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 $\text{Frob}(l)$ in $\text{Gal}(K(E_p)/\mathbb{Q})$ containing the complex conjugation automorphism $\tau$. Let $G_n := \text{Gal}(K_n/K)$ 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 $G_n$, and define

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

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 $G_n$. The class $[P_n]$ does not depend on the choice of $S$. However, recall that $D_n$ was defined as $\prod D_l$, where

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

Here $\sigma_l$ 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 $\sigma_l$ of $G_l$ up to scaling by $(\mathbb{Z}/p)^{l}$. Thus the class $[P_n]$ also depends on the choice of generator up to scaling by $(\mathbb{Z}/p)^{l}$.

Also observe that

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

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

$$E(K) \xrightarrow{p} E(K) \xrightarrow{\delta} H^1(K, E_p) \xrightarrow{p} H^1(K, E) \to 0.$$ 

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

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

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

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

Date: March 7, 2000.
Putting it all together, we get the commutative diagram (4.2)

\[
\begin{array}{cccc}
0 & \rightarrow & H^1(K_n, E(K_n))_p & \rightarrow \\
\downarrow & & \downarrow & \\
0 & \rightarrow & E(K_n)_{\mathfrak{p}} & \rightarrow \\
& & \delta & \\
& & H^1(K, E_p) & \rightarrow \\
& & \cong & \\
& & H^1(K, E_p)^{\mathfrak{g}_n} & \rightarrow \\
& & \delta & \\
& & H^1(K_n, E_p)^{\mathfrak{g}_n} & \rightarrow \\
& & & 0 \\
\end{array}
\]

where all the horizontal and vertical sequences are exact.

We show that Res : \(H^1(K, E_p) \rightarrow H^1(K_n, E_p)^{\mathfrak{g}_n}\) is an isomorphism in the diagram above by showing that \(E_p(K_n)\) is trivial in the Inf-Res exact sequence

\[
0 \rightarrow H^1(K_n, E_p(K_n)) \xrightarrow{\text{Inf}} H^1(K, E_p) \xrightarrow{\text{Res}} H^1(K_n, E_p)^{\mathfrak{g}_n} \rightarrow H^2(K_n, E_p(K_n))
\]

**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 \(\mathfrak{p} \in E_p(K_n)\), the point \(\sigma(\mathfrak{p})\) is still in \(E(K_n)\) and is still annihilated by \(p\), so \(\sigma(\mathfrak{p}) \in E_p(K_n)\). Thus \(\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})\) fixes the one dimensional subspace \(E_p(K_n) = \mathbb{Z}/p\) of \((\mathbb{Z}/p)^2\), so it is a Borel subgroup of \(GL_2(\mathbb{Z}/p)\). This contradicts the assumption, made in the beginning of Section 2, that \(\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p)\).

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 \(\text{Gal}(K_n/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) = GL_2(\mathbb{Z}/p)\). But \(\text{Gal}(K_n/\mathbb{Q})\) 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 \(p > 2\). \(\Box\)

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

\[
\text{Res } c(n) = \delta_n [P_n].
\]

Since \(\text{Res}\) 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 \(\text{Res } d(n) \in H^1(K_n, E)^{\mathfrak{g}_n}\) comes from \([P_n]\) which is two terms back in the exact sequence, so it is 0. Thus \(d(n)\) lifts via \(\text{Inf}\), yielding a unique class \(d(n) \in H^1(K_n, E(K_n))_p\) such that

\[
\text{Inf } d(n) = d(n).
\]

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

\[
f(\sigma) = \sigma \left( \frac{1}{p} P_n \right) - \frac{1}{p} P_n - \frac{(\sigma - 1) P_n}{p},
\]
for \( \sigma \in G_K \). Here \( \frac{1}{p}P_n \) is any \( p \)-th root of \( P_n \) in \( E(\bar{K}) \), and \( \frac{\sigma - 1}{p}P_n \) 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 \( \text{Res} \ f \). 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, \( \text{Res} \ f \) is the cocycle \( f \) with application restricted to \( \sigma \in G_{K_\infty} \). For these \( \sigma \), 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 \( \text{Inf} \), we obtain the cocycle

\[
\tilde{f}(\sigma) = -\frac{(\sigma - 1)P_n}{p}, \quad \text{for } \sigma \in G_n
\]

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 \( \text{Res} \) to \( c(n) \). The first statement then follows immediately from injectivity of \( \delta_n \) in the diagram (4.2).

For the second statement, injectivity of \( \text{Inf} \) 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 \( c(n) \in \text{Im} \delta \). Write \( c(n) = \delta(P) \); then upon pushing \( P \) down to \( E(K_n) \) we see from injectivity of \( \delta_n \) 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**