Part III - Elliptic Curves

Lectured by Tom Fisher

Artur Avameri

Contents

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 $\left(\frac{b}{2}\right)^2=\frac{c+a}{2}\frac{c-a}{2}$, 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 $\left(\frac{u+v}{2},\frac{u-v}{2},\frac{w}{2}\right)$. 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 $\left(\frac{c+d}{2}\right)^2+\left(\frac{c-d}{2}\right)^2=\frac{c^2+d^2}{2}=u=a^2$. This gives a primitive triangle with area $\frac{c^2-d^2}{8}=\frac{v}{4}=\left(\frac{b^2}{2}\right)$.

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 $4w_1^2 = b^2 = v \mid w^2 \implies w_1 \le \frac{w}{2}$, so we're done by infinite descent. $\square$

A variant for polynomials. In the above, K is a field with char $K \neq 2$. Let $\overline{K}$ be the algebraic closure of K and consider for this whole section K with 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 $\max(\deg(a), \deg(b)) \le \frac{1}{2}\max(\deg(u), \deg(v))$, 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

22 Jan 2024, Lecture 2

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

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 $\mathbb{A}^1 \to \mathbb{A}^2$ 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 $\mathrm{ord}_P(f)$ for the order of vanishing of $f \in K(C)$ at P (which is negative if f has a pole at P).

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

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

Example 2.2. $C = \{g = 0\} \subset \mathbb{A}^2$ for $g \in K[x, y]$. Then $K(C) = \mathrm{Frac}\left(\frac{K[x,y]}{(g)}\right)$. 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 $\{Y^2 Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2$. This has only one point at infinity, $P = (0 : 1 : 0)$. Our aim is to compute $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$.

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

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

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 $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$. The Riemann–Roch space of $D \in \mathrm{Div}(C)$ is

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

i.e. the K–vector space of rational functions on C with "poles no worse than specified by D".

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 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 $T_pC = \{Z = 0\}$. 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 contradition 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:

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

2.1 The degree of a morphism

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then $\phi^* : K(C_2) \to K(C_1)$ 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 $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then

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

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

We don't prove this.

In particular, this shows that:

- ϕ is surjective (very important here that we're in $\overline{K}$).
- $|\phi^{-1}(Q)| \leq \deg \phi$.
- 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

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

where $f_0, \ldots, f_n \in K(C)$ 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 $O = O_E$.

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 O_E to $(0 : 1 : 0)$.

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

Fact. If $D \in \mathrm{Div}(E)$ 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 $\mathrm{Gal}(\overline{K}/K)$ (this is unimportant for us and we just write it down to be rigorous).

Proof. $\mathcal{L}(2\cdot O_E)\subset\mathcal{L}(3\cdot O_E)$. Pick bases $1,x$ and $1,x,y$. Note $\operatorname{ord}_{O_E}(x)=-2$ and $\operatorname{ord}_{O_E}(y)=-3$ (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 $\mathcal{L}(6O_E)$ (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 $\mathcal{L}(6O_E)$. 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 $\phi:E\to E'\subset\mathbb{P}^2$ 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 $O_E\mapsto(0:1:0)$.

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

$$[K(E):K(x)]=\deg(E\xrightarrow{x}\mathbb{P}^1)=\operatorname{ord}_{O_E}\left(\frac{1}{x}\right)=2$$
$$[K(E):K(y)]=\deg(E\xrightarrow{y}\mathbb{P}^1)=\operatorname{ord}_{O_E}\left(\frac{1}{y}\right)=3.$$

This gives an inclusion of fields $K(x)\le K(E)$ of degree 2, $K(y)\le K(E)$ of degree 3, while $K(x),K(y)\le K(x,y)\le K(E)$, 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

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

for $r,s,t,u\in K$ with $u\neq0$.

Proof. $\mathcal{L}(2\cdot O_E)=\langle1,x\rangle=\langle1,x'\rangle\implies x=\lambda x'+r$ for some $\lambda,r\in K,\lambda\neq0$. Similarly $\mathcal{L}(3\cdot O_E)=\langle1,x,y\rangle=\langle1,x',y'\rangle\implies y=\mu y'+\sigma x'+t$ for some $\mu,\sigma,t\in K,\mu\neq0$.

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 $\iff$ $\Delta(a_1, \ldots, a_6) \neq 0$, where $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$ is a certain polynomial.

If 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 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 $\iff$ $\begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ 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. $E \cong E' \implies j(E) \cong j(E')$ and the converse holds if $K = \overline{K}$.

Proof. $E \cong E'$ $\iff$ $\begin{cases} a' &= u^4 a \\ b' &= u^6 b \end{cases}$ 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 $O_E \in E(K)$ (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 3^{rd} point of intersction of PQ with E and then let R be the 3^{rd} intersection of $O_E S$ 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) O_E is the identity, since the line through $O_E P$ meets S for the 3^{rd} time at S and then SP meets E for the 3^{rd} time at O_E (drawing a picture makes this obvious).

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

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

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

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

We define $\psi : E \to \mathrm{Pic}^0(E)$ by $P \mapsto [(P) - (O_E)]$.

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 $O_E S$ be given by $l = 0$ and $m = 0$. Then

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

hence $(P) + (Q) \sim (P \oplus Q) + (O_E)$, so $(P \oplus Q) - (O_E) \sim (P) - (O_E) + (Q) - (O_E)$, 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 $\mathrm{div}(f) = (P) - (O_E) - (Q) + (O_E) = (P) - (Q) \implies E \xrightarrow{f} \mathbb{P}^1$ 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 $[D] \in \mathrm{Pic}^0(E)$. Then $D + (O_E)$ has degree 1, so by Riemann–Roch, $\dim \mathcal{L}(D + (O_E)) = 1$, so $\exists 0 \neq f \in \overline{K}(E)$ such that $\mathrm{div}(f) + D + (O_E) \geq 0$, but $\mathrm{div}(f) + D + (O_E)$ has degree 1, so $\mathrm{div}(f) + D + (O_E) = (P)$ for some $P \in E \implies (P) - (O_E) \sim D \implies \psi(P) = [D]$. $\square$

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

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

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

It remains to find formulas for λ and ν.

- Case 1. $x_1 = x_2$, but $P_1 \neq P_2$. Then $P_1 \oplus P_2 = O_E$.
- 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 O_E by definition.
- We have closure and inverses through the formulae above.
- Associativity and commutativity is inherited.

$\square$

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

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

are morphisms of algebraic varieties.

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

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

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

For $P \in E$, let $\tau_P : E \to E$ 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

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

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

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 $[K : Q] < \infty$, $E(K)$ 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 $A \cong$ (finite subgroup) $\times\, \mathbb{Z}^r$. Here r is called the rank of A. The proof of Mordell–Weil gives an upper bound for 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 $\mathbb{C}/\Lambda$ correspond bijectively with Λ–invariant meromorphic functions in $\mathbb{C}$. The function field of $\mathbb{C}/\Lambda$ 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 $[n] : E \to E$ be given by $P \mapsto \underbrace{P \oplus P \oplus \ldots \oplus P}_{n \text{ copies}}$ 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 and (1) holds if $\operatorname{char} K \nmid n$.