KOLYVAGIN'S CONSTRUCTION OF COHOMOLOGY CLASSES

DAVID JAO

ABSTRACT. These notes present the construction of the cohomology classes $c(n), d(n)$ from the Heegner points y_n, given in Section 4 of [Gr].

Fix as before an $n = \prod l$, squarefree, coprime to NDp, with each conjugacy class $\mathrm{Frob}(l)$ in $\mathrm{Gal}(K(E_p)/\mathbb{Q})$ containing the complex conjugation automorphism τ. Let $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$ denote the Galois group of K_n over K, and recall that G_n is the Galois group of K_n over K_1. Choose a set S of coset representatives for G_n in $\mathcal{G}_n$, and define

$$P_n := \sum_{\sigma \in S} \sigma(D_n y_n), \tag{4.1}$$

where the sum is taken in $E(K_n)$.

Proposition 3.6 says the class $[D_n y_n]$ in $E(K_n)/pE(K_n)$ is fixed by G_n. It follows that the class $[P_n]$ in $E(K_n)/pE(K_n)$ is fixed by all of $\mathcal{G}_n$. The class $[P_n]$ does not depend on the choice of S. However, recall that D_n was defined as $\prod D_l$, where

$$D_l := \sum_{i=1}^{l} i \cdot \sigma_l^i = -\sum_{i=1}^{l+1} \frac{\sigma_l^i - 1}{\sigma_l - 1}.$$

Here σ_l is a chosen generator of G_l, a cyclic group of order $l+1$. Since p divides $l+1$ (by (3.3)), we see that $[D_n y_n]$ depends on the choice of generator σ_l of G_l up to scaling by $(\mathbb{Z}/p)^\times$. Thus the class $[P_n]$ also depends on the choice of generator up to scaling by $(\mathbb{Z}/p)^\times$.

Also observe that

$$P_1 = \sum_{\sigma \in \mathrm{Gal}(K_1/K)} \sigma y_1 = \mathrm{Tr}_K^{K_1}(y_1) = y_{1,K}.$$

The exact sequence $0 \longrightarrow E_p \longrightarrow E \xrightarrow{p} E \longrightarrow 0$ gives a long exact sequence in Galois cohomology, a portion of which is

$$E(K) \xrightarrow{p} E(K) \xrightarrow{\delta} H^1(K, E_p) \longrightarrow H^1(K, E) \xrightarrow{p} H^1(K, E)$$

Taking cokernel on the left and kernel on the right yields the short exact sequence

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} H^1(K, E_p) \longrightarrow H^1(K, E)_p \longrightarrow 0.$$

We can play the same game with $H^q(K_n, \cdot)$ to get the short exact sequence

$$0 \longrightarrow E(K_n)/pE(K_n) \xrightarrow{\delta_n} H^1(K_n, E_p) \longrightarrow H^1(K_n, E)_p \longrightarrow 0.$$

Date: March 7, 2000.

Putting it all together, we get the commutative diagram

(4.2)

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(K_n/K, E(K_n))_p & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & \frac{E(K)}{pE(K)} & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \approx \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & \left(\frac{E(K_n)}{pE(K_n)}\right)^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & H^1(K_n, E)_p^{\mathcal{G}_n} & &
\end{array}$$

where all the horizontal and vertical sequences are exact.

We show that Res : $H^1(K, E_p) \longrightarrow H^1(K_n, E_p)^{\mathcal{G}_n}$ is an isomorphism in the diagram above by showing that $E_p(K_n)$ is trivial in the Inf–Res exact sequence

$$0 \longrightarrow H^1(K_n/K, E_p(K_n)) \xrightarrow{\mathrm{Inf}} H^1(K, E_p) \xrightarrow{\mathrm{Res}} H^1(K_n, E_p)^{\mathcal{G}_n} \longrightarrow H^2(K_n/K, E_p(K_n))$$

Lemma 4.3. *The curve E has no p–torsion rational over K_n.*

Proof. We know that $E_p(\bar{K})$ is $(\mathbb{Z}/p)^2$, so if $E_p(K_n)$ is not zero then the only possibilities are $\mathbb{Z}/p$ and $(\mathbb{Z}/p)^2$. Suppose first that $E_p(K_n) = \mathbb{Z}/p$. Let $\sigma \in G_{\mathbb{Q}}$. For $P \in E_p(K_n)$, the point $\sigma(P)$ is still in $E(K_n)$ and is still annihilated by p, so $\sigma(P) \in E_p(K_n)$. Thus $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ fixes the one dimensional subspace $E_p(K_n) = \mathbb{Z}/p$ of $(\mathbb{Z}/p)^2$, so it is a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p)$. This contradicts the assumption, made in the beginning of Section 2, that $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p)$.

Now suppose $E_p(K_n) = E_p = (\mathbb{Z}/p)^2$. Then $\mathbb{Q}(E_p) \subset K_n$, so we have a surjection $\mathrm{Gal}(K_n/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) = GL_2(\mathbb{Z}/p)$. But $\mathrm{Gal}(K_n/\mathbb{Q})$ is a group of dihedral type (has an abelian normal subgroup of index 2), and we know from group theory that $GL_2(\mathbb{Z}/p)$ is not a quotient of any group of dihedral type, for $p > 2$. □

Kolyvagin's cohomology classes are defined as follows. The class $c(n) \in H^1(K, E_p)$ is defined by

$$\mathrm{Res}\ c(n) = \delta_n[P_n]. \tag{4.4}$$

Since Res is an isomorphism, this equation uniquely specifies $c(n)$. The class $d(n)$ is the image of $c(n)$ in $H^1(K, E)_p$. Now Res $d(n) \in H^1(K_n, E)_p^{\mathcal{G}_n}$ comes from $[P_n]$ which is two terms back in the exact sequence, so it is 0. Thus $d(n)$ lifts via Inf, yielding a unique class $\tilde{d}(n) \in H^1(K_n/K, E(K_n))_p$ such that

$$\mathrm{Inf}\ \tilde{d}(n) = d(n). \tag{4.5}$$

Explicitly, $c(n)$ is represented by the cocycle f where

$$f(\sigma) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma - 1)P_n}{p}, \tag{4.6}$$

for $\sigma \in G_K$. Here $\frac{1}{p}P_n$ is any p–th root of P_n in $E(\bar{K})$, and $\frac{(\sigma-1)P_n}{p}$ is the unique p–th root of $(\sigma-1)P_n$ in $E(K_n)$ (existence follows from Proposition 3.6; uniqueness is by Lemma 4.3). To see that this cocycle works, we need only compute $\delta_n[P_n]$ and see that it is equal to Res f. Recall that $\delta_n[P_n]$ is defined by lifting the point P_n via the "multiplication by p" map, taking the coboundary in E coefficients, and then treating the result as a cocycle over E_p coefficients. Thus $\delta_n[P_n]$ is the coboundary sending

$$\sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n.$$

On the other hand, Res f is the cocycle f with application restricted to $\sigma \in G_{K_n}$. For these σ, the term $(\sigma-1)P_n$ is trivial, so

$$(\text{Res } f)(\sigma) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n.$$

Thus f does indeed represent the class $c(n)$.

When we push our representative of $c(n)$ over to $H^1(K,E)_p$, we obtain the following cocycle representative for $d(n)$:

$$\sigma \mapsto -\frac{(\sigma-1)P_n}{p}, \quad \text{for } \sigma \in G_K.$$

The term $\sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n$ has dropped out, since in $H^1(K,E)_p$ this term is a coboundary. Lifting via Inf, we obtain the cocycle

$$\tilde{f}(\sigma) = -\frac{(\sigma-1)P_n}{p}, \quad \text{for } \sigma \in \mathcal{G}_n$$

representing $\tilde{d}(n)$.

Proposition 4.7.

1. *The class $c(n)$ is trivial in $H^1(K,E_p)$ if and only if $P_n \in pE(K_n)$.*
2. *The classes $d(n)$ and $\tilde{d}(n)$ are trivial in their respective cohomology groups if and only if $P_n \in pE(K_n) + E(K)$.*

Proof. Apply the isomorphism Res to $c(n)$. The first statement then follows immediately from injectivity of δ_n in the diagram (4.2).

For the second statement, injectivity of Inf in (4.2) implies that $d(n)$ and $\tilde{d}(n)$ are either both trivial or both nontrivial. But $d(n)$ comes from $c(n)$, so $d(n)$ is trivial if and only if $c(n) \in \operatorname{Im}\delta$. Write $c(n) = \delta(P)$; then upon pushing P down to $E(K_n)$ we see from injectivity of δ_n that $P \equiv P_n \pmod{pE(K_n)}$. Therefore, $d(n)$ is trivial if and only if there exists $P \in E(K)$ such that $P \equiv P_n \pmod{pE(K_n)}$, which is what we wanted to prove. □

By Proposition 4.7, the class $c(1)$ is trivial if and only if $P_1 = y_{1,K}$ is divisible by p in $E(K)$. The classes $d(1)$ and $\tilde{d}(1)$ are always trivial since $P_1 = y_{1,K}$ is in $E(K)$.

References

[Gr] B. Gross, Kolyvagin's Work on Modular Elliptic Curves, in *L-Functions and Arithmetic*, LMS Lecture Notes 153, London Mathematical Society, Cambridge, 1991, pp. 235–256.