EULER SYSTEMS

by

Ruichen Xu

Contents

Introduction

Selmer groups are central objects in number theory. They appear, for example, as certain class groups of number fields and important invariants of the arithmetic of elliptic curves. The machine of Euler systems can provide upper bounds for such groups. In this short note, we will introduce the machinery of Euler systems, following closely the classical book [**Rub00**, Chapter 1-5].

To first have a bird's-eye view on this subject, it is better to directly quote Barry Mazur [**Maz01**]:

> The main machine that has been responsible for much of this "knowledge" is Kolyvagin's technique for bounding Selmer groups, by constructing systematic collections of *global cohomology classes*. Now there are four distinct aspects to any of this work, which we can list "backwards".
>
> 1. Showing that *systematic collections* of global cohomology classes bound Selmer groups.
> 2. Constructing these *systematic collections* of global cohomology classes from *motivic objects* (e.g., from *Heegner points* in the Mordell-Weil group of the elliptic curve as in the work connected to the anti-cyclotomic p-adic L-functions, or from *Beilinson elements* in algebraic K-theory of the elliptic curve as in the work connected to the cyclotomic p-adic L-functions).
> 3. Constructing the motivic objects.
> 4. Connecting the motivic objects to a classical L-function.

Moreover, Mazur [**Maz01**] told young students how to learn this subject:

> Of course it is via these four steps that one sees that a classical L-function attached to the elliptic curve "controls" some aspect of the arithmetic of the elliptic curve. Clearly this is a somewhat intimidating machine. Nevertheless it is one of the "standard techniques" of our field, and is destined to remain so, and to become more general, if not more streamlined, in the coming years. It seems to us that the relatively painless way you can gain some familiarity with this machine is to do three things at once:
>
> 1. Keep the full program in the back of your mind, even if many of the steps are "black boxes".
> 2. Work on one step at a time, but do this in considerable detail.
> 3. Have a single concrete application in mind as a goal.

Following Mazur's suggestion, in this short note, we will (only) introduce the first aspect, namely seeing how a "*systematic collections* of global cohomology classes bound Selmer groups", and along the introduction, we will frequently go back to the classical case, realizing Selmer groups as certain ideal class groups of number fields, using the Euler system of cyclotomic units.

Acknowledgement. — We thank Professor Xin Wan for his guidence. We thank Haidong Li and Zerui Xiang for helpful discussions. The materials here are largely borrowed from [**Rub00**] and the note we took down for the course "Advanced Number Theory" delivered

by Ted Chinberg with the recordings shared online at https://www2.math.upenn.edu/~ted/720F18/hw-720SchedTab.html.

1. Selmer Groups

In this section, we introduce some abstract framework on Selmer groups.

1.1. p-adic Galois representations. — Throughout this note, we assume K is a number field, i.e. a finite extension of $\mathbb{Q}$. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Let p be a rational prime and $\mathcal{O}$ is the ring of integers of a finite extension Φ of $\mathbb{Q}_p$. We assume p is an odd prime for safety.

***Definition 1.1.* —** A **p-adic representation** of G_K with coefficients in $\mathcal{O}$ is a free $\mathcal{O}$-module T of finite rank with a continuous $\mathcal{O}$-linear action of G_K.

Let $\mathbf{D}$ denote the divisible abelian group $\Phi/\mathcal{O}$. We attach to a p-adic representation T with

- $V := T \otimes_{\mathcal{O}} \Phi$,
- $W := V/T = T \otimes_{\mathcal{O}} \mathbf{D}$,
- let M be any nonzero element of $\mathcal{O}$, W_M is the M-torsion part of M, i.e. $W_M = M^{-1}T/T \subseteq W$.

Let v be a place of the number field K, where we allow it to be either a nonarchimedian place or archimedian place. Let K_v is the completion of K at v.

- Let G_{K_v} be the absolute Galois group of K_v, which is a subgroup of G_K.
- Let I_v be the inertia subgroup of G_k, which is the absolute Galois group of the maximal unramified extension K^{ur} of K in $\overline{K}$.[(1)]
- When K_v is nonarchimedian corresponding to a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, let $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$ be the Frobenius automorphism. More explicitly, there is an exact sequence
$$1 \to I_v \to G_{K_v} \to \mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \to 1.$$
Note $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$ is isomorphic to the absolute Galois group of the residue field k_v and $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v) \cong G_{k_v} \cong \widehat{\mathbb{Z}}$, with the latter isomorphism sending the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p}} : x \mapsto x^{|k_v|}$ to $1 \in \widehat{\mathbb{Z}}$.

***Definition 1.2.* —** Suppose B is a G_{K_v}-module. We say B is **unramified** if I_v acts trivially on B.

Then

$$T \text{ is unramified at } v \Leftrightarrow V \text{ is unramified at } v \Leftrightarrow W \text{ is unramified at } v.$$

***Definition 1.3.* —** We say V is a **geometric representation** of G_K if the action of G_K on V is unramified outside a finite set of places and that for each place $v \mid p$, the representation of G_{K_v} on V is potentially semistable (equivalently, de Rham).

[(1)] We remark that when v is an archimedian place, K_v is either $\mathbb{R}$ or $\mathbb{C}$, and the inertia group $I_v = G_K$.

From now on, we always assume that V is geometric. This in particular implies that T is unramified outside a finite set of places.

1.2. Selmer structures and Selmer groups. —

1.2.1. *Selmer structures.* — We let B be a topological G_K-module which is unramified outside a finite set of places.

Definition 1.4. — Let v be a place of K. The **unramified cohomology** of B at v is defined to be

$$H^1_{\mathrm{ur}}(K_v, B) := \ker(H^1(K_v, B) \to H^1(I_v, B)).$$

The unramified cohomology can be computed quite explicitly via the inflation-restriction exact sequence.

Lemma 1.5 **([Rub00**, Lemma 1.3.2]**).** — *Suppose B is a G_{K_v}-module which is either a finitely generated $\mathbb{Z}_p$-module, or a finite-dimensional $\mathbb{Q}_p$-vector space, or a discrete torsion $\mathbb{Z}_p$-module.*

(i) If v is nonarchimedian, then

$$H^1_{\mathrm{ur}}(K_v, B) \cong H^1(K_v^{\mathrm{ur}}/K_v, B) \cong B^{I_v}/(\mathrm{Frob}_{\mathfrak{p}} - 1)B^{I_v}.$$

(ii) If v is nonarchimedian of residue characteristic different from p, then

$$H^1(K_v, B)/H^1_{\mathrm{ur}}(K_v, B) \cong H^1(I_v, B)^{\mathrm{Frob}_{\mathfrak{p}}=1}.$$

(iii) If v is archimedian, then $H^1_{\mathrm{ur}}(K_v, B) = 0$.

Mazur and Rubin [**MR04**, Chapter 2] introduced a general setup for Selmer groups.

Definition 1.6. — A **Selmer structure** of B is a collection of $\mathcal{O}$-submodules

$$\mathcal{F} = (\mathcal{F}_v)_v, \quad \mathcal{F}_v \subseteq H^1(K_v, B)$$

indexed by the places v of K, which satisfies $\mathcal{F}_v = H^1_{\mathrm{ur}}(K_v, B)$ outside a certain finite set of places containing the archemedian places.

Then we can define the corresponding Selmer groups.

Definition 1.7. — Let $\mathcal{F}$ be a Selmer structure of B. We define the **Selmer group** of B with respect to the Selmer structure $\mathcal{F}$ to be

$$\mathrm{Sel}_{\mathcal{F}}(K, B) := \ker\left(H^1(K, B) \to \prod_v \frac{H^1(K_v, B)}{\mathcal{F}_v}\right),$$

where the product is over all places v of K.

1.2.2. *Bloch-Kato Selmer structures*. — In application, what we care the most is the Bloch-Kato Selmer structures and the corresponding Selmer groups.

***Definition 1.8* (Bloch-Kato Selmer group).** — Keep the notations as above.

(i) We define the **finite part** of $H^1(K_v, V)$ by

$$H^1_{\mathrm{f}}(K_v, V) := \begin{cases} H^1_{\mathrm{ur}}(K_v, V), & v \nmid p, \\ \ker(H^1(K_v, V) \to H^1(K_v, V \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{cris}})), & v \mid p. \end{cases}$$

Then the collection $\{H^1_{\mathrm{f}}(K_v, V)\}_v$ is a Selmer structure, called the **Bloch-Kato Selmer structure**, denoted by $\mathcal{F}_{\mathrm{BK}}$.

(ii) The exact sequence $0 \to T \to V \to W \to 0$ yields an exact sequence

$$H^1(K_v, T) \to H^1(K_v, V) \to H^1(K_v, W).$$

We define $H^1_{\mathrm{f}}(K_v, T) \subseteq H^1_{\mathrm{f}}(K, T)$ (resp. $H^1_{\mathrm{f}}(K, W) \subseteq H^1(K, W)$) be the inverse image (resp. image) of $H^1_{\mathrm{f}}(K_v, V)$ under the natural maps.

(iii) For every nonzero $M \in \mathcal{O}$, the inclusion map $W_M \hookrightarrow W$ induces a natural map

$$i_M : H^1(K_v, W_M) \to H^1(K_v, W).$$

We define $H^1_{\mathrm{f}}(K_v, W_M) \subseteq H^1(K_v, W_M)$ to be the inverse image of $H^1_{\mathrm{f}}(K, W)$ under i_M.

(iv) Finally, for V, T, W or W_M, we define the **singular quotient** of $H^1(K_v, -)$ by

$$H^1_{\mathrm{s}}(K_v, -) := H^1(K_v, -)/H^1_{\mathrm{f}}(K_v, -).$$

The Bloch-Kato Selmer structure gives corresponding Selmer groups for V, T, W or W_M

$$\mathrm{Sel}_{\mathrm{BK}}(K, -) := \ker\left(H^1(K, -) \to \prod_v \frac{H^1(K_v, -)}{H^1_{\mathrm{f}}(K_v, -)}\right).$$

This Bloch-Kato Selmer structure is what we care the most. One may turn to [**Ski18**, Section 2.2.2] for many examples in concrete contexts like elliptic curves and modular forms.

It is worthwhile to go to the deeper ramification. Let v be a nonarchimedian place of K of residue characteristic different from p, then there is an exact sequence

$$0 \to T_v \to I_v \to \mathbb{Z}_p \to 0,$$

where T_v has trivial pro-p-part, called the **tame inertia group**. It follows that if M is a power of p, then I_v has a unique subgroup of index M as the inverse image of $M\mathbb{Z}_p$. We denote this subgroup by I_v^M by a slight abuse of notation.

Lemma 1.9. — *There is a canonical isomorphism of I_v-modules*

$$I_v/I_v^M \xrightarrow{\sim} \boldsymbol{\mu}_M,$$

given by $\sigma \mapsto \sigma(\varpi_v^{1/M})/\varpi_v^{1/M}$, where ϖ_v is any uniformizer of K_v.

Proof. — This is a direct application of Kummer theory. See [**Rub00**, Lemma 1.4.5]. □

If $M \in \mathcal{O}$ is nonzero, we let $\overline{M} \in \mathbb{Z}^+$ denote the smallest power of p which is divisible in $\mathcal{O}$ by M. We then fix a generator ζ of $\boldsymbol{\mu}_{\overline{M}}$ and let σ_ζ be the inverse image of ζ under the isomorphism of Lemma 1.9. Then we have the following explicit description of finite parts and singular parts.

Proposition 1.10. — *Suppose that v is a nonarchimedean place of K of residue characteristic different from p, that T is unramified, that $M \in \mathcal{O}$ is nonzero, and that $\boldsymbol{\mu}_{\overline{M}} \subseteq K$. Then evaluating cocycles on Frob_v and σ_ζ induces isomorphisms*

$$\beta_v : H^1_{\mathrm{f}}(K_v, W_M) \xrightarrow{\sim} W_M/(\mathrm{Frob}_v - 1)W_M, \quad \alpha_v : H^1_{\mathrm{s}}(K_v, W_M) \xrightarrow{\sim} W_M^{\mathrm{Frob}_v=1}.$$

respectively.

Proof. — This follows directly from the inflation-restriction exact sequence, with the observation that if K_v is nonarchimedian, then I_v has cohomogical dimension one, so $H^2(K_v^{\mathrm{ur}}/K, W_M^{I_v}) = 0$. Details are in [**Rub00**, Lemma 1.3.2, Lemma 1.4.7(i)]. □

The main goal of this note is to introduce the machine of Euler systems to give an upper bound of the Bloch-Kato Selmer group $\mathrm{Sel}_{\mathrm{BK}}(K, W)$. This is done by, very loosely speaking, delicately manipulating the local informations. To do this, we introduce two other kinds of Selmer structures, which seems to be rather trivial at first glance.

1.2.3. *Relaxed and strict Selmer structures.* — Let Σ be a finite set of places of K and $\mathcal{F}$ be a Selmer structures of B.

Definition 1.11 **(Relaxed Selmer structure).** — We define $\mathcal{F}^\Sigma$ be the Selmer structure

$$(\mathcal{F}^\Sigma)_v = \begin{cases} \mathcal{F}_v, & v \notin \Sigma, \\ H^1(K_v, B), & v \in \Sigma. \end{cases}$$

It is called the relaxed Selmer structure of $\mathcal{F}$ at Σ. It gives the relaxed Selmer group

$$\mathrm{Sel}_{\mathcal{F}^\Sigma}(K, B) = \ker\left(H^1(K_v, B) \to \prod_{v \notin \Sigma} H^1_{\mathrm{s}}(K_v, B) \right).$$

In other words, $\mathrm{Sel}_{\mathcal{F}^\Sigma}(K, B)$ consists of all cohomology classes $c \in H^1(K, B)$ satisfying the local conditions

- $c_v \in H^1_{\mathrm{f}}(K_v, B)$ if $v \notin \Sigma$, and
- *no* restriction for $v \in \Sigma$.

Definition 1.12 **(Strict Selmer structure).** — We define $\mathcal{F}_\Sigma$ be the Selmer structure

$$(\mathcal{F}_\Sigma)_v = \begin{cases} \mathcal{F}_v, & v \notin \Sigma, \\ 0, & v \in \Sigma. \end{cases}$$

It is called the strict Selmer structure of $\mathcal{F}$ at Σ. By definitions, the strict Selmer group is actually given by

$$\mathrm{Sel}_{\mathcal{F}_\Sigma}(K, B) = \ker\left(\mathrm{Sel}_{\mathcal{F}^\Sigma}(K, B) \to \prod_{v \in \Sigma} H^1(K_v, B) \right).$$

In other words, $\mathrm{Sel}_{\mathcal{F}_\Sigma}(K,B)$ consists of all classes $c \in \mathrm{Sel}_{\mathcal{F}^\Sigma}(K,B)$ satisfying the extra local conditions that $c_v = 0$ if $v \in \Sigma$.

Clearly we have the inclusion

$$\mathrm{Sel}_{\mathcal{F}_\Sigma}(K_v,B) \subseteq \mathrm{Sel}_{\mathcal{F}}(K_v,B) \subseteq \mathrm{Sel}_{\mathcal{F}^\Sigma}(K_v,B).$$

When $\Sigma = \emptyset$ is empty, the strict Selmer group and relaxed Selmer group of $\mathcal{F}$ are both simply $\mathrm{Sel}_{\mathcal{F}}(K,B)$. The notations are somewhat cumbersome, so when the Selmer structure $\mathcal{F}$ is clear from contexts, we will simply write

$$\mathrm{Sel}^\Sigma(K,B) := \mathrm{Sel}_{\mathcal{F}^\Sigma}(K_v,B), \quad \mathrm{Sel}_\Sigma(K,B) := \mathrm{Sel}_{\mathcal{F}_\Sigma}(K_v,B).$$

We remark that if Σ contains all primes above p, then the Selmer groups Sel^Σ and Sel_Σ are independent of the choice of the Selmer structure $\mathcal{F}_v$ for v dividing p.

We now list some properties of these relaxed and strict Selmer groups. Proofs of them are not hard and readers can find them in [Rub00] accordingly.

Proposition 1.13 **([Rub00**, Lemma 1.5.4]**).** — *If $M \in \mathcal{O}$ is nonzero and Σ is a finite set of primes of K, then the natural map $\iota_M : H^1(K,W_M) \to H^1(K,W)$ induces a surjection*

$$\mathrm{Sel}^\Sigma(K,W_M) \twoheadrightarrow \mathrm{Sel}^\Sigma(K,W)_M.$$

Note that this proposition need not be true if we replace Sel^Σ by Sel_Σ.

Proposition 1.14 **([Rub00**, Lemma 1.5.6]**).** — *If Σ is a finite set of primes of K, then*

(i) $\mathrm{Sel}^\Sigma(K,T) = \varprojlim_M \mathrm{Sel}^\Sigma(K,W_M)$ *and* $\mathrm{Sel}_\Sigma(K,T) = \varprojlim_M \mathrm{Sel}_\Sigma(K,W_M)$,
(ii) $\mathrm{Sel}^\Sigma(K,W) = \varinjlim_M \mathrm{Sel}^\Sigma(K,W_M)$ *and* $\mathrm{Sel}_\Sigma(K,W) = \varinjlim_M \mathrm{Sel}_\Sigma(K,W_M)$.

Proposition 1.15 **([Rub00**, Lemma 1.5.7]**).** — *If $M \in \mathcal{O}$ is nonzero and Σ is a finite set of primes of K, then*

(i) $\mathrm{Sel}^\Sigma(K,W_M)$ *is finite,*
(ii) $\mathrm{Sel}^\Sigma(K,T)$ *is a finitely generated $\mathcal{O}$-module,*
(iii) *the Pontryain dual of* $\mathrm{Sel}^\Sigma(K,W)$ *is a finitely generated $\mathcal{O}$-module.*

1.3. Duality theorems. — In this subsection, we will introduce the Tate local duality theorem and Poitou-Tate global duality theorems, but without proof.

1.3.1. *Dual representation*. — We first come up with some examples of p-adic representations.

Suppose $\rho : G_K \to \mathcal{O}^\times$ is a continuous character, not necessarily of finite order. Then we can take $T = \mathcal{O}_\rho$, where $\mathcal{O}_\rho$ is a free rank-one $\mathcal{O}$-module on which G_K acts via ρ. Clearly every one dimensional representation arises in this way. For example,

- When ρ is the trivial character, we get $T \cong \mathcal{O}$.
- When $\mathcal{O} = \mathbb{Z}_p$ and ρ is the cyclotomic character

$$\varepsilon_{\mathrm{cyc}} : G_K \to \mathrm{Aut}(\boldsymbol{\mu}_{p^\infty}) \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

Here $T \cong \mathbb{Z}_p(1) := \varprojlim_n \boldsymbol{\mu}_{p^n}$, $V \cong \mathbb{Q}_p(1) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n \boldsymbol{\mu}_{p^n}$ and $W \cong (\mathbb{Q}_p/\mathbb{Z}_p)(1) = \boldsymbol{\mu}_{p^\infty}$.

– For general $\mathcal{O}$, we write $\mathcal{O}(1) = \mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$, $\Phi(1) = \Phi \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(1)$ and write $\mathbf{D}(1) = \mathbf{D} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$.

Definition 1.16. — Let T be a p-adic representation of G_K, then the **dual representation**

$$T^* := \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1)).$$

Then we will also write

$$V^* := \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1)) = \mathrm{Hom}_{\mathcal{O}}(T, \Phi(1)) = T^* \otimes_{\mathcal{O}} \Phi$$

and

$$W^* := V^*/T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathbf{D}(1)).$$

Example 1.17. — If $\rho : G_K \to \mathcal{O}^*$ is a continuous character and $T = \mathcal{O}_\rho$, then $T^* = \mathcal{O}_{\rho^{-1}\varepsilon_{\mathrm{cyc}}}$.

1.3.2. *Local duality.* —

Theorem 1.18 **([Rub00, Theorem 1.4.1], Tate local duality theorem)**
Suppose that either v is nonarchimedian and $0 \leq i \leq 2$ or K is archimedian and $i = 1$, then the cup product and the local invariant map induce perfect pairings

(i) $H^i(K_v, V) \times H^i(K_v, V^*) \to H^2(K_v, \Phi(1)) \xrightarrow{\sim} \Phi$,
(ii) $H^i(K_v, W_M) \times H^i(K_v, W_M^*) \to H^2(K_v, \mathcal{O}(1)/M\mathcal{O}(1)) \xrightarrow{\sim} \mathcal{O}/M\mathcal{O}$,
(iii) $H^i(K_v, T) \times H^i(K_v, W^*) \to H^2(K_v, \mathbf{D}(1)) \xrightarrow{\sim} \mathbf{D}$.

When there will be no confusion, we will denote all of the perfect pairings of Theorem 1.18 by $\langle -, - \rangle_v$. Let B be either V, T, W or W_M and $C \subset H^1(K_v, B)$, then denote $C^\vee \subset H^1(K_v, B^*)$ be the orthogonal complement of C under the pairing $\langle -, - \rangle_v$, called the **Tate dual** of C.

Definition 1.19. — Let $\mathcal{F}$ be a Selmer structure of V, T, W or W_M, we can define its dual Selmer structure [(2)]

$$\mathcal{F}^\perp = (\mathcal{F}_v^\perp)_v, \quad \mathcal{F}_v^\perp \subset H^1(K_v, -)$$

to be the orthogonal complement of $\mathcal{F}_v$ under the pairing $\langle -, - \rangle_v$.

It is easy to see from the definition that the dual Selmer structure for relaxed and strict Selmer structures of $\mathcal{F}$ is given by

$$(\mathcal{F}^\Sigma)^\perp = (\mathcal{F}^\perp)_\Sigma, \quad (\mathcal{F}_\Sigma)^\perp = (\mathcal{F}^\perp)^\Sigma \tag{1.1}$$

for any finite set of places of K. The following proposition describes the dual Selmer structure of Bloch-Kato Selmer structure.

Proposition 1.20. — *Under the pairing $\langle -, - \rangle_v$,*

[(2)] Here the notation might be a liitle bit annoying, yet we do it deliberately to distinguish the following three "duals".

– B^* is the dual of B, where B is either V, T, W or W_M,
– $C^\vee$ is the dual under the local Tate duality for $C \subseteq H^1(K_v, B)$.
– $\mathcal{F}^\perp$ is designed to be the dual Selmer structure of a given Selmer structure $\mathcal{F}$.

Foutunately, we will never come up with Pontryagin duals in this note.

(i) *The finite parts* $H^1_{\mathrm{f}}(K_v, V)$ *and* $H^1_{\mathrm{f}}(K_v, V^*)$ *are orthogonal complements when* v *is archimedian and nonarchimedian of residue characteristic* $\ell \neq p$*. This is also true for* v *dividing* p *if* V *is a geometric representation.*
(ii) *The finite parts* $H^1_{\mathrm{f}}(K_v, T)$ *and* $H^1_{\mathrm{f}}(K_v, W^*)$ *are orthogonal complements.*
(iii) *If* M *in* $\mathcal{O}$ *is nonzero, then* $H^1_{\mathrm{f}}(K_v, W_M)$ *and* $H^1_{\mathrm{f}}(K_v, W_M^*)$ *are orthogonal complements.*

Proof. — For (i), the cases where v is archimedian and nonarchimedian of residue characteristic $\ell \neq p$ are proved in [**Rub00**, Proposition 1.4.2]. The $\ell = p$ case is far more complicated, where one can turn to [**Rub00**, Remark 1.7.1] for references. The claims (ii) and (iii) are [**Rub00**, Proposition 1.4.3]. □

1.3.3. *Global duality*. — The Poitou-Tate global duality theorem compares the Selmer groups of different Selmer conjectures. We first impose a partial ordering on the Selmer structures of M, writing $\mathcal{F}_1 \leq \mathcal{F}_2$, if for all places v of K, $\mathcal{F}_{1,v} \subseteq \mathcal{F}_{2,v}$. In this case, $\mathrm{Sel}_{\mathcal{F}_1}(K, M) \subseteq \mathrm{Sel}_{\mathcal{F}_2}(K, M)$. Note that we also have $\mathcal{F}_2^\perp \leq \mathcal{F}_1^\perp$.

Let M be either V, T, W or W_M.

Theorem 1.21 **([Mil06**, Theorem 4.10]**, Poitou-Tate long exact sequence)**
Suppose $\mathcal{F}_1 \leq \mathcal{F}_2$ *are two Selmer structures of* M*, then we have a long exact sequence*

$$0 \to \mathrm{Sel}_{\mathcal{F}_1}(K, M) \to \mathrm{Sel}_{\mathcal{F}_2}(K, M) \xrightarrow{\mathrm{res}} \prod_v \frac{\mathcal{F}_{2,v}}{\mathcal{F}_{1,v}} \xrightarrow{\mathrm{res}^\vee} \mathrm{Sel}_{\mathcal{F}_1^\perp}(K, M^*)^\vee \to \mathrm{Sel}_{\mathcal{F}_2^\perp}(K, M^*)^\vee \to 0,$$

where res *is the product of natural restriction maps*

$$\mathrm{res}_v : \mathrm{Sel}_{\mathcal{F}_2}(K, M) \to \mathcal{F}_{2,v} \twoheadrightarrow \frac{\mathcal{F}_{2,v}}{\mathcal{F}_{1,v}}$$

and $\mathrm{res}^\vee$ *is the Tate dual of*

$$\mathrm{Sel}_{\mathcal{F}_1^\perp}(K, M) \to \prod_v \mathcal{F}_{1,v}^\perp = \prod_v \left(\frac{H^1(K_v, M)}{\mathcal{F}_{1,v}} \right)^\vee,$$

with the final identification comes via Tate local duality.

Let $\Sigma_0 \subseteq \Sigma$ are finite set of places. Our main interest is to approximate the Bloch-Kato Selmer group $\mathrm{Sel}_{\mathrm{BK}}(K, W)$ step by step by the strict and relaxed Selmer structures. So we consider the Selmer structure

$$\mathcal{F}_{\mathrm{BK},\Sigma} \leq \mathcal{F}_{\mathrm{BK},\Sigma_0} \leq \mathcal{F}_{\mathrm{BK}} \leq \mathcal{F}_{\mathrm{BK}}^{\Sigma_0} \leq \mathcal{F}_{\mathrm{BK}}^{\Sigma}. \tag{1.2}$$

For the sake of this, we write

$$\mathrm{loc}_\Sigma : H^1(K, B) \to \bigoplus_{v \in \Sigma} H^1(K_v, B),$$

$$\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0} : \mathrm{Sel}^\Sigma(K, B) \to \bigoplus_{v \in \Sigma \setminus \Sigma_0} H^1_{\mathrm{s}}(K_v, B),$$

$$\mathrm{loc}^{\mathrm{f}}_{\Sigma,\Sigma_0} : \mathrm{Sel}_{\Sigma_0}(K, B) \to \bigoplus_{v \in \Sigma \setminus \Sigma_0} H^1_f(K_v, B)$$

for the respective localization maps. In this case we have the following corollary.

Theorem 1.22 **([Mil06**, Theorem 1.7.3]**).** — *Suppose* $\Sigma_0 \subseteq \Sigma$ *are finite set of places of* K.

(i) *There are exact sequences*

$$0 \to \mathrm{Sel}^{\Sigma_0}(K,B) \to \mathrm{Sel}^{\Sigma}(K,B) \xrightarrow{\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_{\mathrm{s}}(K_v,B)$$

and

$$0 \to \mathrm{Sel}_{\Sigma_0}(K,B^*) \to \mathrm{Sel}_{\Sigma}(K,B^*) \xrightarrow{\mathrm{loc}^{\mathrm{f}}_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_{\mathrm{f}}(K_v,B).$$

(ii) *There is an isomorphism*

$$\mathrm{Sel}_{\Sigma_0}(K,B^*)/\mathrm{Sel}_{\Sigma}(K,B^*) \xrightarrow{\sim} (\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}))^\vee.$$

Proof. — By applying $\mathcal{F}_1 := \mathcal{F}^{\Sigma_0}_{\mathrm{BK}}$ and $\mathcal{F}_2 := \mathcal{F}^{\Sigma}_{\mathrm{BK}}$ to Theorem 1.21 and observe (1.1) (1.2), we obtain the complete Poitou-Tate long exact sequence

$$0 \to \mathrm{Sel}^{\Sigma_0}(K,B) \to \mathrm{Sel}^{\Sigma}(K,B) \xrightarrow{\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_{\mathrm{s}}(K_v,B) \xrightarrow{\mathrm{res}^\vee} \mathrm{Sel}_{\Sigma_0}(K,B^*)^\vee \to \mathrm{Sel}_{\Sigma}(K,B^*)^\vee \to 0.$$

The first exact sequence in (i) is the first three terms, and the second exact sequence is the Tate dual of the last three terms[(3)]. Write it in a more compact way, we have

$$0 \to \frac{\mathrm{Sel}^{\Sigma}(K,B)}{\mathrm{Sel}^{\Sigma_0}(K,B)} \xrightarrow{\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_{\mathrm{s}}(K_v,B) \to \left(\frac{\mathrm{Sel}_{\Sigma_0}(K,B^*)}{\mathrm{Sel}_{\Sigma}(K,B^*)}\right)^\vee \to 0.$$

We then extract (ii) from it by applying an additional Tate dual. □

Theorem 1.22 will be applied to $B = W_M$ with Σ_0 equal to the empty set or the set of places dividing p, and Σ large enough so that $\mathrm{Sel}_{\Sigma}(K,W_M^*) = 0$. In that situation, Theorem 1.22(iii) implies that

$$|\mathrm{Sel}_{\Sigma_0}(K,W_M^*)| = \left|\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0})\right|. \tag{1.3}$$

Thus if one can produce *enough* cohomology classes in $\mathrm{Sel}^{\Sigma}(K,W_M)$, one obtains a good upper bound on the size of $\mathrm{Sel}_{\Sigma_0}(K,W_M^*)$. The purpose of Euler systems is to construct these classes. Here a basic principle is that to get the knowledge of Selmer groups of W_M^*, we need to go to its dual W_M.

1.4. Example: Ideal class groups. — In this section, we will focus on classical applications of Selmer groups on class groups of number fields.

1.4.1. *Trivial case.* — We consider $T = \mathbb{Z}_p$ with trivial G_K-action. Then $V = \mathbb{Q}_p$ and $W = \mathbb{Q}_p/\mathbb{Z}_p$. For positive integer M, $W_M = \mathbb{Z}/M\mathbb{Z}$. Moreover, let Σ be a finite set of places of K, then

$$\mathrm{Sel}^{\Sigma}(K,W) = \ker\left(H^1(K,W) \to \prod_{v\notin\Sigma} H^1_s(K_v,W)\right).$$

Since W has trivial G_K-action,

$$\mathrm{Sel}^{\Sigma}(K,W) = \{f \in \mathrm{Hom}_{\mathrm{cts}}(G_K,W) : f|_{G_{K_v}}(I_v) = 0, v \notin \Sigma\}.$$

[(3)]We can also apply $\mathcal{F}_1 := \mathcal{F}_{\mathrm{BK},\Sigma}$ and $\mathcal{F}_2 := \mathcal{F}_{\mathrm{BK},\Sigma_0}$ directly to Theorem 1.21 to obtain the second exact sequence in (i).

Let K_Σ be the maximal extension of K in $\overline{K}$ unramified outside the primes in Σ and K_Σ^{ab} be its maximal abelian subextension. Then since W is abelian, every $f \in \mathrm{Sel}^\Sigma(K,W)$ factors through $\mathrm{Gal}(K_\Sigma^{\mathrm{ab}}/K)$. Thus

$$\mathrm{Sel}^\Sigma(K,W) = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K_\Sigma^{\mathrm{ab}}/K), \mathbb{Q}_p/\mathbb{Z}_p).$$

Moreover, $\mathrm{Sel}_\Sigma(K,W)$ consists of continuous homomorphisms $f : \mathrm{Gal}(K_\Sigma^{\mathrm{ab}}/K) \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $f|_{G_{K_v}} = 1$ for all $v \in \Sigma$. Let H_Σ^{ab} be the maximal subfield of K_Σ^{ab} in which every $v \in \Sigma$ splits completely, then it follows that

$$\mathrm{Sel}_\Sigma(K,W) = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(H_\Sigma^{\mathrm{ab}}/K), \mathbb{Q}_p/\mathbb{Z}_p).$$

Then class groups appear when we invoke class field theory.

Example 1.23. **—** When Σ is empty, K_Σ^{ab} is nothing but the Hilbert class field of K, which is a finite Galois extension of K with Galois group isomorphic to the class group A_K of K. So $\mathrm{Sel}^\emptyset(K,W) = \mathrm{Sel}_\emptyset(K,W) = \mathrm{Hom}(A_K, \mathbb{Q}_p/\mathbb{Z}_p)$.

Recall in the previous section, we have seen that to bound the Selmer group of W, we need to construct cohomology classes in the Selmer group in W^*. So it is necessary to consider the dual of this trivial case, which we will call the *classical case* in this note.

1.4.2. *Classical case.* — We recall briefly the background on Kummer maps.

Interlude: Kummer maps. — We now start with any field K (only in this interlude paragraph) and integer $n \geq 1$ that is coprime to the characteristic of K. We fix a seperable closure K^{sep} of K. Then we have a short exact sequence of G_K-modules

$$0 \to \boldsymbol{\mu}_n \to (K^{\mathrm{sep}})^\times \xrightarrow{\times n} (K^{\mathrm{sep}})^\times \to 0,$$

where $\boldsymbol{\mu}_n$ is the G_K-module of n-th roots of unity in K^{sep}. We take the long exact sequence attached to it, and obtain

$$K^\times \xrightarrow{\times n} K^\times \to H^1(K, \boldsymbol{\mu}_n) \to H^1(K, (K^{\mathrm{sep}})^\times) = 0.$$

Here $H^1(K, (K^\times)^{\mathrm{sep}}) = 0$ is due to the Hilbert theorem 90. Then it gives an isomorphism

$$\delta_K : K^\times/K^{\times n} \xrightarrow{\sim} H^1(K, \boldsymbol{\mu}_n).$$

This isomorphism is called the **Kummer map** of K. It has an explicit description by 1-cocycles. Let $a \in K^\times/K^{\times n}$, then δ_K sends it to a cohomology class given by the 1-cocycle

$$c_a : \mathrm{Gal}_K \to \boldsymbol{\mu}_n, \quad \sigma \to \sigma(\sqrt[n]{a})/\sqrt[n]{a},$$

where $\sqrt[n]{a}$ is an n-th root of a in K^{sep}. One checks that this 1-cocycle c_a indeed gives a well-defined cohomology class in $H^1(K, \boldsymbol{\mu}_n)$.

Dual of the trivial case and their H^1. — By Example 1.17, the Tate dual of the previous trivial case is given by

$$T^* = \mathbb{Z}_p(1) = \varprojlim_n \boldsymbol{\mu}_{p^n}, \quad V^* = \mathbb{Q}_p(1), \quad W^* = W \otimes \mathbb{Z}_p(1) = \boldsymbol{\mu}_{p^\infty}.$$

Then by [**Rub00**, Proposition B.2.3], we see that

$$H^1(K, T^*) = H^1(K, \varprojlim_n \boldsymbol{\mu}_{p^n}) \cong \varprojlim_n H^1(K, \boldsymbol{\mu}_{p^n}) \xleftarrow{\sim} \varprojlim_n (K^\times / K^{\times p^n}) =: \widehat{K^\times}.$$

where the middle isomorphism is given by Kummer maps of K and $\widehat{K^\times}$ denotes the pro-p completion of $K^\times$. Moreover, by [**Rub00**, Proposition B.2.4],

$$H^1(K, V^*) = H^1(K, \mathbb{Z}_p(1) \otimes_{\mathbb{Z}} \mathbb{Q}) = \widehat{K^\times} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Later we are more interested in the torsion coefficients: let $M = p^f$ be a positive integer, then $W_M^* = \boldsymbol{\mu}_{p^f}$. Then again by the Kummer map,

$$H^1(K, W_M) = H^1(K, \boldsymbol{\mu}_{p^f}) \xleftarrow{\sim} K^\times / (K^\times)^{p^f}.$$

Bloch-Kato Selmer structure under Kummer map. — Let Σ_p be the finite set of all places of K above p. Let Σ be a finite set of places of K containing Σ_p. This assumption will free ourself from the complicated Selmer structures at Σ_p. For $v \notin \Sigma$, we try to build up the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_{\mathrm{ur}}(K_v, \boldsymbol{\mu}_{p_f}) & \longrightarrow & H^1(K_v, \boldsymbol{\mu}_{p_f}) & \longrightarrow & H^1_{\mathrm{s}}(K_v, \boldsymbol{\mu}_{p_f}) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow{\scriptstyle \delta_{K_v}} & & \uparrow & & \\ 0 & \longrightarrow & \ker(\mathrm{ord}_v) & \longrightarrow & K_v^\times/(K_v^\times)^{p^f} & \xrightarrow{\mathrm{ord}_v} & \mathbb{Z}/p^f & \longrightarrow & 0 \end{array}.$$

Here the middle vertical map is the Kummer map of K_v, which is an isomorphic, and

$$\ker(\mathrm{ord}_v) = \{\alpha \in K_v^\times/(K_v^\times)^{p^f} : p^f \text{ divides } \mathrm{ord}_v(\alpha)\}.$$

We shall show that $H^1_{\mathrm{ur}}(K_v, \boldsymbol{\mu}_{p_f})$ is isomorphic to $\ker(\mathrm{ord}_v)$ via the Kummer map δ_{K_v}. In fact, let $\alpha \in K_v^\times/(K_v^\times)^{p^f}$ that is identified with the cocycle class $[c_\alpha] \in H^1(K_v, \boldsymbol{\mu}_{p^f})$, then $[c_\alpha]$ is unramified means exactly that the cocycle $c_\alpha : \sigma \mapsto \sigma(\alpha^{1/p^f})/\alpha^{1/p^f}$ is trivial on I_v, i.e.

$$\sigma(\alpha^{1/p^f}) = \alpha^{1/p^f}, \quad \text{for any } \sigma \in I_v.$$

This is equivalent to that $K_v(\alpha^{1/p^f})/K_v$ is an unramified extension. As v is not dividing p, this is equivalent to that $p^f \mid \mathrm{ord}_v(\alpha)$.

Therefore, we can fill up the leftmost vertical arrow. By five-lemma, the rightmost vertical arrow is also an isomorphism.

Back to the global situation, the Selmer group $\mathrm{Sel}^\Sigma(K, \boldsymbol{\mu}_{p^f})$ can then be expressed explicitly via the Kummer map δ_K as

$$\mathrm{Sel}^\Sigma(K, \boldsymbol{\mu}_{p^f}) \xleftarrow[\sim]{\delta_K} \{\alpha \in K^\times/(K^\times)^{p^f} : p^f \text{ divides } \mathrm{ord}_v(\alpha), v \notin \Sigma\} =: (K^\times/(K^\times)^{p^f})^\Sigma.$$

Then let $\Sigma_p \subseteq \Sigma_0 \subseteq \Sigma$, the exact sequence in Theorem 1.22(i) is quite explicit as

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}^{\Sigma_0}(K, \boldsymbol{\mu}_{p^f}) & \longrightarrow & \mathrm{Sel}^{\Sigma}(K, \boldsymbol{\mu}_{p^f}) & \xrightarrow{\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}} & H^1_{\mathrm{s}}(K_v, \boldsymbol{\mu}_{p_f}) \\ & & \uparrow & & \uparrow{\scriptstyle \delta_{K_v}} & & \uparrow \\ 0 & \longrightarrow & (K^\times/(K^\times)^{p^f})^{\Sigma_0} & \longrightarrow & (K^\times/(K^\times)^{p^f})^{\Sigma} & \xrightarrow[\bigoplus_{v\in\Sigma\setminus\Sigma_0}\mathrm{ord}_v]{} & \bigoplus_{v\in\Sigma\setminus\Sigma_0}\mathbb{Z}/p^f \end{array}$$

where vertical arrows are isomorphisms given by Kummer maps. So shifting to the explicit bottom line, (1.3) tells us that the key is to calculate the cokernel of the localization map $\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}$. The target itself, as several copies of $\mathbb{Z}/p^f$, has size $p^f\,|\Sigma \setminus \Sigma_0|$, so the key is to figure out the image of $\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}$. It would be great if we could construct the full image of it, but in most cases, we cannot. So by only knowing a part of its image, we can only get a lower bound on the size of $\mathrm{im}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0})$, which means an upper bound of $\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0})$, this is by (1.3) an upper bound of the Selmer group. We will make that procedure explicit in Section 3.

The question is, how to get sufficiently many element in $\mathrm{im}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0})$? We source back to $(K^\times/(K^\times)^{p^f})^{\Sigma}$, the key of doing this is to construct sufficiently many global units in $K^\times$ with *good* local property that they altogether produce a large image under the local orders ord_v.

The machine of Euler systems produces such global units with good local properties in a systematic way. There are roughly three steps.

1. Fix a system of finite Galois extensions F/K and construct classes
$$\mathbf{c}_F \in H^1(F, \boldsymbol{\mu}_{p^f}) = F^\times/(F^\times)^{p^f}.$$
The collection of such cohomology classes $\{\mathbf{c}_F\}_F$ forms an *Euler system*. We will introduce this in Section 2.1.
2. Recall we have the inflation-restriction exact sequence (see, for example, [**NSW08**, (1.6.7)] or [**NSW08**, Section 2.4] for an approach via Hochschild-Serre spectral sequence)
$$0 \to H^1(F/K, \boldsymbol{\mu}_{p^f}^{G_F}) \to H^1(K, \boldsymbol{\mu}_{p^f}) \to H^1(F, \boldsymbol{\mu}_{p^f})^{\mathrm{Gal}(F/K)} \xrightarrow{\mathrm{tg}} H^2(F/K, \boldsymbol{\mu}_{p^f}^{G_F}).$$
So to go back to $H^1(K, \boldsymbol{\mu}_{p^f})$, we need to construct an operator $\mathbb{D}_F \in \mathbb{Z}[\mathrm{Gal}(F/K)]$ such that $\mathbb{D}_F(\mathbf{c}_F)$ is $\mathrm{Gal}(F/K)$-invariant and its image in $H^2(F/K, \boldsymbol{\mu}_{p^f}^{G_F})$ under the transgression map is trivial. Here the operator is called the *Kolyvagin operator* and the resulting classes in $H^1(K, \boldsymbol{\mu}_{p^f})$ is called the *derived cohomology classes*.[(4)] This will be covered in Section 2.2.
3. Along the way of construction, we need to closely examine the local behaviours of the cohomology classes to make them really useful for bounding the Selmer groups. This will be taken care of in Section 2.3.

[(4)] Here the discussion is motivitional, actually the Kolyvagin operators and derived cohomology classes are not precisely defined in this way.

1.4.3. *Twisted cases.* — Before diving into the abstract framework of Euler systems and Kolyvagin derived cohomology classes, we introduce a twisted version of the trivial and classical case, which is the case used in our main application in Section 3.4.

Twisted trivial case. — Suppose that $\chi : G_K \to \mathcal{O}^\times$ is a character of finite prime-to-p order, and let $T = \mathcal{O}_\chi$, a free rank-one $\mathcal{O}$-module on which G_K acts via χ. Let L be a *finite* abelian extension of K of degree prime to p such that χ factors through $\Delta := \mathrm{Gal}(L/K)$. [(5)] We write $\mathbf{D}_\chi = \mathbf{D} \otimes \mathcal{O}_\chi$ and $\Phi_\chi = \Phi \otimes \mathcal{O}_\chi$.

In this case, the Bloch-Kato Selmer structures are quite explicit. Suppose v is a place of K and w is a place of L above v. Then by [**Rub00**, Proposition B.5.3(ii)], the restriction map gives isomorphisms

$$H^1(K_v, V) \cong \left(\oplus_{w|v} \mathrm{Hom}(G_{L_w}, V)\right)^\Delta = \left(\oplus_{w|v} \mathrm{Hom}(G_{L_w}, \Phi_\chi)\right)^\Delta.$$

Moreover, if $v \nmid p$, this isomorphism identifies

$$H^1_{\mathrm{f}}(K_v, V) = H^1_{\mathrm{ur}}(K_v, V) \cong \left(\oplus_{w|v} \mathrm{Hom}(G_{L_w}/I_w, V)\right)^\Delta.$$

A happy coincidence[(6)] is that in this case, even for $v \mid p$, we have

$$H^1_{\mathrm{f}}(K_v, V) = H^1_{\mathrm{ur}}(K_v, V) \tag{1.4}$$

as above. We remark that this coincidence is really essential in the proof of our main application, i.e. Theorem 3.7, since the Euler system approach can only, roughly speaking, end up with an upper bound for the strict Selmer group $\mathrm{Sel}_{\Sigma_p}(K, W)$. This is the drawback of this machine in nature, since from the very definition of Euler systems, it neglects the information at the places away from p. Therefore, to go back to the Bloch-Kato Selmer group $\mathrm{Sel}_{\mathrm{BK}}(K, W)$, we need more information of the representation T at local places v above p.

Since the Bloch-Kato Selmer structure is quite clear in this case, it is not surprise to get the following description of the Bloch-Kato Selmer group, whose proof is quite direct.

Theorem 1.24 **([Rub00**, Proposition 1.6.2]**).** — *We have*

$$\mathrm{Sel}_{\mathrm{BK}}(K, W) \cong \mathrm{Hom}(A_L, \mathbf{D}_\chi)^\Delta = \mathrm{Hom}_{\mathcal{O}}(A_L^\chi, \mathbf{D}),$$

where A_L^χ is the χ-component of A_L.

Twisted classical case. — As we have seen previously, to bound $\mathrm{Sel}_{\mathrm{BK}}(K, W)$, we have to turn to the dual representation. From Example 1.17, we see $T^* = \mathbb{Z}_p(1) \otimes \chi^{-1}$, and the restriction map gives an isomorphism

$$H^1(K, T^*) \cong H^1(L, T^*)^\Delta \cong (\widehat{L^\times} \otimes \mathcal{O}_{\chi^{-1}})^\Delta \cong (L^\times)^\chi. \tag{1.5}$$

This is again quite explicit.

[(5)] A subtle point is that here L is not required to be the smallest extension of K that meets the condition, i.e. $\overline{K}^{\ker \chi}$. In practice, we could make it a little bit larger (but still a finite extension of K). For example, when $K = \mathbb{Q}$, by Kronecker-Weber theorem, L is contained in some cyclotomic field $\mathbb{Q}(\zeta_m)$. When χ is of conductor f, we can let $L = \mathbb{Q}(\zeta_f)$. Moreover, if χ is an even character, L can be $\mathbb{Q}(\zeta_f)^+$, the maximal totally real subextension of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$. Such choice of L makes Theorem 3.7 more explicit.

[(6)] Unfortunately, we have not find its proof in neither [**Rub00**] nor [**MR04**]. Maybe we can leave it to readers that are familiar with p-adic Hodge theory.

2. Euler Systems and Derived Cohomology Classes

In this section, we define Euler systems and their derived cohomology classes, nowadays known as Kolyvagin classes. Readers are sugguested to go back to the examples in Section 1.4 occasionally to get a feel of what is going on.

We continue to use the same notations as in the previous section.

- K is a number field with the ring of integers $\mathcal{O}_K$.
- T is a p-adic Galois representation of G_K, i.e. T is a finite free $\mathcal{O}$-module, where $\mathcal{O}$ is the ring of integers of a finite extension Φ of $\mathbb{Q}_p$. We assume T is unramified outside a finite set of primes.
- T^* is the dual representation of T, defined as $T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1))$.

We will write $K \subseteq_{\mathrm{f}} F$ to indicate that F is a finite extension of K.

Suppose $\mathfrak{q}$ is a prime of K not dividing p and T is unramified at $\mathfrak{q}$. Let $K[\mathfrak{q}]$ be the ray class field of K of modulus $\mathfrak{q}$ and $K(\mathfrak{q})$ be the maximal p-extension of K inside $K[\mathfrak{q}]$. Let $\mathrm{Frob}_{\mathfrak{q}}$ denote the Frobenius of $\mathfrak{q}$ in G_K and define

$$P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*, X) := \det(1 - \mathrm{Frob}_{\mathfrak{q}}^{-1}\,X|T^*) \in \mathcal{O}[X].$$

This is well-defined since T^* is unramified at $\mathfrak{q}$.

2.1. Euler systems. —

We first define what an Euler system is.

***Definition 2.1* (Euler systems). —** Suppose $\mathcal{K}$ is an infinite abelian extension of K and $\mathcal{N}$ is an ideal of $\mathcal{O}_K$ divisible by p and all primes where T is ramified, such that

(i) $\mathcal{K}$ contains $K(\mathfrak{q})$ for every prime $\mathfrak{q}$ of K not dividing $\mathcal{N}$,
(ii) $\mathcal{K}$ contains an $\mathbb{Z}_p^d$-extension K_∞ of K such that no finite prime of K splits completely in K_∞/K.

A collection of cohomology classes

$$\mathbf{c} = \{\mathbf{c}_F \in H^1(F, T) : K \subseteq_{\mathrm{f}} F \subseteq \mathcal{K}\}$$

is an **Euler system** for $(T, \mathcal{K}, \mathcal{N})$ if, whenever $K \subseteq_{\mathrm{f}} F \subseteq_{\mathrm{f}} F' \subseteq \mathcal{K}$, then

$$\mathrm{cor}_{F'/F}(\mathbf{c}_{F'}) = \left(\prod_{\mathfrak{q} \in \Sigma(F'/F)} P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1}) \right) \mathbf{c}_F,$$

where $\Sigma(F'/F)$ is the set of finite primes of K, not dividing $\mathcal{N}$, which ramify in F' but not in F. This condition is called the **norm compatibility condition**.

Here by saying K_∞/K is a $\mathbb{Z}_p^d$-extension, we mean it is a Galois extension with Galois group isomorphic to $\mathbb{Z}_p^d$ for some $d \geq 1$. The condition (ii) is satisfied if K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of K. There does exist $\mathbb{Z}_p$-extensions such that some prime p of K splits completely in K_∞, for example the anticyclotomic $\mathbb{Z}_p$-extension K_∞^{ac} of an imaginary quadratic field K. In such situations, certain "Euler-system-like" objects can also be considered, introduced in [**Rub00**, Section 9.2, 9.4].

2.1.1. *Reformulation with ray class fields.* — We try to get rid of the annoying product over $\Sigma(F'/F)$. To accomplish that, we go to a special tower of K. Let $\mathfrak{m}$ be a modulus of K and let $K[\mathfrak{m}]$ denote the ray class field of K modulo $\mathfrak{m}$. Given $\mathcal{K}$ and $\mathcal{N}$ as in Definition 2.1, an Euler system for $(T, K, \mathcal{N})$ is equivalent to a collection

$$\{\tilde{\mathbf{c}}_{\mathfrak{m}} \in H^1(K[\mathfrak{m}] \cap \mathcal{K}, T) : \text{ for any modulus } \mathfrak{m}\}$$

satisfying

$$\mathrm{cor}_{K[\mathfrak{m}\mathfrak{q}]\cap\mathcal{K}/K[\mathfrak{m}]\cap\mathcal{K}}(\tilde{\mathbf{c}}_{\mathfrak{m}\mathfrak{q}}) = \begin{cases} P(\mathrm{Frob}_{\mathfrak{q}}^{-1}|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\tilde{\mathbf{c}}_{\mathfrak{m}}, & \mathfrak{q} \nmid \mathfrak{m}\mathcal{N}, \\ \tilde{\mathbf{c}}_{\mathfrak{m}}, & \mathfrak{q} \mid \mathfrak{m}\mathcal{N}. \end{cases}$$

For, given such a collection, if F is a subfield of $\mathcal{K}$, then we can define

$$\mathbf{c}_F = \mathrm{cor}_{K[\mathfrak{m}]\cap\mathcal{K}/F}(\tilde{\mathbf{c}}_{\mathfrak{m}}),$$

where $\mathfrak{m}$ is the conductor of F/K. One checks easily that the collection $\mathbf{c}_F$ is an Euler system. Conversely, given an Euler system $\mathbf{c}_F$, we can define

$$\tilde{\mathbf{c}}_{\mathfrak{m}} = \prod_{\mathfrak{q}\in\Sigma[\mathfrak{m}]} P(\mathrm{Frob}_{\mathfrak{q}}^{-1}|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbf{c}_{K[\mathfrak{m}]\cap\mathcal{K}},$$

where $\Sigma[\mathfrak{m}]$ consists of primes $\mathfrak{q}$ which divide $\mathfrak{m}$ but do not divide $\mathcal{N}$, and which are unramified in $(K[\mathfrak{m}] \cap \mathcal{K})/K$.

2.1.2. *Twisted Euler systems.* — Motivated by the twisted cases in Section 1.4.3, we need to make it precise what the twisted Euler system looks like.

Keep the notations as in Section 1.4.3. We fix a generator ξ_χ of $\mathcal{O}_\chi$ and write $T \otimes \chi := T \otimes_{\mathcal{O}} \mathcal{O}_\chi$.

Definition 2.2. — Suppose $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$. If $K \subseteq_{\mathrm{f}} F \subseteq \mathcal{K}$, define $\mathbf{c}_F^\chi \in H^1(F, T \otimes \chi)$ to be the image of $\mathbf{c}_{FL}$ under the composition

$$H^1(FL, T) \xrightarrow{\otimes\xi_\chi} H^1(FL, T) \otimes \mathcal{O}_\chi \cong H^1(FL, T \otimes \chi) \xrightarrow{\mathrm{cor}_{FL/F}} H^1(FL, T \otimes \chi).$$

By the routine verification, we see that the resulting $\{\mathbf{c}_F^\chi\}$ forms an Euler system.

Proposition 2.3 **([Rub00, Proposition 2.4.2]).** — *Let $\mathfrak{f}$ be the conductor of χ, then the collection $\{\mathbf{c}_F^\chi : K \subseteq_{\mathrm{f}} F \subseteq \mathcal{K}\}$ defined above is an Euler system for $(T \otimes \chi, \mathcal{K}, \mathfrak{f}\mathcal{N})$.*

Another easy computation shows the following.

Proposition 2.4 **([Rub00, Lemma 2.4.3]).** — *With notations as in Definition 2.2, suppose $K \subseteq_{\mathrm{f}} F \subseteq K_\infty$ and $L \subseteq L \subseteq_{\mathrm{f}} L' \subseteq \mathcal{K}$. If every prime which ramifies in L'/K is already ramified in L/K, then the image of $\mathbf{c}_F^\chi$ under the composition*

$$H^1(F, T \otimes \chi) \xrightarrow{\mathrm{res}_{FL'/F}} H^1(FL', T \otimes \chi) \xrightarrow{\otimes\xi_\chi^{-1}} H^1(FL', T),$$

is

$$\sum_{\delta\in\mathrm{Gal}(FL'/F)} \chi(\delta)\delta\mathbf{c}_{FL'}.$$

2.1.3. *Example: The Euler system of cyclotomic units.* — In this section, we consider the case $K = \mathbb{Q}$, $\mathcal{O} = \mathbb{Z}_p$ and $T = \mathbb{Z}_p(1)$.[(7)] Then T is unramified outside p. We see immediately that $T^* = \mathbb{Z}_p$ is the trivial G_K-module.

Frobenius polynomial. — Since Frob_q^{-1} acts trivially on T^*, we see that for any prime number $q \neq p$,

$$P(\mathrm{Frob}_q^{-1}\,|T^*; X) = \det(1 - X|\mathbb{Z}_p) = 1 - X.$$

Corestriction map and the norm compatibility. — Let $\mathbb{Q} \subseteq_{\mathrm{f}} F \subseteq_{\mathrm{f}} F'$, then one checks that we have the commutative diagram

$$\begin{array}{ccc} H^1(F', \mathbb{Z}_p(1)) & \xrightarrow{\delta_{F'}} & \widehat{(F')^\times} \\ {\scriptstyle \mathrm{cor}_{F'/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{Nm}_{F'/F}} \\ H^1(F, \mathbb{Z}_p(1)) & \xrightarrow{\delta_F} & \widehat{F^\times} \end{array},$$

where the horizontal maps are corresponding Kummer maps. Moreover, by class field theory (see, for example, [**Mil20**, Example 3.10]), we have an explicit description of the ray class fields $\mathbb{Q}[m]$ for modulus m of $\mathbb{Q}$.

- If $\infty \nmid m$, then $\mathbb{Q}[m] = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, i.e. the maximal real subfield $\mathbb{Q}(\zeta_m)^+$ of $\mathbb{Q}(\zeta_m)$.
- Otherwise $\infty \mid m$, we write $m = \infty m'$, then $\mathbb{Q}[m] = \mathbb{Q}(\zeta_{m'})$.

Therefore, to give an Euler system for $(\mathbb{Z}_p(1), \mathcal{K} = \mathbb{Q}^{\mathrm{ab}}, \mathcal{N} = p\mathbb{Z})$, it suffices to define a system of global units $\tilde{\mathbf{c}}_m \in \widehat{\mathbb{Q}(\zeta_m)^\times}$ (corresponding to the modulus $m\infty$) for all positive integer m satisfying the norm compatibility condition

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{mq})/\mathbb{Q}(\zeta_q)}(\tilde{\mathbf{c}}_{mq}) = \begin{cases} (1 - \mathrm{Frob}_q^{-1})\tilde{\mathbf{c}}_m, & q \nmid mp, \\ \tilde{\mathbf{c}}_m, & q \mid mp. \end{cases} \tag{2.6}$$

Indeed, we should have defined the global units corresponding to the finite modulus m, one checks that

$$\tilde{\mathbf{c}}_{m^+} = \mathrm{Nm}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+}\,\tilde{\mathbf{c}}_m \in (\widehat{\mathbb{Q}(\zeta_m)^+})^\times$$

works.

Cyclotomic units. — We let $\{\zeta_m\}_{m\geq 1}$ be a compatible system of primitive roots of unity, i.e. for each m, ζ_m is a primitive m-th root of unity, and for any $n, m \geq 1$, $\zeta_{mn}^n = \zeta_m$.

We define

$$\tilde{\mathbf{c}}_m := \mathrm{Nm}_{\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)}(1 - \zeta_{mp}) \in \widehat{\mathbb{Q}(\zeta_m)^\times}.$$

This family of global units are called **cyclotomic units**. Then we need to check that cyclotomic units indeed satisfy the norm compatibility condition (2.6). This follows from the following elementary calculations. [(8)]

[(7)] Here our notation is quite opposite to that in Section 1.4, where we used $T = \mathbb{Z}_p$ the trivial action and $T^* = \mathbb{Z}_p(1)$.

[(8)] This is stated in [**Rub00**, Section 3.2], but with a sign error, where Rubin used $\zeta_{m\ell} - 1$ instead of $1 - \zeta_{m\ell}$. This does not seems quite right since one computes $\mathrm{Nm}_{\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)}(\zeta_8 - 1) = 1 - \zeta_4 \neq \zeta_4 - 1$. The problem is that the $\ell = 2$ case should have been considered seperately. By the same way of computation as in our proof,

Lemma 2.5. — *For every positive integer m and prime ℓ, we have the relation*

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m)}(1-\zeta_{m\ell}) = \begin{cases} 1-\zeta_m, & \ell \mid m, \\ (1-\zeta_m)^{1-\mathrm{Frob}_\ell^{-1}}, & \ell \nmid m \text{ and } m>1 \\ \ell, & m=1. \end{cases}$$

Proof. — We first consider the case $\ell \nmid m$ and $m \geq 1$. Then $\zeta_{ml} = \zeta'_m\zeta'_\ell$ for ζ'_m (resp. ζ'_ℓ) be a primitive m-th (resp. ℓ-th) root of unity. Then as $\zeta_m = \zeta_{m\ell}^\ell = (\zeta'_m)^\ell$, we see that $(\zeta'_m)^{\mathrm{Frob}_\ell} = \zeta_m$.

Then we compute the norm

$$\begin{aligned} \mathrm{Nm}_{\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m)}(1-\zeta_{m\ell}) &= \prod_{i=1}^{\ell-1}(1-\zeta'_m(\zeta'_\ell)^i) \\ &= \prod_{i=1}^{\ell-1}(\zeta'_\ell)^i \prod_{i=1}^{\ell-1}((\zeta'_\ell)^{-i}-\zeta'_m) \\ &= (\zeta'_\ell)^{\ell(\ell-1)/2}\prod_{i=1}^{\ell-1}((\zeta'_\ell)^i-\zeta'_m) \\ &= \underbrace{(\zeta'_\ell)^{\ell(\ell-1)/2}(-1)^{\ell-1}}_{(\dagger)}\underbrace{\prod_{i=1}^{\ell-1}(\zeta'_m-(\zeta'_\ell)^i)}_{(\star)}. \end{aligned}$$

Let $\Phi_n(X) \in \mathbb{Z}[X]$ be the n-th cyclotomic polynomial, then we know

$$\Phi_\ell(X) = \prod_{i=1}^{\ell-1}(X-(\zeta'_\ell)^i) = X^{\ell-1}+X^{\ell-2}+\cdots+1 = \frac{1-X^\ell}{1-X}.$$

Then

$$(\star) = \Phi_\ell(\zeta'_m) = \begin{cases} \ell, & m=1, \\ \dfrac{1-(\zeta'_m)^\ell}{1-\zeta'_m} = \dfrac{1-\zeta_m}{1-\zeta_m^{\mathrm{Frob}_\ell^{-1}}} = (1-\zeta_m)^{1-\mathrm{Frob}_\ell^{-1}}, & m>1. \end{cases}$$

Moreover, one checks immediately (by considering whether $\ell=2$ or ℓ being an *odd* prime) that $(\dagger)=1$. So we have finished up this case.

The remaining case that $\ell \mid m$ is easier. One note that

$$\prod_{i=1}^{\ell}(1-\zeta_{m\ell}\zeta_\ell^i) = 1-\zeta_m$$

---

one checks that

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m)}(\zeta_{m\ell}-1) = \begin{cases} \zeta_m-1, & \ell \mid m \text{ and } \ell \neq 2 \\ 1-\zeta_m, & \ell \mid m \text{ and } \ell = 2 \\ (\zeta_m-1)^{1-\mathrm{Frob}_\ell^{-1}}, & \ell \nmid m, m>1 \text{ and } \ell \neq 2 \\ -(\zeta_m-1)^{1-\mathrm{Frob}_\ell^{-1}}, & \ell \nmid m, m>1 \text{ and } \ell = 2 \\ (-1)^{\ell-1}\ell, & m=1. \end{cases}$$

So to avoid messy discussions on the paticular case $\ell=2$, we made a sign adjustment. Accordingly, we made a sign change in Definition 3.6.

always holds no mattter $\ell \mid m$ or not. When $\ell \mid m$, then the left-hand side runs over the conjugates of $1-\zeta_{m\ell}$ under $\mathrm{Gal}(\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m))$, so the product equals the norm. □

Using Lemma 2.5, one can verify that (2.6) holds indeed. Hence we obtain an Euler system for $(\mathbb{Z}_p(1), \mathcal{K}=\mathbb{Q}^{\mathrm{ab}}, \mathcal{N}=p\mathbb{Z})$. We call it the **Euler system of cyclotomic units** and denote it by $\mathbf{c}_{\mathrm{cyc}}$.

The twist of the Euler system of cyclotomic units. — We now further assume that the character $\chi : G_{\mathbb{Q}} \to \mathcal{O}^\times$ is even and nontrivial of conductor f. Under this assumption, we take the field L cut out by χ as $\mathbb{Q}(\zeta_f)^+$. Then $\mathbf{c}_{\mathrm{cyc}}$ gives rise (by Proposition 2.3) to a twisted Euler system $\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}}$ for $(\mathbb{Z}_p(1)\otimes\chi^{-1}, \mathbb{Q}^{\mathrm{ab}}, pf)$.

Moreover, using Proposition 2.4 with $F=K=\mathbb{Q}$, $L=L'=\mathbb{Q}(\zeta_f)^+$, we see that the image of the bottom element $(\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}})_{\mathbb{Q}}$ in $(L^\times)^\chi$ under (1.5) is

$$\begin{aligned}\prod_{\delta\in\mathrm{Gal}(\mathbb{Q}(\zeta_f)^+/\mathbb{Q})} (\delta(\mathbf{c}_{\mathrm{cyc}})_{\mathbb{Q}(\zeta_f)^+})^{\chi^{-1}(\delta)} &= \prod_{\delta\in\mathrm{Gal}(\mathbb{Q}(\zeta_f)^+/\mathbb{Q})} (\delta\,\mathrm{Nm}_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f)^+}((\mathbf{c}_{\mathrm{cyc}})_{\mathbb{Q}(\zeta_f)}))^{\chi^{-1}(\delta)}\\ &= \prod_{\delta\in\mathrm{Gal}(\mathbb{Q}(\zeta_f)^+/\mathbb{Q})} (\delta\,\mathrm{Nm}_{\mathbb{Q}(\zeta_{pf})/\mathbb{Q}(\zeta_f)^+}(\zeta_{pf}-1))^{\chi^{-1}(\delta)}\\ &= \prod_{\delta\in\mathrm{Gal}(\mathbb{Q}(\zeta_{pf})/\mathbb{Q})} (\zeta_{pf}^{\delta}-1)^{\chi^{-1}(\delta)}.\end{aligned}$$

This is again very explicit.

2.2. Derived cohomology classes. — Keep the notation as in the begining of this section. We further let $K(\mathbf{1})$ denote the maximal p-extension of K inside the Hilbert class field of K. Then for any prime $\mathfrak{q}$ of K, class field theory shows that $K(\mathfrak{q})/K(\mathbf{1})$ is unramified outside $\mathfrak{q}$, totally ramified above $\mathfrak{q}$, and cyclic with Galois group canonically isomorphic to the maximal p-quotient of $(\mathcal{O}_K/\mathfrak{q})^\times/(\mathcal{O}_K^\times \pmod{\mathfrak{q}})$. Let $\Gamma_{\mathfrak{q}} = \mathrm{Gal}(K(\mathfrak{q})/K(\mathbf{1}))$.

2.2.1. *Kolyvagin primes.* — Recall we used $\mathcal{N}$ to denote an ideal of $\mathcal{O}_K$ divisible by p and all primes where T is ramified. Define

$$\mathcal{R} := \mathcal{R}(\mathcal{N}) = \{\text{square-free products of primes } \mathfrak{q} \text{ of } K \text{ such that } \mathfrak{q}\nmid\mathcal{N}\}.$$

For any $\mathfrak{r}=\mathfrak{q}_1\cdots\mathfrak{q}_k\in\mathcal{R}$, we define $K(\mathfrak{r})$ to be the compositum $K(\mathfrak{r})=K(\mathfrak{q}_1)\cdots K(\mathfrak{q}_k)$ and we define $\Gamma_{\mathfrak{r}} = \mathrm{Gal}(K(\mathfrak{r})/K(\mathbf{1}))$. Ramification considerations show that the fields $K(\mathfrak{q})$ are linearly disjoint over $K(1)$, so there is a natural isomorphism

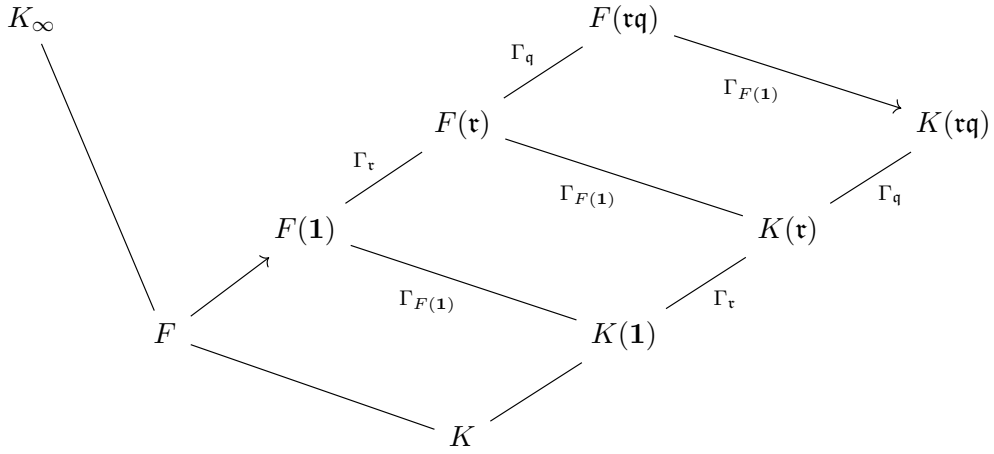
$$\Gamma_{\mathfrak{r}} \cong \prod_{i=1}^{k} \Gamma_{\mathfrak{q}_i},$$

where $\Gamma_{\mathfrak{q}_i}$ is identified with the inertia group of $\mathfrak{q}_i$ in $\Gamma_{\mathfrak{r}}$. For $\mathfrak{s}\mid\mathfrak{r}$, this allows us to view $\Gamma_{\mathfrak{s}}$ as a subgroup of $\Gamma_{\mathfrak{r}}$, as well as a quotient.

Suppose $K\subseteq_{\mathrm{f}} F\subseteq K_\infty$, where K_∞ is a $\mathbb{Z}_p^d$-extension of K with no finite primes that splits completely in K_∞. We define $F(\mathfrak{r})=FK(\mathfrak{r})$ for $\mathfrak{r}\in\mathcal{R}$ or $\mathfrak{r}=\mathbf{1}$.[(9)] By ramification

[(9)] Note that $F(\mathfrak{r})$ is defined to be the compositum of F and $K(\mathfrak{r})$, and in general not the maximal p-extension of F inside the ray class field $F[\mathfrak{r}]$.

considerations again, we see that $\mathrm{Gal}(F(\mathfrak{r})/F(\mathbf{1})) \cong \Gamma_{\mathfrak{r}}$. Let $\Gamma_{F(\mathfrak{r})} = \mathrm{Gal}(F(\mathfrak{r})/K(\mathbf{1}))$. We illustrate these fields and their Galois groups as follows.



Definition 2.6. — Suppose $K \subseteq_{\mathrm{f}} F \subseteq K_\infty$ and $M \in \mathcal{O}$ is nonzero. We define $\mathcal{R}_{F,M}$ to be the set of all $\mathfrak{r} \in \mathcal{R}$ such that for every prime $\mathfrak{q}$ dividing $\mathfrak{r}$,

- $M \mid [K(\mathfrak{q}) : K(\mathbf{1})]$,
- $M \mid P(\mathrm{Frob}_{\mathfrak{q}}^{-1} | T^*, 1)$,
- $\mathfrak{q}$ splits completely in $FK(\mathbf{1})/K$.

We refer to those primes in $\mathcal{R}_{F,M}$ as **Kolyvagin primes**.

Example 2.7 **(Classical case).** — In the classical case where $K = \mathbb{Q}, T = \mathbb{Z}_p(1)$ and the Euler system of cyclotomic units $\mathbf{c}$ of $(\mathbb{Z}_p(1), \mathbb{Q}^{\mathrm{ab}}, 2p)$,

$$\mathcal{R} = \{\text{square-free products of primes } q \text{ of } \mathbb{Q} \text{ such that } q \nmid 2p\}.$$

Then a number r lies in $\mathcal{R}_{F,M}$ means that $r \in \mathcal{R}$ and for any prime divisor q of r,

- $M \mid [\mathbb{Q}(q) : \mathbb{Q}]$, where $\mathbb{Q}(q)$ is the maximal p-subextension of $\mathbb{Q}(\zeta_q)^+/\mathbb{Q}$.
- q splits completely in $F/\mathbb{Q}$.

Here we note that $P(\mathrm{Frob}_q^{-1} | T^*, 1) = 0$, so the second condition in Definition 2.6 holds trivially. Moreover, suppose M is a power of p, then the first condition above is equivalent to that $M \mid (q-1)$.

2.2.2. *Kolyvagin derivatives*. — Let $\mathbf{c} = (\mathbf{c}_F)_F$ be an Euler system for $(T, \mathcal{K}, \mathcal{N})$. The natural projection $T \to W_M$ induces a natural map

$$\pi_M : H^1(F(\mathfrak{r}), T) \to H^1(F(\mathfrak{r}), W_M).$$

We can push the cohomology class $\mathbf{c}_{F(\mathfrak{r})} \in H^1(F(\mathfrak{r}), T)$ forward to $\pi_{M,*}(\mathbf{c}_{F(\mathfrak{r})}) \in H^1(F(\mathfrak{r}), W_M)$. Recall the inflation-restriction exact sequence

$$0 \to H^1(F(\mathfrak{r})/F, W_M^{G_{F(\mathfrak{r})}}) \to H^1(F, W_M) \to H^1(F(\mathfrak{r}), W_M)^{\mathrm{Gal}(F(\mathfrak{r})/F)} \xrightarrow{\mathrm{tg}} H^2(F(\mathfrak{r})/F, W_M^{G_{F(\mathfrak{r})}}).$$

So we have to torture the cohomology class $\pi_{M,*}(\mathbf{c}_{F(\mathfrak{r})})$ by applying an operator $\mathbb{D}_{F,\mathfrak{r}} \in \mathbb{Z}[\mathrm{Gal}(F(\mathfrak{r})/F)]$ arising from the *Kolyvagin operator*, so that

(i) $\mathbb{D}_{F,\mathfrak{r}}(\pi_{M,*}(\mathbf{c}_{F(\mathfrak{r})}))$ is $\mathrm{Gal}(F(\mathfrak{r})/F)$-invariance, and
(ii) its image under the transgression map tg is zero.

We fix a generator ξ of $\varprojlim_n \boldsymbol{\mu}_{p^n}$, and for every prime $\mathfrak{q}$ of K not dividing p, we fix a prime $\mathfrak{Q}$ of $\overline{K}$ above $\mathfrak{q}$. We will fix a generator of $\sigma_\mathfrak{q}$.

Let $p^e = |\Gamma_\mathfrak{q}| = [K(\mathfrak{q}) : K(\mathbf{1})]$ and let $I_\mathfrak{Q}$ denote the inertia group of $\mathfrak{Q}$ in G_K.

- The inertia gruop $I_\mathfrak{Q}$ has a unique cyclic quotient of order M that is canonically isomorphic to $\boldsymbol{\mu}_{p^e}$ by Lemma 1.9. The chosen generator ξ then gives us a generator $\zeta_\mathfrak{q}$ of $\boldsymbol{\mu}_{p^e}$. It lifts to $\xi_\mathfrak{q} \in I_\mathfrak{Q}$.
- Note that $\Gamma_\mathfrak{q}$ itself is a cyclic quotient of $I_\mathfrak{Q}$, the element $\xi_\mathfrak{q} \in I_\mathfrak{Q}$ gives a generator $\sigma_\mathfrak{q}$ of $\Gamma_\mathfrak{q}$.

***Definition 2.8* (Kolyvagin derivative operator). —** We define for any prime $\mathfrak{q}$ not dividing p,

$$\mathbb{D}_\mathfrak{q} = \sum_{i=0}^{|\Gamma_\mathfrak{q}|-1} i\sigma_\mathfrak{q}^i \in \mathbb{Z}[\Gamma_\mathfrak{q}].$$

If $\mathfrak{r} = \mathfrak{q}_1 \cdots \mathfrak{q}_k \in \mathcal{R}$, we define

$$\mathbb{D}_\mathfrak{r} = \prod_{\mathfrak{q}|\mathfrak{r}} \mathbb{D}_\mathfrak{q} \in \mathbb{Z}[\Gamma_\mathfrak{r}],$$

where for $\mathfrak{q} \mid \mathfrak{r}$, we view $\mathbb{D}_q \in \mathbb{Z}[\Gamma_\mathfrak{r}]$.

Recall the definition of $\Gamma_\mathfrak{q}$, naively speaking, Kolyvagin derivative operators takes cohomology classes to those that are invariant under $\mathrm{Gal}(F(\mathfrak{r})/F(\mathbf{1}))$. To further go back to F, we define an extra **norm operator** $\mathbb{N}_{F(\mathbf{1})/F} \in \mathbb{Z}[G_F]$ whose image under restriction to $F(\mathbf{1})$ is the norm element $\sum_{\gamma \in \mathrm{Gal}(F(\mathfrak{r})/F(\mathbf{1}))} \gamma \in \mathbb{Z}[\mathrm{Gal}(F(\mathbf{1})/F)]$. [(10)]

We start with an easy telescoping property. This is crucial for the construction of the derivative classes.

***Proposition 2.9*. —** *We have $(\sigma_\mathfrak{q} - 1)\mathbb{D}_\mathfrak{q} = |\Gamma_\mathfrak{q}| - N_\mathfrak{q}$, where $N_\mathfrak{q} \in \mathbb{Z}[\Gamma_\mathfrak{q}]$ is the norm element of $\Gamma_\mathfrak{q}$.*

Proof. — We directly compute

$$\begin{aligned}
(\sigma_\mathfrak{q} - 1)\mathbb{D}_\mathfrak{q} &= \sum_{i=0}^{|\Gamma_\mathfrak{q}|-1} i\sigma_\mathfrak{q}^{i+1} - \sum_{i=0}^{|\Gamma_\mathfrak{q}|-1} i\sigma_\mathfrak{q}^i \\
&= \sum_{j=1}^{|\Gamma_\mathfrak{q}|} (j-1)\sigma_\mathfrak{q}^j - \sum_{j=1}^{|\Gamma_\mathfrak{q}|-1} j\sigma_\mathfrak{q}^j \\
&= -\sum_{j=1}^{|\Gamma_\mathfrak{q}|-1} \sigma_\mathfrak{q}^j + |\Gamma_\mathfrak{q}| - 1 \\
&= |\Gamma_\mathfrak{q}| - N_\mathfrak{q}.
\end{aligned}$$

Here the last equality follows from that the norm element $N_\mathfrak{q} = 1 + \sigma_\mathfrak{q} + \cdots + \sigma_\mathfrak{q}^{|\Gamma_\mathfrak{q}|-1}$. □

With this telescoping property in hand, we can prove the following proposition.

[(10)] The operator $\mathbb{D}_{F,\mathfrak{r}} \in \mathbb{Z}[\mathrm{Gal}(F(\mathfrak{r})/F)]$ introduced at the beginning of this subsubsection is the composition $\mathbb{N}_{F(\mathbf{1})/F} \circ \mathbb{D}_\mathfrak{r}$.

Proposition 2.10. — *Suppose $M \in \mathcal{O}$ is nonzero, $K \subseteq_{\mathrm{f}} F \subseteq K_\infty$ and $\mathfrak{r} \in \mathcal{R}_{F,M}$. Then the cohomology class $\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ lies in $H^1(F(\mathfrak{r}), W_M)^{\Gamma_{\mathfrak{r}}}$. As a result, the cohomology class $\mathbb{N}_{F(\mathbf{1})/F}\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ is invariant under the $\mathrm{Gal}(F(\mathfrak{r})/F)$-action.*

Proof. — We will show that

$$(\sigma - 1)\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})} \in MH^1(F(\mathfrak{r}), T), \text{ for every } \sigma \in \mathrm{Gal}(F(\mathfrak{r})/F(\mathbf{1})),$$

and then the proposition follows. The proof is by induction on the number of primes dividing $\mathfrak{r}$. If $\mathfrak{r} = 1$, there is nothing to prove. In general, say $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$ for $\mathfrak{s}, \mathfrak{q} \in \mathcal{R}_{F,M}$ with $\mathfrak{q}$ being a prime ideal. We assume by assumption that

$$\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{s})} \in H^1(F(\mathfrak{s}), W_M)^{\mathrm{Gal}(F(\mathfrak{s})/F(\mathbf{1}))}.$$

We regard it as in $H^1(F(\mathfrak{r}), W_M)^{\mathrm{Gal}(F(\mathfrak{r})/F(\mathbf{1}))}$ by the natural restriction. Since the $\sigma_{\mathfrak{q}}$'s generate $\Gamma_{\mathfrak{r}}$, it suffices to prove

$$(\sigma_{\mathfrak{q}} - 1)\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})} = 0 \in H^1(F(\mathfrak{r}), W_M) = H^1(F(\mathfrak{r}), T/MT).$$

We compute

$$\begin{aligned}(\sigma_{\mathfrak{q}} - 1)\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})} &= (\sigma_{\mathfrak{q}} - 1)\mathbb{D}_{\mathfrak{q}}\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{r})} \\ &= (|\Gamma_{\mathfrak{q}}| - N_{\mathfrak{q}})\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{r})} \\ &= |\Gamma_{\mathfrak{q}}|\,\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{r})} - \mathbb{D}_{\mathfrak{s}}N_{\mathfrak{q}}\mathbf{c}_{F(\mathfrak{r})}.\end{aligned}$$

Here the second equality follows from the telescoping property (Proposition 2.9) and the third equality holds by commuting $\mathbb{D}_{\mathfrak{s}}$ and $N_{\mathfrak{q}}$.[(11)] Then invoking the norm compatibility condition of the Euler system $\mathbf{c}$, i.e.

$$\mathrm{cor}_{F(\mathfrak{r})/F(\mathfrak{s})}\,\mathbf{c}_{F(\mathfrak{r})} = P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbf{c}_{F(\mathfrak{s})},$$

we see that

$$N_{\mathfrak{q}}\mathbf{c}_{F(\mathfrak{r})} = P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbf{c}_{F(\mathfrak{s})}$$

since the composition

$$H^1(F(\mathfrak{r}), T) \xrightarrow{\mathrm{cor}_{F(\mathfrak{r})/F(\mathfrak{s})}} H^1(F(\mathfrak{s}), T) \xrightarrow{\mathrm{res}_{F(\mathfrak{r})/F(\mathfrak{s})}} H^1(F(\mathfrak{r}), T)$$

is the multiplication by the norm element $N_{\mathfrak{q}}$ (see, for example, [**NSW08**, (1.5.7)]). Combine what we have obtained together,

$$(\sigma_{\mathfrak{q}} - 1)\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})} = |\Gamma_{\mathfrak{q}}|\,\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{r})} - P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{s})} \in H^1(F(\mathfrak{r}), T).$$

Now we pass to the cohomology classes of coefficient W_M by modding M. By the induction hypothesis, we see that

$$P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{s})} \equiv P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; 1)\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{s})}, \pmod{(\mathrm{Fr}_{\mathfrak{q}} - 1)\mathbb{D}_{\mathfrak{s}}\mathbf{c}_{F(\mathfrak{s})}}.$$

Since $\mathfrak{q} \in \mathcal{R}_{F,M}$, $M \mid |\Gamma_{\mathfrak{q}}|$ and $M \mid P(\mathrm{Frob}_{\mathfrak{q}}^{-1}\,|T^*; 1)$, the result follows. □

[(11)] Note that both $\mathbb{D}_{\mathfrak{s}}$ and $N_{\mathfrak{q}}$ are elements of the group algebra $\mathbb{Z}[\Gamma_{\mathfrak{q}}]$ and $\Gamma_{\mathfrak{q}}$ is an abelian group.

To further simplify our discussion, we pose the assumption that

$$W^{G_{F(\mathfrak{r})}} = 0, \quad \mathfrak{r} \in \mathcal{R}_{F,M}. \tag{null}$$

Then certainly $H^i(F(\mathfrak{r})/F, W_M^{G_{F(\mathfrak{r})}}) = 0$ for all $i \geq 0$. From the inflation-restriction exact sequence, this implies

$$\mathrm{res}_{F(\mathfrak{r})/F} : H^1(F, W_M) \to H^1(F(\mathfrak{r}), W_M)^{\mathrm{Gal}(F(\mathfrak{r})/F)}$$

is an isomorphism.

Definition 2.11. — Keep the notations and assumption (null), we define $\kappa_{[F,\mathfrak{r},M]} \in H^1(F, W_M)$ to be the inverse image of $\mathbb{N}_{F(\mathbf{1})/F}\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ via the restriction map $\mathrm{res}_{F(\mathfrak{r})/F}$.

When (null) is not satisfied, then the map $\mathrm{res}_{F(\mathfrak{r})/F}$ may not be an isomorphism. Then by using the preparations in [**Rub00**, Section 4.2-4.3], $\mathbb{N}_{F(\mathbf{1})/F}\mathbb{D}_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ will always has a canonical inverse image under $\mathrm{res}_{F(\mathfrak{r})/F}$. That inverse image will be our class $\kappa_{[F,\mathfrak{r},M]}$. Readers can find these details in [**Rub00**, Section 4.4].

We remark that the assumption (null) is practible, since it is satisfied for the classical case (Section 1.4.2). Indeed, $W = \boldsymbol{\mu}_{p^\infty}$ and hence $W^{G_{F(\mathfrak{r})}} = \boldsymbol{\mu}_{p^\infty}(F(\mathfrak{r}))$, i.e. all the p-power root of unity in $F(\mathfrak{r})$. However, being a p-extension of a totally real field $\mathbb{Q}$, the $F(\mathfrak{r})$ is totally real as well, hence the only p-power root of unity in $F(\mathfrak{r})$ is 1. Note that here we seriously used that p is an *odd* prime.

2.3. Local properties of the derivative classes. — In this section, the main two goals are [(12)]

(i) Show that $\kappa_{[F,\mathfrak{r},M]}$ defines a class in $\mathrm{Sel}^{\Sigma}(F, W_M)$ for any finite set of places of K containing $\Sigma_{p\mathfrak{r}}$, i.e. the set of primes of K dividing $p\mathfrak{r}$.
(ii) Calculate $\mathrm{loc}^{\mathrm{s}}_{\Sigma,\Sigma_0}(\kappa_{[F,\mathfrak{r},M]})$ for any finite set of primes $\Sigma_{p\mathfrak{r}} \subseteq \Sigma_0 \subseteq \Sigma$.

For goal (i), we formulate it into the following theorem.

Theorem 2.12. — *Suppose that $M \in \mathcal{O}$ is nonzero, that $K \subset_{\mathrm{f}} F \subseteq K_\infty$, and that $\mathfrak{r} \in \mathcal{R}_{F,M}$. For every place w of F not dividing $p\mathfrak{r}$,*

$$(\kappa_{F,\mathfrak{r},M})_w \in H^1_{\mathrm{f}}(F_w, W_M).$$

In other words, $\kappa_{[F,\mathfrak{r},M]} \in \mathrm{Sel}^{\Sigma_{p\mathfrak{r}}}(F, W_M)$.

Unfortunately, the proof is quite complicated, so we only show it in the classical case. The general proof can be found in [**Rub00**, Section 4.6].

Proof in the classical case. — In the classical case (Section 1.4.2), we view $\kappa_{[F,\mathfrak{r},M]} \in H^1(F, \boldsymbol{\mu}_{p^f}) = F^\times/(F^\times)^{p^f}$. Hence it suffices to show that if $w \nmid p\mathfrak{r}$, then $p^f \mid \mathrm{ord}_w(\kappa_{[F,\mathfrak{r},M]})$. It follows immediately from the elementary claims:

(a) $(\mathbf{c}_{\mathrm{cyc}})_{\mathbb{Q}(\zeta_r)}$ is a global unit unless $r = 1$.
(b) $(\mathbf{c}_{\mathrm{cyc}})_{\mathbb{Q}}$ is a unit in $\mathcal{O}_{F_w}$ for $w \nmid p\mathfrak{r}$.

[(12)] The goal (i) is actually asking about the local behavior of $\kappa_{[F,\mathfrak{r},M]}$ at primes not dividing $p\mathfrak{r}$, being the main topic of [**Rub00**, Section 4.6]. The goal (ii) is essentially inverstigating the local behaviors of $\kappa_{[F,\mathfrak{r},M]}$ at primes not dividing $p\mathfrak{r}$, being the main topic of [**Rub00**, Section 4.7], which turn out to be more challenging.

The proof of these claims are left to the readers. □

Our main focus in this subsection will be on the goal (ii).

2.3.1. *The finite-singular comparision map.* — In this section, we define the finite-singular comparision map, which built a bridge between the derived cohomology classes $\kappa_{[F,\mathfrak{r}\mathfrak{q},M]}$ and $\kappa_{[F,\mathfrak{r},M]}$. Before that, the following proposition is useful. The proof is not hard.

Proposition 2.13 **([Rub00, Lemma 4.1.2]).** — *Suppose $\mathfrak{q} \in \mathcal{R}_{K,M}$ with $\mathbf{N}(\mathfrak{q})$ be its norm and $M \in \mathcal{O}$ is nonzero.*

(i) *The prime $\mathfrak{q}$ splits in $K(\boldsymbol{\mu}_{\overline{M}}, (\mathcal{O}_K^\times)^{1/\overline{M}})$.*
(ii) $P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; \mathbf{N}(\mathfrak{q})\,\mathrm{Frob}_\mathfrak{q}^{-1})$ *annihilates* T.
(iii) $P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; X) \equiv \det(1 - \mathrm{Frob}_\mathfrak{q} X|W_M) \pmod M$.
(iv) $P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; \mathrm{Frob}_\mathfrak{q}^{-1})$ *annihilates* W_M.

Proposition 2.14. — *Suppose $M \in \mathcal{O}$ is nonzero and $\mathfrak{q} \in \mathcal{R}_{K,M}$ is prime. Then there is a unique $Q_\mathfrak{q}(X) \in (\mathcal{O}/M\mathcal{O})[X]$ such that*

$$P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; X) \equiv (X-1)Q_\mathfrak{q}(X) \pmod M.$$

Proof. — The proof is by brute force. We define [(13)]

$$Q_\mathfrak{q}(X) = \frac{P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; X) - P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; 1)}{X-1}.$$

Since $\mathfrak{q} \in \mathcal{R}_{K,M}$, we know that $M \mid P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; 1)$, so this polynomial has the desired property. The uniqueness comes from the fact that $X - 1$ is not a zero divisor in $(\mathcal{O}/M\mathcal{O})[X]$. □

Example 2.15 **(Classical case).** — Recall that in the classical case, $P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; X) = 1 - X$, hence $Q_\mathfrak{q}(X) = -1$ by the uniqueness of $Q_\mathfrak{q}(X)$.

Finally we can define the finite-singlar comparision map. For any prime $\mathfrak{q} \in \mathcal{R}_{K,M}$, so in particular $\mathfrak{q}$ does not divide p, we have the explicit isomorphisms $\alpha_\mathfrak{q}$ and $\beta_\mathfrak{q}$ given in Proposition 1.10 as

$$\alpha_\mathfrak{q} : H^1_\mathrm{s}(K_\mathfrak{q}, W_M) \xrightarrow{\sim} W_M^{\mathrm{Frob}_\mathfrak{q}=1}, \quad \beta_\mathfrak{q} : H^1_\mathrm{f}(K_\mathfrak{q}, W_M) \xrightarrow{\sim} W_M/(\mathrm{Frob}_\mathfrak{q} - 1)W_M.$$

If $\mathfrak{q} \in \mathcal{R}_{K,M}$, then $P(\mathrm{Frob}_\mathfrak{q}^{-1}|T^*; \mathrm{Frob}_\mathfrak{q}^{-1})$ annihilates W_M by Proposition 2.13. Thus the polynomial $Q_\mathfrak{q}$ in Proposition 2.14 induces a map

$$Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1}) : W_M/(\mathrm{Frob}_\mathfrak{q} - 1)W_M \to W_M^{\mathrm{Frob}_\mathfrak{q}=1}.$$

[(13)] Note that $Q_\mathfrak{q}(X) \in \mathcal{O}[X]$ since for any polynomial $f(X) \in \mathcal{O}[X]$, $X - 1$ divides $f(X) - f(1)$.

Then the **finite-singular comparison map** is defined via the dash arrow in the following diagram to make it commute

$$\begin{array}{ccccc} c & & H^1_{\mathrm{f}}(K_{\mathfrak{q}}, W_M) & \overset{\phi^{\mathrm{fs}}_{\mathfrak{q}}}{\dashrightarrow} & H^1_{\mathrm{s}}(K_{\mathfrak{q}}, W_M) & & c \\ \downarrow & & \downarrow{\scriptstyle \beta_{\mathfrak{q}}} & & \downarrow{\scriptstyle \alpha_{\mathfrak{q}}} & & \downarrow \\ c(\mathrm{Frob}_{\mathfrak{q}}) & & W_M/(\mathrm{Frob}_{\mathfrak{q}}-1)W_M & \xrightarrow[Q_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}}^{-1})]{} & W_M^{\mathrm{Frob}_{\mathfrak{q}}=1} & & c(\overline{\sigma}_{\mathfrak{q}}) \end{array} . \tag{2.7}$$

In other words, $\phi^{\mathrm{fs}}_{\mathfrak{q}} := \alpha_{\mathfrak{q}}^{-1} \circ Q_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}}^{-1}) \circ \beta_{\mathfrak{q}}$. Recall that the choices of $\sigma_{\mathfrak{q}} \in \Gamma_{\mathfrak{q}}$ and $\mathrm{Frob}_{\mathfrak{q}}$ depend on the choice of a prime $\mathfrak{Q}$ of $\overline{K}$ above $\mathfrak{q}$. We use the same choice for both and further fix an element $\overline{\sigma}_{\mathfrak{q}}$ in the inertia group of $\mathfrak{Q}$ extending $\sigma_{\mathfrak{q}} \in \Gamma_{\mathfrak{q}}$.

2.3.2. *Kolyvagin property of the derived cohomology classes.* —

Theorem 2.16. — *Suppose $M \in \mathcal{O}$ is nonzero, $K \subseteq_{\mathrm{f}} F \subseteq K_\infty$, $\mathfrak{q}$ is a prime of K and $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$. Let $\phi^{\mathrm{fs}}_{\mathfrak{q}} : H^1_{\mathrm{f}}(K_{\mathfrak{q}}, W_M) \to H^1_{\mathrm{s}}(K_{\mathfrak{q}}, W_M)$ be the finite-singular comparison map, and $(\kappa_{[F,\mathfrak{r}\mathfrak{q},M]})^s_{\mathfrak{q}}$ denotes the image of $\kappa_{F,\mathfrak{r}\mathfrak{q},M}$ in $H^1_{\mathrm{s}}(F_{\mathfrak{Q}}, W_M)$, then*

$$(\kappa_{[F,\mathfrak{r}\mathfrak{q},M]})^s_{\mathfrak{q}} = \phi^{\mathrm{fs}}_{\mathfrak{q}}(\kappa_{[F,\mathfrak{r},M]}).$$

This main theorem tells us that the singular part of $\kappa_{[F,\mathfrak{r}\mathfrak{q},M]}$ at $\mathfrak{q}$ is controlled by the finite localization of $\kappa_{[F,\mathfrak{r},M]}$ at $\mathfrak{q}$.

Suppose B is an $\mathcal{O}$-module. Recall that $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$. If $b \in B$, we define

$$\mathrm{order}(b, B) = \inf\{n \geq 0 : \mathfrak{p}^n b = 0\} \leq \infty.$$

Corollary 2.17. — *Keeps the assumptions in the Theorem 2.16, suppose further that $W_M/(\mathrm{Frob}_{\mathfrak{q}} - 1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$. Then*

$$\mathrm{order}((\kappa_{[F,\mathfrak{r}\mathfrak{q},M]})^s_{\mathfrak{q}}, H^1_{\mathrm{s}}(K_{\mathfrak{q}}, W_M)) = \mathrm{order}((\kappa_{[F,\mathfrak{r},M]})_{\mathfrak{q}}, H^1_{\mathrm{f}}(K_{\mathfrak{q}}, W_M)).$$

To prove this corollary, the following lemma will be used in determining when the map $Q_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}}^{-1})$ is an isomorphism.

Lemma 2.18 **([Rub00**, Corollary A.2.7]**).** — *Suppose*

(i) *τ is an $\mathcal{O}$-linear automorphism of W_M such that $W_M/(\tau - 1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$,*
(ii) *$Q(X) \in (\mathcal{O}/M\mathcal{O})[X]$ is such that $(1 - X)Q(X) = \det(1 - \tau^{-1}X|W_M)$.*

Then the map

$$Q(\tau) : W_M/(\tau - 1)W_M \to W_M^{\tau=1}$$

is an isomorphism.

Proof of Corollary 2.17. — The result follows from Theorem 2.16 once we prove that the map $\phi^{\mathrm{fs}}_{\mathfrak{q}}$ is an isomorphism. The maps $\alpha_{\mathfrak{q}}$ and $\beta_{\mathfrak{q}}$ are both isomorphisms, and by Proposition 2.13(iii) and Lemma 2.18, we see $Q_{\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{q}}^{-1})$ is an isomorphism, by applying with $\tau = \mathrm{Frob}_{\mathfrak{q}}^{-1}$ and $Q(X) = Q_{\mathfrak{q}}(X)$ in Lemma 2.18. □

In the rest of this subsection, we shall give a rough proof of Theorem 2.16. From the diagram (2.7), the basic idea is to compute and compare the value of $\kappa_{[F,\mathfrak{r}\mathfrak{q},M]}$ (resp. $\kappa_{[F,\mathfrak{r},M]}$) on $\overline{\sigma}_\mathfrak{q}$ (resp. $\mathrm{Frob}_\mathfrak{q}$).

Naive proof of Theorem 2.16. — Naively from the description of Kummer maps, we have

$$\kappa_{[F,\mathfrak{r}\mathfrak{q},M]}(\overline{\sigma}_\mathfrak{q}) \approx \frac{\overline{\sigma}_q((\mathbb{D}_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M})}{(\mathbb{D}_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M}} = (\overline{\sigma}_\mathfrak{q}-1)((\mathbb{D}_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M}).$$

and

$$\kappa_{[F,\mathfrak{r},M]}(\mathrm{Frob}_\mathfrak{q}) \approx \frac{\mathrm{Frob}_q((\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M})}{(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M}} = (\mathrm{Frob}_\mathfrak{q}-1)(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M},$$

though we have not defined what a "M-th power root" of cohomology classes means. But this does little harm to the following calculations.

We compute

$$\begin{aligned} Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})(\mathrm{Frob}_\mathfrak{q}^{-1}-1)(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})(\mathrm{Frob}_\mathfrak{q}) &= P(\mathrm{Frob}_\mathfrak{q}^{-1}\,|T^*;\mathrm{Frob}_\mathfrak{q}^{-1})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})(\mathrm{Frob}_\mathfrak{q}) \\ &\equiv 0 \pmod{M}, \end{aligned} \tag{2.8}$$

where the first equality follows from the defining property of $Q_\mathfrak{q}$ and the second congruence follows froms Proposition 2.13(iii) that $P(\mathrm{Frob}_\mathfrak{q}^{-1}\,|T^*;\mathrm{Frob}_\mathfrak{q}^{-1})$ annihilates W_M.

Then modding M, we have

$$\begin{aligned} &Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})(\mathrm{Frob}_\mathfrak{q}) - \kappa_{[F,\mathfrak{r}\mathfrak{q},M]}(\overline{\sigma}_\mathfrak{q}) \\ &\quad\equiv Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})\,\mathrm{Frob}_\mathfrak{q}^{-1}(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})(\mathrm{Frob}_\mathfrak{q}) - \kappa_{[F,\mathfrak{r}\mathfrak{q},M]}(\overline{\sigma}_\mathfrak{q}) \\ &\quad\approx Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})\,\mathrm{Frob}_\mathfrak{q}^{-1}(\mathrm{Frob}_\mathfrak{q}-1)(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M} - (\overline{\sigma}_\mathfrak{q}-1)((\mathbb{D}_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M}) \\ &\quad= Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})(1-\mathrm{Frob}_\mathfrak{q}^{-1})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M} - ((\overline{\sigma}_\mathfrak{q}-1)\mathbb{D}_\mathfrak{q})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M} \\ &\quad= -P(\mathrm{Frob}_\mathfrak{q}^{-1}\,|T^*;\mathrm{Frob}_\mathfrak{q}^{-1})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})^{1/M} - |\Gamma_\mathfrak{q}|\,(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M} + (N_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})^{1/M}. \end{aligned}$$

Here the first congruence is from (2.8) and we used the telescoping property (Proposition 2.9) in the last equality.

Then by the observations that $N_\mathfrak{q}$ and $\mathbb{D}_\mathfrak{r}$ commute and the norm element $N_q = \mathrm{res}\circ\mathrm{cor}$, we get from the norm compatibility condition of the Euler system that

$$N_\mathfrak{q}\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} = \mathbb{D}_\mathfrak{r}N_\mathfrak{q}\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} = \mathbb{D}_\mathfrak{r}\,\mathrm{cor}_{F(\mathfrak{r}\mathfrak{q})/F(\mathfrak{r})}\,\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} = P(\mathrm{Frob}_\mathfrak{q}^{-1}\,|T^*;\mathrm{Frob}_\mathfrak{q}^{-1})\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})}.$$

Take it back to the above computations, since $M \mid |\Gamma_\mathfrak{q}| = [K(\mathfrak{q}):K]$, we see that

$$Q_\mathfrak{q}(\mathrm{Frob}_\mathfrak{q}^{-1})(\mathbb{D}_\mathfrak{r}\mathbf{c}_{F(\mathfrak{r})})(\mathrm{Frob}_\mathfrak{q}) = \kappa_{[F,\mathfrak{r}\mathfrak{q},M]}(\overline{\sigma}_\mathfrak{q}),$$

which "proves" Theorem 2.16. □

When we do have the Kummer maps, for example in our classical case, the proof is a strict one. Otherwise we need to clarify what we mean by taking M-th power root of cohomology classes. This is the point that makes the arguments in [**Rub00**, Chapter 4] quite complicated. Very roughly speaking, to imitate the Kummer map, it is defined in [**Rub00**, Definition 4.4.4] for every finite extension L over K, a G_K-module

$$\mathbb{W}_M = \mathrm{Ind}_{\{1\}}^{G_L}(W_M) = \mathrm{Maps}(G_K, W_M)$$

and use

$$0 \to W_M \to \mathbb{W}_M \to \mathbb{W}_M/W_M \to 0$$

to imitate the Kummer sequence. Indeed, taking the Galois cohomology, we obtain that

$$0 \to W_M^{G_L} \to \mathbb{W}_M^{G_L} \to (\mathbb{W}_M/W_M)^{G_L} \xrightarrow{\delta_L} H^1(L, W_M) \to 0,$$

once we note that due to Shapiro's lemma (see, for example, [NSW08, (1.6.4)]), $H^1(L, \mathbb{W}_M) = 0$. Then here δ_L is an imitation of the Kummer map. Readers can turn to [Rub00, Chapter 4] to see how this works.

3. Bounding Selmer Groups

We keep the notations in previous sections. Fix an Euler system $\mathbf{c}$ for $(T, \mathcal{K}, \mathcal{N})$ for some $\mathcal{K}$ and $\mathcal{N}$. If M is a power of p, we will write $\mathcal{R}_M := \mathcal{R}_{K,M}$ for short.

Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$ and let $\Bbbk = \mathcal{O}/\mathfrak{p}$ be the residue field. Let $N := K(\mathbf{1})(\boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty}) \subseteq \overline{K}$ and $\Omega := NK(W)$ where $K(W)$ denotes the smallest extension of K such that $G_{K(W)}$ acts trivially on W.

We will make use of the following hypothesis on the Galois representation T.

Hypothesis $\mathrm{Hyp}(K, T)$. There is an element $\tau \in \mathrm{Gal}(\overline{K}/N)$ such that $T/(\tau - 1)T$ is free of rank one over $\mathcal{O}$ and $T \otimes_{\mathcal{O}} \Bbbk$ is an irreducible $\Bbbk[G_K]$-module.

Then we state the main result on the upper bound of the Selmer groups.

Definition 3.1. — If $\mathbf{c}$ is an Euler system, we define the **index of divisibility** of $\mathbf{c}$ to be

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) := \sup\{n : \mathbf{c}_K \in \mathfrak{p}^n H^1(K, T) + H^1(K, T)_{\mathrm{tors}}\} \leq \infty.$$

In other words, $\mathfrak{p}^{\mathrm{ind}_{\mathcal{O}}(\mathbf{c})}$ the largest power of the maximal ideal $\mathfrak{p}$ by which $\mathbf{c}_K$ can be divided in $P(K, T) := H^1(K, T)/H^1(K, T)_{\mathrm{tors}}$.

We write $\mathrm{len}_{\mathcal{O}}(B)$ for the length of an $\mathcal{O}$-module B, so that $|B| = |\Bbbk|^{\mathrm{len}_{\mathcal{O}}(B)}$.

***Theorem 3.2* (Upper bound of Selmer groups).** — *Suppose that $p > 2$ and T satisfies* $\mathrm{Hyp}(K, T)$. *If $\mathbf{c}$ is an Euler system for T, then*

$$\mathrm{len}_{\mathcal{O}}(\mathrm{Sel}_{\Sigma_p}(K, W^*)) \leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + n_W + n_W^*,$$

where

$$n_W := \mathrm{len}_{\mathcal{O}}(H^1(\Omega/K, W) \cap \mathrm{Sel}^{\Sigma_p}(K, W)),$$

and

$$n_W^* := \mathrm{len}_{\mathcal{O}}(H^1(\Omega/K, W^*) \cap \mathrm{Sel}_{\Sigma_p}(K, W^*)).$$

A first thing to remark that is that the index $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is only related to the *bottom element* $\mathbf{c}_K$.

The rest of this section is devoted to prove Theorem 3.2 and introduce its application to class groups. Let Σ be a finite set of places of K. Consider the localization map

$$\mathrm{Sel}^{\Sigma \cup \Sigma_p}(K, W_M) \xrightarrow{\mathrm{loc}^{\mathrm{s}}_{\Sigma \cup \Sigma_p, \Sigma_p, W_M}} \bigoplus_{v \in \Sigma} H^1_{\mathrm{s}}(K_v, W_M) \twoheadrightarrow \mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma \cup \Sigma_p, \Sigma_p, W_M}).$$

To ease the notation, we write $\mathrm{loc}^{\mathrm{S}}_{\Sigma,W_M} := \mathrm{loc}^{\mathrm{S}}_{\Sigma\cup\Sigma_p,\Sigma_p,W_M}$ and write $\mathrm{loc}^{\mathrm{S}}_{\Sigma,W}$ in exactly the same way with W_M replaced by W.

3.1. At the bottom of the Euler system. — If $M \in \mathcal{O}$ is nonzero, we let $\iota_M : H^1(K,W_M) \to H^1(K,W)$ denote the map induced by the inclusion of W_M in W.

Proposition 3.3. — *Suppose M is a power of p and $\mathrm{ord}_{\mathfrak{p}} M \geq \mathrm{ind}_{\mathcal{O}}(\mathbf{c})$. Then*

$$\mathrm{order}(\iota_M(\kappa_{[1,M]}), H^1(K,W)) = \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

Proof. — We first note that $H^1(K,V) = H^1(K,T)\otimes_{\mathcal{O}}\Phi$. It follows essentially from [Rub00, Proposition B.2.4]. Then we consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \xrightarrow{\times M} & T & \longrightarrow & W_M & \longrightarrow & 0 \\ & & \mathrm{id}\Big\| & & \times M^{-1}\Big\downarrow & & \Big\downarrow\times M^{-1} & & \\ 0 & \longrightarrow & T & \longrightarrow & V & \longrightarrow & W & \longrightarrow & 0 \end{array}$$

and take the Galois cohomology $H^1(K,-)$, we get

$$\begin{array}{ccccc} H^1(K,T) & \xrightarrow{\times M} & H^1(K,T) & \longrightarrow & H^1(K,W_M) \\ \Big\| & & \phi_1:\times M^{-1}\Big\downarrow & & \Big\downarrow \\ H^1(K,T) & \xrightarrow[\phi_2]{} & H^1(K,V) & \xrightarrow[\phi_3]{} & H^1(K,W) \end{array}.$$

Gazing at the diagram, we observe that

- $\ker\phi_1 = H^1(K,T)_{\mathrm{tors}}$ by the previous observation that $H^1(K,V) = H^1(K,T)\otimes_{\mathcal{O}}\Phi$.
- $\ker(\phi_3) = \mathrm{im}(\phi_2) = \phi_1(M\cdot H^1(K,T))$.

So

$$\ker(\phi_3\circ\phi_1) = \{z\in H^1(K,T) : \phi_1(z)\in\ker\phi_3\} = MH^1(K,T) + H^1(K,T)_{\mathrm{tors}}.$$

Back to our situation, by the definition of the Kolyvagin derivative class $\kappa_{[1,M]}$, we see precisely

$$\iota_M(\kappa_{[1,M]}) = (\phi_3\circ\phi_1)\mathbf{c}_K.$$

So

$$\begin{aligned} \mathrm{order}(\iota_M(\kappa_{[1,M]}), H^1(K,W)) &= \min\{n\geq 0 : \mathfrak{p}^n\mathbf{c}_K\in\ker(\phi_3\circ\phi_1)\} \\ &= \mathrm{order}\left(\mathbf{c}_K, \frac{H^1(K,T)}{MH^1(K,T)+H^1(K,T)_{\mathrm{tors}}}\right) \\ &= \mathrm{order}(\mathbf{c}_K, P(K,T)/MP(K,T)), \end{aligned}$$

where $P(K,T) = H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$. Since $P(K,T)$ is a finitely generated [(14)] torsion free $\mathcal{O}$-module, it follows from the definition of $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ that

$$\mathrm{order}(\mathbf{c}_K, P(K,T)/MP(K,T)) = \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}), \tag{3.9}$$

which proves the proposition. □

[(14)] Here the finiteness follows from the finiteness of $H^1(K,T)$ over $\mathcal{O}$, i.e. [Rub00, Proposition B.2.7]. The finiteness is vital since we can then use the structure theorem for finitely generated $\mathcal{O}$-modules and $\mathcal{O}/M\mathcal{O}$-modules to deduce (3.9).

3.2. Chebotarev machine. — As we have skectched at the begining of this section, the most technical part is to choose a set of places Σ of K carefully so that the Kolyvagin derived cohomology classes $\kappa_{[\mathfrak{r},M]}$ has large image under $\mathrm{loc}^{\mathrm{s}}_{\Sigma\cup\Sigma_p,\Sigma_p}$. We shall see shortly that we have huge amount of such primes, provided essentially by Chebotarev density theorem.

Proposition 3.4 **([Rub00**, Lemma 5.2.3]**).** — *Fix a power M of p. Suppose C is a finite subset of $H^1(K,W_M^*)$ and let $k=|C|$. Then there exists a finite set $\Sigma=\{\mathfrak{q}_1,\dots,\mathfrak{q}_k\}$ of primes of K such that for $1\le i\le k$,*

(i) $\mathfrak{q}_i\in\mathcal{R}_M$,
(ii) $\mathrm{Frob}_{\mathfrak{q}_i}$ *is in the conjugacy class of* τ *in* $\mathrm{Gal}(K(W_M)/K)$,
(iii) *writing* $\mathfrak{r}_j=\prod_{t=1}^{j}\mathfrak{q}_t$ *and* $\mathfrak{r}_0=1$, *we have*

$$\mathrm{order}((\kappa_{[\mathfrak{r}_{i-1},M]})_{\mathfrak{q}_i},H^1_{\mathrm{f}}(K_{\mathfrak{q}_i},W_M))\ge\mathrm{order}(\mathrm{res}_{\Omega/K}(\kappa_{[\mathfrak{r}_{i-1},M]})),H^1(\Omega,W_M)),$$

(iv) $\{\eta\in C:\eta_{\mathfrak{q}}=0$ *for every* $\mathfrak{q}\in\Sigma\}\subseteq H^1(\Omega/K,W_M^*)$.

Besides the Chebotarev density theorem, another key observation is that orders of cohomology classes can be controlled by their values of representing cocycles on particular Galois group elements. This is the content of [**Rub00**, Lemma 5.2.1].

3.3. Bounding Selmer groups. —

Proposition 3.5. — *Suppose that $\mathfrak{m}=\mathfrak{p}^n$ is a nonzero ideal of $\mathcal{O}$, that $k\in\mathbb{Z}^+$, and M is a power of p such that*

$$\mathrm{ord}_{\mathfrak{p}}M\ge n+(k+1)n_W+\mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

[(15)] *Suppose further that $\Sigma=\{\mathfrak{q}_1,\dots,\mathfrak{q}_k\}\subseteq\mathcal{R}_M$ is a finite set of primes of K such that for $1\le i\le k$,*

(i) $\mathrm{Frob}_{\mathfrak{q}_i}$ *is in the conjugacy class of* τ *in* $\mathrm{Gal}(K(W_M)/K)$,
(ii) *writing* $\mathfrak{r}_j=\prod_{t=1}^{j}\mathfrak{q}_t$ *and* $\mathfrak{r}_0=1$, *we have*

$$\mathrm{order}((\kappa_{[\mathfrak{r}_{i-1},M]})_{\mathfrak{q}_i},H^1_{\mathrm{f}}(K_{\mathfrak{q}_i},W_M))\ge\mathrm{order}(\mathrm{res}_{\Omega/K}(\kappa_{[\mathfrak{r}_{i-1},M]})),H^1(\Omega,W_M)).$$

Then the map $\mathrm{loc}^{\mathrm{s}}_{\Sigma,W_{\mathfrak{m}}}$ satisfies

$$\mathrm{len}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma,W_{\mathfrak{m}}}))\le\mathrm{ind}_{\mathcal{O}}(\mathbf{c})+n_W.$$

The proof of this proposition is also a technical one. We prefer to give a proof under the mild additional hypothesis

$$W^{G_K}=0,\quad H^1(\Omega/K,W)=0,\tag{vanishing}$$

just as what Rubin did. For general proof, readers can turn to [**Rub00**, Section 5.2, pp.111-114].

[(15)] Note that since $\mathcal{O}$ is the ring of integer of a local number field Φ, its maximal $\mathfrak{p}$ is a principle ideal generated by a unformizer ϖ. Then $\mathfrak{m}=(\varpi)^n$. We regard $\mathfrak{m}$ simply as the nonzero element $\varpi^n\in\mathcal{O}$. By the condition on $\mathrm{ord}_{\mathfrak{p}}M$, we see that $\mathfrak{m}\mid M$, so there is an inclusion $W_{\mathfrak{m}}\to W_M$. It induces a natural map

$$\iota_{\mathfrak{m},M}:H^1(K,W_{\mathfrak{m}})\to H^1(K,W_M).$$

Proof of Propsition 3.5 under the assumption (vanishing). — Note that by assumption (i), $W_M/(\mathrm{Frob}_{\mathfrak{q}_i}-1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$[16]. Therefore we can apply Corollary 2.17 with $\mathfrak{q}=\mathfrak{q}_i$ and $\mathfrak{r}=\mathfrak{r}_{i-1}$ to relate the classes $\kappa_{[\mathfrak{r}_{i-1},M]}$ and $\kappa_{[\mathfrak{r}_i,M]}$. This is the key to the proof.

By the assumption (vanishing)[17], all of the maps

$$H^1(K,W_{\mathfrak{m}})\xrightarrow{\iota_{\mathfrak{m},M}}H^1(K,W_M)\xrightarrow{\iota_M}H^1(K,W)\xrightarrow{\mathrm{res}_{\Omega/K}}H^1(\Omega,W)$$

are injective. Therefore for $0\le i\le k$, we can define

$$\begin{aligned}\mathfrak{d}_i :&= \mathrm{order}(\kappa_{[\mathfrak{r}_i,M]},H^1(K,W_M))\\ &= \mathrm{order}(\iota_M(\kappa_{[\mathfrak{r}_i,M]}),H^1(K,W))\\ &= \mathrm{order}(\mathrm{res}_{\Omega/K}\,\iota_M(\kappa_{[\mathfrak{r}_i,M]}),H^1(\Omega,W))\\ &= \mathrm{order}(\mathrm{res}_{\Omega/K}(\kappa_{[\mathfrak{r}_i,M]}),H^1(\Omega,W_M)).\end{aligned}$$

On the bottom, we have by Proposition 3.3

$$\mathfrak{d}_0=\mathrm{ord}_{\mathfrak{p}}(M)-\mathrm{ind}_{\mathcal{O}}(\mathbf{c})\ge n$$

and we propagate using the Kolyvagin property (i.e. Corollary 2.17) that

$$\mathfrak{d}_i\ge\mathrm{order}((\kappa_{[\mathfrak{r}_i,M]})^{\mathrm{s}}_{\mathfrak{q}_i},H^1_{\mathrm{s}}(K_{\mathfrak{q}_i},W_M))=\mathrm{order}((\kappa_{[\mathfrak{r}_{i-1},M]})_{\mathfrak{q}_i},H^1_{\mathrm{f}}(K_{\mathfrak{q}_i},W_M))\ge\mathfrak{d}_{i-1}\quad(3.10)$$

to see at least $\mathfrak{d}_i\ge n$ for every i.

Now we begin to *approximate* the image of $\mathrm{loc}^{\mathrm{s}}_{\Sigma,W_{\mathfrak{m}}}$, i.e. $\mathrm{loc}^{\mathrm{s}}_{\Sigma,W_{\mathfrak{m}}}(\mathrm{Sel}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}}))$ by

(a) first constructing a filtration $\{A^{(i)}\}$ of $\mathrm{Sel}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}})$ using the Kolyvagin derived cohomology classes,
(b) and compute the length of the image of this filtration under $\mathrm{loc}^{\mathrm{s}}_{\Sigma,W_{\mathfrak{m}}}$.

Consider the natural maps

$$\begin{array}{ccccc}H^1(K,W_{\mathfrak{m}}) & \xrightarrow{\iota_{\mathfrak{m},M}} & H^1(K,W_M) & \xhookrightarrow{\iota_M} & H^1(K,W)\\ \uparrow & & \uparrow & & \uparrow\\ \mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}}) & \dashrightarrow & \mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)_{\mathfrak{m}} & \xhookrightarrow{\iota_M} & \mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W)_M\end{array}$$

$$\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)_{\mathfrak{m}}\xrightarrow{\iota_{\mathfrak{m}}}\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W)_M$$

It follows from Proposition 1.13 that the bended arrow ι_M exists and is surjective. By the injectivity of ι_M, we see that the dashed arrow

$$\iota_{\mathfrak{m},M}:\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}})\to\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)_{\mathfrak{m}}$$

is surjective. Recall Theorem 2.12 shows that $\kappa_{[\mathfrak{r}_i,M]}\in\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)$. Therefore we can choose $\overline{\kappa}_i\in\mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}})$ such that

$$\mathcal{O}\iota_{\mathfrak{m},M}(\overline{\kappa}_i)=\mathfrak{p}^{\mathfrak{d}_i-n}\kappa_{[\mathfrak{r}_i,M]}.$$

[16] Recall that in this section, the Euler system $\mathbf{c}$ satisfies the hypothesis $\mathrm{Hyp}(K,T)$.
[17] This is the only place where we used this hypothesis in the proof.

If $1 \le i \le k$, let $A^{(i)}$ denote the $\mathcal{O}$-submodule of $H^1(K, W_{\mathfrak{m}})$ generated by $\{\overline{\kappa}_1, \dots, \overline{\kappa}_i\}$, and let $A^{(0)} = 0$. Then

$$A^{(i)} \subseteq \mathrm{Sel}^{\Sigma_{p\mathfrak{r}_i}}(K, W_{\mathfrak{m}}) \subseteq \mathrm{Sel}^{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}}).$$

So for $1 \le i \le k$, writing $\mathrm{loc}^{\mathrm{s}}_{\Sigma}$ for $\mathrm{loc}^{\mathrm{s}}_{\Sigma, W_{\mathfrak{m}}}$, we have a filtration

$$\mathrm{loc}^{\mathrm{s}}_{\Sigma}(\mathrm{Sel}^{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}})) \supseteq \mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(k)}) \supseteq \mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(k-1)}) \cdots \supseteq \mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(1)}) \supseteq \mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(0)}) = 0$$

We compute the length of each graded pieces. Note that restriction to $\mathfrak{q}_i$ induces a surjective map

$$\mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(i)})/\mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(i)}) \twoheadrightarrow \mathcal{O}(\overline{\kappa}_i)^{\mathrm{s}}_{\mathfrak{q}_i} \subseteq H^1_{\mathrm{s}}(K_{\mathfrak{q}_i}, W_{\mathfrak{m}}).$$

Hence for $1 \le i \le k$, (3.10) shows that

$$\begin{aligned}
\mathrm{len}_{\mathcal{O}}(\mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(i)})/\mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(i)})) &\ge \mathrm{order}((\overline{\kappa}_i)^{\mathrm{s}}_{\mathfrak{q}_i}, H^1_{\mathrm{s}}(K_{\mathfrak{q}_i}, W_{\mathfrak{m}})) \\
&\ge \mathrm{ord}((\kappa_{[\mathfrak{r}_i, M]})^{\mathrm{s}}_{\mathfrak{q}_i}, H^1_{\mathrm{s}}(K_{\mathfrak{q}_i}, W_M)) - (\mathfrak{d}_i - n) \\
&\ge \mathfrak{d}_{i-1} - \mathfrak{d}_i + n.
\end{aligned}$$

Here the second "$\ge$" follows from the construction of $\overline{\kappa}_i$, and the third "$\ge$" invokes the Kolyvagin property (3.10) again. Then we conclude that

$$\begin{aligned}
\mathrm{len}_{\mathcal{O}}(\mathrm{loc}^{\mathrm{s}}_{\Sigma}(\mathrm{Sel}^{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}})) &\ge \mathrm{len}_{\mathcal{O}}(\mathrm{loc}^{\mathrm{s}}_{\Sigma}(A^{(k)})) \\
&\ge \sum_{i=1}^{k} (n + \mathfrak{d}_{i-1} - \mathfrak{d}_i) \\
&= kn + \mathfrak{d}_0 - \mathfrak{d}_k \\
&= kn + \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) - \mathfrak{d}_k \\
&\ge kn - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}).
\end{aligned}$$

Here the fourth line uses Proposition 3.3 that $\mathfrak{d}_0 = \mathrm{ord}_{\mathfrak{p}}(M) - \mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ and the last line follows from the trivial estimate that $\mathfrak{d}_k \le \mathrm{ord}_{\mathfrak{p}} M$.

Finally, for every prime $\mathfrak{q} \in \mathcal{R}_M$, we have $H^1_{\mathrm{s}}(K_{\mathfrak{q}}, W_{\mathfrak{m}}) = W_{\mathfrak{m}}^{\mathrm{Frob}_{\mathfrak{q}}=1}$ by Proposition 1.10, so

$$\mathrm{len}_{\mathcal{O}}\left(\bigoplus_{\mathfrak{q}\in\Sigma} H^1_{\mathrm{s}}(K_{\mathfrak{q}}, W_{\mathfrak{m}})\right) = k\,\mathrm{len}_{\mathcal{O}}(W_{\mathfrak{m}}^{\mathrm{Frob}_{\mathfrak{q}}=1}) = k\,\mathrm{len}_{\mathcal{O}}(W_{\mathfrak{m}}/(\mathrm{Frob}_{\mathfrak{q}} - 1)W_{\mathfrak{m}}) = kn.$$

Here the second equality follows from Lemma 2.18. Thus, $\mathrm{len}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma})) \le \mathrm{ind}_{\mathcal{O}}(\mathbf{c})$, as desired. □

Then we can finally prove Theorem 3.2. Now it is not hard as we have prepared almost everything for it.

Proof of Theorem 3.2. — We fix a nonzero ideal $\mathfrak{m} = \mathfrak{p}^n$ of $\mathcal{O}$. Let C be the image of $\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*)$ in $H^1(K, W_M^*)$ via

$$\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*) \hookrightarrow H^1(K, W_{\mathfrak{m}}) \xrightarrow{\iota_{\mathfrak{m},M}} H^1(K, W_M).$$

The image is indeed finite by Proposition 1.15(i). We assume $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is finite since otherwise there is nothing to prove, and hence we can choose M is a power of p large enough so that

$$\mathrm{ord}_{\mathfrak{p}} M > n + (\left|\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*)\right|)n_W + \mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

Apply Proposition 3.4 with this group C and let Σ be a set of primes produced by that lemma, and apply Proposition 3.5 with this set Σ, we see

$$\mathrm{len}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^{\mathrm{s}}_{\Sigma, W_{\mathfrak{m}}})) \leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + n_W.$$

Combining with Theorem 1.22(ii) shows that

$$\mathrm{len}_{\mathcal{O}}(\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*)/\mathrm{Sel}_{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}}^*)) \leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + n_W$$

and therefore,

$$\mathrm{len}_{\mathcal{O}}(\iota_{\mathfrak{m}}(\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*))) \leq \mathrm{len}_{\mathcal{O}}(\iota_{\mathfrak{m}}(\mathrm{Sel}_{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}}^*))) + \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + n_W.$$

The local condition guaranteed by Proposition 3.4(iv) implies that

$$\iota_{\mathfrak{m}}(\mathrm{Sel}_{\Sigma\cup\Sigma_p}(K, W_{\mathfrak{m}}^*)) \subseteq H^1(\Omega/K, W^*) \cap \mathrm{Sel}_{\Sigma_p}(K, W^*).$$

By the definition of n_W^*, we see that

$$\mathrm{len}_{\mathcal{O}}(\iota_{\mathfrak{m}}(\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*))) \leq n_W^* + \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + n_W.$$

Since this holds for every $\mathfrak{m}$, and $\mathrm{Sel}_{\Sigma_p}(K, W^*) = \varinjlim_{\mathfrak{m}} \iota_{\mathfrak{m}}(\mathrm{Sel}_{\Sigma_p}(K, W_{\mathfrak{m}}^*))$ by Proposition 1.14(ii), Theorem 3.2 follows. □

3.4. Application to class groups. — We are finally ready to state and prove the main application.

***Definition 3.6.* —** Let $\mathcal{E}_L$ denote the group of global units of $L = \mathbb{Q}(\zeta_f)^+$. We define the group of **χ-cyclotomic units** $\mathcal{C}_{L,\chi}$ to be the subgroup of $\mathcal{E}_L^\chi$ generated over $\mathcal{O}[\mathrm{Gal}(L/\mathbb{Q})]$ by

$$\xi_{L,\chi} := \prod_{\delta \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})} (1 - \zeta_f^\delta)^{\chi^{-1}(\delta)}.$$

The mysterious χ-cyclotomic unit $\xi_{L,\chi}$ is not far from what we have seen so far. Indeed, it follows directly from the previous calculation on $(\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}})_{\mathbb{Q}}$ in Section 2.1.3 and Lemma 2.5 that

$$(\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}})_{\mathbb{Q}} = \xi_{L,\chi}^{1-\chi^{-1}(p)}, \tag{3.11}$$

where $\chi(p) = 0$ if $p \mid f$. If we assume further that

$$p > 2, \quad \chi \text{ has order prime to } p \text{ and } \chi(p) \neq 1, \tag{Koly}$$

then we have $1 - \chi^{-1}(p) \in \mathcal{O}^\times$, so $(\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}})_{\mathbb{Q}}$ generates $\mathcal{C}_{L,\chi}$ as well.

The main result is the following, originally proved by Mazur and Wiles [MW84] using automorphic methods. The proof given here is due to Kolyvagin [Kol90].

***Theorem 3.7.* —** *Suppose that χ is an even character satisfying the assumption (Koly), then*

$$\left|A_L^\chi\right| \text{ divides } [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

Proof. — We will apply Theorem 3.2 with the Euler system $\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}}$ of $(\mathbb{Z}_p(1)\otimes\chi^{-1}, \mathbb{Q}^{\mathrm{ab}}, pf)$ constructed from cyclotomic units above. Since $\mathrm{rank}_{\mathcal{O}}(\mathbb{Z}_p(1)\otimes\chi^{-1}) = 1$, we see that $\mathrm{Hyp}(\mathbb{Q}, \mathbb{Z}_p(1)\otimes\chi^{-1})$ is satisfied with $\tau = 1$. Further, in this case, $\Omega = L(\boldsymbol{\mu}_{p^\infty})$. Since χ is nontrivial and even, n_W and n_W^* in Theorem 3.2 are both zero by [**Rub00**, Lemma 3.1.1].

Moreover, we can see that[(18)]

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c}_{\mathrm{cyc}}^{\chi^{-1}}) = \mathrm{len}_{\mathcal{O}}(\mathcal{E}_L^{\chi}/\mathcal{C}_{L,\chi}).$$

Putting all of this together, Theorem 3.2 in this case yields

$$\left|\mathrm{Sel}_{\Sigma_p}(\mathbb{Q}, W)\right| \text{ divides } [\mathcal{E}_L^{\chi} : \mathcal{C}_{L,\chi}].$$

The last thing is to compare the strict Selmer group $\mathrm{Sel}_{\Sigma_p}(\mathbb{Q}, W)$ and the original Bloch-Kato Selmer group $\mathrm{Sel}_{\mathrm{BK}}(\mathbb{Q}, W)$. In our case, by the happy coincidence (1.4),

$$H^1_{\mathrm{f}}(\mathbb{Q}_p, V) = H^1_{\mathrm{ur}}(\mathbb{Q}_p, V) = V^{I_p}/(\mathrm{Frob}_p - 1)V^{I_p} = V^{I_p}/(\chi(p) - 1)V^{I_p} = 0$$

since $\chi(p) \neq 1$ and the second equality is from Lemma 1.5(i). Therefore $H^1_{\mathrm{f}}(\mathbb{Q}_p, W) = 0$ and hence

$$\mathrm{Sel}_{\mathrm{BK}}(\mathbb{Q}, W) = \mathrm{Sel}_{\Sigma_p}(\mathbb{Q}, W).$$

Hence by Theorem 1.24, we see $\left|A_L^{\chi}\right|$ divides $[\mathcal{E}_L^{\chi} : \mathcal{C}_{L,\chi}]$, as desired. □

Moreover, this upper bound is sharp if we invoke the class number formula.

Corollary 3.8 **([Rub90**, Theorem 4.2]**).** — *Suppose χ is an even character satisfying the assumption* (Koly)*, then*

$$\left|A_L^{\chi}\right| = [\mathcal{E}_L^{\chi} : \mathcal{C}_{L,\chi}].$$

We remark that if $\chi(p) = 1$, then (3.11) shows that $(\mathbf{c}_{\mathrm{cyc}}^{\chi})_{\mathbb{Q}} = 0$, so Theorem 3.2 is of no use. To make these up , see [**Rub00**, Remark 3.2.5] for some explanations.

References

[Kol90] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990. 32

[Maz01] Barry Mazur. Student Projects for the Arizona Winter School 2001, 2001. Available at https://swc-math.github.io/aws/2001/notes.html. 2

[Mil06] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006. 9

[Mil20] J.S. Milne. Class Field Theory (v4.03), 2020. Available at www.jmilne.org/math/. 17

[MR04] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004. 4, 14

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of **Q**. *Invent. Math.*, 76(2):179–330, 1984. 32

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008. 13, 22, 27

[Rub90] Karl Rubin. The main conjecture. In *Cyclotomic Fields I and II*, volume 121 of *Graduate Texts in Mathematics*, pages 397–419. Springer New York, 1990. 33

[(18)] A few more argument is needed here, see [**Rub00**, Proof of Theorem 3.2.3].

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study. 2, 4, 5, 6, 7, 8, 9, 12, 14, 15, 16, 17, 23, 24, 25, 26, 27, 28, 29, 33

[Ski18] Christopher Skinner. Lectures on the Iwasawa Theory of Elliptic Curves, 2018. Available at https://swc-math.github.io/aws/2018/. 5

February 14, 2025

Ruichen Xu, Ph.D student at Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Science, No. 55 Zhongguancun East Road, Beijing, 100190, China.
E-mail : xuruichen21@mails.ucas.ac.cn