Kolyvagin systems

Alex Sheng

October 22, 2025

This set of notes was used for a talk I gave for the RTG seminar on Euler systems at the University of Michigan, Fall 2024. The reference I used were Washington's *Introduction to Cyclotomic Fields* (Chapter 15) and Rubin's *Euler Systems* (Chapter 4).

Notations.

Fix a rational prime p and a finite extension $\Phi/\mathbf{Q}_p$ with ring of integers $\mathcal{O}$. This Φ and $\mathcal{O}$ will be our "coefficient field/ring". For simplicity, just think of $\Phi = \mathbf{Q}_p$ and $\mathcal{O} = \mathbf{Z}_p$.

Let K be a field of characteristic 0. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. Let T be a free $\mathcal{O}$-module that is a p-adic representation of G_K. Fix M to be a large power of p and let $W_M = T/MT$. In practice, if $T = \mathbf{Z}_p(1)$, then $W_{p^m} \simeq \mu_{p^m}$ the p^m-th roots of unity; if $T = T_p(E)$ the p-adic Tate of module of an elliptic curve E, then $W_{p^m} \simeq E[p^m]$ are the p^m-torsion points.

Basic definitions.

Let K_∞/K be a fixed $\mathbf{Z}_p^d$-extension. This will serve as our ambient field. For each finite extension $K \subset_f F \subset K_\infty$, let $\mathcal{R}_F$ be the set of squarefree products of so-called *Kolyvagin primes* (rational primes satisfying certain properties). A *Kolyvagin system* for T is a family of classes

$$\left\{\kappa_{F,r} \in H^1(F, W_M) \mid K \subset_f F \subset K_\infty,\, r \in \mathcal{R}_F\right\}$$

satisfying two axioms:

(i) (unramified away from pr) for every place $w \nmid pr$ of F where T is unramified, the localization lies in the the finite part of H^1, i.e.

$$\mathrm{loc}_w(\kappa_{F,r}) \in H^1_f(F_w, W_M);$$

equivalently, $\kappa_{F,r} \in \mathcal{S}^\Sigma(F, W_M)$, where $\Sigma \supset \{p, r\}$;

(ii) (finite-to-singular transition at a new prime ℓ) for every Kolyvagin prime $\ell \nmid pr$, the so-called *finite-to-singular comparison map*

$$\phi_\ell^{fs} : H^1_f(F_\ell, W_M) \xrightarrow{\simeq} H^1_s(F_\ell, W_M)$$

sends $\mathrm{loc}_\ell(\kappa_{F,r})$ to $\mathrm{loc}_\ell(\kappa_{F,\ell r})$ in $H^1_s(F_\ell, W_M)$.

That is, a Kolyvagin system is just a compatible family of global classes that are unramified at all places away from p and level r, and whose behavior at a newly added prime ℓ is controlled by the the finite-to-singular comparison map. (In Rubin's book, he showed that the derivative classes attached to an Euler system satisfy precisely these conditions.) We will see how, by carefully choosing these primes ℓ, Kolyvagin system can be used to bound the size of class groups. The comparison map should be thought of as a systematic way of achieving this goal.

Kolyvagin primes $\mathcal{R}_F$.

Let ℓ be a rational prime and assume that T is unramified at ℓ. Consider the Cartier dual $T^* = \mathrm{Hom}(T, \mathbf{Z}_p(1))$ of T, which is a G_k-module via

$$g \cdot \varphi(t) = \chi(g)\varphi(g^{-1}t)$$

In particular, the action of the arithmetic Frobenius Fr_ℓ^{-1} on T^* has characteristic polynomial

$$P_\ell(x) = \det\big(1 - \mathrm{Fr}_\ell^{-1} x \mid T^*\big).$$

(Note: Rubin uses $p_A(x) = \det(I - Ax)$ instead of $p_A^\#(x) = \det(xI - A)$ for the characteristic polynomial. The two conventions are related by $p_A(x) = (-x)^n p_A^\#(1/x)$ in dimension n.)

A rational prime ℓ is a *Kolyvagin prime* if the following conditions are met:

(i) T is unramified at ℓ and $\ell \equiv 1 \mod M$

(ii) ℓ splits completely in $F(\mu_{p^\infty})/K$, i.e., Fr_ℓ acts trivially on μ_{p^∞};

(iii) $P_\ell(1) \equiv 0 \mod M$.

Why these conditions? Recall that we have identifications (using inflation-deflation)

$$H^1_f(F_\lambda, W_M) \simeq W_M/(\mathrm{Fr}_\ell - 1)W_M \quad \text{and} \quad H^1_s(F_\lambda, W_M) \simeq W_M^{\mathrm{Fr}_\ell = 1}.$$

Conditions (ii) and (iii) guarantees that both the Frobenius coinvariant $(W_M)_{\mathrm{Fr}_\ell}$ and the invariant $W_M^{\mathrm{Fr}_\ell}$ are in fact canonically isomorphic to W_M itself. One can think of (ii) and (iii) as technical conditions that make the comparison map work. In the example we turn to shortly, they are automatically satisfied, and only (i) needs to be imposed.

The comparison map

Once we've identified the finite part and the singular part of H^1 with the Frobenius coinvariant and invariant respectively, we just need a map that goes from the coinvariant to the invariant. There is a general method to do that.

Let R be a ring, $W \subset R$ an ideal, and W an R/M-module with endomorphism F. Assume that there is a polynomial $P(x) \in R[x]$ such that

(i) $P(F) = 0$ on a lift of W (so also on W by reduction), and

(ii) $P(1) \equiv 0 \mod M$, so that $P(1)$ kills W.

Define

$$Q(x) = \frac{P(x) - P(1)}{x - 1} \in (R/M)[x].$$

Then one can check that evaluating at F gives a well-defined map

$$Q(F) : W/(F-1)W \to W^{F=1}$$

of (R/M)-modules from F-coinvariants to F-invariants.

Specializing to our case, we see that the characteristic polynomial $P_\ell(x)$ of Fr_ℓ^{-1} satisfies (i) by Cayley-Hamilton and (ii) by condition (iii) of Kolyvagin prime. We define $Q_\ell(x) \in (\mathcal{O}/M\mathcal{O})[x]$ by

$$P_\ell(x) \equiv (x-1)Q_\ell(x) \mod M.$$

Evaluating Q_ℓ at Fr_ℓ^{-1} thus gives a map

$$H^1_f(F_\lambda, W_M) \xrightarrow{\simeq} W_M/(\mathrm{Fr}_\ell - 1)W_M \xrightarrow{\phi_\ell^{fs}} W_M^{\mathrm{Fr}_\ell=1} \xrightarrow{\simeq} H^1_s(F_\lambda, W_M).$$

Sanity check: say $W_m \simeq \mathcal{O}/M$ is one-dimensional and F acts by $a \equiv 1 \bmod M$. Then $P(x) = 1-ax$, and $Q(x) = -a$. So ϕ^{fs} is just nothing but multiplication by $-a$.

Example (mention the goal)

We will discuss an example of deriving a Kolyvagin system using a Euler system, and using the Kolyvagin system to bound ideal class group. The reference for this part is Washington §15.3.

We still fix a rational odd prime p and a large power M of p. Let $T = \mathbf{Z}_p(1)$, so $W_M \simeq \mu_M$. We study the finite extension $F = \mathbf{Q}(\zeta_f)^+/\mathbf{Q}$ with $(f,p) = 1$. In this setup, conditions (ii) and (iii) in the definition of a Kolyvagin prime is automatically satisfied, and we only need to stipulate (i). Thus, $L \in \mathcal{R}_F$ is a squarefree product of primes, each congruent to 1 mod fM. We denote by $F(L)$ the extension $F(\prod_{\ell|L} \zeta_\ell)$.

For each L, pick a cyclotomic unit $\alpha(L) \in F(L)^\times$ satisfying two axioms:

(i) for any Kolyvagin prime $\ell \nmid L$,

$$\mathrm{Nm}_{F(\ell L)/F(L)}(\alpha(\ell L)) = \alpha(L)^{\mathrm{Fr}_\ell - 1},$$

where Frob_ℓ is the Frobenius in $F(L)/\mathbf{Q}$;

(ii) $\alpha(\ell L) \equiv \alpha(L)$ modulo all primes of $F(\ell L)$ above ℓ.

This is the input of a Euler system data. As can be checked, a good such choice of $\alpha(L)$ is

$$\alpha(L) = \prod_j ((1-\zeta_f^j\zeta_L)(1-\zeta_f^{-j}\zeta_L))^{a_j}.$$

For each $\ell \mid L$, fix a generator σ_ℓ of $\mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ (and extend it to $\mathrm{Gal}(F(\ell L)/F(L))$ so that σ_ℓ is the identity on roots of unity prime to ℓ), and define operators

$$D_\ell = \sum_{j=0}^{\ell-2} j\sigma_\ell^j \quad \text{and} \quad N_\ell = \sum_{j=0}^{\ell-2} \sigma_\ell^j.$$

Then one can check that $(\sigma_\ell - 1)D_\ell = (\ell-1) - N_\ell$ in the group ring $\mathbf{Z}[\mathrm{Gal}(F(\ell L)/F(L))]$. We also define $D_L = \prod_{\ell|L} D_\ell$. These are concrete manifestations of Kolyvagin's derivative constructions, which are used to get a Kolyvagin system from an Euler system.

Proposition (15.10)**.** *There exists elements $\kappa(L) \in F^\times$ and $\beta_L \in F(L)^\times$ such that*

$$D_L\alpha(L) = \kappa(L) \cdot \beta_L^M.$$

The Kummer map $F^\times \twoheadrightarrow F^\times/(F^\times)^M \cong H^1(F, \mu_M)$ give a class $\kappa_L = [\kappa(L)] \in H^1(F, \mu_M)$.

Claim. *The class $\kappa_L \in H^1(F, \mu_M)$ obtained belongs to a Kolyvagin system.*

Pick a prime $w \nmid pL$, so that $H^1_f(F_w, \mu_M)$ is characterized by those elements of

$$H^1(F_w, \mu_M) \simeq F_w^\times / (F_w^\times)^M$$

whose w-adic valuation is 0 mod M. Now, since $D_L\alpha(L)$ is a unit in $F(L)$, we have $(\kappa(L)) = (\beta_L^{-1})^M$ as ideals of $F(L)$, so $v_w(\kappa(L)) = 0$, so the first axiom of Kolyvagin system is satisfied.

To verify the second axiom, choose $s \in \mathbf{F}_\ell^\times$. Since $\ell \equiv 1 \bmod fM$, the residue field of F at λ (a prime over ℓ in F) is $\mathbf{F}_\ell$, so to record the "position" of κ_L in $H^1_f(F_\lambda, \mu_M)$, it suffices to say $\kappa(L) \equiv s^a \bmod \lambda$. The following proposition tells us the image of κ_L under the comparison map.

Proposition (15.12)**.** *Suppose $\kappa_L \equiv s^a \mod \lambda$. Then the λ-adic valuation of $\kappa_{\ell L}$ satisfies*

$$v_\lambda(\kappa_{\ell L}) \equiv -a \mod M.$$

In other words, at a new prime, the comparison map sends κ_L to an element $\kappa_{\ell L}$ which lies in $H^1_s(F_\lambda, \mu_M)$, and whose "position" inside is expressed by a. The data of the exponent in the residue field encodes the valuation data at a new prime. This is the manifestation of the comparison map in a concrete setting.

Application: bounding class groups

To simplify further, we restrict our attention to $F = \mathbf{Q}(\zeta_p)^+$. Let A be the p-part of the class group of F. Let $M = p \cdot |A^+| \cdot |(E/C)_p|$. Let χ be a nontrivial even character, and for simplicity let us also assume $\varepsilon_\chi A \simeq \mathbf{Z}/p^t\mathbf{Z}$ is cyclic, generated by an ideal class $[\lambda]$.

We shall also make our life easier by assuming $L = 1$. Chebotarev guarantees the existence of a rational prime ℓ satisfying $\ell \equiv 1 \bmod M$ (i.e., a Kolyvagin prime) one of whose prime divisors is λ. The following proposition tells us how a Kolyvagin system can be used to bound the order $[\lambda]$ in $\varepsilon_\chi A$, and thence the order of $\varepsilon_\chi A$ itself.

Proposition (15.13)**.** *Suppose $[\lambda]$ has order e in $\varepsilon_\chi A$. Suppose*

(i) $\varepsilon_\chi \kappa(\ell) \in (F^\times)^{p^r}$ (with $p^r \le M$ and $Mp^{-r} \cdot |A^+| = 0$), and

(ii) $\varepsilon_\chi \kappa(1) \equiv s^a \mod \lambda$, where $p^{r'} || a$ (and $p^{r'} < M$).

Then $r' \ge r$ and $e \mid p^{r'-r}$.

Sketch of proof. Using the comparison map, (ii) translates to $v_\lambda(\kappa(\ell)) \equiv -a \bmod M$. Now, since $\kappa(\ell)$ is a global p^r-th power by (i), after taking the p^r-th root, we see that $[\lambda]$ is killed by raising to the $-a/p^r$-th power in $\varepsilon_\chi A$. □

Corollary. *The order of the class group $|\varepsilon_\chi A|$ is bounded by the order $|(E/C)_p|$.*

Proof. Simply pick $\kappa(1) \in F^\times$ so that $r' = v_p(|(E/C)_p|)$. □

Remark (On the Chebotarev argument)**.** Three conditions are prescribed for such ℓ: $\lambda \mid \ell$, $\ell \equiv 1 \bmod M$, and arranging the Frobenius of ℓ acts on $\kappa(1)$ in such a way that its image modulo λ has exactly order a with $p^{r'} || a$. The first condition translates to that the Frobenius of ℓ is in a specific conjugacy class in $\mathrm{Gal}(H/F)$ where H is the Hilbert class field of F; the second condition translates to the Frobenius of ℓ being trivial in $\mathrm{Gal}(\mathbf{Q}(\zeta_M)/\mathbf{Q})$ (since ℓ splits completely in $\mathbf{Q}(\zeta_M)$). So the Frobenius of ℓ should land in a certain conjugacy class inside $\mathrm{Gal}(L/\mathbf{Q})$, where

$$L = H \cdot \mathbf{Q}(\zeta_M) \cdot F(\kappa(1)^{1/p^{r'}}).$$

Chebotarev applies since $L/\mathbf{Q}$ is finite.