What can be found in Introduction to Kolyvagin systems by B.Mazur and K.Rubin?

Aleksei Samoilenko

14 January 2026

Overview

1. Cyclotomic unit Euler systems
2. Cyclotomic unit Kolyvagin systems
3. Selmer sheaf
4. Stub subsheaf
5. Kolyvagin systems for general Galois representations

Cyclotomic units

- Let $F = \mathbb{Q}(\mu_p)$ and $\mathcal{O} = \mathbb{Z}[\mu_p]$
- Define

$$\mathcal{P} = \{\text{rational primes } \ell \equiv 1 \mod p^k\}$$

$$\mathcal{N} = \{\text{square free products of primes from } \mathcal{P}\}$$

- Defining property of Euler system:
    - $1 - \zeta_{np}$ is a unit if $n \neq 1$
    - $\mathrm{N}_{F(\mu_{npl})/F(\mu_{np})}(1 - \zeta_{npl}) = (1 - \zeta_{np})^{Frob_\ell - 1}$

Cyclotomic unit Kolyvagin system for $\mu_{p^k} \otimes \chi^{-1}$

- Next step is to construct Kolyvagin system from cyclotomic Euler system above
- Kolyvagin's machine produces a collection of "derivative classes"

$$\{\kappa_n^{cycl} \in (F^\times/p^k)^\chi | n \in \mathcal{N}\}$$

Theorem

1. $\kappa_1^{cycl} = (1-\zeta_p)^\chi$
2. $\mathrm{ord}_\lambda(\kappa_n^{cycl}) \equiv 0 \mod p^k$ *if* $\lambda \nmid n$
3. $\mathrm{ord}_\lambda(\kappa_n^{cycl}) \equiv \log_\lambda(\kappa_{n/\ell}^{cycl}) \mod p^k$ *if* $\lambda \mid \ell \mid n$

Idea behind κ_n

- Each κ_n gives principal ideal
- Principal ideals $=$ relations in class group
- Cleverly choosing a good sequence of integers n, one can produce enough relations on class group to bound

- It would be nice if we can recover all elements in $\{\kappa_n\}$ using theorem above
- In general it can be done only modulo some subgroup

$$H(1) = \{\alpha \in F^\times/p^k \mid \mathrm{ord}_\lambda(\alpha) \equiv 0 \mod p^k\}$$

- It's called Selmer group because

$$H(1) = \mathrm{Ker}(H^1(\mathbb{Q}, \mathbb{G}_m[p^k])^\chi \to \prod_\ell H^1(\mathbb{Q}_\ell, \mathbb{G}_m[p^k])^\chi)$$

- $H(1)$ is an extension of $A_F^\chi[p^k]$ by $(\mathcal{O}^\times/p^k)^\chi$

$$0 \to (\mathcal{O}^\times/p^k)^\chi \to H(1) \to A_F^\chi[p^k] \to 0$$

$$\alpha \mapsto \alpha \mapsto \mathfrak{a}$$

where $\mathfrak{a}^{p^k} = (a)$, it's defined exactly modulo units

Transverse subgroup

- Image of $\mathbb{Z}/p^k$ in $\mathbb{Q}_\ell^\times/p^k$ under $1 \mapsto \ell$ called transverse subgroup and denoted by $(\mathbb{Q}_\ell^\times/p^k)_{tr}$
$$\mathbb{Q}_\ell^\times/p^k = \mathbb{Z}_\ell^\times/p^k \oplus (\mathbb{Q}_\ell^\times/p^k)_{tr}$$
- And for every $\ell \in \mathcal{P}$
$$(F_\lambda^\times/p^k)^\chi = (\mathcal{O}_\lambda^\times/p^k)^\chi \oplus (F_\lambda^\times/p^k)_{tr}^\chi$$
is a splitting into a product of two cyclic groups of order p^k

Modified Selmer groups

- For $n \in \mathcal{N}$ define

$$H(n) = \{\alpha \in (F^\times/p^k)^\chi \mid \text{ if } \ell \mid n \text{ then } \alpha_\ell \in (F_\ell^\times/p^k)^\chi_{tr}, \text{ else } \alpha_\ell \in (\mathcal{O}_\ell^\times/p^k)^\chi\}$$

- $H(1)$ related to class group
- Modified means that we have changed the defining local condition at primes dividing n allowing them to ramify in controlled way

Finite to singular map

- If $\ell \in \mathcal{P}$ define finite to singular isomorphism as

$$\phi_\ell^{fs} : (\mathcal{O}_\ell^\times / p^k)^\chi \to (F_\ell^\times / p^k)_{tr}^\chi$$

- This is the unique map which makes the diagram of isomorphisms commute

Theorem

1. $\kappa_n^{cycl} \in H(n)$
2. *If* $\ell \mid n$ *then* $(\kappa_n^{cycl})_\ell = \phi_\ell^{fs}((\kappa_{n/\ell}^{cycl})_\ell)$

Corollary

If κ_d^{cycl} is known for every d properly dividing n, then theorem determines κ_n^{cycl} modulo

$$\{\alpha \in (F^\times/p^k)^\chi \mid \alpha_\ell \in (\mathcal{O}_\ell^\times/p^k)^\chi \text{ for every prime } \ell \text{, and } \alpha_\ell \equiv 1 \mod \ell\}$$

for sufficiently large n this group is trivial

Selmer sheaf and Kolyvagin system attached to $\mu_p \otimes \chi^{-1}$

- Let $\mathcal{X}$ be a graph on $\mathcal{N}$
- Sheaf on $\mathcal{X}$ consist of
  - a stalk over every vertex
  - a stalk over every edge
  - if e is an edge and v is one of its vertices, a homomorphism from the stalk over v to the stalk over e
- Selmer sheaf $\mathcal{H}$ on $\mathcal{X}$ defined as follows
  - a stalk over n is a $H(n)$
  - a stalk over edge ℓ is a $(F_\ell^\times/p^k)^\chi_{tr}$ (denote it by $H(e)$)
  - maps: ϕ_ℓ^{fs} from n and just localization from $n\ell$
- Global section is a consistent collection $\{\kappa_n \in H(n) | n \in \mathcal{N}\}$
- Kolyvagin system is a global section of Selmer sheaf
- Previously mentioned theorem is equal to say that $\{\kappa_n^{cycl}\}$ is a Kolyvagin system

Modified Selmer groups attached to $\mu_p \otimes \chi^{-1}$

- For character $\chi \neq 1, \omega$ let $r = r(\chi)$ denote its parity
- Get back to

$$0 \to (\mathcal{O}^\times/p^k)^\chi \to H(1) \to A_F^\chi[p^k] \to 0$$

- $(\mathcal{O}^\times/p^k)^\chi$ is free $\mathbb{Z}/p^k\mathbb{Z}$-module of rank r. Hence $H(1)$ contains free $\mathbb{Z}/p^k\mathbb{Z}$-module of rank r

Proposition

For every $n \in \mathcal{N}$, $H(n)$ contains a free $\mathbb{Z}/p^k\mathbb{Z}$-module of rank r

Core vertexes

- Define $\lambda^*(n) = \dim_{\mathbb{F}_p} H(n)[p] - r$
- Vertex n is called core if $\lambda^*(n) = 0$
- n is core iff $H(n) = (\mathbb{Z}/p^k\mathbb{Z})^r$

Proposition

1. $\mid \lambda^*(n) - \lambda^*(n\ell) \mid \leq 1$
2. If $\lambda^*(n) \geq 1$ then there exist infinitely many primes in $\mathcal{P}$ s.t. $\lambda^*(n\ell) = \lambda^*(n) - 1$
3. If $\lambda^*(n) = t$ there is a path of length t from n to a core vertex

Stub subgroup

- Let A is a finite abelian group $d \geq 0$
- Define d-stub of A as maximal subgroup $A' \subseteq A$ of the form $[A : C]A$ where C is subgroup generated by d elements
- A' can be generated by d elements
- If A generated by d elements then $A' = A$
- If $d = 0$ then $A' = 0$
- If $d = 1$ then A' is a canonical cyclic subgroup

- Define $H'(n)$ as r-stub of $H(n)$
- From proposition above $H'(n) = \frac{|H(n)|}{p^{kr}} H(n)$
- If χ odd, then $H'(n) = 0$, else $H'(n)$ cyclic subgroup
- For $n = 1$ from the above s.e.s. $H'(n) = \mid A_F^{\chi}[p^k] \mid \cdot H(1)$
- If n is core then $H'(n) = H(n)$

Bounding class number

Theorem (Kolyvagin induction)

Let $\{\kappa_n\}$ is a Kolyvagin system, then $\kappa_n \in H'(n)$ for every n

If χ is odd, then there is no nonzero Kolyvagin systems

Corollary

If $\{\kappa_n\}$ is a Kolyvagin system for $\mu_p \otimes \chi^{-1}$ then

$$\mid A_F^{\chi} \mid \leq \max\{p^i \mid \kappa_1 \in (F^{\times})^{p^i}/(F^{\times})^{p^k}\}$$

Computation

- If we know class κ_1 r.h.s. can be computed
- Consider S-units for $S = \{\text{primes dividing } \kappa_1\}$
- It's a finitely generated abelian group, we can find this generators
- Decompose projection κ_1^χ and check p-valuation of exponents

Stub subsheaf

- Define stub subsheaf as $\mathcal{H}' \subset \mathcal{H}$
  - Stalk at n is $H'(n)$
  - Stalk at ℓ is image of $H'(n)$ under ψ_n^ℓ
  - Homomorphisms are restrictions $\bar{\psi}_n^\ell$

Theorem (Reformulated)

Every global section of $\mathcal{H}$ is actually a section of $\mathcal{H}'$

- Surjective path is a path s.t. map $H'(n) \to H'(e)$ is isomorphism

$$\cdots H'(n_{i-1}) \twoheadrightarrow H'(e_i) \xleftarrow{\sim} H'(n_i) \twoheadrightarrow H'(e_{i+1}) \xleftarrow{\sim} H'(n_{i+1}) \cdots$$

Rigidity

Theorem

1. *Suppose n is core vertex. Then for every $m \in \mathcal{N}$ there is surjective path from n to m*
2. *If P, Q two surjective paths between n, m then two maps equal in $Hom(H'(n), H'(m))$*

- Theorem says that if we restrict on subgraph on core vertices and edges that induce iso on stalks, theorem says that it's connected and provides canonical isomorphism $H(n) \simeq H(m)$
- We say that $\mathcal{H}'$ has trivial monodromy

Corollary

For core n specialization map $\boldsymbol{KS} \to H(n)$ is an isomorphism

Primitive systems

- We say that system $\boldsymbol{\kappa}$ is primitive if it generate $\boldsymbol{KS}$

Theorem

The following statements are equivalent

1. $\boldsymbol{\kappa}$ *is primtive*
2. κ_n *generates* $H'(n)$ *for every* n
3. κ_n *generates* $H'(n)$ *for some* n *with nonzero* $H(n)$

If $\boldsymbol{\kappa} \in \boldsymbol{KS}$ with $\kappa_1 \neq 1$, then $\boldsymbol{\kappa}$ is primitive iff

$$| A_F^{\chi}[p^k] | = \max\{p^i \mid \kappa_1 \in (F^{\times})^{p^i}/(F^{\times})^{p^k}\}$$

Back to cyclotomic system

The results above apply to every Kolyvagin system, and prove the existence of Kolyvagin systems for even characters χ without making use of the cyclotomic unit Kolyvagin system

Theorem

The cyclotomic unit Kolyvagin system is primitive

- Proof based on Gras conjecture proved by Mazur and Wiles
- Alternative proof given by Kolyvagin using analytic class number formula

Kolyvagin systems for general Galois representations

- Fix $\mathbb{Z}/p^k\mathbb{Z}[Gal(\mathbb{Q})]$-module T
- Most interesting cases are $\mu_p \otimes \chi^{-1}$ and $E[p^k]$
- Associate $H(1) = \{c \in H^1(\mathbb{Q}, T) \mid c_\ell \in H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)\}$
- We require that for all but finitely many ℓ $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = H^1_{unr}(\mathbb{Q}_\ell, T) := \mathrm{Ker}(H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell^{unr}, T))$
- $\mathcal{P}$ consist of prime ℓ's s.t.
    - T unramified at ℓ
    - $\ell \equiv 1 \mod p^k$
    - $\det(1 - Frob_\ell \mid T) = 0$
    - $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = H^1_{unr}(\mathbb{Q}_\ell, T)$

Finite and singular parts

Proposition

We again have a decomposition

$$H^1(\mathbb{Q}_\ell, T) = H^1_{unr}(\mathbb{Q}_\ell, T) \oplus H^1_{tr}(\mathbb{Q}_\ell, T)$$

and finite to singular map

$$\phi_\ell^{fs} : H^1_{unr}(\mathbb{Q}_\ell, T) \to H^1_{tr}(\mathbb{Q}_\ell, T)$$

where $H^1_{tr}(\mathbb{Q}_\ell, T) := \mathrm{Ker}(H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell(\mu_\ell), T))$

- Define the graph, Selmer sheaf and Kolyvagin systems as before

General modified Selmer groups

- Let T^* be Cartier dual of T
- $H^*(n)$ is the set of classes $c \in H^1(\mathbb{Q}_\ell, T^*)$ s.t.
    - c_ℓ orthogonal to $H^1_{unr}(\mathbb{Q}_\ell, T)$, if $\ell \nmid n$
    - c_ℓ orthogonal to $H^1_{tr}(\mathbb{Q}_\ell, T)$, if $\ell \mid n$

Theorem

Assuming some technical hypothesis, there is an integer $r(\chi)$ s.t.

- $H(n) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r \oplus H^*(n)$, *if* $r \geq 0$
- $H(n) \oplus (\mathbb{Z}/p^k\mathbb{Z})^{-r} = H^*(n)$, *if* $r \leq 0$

- Define $\chi(T) = \max\{0, r(T)\}$ and $\chi(T)$-stub subgroup $H'(n) =\mid H^*(n) \mid H(n)$

General results

Theorem

- *If $\chi(T) = 0$ there is no Kolyvagin systems*
- *If $\chi(T) = 1$ **KS** is a cyclic group of order p^k*
- *If $\chi(T) > 1$ then **KS** contains a free $\mathbb{Z}/p^k\mathbb{Z}$ module of any finite rank*

Theorem

Suppose $\chi(T) = 1$, then $\kappa_n \in H'(n)$ and following statements are equal

- *$\boldsymbol{\kappa}$ generates $\boldsymbol{KS}(T)$*
- *κ_n generates $H'(n)$ for every n*
- *Nonzero κ_n generates $H'(n)$ for some n*

It is still true under additional hypotheses that if $\chi(T) > 1$, then $\kappa_n \in H'(n)$ for every n

Bounding dual Selmer group

Corollary

1. For $\chi(T) \geq 1$ and $\boldsymbol{\kappa} \in \boldsymbol{KS}$

$$| H^*(1) | \leq \max\{p^i \mid \kappa_1 \in p^i H^1(\mathbb{Q}, T)\}$$

2. If $\chi(T) = 1$ then there is equality iff $\boldsymbol{\kappa}$ generates $\boldsymbol{KS}$

References

Mazur, B. and Rubin, K.
Introduction to Kolyvagin systems.

Mazur, B. and Rubin, K.
Kolyvagin systems.

Rubin, K.
Euler systems and Kolyvagin systems.