subgroup

4.1 Basic Results

Throughout this section, let K be a number field and $\mathfrak{p}$ a finite prime of K. By $K_{\mathfrak{p}}$ we mean the completion of K at $\mathfrak{p}$. By $\mathbb{F}_{\mathfrak{p}}$ we mean the residue field of $K_{\mathfrak{p}}$. By $v_{\mathfrak{p}}$ we mean the $\mathfrak{p}$-adic valuation on $K_{\mathfrak{p}}$.

Definition 4.1.1. Let E/K be an elliptic curve. We say that a prime $\mathfrak{p}$ of K is a **prime of good reduction** (resp. **prime of bad reduction**) for E if $E/K_{\mathfrak{p}}$ has good reduction (resp. bad reduction).

Lemma 4.1.2. *Let E/K be an elliptic curve. Then E has only finitely many primes of bad reduction.*

Proof. Fix a Weierstrass equation for E with $a_1, \ldots, a_6 \in \mathcal{O}_K$. Since E is non-singular, we necessarily have that $\Delta \neq 0$ and $\Delta \in \mathcal{O}_K$. Write

$$(\Delta) = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_r^{\alpha_r}$$

for the unique factorisation of (Δ) into prime ideals. Let $S = \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_r \,\}$. If $\mathfrak{p} \notin S$ then $v_{\mathfrak{p}}(\Delta) = 0$ so that $E/K_{\mathfrak{p}}$ has good reduction. Hence the primes of bad reduction of E are contained in S. □

Remark. If K has class number 1, for example $\mathbb{Q}$, then there exists a globally minimal Weierstrass model for E.

Lemma 4.1.3. *Let E/K be a number field. Then $E(K)_{\mathrm{tors}}$ is finite.*

Proof. Fix a prime of good reduction $\mathfrak{p}$ of K. Then $E(K)_{\mathrm{tors}} \subseteq E(K_{\mathfrak{p}})_{\mathrm{tors}}$. But Theorem 3.2.17 implies that the latter is finite. □

Lemma 4.1.4. *Let E/K be an elliptic curve and $\mathfrak{p}$ a prime of good reduction of E. If $\mathfrak{p} \nmid n$ for some integer n then reduction modulo p induces an injective group homomorphism*

$$E(K)[n] \hookrightarrow E(K_{\mathfrak{p}})[n] \hookrightarrow \widetilde{E}(\mathbb{F}_{\mathfrak{p}})$$

Proof. By Proposition 3.2.12, we have a group homomorphism

$$E(K_{\mathfrak{p}}) \to \widetilde{E}(\mathbb{F}_{\mathfrak{p}})$$

with kernel $E_1(K_{\mathfrak{p}})$. By Corollary 3.1.14 and the fact that $\mathfrak{p} \nmid n$, $E_1(K_{\mathfrak{p}})$ has no n-torsion and so we get the claimed injection. □

p	2	3	5	7	11	13
$\lvert\widetilde{E}(\mathbb{F}_p)\rvert$	5	5	5	10	-	10

Example 4.1.5. Consider the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation $y^2 - y = x^3 - x^2$. Then $\Delta = -11$. Hence E has good reduction at all primes $p \neq 11$. Through calculations, it can be shown that

The subgroup of $E(\mathbb{Q})_{\text{tors}}$ corresponding to all the non 2-torsion points embeds into $\mathbb{F}_2$. Hence $|E(\mathbb{Q})_{\text{tors}}|$ divides $2^a \cdot 5$ for some $a \geq 0$. Similarly, $|E(\mathbb{Q})_{\text{tors}}|$ divides $3^b \cdot 5$ for some $b \geq 0$. It then follows that $|E(\mathbb{Q})_{\text{tors}}|$ divides 5. Hence it is either trivial or the cyclic group of order 5. Let $T = (0,0) \in E(\mathbb{Q})$. A calculation shows that $5T = \mathcal{O}_E$ so that, indeed, $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$.

Example 4.1.6. Consider the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation $y^2 + y = x^3 + x^2$. Then $\Delta = -43$. Hence E has good reduction at all primes $p \neq 11$. Through calculations, it can be shown that

p	2	3	5	7	11	13
$\lvert\widetilde{E}(\mathbb{F}_p)\rvert$	5	6	10	8	9	19

The subgroup of $E(\mathbb{Q})_{\text{tors}}$ corresponding to all the non 2-torsion points embeds into $\mathbb{F}_2$. Hence $|E(\mathbb{Q})_{\text{tors}}|$ divides $2^a \cdot 5$ for some $a \geq 0$. Similarly, $|E(\mathbb{Q})_{\text{tors}}|$ divides $11^b \cdot 9$ for some $b \geq 0$. But then it is clear that $E(\mathbb{Q})_{\text{tors}} = 0$. Hence $T = (0,0) \in E(\mathbb{Q})$ has infinite order whence $\text{rank}(E(\mathbb{Q})) \geq 1$.

Example 4.1.7. Consider the elliptic curve $E_D/\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 - D^2x$ for some square-free $D \in \mathbb{Z}$. Then $\Delta = 2^6D^6$. Since the Weierstrass equation is in Legendre form, the 2-torsion is given by roots of the cubic:

$$E_D(\mathbb{Q})[2] = \{\, 0, (0,0), (\pm D, 0) \,\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Define $f(X) = X^3 - D^2X$ and suppose that $p \nmid 2D$. Then

$$|\widetilde{E_D}(\mathbb{F}_p)| = 1 + \left(\sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right) + 1 \right)$$

where the term of the summation is the Legendre symbol plus 1 (which accounts for the -1 in the definition and the fact that if f(X) is a square then its a square in 2 ways). Now, $f(X)$ is odd. If $p \equiv 3 \pmod 4$ then

$$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{f(x)}{p} \right) = -\left(\frac{f(x)}{p} \right)$$

Hence the Legendre symbols all cancel out and we are left with $|\widetilde{E_D}(\mathbb{F}_p)| = p + 1$. Now let $m = |E_D(\mathbb{Q})_{\text{tors}}|$. Then $4 \mid m \mid p + 1$ for all sufficiently large primes p with $p \equiv 3 \pmod 4$. We claim that $8 \nmid m$. Suppose that it does and consider the sequence $\{\, 8n + 3 \,\}_{n \in \mathbb{N}}$. If $8n+3$

were prime for some n then it would be congruent to 3 (mod 4). Hence for sufficiently large n, we would have that $8 \mid m \mid 8n+4$ which is absurd. Thus $8n+3$ is not prime for any $n \in \mathbb{N}$. But this contradicts Dirichlet's Theorem on Primes in Arithmetic Progressions. Therefore we must have $8 \nmid m$. Hence $m = 4$ and we see that $E_D(\mathbb{Q})_{\text{tors}} = (\mathbb{Z}/2\mathbb{Z})^2$. Then

$$\text{rank}(E_D(\mathbb{Q})) \geq 1 \iff \exists\, x, y \in \mathbb{Q}, y^2 = x^3 - D^2 x \iff D \text{ is congruent}$$

4.2 Criterion of Lutz-Nagell

Lemma 4.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass Equation with $a_1, \ldots, a_6 \in \mathbb{Z}$. Let $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$. Then*

1. *$4x, 8y \in \mathbb{Z}$.*
2. *If $2 \mid a_1$ or $2T \neq 0$ then $x, y \in \mathbb{Z}$.*

Proof. Fix a prime p and consider

$$E_r(\mathbb{Q}_p) = \widehat{E}(p^r\mathbb{Z}_p) = \{\, (x, y) \in E(\mathbb{Q}_p) \mid v_p(x) \leq -2r, v_p(y) \leq -3r \,\} \cup \{\, 0 \,\}$$

By Lemma 3.2.2, we see that

$$E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p) = \{\, (x, y) \in E(\mathbb{Q}_p \mid v_p(x) \geq 0, v_p(y) \geq 0 \,\}$$
$$E_r(\mathbb{Q}_p) \setminus E_{r-1}(\mathbb{Q}_p) = \{\, (x, y) \in E_r(\mathbb{Q}_p \mid v_p(x) \geq -2r, v_p(y) \geq -3r \,\}$$

Moreover,

$$\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_{p,})$$

for $r > \frac{1}{p-1}$. This implies that $\widehat{E}(4\mathbb{Z}_2)$ and $\widehat{E}(p\mathbb{Z}_p)$ are torsion free for all odd p. We must therefore have that $v_2(x) \geq -2$, $v_2(y) \geq -3$, $v_p(x) \geq 0$ and $v_p(y) \geq 0$. This implies that $4x, 8y \in \mathbb{Z}$ as claimed.

To prove the second claim, suppose that $T \in \widehat{E}(2\mathbb{Z}_2)$. Recall that

$$\widehat{E}(2\mathbb{Z}_2)\big/\widehat{E}(4\mathbb{Z}_2) \cong \mathbb{F}_2$$

Since $\widehat{E}(4\mathbb{Z}_2)$ is torsion free, it follows that the class of T, $[T]$, maps to 1 under this isomorphism. But then $2[T] = 0$ and so $2T \in \widehat{E}(4\mathbb{Z}_2)$. Since the latter is torsion free, we must have that $2T = 0$. Hence

$$(x, y) = T = -T = (x, -y - a_1x - a_3)$$

Equating the second coordinates, we have that $2y+a_1x+a_3 = 0$. Since $T \in \widehat{E}(2\mathbb{Z}_2)\setminus\widehat{E}(4\mathbb{Z}_2)$, we necessarily have that $v_2(x) = -2$ and $v_2(y) = -3$. Multiplying the equation by 4, we then have $8y + a_1(4x) + 4a_3 = 0$. Then $8y$ and $4x$ are necessarily odd and $4a_3$ is necessarily even. It then follows that a_1 must be odd.

Hence if T is not a 2-torsion point or if a_1 is even, we derive a contradiction. This forces $T \notin \widehat{E}(2\mathbb{Z}_2)$ whence $x, y \in \mathbb{Z}$. □

Theorem 4.2.2 (Lutz-Nagell)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{Z}$. Let $\mathcal{O}_E \neq T \in E(\mathbb{Q})_{\text{tors}}$, say $T = (x, y)$. Then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2 \mid \Delta$.*

Proof. First suppose that T is a 2-torsion point. Then $y = 0$ since the Weierstrass equation is in Legendre form. Now suppose that $0 \neq 2T = (x_2, y_2)$. By Lemma 4.2.1, $x_2, y_2 \in \mathbb{Z}$. Write $f(X) = X^3 + aX + b$. Using the explicit addition law (and the fact that we are adding the same point to itself so we need to make use of the tangent line at T), we have

$$x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$$

Since everything is an integer, we necessarily have that $y \mid f'(x)$. Now, E is non-singular so that $f(X)$ and $f'(X)$ are coprime. Clearly, then, $f(X)$ and $f'(X)^2$ are coprime so there exists $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. A clever guess (or a lengthy calculation) explicitly yields

$$\frac{3x^2 + 4a}{4a^3 + 27b^2} f'(X)^2 - \frac{27(X^3 + aX - b)}{4a^3 + 27b^2} f(X) = 1$$

so that

$$(3x^2 + 4a)f'(X)^2 - 27(X^3 + aX - b)f(X) = 4a^3 + 27b^2$$

Since $y^2 = f(x)$ and $y \mid f'(x)$, it then follows that $y^2 \mid 4a^3 + 27b^2$ as claimed. □

Remark. Mazur showed that the torsion group is one of the following

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if } 1 \leq n \leq 12, n \neq 1 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & \text{if } 1 \leq n \leq 4 \end{cases}$$

5 Kummer Theory

5.1 Kummer Extensions

Let K be a field such that $\text{char}(K) \nmid n$. Let μ_n be the group of n^{th} roots of unity in $\overline{K}$ and suppose that $\mu_n \subseteq K$.

Lemma 5.1.1. *Let $\Delta \subseteq K^\times/(K^\times)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$. Then L/K is Galois and $\text{Gal}(L/K) \cong \text{Hom}(\Delta, \mu_n)$.*

Proof. Since $\mu_n \subseteq K$, it follows that L is normal. Since $\text{char}(K) \nmid n$, L is also separable so that L is Galois. Now define the so-called **Kummer pairing**

$$\begin{aligned} \langle \cdot, \cdot \rangle : \text{Gal}(L/K) \times \Delta &\to \mu_n \\ (\sigma, x) &\mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \end{aligned}$$

We first check that this is well-defined. In other words, $\langle \cdot, \cdot \rangle$ does not depend on the chosen n^{th} root of x. Suppose that $\alpha^n = \beta^n = x$. Then $(\alpha/\beta)^n = 1$ so that $\alpha/\beta \in \mu_n \subseteq K$. It then follows that $\sigma(\alpha/\beta) = \alpha/\beta$ for all $\sigma \in \text{Gal}(L/K)$ so that $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$ for all $\sigma \in \text{Gal}(L/K)$.

We next show that $\langle \cdot, \cdot \rangle$ is bilinear. Indeed, we have

$$\langle \sigma\tau, x \rangle = \frac{(\sigma\tau)(\sqrt[n]{x})}{\sqrt[n]{x}} = \frac{(\sigma\tau)(\sqrt[n]{x})}{\tau(\sqrt[n]{x})} \frac{\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle$$

where we have used the fact that $\tau(\sqrt[n]{x})$ is another n^{th} root of x. Moreover,

$$\langle \sigma, xy \rangle = \frac{\sigma(\sqrt[n]{xy})}{\sqrt[n]{xy}} = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \frac{\sigma(\sqrt[n]{y})}{\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, y \rangle$$

We now claim that $\langle \cdot, \cdot \rangle$ is non-degenerate. We first check non-degeneracy in the first argument. Fix $\sigma \in \mathrm{Gal}(L/K)$. Then

$$\begin{aligned} \langle \sigma, x \rangle = 1 \text{ for all } x \in \Delta &\implies \sigma(\sqrt[n]{x}) = \sqrt[n]{x} \text{ for all } x \in \Delta \\ &\implies \sigma \text{ fixes } L \\ &\implies \sigma = 1 \end{aligned}$$

We now check non-degeneracy in the second argument. Fix $x \in \Delta$. Then

$$\begin{aligned} \langle \sigma, x \rangle = 1 \text{ for all } \sigma \in \mathrm{Gal}(L/K) &\implies \sigma(\sqrt[n]{x}) = \sqrt[n]{x} \text{ for all } \sigma \in \mathrm{Gal}(L/K) \\ &\implies \sqrt[n]{x} \in K \\ &\implies x \in (K^\times)^n \end{aligned}$$

The Kummer pairing induces group homomorphisms

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \mathrm{Hom}(\Delta, \mu_n) \\ \Delta &\to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \end{aligned}$$

which are injections by non-degeneracy. Viewing $\mathrm{Hom}(\Delta, \mu_n)$ as the dual to Δ, it is an abelian group of exponent dividing n whence $\mathrm{Gal}(L/K)$ is as well. Moreover this injections imply that

$$|\operatorname{Gal}(L/K)| \leq |\Delta| \leq |\operatorname{Gal}(L/K)|$$

Hence the above injections are in fact isomorphisms and $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$ as claimed. □

Theorem 5.1.2. *There is a one-to-one correspondence*

$$\begin{gathered} \left\{ \begin{array}{c} \textit{finite subgroups of} \\ K^\times/(K^\times)^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite abelian extensions} \\ \textit{of exponent dividing } n \end{array} \right\} \\ \Delta \longmapsto K(\sqrt[n]{\Delta}) \\ \frac{(L^\times)^n \cap K^\times}{(K^\times)^n} \longleftarrow\!\shortmid L \end{gathered}$$

Proof. Fix an abelian extension L/K of exponent dividing n. Define

$$\Delta = \frac{(L^\times)^n \cap K^\times}{(K^\times)^n}$$

Then, clearly, $K(\sqrt[n]{\Delta}) \subseteq L$. We need to show that they are in fact equal. Let $G = \mathrm{Gal}(L/K)$. Then the Kummer pairing induces an injection

$$\phi : \Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$$

We claim that ϕ is surjective. To this end, fix a group homomorphism $\chi : G \to \mu_n$. Since distinct automorphisms are linearly independent, there must exist $a \in L$ such that

$$y = \sum_{\tau \in G} \chi(\tau)^{-1} \tau(a) \neq 0$$

Now fix $\sigma \in G$. Then

$$\begin{aligned}
\sigma(y) &= \sum_{\tau \in G} \chi(\tau)^{-1} \sigma\tau(a) \\
&= \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1} \tau(a) \\
&= \sum_{\tau \in G} \chi(\sigma^{-1})^{-1} \chi(\tau)^{-1} \\
&= \chi(\sigma) y
\end{aligned}$$

But $\chi(\sigma)$ is an n^{th} root of unity so we must have that $\sigma(y^n) = y^n$ for all $\sigma \in G$. Set $x = y^n$. Then $x \in K^\times \cap (L^\times)^n$ so $x \in \Delta$ and is a prieimage of χ under ϕ. Hence ϕ is surjective as claimed.

We thus have that $|\Delta| \cong \mathrm{Hom}(G, \mu_n)$ so that $|\Delta| = |G|$. By Lemma 5.1.1 we then have that

$$[K(\sqrt[n]{\Delta}) : K] = |\Delta| = |G| = [L : K]$$

and so $L = K(\sqrt[n]{\Delta})$. It remains to show that if $\Delta \subseteq \frac{(K^\times}{K^\times)}$ and

$$\Delta' = \frac{(L^\times)^n \cap K^\times}{(K^\times)^n}$$

then $\Delta = \Delta'$. It is clear that $\Delta \subseteq \Delta'$ so that $L = K^\times(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'}) \subseteq L$. Lemma 5.1.1 then implies that $|\Delta| = |\Delta'|$ so that $\Delta = \Delta'$. □

Lemma 5.1.3. *Let K be a number field and S a finite set of primes of K, $n \geq 2$. Then the set*

$$K(S, n) = \left\{ x \in {K^\times}/{(K^\times)^n} \;\middle|\; v_\mathfrak{p}(x) \equiv 0 \pmod{n} \text{ for all } \mathfrak{p} \notin S \right\}$$

is finite.

Proof. Consider the group homomorphism

$$\begin{aligned}
K(S, n) &\to \left({\mathbb{Z}}/{n\mathbb{Z}}\right)^{|S|} \\
x &\mapsto (v_\mathfrak{p}(x))_{\mathfrak{p} \in S}
\end{aligned}$$

This clearly has kernel $K(\varnothing, n)$. If we can show that $K(\varnothing, n)$ is finite then this will imply that $K(S, n)$ is finite since the codomain of the above homomorphism is finite.

Let $x \in K^\times$ represent an element of $K(\varnothing, n)$. Then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a}$ of K. We then have an exact sequence

$$0 \longrightarrow {(\mathcal{O}_K)^\times}/{(\mathcal{O}_K^\times)^n} \longrightarrow K(\varnothing, n) \longrightarrow \mathcal{C}_K[n] \longrightarrow 0$$

$$x \longmapsto [\mathfrak{a}]$$

where $\mathcal{C}_K$ is the ideal class group of K which is finite. Moreover, Dirichlet's Unit Theorem implies that $\mathcal{O}_K^\times$ is finitely generated so we must have that $K(\varnothing, n)$ is finite. □

Proposition 5.1.4. *Let K be a number field such that $\mu_n \subseteq K$. Let S be a a finite set of primes of K. Then there are only finitely many abelian extensions L/K of exponent dividing n that are unramified at all primes $\mathfrak{p} \notin S$.*

Proof. Fix an abelian extension L/K of exponent n, unramified at all primes $\mathfrak{p} \notin S$. By Theorem 5.1.2, $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subseteq K^\times/(K^\times)^n$. Let $\mathfrak{p}$ be a prime of K and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

its unique factorisation into prime ideals in $\mathcal{O}_L$. If $x \in K^\times$ represents an element of Δ then

$$n v_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$$

Now if $\mathfrak{p} \notin S$ then all the e_i are 1 so that $v_{\mathfrak{p}(x)} \equiv 0 \pmod{n}$ for all $x \in K^\times$. Lemma 5.1.3 then implies that there are only finitely many such extensions L. □

6 The Mordell-Weil Theorem

6.1 The Weak Mordell-Weil Theorem

Lemma 6.1.1. *Let K be a field and E/K an elliptic curve. If L/K is a finite Galois extension then the natural map induced by the inclusion*

$$\phi : E(K)/nE(K) \to E(L)/nE(L)$$

has finite kernel.

Proof. Let $P \in E(K)$ represent an element of the kernel of the above mapping. Then $P = nQ$ for some $Q \in E(L)$. Given $\sigma \in \mathrm{Gal}(L/K)$ we have

$$n(\sigma(Q) - Q) = \sigma(P) - P = 0$$

so that $\sigma(Q) - Q \in E[n]$. Now consider the map

$$\begin{aligned} \mathrm{Gal}(L/K) &\to E[n] \\ \sigma &\mapsto \sigma(Q) - Q \end{aligned}$$

Since both $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, there are only finitely many possibilities for this map.

Now suppose that $P_1, P_2 \in E(K)$ with $nQ_i = P_i$ for some $Q_i \in E(L)$. If $\sigma(Q_1) - Q_1 = \sigma(Q_2) - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma(Q_1 - Q_2) = Q_1 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$ and so $Q_1 - Q_2 \in E(K)$ whence $P_1 - P_2 \in nE(K)$. □

Theorem 6.1.2 (Weak Mordell-Weil Theorem)**.** *Let K be a number field and E/K an elliptic curve. If $n \geq 2$ then $E(K)/nE(K)$ is finite.*

Proof. By Lemma 6.1.1 we may assume, without loss of generality, that $\mu_n \subseteq K$ and $E[n] \subseteq E(K)$. Let S be the set of all primes of bad reduction for E together with all primes of K dividing n. For each $P \in E(K)$, the extension $K([n]^{-1}P)/K$ is unramified at all primes outside of S by Theorem 3.2.18. Fix $Q \in [n]^{-1}P$. Note that

$$[n]^{-1}P = \{\, Q + T \mid T \in E[n] \,\}$$

But $E[n] \subseteq E(K)$ so we have that $K(Q) = K([n]^{-1}P)$ which is a Galois extension. We claim that $\mathrm{Gal}(L/K)$ injects into $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ via the map

$$\begin{aligned} \phi : \mathrm{Gal}(K(Q)/K) &\to E[n] \\ \sigma &\mapsto \sigma(Q) - Q \end{aligned}$$

We must first show that this is a group homomorphism. Indeed, we have

$$(\sigma\tau)(Q) - Q = \sigma(\tau(Q) - Q) + \sigma(Q) - Q = \tau(Q) - Q + \sigma(Q) - Q$$

To see that it is injective, suppose that $\sigma(Q) - Q = 0$. Then σ fixes $K(Q)$ pointwise whence $\sigma = 1$.

We thus see that $K(Q)/K$ is an abelian extension of exponent dividing n and unramified outside of S. Proposition 5.1.4 then implies that there are only finitely many possibilities for $K(Q)$. Let L be the compositum (inside $\bar{K}$) of all these extensions. Then L/K is finite and Galois and the natural map

$$E(K)/nE(K) \to E(L)/nE(L)$$

is the zero map since every $P \in E(K)$ is $nQ = P$ for some $Q \in E(L)$. Lemma 6.1.1 then implies that $E(K)/nE(K)$ is finite. □

Remark. If $K = \mathbb{R}, \mathbb{C}$ or a finite extension of $\mathbb{Q}_p$ then $E(K)/nE(K)$ is finite but $E(K)$ is not finitely generated (indeed, it is uncountable).

6.2 Heights

For simplicity, we assume that $K = \mathbb{Q}$.

Definition 6.2.1. We define a function

$$\begin{aligned} H : \mathbb{P}^n(\mathbb{Q}) &\to \mathbb{Z} \\ P &\mapsto \max_{0 \le i \le n} |a_i| \end{aligned}$$

where $P = [a_0 : a_1 : \cdots : a_n]$ is a representative of P satisfying $a_i \in \mathbb{Z}$ and $\gcd_i(a_i) = 1$.

Lemma 6.2.2. *Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogeneous polynomials of degree d. Define the function*

$$\begin{aligned} F : \mathbb{P}^1(\mathbb{Q}) &\to \mathbb{P}^1(\mathbb{Q}) \\ (x_1 : x_2) &\mapsto (f_1(x_1, x_2) : f_2(x_1, x_2)) \end{aligned}$$

Then there exists $C_1, C_2 > 0$ such that

$$C_1 H(P)^d \le H(F(P)) \le C_2 H(P)^d$$

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

Proof. Without loss of generality, we may assume that $f_1, f_2 \in \mathbb{Z}$. We first exhibit an upper bound. Write $P = [a : b]$ with $a, b \in \mathbb{Z}$ coprime. Then

$$H(F(P)) \leq \max\{|f_1(a,b)|, |f_2(a,b)|\} \leq C_2 \max\{|a|^d, |b|^d\}$$

where C_2 is the maximum over i of the sum of the absolute values of the coefficients of f_i.

We now exhibit the lower bound. We claim that there exist homogeneous polynomials $g_{ij} \in \mathbb{Z}[X_1, X_2]$ of degree $d-1$ and an integer $k > 0$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = k X_i^{2d-1}$$

Indeed, applying Euclid's algorithm to $f_1(X, 1)$ and $f_2(X, 1)$ yield polynomials $r, s \in \mathbb{Q}[X]$ of degree striclty less than d such that

$$r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1$$

since $f_1(X, 1)$ and $f_2(X, 1)$ are coprime. Homogenising and clearing denominators gives the desired equation with $i = 2$. We can repeat this argument for $i = 1$ to get the desired g_{ij}.

Now write $P = [a_1 : a_2]$ with $a_1, a_2 \in \mathbb{Z}$ coprime. Then the above argument gives

$$\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = k a_i^{2d-1}$$

for $i = 1, 2$. Then $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(k a_1^{2d-1}, k a_2^{2d-1}) = k$. But we also have

$$|k a_i^{2d-1}| \leq \max_{j=1,2}(|f_j(a_1, a_2)|) \sum_{j=1}^{2} |g_{ij}(a_1, a_2)|$$

Trivially, $\max_{j=1,2}(|f_j(a_1, a_2)| \leq k H(F(P))$. Moreover, $\sum_{j=1}^{2} |g_{ij}(a_1, a_2)| \leq \gamma_i H(P)^{d-1}$ where γ_i is the sum over j of the absolute values of the coefficients of g_{ij}. Hence

$$|a_i|^{2d-1} \leq \gamma_i H(F(P) H(P)^{d-1}$$

so that

$$H(P)^{2d-1} \leq \max\{\gamma_1, \gamma_2\} H(F(P)) H(P)^{d-1}$$

whence

$$\frac{1}{\max\{\gamma_1, \gamma_2\}} H(P)^d \leq H(F(P))$$

□

Remark. Given $x \in \mathbb{Q}$, let $H(x) := H(x : 1)$.

Definition 6.2.3. Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. We define the **height** on E to be the function

$$\begin{aligned} H : E(\mathbb{Q}) &\to \mathbb{R}_{\geq 1} \\ P &\mapsto \begin{cases} H(x) & \text{if } P = (x, y) \\ 1 & \text{if } P = \mathcal{O}_E \end{cases} \end{aligned}$$

Moreover, we define the **logarithmic height** to be the function

$$\begin{aligned} h : E(\mathbb{Q}) &\to \mathbb{R}_{>0} \\ P &\mapsto \log H(P) \end{aligned}$$

Lemma 6.2.4. *Let E and E' be elliptic curves over $\mathbb{Q}$ and $\phi : E_1 \to E_2$ an isogeny defined over $\mathbb{Q}$. Then there exists a constant $C > 0$ such that*

$$|h(\phi(P)) - (\deg \phi)h(P)| \leq C$$

for all $P \in E(\mathbb{Q})$.

Proof. By Lemma 2.4.8 we have a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle x_1} & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1_K & \xrightarrow{\xi} & \mathbb{P}^1_K \end{array}$$

such that $\deg \phi = \deg \xi = d$, say. By Lemma 6.2.2, there exists constants $C_1, C_2 > 0$ such that

$$C_1 H(P)^d \leq H(\phi(P)) \leq C_2 H(P)^d$$

Taking logarithms across this inequality yields

$$|h(\phi(P)) - dh(p)| \leq \max\{\log(c_2), -\log(c_1)\}$$

as desired. □

Example 6.2.5. $\phi = [2] : E \to E$. Then there exists $c > 0$ such that

$$|h(2P) - 4h(P)| \leq C$$

for all $P \in E(\mathbb{Q})$.

Proposition 6.2.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Then the function*

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

*is well-defined and called the **canonical height** on E.*

Proof. We need to show that this limit actually exists. We shall thus show that for all $P \in E(\mathbb{Q})$, the sequence $\left\{ \frac{1}{4^n} h(2^n P) \right\}_{n\in\mathbb{N}}$ is Cauchy in $\mathbb{R}$. To this end, fix $m \geq n$. Then

$$\begin{aligned} \left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| &\leq \sum_{r=n}^{m+1} \left| \frac{1}{4^{r+1}} h(2^m P) - \frac{1}{4^r} h(2^n P) \right| \\ &\leq \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} |h(2^{r+1} P) - 4h(2^r P)| \end{aligned}$$

By Lemma 6.2.4, we can bound the absolute value by some $c > 0$. So

$$\left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| \leq c \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} = \frac{c}{3 \cdot 4^n}$$

which goes to 0 as $n \to \infty$. Hence the series is Cauchy and the canonical height is well-defined. □

Lemma 6.2.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $|h(P) - \widehat{h}(P)|$ is bounded for all $P \in E(\mathbb{Q})$.*

Proof. This is immediate upon setting $n = 0$ in the above proof and taking $m \to \infty$. □

Lemma 6.2.8. *Let $E/\mathbb{Q}$ be an elliptic curve. Then for all $B > 0$, the set*

$$\{ P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq B \}$$

is finite

Proof. If $\widehat{h}(P)$ is bounded then so is $h(P)$. Then there are only finitely many possibilities for the x-coordinate of P. Moreover, given any x, there is at most 2 values of y such that $(x, y) \in E(\mathbb{Q})$ so there can only be finitely many such P. □

Lemma 6.2.9. *Let $\phi : E \to E'$ be an isogeny of elliptic curves defined over $\mathbb{Q}$. Then*

$$\widehat{h}(\phi(P)) = (\deg \phi)\widehat{h}(P)$$

for all $P \in \mathbb{Q}$.

Proof. By Lemma 6.2.4, there exists a constant $c > 0$ such that

$$|h(\phi(P)) - (\deg \phi)h(P)| < c$$

We can replace P by $2^n P$ and divide through by 4^n to get

$$\left| \frac{1}{4^n} h(2^n \phi(P)) - \frac{\deg \phi}{4^n} h(2^n P) \right| < \frac{c}{4^n}$$

Passing to the limit $n \to \infty$ yields the assertion of the Lemma. □

Remark. The above Lemma shows that the canonical height is independent of the choice of Weierstrass equation (two Weierstrass models are isomorphic so the isogeny between them has degree 1). Moreover, taking $\phi = [n]$ shows that $\widehat{h}(nP) = n^2 \widehat{h}(P)$.

Lemma 6.2.10. *Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists $C > 0$ such that*

$$H(P + Q)H(P - Q) \leq CH(P)^2 H(Q)^2$$

for all $P, Q \in E(\mathbb{Q})$ with $P + Q, P - Q, P, Q \neq \mathcal{O}_E$.

Proof. Let E have Weierstrass equation

$$y^2 = x^3 + ax + b$$

Let $x_1, \ldots, x_4$ be the x-coordinates of $P, Q, P + Q, P - Q$ respectively. By Lemma 2.4.12, there exist polynomials $w_0, w_1, w_2 \in \mathbb{Z}[x_1, x_2]$ of degree at most 2 in x_1 and degree at most 2 in x_2 such that we have an equality of ratios

$$(1 : x_3 - x_4 : x_3 x_4) = (w_0 : w_1 : w_2)$$

Write $x_i = r_i/s_i$ for $r_i, s_i \in \mathbb{Z}$ coprime. Then

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = ((r_1 s_2 - r_2 s_2)^2 : \cdots : \ldots)$$

Note that $\gcd(s_1 s_4, r_3 s_4 - r_4 s_3, r_3 r_4) = 1$. Then

$$\begin{aligned} H(P + Q)H(P - Q) &= \max\{|r_3|, |s_3|\} \max\{|r_4|, |s_4|\} \\ &\leq 2 \max\{|s_3 s_4|, |r_3 s_4 + r_4 s_3|, |r_3 r_4|\} \\ &\leq CH(P)^2 H(Q)^2 \end{aligned}$$

for some constant C depending on E but not on P or Q. □

Theorem 6.2.11. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is a quadratic form.*

Proof. By Lemma 6.2.10, there exists a constant $C > 0$ such that

$$H(P+Q)H(P-Q) \leq CH(P)^2H(Q)^2$$

for all $P, Q \in E(\mathbb{Q})$ such that $P, Q, P+Q, P-Q \neq \mathcal{O}_E$. Taking the logarithm across this inequality yields

$$h(P+Q) + h(P-Q) \leq c' + 2h(P) + 2h(Q)$$

for some constant $c' > 0$ and for all $P, Q \in E(\mathbb{Q})$ such that $P, Q, P+Q, P-Q \neq \mathcal{O}_E$. Now, if P or Q are $\mathcal{O}_E$ then we trivially have such a bound. If $P - Q = \mathcal{O}_E$ then $P = Q$ and so the fact that $|h(2P) - 4h(P)|$ is bounded also ensures that we have such a bound in this case. The case where $P + Q = \mathcal{O}_E$ is similar (since the x coordinates of inverses are the same).

Replacing P and Q by 2^nP and 2^nQ, dividing through by 4^n and then passing to the limit $n \to \infty$ then gives

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

Replacing P, Q with $P+Q$ and $P-Q$ and using the fact that $\widehat{h}(2P) = 4\widehat{h}(P)$ yields

$$4\widehat{h}(P) + 4\widehat{Q}) \leq 2\widehat{h}(P+Q) + 2\widehat{h}(P-Q)$$

so that $\widehat{h}$ satisfies the parallelogram law. Hence $\widehat{h}$ is a quadratic form. □

Remark. Let K be a number field and $P = [a_0 : \cdots : a_n] \in \mathbb{P}^n(K)$. We define $H(P) = \prod_{\mathfrak{p}} \max_{0 \leq i \leq n} |a_i|_{\mathfrak{p}}$ for the primes of K where the absolute values are normalised so that $\prod_{\mathfrak{p}} |x|_{\mathfrak{p}}$ for all $x \in K^\times$. For $x \in K$, let $H(x) = H([x:1]) = \prod_{\mathfrak{p}} \max\{|x|_{\mathfrak{p}}, 1\}$. Then we have similar results as before for this H.

6.3 Proving the Mordell-Weil Theorem

Theorem 6.3.1 (Mordell-Weil)**.** *Let K be a number field and E/K an elliptic curve. Then $E(K)$ is a finitely generated abelian group.*

Proof. Fix an integer $n \geq 2$. By the Weak Mordell-Weil Theorem, we know that $E(K)/nE(K)$ is finite. Choose coset representatives $P_1, \ldots, P_r \in E(K)$ for this factor group. Define the set

$$\Sigma = \{\, P \in E(K) \mid \widehat{h}(P) \leq \max_{1 \leq i \leq r} \widehat{h}(P_i) \,\}$$

We claim that Σ generates $E(K)$. Suppose that Σ does not generate $E(K)$. Then there exists $P \in E(K)$ of minimal height that does not lie in the subgroup of $E(K)$ generated by Σ. Indeed fix $P \notin \langle \Sigma \rangle$. Then the set

$$\{\, Q \in E(K) \mid \widehat{h}(Q) \leq \widehat{h}(P), Q \notin \langle \Sigma \rangle \,\}$$

is finite so it has an element with minimal height. Since the P_i are coset representatives of $E(K)/nE(K)$, we must have that $P = P_i + nQ$ for some $1 \leq i \leq r$ and $Q \notin \langle \Sigma \rangle$. By the minimality of $\widehat{h}(P)$, we have that $\widehat{h}(P) \leq \widehat{h}(Q)$. Then

$$\begin{aligned} 4\widehat{h}(P) \leq 4\widehat{h}(Q) \leq n^2\widehat{h}(Q) = \widehat{h}(nQ) &= \widehat{h}(P - Pi) \\ &\leq \widehat{h}(P - P_i) + \widehat{h}(P + P_i) \\ &= 2\widehat{h}(P) + 2\widehat{h}(P_i) \end{aligned}$$

so that $\widehat{h}(P) \leq \widehat{h}(P_i)$. But then $P \in \Sigma$ which is a contradiction. Hence Σ generates $E(K)$. Now, Σ is finite which implies that $E(K)$ is finitely generated as claimed. $\square$

7 Dual Isogenies and the Weil Pairing

7.1 Dual Isogenies

Throughout this section, assume that K is a perfect field.

Proposition 7.1.1. *Let E/K be an elliptic curve and $\Phi \subseteq E(K)$ a finite $G(\bar{K}/K)$-stable subgroup. Then there exists an elliptic curve E' defined over K and a separable isogeny $\phi : E \to E'$ such that every isogeny $\psi : E \to E'$ with $\Phi \subseteq \ker \psi$ factors uniquely through ϕ.*

Proof. Proof omitted. $\square$

Proposition 7.1.2. *Let $\phi : E \to E'$ be an isogeny of elliptic curves. Then there exists a unique isogeny $\widehat{\phi} : E' \to E$ such that $\widehat{\phi}\phi = [\deg \phi]$. We refer to $\widehat{\phi}$ as the **dual isogeny**.*

Proof. We shall only prove the case where ϕ is separable. Indeed, if ϕ is separable then $|\ker \phi| = n$ so that $\ker \phi \subseteq E[n] = \ker[n]$. Applying Proposition 7.1.1 with $\psi = [n]$.

To see that $\widehat{\psi}$ is unique, suppose that ψ_1 and ψ_2 satisfy $\psi_1 \circ \phi = \psi_2 \circ \phi$. Then $(\psi_1 - \psi_2) \circ \phi = 0$ so that $\deg(\psi_1 - \psi_2)\deg(\phi) = 0$. But $\deg(\phi) \neq 0$ so $\deg(\psi_1 - \psi_2) = 0$. But then $\psi_1 = \psi_2$. $\square$

Remark.

1. $E \sim E' \iff E, E'$ are isogenous is an equivalence relation.
2. $\deg[n] = n^2 \implies \widehat{[n]} = [n]$ and so $\deg \phi = \deg \widehat{\phi}$.
3. $\phi\widehat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$ so $\phi\widehat{\phi} = [n]_{E'}$. In particular, $\widehat{\widehat{\phi}} = \phi$.
4. If $\phi : E \to E'$, $\psi : E' \to E''$ are isogenies then $\widehat{\psi\phi} = \widehat{\phi}\widehat{\psi}$.
5. If $\phi \in \mathrm{End}(E)$ then $\phi^2 - (\mathrm{tr}\,\phi)\phi + \deg \phi = 0$ so that $\widehat{\phi} = (\mathrm{tr}\,\phi) - \phi$ whence $\mathrm{tr}(\phi) = \phi + \widehat{\phi}$.

Lemma 7.1.3. *Let E and E' be elliptic curves and $\phi, \psi \in \mathrm{Hom}(E, E')$. Then*

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$$

Proof. First suppose that $E = E'$. Then

$$\phi + \psi + \widehat{\phi + \psi} = \mathrm{tr}(\phi + \psi) = \mathrm{tr}\,\phi + \mathrm{tr}\,\psi = \phi + \widehat{\phi} + \psi + \widehat{\psi}$$

so that $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.

Now, for the general case, we have that

$$\widehat{\phi + \psi}\phi = \widehat{\phi}\widehat{\phi + \widehat{\phi}}\psi = \widehat{\phi}\phi + \widehat{\psi}\phi = (\widehat{\phi} + \widehat{\psi})\phi$$

whence $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$ $\square$

7.2 The Weil Pairing

Definition 7.2.1. Let E be an elliptic curve. We define a map

$$\begin{aligned} \text{sum} : \text{Div}(E) &\to E \\ \sum n_p(P) &\mapsto \sum n_p P \end{aligned}$$

Lemma 7.2.2. *Let E be an elliptic curve and $D \in \text{Div}(E)$ a divisor. Then $D \sim 0$ if and only if $\deg D = 0$ and $\text{sum} D = \mathcal{O}_E$.*

Proof. Recall that we have an isomorphism

$$\begin{aligned} \phi : E &\to \text{Pic}^0(E) \\ P &\mapsto [P - 0] \end{aligned}$$

Composing this with sum, we see that $(P) - (Q) \in \text{Div}^0(E)$ maps to $P - Q$ maps to $\phi(P) - \phi(Q) = [P-0] - [Q-0] = [P-Q]$. Hence, in general, $D \in \text{Div}^0(E)$ maps to $[D]$. $\square$

We now define the **Weil pairing**. Suppose we have an isogeny of elliptic curves $\phi : E \to E'$ of degree n and assume that the base field K satisfies $\text{char}(K) \nmid n$. The Weil pairing shall be a mapping

$$e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \mu_n$$

Fix $T \in E'[\phi]$. Then $T \in \ker(\phi\widehat{\phi}) = \ker[n]$ so that $nT = \mathcal{O}_{E'}$. By Lemma 7.2.2, we then have that $n(T) - n(\mathcal{O}_{E'}) \sim 0$ so that $n(T) \sim n(\mathcal{O}_{E'})$. By definition of this equivalence relation, we can find $f \in \overline{K}(E')^\times$ such that $\text{div}(f) = n(T) - n(\mathcal{O}_{E'})$.

Now choose $T_0 \in E(\overline{K})$ such that $\phi(T_0) = T$. Then

$$\begin{aligned} \phi^*(T) - \phi^*(\mathcal{O}_{E'}) &= \sum_{P \in \phi^{-1}(T)} e_\phi(P)(P) - \sum_{P \in \phi^{-1}(T)} e_\phi(P)(\mathcal{O}_E) \\ &= \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P) \end{aligned}$$

where we have used the fact that isogenies do not ramify. Since $|E[\phi]| = \deg \phi = n$, the above divisor has sum

$$nT_0 = \widehat{\phi}\phi(T_0) = \widehat{\phi}(T) = 0$$

So appealing to Lemma 7.2.2 once more shows that there exists $g \in \overline{K}(E)^\times$ such that $\text{div}(g) = \phi^*(T) - \phi^*(\mathcal{O}_E)$. Now,

$$\text{div}(\phi^* f) = \phi^*(\text{div}(f)) = n(\phi^*(T) - \phi^*(\mathcal{O}_{E'})) = \text{div}(g^n)$$

Since any two rational functions with the same divisor are the same up to a constant, we have $\phi^* f = c g^n$ for some $c \in \overline{K}^\times$. After rescaling f, we may assume that $c = 1$ so that $\phi^* f = g^n$.

Now fix $S \in E[\phi]$. Then

$$\begin{aligned} \text{div}(\tau_S^* g) &= \tau_S^* \text{div}(g) \\ &= \tau_S^* (\phi^*(T) - \phi^*(\mathcal{O}_E)) \\ &= (\phi \circ \tau_S)^*(T) - (\phi \circ \tau_S)^*(\mathcal{O}_E) \\ &= \phi^*(T) - \phi^*(\mathcal{O}_E) \\ &= \text{div}(g) \end{aligned}$$

Hence there exists $\zeta \in \overline{K}^\times$ such that $\tau_S^*(g) = g$. In other words,

$$\zeta = \frac{g(X+S)}{g(X)}$$

independently of the choice of $X \in E(K)$. Since $S \in E[\phi]$, we then have

$$\zeta^n = \frac{g(X+S)^n}{g(X)^n} = \frac{f(\phi(X+S))}{f(\phi(X))} = \frac{f(\phi(X))}{f(\phi(X))} = 1$$

We then define

$$e_\phi(S,T) = \frac{g(X+S)}{g(X)}$$

Proposition 7.2.3. *Let $\phi : E \to E'$ be an isogeny of elliptic curves of degree n. Then e_ϕ is bilinear and non-degenerate.*

Proof. We first check linearity in the first argument. We have

$$\begin{aligned} e_\phi(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X+S_2)}\frac{g(X+S_2)}{g(X)} \\ &= e_\phi(S_1,T) + e_\phi(S_2,T) \end{aligned}$$

We next check linearity in the second argument. To this end, fix $T_1, T_2 \in E'[\widehat{\phi}]$. Then we can find $f_1, f_2 \in \overline{K}(E')^\times$ such that $\mathrm{div}(f_1) = n(T_1) - n(\mathcal{O}_{E'})$ and $\mathrm{div}(f_2) = n(T_2) - n(\mathcal{O}_{E'})$. Moreover, we can find $g_1, g_2 \in \overline{K}(E')^\times$ such that $\phi^* f_1 = g_1^n$ and $\phi^* f_2 = g_2^n$. By Lemma 7.2.2, there exists $h \in \overline{K}(E')$ such that

$$\mathrm{div}(h) = (T_1) + (T_2) - (T_1+T_2) - (0_{\mathcal{E}'})$$

Now define

$$f = \frac{f_1 f_2}{h^n}, g = \frac{g_1 g_2}{\phi^* h}$$

We have that

$$\begin{aligned} \mathrm{div}(f) &= \mathrm{div}(f_1) + \mathrm{div}(f_2) - n\mathrm{div}(h) \\ &= n(T_1) - n(\mathcal{O}_{E'}) + n(T_2) - n(\mathcal{O}_{E'}) - n(T_1) - n(T_2) \\ &\quad + n(T_1+T_2) + n(\mathcal{O}_{E'}) \\ &= n(T_1+T_2) - n(\mathcal{O}_{E'}) \end{aligned}$$

Moreover

$$\phi^* f = \frac{\phi^* f_1 \phi^* f_2}{(\phi^* h)^n} = \left(\frac{g_1 g_2}{\phi^* h}\right)^n = g^n$$

So that

$$e_\phi(S, T_1+T_2) = \frac{g(X+S)}{g(X)} = \frac{g_1(X+S)g_2(X+S)}{g_1(X)g_2(X)}\frac{h(\phi(X))}{h(\phi(X+S))} = e_\phi(S,T_1)e_\phi(S,T_2)$$

We first check non-degeneracy on the left. To this end, fix $T \in E'[\widehat{\phi}]$ and suppose that $e_\phi(S,T) = 1$ for all $S \in E[\phi]$. We need to show that $T = \mathcal{O}_E$. We have that $g(X+S) = g(X)$

for all $S \in E[\phi]$ and $X \in E(\overline{K})$. This implies that $\tau_S^* g = g$ for all $S \in E[\phi]$. Note that we have a Galois extension $\overline{K}(E)/\phi^*\overline{K}(E')$ with Galois group $E[\phi]$ which acts on $\overline{K}(E)$ as τ_S^*. Since $\tau_S^* g = g$ for all S, it follows by Galois Theory that $g \in \phi^*\overline{K}(E')$ so $g = \phi^* h$ for some $h \in \overline{K}(E')$. So then $\phi^* f = g^n = \phi^* h^n$ whence $f = h^n$. We must therefore have that $\mathrm{div}(h) = (T) - (\mathcal{O}_E)$ and so, forcibly, $T = \mathcal{O}_E$.

We have shown that there exists an injection

$$\begin{aligned} E'[\widehat{\phi}] &\hookrightarrow \mathrm{Hom}(E[\phi], \mu_n) \\ T &\mapsto e_\phi(\cdot, T) \end{aligned}$$

But, $|E[\phi]| = |E[\widehat{\phi}]| = n$. Hence the above injection must be an isomorphism. We then immediately have non-degeneracy on the right by group-theoretic considerations. □

Proposition 7.2.4. *Let $\phi : E \to E'$ be an isogeny of elliptic curves of degree n and defined over K. Then e_ϕ is $\mathrm{Gal}(\overline{K}/K)$-equivariant.*

Proof. By the definition of e_ϕ, we have that $\mathrm{div}(f) = n(T) - n(\mathcal{O}_{E'})$ and $\phi^* f = g^n$. Then $\mathrm{div}(\sigma f) = n(\sigma(T)) - n(\mathcal{O}_{E'})$ and $\phi^*(\sigma(f)) = (\sigma(g))^n$. Hence

$$\begin{aligned} e_\phi = (\sigma(S), \sigma(T)) &= \frac{(\sigma(g))(\sigma(S) + X)}{(\sigma(g))(X)} \\ &= \frac{(\sigma(g))(\sigma(S) + \sigma(X))}{(\sigma(g))(\sigma(X))} \\ &= \sigma\left(\frac{g(X+S)}{g(X)}\right) \\ &= \sigma(e_\phi(S, T)) \end{aligned}$$

□

Remark. If we take $\phi = [n]$ then we infact get a Weil pairing $e_n(S, T) \to \mu_n$ instead of μ_{n^2}. This is because all the argumentation above works with n^2 replaced by n.

Corollary 7.2.5. *Let E/K be an elliptic curve and suppose that $E[n] \subseteq E(K)$. Then $\mu_n \subseteq K$.*

Proof. Fix $S \in E[n]$ of exact order n. By the non-degeneracy of the Weil pairing, we have that there exists $e_n(S, T) = \zeta_n$ for some primitive n^{th} root of unity ζ_n. Now fix $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We have

$$\sigma(\zeta_n) = \sigma(e_n(S, T)) = e_n(\sigma(S), \sigma(T)) = e_n(S, T) = \zeta_n$$

and so $\zeta_n \in K$ whence $\mu_n \subseteq K$. □

8 Galois Cohomology

8.1 Definitions and Facts

Definition 8.1.1. Let G be a finite group. We define a ***G*-module** to be an abelian group M together with an action of G which is compatible with the group structure of A. We denote the action of $\sigma \in G$ by $m \mapsto m^\sigma$.

Definition 8.1.2. Let M be a G-module. We define the **0^{th}-cohomology group** of M to be

$$H^0(G,M) = M^G = \{\, m \in M \mid m^\sigma = m \text{ for all } \sigma \in G \,\}$$

We define the **1-cochains** of M to be

$$C^1(G,M) = \{\, f : G \to M \,\}$$

We define the **1-cocycles** of M to be

$$Z^1(G,M) = \{\, (a_\sigma)_{\sigma\in G} \mid a_\tau^\sigma = a_\sigma \text{ for all } \sigma,\tau \in G \,\}$$

We define the **1-coboundaries** of M to be

$$B^1(G,M) = \{\, (b^\sigma - b)_{\sigma\in G} \mid b \in M \,\}$$

Finally, we define the **1^{st}-cohomology group** of M to be

$$H^1(G,M) = \frac{Z^1(G,M)}{B^1(G,M)}$$

Remark. If G acts trivially on M then $H^1(G,M) = \mathrm{Hom}(G,M)$.

Theorem 8.1.3. *Every short exact sequence of G-modules*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

induces a long exact sequence of cohomology groups

$$0 \longrightarrow H^0(G,P) \xrightarrow{\phi^0} H^0(G,M) \xrightarrow{\psi^0} H(G,N) \xrightarrow{\delta} H^1(G,P) \xrightarrow{\phi^1} H^1(G,M) \xrightarrow{\psi^1} H^1(G,N)$$

*where δ is the **connecting** homomorphism defined as follows. Fix $n \in H^0(G,N)$ and choose $m \in M$ such that $\psi(m) = n$. Define the cochain $f \in C^1(G,M)$ by $f(\sigma) = m^\sigma - m$ and set $\delta(n) = [f]$.*

Proof. Proof omitted. □

Theorem 8.1.4. *Let M be a G-module and $H \triangleleft G$ a sub-group. Then M^H is naturally a G/H-module and we have a **inflation-restriction** sequence*

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

Proof. Proof omitted. □

Definition 8.1.5. Let K be a perfect field, $\mathrm{Gal}(\overline{K}/K)$ the topological group with basis of open subgroups $\mathrm{Gal}(\overline{K}/L)$ for $[L:K] < \infty$. Setting $G = \mathrm{Gal}(\overline{K}/K)$, we modify the previous definitions by insisting that the group action of G on an abelian group M induces open stabiliser subgroups of G and that the 1-cochains of M are all continuous when M is equipped with the discrete topology. All the definitions then follow through as before. In fact, we have

$$H^1(\mathrm{Gal}(\bar{K}/K),M) = \varinjlim_{L/K \text{ finite}} H^1(\mathrm{Gal}(L/K), M^{\mathrm{Gal}(\bar{K}/L)})$$

where the direct limit is taken with respect to the inflation maps.

Theorem 8.1.6 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension. Then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0$$

Proof. Fix $(m_\sigma)_{\sigma\in G} \in Z^1(G, L^\times)$ where $G = \mathrm{Gal}(L/K)$. We claim that this is infact 1-coboundary. Since distinct automorphisms are linearly independent, there exists some $y \in L$ such that

$$x = \sum_{\tau\in G} m_\tau^{-1}\tau(y) \neq 0$$

Then

$$\begin{aligned}\sigma(x) &= \sum_{\tau\in G} \sigma(m_\tau)^{-1}(\sigma\tau)(y)\\ &= m_\sigma \sum_{\tau\in G} m_{\sigma\tau}^{-1}(\sigma\tau)(y)\\ &= m_\sigma x\end{aligned}$$

so that $m_\sigma = \frac{\sigma(x)}{x}$ whence $(m_\sigma)_{\sigma\in G} \in B^1(G, L^\times)$. □

Corollary 8.1.7. *Let K be a perfect field. Then*

$$H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = 0$$

Corollary 8.1.8. *Let K be a perfect field such that* $\mathrm{char}(K) \nmid n$*. Then*

$$H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong {K^\times}\big/{(K^\times)^n}$$

Proof. Consider the short exact sequence

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{x\mapsto x^n} \overline{K}^\times \longrightarrow 0$$

This induces a long exact sequence

$$K^\times \xrightarrow{x\mapsto x^n} K^\times \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$$

But the latter is zero by Hilbert's Theorem 90 so we get an exact sequence

$$0 \longrightarrow {K^\times}\big/{(K^\times)^n} \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \longrightarrow 0$$

as desired. □

Remark. Now if $\mu_n \subseteq K$ then the action of $\mathrm{Gal}(\overline{K}/K)$ on μ_n is trivial so we get

$$\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong {K^\times}\big/{(K^\times)^n}$$

Remark. From now on, we shall use the notation $H^1(K, \cdot) := H^1(\mathrm{Gal}(\overline{K}/K, \cdot)$.

8.2 The Selmer and Tate-Shafarevich Groups

Let $\phi : E \to E'$ be a non-constant isogeny of elliptic curves over a field K. Write E for $E(\overline{K})$. Then we have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

which yields a long exact sequence of cohomology groups

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E) \xrightarrow{\phi^1} H^1(K, E')$$

Which induces a short-exact sequence

$$0 \longrightarrow E'(K)/\phi E(K) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E)[\phi] \longrightarrow 0$$

Now let K be a number field and M_K its set of primes, finite and infinite. For a given prime $\mathfrak{p}$, we fix an embedding $\overline{K} \subseteq \overline{K_\mathfrak{p}}$ so that $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}) \subseteq \mathrm{Gal}(\overline{K}/K)$. By the above results, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & \cdots\searrow & \downarrow{\scriptstyle \mathrm{res}} & & \\
0 & \longrightarrow & \prod_{\mathfrak{p}\in M_K} E'(K_\mathfrak{p})/\phi E(K_\mathfrak{p}) & \xrightarrow{\delta} & \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E[\phi]) & \longrightarrow & \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E)[\phi] & \longrightarrow & 0
\end{array}$$

Where the restriction maps are given coordinate wise by $\mathrm{res}_\mathfrak{p}$, the corresponding restriction map at the prime $\mathfrak{p}$.

Definition 8.2.1. We define the **ϕ-Selmer group** to be the kernel of the dotted homomorphism in the diagram above:

$$\begin{aligned}
S^{(\phi)}(E/K) &= \ker\left(H^1(K, E[\phi]) \to \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E)\right) \\
&= \{\, \alpha \in H^1(K, E[\phi]) \mid \mathrm{res}_\mathfrak{p}(\alpha) \in \mathrm{im}(\delta_\mathfrak{p}) \ \forall\, \mathfrak{p} \in M_K \,\}
\end{aligned}$$

Moreover, we define the **Tate-Shafarevich group** to be

$$Ш(E/K) = \ker\left(H^1(K, E) \to \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E)\right)$$

Proposition 8.2.2. *There exists an exact sequence*

$$0 \longrightarrow E'(K)/\phi E(K) \longrightarrow S^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0$$

In particular, if $S^{(\phi)}(E)$ is finite then so is $E(K)/\phi E(K)$.

Proof. Apply Snake Lemma to the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/\phi E(K) & \longrightarrow & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E)[\phi] & \xrightarrow{\sim} & \prod_{\mathfrak{p}\in M_K} H^1(K_\mathfrak{p}, E)[\phi] & \longrightarrow & 0
\end{array}$$

□

Remark. It is conjectured that the Tate-Shafarevich group is finite.

Definition 8.2.3. Let K be a number field and $S \subseteq M_K$ a finite set of primes of K containing all infinite primes. Define

$$H^1(K, M; S) = \ker\left(H^1(K, M) \to \prod_{\mathfrak{p} \notin S} H^1(K_{\mathfrak{p}}^{\mathrm{ur}}, M)\right)$$

Lemma 8.2.4. *Let K be a number field and $\phi : E \to E'$ an isogeny of elliptic curves over K. Let $S \subseteq M_K$ be the set containing all primes of bad reduction for E, all infinite primes of K and all primes dividing n. Then $S^{(\phi)}(E/K) \subseteq H^1(K, E[\phi], S)$.*

Proof. Let $n = \deg \phi$. By the proof of Theorem 3.2.18, we know that multiplication by n is surjective on $E(K_{\mathfrak{p}}^{\mathrm{ur}})$ so that the isogeny $\phi : E(K_{\mathfrak{p}}^{\mathrm{ur}}) \to E'(K_{\mathfrak{p}}^{\mathrm{ur}})$ is also surjective since $\phi\widehat{\phi} = [n]$. We then have a commutative diagram with exact rows

$$\begin{array}{ccccc} E(K_{\mathfrak{p}}) & \xrightarrow{\phi} & E'(K_{\mathfrak{p}}) & \xrightarrow{\delta_{\mathfrak{p}}} & H^1(K_{\mathfrak{p}}, E[\phi]) \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} \\ E(K_{\mathfrak{p}}^{\mathrm{ur}}) & \xrightarrow{\phi} & E'(K_{\mathfrak{p}}^{\mathrm{ur}}) & \xrightarrow{\psi} & H^1(K_{\mathfrak{p}}^{\mathrm{ur}}, E[\phi]) \end{array}$$

Now suppose that $x \in S^{(\phi)}(E/K)$. Then, in particular, $\mathrm{res}_{\mathfrak{p}}(x) \in \mathrm{im}(\delta_{\mathfrak{p}})$. But then $\mathrm{res}_{\mathfrak{p}}(x) \in \mathrm{im}(\psi) = 0$ since ϕ is surjective. This holds for arbitrary $\mathfrak{p} \notin S$ so we must therefore have that $x \in H^1(K, E[\phi]; S)$. □

Theorem 8.2.5. *Let K be a number field and $\phi : E \to E'$ an isogeny of elliptic curves over K. Then $S^{(\phi)}(E/K)$ is finite.*

Proof. By Lemma 8.2.4, it suffices to show that $H^1(K, M, S)$ is finite for any G-module M and finite set of places $S \subseteq M_K$. Let L/K be a finite Galois extension. Then we have an inflation-restriction sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), M^{\mathrm{Gal}(\overline{K}/L)}) \xrightarrow{\inf} H^1(K, M) \xrightarrow{\mathrm{res}} H^1(L, M)$$

Since $H^1(K, M; S) \subseteq H^1(K, M)$, we can replace K with any finite Galois extension L. We may thus assume, without loss of generality, that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on M. Note that $H^1(K, M_1 \times M_2) \cong H^1(K, M_1) \times H^1(K, M_2)$ so we may also assume that M is cyclic, say of order n. Finally, we can assume that $\mu_n \subseteq K$ so that $M \cong \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module. It thus suffices to show that $H^1(K, \mu_n; S)$ is finite. By Hilbert's Theorem 90, we have that $H^1(K, \mu_n) \cong K^\times/(K^\times)^n$ so then

$$H^1(K, \mu_n; S) = \ker\left(K^\times\big/(K^\times)^n \to \prod_{\mathfrak{p} \notin S} (K_{\mathfrak{p}}^{\mathrm{ur}})^\times/((K_{\mathfrak{p}}^{\mathrm{ur}})^\times)^n\right) \subseteq K(S, n)$$

which is finite by Proposition 5.1.3. □

Remark. This Theorem gives another proof of the Weak Mordell-Weil Theorem in light of the exact sequence of Proposition 8.2.2.

8.3 Descent by Cyclic Isogeny

Let $\phi : E \to E'$ be an isogeny of elliptic curves over a number field K. Suppose that $E'[\widehat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ and is generated by $T \in E'(K)$. The Weil pairing provides us with an isomorphism

$$\begin{aligned} E[\phi] &\to \mu_n \\ S &\mapsto e_\phi(S, T) \end{aligned}$$

so that $E[\phi]$ and μ_n are isomorphic as $\mathrm{Gal}(\overline{K}/K)$-modules. We thus have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

which yields a long exact sequence of cohomology groups

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \longrightarrow H^1(K, E)$$

By Hilbert's Theorem 90, we have an isomorphism

$$\begin{aligned} h : {K^\times}\big/{(K^\times)^n} &\to H^1(K, \mu_n) \\ x &\mapsto \left(\frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \right)_\sigma \end{aligned}$$

so we get a commutative diagram with exact row

$$\begin{array}{ccccccc} E(K) & \xrightarrow{\phi} & E'(K) & \xrightarrow{\delta} & H^1(K, \mu_n) & \longrightarrow & H^1(K, E) \\ & & & \searrow^{\alpha} & \downarrow{\scriptstyle h^{-1}} & & \\ & & & & {K^\times}\big/{(K^\times)^n} & & \end{array}$$

Theorem 8.3.1. *Let $f \in K(E'), g \in K(E)$ be rational functions such that $\mathrm{div}(f) = n(T) - n(\mathcal{O}_{E'})$ and $\phi^* f = g^n$. Then*

$$\alpha(P) \equiv f(P) \pmod{(K^\times)^n}$$

for all $P \in E'(K) \setminus \{ \mathcal{O}_{E'}, T \}$.

Proof. Fix $P \notin \{ \mathcal{O}_{E'}, T \}$. Since ϕ is surjective, we can choose $Q \in E(\overline{K})$ such that $\phi(Q) = P$. Then $\delta(P) \in H^1(K, \mu_n)$ is represented by the 1-cocycle $(\sigma \mapsto \sigma(Q) - Q)$. Then

$$e_\phi(\sigma(Q) - Q), T) = \frac{g(\sigma(Q) - Q + X)}{g(X)}$$

for all $X \in E(\overline{K})$ away from the zeroes and poles of g. Taking $X = Q$, we have

$$e_\phi(\sigma(Q) - Q), T) = \frac{\sigma(Q)}{g(Q)} = \frac{\sigma(g(Q))}{g(Q))} = \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}$$

It then follows that

$$\alpha(P) \equiv f(P) \pmod{(K^\times)^n}$$

□

8.4 Descent by 2-Isogeny

Let K be a number field and consdier the elliptic curves E, E' over K with Weierstrass equations

$$E : y^2 = x(x^2 + ax + b)$$
$$E' : y^2 = x(x^2 + a'x + b')$$

where $a' = 2a$ and $b' = a^2 - 4b$. Consider the isogenies

$$\begin{aligned}
&\phi : E \to E' \\
&(x, y) \mapsto \left(\left(\frac{x}{y} \right)^2, \frac{y^2(x^2 - b)}{x^2} \right) \\
&\widehat{\phi} : E' \to E \\
&(x, y) \mapsto \left(\left(\frac{x}{2y} \right)^2, \frac{y^2(x^2 - b')}{8x^2} \right)
\end{aligned}$$

By Lemma 2.4.8, these isogenies have degree 2. After a (tedious) calculation, one can show that they are indeed dual. It is clear that $E[\phi] = \{ \mathcal{O}_E, T \}$ and $E'[\widehat{\phi}] = \{ \mathcal{O}_{E'}, T' \}$ where $T = (0, 0) \in E(K)$ and $T' = (0, 0) \in E'(K)$.

Proposition 8.4.1. *There exists a group homomorphism*

$$\alpha : E'(K) \to {K^\times}/{(K^\times)^2}$$
$$(x, y) \mapsto \begin{cases} x \pmod{(K^\times)^2} & \text{if } x \neq 0 \\ b' \pmod{(K^\times)^2} & \text{if } x = 0 \end{cases}$$

whose kernel is exactly $\phi E(K)$.

Proof. The first part of the definition immediate upon applying Theorem 8.3.1 with $f = x$ and $g = y/x$. To see the second part, we explicit calculate $\delta(T')$. Note that a preimage P of T' under ϕ will necessarily have $y = 0$. Then a non-trivial x-coordinate for P will be a solution t of $x^2 + ax + b$. Let $L = K(t)$. Note that b' is the discriminant of $x^2 + ax + b$ so in fact, $L = (\sqrt{b'})$. Then $\delta(P)$ is represented by a 1-cocycle which is 0 on $\mathrm{Gal}(\bar{K}/L)$. Under the isomorphism $h : K^\times/(K^\times)^2 \to H^1(K, \mu_n)$, the equivalence class of this 1-cocycle corresponds to an element $u \in K^\times/(K^\times)^2$ such that $L = K(\sqrt{u})$. Hence $u = b'$ as claimed. □

Lemma 8.4.2. *Consider the injections*

$$\alpha_E : \frac{E(K)}{\widehat{\phi}E'(K)} \hookrightarrow {K^\times}/{(K^\times)^2}$$
$$\alpha_{E'} : \frac{E'(K)}{\phi E(K)} \hookrightarrow {K^\times}/{(K^\times)^2}$$

Then

$$2^{\mathrm{rank}(E(K))} = \frac{|\mathrm{im}(\alpha_E)||\mathrm{im}(\alpha_{E'})|}{4}$$

Proof. Since $\widehat{\phi}\phi = [2]_E$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} & & E(K) & \xrightarrow{\phi} & E'(K) & \longrightarrow & \operatorname{coker}(\phi) \longrightarrow 0 \\ & & \downarrow{\scriptstyle [2]_E} & & \downarrow{\scriptstyle \widehat{\phi}} & & \downarrow \\ 0 & \longrightarrow & E(K) & \xrightarrow{id} & E(K) & \longrightarrow & 0 \end{array}$$

Applying the Snake Lemma (and preprending with $\ker(\phi)$, we have an exact sequence)

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[2] \xrightarrow{\phi} E'(K)[\widehat{\phi}]$$

$$\frac{E'(K)}{\phi E(K)} \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \longrightarrow \frac{E(K)}{\widehat{\phi}E'(K)} \longrightarrow 0$$

Now, $E(K)[\phi], E(K)[\phi] \cong \mathbb{Z}/2\mathbb{Z}$, $E'(K)/\phi E(K) \cong \operatorname{im}(\alpha_{E'})$ and $E(K)/\widehat{\phi}E(K) \cong \operatorname{im}(\alpha_E)$. Hence this exact sequence is infact

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow E(K)[2] \xrightarrow{\phi} \mathbb{Z}/2\mathbb{Z}$$

$$\operatorname{im}(\alpha_{E'}) \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \longrightarrow \operatorname{im}(\alpha_E) \longrightarrow 0$$

Recall that given any exact sequence of abelian groups $\{ G_i \}_{0 \le i \le n}$, we have the following identity:

$$\prod_{i=0}^{n} |G_i|^{-1^i} = 1$$

From this we see that

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{im}(\alpha_E)||\operatorname{im}(\alpha_{E'})|}{4}$$

Now, by the Mordell-Weil Theorem, $E(K)$ is finitely generated, say $E(K) = \Delta \times \mathbb{Z}^r$ for some finite group Δ and $r \ge 0$. Then

$$E(K)/2E(K) \cong \Delta/2\Delta \times \left(\mathbb{Z}/2\mathbb{Z}\right)^r$$

Moreover, $E(K)[2] \cong \Delta[2]$. Since Δ is finite, we have $|\Delta/2\Delta| = \Delta[2]$ so that

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r$$

as desired. □

Lemma 8.4.3. *Let K be a number field and $a, b \in \mathcal{O}_K$. Let E/K be an elliptic curve with Weierstrass equation $y^2 = x(x^2 + ax + b)$. Then $\operatorname{im}(\alpha_E) \subseteq K(S, 2)$ where S is the set of primes dividing b.*

Proof. Recall that

$$K(S,2) = \left\{ x \in {}^{K^\times}\!/_{(K^\times)^2} \;\middle|\; v_\mathfrak{p}(x) \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \notin S \right\}$$

We need to show that for all primes $\mathfrak{p}$ of K such that $v_\mathfrak{p}(b) = 0$, we have that $v_\mathfrak{p}(x)$ is even for all $x \in \mathrm{im}(\alpha_E)$. To this end, fix $x \in \mathrm{im}(\alpha_E)$.

First suppose that $v_\mathfrak{p}(x) < 0$. Then Lemma 3.2.2 implies that $v_\mathfrak{p}(x) = -2r$ for some integer r so it is indeed even.

The assertion is trivial if $v_\mathfrak{p}(x) = 0$ so assume that $v_\mathfrak{p}(x) > 0$. Then $v_\mathfrak{p}(x^2 + ax + b) = 0$ so that $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2) = 2v_\mathfrak{p}(y)$ as claimed. □

Lemma 8.4.4. *Let K be a number field and $a, b \in \mathcal{O}_K$. Let E/K be an elliptic curve with Weierstrass equation $y^2 = x(x^2 + ax + b)$. If $b = b_1 b_2$ then $b_1(K^\times)^2 \in \mathrm{im}(\alpha_E)$ if and only if the equation*

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$$

is soluble for $u, v, w \in K$ not all zero.

Proof. If either $b_1 \in (K^\times)^2$ or $b_2 \in K(\times)^2$ then $b \cong b_1 \pmod{(K^\times)^2}$. Since $\alpha_E(T) = b(K^\times)^2$ the condition of the Lemma is satisfied. Hence we can assume that $b_1, b_2 \notin (K^\times)^2$. Then

$$\begin{aligned} b_1(K^\times)^2 \in \mathrm{im}(\alpha_E) &\iff \exists\, (x,y) \in E(K) \text{ such that } x = b_1 t^2 \text{ for some } t \in K^\times \\ &\implies y^2 = (b_1 t^2)((b_1 t^2)^2 + a(b_1 t^2) + b) \\ &\implies \left(\frac{y}{b_1 t}\right) = b_1 t^2 + a t^2 + b_2 \end{aligned}$$

Hence the equation has solution $w = \frac{y}{b_1 t}, u = t, v = -1$.

Conversely, suppose that we have a solution $u, v, w \in K$ to the above equation. Then $uv \neq 0$. By massaging the equation, we see that

$$\left(b_1 \left(\frac{u}{v}\right)^2, b_1 \left(\frac{uw}{v^3}\right) \right)$$

is a point in $E(K)$ whose x-coordinate is b_1 up to squares. □

Example 8.4.5.

$$w^2 = -u^4 - 4v^4$$

This is clearly insoluble over $\mathbb{Q}$ so $b_1(K^\times)^2 \notin \mathrm{im}(\alpha_{E'})$. Now suppose that $b_1 = 2$ so that $b_2 = 2$. Consider the equation

$$w^2 = 2u^4 + 2v^4$$

This clearly has solution $(u, v, w) = (1, 1, 2)$ so that $2(K^\times)^2 \in \mathrm{im}(\alpha_{E'})$. Finally, suppose that $b_1 = -2$ so that $b_2 = -2$. Consider the equation

$$w^2 = -2u^4 - 2v^4$$

This is clearly insoluble over $\mathbb{Q}$ so $b_1(K^\times)^2 \notin \mathrm{im}(\alpha_{E'})$. We thus see that $\mathrm{im}(\alpha_{E'}) = \langle 2 \rangle$. It then follows that $\mathrm{rank}\, E(\mathbb{Q}) = 0$.

Lemma 8.4.6. *Let K be a number field and $a, b \in \mathcal{O}_K$. Let E/K be an elliptic curve with Weierstrass equation $y^2 = x(x^2 + ax + b)$. If $b = b_1 b_2$ then*

$$\begin{aligned}\mathrm{im}(\alpha_{E'}) &\subseteq S^{(\phi)}(E/K) \\ &= \{\, b_1(\mathbb{Q}^\times)^2 \mid w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \text{ is soluble over } K_\mathfrak{p}\ \forall\, \mathfrak{p} \in M_K \,\}\end{aligned}$$

Proof. This is immediate from the definition of the Selmer group and the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi E(K) & \longrightarrow & S^{(\phi)}(E/K) & \longrightarrow & Ш(E/K)[\phi] & \longrightarrow & 0 \\ & & & \searrow^{\alpha_{E'}} & \downarrow & & & & \\ & & & & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & & & & \end{array}$$

□

Proposition 8.4.7. *Let $a, b \in \mathbb{Z}$ such that $b = b_1 b_2$ for some integers b_1 and b_2. If p is a rational prime such that $p \nmid 2b(a^2 - 4b)$ then the equation $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ is solvable over $\mathbb{Q}_p$.*

Proof. Proof omitted. □

Example 8.4.8. Consider the elliptic curve $E/\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + px$ where p is a rational prime congruent to 5 modulo 8. Let $E'/\mathbb{Q}$ be the elliptic curve with Weierstrass equation $y^2 = x^3 - 4px = x(x^2 - 4p)$. We have that

$$\mathrm{im}(\alpha_E) \subseteq \mathbb{Q}(\{\, p \,\}, 2) = \langle -1, p \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

Now suppose that $b_1 = -1$ so that $b_2 = -p$. Consider the equation

$$w^2 = -u^4 - pv^4$$

which is insoluble over $\mathbb{Q}$ so that $-1(\mathbb{Q}^\times)^2 \notin \mathrm{im}(\alpha_E)$. Now consider $b_1 = p$ so that $b_2 = 1$. Consider the equation

$$w^2 = pu^4 + v^4$$

This has a solution $(w, u, v) = (4, 0, 2)$ so that $p(K^\times)^2 \in \mathrm{im}(\alpha_E)$ (or we could have used the fact that $\alpha_E(T) = p(K^\times)^2$). Hence $\mathrm{im}(\alpha_E) = \langle p \rangle$.

On the other hand,

$$\mathrm{im}(\alpha_{E'}) \subseteq \mathbb{Q}(\{\, 2, p \,\}, 2) = \langle -1, 2, p \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

$\langle -1, 2, p \rangle$ has the non-trivial elements $2, -2, p, -p$. Note that $\alpha_{E'}(T') = -p(\mathbb{Q}^\times)^2$ so we have to check the following three cases:

$$b_1 = 2, b_2 = -2p \implies w^2 = 2u^4 - 2pv^4 \tag{2}$$
$$b_1 = -2, b_2 = 2p \implies w^2 = -2u^4 + 2pv^4 \tag{3}$$
$$b_1 = p, b_2 = -4 \implies w^2 = pu^4 - 4v^4 \tag{4}$$

First suppose that Equation 2 is soluble over $\mathbb{Q}$. Without loss of generality, we may assume that $(u, v, w) \in \mathbb{Z}^3$ with $\gcd(u, v) = 1$. If $p \mid u$ then $p \mid w$ and so $p \mid v$ which is a contradiction to $\gcd(u, v) = 1$. Hence we must have that $w^2 \equiv 2u^4 \pmod{p}$. We must therefore have that

2 is a square modulo p. But $p \cong 5 mod 8$ so this is a contradiction (just check with $p = 5$, for example). Hence Equation 2 is not soluble over $\mathbb{Q}$. By a similar argumentation, Equation 3 is not soluble over $\mathbb{Q}$ since -2 is not a square modulo p.

Thus far, we have that $\text{im}(\alpha_{E'}) \subseteq \langle -1, p \rangle$. Hence $\text{rank}/, E(\mathbb{Q}) = 0$ if Equation 4 is insoluble over $\mathbb{Q}$ and is 1 otherwise. Note that Equation 4 is solvable over $\mathbb{Q}_p$ since $p \equiv 1 \pmod 4$ so that -1 is a square in $\mathbb{F}_p$ whence it is a square in $\mathbb{Z}_p$. Moreover, it is also soluble over $\mathbb{Q}_2$ since $p - 4$ is a square in $\mathbb{Z}_2$ and soluble over $\mathbb{R}$ since p is a square in $\mathbb{R}$.

It is conejctured that $\text{rank}(E(\mathbb{Q}) = 1$ for all $p \equiv 5 \pmod 8$.

Definition 8.4.9. Let $a, b \in \mathbb{Z}$ such that $b = b_1 b_2$ for some integers b_1 and b_2. Let C be the smooth projective curve given by the equation $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$.

Example 8.4.10. Consider the elliptic curve $E/\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + 17x = x(x^2 + 17)$. Let $E'/\mathbb{Q}$ be the elliptic curve with Weierstrass equation $y^2 = x^3 - 4 \cdot 17x - x(x^2 - 4 \cdot 17)$. We have that

$$\text{im}(\alpha_E) \subseteq \mathbb{Q}(\{ 17 \}, 2) = \langle -1, 17 \rangle \subseteq {\mathbb{Q}^\times}/{(\mathbb{Q}^\times)^2}$$

First note that $\alpha_E(T) = 17(\mathbb{Q}^\times)^2$. Now suppose that $b_1 = -1$ so that $b_2 = -17$. We consider solubility over $\mathbb{Q}$ of the equation

$$w^2 = -u^4 - 17v^4$$

This clearly has no solutions in $\mathbb{Q}$ so we have that $\text{im}(\alpha_E) = \langle 17 \rangle$.

On the other hand, we have that

$$\text{im}(\alpha_{E'}) \subseteq \mathbb{Q}(\{ 2, 17 \}, 2) = \langle -1, 2, 17 \rangle$$

This has 5 non-trivial elements, namely $-1, 2, -2, 17, -17$. We must check solubility of the following equations:

$$\begin{aligned} b_1 = 2, b_2 = -2p &\implies w^2 = 2u^4 - 2pv^4 \\ b_1 = -2, b_2 = 2p &\implies w^2 = -2u^4 + 2pv^4 \\ b_1 = p, b_2 = -4 &\implies w^2 = pu^4 - 4v^4 \end{aligned}$$

We will just check solubility of the first one. To this end let C be the curve given by $w^2 = 2u^4 - 2pv^4$. Replacing w with $2w$ we have $2w^2 = u^4 - 17v^4$. By Hensel's Lemma, we know that $17 \in (\mathbb{Z}_2^\times)^4$ so $C(\mathbb{Q}_2)$ contains an element represented by $(w, u, v) = (0, 1, \sqrt[4]{17}^{-1})$. Similarly, $C(\mathbb{Q}_1 7) \neq \varnothing$ since $2 \in (\mathbb{Z}_{17}^\times)^2$. Finally, $C(\mathbb{R}) \neq \varnothing$ since $\sqrt{2} \in \mathbb{R}$. By Proposition 8.4.7, $C(\mathbb{Q}_p) \neq \varnothing$ for all primes $p \nmid [2 \cdot 17(4 \cdot 17)]$ so that $C(\mathbb{Q}_\mathfrak{p}) \neq \varnothing$ for all $\mathfrak{p} \in M_\mathbb{Q}$.

On the other hand, suppose that (u, v, w) represents an element of $C(\mathbb{Q})$. Without loss of generality, $u, v \in \mathbb{Z}$ are coprime so that $w \in \mathbb{Z}$ and we may further assume that $w > 0$. Now, if $17 \mid w$ then $17 \mid u$ and $17 \mid v$ which is a contradiction so we may assume that if $p \mid w$ then $p \neq 17$ and 17 is a square mod p. By quadratic reciprocity, we have that

$$\left(\frac{17}{p}\right)\left(\frac{p}{17}\right) = -1^{\frac{17-1}{2}\frac{p-1}{2}}$$

for all odd primes p. Then p is a square mod 17. Moreover, 2 is also a square mod 17 so that w is a square mod 17. But $2w^2 \equiv u^4 \pmod{17}$ so we must have that 2 is a fourth power in $\mathbb{F}_{17}^\times$. But the latter set is $\langle \pm 1, \pm 4 \rangle$ which is a contradiction. Hence $C(\mathbb{Q}) = \varnothing$. We thus refer to C as a counter example of the Hasse principle: it is a non-trivial element of $Ш(E/\mathbb{Q})$. In other words, it is a homogeneous space for which $C(\mathbb{Q}_\mathfrak{p}) \neq \varnothing$ for all $\mathfrak{p} \in M_\mathbb{Q}$ but $C(\mathbb{Q}) = \varnothing$.

9 The Birch and Swinnerton-Dyer Conjecture

Definition 9.1. Let $E/\mathbb{Q}$ be an elliptic curve. We define the ***L*-function** of E to be

$$L(E,s) = \prod_p L_p(E,s)$$

where

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{if } E \text{ has good reduction at } p \\ (1-p^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } p \\ (1+p^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

where $a_p = |\widetilde{E}(\mathbb{F}_p)|$.

By Hasse's Theorem, $|a_p| \leq 2\sqrt{p}$ so $L(E,s)$ converges for $\Re(s) \geq \frac{3}{2}$.

Theorem 9.2 (Wiles, Breuil, Conrad, Diamond, Taylor)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $L(E,s)$ is the L-function of a weight-2 modular form and hence has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation $L(E,s) = L(E,2-s)$.*

Conjecture 9.3 (Weak BSD)**.** *Let E an elliptic curve defined over $\mathbb{Q}$ and $L(E,s)$ its L-function. Then the rank of the abelian group $E(K)$ is equal to the order of vanishing $L(E,s)$ at $s=1$.*

Conjecture 9.4 (Strong BSD)**.** *Let E an elliptic curve defined over $\mathbb{Q}$ of rank r and $L(E,s)$ its L-function. Then*

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

where $\Omega_E = \int_{E(\mathbb{R})} |\omega_E|$, $\mathrm{Reg}(E)$ is the elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, $Ш(E)$ is the Tate-Shafarevich group of E and $c_p = |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$ is the Tamagawa number of $E/\mathbb{Q}_p$.

Theorem 9.5 (Kolyvagin)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If the order of vanishing of $L(E,s) = 0, 1$ then weak BSD is true and $|Ш(E/\mathbb{Q})| < \infty$.*