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 $\mathrm{Sel}_n(E)$ is the kernel of the composite map

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

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

$$0 \to E(K)/nE(K) \to \mathrm{Sel}_n(E) \to Ш(E)[n] \to 0.$$

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 PGL_3 on V by

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

A ternary cubic form has a Hessian:

$$\mathrm{Hess}(f) = \det \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{pmatrix}.$$

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

$$\mathcal{O}(3) \to M_{3\times 3}(\mathcal{O}(1)) \xrightarrow{\det} \mathcal{O}(3).$$

1.2.1. **Examples.**

(1) $$\mathrm{Hess}(x^3) = 0$$

(2) $$\mathrm{Hess}(x^3 + y^3 + z^3) = 6^3 xyz.$$

Date: May 12, 2015.

1.2.2. We define $I, J \in \mathbb{Q}[a_1, \dots, a_{10}]$ by the formulas

$$\mathrm{Hess}^2(f) = 12288 I(f)^2 f + 512 J(f)\,\mathrm{Hess}(f),$$

and

$$\Delta = \frac{4I^3 - J^2}{27}.$$

The invariants I, J define a map $V = \mathbb{A}^{10} \to \mathbb{A}^2$. 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 PGL_3 on $\mathbb{P}^\vee V$ and a map

$$\bar{V}^{st} \to B$$

from an open subscheme of $\mathbb{P}^\vee V$ to the weighted projective line $t^2 = u^3$ which is a good quotient for the PGL_3 action. Given

$$(i, j) : \operatorname{Spec} R \to B$$

we write $\bar{V}_{i,j}$ for the fiber of $\bar{V}^{st}$ over (i, j). If (i, j) maps into the open subscheme $\{\Delta \neq 0\} \subset B$, then $\bar{V}_{i,j}(R)$ 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

$$\mathrm{Sel}_3(E) = \big\{ f \in V_{i,j}(k) \;\big|\; C_f(k_p) \neq 0 \text{ for all primes } p \text{ of } k \big\} / PGL_3(k).$$

2. Global version of theorem

2.1. Construction of obstruction map. There's a map $E[n] \to \mathrm{PGL}_n$ 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, τ_x denotes translation by x. The choice of such an isomorphism ϕ 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 ϕ. 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

$$0 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 0$$

now gives us a map

$$H^1\big((\operatorname{Spec} k)_{\text{ét}}, \mathrm{PGL}_n\big) \to H^2\big(\operatorname{Spec} k)_{\text{ét}}, \mathbb{G}_m).$$

We define Ob to be the composite

$$H^1\big((\operatorname{Spec} k)_{\text{ét}}, E[n]\big) \to H^1\big((\operatorname{Spec} k)_{\text{ét}}, \mathrm{PGL}_n\big) \to H^2\big((\operatorname{Spec} k)_{\text{ét}}, \mathbb{G}_m).$$

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

$$\ker Ob = V_{i,j}(k)/PGL_3(k).$$

[1] Maybe we should write $\mathrm{PGL}(\mathbb{P})$ instead of PGL_n to avoid choosing a basis, but then the two P's are redundant, so maybe just '$\mathrm{Aut}\,\mathbb{P}$'.

2.3. Stacky generalities. Let $\mathcal{C}$ be a site with terminal object S. (Examples: (1) The big étale 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

$$\begin{tikzcd} \mathcal{G} \arrow[rr] \arrow[dr] & & \mathrm{Torsors}(\mathrm{Aut}\, g) \arrow[dl] \\ & \mathcal{C} & \end{tikzcd} \qquad \text{given by} \qquad g' \mapsto \mathrm{Isom}(g', g).$$

Taking isomorphism classes of objects, we obtain

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

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 étale 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

$$\begin{tikzcd} C' \arrow[r] \arrow[d, "h"'] & P' \arrow[d, "\Phi"] \\ C \arrow[r] & P \end{tikzcd}$$

in which h is an E-equivariant isomorphism and Φ is an isomorphism. Twists of g form a trivial étale gerbe.

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

Proof. An automorphism of E as trivial E-torsor is a translation map τ_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

$$\begin{aligned} \tau_x^* n[e] \sim n[e] &\text{ iff } \tau_x^*[e] - [e] \text{ is } n\text{-tosion} \\ &\text{ iff } [-x] - [e] = [y] - [e] \text{ for some } y \in E[n] \\ &\text{ iff } x \in E[n]. \end{aligned}$$

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

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

Indeed

$$\begin{aligned} L &= g^* \mathcal{O}_{\mathbb{P}} \\ &= g^* \Phi^* \mathcal{O}_{\mathbb{P}} \\ &= h^* g^* \mathcal{O}_{\mathbb{P}} \\ &= h^* L. \end{aligned}$$

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

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

is uniquely determined by h. $\square$

2.6. Corollary. We have ($S = \operatorname{Spec} k$):

$$H^1\big(S_{\text{ét}}, E[n]\big) = \{\text{Twists of } g : E \to \mathbb{P}\}/\cong .$$

2.7. Proof of Proposition. We may now complete the proof of the global form of the proposition by constructing a bijection

$$\{\text{twists } g' : C \to P \text{ over } k \text{ with } P \text{ trivial}\}/\cong \xrightarrow{\cong} V_{i,j}(k)/\operatorname{PGL}_3(k).$$

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 $f \in H^0\big(\mathbb{P}, \mathcal{O}(3)\big)$ for C, unique up to scalar.

Next, given g, g' and an isomorphism

$$\begin{tikzcd} C' \arrow[r, "g'"] \arrow[d] & \mathbb{P} \arrow[d, "\gamma"] \\ C \arrow[r, "g"'] & \mathbb{P} \end{tikzcd}$$

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 θ-group. It's helpful to think of the map to PGL_n in terms of the θ-group of L. Let $\mathcal{G}_n$ be the group of pairs (x, ϕ) where $x \in E[n]$ and ϕ is an isomorphism

$$\tau_x^* L \xrightarrow{\cong} L.$$

Then $\mathcal{G}_n$ fits into a short exact sequence which maps to the short exact sequence for PGL_n as in the following diagram.

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & \mathcal{G}_n \arrow[r] \arrow[d] & E[n] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathbb{G}_m \arrow[r] & \operatorname{GL}_n \arrow[r] & \operatorname{PGL}_n \arrow[r] & 0 \end{tikzcd}$$

3.2. A period-index solution. If C is an E-torsor, its *period* is its order as an element of $H^1(\operatorname{Spec} k, E)$. 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 $C \in Ш(E)$, 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:

$$\begin{tikzcd} H^1(k, \operatorname{PGL}_n) \arrow[r, hook] \arrow[d] & H^2(k, \mathbb{G}_m) \arrow[d, hook] \\ \prod_v H^1(k_v, \operatorname{PGL}_n) \arrow[r] & \prod_v H^2(k_v, \mathbb{G}_m), \end{tikzcd}$$

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

$$\begin{tikzcd} 0 \arrow[r] & E(k)/nE(k) \arrow[r] \arrow[d] & H^1(k, E[n]) \arrow[r, "\alpha"] \arrow[d] & H^1(E)[n] \arrow[r] \arrow[d, "Ob"] & 0 \\ & 0 \arrow[r] & H^1(k, \mathrm{PGL}_n) \arrow[r, "\beta"'] & H^2(k, \mathbb{G}_m). & \end{tikzcd}$$

(For the factorization, it would be sufficient to show that $E[n] \to \mathrm{PGL}_n$ has normal image N and that $\mathrm{PGL}_n(k) \twoheadrightarrow (\mathrm{PGL}_n/N)(k)$. This is not strictly necessary however for the proof.) Suppose $C \in Ш(E)$ has period n. Then in particular C belongs to $H^1(E)[n]$. By the surjectivity of α, 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

$$\ker Ob = V_{i,j}(k)/PGL_3(k),$$

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

$$\begin{tikzcd} \mathrm{Sel}_3(E) \arrow[r, dotted, "\cong"] \arrow[d] & \mathrm{Ker} \arrow[d] \\ \ker Ob(k) \arrow[r, equal] \arrow[d] & \bar{V}_{i,j}(k)/PGL_3(k) \arrow[d] \\ \prod_p \ker Ob(k_p) \arrow[r, equal] & \prod_p \bar{V}_{i,j}(k_p)/PGL_3(k_p) \end{tikzcd}$$

inducing a bijection as in the theorem.

References

[BS] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[Cas] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[Fis] Tom Fisher. Testing equivalence of ternary cubics. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 333–345. Springer, Berlin, 2006.

[O'N] Catherine O'Neil. The period-index obstruction for elliptic curves. *J. Number Theory*, 95(2):329–339, 2002.

Fakultät für Mathematik, Universität Duisburg-Essen, Thea-Leymann-Strasse 9, 45127 Essen, Germany, E-mail address: `ishaidc@gmail.com`