ALGANT Master Thesis

Duality theorems and Kolyvagin systems for elliptic curves

Marco Morosin

advised by
Prof. Massimo Bertolini

Outline

- State duality theorems for Galois cohomology
- Use them to define Kolyvagin systems
- Show how Kolyvagin systems control the Selmer groups of an elliptic curve

- K non-archimedean local field of characteristic 0.
- $M \in \mathrm{Gal}(\overline{K}/K)\text{-}\mathrm{Mod}$. Think of the n-torsion of an elliptic curve,

$$M = E_n := \ker\left(\cdot n\colon E(\overline{K}) \to E(\overline{K})\right).$$

- $H^r(K, M)$ the Galois cohomology groups.
- $M^D := \mathrm{Hom}(M, \overline{K}^\times)$ with a natural map $M^D \times M \to \overline{K}^\times$.
- Taking cup product and recalling local class field theory, we get a pairing

$$H^r(K, M^D) \times H^{2-r}(K, M) \xrightarrow{\cup} H^2(K, \overline{K}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

  $(0 \leqslant r \leqslant 2)$ and the induced morphism

$$H^r(K, M^D) \to \mathrm{Hom}\left(H^{2-r}(K, M),\ \mathbb{Q}/\mathbb{Z}\right).$$

Local Tate duality

If M is finite, this is an isomorphism.

Now: K number field, E/K elliptic curve, $M = E_{p^k}$, $R = \mathbb{Z}/p^k\mathbb{Z}$.

Recall

The p^k-Selmer module $\mathrm{Sel}_{p^k}(K, E)$ is the set of $c \in H^1(K, E_{p^k})$ such that all localizations satisfy

$$\mathrm{loc}_{\mathfrak{q}}(c) \in \mathrm{im}\left(\delta_{\mathfrak{q}} \colon E(K_{\mathfrak{q}}) \to H^1(K_{\mathfrak{q}}, E_{p^k})\right).$$

General Selmer modules

- Choose R-submodules $H^1_{\mathcal{F}}(K_{\mathfrak{q}}, M) \subset H^1(K_{\mathfrak{q}}, M)$ for finitely many primes (for all the other primes set the unramified condition).
- The Selmer module $H^1_{\mathcal{F}}(K, M)$ is the set of $c \in H^1(K, M)$ with $\mathrm{loc}_{\mathfrak{q}}(c) \in H^1_{\mathcal{F}}(K_{\mathfrak{q}}, M)$ for all $\mathfrak{q}$.

The dual Selmer module $H^1_{\mathcal{F}^D}(K, M^D)$

is obtained from the local conditions $H^1_{\mathcal{F}^D}(K_{\mathfrak{q}}, M^D) \coloneqq H^1_{\mathcal{F}}(K_{\mathfrak{q}}, M)^{\perp}$, orthogonal complements via the local Tate pairing.

Definition/Proposition

The *core rank* of $(\mathcal{F}, M)$ is the unique $r \in \mathbb{N}$ such that

$$H^1_{\mathcal{F}}(K, M) \cong H^1_{\mathcal{F}^D}(K, M^D) \oplus R^r$$

- If $\mathcal{F}$ is the usual p^k-Selmer structure, then $E_{p^k} = E^D_{p^k}$ and $\mathcal{F} = \mathcal{F}^D$, so the dual Selmer module is still $\mathrm{Sel}_{p^k}(K, E)$.
- We modify the usual Selmer structure by relaxing the condition above p:

$$H^1_{\mathcal{F}}(K_{\mathfrak{q}}, E_{p^k}) = \begin{cases} \mathrm{im}\left(\delta_{\mathfrak{q}} \colon E(K_{\mathfrak{q}}) \to H^1(K_{\mathfrak{q}}, E_n)\right) & \mathfrak{q} \nmid p \\ H^1(K_{\mathfrak{q}}, E_{p^k}) & \mathfrak{q} \mid p \end{cases}$$

  This new structure $\mathcal{F}$ has core rank $[K : \mathbb{Q}]$.
- To study $\mathrm{Sel}_{p^k}(K, E)$ it is enough to study $H^1_{\mathcal{F}^D}(K, M^D)$.

From now on we let $\mathcal{F}$ be this Selmer structure and we look for results for $H^1_{\mathcal{F}^D}(K, M^D)$.

We begin with the case of core rank 1: $K = \mathbb{Q}$.

Constructing Kolyvagin systems

For ℓ rational prime, consider

$$H^1_{\mathrm{un}}(\mathbb{Q}_\ell, M) := \ker\left(H^1(\mathbb{Q}_\ell, M) \to H^1(\mathbb{Q}_\ell^{\mathrm{un}}, M)\right)$$
$$H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) := \ker\left(H^1(\mathbb{Q}_\ell, M) \to H^1(\mathbb{Q}_\ell(\mu_\ell), M)\right)$$

and set $G_\ell := \mathrm{Gal}(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell)$, an abelian group.

There is a set of primes $\mathcal{P}$ of positive density such that:

- $H^1(\mathbb{Q}_\ell, M) = H^1_{\mathrm{un}}(\mathbb{Q}_\ell, M) \oplus H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M)$.
- there are isomorphisms $\varphi_\ell \colon H^1_{\mathrm{un}}(\mathbb{Q}_\ell, M) \xrightarrow{\sim} H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) \otimes G_\ell$

This gives maps $\varphi_\ell \circ \mathrm{pr}_{\mathrm{un}} \circ \mathrm{loc}_\ell$ and $\mathrm{pr}_{\mathrm{tr}} \circ \mathrm{loc}_\ell$:

$$H^1(\mathbb{Q}, M) \longrightarrow H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) \otimes G_\ell \longleftarrow H^1(\mathbb{Q}, M) \otimes G_\ell$$

Let $\mathfrak{n}$ be a squarefree product of primes of $\mathcal{P}$. Modify the Selmer structure:

$$H^1_{\mathcal{F}(\mathfrak{n})}(\mathbb{Q}_\ell, M) := \begin{cases} H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) & \ell \mid \mathfrak{n} \\ H^1_{\mathcal{F}}(\mathbb{Q}_\ell, M) & \text{otherwise} \end{cases}$$

and set $G_\mathfrak{n} = \bigotimes_{\ell|\mathfrak{n}} \mathrm{Gal}(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell)$. Now we may compare:

$$\underbrace{H^1_{\mathcal{F}(\mathfrak{n})}(\mathbb{Q}, M) \otimes G_\mathfrak{n}}_{\mathcal{S}(\mathfrak{n})} \longrightarrow H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) \otimes G_{\mathfrak{n}\ell} \longleftarrow \underbrace{H^1_{\mathcal{F}(\mathfrak{n}\ell)}(\mathbb{Q}, M) \otimes G_{\mathfrak{n}\ell}}_{\mathcal{S}(\mathfrak{n}\ell)}$$

Definition

A Kolyvagin system (of core rank 1) is a collection

$$\{\kappa_\mathfrak{n} \in \mathcal{S}(\mathfrak{n})\}_\mathfrak{n}$$

such that the images of $\kappa_\mathfrak{n}$ and $\kappa_{\mathfrak{n}\ell}$ coincide in the above diagram.

- The $\kappa_\mathfrak{n}$ are actually in $p^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})$, where $\lambda(\mathfrak{n}) := \mathrm{len}\, H^1_{\mathcal{F}(\mathfrak{n})^D}(K, M^D)$.
- We are interested in $\lambda(1) = \mathrm{len}\, H^1_{\mathcal{F}^D}(K, M^D)$: we look at κ_1...

In core rank r

- For a general K, $\mathbb{Q}_\ell(\mu_\ell)$ must be replaced by the *ray class field* mod $\mathfrak{q}$.
- We must take exterior powers

$$\mathcal{S}(\mathfrak{n}) := \bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, M) \otimes G_\mathfrak{n}$$

  (intuitively: regulators of elliptic curves are defined as determinants).
- Again we find maps from $\mathcal{S}(\mathfrak{n})$ and $\mathcal{S}(\mathfrak{nq})$ into some common module.
- Here we want to *restrict* to systems of the form

$$\{\kappa_\mathfrak{n} \in p^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})\}.$$

Theorem

The R-module $\mathbf{KS}'_r(M)$ of such systems is free of rank 1.

The idea

The isomorphism $H^1_{\mathcal{F}}(K, M) \cong H^1_{\mathcal{F}^D}(K, M^D) \oplus R^r$ implies

$$\kappa_1 \in p^{\lambda(1)} \mathcal{S}(1) \cong p^{\lambda(1)} R$$

which is a module of length $k - \lambda(1)$, if non-zero. Then $\operatorname{len} R\kappa_1 \leqslant k - \lambda(1)$.

Theorem

Let $\kappa \in \mathbf{KS}'_r(M)$.

- if $\kappa_1 \neq 0$, then

$$\operatorname{len} H^1_{\mathcal{F}^D}(K, M^D) \leqslant k - \operatorname{len} R\kappa_1 = \max\{i \mid \kappa_1 \in p^i \textstyle\bigwedge^r H^1_{\mathcal{F}}(K, M)\}$$

- if κ generates $\mathbf{KS}'_r(M)$ and $\kappa_1 \neq 0$, then equality holds.
- if κ generates $\mathbf{KS}'_r(M)$ and $\kappa_1 = 0$, then $\operatorname{len} H^1_{\mathcal{F}^D}(K, M^D) \geqslant k$.

How to find Kolyvagin systems?

In core rank 1, they are derived from *Euler systems*.

- There are some known Euler systems...
- ...and a map $\mathbf{ES}(M) \to \mathbf{KS}(M)$.
- This links L-values to arithmetic objects.

In higher core rank, the theory is still being developed.

- $\mathbf{ES}_r(M)$?
- $\mathbf{ES}_r(M) \to \mathbf{KS}_r(M)$?

Main references

1. J.S. Milne. *Arithmetic Duality Theorems. Third Edition.* 2020.
2. B. Mazur and K. Rubin. *Controlling Selmer groups in the higher core rank case.* Journal de Théorie des Nombres de Bordeaux. 2016.