

Part III - Elliptic Curves

Lectured by Tom Fisher

Artur Avameri

Contents

0	Introduction	2
1	Fermat's Method of Infinite Descent	2
2	Some remarks on algebraic curves	3
2.1	The degree of a morphism	6
3	Weierstrass equations	7
4	The Group Law	9
5	Isogenies	13
6	The invariant differential	17
7	Elliptic curves over finite fields	20
8	Formal groups	23
9	Elliptic curves over local fields	28

0 Introduction

19 Jan 2024,

Lecture 1

The best books for the course include *The arithmetic of elliptic curves* by Silverman, Springer 1996, and *Lectures on elliptic curves* by Cassels, CUP 1991.

1 Fermat's Method of Infinite Descent

A right-angled triangle Δ has $a^2 + b^2 = c^2$ and $\text{area}(\Delta) = \frac{1}{2}ab$.

Definition 1.1. Δ is **rational** if $a, b, c \in \mathbb{Q}$. Δ is **primitive** if $a, b, c \in \mathbb{Z}$ are coprime.

Note that a primitive triangle has pairwise coprime side lengths because $a^2 + b^2 = c^2$.

Lemma 1.1. Every primitive triangle is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for some integers $u > v > 0$.

Proof. WLOG let a, b, c be odd, even, odd. Then $(\frac{b}{2})^2 = \frac{c+a}{2} \frac{c-a}{2}$, where we note that the RHS is a product of positive coprime integers. By unique factorization, $\frac{c+a}{2} = u^2, \frac{c-a}{2} = v^2$ for $u, v \in \mathbb{Z}$. This gives the desired result. \square

Definition 1.2. $D \in \mathbb{Q}_{>0}$ is a **congruent** number if there exists a rational triangle Δ with $\text{area}(\Delta) = D$.

Note that it suffices to consider $D \in \mathbb{Z}_{>0}$ squarefree.

Example 1.1. $D = 5, 6$ are congruent.

Lemma 1.2. $D \in \mathbb{Q}_{>0}$ is congruent $\iff Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}, y \neq 0$.

Proof. Lemma 1.1 shows that D congruent $\implies Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$. This implication also obviously goes the other way. To finish, divide through by w^4 and take $x = \frac{u}{v}, y = \frac{w}{v^2}$. \square

Fermat showed that 1 is not a congruent number.

Theorem 1.3. There is no solution to $w^2 = uv(u + v)(u - v)$ for $u, v, w \in \mathbb{Z}, w \neq 0$.

Proof. WLOG assume u, v are coprime and that $u, w > 0$. If $v < 0$, then replace (u, v, w) by $(-v, u, w)$. If u, v are both odd, then replace (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$. Then $u, v, u+v, u-v$ are pairwise coprime positive integers with their product a square, so by unique factorization in \mathbb{Z} , $u = a^2, v = b^2, u + v = c^2, u - v = d^2$ for $a, b, c, d \in \mathbb{Z}$.

Since $u \not\equiv v \pmod{2}$, both c and d are odd. Then $(\frac{c+d}{2})^2 + (\frac{c-d}{2})^2 = \frac{c^2+d^2}{2} = u = a^2$. This gives a primitive triangle with area $\frac{c^2-d^2}{8} = \frac{v}{4} = (\frac{b^2}{2})$.

Let $w_1 = \frac{b}{2}$, then by Lemma 1.1, $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$ for some $u_1, v_1 \in \mathbb{Z}$. Hence we have a new solution to our original question, with $4w_1^2 = b^2 = v \mid w^2 \implies w_1 \leq \frac{w}{2}$, so we're done by infinite descent. \square

A variant for polynomials. In the above, K is a field with $\text{char } K \neq 2$. Let \overline{K} be the algebraic closure of K and consider for this whole section K with $\text{char } K \neq 2$.

Lemma 1.4. Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in K$.

Proof. WLOG let $K = \overline{K}$ by extending if necessary. Changing coordinates on \mathbb{P}^1 (i.e. multiplying by a 2×2 invertible matrix), we may assume that the points $(\alpha : \beta)$ are $(1 : 0)$, $(0 : 1)$, $(1 : -1)$, $(1 : -\lambda)$ for $\lambda \in K \setminus \{0, 1\}$. Since our field is algebraically closed, let $\mu = \sqrt{\lambda}$. Then $u = a^2, v = b^2, u - v = (a + b)(a - b), u - \lambda v = (a + \mu b)(a - \mu b)$.

Unique factorization in $K[t]$ implies that $a + b, a - b, a + \mu b, a - \mu b$ are squares (since the necessary terms are coprime up to units, i.e. constants). But $\max(\deg(a), \deg(b)) \leq \frac{1}{2} \max(\deg(u), \deg(v))$, so by Fermat's method of infinite descent, $u, v \in K$. \square

Definition 1.3. (i) An **elliptic curve** E/K is the projective closure of the plane affine curve $y^2 = f(x)$ (this is called a Weierstrass equation) where $f \in K[x]$ is a monic cubic polynomial with distinct roots in \overline{K} .

(ii) For L/K any field extension, $E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{0\}$ (the point at infinity in the projective closure), it turns out that $E(L)$ is naturally an abelian group.

In this course, we study $E(K)$ for K a finite field, local field, number field.

Lemma 1.2 and Theorem 1.3 show that if $E : y^2 = x^3 - x$, then $E(\mathbb{Q}) = \{0, (0, 0), (\pm 1, 0)\}$.

Corollary 1.5. Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Proof. WLOG $K = \overline{K}$. By a change of coordinates, we may assume $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ for $u, v \in K(t)$ coprime. Then $w^2 = uv(u-v)(u-\lambda v)$ for some $w \in K[t]$. Unique factorization in $K[t]$ shows that $u, v, u-v, u-\lambda v$ are all squares, so by Lemma 1.4, $u, v \in K$, so $x, y \in K$. \square

2 Some remarks on algebraic curves

In this section, work over an algebraically closed field $K = \overline{K}$.

22 Jan 2024,
Lecture 2

Definition 2.1. A plane curve $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$ (for $f \in K[x, y]$ irreducible) is **rational** if it has a rational parametrization, i.e. $\exists \phi, \psi \in K(t)$ such that

- (i) The map $\mathbb{A}^1 \rightarrow \mathbb{A}^2$ by $t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finite set}\}$.
- (ii) $f(\phi(t), \psi(t)) = 0$ in $K(t)$.

Example 2.1. (a) Any nonsingular conic is rational. For example, for $x^2 + y^2 = 1$, take a line with slope t through $(-1, 0)$ (the anchor) and solve to get the rational parametrization $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

(b) Any singular plane cubic is rational, for example $y^2 = x^3$ giving $(x, y) = (t^2, t^3)$ with the anchor at the singularity $(0, 0)$ and $y^2 = x^2(x+1)$ with the parametrization to be computed on Ex. Sheet 1 (anchor still at $(0, 0)$).

(c) Corollary 1.5 shows that elliptic curves are not rational.

Remark. The genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C . If $K = \mathbb{C}$, then $g(C)$ is the genus of the Riemann surface. A smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$.

Proposition 2.1. (Here we still assume $K = \overline{K}$). Let C be a smooth projective curve.

- C is rational (see Definition 2.1) $\iff g(C) = 0$.
- C is an elliptic curve $\iff g(C) = 1$.

Proof. (i) Omitted.

(ii) (\implies): Check C is a smooth plane curve in \mathbb{P}^2 (see Ex. Sheet 1) and use the above remark.

(\impliedby): We will see this later.

□

Order of vanishing. Let C be an algebraic curve with function field $K(C)$ and let $P \in C$ be a smooth point. Write $\text{ord}_P(f)$ for the order of vanishing of $f \in K(C)$ at P (which is negative if f has a pole at P).

Fact. $\text{ord}_P : K(C)^\times \rightarrow \mathbb{Z}$ is a discrete valuation, i.e. $\text{ord}_P(f_1 f_2) = \text{ord}_P(f_1) + \text{ord}_P(f_2)$ and $\text{ord}_P(f_1 + f_2) \geq \min(\text{ord}_P(f_1), \text{ord}_P(f_2))$.

Definition 2.2. We say $t \in K(C)^\times$ is a **uniformizer** at P if $\text{ord}_P(t) = 1$.

Example 2.2. $C = \{g = 0\} \subset \mathbb{A}^2$ for $g \in K[x, y]$. Then $K(C) = \text{Frac} \left(\frac{K[x, y]}{(g)} \right)$. Write $g = g_0 + g_1(x, y) + g_2(x, y) + \dots$ for g_i homogeneous of degree i . Suppose $P = (0, 0)$ is a smooth point, e.g. $g_0 = 0$ and let $g_1(x, y) = \alpha x + \beta y$ with α, β not both zero ($\alpha x + \beta y = 0$ gives a tangent to the curve at P). Let $\gamma, \delta \in K$ and consider also the line $\gamma x + \delta y$ through P . Then it is a fact that $\gamma x + \delta y \in K(C)$ is a uniformizer at P if and only if $\alpha\delta - \beta\gamma \neq 0$.

Example 2.3. Consider $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$ for $\lambda \neq 0, 1$ and consider its projective closure by taking $x = \frac{X}{Z}, y = \frac{Y}{Z}$ to get $\{Y^2Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2$. This has only one point at infinity, $P = (0 : 1 : 0)$. Our aim is to compute $\text{ord}_P(x)$ and $\text{ord}_P(y)$.

For this, put $t = \frac{X}{Y}, w = \frac{Z}{Y}$, so $w \stackrel{(\dagger)}{=} t(t-w)(t-\lambda w)$. Now P is the point $(t, w) = (0, 0)$, which is a smooth point with $\text{ord}_P(t) = \text{ord}_P(t-w) = \text{ord}_P(t-\lambda w) = 1$, so (\dagger) gives $\text{ord}_P(w) = 3$. We now find

$$\begin{aligned} \text{ord}_P(x) &= \text{ord}_P \left(\frac{X}{Z} \right) = \text{ord}_P \left(\frac{t}{w} \right) = 1 - 3 = -2 \\ \text{ord}_P(y) &= \text{ord}_P \left(\frac{Y}{Z} \right) = \text{ord}_P \left(\frac{1}{w} \right) = -3. \end{aligned}$$

Riemann–Roch space. Let C be a smooth projective curve.

Definition 2.3. A **divisor** is a formal sum of points on C , say $D = \sum_{P \in C} n_P P$ where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. We say $\deg D = \sum_{P \in C} n_P$.

D is **effective** (written $D \geq 0$) if $n_P \geq 0 \ \forall P \in C$. If $f \in K(C)^\times$, then $\text{div}(f) = \sum_{P \in C} \text{ord}_P(f) P$. The Riemann–Roch space of $D \in \text{Div}(C)$ is

$$\mathcal{L}(D) = \{f \in K(C)^\times \mid \text{div}(f) + D \geq 0\} \cup \{0\},$$

i.e. the K -vector space of rational functions on C with "poles no worse than specified by D " (i.e. every coefficient of $\text{div}(f) + D$ is nonnegative).

We quote Riemann–Roch for surfaces of genus 1: We have

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

Example 2.4. We revisit Example 2.3. We have $\mathcal{L}(2P) = \langle 1, x \rangle$ and $\mathcal{L}(3P) = \langle 1, x, y \rangle$.

We still have $\text{char } K \neq 2$ and $\overline{K} = K$.

24 Jan 2024,
Lecture 3

Proposition 2.2. Let $C \subset \mathbb{P}^2$ be a smooth plane cubic and let $P \in C$ be a point of inflection. Then we may change coordinates such that $C : Y^2Z = X(X - Z)(X - \lambda Z)$ and $P = (0 : 1 : 0)$ (for some $\lambda \neq 0, 1$).

Proof. First change coordinates such that $P = (0 : 1 : 0)$. Then change coordinates such that the tangent line becomes $T_P C = \{Z = 0\}$. Say $C = \{F(X, Y, Z) = 0\} \subset \mathbb{P}^2$. A point on the tangent line is of the form $(t : 1 : 0)$ and since $P \in C$ is a point of inflection, we get $F(t, 1, 0) = \text{const} \cdot t^3$, i.e. F has no terms X^2Y, XY^2 or Y^3 .

Hence $F = \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$. Notably, Y^2Z has a nonzero coefficient, otherwise $P \in C$ would be singular, a contradiction to C being smooth. The coefficient of X^3 is nonzero as well, otherwise $Z \mid F$. We are free to rescale X, Y, Z, F , so WLOG C is defined by

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

Substituting $Y \mapsto Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$, we may assume $a_1 = a_3 = 0$. This gives

$$C : Y^2Z = Z^3 f\left(\frac{X}{Z}\right)$$

for a monic cubic polynomial f . Since C is smooth, f has distinct roots, WLOG $0, 1, \lambda$, so $C : Y^2Z = X(X - Z)(X - \lambda Z)$. \square

The form $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ is the Weierstrass form. The form $Y^2Z = X(X - Z)(X - \lambda Z)$ is the Legendre form.

Remark. It can be shown that the points of inflection of a plane curve $C = \{F(X_1, X_2, X_3) = 0\} \subset \mathbb{P}^2$ are given by solving the Hessian:

$$\begin{cases} \det H = \det \left(\frac{\partial^2 F}{\partial X_i \partial X_j} \right) = 0 \\ F(X_1, X_2, X_3) = 0. \end{cases}$$

2.1 The degree of a morphism

Let $\phi : C_1 \rightarrow C_2$ be a nonconstant morphism of smooth projective curves. Then $\phi^* : K(C_2) \rightarrow K(C_1)$ by $f \mapsto f \circ \phi$, giving an injective map $\phi^* K(C_2)$ to $K(C_1)$.

Definition 2.4. The **degree** of ϕ is $\deg \phi = [K(C_1) : \phi^* K(C_2)]$.

We say ϕ is **separable** if $K(C_1)/\phi^* K(C_2)$ is a separable field extension.

Suppose $P \in C_1, Q \in C_2$ and $\phi : P \mapsto Q$. Let $t \in K(C_2)$ be a uniformizer at Q .

Definition 2.5. $e_\phi(P) = \text{ord}_P(\phi^* t)$, which is always ≥ 1 and independent of t .

Theorem 2.3. Let $\phi : C_1 \rightarrow C_2$ be a nonconstant morphism of smooth projective curves. Then

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi \quad \forall Q \in C_2.$$

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

We don't prove this.

In particular, this shows that:

- (i) ϕ is surjective (very important here that we're in \overline{K}).
- (ii) $|\phi^{-1}(Q)| \leq \deg \phi$.
- (iii) If ϕ is separable, then equality holds in (ii) for all but finitely many points $Q \in C_2$.

Important remark. Let C be an algebraic curve. A rational map is given by

$$\begin{aligned} C &\rightarrow \mathbb{P}^n \\ \phi &\mapsto (f_0, f_1, \dots, f_n) \end{aligned}$$

where $f_0, \dots, f_n \in K(C)$ are not all zero. Then we have a fact: If C is smooth, then ϕ is a morphism. This saves us a lot of time (we can go from a rational map to a morphism immediately).

3 Weierstrass equations

We now drop the assumption that $\overline{K} = K$, but we will still assume that K is perfect.

Definition 3.1. An **elliptic curve** E/K is a smooth projective curve of genus 1 defined over K with a specified K -rational point $O = 0_E$.

Example 3.1. $\{X^3 + pY^3 + p^2Z^3 = 0\} \subset \mathbb{P}^2$ is not an elliptic curve over \mathbb{Q} , since it has no \mathbb{Q} -rational point.

Theorem 3.1. Every elliptic curve E is isomorphic over K to a curve in Weierstrass form via an isomorphism taking 0_E to $(0 : 1 : 0)$.

Remark. Proposition 2.2 treated the special case where E is a smooth plane cubic and 0_E is a point of inflection.

Fact. If $D \in \text{Div}(E)$ is defined over K , then $\mathcal{L}(D)$ has a basis in $K(E)$ (not just in $\overline{K}(E)$). Here D is defined over K if it is fixed by $\text{Gal}(\overline{K}/K)$ (this is unimportant for us and we just write it down to be rigorous).

Proof. $\mathcal{L}(2 \cdot 0_E) \subset \mathcal{L}(3 \cdot 0_E)$. Pick bases $1, x$ and $1, x, y$. Note $\text{ord}_{0_E}(x) = -2$ and $\text{ord}_{0_E}(y) = -3$ (else x, y don't give a basis). The 7 elements $1, x, y, x^2, xy, x^3, y^2$ lie in the 6-dimensional vector space $\mathcal{L}(60_E)$ (as they have at most a sixth order pole), so they must satisfy a linear dependence relation.

Leaving out x^3 or y^2 leaves us with 6 elements, all with different order poles, giving a basis for $\mathcal{L}(60_E)$. Hence the coefficients of x^3 and y^2 are nonzero, so by rescaling x, y (if necessary) we get

$$E' : y^2 + a_1xy + a_2y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$. Let E' be the curve defined by this equation (or rather its projective closure). There is a morphism $\phi : E \rightarrow E' \subset \mathbb{P}^2$ by $P \mapsto (x(P) : y(P) : 1) = \left(\frac{x}{y}(P) : 1 : \frac{1}{y}(P)\right)$. (Since E is smooth, we know that this rational map is a morphism). Hence $0_E \mapsto (0 : 1 : 0)$.

We have $E \xrightarrow{x} \mathbb{P}^1$ by $x \mapsto (x : 1)$ (and similarly for y), so

$$\begin{aligned} [K(E) : K(x)] &= \deg(E \xrightarrow{x} \mathbb{P}^1) = \text{ord}_{0_E} \left(\frac{1}{x} \right) = 2 \\ [K(E) : K(y)] &= \deg(E \xrightarrow{y} \mathbb{P}^1) = \text{ord}_{0_E} \left(\frac{1}{y} \right) = 3. \end{aligned}$$

This gives an inclusion of fields $K(x) \leq K(E)$ of degree 2, $K(y) \leq K(E)$ of degree 3, while $K(x), K(y) \leq K(x, y) \leq K(E)$, so tower law gives $[K(E) : K(x, y)] = 1 \implies K(E) = K(x, y) = \phi^* K(E') \implies \deg \phi = 1$. (draw a picture!). This gives us an inverse that is a rational map, which we want to show is a morphism. For this, we just need to show that E' is smooth.

If E' were singular, then E and E' are rational, a contradiction. So E' is smooth and hence ϕ^{-1} is a morphism, so ϕ is an isomorphism. \square

Proposition 3.2. Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over $K \iff$ the equations are related by a change of variables

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

for $r, s, t, u \in K$ with $u \neq 0$.

Proof. $\mathcal{L}(2 \cdot 0_E) = \langle 1, x \rangle = \langle 1, x' \rangle \implies x = \lambda x' + r$ for some $\lambda, r \in K, \lambda \neq 0$. Similarly $\mathcal{L}(3 \cdot 0_E) = \langle 1, x, y \rangle = \langle 1, x', y' \rangle \implies y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K, \mu \neq 0$.

Looking at the coefficients of x^3 and y^2 tells us that $\lambda^3 = \mu^2$, so $\lambda = u^2, \mu = u^3$ for some $u \in K^\times$. Put $s = \frac{\sigma}{u^2}$ to conclude. \square

A Weierstrass equation defines an elliptic curve \iff it defines a smooth curve $\iff \Delta(a_1, \dots, a_6) \neq 0$, where $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is a certain polynomial.

If $\text{char } K \neq 2, 3$, we may reduce to the case $E : y^2 = x^3 + ax + b$. In this case, the discriminant is $\Delta = -16(4a^3 + 27b^2)$.

Corollary 3.3. Assume $\text{char } K \neq 2, 3$. Elliptic curves

$$\begin{aligned} E : y^2 &= x^3 + ax + b \\ E' : y^2 &= x^3 + a'x + b' \end{aligned}$$

are isomorphic over $K \iff \begin{cases} a' = u^4a \\ b' = u^6b \end{cases} \text{ for some } u \in K^\times.$

Proof. E, E' are related by a substitution as in Proposition 3.2 with $r = s = t = 0$. \square

Definition 3.2. The j -invariant is $j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}$.

Corollary 3.4. $E \cong E' \implies j(E) = j(E')$ and the converse holds if $K = \overline{K}$.

Proof. $E \cong E' \iff \begin{cases} a' = u^4a \\ b' = u^6b \end{cases} \text{ for some } u \in K^\times \implies (a^3 : b^2) = ((a')^3 : (b')^2) \iff j(E) = j(E').$ The middle step is reversible if $K = \overline{K}$. \square

4 The Group Law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic with $0_E \in E(K)$ (not immediately assumed to be in Weierstrass form). E meets any line in 3 points, counted with multiplicity.

For $P, Q \in E$, let S be the 3rd point of intersection of PQ with E and then let R be the 3rd intersection of $0_E S$ with E . We define $P \oplus Q = R$. (Later we drop the circle and just write $+$). If $P = Q$, instead take the tangent line at P , i.e. $T_P E$, etc. This is the "chord and tangent process".

Theorem 4.1. (E, \oplus) is an abelian group.

Remark. Here E means $E(\overline{K})$ since we haven't specified a field yet.

Proof. (i) \oplus is commutative trivially.

(ii) 0_E is the identity, since the line through $0_E P$ meets E for the 3rd time at S and then SP meets E for the 3rd time at 0_E (drawing a picture makes this obvious).

(iii) Inverses: Let S be the 3rd intersection of T_{0_E} with E and Q the 3rd intersection of PS with E . Then $P \oplus Q = 0_E$.

(iv) Associativity is much harder. We have some setup:

Definition 4.1. $D_1, D_2 \in \text{Div}(E)$ are **linearly equivalent** if $\exists f \in K(E)^\times$ such that $\text{div}(f) = D_1 - D_2$. Write $D_1 \sim D_2$ and $[D] = \{D' \mid D' \sim D\}$.

Definition 4.2. The **Picard group** is $\text{Pic}(E) = \text{Div}(E)/\sim$. Also define $\text{Pic}^0(E) = \text{Div}^0(E)/\sim$ where $\text{Div}^0(E) = \{D \in \text{Div}(E) \mid \deg(D) = 0\}$.

We define $\psi : E \rightarrow \text{Pic}^0(E)$ by $P \mapsto [(P) - (0_E)]$.

Proposition 4.2. (i) $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) ψ is a bijection.

Proof. (i) WLOG let the lines PQ and 0_ES be given by $l = 0$ and $m = 0$.

Then

$$\text{div}\left(\frac{l}{m}\right) = (P) + (S) + (Q) - (0_E) - (S) - (R),$$

hence $(P) + (Q) \sim (P \oplus Q) + (0_E)$, so $(P \oplus Q) - (0_E) \sim (P) - (0_E) + (Q) - (0_E)$, so $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) Injectivity: Suppose $\psi(P) = \psi(Q)$ for $P \neq Q$. Then $\exists f \in \overline{K}(E)^\times$ such that $\text{div}(f) = (P) - (0_E) - (Q) + (0_E) = (P) - (Q) \implies E \xrightarrow{f} \mathbb{P}^1$ has degree 1 (for example since evaluation at 0 on the affine line gives that P has one root and Q has one pole), so $E \cong \mathbb{P}^1$, a contradiction.

Surjectivity: Let $[D] \in \text{Pic}^0(E)$. Then $D + (0_E)$ has degree 1, so by Riemann–Roch, $\dim \mathcal{L}(D + (0_E)) = 1$, so $\exists 0 \neq f \in \overline{K}(E)$ such that $\text{div}(f) + D + (0_E) \geq 0$, but $\text{div}(f) + D + (0_E)$ has degree 1, so $\text{div}(f) + D + (0_E) = (P)$ for some $P \in E \implies (P) - (0_E) \sim D \implies \psi(P) = [D]$.

□

We conclude that ψ identifies (E, \oplus) with $(\text{Pic}^0(E), +)$, so \oplus is associative.

□

29 Jan 2024,
Lecture 5

Formulae for E in Weierstrass form. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Choose two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on it. Let the line through P_1 and P_2 be given by $y = \lambda x + \nu$ and let it meet E again at $P' = (x', y')$. We want to find $P_1 \oplus P_2 = P_3 = (x_3, y_3) = \ominus P'$ for $\ominus P$ the reflection of P across the x -axis. We easily compute $\ominus P_1 = (x_1, -(a_1x + a_3) - y_1)$.

Substituting $y = \lambda x + \nu$ into our equation for E and looking at the coefficient of x^2 gives $\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x' = x_1 + x_2 + x_3$, so $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$. For y_3 we find

$$y_3 = -(a_1x' + a_3) - y' = -(a_1x_3 + a_3) - (\lambda x_3 + \nu) = -(\lambda + a_1)x_3 - a_3 - \nu.$$

It remains to find formulas for λ and ν .

- Case 1. $x_1 = x_2$, but $P_1 \neq P_2$. Then $P_1 \oplus P_2 = 0_E$.
- Case 2. $x_1 \neq x_2$. Then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$.
- Case 3. $P_1 = P_2$. In this case, compute the equation for the tangent line to get λ, ν as rational expressions in x_1, x_2, y_1, y_2 .

Corollary 4.3. $E(K)$ is an abelian group.

Proof. $E(K)$ is a subgroup of (E, \oplus) .

- It has identity 0_E by definition.
- We have closure and inverses through the formulae above.
- Associativity and commutativity is inherited.

□

Theorem 4.4. Elliptic curves are group varieties, i.e.

$$\begin{aligned} [-1] : E &\rightarrow E, P \mapsto \ominus P \\ \oplus : E \times E &\rightarrow E, (P, Q) \mapsto P \oplus Q \end{aligned}$$

are morphisms of algebraic varieties.

Proof. By the above formulae, $[-1] : E \rightarrow E$ is a rational map, i.e. a morphism by our important remark.

For \oplus , note by the above formulae that $\oplus : E \times E \rightarrow E$ is a rational map regular on

$$U = \{(P, Q) \in E \times E \mid 0_E \notin \{P, Q, P \oplus Q, P \ominus Q\}\}.$$

For $P \in E$, let $\tau_P : E \rightarrow E$ be the "translation by P " map, given by $X \mapsto P \oplus X$. τ_P is a rational map, hence a morphism. Now for $A, B \in E$, we factor \oplus as

$$E \times E \xrightarrow{\tau_{\ominus A} \times \tau_{\ominus B}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A \oplus B}} E.$$

This shows \oplus is regular on $(\tau_A \times \tau_B)(U)$, so \oplus is regular on $E \times E$. □

Statement of results. The following isomorphisms in (i), (ii), (iv) respect the relevant topologies.

(i) $K = \mathbb{C}$. Then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ for Λ a lattice.

(ii) $K = \mathbb{R}$. Then

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

(iii) $K = \mathbb{F}_q$. Then $||E(\mathbb{F}_q)| - (q + 1)| \leq 2\sqrt{q}$. This is Hasse's Theorem.

(iv) For a local field $[K : \mathbb{Q}_p] < \infty$ with ring of integers \mathcal{O}_K , $E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

(v) For a number field $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group (this is the Mordell–Weil Theorem). Basic group theory says that if A is a finitely generated abelian group, then $A \cong (\text{finite subgroup}) \times \mathbb{Z}^r$. Here r is called the rank of A . The proof of Mordell–Weil gives an upper bound for $\text{rank } E(K)$, but there is no known algorithm to compute the rank in all cases.

Brief remarks on the case $K = \mathbb{C}$. Let $\Lambda = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$ where ω_1, ω_2 are a basis for \mathbb{C} as an \mathbb{R} -vector space. Then meromorphic functions on the Riemann surface \mathbb{C}/Λ correspond bijectively with Λ -invariant meromorphic functions in \mathbb{C} . The function field of \mathbb{C}/Λ is generated by $\wp(z)$ and $\wp'(z)$, where

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right) \\ \wp'(z) &= -2 \sum_{\lambda \in \Lambda} \frac{1}{(z - \lambda)^3}. \end{aligned}$$

These satisfy $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some constants $g_2, g_3 \in \mathbb{C}$ depending on Λ . One shows $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where $E : y^2 = 4x^3 - g_2x - g_3$ which is an isomorphism on both groups (via $z \mapsto (\wp(z), \wp'(z))$) and on Riemann surfaces. We have the following result:

Theorem 4.5 (Uniformization theorem). Every elliptic curve over \mathbb{C} arises in this way.

Definition 4.3. For $n \in \mathbb{Z}$, let $[n] : E \rightarrow E$ be given by $P \mapsto \underbrace{P \oplus P \oplus \dots \oplus P}_{n \text{ copies}}$

if $n > 0$ and $[-n] = [-1] \circ [n]$.

Definition 4.4. The n -torsion subgroup of E is

$$E[n] = \ker(E \xrightarrow{[n]} E).$$

If $K = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $\deg[n] = n^2$. Call these results (1) and (2). We will show that (2) holds over any field $K = \overline{K}$ and (1) holds if $\text{char } K \nmid n$. We sometimes abuse notation and write $E[n] = E[n](\overline{K})$.

31 Jan 2024,
Lecture 6

Lemma 4.6. Assume $\text{char } K \neq 2$ and $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$ (with $e_i \in \overline{K}$). Then $E[2] = \{0, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^\times$.

Proof. Let $P = (x, y) \in E$. Then $2[P] = 0 \iff P = -P \iff (x, y) = (x, -y) \iff y = 0$. \square

5 Isogenies

Let E_1, E_2 be elliptic curves.

Definition 5.1. (i) An **isogeny** $\phi : E_1 \rightarrow E_2$ is a nonconstant morphism with $\phi(0_{E_1}) = 0_{E_2}$.

(ii) We say E_1 and E_2 are **isogenous** if there is an isogeny between them.

In (i), nonconstant is equivalent to surjective on \overline{K} -points. See Theorem 2.3.

Definition 5.2. $\text{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \rightarrow E_2\} \cup \{0\}$ (the constant map at 0_E). This is an abelian group under $(\phi + \psi)(P) := \phi(P) \oplus \psi(P)$.

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies, then $\psi \circ \phi$ is an isogeny. By tower law, $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$.

Proposition 5.1. If $0 \neq n \in \mathbb{Z}$, then $[n] : E \rightarrow E$ is an isogeny.

Proof. $[n]$ is a morphism by Theorem 4.4. We need to show $[n] \neq [0]$. Assume $\text{char } K \neq 2$.

- Case $n = 2$. Lemma 4.6 implies that $E[2] \neq E$, so $[2] \neq 0$.
- Case n odd. Lemma 4.6 implies that $\exists 0 \neq T \in E[2]$. Then $nT = T \neq 0$, so $[n] \neq [0]$.

Now use $[mn] = [m] \circ [n]$ to conclude.

If $\text{char } K = 2$, then we can replace Lemma 4.6 with an explicit lemma about 3-torsion points. \square

Corollary 5.2. $\text{Hom}(E_1, E_2)$ is a torsion-free \mathbb{Z} -module.

Theorem 5.3. Let $\phi : E_1 \rightarrow E_2$ be an isogeny. Then

$$\phi(P + Q) = \phi(P) + \phi(Q) \quad \forall P, Q \in E.$$

Sketch proof. ϕ induces a map $\phi_* : \text{Div}^0(E_1) \rightarrow \text{Div}^0(E_2)$ by $\sum_{P \in E_1} n_P P \mapsto \sum_{P \in E_2} n_P \phi(P)$. Recall $\phi^* : K(E_2) \hookrightarrow K(E_1)$.

Fact. If $f \in K(E_1)$, then $\text{div}(N_{K(E_1)/K(E_2)}f) = \phi^*(\text{div } f)$. So ϕ_* sends principal divisors to principal divisors. Since $\phi(0_{E_1}) = 0_{E_2}$, the following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow f & & \downarrow g \\ \text{Pic}^0(E_1) & \xrightarrow{\phi_*} & \text{Pic}^0(E_2) \end{array}$$

(with $f(P) = [(P) - (0_{E_1})]$, $g(Q) = [(Q) - (0_{E_2})]$). Since ϕ_* is a group homomorphism, ϕ is a group homomorphism. \square

Lemma 5.4. Let $\phi : E_1 \rightarrow E_2$ be an isogeny. Then there exists a morphism ξ making the following diagram commute:

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

with x_i the x -coordinate in a Weierstrass equation for E_i . Moreover, if $\xi(t) = \frac{r(t)}{s(t)}$ with $r, s \in K[t]$ coprime, then $\deg(\phi) = \deg(\xi) = \max(\deg(r), \deg(s))$.

Proof. For $i = 1, 2$, $K(E_i)/K(x_i)$ is a degree 2 Galois extension with Galois group generated by $[-1]^*$. By Theorem 5.3, $\phi \circ [-1] = [-1] \circ \phi$, so if $f \in K(x_2)$, then $[-1]^*(\phi^*f) = \phi^*([-1]^*f) = \phi^*f$ and hence $\phi^*f \in K(x_1)$. Hence we find

$$\begin{array}{ccc} & K(E_1) = K(x_1, y_1) & \\ & \swarrow 2 & \downarrow \\ K(x_1) & & K(E_2) = K(x_2, y_2) \\ \downarrow & \swarrow 2 & \\ K(x_2) & & \end{array} \cdot$$

In particular, $\phi^*x_2 = \xi(x_1)$ for some $\xi \in K(t)$. By tower law, $2\deg(\phi) = 2\deg(\xi) \implies \deg(\phi) = \deg(\xi)$. Now $K(x_2) \hookrightarrow K(x_1)$ by $x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)}$ for $r, s \in K[t]$ coprime. Then minimal polynomial of x_1 over $K(x_2)$ is $F(t) = r(t) - s(t)x_2 \in K(x_2)[t]$. This is true as $F(x_1) = 0$, F is irreducible on $K[x_2, t]$ (since r, s are coprime) and by Gauss' Lemma, F is irreducible on $K(x_2)[t]$. Hence $\deg(\phi) = \deg(\xi) = [K(x_1) : K(x_2)] = \deg(F) = \max(\deg(r), \deg(s))$. \square

Lemma 5.5. $\deg[2] = 4$.

Proof. Assume $\text{char } K \neq 2, 3$, so $E : y^2 = x^3 + ax + b = f(x)$. If $P = (x, y)$, then $x(2P) = \left(\frac{3x^2+a}{2y}\right)^2 - 2x = \frac{(3x^2+a)^2 - 2xf(x)}{4f(x)}$. The numerator and denominator are coprime, since otherwise $\exists \theta \in \overline{K}$ with $f(\theta) = f'(\theta) = 0$, meaning f has a multiple root, contradiction. We are now done by Lemma 5.4, since $\deg[2] = \max(3, 4) = 4$. \square

Definition 5.3. Let A be an abelian group. Then a map $q : A \rightarrow \mathbb{Z}$ is a quadratic form if

- (i) $q(nx) = n^2q(x) \forall n \in \mathbb{Z}, x \in A$.
- (ii) $(x, y) \mapsto q(x+y) - q(x) - q(y)$ is \mathbb{Z} -bilinear.

Lemma 5.6. $q : A \rightarrow \mathbb{Z}$ is a quadratic form if and only if it satisfies the parallelogram law $q(x+y) + q(x-y) = 2q(x) + 2q(y) \forall x, y \in A$.

Proof. (\implies). Let $\langle x, y \rangle = q(x+y) - q(x) - q(y)$. Then $\langle x, x \rangle = q(2x) - 2q(x) = 2q(x)$ by (i) with $n = 2$. By (ii), $\langle x+y, x+y \rangle + \langle x-y, x-y \rangle = 2\langle x, x \rangle + 2\langle y, y \rangle$, which implies $q(x+y) + q(x-y) = 2q(x) + 2q(y)$.

(\impliedby). This is on Ex. Sheet 2. \square

02 Jan 2024,
Lecture 7

Theorem 5.7. $\deg : \text{Hom}(E_1, E_2) \rightarrow \mathbb{Z}$ is a quadratic form (with $\deg(0) = 0$).

Proof. Assume $\text{char } K \neq 2, 3$ and write $E_2 = y^2 = x^3 + ax + b$. Let $P, Q \in E_2$ with $P, Q, P+Q, P-Q$ all nonzero and let x_1, x_2, x_3, x_4 be the x -coordinates of these points.

Lemma 5.8. There exist polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree ≤ 2 in x_1 and of degree ≤ 2 in x_2 such that

$$(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$$

Proof. Method 1: Direct calculation (results on the formula sheet) gives the result (e.g. $W_0 = (x_1 - x_2)^2$).

Method 2: Let $y = \lambda x + \nu$ be the line through P and Q . Substituting, we get $x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3$ where s_i is the i^{th} symmetric polynomial in x_1, x_2, x_3 . Comparing coefficients gives $\lambda^2 = s_1, -2\lambda\nu = s_2 - a, \nu^2 = s_3 + b$. Eliminating λ and ν gives

$$F(x_1, x_2, x_3) = (s_2 - a)^2 - 4s_1(s_3 + b) = 0,$$

where F has degree at most 2 in each x_i . Hence x_3 is a root of the quadratic $W(t) = F(x_1, x_2, t)$. Repeating this for the line through P and $-Q$ shows that

x_4 is the other root of $W(t)$. Therefore

$$\begin{aligned} W(t) &= W_0(t - x_3)(t - x_4) = W_0t^2 - W_1t + W_2 \\ \implies (1 : x_3 + x_4 : x_3x_4) &= (W_0 : W_1 : W_2). \end{aligned}$$

□

We now show that if $\phi, \psi \in \text{Hom}(E_1, E_2)$, then $\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg(\phi) + 2\deg(\psi)$. We may assume that $\phi, \psi, \phi + \psi, \phi - \psi$ are not the zero maps (otherwise we're done trivially, or use $\deg[-1] = 1, \deg[2] = 4$). Now

$$\begin{aligned} \phi : (x, y) &\mapsto (\xi_1(x), \dots) \\ \psi : (x, y) &\mapsto (\xi_2(x), \dots) \\ \phi + \psi : (x, y) &\mapsto (\xi_3(x), \dots) \\ \phi - \psi : (x, y) &\mapsto (\xi_4(x), \dots). \end{aligned}$$

Lemma 5.8 implies $(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : \dots)$. Say $\xi_i = \frac{r_i}{s_i}$ for $r_i, s_i \in K[t]$ coprime. This gives

$$(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) \stackrel{(\star)}{=} ((r_1s_2 - r_2s_1)^2 : \dots)$$

where every term is quadratic in r_3, r_4, s_3 and s_4 . Hence (as the terms on the LHS of (\star) are coprime)

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

Now replace ϕ and ψ by $\phi + \psi$ and $\phi - \psi$ and use $\deg[2] = 4$ to get

$$4\deg(\phi) + 4\deg(\psi) = \deg(2\phi) + \deg(2\psi) \leq 2\deg(\phi + \psi) + 2\deg(\phi - \psi).$$

This gives the parallelogram law, so \deg is a quadratic form. □

Corollary 5.9. $\deg(n\phi) = n^2\deg(\phi)$. In particular, $\deg[n] = n^2$.

Example 5.1. Let E/K be an elliptic curve. Suppose $\text{char } K \neq 2$ and $0 \neq T \in E(K)[2]$. WLOG let $E : y^2 = x(x^2 + ax + b)$ for $a, b \in K, b(a^2 - 4b) \neq 0$ (by moving a root to zero) and WLOG $T = (0, 0)$.

If $P = (x, y)$ and $P' = P + T = (x', y')$, then

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

We let $\xi = x + x' + a = \left(\frac{y}{x}\right)^2$, $\eta = y + y' = \frac{y}{x} \left(x - \frac{b}{x}\right)$. Then

$$\eta^2 = \left(\frac{y}{x}\right)^2 \left(\left(x + \frac{b}{x}\right)^2 - 4b \right) = \xi((\xi - a)^2 - 4b) = \xi(\xi^2 - 2a\xi + a^2 - 4b).$$

Let $E' : y^2 = x(x^2 + a'x + b')$ with $a' = -2a$, $b' = a^2 - 4b$. There is an isogeny $\phi : E \rightarrow E'$ given by $(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1\right)$.

Sanity check/finding where 0_E maps to: x is a double pole, y is a triple pole, so $\left(\frac{y}{x}\right)^2$ is a double pole and $\frac{y(x^2 - b)}{x^2}$ is a triple pole (and the last coordinate 1 has degree 0). Multiplying through by a cube of a uniformizer, the degrees go from $(-2, -3, 0)$ to $(1, 0, 3)$, so $0_E \mapsto (0 : 1 : 0)$.

To compute $\deg(\phi)$, $\left(\frac{y}{x}\right)^2 = \frac{x^2 + ax + b}{x}$ with the numerator and denominator coprime as $b \neq 0$, so by Lemma 5.4, $\deg(\phi) = 2$. We say ϕ is a **2-isogeny**.

6 The invariant differential

For C some algebraic curve over $K = \overline{K}$.

Definition 6.1. The space of differentials Ω_C (sometimes called one-forms) is the $K(C)$ -vector space generated by df for all $f \in K(C)$ subject to the relations

(i) $d(f + g) = df + dg$.

(ii) $d(fg) = f dg + g df$.

(iii) $da = 0 \ \forall a \in K$.

Fact. Ω_C is a 1-dimensional $K(C)$ -vector space.

Let $0 \neq \omega \in \Omega_C$, let $P \in C$ be a smooth point and let $t \in K(C)$ be a uniformizer at P . Then $\omega = f dt$ for some $f \in K(C)^\times$. We define $\text{ord}_P(\omega) = \text{ord}_P(f)$, which is independent of the choice of t .

Fact. Suppose $f \in K(C)^\times$ with $\text{ord}_P(f) = n \neq 0$. If $\text{char } K \nmid n$, then $\text{ord}_P(df) = n - 1$.

We assume that C is a smooth projective curve.

Definition 6.2. We define $\text{div}(\omega) = \sum_{P \in C} \text{ord}_P(\omega) P \in \text{Div}(C)$. Here we use the fact that $\text{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

05 Feb 2024,
Lecture 8

Definition 6.3. A differential $\omega \in \Omega_C$ is regular if $\text{div}(\omega) \geq 0$. We define the genus $g(C)$ of C to be

$$g(C) = \dim_K \{\omega \in \Omega_C \mid \text{div}(\omega) \geq 0\},$$

where the set on the RHS is the set of regular differentials.

As a consequence of Riemann–Roch, we have that if $0 \neq \omega \in \Omega_C$, then $\deg(\text{div}(\omega)) = 2g(C) - 2$.

Lemma 6.1. Assume $\text{char } K \neq 2$ and let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ for e_1, e_2, e_3 distinct. Then $\omega = \frac{dx}{y}$ is a differential on E with no zeroes or poles, which implies $g(E) = 1$. In particular, the K -vector space of regular differentials on E is 1-dimensional (see previous fact), spanned by ω .

Proof. Let $T_i = (e_i, 0)$. Then $E[2] = \{0, T_1, T_2, T_3\}$ and $\text{div}(y) \stackrel{(\dagger)}{=} (T_1) + (T_2) + (T_3) - 3(0)$. For $0 \neq P \in E$, $\text{div}(x - x_P) = (P) + (-P) - 2(0)$.

- If $P \in E \setminus E[2]$, then $\text{ord}(x - x_P) = 1 \implies \text{ord}_P(dx) = 0$.
- If $P = T_i$, then $\text{ord}_P(x - x_P) = 2 \implies \text{ord}_P(dx) = 1$.
- If $P = 0$, then $\text{ord}_P(x) = -2 \implies \text{ord}_P(dx) = -3$.

Hence $\text{div}(dx) = (T_1) + (T_2) + (T_3) - 3(0)$, which with (\dagger) gives $\text{div}\left(\frac{dx}{y}\right) = 0$. \square

Definition 6.4. For $\phi : C_1 \rightarrow C_2$ a nonconstant morphism, we define

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

Lemma 6.2. Let $P \in E$, $\tau_P : E \rightarrow E$ by $X \mapsto X + P$ and $\omega = \frac{dx}{y}$ as above. Then $\tau_P^* \omega = \omega$. We say ω is the **invariant differential**.

Proof. $\tau_P^* \omega$ is a regular differential on E , so $\tau_P^* \omega = \lambda_P \omega$ for some $\lambda_P \in K^\times$. The map $E \rightarrow \mathbb{P}^1$ by $P \mapsto \lambda_P$ is a morphism of smooth projective curves, but it is not surjective (as it misses 0 and ∞). Hence it is constant by Theorem 2.3, i.e. $\exists \lambda \in K^\times$ such that $\tau_P^* \omega = \lambda \omega \forall P \in E$. Taking $P = 0$ shows $\lambda = 1$. \square

Remark. If $K = \mathbb{C}$ and $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ by $z \mapsto (\wp(z), \wp'(z)) := (x, y)$, then $\frac{dx}{y} = \frac{\wp'(z)dz}{\wp'(z)} = dz$, which is invariant under $z \mapsto z + \text{const}$.

Lemma 6.3. Let $\phi, \psi \in \text{Hom}(E_1, E_2)$. Let ω be the invariant differential on E_2 . Then $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$.

Proof. Write E for E_2 . We have the maps

$$\begin{aligned} E \times E &\rightarrow E \\ \mu : (P, Q) &\mapsto P + Q \\ \text{pr}_1 : (P, Q) &\mapsto P \\ \text{pr}_2 : (P, Q) &\mapsto Q. \end{aligned}$$

Fact. $\Omega_{E \times E}$ is a 2-dimensional $K(E \times E)$ -vector space with basis $\text{pr}_1^* \omega$ and $\text{pr}_2^* \omega$. Consequently, $\mu^* \omega \stackrel{(\dagger)}{=} f \text{pr}_1^* \omega + g \text{pr}_2^* \omega$ for some $f, g \in K(E \times E)$.

For fixed $Q \in E$, let $i_Q : E \rightarrow E \times E$ by $P \mapsto (P, Q)$. Applying i_Q^* to (\dagger) gives

$$\begin{aligned} \underbrace{(\mu \circ i_Q)^* \omega}_{\tau_Q} &= (i_Q^* f) \underbrace{(\text{pr}_1 \circ i_Q)^* \omega}_{\text{identity map}} + (i_Q^* g) \underbrace{(\text{pr}_2 \circ i_Q)^* \omega}_{\text{constant map}} \\ \implies \tau_Q^* \omega &= (i_Q^* f) \omega + 0. \end{aligned}$$

As $\tau_Q^* \omega = \omega$ by the previous lemma, we conclude $i_Q^* f = 1 \ \forall q \in E$, so $f(P, Q) = 1 \ \forall P, Q \in E$. Similarly $g(P, Q) = 1 \ \forall P, Q \in E$, so (\dagger) gives $\mu^* \omega = \text{pr}_1^* \omega + \text{pr}_2^* \omega$. Now pull back using

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

to get $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$. \square

Lemma 6.4. Let $\phi : C_1 \rightarrow C_2$ be a nonconstant morphism. Then ϕ is separable if and only if $\phi^* : \Omega_{C_2} \rightarrow \Omega_{C_1}$ is nonzero.

Proof. Omitted. \square

Example 6.1. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ be the multiplicative group. For $n \geq 2$ an integer, consider $\phi : \mathbb{G}_m \rightarrow \mathbb{G}_m$ by $x \mapsto x^n$. Then $\phi^*(dx) = d(x^n) = nx^{n-1}dx$. So if $\text{char } K \nmid n$, then ϕ is separable, so $|\phi^{-1}(Q)| = \deg \phi$ for all but at most finitely many $Q \in \mathbb{G}_m$.

But ϕ is a group homomorphism, so $|\phi^{-1}(Q)| = |\ker(Q)| \ \forall Q \in \mathbb{G}_m$. Hence $|\ker Q| = \deg \phi = n$. This shows that $K = \overline{K}$ contains exactly n distinct n^{th} roots of unity.

07 Feb 2024,
Lecture 9

Theorem 6.5. ¹If $\text{char } K \nmid n$, then $E[n] = (\mathbb{Z}/n\mathbb{Z})^2$.

¹Remember that $\overline{K} = K$ here.

Proof. Lemma 6.3 and induction imply $[n]^*\omega = n\omega$ where $\text{char } K \nmid n$, so $[n]$ is separable by Lemma 6.4. Hence $|[n]^{-1}(Q)| = \deg[n]$ for all but finitely many points $Q \in E$. But $[n]$ is a group homomorphism, so $|[n]^{-1}Q| = |E[n]| \ \forall Q \in E$. We conclude that $|E[n]| = \deg[n] = n^2$ by Corollary 5.9.

By classification of finite abelian groups, $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid d_2 \mid \dots \mid d_t$, but $d_t \mid n$, and if p is a prime with $p \mid d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$, so $|E[p]| = p^2$, so $t = 2$. Hence $d_1 \mid d_2 \mid n$ with $d_1 d_2 = n^2$, so $d_1 = d_2 = n$ and so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. \square

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

Remark about the remark. Do not use this remark to trivialize a question on Ex. Sheet 2.

7 Elliptic curves over finite fields

Lemma 7.1. Let A be an abelian group. Let $q : A \rightarrow \mathbb{Z}$ be a positive definite quadratic form. Then

$$\underbrace{|q(x+y) - q(x) - q(y)|}_{\langle x, y \rangle} \leq 2\sqrt{q(x)q(y)}.$$

Proof. We may assume $x \neq 0$, otherwise the result is clear. Hence $q(x) \neq 0$. Let $m, n \in \mathbb{Z}$, then

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

Get rid of the first term by taking $m = -\langle x, y \rangle$ and $n = 2q(x)$ to deduce $\langle x, y \rangle^2 \leq 4q(x)q(y)$, so the result follows. \square

Theorem 7.2 (Hasse). Let E/\mathbb{F}_q be an elliptic curve. Then

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

Proof. Recall $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r , generated by the Frobenius map $x \mapsto x^q$. Let E have Weierstrass equation with coefficients $a_1, \dots, a_6 \in \mathbb{F}_q$ (and note that $a_i^q = a_i \ \forall i$).

Define the Frobenius endomorphism $\phi : E \rightarrow E$ by $(x, y) \mapsto (x^q, y^q)$, which is an isogeny of degree q . Then $E(\mathbb{F}_q) = \{P \in E \mid \phi(P) = P\} = \ker(1 - \phi)$. We have

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

as $q = p^n$, so $p \mid q$. By Lemma 6.3,

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

so $1 - \phi$ is separable. By Theorem 2.3 and the fact that $1 - \phi$ is a group homomorphism, we argue in the proof of Theorem 6.5 that

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

The map $\deg : \text{Hom}(E, E) \rightarrow \mathbb{Z}$ is a positive definite quadratic form by Theorem 5.7. Hence by Lemma 7.1,

$$\begin{aligned} |\deg(1 - \phi) - 1 - \deg\phi| &\leq 2\sqrt{\deg\phi} \\ \implies |\#E(\mathbb{F}_q) - q - 1| &\leq 2\sqrt{q}. \end{aligned} \quad \square$$

Definition 7.1. For $\phi, \psi \in \text{End}(E) = \text{Hom}(E, E)$, we put $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ and $\text{tr}(\phi) = \langle \phi, 1 \rangle$.

Corollary 7.3. Let E/\mathbb{F}_q be an elliptic curve and let $\phi \in \text{End}(E)$ be the q^{th} power Frobenius map. Then $\#E(\mathbb{F}_q) = q + 1 - \text{tr}(\phi)$ and $|\text{tr}(\phi)| \leq 2\sqrt{q}$.

Zeta functions. For K a number field,

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

For K a function field, i.e. $K = \mathbb{F}_q(C)$ where C is a smooth projective curve,

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

where $|C| = \{\text{closed points of } C\} = \{\text{orbits for the action of } \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \text{ on } C(\overline{\mathbb{F}_q})\}$ and $Nx = q^{\deg x}$, where $\deg x$ is the size of the corresponding orbit (these definitions are borrowed from scheme theory). We have $\zeta_K(s) = F(q^{-s})$ for

some $F \in \mathbb{Q}[[T]]$. We have

$$\begin{aligned}
 F(T) &= \prod_{x \in |C|} (1 - T^{\deg x})^{-1} \\
 \implies \log F(T) &= \sum_{x \in |C|} \sum_{m=1}^{\infty} \frac{1}{m} T^{m \deg x} \\
 \implies T \frac{d}{dT} \log F(T) &= \sum_{x \in |C|} \sum_{m=1}^{\infty} \deg x T^{m \deg x} \\
 &= \sum_{n=1}^{\infty} \left(\sum_{x \in |C|, \deg x | n} \deg x \right) T^n \\
 &= \sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) T^n \\
 \implies F(T) &= \exp \left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n \right).
 \end{aligned}$$

Definition 7.2. The zeta function of a smooth projective curve C/\mathbb{F}_q is

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

09 Feb 2024,
Lecture 10

Theorem 7.4. Let E/\mathbb{F}_q be an elliptic curve with $\#E(\mathbb{F}_q) = q + 1 - a$. Then

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

Proof. Let $\phi : E \rightarrow E$ be the q -power Frobenius map. By Corollary 7.3, $\#E(\mathbb{F}_q) = q + 1 - \text{tr}(\phi)$, so $\text{tr}(\phi) = a$ and $\deg(\phi) = q$. By a result from Ex. Sheet 2, $\phi^2 - a\phi + q = 0$. Hence $\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$. As the trace is linear, $\text{tr}(\phi^{n+2}) - a\text{tr}(\phi^{n+1}) + q\text{tr}(\phi^n) = 0$. The second order difference equation with initial conditions $\text{tr}(1) = \langle 1, 1 \rangle = 2^2 - 1^2 - 1^2 = 2$ and $\text{tr}(\phi) = a$ has solution

$$\text{tr}(\phi^n) = \alpha^n + \beta^n$$

for $\alpha, \beta \in \mathbb{C}$ are roots of $X^2 - aX + q = 0$.² Apply Corollary 7.3 again to get

²We don't need to worry about the case where the roots are equal, since we don't want a general solution, just a solution satisfying our initial conditions.

that $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \text{tr}(\phi^n) = 1 + q^n - \alpha^n - \beta^n$. Hence

$$\begin{aligned} Z_E(T) &= \exp \sum_{n=1}^{\infty} \left(\frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n} \right) \\ &= \exp(-\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T)) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \\ &= \frac{1 - aT + qT^2}{(1-T)(1-qT)}. \end{aligned} \quad \square$$

Remark. Hasse's theorem tells us that $|a| \leq 2\sqrt{q}$, so the discriminant $a^2 - q$ is nonpositive, so the roots are complex conjugates, i.e. $\alpha = \bar{\beta}$, and $|\alpha| = |\beta| \stackrel{(\dagger)}{=} \sqrt{q}$.

Let $K = \mathbb{F}_q(E)$, then $\zeta_K(s) = 0 \implies Z_E(q^{-s}) = 0 \implies q^{-s} \in \{\frac{1}{\alpha}, \frac{1}{\beta}\} \implies q^s \in \{\alpha, \beta\} \implies q^{\text{Re}(s)} = |\alpha| = |\beta| \implies \text{Re}(s) = \frac{1}{2}$. This proves the Riemann hypothesis for elliptic curves over finite fields.

8 Formal groups

Definition 8.1. Let R be a ring and $I \subset R$ an ideal. The I -**adic topology** on R has basis $\{r + I^n \mid r \in R, n \geq 1\}$.

Definition 8.2. A sequence (x_n) in R is **Cauchy** if $\forall k, \exists N$ such that $x_m - x_n \in I^k \forall m, n \geq N$.

Definition 8.3. R is **complete** if

- (i) $\bigcap_{n \geq 0} I^n = \{0\}$ (this is a Hausdorff-type condition).
- (ii) Every Cauchy sequence converges.

Useful remark. If $x \in I$, then $\frac{1}{1-x} = 1 + x + x^2 + \dots$. This exists as the sequence of partial sums form a Cauchy sequence, and then we check that the result it converges to is an inverse for $\frac{1}{1-x}$. Hence $1 - x \in R^\times$.

Example 8.1. Basically the only two examples we care about in this course are:

- $R = \mathbb{Z}_p$, the p -adic integers, and $I = p\mathbb{Z}_p$.
- $R = \mathbb{Z}[[t]]$ and $I = (t)$.

Lemma 8.1 (Hensel's lemma). Let R be complete with respect to an ideal I . Let $F \in R[X]$, $s \geq 1$ with $s \in \mathbb{Z}$. Suppose $a \in R$ satisfies

$$\begin{aligned} F(a) &\equiv 0 \pmod{I^s} \\ F'(a) &\in R^\times \end{aligned}$$

Then there exists a unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I^s}$.

Proof. Let $u \in R^\times$ be such that $F'(a) = u \pmod{I}$ (e.g. we could take $u = F'(a)$). Replacing $F(X)$ by $\frac{F(X+a)}{u}$ we may assume $a = 0$ and $F'(0) \equiv 1 \pmod{I}$. We put $x_0 = 0$ and $x_{n+1} \stackrel{(\dagger)}{=} x_n - F(x_n)$. Each induction shows that $x_n \equiv 0 \pmod{I^s} \forall n$ (\ddagger) . Now use the useful identity

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y))$$

for some $G, H \in R[X, Y]$. Call this identity (\star) .

We claim that $x_{n+1} \equiv x_n \pmod{I^{n+s}} \forall n \geq 0$. To prove this, use induction. The case $n = 0$ is clear. Suppose $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$. By (\star) ,

$$F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1 + c)$$

for some $c \in I$. Modulo I^{n+s} we now use (\ddagger) to get

$$\begin{aligned} F(x_n) - F(x_{n-1}) &\equiv x_n - x_{n-1} \pmod{I^{n+s}} \\ \implies x_n - F(x_n) &\equiv x_{n-1} - F(x_{n-1}) \pmod{I^{n+s}} \\ \implies x_{n+1} &\equiv x_n \pmod{I^{n+s}}. \end{aligned}$$

Hence $(x_n)_{n \geq 0}$ is Cauchy, and R is complete, so $x_n \rightarrow b$ as $n \rightarrow \infty$ for some $b \in R$. Taking the limit in (\dagger) gives $b = b - F(b)$ (as the polynomial is continuous in our topology), so $F(b) = 0$. Taking the limit in (\ddagger) gives $b \equiv 0 \equiv a \pmod{I^s}$.

For uniqueness, if b_1, b_2 work, then plug them into (\star) and use the useful remark that $1 - x$ is a unit to get that $b_1 = b_2$. \square

Write $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ and look at its affine piece $Y \neq 0$ with $t = -\frac{X}{Y}, w = -\frac{Z}{Y}$ (the minus signs are here to match Silverman's book). We get

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 = f(t, w).$$

We apply Hensel's lemma (Lemma 8.1) with $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, $I = (t)$ and $F(X) = X - f(t, X) \in R[X]$. We take $s = 3$, $a = 0$ and check that $F(a) = F(0) = -f(t, 0) = -t^3 \equiv 0 \pmod{I^3}$ and $F'(0) = 1 - a_1t - a_2t^2 \in R^\times$

by our useful remark, so the assumptions hold. Hence there exists a unique $\omega(t) \in R = \mathbb{Z}[a_1, \dots, a_6][[t]]$ such that $\omega(t) = f(t, w(t))$ and $w(t) \equiv 0 \pmod{t^3}$.

Remarks.

(i) Taking $u = 1$ in the proof of Hensel's lemma gives $w(t) = \lim_{n \rightarrow \infty} w_n(t)$ where $w_0(t) = 0$, $w_{n+1}(t) = f(t, w_n(t))$.

(ii) In fact, $w(t) = t^3(1 + A_1 t + A_2 t^2 + \dots)$ where $A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1 a_2 + 2a_3$, etc. (i.e. we can compute the series explicitly).

12 Feb 2024,
Lecture 11

Lemma 8.2. Let R be an integral domain, complete with respect to an ideal I . Let $a_0, \dots, a_6 \in R$ and let $K = \text{Frac}(R)$. Then

$$\widehat{E}(I) := \{(t, w) \in E(K) \mid t, w \in I\}$$

is a subgroup of $E(K)$.

Remark. By uniqueness in Hensel's lemma, $\widehat{E}(I) = \{(t, w(t)) \in E(K) \mid t \in I\}$.

Proof. Taking $(t, w) = (0, 0)$ shows $0_E \in \widehat{E}(I)$. So it suffices to show that if $P_1, P_2 \in \widehat{E}(I)$, then $P_3 := -P_1 - P_2 \in \widehat{E}(I)$. Since we're working over an affine piece with the identity at 0, we know three points sum to zero if and only if they lie on the same line. Say $P_i = (t_i, w_i)$ with the line $P_1 P_2$ given by $w = \lambda t + \nu$. We have $P_1, P_2 \in \widehat{E}(I) \implies t_1, t_2 \in I$ and $w_1 = w(t_1), w_2 = w(t_2)$. Write $w(t) = \sum_{n=2}^{\infty} A_{n-2} t^{n+1}$ with $A_0 = 1$. We have

$$\lambda = \begin{cases} \frac{w(t_2) - w(t_1)}{t_2 - t_1} & \text{if } t_1 \neq t_2 \\ w'(t_1) & \text{if } t_1 = t_2 \end{cases} = \sum_{n=2}^{\infty} A_{n-2} (t_1^n + t_1^{n-1} t_2 + \dots + t_2^n) \in I,$$

$$\nu = w_1 - \lambda t_1 \in I.$$

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

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4 t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3.$$

Let

$$A = (\text{coeff. of } t^3) = 1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3,$$

$$B = (\text{coeff. of } t^2) = a_1 \lambda + a_2 \nu + a_3 \lambda^2 + 2a_4 \lambda \nu + 3a_6 \lambda^2 \nu.$$

We have $A \in R^\times$, $B \in I$. Hence $t_3 = \frac{-B}{A} - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. \square

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$ and $I = (t)$ and using Lemma 8.2 implies $\exists \iota \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $\iota(0) = 0$ such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$.

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ and $I = (t_1, t_2)$ and using Lemma 8.2 implies $\exists F \in \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ with $F(0, 0) = 0$ and

$$(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))).$$

In fact, $F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \dots$

By properties of the group law, we deduce

- (i) $F(X, Y) = F(Y, X)$,
- (ii) $F(X, 0) = X$ and $F(0, Y) = Y$,
- (iii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$,
- (iv) $F(X, \iota(X)) = 0$.

Definition 8.4. Let R be a ring. A **formal group** over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying the first three axioms above.

An exercise on Ex. Sheet 2 asks us to show that the first three conditions imply the fourth, i.e. there is a unique $\iota(X) = -X + \dots \in R[[X]]$ such that $F(X, \iota(X)) = 0$.

Example 8.2. (i) The additive formal group $F(X, Y) = X + Y$, called $\widehat{\mathbb{G}}_a$.

(ii) The multiplicative formal group $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$, called $\widehat{\mathbb{G}}_m$.

(iii) The formal group of an elliptic curve, $F(X, Y) = [\text{see above}]$, called \widehat{E} .

Definition 8.5. Let \mathcal{F} and \mathcal{G} be formal groups over R given by power series F and G .

- (i) A **morphism** $\mathcal{F} \rightarrow \mathcal{G}$ is a power series $f \in R[[T]]$ such that $f(0) = 0$ satisfying $f(F(X, Y)) = G(f(X), f(Y))$.
- (ii) We say \mathcal{F} is **isomorphic** to \mathcal{G} , i.e. $\mathcal{F} \cong \mathcal{G}$ if there exist morphisms $\mathcal{F} \xrightarrow{f} \mathcal{G}$ and $\mathcal{G} \xrightarrow{g} \mathcal{F}$ such that $f(g(T)) = g(f(T)) = T$.

Theorem 8.3. If $\text{char } R = 0$, then any formal group \mathcal{F} over R is isomorphic to $\widehat{\mathbb{G}}_a$ over $R \otimes \mathbb{Q}$. (In other words, our conditions are $\text{char } R = 0$ and "the integers are invertible"). More precisely:

- (i) 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

$$\log(F(X, Y)) = \log(X) + \log(Y). \quad (\star)$$

- (ii) There is a unique power series $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$ with $b_i \in R$ such that

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

Proof. (i) Notation: Write $F_1(X, Y) = \frac{\partial F}{\partial X}(X, Y)$. Uniqueness: Let $p(T) = \frac{d}{dT} \log T = 1 + a_2T + a_3T^2 + \dots$. Differentiating (\star) with respect to X gives $p(F(X, Y))F_1(X, Y) = p(X) + 0$. Putting $X = 0$ gives $P(Y)F_1(0, Y) = 1$, so $p(Y) = \frac{1}{F_1(0, Y)}$, proving uniqueness.

Existence: Let $p(T) = F_1(0, T)^{-1} = 1 + a_2T + a_3T^2 + \dots$ for some $a_i \in R$. Define $\log T = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$, so $p(T) = \frac{d}{dT} \log T$. Then

$$\begin{aligned} F(F(X, Y), Z) &= F(X, F(Y, Z)) \\ \xrightarrow{\frac{d}{dX}} F_1(F(X, Y), Z)F_1(X, Y) &= F_1(X, F(Y, Z)) \\ \xrightarrow{X=0} F_1(Y, Z)p(Y)^{-1} &= p(F(Y, Z))^{-1} \\ \implies F_1(Y, Z)p(F(Y, Z)) &= p(Y) \\ \xrightarrow{\text{intg. wrt } Y} \log(F(Y, Z)) &= \log(Y) + h(Z) \end{aligned}$$

for some power series H . But the symmetry in Y and Z implies that $h(Z) = \log Z$, so we're done.

14 Feb 2024,
Lecture 12

- (ii) For this, use

Lemma 8.4. Let $f(T) = aT + \dots \in R[[T]]$ with $a \in R^\times$. Then there exists a unique $g(T) = a^{-1}T + \dots \in R[[T]]$ with $f(g(T)) = g(f(T)) = T$.

Proof. We construct polynomials $g_n(T) \in R[T]$ such that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$. Then $g(T) = \lim_{n \rightarrow \infty} g_n(T)$ satisfies $f(g(T)) = T$. To start the induction, set $g_1(T) = a^{-1}T$.

Now suppose $n \geq 2$, so $g_{n-1}(T)$ exists, so $f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$ for some $b \in R$. We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for $\lambda \in R$ to be chosen later. Then $f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) = f(g_{n-1}(T)) + \lambda aT^n \equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}$, so we take $\lambda = -ba^{-1}$ (then $\lambda \in R$ as $b \in R, a \in R^\times$), completing the induction step.

We get $g(T) = a^{-1}T + \dots \in R[[T]]$ such that $f(g(T)) = T$ (\dagger). Applying the same construction to g gives $h(T) = a + \dots \in R[[T]]$ such that $g(h(T)) = T$ (\ddagger). Now note that $f(T) \stackrel{(\dagger)}{=} f(g(h(T))) \stackrel{(\ddagger)}{=} h(T)$, so $f = h$. \square

The result now follows from this lemma and Ex. Sheet 2 Q5 (which allows us to control the denominators, so they'd be $n!$).

\square

Notation. Let \mathcal{F} be a formal group (e.g. $\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_m, \widehat{E}$) given by a power series $F \in R[[X, Y]]$. Suppose R is complete with respect to an ideal I . For $x, y \in I$, define $x \oplus_{\mathcal{F}} y = F(x, y) \in I$. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group.

Example 8.3. • $\widehat{\mathbb{G}}_a(I) = (I, +)$,

• $\widehat{\mathbb{G}}_m(I) = (1 + I, \times)$,

• $\widehat{E}(I) = \text{subgroup of } E(K) \text{ in Lemma 8.2.}$

Corollary 8.5. Let \mathcal{F} be a formal group over R and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then

- (i) $[n] : \mathcal{F} \rightarrow \mathcal{F}$ is an isomorphism of formal groups.
- (ii) If R is complete with respect to an ideal I , then $\mathcal{F}(I) \xrightarrow{\times n} \mathcal{F}(I)$ is an isomorphism of groups. In particular, $\mathcal{F}(I)$ has no n -torsion.

Proof. We define $[1](T) = T$ and $[n](T) = F([n-1]T, T) \forall n \geq 2$. (For $n < 0$, use $[-1](T) = \iota(T)$). Since $F(X, Y) = X + Y + XY(\dots)$, we have $[2](T) = f(T, T) = 2T + \dots$. By induction we get $[n](T) = nT + \dots \in R[[T]]$. Lemma 8.4 shows that if $n \in R^\times$, then $[n]$ is an isomorphism. This proves (i). Part (ii) now follows. \square

9 Elliptic curves over local fields

Let K be a field, complete with respect to a discrete valuation $v : K \rightarrow \mathbb{Z}$. (Here complete means complete with respect to the metric given by the absolute value arising from v .)

- The **valuation ring** is $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.
- The **unit group** is $\mathcal{O}_K^\times = \{x \in K^\times \mid v(x) = 0\}$.
- The **maximal ideal** is $\pi\mathcal{O}_K$, where $v(\pi) = 1$.
- The **residue field** is $k = \mathcal{O}_K / \pi\mathcal{O}_K$.

We assume that $\text{char } K = 0$, but $\text{char}(k) = p > 0$ (i.e. we are in the mixed characteristic case). The key example to keep in mind is $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, k = \mathbb{F}_p$. Now let E/K be an elliptic curve.

Definition 9.1. A Weierstrass equation for E with coefficients $a_1, \dots, a_6 \in K$ is **integral** if $a_1, \dots, a_6 \in \mathcal{O}_K$ and **minimal** if $v(\Delta)$ is minimal among all integral Weierstrass equations for E .

Remarks.

- (i) Rescaling $x = u^2 x', y = u^3 y'$ gives $a_i = u^i a'_i$, so we can clear denominators, so integral Weierstrass equations exist.
- (ii) $a_1, \dots, a_6 \in \mathcal{O}_K \implies \Delta \in \mathcal{O}_K \implies v(\Delta) \geq 0 \implies$ minimal Weierstrass equations exist.
- (iii) If $\text{char}(k) \neq 2, 3$, then there exists a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$.

Lemma 9.1. Let E/K have integral Weierstrass equation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$. Let $0 \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $\begin{cases} v(x) = -2s \\ v(y) = -3s \end{cases}$ for some $s \geq 1$. (Compare this with Ex. Sheet 1 Q5.)

Proof. • Case $v(x) \geq 0$: Suppose $v(y) < 0$. Then $v(\text{LHS}) = v(y^2) < 0$ while $v(\text{RHS}) \geq 0$, a contradiction. Hence $v(y) \geq 0$, so $x, y \in \mathcal{O}_K$.

- Case $v(x) < 0$: We have $v(\text{LHS}) \geq \min(2v(y), v(x) + v(y), v(y))$ and $v(\text{RHS}) = 3v(x)$. Go through 3 cases based on which element is minimal to get $v(y) < v(x)$ in every case. Now $v(\text{LHS}) = 2v(y)$, $v(\text{RHS}) = 3v(x)$, so we're done.

□

If K is complete, then \mathcal{O}_K is complete with respect to $\pi^r \mathcal{O}_K$ for any $r \geq 1$. We fix a minimal Weierstrass equation for E/K . This gives rise to a formal group \hat{E} over \mathcal{O}_K . Take $R = \mathcal{O}_K$, $I = \pi^r \mathcal{O}_K$ for $r \geq 1$ in Lemma 8.2 to get

$$\begin{aligned} \hat{E}(\pi^r \mathcal{O}_K) &= \left\{ (x, y) \in E(K) \mid -\frac{x}{y}, -\frac{1}{y} \in \pi^r \mathcal{O}_K \right\} \cup \{0\} \\ &= \left\{ (x, y) \in E(K) \mid v\left(\frac{x}{y}\right) \geq r, v\left(\frac{1}{y}\right) \geq r \right\} \cup \{0\} \\ &= \{(x, y) \in E(K) \mid v(x) = -2s, v(y) = -3s \text{ for some } s \geq r\} \cup \{0\} \\ &= \{(x, y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}. \end{aligned}$$

By Lemma 8.2 this is a subgroup of $E(K)$, call it $E_r(K)$. It is also clear that $\dots \subset E_3(K) \subset E_2(K) \subset E_1(K) \subset E(K)$. More generally, for \mathcal{F} a formal group over \mathcal{O}_K we have $\dots \subset \mathcal{F}(\pi^3 \mathcal{O}_K) \subset \mathcal{F}(\pi^2 \mathcal{O}_K) \subset \mathcal{F}(\mathcal{O}_K)$. We claim that

- $\mathcal{F}(\pi^r \mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for r sufficiently large,
- $\mathcal{F}(\pi^r \mathcal{O}_K) / \mathcal{F}(\pi^{r+1} \mathcal{O}_K) \cong (k, +) \forall r \geq 1$.

Reminder. Remember that we always have $\text{char } K = 0, \text{char}(k) = p > 0$.

Theorem 9.2. Let \mathcal{F} be a formal group over \mathcal{O}_K . Let $e = v(p)$. If $r > \frac{e}{p-1}$, then

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

is an isomorphism of groups with inverse

$$\exp : \widehat{\mathbb{G}}_a(\pi^r \mathcal{O}_K) \xrightarrow{\sim} \mathcal{F}(\pi^r \mathcal{O}_K).$$

Remark. We have $\widehat{\mathbb{G}}_a(\pi^r \mathcal{O}_K) = (\pi^r \mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$.

Proof. For $x \in \pi^r \mathcal{O}_K$, we must show that the power series $\log(x)$ and $\exp(x)$ converge to elements in $\pi^r \mathcal{O}_K$. Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$ with $b_i \in \mathcal{O}_K$.

Claim. $v_p(n!) \leq \frac{n-1}{p-1}$.

Proof of claim. Write

$$v_p(n!) = \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor < \sum_{r=1}^{\infty} \frac{n}{p^r} = \frac{n \cdot \frac{1}{p}}{1 - \frac{1}{p}} = \frac{n}{p-1}.$$

Clearing denominators, $(p-1)v_p(n!) < n \implies v_p(n!) \leq \frac{n-1}{p-1}$. \square

Now $v\left(\frac{b_n x^n}{n!}\right) \geq nr - e\left(\frac{n-1}{p-1}\right) = (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0} + r$. This is always

$\geq r$ and tends to infinity as $n \rightarrow \infty$. Hence $\exp(x)$ converges to an element of $\pi^r \mathcal{O}_K$. The same argument works for \log . \square

Lemma 9.3. We have $\mathcal{F}(\pi^r \mathcal{O}_K)/\mathcal{F}(\pi^{r+1} \mathcal{O}_K) \cong (k, +) \forall r \geq 1$.

Proof. Our definition of a formal group gives $F(X, Y) = X + Y + XY(\dots)$. So if $x, y \in \mathcal{O}_K$, then $F(\pi^r x, \pi^r y) \equiv \pi^r(x + y) \pmod{\pi^{r+1}}$. Therefore $\mathcal{F}(\pi^r \mathcal{O}_K) \rightarrow (k, +)$ by $\pi^r x \mapsto x \pmod{\pi}$ is a surjective group homomorphism with kernel $\mathcal{F}(\pi^{r+1} \mathcal{O}_K)$. \square

Corollary 9.4. If $|k| < \infty$, then $\mathcal{F}(\pi \mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

Notation. Denote reduction mod π , $\mathcal{O}_K \rightarrow \mathcal{O}_K/\pi \mathcal{O}_K = k$ by $x \mapsto \tilde{x}$.

Proposition 9.5. Let E/K be an elliptic curve. Then the reductions mod π of any two minimal Weierstrass equations for E define isomorphic curves over k .

Proof. Say the Weierstrass equations are related by $[u, r, s, t]$ with $u \in K^\times, r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$, but both equations are minimal, so $v(u) = 0 \implies u \in \mathcal{O}_K^\times$. The transformation formulae (on the formula sheet) for the a_i and b_i combined with the fact that \mathcal{O}_K is algebraically closed imply $r, s, t \in \mathcal{O}_K$. The Weierstrass equations of the reduction mod π are now related by $[\tilde{u}, \tilde{r}, \tilde{s}, \tilde{t}]$ with $\tilde{u} \in k^\times, \tilde{r}, \tilde{s}, \tilde{t} \in k$. \square

Definition 9.2. The reduction \tilde{E}/k of E/K is defined by the reduction mod π of a minimal Weierstrass equation for E . We say E has **good reduction** if \tilde{E} is nonsingular (and so \tilde{E} is an elliptic curve), otherwise E has **bad reduction**.

For an integral Weierstrass equation,

- $v(\Delta) = 0 \implies$ good reduction.
- $0 < v(\Delta) < 12 \implies$ bad reduction.
- $v(\Delta) \geq 12 \implies$ beware that the equation might not be minimal, more information is needed.

There is a well-defined map $\mathbb{P}^2(K) \rightarrow \mathbb{P}^2(k)$ by $(x : y : z) \mapsto (\tilde{x} : \tilde{y} : \tilde{z})$. (Here we must choose a representative for $(x : y : z)$ such that $\min(v(x), v(y), v(z)) = 0$.) We restrict to get a map $E(K) \rightarrow \tilde{E}(k)$ by $P \mapsto \tilde{P}$.

If $P = (x, y) \in E(K)$, then by Lemma 9.1, either $x, y \in \mathcal{O}_K$, so $\tilde{P} = (\tilde{x}, \tilde{y}) \in \tilde{E}(k)$, or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$, so $P = (x : y : 1) = (\pi^{3s}x : \pi^{3s}y : \pi^{3s})$, so $\tilde{P} = (0 : 1 : 0)$. Therefore

$$\hat{E}(\pi\mathcal{O}_K) = E_1(K) = \{P \in E(K) \mid \tilde{P} = 0\},$$

the **kernel of reduction**. Let

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

We have a remarkable fact: the chord and tangent process still defines a group law on \tilde{E}_{ns} . However, in the case of bad reductions, either $\tilde{E}_{\text{ns}} \cong \mathbb{G}_a$ or $\tilde{E}_{\text{ns}} \cong \mathbb{G}_m$ (the additive reduction or the multiplicative reduction).