Explicit descent on elliptic curves, I

Tom Fisher

12th July 2005

Abstract

These are my notes for my talk in Bremen, describing part of joint work with Cremona, O'Neil, Simon and Stoll.

Let E be an elliptic curve over a perfect field K. Let $n \geq 2$ be an integer and suppose $\mathrm{char}(K) \nmid n$. Taking Galois cohomology of the exact sequence

$$0 \to E[n] \to E \to E \to 0$$

we obtain the Kummer exact sequence

$$E(K) \to H^1(K, E[n]) \to H^1(K, E).$$

Elements of the group on the left (resp. right) may be intepreted as points (resp. torsors). In the course of this talk we will see several different intepretations of the group in the middle.

We start with an algebraic description in terms of the étale algebra

$$R = \mathrm{Map}_K(E[n], \overline{K}).$$

Notice that R is a product of (finite) field extensions of K. In the case $n = 3$ we would "typically" have $R = K \times L$ where L/K is a field extension of degree 8. This is much better than working with $K(E[3])$. We also write

$$\overline{R} = R \otimes_K \overline{K} = \mathrm{Map}(E[n], \overline{K}).$$

The Weil pairing defines a map

$$w : E[n] \to \mathrm{Map}(E[n], \mu_n) = \mu_n(\overline{R})$$

which induces

$$w_* : H^1(K, E[n]) \to H^1(K, \mu_n(\overline{R})) \simeq R^\times/(R^\times)^n.$$

The isomorphism on the right comes from applying Hilbert's theorem 90 to each constituent field of R.

For $n = p$ a prime, Schaefer and Stoll show that w_* is injective and describe its image. So for K a number field, they can compute $S^{(p)}(E/K)$ as a subgroup of $R^\times/(R^\times)^p$. Their method is actually practical for $K = \mathbf{Q}$ and $n = 3$.

To give other interpretations of $H^1(K, E[n])$ we use the following general principle

"$H^1(K, \mathrm{Aut}(X))$ parametrises twists of X".

Definition 1 *A diagram $[C \to S]$ is a morphism from a torsor C under E to a scheme S. We say that diagrams $[C_1 \to S_1]$ and $[C_2 \to S_2]$ are isomorphic if there is an isomorphism of torsors $C_1 \simeq C_2$ and an isomorphism of schemes $S_1 \simeq S_2$ so that*

$$\begin{array}{ccc} C_1 & \longrightarrow & S_2 \\ \simeq \downarrow & & \downarrow \simeq \\ C_2 & \longrightarrow & S_2 \end{array}$$

commutes.

Lemma 2 $\mathrm{Aut}[E \stackrel{|n.0|}{\to} \mathbb{P}^{n-1}] \simeq E[n]$.

Definition 3 *A Brauer-Severi diagram $[C \to S]$ is a twist of $[E \stackrel{|n.0|}{\to} \mathbb{P}^{n-1}]$.*

It follows that $H^1(K, E[n])$ parametrises Brauer-Severi diagrams. Moreover there is an obstruction map

$$\begin{array}{rcl} H^1(K, E[n]) & \to & \mathrm{Br}(K) \\ [C \to S] & \mapsto & S. \end{array}$$

Our aim may be stated as follows. Given $\alpha \in R^\times/(R^\times)^3$ representing an element of $S^{(3)}(E/K)$, find an equation for the corresponding plane cubic $[C \to \mathbb{P}^2]$. We expect that any successful method will need to use some explicit analogue of the Hasse Principle for Brauer-Severi varieties.

We consider central extensions of $E[n]$ by $\mathbf{G_m}$

$$0 \to \mathbf{G_m} \to \Lambda \to E[n] \to 0.$$

Definition 4 *Extensions Λ_1 and Λ_2 are isomorphic if there is a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G_m} & \longrightarrow & \Lambda_1 & \longrightarrow & E[n] & \longrightarrow & 0 \\ & & \| & & \downarrow \simeq & & \| & & \\ 0 & \longrightarrow & \mathbf{G_m} & \longrightarrow & \Lambda_2 & \longrightarrow & E[n] & \longrightarrow & 0. \end{array}$$

Lemma 5 $\mathrm{Aut}(\Lambda) \simeq \mathrm{Hom}(E[n], \mathbf{G_m}) \simeq E[n]$.

Taking $\Lambda_0 = \mathbf{G_m} \times E[n]$ we identify

$$H^1(K, E[n]) \longleftrightarrow \{\text{twists of} \Lambda_0\}$$

These are the commutative extensions of $E[n]$ by $\mathbf{G_m}$. So in fact we have identified $H^1(K, E[n]) = \mathrm{Ext}^1_K(E[n], \mathbf{G_m})$.

By Hilbert's theorem 90, any central extension Λ has a Galois equivariant section $\phi : E[n] \to \Lambda$. In general ϕ is not a group homomorphism. Any two choices of ϕ differ by an element of

$$\mathrm{Map}_K(E[n], \overline{K}^\times) = R^\times.$$

We define $\alpha \in R^\times$ via

$$\phi(T)^n = \alpha(T) \qquad \text{for all } T \in E[n].$$

This gives a map

$$\begin{array}{rcl} H^1(K, E[n]) & \to & R^\times/(R^\times)^n \\ \Lambda & \mapsto & \alpha \end{array}$$

which turns out to be the map w_* we met before. In particular this map is injective when n is prime, but counterexamples to this statement are known when $n = 4$.

In a variant of this construction we define

$$\rho \in (R \otimes R)^\times = \mathrm{Map}_K(E[n] \times E[n], \overline{K}^\times)$$

via

$$\phi(S)\phi(T) = \rho(S, T)\phi(S + T) \qquad \text{for all } S, T \in E[n].$$

This gives an injection (for every n)

$$\begin{array}{rcl} H^1(K, E[n]) & \to & (R \otimes R)^\times/\partial R^\times \\ \Lambda & \mapsto & \rho \end{array}$$

where $\partial : R^\times \to (R \otimes R)^\times$ is defined by

$$(\partial\gamma)(S,T) = \frac{\gamma(S)\gamma(T)}{\gamma(S+T)}.$$

We write H for the image of $H^1(K, E[n])$ in $(R \otimes R)^\times / \partial R^\times$. It may be characterised by properties derived from the requirements that Λ is commutative and associative. In practice we convert $\alpha \in R^\times$ (as computed by Schaefer and Stoll) to $\rho \in (R \otimes R)^\times$ via $\rho = \sqrt[n]{\partial\alpha}$.

Lemma 6 *Let*

$$0 \to \mathbf{G_m} \to \Lambda \to E[n] \to 0$$

be any central extension of $E[n]$ by $\mathbf{G_m}$. Then there is a unique K-algebra F with $[F : K] = n^2$ such that
(i) there exists $\iota : \Lambda \to (F \otimes_K \overline{K})^\times$ a Galois equivariant group homomorphism that preserves scalars,
(ii) the image of ι spans $\overline{F}$ as a $\overline{K}$-vector space.

If we interpret $H^1(K, E[n])$ as commutative extensions of $E[n]$ by $\mathbf{G_m}$ then F will be a commutative K-algebra. This algebra is closely related to another interpretation of $H^1(K, E[n])$:

$$H^1(K, E[n]) \longleftrightarrow \{E[n]\text{-torsors } E[n] \times \Phi \to \Phi\}.$$

For example the points of inflection of a plane cubic $[C \to \mathbb{P}^2]$ naturally form an $E[3]$-torsor.

Lemma 7 *F is the étale algebra of Φ.*

We give the idea of the proof. We start by taking F to be the étale algebra of Φ. Since $E[n]$ acts on Φ it also acts on $\overline{F}^\times = \mathrm{Map}(\Phi, \overline{K}^\times)$. The eigenvectors for this action form a group

$$\Lambda = \left\{ \alpha \in \overline{F}^\times \;\middle|\; \begin{array}{c} \text{there exists } T \in E[n] \text{ such that} \\ \alpha(S+P) = e_n(S,T)\alpha(P) \text{ for all } S \in E[n], P \in \Phi \end{array} \right\}.$$

We obtain a commutative extension

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{G_m} & \to & \Lambda & \to & E[n] & \to & 0 \\ & & & & \alpha & \mapsto & T. & & \end{array}$$

By construction F is the algebra determined by Λ. (Of course one still has to check that Λ is the right commutative extension.)

In practice F is constructed as follows. The group law

$$E[n] \times E[n] \to E[n]$$

induces a comultiplication

$$\Delta : R \to R \otimes R.$$

Viewing $R \otimes R$ as an R-algebra via Δ there is a trace map

$$\mathrm{Tr} : R \otimes R \to R.$$

It turns out that $F = (R, +, *_\rho)$ where the new multiplication $*_\rho : R \otimes R \to R$ is given by

$$\alpha *_\rho \beta = \mathrm{Tr}(\rho.\alpha \otimes \beta).$$

Thus computing the field of definition of a point of inflection on our plane cubic is much easier than finding an equation for the plane cubic itself. For the latter we have to contend with the obstruction map.

By considering the action of $E[n]$ on the base diagram

$$[E \xrightarrow{|n.0|} \mathbb{P}^{n-1}]$$

we obtain a character $\chi_E : E[n] \to \mathrm{PGL}_n$. Let Θ_E be the inverse image of $\mathrm{im}(\chi_E)$ in GL_n. Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G_m} & \longrightarrow & \Theta_E & \longrightarrow & E[n] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle \chi_E} & & \\ 0 & \longrightarrow & \mathbf{G_m} & \longrightarrow & \mathrm{GL}_n & \longrightarrow & \mathrm{PGL}_n & \longrightarrow & 0. \end{array}$$

Now Θ_E assumes the role played by Λ_0 earlier. We identify

$$H^1(K, E[n]) \longleftrightarrow \{\text{twists of } \Theta_E\}$$

We call these twists theta groups. (They are characterised among all central extension by the fact the commutator is given by the Weil pairing.) Using

theta groups we identify $H^1(K, E[n])$ with a certain coset εH of H in $(R \otimes R)^\times / \partial R^\times$. Here $\varepsilon \in (R \otimes R)^\times$ describes the extension Θ_E itself.

Given a theta group Θ we construct a K-algebra A as in Lemma 6, *i.e.* $[A : K] = n^2$ with $\Theta \hookrightarrow (A \otimes \overline{K})^\times$, etc. In the case of Θ_E the above diagram identifies $A \simeq \mathrm{Mat}(n, K)$. So in general A is a central simple algebra. This gives another interpretation of the obstruction map

$$\begin{array}{rcl} H^1(K, E[n]) & \to & \mathrm{Br}(K) \\ \Theta & \mapsto & A. \end{array}$$

Our algorithm has the following main steps:

1. Start with $\rho \in S^{(n)}(E/K) \subset (R \otimes R)^\times / \partial R^\times$.
2. Compute structure constants for $A = (R, +, *_{\varepsilon\rho})$.
3. Find an isomorphism $A \simeq \mathrm{Mat}(n, K)$.
4. Recover equations for $C \to \mathbb{P}^{n-1}$.
5. Minimise and reduce the equations.

In fact after Step 3 we can compute $M \in \mathrm{GL}_n(R)$ describing the action of $E[n]$ on $[C \to \mathbb{P}^{n-1}]$. In the case $n = 3$ this is usually enough to determine an equation for C via ad hoc methods. (We can compute the pencil of cubics preserved by M and typically only one curve in the pencil will have Jacobian E.) Cathy's talk will describe another approach to Step 4.