The group law on elliptic curves

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden

Elliptic curves

"The theory of elliptic curves is a showpiece of modern mathematics."

Elliptic curves play a key role both in the proof of *Fermat's Last Theorem* and in the construction of the best *cryptographic schemes* available.

Undergraduates have good reasons to wish to know more about elliptic curves. What can we teach them?

The first non-trivial theorem

Let k be a field. An *elliptic curve* over k is a "smooth curve" defined by an equation of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with all $a_i \in k$.

Fact. *The set of points in the "projective plane" over k that satisfy the equation has a "natural addition law" that turns it into an abelian group.*

To be done:

1: Turn the **Fact** into a **Theorem**: define everything!

2: Prove the **Theorem**.

What I shall do

1: I will briefly recall the algebraic definitions of the geometric terms to be used. A good reference: *Ideals, varieties and algorithms*, by Cox, Little, & O'Shea.
I will define the addition law.

2: I will outline a proof that we do get an abelian group. The proof depends on basic properties of *commutative rings*. I shall use a ring that has a formal resemblance to the ring $\mathbf{Z}[\mathrm{i}]$ of *Gaussian integers*.

Promise: all details I omit are indeed details.

Zero sets of polynomials

Let k be a field with algebraic closure $\bar{k}$, and $n \in \mathbf{Z}_{\geq 0}$. Projective n-space over k is

$$\mathbf{P}^n(k) = (k^{n+1} \backslash \{0\})/k^*.$$

For $F \in k[X_0, \ldots, X_n]$ non-zero and homogeneous, put

$$\mathrm{Z}(F) = \{(x_0 : \ldots : x_n) \in \mathbf{P}^n(\bar{k}) : F(x_0, \ldots, x_n) = 0\}.$$

It is a *hypersurface of degree* $\deg F$ in $\mathbf{P}^n(\bar{k})$, defined over k.

If $n = 1$, then $\mathrm{Z}(F)$ consists of $\deg F$ points, counting multiplicities: $\mathrm{Z}(F) = \{\!\{P_1, \ldots, P_{\deg F}\}\!\}$. The bold-faced braces indicate that this is a set *with multiplicities*.

Plane curves

Now let $n = 2$, and write X, Y, Z for X_0, X_1, X_2.

A hypersurface in $\mathbf{P}^2(\bar{k})$ is called a *plane curve*, and if the degree is 1 it is called a *line*:

$$L = \mathrm{Z}(aX + bY + cZ) \quad \text{with } a, b, c \text{ not all } 0.$$

One may identify a line L with $\mathbf{P}^1(\bar{k})$. If $aX + bY + cZ$ does not divide F, then $L \cap \mathrm{Z}(F)$ will be identified with a hypersurface of degree $\deg F$ in $\mathbf{P}^1(\bar{k})$, so it consists of $\deg F$ points: $L \cap \mathrm{Z}(F) = \{P_1, \ldots, P_{\deg F}\}$.

Non-singular points

Let $F \in k[X, Y, Z]$ be non-zero and homogeneous, with partial derivatives F_X, F_Y, F_Z. We call a point $P = (x : y : z) \in \mathrm{Z}(F)$ *non-singular* if not all of

$$a = F_X(x, y, z), \quad b = F_Y(x, y, z) \quad c = F_Z(x, y, z)$$

are zero. In that case $L = \mathrm{Z}(aX + bY + cZ)$ is the unique *tangent line* to $\mathrm{Z}(F)$ through P, in the sense that P is a point of $L \cap \mathrm{Z}(F)$ of multiplicity at least 2.

The curve $\mathrm{Z}(F)$ is called *smooth* if all $P \in \mathrm{Z}(F)$ are non-singular.

Weierstrass curves

Let k be a field. We call a polynomial W of the form

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

with all $a_i \in k$ a *Weierstrass polynomial* over k. The plane curve $\mathrm{Z}(W)$ of degree 3 is called a *Weierstrass curve* over k. It is an *elliptic curve* if it is smooth.

Let $E = \mathrm{Z}(W)$ be a Weierstrass curve over k. Write

$$E(k) = E \cap \mathbf{P}^n(k),$$

$$E(k)_{\mathrm{ns}} = \{\text{non-singular points on } E(k)\}.$$

Note: $O = (0 : 1 : 0) \in E(k)_{\mathrm{ns}}$.

The chord and tangent process

Let E be a Weierstrass curve over a field k.

Theorem. *Let L be a line in $\mathbf{P}^2(\bar{k})$ with $L \cap E = \{P, Q, R\}$. Suppose that P and Q belong to $E(k)_{\mathrm{ns}}$. Then so does R.*

Put $P + Q = S$ if there are lines L and M in $\mathbf{P}^2(\bar{k})$ such that $L \cap E = \{P, Q, R\}$ and $M \cap E = \{O, R, S\}$. This is a well-defined operation on $E(k)_{\mathrm{ns}}$!

Theorem. *The operation $+$ makes $E(k)_{\mathrm{ns}}$ into an abelian group with neutral element O.*

Two examples

Put $k = \mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$, and let E_1 and E_2 be the Weierstrass curves over k defined by

$$W_1 = Y^2Z + XYZ - X^3 - X^2Z,$$
$$W_2 = Y^2Z + XYZ - X^3 - XZ^2.$$

Then $E_1(k)$ and $E_2(k)$ both consist of the four points

$$(0:1:0), (0:0:1), (1:0:1), (1:1:1).$$

The point $(0:0:1)$ is singular on E_1 and non-singular on E_2, and the other points are non-singular on both.

The group $E_1(k)_{\mathrm{ns}}$ consists of three collinear points, and is cyclic of order 3. The group $E_2(k)_{\mathrm{ns}}$ is cyclic of order 4.

Infinite and finite points

Generally, $O = (0 : 1 : 0)$ is the only point on $E(k)$ with $z = 0$. It is non-singular, with tangent line $\mathrm{Z}(Z)$, and $\mathrm{Z}(Z) \cap E(k) = \{O, O, O\}$.

A "finite" point $(x : y : 1)$ is on $E(k)$ if and only if $w = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$ vanishes in (x, y).

The point $(0 : 0 : 1)$ is a singular point on $E(k)$ if and only if w is in the $k[X, Y]$-ideal $(X^2, XY, Y^2) = (X, Y)^2$.

Likewise, $(x : y : 1)$ is a singular point on $E(k)$ if and only if $w \in (X - x, Y - y)^2$.

The hero of the story

We write $A = k[X, Y]/(w)$, which is a commutative ring containing k.

Each finite $(x : y : 1) \in E(k)$ gives a *ring homomorphism* $\varphi\colon A \to k$ with $X \mapsto x$, $Y \mapsto y$, and an *ideal* $\mathfrak{m} = \ker \varphi$.

The set $E(k)\backslash\{O\}$ is in bijection with the set of A-ideals $\mathfrak{m}$ with $\dim_k(A/\mathfrak{m}) = 1$.

The set $E(k)_{\mathrm{ns}}\backslash\{O\}$ is in bijection with the set of A-ideals $\mathfrak{m}$ with $\dim_k(A/\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

Hence $E(k)_{\mathrm{ns}}$ is in bijection with the set of A-ideals $\mathfrak{m}$ with $\dim_k(A/\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

Euclidean rings

The ring $\mathbf{Z}$ comes with the function $\mathbf{Z} \to \mathbf{Z}_{\geq 0}$, $n \mapsto |n|$. It satisfies

$$|nm| = |n| \cdot |m|, \quad |n| = \#(\mathbf{Z}/n\mathbf{Z}) \ \text{ (for } n \neq 0).$$

For a field k, the polynomial ring $k[X]$ comes with the function $\deg\colon k[X]\backslash\{0\} \to \mathbf{Z}_{\geq 0}$. It satisfies

$$\deg(fg) = \deg f + \deg g, \quad \deg f = \dim_k(k[X]/(f))$$

because $1, X, \ldots, X^{(\deg f)-1}$ yield a k-basis for $k[X]/(f)$.

Gaussian integers

The ring of *Gaussian integers* is

$$\mathbf{Z}[\mathrm{i}] = \{a + b\mathrm{i} : a, b \in \mathbf{Z}\}.$$

It has a ring automorphism $^-$ defined by $\overline{a + b\mathrm{i}} = a - b\mathrm{i}$, and a *norm map* $\mathbf{Z}[\mathrm{i}] \to \mathbf{Z}$ sending $\alpha = a + b\mathrm{i}$ to $\alpha\bar{\alpha} = a^2 + b^2$.

The norm map makes $\mathbf{Z}[\mathrm{i}]$ into a Euclidean ring.

The counting norm

Theorem. *One has* $\#\mathbf{Z}[\mathrm{i}]/\alpha\mathbf{Z}[\mathrm{i}] = \alpha\bar{\alpha}$ *for* $\alpha \neq 0$.

Proof. Put $\mathfrak{N}(\alpha) = \#\mathbf{Z}[\mathrm{i}]/\alpha\mathbf{Z}[\mathrm{i}]$. One has:

- $\mathfrak{N}(\alpha) = \mathfrak{N}(\bar{\alpha})$ because $\#\mathbf{Z}[\mathrm{i}]/\alpha\mathbf{Z}[\mathrm{i}] \cong \#\mathbf{Z}[\mathrm{i}]/\bar{\alpha}\mathbf{Z}[\mathrm{i}]$.
- $\mathfrak{N}(m) = m^2$ for $m \in \mathbf{Z}\backslash\{0\}$ because
$$\mathbf{Z}[\mathrm{i}]/m\mathbf{Z}[\mathrm{i}] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \text{ as groups.}$$
- $\mathfrak{N}(\alpha\beta) = \mathfrak{N}(\alpha)\mathfrak{N}(\beta)$ because of the exact sequence
$$0 \to \mathbf{Z}[\mathrm{i}]/\alpha\mathbf{Z}[\mathrm{i}] \xrightarrow{\beta} \mathbf{Z}[\mathrm{i}]/\alpha\beta\mathbf{Z}[\mathrm{i}] \to \mathbf{Z}[\mathrm{i}]/\beta\mathbf{Z}[\mathrm{i}] \to 0.$$

Now $\mathfrak{N}(\alpha)^2 = \mathfrak{N}(\alpha)\mathfrak{N}(\bar{\alpha}) = \mathfrak{N}(\alpha\bar{\alpha}) = (\alpha\bar{\alpha})^2$, done!

An analogous ring

One has

$$\mathbf{Z}[\mathrm{i}] \cong \mathbf{Z}[Y]/(Y^2+1), \quad \mathbf{Z}[\mathrm{i}] = \mathbf{Z} \oplus \mathbf{Z}\mathrm{i}, \quad \mathrm{i}^2 = -1.$$

With $w = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$ we defined

$$A = k[X,Y]/(w).$$

Write $w = Y^2 - uY - v$ with u, $v \in k[X]$. Then if Y denotes the coset $Y + (w)$, one has

$$A = k[X][Y]/(Y^2 - uY - v) = k[X] \oplus k[X]\mathrm{Y},$$
$$\mathrm{Y}^2 = v + u\mathrm{Y}, \quad \deg u \leq 1, \quad \deg v = 3.$$

The counting norm again

Analogously to $Y^2 + 1 = (Y - \mathrm{i})(Y - \bar{\mathrm{i}})$, one has

$$Y^2 - uY - v = (Y - \mathrm{Y})(Y - \bar{\mathrm{Y}}),$$

where $\bar{\mathrm{Y}} = u - \mathrm{Y}$. This gives rise to a ring automorphism

$$^- : A \to A, \quad \overline{f + g\mathrm{Y}} = f + g\bar{\mathrm{Y}} \quad (f, g \in k[X])$$

and to a norm map $A \to k[X]$ sending $\alpha = f + g\mathrm{Y} \in A$ to $\alpha\bar{\alpha} = f^2 + fgu - g^2v \in k[X]$.

Theorem. *One has* $\dim_k(A/\alpha A) = \deg(\alpha\bar{\alpha})$ *for* $\alpha \neq 0$.

This is proved exactly as for $\mathbf{Z}[\mathrm{i}]$!

The degree of the norm

For $\alpha = f + g\mathrm{Y} \in A$ one has

$\deg(\alpha\bar{\alpha}) = \deg(f^2 + fgu - g^2 v) = \max\{2\deg f, 3 + 2\deg g\}$.

It follows that A is a *domain*. Also:

Theorem. *The elements* e_0, e_2, e_3, e_4, ... *of* A *defined by*

$$e_{2j} = X^j, \quad e_{3+2j} = X^j\mathrm{Y} \quad (j \geq 0)$$

form a basis of A *over* k, *and for* $\alpha = \sum_{i \neq 1} c_i e_i \in A$ *(with* $c_i \in k$ *not all zero), one has* $\deg(\alpha\bar{\alpha}) = \max\{i : c_i \neq 0\}$.

The absence of e_1 implies that A is *not Euclidean*.

Poor man's Riemann–Roch

Theorem. *For each ideal* $\mathfrak{a}$ *of* A *there is a unique principal ideal* $\alpha A \subset \mathfrak{a}$ *such that* $\dim_k(\mathfrak{a}/\alpha A) \leq 1$.

Outline of proof. First show that $\dim_k(A/\mathfrak{a}) = m$ (say) is *finite* if $\mathfrak{a} \neq 0$. The $m+1$ elements e_0, e_2, $\ldots$, e_{m+1} become linearly dependent in $A/\mathfrak{a}$, so some non-zero $\alpha = \sum_{1 \neq i \leq m+1} c_i e_i$ is in $\mathfrak{a}$, and then $\dim_k(A/\alpha A) = \max\{i : c_i \neq 0\} \leq m+1$. This proves existence. One proves uniqueness similarly.

One can deduce: A is a PID if and only if $E(k) = \{O\}$.

The Picard group

The *Picard group* $\operatorname{Pic} B$ of a domain B is the set of "equivalence" classes $[\mathfrak{a}]$ of "invertible" ideals $\mathfrak{a} \subset B$, with multiplication $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{ab}]$. It is *abelian*.

Here $\mathfrak{a}$ is *invertible* if $\mathfrak{ab} = \alpha B$ for some ideal $\mathfrak{b}$ and some non-zero $\alpha \in B$.

Two invertible ideals $\mathfrak{a}$, $\mathfrak{b}$ are *equivalent* if there are non-zero α, $\beta \in B$ with $\beta\mathfrak{a} = \alpha\mathfrak{b}$.

We shall show that $E(k)_{\mathrm{ns}}$ is a group by exhibiting a bijection $E(k)_{\mathrm{ns}} \cong \operatorname{Pic} A$.

Putting things together

Reminder: $E(k)_{\mathrm{ns}}$ is in bijection with the set $\mathcal{S}$ of A-ideals $\mathfrak{m}$ with $\dim_k(A/\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

We make $\mathcal{S}$ (and hence $E(k)_{\mathrm{ns}}$) into a group by proving that $\mathfrak{m} \mapsto [\mathfrak{m}]$ defines a bijection $\mathcal{S} \to \operatorname{Pic} A$.

Ingredients of the proof:

- a technical lemma showing that an A-ideal $\mathfrak{m}$ with $\dim_k(A/\mathfrak{m}) = 1$ is in $\mathcal{S}$ if and only if $\mathfrak{m}$ is invertible;

- poor man's Riemann–Roch, which shows that for any $[\mathfrak{a}] \in \operatorname{Pic} A$ there is a unique $\mathfrak{m} \in \mathcal{S}$ with $[\mathfrak{a}][\mathfrak{m}] = 1$.

The technical lemma

Lemma. *Let* $\mathfrak{m} = (\alpha, \beta)$ *be a maximal ideal of a domain* B*. Then:* $\mathfrak{m}$ *is invertible* $\Leftrightarrow \dim_{B/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$.

$\Rightarrow$: use that $\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{m}$ gives a bijection {ideals $\mathfrak{a}$ between B and $\mathfrak{m}$} $\to$ {ideals between $\mathfrak{m}$ and $\mathfrak{m}^2$}.

$\Leftarrow$: if (say) $\mathfrak{m} = \alpha B + \mathfrak{m}^2$ then $\beta \in \alpha B + \mathfrak{m}^2 = (\alpha, \beta^2)$, so there is $\gamma \in B$ with $\beta \equiv \gamma\beta^2 \bmod \alpha B$, and then $\mathfrak{n} = (\alpha, 1 - \gamma\beta)$ satisfies $\mathfrak{m}\mathfrak{n} = \alpha B$.

Summary of the group law

To add P, Q in the group $E(k)_{\mathrm{ns}}$:

- find the corresponding A-ideals $\mathfrak{m}$, $\mathfrak{n} \in \mathcal{S}$;
- compute the ideal product $\mathfrak{mn} = \mathfrak{a}$ in A;
- determine the unique $\mathfrak{l} \in \mathcal{S}$ such that $\mathfrak{al}$ is principal;
- find the point in $E(k)_{\mathrm{ns}}$ corresponding to $\bar{\mathfrak{l}} \in \mathcal{S}$.

That is $P + Q$! Since all proofs are completely explicit, one verifies without trouble that $P + Q$ can equivalently be obtained by the chord and tangent process.

Tableau de la troupe (1)

Euclid of Alexandria, Greek mathematician, ∼300 BC.

Pierre de Fermat, French mathematician, 1601–1665.

Carl Friedrich Gauss, German mathematician, 1777–1855.

Niels Henrik Abel, Norwegian mathematician, 1802–1829.

Karl Weierstrass, German mathematician, 1815–1897.

Bernhard Riemann, German mathematician, 1826–1866.

Tableau de la troupe (2)

Gustav Roch, German mathematician, 1839–1866.

Émile Picard, French mathematician, 1856–1941.

David Cox, American mathematician, 1948.

John Little, American mathematician, 1956.

Donal O'Shea, Canadian mathematician, 1952.