Talk 2: Elliptic Curves

Anish Ray
University of Muenster

04 May 2022

Aim of the talk

(*i*) Define the notion of an elliptic curve and show that each elliptic curve has a Weierstrass equation.
(*ii*) Use the Riemann–Roch theorem to describe a group law on the points of an elliptic curve E and show that it is equivalent to the "geometric group law" described by the **Composition Law** in the last talk.
(*iii*) Conclude by showing that the group operations on an elliptic curve define morphisms.

Notations

- K perfect field, i.e., every algebraic extension of K is separable,
- $\bar{K}$ a fixed algebraic closure of K,
- K^* group of units of K,
- E a smooth curve,
- E/K E is defined over K,
- $K(E)$ the function field of E over K,

Let E be a smooth curve of genus one. For example, the nonsingular Weierstrass equations studied in the last talk define curves of this sort. As we have seen, such Weierstrass curves can be given the structure of an abelian group. In order to make a set into a group, clearly an initial requirement is to choose a distinguished (identity) element. This leads to the following definition.

Definition. *An elliptic curve is a pair (E, O), where E is a nonsingular curve of genus one and $O \in E$. The elliptic curve E is defined over K, if E is defined over K as a curve and $O \in E(K)$.*

Next, we use the Riemann–Roch theorem to show that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve in order to connect the definition above to the material covered in the last talk.

Proposition 1. *Let E be an elliptic curve defined over K.*
(a) There exist functions $x, y \in K(E)$ such that the map

$$\phi : E \to \mathbb{P}^2, \quad \phi = [x, y, 1],$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \cdots, a_6 \in K$ and satisfying $\phi(O) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E.
(b)Any two Weierstrass equations for E as in (a) are related by a linear change of variables of the form

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

with $u \in K^*$ and $r, s, t \in K$.
(c) Conversely, every smooth cubic curve C given by a Weierstrass equation as in (a) is an elliptic curve defined over K with base point $O = [0, 1, 0]$.

Proof. We look at the vector spaces $\mathcal{L}(n(O))$ for $n = 1, 2, \cdots$. By the corollary (II.5.5(c)), with $g = 1$, we have

$$l(n(O)) = \dim \mathcal{L}(n(O)) = n, \quad \forall n \geq 1.$$

Thus we can choose functions $x, y \in K(E)$ as in Proposition (II.5.8) so that $\{1, x\}$ is a basis for $\mathcal{L}(2(O))$ and so that $\{1, x, y\}$ is a basis for $\mathcal{L}(3(O))$. Note that x must have a pole of exact order 2 at O, and similarly y must have a

pole of exact order 3 at O. Now we observe that $\mathcal{L}(6(O))$ has dimension 6, but it contains the seven functions

$$1, x, y, x^2, xy, y^2 \text{ and } x^3.$$

It follows that there is a linear relation

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7y^3 = 0,$$

where by Proposition (II.5.8) we may take $A_1, \cdots, A_7 \in K$. Note that $A_6A_7 \neq 0$, since otherwise every term would have a pole at O of a different order, and so all of the A_j 's would vanish. Replacing x and y by $-A_6A_7x$ and $A_6A_7^2y$, respectively, and dividing by $A_6^3A_7^4$, we get a cubic equation in Weierstrass form. This gives a map

$$\phi : E \to \mathbb{P}^2, \quad \phi = [x, y, 1],$$

whose image C lies in the locus described by a Weierstrass equation. Note that $\phi : E \to C$ is a morphism from Proposition (II.2.1), and that it is surjective from Theorem (II.2.3). Further, we have $\phi(O) = [0, 1, 0]$, since y has a higher-order pole than x at the point O. The next step is to show that the map $\phi : E \to C \subset \mathbb{P}^2$ has degree-one, or equivalently, to show that $K(E) = K(x, y)$. Consider the map $[x, 1] : E \to \mathbb{P}^1$. Since x has a double pole at O and no other poles, Proposition (II.2.6(a)) says that this map has degree 2. Thus $[K(E) : K(x)] = 2$. Similarly, the map $[y, 1] : E \to \mathbb{P}^1$ has degree 3, so $[K(E) : K(y)] = 3$. Therefore, $[K(E) : K(x, y)]$ divides both 2 and 3, so it must equal 1. Next we show that C is smooth. Suppose that C is singular. Then from Theorem (III.1.6), there is a rational map $\psi : C \to \mathbb{P}^1$ of degree one. It follows that the composition $\psi \circ \phi : E \to \mathbb{P}^1$ is a map of degree one between smooth curves, so from corollary (II.2.4.1), it is an isomorphism. This contradicts the fact that E has genus one and $\mathbb{P}^1$ has genus zero. Therefore C is smooth, and now another application of corollary (II.2.4.1) shows that the degree one map $\phi : E \to C$ is an isomorphism.
(b) Let $\{x, y\}$ and $\{x', y'\}$ be two sets of Weierstrass coordinate functions on E. Then x and x' have poles of order 2 at O, and y and y' have poles of order 3 at O. Hence $\{1, x\}$ and $\{1, x'\}$ are both bases for $\mathcal{L}(2(O))$, and similarly $\{1, x, y\}$ and $1, x', y'$ are both bases for $\mathcal{L}(3(O))$. Thus there are constants

$$u_1, u_2 \in K^* \quad \text{and } r, s_2, t \in K$$

such that

$$x = u_1x' + r \quad \text{and } y = u_2y' + s_2x' + t.$$

Since both (x, y) and (x', y') satisfy Weierstrass equations in which the Y^2 and X^3 terms have coefficient 1, we have $u_1^3 = u_2^2$. Letting $u = u_2/u_1$ and $s = s_2/u^2$ puts the change of variables formula into the desired form.
(c) Let E be given by a nonsingular Weierstrass equation. We have seen in Proposition (III.1.5) that the differential

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

has neither zeros nor poles, so $div(\omega) = 0$. Corollary (II.5.5(b)) then tells us that

$$2\text{genus}(E) - 2 = \deg \text{div}(\omega) = 0$$

so E has genus one, and taking $[0, 1, 0]$ as the base point makes E into an elliptic curve. □

Remark 1. *Note that proposition* $1(b)$ *does not imply that if two Weierstrass equations have coefficients in a given field* K*, then every change of variables mapping one to the other has coefficients in* K*.*

Lemma 1. *Let* C *be a curve of genus one and let* $P, Q \in C$*. Then*

$$(P) \sim (Q) \Leftrightarrow P = Q.$$

Proof. Suppose that $(P) \sim (Q)$, and choose $f \in \bar{K}(C)^*$ such that $\text{div}(f) = (P) - (Q)$. Then $f \in \mathcal{L}((Q))$. The Riemann-Roch theorem tells us that $\dim \mathcal{L}((Q)) = 1$. But $\mathcal{L}((Q))$ certainly contains the constant functions; hence $f \in \bar{K}$ and $P = Q$. □

Proposition 2. *Let* (E, O) *be an elliptic curve.*
*(a) For every degree-*0 *divisor* $D \in Div^0(E)$ *there exists a unique point* $P \in E$ *satisfying*

$$D \sim (P) - (O).$$

Define $\sigma : Div^0(E) \to E$ *to be the map that sends* D *to its associated* P*.*
(b) The map σ *is surjective.*
(c) Let $D_1, D_2 \in Div^0(E)$*. Then* $\sigma(D_1) = \sigma(D_2) \Leftrightarrow D_1 \sim D_2$*. Thus* σ *induces a bijection of sets (which we also denote by* σ*)*

$$\sigma : Pic^0(E) \xrightarrow{\sim} E.$$

(d) The inverse to σ *is the map*

$$\kappa : E \xrightarrow{\sim} Pic^0(E), \quad P \mapsto (\textit{divisor class of } (P) - (O)).$$

(e) If E *is given by a Weierstrass equation, then the "geometric group law" on* E *described by the* ***Composition Law*** *and the "algebraic group law" induced from* $Pic^0(E)$ *using* σ *are the same.*

Proof. (a) Since E has genus one, the Riemann–Roch theorem says that $\dim \mathcal{L}(D+(O)) = 1$. Let $f \in \bar{K}(E)$ be a nonzero element of $\mathcal{L}(D+(O))$, so f is a basis for this one-dimensional vector space. Since $\operatorname{div}(f) \geq -D-(O)$ and $\deg(\operatorname{div}(f)) = 0$, so it follows that $\operatorname{div}(f) = -D-(O)+(P)$ for some $P \in E$. Hence

$$D \sim (P) - (O),$$

which gives the existence of a point with the desired property. Next, suppose that $P' \in E$ has the same property. Then

$$(P) \sim D + (O) \sim (P')$$

so Lemma 1 tell us that $P = P'$. Hence, P is unique.
(b) For any $P \in E$ we have,

$$\sigma((P) - (O)) = P.$$

(c) Let $D_1, D_2 \in \operatorname{Div}^0(E)$, and set $P_i = \sigma(D_i)$, $i = 1, 2$. Then we have, $(P_1) - (P_2) \sim D_1 - D_2$. Thus, if $P_1 = P_2$, then $D_1 \sim D_2$; and conversely, if $D_1 \sim D_2$, then $P_1 = P_2$.
(d) This is trivial.
(e)Let E be given by a Weierstrass equation and let $P, Q \in E$. It suffices to show that

$$\kappa(P+Q) = \kappa(P) + \kappa(Q),$$

here the first '+' is addition on E using the composition law, while the second '+' is addition of divisor classes on $\operatorname{Pic}^0(E)$. Let $f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$ give the line L in $\mathbb{P}^2$ going through P and Q, let R be the third point of intersection of L with E, and let $f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ be the line L' through R and O. Then from the definition of addition on E the fact that the line $Z = 0$ intersects E at O with multiplicity 3, we have

$$\begin{aligned} \operatorname{div}(f/Z) &= (P) + (Q) + (R) - 3(O), \\ \operatorname{div}(f'/Z) &= (R) + (P+Q) - 2(O). \end{aligned}$$

Hence, $(P+Q) - (P) - (Q) + (O) = \operatorname{div}(f/f') \sim 0$, so

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0.$$

This proves that κ is a group homomorphism. □

We now prove the fundamental fact that the addition law on an elliptic curve is a morphism. Addition is a map $E \times E \to E$ and the variety $E \times E$ has dimension 2, so we cannot use Theorem (II.2.1) directly; but it will play a crucial role in the proof.

Theorem 2. *Let E/K be an elliptic curve. Then the equations mentioned in the group law algorithm* 0.13 *giving the group law on E define morphisms*

$$+ : E \times E \to E, \qquad (P_1, P_2) \mapsto P_1 + P_2,$$

$$- : E \to E, \qquad P \mapsto -P.$$

Proof. First, the negation map

$$(x, y) \mapsto (x, -y - a_1 x - a_3)$$

is clearly a rational map $E \to E$. Since E is smooth, it follows from Theorem (II.2.1) that negation is a morphism. Next we fix a point $Q \neq O$ on E and consider the translation-by-Q map

$$\tau : E \to E, \qquad \tau(P) = P + Q.$$

From the addition formula given in (III.2.3(c)), this is clearly a rational map; and thus, again using Theorem (II.2.1), it is a morphism. In fact, since τ has an inverse, namely $P \mapsto P - Q$, it is an isomorphism. Finally, consider the general addition map $+ : E \times E \to E$. From $0.13(c)$ we see that it is a morphism except possibly at pairs of points having one of the following forms,

$$(P, P), \quad (P, -P), \quad (P, O), \quad \text{and} \quad (O, P),$$

since for pairs of points not of this form, the rational functions

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

on $E \times E$ are well-defined. To deal with the four exceptional cases, let τ_1 and τ_2 be translation maps as above for points Q_1 and Q_2, respectively. Consider the composition of maps

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

Since the group law on E is associative and commutative, the net effect of the above maps is as follows:

$$\begin{aligned} (P_1, P_2) &\xmapsto{\tau_1 \times \tau_2} (P_1 + Q_1, P_2 + Q_2) \\ &\xmapsto{+} P_1 + Q_1 + P_2 + Q_2 \\ &\xmapsto{\tau_1^{-1}} P_1 + P_2 + Q_2 \\ &\xmapsto{\tau_2^{-1}} P_1 + P_2. \end{aligned}$$

Thus the rational map ϕ agrees with the addition map wherever they are both defined. Further, since the τ_i's are isomorphisms, it follows from the above discussion that ϕ is a morphism except possibly at pairs of points of the form

$$(P-Q_1, P-Q_2), \quad (P-Q_1, -P-Q_2), \quad (P-Q_1, -Q_2), \quad \text{and} (-Q_1, P-Q_2).$$

But Q_1 and Q_2 are arbitrary points. Hence by varying Q_1 and Q_2, we can find a finite set of rational maps

$$\phi_1, \phi_2, \cdots, \phi_n : E \times E \to E$$

with the following properties:
(i) ϕ_1 is the addition map given in 0.13(c).
(ii) For each $(P_1, P_2) \in E \times E$, some ϕ_i is defined at (P_1, P_2).
(iii) If ϕ_i and ϕ_j are both defined at (P_1, P_2), then $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.
It follows that addition is defined on all of $E \times E$, so it is a morphism. □

Remark 2. *During the course of proving Theorem* 2*, we noted that the formulas in (III.2.3(c)) make it clear that the addition map* $+ : E \times E \to E$ *is a morphism except possibly at pairs of points of the form* $(P, \pm P)$*,* (P, O)*, or* (O, P)*. Rather than using translation maps to circumvent this difficulty, one can work directly with the definition of morphism using explicit equations.*

References

[1] Joseph H. Silverman *The Arithmetic of Elliptic Curves*, Springer 2nd edition.