OBSTRUCTIONS TO RATIONAL POINTS ON CURVES COMING FROM THE NILPOTENT GEOMETRIC FUNDAMENTAL GROUP

JORDAN ELLENBERG

Let X be a hyperbolic curve over a number field K. Hyperbolic means that either $g \geq 2$, or $g = 1$ and ≥ 1 puncture, or $g = 0$ and ≥ 3 punctures. Let S be the set of primes of bad reduction. Assume there is a point $b \in X(K)$.

Recall: There is a map

$$X(K) \to H^1(G_K, \pi_1(X_{\overline{K}}))$$

where $\pi_1(X_{\overline{K}})$ is an abbreviation for $\pi_1^{\text{et}}(X_{\overline{K}})$, which is isomorphic to the profinite completion of $\pi_1^{\text{top}}(X(\mathbb{C}))$. What is this map? Given a finite Galois cover $Y_{\overline{K}} \to X_{\overline{K}}$ with a model $\pi\colon Y \to X$ with $\pi^{-1}(b)(K) \neq \emptyset$, and given $x \in X(K)$, there exists a unique twist $\pi^\xi\colon Y^\xi \to X$ of Y such that $\pi_\xi^{-1}(x)(K) \neq \emptyset$. We get a map $X(K) \to H^1(G_K, G)$ sending each x to the corresponding ξ. The section conjecture says that the induced map

$$X(K) \to H^1(G_K, \pi_1^{\text{et}}(X_{\overline{K}}))$$

is a bijection.

It is much easier to consider groups smaller than $\pi_1^{\text{et}}(X_{\overline{K}})$. For instance, one can write $\pi^{[n]}$ for $\pi_1^{\text{et}}(X_{\overline{K}})^{\text{pro-}p}/L^n\pi_1^{\text{et}}(X_{\overline{K}})^{\text{pro-}p}$. So we get

$$X(K) \to H^1(G_K, \pi_1^{[n]}).$$

and these fit together in a diagram

$$\begin{array}{ccccc}
 & & H^1(G_K, \pi^{[4]}) & & \\
 & \nearrow & \downarrow & & \\
 & & H^1(G_K, \pi^{[3]}) & & \\
 & \nearrow & \downarrow \theta & & \\
X(K) & \xrightarrow{\kappa} & H^1(G_K, \pi^{[2]}) & = & T_pJ,
\end{array}$$

where T_pJ is the Tate module. There is also the diagram

$$\begin{array}{ccccc}
 & & H^1(G_K, U_4) & & \\
 & \nearrow & \downarrow & & \\
 & & H^1(G_K, U_3) & & \\
 & \nearrow & \downarrow & & \\
X(K) & \longrightarrow & H^1(G_K, U_2) & = & T_pJ \otimes \mathbb{Q}_p,
\end{array}$$

Date: February 6, 2007.

When $n = 2$, the map $X(K) \to H^1(G_K, T_pJ)$ factors through the descent map $J(K) \to H^1(G_K, T_pJ)$.

Note: $X(K)$ is contained in the image of θ in $H^1(G_K, \pi_1^{[2]})$.

There is an exact sequence in Galois cohomology

$$H^1(G_K, \pi_1^{[3]}) \to H^1(G_K, \pi_1^{[2]}) \xrightarrow{\delta} H^2(G_K, \ker(\pi_1^{[3]} \to \pi_1^{[2]})).$$

Note that $\pi_1^{[3]}$ sits in a sequence

$$1 \to M \to \pi_1^{[3]} \to \pi_1^{[2]} \to 1.$$

Minhyong, in his talk, had

$$H^1(G_K, U^2) \xrightarrow{\delta} H^1(G_K, U^3 \backslash U^2),$$

which is our δ tensored with $\mathbb{Q}_p$.

In fact, let $T = \{\text{bad primes}\} \cup \{p\}$ and write

$$\begin{array}{ccc} H^1(G_T(K), \pi_1^{[2]}) & \xrightarrow{\delta} & H^2(G_T(K), M) \\ \uparrow & \nearrow_{\delta} & \\ J(K) & & \end{array}$$

Then δ is an obstruction to K-points of the Jacobian arising from K-points of X.

Remark 0.1. In general, given a central extension

$$1 \to A \to B \to C \to 1,$$

the map

$$H^1(G, C) \to H^2(G, A)$$

is a quadratic form; i.e., $\delta(x + y) - \delta(x) - \delta(y)$ is bilinear.

In our situation, the quadratic form turns out to be cup product for

$$\begin{aligned} \bigwedge^2 \pi_1^{[2]} &\to M \\ x, y &\mapsto [x, y]. \end{aligned}$$

We get

$$\operatorname{Sym}^2 H^1(G_T(K), \pi_1^{[2]}) \to H^2(G_T(K), \bigwedge \pi_1^{[2]}) \xrightarrow{m} H^2(G_T(K), M).$$

Suppose $p \neq 2$. Then $\delta(x) = \frac{1}{2} m(x \cup x) + L(x)$ with L linear.

Example 0.2. Suppose $X = \mathbb{P}^1 - \{0, 1, \infty\}$. Let b be a tangential base point at 0. Then $\pi_1^{[2]} = \mathbb{Z}_p(1)^2$ (i.e., $\mathbb{Z}_p \times \mathbb{Z}_p$ as group, with G_K acting via the cyclotomic character), and $J = \mathbb{G}_m^2$. The map $X \to J$ sends t to $(t, 1 - t)$. Now $\pi_1^{[3]}$ is the Heisenberg group, which sits in an exact sequence

$$1 \to M \to \pi_1^{[3]} \to \mathbb{Z}_p(1)^2 \to 1$$

with $M = \bigwedge^2 \pi^{[2]} = \bigwedge^2 \mathbb{Z}_p(1) = \mathbb{Z}_p(2)$. Now

$$\delta \colon H^1(G_K, \mathbb{Z}_p(1)^2) \to H^2(G_K, \mathbb{Z}_p(2))$$

and $J(K) = K^\times \times K^\times$ maps into the group on the left. This sends a, b to the Hilbert symbol $(a, b) \in K_2K$. If $p = 2$ and we work modulo 2, this is just the quadratic Hilbert symbol $(a, b)_2$, which is 0 exactly when $x^2 - ay^2 - bz^2$ has a rational point. And indeed $(a, 1-a) = 0$ in K_2K. In this case δ is torsion. In particular, if we tensor with $\mathbb{Q}_p$ (as in Minhyong's talk), then δ becomes 0. (Maybe this happens in all cases?) Thus $H^1(G_K, U^3) \to H^1(G_K, U^2)$ is surjective. Here δ is torsion, but not usually trivial; e.g., it can tell you something about the image of $X(\mathbb{R})$ in $J(\mathbb{R})$ or about the image of $X(K_v)$ in $J(K_v)/\ell J(K_v)$.