Elliptic curves, Néron models, and duality

Jean Gillibert

Durham, Pure Maths Colloquium

26th February 2007

Elliptic curves and Weierstrass equations

Let K be a field

Definition: An elliptic curve over K is a non-singular projective K-curve of genus 1, together with a K-rational point.

Suppose now that $\mathrm{char}(K) \neq 2, 3$

Let E be an elliptic curve over K. Then E can be defined in the projective plane $\mathbb{P}^2_K$ by an equation in Weierstrass form

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

One defines the discriminant of E as being the quantity

$$\Delta = 4a^3 + 27b^2$$

The fact that E is non-singular is equivalent to the fact that Δ is a non-zero element of K.

Elliptic curves as algebraic groups

let E an elliptic curve, and O its canonical rational point. Then one proves that the map

$$\begin{aligned} E(K) &\longrightarrow \mathrm{Pic}^0(E) \\ P &\longmapsto (P) - (O) \end{aligned}$$

is an isomorphism. This remains true after any base change. From this one deduces the following

Corollary: An elliptic curve has a canonical structure of (commutative) algebraic group.

In fact, E is isomorphic to its Jacobian variety $\underline{\mathrm{Pic}}^0_E$.

The fundamental scheme of arithmetic

Suppose K is a number field. Let $\mathcal{O}_K$ be its ring of integers.

Let $S = \mathrm{Spec}(\mathcal{O}_K)$ be the spectrum of $\mathcal{O}_K$.

S is a scheme of dimension 1 (that is, S is a curve).

Points of S are prime ideals of $\mathcal{O}_K$, including the zero ideal, which is called the generic point.

The generic point is dense in S. Other points are closed in S.

The residue field of a closed point $\mathfrak{p} \in S$ is the quotient $\mathcal{O}_K/\mathfrak{p}$.

The residue field of the generic point is the field K itself.

We denote by $k(s)$ the residue field of a point $s \in S$.

Integral models

An S-scheme is a scheme $\mathcal{X}$ together with a morphism of schemes $f : \mathcal{X} \to S$, called the structural morphism of $\mathcal{X}$.

Let $s \in S$ be a point of S.

The fiber of $\mathcal{X}$ at s, denoted by $\mathcal{X}_{k(s)}$, is by definition the fiber product $\mathcal{X} \times_S k(s)$.

$\mathcal{X}_{k(s)}$ is a variety over the field $k(s)$, which, as a topological space, can be identified with the set $f^{-1}(\{s\})$.

An S-scheme can be seen as a nice (i.e. continuous) family of varieties over the residue fields of the points of S.

An S-model of E is an S-scheme $\mathcal{X}$ whose generic fiber $\mathcal{X}_K$ is isomorphic to E.

Chasing denominators

Let us start from a Weierstrass equation of E

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

where a and b are in K.

Let us write $a = \alpha/d^4$ and $b = \beta/d^6$ where α, β and d are elements of $\mathcal{O}_K$. The equation above can be rewritten

$$d^6y^2 = d^6x^3 + \alpha d^2x + \beta$$

which, after change of variables $\mathrm{Y} = d^3y$, $\mathrm{X} = d^2x$, becomes

$$\mathrm{Y}^2 = \mathrm{X}^3 + \alpha\mathrm{X} + \beta$$

This equation defines a closed subvariety $\mathcal{X}$ of the projective plane $\mathbb{P}^2_S$ over S, which is an S-model of E.

The fibers of $\mathcal{X}$

Let $\mathfrak{p} \in S$ be a closed point of S

The fiber $\mathcal{X}_{k(\mathfrak{p})}$of $\mathcal{X}$ at $\mathfrak{p}$ is obtained by reducing modulo $\mathfrak{p}$ the equation

$$\mathrm{Y}^2 = \mathrm{X}^3 + \alpha\mathrm{X} + \beta$$

If $\mathfrak{p}$ does not divides $4\alpha^3 + 27\beta^2$, then $\mathcal{X}_{k(\mathfrak{p})}$ is an elliptic curve over $k(\mathfrak{p})$; one says that E has *good reduction* at $\mathfrak{p}$.

If $\mathfrak{p}$ divides $4\alpha^3 + 27\beta^2$, then E has *bad reduction* at $\mathfrak{p}$.

In this case, $\mathcal{X}_{k(\mathfrak{p})}$ is a singular cubic curve over $k(\mathfrak{p})$. Let us denote by $\mathcal{X}^{\mathrm{ns}}_{k(\mathfrak{p})}$ the set of its non-singular points. Then $\mathcal{X}^{\mathrm{ns}}_{k(\mathfrak{p})}$ has again an algebraic group structure.

Bad reduction

In this case $\mathcal{X}^{\mathrm{ns}}_{k(\mathfrak{p})}$ is an algebraic group of dimension 1 over $k(\mathfrak{p})$, which is *not* an elliptic curve.

One proves in fact that there are only three types of algebraic groups of dimension 1 over a field :

– elliptic curves

– the multiplicative group $\mathbf{G}_{\mathrm{m}}$ and its quadratic twists

– the additive group $\mathbf{G}_{\mathrm{a}}$

In the second case, we say that E has multiplicative reduction at $\mathfrak{p}$

In the third case, we say that E has additive reduction at $\mathfrak{p}$

Lack of points ?

Let $\mathcal{X}^{\mathrm{sm}}$ be the smooth locus of $\mathcal{X}$; for any closed point $\mathfrak{p} \in S$, the fiber $(\mathcal{X}^{\mathrm{sm}})_{k(\mathfrak{p})}$ is the set $\mathcal{X}^{\mathrm{ns}}_{k(\mathfrak{p})}$ of non-singular points of $\mathcal{X}_{k(\mathfrak{p})}$.

One proves that the group law of E extends to $\mathcal{X}^{\mathrm{sm}}$.

$\mathcal{X}^{\mathrm{sm}}(S)$ can be identified with the elements of $\mathcal{X}(S) = E(K)$ having everywhere non-singular reduction. In general, this is a strict subset of $E(K)$.

We should find a way to recover all the points in our nice model – while still keeping the smoothness and the group law.

Reduction to the strictly local case

If we consider the restriction $\mathcal{X}_U$ of $\mathcal{X}$ to the open subset $U \subseteq S$ where E has good reduction, then $\mathcal{X}_U(U) = E(K)$.

We say that $\mathcal{X}_U$ is an elliptic curve over U.

Now, let $\mathfrak{p} \in S - U$ be a point of bad reduction (there is a finite number of such points).

Let $\mathcal{O}_{K,\mathfrak{p}}$ be the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, and let $S_\mathfrak{p} = \mathrm{Spec}(\mathcal{O}_{K,\mathfrak{p}})$.

Let $\mathcal{O}^{sh}_{K,\mathfrak{p}}$ be the *strict henselization* of $\mathcal{O}_{K,\mathfrak{p}}$. This is a henselian discrete valuation ring, whose residue field is the algebraic closure of the field $k(\mathfrak{p})$. Let $K^{sh}_\mathfrak{p}$ be the fraction field of $\mathcal{O}^{sh}_{K,\mathfrak{p}}$.

Let $S^{sh}_\mathfrak{p} = \mathrm{Spec}(\mathcal{O}^{sh}_{K,\mathfrak{p}})$. The morphism $S^{sh}_\mathfrak{p} \to S_\mathfrak{p}$ is *faithfully flat*; we may work over $S^{sh}_\mathfrak{p}$ and then deduce results over $S_\mathfrak{p}$ by descent.

End of construction

Let us fix a set $x_1, \ldots, x_r$ of representatives of $E(K_{\mathfrak{p}}^{sh}) = \mathcal{X}_{\mathfrak{p}}^{sh}(S_{\mathfrak{p}}^{sh})$ modulo $(\mathcal{X}^{\mathrm{sm}})_{\mathfrak{p}}^{sh}(S_{\mathfrak{p}}^{sh})$.

Let $\mathcal{X}_{\mathfrak{p}}^1, \ldots, \mathcal{X}_{\mathfrak{p}}^r$ be r copies of $(\mathcal{X}^{\mathrm{sm}})_{\mathfrak{p}}^{sh}$, then the map

$$\coprod_{i=1}^r \mathcal{X}_{\mathfrak{p}}^i(S_{\mathfrak{p}}^{sh}) \longrightarrow E(K_{\mathfrak{p}}^{sh})$$

which sends $y \in \mathcal{X}_{\mathfrak{p}}^i(S_{\mathfrak{p}}^{sh})$ to $y + x_i$, is bijective.

Gluing the $\mathcal{X}_{\mathfrak{p}}^i$ along the generic fiber, we obtain an $S_{\mathfrak{p}}^{sh}$-model $\mathcal{E}_{\mathfrak{p}}^{sh}$ of E which is a smooth group scheme over $S_{\mathfrak{p}}^{sh}$, and such that

$$\mathcal{E}_{\mathfrak{p}}^{sh}(S_{\mathfrak{p}}^{sh}) = E(K_{\mathfrak{p}}^{sh}).$$

By descent from $S_{\mathfrak{p}}^{sh}$ to $S_{\mathfrak{p}}$, one gets an $S_{\mathfrak{p}}$-model $\mathcal{E}_{\mathfrak{p}}$ of E satisfying the same properties.

Furthermore, $\mathcal{X}_{\mathfrak{p}}^{\mathrm{sm}}$ is the identity component of $\mathcal{E}_{\mathfrak{p}}$.

The Néron model

Let $\mathcal{E}$ be the S-model obtained by gluing $\mathcal{X}_U$ and the $\mathcal{E}_{\mathfrak{p}}$ over S.

Theorem: $\mathcal{E}$ is a finite type smooth group scheme over S. Moreover, for all $Y \to S$ smooth, the "restriction to the generic fiber" map

$$\mathrm{Hom}_S(Y, \mathcal{E}) \longrightarrow \mathrm{Hom}_K(Y_K, E)$$

is bijective.

Definition: Such a model is called the Néron model of E, it is unique (up to isomorphism).

Remarks: – Smoothness of $\mathcal{E}$ generalizes non-singularity of E.

– We have an isomorphism $\mathcal{E}(S) \simeq E(K)$.

– More generally, for any unramified extension L/K, we have an isomorphism $\mathcal{E}(\mathrm{Spec}(\mathcal{O}_L)) \simeq E(L)$

Duality over a field

All sheaves considered here are for the étale topology.

We have a canonical isomorphism between E and its Jacobian

$$E \xrightarrow{\sim} \underline{\mathrm{Pic}}^0_E$$

In fact, according to André Weil, we have isomorphisms

$$E \xrightarrow{\sim} \underline{\mathrm{Ext}}^1(E, \mathbf{G}_\mathrm{m}) \xrightarrow{\sim} \underline{\mathrm{Pic}}^0_E$$

This means that any zero-degree line bundle $\mathcal{L}$ on E can be endowed with a structure of extension of E by $\mathbf{G}_\mathrm{m}$, i.e. we have a group structure on $\mathcal{L}$ together with an exact sequence

$$0 \longrightarrow \mathbf{G}_\mathrm{m} \longrightarrow \mathcal{L} \longrightarrow E \longrightarrow 0$$

Consequences: the dual isogeny

Let $\phi : E \to F$ be an isogeny, that is, a finite surjective morphism of algebraic groups. Then F is an elliptic curve, and the kernel G of ϕ is a finite flat algebraic group over K.

If we apply the functor $\underline{\mathrm{Hom}}(-, \mathbf{G}_{\mathrm{m}})$ to the exact sequence

$$0 \longrightarrow G \longrightarrow E \xrightarrow{\phi} F \longrightarrow 0$$

we get a (long) exact sequence of cohomology

$$\cdots \to 0 = \underline{\mathrm{Hom}}(E, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Hom}}(G, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Ext}}^1(F, \mathbf{G}_{\mathrm{m}})$$

$$\to \underline{\mathrm{Ext}}^1(E, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Ext}}^1(G, \mathbf{G}_{\mathrm{m}}) = 0 \to \cdots$$

from which one can extract a short exact sequence !

Cartier duality, Weil pairing

We know that $\underline{\mathrm{Ext}}^1(E, \mathbf{G}_\mathrm{m}) \simeq E$ and $\underline{\mathrm{Ext}}^1(F, \mathbf{G}_\mathrm{m}) \simeq F$

Moreover, $\underline{\mathrm{Hom}}(G, \mathbf{G}_\mathrm{m})$ is the Cartier dual G^D of G

The exact sequence above can be rewritten as

$$0 \longrightarrow G^D \longrightarrow F \xrightarrow{\phi^*} E \longrightarrow 0$$

One says that ϕ^* is the dual isogeny of ϕ.

In the case when $\phi = [n]$ is given by the multiplication by an integer n on E, the dual isogeny is $[n]$ itself. We therefore obtain a canonical isomorphism $E[n] \simeq E[n]^D$, together with a pairing

$$E[n] \times_K E[n] \longrightarrow \mathbf{G}_\mathrm{m}$$

This is the so-called Weil pairing (in fact, it has values in μ_n).

Néron models and the smooth site

Let us consider the category of smooth schemes over S, endowed with the étale topology, which we call the *smooth site* over S.

Let $j : \eta \to S$ be the inclusion of the generic point of S. The universal property of the Néron model can be expressed is the language of sheaves in the following way

$$\mathcal{E} = j_* E$$

that is, $\mathcal{E}$ is the direct image of E on the smooth site.

Duality for the Néron model ?

Let us start from the isomorphism

$$E \simeq \underline{\mathrm{Ext}}^1(E, \mathbf{G}_\mathrm{m})$$

It is natural to apply the functor j_* on both sides.

Using the fact that $\underline{\mathrm{Hom}}(\mathcal{E}, \mathbf{G}_\mathrm{m}) = 0$ and $R^1 j_* \mathbf{G}_\mathrm{m} = 0$, we obtain an isomorphism

$$\mathcal{E} \simeq j_* \underline{\mathrm{Ext}}^1(E, \mathbf{G}_\mathrm{m}) \simeq \underline{\mathrm{Ext}}^1(\mathcal{E}, j_* \mathbf{G}_\mathrm{m})$$

Now, we want to compare the sheaves $\underline{\mathrm{Ext}}^1(\mathcal{E}, j_* \mathbf{G}_\mathrm{m})$ and $\underline{\mathrm{Ext}}^1(\mathcal{E}, \mathbf{G}_\mathrm{m})$.

Some more sheaves

Let $\mathcal{E}^0$ be the identity component of $\mathcal{E}$, and let Φ be the quotient sheaf $\mathcal{E}/\mathcal{E}^0$. This is a skyscraper étale sheaf over S, with stalk zero at places of good reduction, and finite stalks otherwise.

In fact, we get a commutative diagram with exact lines

$$\begin{array}{ccccccc} 0 \to & \mathcal{E}^0 & \longrightarrow & \mathcal{E} & \longrightarrow & \Phi \\ & \downarrow & & \| & & \downarrow \\ 0 \to & \underline{\mathrm{Ext}}^1(\mathcal{E}, \mathbf{G}_\mathrm{m}) & \longrightarrow & \underline{\mathrm{Ext}}^1(\mathcal{E}, j_*\mathbf{G}_\mathrm{m}) & \longrightarrow & \underline{\mathrm{Hom}}(\Phi, \mathbb{Q}/\mathbb{Z}) \end{array}$$

The existence of left and right vertical arrows follow from the fact that

$$\mathrm{Hom}(\mathcal{E}^0, \underline{\mathrm{Hom}}(\Phi, \mathbb{Q}/\mathbb{Z})) = 0$$

Grothendieck's pairing

The map $\Phi \to \underline{\mathrm{Hom}}(\Phi, \mathbb{Q}/\mathbb{Z})$ induces a pairing (first defined by Grothendieck in [SGA 7])

$$\Phi \times_S \Phi \to \mathbb{Q}/\mathbb{Z}$$

Which is proved to be non-degenerate in our case.

Thus, we have an isomorphism

$$\mathcal{E}^0 \simeq \underline{\mathrm{Ext}}^1(\mathcal{E}, \mathbf{G}_\mathrm{m})$$

More generally, if Γ and Γ' are subgroups of Φ which are orthogonal under the pairing, then we get an isomorphism

$$\mathcal{E}^\Gamma \simeq \underline{\mathrm{Ext}}^1(\mathcal{E}^{\Gamma'}, \mathbf{G}_\mathrm{m})$$

Néron models and the flat site

Problems: – if G is a finite flat subgroup of $\mathcal{E}$, the quotient $\mathcal{E}/G$ for the étale topology needs not to be representable by a smooth group scheme, unless G is étale over S.

– if G is a finite flat group scheme over S, the sheaf $\underline{\mathrm{Ext}}^1(G, \mathbf{G}_\mathrm{m})$ needs not to be 0 in the smooth site, even if G is étale over S.

A solution is to replace the smooth site by the flat site, that is the category of flat schemes over S, endowed with the fppf topology.

If G is a finite flat subgroup of $\mathcal{E}$, and if $\mathcal{E}$ has semi-stable reduction, the quotient $\mathcal{E}/G$ for the fppf topology is an open subgroup $\mathcal{F}^\Lambda$ of the Néron model $\mathcal{F}$ of $F := E/G_K$.

Another dual exact sequence

from the sequence

$$0 \longrightarrow G \longrightarrow \mathcal{E} \xrightarrow{\phi} \mathcal{F}^{\Lambda} \longrightarrow 0$$

one deduces a sequence

$$0 \longrightarrow G^D \longrightarrow \underline{\mathrm{Ext}}^1(\mathcal{F}^{\Lambda}, \mathbf{G}_{\mathrm{m}}) \xrightarrow{\phi^*} \underline{\mathrm{Ext}}^1(\mathcal{E}, \mathbf{G}_{\mathrm{m}}) \longrightarrow 0$$

Moreover, the group schemes involved here being smooth, one has, by comparison between étale and fppf topology

$$\mathrm{Ext}^1(\mathcal{F}^{\Lambda}, \mathbf{G}_{\mathrm{m}}) = \mathcal{F}^{\Lambda'}(S)$$

$$\mathrm{Ext}^1(\mathcal{E}, \mathbf{G}_{\mathrm{m}}) = \mathcal{E}^0(S)$$

like in the smooth site.