GEOMETRY OF 3-SELMER CLASSES
IN THE ALGEBRAIC GEOMETRY LEARNING SEMINAR
AT ESSEN
7 MAY 2015
ISHAI DAN-COHEN

Abstract. We discuss the geometry of 3-Selmer classes of elliptic curves over a number field, following Cassels [Cas], O’Neil [O’N], and Fisher [Fis], apropos the work [BS] of Bhargava-Shankar establishing parts of the Birch and Swinnerton-Dyer conjecture for a positive proportion of elliptic curves over \( \mathbb{Q} \).

1. Statement of theorem

1.1. The Selmer group. Let \( E \) be an elliptic curve over a number field \( k \), and let \( n \) be a natural number. Recall that the \( n \)-Selmer group, denoted \( \text{Sel}_n(E) \) is the kernel of the composite map

\[
H^1((\text{Spec } K)_{\text{ét}}, E[n]) \to H^1((\text{Spec } K)_{\text{ét}}, E) \to \prod_p H^1((\text{Spec } K_p)_{\text{ét}}, E_{\mathbb{Q}_p}),
\]

where \( p \) ranges over all finite places of \( K \). So \( \text{Sel}_n(E) \) fits into a short exact sequence

\[
0 \to E(K)/nE(K) \to \text{Sel}_n(E) \to \text{III}(E)[n] \to 0.
\]

1.2. Ternary cubics. A ternary cubic form is a homogeneous polynomial of degree 3 in 3 variables. The space \( V \) of ternary cubic forms is naturally isomorphic to \( \mathbb{A}^{10} \). We define an action of \( \text{PGL}_3 \) on \( V \) by

\[
(\gamma f)(x, y, z) = \det(\gamma)^{-1} f((x, y, z)\gamma).
\]

A ternary cubic form has a Hessian:

\[
\text{Hess}(f) = \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{vmatrix}.
\]

Hess may be localized on \( \mathbb{P}^3 \) via

\[
\mathcal{O}(3) \to M_{3 \times 3}(\mathcal{O}(1)) \xrightarrow{\text{det}} \mathcal{O}(3).
\]

1.2.1. Examples.

1. \( \text{Hess}(x^3) = 0 \)
2. \( \text{Hess}(x^3 + y^3 + z^3) = 6^3xyz. \)
1.2.2. We define \( I, J \in \mathbb{Q}[a_1, \ldots, a_{10}] \) by the formulas
\[
\text{Hess}^2(f) = 12288 I(f)^2 f + 512 J(f) \text{Hess}(f),
\]
and
\[
\Delta = \frac{4I^3 - J^2}{27}.
\]

The invariants \( I, J \) define a map \( V = \mathbb{A}^3 \rightarrow \mathbb{A}^2 \). One checks that this action is equivariant for the usual action of \( \mathbb{G}_m \) on \( V \) and for the action of weights \((4, 6)\) on \( \mathbb{A}^2 \). Puncturing at the origin and moding out by the \( \mathbb{G}_m \)-actions, we obtain an action of \( \text{PGL}_3 \) on \( \mathbb{P}^3 \) and a map
\[
\bar{V} \rightarrow B
\]
from an open subscheme of \( \mathbb{P}^3 \) to the weighted projective line \( \ell^2 = u^3 \) which is a good quotient for the \( \text{PGL}_3 \) action. Given
\[
(i, j) : \text{Spec} \ R \rightarrow B
\]
we write \( V_{i,j} \) for the fiber of \( \bar{V} \) over \( (i, j) \). If \( (i, j) \) maps into the open subscheme \( \{ \Delta \neq 0 \} \subset B \), then \( V_{i,j}(R) \) consists of all ternary cubics \( f \) with coefficients in \( R \) and invariants \( I(f) = i \) and \( J(f) = j \).

1.3. Theorem. Let \( k \) be a number field and \( E \) the elliptic curve over \( k \) given by
\[
y^2 = x^3 + Ax + B.
\]
Let \( f_0 = x^3 + Ax + B - y^2 \) and let \( i = I(f_0), j = J(f_0) \). If \( f \in V(R) \) is a ternary cubic form, we write \( C_f \) for the associated hypersurface in \( \mathbb{P}^2_R \). Then there’s a bijection
\[
\text{Sel}_3(E) = \{ f \in V_{i,j}(k) \mid C_f(k_p) \neq 0 \text{ for all primes } p \text{ of } k \}/\text{PGL}_3(k).
\]

2. Global version of theorem

2.1. Construction of obstruction map. There’s a map \( E[n] \rightarrow \text{PGL}_n \) defined as follows. Let \( L = \mathcal{O}(ne), e \) being the identity element of \( E \). Then if \( x \) is a point of \( E[n] \), then
\[
\tau_x^* L \cong L.
\]
Here, \( \tau_x \) denotes translation by \( x \). The choice of such an isomorphism \( \phi \) is unique up to \( \mathbb{G}_m(E) = \mathbb{G}_m(S) \) (\( S \) being the base). The induced automorphism of \( \mathbb{P} = \mathbb{P}^H_0(E, L) \) is independent of the choice of \( \phi \). A trivial application of Riemann Roch shows that \( H^0(L) \) has dimension \( n \), completing the construction of the map after a choice of coordinates.\(^1\)

The exact sequence
\[
0 \rightarrow \mathbb{G}_m \rightarrow \text{GL}_n \rightarrow \text{PGL}_n \rightarrow 0
\]
now gives us a map
\[
H^1((\text{Spec} \ k)_{\text{ét}}, \text{PGL}_n) \rightarrow H^2((\text{Spec} \ k)_{\text{ét}}, \mathbb{G}_m).
\]
We define \( \text{Ob} \) to be the composite
\[
H^1((\text{Spec} \ k)_{\text{ét}}, E[n]) \rightarrow H^1((\text{Spec} \ k)_{\text{ét}}, \text{PGL}_n) \rightarrow H^2((\text{Spec} \ k)_{\text{ét}}, \mathbb{G}_m).
\]

2.2. Proposition. Set \( n = 3 \) as in the theorem, let \( k \) be a field of characteristic not 3, and let \( E, A, B, i, j \) be as in the theorem. Then there’s a bijection
\[
\ker \text{Ob} = V_{i,j}(k)/\text{PGL}_3(k).
\]

\(^{1}\text{Maybe we should write PGL}(\mathbb{P}) \text{ instead of PGL}_n \text{ to avoid choosing a basis, but then the two P's are redundant, so maybe just ‘Aut } \mathbb{P} \text{’}.\)
2.3. Stacky generalities. Let $\mathcal{C}$ be a site with terminal object $S$. (Examples: (1) The big \'{e}tale site of a scheme $S$, or (2) more generally, $\mathcal{C}|_S$ for any site $\mathcal{C}$ and any object $S \in \mathcal{C}$, or (3) most generally, a topos with its canonical topology.) Let $\mathcal{G} \to \mathcal{C}$ be a trivial gerbe, and $g \mapsto S$ an object over $S$. Then there’s an equivalence of stacks

$$\xymatrix{ \mathcal{G} \ar[r] \ar[d] & \text{Torsors} (\text{Aut } g) \ar[d] \ar[r] & \text{given by } g' \mapsto \text{Isom} (g', g).}$$

Taking isomorphism classes of objects, we obtain

$$\pi_0 (\mathcal{G} (S)) = H^1 (S, \text{Aut } E).$$

2.4. Twists of $E \to \mathbb{P}$. By a twist of $g : E \to \mathbb{P}$ we mean an $E$-torsor $C$ plus a map $g' : C \to P$ to a scheme $P$ such that after a surjective \'{e}tale base-change, $C$ becomes trivial, and the map to $P$ becomes isomorphic to the pullback of $E \to \mathbb{P}$. A morphism of twists is a commuting square

$$\xymatrix{C' \ar[r] \ar[d]_h & P' \ar[d]^-\Phi \ar[r] & P \ar[d]^\Phi \ar[r] & \mathcal{G} \ar[r] \ar[d] & \text{Torsors} (\text{Aut } g) \ar[d] \ar[r] & \text{given by } g' \mapsto \text{Isom} (g', g).}$$

in which $h$ is an $E$-equivariant isomorphism and $\Phi$ is an isomorphism. Twists of $g$ form a trivial \'{e}tale gerbe.

2.5. Lemma. We have $\text{Aut } (g) = E[n]$.

Proof. An automorphism of $E$ as trivial $E$-torsor is a translation map $\tau_x$ for some $x \in E$. Then, using the bijectivity of the map

$$y \mapsto [y] - [e]$$

to the Jacobain, suitably interpreted over an arbitrary base, we have

$$\tau_x^* n[e] \sim n[e] \text{ iff } \tau_x^* [e] - [e] \text{ is } n\text{-torsion}$$

$$\text{iff } [\tau_x^* e] - [e] = [y] - [e] \text{ for some } y \in E[n]$$

$$\text{iff } x \in E[n].$$

Given an automorphism $(h, \Phi)$ of $g : E \to \mathbb{P}$, we have

$$\phi : h^* L \cong L.$$ 

Indeed

$$L = g^* O_\mathbb{P}$$

$$= g^* \Phi^* O_\mathbb{P}$$

$$= h^* g^* O_\mathbb{P}$$

$$= h^* L.$$ 

Hence $h = \tau_x$ with $x \in E[n]$. Moreover, the isomorphism of line bundles $\phi$ is uniquely determined up to a scalar, so

$$\Phi = \Gamma (E, \phi)$$

is uniquely determined by $h$. □
2.6. Corollary. We have \((S = \text{Spec} \, k)\):
\[
H^1(S_{\text{et}}, E[n]) = \{\text{Twists of } g : E \to \mathbb{P}\}/ \cong .
\]

2.7. Proof of Proposition. We may now complete the proof of the global form of the proposition by constructing a bijection
\[
\{\text{twists } g' : C \to P \text{ over } k \text{ with } P \text{ trivial}\}/ \cong \cong \sim \sim - \to V_{i,j}(k)/\text{PGL}_3(k).
\]
Since \(L = \mathcal{O}(3)\) is very ample, all twists \(g : C \to P\) are closed immersions. Given a twist \(g : C \to P\) of \(g_0 : E \to \mathbb{P}\) with \(P\) trivial, we pick arbitrarily an isomorphism \(P \cong \mathbb{P}\), and then pick an equation \(f \in H^0(\mathbb{P}, \mathcal{O}(3))\) for \(C\), unique up to scalar.

Next, given \(g, g'\) and an isomorphism
\[
\begin{array}{ccc}
C' & \xrightarrow{g'} & \mathbb{P} \\
\downarrow & & \downarrow \\
C & \xrightarrow{g} & \mathbb{P}
\end{array}
\]
one has to check that for some choice of associated equations \(f, f'\), we have \(f' = \gamma f\); explicitly,
\[
f(x\gamma) = (\det \gamma)f'(x)
\]
for all \(x \in k^3\). QED.

3. The Period-Index problem

3.1. Relationship to \(\theta\)-group. It’s helpful to think of the map to \(\text{PGL}_n\) in terms of the \(\theta\)-group of \(L\). Let \(G_n\) be the group of pairs \((x, \phi)\) where \(x \in E[n]\) and \(\phi\) is an isomorphism
\[
\tau_x^* L \cong L.
\]
Then \(G_n\) fits into a short exact sequence which maps to the short exact sequence for \(\text{PGL}_n\) as in the following diagram.
\[
\begin{array}{cccc}
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G_n & \longrightarrow & E[n] & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \text{GL}_n & \longrightarrow & \text{PGL}_n & \longrightarrow & 0
\end{array}
\]

3.2. A period-index solution. If \(C\) is an \(E\)-torsor, its period is its order as an element of \(H^1(\text{Spec} \, k, E)\). Its period is the smallest natural number \(d\) such that there exists a map to projective space of degree \(d\). The phrase period-index problem refers to the problem of determining the relationship between the period and the index.

3.2.1. Proposition. If \(C \in \mathcal{M}(E)\), then its period and index are equal.

Proof. By Hilbert 90 and the Albert-Brauer-Hasse-Noether theorem, we have a commutative square with injections as shown:
\[
\begin{array}{ccc}
H^1(k, \text{PGL}_n) & \longrightarrow & H^2(k, \mathbb{G}_m) \\
\downarrow & & \downarrow \\
\prod_v H^1(k_v, \text{PGL}_n) & \longrightarrow & \prod_v H^2(k_v, \mathbb{G}_m),
\end{array}
\]
from which it follows that a Brauer-Severi variety which possesses a point at every place possesses a \(k\)-point. Note that a Brauer-Severi variety automatically possesses a point at each infinite place.
Using the Kummer exact sequence for $E$ and again Hilbert 90, there’s a map of exact sequences

\[
0 \longrightarrow E(k)/nE(k) \longrightarrow H^1(k, E[n]) \longrightarrow H^1(E)[n] \longrightarrow 0
\]

\[
0 \longrightarrow H^1(k, \text{PGL}_n) \longrightarrow H^2(k, \mathbb{G}_m).
\]

(For the factorization, it would be sufficient to show that $E[n] \to \text{PGL}_n$ has normal image $N$ and that $\text{PGL}_n(k) \to (\text{PGL}_n / N)(k)$. This is not strictly necessary however for the proof.) Suppose $C \in \text{III}(E)$ has period $n$. Then in particular $C$ belongs to $H^1(E)[n]$. By the surjectivity of $\alpha$, $C$ admits a map $g : C \to P$ to a Brauer-Severi variety. Then $\beta(P)$ is trivial at each finite place $v$ of $k$. By Hilbert 90 applied to $k_v$, we then have $P_v$ trivial at each finite place $v$.

Since $P$ is automatically trivial at all infinite places, it follows that $P \cong \mathbb{P}^n$. The resulting map $C \to \mathbb{P}^n$ has degree $n$. It follows that the index is no greater than the period. We omit the proof of the reverse inequality. □

3.3. Proof of Theorem. Under the equality

\[
\ker \text{Ob} = V_{i,j}(k)/\text{PGL}_3(k),
\]

the identity element of the left corresponds to $C \to \mathbb{P}$ with $C$ trivial. This is clear. By the Hasse principle for Brauer-Severi varieties, classes that are unobstructed locally are unobstructed globally. So by functoriality of the above isomorphism, we have a commuting diagram

\[
\begin{array}{cccccc}
\text{Sel}_3(E) & \xrightarrow{\cong} & \text{Ker} & \\
\downarrow & & \downarrow & \\
\ker \text{Ob}(k) & \xrightarrow{\cong} & V_{i,j}(k)/\text{PGL}_3(k) & \\
\downarrow & & \downarrow & \\
\prod_p \ker \text{Ob}(k_p) & \xrightarrow{\cong} & \prod_p V_{i,j}(k_p)/\text{PGL}_3(k_p) & \\
\end{array}
\]

inducing a bijection as in the theorem.

References


