Kolyvagin systems and higher Fitting ideals of Selmer groups

Alberto Angurel

7th January 2026

Contents

Chapter 1

Selmer structures

1.1 Local cohomology and Kolyvagin primes

Notation 1.1.1. Let K be a number field. Fix an algebraic closure $\overline{K}$ of K. For every finite extension F/K, denote its absolute Galois group by $G_F = \mathrm{Gal}(\overline{K}/F)$.

Assumption 1.1.2. Let R be a local, artinian and self-injective ring with maximal ideal $\mathfrak{m}$ and finite residue field k of characteristic $p \geq 5$. Let T be an $R[[G_K]]$-module, which is free and finitely generated as an R-module and is only ramified at finitely many primes.

Notation 1.1.3. (Duality) We will use the following duals of T

$$T^\vee = \mathrm{Hom}(T, \mathbb{Q}_p/\mathbb{Z}_p), \quad T^* = \mathrm{Hom}(T, \mu_{p^\infty}), \quad T^+ = \mathrm{Hom}(T, R)$$

Notation 1.1.4. We denote by $K(T)$ to the minimal Galois extension such that $G_{K(T)}$ acts trivially on T. Let M be the minimal $n \in \mathbb{N}$ such that $p^n R = 0$ and let $K(1)$ be the maximal p-extension inside the Hilbert class field of K. Denote

$$K_M = K\big(\mu_M, (\mathcal{O}_K^\times)^{1/M}\big)K(1), \quad K(T)_M = K(T)K_M$$

We assume the following assumptions:

Assumption 1.1.5. We assume the following assumptions:

- (T1) $T/\mathfrak{m}T$ is an irreducible $k[[G_K]]$-module.
- (T2) There exists $\tau \in G_{K_M}$ such that $T/(\tau - 1)T \cong R$ as R-modules.
- (T3) $H^1(K(T)_M/K, T) = H^1(K(T)_M/K, T^*) = 0$.

Remark 1.1.6. Assume that the homomorphism $\rho : G_\mathbb{Q} \to \mathrm{Aut}(T) \cong GL_{\mathrm{rank}(T)}(R)$ induced by the Galois action is surjective. Then all three Assumptions 1.1.5 hold. Indeed, (T1) and (T2) are clear.

For (T3), note that the order of $R^\times$ is divisible by $p-1$. It implies that the order of $GL_{\mathrm{rank}(T)}(R)$ and, therefore, the order of $\mathrm{Gal}(K(T)_M/K)$, are also divisible by $p-1$.

Then there is a subgroup $\Delta \subset \mathrm{Gal}(K(T)_M/K)$ of order $p-1$. For every $A \in \{T, T^*\}$, there is an inflation-restriction exact sequence

$$0 \longrightarrow H^1\big(\mathrm{Gal}(K(T)_M/K)/\Delta, A^\Delta\big) \longrightarrow H^1(K(T)_M/K, A) \longrightarrow H^1(\Delta, A)$$

Note that the first cohomology group vanishes since $A^\Delta = 0$ and the third one is also zero since the order of Δ is prime to p. Therefore, $H^1(K(T)_M/K, A)$ needs to be zero.

Proposition 1.1.7. If T satisfies Assumption 1.1.5, then $H^0(K, T/I) = 0$ for every ideal I of R

Proof. By (T1), either $(T/\mathfrak{m}T)^{G_K} = 0$ or $T/\mathfrak{m}T$ is the trivial representation. Since the latter does not satisfy (T3), then the former holds. It implies that $(T/I)^{G_K} = 0$. □

There is a set of primes playing a crucial role in this theory.

Definition 1.1.8. A prime q is said to be a *Kolyvagin prime* if Frob_q is conjugate to τ in $\mathrm{Gal}(K(T)_M/K)$.

Notation 1.1.9. We define the following sets:

- $\mathcal{P}^{(R)}$: set of Kolyvagin primes.
- $\mathcal{N}^{(R)}$: set of square-free product of Kolyvagin primes.
- $\mathcal{N}_i^{(R)}$: set of square-free products of i Kolyvagin primes.

When there is no risk of confusion, we will drop the reference to R.

The reason to choose these primes is that we can control its local cohomology, since the finite and singular cohomology groups, defined below, are free cyclic R-modules.

Definition 1.1.10. (Finite cohomology) Let ℓ be a finite place of K, not dividing p. Assume T is unramified at ℓ. The *finite cohomology* group at ℓ is defined as

$$H^i_{\mathrm{f}}(K_\ell, T) := H^i(K_\ell^{\mathrm{ur}}, T) = \ker\Big(H^i(K_\ell, T) \to H^i(\mathcal{I}_\ell, T)\Big)$$

where K_ℓ^{ur}/K is the maximal unramified extension of K, $\mathcal{I}_\ell$ is the inertia subgroup of G_{K_ℓ}, and the second equality follows from the inflation-restriction sequence.

comment on finite cohomology for other primes

Definition 1.1.11. (Singular cohomology) Let ℓ be a finite place of K as in Definition 1.1.10. The *singular cohomology* at ℓ is the quotients

$$H^i_{\mathrm{s}}(K_\ell, T) = H^i(K_\ell, T) \Big/ H^i_{\mathrm{f}}(K_\ell, T)$$

When ℓ is a Kolyvagin prime, the singular cohomology can be also identified with a subgroup of $H^1(K_\ell, T)$.

Proposition 1.1.12. ([MR04, Lemma 1.2.1]) If $\ell \in \mathcal{P}$, the canonical short exact sequence

$$0 \longrightarrow H^1_{\mathrm{f}}(K_\ell, T) \longrightarrow H^1(K_\ell, T) \longrightarrow H^1_s(K_\ell, T) \longrightarrow 0 \tag{1.1}$$

splits canonically. Moreover, there exist isomorphisms of free cyclic R-modules

$$H^1_{\mathrm{f}}(K_\ell, T) \cong T/(\tau - 1)T,\ H^1_{\mathrm{s}}(K_\ell, T) \cong T^{\tau=1}$$

Remark 1.1.13. The first isomorphism is canonical from the identification

$$H^1_{\mathrm{f}}(K_\ell, T) \cong T/(\mathrm{Frob}_\ell - 1)T \cong T/(\tau - 1)T$$

However, the second one is only canonical after tensoring with the Galois group $\mathcal{G}_\ell = \mathrm{Gal}(K(\ell)/K(1))$, where $K(\ell)$ is defined as the maximal p-extension inside the ray class field modulo ℓ. Following [MR04, Lemma 1.2.1]:

$$H^1_{\mathrm{s}}(K_\ell, T) \otimes_{\mathbb{Z}} \mathcal{G}_\ell \cong \mathrm{Hom}(\mathcal{I}_\ell, T^{\mathrm{Frob}_\ell=1}) \otimes \mathcal{G}_\ell \cong T^{\mathrm{Frob}_\ell=1} \cong T^{\tau=1}$$

Definition 1.1.14. (Transverse cohomology) Let $\ell \in \mathcal{P}$. The *transverse cohomology* sugbgroup is defined as

$$H^1_{\mathrm{tr}}(K_\ell, T) := H^1\big(K(\ell)_\ell/K_\ell, T^{G_{K(\ell)_\ell}}\big) \hookrightarrow H^1(K_\ell, T)$$

Proposition 1.1.15. ([MR04, Lemma 1.2.4]) $H^1_{\mathrm{tr}}(K_\ell, T)$ is the image of the canonical splitting in Equation (1.1). Note it is canonically isomorphic to $H^1_{\mathrm{s}}(K_\ell, T)$.

There is a canonical comparison isomorphism between the finite and the singular cohomology at a Kolyvagin prime ℓ.

Proposition 1.1.16. ([MR04, Lemma 1.2.3]) Let $\ell \in \mathcal{P}$. Then there is a canonical isomorphism, known as *finite-singular map*,

$$\varphi^{\mathrm{fs}}_\ell :\ H^1_{\mathrm{f}}(K_\ell, T) \to H^1_{\mathrm{s}}(K_\ell, T) \otimes \mathcal{G}_\ell$$

Notation 1.1.17. In order to simplify notation, we fix once and for all, and for each Kolyvagin prime $\ell \in \mathcal{P}$, a generator τ_ℓ of $\mathcal{G}_\ell$. This choice, together with the finite singular map, fixes an isomorphism between $H^1_{\mathrm{f}}(K_\ell, T)$ and $H^1_{\mathrm{s}}(K_\ell, T)$.

The finite and transverse cohomology groups behave well under local Tate duality.

Proposition 1.1.18. (Local Tate duality) There is a perfect pairing

$$H^1(K_\ell, T) \times H^1(K_\ell, T^*) \to \mathbb{Q}_p/\mathbb{Z}_p$$

Under this pairing,

- $H^1_{\mathrm{f}}(K, T)$ and $H^1_{\mathrm{f}}(K, T^*)$ are annihilators of each other.
- $H^1_{\mathrm{tr}}(K, T)$ and $H^1_{\mathrm{tr}}(K, T^*)$ are annihilators of each other.

1.2 Selmer modules

In this section, we introduce the concepts of Selmer structures and their associated Selmer modules. They are subgroups of the Global Galois cohomolgy which are cut out by local conditions. The can be used to determine the structure of important arithmetic objects like class groups of number fields or Mordell-Weil groups of abelian varieties.

Definition 1.2.1. A *Selmer structure* $\mathcal{F}$ on T is a collection of the following data:

- A finite set $\Sigma(\mathcal{F})$ of places of K, including all archimedean and p-adic primes and all the primes where T is ramified.
- For every $\ell \in \Sigma(\mathcal{F})$, a choice of an $R[[G_{K_\ell}]]$-submodule

$$H^1_{\mathcal{F}}(K_\ell, T) \subset H^1(K_\ell, T)$$

  This choice is known as *local condition* at ℓ.

Definition 1.2.2. The *Selmer module* associated to a Selmer structure is

$$H^1_{\mathcal{F}}(K, T) = \ker\left(H^1(K^\Sigma/K, T) \to \prod_{\ell \in \Sigma} H^1(K_\ell, T)\right)$$

where K^Σ/K is the maximal extension unramified outside Σ and the map is the composition of inflation and restriction map

Remark 1.2.3. When $\ell \notin \Sigma(\mathcal{F})$, we say the local condition at ℓ is

$$H^1_{\mathcal{F}}(K_\ell, T) = H^1_f(K_\ell, T)$$

Under this identification, the Selmer module only depends on the local conditions, and not on the set $\Sigma(\mathcal{F})$, being

$$H^1_{\mathcal{F}}(K, T) = \ker\left(H^1(K, T) \to \prod_{\ell \in \mathbb{P}} H^1(K_\ell, T)\right)$$

In order to compare Selmer structures, Poitou-Tate global duality is helpful. In order to introduce the global duality exact sequence, we need to introduce the concept of dual Selmer structure.

Definition 1.2.4. (Dual Selmer structure) If $\mathcal{F}$ is a Selmer structure defined on T, there is a *dual Selmer structure* defined on T by the data

- $\Sigma_{\mathcal{F}^*} = \Sigma_{\mathcal{F}}$
- For $\ell \in \Sigma$, $H^1_{\mathcal{F}^*}(K_\ell, T)$ is defined to be the annihilator of $H^1_{\mathcal{F}}(K_\ell, T)$ under the pairing in Proposition 1.1.18.

Proposition 1.2.5. ([MR04, theorem 2.3.4]) Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures of T such that $H^1_{\mathcal{F}}(K_\ell, T) \subset H^1_{\mathcal{G}}(K_\ell, T)$ for every prime ℓ. Then the following sequence, where the third map is induced by proposition 1.1.18, is exact.

$$H^1_{\mathcal{F}}(K,T) \rightarrowtail H^1_{\mathcal{G}}(K,T) \longrightarrow \bigoplus_{\ell \in \Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_\ell,T)}{H^1_{\mathcal{F}}(K_\ell,T)} \longrightarrow H^1_{\mathcal{G}}(K,T^*)^\vee \twoheadrightarrow H^1_{\mathcal{F}}(K,T^*)^\vee$$

Notation 1.2.6. Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures. We say $\mathcal{F} \leq \mathcal{G}$ if

$$H^1_{\mathcal{F}}(K_\ell,T) \subset H^1_{\mathcal{G}}(K_\ell,T) \ \forall \ell \in \mathcal{P}$$

Local conditions propagates naturally to submodules and quotients of T.

Definition 1.2.7. (Propagation to submodules) Let $T' \hookrightarrow T$ be a submodule. This inclusion induces a map

$$\mu : \ H^1(K,T') \to H^1(K,T)$$

A local condition at T propagates to T' as

$$H^1_{\mathcal{F}}(K_\ell,T') = \mu^{-1}\big(H^1_{\mathcal{F}}(K_\ell,T)\big)$$

Definition 1.2.8. (Propagation to quotients) Let $T \hookrightarrow T''$ be a quotient map. It a map

$$\varepsilon : \ H^1(K,T) \to H^1(K,T'')$$

A local condition at T propagates to T' as

$$H^1_{\mathcal{F}}(K_\ell,T'') = \varepsilon\big(H^1_{\mathcal{F}}(K_\ell,T)\big)$$

Remark 1.2.9. Let $T_1 \subset T_2 \subset T$ be two submodules of T. The propagation of a local condition to the subquotient T_2/T_1 is independent of the order in which we perform the operations.

With the definition of the propagation of Selmer structures, we can compare the Selmer groups of submodules with the torsion of the Selmer group.

Proposition 1.2.10. ([MR04, Lemma 3.5.3], [BSS18, Proposition 3.5]) Under Assumptions 1.1.5, for every ideal I of R, the inclusion $T^*[I] \hookrightarrow T^*$ induces an isomorphism

$$H^1_{\mathcal{F}}(K,T^*[I]) \cong H^1_{\mathcal{F}}(K,T^*)[I]$$

In this theory, it is required to impose a technical condition on the Selmer structures that guarantees good behaviour under the propagation.

Definition 1.2.11. (Cartesian Selmer structure) A Selmer structure $\mathcal{F}$ is said to be *cartesian* if the map

$$H^1_{/\mathcal{F}}(K_\ell,T \otimes k) \to H^1_{/\mathcal{F}}(K_\ell,T)$$

is injective for every prime ℓ.

Remark 1.2.12. It is enough to check the cartesian condition for $\ell \in \Sigma_{\mathcal{F}}$. Indeed, when $\ell \notin \Sigma_{\mathcal{F}}$, then

$$H^1_{\mathcal{F}}(K_\ell, T) = H^1_{\mathrm{f}}(K_\ell, T) \Rightarrow H^1_{\mathcal{F}}(K_\ell, T) = H^1_{\mathrm{s}}(K_q, T) = \mathrm{Hom}(\mathcal{I}_q, T^{\mathrm{Frob}_\ell = 1})$$

which is a cartesian local condition because Hom is a left exact functor.

When the Selmer structure is cartesian, the Selmer group of some quotients of T can be also identified with the torsion of the Selmer group.

Proposition 1.2.13. Assume Assumptions 1.1.5 and that I is an ideal of R such that $R[I]$ is principal. The multiplication by a generator π induces an injection $T/I \hookrightarrow T$, which itself induces an isomorphism

$$H^1_{\mathcal{F}}(K, T/I) \hookrightarrow H^1_{\mathcal{F}}(K, T)[I]$$

Proof. Multiplication by π induces an isomorphism $T/I \cong T[I]$. Therefore, Proposition 1.2.10 implies that

$$H^1_{\mathcal{F}}(K, T/I) \cong H^1_{\mathcal{F}}(K, T[I]) \cong H^1_{\mathcal{F}}(K, T)[I]$$

□

The theory of Kolyvagin systems is dependent on the core rank, which is an invariant associated to the Selmer structure, that measures the difference in dimension between the Selmer module and the Selmer module of the dual structure.

Definition 1.2.14. (Core rank) Let $\mathcal{F}$ be a Selmer strucure on T. The *core rank* of $\mathcal{F}$ is the integer

$$\chi(\mathcal{F}) := \dim_k H^1_{\mathcal{F}}(K, T \otimes k) - \dim_k H^1_{\mathcal{F}}(K, T^*[\mathfrak{m}])$$

Remark 1.2.15. We will assume $\chi(\mathcal{F})$ is non-negative. Otherwise, one could swap the roles of F^* and T^* since $\chi(\mathcal{F}^*) = -\chi(\mathcal{F})$.

When the Selmer strcuture is cartesian, the core rank can determine the relation of the full Selmer group with the one of the dual Selmer structure.

Proposition 1.2.16. ([MR04, Theorem 4.1.5.]) Let R be a principal, artinian, local ring and let $\mathcal{F}$ be a cartesian Selmer structure of core rank $\chi(\mathcal{F}) \geq 0$. Then there is a non-canonical homomorphism

$$H^1_{\mathcal{F}}(K, T) = R^{\chi(\mathcal{F})} \oplus H^1_{\mathcal{F}}(K, T^*)$$

The argument to compute the structure of a Selmer group involve modifying the local conditions suitabily at certain primes. In order to do that, we will set the following definition.

Definition 1.2.17. Let $\mathcal{F}$ be a Selmer structure and let a, b and c be pairwise coprime square-free integers. Assume $c \in \mathcal{N}$. Define the Selmer structure $\mathcal{F}_a^b(c)$ by the local conditions

$$H^1_{\mathcal{F}_a^b(c)}(\mathbb{Q}, T) = \begin{cases} H^1(\mathbb{Q}_\ell, T) & \text{if } \ell | a \\ 0 & \text{if } \ell | b \\ H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T) & \text{if } \ell | c \\ H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) & \text{otherwise} \end{cases}$$

By Proposition 1.1.18, we can determine explicitly the dual of the modified Selmer structures.

Proposition 1.2.18. Let $\mathcal{F}$ be a cartesian Selmer structure and let $a, b, c \in \mathcal{N}$ be pairwise coprime. Then

$$\left(\mathcal{F}_a^b(c)\right)^* = (\mathcal{F}^*)_b^a(c)$$

We can relate the core rank of $\mathcal{F}_a^b(c)$ with the core rank of $\mathcal{F}$ and the number of prime divisors of a and b.

Notation 1.2.19. For every $n \in \mathcal{N}$, we denote by $\nu(n)$ to the number of prime divisors of n.

Proposition 1.2.20. ([Sak18, Corollary 3.21]) Let $\mathcal{F}$ be a cartesian Selmer structure and let $a, b, c \in \mathcal{N}$ be pairwise coprime. Then $\mathcal{F}_a^b(c)$ is also cartesian and

$$\chi(\mathcal{F}_a^b(c)) = \chi(\mathcal{F}) + \nu(b) - \nu(a)$$

The Kolyvagin system argument involve the modification of certain conditions in order to make the Selmer module smaller. For this reason, we will finish this section with some technical lemmas that will be used repeatedly. We start with an application of Chebotarev density theorem that proves the existence of Kolyvagin primes such that their localisation does not annihilate certain elements in the local cohomology group.

Proposition 1.2.21. ([BSS18, Lemma 3.9]) Consider non-zero cohomology classes

$$c_1, \dots, c_s \in H^1(K, T), \quad c_1^*, \dots, c_t^* \in H^1(K, T^*)$$

If $s + t < p$, there is a Kolyvagin prime $\ell \in \mathcal{P}$ such that $\mathrm{loc}_\ell(c_i)$ and $\mathrm{loc}_\ell(c_i^*)$ are all non-zero.

Lemma 1.2.22. ([MR04, Lemma 4.1.7]) Let $\mathcal{F}$ be a Selmer structure and let $\ell \notin \Sigma_{\mathcal{F}}$ be a prime satisfying that

$$\mathrm{loc}_\ell : \ H^1_{\mathcal{F}}(K, T) \to H^1_{\mathrm{f}}(K_\ell, T)$$

is surjective. Then $H^1_{\mathcal{F}(\ell)}(K, T^*) = H^1_{\mathcal{F}_\ell}(K, T^*)$.

Proof. The surjectivity of loc_ℓ, together with the exact sequence of Proposition 1.2.5 with Selmer structures $\mathcal{F}_\ell$ and $\mathcal{F}$ implies that

$$H^1_{(\mathcal{F}^*)^\ell}(K, T^*) = H^1_{\mathcal{F}^*}(K, T^*) \tag{1.2}$$

By construction, we obtain

$$H^1_{(\mathcal{F}^*)_\ell}(K,T^*) = H^1_{\mathcal{F}^*}(K,T^*) \cap H^1_{(\mathcal{F}^*)(\ell)}(K,T^*)$$

By equation (1.2)

$$H^1_{(\mathcal{F}^*)_\ell}(K,T^*) = H^1_{(\mathcal{F}^*)^\ell}(K,T^*) \cap H^1_{(\mathcal{F}^*)(\ell)}(K,T^*)$$

Since $H^1_{(\mathcal{F}^*)(\ell)}(K,T^*) \subset H^1_{(\mathcal{F}^*)^\ell}(K,T^*)$, we get that

$$H^1_{(\mathcal{F}^*)_\ell}(K,T^*) = H^1_{(\mathcal{F}^*)(\ell)}(K,T^*)$$

□

For the rest of this section, we assume R is a principal ring. The next two lemmas show how we can make the Selmer group smaller by swapping the local condition at certain appropppriate prime ℓ. The situation when $\chi(\mathcal{F}) \geq 1$ was done in [MR04].

Lemma 1.2.23. (see [MR04, Proposition 4.5.8]) Assume R is principal and let $\mathcal{F}$ be a cartesian Selmer structure. Assume that $H^1_{\mathcal{F}}(K,T)$ contains a submodule isomorphic to R and that

$$H^1_{\mathcal{F}}(K,T^*) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some exponents $e_1 \geq e_2 \geq \cdots \geq e_s$. Then there exists a Kolyvagin prime $\ell \in \mathcal{P}$ such that

$$H^1_{\mathcal{F}^*(\ell)}(K,T^*) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Remark 1.2.24. When $\chi(\mathcal{F}) \geq 1$, the Selmer group $H^1_{\mathcal{F}}(K,T)$ always contains a submodule isomorphic to R, since there is a non-canonical isomorphisms

$$H^1_{\mathcal{F}}(K,T) \approx R^{\chi(\mathcal{F})} \oplus H^1_{\mathcal{F}^*}(K,T^*)$$

Proof of Lemma 1.2.23. Recall that $k = \text{length}(R)$ and let π be a generator of $\mathfrak{m}$. Choose classes $c \in H^1_{\mathcal{F}}(K,T)$ and $c^* \in H^1_{\mathcal{F}^*}(K,T^*)$ such that $\pi^{k-1}c \neq 0$ and $\pi^{e_1-1}c^* \neq 0$. By Proposition 1.2.21, there is a Kolyvagin prime $\ell \in \mathcal{P}$ such that

$$\text{loc}_\ell(\pi^{k-1}c) \neq 0, \quad \text{loc}_\ell(\pi^{e_1-1}c^*) \neq 0$$

The first condition implies that loc_ℓ is surjective, so Lemma 1.2.23 implies that

$$H^1_{(\mathcal{F}^*)(\ell)}(K,T^*) = H^1_{(\mathcal{F}^*)_\ell}(K,T^*) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$ □

When $\chi(\mathcal{F}) = 0$, we need to study quotients of T in order to apply 1.2.22 and, when recovering the information about the Selmer group of T, we only get partial information. The next lemma is the technical base for the main Theorems cite about the structure of Selmer group of core rank zero.

Lemma 1.2.25. Assume R is principal and let $\mathcal{F}$ be a cartesian Selmer structure such that $\chi(\mathcal{F}) = 0$. Assume that

$$H^1_{\mathcal{F}}(K,T) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some exponents $e_1 \geq e_2 \geq \cdots \geq e_s$. Then there exists a Kolyvagin prime $\ell \in \mathcal{P}$ and an integer t, such that $e_2 \leq t \leq k$.

$$H^1_{\mathcal{F}}(K,T) \approx R/\mathfrak{m}^{t} \times R/\mathfrak{m}^{e_3} \cdots \times R/\mathfrak{m}^{e_s}$$

If, moreover, $e_1 > e_2$, the integer t can be chosen equal to e_2.

Proof. Since $\chi(\mathcal{F}) = 0$, Proposition 1.2.16 implies that

$$H^1_{\mathcal{F}^*}(K,T^*) \approx H^1_{\mathcal{F}}(K,T) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

We pick classes $c \in H^1_{\mathcal{F}}(K,T)$ and $c^* \in H^1_{\mathcal{F}^*}(K,T^*)$ such that $\pi^{e_1}c \neq 0$ and $\pi^{e_1}c^* \neq 0$. By Proposition 1.2.21, we can choose a Kolyvagin prime $\ell \in \mathcal{P}$ such that

$$\mathrm{loc}_\ell(\pi^{e_1-1}c) \neq 0, \quad \mathrm{loc}_\ell(\pi^{e_1-1}c^*) \neq 0$$

Consider the diagram

$$\begin{array}{ccc} H^1_{\mathcal{F}}(K,T/\mathfrak{m}^{e_1}) & \xrightarrow{\mathrm{loc}_\ell} & H^1_{\mathrm{f}}(K_\ell,T/\mathfrak{m}^{e_1}) \\ \downarrow{\scriptstyle \pi^{k-e_1}} & & \downarrow{\scriptstyle \pi^{k-e_1}} \\ H^1_{\mathcal{F}}(K,T) & \xrightarrow{\mathrm{loc}_\ell} & H^1_{\mathrm{f}}(K_\ell,T/\mathfrak{m}^{e_1}) \end{array}$$

By Proposition 1.2.13, the leftmost vertical map is surjective, so there is some $c' \in H^1_{\mathcal{F}}(K,T/\mathfrak{m}^{e_1})$ such that $\mathrm{loc}_\ell(\pi^{e_1}c') \neq 0$.

Note that the element $\tau \in G_K$ from (T2) in Assumption 1.1.5 satisfies that

$$T/(\mathfrak{m}^{e_1}, \tau - 1) \cong R/\mathfrak{m}^{e_1}$$

and, since $K(T/\mathfrak{m}^{e_1})_{e_1} \subset K(T)_K$, then Frob_ℓ is conjugate to τ in $\mathrm{Gal}(K(T/\mathfrak{m}^{e_1})_{e_1}/K)$, so it is a Kolyvagin prime for $T/\mathfrak{m}^{e_1}$. Then we can apply Lemma 1.2.22 to guarantee that

$$H^1_{(\mathcal{F}^*)(\ell)}(K,T^*[\mathfrak{m}^{e_1}]) = H^1_{(\mathcal{F}^*)_\ell}(K,T^*[\mathfrak{m}^{e_1}]) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

By Propositions 1.2.16 and 1.2.10,

$$H^1_{\mathcal{F}(\ell)}(K,T)[\mathfrak{m}^{e_1}] \cong H^1_{\mathcal{F}^*(\ell)}(\mathbb{Q},T^*)[\mathfrak{m}^{e_1}] \cong H^1_{\mathcal{F}^*(\ell)}(\mathbb{Q},T^*[\mathfrak{m}^{e_1}]) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Since $\chi(\mathcal{F}^\ell) = 1$ by Proposition 1.2.20, then Proposition 1.2.16 implies that

$$H^1_{\mathcal{F}(\ell)}(\mathbb{Q},T) \subset H^1_{\mathcal{F}^\ell}(\mathbb{Q},T) \approx R \oplus H^1_{\mathcal{F}^*_\ell}(\mathbb{Q},T^*)$$

Therefore, $H^1_{\mathcal{F}(\ell)}(\mathbb{Q},T)$ can be injected into $R \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$ and its $\mathfrak{m}^{e_1}$-torsion is isomorphic to $R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$. Under those considerations, the lemma follows by the structure theorem of $R/\mathfrak{m}^k$-modules. □

Even in the case $\chi(\mathcal{F}) = 0$, we can improve Lemma 1.2.25 to obtain a result of the kind of Lemma 1.2.23 even when the Selmer group does not contain submodules isomorphic to R, but assuming some hypothesis about T not being residually self-dual.

Assumption 1.2.26. Consider the following assumptions to rule out self-duality in T

- (N1) $T/\mathfrak{m}T$ is not isomorphic to $T^*[\mathfrak{m}]$ as $k[[G_K]]$-modules.
- (N2) The image of the homomorphism $R \to \mathrm{End}(T)$ is contained in the image of $\mathbb{Z}_p[[G_{\mathbb{Q}}]] \to \mathrm{End}(T)$.

Under those assumptions, we have a stronger application of the Chebotarev density theorem

Proposition 1.2.27. ([MR04, proposition 3.6.2]) Assume that T satisfies Assumptions 1.1.5 and 1.2.26. Let $C \subset H^1(K,T)$ and $D \subset H^1(K,T^*)$ be finite submodules and choose homomorphisms

$$\phi:\ C \to R, \quad \psi : D \to R$$

There exists a set $S \subset \mathcal{P}$ of positive density such that for all $\ell \in S$

$$C \cap \ker\left[\mathrm{loc}_\ell:\ H^1(K,T) \to H^1(K_\ell,T)\right] = \ker(\phi)$$
$$D \cap \ker\left[\mathrm{loc}_\ell:\ H^1(K,T^*) \to H^1(K_\ell,T^*)\right] = \ker(\psi)$$

Lemma 1.2.28. Let $\mathcal{F}$ be a cartesian Selmer structure satisfying Assumptions 1.1.5 and 1.2.26. Assume that

$$H^1_{\mathcal{F}}(\mathbb{Q},T) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some $e_1 \geq \ldots \geq e_s \in \mathbb{N}$. Then there are infinitely many primes $\ell \in \mathcal{P}_k$ such that

$$H^1_{\mathcal{F}(\ell)}(\mathbb{Q},T) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Proof. When $e_1 = \mathrm{length}(R)$, the result follows from Lemma 1.2.23. Hence we can assume without lost of generality that $e_1 < \mathrm{length}(R)$.

Similarly to the proof of Lemma 1.2.25, we can use Proposition 1.2.21 to find an auxiliary prime $q \in \mathcal{P}$ such that the localisation maps

$$\mathrm{loc}_q:\ H^1_{\mathcal{F}}(K,T) \to H^1_{\mathrm{f}}(K_q,T)[\mathfrak{m}^{e_1}], \quad \mathrm{loc}_q:\ H^1_{\mathcal{F}^*}(K,T^*) \to H^1_{\mathrm{f}}(K_q,T^*)[\mathfrak{m}^{e_1}]$$

are surjective. Hence

$$H^1_{(\mathcal{F}^*)_q}(\mathbb{Q},T^*) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Since $\chi(\mathcal{F}^q) = 1$ by Proposition 1.2.20, Proposition 1.2.16 implies that

$$H^1_{\mathcal{F}^q}(\mathbb{Q},T) \approx R \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s} \tag{1.3}$$

By Proposition 1.2.27, we can find infinitely many primes ℓ satisfying the following:

- The kernel of the localisations loc_ℓ and loc_b defined on $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)$ are the same. Following Remark 1.1.13, we can define non-canonical isomorphisms

$$H^1_{\mathrm{f}}(K_q, T^*) \cong H^1_{\mathrm{f}}(K_\ell, T^*) \cong T^*/(\tau - 1) \cong R \tag{1.4}$$

  Under this isomorphism, we can understand loc_q and loc_ℓ as elements in the dual space $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^+$. In this setting, the above condition implies that there exists a unit $u \in R^\times$ such that $\mathrm{loc}_\ell = u\mathrm{loc}_q$.

- The kernel of the finite localisation map

$$\mathrm{loc}_\ell : \ H^1_{\mathcal{F}}(K, T) \to H^1_{\mathrm{f}}(K_\ell, T)$$

  coincides with $H^1_{\mathcal{F}_q}(K, T)$. It implies that

$$H^1_{\mathcal{F}_{q\ell}}(K, T) = H^1_{\mathcal{F}_q}(K, T) \approx R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Since $\chi(\mathcal{F}^{q\ell}) = 2$ by Proposition 1.2.20, then Proposition 1.2.16 gives an isomorphism

$$H^1_{\mathcal{F}^{q\ell}}(K, T) \approx R^2 \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

By proposition 1.2.5, we can consider the following exact sequence

$$H^1_{\mathcal{F}^{q\ell}}(K, T) \longrightarrow H^1_{\mathrm{s}}(K_q, T) \oplus H^1_{\mathrm{s}}(K_\ell, T) \longrightarrow H^1_{\mathcal{F}^*}(K, T^*)^\vee$$

Dualising the isomorphisms in (1.4), we obtain an isomorphism

$$H^1_{\mathrm{s}}(K_q, T) \oplus H^1_{\mathrm{s}}(K_\ell, T) \cong R^2 \tag{1.5}$$

such that the element $(1, -u^{-1})$ belongs to the kernel of the second map. Therefore, there is an element $z \in H^1_{\mathcal{F}^{\ell b}}(\mathbb{Q}, T)$ such that $\mathrm{loc}_q(z) = 1$ and $\mathrm{loc}_\ell(z) = -u^{-1}$, under the identifications in (1.5)

It implies that the relaxed Selmer groups splits as follows.

$$H^1_{\mathcal{F}^{q\ell}}(K, T) = Rz \oplus H^1_{\mathcal{F}^q}(K, T) = Rz \oplus H^1_{\mathcal{F}^\ell}(K, T) \tag{1.6}$$

We want to show now that

$$\Pi_\ell \circ \mathrm{loc}_\ell : \ H^1_{\mathcal{F}^\ell}(K, T) \to H^1_{\mathrm{f}}(K_\ell, T)$$

where $\Pi_\ell : \ H^1(K_\ell, T) \to H^1_{\mathrm{f}}(K_\ell, T)$ is the projection of Proposition 1.1.12, is also surjective.

Indeed, let $x \in H^1_{\mathcal{F}^\ell}(K, T)$ be such that $\pi^{k-1}x \neq 0$, where π is a generator of $\mathfrak{m}$. By (1.6), there is a unique decomposition $x = \alpha z + \beta$, where $\alpha \in R$ and $\beta \in H^1_{\mathcal{F}^q}(K, T)$. Since

$$H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T) \cong R \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

then $\pi^{k-e_1}x \in H^1_{\mathcal{F}}(K, T) \subset H^1_{\mathcal{F}^q}(\mathbb{Q}, T)$ so $\alpha \in \mathfrak{m}^{e_1}$. Then $\pi^{k-1}\beta \neq 0$. By the assumptions on the prime ℓ,

$$\mathrm{loc}_\ell\big(H^1_{\mathcal{F}^q}(K, T)\big) = H^1_{\mathrm{f}}(K_\ell, T)$$

the isomorphism in (1.3) implies that $\mathrm{loc}_\ell(\beta)$ generates $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T)$. Indeed, every element of $H^1_{\mathcal{F}^q}(K, T)$ is a linear combination of β and elements of $\mathfrak{m}^{e_2}$-torsion, so loc_ℓ would only be surjective when loc_β generates the whole $H^1_{\mathrm{f}}(K_\ell, T)$.

We have that

$$(\Pi_\ell \circ \mathrm{loc}_\ell)(x) - (\Pi_\ell \circ \mathrm{loc}_\ell)(\beta) = \alpha(\Pi_\ell \circ \mathrm{loc}_\ell)(z) \in \mathfrak{m}^{e_1} H^1_{\mathrm{f}}(K_\ell, T)$$

Then $(\Pi_\ell \circ \mathrm{loc}_\ell)(x)$ also generates $H^1_{\mathrm{f}}(K_\ell, T)$ and thus

$$\Pi_\ell \circ \mathrm{loc}_\ell : \ H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k) \to H^1_{\mathrm{f}}(K_\ell, T)$$

is also surjective. Then the structure theorem over principal ideal domains implies

$$H^1_{\mathcal{F}(\ell)}(\mathbb{Q}, T/\mathfrak{m}^k) = \ker\left(\Pi_\ell \circ \mathrm{loc}_\ell : H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k) \to H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)\right) \cong R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$

□

Chapter 2

Kolyvagin systems

2.1 Kolyvagin systems and theta ideals

In this section, we outline the classical theory of Kolyvagin systems, as described in [MR04]. This theory is limited to principal coefficient rings R and core rank being equal to one.

Assumption 2.1.1. Assume, in addition to Assumption 1.1.2 that R is a principal ring, with π denoting a generator of the maximal ideal. Moreover, consider a cartesian Selmer structure of core rank $\chi(\mathcal{F}) = 1$.

Notation 2.1.2. In order to simplify the notation, we fix a generator τ_ℓ of $\mathcal{G}_\ell = \mathrm{Gal}(K(\ell)/K)$ for every Kolyvagin prime $\ell \in \mathcal{P}$. This choice fixes, by Proposition 1.1.16, an isomorphism

$$\varphi_\ell^{\mathrm{fs}} : H^1_{\mathrm{f}}(K_\ell, T) \to H^1_{\mathrm{s}}(K_\ell, T)$$

Definition 2.1.3. A *Kolyvagin system* for a Selmer structure $\mathcal{F}$

$$\kappa = \left\{ \kappa_n \in H^1_{\mathcal{F}(n)}(K, T) : \ n \in \mathcal{N} \right\}$$

satisfying the following relation for every $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$ not dividing n. By the definition of Selmer module, we have that

$$\mathrm{loc}_\ell(\kappa_n) \in H^1_{\mathcal{F}(n)}(K_\ell, T) = H^1_{\mathrm{f}}(K_\ell, T), \quad \mathrm{loc}_\ell(\kappa_{n\ell}) \in H^1_{\mathcal{F}(n\ell)}(K_\ell, T) = H^1_{\mathrm{tr}}(K_\ell, T)$$

The collection κ is a Kolyvagin system if the following is satisfied

$$\mathrm{loc}_\ell(\kappa_{n\ell}) = \phi_\ell^{\mathrm{fs}} \circ \mathrm{loc}_\ell(\kappa_n) \tag{2.1}$$

for every $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$ not dividing n.

Remark 2.1.4. The set of Kolyvagin systems has a natural structure of R-module. It will be denoted by $\mathrm{KS}(\mathcal{F})$.

Kolyvagin systems carry information about the structure of the Selmer group. The key idea is to look at the classes κ_n, where $n \in \mathcal{N}_i$ for the different non-negative integers i. The information carried by a single class κ_n is seen in its index.

Definition 2.1.5. Let M be an R-module and let $a \in M$. Consider the canonical map into the bidual module

$$\Phi : \ M \to M^{++} : a \in M \mapsto \big[\varphi \in \mathrm{Hom}(M,R) \mapsto \varphi(a)\big]$$

The *index* of a is defined as

$$\mathrm{ind}(a,M) = \mathrm{Im}(\Phi(a))$$

Remark 2.1.6. When R is a principal, local, artinian ring with maximal ideal $\mathfrak{m}$, the index of an element $a \in M$ coincides

$$\mathrm{ind}(a) = \mathfrak{m}^{\max\{j \in \mathbb{N}:\ a \in \mathfrak{m}^j M\}}$$

Notation 2.1.7. When there is no risk of confussion, we will denote $\mathrm{ind}(a)$ instead of $\mathrm{ind}(a,M)$.

We can now define the ideals Θ_i as the ideals in R generated by the indices of all κ_n where $n \in \mathcal{N}_i$.

Definition 2.1.8. Let $\kappa \in \mathrm{KS}(\mathcal{F})$. The theta ideals of κ are defined as

$$\Theta_i(\kappa) := \sum_{n \in \mathcal{N}_i} \mathrm{ind}\Big(\kappa_n, H^1_{\mathcal{F}(n)}(K,T)\Big)$$

Theorem 2.1.9. ([MR04, Theorem 4.3.3]) Under Assumption 2.1.1, $\mathrm{KS}(\mathcal{F})$ is a free, cyclic R-module.

2.2 Selmer structures of core rank 1

The generators of $\mathrm{KS}(\mathcal{F})$ are the Kolyvagin systems carrying information about the Selmer group.

Definition 2.2.1. A Kolyvagin system is said to be *primitive* if it generates $\mathrm{KS}(\mathcal{F})$ as an R-module.

We can now state the main theorem of loc. cit., which relates the theta ideals of a primitive Kolyvagin systems with the (higher) Fitting ideals of the Selmer group.

Theorem 2.2.2. ([MR04, Theorem 4.5.9]) Let R be a principal, artinian, local ring with finite residue field, and let T be an $R[[G_K]]$-module, which is free and finitely generated as R-module and unramified only at finitely many places. Let $\mathcal{F}$ be a cartesian Selmer structure on T of core rank $\chi(\mathcal{F}) = 1$. If $\kappa \in \mathrm{KS}(\mathcal{F})$ is a primitive Kolyvagin system, then

$$\Theta_i(\kappa) = \mathrm{Fitt}^R_i(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*))$$

The proof of Theorem 2.2.2 is divided in the following two lemmas:

Lemma 2.2.3. ([MR04, Corollary 4.5.4.]) Under Assumption 2.1.1, if $\kappa \in \mathrm{KS}(T)$ is a Kolyvagin system and $n \in \mathcal{N}$, then

$$\mathrm{ind}(\kappa_n) = \mathrm{Fitt}^0\big(H^1_{\mathcal{F}^*(n)}(K,T^*)\big)$$

Lemma 2.2.4. Under Assumption 2.1.1, then

$$\mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}^*}(K,T^*)\big) = \sum_{n\in\mathcal{N}_i} \mathrm{Fitt}^0\big(H^1_{(\mathcal{F}^*)(n)}(K,T^*)\big)$$

2.2.1 Proof of Lemma 2.2.4

In order to prove Lemma 2.2.4, we start by showing, for any $n \in \mathcal{N}_i$, the inclusion

$$\mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}^*(n)}(K,T^*)\big) \subset \mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$$

Consider the exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^*_n}(K,T) \longrightarrow H^1_{\mathcal{F}^*}(K,T) \longrightarrow \textstyle\prod_{\ell|n} H^1_{\mathrm{f}}\mathcal{F}^*(K,T)$$

Since all the prime divisors of n are Kolyvagin primes, the last term is isomorphic to $R^{\nu(n)}$. The description of Fitting ideals over principal rings in Proposition A.1.4 implies that

$$\mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}^*_n}(K,T)\big) \subset \mathrm{Fitt}^R_{\nu(n)}\big(H^1_{\mathcal{F}^*}(K,T)\big)$$

Since $H^1_{\mathcal{F}^*_n}(K,T) \subset H^1_{\mathcal{F}^*(n)}(K,T)$, then

$$\mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}^*(n)}(K,T)\big) \subset \mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}^*_n}(K,T)\big)$$

Combining both inclusions, we conclude the proof of this inclusion.

In order to deal with the other inclusion, we need to construct, for each $i \in \mathbb{Z}_{\geq 0}$, a vertex $n_i \in \mathcal{N}_i$ such that

$$\mathrm{Fitt}^0\big(H^1_{(\mathcal{F}^*)(n_i)}(K,T^*)\big) = \mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$$

Assume we we have a structural homomorphism

$$H^1_{\mathcal{F}}(K,T^*) \approx R^r \times R/\mathfrak{m}^{e_1} \times \cdots R/\mathfrak{m}^{e_s}$$

An inductive application of Lemma 1.2.23 (see also Remark 1.2.24) construct vertices $n_i \in \mathcal{N}_i$ such that

$$H^1_{\mathcal{F}(n_i)}(K,T) \cong R^{r-i} \times R/\mathfrak{m}^{e_1} \times \cdots R/\mathfrak{m}^{e_s} \text{ for } i \leq r$$
$$H^1_{\mathcal{F}(n_{r+j})}(K,T) \cong R/\mathfrak{m}^{e_{j+1}} \times \cdots R/\mathfrak{m}^{e_s} \text{ for } j \geq 1$$

This proves the other inclusion, what concludes the proof of this lemma.

2.3 Selmer structures of rank 0

When $\mathcal{F}$ is a cartesian Selmer structure of core rank 0, we cannot apply the argument above since the only Kolyvagin system is the trivial one.

Theorem 2.3.1. ([MR04, Theorem 4.2.2]) Let $\mathcal{F}$ be a cartesian Selmer structure such that $\chi(\mathcal{F}) = 0$. Then $\mathrm{KS}(\mathcal{F}) = 0$.

The method we will use for the computation of the Selmer module $H^1_{\mathcal{F}}(K,T)$ involves considering an auxiliary Selmer structure $\mathcal{G} \geq \mathcal{F}$, also cartesian, such that $\chi(\mathcal{G}) = 1$. One can show that $\mathcal{F}$ and $\mathcal{G}$ only differ in one local condition.

Proposition 2.3.2. There exists a unique prime ℓ such that $H^1_{\mathcal{F}}(K_q,T) \subsetneq H^1_{\mathcal{G}}(K_q,T)$. Moreover, there is a non-canonical homomorphism

$$H^1_{\mathcal{G}/\mathcal{F}}(K_q,T) := H^1_{\mathcal{G}}(K_q,T) \,/\, H^1_{\mathcal{F}}(K_q,T) \approx R$$

Proof. By Proposition 1.2.5, there is an global-duality exact sequence for $\overline{T} := T \otimes k$

$$H^1_{\mathcal{F}}(K,\overline{T}) \lhook\joinrel\longrightarrow H^1_{\mathcal{G}}(K,\overline{T}) \longrightarrow \bigoplus_{q\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_q,\overline{T})}{H^1_{\mathcal{F}}(K_q,\overline{T})} \longrightarrow H^1_{\mathcal{G}}(K,\overline{T}^*)^\vee \twoheadrightarrow H^1_{\mathcal{F}}(K,\overline{T}^*)^\vee$$

Since $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$, Definition 1.2.14 and dimension counting implies that

$$\dim_k \left(\bigoplus_{q\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_q,\overline{T})}{H^1_{\mathcal{F}}(K_q,\overline{T})} \right) = 1$$

Therefore, there exists a unique prime ℓ such that $H^1_{\mathcal{F}}(K_\ell,\overline{T}) \subsetneq H^1_{\mathcal{G}}(K_\ell,\overline{T})$. Hence $H^1_{\mathcal{F}}(K_\ell,T) \subsetneq H^1_{\mathcal{G}}(K_\ell,T)$.

For all other primes $q \neq \ell$, we can apply [MR04, Lemma 1.1.5], which says that for every pair of cartesian Selmer structures $\mathcal{F}$ and $\mathcal{G}$, the quantity

$$\mathrm{length}\big(H^1_{\mathcal{G}}(K_q,T\otimes R/\mathfrak{m}^i)\big) - \mathrm{length}\big(H^1_{\mathcal{F}}(K_q,T\otimes R/\mathfrak{m}^i)\big) \tag{2.2}$$

is linearly dependent on i. Since it vanishes for $i = 1$, then $H^1_{\mathcal{F}}(K_q,T) = H^1_{\mathcal{G}}(K_q,T)$.

For the prime ℓ, [MR04, Lemma 1.1.5] implies that

$$\mathrm{length}\big(H^1_{\mathcal{G}/\mathcal{F}}(K_q,T)\big) = \mathrm{length}(R) \tag{2.3}$$

Consider he following composition, which coincides with the multiplication by π^{k-1}.

$$H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T) \longrightarrow H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T\otimes k) \xrightarrow{\pi^{k-1}} H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T)$$

The first map is surjective by the propagation of Selmer structures and the second one is injective since $\mathcal{F}$ is cartesian. By the induction hypothesis, $H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T)$ is an R of length k whose $\mathfrak{m}^{k-1}$-torsion induces a non-trivial quptient. Hence, the structure theorem implies that

$$H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T) \cong R$$

□

Remark 2.3.3. If we choose a Kolyvagin prime, or any other prime ℓ such that $H^1_{/\mathcal{F}}(K_\ell, T) \cong R$, the Selmer structure $\mathcal{G} = \mathcal{F}^\ell$ is cartesian with $\chi(\mathcal{F}^\ell) = 1$.

Now, we describe a process in which Kolyvagin systems for $\mathcal{G}$ describe the Selmer module $H^1_{\mathcal{F}}(K, T)$. In order to do that, we need to localise the Kolyvagin systems at the prime at which $\mathcal{F}$ and $\mathcal{G}$ differ.

Definition 2.3.4. Let $\mathcal{F} \leq \mathcal{G}$ be two Selmer structures with $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$ differing at the prime ℓ and let $\kappa \in \mathrm{KS}(\mathcal{G})$. Define the quantities δ associated to κ by

$$\delta_n(\kappa, \mathcal{F}) := \mathrm{loc}_\ell(\kappa_n) \in H^1_{\mathcal{G}}(K_\ell, T) \,/\, H^1_{\mathcal{F}}(K_\ell, T) \ \forall n \in \mathcal{N}$$

The quantities δ_n can be used to define the Θ ideals of rank 0.

Definition 2.3.5. Let $\mathcal{F} \leq \mathcal{G}$ be two Selmer structures such that $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$ differing at the prime ℓ and let $\kappa \in \mathrm{KS}(\mathcal{G})$. We can define the ideals of R

$$\Theta^{(0)}_i(\kappa, \mathcal{F}) := \sum_{n \in \mathcal{N}_i} \mathrm{ind}\Big(\delta_n(\kappa, \mathcal{F}), H^1_{\mathcal{G}/\mathcal{F}}(K_\ell, T)\Big)$$

The comparison between the ideals $\Theta^{(0)}_i(\kappa, \mathcal{F})$ and the Fitting ideals of $H^1_{\mathcal{F}}(K, T)$ leads to the first main result of this thesis.

Theorem 2.3.6. Let R be a principal, artinian, local ring with finite residue field, let T be an $R[[G_K]]$-module, unramified only at finitely many places which is free and finitely generated as an R-module. Assume $\mathcal{F} \leq \mathcal{G}$ are cartesian Selmer structures on T satisfying that $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$. If $\kappa \in \mathrm{KS}(\mathcal{G})$ is a primitive Kolyvagin system, then

$$\Theta^{(0)}_i(\kappa, \mathcal{F}) \subset \mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}}(K, T)\big) \ \forall i \in \mathbb{Z}_{\geq 0} \tag{2.4}$$

Moreover, if one of the following conditions is satisfied

(i) $i \leq \dim_k\Big(H^1_{\mathcal{F}}(K, T) \Big/ H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^{k-1}]\Big) =: r$

(ii) $\Theta^{(0)}_{i-1}(\kappa, \mathcal{F}) \subsetneq \mathrm{Fitt}^R_{i-1}\big(H^1_{\mathcal{F}}(K, T)\big)$

(iii) There is some $k \in \mathbb{N}$ and some $n \in \mathcal{N}$ such that $\nu(n) = i - 1$, $\Theta_{i-1}(\kappa) = \delta_n R$ and

$$H^1_{\mathcal{F}(n)}(\mathbb{Q}, T) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some $e_1 > e_2 \geq \cdots \geq e_s$.

then the equality $\Theta^{(0)}_i(\kappa, \mathcal{F}) = \mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}}(\mathbb{Q}, T)\big)$ holds.

Similarly to the results in §2.1, the proof is divided in the following lemmas, which will be proven in the next subsections.

Lemma 2.3.7. If $\kappa \in \mathrm{KS}(\mathcal{G})$ is a primitive Kolyvagin system and $n \in \mathcal{N}$, then

$$\mathrm{ind}(\delta_n) = \mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}(n)}(K, T)\big)$$

Lemma 2.3.8. If $\mathcal{F}$ is a cartesian

$$\sum_{n\in\mathcal{N}_i} \mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*(n)}(K,T^*)\big) \subset \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$$

Proof. Analogous to the similar inclusion in Lemma 2.2.4. □

In order to prove the other inclusion, whenever it holds, we will construct a vertex $n_i \in \mathcal{N}_i$ such that

$$\mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*(n_i)}(K,T^*)\big) = \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$$

Note that the equality holds trivially when $i < r$, since $\mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$ vanishes. For $i = r$, the equality is proven in the following lemma.

Lemma 2.3.9. There exists some vertex $n_r \in \mathcal{N}_r$ such that

$$\mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*(n_r)}(K,T)\big) = \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(K,T)\big)$$

Lemma 2.3.9 completes the proof of the equality $\Theta_i^{(0)}(\kappa,\mathcal{F}) = \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(\mathbb{Q},T)\big)$ under assumption (i).

Note that Lemma 2.3.9 determines the structure of the modified Selmer group. Indeed, assume there is a structural homomorphism

$$H^1_{\mathcal{F}}(K,T) \approx R^r \times R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some exponents $e_1 \geq \cdots \geq e_s$, all being at most $k-1$. Then there is an homomorphism

$$H^1_{\mathcal{F}(n_r)}(K,T) \approx R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

We can extend this construction to higher values of i.

Lemma 2.3.10. For every $j \geq 0$, we can either construct a vertex

- $n_{r+j} \in \mathcal{N}_{r+j}$ such that $H^1_{\mathcal{F}(n_{r+j})}(K,T) \cong R/\mathfrak{m}^{e_{j+1}} \times \cdots \times R/\mathfrak{m}^{e_s}$.
- $n_{r+j+1} \in \mathcal{N}_{r+j+1}$ such that $H^1_{\mathcal{F}(n_{r+j+1})}(K,T) \cong R/\mathfrak{m}^{e_{j+1}} \times \cdots \times R/\mathfrak{m}^{e_s}$.

Note that such vertices guarantee the equality in Theorem 2.3.6 for their respective indices.

Corollary 2.3.11. For the indices $k \geq 0$ such that there exists an element $n_r \in \mathcal{N}_r$ as in Lemma 2.3.10, there is an equality

$$\sum_{n\in\mathcal{N}_{r+k}} \mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*(n)}(K,T^*)\big) \subset \mathrm{Fitt}_{r+k}^R\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$$

Corollary 2.3.11 proves the equality $\Theta_i^{(0)}(\kappa,\mathcal{F}) = \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(\mathbb{Q},T)\big)$ under assumption (i). Indeed, if such equality does not hold for some index $i-1 = r+j-1$, the vertex n_{r+j-1} in Lemma 2.3.10 cannot be constructed. Hence, Lemma 2.3.10 guarantees the existence of the vertex n_{r+j}, which proves the equality for the index $i = r+j$ by Corollary 2.3.11.

This concludes the proof of Theorem 2.3.6. The inclusion is a direct consequence of Lemmas 2.3.7 and 2.3.8. Lemma 2.3.9 and Corollary 2.3.11 proves the equality under the first or second assumption. If we are in the situation of the third assumption for some index $i-1 = r+j-1$, the proof of Lemma 2.3.10 shows that we can construct the vertex $n_{r+j} \in \mathcal{N}_{r+j}$ satisfying that

$$H^1_{\mathcal{F}(n_{r+j})}(K,T) \cong R/\mathfrak{m}^{e_{j+1}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

This construction proves the equality for the index $i = r+j$.

Theorem 2.3.6 requires $\mathcal{G}$ to be a primitive Kolyvagin system. This fact can also be checked from the quantities δ_n.

Theorem 2.3.12. Let R be a principal, artinian, local ring with finite residue field, let T be an $R[[G_K]]$-module, unramified only at finitely many places which is free and finitely generated as an R-module. Assume $\mathcal{F} \leq \mathcal{G}$ are cartesian Selmer structures on T satisfying that $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$. If $\kappa \in KS(\mathcal{G})$, then κ is primitive if and only if there is $n \in \mathcal{N}$ such that

$$\mathrm{ind}\big(\delta_n(\kappa,\mathcal{F}), H^1_{\mathcal{G}/\mathcal{F}}(K,T)\big) = R$$

Proof. If κ is not primitive, there is a primitive Kolyvagin systems κ' such that $\kappa = a\kappa'$ and $a \in R \setminus R^\times$. Then

$$\mathrm{ind}\big(\delta_n(\kappa,\mathcal{F})\big) = (a)\,\mathrm{ind}\big(\delta_n(\kappa',\mathcal{F})\big) \subset aR$$

Conversely, if κ is primitive, Lemma 2.3.7 reduces the proof to finding some $n \in \mathcal{N}$ such that

$$H^1_{\mathcal{F}(n)}(K,T) = 0$$

By Proposition 1.2.13, this is equivalent to

$$H^1_{\mathcal{F}(n)}(K, T\otimes k) = 0$$

Such $n \in \mathbb{N}$ can be obtained by an inductive application of Lemma 1.2.23 on the k representation $T \otimes k$. □

2.3.1 Proof of Lemma 2.3.7

The proof of Lemma 2.3.7 involves comparing the indices of κ_n and δ_n, so we can then apply Lemma 2.2.3.

Lemma 2.3.13. For every $n \in \mathcal{N}$, let

$$C_n := \mathrm{coker}\left(\mathrm{loc}_\ell :\ H^1_{\mathcal{G}}(K,T) \to H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T)\right)$$

Then $\mathrm{ind}(\delta_n) = \mathrm{ind}(\kappa_n)\cdot \mathrm{Fitt}^{(0)}(C_n)$.

Proof. Note that Proposition 1.2.16 and Proposition 1.2.20 implies the existence of a non-canonical isomorphism

$$H^1_{\mathcal{G}(n)}(K,T) \approx R \oplus H^1_{\mathcal{G}^*(n)}(K,T^*) \tag{2.5}$$

Let (x_n, y_n) be the components of κ_n under this identification. By Lemma 2.2.3, $\mathrm{ind}(\kappa_n) = \mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*}(K,T^*)\big)$, then $y_n = 0$ and x_n is a generator of $\mathrm{ind}(\kappa_n)$. The decomposition in (2.5) induces a map in R^+ defined by

$$R \longrightarrow H^1_{\mathcal{G}}(K,T) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathcal{G}/\mathcal{F}}(K_\ell,T) \longrightarrow R$$

The composite map is the multiplication by some $a \in R$, which is also a generator of $\mathrm{Fitt}^0(C_n)$. Therefore,

$$\mathrm{ind}(\delta_n) = \mathrm{ind}(\kappa_n)\mathrm{Fitt}_0^R(C_n)$$

□

Proof of Lemma 2.3.7. The exact sequence in Proposition 1.2.5 induces a short exact sequence

$$0 \longrightarrow C_n \longrightarrow H^1_{\mathcal{F}^*(n)}(K,T)^\vee \longrightarrow H^1_{\mathcal{G}^*(n)}(K,T)^\vee \longrightarrow 0$$

We then have the identity of Fitting ideals

$$\mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*(n)}(K,T)\big) = \mathrm{Fitt}_0^R\big(C_n\big)\mathrm{Fitt}_0^R\big(H^1_{\mathcal{G}^*(n)}(K,T)\big) = \mathrm{Fitt}_0^R\big(C_n\big)\,\mathrm{ind}(\kappa_n) = \mathrm{ind}(\delta_n)$$

where the second inequality follows from Lemma 2.2.3 and the last one from Lemma 2.3.13. □

2.3.2 Proof of Lemma 2.3.9

The proof is obtained as an inductive application of Lemma 1.2.23. By the structure theorem of finitely generated R-modules, and the definition of core rank, there are non-canonical homomorphisms

$$H^1_{\mathcal{F}}(K,T) = H^1_{\mathcal{F}^*}(K,T^*) = R^r \times R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

We will construct inductively a vertex $n_i \in \mathcal{N}_i$, where $i \leq r$, such that

$$H^1_{\mathcal{F}(n_i)}(K,T) \approx H^1_{\mathcal{F}^(n_i)}(K,T^*) \approx R^{r-i} \times R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Indeed, assume we have constructed $n_i \in \mathcal{N}_i$ for some $i \leq r-1$. Clearly, $H^1_{\mathcal{F}(n_i)}(K,T)$ contains a submodule isomorphic to R, so Lemma 1.2.23 implies the existence of a prime ℓ_{i+1} such that for $n_{i+1} = n_i\ell_{i+1}$, we get that

$$H^1_{\mathcal{F}^(n_{i+1})}(K,T^*) \approx R^{r-(i+1)} \times R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

Since $\chi(\mathcal{F}) = 0$, there is a non-canonical homomorphism

$$H^1_{\mathcal{F}(n_{i+1})}(K,T) \approx H^1_{\mathcal{F}^*(n_{i+1})}(K,T^*) \approx R^{r-(i+1)} \times R/\mathfrak{m}^{e_1} \times \cdots \times R/\mathfrak{m}^{e_s}$$

2.3.3 Proof of Lemma 2.3.10

Note that the element $n_r \in \mathcal{N}_r$ was already constructed in Lemma 2.3.9. An inductive application of Lemma 1.2.25, implies the existence of an element $n_{r+j} \in \mathcal{N}_{r+j}$ such that

$$H^1_{\mathcal{F}(n_{r+j})}(K,T) \approx H^1_{\mathcal{F}^*(n_{r+j})}(K,T^*) \approx R/\mathfrak{m}^{t_{j+1}} \times R/\mathfrak{m}^{e_{j+2}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

where $t_{j+1} \geq e_{j+1}$. We assume that we construct this elements minimising the exponents t_{j+1} in every step.

For an index j, if $t_{j+1} = e_{j+1}$, then the element $n_{r+j} \in \mathcal{N}_{r+j}$ satisfy the hypothesis of Lemma 2.3.10.

Otherwise, if $t_{j+1} > e_{j+1}$, then $t_{j+1} > e_{j+2}$ as well , so the last remark in Lemma 1.2.25 guarantees the existence of a prime ℓ_{r+j+1} such that, when $n_{r+j+1} = n_{r+j}\ell_{r+j+1}$, the exponent t_{j+2} coincides with e_{j+2}. By the minimality assumption on t_{j+2}, we know that

$$H^1_{\mathcal{F}(n_{r+j+1})}(K,T) \approx H^1_{\mathcal{F}^*(n_{r+j+1})}(K,T^*) \approx R/\mathfrak{m}^{e_{j+2}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

2.4 Non-self dual Galois representations of rank 0

This section is devoted to the computation of the Fitting ideals of a Selmer module $H^1_{\mathcal{F}}(K,T)$ of a cartesian Selmer structure of core rank $\chi(\mathcal{F}) = 0$, defined over a Galois representation T satisfying Assumptions 1.2.26.

Theorem 2.4.1. Let R be a principal, artinian, local ring with finite residue field, let T be an $R[[G_K]]$-module unramified only at finitely many places, and let $\mathcal{F} \leq \mathcal{G}$ be a cartesian Selmer structures on T satisfying Assumptions 1.2.26 and $\chi(\mathcal{G}) = 1$. If $\kappa \in \mathrm{KS}(\mathcal{G})$ is a primitive Kolyvagin system, then

$$\Theta^{(0)}_i(\kappa,\mathcal{F}) = \mathrm{Fitt}^R_i(H^1_{\mathcal{F}}(K,T))$$

Note that the inclusion

$$\Theta^{(0)}_i(\kappa,\mathcal{F}) \subset \mathrm{Fitt}^R_i(H^1_{\mathcal{F}}(K,T))$$

is proven by theorem 2.3.6. In addition, Lemma 2.3.7 reduce the proof of the other inclusion to the following lemma.

Lemma 2.4.2. For every $i \in \mathbb{Z}_{\geq 0}$, there exists some vertex $n_i \in \mathcal{N}_i$ such that

$$\mathrm{Fitt}^R_0\big(H^1_{\mathcal{F}^*(n_i)}(K,T)\big) = \mathrm{Fitt}^R_i\big(H^1_{\mathcal{F}}(K,T)\big)$$

Proof. Assume we we have a structural homomorphism

$$H^1_{\mathcal{F}}(K,T^*) \approx R^r \times R/\mathfrak{m}^{e_1} \times \cdots R/\mathfrak{m}^{e_s}$$

An inductive application of Lemma 1.2.28 (see also Remark 1.2.24) construct vertices $n_i \in \mathcal{N}_i$ such that

$$H^1_{\mathcal{F}(n_i)}(K,T) \cong R^{r-i} \times R/\mathfrak{m}^{e_1} \times \cdots R/\mathfrak{m}^{e_s} \text{ for } i \leq r$$
$$H^1_{\mathcal{F}(n_{r+j})}(K,T) \cong R/\mathfrak{m}^{e_{j+1}} \times \cdots R/\mathfrak{m}^{e_s} \text{ for } j \geq 1$$

This proves the other inclusion, what concludes the proof of this lemma.

□

2.5 Selmer groups over discrete valuation rings

this section has not been written yet. These are materials from the paper

Remark 2.5.1. Assume either

- R is a discrete valuation ring.
- length$(R) \geq$ length $\left(H^1_{\mathcal{F}}(\mathbb{Q},T)_{\text{tors}}\right)$.

Then $\text{rank}_R(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee)$ is the minimal i such that $\Theta_i \neq 0$.

Provided that we know the ideals $\Theta_i(\kappa)$, theorem **??** determines the Fitting ideals of the dual Selmer group

Corollary 2.5.2. Assume R is a discrete valuation ring and write $\Theta_i(\kappa) = \mathfrak{m}^{n_i}$. Then

$$\text{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee\right) = \mathfrak{m}^{\min\left\{n_i, \frac{n_{i+1}+n_{i-1}}{2}\right\}}$$

Proof. Write $\text{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee\right) = \mathfrak{m}^{m_i}$, so the inequality in theorem **??** implies that $n_i \geq m_i$. By the structure theorem of finitely generated modules over principal ideal domains, the following inequality holds for $i \in \mathbb{N}$:

$$m_{i+1} - m_i \geq m_i - m_{i-1}$$

Hence the index m_i can be upper bounded using m_{i-1} and m_{i+1}:

$$m_i \leq \frac{m_{i+1}+m_{i-1}}{2} \tag{2.6}$$

Assume that $n_i = m_i$. Then

$$m_i \leq \frac{m_{i+1}+m_{i-1}}{2} \leq \frac{n_{i+1}+n_{i-1}}{2} \Rightarrow m_i = \min\left\{n_i, \frac{n_{i+1}+n_{i-1}}{2}\right\}$$

Assume that $n_i > m_i$. Theorem **??** can be applied to $i+1$. Since condition (ii) in this theorem holds by our assumption, we obtain that $m_{i+1} = n_{i+1}$. On the other hang, assume by contradiction that $n_{i-1} > m_{i-1}$. In this case, theorem **??**, would imply that $n_i = m_i$, contradicting our assumption. Therefore, $n_{i-1} = m_{i-1}$. Moreover, condition

(iii) in theorem **??** cannot be satisfied since, otherwise, our assumption would not be true. Hence, the equality holds in equation (2.6) and we obtain

$$m_i = \frac{m_{i+1} + m_{i-1}}{2} = \frac{n_{i+1} + n_{i-1}}{2} = \min\left\{n_i, \frac{n_{i+1} + n_{i-1}}{2}\right\}$$

□

Under those assumptions, the following improvement of theorem **??** is true. Sakamoto proves the equality (**??**) below under stronger assumptions when the coefficient ring R is a Gorenstein ring of dimension zero. In particular, R. Sakamoto's result only worked when $H^1_{\mathcal{F}}(\mathbb{Q}, T) = 0$. However, when R is a principal ring, we can weaken the assumptions to obtain the following result.

Chapter 3

Patched Cohomology

3.1 Ultrafilters

3.1.1 Definition

Definition 3.1.1. A *filter* in the natural numbers is a collection of sets $\mathcal{U}$ in in the power set $\mathcal{P}(\mathbb{N})$ such that

- (F0) The empty set does not belong to $\mathcal{U}$.
- (F1) If $S_1 \subset S_2$ and $S_1 \in \mathcal{U}$, then $S_2 \in \mathcal{U}$.
- (F2) If $S_1, S_2 \in \mathcal{U}$, then $S_1 \cap S_2 \in \mathcal{U}$.

We say that a filter is an *ultrafilter* if it also satisfies the following condition

- (UF) For every set $S \in \mathcal{P}(\mathbb{N})$, either $S \in \mathcal{U}$ or $\mathbb{N} \setminus S \in \mathcal{U}$.

The key property of ultrafilters is that (UF) generalises to finite partitions, i.e., ultrafilters contain exactly one set in every finite partion of $\mathbb{N}$.

Proposition 3.1.2. Let $\mathcal{U}$ be an ultrafilter and let $\{P_1, \dots, P_s\}$ be a partition of $\mathbb{N}$. Then there exists a unique i such that $P_i \in \mathcal{U}$.

Proof. It follows from an inductive application of (UF). □

Last proposition can be reinterpreted in the following form:

Corollary 3.1.3. ([Swe22, proposition 2.1.2]) Let $\mathcal{U}$ be an ultrafilter, let $S \in \mathcal{U}$ and let C be a finite set. For every map $f:\ S \to C$, there exists a unique $c \in C$ such that $f^{-1}(c) \in \mathcal{U}$.

The only ultrafilters we can explicitly describe are those formed by the subsets of the naturals containing one specific element, known as principal ultrafilters.

Definition 3.1.4. Let $a \in \mathbb{N}$. The collection of sets

$$\mathcal{U}_a = \{S \subset \mathbb{N} :\ a \in S\}$$

is an ultrafilter. These are known as *principal ultrafilters*.

In fact, principal ultrafilters are the only ones containing finite sets.

Proposition 3.1.5. Let $\mathcal{U}$ be an ultrafilter and assume there is a finite set S that belongs to $\mathcal{U}$. Then there exists an element $a \in S$ such that $\mathcal{U} = \mathcal{U}_a$.

Proof. Consider the finite union

$$\mathbb{N} = (\mathbb{N} \setminus S) \cup \bigcup_{a \in S} \{a\}$$

By proposition 3.1.2, one of the above sets belong to $\mathcal{U}$. Since $(\mathbb{N} \setminus S)$ does not, there is some $a \in S$ such that $\{a\} \in \mathcal{U}$. By (F2), $\mathcal{U}_a \in \mathcal{U}$.

In order to show the equality, assume there exists $T \in \mathcal{U} \setminus \mathcal{U}_a$. Then $T \cap \{a\} = \emptyset \in \mathcal{U}$, contradicting (F0). Therefore, $\mathcal{U} = \mathcal{U}_a$. □

However, those ultrafilters which are interesting for our purposes are the non-principal ones. Although they cannot be explicitly constructed, its existence is guaranteed, assuming the axiom of choice, by the analogy between ultrafilters and maximal ideals shown in Proposition 3.1.10 below. They are those ultrafilters containing the Fréchet filter consisting of sets with finite complement.

Definition 3.1.6. The *Fréchet filter* is the collection of subsets of the natural number defined as

$$\mathcal{F} = \{S \subset \mathbb{N} : \ \mathbb{N} \setminus S \text{ finite}\}$$

3.1.2 Analogy between ultrafilters and ideals

The set $\mathbb{P}(\mathbb{N})$ can be endowed with a natural structure of a boolean ring. In order to do that, we define a set-theoretic bijection to the functions on the naturals with values on the finite field with two elements $\mathbb{F}_2$:

$$\mathbb{P}(\mathbb{N}) \to \mathcal{C}(\mathbb{N}, \mathbb{F}_2) : \ A \mapsto 1 - \chi_A$$

where χ_A is the characteristic function. The natural boolean structure in $\mathcal{C}(\mathbb{N}, \mathbb{F}_2)$ induces, via the above bijection, a boolean ring structure in $Pb(\mathbb{N})$. It is possible to explicitly describe the operations in $\mathbb{P}(\mathbb{N})$.

Definition 3.1.7. The *filtered* boolean structure $\mathcal{B}(\mathbb{N})$ in $\mathbb{P}(\mathbb{N})$ is given by the operations

$$A + B = (A \cap B) \cup (A^c \cap B^c), \quad A \cdot B = (A \cup B)$$

where S^c denotes the complementary set and Δ denotes the symmetric difference.

Remark 3.1.8. The boolean ring structure in 3.1.7 is not the standard one in the literature, but it is the conjugation by the involution obtained by sending each set to its complementary.

We can now identify filters and ultrafilters with ideals and maximal ideals[1].

Proposition 3.1.9. The filters coincides with the ideals in the boolean ring in $\mathbb{P}(\mathbb{N})$ which are different to 1.

[1] With the standard convention, filters (resp. ultrafilters) are the set of complements of ideals (resp. maximal ideals)

Proof. Let $\mathcal{F}$ be a filter in $\mathbb{P}(\mathbb{N})$ and let $A, B \in \mathcal{F}$. Then

$$A + B = (A \cap B) \cup (A^c \cap B^c) \supset A \cap B \in \mathcal{F}$$

by (F1). Therefore, $A + B \in \mathcal{F}$ by (F2). If $T \subset N$, then

$$A \cdot T = A \cup T \supset A \in \mathcal{F}$$

by (F2). Finally, (F0) implies that $\mathcal{F}$ is not the full $\mathcal{P}(\mathcal{N})$.

Conversely, assume $\mathcal{F}$ is an ideal strictly contained in $\mathbb{P}(\mathbb{N})$. Since the unit element in $\mathbb{P}(\mathbb{N})$ is the empty set, then (F0) needs to hold. Assume that $S \in \mathcal{F}$ and $S \subset T$, then $T = S \cdot T$, so it belongs to $\mathcal{F}$, which proves (F2). Finally, if $A, B \in \mathcal{F}$, then

$$A \cap B \subset (A \cap B) \cup (A^c \cap B^c) = A + B \in \mathcal{F}$$

Then $A \cap B = (A + B) \cdot (A \cap B)$, so (F1) holds. □

Proposition 3.1.10. The ultrafilters in $\mathbb{P}(\mathbb{N})$ are exactly the maximal ideals of $\mathcal{B}(\mathbb{N})$.

Proof. Let $\mathcal{U}$ be an ultrafilter. By Proposition 3.1.9, $\mathcal{U}$ is an ideal of $\mathcal{B}(\mathbb{N})$. Let $A = \mathbb{P}(\mathbb{N})/\mathcal{U}$ be its quotient ring. Note that, for any $S \subset \mathbb{N}$, then either $S \in \mathcal{U}$ or

$$S = \emptyset + S^c \in \emptyset + \mathcal{U}$$

because $S^c \in \mathcal{U}$ by (UF). Hence A is the ring with two elements, so its a field and hence $\mathcal{U}$ is a maximal ideal.

Conversely, assume $\mathcal{U}$ is a maximal ideal, so $A = \mathbb{P}(\mathbb{N})/\mathcal{U}$ is a boolean field. Then $A = \mathbb{F}_2$ since every element is a root of $x(x-1)$. Then, for any $S \subset \mathbb{N}$, either $S \in \mathcal{U}$ or $1 + S \in \mathcal{U}$. This is equivalent to (UF) since $1 + S = \emptyset + S = S^c$. □

3.1.3 Ultraproducts

In this section, we will use the concept of ultrafilters to patch sequences of sets.

Definition 3.1.11. Let $\mathcal{U}$ be an ultrafilter and let $(M_n)_{n\in\mathbb{N}} \in \mathcal{C}^{\mathbb{N}}$. The *ultraproduct* $\mathcal{U}(M_n)$ is defined as

$$\mathcal{U}(M_n) = \prod_{n\in\mathbb{N}} M_n \Big/ \sim$$

where $\sim$ is the equivalence relation defined as $(m_n) \sim (m'_n)$ if $m_n = m'_n$ for $\mathcal{U}$-many n.

Proposition 3.1.12. (Functoriality of the ultraproduct, [Swe22, Proposition 2.1.4]) The ultraproduct $\mathcal{U}$ defines a functor $\mathcal{C}^{\mathbb{N}} \to \mathcal{C}$.

Proof. Let $\varphi : (A_n) \to (B_n)$ be a morphism in $\mathcal{C}^{\mathbb{N}}$. By definition, φ is a collection of morphisms $\varphi_i : A_i \to B_i$. Their product induces a morphism

$$\overline{\varphi} = \prod_{n\in\mathbb{N}} \varphi_n : \prod_{n\in\mathbb{N}} A_n \to \prod_{n\in\mathbb{N}} B_n$$

This product morphism restricts well to the ultraproduct, resulting in a map

$$\varphi^{\mathcal{U}} : \mathcal{U}(A_n) \to \mathcal{U}(B_n)$$

Indeed, if $(\alpha_i), (\alpha_i') \in \prod_{n\in\mathbb{N}} A_n$ are two equivalent sequences, then $\alpha_i = \alpha_i'$ for $\mathcal{U}$-many i. Then $\varphi(\alpha_i) = \varphi(\alpha_i')$ for $\mathcal{U}$-many i. It implies that $\overline{\varphi}(\alpha_i)$ and $\overline{\varphi}(\alpha_i')$ are equivalent sequences in $\prod_{n\in\mathbb{N}} B_n$. Hence, $\varphi^{\mathcal{U}}$ is well defined and, since it clearly behaves well with the composition, the ultraproduct is functorial. □

The ultraproduct also behave well with direct products.

Proposition 3.1.13. If (A_n) and (B_n) are sequences of sets, modules or rings, there is a canonical identification

$$\mathcal{U}(A_n \times B_n) = \mathcal{U}(A_n) \times \mathcal{U}(B_n)$$

Proof. The canonical map

$$\prod_{n\in\mathbb{N}} A_n \times B_n \to \left(\prod_{n\in\mathbb{N}} A_n\right) \times \prod_{n\in\mathbb{N}} B_n,\ (a_n, b_n)_{n\in\mathbb{N}} \mapsto \left[(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}\right]$$

respects the equivalence relation given by the ultrafilter. Indeed, if two sequences $\{(a_n, b_n)\}_{n\in\mathbb{N}}$ and $\{(a_n', b_n')\}_{n\in\mathbb{N}}$ are equivalent, the set

$$S := \{n \in \mathbb{N} : \ (a_n, b_n) = (a_n', b_n')\} \in \mathcal{U}$$

Therefore, by (F2),

$$S_a = \{n \in \mathbb{N} : \ a_n = a_n'\} \in \mathcal{U}$$

since it contains S. Hence (a_n) is equivalent to (a_n'). Similarly, (b_n) and (b_n') are also equivalent. Then the map $\mathcal{U}(A_n \times B_n) \to \mathcal{U}(A_n) \times \mathcal{U}(B_n)$ is well defined.

Conversely, if we have two pair of equivalent sequences (a_n) and (a_n'), and (b_n) and (b_n'). We denote by S_a and S_b the set of indices in which they coincide, then

$$\{n \in \mathbb{N} : (a_n, b_n) = (a_n', b_n')\} = S_a \cap \S_b \in \mathcal{U}$$

by (F1). Then (a_n, b_n) and (a_n', b_n') are two equivalent sequences in $(A_n \times B_n)$, so the inverse map $\mathcal{U}(A_n) \times \mathcal{U}(B_n) \to \mathcal{U}(A_n \times B_n)$ is also well defined. □

The behavior of the ultrafilter with the Hom functor is not as satisfying, since we only get an injective map.

Proposition 3.1.14. Let A_n, B_n be two sequences in $\mathcal{C}^{\mathbb{N}}$. Then there is an injection

$$\Psi : \mathcal{U}(\mathrm{Hom}(A_n, B_n)) \hookrightarrow \mathrm{Hom}\big(\mathcal{U}(A_n), \mathcal{U}(B_n)\big)$$

Proof. Let (φ_n) be the sequence representing an element in $\mathcal{U}(\mathrm{Hom}(A_n, B_n))$ and let (a_n) be a sequence representing an element in B_n. We assign the sequence $\varphi_n(a_n) \in \mathcal{U}(B_n)$. Clearly, this assignment behaves well under the ultrafilter equivalences in both $\mathcal{U}(\mathrm{Hom}(A_n, B_n))$ and $\mathcal{U}(A_n)$, so it defines a map

$$\Psi : \mathcal{U}(\mathrm{Hom}(A_n, B_n)) \to \mathrm{Hom}\big(\mathcal{U}(A_n), \mathcal{U}(B_n)\big)$$

In order to check injectivity, consider another sequence (ψ_n) induces the same element in $\mathrm{Hom}\big(\mathcal{U}(A_n), \mathcal{U}(B_n)\big)$. For the sake of contradiction, assume that (φ_n) and (ψ_n) are not equivalent, i.e., the set

$$S = \{n \in \mathbb{N} : \ \varphi_n \neq \psi_n\} \in \mathcal{U}$$

Choose a sequence $(a_n) \in (A_n)$ where $\varphi_n(a_n) \neq \psi_n(a_n)$ for every $n \in S$. Hence $(\varphi_n(a_n))$ and $(\psi_n(a_n))$ represent different elements in $\mathcal{U}(B_n)$, so $\Psi(\varphi_n) \neq \Psi(\psi_n)$. □

Notation 3.1.15. If M is a set, we will denote by $\mathcal{U}(M)$ to the ultraproduct of the sequence (M_n) in which $M_n = M$ for all n.

Remark 3.1.16. If M_n have some extra structure such as pointed sets, groups or rings, the ultraproduct $\mathcal{U}(M_n)$ would also be endowed with such structure.

Proposition 3.1.17. ([Swe22, proposition 2.1.5]) Assume $\mathcal{C}$ is a category of pointed sets. Then the ultraproduct $\mathcal{U}$ is an exact functor.

Proof. We will denote by 0 the distinguished point in every object of $\mathcal{C}$. Assume we have an exact sequence in $\mathcal{C}^{\mathbb{N}}$,

$$0 \longrightarrow (A_n) \xrightarrow{\overline{\mu}} B_n \xrightarrow{\overline{\varepsilon}} C_n \xrightarrow{0} 0$$

We start by showing the injectivity of $\mu^{\mathcal{U}}$. Let $\alpha = (\alpha_n) \in \ker(\mu^{\mathcal{U}})$, which means that $\mu_i(\alpha_i) = 0$ for $\mathcal{U}$-many i. Since μ_i are injective maps, then $\alpha_i = 0$ for $\mathcal{U}$-many i, so $(\alpha_i) \equiv 0$ in $\mathcal{U}(A_n)$. Thus $\mu^{\mathcal{U}}$ is injective.

The composition of $\varepsilon^{\mathcal{U}} \circ \mu^{\mathcal{U}}$ vanishes, since $\overline{\varepsilon} \circ \overline{\mu}$ also does. Conversely, let $\beta = (\beta_n) \in \ker(\varepsilon^{\mathcal{U}})$. Let S_β be the set of indices such that $\varepsilon_i(\beta_i) = 0$. For those indices, $\beta_i \in \mathrm{Im}(\mu_i)$. We can thus define $\alpha = (\alpha_i)$ by

$$\begin{cases} \alpha_i \in \mu_i^{-1}(\beta_i) & \text{if } i \in S_\beta \\ \alpha_i = 0 & \text{if } i \notin S_\beta \end{cases}$$

Clearly $(\mu_i(\alpha_i))$ is equivalent to (β_i), so $\beta \in \mu^{\mathcal{U}}$.

Finally, the surjectivity of $\varepsilon^{\mathcal{U}}$ follows from being a quotient map of the surjective map $\overline{\varepsilon}$. □

In general, it is difficult to compute the ultraproduct, but there is a special case in which it is explicit, when we have sequence of finite sets of bounded order.

Lemma 3.1.18. Let (M_n) be a sequence of sets satisfying that there is a finite set such that $M_n = M$ for all n. Then the diagonal map $\Delta : \ M \to \mathcal{U}(M_n)$ is an isomorphism.

Proof. By (F0), the above map is clearly injective, so we only need to check surjectivity. A sequence $(m_n) \in \prod_{n\in\mathbb{N}} M$ induces a map

$$f : \mathbb{N} \to M : \ m \mapsto m_n$$

Since M is finite, corollary 3.1.3 implies that there exists a unique $m \in M$ such that $f^{-1}(\{m\}) \in \mathcal{U}$. Hence (m_n) is equivalent to the constant sequence (m), so it belongs to the image of Δ. □

Corollary 3.1.19. Let M_n be a sequence of finite sets whose orders are bounded above by some constant C. Then the ultraproduct $\mathcal{U}(M_n)$ is finite with order less by C.

Proof. Let S be a set of cardinality C. For each $n \in \mathbb{N}$, fix an injection

$$\mu_n : \ M_n \hookrightarrow S$$

By Proposition 3.1.17 and Lemma 3.1.18, there is an injection

$$\mathcal{U}(M_n) \hookrightarrow \mathcal{U}(S) \cong S$$

Thus, $\mathcal{U}(M_n)$ is finite with order bounded by C. □

3.1.4 Ultraprimes

An example of ultraproduct of infinite sets leads to the concept of ultraprimes, which are the elements in the ultraproduct of the constant sequence of the set of prime numbers. We will not attempt to give a description of this ultraproduct, but its elements will play an important role in this theory.

Fix a non-principal ultrafilter $\mathcal{U}$ and a number field K. Denote by $\mathbb{P}$ the set of primes in K.

Definition 3.1.20. An *ultraprime* $\mathfrak{u}$ is an element of $\mathcal{U}(\mathbb{P})$. More specifically, it is represented by a sequence of prime numbers $(\ell_n)_{n\in\mathbb{N}}$, and two sequences represent the same ultraprime if they coindice in $\mathcal{U}$-many primes.

Remark 3.1.21. The primes $\mathbb{P}$ are contained in the ultraprimes $\mathcal{U}(\mathbb{P})$ via the diagonal map, i.e., a prime ℓ is identified with the equivalence class of the constant sequence (ℓ). The image of $\mathbb{P} \hookrightarrow \mathcal{U}(\mathbb{P})$ is sometimes referred as *constant ultraprimes*.

We can use Corollary 3.1.3 to define the Frobenius element associated to an ultraprime $\mathfrak{u}$ in the absolute Galois group G_K.

Proposition 3.1.22. Let $\mathfrak{u} = (\ell_n)$ be an ultraprime and let L/K be a finite Galois extension of number fields. Then there exists a unique element σ such that $\mathrm{Frob}_{\ell_n}|_{L/K} = \sigma$ for $\mathcal{U}$-many n. This element is called the *Frobenius* automorphism of $\mathfrak{u}$ at L/K.

Proof. The sequence (ℓ_n) defines a map

$$F : \ \mathbb{N} \to \mathrm{Gal}(L/K) : \ n \mapsto \mathrm{Frob}_{\ell_n}$$

Since $\mathrm{Gal}(L/K)$ is finite, Corollary 3.1.3 says that there exists a unique $\sigma \in \mathrm{Gal}(L/K)$ such that $F^{-1}(\{\sigma\}) \in \mathcal{U}$.

If we take an equivalent sequence ℓ'_n, the set

$$S = \{n \in \mathbb{N} : \ \ell_n = \ell'_n\} \in \mathcal{U}$$

Then, by (F1) and (F2)

$$S \cap F^{-1}(\{\sigma\}) \subset \{n \in \mathbb{N} : \ \mathrm{Frob}_{\ell'_n} = \sigma\} \in \mathcal{U}$$

Hence the definition of $\mathrm{Frob}_{\mathfrak{u}}$ is independent of the sequence representing it. □

Definition 3.1.23. Let $\mathfrak{u} = (\ell_n)$ be an ultraprime. The Frobenius automorphism $\mathrm{Frob}_{\mathfrak{u}}$ is defined as

$$\mathrm{Frob}_{\mathfrak{u}} = \left(\mathrm{Frob}_{\mathfrak{u}}|_{L/K}\right)_{L/K} \in \varprojlim_{L/K} \mathrm{Gal}(L/K) = G_K$$

Remark 3.1.24. In order to guarantee that Definition 3.1.23 is consistent, we need to show that $\mathrm{Frob}_{\mathfrak{u}}$ behaves well under the restriction of finite extensions L'/L. Let (ℓ_n) be a sequence representing $\mathfrak{u}$ such that $\mathrm{Frob}_{\ell_n} \mid_{L'} = \sigma$, for some $\sigma \in \mathrm{Gal}(L'/K)$ for $\mathcal{U}$-many n. For all those n, $\mathrm{Frob}_{\ell_n} \mid_L = \sigma \mid_L$, so $\sigma \mid_L$ coincides with Frob_{ℓ_n} for $\mathcal{U}$-many n.

Remark 3.1.25. Definition 3.1.23 is consistent with the standard definition of Frobenius automorphims: if $\mathfrak{u} = (\ell)$ is a constant ultraprime, then $\mathrm{Frob}_{\mathfrak{u}} = \mathrm{Frob}_{\ell}$.

Ultraprimes have their own version of Chebotarev density theorem, which is stronger than the classical version. Its main advantage is that it is not longer restricted to finite extensions.

Definition 3.1.26. Let K be a number field and let $\sigma \in G_K$, there exists an ultraprime $\mathfrak{u}$ such that $\mathrm{Frob}_{\mathfrak{u}} = \sigma$.

Proof. Let $(L_n)_{n\in\mathbb{N}}$ be an ordering of all the finite extensions of K. For every $n \in \mathbb{N}$, define $E_n = L_1 \cdots L_n$. By Chebotarev's density theorem, there exists a prime ℓ_n such that $\mathrm{Frob}_{\ell_n} = \sigma|_{E_n}$.

Consider the prime $\mathfrak{u} = (\ell_n)$. Let L be a number field. Then there exists a natural number n_0 such that $L = L_{n_0}$. Then $\mathrm{Frob}_{\ell_n}|_L = \sigma_L$ for all $n \geq n_0$ and, therefore, for $\mathcal{U}$-many $\mathcal{N}$. Hence $\mathrm{Frob}_{\mathfrak{u}}|_L = \sigma_L$ for all number fields L, so $\mathrm{Frob}_{\mathfrak{u}} = \sigma$. □

The construction of the Frobenius is used to artificially define the local Galois group at the ultraprime. It is a generalization of the tame quotient of the classical local Galois groups.

Definition 3.1.27. Let $\mathfrak{u}$ be a non-constant ultraprime. The *local Galois group* $G_{\mathfrak{u}}$ is defined as the semidirect product $\widehat{\mathbb{Z}}(1) \rtimes \langle \mathrm{Frob}_{\mathfrak{u}} \rangle$, where $\langle \mathrm{Frob}_{\mathfrak{u}} \rangle$ is the free profinite group generated by one element which acts by $\mathrm{Frob}_{\mathfrak{u}} \in G_K$ on $\widehat{Z}(1)$.

The *inertia subgroup* $I_{\mathfrak{u}} \subset G_{\mathfrak{u}}$ is the normal subgroup $\widehat{\mathbb{Z}}(1)$.

Remark 3.1.28. Note that, when $\mathfrak{u}$ is a constant ultraprime, the semidirect product $\widehat{\mathbb{Z}}(1) \rtimes \langle \mathrm{Frob}_{\mathfrak{u}} \rangle$ coincides with the tame inertia quotient of the Galois group $G_{\mathfrak{u}}$.

We impose that $G_{\mathfrak{u}}$ acts unramifiedly on Galois modules.

Definition 3.1.29. Let T be a G_K-module. We define an action of $G_{\mathfrak{u}}$ on T via the quotient $G_{\mathfrak{u}} \twoheadrightarrow \langle \mathrm{Frob}_{\mathfrak{u}} \rangle$.

3.2 Patched cohomology

3.2.1 Construction

In this section, we use the ultraproduct defined in the previous one to introduce the notion of patched cohomology. In order to have control over the patched cohomology groups, we define if first for finite coefficient rings as an ultraproduct of cohomology groups, and then we extend the definition to either profinite or ind-finite coefficient rings by taking limits.

Definition 3.2.1. Let T be a finite group endowed with actions from a sequence groups $G = (G_n)_{n\in\mathbb{N}} \in \mathcal{U}(\{\text{groups}\})$ (technically, it is only needed that the action is well defined for $\mathcal{U}$-many n). The $\mathcal{U}$-patched cohomology group is defined as

$$\mathbf{H}^i(G,T) = \mathcal{U}(H^i(G_n,T))$$

If T is a profinite group, we define the patched cohomology as

$$\mathbf{H}^i(G,T) = \varprojlim_{T\twoheadrightarrow T'} \mathbf{H}^i(G,T/T')$$

where the limit is taken over all the finite quotients of T.

Similarly, when T is an ind-finite group, the patched cohomology is defined as

$$\mathbf{H}^i(G,T) = \varinjlim_{T'\hookrightarrow T} \mathbf{H}^i(G,T')$$

where the limit is taken over all the finite subgroups of T.

Proposition 3.2.2. The assignment

$$T \mapsto \mathbf{H}^i(G,T)$$

is a functor from the category of either finite groups, pro-finite groups and ind-finite groups to the category of groups.

Proof. It follows from the functorial properties of cohomology groups, ultraproducts and inverse and direct limits. □

Proposition 3.2.3. Let

$$0 \longrightarrow A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \longrightarrow 0$$

be an exact sequence of continuous maps of profinite groups. Assume A, B and C are endowed with an action of $G = (G_n)$. Then there is a long cohomological exact sequence

diagram of long cohomology sequence

Proof. Let I be a directed set indexing the finite quotients of B, i.e., all the finite quotients of B are of the form B/β_i, for some $i \in I$. Since B is profinite, we have that

$$\bigcap_{i\in I} \beta_i = 0$$

Since μ is injective,

$$\bigcap_{i\in I} \mu^{-1}(\beta_i) = 0$$

Hence they A can be computed as the inverse limit

$$H^i(G, A) = \varprojlim_{A \twoheadrightarrow A'} \mathbf{H}^i(G, A') = \varprojlim_{i\in I} \mathbf{H}^i(G, A/\mu^{-1}(\beta_i))$$

Similarly,

$$\bigcap_{i\in I} \varepsilon(\beta_i) = 0$$

Thus,

$$H^i(G, C) = \varprojlim_{C \twoheadrightarrow C'} \mathbf{H}^i(G, C/C') = \varprojlim_{i\in I} \mathbf{H}^i(G, C/\varepsilon(\beta_i))$$

review null intersection and inverse limit (cofinal) For each $i \in I$, there is an exact sequence

$$0 \longrightarrow A/\mu^{-1}(\beta_i) \xrightarrow{\mu} B/\beta_i \xrightarrow{\varepsilon} C/\varepsilon(\beta_i) \longrightarrow 0$$

For each n there is a long exact sequence in the cohomology of G_n. Since the $\mathcal{U}$-patching is an exact functor, it induces a long exact sequence in the patching cohomology of the finite quotients: diagram

Conditions for inverse limit to be exact □

3.2.2 Local patched cohomology

In this section, we outline the basic properties of the local cohomology at an ultraprime $\mathfrak{u}$, defined as the patching of the local cohomology of the primes defining $\mathfrak{u}$.

Definition 3.2.4. Let $\mathfrak{u}$ be an ultraprime represented by the sequence (ℓ_n). The local patched cohomology group is defined as

$$\mathbf{H}^i(K_{\mathfrak{u}}, T) := \mathbf{H}^i\big((G_{K_{\ell_n}}), T\big)$$

In the local case, the local patched cohomology coincides the group cohomology of the local Galois group defined in Definition 3.1.27.

Proposition 3.2.5. Let T be an $R[[G_K]]$-module either finite, profinite or ind-finite, and let $\mathfrak{u}$ be an ultraprime represented by the sequence (ℓ_n). Then

$$\mathbf{H}^i(K_{\mathfrak{u}}, T) = \mathbf{H}^i(G_{\mathfrak{u}}, T)$$

Proof. By taking limits, we only need to prove it when T is finite. If $\mathfrak{u}$ is a constant ultraprime, it follows from the finiteness of classical local Galois cohomology and Lemma 3.1.18.

Hence we can assume that $\mathcal{U}$ is a non-constant ultraprime. For $\mathcal{U}$-many n, the action of G_{ℓ_n} on T is unramified, Frob_{ℓ_n} acts on T like $\mathrm{Frob}_{\mathfrak{u}}$ and $\ell_n \nmid \#T$. For those values, we have that

$$H^i(G_{\ell_n}, T) = H^i(G^{\mathrm{t}}_{\ell_n}, T)$$

where $G^{\mathrm{t}}_{\ell_n}$ is Galois group of the maximal tamely ramified extension. complete □

From this prove, we can prove the following corollary.

Corollary 3.2.6. Let $\mathfrak{u} = (\ell_n)$ be an ultraprime and let T be a finite group endowed with an action of $G_{\mathfrak{u}}$. For $\mathcal{U}$-many n, there is an isomorphism

$$\varphi_i^{\mathfrak{u}} : \ \mathbf{H}^1(K_{\mathfrak{u}}, T) \cong H^1(K_{\ell_i}, T)$$

Definition 3.2.7. (Cohomology of the inertia subgroup) Let $\mathfrak{u}$ an ultraprime represented by the sequence (ℓ_n). The cohomology of the inertia subgroup is the patching

$$\mathbf{H}^i(\mathcal{I}_{\mathfrak{u}}, T) = \mathbf{H}^i\big(I_{\ell_n}, T\big)$$

Definition 3.2.8. (Finite cohomology) We define the *finite cohomology* group as

$$\mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}}, T) = \ker\Big(\mathbf{H}^1(K_{\mathfrak{u}}, T) \to \mathbf{H}^1(I_{\mathfrak{u}}, T)\Big)$$

local duality

We can generalise the concept of Kolyvagin primes to this setting, with the advantage that there are Kolyvagin ultraprimes even for infinite coefficient rings. In order to define this notion, we need to set some assumptions

Assumption 3.2.9. Let R be a profinite, local ring that can be described as

$$R = \varprojlim R_n$$

where R_n is a self-injective, finite, local ring. In addition, let T be a $R[[G_K]]$-module that is finitely generated as R-module.

Notation 3.2.10. Recall that $K(T)$ is the kernel of the action $\rho : \ G_K \to \mathrm{Aut}(T)$ and let

$$K(T)_{p^\infty} = K(T)K(1)(\mu_{p^\infty})$$

Assumption 3.2.11. In addition, we assume the following assumptions:

- (T1) $T/\mathfrak{m}T$ is an irreducible $k[[G_K]]$-module.
- (T2) There exists $\tau \in G_{K_M}$ such that $T/(\tau - 1)T \cong R$ as R-modules.
- (T3) $H^1(K(T)_{p^\infty}/K, T) = H^1(K(T)_{p^\infty}/K, T^*(1)) = 0$.

Definition 3.2.12. An ultraprime is said to be a *Kolyvagin ultraprime* is $\mathrm{Frob}_{\mathfrak{u}}$ is conjugate to τ in $\mathrm{Gal}(K(T)_{p^\infty}/K)$.

We can describe explicitly the local cohomology of Kolyvagin ultraprimes.

Proposition 3.2.13. Let $\mathfrak{u}$ be a Kolyvagin ultraprime. Then there is an homomorphism

$$\mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}}, T) \cong T/(\mathrm{Frob}_{\mathfrak{u}} - 1)T$$

Local Tate duality extend to patched cohomology.

Proposition 3.2.14. (Local duality) Let T be either a finite, profinite or ind-finite group and let $\mathfrak{u} = (\ell_n)$ be an ultraprime. Then there is a non-degenerate pairing

$$\mathbf{H}^1(K_{\mathfrak{u}}, T) \times \mathbf{H}^1(K_{\mathfrak{u}}, T^*) \to \mathbb{Q}/\mathbb{Z}$$

Proof. Assume first that T is finite. Then

$$\mathbf{H}^1(K_{\mathfrak{u}}, T) = \mathcal{U}\big(H^1(K_{\ell_n}, T)\big), \quad \mathbf{H}^1(K_{\mathfrak{u}}, T^*) = \mathcal{U}\big(H^1(K_{\ell_n}, T^*)\big)$$

Hence, by Proposition 3.1.13

$$\mathbf{H}^1(K_{\mathfrak{u}}, T) \times \mathbf{H}^1(K_{\mathfrak{u}}, T^*) = \mathcal{U}\Big(H^1(K_{\ell_n}, T) \times H^1(K_{\ell_n}, T^*)\Big)$$

Classical Tate duality, together with the functoriality of the ultraproduct, induces a pairing

$$\mathbf{H}^1(K_{\mathfrak{u}}, T) \times \mathbf{H}^1(K_{\mathfrak{u}}, T^*) \to \mathcal{U}\left(\frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right) = \frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}$$

Since classical local duality is non-degenerate, and the ultraproduct is an exact functor, there is an injection

$$\mathcal{U}\big(H^1(K_{\ell_n}, T)\big) \hookrightarrow \mathcal{U}\left(\mathrm{Hom}\left(H^1(K_{\ell_n}, T^*), \frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right)\right)$$

Applying Proposition 3.1.14, we also obtain the injection

$$\mathcal{U}\big(H^1(K_{\ell_n}, T)\big) \hookrightarrow \mathrm{Hom}\left(\mathcal{U}\big(H^1(K_{\ell_n}, T^*)\big), \mathcal{U}\left(\frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right)\right)$$

Therefore, the patched local duality pairing is non-degenerate on the left. Similarly, it is also non-degenerate on the right factor.

Assume now that T is profinite, which implies that T^* is ind-finite. Then

$$\mathbf{H}^1(K_{\mathfrak{u}}, T) = \varprojlim_{T \twoheadrightarrow T'} \mathbf{H}^1(K_{\mathfrak{u}}, T'), \quad \mathbf{H}^1(K_{\mathfrak{u}}, T^*) = \varinjlim_{T \twoheadrightarrow T'} \mathbf{H}^1(K_{\mathfrak{u}}, (T')^*)$$

Hence, local duality for patched cohomology groups with finite coefficients induces a perfect pairing

$$\varprojlim_{T \twoheadrightarrow T'} \mathbf{H}^1(K_{\mathfrak{u}}, T') \times \varinjlim_{T \twoheadrightarrow T'} \mathbf{H}^1(K_{\mathfrak{u}}, (T')^*) \to \mathbb{Q}/\mathbb{Z}$$

It proves local duality for profinite T. When T is ind-finite, an analogous proof completes the result. □

finite cohomology annihilators

3.2.3 Global patched cohomology

The first goal of this section is defining the concept of the patched cohomology group outside the square-free (formal) product of ultraprimes.

Definition 3.2.15. Let $\mathfrak{u}_1 = \left(\ell_k^{(1)}\right)_{k\in\mathbb{N}}, \dots, \mathfrak{u}_s = \left(\ell_k^{(s)}\right)_{k\in\mathbb{N}}$ be a finite set of (distinct) ultraprimes. Its product is defined as

$$\mathfrak{u}_1 \cdots \mathfrak{u}_s = (\ell_n^1 \cdots \ell_n^{(s)})_{n\in\mathbb{N}} \in \mathcal{U}(\mathbb{N})$$

The set of square-free products of Kolyvagin ultraprimes is denoted by $\mathcal{N}$.

Definition 3.2.16. ([Swe22, Definition 2.4.2]) Let T be either a finite, profinite or ind-finite $R[[G_K]]$ module and let $\mathfrak{n} \in \mathcal{N}$ be represented by the sequence (n_i). We defined the maximal patched cohomology group unramified at $\mathfrak{n}$ by

$$\mathbf{H}^i(K^{\mathfrak{n}}/K, T) := \mathbf{H}^i\big(\mathrm{Gal}(K^{n_i}/K), T^{G_{K_{n_i}}}\big)$$

where K^{n_i} represents the maximal extension of K unramified outside the prime divisors of n_i. Note that this definition is independent of the sequence representing $\mathfrak{n}$.

Notation 3.2.17. If S is a finite set of distinct ultraprimes and n is the product of all the ultraprimes in S, we will also denote $\mathbf{H}^i(K^{\mathfrak{n}}/K, T)$ by $\mathbf{H}^i(K^{\Sigma}/K, T)$.

The basic property of the global patched finite groups is its finiteness.

Proposition 3.2.18. ([Swe22, Lemma 2.4.5.]) Let T be a finite group unramified outside a finite set $S \subset \mathcal{U}(\mathbb{P})$. The patched cohomology groups $\mathbf{H}^i(K^S/K, T)$ are finite for all $i \geq 0$.

Proof

Remark 3.2.19. If $S_1 \subset S_2 \subset \mathcal{U}(\mathbb{P})$ are two finite sets of ultraprimes. Then there is a natural map

$$\mathbf{H}^1(K^{S_1}/K, T) \hookrightarrow \mathbf{H}^1(K^{S_2}/K, T)$$

When T is finite, it is induced by a sequence of inflation maps. The general case, when T is profinite and ind-finite, follows by taking limits.

Definition 3.2.20. ([Swe22, p. 2.4.6.]) Assume that T is unramified outside a finite set of primes S_0. The absolute global patched cohomology group is defined as

$$\mathbf{H}^1(K, T) = \varinjlim_{S_0 \subset S \subset \mathcal{U}(\mathbb{P})} \mathbf{H}(K^S/K, T)$$

where the limit is taken over all the finite sets and the transition maps are the ones defined in Remark 3.2.19.

Definition 3.2.21. Let S be a finite set of ultraprimes and let $\mathfrak{u}$ be an ultraprime. There exists a restriction map

$$\mathrm{res}: \ \mathbf{H}^1(K^S/K, T) \to \mathbf{H}^1(K_{\mathfrak{u}}, T)$$

induced, when T is finite, by the restriction map in every factor of the ultraproduct. When T is profinite (resp. ind-finite), res is obtained as the limit of the restriction map in the cohomology of the finite quotients (resp. submodules).

We now show that the above definition is, in fact, the unramified subgroup of the global patched cohomology.

Proposition 3.2.22. ([Swe22, Proposition 2.4.11.]) Let $S \subset \mathcal{U}(\mathbb{P})$ be a finite set of ultraprimes and let T be unramified outside S_0. Then

$$\mathbf{H}^1(K^S/K, T) = \ker\Big(\mathbf{H}^1(K, T) \to \prod_{\mathfrak{u} \in \mathcal{U}(\mathbb{P})\setminus S} \frac{\mathbf{H}^1(K_\mathfrak{u}, T)}{\mathbf{H}^1(\mathcal{I}_\mathfrak{u}, T)}\Big)$$

3.3 Patched Selmer groups

3.3.1 Patched Selmer structures

Following [Swe22], we can now define the Selmer structures in this setting. The main innovation is they also include local conditions at non-constant ultraprimes.

Definition 3.3.1. A *Selmer structure* $\mathcal{F}$ is a consists of the following data:

- A finite set $\Sigma_\mathcal{F}$ of $\mathcal{U}(\mathbb{P})$ containing all constant ultraprimes lying over p, ∞ or ramified primes of T.
- For each $\mathfrak{u} \in S$, a closed R-submodule

$$\mathbf{H}^1_\mathcal{F}(K_\mathfrak{u}, T) \subset \mathbf{H}^1(K_\mathfrak{u}, T)$$

Definition 3.3.2. The Selmer group of a Selmer structure $\mathcal{F}$ is defined as

$$\mathbf{H}^1_\mathcal{F}(K, T) := \ker\left(\mathbf{H}^1(K^\Sigma/K, T) \to \prod_{\mathfrak{u} \in \Sigma} \frac{\mathbf{H}^1(K_\mathfrak{u}, T)}{\mathbf{H}^1_\mathcal{F}(K_\mathfrak{u}, T)}\right)$$

Remark 3.3.3. By Proposition 3.2.22, a Selmer structure depend only on the local conditions. If we set $\mathbf{H}^1_\mathcal{F}(K_\mathfrak{u}, T) := \mathbf{H}^1_\mathrm{f}(K_\mathfrak{u}, T)$ whenever $\mathfrak{u} \notin \mathcal{F}$, then

$$\mathbf{H}^1_\mathcal{F}(K, T) = \ker\left(\mathbf{H}^1(K, T) \to \prod_{\mathfrak{u} \in \mathcal{U}(\mathbb{P})} \frac{\mathbf{H}^1(K_\mathfrak{u}, T)}{\mathbf{H}^1_\mathcal{F}(K_\mathfrak{u}, T)}\right)$$

Remark 3.3.4. Local conditions propagate to quotients and submodules as in Definitions 1.2.7 and 1.2.8.

We can recover the Selmer group as the limit of the propagated Selmer groups with finite coefficients.

Proposition 3.3.5. ([Swe22, Proposition 2.5.6]) Let T be a profinite group and let $\mathcal{F}$ be a Selmer structure defined on T. Then

$$\mathbf{H}^1_\mathcal{F}(K, T) = \varprojlim_{T \twoheadrightarrow T'} \mathbf{H}^1_\mathcal{F}(K, T')$$

where the limit is taken over the finite quotients T' of T and $\mathbf{H}^1_\mathcal{F}(K, T')$ is the Selmer group of the propagated Selmer structure, as defined in Definition 1.2.7.

Proof. Since the inverse limit is exact on finite groups,

$$\begin{aligned}\varprojlim_{T\twoheadrightarrow T'} \mathbf{H}^1_{\mathcal{F}}(K,T) &= \varprojlim_{T\twoheadrightarrow T'} \ker\left(\mathbf{H}^1\big(K^{\Sigma_{\mathcal{F}}}/K,T'\big) \to \prod_{\mathfrak{u}\in\Sigma_{\mathcal{F}^*}} \mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T)\right)\\ &= \ker\left(\mathbf{H}^1\big(K^{\Sigma_{\mathcal{F}}}/K,T\big) \to \prod_{\mathfrak{u}\in\Sigma_{\mathcal{F}^*}} \varprojlim_{T\twoheadrightarrow T'} \mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T')\right)\end{aligned}$$

By the definition of propagated Selmer structure and the closedness of $\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T)$, we obtain that

$$\mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T) = \varprojlim_{T\twoheadrightarrow T'} \mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T')$$

which finish the proof of this proposition. □

The next dual proposition is proven similarly.

Proposition 3.3.6. ([Swe22, Proposition 2.5.6]) Let T be an ind-finite group and let $\mathcal{F}$ be a Selmer structure defined on T. Then

$$\mathbf{H}^1_{\mathcal{F}}(K,T) = \varinjlim_{T'\hookrightarrow T} \mathbf{H}^1_{\mathcal{F}}(K,T')$$

where the limit is taken over the finite submodules T' of T and $\mathbf{H}^1_{\mathcal{F}}(K,T')$ is the Selmer group of the propagated Selmer structure, as defined in Definition 1.2.8.

The next technical lemma shows that, in the finite case, patched Selmer groups can be obtained from patching classical Selmer groups.

Lemma 3.3.7. Let $\mathcal{F}\leq\mathcal{G}$ be two Selmer structures defined on a finite Galois module T. Then there are sequences of classical Selmer structures $(\mathcal{F}_i)$ and $(\mathcal{G}_i)$ such that $\mathcal{F}_i\leq\mathcal{G}_i$ for all $i\in\mathbb{N}$ and all ultraprimes $\mathfrak{u}$,

$$\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{F}_i}(K_{\mathfrak{u}},T)\big),\ \mathbf{H}^1_{\mathcal{G}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{G}_i}(K_{\mathfrak{u}},T)\big)$$

Moreover, we can construct the patched Selmer group as the ultraproduct of classical Selmer groups

$$\mathbf{H}^1_{\mathcal{F}}(K,T) = \mathcal{U}\big(H^1_{\mathcal{F}_i}(K,T)\big),\ \mathbf{H}^1_{\mathcal{G}}(K,T) = \mathcal{U}\big(H^1_{\mathcal{G}_i}(K,T)\big)$$

Proof. For an ultraprime $\mathfrak{u}\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}$, fix a representing sequence $(\mathfrak{u}_i)$ and let $W_{\mathfrak{u}}$ be the set of indices such that there is an isomorphism $\varphi_i^{\mathfrak{u}}:\ H^1(K_{\ell_i},T)\cong\mathbf{H}^1(K_{\mathfrak{u}},T)$. Note that Corollary 3.2.6 implies that $W_{\mathfrak{u}}\in\mathcal{U}$.

For every $i\in\mathbb{N}$, define the classical Selmer structre by $\Sigma_{\mathcal{F}_i}=\{\mathfrak{u}_i:\ \mathfrak{u}\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}\}$ and local conditions

$$\begin{aligned}H^1_{\mathcal{F}_i}(K_{\mathfrak{u}_i},T) &= (\varphi_i^{\mathfrak{u}})^{-1}\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) && \text{if } i\in W_{\mathfrak{u}}\\ H^1_{\mathcal{F}_i}(K_{\mathfrak{u}_i},T) &= 0 && \text{if } i\notin W_{\mathfrak{u}}\end{aligned}$$

This definition implies that $\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T)=\mathcal{U}\big(H^1_{\mathcal{F}}(K_{\mathfrak{u}_i},T)\big)$. Therefore, Proposition 3.1.17 implies that

$$\ker\left[\mathbf{H}^1(K^{\mathfrak{n}}/K,T)\to\prod_{\mathfrak{u}|\mathfrak{n}}\mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T)\right] = \ker\left[\mathcal{U}\big(H^1(K^{n_i}/K,T)\big)\to\prod_{\mathfrak{u}_i|\mathfrak{n}_i}\mathcal{U}\big(H^1_{/\mathcal{F}}(K_{\mathfrak{u}_i},T)\big)\right]$$

Again by the exactness of the ultraproduct given in Proposition 3.1.17 implies that

$$\mathbf{H}^1_{\mathcal{F}}(K,T) = \mathcal{U}\big(H^1_{\mathcal{F}_i}(K,T)\big)$$

Similarly, define Selmer structures $\mathcal{G}_i$ by $\Sigma_{\mathcal{G}_i} = \{\mathfrak{u}_i : \mathfrak{u} \in \Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}\}$ and local conditions

$$\begin{aligned} H^1_{\mathcal{G}_i}(K_{\mathfrak{u}_i},T) &= (\varphi_i^{\mathfrak{u}})^{-1}\mathbf{H}^1_{\mathcal{G}}(K_{\mathfrak{u}},T) \quad \text{if } i \in W_{\mathfrak{u}} \\ H^1_{\mathcal{G}_i}(K_{\mathfrak{u}_i},T) &= H^1(K_{\mathfrak{u}_i},T) \qquad\qquad \text{if } i \notin W_{\mathfrak{u}} \end{aligned}$$

By construction $\mathcal{F}_i \leq \mathcal{G}_i$ and, analogously,

$$\mathbf{H}^1_{\mathcal{G}}(K,T) = \mathcal{U}\big(H^1_{\mathcal{G}_i}(K,T)\big)$$

□

We can use local duality to define dual Selmer structures as in Definition 1.2.4

Definition 3.3.8. (Dual Selmer structure) Let $\mathcal{F}$ be a Selmer structure on T. The we can define a *dual Selmer structure* $\mathcal{F}^*$ on T^* by defining the local condition $\mathbf{H}^1(K_{\mathfrak{u}},T^*)$ as the the annihilator of $\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T)$ under the local duality pairing in Proposition 3.2.14

Dual patched Selmer structures can be also obtained by patching the dual Selmer structures in the classical setting.

Lemma 3.3.9. Let $\mathcal{F}$ a patched Selmer structure defined on a finite group T and let $\mathcal{F}_i$ be classical Selmer structures such that

$$\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{F}}(K_{\mathfrak{u}},T)\big)$$

Then, we have that

$$\mathbf{H}^1_{\mathcal{F}^*}(K_{\mathfrak{u}},T^*) = \mathcal{U}\big(H^1_{\mathcal{F}^*_i}(K_{\mathfrak{u}},T^*)\big)$$

Proof. By Definition 3.3.8, for every ultraprime $\mathfrak{u} = (\ell_i)$, we have that

$$\mathbf{H}^1_{\mathcal{F}^*}(K_{\mathfrak{u}},T^*) = \ker\left(H^1(K_{\mathfrak{u}},T^*) \to \mathrm{Hom}\left(H^1_{\mathcal{F}}(K_{\mathfrak{u}},T) \to \frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right)\right)$$

where the map is induced by local duality, as stated in Proposition 3.2.14. This map can be also written as the composite

$$\begin{aligned} \mathcal{U}\big(H^1(K_{\ell_i},T^*)\big) &\to \mathcal{U}\left(\mathrm{Hom}\left(H^1_{\mathcal{F}_i}(K_{\ell_i},T), \frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right)\right) \\ &\hookrightarrow \mathrm{Hom}\left(\mathcal{U}\big(H^1_{\mathcal{F}_i}(K_{\ell_i},T)\big), \mathcal{U}\left(\frac{(\#T)^{-1}\mathbb{Z}}{\mathbb{Z}}\right)\right) \end{aligned}$$

where the second map is the injection given in Proposition 3.1.14. By Proposition 1.1.18 and 3.1.17, we can compute the kernel of this map as

$$\mathbf{H}^1_{\mathcal{F}^*}(K_{\mathfrak{u}},T^*) = \mathcal{U}\big(H^1_{\mathcal{F}^*_i}(K_{\ell_i},T^*)\big)$$

□

There is also a global duality exact sequence in this setting.

Proposition 3.3.10. (Global duality) Let $\mathcal{F} \leq \mathcal{G}$ be two Selmer stuctures. Then there is a global duality exact sequence

$$H^1_{\mathcal{F}}(K,T) \rightarrowtail H^1_{\mathcal{G}}(K,T) \longrightarrow \bigoplus_{\ell \in \Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_\ell,T)}{H^1_{\mathcal{F}}(K_\ell,T)} \longrightarrow H^1_{\mathcal{G}^*}(K,T^*)^\vee \twoheadrightarrow H^1_{\mathcal{F}^*}(K,T^*)^\vee$$

Proof. Assume first that T is finite. Let $\mathfrak{n} = (n_k)_{k\in\mathbb{N}}$ be the square-free product of all ultraprimes in $\Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}$. By Lemma 3.3.7, there are sequences of classical Selmer structures $(\mathcal{F}_i)$ and $(\mathcal{G}_i)$, where $\mathcal{F}_i \leq \mathcal{G}_i$, and

$$\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{F}_i}(K_{\mathfrak{u}_i},T)\big),\ \mathbf{H}^1_{\mathcal{G}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{G}_i}(K_{\mathfrak{u}_i},T)\big)$$

By the exactness of the ultraproduct shown in Proposition 3.1.17, the Selmer groups of $\mathcal{F}$ and $\mathcal{G}$ are also ultraproducts of classical Selmer groups:

$$\mathbf{H}^1_{\mathcal{F}}(K,T) = \mathcal{U}\big(H^1_{\mathcal{F}_i}(K,T)\big),\ \mathbf{H}^1_{\mathcal{G}}(K_{\mathfrak{u}},T) = \mathcal{U}\big(H^1_{\mathcal{G}}(K,T)\big)$$

By Lemma 3.3.9 and Proposition 3.1.17, the dual Selmer groups can be also obtained as an ultraproduct of classical Selmer groups:

$$\mathbf{H}^1_{\mathcal{F}^*}(K,T^*) = \mathcal{U}\big(H^1_{\mathcal{F}^*_i}(K,T^*)\big),\ \mathbf{H}^1_{\mathcal{G}^*}(K_{\mathfrak{u}},T^*) = \mathcal{U}\big(H^1_{\mathcal{G}^*}(K,T^*)\big)$$

Then the global duality exact sequence is

$$\mathcal{U}\big(H^1_{\mathcal{F}_i}(K,T)\big) \rightarrowtail \mathcal{U}\big(H^1_{\mathcal{G}}(K,T)\big) \longrightarrow \mathcal{U}\Big(\bigoplus_{\ell} \frac{H^1_{\mathcal{G}}(K_\ell,T)}{H^1_{\mathcal{F}}(K_\ell,T)}\Big) \longrightarrow \mathcal{U}\big(H^1_{\mathcal{G}^*}(K,T^*)^\vee\big) \twoheadrightarrow \mathcal{U}\big(H^1_{\mathcal{F}^*}(K,T^*)^\vee\big)$$

which is exact by Proposition 3.1.17.

When T is profinite (resp. ind-finite), then Proposition 3.3.5 (resp. Proposition 3.3.6) implies that the above exact sequence can be obtained as the inverse (resp. direct) limit of the associated exact sequences for the finite quotients (resp. submodules) of T. □

3.3.2 Patched Selmer modules

In this section, we endow the group T with an module structure and will try to reprove the resutls in §1.2

Notation 3.3.11. Let R be a complete, local ring with finite residue field k and let T be an $R[[G_K]]$-module that is free and finitely generated as an R-module.

Proposition 3.3.12. Under Assumptions 3.2.11, for every finitely generated ideal I of R, the inclusion $T^*[I] \hookrightarrow T^*$ induces an isomorphism

$$H^1_{\mathcal{F}^*}(K,T^*[I]) \cong H^1_{\mathcal{F}}(K,T^*)[I]$$

Proof. Hence, Propostion long exact sequence induces an injection

$$H^1(K^{\mathfrak{n}_i}/K, T^*[I]) \hookrightarrow H^1(K^{\mathfrak{n}_i}/K, T^*)[I]$$

By Definition 3.3.1, there is an injection

$$H^1_{\mathcal{F}}(K, T^*[I]) \hookrightarrow H^1_{\mathcal{F}}(K, T^*)[I]$$

Let $\mathfrak{n}$ be the square-free product of all primes in $\Sigma_{\mathcal{F}}$. By (T1) in Assumption 3.2.11, we have that need to redo with quotients of T^*

$$\mathbf{H}^0(K^{\mathfrak{n}}, T^*) = H^0(K, T^*) = 0$$

Consider the exact sequence

$$0 \longrightarrow T^*[I] \longrightarrow T^* \longrightarrow T^*/T^*[I]$$

By Propostion long exact sequence, it induces an exact sequence

$$0 \longrightarrow \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*[I]\big) \longrightarrow \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big) \longrightarrow \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*/T^*[I]\big) \longrightarrow 0 \tag{3.1}$$

Let $\{r_1, \cdots, r_d\}$ be a minimal set of generators of I. It induces an injection

$$T^*/T^*[I] \hookrightarrow (T^*)^d, \ t \mapsto (r_1 t, \ldots, r_d t)$$

By cite $H^0 = 0$, it induces an injection

$$\mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*/T^*[I]\big) \hookrightarrow \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big)^d$$

complete Since the composition

$$\mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big) \to \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*/T^*[I]\big) \hookrightarrow \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big)^d$$

is the multiplication by $(r_1, \ldots, r_d)$, its kernel coincides with $\mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big)[I]$. Since the second map is injective, the kernel coincices with the kernel of the first map. From (3.1), we can conclude that

$$\mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*[I]\big) = \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big)[I]$$

Consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathbf{H}^1_{\mathcal{F}}(K, T^*[I]) & \longrightarrow & \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*[I]\big) & \longrightarrow & \bigoplus_{\mathfrak{u} \in \Sigma^*_{\mathcal{F}}} \mathbf{H}^1_{/\mathcal{F}^*}(K_{\mathfrak{u}}, T^*[I]) \\
 & & \downarrow & & \downarrow \sim & & \downarrow \\
0 & \longrightarrow & \mathbf{H}^1_{\mathcal{F}}(K, T^*)[I] & \longrightarrow & \mathbf{H}^1\big(K^{\mathfrak{n}}/K, T^*\big)[I] & \longrightarrow & \bigoplus_{\mathfrak{u} \in \Sigma^*_{\mathcal{F}}} \mathbf{H}^1_{/\mathcal{F}^*}(K_{\mathfrak{u}}, T^*)[I]
\end{array}$$

We have already seen that the middle vertical arrow is an isomorphism. The right vertical arrow is injective, since its dual $\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}}, T) \twoheadrightarrow \mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}}, T/I)$ is surjective by definition of propagated Selmer structures. Therefore, the leftmost vertical arrow is also an isomorphism. □

3.3.3 Suitable ultraprimes

This section is devoted to prove analogues of Propositions 1.2.21 and 1.2.27

might be needed to do it individually in every case

3.3.4 Patched Selmer modules over discrete valuation rings

Notation 3.3.13. Let R be a discrete valuation ring and let T be an $R[[G_K]]$-module that is free and finitely generated as an R-module.

Remark 3.3.14. Note that we can compute the patched cohomology groups as the limits

$$\mathbf{H}^1(G,T) = \varprojlim_n \mathbf{H}^1\left(G, T/\mathfrak{m}^i T\right), \quad \mathbf{H}^1(G,T) = \varinjlim_n \mathbf{H}^1\left(G, T[\mathfrak{m}^i]\right)$$

since T/m^iT (resp. $T^*[m^i]$) is a cofinal sequence in the finite quotients of T (resp. finite submodules of T^*).

We will be interested in studying local conditions that are cartesian.

Definition 3.3.15. (Cartesian local condition) A local condition $\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T) \subset \mathbf{H}^1(K_\mathfrak{u}, T)$ is called *cartesian* if $H^1_{/\mathcal{F}}(K_\mathfrak{u}, T)$ is a torsion-free R-module. A Selmer structure is said to be cartesian is all of its local conditions are cartesian.

Remark 3.3.16. By [MR04, Lemma 3.7.1], if a Selmer structure on T is cartesian as in Definition 3.3.15, the propagated Selmer structure to a finite quotient $T/\mathfrak{m}^i$ will be cartesian in the sense of Definition 1.2.11.

finite cohomology

When a Selmer structure is cartesian, the propagated Selmer group of quotients of T can be described as a quotient of the Selmer group of T. The proof of the next proposition follows the one of [MR04, Lemma 3.7.1]

Proposition 3.3.17. Let $\mathcal{F}$ be a cartesian Selmer structure. For $k \in \mathcal{N}$, there is an injection with finite cokernel C

$$\mathbf{H}^1_{\mathcal{F}}(K,T)/\mathfrak{m}^k \hookrightarrow \mathbf{H}^1_{\mathcal{F}}(K, T/\mathfrak{m}^k)$$

Proof. Let $\mathfrak{n}$ be the square-free product of the ultraprimes in $\Sigma_\mathcal{F}$ and let π be a generator of $\mathfrak{m}$. Consider the exact sequence

$$0 \longrightarrow T \xrightarrow{\pi^k} T \longrightarrow T/\mathfrak{m}^k$$

It induces an injection

$$\mathbf{H}^1(K^\mathfrak{n}/K, T)/\mathfrak{m}^k \hookrightarrow \mathbf{H}^1(K^\mathfrak{n}/K, T/\mathfrak{m}^k)$$

By the definition of Selmer group, there is a module D fitting into an exact sequence

$$0 \longrightarrow \frac{\mathbf{H}^1(K^\mathfrak{n}/K,T)}{\mathbf{H}^1_{\mathcal{F}}(K,T)} \longrightarrow \prod_{\mathfrak{u}\in\Sigma_\mathcal{F}} \frac{\mathbf{H}^1(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u},T)} D \longrightarrow 0$$

Since the Selmer structure is cartesian, the product is $\mathfrak{m}$-torsion-free, so the domain is torsion free as well. The snake's lemma implies that the left vertical map in the following diagram is injective.

$$\begin{array}{ccccc} \mathbf{H}^1_{\mathcal{F}}(K,T)/\mathfrak{m}^k & \xrightarrow{f} & \mathbf{H}^1_{\mathcal{F}}(K,T/\mathfrak{m}^k) & \twoheadrightarrow & C \\ \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} \\ \mathbf{H}^1(K^{\mathfrak{n}}/K,T)/\mathfrak{m}^k & \hookrightarrow & \mathbf{H}^1(K^{\mathfrak{n}}/K,T/\mathfrak{m}^k) & \twoheadrightarrow & \mathbf{H}^2(K^n/K,T)[\mathfrak{m}] \end{array}$$

Hence the map f is also injective. Here, C is defined as the cokernel of the first map. By the snake's lemma, there is an isomorphism

$$\ker(g_3) = \ker\big(\operatorname{coker}(g_1) \to \operatorname{coker}(g_2)\big)$$

By the definition of Selmer groups, the kernel map $\operatorname{coker}(g_1) \to \operatorname{coker}(g_2)$ coincides by the one of the map

$$\frac{\mathbf{H}^1(K^{\mathfrak{n}}/K,T)}{\mathfrak{m}^k\mathbf{H}^1(K^{\mathfrak{n}}/K,T) + \mathbf{H}^1_{\mathcal{F}}(K,T)} \to \prod_{\mathfrak{u}\in\mathcal{U}(\mathbb{P})} \mathbf{H}^1_{/\mathcal{F}}(K_{\mathfrak{u}},T/\mathfrak{m}^k)$$

$$\operatorname{length}(C) \leq \operatorname{length}\big(\mathbf{H}^2(K,T[\mathfrak{m}^k])\big)$$

explain further, long exact sequence of patched cohomology, Mazur Rubin 3.7.1

□

We now prove an analogue of Proposition 1.2.16 for patched Selmer structures. Recall that core rank was defined in the classical setting in Definition 1.2.14 and it is define in the same way in this patched setting.

Proposition 3.3.18. Let $\mathcal{F}$ be a cartesian Selmer structure on T of core rank $\chi(\mathcal{F})$. For every $k \geq 0$, there is a non-canonical isomorphism

$$\mathbf{H}^1_{\mathcal{F}}(K,T/\mathfrak{m}^k) \cong \Big(R/\mathfrak{m}^k\Big)^{\chi(\mathcal{F})} \oplus \mathbf{H}^1_{\mathcal{F}^*}(K,T^*[\mathfrak{m}^k])$$

Proof. write □

assumptions on H^0

Proposition 3.3.19. Let $\mathcal{F}$ be a cartesian Selmer structure on T of core rank $\chi(\mathcal{F})$. Then

$$\operatorname{rank}_R \mathbf{H}^1(K,T) - \operatorname{rank}_R \mathbf{H}^1(K,T^*)^\vee = \chi(\mathcal{F})$$

Proof. For every $k \geq 0$, there is an isomorphism proof needed

$$\mathbf{H}^1_{\mathcal{F}}(K,T^*[\mathfrak{m}^k]) \cong \mathbf{H}^1(K,T^*)[\mathfrak{m}^k]$$

Therefore, $\mathbf{H}^1(K,T^*)$ is cofinitely generated, so there are constants a and b such that

$$\operatorname{length}\big(\mathbf{H}^1_{\mathcal{F}}(K,T^*[\mathfrak{m}^k])\big) = ak+b$$

By Proposition 3.3.18, then

$$\operatorname{length}\big(\operatorname{rank}_R \mathbf{H}^1(K,T/\mathfrak{m}^k)\big) = (a+\chi(\mathcal{F}))k+b$$

By Proposition 3.3.17, there is a constant f such that

$$(a+\chi(\mathcal{F}))k+b-f \leq \operatorname{length}\big(\operatorname{rank}_R \mathbf{H}^1(K,T)/\mathfrak{m}^k\big) \leq (a+\chi(\mathcal{F}))k+b$$

Hence $\mathbf{H}^1(K,T)$ is also finitely generated of rank $a+\chi(\mathcal{F})$. □

Under assumptions 1.1.5, the profinite Selmer groups are free modules.

Proposition 3.3.20. Assume T satisfies Assumption 1.1.5 and $\mathcal{F}$ is any Selmer structure. Then $H^1_{\mathcal{F}}(K,T)$ is a free R-module. Moreover, if $\mathcal{F}$ is a cartesian, then the quotient

$$\frac{\mathbf{H}^1(K,T)}{\mathbf{H}^1_{\mathcal{F}}(K,T)}$$

is torsion free.

Proof. Consider the exact sequence

$$0 \longrightarrow T \longrightarrow T \longrightarrow T/\mathfrak{m} \longrightarrow 0$$

Then (T1) implies that $H^0(K,T/\mathfrak{m})$, so $\mathbf{H}^1(K,T)$ contains no torsion. By the definition of Selmer module, there is an injection

$$\frac{\mathbf{H}^1(K,T)}{\mathbf{H}^1_{\mathcal{F}}(K,T)} \hookrightarrow \bigoplus_{\mathfrak{u}\in\mathcal{U}(\mathcal{P})} \frac{\mathbf{H}^1(K_{\mathfrak{u}},T)}{\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T)}$$

Since $\mathcal{F}$ is cartesian, the latter is torsion-free, which implies that the domain is also torsion-free. □

3.4 Ultra Kolyvagin systems

Definition 3.4.1. An *ultra Kolyvagin system* for a Selmer structure $\mathcal{F}$

$$\kappa = \Big\{\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q},T) :\ n\in\mathcal{N}\Big\}$$

satisfying the following relation for every $n\in\mathcal{N}$ and $\ell\in\mathcal{P}$ not dividing n. By the definition of Selmer module, we have that

$$\operatorname{loc}_\ell(\kappa_n) \in H^1_{\mathcal{F}(n)}(K_\ell,T) = H^1_{\mathrm{f}}(K_\ell,T), \quad \operatorname{loc}_\ell(\kappa_{n\ell}) \in H^1_{\mathcal{F}(n\ell)}(K_\ell,T) = H^1_{\mathrm{tr}}(K_\ell,T)$$

The collection κ is a Kolyvagin system if the following is satisfied

$$\operatorname{loc}_\ell(\kappa_{n\ell}) = \phi^{\mathrm{fs}}_\ell \circ \operatorname{loc}_\ell(\kappa_n)$$

for every $n\in\mathcal{N}$ and $\ell\in\mathcal{P}$ not dividing n.

Chapter 4

Kolyvagin systems over the Iwasawa algebra

The results in previous chapters were limited to principal rings. Here, we generalise previous results to compute the Fitting ideal over the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[T]]$. For that we need to consider Kolyvagin systems consisting of collections of classes in exterior biduals of Selmer groups, as defined in [BSS18]. In this chaper, we combine this setting with the patched Selmer groups defined in Chapter 3 following [Swe22]. This new setting presents some technical complications, since the coefficient ring Λ is no longer self-injective, a condition required in the construction in [BSS18].

4.1 Iwasawa Selmer modules

In this chapter, we will assume that we are working with a Galois representation $\mathbf{T}$ over the Iwasawa algebra.

Assumption 4.1.1. Let $\Lambda = \mathbb{Z}_p[[X]]$ be the classical Iwasawa algebra and let $\mathbf{T}$ be a $\Lambda[[G_K]]$-module that is free and finitely generated as a Λ-module.

We will aim to develop a theory of Kolyvagin systems to study Selmer groups defined on $\mathbf{T}$. We will use the patched cohomology setting, as in Definition 3.3.1.

Notation 4.1.2. We denote $\mathbf{T}_{n,m} = \mathbf{T}/(p^n, X^m)\mathbf{T}$.

The definition of patched Selmer structures for these Galois representations is included in Definition 3.3.1. But the definition of patched cartesian Selmer structures, established in Definition 3.3.15, was exclusive for discrete valuation rings. However, a similar definition applies to Iwasawa Selmer modules.

Definition 4.1.3. (Cartesian local condition) A local condition $\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T) \subset \mathbf{H}^1(K_\mathfrak{u}, T)$ is called *cartesian* if $H^1_{/\mathcal{F}}(K_\mathfrak{u}, T)$ is a torsion-free R-module. A Selmer structure is said to be cartesian is all of its local conditions are cartesian.

Proposition 4.1.4. Let $\mathcal{F}$ be a cartesian Selmer structure and let $f \in \Lambda$. Then there is an injection

$$\mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T})/f\mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T}) \hookrightarrow \mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T}/f\mathbf{T})$$

Proof. Let $\mathfrak{n}$ be the product of the ultraprimes in $\Sigma_{\mathcal{F}}$. Consider the exact sequence

$$0 \longrightarrow \mathbf{T} \longrightarrow \mathbf{T} \longrightarrow \mathbf{T}/f\mathbf{T} \longrightarrow 0$$

long cohomological exact sequence induces an injection

$$\mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T})/f\mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}) \hookrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}/f\mathbf{T})$$

Since $\prod_{\mathfrak{u}\in\Sigma_{\mathcal{F}}} \mathbf{H}^1(K_{\mathfrak{u}}, \mathbf{T})$ contains no f-torsion, there is another injection

$$\mathbf{H}^1_{\mathcal{F}}(K^{\mathfrak{n}}/K, \mathbf{T})/f\mathbf{H}^1_{\mathcal{F}}(K^{\mathfrak{n}}/K, \mathbf{T}) \hookrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T})/f\mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T})$$

which completes the proof. □

We want to prove an analogue with quotients by the elements divisible by the maximal ideal $\mathfrak{m}$. Since the maximal ideal is not principal, we need to impose an extra assumption on $H^2(K, \mathbf{T})$ containing no finite Λ-submodules.

Assumption 4.1.5. The cohomology group $\mathbf{H}^2(K, \mathbf{T})$ contains no finite Λ-submodules.

Proposition 4.1.6. Let $\mathcal{F}$ be a cartesian Selmer structure and recall $\mathfrak{m}$ is the maximal ideal of Λ. Then there is an injection

$$\mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T})/\mathfrak{m} \hookrightarrow \mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T}/\mathfrak{m})$$

comment of unramified patched cohomology

Proof. Recall that $\mathfrak{n}$ is the product of all the primes in $\Sigma_{\mathcal{F}}$. By Proposition 4.1.4,

$$\mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T})/X \hookrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}/X\mathbf{T}) \twoheadrightarrow \mathbf{H}^2(K^{\mathfrak{n}}/K, \mathbf{T})[X]$$

Snake's lemma induces another exact sequence

$$\mathbf{H}^2(K^{\mathfrak{n}}/K, \mathbf{T})[\mathfrak{m}] \longrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T})/\mathfrak{m} \longrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}/X\mathbf{T})/p$$

By Assumption 4.1.5, the first term vanishes, so the second map is injective. Now consider the exact sequence

$$0 \longrightarrow \mathbf{T}/X\mathbf{T} \xrightarrow{p} \mathbf{T}/X\mathbf{T} \longrightarrow \mathbf{T}/\mathfrak{m}\mathbf{T} \longrightarrow 0$$

It induces an injection

$$\mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}/X\mathbf{T})/p \hookrightarrow \mathbf{H}^1(K^{\mathfrak{n}}/K, \mathbf{T}/\mathfrak{m}\mathbf{T})$$

Combining it with the injection above, we obtain an injection

$$\mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T})/\mathfrak{m} \hookrightarrow \mathbf{H}^1_{\mathcal{F}}(K, \mathbf{T}/\mathfrak{m})$$

□

4.1.1 Suitable ultraprimes

This section is devoted to proving analogues of Propositions 1.2.21 and 1.2.27 in the setting of patched Iwasawa Selmer groups. The method we will use involves a recursive application of Proposition 1.2.21 to construct certain ultraprimes satisfying certain properties.

Proposition 4.1.7. Let $\mathbf{T}$ be a Galois representation over the Iwasawa algebra satisfying Assumptions 3.2.11 and 4.1.5. Assume that $\mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T})$ does not vanish. Then there is an ultraprime $\mathfrak{u}$ such that $\mathrm{loc}_{\mathfrak{u}} \neq 0$, whose construction involves two choices.

Proof. By Nakayama's lemma, there exists $\alpha \in \mathbf{H}^1(K,\mathbf{T}) \setminus \mathfrak{m}\mathbf{H}^1(K,\mathbf{T})$. Write

$$\alpha = (\alpha_{n,m}) \in \varprojlim_{n,m} \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{n,m}) = \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{n,m})$$

Since $\alpha \notin \mathfrak{m}\mathbf{H}^1(K,\mathbf{T})$, Proposition 4.1.6 implies that $\alpha_{1,1} \neq 0$. For every $a \in \mathbb{N}$, $\alpha_{a,a}$ projects to $\alpha_{1,1}$ under the map

$$\mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{a,a}) \to \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{1,1})$$

Hence $\alpha_{a,a}$ does not belong to the kernel of this projection, i.e.,

$$p^{a-1}X^{a-1}\alpha_{a,a} \neq 0$$

For every $a \in \mathbb{N}$, choose a sequence $\left(\alpha^{(i)}_{a,a}\right)$ representing $\alpha_{a,a}$. By the definition of ultraproduct and the closedness of ultrafilters under intersections, there is a set $S_a \in \mathcal{U}$ such that

$$p^{a-1}X^{a-1}\alpha^{(i)}_{a,a} \neq 0 \ \forall i \in S_a$$

Denote $\iota_a : \mathbb{N} \to S_a$ the unique increasing bijection.

For every a, we can choose, by Proposition 1.2.21, a Kolyvagin prime $\ell_a \in \mathcal{P}(T_{a,a})$ such that

$$\mathrm{loc}_{\ell_a}\left(p^{a-1}X^{a-1}\alpha^{\iota(a)}_{a,a}\right) \neq 0$$

This implies that the map

$$\mathrm{loc}_{\ell_a} : \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{a,a}) \to \mathbf{H}^1_{\mathrm{f}}(K,\mathbf{T}_{a,a})$$

is surjective.

Construct the ultraprime $\mathfrak{u}$ represented by the sequence $(\ell_a)_{a\in\mathbb{N}}$. Consider the maps

$$\mathrm{loc}_{\mathfrak{u}} : \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{a,a}) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}},\mathbf{T}_{a,a})$$

Since $\ell_a \in \mathcal{P}(T_{a,a})$ is a Kolyvagin ultraprime, $\mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}},T_{a,a})$ is a free, cyclic $\Lambda_{a,a}$-module.

For every $b \geq a$, the construction implies that

$$\mathrm{loc}_{\ell_b}\left(p^{b-1}X^{b-1}\alpha^{\iota(b)}_{b,b}\right) \neq 0$$

It implies that the top horizontal arrow of the following diagram is surjective.

$$\begin{array}{ccc} \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{b,b}) & \xrightarrow{\mathrm{loc}_{\ell_b}} & \mathbf{H}^1_{\mathrm{f}}(K_{\ell_b},\mathbf{T}_{b,b}) \\ \downarrow & & \downarrow \\ \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{a,a}) & \xrightarrow{\mathrm{loc}_{\ell_b}} & \mathbf{H}^1_{\mathrm{f}}(K_{\ell_b},\mathbf{T}_{a,a}) \end{array}$$

The rightmost vertical arrow is surjective because $\ell_b \in \mathcal{P}(T_{b,b})$. Therefore, the bottom horizontal arrow is also surjective.

By 3.1.17, the patched map

$$\mathrm{loc}_{\mathfrak{u}}:\ \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}_{a,a}) \to \mathbf{H}^1(K_{\mathfrak{u}},\mathbf{T}_{a,a})$$

is also surjective for all $a \in \mathcal{N}$. Since the inverse limit is right exact, the following map is also surjective

$$\mathrm{loc}_{\mathfrak{u}}:\ \mathbf{H}^1_{\mathcal{F}}(K,\mathbf{T}) \to \mathbf{H}^1(K_{\mathfrak{u}},\mathbf{T})$$

□

On the dual side, we can construct suitable Kolyvagin ultraprimes controlling the Selmer group.

Proposition 4.1.8. Let $\mathbf{T}$ be a Galois representation over the Iwasawa algebra satisfying Assumptions 3.2.11. Then there is some $\mathfrak{n} \in \mathcal{N}$ such that

$$\mathbf{H}^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,\mathbf{T}^*) = 0$$

Proof. Let $\{r^1,\dots,r^s\}$ be a basis of $\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*[\mathfrak{m}])$ as a k-vector space. By Lemmas 3.3.7 and 3.3.9, there is a sequence of Selmer structures $\mathcal{F}_i$ such that

$$\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*[\mathfrak{m}]) = \mathcal{U}_i\big(\mathbf{H}^1_{(\mathcal{F}_i)^*}(K,\mathbf{T}^*[\mathfrak{m}])\big)$$

For every $j \in \{1,\dots,s\}$ choose a sequence $(r_i^j)_{i\in\mathbb{N}}$, where $r_i^j \in H^1_{(\mathcal{F}_i)^*}(K,\mathbf{T}^*[\mathfrak{m}])$, representing r^j. There is a set of indices $S \in \mathcal{U}$ such that, for all $i \in S$, the set $\{r_i^1,\dots,r_i^s\}$ is a basis of $H^1_{(\mathcal{F}_i)^*}(K,\mathbf{T}^*[\mathfrak{m}])$.

For every $a \in S$, by Proposition 3.3.12, there is an injection

$$\mathbf{H}^1(K,\mathbf{T}^*[m]) \hookrightarrow \mathbf{H}^1(K,\mathbf{T}^*_{a,a})$$

For every $j \in \{1,\dots,s\}$ and $a \in \mathbb{N}$, we can choose a Kolyvagin prime in $\ell_a^j \in \mathcal{P}(T_{a,a})$ satisfying that

$$\mathrm{loc}_{\ell_a^j}(r_{a^j}) \neq 0$$

Choose ultraprimes $\mathfrak{u}^1 = (\mathfrak{u}_i^1)_{i\in\mathbb{N}},\dots,\mathfrak{u}^s = (\mathfrak{u}_i^s)_{i\in\mathbb{N}}$ satisfying that $\mathfrak{u}_a^j = \ell_a^j$ for each $j = 1,\dots,s$ and $a \in S$.

Define $n_a := \mathfrak{u}_a^1 \cdots \mathfrak{u}_a^s$ for each $a \in \mathbb{N}$. Then, we have that

$$H^1_{(\mathcal{F}_a)^*_{n_a}}(K, \mathbf{T}^*[\mathfrak{m}]) = 0 \; foralla \in S$$

If $\mathfrak{n} = \mathfrak{u}^1 \cdots \mathfrak{u}^s$, Lemma 3.3.12 implies that

$$\mathbf{H}^1_{(\mathcal{F}^*)_\mathfrak{n}}(K, \mathbf{T}^*)[\mathfrak{m}] = \mathbf{H}^1_{(\mathcal{F}^*)_\mathfrak{n}}(K, \mathbf{T}^*[\mathfrak{m}]) = \mathcal{U}_a\big(H^1_{(\mathcal{F}_a)^*_{n_a}}(K, \mathbf{T}^*[\mathfrak{m}]) = 0\big) = 0$$

□

By combining choices of primes in the proofs of Propositions 4.1.7 and 4.1.8, we can obtain the following improved version of the last proposition.

Corollary 4.1.9. Let $\mathbf{T}$ be a Galois representation over the Iwasawa algebra satisfying Assumptions 3.2.11 and let $\mathcal{F}$ be a cartesian Selmer structure of positive core rank. Then there is some $\mathfrak{n} \in \mathcal{N}$ such that

$$\mathbf{H}^1_{(\mathcal{F}^*)_{(\mathfrak{n})}}(K, \mathbf{T}^*) = 0$$

Proof. By a combination of the proofs of Propositions 4.1.7 and 4.1.8, we can construct ultraprimes $\mathfrak{u}^1, \ldots, \mathfrak{u}^j$ such that

$$\mathrm{loc}_{\mathfrak{u}^j} : \; \mathbf{H}^1_{\mathcal{F}(\mathfrak{u}^1 \ldots \mathfrak{u}^{j-1})}(K, \mathbf{T}) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}^j}, \mathbf{T})$$

is surjective for each $j = 1, \ldots, s$ and

$$\mathbf{H}^1_{(\mathcal{F}^*)_\mathfrak{n}}(K, \mathbf{T}^*) = 0$$

Indeed, we can construct the ultraprimes in Proposition 4.1.8 individually satisfying Proposition 4.1.7, since $\mathbf{H}^1_{\mathcal{F}(\mathfrak{u}^1 \ldots \mathfrak{u}^{j-1})}(K, \mathbf{T}) \neq 0$ since the core rank of $\mathcal{F}(\mathfrak{u}^1 \ldots \mathfrak{u}^{j-1})$ is positive. complete □

4.2 Stark Systems

Let $m, n \in \mathcal{N}$ be square-free products of Kolyvagin ultraprimes such that $m \mid n$. There is an exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}^m}(K, T) \longrightarrow \mathbf{H}^1_{\mathcal{F}^n}(K, T) \longrightarrow \prod_{\ell \mid \frac{n}{m}} \mathbf{H}^1_{\mathrm{s}}(K_\ell, T)$$

By proposition **??**, this exact sequence induces a map

$$\Phi_{n,m} : \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(K, T) \to \bigcap^{r+\nu(m)} \mathbf{H}^1_{\mathcal{F}^m}(K, T)$$

Remark 4.2.1. Note that the map $\Phi_{n,m}$ is dependent on a choice of an isomorphism $\mathbf{H}^1_{\mathrm{s}}(\mathbb{Q}, T) \cong R$, or equivalently, an element in $\mathbf{H}^1_{\mathrm{s}}(K_\ell, T)^\times$. From now on, we assume we have fixed such isomorphism for every $\ell \in \mathcal{P}$.

Lemma 4.2.2. Let $\mathfrak{m}, n, r \in \mathcal{N}$ be square-free products of Kolyvagin ultraprimes such that $m \mid n \mid r$. Then

$$\phi_{r,m} = \phi_{r,n} \circ \phi_{n,m}$$

Proof. do □

Therefore, the set of maps $\phi_{n,m}$ forms an inverse system, so it makes sense to consider the elements in the inverse limit.

Definition 4.2.3. The set of Stark systems of $\mathcal{F}$ is defined as the inverse limit

$$\mathbf{SS}(\mathcal{F}) := \varprojlim_{n \in \mathcal{N}} \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, T)$$

4.2.1 The module of Stark systems

Definition 4.2.3 might seem abstract, but the Stark systems can be controlled by their values at some particular $n \in \mathcal{N}$.

Definition 4.2.4. A *weak core vertex* of rank r is a square-free product of ultraprimes $n \in \mathcal{N}$ such that $\mathbf{H}^1_{\mathcal{F}^*_n}(\mathbb{Q}, \mathbf{T}^*) = 0$ and $\mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})$ is a free Λ-module of rank $r + \nu(n)$.

prove existence of weak core vertices

comments on the rank

The main theorem of this section shows that the Starks systems are controlled by their values at weak core vertices.

Theorem 4.2.5. Let $n \in \mathcal{N}$ be a core vertex. Then the projection map

$$\mathbf{SS}(\mathcal{F}) \to \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})$$

is an isomorphism.

Lemma 4.2.6. Let $n \in \mathcal{N}$ be a weak core vertex and let $m \in \mathcal{N}$ be such that $n \mid m$. Then m is also a weak core vertex.

Proof. Since $n \mid m$, then $\mathbf{H}^1_{\mathcal{F}_m}(\mathbb{Q}, T)$ is contained in $\mathbf{H}^1_{\mathcal{F}_n}(\mathbb{Q}, T)$, so it also vanishes. The exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T}) \longrightarrow \mathbf{H}^1_{\mathcal{F}^m}(\mathbb{Q}, \mathbf{T}) \longrightarrow \bigoplus_{\mathfrak{u} \mid \frac{m}{n}} \mathbf{H}^1_s(\mathbb{Q}_\mathfrak{u}, \mathbf{T}) \longrightarrow 0$$

The first and third terms of this exact sequence are free modules of ranks $r + \nu(n)$ and $\nu(m) - \nu(n)$. Hence $\mathbf{H}^1_{\mathcal{F}^m}(\mathbb{Q}, \mathbf{T})$ is free of rank $r + \nu(n)$. □

Proof of Theorem 4.2.5. We only need to prove that if $n \in \mathcal{N}$ is a core vertex and $\ell \in \mathcal{P}$ does not divide n, the map

$$\bigcap^{r+\nu(n\ell)} \mathbf{H}^1_{\mathcal{F}^{n\ell}}(\mathbb{Q}, \mathbf{T}) \to \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})$$

is an isomorphism. This map is induced by the exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T}) \longrightarrow \mathbf{H}^1_{\mathcal{F}^{n\ell}}(\mathbb{Q}, \mathbf{T}) \longrightarrow \mathbf{H}^1_s(\mathbb{Q}_\ell, \mathbf{T}) \longrightarrow 0$$

Since $\mathrm{Ext}^1(\Lambda, \Lambda) = 0$, the dual map $\mathbf{H}^1_{\mathcal{F}^{n\ell}}(\mathbb{Q}, \mathbf{T})^+ \to \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})^+$ is surjective. Hence we can construct an injective map

$$\bigwedge^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})^+ \to \bigwedge^{r+\nu(n\ell)} \mathbf{H}^1_{\mathcal{F}^{n\ell}}(\mathbb{Q}, \mathbf{T})^+$$

which turns out to be an isomorphism since both are free Λ-modules of rank 1. Therefore, its dual map is also an isomorphism. □

If we assume the existence of core vertices, we know that the module of Stark systems is free of rank one.

Assumption 4.2.7. There exist an integer r and $n \in \mathcal{N}$ such that $\mathbf{H}^1_{\mathcal{F}^*}(\mathbb{Q}, \mathbf{T}^*) = 0$ and $\mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q}, \mathbf{T})$ is a free Λ-module of rank $r + \nu(n)$.

Corollary 4.2.8. Under assumption 4.2.7, the module of Stark systems $\mathbf{SS}(\mathcal{F})$ is a free Λ-module of rank one. The generators of $\mathbf{SS}(\mathcal{F})$ are called *primitive* Stark systems.

Theorem 4.2.9. Let $\varepsilon = (\varepsilon)_{n\in\mathcal{N}}$ be a generator of $\mathbf{SS}(\mathcal{F})$. For every $m \in \mathcal{N}$, the image of $\varepsilon_m \in \mathrm{Hom}\left(\bigwedge^{r+\nu(m)} \mathbf{H}^1_{\mathcal{F}^m}(K, \mathbf{T})^+, \Lambda\right)$ contains the 0^{th} Fitting ideal of $\mathbf{H}^1_{\mathcal{F}^*_m}(\mathbb{Q}, \mathbf{T}^*)$ with finite index.

Proof. By Assumption 4.2.7 and Lemma 4.2.6, there exists a core vertex n such that $m \mid n$, which leads to the following exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}^n}(K, \mathbf{T}) \longrightarrow \mathbf{H}^1_{\mathcal{F}^m}(K, \mathbf{T}) \longrightarrow \textstyle\prod_{\mathfrak{u}|n/m} \mathbf{H}^1_{\mathrm{s}}(K_\mathfrak{u}, \mathbf{T}) \longrightarrow \mathbf{H}^1_{\mathcal{F}^*_m}(K, \mathbf{T}^*) \longrightarrow 0$$

which induces a map

$$\phi_{n,m} : \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(K, \mathbf{T}) \to \bigcap^{r+\nu(m)} \mathbf{H}^1_{\mathcal{F}^m}(K, \mathbf{T})$$

Since ε generates $\mathbf{SS}(\mathcal{F})$, Theorem 4.2.5 implies that ε_n generates $\bigcap^{r+\nu(n)}$. Since $\varepsilon_m = \phi_{n,m}(\varepsilon_n)$, then proposition A.2.14 implies that the image of ε_n contains $\mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}_m}(\mathbb{Q}, \mathbf{T}^*))$ with finite index. □

4.2.2 Higher Fitting ideals of the Selmer group

Stark systems also determine the higher Fitting ideals of Selmer group. For that, we need to define a sequence of theta ideals associated to a Stark system, similarly to the ones defined previously to Kolyvagin systems.

Definition 4.2.10. Let $\varepsilon = (\varepsilon_n)_{n\in\mathcal{N}} \in SS(\mathcal{F})$ be an Stark system. For each non-negative integer i, we define the i^{th} theta ideal by

$$\Theta_i(\varepsilon) = \sum_{n\in\mathcal{N}_i} \mathrm{Im}(\varepsilon_n)$$

where ε_n is understood as an element of $\mathrm{Hom}\left(\bigwedge^{r+\nu(m)} \mathbf{H}^1_{\mathcal{F}^m}(K,\mathbf{T})^+, \Lambda\right)$.

4.3 Kolyvagin systems

4.3.1 Definition of Kolyvagin systems

The exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}(n)_\ell}(\mathbb{Q},T) \longrightarrow \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q},T) \longrightarrow \mathbf{H}^1_{\mathrm{f}}(\mathbb{Q}_\ell,T) \cong \Lambda$$

induces a map, using proposition **??**

$$\nu_\ell : \bigcap^{r} \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q},T) \to \bigcap^{r-1} \mathbf{H}^1_{\mathcal{F}(n)_\ell}(\mathbb{Q},T)$$

On the other hand, the exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}(n)_\ell}(\mathbb{Q},T) \longrightarrow \mathbf{H}^1_{\mathcal{F}(n\ell)}(\mathbb{Q},T) \longrightarrow \mathbf{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell,T) \cong \Lambda$$

induces a map

$$\varphi^{\mathrm{fs}}_\ell : \bigcap^{r} \mathbf{H}^1_{\mathcal{F}(n\ell)}(\mathbb{Q},T) \to \bigcap^{r-1} \mathbf{H}^1_{\mathcal{F}(n)_\ell}(\mathbb{Q},T)$$

Definition 4.3.1. A *Kolyvagin system* of rank r is an element

$$(\kappa_n)_{n\in\mathcal{N}} \in \prod_{n\in\mathcal{N}} \bigcap_{r} \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q},T)$$

satisfying for all $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$ not dividing n that

$$\varphi^{\mathrm{fs}}_\ell(\kappa_{n\ell}) = \nu_\ell(\kappa_n)$$

4.3.2 Regulator map

The exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q},T) \longrightarrow \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q},T) \longrightarrow \textstyle\prod_{\ell|n} \mathbf{H}^1_{\mathrm{f}}(\mathbb{Q}_\ell,T) \;\cong \Lambda^{\nu(n)}$$

induces, by propositon **??**, a map

$$\mathrm{Reg}_n : \bigcap^{r+\nu(n)} \mathbf{H}^1_{\mathcal{F}^n}(\mathbb{Q},T) \to \bigcap^{r} \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q},T)$$

Theorem 4.3.2. Combined for all $n \in \mathcal{N}$, the maps Reg_n induce a regulator map

$$\mathrm{Reg}: \ \mathbf{SS}(\mathcal{F}) \to \mathbf{KS}(\mathcal{F})$$

Proof. □

Theorem 4.3.3. The regulator map $\mathrm{Reg}: \ \mathbf{SS}(\mathcal{F}) \to \mathbf{KS}(\mathcal{F})$ is an isomorphism.

Theorem 4.3.4. Let κ be a primitive Kolyvagin system. Then $\mathrm{Im}(\kappa_n)$ contains the Fitting ideal $\mathrm{Fitt}_0\left(\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*)^\vee\right)$ with finite index.

Proof. Since κ is a primitive Kolyvagin system, theorem 4.3.2 implies the existence of a primitive Stark system $\varepsilon = (\varepsilon_n)_{n\in\mathcal{N}}$ such that $\mathrm{Reg}(\epsilon) = \kappa$.

Let m be a core vertex such that $n \mid m$. Consider the exact sequence

$$0 \longrightarrow \mathbf{H}^1_{\mathcal{F}(n)}(\mathbb{Q}, T) \longrightarrow \mathbf{H}^1_{\mathcal{F}^m}(\mathbb{Q}, T) \longrightarrow \bigoplus_{\ell|n} \mathbf{H}^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) \oplus_{\ell|m/n} \mathbf{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T)$$

$$\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*)^\vee \longrightarrow 0$$

The map induced by proposition **??** is $\mathrm{Reg}_n \circ \phi_{m,n}$ and sends ε_m to κ_n. Hence, by proposition A.2.14, $\mathrm{Im}(\kappa_n)$ contains $\mathrm{Fitt}_0\left(\mathbf{H}^1_{\mathcal{F}}(\mathbb{Q}, T^*)^\vee\right)$ with finite index. □

Corollary 4.3.5. For every $\kappa \in \mathrm{KS}(\mathbf{T})$ and every height 1 prime ideal of Λ, the localization $\mathrm{Im}(\kappa_n)$ is contained in $\mathrm{Fitt}_0\left(\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*)^\vee\right)_\beta$.

Proof. Then κ is primitive, the corollary follows from Theorem 4.3.4 since the localization at β of every finite Λ-module vanishes.

When κ is not primitive, then $\kappa = f\widetilde{\kappa}$ for some $f \in \Lambda$ and some primitive Kolyvagin system $\widetilde{\kappa}$. Since the result is true for $\widetilde{\kappa}$ and $\mathrm{Im}(\kappa_n) \subset \mathrm{Im}(\widetilde{\kappa}_n)$, the corollary also holds for κ. □

4.4 Structure of the Selmer group

4.4.1 Fitting ideal and Λ-modules up to pseudo-isomorphism

Let M be a Λ module which admits a pseudo-isomorphism

$$M \cong \Lambda^r \times \prod_{i=1}^{s} \Lambda^s$$

4.4.2 Fitting ideals of the Selmer groups

Lemma 4.4.1. Let n be a core vertex. Then

$$\mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T})) = \sum_{\mathfrak{u}|n} \mathrm{Fitt}^{i-1}(\mathbf{H}^1_{(\mathcal{F}^*)_\mathfrak{u}}(K,\mathbf{T}))$$

Corollary 4.4.2.

$$\mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T})^\vee) = \sum_{\mathfrak{u}\in\mathcal{P}} \mathrm{Fitt}^{i-1}(\mathbf{H}^1_{(\mathcal{F}^*)_\mathfrak{u}}(K,\mathbf{T})^\vee)$$

Corollary 4.4.3.

$$\mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee) = \sum_{n\in\mathcal{N}^i(\mathcal{P})} \mathrm{Fitt}^0(\mathbf{H}^1_{(\mathcal{F}^*)_n}(K,\mathbf{T}^*)^\vee)$$

Corollary 4.4.4.

$$\sum_{n\in\mathcal{N}^i(\mathcal{P})} \mathrm{Fitt}^0(\mathbf{H}^1_{(\mathcal{F}^*)(n)}(K,\mathbf{T}^*)^\vee) \subset \mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee)$$

with finite index.

Proof. Since $\mathrm{Fitt}^0(\mathbf{H}^1_{(\mathcal{F}^*)_n}(K,\mathbf{T}^*)^\vee)$ is contained in $\mathbf{H}^1_{(\mathcal{F}^*)(n)}(K,\mathbf{T}^*)^\vee$, then

$$\mathrm{Fitt}^0(\mathbf{H}^1_{(\mathcal{F}^*)(n)}(K,\mathbf{T}^*)^\vee) \subset \mathrm{Fitt}^0(\mathbf{H}^1_{(\mathcal{F}^*)_n}(K,\mathbf{T}^*)^\vee)$$

Hence the proposition follows from □

Let κ be a primitive Kolyvagin system.

Definition 4.4.5. Let $\kappa \in \mathbf{KS}(\mathbf{T})$ be a Kolyvagin system. The i^{th} Theta ideal of κ is

$$\Theta_i(\kappa) := \sum_{n\in\mathcal{N}^i(\mathcal{P})} \mathrm{Im}(\kappa_n)$$

Proposition 4.4.6. Let $\kappa \in \mathbf{KS}(\mathbf{T})$. Then

$$\Theta_i(\kappa) \subset_{\mathrm{f}} \mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*))$$

Proof. By Theorem 4.3.4,

$$\mathrm{Im}(\kappa_n) \subset_{\mathrm{f}} \mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q},\mathbf{T}^*)^\vee)$$

Equivalently, for every height 1 prime ideal,

$$\mathrm{Im}(\kappa_n)_\beta \subset \mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q},\mathbf{T}^*)^\vee)_\beta$$

Hence, by corollary 4.4.4,

$$\Theta_i(\kappa)_\beta = \sum_{n\in\mathcal{N}^i(\mathcal{P})} \mathrm{Im}(\kappa_n)_\beta \subset \sum_{n\in\mathcal{N}^i(\mathcal{P})} \mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}(n)^*}(\mathbb{Q},\mathbf{T}^*)^\vee)_\beta \subset \mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee)_\beta$$

Since it holds for all height 1 prime ideals β,

$$\Theta_i(\kappa) \subset_{\mathrm{f}} \mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee)$$

□

Theorem 4.4.7. Let $\kappa \in \mathbf{KS}(\mathbf{T})$ be a primitive Kolyvagin system. Then

$$\mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee) \subset_{\mathrm{f}} \Theta_i(\kappa)$$

Proof. $\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee$ is a finitely generated Λ-module, so it admits a pseudo-isomorphism

$$\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee \approx \Lambda^r \times \prod_{i=1}^{s}\prod_{j=1}^{k_i} \Lambda/(f_i^{\alpha_{i,j}})$$

where r is a non-negative integer and f_i are either the prime p or irreducible distinguished polynomials.

An inductive application of Corollaries **??** and **??** proves the existence of ultraprimes $\mathfrak{u}_1,\dots,\mathfrak{u}_r,\mathfrak{v}_1,\dots\mathfrak{v}_t$, where t is the maximum of $k_1,\dots,k_s$ such that

$$\mathbf{H}^1_{(\mathcal{F}^*)(\mathfrak{u}_1\cdots\mathfrak{u}_\alpha)}(\mathbb{Q},\mathbf{T}) \approx \Lambda^{r-i} \times \prod_{i=1}^{s}\prod_{j=1}^{k_i} \Lambda/(f_i^{\alpha_{i,j}}) \quad \forall \alpha = 0,\dots,r$$

$$\mathbf{H}^1_{(\mathcal{F}^*)(\mathfrak{u}_1\cdots\mathfrak{u}_r\mathfrak{v}_1\cdots\mathfrak{v}_j)}(K,\mathbf{T}^*) \approx \prod_{i=1}^{s}\prod_{j=\beta+1}^{k_i} \Lambda/(f_i^{\alpha_{i,j}}) \quad \forall \beta = 0,\dots,t$$

If we define kn_i as the formal square-free product of the first i primes of $(\mathfrak{u}_1,\dots,\mathfrak{u}_r,\mathfrak{v}_1,\dots,kv_s)$, we obtain that

$$\mathrm{Fitt}^i(\mathbf{H}^1_{\mathcal{F}^*}(K,\mathbf{T}^*)^\vee) \subset_{\mathrm{f}} \mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}^*(\mathfrak{n}_i)})$$

By Theorem 4.3.4, the latter is contained up to finite index in Θ_i, so this proof is concluded. □

Chapter 5

Cartesian systems

5.1 The graph of cartesian Selmer structures

Definition 5.1.1. We consider the directed graph whose vertices are the cartesian Selmer structures on T and there is an arrow $\mathcal{G} \to \mathcal{F}$ joining two Selmer structures $\mathcal{F}$ and $\mathcal{G}$ whenever $\mathcal{F} \leq \mathcal{G}$.

Proposition 5.1.2. Let $\mathcal{F} \leq \mathcal{G}$ be cartesian Selmer structures. Then the module

$$\mathcal{L}_{\mathcal{G}/\mathcal{F}} = \bigoplus_{\mathfrak{u} \in \mathcal{U}(\mathbb{P})} \mathbf{H}^1_{\mathcal{G}/\mathcal{F}}(K_\mathfrak{u}, T) = \bigoplus_{\mathfrak{u} \in \mathcal{U}(\mathbb{P})} \frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u}, T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T)}$$

is a free, finitely generated R-module of rank $\chi(\mathcal{G}) - \chi(\mathcal{F})$.

Proof. Since $\mathcal{G}$ is cartesian, the R-module

$$\bigoplus_{\mathfrak{u} \in \mathcal{U}(\mathbb{P})} \mathbf{H}^1_{/\mathcal{G}}(K_\mathfrak{u}, T)$$

is torsion-free. Since $\mathcal{L}_{\mathcal{G}/\mathcal{F}}$ is a finitely-generated submodule, it is free by the structure theorem. By Proposition 3.3.10, there is an exact sequence

$$H^1_{\mathcal{F}}(K,T) \rightarrowtail H^1_{\mathcal{G}}(K,T) \longrightarrow \mathcal{L}_{\mathcal{G}/\mathcal{F}} \longrightarrow H^1_{\mathcal{F}^*}(K,T^*)^\vee \twoheadrightarrow H^1_{\mathcal{G}^*}(K,T^*)^\vee$$

By Proposition 3.3.19, we see that the rank of $\mathcal{L}_{\mathcal{G}/\mathcal{F}}$ is $\chi(\mathcal{G}) - \chi(\mathcal{F})$. □

We want to extend the definition of $\mathcal{L}_{\mathcal{G}/\mathcal{F}}$ for every pair of Selmer structures $\mathcal{F}$ and $\mathcal{G}$, not necessarily comparable.

Definition 5.1.3. Let $\mathcal{F}$ and $\mathcal{G}$ be cartesian Selmer structures. We define the *local quotient* as

$$\mathcal{L}_{\mathcal{G}/\mathcal{F}} := \bigoplus_{\mathfrak{u} \in \Sigma_{\mathcal{F}<\mathcal{G}}} \frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u}, T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T)} \oplus \bigoplus_{\mathfrak{u} \in \Sigma_{\mathcal{G}<\mathcal{F}}} \left(\frac{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T)}{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u}, T)} \right)^+$$

where $\Sigma_{\mathcal{F}<\mathcal{G}}$ (resp. $\Sigma_{\mathcal{G}<\mathcal{F}}$) is the set of ultraprimes $\mathfrak{u} \in \Sigma_\mathcal{F} \cup \Sigma_\mathcal{G}$ such that $\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T) \subset \mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u}, T)$ (resp. $\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u}, T) \subset \mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u}, T)$).

Proposition 5.1.4. Let $\mathcal{F} \leq \mathcal{G}$ be cartesian Selmer structures. There is a canonical homomorphism

$$\phi_{\mathcal{G},\mathcal{F}} : \bigcap^{\chi(\mathcal{G})} \mathbf{H}^1_{\mathcal{G}}(K,T) \otimes \det(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}}) \to \bigcap^{\chi(\mathcal{F})} \mathbf{H}^1_{\mathcal{F}}(K,T)$$

Proof. Since $\mathcal{L}_{\mathcal{G}/\mathcal{F}}$ is a free R-module of rank $\chi(\mathcal{G}) - \chi(\mathcal{F})$, Proposition A.2.10 constructs the map $\phi_{\mathcal{G},\mathcal{F}}$. □

Definition 5.1.5. Fix a base cartesian Selmer structure $\mathcal{F}_0$. For every cartesian Selmer structure $\mathcal{F}$, define

$$\mathbf{X}(\mathcal{F}) = \mathbf{X}_{\mathcal{F}_0}(\mathcal{F}) = \bigcap^{\chi(\mathcal{F})} \mathbf{H}^1_{\mathcal{F}}(K,T) \otimes \det(\mathcal{L}^+_{\mathcal{F}/\mathcal{F}_0})$$

Proposition 5.1.6. Let $\mathcal{F} \leq \mathcal{G}$ be two cartesian Selmer structures. Then there is a map

$$\phi_{\mathcal{G}/\mathcal{F}} : \mathbf{X}_{\mathcal{F}_0}(\mathcal{G}) \to \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$$

In order to prove this result, we need the following lemma.

Lemma 5.1.7. Let $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{F}_0$ be cartesian Selmer structures such that $\mathcal{F} \leq \mathcal{G}$. Then there is a canonical isomorphism

$$\det(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}_0}) = \det(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}}) \otimes \det(\mathcal{L}^+_{\mathcal{F}/\mathcal{F}_0})$$

Proof. We can split the determinant of $\mathcal{L}^+_{\mathcal{G}/\mathcal{F}}$ as

$$\det\big(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}_0}\big) = \det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}_0<\mathcal{G}}} \left(\frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}_0}(K_\mathfrak{u},T)}\right)^+\right) \otimes \det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{G}<\mathcal{F}_0}} \frac{\mathbf{H}^1_{\mathcal{F}_0}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u},T)}\right)$$

Here, all the summands are free R-modules, so we can identify them with their biduals. Since $\mathcal{F} \leq \mathcal{G}$, there is a partition $\Sigma_{\mathcal{F}_0<\mathcal{G}} = \Sigma_{\mathcal{F}\leq\mathcal{F}_0<\mathcal{G}} \sqcup \Sigma_{\mathcal{F}_0<\mathcal{F}\leq\mathcal{G}}$ Hence we can use Propositions A.2.3 and A.2.4 to split the first determinant as

$$\begin{aligned}
&\det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}_0<\mathcal{G}}} \left(\frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}_0}(K_\mathfrak{u},T)}\right)^+\right) = \\
&\det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}\leq\mathcal{F}_0<\mathcal{G}}} \left(\frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u},T)}\right)^+\right) \otimes \det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}\leq\mathcal{F}_0<\mathcal{G}}} \frac{\mathbf{H}^1_{\mathcal{F}_0}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u},T)}\right) \otimes \\
&\det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}_0<\mathcal{F}\leq\mathcal{G}}} \left(\frac{\mathbf{H}^1_{\mathcal{G}}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u},T)}\right)^+\right) \otimes \det\left(\bigoplus_{\mathfrak{u}\in\Sigma_{\mathcal{F}_0<\mathcal{F}\leq\mathcal{G}}} \left(\frac{\mathbf{H}^1_{\mathcal{F}}(K_\mathfrak{u},T)}{\mathbf{H}^1_{\mathcal{F}_0}(K_\mathfrak{u},T)}\right)^+\right)
\end{aligned}$$

Since $\mathcal{F} \leq \mathcal{G}$, the sets $\Sigma_{\mathcal{G}<\mathcal{F}_0}$ and $\Sigma_{\mathcal{F}\leq\mathcal{G}<\mathcal{F}_0} \sqcup \Sigma_{\mathcal{G}<\mathcal{F}\leq\mathcal{F}_0}$ coincide. Similarly, we can use Propositions A.2.3 and A.2.4 to split the determinant as

$$\det\left(\bigoplus_{u\in\Sigma_{\mathcal{G}<\mathcal{F}_0}} \frac{\mathbf{H}^1_{\mathcal{F}_0}(K_u,T)}{\mathbf{H}^1_{\mathcal{G}}(K_u,T)}\right) =$$
$$\det\left(\bigoplus_{u\in\Sigma_{\mathcal{F}\leq\mathcal{G}<\mathcal{F}_0}} \frac{\mathbf{H}^1_{\mathcal{F}_0}(K_u,T)}{\mathbf{H}^1_{\mathcal{F}}(K_u,T)}\right) \otimes \det\left(\bigoplus_{u\in\Sigma_{\mathcal{F}\leq\mathcal{G}<\mathcal{F}_0}} \left(\frac{\mathbf{H}^1_{\mathcal{G}}(K_u,T)}{\mathbf{H}^1_{\mathcal{F}}(K_u,T)}\right)^+\right)$$

By grouping the different terms, we obtain that

$$\det(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}_0}) = \det(\mathcal{L}^+_{\mathcal{G}/\mathcal{F}}) \otimes \det(\mathcal{L}^+_{\mathcal{F}/\mathcal{F}_0})$$

revise sign conventions with direct sums □

Proof of Proposition 5.1.6. By Lemma 5.1.7, tensoring the map from Proposition 5.1.4 with the identity on $\det(\mathcal{L}^+_{\mathcal{F}/\mathcal{F}_0})$, we obtain the desired map $\phi_{\mathcal{G}/\mathcal{F}}$. □

Proposition 5.1.8. The assignment $\mathcal{F} \to \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$ forms an inverse system indexed by the set of cartesian Selmer structure.

Proof. do □

Definition 5.1.9. We define the set of cartesian systems as the elements in the inverse limit

$$\mathrm{CART}_{\mathcal{F}_0} = \varprojlim_{\mathcal{F}} \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$$

where the limit is taken over all cartesian Selmer structures.

5.1.1 Core cartesian Selmer structures

Definition 5.1.10. A cartesian Selmer structure is called a *core structure* when

$$\mathbf{H}^1_{\mathcal{F}^*}(K,T) = 0$$

Proposition 5.1.11. Under Assumptions 3.2.11, for every cartesian Selmer structure $\mathcal{F}$, there is core structure G such that $\mathcal{F} \leq \mathcal{G}$.

Proof. complete □

Proposition 5.1.12. Let $\mathcal{F} \leq \mathcal{G}$ be two core Selmer structures. Then the map $\mathbf{X}_{\mathcal{F}_0}(\mathcal{G}) \to \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$ is an isomorphism.

Proof. complete □

Similarly to what happened with Kolyvagin and Stark systems, cartesian systems can be controlled by core Selmer structures.

Proposition 5.1.13. Let $\mathcal{F}$ be a core Selmer structure. Then the map

$$\mathrm{CART}_{\mathcal{F}_0} \to \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$$

is an isomorphism.

Proof. Let $c \in \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$. We will show that there is a unique $\varepsilon \in \mathrm{CART}$ such that $\varepsilon_{\mathcal{F}} = c$.

Let $\mathcal{G}$ be a cartesian structure. By Proposition 5.1.11, there is a core Selmer structure $\mathcal{H}$ such that $\mathcal{F} \leq \mathcal{H}$ and $\mathcal{G} \leq \mathcal{H}$. Since the maps $\phi_{\mathcal{H},\mathcal{F}} : \mathbf{X}(\mathcal{H}) \to \mathbf{X}(\mathcal{F})$ is an isomorphism by Proposition 5.1.12, the definition of the inverse limit implies that $\varepsilon_{\mathcal{G}}$ is the image of the $\varepsilon_{\mathcal{F}}$ under the map

$$\phi_{\mathcal{H},\mathcal{G}} \circ \phi_{\mathcal{H},\mathcal{F}}^{-1} : \ \mathbf{X}(\mathcal{F}) \to \mathbf{X}(\mathcal{G}) : \ \varepsilon_{\mathcal{F}} \to \varepsilon_{\mathcal{G}}$$

Hence, the element is determined by c. Morevoer, this definition clearly defines an element of CART, so the projection map is an isomorphism. □

We can now prove that the module of cartesian systems is free of rank one over R.

Proposition 5.1.14. Let $\mathcal{F}$ be a core Selmer structure. Then $\mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$ is a free, cyclic R-module.

Proof. □

Corollary 5.1.15. The module of cartesian systems $\mathrm{CART}_{\mathcal{F}_0}$ is a free, cyclic R-module.

5.2 Partial cartesian systems

In practice, constructing a cartesian system is complicated, and we are only able to construct classes for a subgraph of the cartesian Selmer structures. The goal of this section will be to establish conditions on the subgraph that guarantee that a collection of classes in the subgraph extend (uniquely) to a cartesian system.

Definition 5.2.1. Let G be a subgraph of the graph of cartesian Selmer structures in definition 5.1.1, denoted *partial cartesian graph.* A *partial cartesian system* for G is an element of the inverse limit

$$\mathrm{CART}_{\mathcal{F}_0}(G) = \varprojlim_{\mathcal{F} \in G} \mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$$

Therefore, a partial cartesian system is a collection of classes $\varepsilon_{\mathcal{F}}$ for every $\mathcal{F} \in G$ such that, for every arrow $\mathcal{G} \to \mathcal{F}$ in G, $\phi_{\mathcal{G},\mathcal{F}}(\varepsilon_{\mathcal{G}}) = \varepsilon_{\mathcal{F}}$.

Remark 5.2.2. For every partial cartesian graph, there is canonical restriction map

$$\mathrm{CART}_{\mathcal{F}_0} \to \mathrm{CART}_{\mathcal{F}_0}(G)$$

Kolyvagin and Stark systems are examples of partial cartesian systems.

Explain Kolyvagin and Stark systems

Notation 5.2.3. For every subgraph G of the cartesian Selmer structures. We denote by G_0 to the subgraph of G whose vertices are the core cartesian Selmer structures in G and the edges are the edges of G connecting two of those structures. We also denote the enhanced graph $\widetilde{G}$ by adding, whenever there is an arrow in G, $\mathcal{F} \to \mathcal{G}$, joining two core structures, an arrow in the opposite direction, $\mathcal{G} \to \mathcal{F}$. The reason for doing so is Proposition 5.1.12.

Proposition 5.2.4. Assume we have two paths

$$\mathcal{F} \to \mathcal{H}_1 \to \cdots \mathcal{H}_s \to \mathcal{G}$$
$$FF \to \mathcal{H}'_1 \to \cdots \mathcal{H}'_{s'} \to \mathcal{G}$$

Then the maps $\mathbf{X}_{\mathcal{F}_0}\mathcal{F} \to \mathbf{X}_{\mathcal{F}_0}(\mathcal{G})$ induced by both paths coincide.

Proof. □

The next results concern about situations in which the map in Remark 5.2.2 is surjective.

Proposition 5.2.5. Let $G = G_0$ be a connected partial cartesian graph whose vertices are core structures. Then the map in Remark 5.2.2 is an isomorphism.

Proof. For any two Selmer structures $\mathcal{F}$ and $\mathcal{G}$ in G_0, we can choose a path in $\widetilde{G}$.

$$\mathcal{F} \to \mathcal{H}_1 \to \cdots \to \mathcal{H}_s \to \mathcal{G}$$

By Proposition 5.1.12, there are isomorphisms

$$\mathbf{X}_{\mathcal{F}_0}(\mathcal{F}) \cong \mathbf{X}_{\mathcal{F}_0}(\mathcal{H}_1) \cong \cdots \cong \mathbf{X}_{\mathcal{F}_0}(\mathcal{H}_s) \cong \mathbf{X}_{\mathcal{F}_0}(\mathcal{G})$$

For every $\varepsilon \in \mathrm{CART}_{\mathcal{F}_0}(G_0)$, $\varepsilon_{\mathcal{F}}$ and $\varepsilon_{\mathcal{G}}$ are identified by this isomorphism. Hence, $\mathrm{CART}_{\mathcal{F}_0}(G_0)$ is isomorphic to $\mathbf{X}_{\mathcal{F}_0}(\mathcal{F})$.

Choose a core Selmer structure $\mathcal{F}$. By Proposition 5.1.13, the map in Remark 5.2.2 is the following isomorphism.

$$\mathrm{CART}_{\mathcal{F}_0} \cong \mathbf{X}_{\mathcal{F}_0}(\mathcal{F}) \cong \mathrm{CART}_{\mathcal{F}_0}(G)$$

□

Proposition 5.2.6. Let G be a non-empty partial cartesian graph

- The graph G_0 is connected.
- For every $\mathcal{F} \in G$, there is some core Selmer structure $\mathcal{G} \in G_0$ such that $\mathcal{F} \leq \mathcal{G}_0$.

Then the map in Remark 5.2.2 is an isomorphism.

Proof. The second assumption implies that G_0 is non-empty. By Proposition 5.2.5, there is an isomorphism

$$\mathrm{CART}_{\mathcal{F}_0} \to \mathrm{CART}_{\mathcal{F}_0}(G_0)$$

complete □

5.3 Higher dimensional Kolyvagin systems

5.3.1 Higher dimensional Kolyvagin primes

In this section, we assume the weaker version of Assumption 1.1.5.

Assumption 5.3.1. We assume the following assumptions:

- (T1) $T/\mathfrak{m}T$ is an irreducible $k[[G_K]]$-module.
- (T3) $H^1(K(T)_M/K, T) = H^1(K(T)_M/K, T^*) = 0$.
- (N1) $T/\mathfrak{m}T$ is not isomorphic to $T^*[\mathfrak{m}]$ as $k[[G_K]]$-modules.
- (N2) The image of the homomorphism $R \to \mathrm{End}(T)$ is contained in the image of $\mathbb{Z}_p[[G_{\mathbb{Q}}]] \to \mathrm{End}(T)$.

We are not assuming the existence of τ such that $T/(\tau-1)T$ is a free, cyclic R-module. However, there always exist $\tau \in G_K$ such that $T/(\tau-1)T$ is a free R-module of rank d.

Notation 5.3.2. Fix some $\tau \in G_{K_M}$ such that $T/(\tau-1)T \cong R^d$, minimizing the exponent d.

Similarly to Definition 1.1.8, we define the Kolyvagin primes $\ell \in \mathcal{P}_\tau$ as those not belonging to $\Sigma_{\mathcal{F}}$ and whose Frobenius automorphism is conjugate to τ in $\mathrm{Gal}(K(T)_M/K)$. We also denote by $\mathcal{N}_\tau$ (resp. by $\mathcal{N}_\tau^i$) to the set of square-free products of Kolyvagin primes (resp. square-free products of exactly i-primes).

Let $\ell \in \mathcal{P}_\tau$. Since Frob_ℓ is trivial in $\mathrm{Gal}(K_M/K)$, then comment there is an splitting

$$H^1(K_\ell, T) = H^1_{\mathrm{f}}(K_\ell, T) \oplus H^1_{\mathrm{tr}}(K_\ell, T)$$

which is a free R module of rank d.

For every $\mathfrak{u} = (\ell_i)_{i\in\mathbb{N}} \in \mathcal{P}_\tau$, we have some freedom in the choices of the primes at $\overline{Q}$ above ℓ_i. We can make this choices so $\mathrm{Frob}_{\mathfrak{u}} = \tau$ in $\mathrm{Gal}(K(T)_M/K)$, instead of being only conjugates. Then there is an isomorphism

$$H^1_{\mathrm{f}}(K_{\mathfrak{u}}, T) \cong T/(\mathrm{Frob}_{\mathfrak{u}} - 1)T = T/(\tau-1)T,\ c \mapsto c(\mathrm{Frob}_{\mathfrak{u}}) + (\tau-1)T$$

After fixing a generator of $\mathcal{G}_\ell$, there is another canonical ismorphisms.

$$\phi^{\mathrm{fs}}_{\mathfrak{u}} :\ H^1_{\mathrm{f}}(K_{\mathfrak{u}}, T) \to H^1_{\mathrm{tr}}(K_{\mathfrak{u}}, T)$$

5.3.2 Admissible elements

Definition 5.3.3. An element $\mathfrak{n} \in \mathcal{N}$ is said to be *admissible* if, for every $\mathfrak{u} \mid \mathfrak{n}$, the map

$$\mathrm{loc}_{\mathfrak{u}} :\ \mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}}}(K, T) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}}, T)$$

Denote by $\mathcal{A}$ the set of admissible $n \in \mathcal{N}$. For every admissible $\mathfrak{n} \in \mathcal{A}$, denote by $A_{\mathfrak{n},\mathfrak{u}}$ the minimal indivisible free R-subgroup of $\mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}}, T)$ containing $\mathrm{Im}(\mathrm{loc}_{\mathfrak{u}})$.

The next proposition gives a method to construct admissible products.

Proposition 5.3.4. Let $\mathfrak{u}_1, \dots, \mathfrak{u}_s \in \mathcal{P}$ be a set of Kolyvagin ultraprimes satisfying that for all $i = 1, \dots, s$,

- The image of $\mathrm{loc}_{\mathfrak{u}_i} : \mathbf{H}^1_{\mathcal{F}^{\mathfrak{u}_1 \cdots \mathfrak{u}_{i-1}}}(K, T) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T)$ is contained in a free rank 1 R-submodule.
- For every $j \in \{1, \dots, i-1\}$, we have that

$$\mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_1 \cdots \mathfrak{u}_{i-1}}_{\mathfrak{u}_i}}(K, T^*) + \mathbf{H}^1_{\mathcal{F}^*_{\mathfrak{u}_1 \cdots \mathfrak{u}_{i-1}}}(K, T^*) = \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_1 \cdots \mathfrak{u}_{i-1}}}(K, T^*)$$

Then $\mathfrak{n} := \mathfrak{u}_1 \cdots \mathfrak{u}_s$ is admissible.

Proof. Consider the exact sequence

$$\mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}_i}_{\mathfrak{u}_i}}(K, T) \rightarrowtail \mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}_i}}(K, T) \longrightarrow \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T) \longrightarrow \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{\mathfrak{n}/\mathfrak{u}_i}}(K, T^*)^\vee \twoheadrightarrow \mathbf{H}^1_{(\mathcal{F}^*)_{\mathfrak{n}/\mathfrak{u}_i}}(K, T^*)^\vee$$

Denote $r_i := \mathfrak{u}_1 \cdots \mathfrak{u}_{i-1}$ and $s_i := \mathfrak{u}_{i+1} \cdots \mathfrak{u}_s$. We claim that, for every $j = i+1, \dots, s$, the images of the maps

$$\begin{aligned} \mathrm{loc}^*_{\mathfrak{u}_i} :\ & \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i \mathfrak{u}_{i+1} \cdots \mathfrak{u}_{j-1}}}(K, T^*) \to \mathbf{H}^1_{\mathrm{s}}(K_{\mathfrak{u}_i}, T^*) \\ \mathrm{loc}^*_{\mathfrak{u}_i} :\ & \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i \mathfrak{u}_{i+1} \cdots \mathfrak{u}_{j-1} \mathfrak{u}_j}}(K, T^*) \to \mathbf{H}^1_{\mathrm{s}}(K_{\mathfrak{u}_i}, T^*) \end{aligned}$$

By the second assumption on the choice of the prime $\mathfrak{u}_j$ implies that

$$\mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i \mathfrak{u}_{i+1} \cdots \mathfrak{u}_{j-1} \mathfrak{u}_j}}(K, T^*) + H^1_{(\mathcal{F}^*)_{\mathfrak{u}_1 \cdots \mathfrak{u}_{j-1}}}(K, T^*) = \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i \mathfrak{u}_{i+1} \cdots \mathfrak{u}_{j-1}}}(K, T^*)$$

Since the second summand is contained in the kernel of $\mathrm{loc}_{\mathfrak{u}_i}$, the images of both maps coincide. By induction, we can construct an exact sequence

$$\mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}_i}_{\mathfrak{u}_i}}(K, T) \rightarrowtail \mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}_i}}(K, T) \longrightarrow \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T) \longrightarrow \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i}}(K, T^*)^\vee \twoheadrightarrow \mathbf{H}^1_{(\mathcal{F}^*)_{r_i}}(K, T^*)^\vee$$

Comparing it with the exact sequence

$$\mathbf{H}^1_{\mathcal{F}^{r_i}_{\mathfrak{u}_i}}(K, T) \rightarrowtail \mathbf{H}^1_{\mathcal{F}^{r_i}}(K, T) \longrightarrow \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T) \longrightarrow \mathbf{H}^1_{(\mathcal{F}^*)^{\mathfrak{u}_i}_{r_i}}(K, T^*)^\vee \twoheadrightarrow \mathbf{H}^1_{(\mathcal{F}^*)_{r_i}}(K, T^*)^\vee$$

we can see that the images of the following maps coincide:

$$\begin{aligned} \mathrm{loc}_{\mathfrak{u}_i} :\ & \mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}_i}}(K, T) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T) \\ \mathrm{loc}_{\mathfrak{u}_i} :\ & \mathbf{H}^1_{\mathcal{F}^{r_i}}(K, T) \to \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}_i}, T) \end{aligned}$$

The image of the second map is contained one-dimensional, free R-module by the first assumption on the choice of the prime $\mathfrak{u}_i$. Hence the image of the first map is also contained in a one-dimensional, free R-module. Since that holds for every prime divisor of $\mathfrak{n}$, then $\mathfrak{n}$ is admissible. □

5.3.3 Suitable higher dimensional Kolyvagin primes

The goal of this section is to adapt Proposition 1.2.27 to higher dimensional Kolyvagin primes. We adapt the proof of [MR04, Proposition 3.6.2] to this situation.

Proposition 5.3.5. Assume Assumptions 5.3.1. Let $C \subset \mathbf{H}^1(K,T)$ be a finitely-generated R-module and let $D \subset \mathbf{H}^1(K,T^*)$ be a cofinitely generated R-module. Assume $\tau \in G_{K_M}$ is as in Notation 5.3.2. Assume we have maps

$$\phi:\ C \to T/(\tau-1)T,\ \ \psi:\ D \to T^*/(\tau-1)T^*$$

Then there is a τ-Kolyvagin ultraprime $\mathfrak{u} \in \mathcal{P}_\tau$ such that the maps

$$\mathrm{loc}_{\mathfrak{u}}:\ C \to T/(\tau-1)T,\quad \mathrm{loc}^*_{\mathfrak{u}}:\ D \to T^*/(\tau-1)T^*$$

coincide with ϕ and ψ, respectively.

Proof. Since C is finitely generated, there exists a square-free product of ultraprimes $\mathfrak{n}$ such that $C \subset \mathbf{H}^1(K^{\mathfrak{n}}/K,T)$.

Denote by C_k the image of C under the projection to $\mathbf{H}^1(K,T/\mathfrak{m}^k)$ and by D_k the intersection of D with $\mathbf{H}^1(K,T^*)[\mathfrak{m}^k]$. The assumptions on C and D imply that both C_k and D_k are finite. Since C is finitely generated, it is compact, to it equal to

$$C = \varprojlim_k C_k \subset \varprojlim_k \mathbf{H}^1(K^{\mathfrak{n}}/K,T/\mathfrak{m}^k)$$

From ϕ and ψ, we obtain the maps

$$\phi_n:\ \mathbf{H}^1(K^{\mathfrak{n}}/K,T/\mathfrak{m}^k) \to T/(\mathfrak{m}^k,\tau-1)T,\quad \psi_m:\ \mathbf{H}^1(K,T^*[\mathfrak{m}^n]) \to T^*[\mathfrak{m}^k]/(\tau-1)T^*[\mathfrak{m}^k]$$

Let $(n_i)_{i\in\mathbb{N}}$ be a sequence of square-free integers representing $\mathfrak{n}$. Then

$$\mathbf{H}^1(K^{\mathfrak{n}}/K,T/\mathfrak{m}^k) = \mathcal{U}_i\big(H^1(K^{n_i}/K,T/\mathfrak{m}^k)\big)$$

result needed, there are subgroups $C_k^{(i)} \subset H^1(K^{n_i}/K,T/\mathfrak{m}^k)$ such that

$$C_k = \mathcal{U}_i\big(C_k^{(i)}\big)$$

Since C_k is finite, then $C_k \cong C_k^{(i)}$ for $\mathcal{U}$-many i. Let S_k be the set of indices for which this isomorphism holds. Then we have a decreasing sequence of sets $(S_k) \subset \mathcal{U}$. more comment

Claim: There exists a τ-Kolyvagin prime $\ell_k^i \in \mathcal{P}_\tau(T/\mathfrak{m}^k)$ not dividing n_i such that

$$\mathrm{loc}_{\ell_k^i}:\ C_k^{(i)} \hookrightarrow H^1(K^{n_i}/K,T/\mathfrak{m}^k) \to H^1_{\mathrm{f}}(K_{\ell_k^{(i)}},T/m^k) = T/(\mathfrak{m}^k,\tau-1)T$$

coincides with ϕ_k. Note that it implies that the map proof required

$$\mathrm{loc}_{\ell_k^i}:\ C_{k'}^{(i)} \to T/(\mathfrak{m}^{k'},\tau-1)$$

coincides with $\phi_{k'}$.

Consider the ultraprime $\mathfrak{u}$ represented by the sequence $(\ell_a^a)_{a\in\mathbb{N}}$.

complete □

5.4 Kolyvagin systems

Definition 2.1.3 can be generalised to this setting with the only modification of the original Kolyvagin primes in $\mathcal{P}$ to rank d Kolyvagin primes in $\mathcal{P}_\tau$.

Definition 5.4.1. A *τ-Kolyvagin system* for a Selmer structure $\mathcal{F}$

$$\kappa = \left\{ \kappa_{\mathfrak{n}} \in H^1_{\mathcal{F}(\mathfrak{n})}(K,T) : \ \mathfrak{n} \in \mathcal{A}_\tau \right\}$$

satisfying the following relation for every $\mathfrak{n} \in \mathcal{A}_\tau$ and $\mathfrak{u} \in \mathcal{P}_\tau$ not dividing $\mathfrak{n}$. By the definition of Selmer module, we have that

$$\mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}}) \in H^1_{\mathcal{F}(\mathfrak{n})}(K_{\mathfrak{u}},T) = H^1_{\mathrm{f}}(K_{\mathfrak{u}},T), \quad \mathrm{loc}_{\ell}(\kappa_{\mathfrak{n}\mathfrak{u}}) \in H^1_{\mathcal{F}(\mathfrak{n}\mathfrak{u})}(K_{\mathfrak{u}},T) = H^1_{\mathrm{tr}}(K_{\mathfrak{u}},T)$$

The collection κ is a Kolyvagin system if the following is satisfied

$$\mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}\mathfrak{u}}) = \phi^{\mathrm{fs}}_{\mathfrak{u}} \circ \mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}}) \tag{5.1}$$

for every $\mathfrak{n} \in \mathcal{A}_\tau$ and $\mathfrak{u} \in \mathcal{P}_\tau$ not dividing n.

We will aim to construct a partial cartesian system from the classes κ_n, where κ is a τ-Kolyvagin systems and $n \in \mathcal{N}_\tau$ is admissible.

Recall that, when $n \in \mathcal{A}_\tau$ is admissible, we had defined a free, cyclic R-submodule $A_{\mathfrak{n},\mathfrak{u}}$ such that

$$\mathrm{loc}_{\mathfrak{u}}\big(H^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}}}(K,T)\big) \subset A_{\mathfrak{n},\mathfrak{u}} \subset H^1_{\mathrm{f}}(K,T)$$

Proposition 5.4.2. Assume that $\mathbf{H}^1_{\mathcal{F}}(K,T) \neq \mathbf{H}^1_{\mathcal{F}_{\mathfrak{u}}}(K,T)$. Then $A_{\mathfrak{n},\mathfrak{u}}$ coincides for all admissible $\mathfrak{n}$ dividing $\mathfrak{u}$.

Choose a free R-module $B_{n,\mathfrak{u}}$ of rank $d-1$ such that

$$A_{\mathfrak{n},\mathfrak{u}} \oplus B_{\mathfrak{n},\mathfrak{u}} = H^1_{\mathrm{f}}(K,T)$$

We can define, for every admissible $\mathfrak{n} \in \mathcal{N}$, a Selmer structure $\mathcal{F}[\mathfrak{n}]$.

Definition 5.4.3. Let $\mathfrak{n} \in \mathcal{N}$ be admissible. Define the Selmer structure $\mathcal{F}[\mathfrak{n}]$ by the local conditions

$$\begin{cases} \mathbf{H}^1_{\mathcal{F}[n]}(K_{\mathfrak{u}},T) = B_n \oplus \phi^{\mathrm{fs}}_{\mathfrak{u}}(A_n) & \text{if } \mathfrak{u} \mid \mathfrak{n} \\ \mathbf{H}^1_{\mathcal{F}[n]}(K_{\mathfrak{u}},T) = \mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) & \text{if } \mathfrak{u} \nmid \mathfrak{n} \end{cases}$$

Proposition 5.4.4. Let $\kappa \in \mathrm{KS}_\tau(\mathcal{F})$. For every admissible $n \in \mathcal{N}_\tau$, $\kappa_n \in \mathbf{H}^1_{\mathcal{F}[n]}(K,T)$.

Proof. For every $\mathfrak{u} \nmid \mathfrak{n}$, then

$$\mathrm{loc}_{\mathfrak{u}}(\kappa_n) \in \mathbf{H}^1_{\mathcal{F}(n)}(K,T) = \mathbf{H}^1_{\mathcal{F}[n]}(K,T)$$

Alternatively, when $\mathfrak{u} \mid \mathfrak{n}$, we have that

$$\phi^{\mathrm{fs}}_{\mathfrak{u}} \circ \mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}/\mathfrak{u}}) = \mathrm{loc}_{\mathfrak{u}}(\kappa_k n)$$

Since $\mathfrak{n}$ is admissible, the definition of $A_{\mathfrak{n},\mathfrak{u}}$ implies that

$$\mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}/k\mathfrak{u}}) \in \mathrm{loc}_{\mathfrak{u}}\big(\mathbf{H}^1_{\mathcal{F}(\mathfrak{n}/\mathfrak{u})}(K,T)\big) \subset \mathrm{loc}_{\mathfrak{u}}\big(\mathbf{H}^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{u}}}(K,T)\big) \subset A_n$$

Therefore,

$$\mathrm{loc}_{\mathfrak{u}}(\kappa_{\mathfrak{n}}) \in \phi^{\mathrm{fs}}_{\mathfrak{u}}(A_{\mathfrak{n}}) \subset \mathbf{H}^1_{\mathcal{F}[n]}(K,T)$$

□

We can also define partially relaxed and restricted Selmer structures at admissible elements.

Definition 5.4.5. Let $\mathfrak{a},\mathfrak{b},\mathfrak{n} \in \mathcal{A}$ be admissible elements such that $\mathfrak{a} \mid \mathfrak{n}$, $\mathfrak{b} \mid \mathfrak{n}$ and $\mathfrak{a}$ and $\mathfrak{b}$ are pairwise coprime. The Selmer structure $\mathcal{F}[\mathfrak{n}^{\mathfrak{b}}_{\mathfrak{a}}]$ is defined by the local conditions

$$\begin{cases} \mathbf{H}^1_{\mathcal{F}[n^{\mathfrak{b}}_{\mathfrak{a}}]}(K_{\mathfrak{u}},T) = B_n & \text{if } \mathfrak{u} \mid \mathfrak{a} \\ \mathbf{H}^1_{\mathcal{F}[n^{\mathfrak{b}}_{\mathfrak{a}}]}(K_{\mathfrak{u}},T) = \mathbf{H}^1_{\mathrm{f}}(K_{\mathfrak{u}},T) \oplus \phi^{\mathrm{fs}}_{\mathfrak{u}}(A_n) & \text{if } \mathfrak{u} \mid \mathfrak{b} \\ \mathbf{H}^1_{\mathcal{F}[n^{\mathfrak{b}}_{\mathfrak{a}}]}(K_{\mathfrak{u}},T) = B_n \oplus \phi^{\mathrm{fs}}_{\mathfrak{u}}(A_n) & \text{if } \mathfrak{u} \mid \mathfrak{n}/\mathfrak{a}\mathfrak{b} \\ \mathbf{H}^1_{\mathcal{F}[n^{\mathfrak{b}}_{\mathfrak{a}}]}(K_{\mathfrak{u}},T) = \mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}},T) & \text{if } \mathfrak{u} \nmid n \end{cases}$$

Chapter 6

Selmer group of an elliptic curve

6.0.1 Main results

only copied

The aim of this section is to apply the results from the previous one to compute the Galois structure of the classical Selmer group of an elliptic curve (defined over $\mathbb{Q}$) over certain abelian extensions.

Throughout this section, let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ and let $p \geq 5$ be a prime number. Denote by N the conductor of E and by T the Tate module of E.

Assume the following hypothesis.

- (E1) The homomorphism $\rho : \ G_{\mathbb{Q}} \to \mathrm{Aut}(T)$ induced by the Galois action is surjective.
- (E2) Either the Manin constant c_0 or c_1 is prime to p.

Assumptions (E1) is necessary to ensure that T satisfies the assumptions **??**-**??**. Assumption (E2) is necessary to guarantee the integrality of the modular symbols, which will be defined below.

By the modularity theorem, there exist morphisms

$$\varphi_0 : \ X_0(N) \to E, \quad \varphi_1 : \ X_1(N) \to E$$

where $X_0(N)$ and $X_1(N)$ are the modular curves associated to the groups $\Gamma_0(N)$ and $\Gamma_1(N)$, respectively. We may choose φ_0 and φ_1 of minimal degree.

The modularity theorem also proves the existence of a newform f of weight 2 and level N associated to the isogeny class of E. Fixing a Néron differential ω_E, there exist some constants $c_0(E)$ and $c_1(E)$ such that[1]

$$\varphi_0^*(\omega) = c_0(E) 2\pi i f(\tau)\, d\tau, \quad \varphi_1^*(\omega) = c_1(E) 2\pi i f(\tau)\, d\tau$$

The Manin constant $c_0(E)$ is an integer (see [Edi91, proposition 2]) and is conjecturally equal to 1 if E is an X_0-optimal elliptic curve, i.e., the degree of φ_0 is minimal among

[1] We may choose φ_0 and φ_1 in a way that both $c_0(E)$ and $c_1(E)$ are positive.

all modular parametrizations of curves in the isogeny class of E (see [Man72, §5]). The conjecture was proven in [Maz78] if E is semistable. In particular, it is proven that, for an X_0-optimal elliptic curve, $c_0(E)$ is only divisible by 2 and primes of additive reduction. By (E1), E does not admit any p-isogeny. Hence $c_0(E)$ is conjecturally prime to p under assumption (E1).

The constant $c_1(E)$ was conjectured to be 1 for all elliptic curves by Stevens in [Ste89, conjecture 1].

By the modularity theorem, we can define for an elliptic curve the modular symbols of its associated modular form. In fact, if f is the modular form associated to the isogeny class of E, the modular symbol of E for some $\frac{a}{m} \in \mathbb{Q}$ is defined as

$$\lambda\left(\frac{a}{m}\right) := \int_{i\infty}^{\frac{a}{m}} 2\pi i f(z)\, dz$$

where the integral follows the vertical line in the upper half plane from the cusp at infinity to $\frac{a}{m} \in \mathbb{Q}$.

The modular symbols satisfy the following relation (see [WW22, lemma 5]):

$$\lambda\left(\frac{-a}{m}\right) = \overline{\lambda\left(\frac{a}{m}\right)}$$

We can consider the real and imaginary parts of the modular symbols and normalise them by one of the Néron periods $\Omega_E^{\pm}$ to obtain rational numbers carrying important arithmetic information.

$$\left[\frac{a}{m}\right]^{\pm} = \frac{\lambda\left(\frac{a}{m}\right) \pm \lambda\left(\frac{-a}{m}\right)}{2\Omega_E^{\pm}} \in \mathbb{Q} \tag{6.1}$$

Assumption (E2) is required to ensure that the denominator of $\left[\frac{a}{m}\right]^{\pm}$ is not divisible by p. Thus

$$\left[\frac{a}{m}\right]^{\pm} \in \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$$

Although we need the elliptic curve E to be defined over $\mathbb{Q}$ in order to apply the modularity theorem to make use of the modular symbols, we will study the properties of the Mordell-Weil group over a finite abelian extension $K/\mathbb{Q}$ satisfying the following hypotheses:

- (K1) $K/\mathbb{Q}$ is unramified at p and at every prime at which E has bad reduction.
- (K2) The degree $[K : \mathbb{Q}]$ is prime to p.
- (K3) $E(K_{\mathfrak{p}})[p] = \{O\}$ for every prime $\mathfrak{p}$ of K above p.
- (K4) All the Tamagawa numbers of E over K are prime to p.
- (K5) For every character χ of $\mathrm{Gal}(K/\mathbb{Q})$, the Iwasawa main conjecture localised at $X\Lambda$ holds for the modular form f_χ, which is defined in (6.2) below.

Throughout this section, denote by G the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Also, let d and c be the degree and the conductor of $K/\mathbb{Q}$, respectively. We will also denote by $\mathcal{O}_d$ the

ring of integers of $\mathbb{Q}_p(\mu_d)$ and $\Lambda_d := \Lambda \otimes \mathcal{O}_d$, where Λ is the Iwasawa algebra defined in §**??**.

Assumption (K5) deserves some comment. If $f = \sum_{n=1}^{\infty} a_n q^n$ is the newform associated to E, the χ-twist of f is defined as

$$f_\chi = \sum_{n=1}^{\infty} \chi(n) a_n q^n \in S_2(Y_1(N \operatorname{cond}(\chi)^2), \chi^2) \tag{6.2}$$

Remark 6.0.1. With this definition of f_χ, we have that

$$L(f_\chi, s) = L(E, \chi, s)$$

Indeed, the L-function of the twisted modular form is defined as

$$L(f_\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n) a_n}{n^s} = \prod_{\ell} \left(1 - \ell^{-s}\chi(\ell) a_\ell + \mathbf{1}_N(\ell)\ell^{1-2s}\chi(\ell)^2\right)^{-1}$$

where N is the level of f and $\mathbf{1}_N(\ell)$ is the trivial Dirichlet character modulo N, given by $\mathbf{1}_N(m) = 1$ if $\gcd(N, m) = 1$ and $\mathbf{1}_N(m) = 0$ otherwise.

This definition coincides with the motivic L-function of $T_pE \otimes \mathcal{O}_d(\chi)$, where χ is normalised such that $\chi(\ell) = \chi(\mathrm{Frob}_\ell)$, where Frob_ℓ denotes the arithmetic Frobenius. In this setting, when $\ell \neq p$, the Euler factor is

$$P_\ell(T)_\chi := \det_{\mathcal{O}_d \otimes \mathbb{Q}_\ell} \left(1 - \mathrm{Frob}_\ell^{-1} T | ((T_p \otimes \mathcal{O}_d(\chi))^*)^{I_\ell}\right) = 1 - \ell\chi(\ell) a_\ell T + \mathbf{1}_N(\ell)\ell\chi(\ell)^2 T^2$$

In case, $\ell = p$, one would obtain the same formula using Fontaine's period ring B_{crys}:

$$P_p(T)_\chi = \left(1 - \mathrm{Frob}_\ell^{-1} T | (T_p \otimes \mathcal{O}_d(\chi))^* \otimes B_{\mathrm{crys}}\right) = 1 - p\chi(p) a_p T + \mathbf{1}_N(p) p\chi(p)^2 T^2$$

Then the motivic L-function is defined as

$$L(T_pE \otimes \mathcal{O}_d(\chi), s) := \prod_{\ell} P_\ell(\ell^{-s}) = \prod_{\ell} (1 - \ell^{-s}\chi(\ell) a_\ell + \mathbf{1}_N(\ell)\ell^{1-2s}\chi(\ell)^2) = L(f_\chi, s)$$

We assume the Iwasawa main conjecture in the sense of Kato.

Conjecture 6.0.2. (Iwasawa main conjecture for f_χ in the sense of Kato) Define the Iwasawa algebra

$$H^1_{\mathrm{IW}}(\mathbb{Q}_\infty, T \otimes \mathcal{O}_d(\chi)) := \varprojlim_n H^1(\mathbb{Q}_n, T \otimes \mathcal{O}_d(\chi))$$

Also denote

$$X_\infty := \mathrm{Hom}(H^1_{\mathcal{F}_{\Lambda^*}}(\mathbb{Q}, (T \otimes \Lambda_d(\chi))^*), \mathbb{Q}_p/\mathbb{Z}_p)$$

Let $z_{\mathbb{Q}_\infty, \chi} \in H^1_{\mathrm{IW}}(\mathbb{Q}_\infty, T \otimes \chi)$ be the χ-twist of Kato's zeta element (see (6.8) and (6.14)). The Iwasawa main conjecture is the equality of Λ-ideals

$$\mathrm{char}\left(\frac{H^1_{\mathrm{IW}}(\mathbb{Q}_\infty, T \otimes \mathcal{O}_d(\chi))}{\Lambda z_{\mathbb{Q}_\infty, \chi}}\right) = \mathrm{char}(X_\infty)$$

Remark 6.0.3. By theorem **??**, conjecture 6.0.2 is equivalent to the primitivity of the χ-twisted Kato's Kolyvagin system over $\mathbb{Q}_\infty$. An argument analogous to remark 6.0.27 shows that this is equivalent to the primality of certain Kato's Kolyvagin system for f_χ.

Remark 6.0.4. Iwasawa main conjecture for f_χ was proven in [SU14, theorem 1] when p does not divide the level of f_χ, which, under our assumption (K1), is equivalent to E having good reduction at p, and the existence of an auxilliary prime $\ell \mid\mid N$ such that χ is unramified at ℓ and the reduction modulo ℓ of the Galois representation $\overline{\rho}_{f_\chi}$ satisfies that $\dim_{\mathbb{F}_\ell} \overline{\rho}_{f_\chi}^{\mathcal{I}_\ell} = 1$ and $\dim_{\mathbb{F}_\ell} \overline{\rho}_{f_\chi}^{G_{\mathbb{Q}_\ell}} = 0$.

The proof of the Iwasawa main conjecture was extended in [FW22, theorem 1.1] to some cases in which E has bad reduction at p, assuming the existence of the above auxiliary prime ℓ and that the semisimplification of $\overline{\rho}|_{G_{\mathbb{Q}_p}}$ is different to $\psi \oplus \psi$ and $\psi \oplus \chi_{\text{cyc}}\psi$ for any character ψ and the cyclotomic character χ_{cyc}.

However, assumption (K5) only assumes a weaker Iwasawa main conjecture: a special case of the following conjecture when $\beta = X\Lambda$.

Conjecture 6.0.5. (Localised Iwasawa main conjecture for f_χ) Let β be a height one prime ideal of Λ. The Iwasawa main conjecture localised at β is the equality

$$\text{ord}_\beta\left(\text{char}\left(\frac{H^1_{\text{IW}}(\mathbb{Q}_\infty, T \otimes \mathcal{O}_d(\chi))}{\Lambda z^\infty_{\mathbb{Q}_\infty,\chi}}\right)\right) = \text{ord}_\beta\left(\text{char}(X_\infty)\right)$$

We want to describe the Galois structure of the classical Selmer group $\text{Sel}(K, E[p^\infty])$. Indeed, the Selmer group $\text{Sel}(K, E[p^\infty])$ have a natural action of the Galois group $\text{Gal}(K/\mathbb{Q})$, in which the Galois automorphism acts by conjugation on the cohomology group. Hence, it has a $\mathbb{Z}_p[G]$-module structure, which is the one we are interested in.

By Shapiro's lemma (see [NSW00, proposition 1.6.4]), there is an isomorphism

$$H^1(K, T) \cong H^1\left(\mathbb{Q}, \text{Ind}_{G_K}^{G_\mathbb{Q}}(T)\right) \cong H^1(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$$

At this point, it is important to make a remark on the Galois action on $T \otimes \mathbb{Z}_p[G]$. In order to construct the Galois cohomology group $H^1(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$, we need $T \otimes \mathbb{Z}_p[G]$ to be endowed with a continuous action of $G_\mathbb{Q}$. It is given by the following formula:

$$\sigma(t \otimes x) = \sigma t \otimes \sigma x \ \forall \sigma \in G, \ \forall t \in T, \ \forall x \in \mathbb{Z}_p[G]$$

However, cohomological conjugation endowes $H^1(K, T)$ with a natural G-action. The way to see this action in $H^1(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$ is considering $T \otimes \mathbb{Z}_p[G]$ as a $\mathbb{Z}_p[G]$-module with the multiplication by the elements of G given by

$$\sigma(t \otimes x) = t \otimes x\sigma^{-1} \ \forall \sigma \in G, \ \forall t \in T, \ \forall x \in \mathbb{Z}_p[G]$$

When $T \otimes \mathbb{Z}_p[G]$ is a $\mathbb{Z}_p[G]$-module, then $H^1(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$ is also a $\mathbb{Z}_p[G]$-module. In this situation, Shapiro's lemma isomorphism respects the $\mathbb{Z}_p[G]$-structures.

We know study the local conditions used to define the Selmer group. Let ℓ be a rational prime and let v be a prime of K above ℓ. Denote by $G_{v/\ell}$ to the Galois group

$\mathrm{Gal}(K_v/\mathbb{Q}_\ell)$, which is canonically isomorphic to a subgroup of G. Shapiro's lemma can also be applied to the local cohomology groups.

$$H^1(K_v, T) \cong H^1\big(\mathbb{Q}, T \otimes \mathbb{Z}_p[G_{v/\ell}]\big)$$

The classical local condition at a prime v of K is defined as the image of the Kummer map.

$$H^1_{\mathcal{F}_{\mathrm{cl}}}(K_v, T) = \mathrm{Im}\Big(E(K_v)\widehat{\otimes}\mathbb{Z}_p \to H^1(K_v, T)\Big)$$

When $\ell \neq p$, this local condiction coincides with the finite cohomology subgroup:

$$H^1_{\mathcal{F}_{\mathrm{cl}}}(K_v, T) = \ker\Big(H^1(K_v, T) \to H^1(\mathcal{I}_{v/\ell}, T \otimes \mathbb{Q}_p)\Big)$$

where $\mathcal{I}_{v/\ell}$ is the inertia subgroup of $G_{v/\ell}$. When $\ell = p$, the classical condition can be described purely in terms of T, by using p-adic Hodge theory. In this case, the classical local condition coincides with the Bloch-Kato local condition defined in §**??**:

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(K_v, T) := \ker\Big(H^1(K_v, T) \to H^1(K_v, T \otimes B_{\mathrm{crys}})\Big)$$

The Bloch-Kato Selmer structure can be defined similarly for $H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[G_{v/p}])$:

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[G_{v/p}]) = \ker\Big(H^1(\mathbb{Q}_p, T \otimes \mathbb{Z}_p[G_{v/p}]) \to H^1(K_v, T \otimes \mathbb{Z}_p[G_{v/p}] \otimes B_{\mathrm{crys}})\Big)$$

The isomorphism given by Shapiro's lemma identifies both Bloch-Kato conditions:

$$H^1_{\mathcal{F}_{\mathrm{cl}}}(K, T) \cong H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$$

Since $\mathbb{Z}_p[G]$ is not a local ring, we cannot apply the general theory of Kolyvagin systems directly. Since the order of G is prime to p by (K2), we can split the Selmer group into character parts. In order to do that, we tensor it with $\mathcal{O}_d$.

We thus get an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathbb{Z}_p[G]) \otimes \mathcal{O}_d \cong H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d[G]) = \bigoplus_{\chi \in \widehat{G}} H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes e_\chi \mathcal{O}_d[G])$$

where e_χ is the idempotent element associated to the character χ, defined in (6.9) below.

Since $T \otimes e_\chi \mathcal{O}_d[G]$ is isomorphic to $T \otimes \mathcal{O}_d(\chi)$, where $\mathcal{O}_d(\chi)$ is $\mathcal{O}_d$ endowed with an action of G given by $\sigma x = \chi(\sigma)x$, we have an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathbb{Z}_p[G]) \otimes \mathcal{O}_d \cong \bigoplus_{\chi \in \widehat{G}} H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$$

Therefore, we can study the groups $H^1(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$ instead. The Galois structure of $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathbb{Z}_p[G])$ is completely determined by the $\mathcal{O}_d$ structure of $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$ of every χ (see §6.0.9 for examples of this process). Since $\mathcal{O}_d$ is a principal local ring, we can apply the general theory of Kolyvagin systems to study this cohomology group.

Knowing the Fitting ideals of the twisted Selmer groups, we can determine $H^1_{\mathcal{F}_{\mathrm{BK}}}(K, T)$ up to isomprphism.

Proposition 6.0.6. The Fitting ideals of $H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T)$ can be computed as:

$$\mathrm{Fitt}^i_{\mathbb{Z}_p[G]}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T)\big) = \mathbb{Z}_p[G] \cap \left(\sum_{\chi \in \widehat{G}} e_{\overline{\chi}} \, \mathrm{Fitt}^i_{\mathcal{O}_d}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(Q, T \otimes \mathcal{O}_d(\chi))\big) \right) \tag{6.3}$$

Moreover, there is an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T) \approx \bigoplus_i \mathbb{Z}_p[G]/I_i$$

where I_i are ideals of $\mathbb{Z}_p[G]$ satisfying that $I_{i-1} \subset I_i$ for all i and that

$$\mathrm{Fitt}^{i-1}_{\mathbb{Z}_p[G]} H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T) = I_i \, \mathrm{Fitt}^i_{Z_p[G]} H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T)$$

Proof. By the definition of the Fitting ideals, we can compute

$$\mathrm{Fitt}^i_{\mathbb{Z}_p[G]}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T)\big) = \mathrm{Fitt}^i_{\mathcal{O}_d[G]}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T) \otimes \mathcal{O}_d\big)$$

Since $\mathcal{O}_d[G] = \bigoplus_{\chi \in \widehat{G}} e_\chi \mathcal{O}_d[G]$, then

$$\mathrm{Fitt}^i_{\mathcal{O}_d[G]}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(K,T) \otimes \mathcal{O}_d\big) = \left(\sum_{\chi \in \widehat{G}} e_{\overline{\chi}} \, \mathrm{Fitt}^i_{\mathcal{O}_d}\big(H^1_{\mathcal{F}_{\mathrm{BK}}}(Q, T \otimes \mathcal{O}_d(\chi))\big) \right)$$

Then (6.3) follows from [AM69, proposition 1.17] since every ideal of $\mathbb{Z}_p[G]$ is a contracted ideal under the inclusion $\mathbb{Z}_p[G] \hookrightarrow \mathcal{O}_d[G]$. Indeed, if $G = C_{n_1} \times \cdots \times C_{n_s}$, where C_j represents the cyclic group of j elements and $n_i \mid n_{i-1}$ for all i. Hence,

$$\mathbb{Z}_p[G] \cong \mathbb{Z}_p[C_{n_1}][C_{n_2}] \cdots [C_{n_s}]$$

If $\mathcal{O}$ is an unramified discrete valuation ring with with residue field k and residue characteristic p and j is prime to p, then

$$\mathcal{O}[C_j] \approx \mathcal{O}[T]/(T^j - 1) \cong \bigoplus_k \mathcal{O}[T]/(f_k(T))$$

where $f_k(T)$ are the irreducible factors of $T^j - 1$, which are all distinct. By Gauss's and Hensel's lemmas, the reductions $\overline{f_k}(T)$ are irreducible in $k[T]$ and, therefore, $\mathcal{O}[T]/(f_k(T))$ are unramified discrete valuation rings.

By repeating this process for every cyclic factor of G, we obtain a decomposition

$$\mathbb{Z}_p[G] \approx \bigoplus_k \mathcal{O}_k$$

where every $\mathcal{O}_{k'}$ is an unramified discrete valuation ring, associated to a Galois orbit the characters $G \to \overline{\mathbb{Z}_p}$.

The above decomposition implies that every non-zero ideal in $\mathbb{Z}_p[G]$ is the product of maximal ideals. Since the zero ideal is contracted because the map $\mathbb{Z}_p[G] \to \mathcal{O}_d[G]$ is

injective, we just need to prove that the maximal ideals of $\mathbb{Z}_p[G]$ are contracted. Every maximal ideal of $\mathbb{Z}_p[G]$ is of the form

$$\mathfrak{m}_i = \bigoplus_{k \neq i} \mathcal{O}_k \oplus p\mathcal{O}_i$$

If e_i is the idempotent element associated to $\mathcal{O}_i$, then there are some characters $\chi_{i_1}, \ldots, \chi_{i_t} \in \widehat{G}$ such that

$$e_i = \sum_{j=1}^{t} e_{\chi_{i_1}}$$

Hence

$$m_i = \mathbb{Z}_p[G] \cap \left[\left(\sum_{j=1}^{t} e_{\chi_{i_1}} \right) p\mathcal{O}_d[G] + \left(1 - \sum_{j=1}^{t} e_{\chi_{i_1}} \right) \mathcal{O}_d[G] \right]$$

The second part of this proposition follows by applying the structure theorem of finitely generated modules over principal ideal domains to the discrete valuation rings in the decomposition of $\mathbb{Z}_p[G]$. □

We have already established the $\mathbb{Z}_p$-module and the Selmer structure we are going to study. In order to complete the Selmer triple, we need to establish which will be our set of Kolyvagin primes $\mathcal{P}$.

Definition 6.0.7. The Selmer triple we are going to study is defined as follows.

- $T = T_pE \otimes \mathcal{O}_d(\chi)$, where T_pE is the Tate module of the elliptic curve and $\mathcal{O}_d(\chi)$ is $\mathbb{Z}_p[\chi]$ twisted by a character χ of G with values in $\overline{\mathbb{Z}}_p$.
- The Selmer strucure is the Bloch-Kato Selmer structure (see definition **??**).
- The set of Kolyvagin primes $\mathcal{P}$ is formed by the good reduction primes that are unramified and split completely at $K/\mathbb{Q}$.

Remark 6.0.8. For every $k \in \mathbb{N}$, the set of primes $\mathcal{P} \cap \mathcal{P}_k$ is $\mathcal{P}_{k,K}$, i.e., the primes ℓ satisfying the following conditions.

- (PE0) E has good reduction at ℓ and ℓ is unramified in $K/\mathbb{Q}$.
- (PE1) $\ell \equiv 1 \mod p^k$.
- (PE2) $\widetilde{E}_\ell(\mathbb{F}_\ell)[p^k]$ is free of rank one over $\mathbb{Z}/p^k$.
- (PE3) ℓ splits completely in $K/\mathbb{Q}$.

In order to study the structure of $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$, we define some twists of the Kurihara numbers. Kurihara numbers were defined by M. Kurihara in [Kur14a] and [Kur14b]. In those articles, they were related to the structure of the Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$ and the veracity of the Iwasawa main conjecture. The definition given by M. Kurihara was the particular case of our definition 6.0.9 below when χ is the trivial character. In this definition, we twist the Kurihara numbers by the different characters χ of G, so we can get information about the structure of $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$.

Definition 6.0.9. Let $n \in \mathcal{N}(\mathcal{P}_{k,K})$ and let χ be a Dirichlet character of character of conductor c. We define the *twisted Kurihara number* as

$$\widetilde{\delta}_{n,\chi} = \sum_{a\in(\mathbb{Z}/cn\mathbb{Z})^*} \overline{\chi}(a)\left[\frac{a}{cn}\right]^{\chi(-1)} \left(\prod_{\ell|n} \log_{\eta_\ell}^p(a)\right) \in \mathcal{O}_d/p^{k_n} \tag{6.4}$$

where η_ℓ is a generator of $(\mathbb{Z}/\ell)^\times$ and $\log_{\eta_\ell}^p(a)$ is the unique $x \in \mathbb{Z}/p^k$ such that $\eta_\ell^{-x}a$ has order prime to p in $(\mathbb{Z}/\ell)^\times$ (see definition 6.0.34). Here k_n is the minimal $k \in \mathbb{N}$ such that $n \in \mathcal{N}_k$.

Remark 6.0.10. The definition of the twisted Kurihara numbers depends on the choice of the primive roots η_ℓ for the prime divisors ℓ of n. However, the p-adic valuation of $\delta_{n,\chi}$ is independent of this choice.

Remark 6.0.11. Note that for $n = 1$, the Birch formula in [MTT86, (I.8.6)] relates the twisted Kurihara number with the twisted special L-value:

$$\delta_{1,\chi} = \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^*} \overline{\chi}(a)\left[\frac{a}{c}\right]^{\chi(-1)} = \frac{1}{\tau(\overline{\chi})}\frac{L(E,\chi,1)}{\Omega_E^{\chi(-1)}}$$

where $\tau(\chi)$ is the Gauss sum of χ.

Definition 6.0.12. Define the quantities

$$\begin{aligned}
&\mathrm{ord}(\delta_{n,\chi}) := \max\{j \in \mathbb{N}\cup\{0,\infty\} : \delta_n \in p^j(\mathcal{O}_d/p^{k_n})\}\\
&\partial^{(i)}(\delta_\chi) := \min\{\mathrm{ord}(\delta_{n,\chi}) : n \in \mathcal{N}, \nu(n) = i\}\\
&\partial^{(\infty)}(\delta_\chi) = \min\{\partial^{(i)}(\delta_\chi) :\ i \in \mathbb{N}_0\}
\end{aligned}$$

In analogy with definition **??**, define the ideals $\Theta_{i,\chi}$ as

$$\Theta_{i,\chi} = p^{\partial^{(i)}(\delta_\chi)}\mathcal{O}_d \subset \mathcal{O}_d$$

The following theorem describes the group structure of the Bloch-Kato Selmer group of $T(\chi)$ in terms of the χ-twisted Kurihara numbers.

Theorem 6.0.13. Let $E/\mathbb{Q}$ and $p \geq 5$ be an elliptic curve and a prime number satisfying (E1)-(E2) and let $K/\mathbb{Q}$ be an abelian extension satisfying (K1)-(K5). Then $\partial^{(\infty)}(\widetilde{\delta}_\chi)$ is finite. Call r to the minimum i such that $\Theta_{i,\chi} \neq 0$ and s to the minimum j such that $\partial^{(j)}(\widetilde{\delta}_\chi) = \partial^{(\infty)}(\widetilde{\delta}_\chi)$. Also, denote by n_i the exponent $\Theta_{i,\chi} = (p)^{n_i}$ and $a_i = \frac{n_i - n_{i+2}}{2}$.

1. If $\chi = \overline{\chi}$, then

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T\otimes\mathcal{O}_d(\chi)) \approx \mathcal{O}_d^r \oplus (\mathcal{O}_d/p^{a_r})^2 \oplus (\mathcal{O}_d/p^{a_{r+2}})^2 \oplus \cdots \oplus (\mathcal{O}_d/p^{a_{s-2}})^2$$

2. If $\chi \neq \overline{\chi}$, then

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T\otimes\mathcal{O}_d(\chi)) \approx \mathcal{O}_d^r \oplus \mathcal{O}_d/p^{n_r - n_{r+1}} \oplus \mathcal{O}_d/p^{n_{r+1}-n_{r+2}} \oplus \cdots \oplus \mathcal{O}_d/p^{n_{s-1}-n_s}$$

Remark 6.0.14. Theorem 6.0.13 when $K = \mathbb{Q}$ is a result of C.H. Kim in [Kim25].

Remark 6.0.15. It is enough to prove theorem 6.0.13 for the primitive characters of G, i.e., those of conductor c. Indeed, if χ is a character of conductor m, consider $K_m = K \cap \mathbb{Q}(\mu_m)$. Note that χ is a primitive character of $\mathrm{Gal}(K_m/\mathbb{Q})$. Since $[K : K_m]$ is prime to p,

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(K_m, T) \cong H^1_{\mathcal{F}_{\mathrm{BK}}}(K, T)^{\mathrm{Gal}(K/K_m)}$$

Hence the χ parts of both Selmer group coincide. Hence if theorem 6.0.13 holds for K_m and χ, it also holds for K and χ.

Remark 6.0.16. When χ is the trivial character, M. Kurihara conjectured in [Kur14b] the existence of of some $n \in \mathcal{N}$ such that $\mathrm{ord}(\delta_n)$ is equal to zero. When p is a prime of ordinary reduction, M. Kurihara proved it under the assumptions of the non-degeneracy of the p-adic height pairing and the Iwasawa main conjecture (see [Kur14a, theorem B]). An analogue statement can be conjecured for other characters.

Conjecture 6.0.17. There exists some $n \in \mathcal{N}$ such that $\mathrm{ord}(\delta_{n,\chi}) = 0$. In other words, $\partial^{(\infty)}(\delta_{n,\chi}) = 0$.

When χ is the trivial character, R. Sakamoto proved in [Sak22, theorem 1.2] (see also [Kim25, theorem 1.11]) that M. Kurihara's conjecture is equivalent to the Iwasawa main conjecture.

Theorem 6.0.18. Let $E/\mathbb{Q}$ and $p \geq 5$ be an elliptic curve and a prime number satisfying (E1)-(E2), let $K/\mathbb{Q}$ be an abelian extension satisfying (K1)-(K5) and let χ be a character of $\mathrm{Gal}(K/\mathbb{Q})$. Then $\partial^{(\infty)}(\delta_\chi) = 0$ if and only if the Iwasawa main conjecture 6.0.2 holds true.

The rest of §6 is dedicated to the proofs of theorems 6.0.13 and 6.0.18. Theorem 6.0.13 is just an application of theorems **??** and **??**. In order to prove it, we need to check that the Selmer triple satisfies the assumptions of these theorems.

Proposition 6.0.19. The Selmer triple $(T \otimes \mathcal{O}_d(\chi), \mathcal{F}_{\mathrm{cl}}, \mathcal{P})$ satisfies the assumptions **??**-**??** made in §**??**.

Proof. Assumptions **??** and **??** are obvious. **??** holds from 6.0.8

Note that $\mathbb{Q}(T)$ is only ramified at p and at bad primes of E, so $\mathbb{Q}(T) \cap K$ is unramified at every prime by (K1). Since $\mathbb{Q}$ has class number 1, then $\mathbb{Q}(T) \cap K = \mathbb{Q}$. Therefore, every $\sigma \in \mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q})$ can be lifted to some $\widetilde{\sigma} \in G_{\mathbb{Q}}$ such that $\chi(\widetilde{\sigma}) = 1$.

Every basis of T as a $\mathbb{Z}_p$-module is a basis of $T \otimes \mathcal{O}_d(\chi)$ as an $\mathcal{O}_d$-module. After fixing such a basis, the representation induces a map $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_d)$. By (E1), the image of this map contains $\mathrm{GL}_2(\mathbb{Z}_p)$, so **??** and **??** hold true.

Let $\Delta \subset \mathrm{GL}_2(\mathcal{O}_d)$ be the subgroup formed by the matrices ζI, where I is the identity matrix and ζ is a $(p-1)^{\text{th}}$-root of unity. Since the image of the map $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_d)$ considered above contains $\mathrm{GL}_2(\mathbb{Z}_p)$, there is an inclusion $\Delta \hookrightarrow \mathrm{Gal}(\mathbb{Q}(T \otimes \mathcal{O}_d(\chi))/\mathbb{Q})$. If we denote the latter Galois group by H, consider the inflation-restriction sequence

$$0 \longrightarrow H^1\big(H/\Delta, (T/p \otimes \mathcal{O}_d(\chi))^{\Delta}\big) \longrightarrow H^1\big(H, T/p \otimes \mathcal{O}_d(\chi)\big) \longrightarrow H^1\big(\Delta, T/p \otimes \mathcal{O}_d(\chi)\big)$$

Since $T(\chi)^{\Delta} = 0$ and the order of Δ is prime to p, then $H^1(\mathbb{Q}(T\otimes\mathcal{O}_d(\chi))/\mathbb{Q}, T/p) = 0$. Therefore, **??** is proven since the Weil pairing implies that $\mathbb{Q}(T, \mu_p^{\infty}) = \mathbb{Q}(T)$ and $T/p \cong T^*[p]$.

For every $\ell \in \Sigma(\mathcal{F}_{cl})$ and every prime v of K above ℓ, let $G_{v/\ell} = \mathrm{Gal}(K_v/\mathbb{Q}_\ell)$ and let $H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_\ell, T\otimes\mathcal{O}_d(\chi))$ be the quotient $H^1(\mathbb{Q}_\ell, T\otimes\mathcal{O}_d(\chi))/H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_\ell, T\otimes\mathcal{O}_d(\chi))$. Since $\#G_v$ is prime to p,

$$H^1_{/\mathcal{F}_{\mathrm{BK}}}\big(\mathbb{Q}_\ell, T\otimes\mathcal{O}_d(\chi)\big) \cong H^1_{\mathcal{F}_{\mathrm{BK}}}\big(\mathbb{Q}_\ell, T^*\otimes\mathcal{O}_d(\overline{\chi})\big)^\vee \cong \Big(H^1_{\mathcal{F}_{\mathrm{BK}}}\Big(K_v, E[p^\infty]\otimes\mathcal{O}_d(\overline{\chi})\Big)^\vee\Big)_{G_{v/\ell}}$$

The last cohomology group vanishes when $\ell \neq p$. Otherwise, we can compute

$$H^1_{\mathcal{F}_{\mathrm{BK}}}\Big((K_v, E[p^\infty])^\vee\otimes\mathcal{O}_d(\chi)\Big)_{G_{v/p}} \cong \Big(\varprojlim_{n\in\mathbb{N}} E(K_v)/p^n\otimes\mathcal{O}_d(\chi)\Big)_{G_{v/p}} = \Big(E(K_v)\otimes\mathcal{O}_d(\chi)\Big)_{G_{v/p}} \tag{6.5}$$

Since $E(K_v)$ contains no p-torsion when $v \mid p$ by (K3), then $E(K_v)$ is a free of rank one $\mathbb{Z}_p[G_{v/p}]$-module. Hence $(E(K_v)\otimes\mathcal{O}_d(\chi))_{G_{v/p}}$ is torsion-free and $\mathcal{F}_{\mathrm{BK}}$ is cartesian by [MR04, lemma 3.7.1]. Thus **??** holds true.

Since $H^1_{\mathcal{F}_{\mathrm{cl}}}(K, T) = H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T\otimes\mathbb{Z}_p[G])$ is a self dual Galois representation by [DD09, theorem 1.1], we have that

$$H^1_{\mathcal{F}_{\mathrm{BK}}}\big(\mathbb{Q}, T/p^k\otimes\mathcal{O}_d(\chi)\big) \cong H^1_{\mathcal{F}_{\mathrm{BK}}}\big(\mathbb{Q}, T^*[p^k]\otimes\mathcal{O}_d(\overline{\chi})\big)$$

and hence $\chi(T\otimes\mathcal{O}_d(\chi), \mathcal{F}_{\mathrm{BK}}) = 0$, so **??** holds. For **??**, it holds for the prime p by (K3). Indeed, from the computation in (6.5), one can deduce that $H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi))$ is free of rank one over $\mathcal{O}_d$ and, from the local duality in proposition 1.1.18, we have that

$$H^2(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi)) \cong H^0(\mathbb{Q}_v, E[p^\infty]\otimes\mathcal{O}_d(\overline{\chi}))^\vee = 0 \qquad \square$$

The proof of theorems 6.0.13 and 6.0.18 is structured as follows. §6.0.2-§6.0.6 are dedicated to relate Kato's Euler system to the Kurihara numbers. In §6.0.2, we introduce Kato's Euler system for T_pE, originally constructed in [Kat04], and its link to the special L-values via the dual exponential map, following [Kat21]. In §6.0.3, we apply the twisting process explained in [Rub00, §II.4] to obtain an Euler systems for $T\otimes\mathcal{O}_d(\chi)$. In §6.0.4, we use the interpolation property of Mazur-Tate elements to relate them to Kato's Euler system. After applying the Kolyvagin derivative, we obtain a relation between Kato's Euler system and Kurihara numbers.

This relation is obtained through the dual exponential map. Therefore, it is necessary to compute the image of the integral cohomology group under the dual exponential map, as done in §6.0.5. With this computations, we can prove the equality between the orders of the twisted Kato's Kolyvagin system and the twisted Kurihara numbers in §6.0.6.

The proof of theorem 6.0.18, based on the equivalence between the Iwasawa main conjecture and the primitivity of Kato's Euler system, is concluded in §6.0.7. §6.0.8 is dedicated to the proof of theorem 6.0.13 as an application of theorems **??** and **??** and the functional equation of the Kurihara numbers ([Kur14b, lemma 5.2.1]).

6.0.2 Dual exponential map

K. Kato constructed in [Kat04] an Euler system for the Tate module of an elliptic curve T and defined an exponential map to relate this Euler system to the special values of the twisted L-functions of the elliptic curve.

Using the Néron differential ω_E we had already fixed, we can define the dual exponential map (see [BK90, definition 3.10])

$$\exp^*_{\omega_E} : \ H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, T) \otimes \mathbb{Q}_p \to F_\mathfrak{p}$$

where $F_\mathfrak{p}$ is the completion at a prime $\mathfrak{p}$ above p of an abelian extension $F/\mathbb{Q}$ and $H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, T)$ is the quotient $H^1(F_\mathfrak{p}, T)/H^1_{\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, T)$.

We will sketch the construction of the exponential map from [BK90]. The following is the fundamental short exact sequence from p-adic Hodge theory

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{crys}}^{\varphi=1} \oplus B^+_{\mathrm{dR}} \longrightarrow B_{\mathrm{dR}} \longrightarrow 0 \tag{6.6}$$

where B_{crys} and B_{dR} are the crystalline and de Rahm period rings. For $V := T \otimes \mathbb{Q}_p$, we denote

$$D_{\mathrm{crys}}(V) = (B_{\mathrm{crys}} \otimes V)^{G_{F_\mathfrak{p}}}, \quad D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes V)^{G_{F_\mathfrak{p}}}, \quad D_{\mathrm{dR}}(V)^+ = (B^+_{\mathrm{dR}} \otimes V)^{G_{F_\mathfrak{p}}}$$

If we consider the cohomological exact sequence in (6.6) tensored with V,

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow D_{\mathrm{crys}}(V)^{\varphi=1} \oplus D_{\mathrm{dR}}(V)^+ \longrightarrow D_{\mathrm{dR}}(V) \longrightarrow H^1_{\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, V) \longrightarrow 0$$

Since the tangent space of E is isomorphic to $D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}(V)^+$, this exact sequence induces a surjective map

$$\exp : \ \tan(E/F_\mathfrak{p}) \to H^1_{\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, V)$$

The dual ω_E^* of the Neron differential generates the tangent space of $E/F_\mathfrak{p}$ as an $F_\mathfrak{p}$-vector space, so we can consider the exponential as a map from $F_\mathfrak{p}$,

$$\exp_{\omega_E} : \ F_\mathfrak{p} \to H^1_{\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, V)$$

Its dual map is the one we will be interested in.

$$\exp^*_{\omega_E} : \ H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, V) \to \mathrm{Hom}(F_\mathfrak{p}, \mathbb{Q}_p)$$

We can identify the latter with $F_\mathfrak{p}$ via the following isomorphism

$$F_\mathfrak{p} \to \mathrm{Hom}(F_\mathfrak{p}, \mathbb{Q}_p), \ x \mapsto (y \mapsto \mathrm{Tr}_{F_\mathfrak{p}/\mathbb{Q}_p}(xy)) \tag{6.7}$$

The above map is defined for every Galois representation using p-adic Hodge theory. However, when T is the Tate module of an elliptic curve E, the exponential map has a geometrical meaning (see [BK90, example 3.10.1]). Note that in this case

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(F_\mathfrak{p}, T) = \varprojlim_n E(F_\mathfrak{p})/p^n$$

Then the exponential map coincides with the Lie group exponential map defined on the elliptic curve. Moreover, it can be also understood as the tensor with $\mathbb{Q}_p$ of the formal group exponential map defined on certain power of the maximal ideal of the ring of integers of $F_{\mathfrak{p}}$.

We will be interested in the image under this map of elements coming from the global cohomology group $H^1(F,T)$. In order to do that, we consider the localisation at a rational prime q as the direct sum of the localisation maps above every prime v above q

$$\mathrm{loc}_q^s:\ H^1(F,V)\to\bigoplus_{v|q} H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_v,V)$$

Then there is an Euler system $(z_F)_{F\in\Omega}$ satisfying the following interpolation property (see [Kat21], theorem 6.1). Fix an inclusion $\overline{\mathbb{Q}}\subset\mathbb{C}$; for every character ψ of $\mathrm{Gal}(F/\mathbb{Q})$, we have that

$$\sum_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}\psi(\sigma)\sigma(\exp^*_{\omega_E}(\mathrm{loc}_s^p(z_F)))=\frac{L_{S_F\cup\{p\}}(E,\psi,1)}{\Omega^{\psi(-1)}}\in F\otimes\mathbb{Q}_p \tag{6.8}$$

where S_F is the primes ramifying at $F/\mathbb{Q}$ and $\Omega^{\pm}$ denote the Néron periods of E. Here $L_{S_F\cup\{p\}}(E,\psi,1)$ is the $S_F\cup\{p\}$-truncated and ψ-twisted L-function, defined as

$$L_{S_F\cup\{p\}}(E,\psi,s)=\prod_{\ell\notin S_F,\ell\neq p}(1-a_\ell\psi(\ell)\ell^{-s}+\mathbf{1}_N(\ell)\psi(\ell)^2\ell^{1-2s})^{-1}$$

Call $w_F:=\exp^*_{\omega_E}(\mathrm{loc}_p^s(z_F))$ and, for every character ψ of $\mathrm{Gal}(F/\mathbb{Q})$, define the idempotent element as

$$e_\psi:=\frac{1}{[F:\mathbb{Q}]}\sum_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}\overline{\psi}(\sigma)\sigma\in\mathbb{Z}_p[\psi][\mathrm{Gal}(F/\mathbb{Q})] \tag{6.9}$$

where $\mathbb{Z}_p[\psi]$ is the ring obtained by adjoining the values of ψ to $\mathbb{Z}_p$. Then equation (6.8) can be written as

$$e_\psi w_F=\frac{1}{[F:\mathbb{Q}]}\frac{L_{S_F\cup\{p\}}(E,\overline{\psi},1)}{\Omega^{\psi(-1)}} \tag{6.10}$$

For every $n,m\in\mathbb{N}$ such that $m\mid n$, we use the following notation. We call $\tilde{n}$ the product of all the primes dividing n and $r(m,n):=\mathrm{lcm}(\tilde{n},m)$. Furthermore, let $s(m,n):=\frac{r(m,n)}{m}$ be the product of primes dividing n but not m. Note that m and $s(m,n)$ are relatively prime. When there is no risk of confussion, we will denote these quantities by r and s.

For the remaining of this section, fix $n\in\mathbb{N}$ divisible by neither p nor any bad prime of E. For every character ψ of conductor m, the algebraic L-value is defined as

$$\mathcal{L}_n(E,\psi):=\frac{L_{S_n\cup\{p\}}(E,\psi,1)}{\varphi(n)e_{\overline{\psi}}(\zeta_r)\Omega^{\psi(-1)}}=(-1)^{\nu(s)}\overline{\psi}(s)\frac{\varphi(r)L_{S_n\cup\{p\}}(E,\psi,1)}{\varphi(n)\varphi(m)e_{\overline{\psi}}(\zeta_m)\Omega^{\psi(-1)}}$$

where S_n is the set of prime divisors of n and φ represents the Euler totient function and $\zeta_j=e^{\frac{2\pi i}{j}}\in\mathbb{C}$. This is a modification of the definition in [WW22] to consider the

cases when ψ is a non-primitive character. Note that, when ψ is primitive, the product $\varphi(n)e_{\overline{\psi}}(\zeta_r)$ coincides with the Gauss sum of ψ. It is worth mentioning that the last equality comes from the fact that

$$e_{\overline{\psi}}(\zeta_r) = \frac{\varphi(m)}{\varphi(r)} e_{\overline{\psi}}\Big(\mathrm{Tr}_{\mathbb{Q}(\mu_r)/\mathbb{Q}(\mu_m)}(\zeta_r)\Big) = \frac{\varphi(m)}{\varphi(r)} e_{\overline{\psi}}\Big((-1)^{\nu(s)}\zeta_m^{(s^{-1})}\Big) = \frac{(-1)^{\nu(s)}\varphi(m)}{\overline{\psi}(s)\varphi(r)} e_{\overline{\psi}}(\zeta_m) \tag{6.11}$$

where s^{-1} is the inverse of s mod m.

If we let $\mathcal{D}_n$ be the set of Dirichlet characters modulo n, we can define the Stickelberger element as

$$\Theta_n := \sum_{\psi\in\mathcal{D}_n} \mathcal{L}_n\big(E,\overline{\psi}\big)e_\psi \in \mathbb{Q}_p[\zeta_{\varphi(n)}][\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$$

We can lower bound the p-adic valuation of the ψ-parts of Θ_n for certain characters. In order to do that, define

$$k'_\psi := v_p\left(\frac{1 - a_p\psi(p) + \mathbf{1}_N(p)\psi(p)^2}{p}\right) \tag{6.12}$$

Proposition 6.0.20. Let $m \in \mathbb{N}$ be an integer prime to Np and let ψ be a character of conductor m, satisfying that $r(m,n) = n$ or, equivalently, that $\gcd(m, n/m) = 1$. Then $\psi(\Theta_n) = \mathcal{L}_n\big(E,\overline{\psi}\big) \in p^{k'_\psi}\mathbb{Z}_p[\psi]$.

Proof. By assumption (E2) and [WW22, theorem 2], the primitive algebraic L-value, defined as $\mathcal{L}\big(E,\overline{\psi}\big) := \frac{L(E,\overline{\psi},1)}{\varphi(m)e_\psi(\zeta_m)\Omega^{\psi(-1)}}$ belongs to $\mathbb{Z}_p[\psi]$. It satisfies an explicit relation with $\mathcal{L}_n\big(E,\overline{\psi}\big)$

$$\mathcal{L}_n(E,\overline{\psi}) = (-1)^{\nu(s)}\psi(s)\frac{\varphi(r)}{\varphi(n)} \prod_{\ell\in(S_n\cup\{p\})\setminus S_m} \left(\frac{\ell - a_\ell\overline{\psi}(\ell) + \mathbf{1}_N(\ell)\overline{\psi}(\ell)^2}{\ell}\right) \mathcal{L}\big(E,\overline{\psi}\big)$$

When $r = n$, all of the terms in the right hand side belong to $\mathbb{Z}_p[\psi]$ with the possible exception of the Euler factor at p, which has p-adic valuation $k'_{\overline{\psi}}$, which is the same as the one of k'_ψ. Therefore,

$$\mathcal{L}_n\big(E,\overline{\psi}\big) \in p^{k'_\psi}\mathbb{Z}_p[\psi] \qquad \square$$

Stickelberger elements can be also defined for every abelian extension of $\mathbb{Q}$. If $F/\mathbb{Q}$ is an abelian extension of conductor n, consider the projection

$$c_{\mathbb{Q}(\mu_n),F} :\ \mathbb{Q}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})] \to \mathbb{Q}_p[\mathrm{Gal}(F/\mathbb{Q})],\ \sigma \mapsto \sigma|_F$$

Definition 6.0.21. Let $F/\mathbb{Q}$ be an abelian extension of conductor n. Then we define the Stickelberger element of F as

$$\Theta_F := c_{\mathbb{Q}(\mu_n),F}\Theta_n$$

The way to relate the Stickelberger elements to Kato's Euler system is by considering their action on certain elements in $\mathbb{Q}(\mu_n)$.

Definition 6.0.22. For every $n \in \mathbb{N}$, consider the element

$$\xi_n = \sum_{\tilde{n}|d|n} \zeta_d$$

Lemma 6.0.23. If ψ is a Dirichlet character modulo n of conductor m, then

$$e_\psi(\xi_n) = e_\psi(\zeta_{r(m,n)})$$

Proof. For every d dividing n, let $d' = \gcd(d, m)$. For every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d'}))$, we can find a lift $\widetilde{\sigma} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_{d'}))$ such that

$$\widetilde{\sigma}\,|_{\mathbb{Q}(\mu_d)} = \sigma \text{ and } \quad \widetilde{\sigma}\,|_{\mathbb{Q}(\mu_m)} = \mathrm{Id}|_{\mathbb{Q}(\mu_m)}$$

Since ψ has conductor m,

$$e_\psi(\sigma(\zeta_d)) = e_\psi(\widetilde{\sigma}(\zeta_d)) = e_\psi(\zeta_d)\ \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d'}))$$

Therefore

$$e_\psi(\zeta_d) = \frac{1}{[\mathbb{Q}(\mu_d) : \mathbb{Q}(\mu_{d'})]} e_\psi(\mathrm{Tr}_{\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d'})}\zeta_d)$$

Assume first that there is a prime ℓ such that $v_\ell(d) > v_\ell(m) \geq 1$. Then $\gcd(d, m) \mid \frac{d}{\ell}$, so

$$\mathrm{Tr}_{\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d'})}\zeta_d = \mathrm{Tr}_{\mathbb{Q}(\mu_{d/\ell})/\mathbb{Q}(\mu_{d'})}\left(\mathrm{Tr}_{\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d/\ell})}\zeta_d\right)$$

However, $\mathrm{Tr}_{\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{d/\ell})}\zeta_d = 0$ because $\ell \mid \frac{d}{\ell}$. Indeed, ζ_d is a root of the polynomial $P(T) = T^\ell - \zeta_{d/\ell}$. Since $[\mathbb{Q}(\mu_d) : \mathbb{Q}(\mu_{d/\ell})] = \ell$ because $\ell^2 \mid d$, then $P(T)$ is irreducible. The sum of the roots of P is zero and, hence, so is the trace of ζ_d. Therefore, $e_\psi(\zeta_d) = 0$ in this case.

Given some d such that the above prime ℓ does not exist, then $d \mid r$. Moreover, assume $d < r$. Since $\tilde{n} \mid d$, then $d' < m$

$$e_\psi(\zeta_d) = \frac{1}{[\mathbb{Q}(\mu_d) : \mathbb{Q}(\mu_{d'})]} e_\psi(\mathrm{Tr}_{\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu'_d)}\zeta_d)$$

Since ψ has conductor m, then $e_\psi(x) = 0$ for every $x \in \mathbb{Q}(\mu_{d'})$ and, therefore, $e_\psi(\zeta_d) = 0$.

The only remaining term is ζ_r, so

$$e_\psi(\xi_n) = \sum_{\tilde{n}|d|n} e_\psi(\zeta_d) = e_\psi(\zeta_r)$$

□

The concept of ξ_n extends naturally to abelian extensions of $\mathbb{Q}$. Assume $F/\mathbb{Q}$ is an abelian extension of conductor n. Define

$$\xi_F := \mathrm{Tr}_{\mathbb{Q}(\mu_n)/F}\xi_n$$

Corollary 6.0.24. If $F/\mathbb{Q}$ is an abelian extension of conductor n and ψ is a character of conductor m whose fixed field contains F, then

$$e_\psi(\xi_F) = [\mathbb{Q}(\mu_n) : F] e_\psi(\zeta_r)$$

Proof. Since F contains the fixed field of ψ, by lemma 6.0.23,

$$e_\psi(\xi_F) = [\mathbb{Q}(\mu_n) : F] e_\psi(\xi_n) = [\mathbb{Q}(\mu_n) : F] e_\psi(\zeta_r)$$

□

We can compute

$$e_\psi(\Theta_F(\xi_F)) = \Theta_n e_\psi(\xi_F) = [\mathbb{Q}(\mu_n) : F] \Theta_n e_\psi(\zeta_r) = [\mathbb{Q}(\mu_n) : F] \mathcal{L}_n\big(E, \overline{\psi}\big) e_\psi(\zeta_r)$$

Thus,

$$e_\psi(\Theta_F(\xi_F)) = \frac{L_{S_n \cup \{p\}}(E, \overline{\psi}, 1)}{[F : \mathbb{Q}] \Omega^{\psi(-1)}} \in F \otimes \mathbb{Q}_p$$

Since that is true for all characters, we can conclude from equation (6.10) that

$$w_F = \Theta_F(\xi_F) \in F \otimes \mathbb{Q}_p \tag{6.13}$$

6.0.3 Twisting of Kato's Euler system

According to definition 6.0.7, we are interested in studying the representation

$$T(\chi) := T_p E \otimes \mathcal{O}_d(\chi)$$

where χ is a primitive character of G. In order to do that, we have to apply the twisting process of Euler systems described in [Rub00, §II.4]. Define

$$z_{F,\chi} := \mathrm{cor}_{KF/F}(z_{KF} \otimes 1_\chi) \tag{6.14}$$

where 1_χ represents the unit element in $\mathcal{O}_d(\chi)$.

The goal of this section is to describe the dual exponetial of the twisted zeta element. In particular, with the notation of (6.13), we want to show that this value coincides with the $\overline{\chi}$ part of $\Theta_{KF}(\xi_{KF})$.

Proposition 6.0.25. ([Rub00, proposition II.4.2]) The collection $\{z_{F,\chi}\}_{F \in \Omega}$ is an Euler system for $T(\chi)$.

We will now describe the dual exponential map of $V \otimes \mathcal{O}_d(\chi)$. Note that V and $V \otimes \mathcal{O}_d(\overline{\chi})$ are equal as $G_{(KF)_w}$-modules for every prime w of KF above p. Hence we can consider the exponential map

$$\exp : \bigoplus_{w|p} \frac{(B_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi}))^{G_{(KF)_w}}}{(B^+_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi}))^{G_{(KF)_w}}} \to \bigoplus_{w|p} H^1_{\mathcal{F}_{\mathrm{BK}}}((KF)_w, V \otimes \mathcal{O}_d(\overline{\chi}))$$

For every w, we have an isomorphism (depending on fixing a Weierstrass model for E)

$$\frac{(B_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi}))^{G_{(KF)_w}}}{(B^+_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi}))^{G_{(KF)_w}}} \cong (KF)_w \otimes \mathcal{O}_d(\overline{\chi})$$

Since $G_{w/v} := \mathrm{Gal}((KF)_w/F_v)$ is finite, then $H^1\left((KF)_w/F_v, B^+_{\mathrm{dR}} \otimes V \otimes \overline{\chi}\right) = 0$, so

$$\left(\frac{\left(B_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi})\right)^{G_{(KF)_w}}}{\left(B^+_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi})\right)^{G_{(KF)_w}}}\right)^{G_w} = \frac{\left(B_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi})\right)^{G_{F_v}}}{\left(B^+_{\mathrm{dR}} \otimes V \otimes \mathcal{O}_d(\overline{\chi})\right)^{G_{F_v}}}$$

By considering the direct sum over all $w \mid p$, the exponential map over F_v can be written as

$$\exp_{\omega_E,\overline{\chi}} : \left(KF \otimes \mathbb{Q}_p \otimes \mathcal{O}_d(\overline{\chi})\right)^{\mathrm{Gal}(KF/F)} \to \bigoplus_{v|p} H^1_{\mathcal{F}_{\mathrm{BK}}}\left((F_v, V \otimes \mathcal{O}_d(\overline{\chi}))\right)$$

Note that the first term is the χ-part of $KF \otimes \mathbb{Q}_p$. Hence the dual exponential map can be written as

$$\exp^*_{\omega_E,\overline{\chi}} : \bigoplus_{v|p} H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_v, V \otimes \mathcal{O}_d(\chi)) \to \mathrm{Hom}\big(e_\chi(KF \otimes L), \mathbb{Q}_p\big) \cong e_{\overline{\chi}}\big((KF) \otimes L\big)$$

where we denote $L = \mathcal{O}_d \otimes \mathbb{Q}_p$ and the last isomorphism comes from the fact that the identification in (6.7) is Galois equivariant. Note that we are also using (6.7) to identify $\mathrm{Hom}(L, \mathbb{Q}_p) \cong L$.

In an abuse of notation, we will also denote by $\exp^*_{\omega_E,\overline{\chi}}$ to the following map

$$\exp^*_{\omega_E,\overline{\chi}} : H^1(F, V \otimes \mathcal{O}_d(\chi)) \to \bigoplus_{v|p} H^1_{/\mathcal{F}_{\mathrm{BK}}}(F_v, V \otimes \mathcal{O}_d(\chi)) \to e_{\overline{\chi}}((KF) \otimes L)$$

Now we will describe how the twisting process in (6.14) is reflected in the images of the dual exponential map.

First note that over KF, the map $\exp^*_{\omega_E,\overline{\chi}}$ coincides with $\exp^*_{\omega_E} \otimes \mathcal{O}_d(\chi)$. Hence we just need to see how $\exp^*_{\omega_E,\overline{\chi}}$ behaves under the corestriction.

Proposition 6.0.26. Let $c \in H^1(F, V \otimes \mathcal{O}_d(\chi))$ and $d = \mathrm{cor}_{KF/F}\, c \in H^1(KF, V \otimes \mathcal{O}_d(\chi))$. Then

$$\exp^*_{\omega_E,\overline{\chi}}(d) = N_{KF/F} \exp^*_{\omega_E,\overline{\chi}}(c) \in (KF \otimes \mathbb{Q}_p \otimes \mathcal{O}_d(\chi))^{G_F}$$

Proof. Localising at primes above p, we have that

$$\mathrm{loc}^s_p(d) = \left(\bigoplus_{w|p} \mathrm{cor}_{(KF)_w/F_v}\right)(\mathrm{loc}^s_p(c))$$

By [NSW00, propostion 1.5.3 (iv)], if we understand $\mathrm{loc}_p^s(c)^\vee$ and $\mathrm{loc}_p^s(d)^\vee$ as maps into the duals of the finite cohomology groups, we have that

$$\mathrm{loc}_p^s(c)^\vee = \mathrm{loc}_p^s(d)^\vee \circ \left(\bigoplus_{w|p} \mathrm{res}_{(KF)_w/F_v} \right)$$

By [NSW00, proposition 1.5.2], the following digram is commutative

$$\begin{array}{ccccc}
(KF \otimes \mathbb{Q}_p \otimes \overline{\chi})^{G_F} & \xrightarrow{\exp_{\omega_E}} & \bigoplus_{v|p} H^1_{\mathrm{f}}(F_v, V \otimes \overline{\chi}) & \xrightarrow{\mathrm{loc}_p^s(d)^\vee} & \mathbb{Q}_p \\
\downarrow \subset & & \downarrow \bigoplus_{v|p} \mathrm{res} & & \downarrow = \\
KF \otimes \mathbb{Q}_p \otimes \overline{\chi} & \xrightarrow{\exp_{\omega_E}} & \bigoplus_{w|p} H^1_{\mathrm{f}}((KF)_w, V \otimes \overline{\chi}) & \xrightarrow{\mathrm{loc}_p^s(c)^\vee} & \mathbb{Q}_p
\end{array}$$

Therefore, $\exp^*_{\omega_E,\chi}(d)$ is the restriction to $(KF \otimes \mathbb{Q}_p \otimes \overline{\chi})^{G_F}$ of $\exp^*_{\omega_E,\chi}(c)$. Under the identification (6.7), that means

$$\exp^*_{\omega_E,\chi}(d) = N_{KF/F} \exp^*_{\omega_E,\chi}(c)$$

□

If $K \cap F = \mathbb{Q}$, the dual exponential map of the twisted Kato's Euler system is

$$w_{F,\chi} := \exp^*_{\omega_E,\overline{\chi}}(z_{F,\chi}) = N_{KF/F}(\exp^*_{\omega_E,\overline{\chi}}(z_{KF} \otimes 1_\chi)) = [K : \mathbb{Q}] e_{\overline{\chi}}(\omega_{KF})$$

By equation (6.13),

$$w_{F,\chi} = [K : \mathbb{Q}] e_{\overline{\chi}}(\Theta_{KF}(\xi_{KF})) = d\, e_{\overline{\chi}}(\Theta_{KF})(\xi_{KF}) \tag{6.15}$$

Remark 6.0.27. Kato's theory is not exclusive for elliptic curves, but can be done for modular forms. In particular, we can apply it to the modular form f_χ, for some character χ of G, in order to obtain an Euler system $z_F^\chi \in H^1(F, V \otimes \mathcal{O}_d(\chi))$ satisfying the interpolation property. It is essentially the same Euler system as the one defined in (6.14).

Let g be a modular form and let K_g be its field of coefficients. Let λ be a prime of K_g above p. Kato defined in [Kat04, §6.3] the $\mathbb{Q}_p$-vector space $V_{K_{g,\lambda}}(g)$ to be the maximal Hecke eigenquotient of $H^1_{\text{ét}}(Y_1(N), K_{g,\lambda})$ associated to g. Every $\gamma \in V_{K_{g,\lambda}(g)}$ can be used to construct an Euler system z_γ which can be characterised by an interpolation property.

If we denote $S(g)$ to the Hecke eigenspace of $S_2(Y_1(N))$ containing g and $V_{\mathbb{C}}(g) = V_{K_g,\lambda}(g) \otimes_{K_{g,\lambda}} \mathbb{C}$, the period map defined in [Kat04, §4.10] induces a map

$$\mathrm{per}: \ S(g) \to V_{\mathbb{C}}(g)$$

Let F be a number field and let ψ be a character of $\mathrm{Gal}(F/\mathbb{Q})$. Then the interpolation property for z_γ can be written as

$$\sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \psi(\sigma) \mathrm{per}(\sigma(\exp^*(\mathrm{loc}_s^p(z_{\gamma,F}))))^{\psi(-1)} = L_{S_F \cup \{p\}}(g, \chi, 1) \gamma^{\psi(-1)}$$

where, for some $\eta \in V_{K_g,\lambda}(g)$, $\eta^{\pm}$ denotes the projection of η to the eigenspace in which the complex conjugation acts by multiplication with $\pm$. Note that (6.8) can be obtained after choosing a suitable γ_0 (see [Kat21, theorem 6.1]).

This interpolation property can be used to compare the χ-twisted Euler systems constructed for f in (6.14), denoted by $z^f_{F,\chi}$ and the Euler system for f_χ, constructed for a suitable $\gamma \in V_{L_\lambda}(f_\chi)$, where λ is a prime of L above p. This Euler system will be denoted by $z^{f_\chi}_{\gamma_F}$.

We follow the argument in [Kat04, §14.6]. There is an isomorphism of Galois representations

$$\Psi : \ V_{\mathbb{Q}_p}(f) \otimes L_\lambda(\chi) \cong V_{L_\lambda}(f_\chi) \tag{6.16}$$

Choose $\gamma = \Psi(\gamma_0 \otimes 1)$. Note that $\gamma^{\pm\chi(-1)} = \Psi(\gamma^{\pm} \otimes 1)$. The isomorphism in (6.16) induces an isomorphism of cohomology groups:

$$H^1(F, V_{\mathbb{Q}_p}(f) \otimes L_\lambda(\chi)) \cong H^1(F, V_{L_\lambda}(f_\chi)) \tag{6.17}$$

Choose γ the image of $\gamma_0 \otimes 1$ under the isomorphism

We claim that $z^{f_\chi}_{\gamma,F}$ is the image of $z^f_{\chi,F}$ under the isomorphism in (6.17). Consider the commutative diagram

$$\begin{array}{ccccc}
H^1(F, V_{\mathbb{Q}_p}(f) \otimes L_\lambda(\chi)) & \xrightarrow{\exp^*} & S(f) \otimes L_\lambda(\chi) & \xrightarrow{\text{per}} & V_{\mathbb{C}}(f) \\
\downarrow \sim & & & & \downarrow \sim \\
H^1(F, V_{L_\lambda}(f_\chi)) & \xrightarrow{\exp^*} & S(f_\chi) \otimes L_\lambda & \xrightarrow{\text{per}} & V_{\mathbb{C}}(f_\chi)
\end{array}$$

Following [Kat21, (6.3)], we can compute the image of the zeta elements under the composition $\text{per} \circ \exp^*$. If ψ is a character of $\text{Gal}(F/\mathbb{Q})$, we have that

$$\begin{aligned}
(\text{per} \circ \exp^*)\Big(e_\psi\big(z^f_{F,\chi}\big)\Big) &= L_{S_F \cup \{p\}}(E, \chi\psi, 1)(\gamma_0^{\chi\psi(-1)} \otimes 1_{\mathbb{C}}) \\
(\text{per} \circ \exp^*)\Big(e_\psi\big(z^{f_\chi}_{\gamma,F}\big)\Big) &= L_{S_F \cup \{p\}}(f_\chi, \psi, 1)(\gamma^{\psi(-1)} \otimes 1_{\mathbb{C}})
\end{aligned}$$

Since $L_{S_F \cup \{p\}}(E, \chi\psi) = L_{S_F \cup \{p\}}(f_\chi, \psi)$ and $\gamma_0^{\chi\psi(-1)} \otimes 1_{\mathbb{C}}$ is identified with $\gamma^{\psi(-1)} \otimes 1_{\mathbb{C}}$ under the isomorphism on the right, the images of both zeta elements are the same under the identifications made. Since the compositions $\text{per} \circ \exp^*$ are injective maps, we can conclude that both zeta elements are identified under the isomorphism

$$H^1(F, V_{\mathbb{Q}_p}(f) \otimes L_\lambda(\chi)) \cong H^1(F, V_{L_\lambda}(f_\chi))$$

6.0.4 Mazur-Tate elements and Kolyvagin derivative

Using the interpolation in (6.10), we can relate ω_F to Mazur-Tate elements defined in [MT87]. The main advantage of this relation is that Mazur-Tate elements have an explicit formula in terms of the modular symbols defined in (6.1), which is a key fact in the relation between Kato's Euler system and the Kurihara numbers.

Definition 6.0.28. Let $n \in \mathbb{Z}$. The *Mazur-Tate modular element* for n is defined as

$$\theta_n = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} \left(\left[\frac{a}{n}\right]^+ + \left[\frac{a}{n}\right]^- \right) \sigma_a \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$$

where σ_a is the element of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ that sends ζ_n to ζ_n^a. The integrality of the Mazur-Tate modular elements holds true under assumption (E2).

Mazur-Tate elements can be also defined for abelian extensions of $\mathbb{Q}$.

Definition 6.0.29. Let $F/\mathbb{Q}$ be an abelian extension of conductor n. Then the Mazur-Tate element of F is defined as

$$\theta_F := c_{\mathbb{Q}(\mu_n)/F}\theta_n$$

Mazur-Tate elements can be related to special L-values by using the Birch's formula (see [MTT86, formula (8.6)])

Proposition 6.0.30. ([MT87, §1.4],[WW22, lemma 6, proposition 7]) If ψ is a Dirichlet character of conductor n, then

$$\psi(\theta_n) = \frac{n}{\varphi(n)e_\psi(\zeta_n)} \frac{L_{S_n}(E, \overline{\psi}, 1)}{\Omega^{\psi(-1)}} \in \mathbb{Z}_p[\psi]$$

where S_n is the set of primes dividing n and $\varphi(n)$ is the Euler totient function. Note that the product $\varphi(n)e_\psi(\zeta_n)$ coincides with the Gauss sum $\tau(\overline{\psi})$.

For primitive characters, the ψ parts of the Mazur-Tate element are easily comparable using the ψ parts of Θ_n.

Corollary 6.0.31. If ψ is a Dirichlet character of conductor n, then

$$\psi(\Theta_n) = \frac{1}{n}\psi(\theta_n)(1 - p^{-1}a_p\overline{\psi}(p) - p^{-1}\mathbf{1}_N(p)\overline{\psi}(p)^2)$$

For every $n \in \mathcal{N}_k$, recall that $\mathbb{Q}(n)$ is the maximal p-subextension inside $\mathbb{Q}(\mu_n)$ and let $K(n) := K\mathbb{Q}(n)$. Note that there is a canonical identification

$$\mathrm{Gal}(K(n)/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q}) = G \times \mathcal{G}_n \tag{6.18}$$

We can use corollary 6.0.31 to compare $\Theta_{K(n)}$ and $\theta_{K(n)}$ as elements in the group ring $\mathbb{Z}_p[\mathrm{Gal}(K(n)/\mathbb{Q})]$. We follow the process in [Ota18] and [KKS20]. However, in our case, we only have the equality for the primitive character parts. That implies that both elements are not necessarily equal, but they are related enough so we can compare their Kolyvagin derivatives.

Consider the element

$$\Upsilon_{K(n)} := \Theta_K(n) - \frac{1}{n}(1 - p^{-1}a_p\mathrm{Frob}_p^{-1} - p^{-1}\mathbf{1}_N(p)\mathrm{Frob}_p^{-2})\theta_{K(n)} \in \mathbb{Z}_p[G]$$

The following result can be deduced from corollary 6.0.31

Corollary 6.0.32. For every primitive character ψ of $\mathrm{Gal}(K(n)/\mathbb{Q})$, we have that

$$e_\psi \Upsilon_{K(n)} = 0$$

Recall that χ was a primitive character of $\mathrm{Gal}(K/\mathbb{Q})$ which was used to construct $T(\chi)$. Using the identification in equation (6.18), we can consider $\chi(\Theta_n)$ and $\chi(\theta_n)$ as elements in $\mathbb{Z}_p[\chi][\mathcal{G}_n]$. For every Dirichlet character ψ of conductor n, then $\chi \times \psi$ is a primitive character of $\mathrm{Gal}(K(n)/\mathbb{Q})$ and we have that

$$e_{\chi\times\psi} \Upsilon_{K(n)} = 0$$

Hence

$$\chi\left(\Theta_{K(n)} - \frac{1}{n}(1 - p^{-1}a_p\mathrm{Frob}_p^{-1} + p^{-1}\mathbf{1}_N(p)\mathrm{Frob}_p^{-2})\theta_{K(n)}\right) = \sum_{\ell|n} \nu_{n,n/\ell}\ \alpha_{n,\ell} \quad (6.19)$$

where $\nu_{n,n\ell}:\ \mathbb{Q}_p[\zeta_{cn}][\mathcal{G}_{n/\ell}] \to \mathbb{Q}_p[\zeta_{cn}][\mathcal{G}_n]$ is the norm map and $\alpha_{n,\ell}$ is certain element in $\mathbb{Q}_p[\zeta_{cn}][\mathcal{G}_{n\ell}]$, which we do not need to determine explicitly.

For every character ψ' of $\mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q})$ (not necessarily primitive), $\chi\times\psi'$ has conductor m satisfying that $r(m, cn) = cn$. Therefore, proposition 6.0.20 implies that $\chi(\Theta_{K(n)}) \in p^{k'_\chi}\mathbb{Z}_p[\mathcal{G}_n]$. Hence $\alpha_{n,\ell} \in p^{k'_\chi}\mathbb{Z}_p[\zeta_{cn}][\mathcal{G}_{n/\ell}]$ for every prime divisor ℓ of n.

That is enough to relate the Kolyvagin derivatives of the (primitive) character parts of $\Theta_{K(n)}$ and $\theta_{K(n)}$.

Proposition 6.0.33. Let χ be a primitive character of $\mathrm{Gal}(K/\mathbb{Q})$ and let $n \in \mathcal{N}_k$,. Then the Kolyvagin derivative, defined in definition **??** can be computed as

$$D_n\chi(\Theta_{K(n)}) \equiv \frac{1}{n}\left(1 - p^{-1}a_p\overline{\chi}(p) + p^{-1}\mathbf{1}_N(p)\overline{\chi}(p)^2\right) D_n\chi(\theta_{K(n)}) \mod p^{k+k'_\chi}\mathbb{Z}_p[\chi][\mathcal{G}_n]$$

Proof. Note that, since $\mathrm{Gal}(K(n)/\mathbb{Q})$ is abelian,

$$\begin{aligned}
&D_n\left(\chi\left((1 - p^{-1}a_p\mathrm{Frob}_p^{-1} + p^{-1}\mathbf{1}_N(p)\mathrm{Frob}_p^{-2})\theta_{K(n)}\right)\right) = \\
&\chi\left(1 - p^{-1}a_p\mathrm{Frob}_p^{-1} - p^{-1}\mathrm{Frob}_p^{-2}\right) D_n(\chi(\theta_{K(n)})) = \\
&(1 - p^{-1}a_p\overline{\chi}(p) + p^{-1}\mathbf{1}_N(p)\overline{\chi}(p)^2)D_n(\chi(\theta_{K(n)}))
\end{aligned}$$

By equation (6.19), it is enough to prove that, for every prime divisor ℓ of n,

$$D_n\,\nu_{n,n/\ell}\alpha \in p^{k+k'_\chi}\mathbb{Z}_p[\psi][\mathcal{G}_n]$$

for every $\alpha \in p^{k'_\chi}\mathbb{Z}_p[\psi][\mathcal{G}_{n/\ell}]$. In fact, since $\nu_{n,n/\ell}\alpha$ is $\mathcal{G}_\ell$ invariant, then

$$D_\ell\nu_{n,n/\ell}\alpha = \frac{p^{n_\ell}(p^{n_\ell} - 1)}{2}\nu_{n,n/\ell}\alpha \in p^{k+k'_\chi}\mathbb{Z}_p[\psi][\mathcal{G}_n]$$

since $\ell \in \mathcal{P}_k$. Thus

$$D_n\nu_{n,n/\ell}\alpha = D_{n/\ell}D_\ell\nu_{n,n/\ell}\alpha \in p^{k+k'_\chi}\mathbb{Z}_p[\psi][\mathcal{G}_n]$$

□

By proposition **??**, for every $n \in \mathcal{N}_k$, $D_n z_{K\mathbb{Q}(n)}$ is invariant under the action of $\mathcal{G}_n$ modulo p^k. Consequently, $D_n\Theta_{K\mathbb{Q}(n)}$ and, therefore, $D_n\theta_{K\mathbb{Q}(n)}$ are $\mathcal{G}_n$-invariants modulo p^k. This is equivalent to

$$D_n\Theta_{K(n)}(\zeta_{K(n)}),\ D_n\theta_{K(n)}(\zeta_{K(n)}) \in K \otimes \mathbb{Q}_p$$

In order to compute this value, proposition 6.0.36 below is very useful. Before stating it, we need to define a p-primary logarithm in $(\mathbb{Z}/\ell)^\times$.

Definition 6.0.34. Assume H is a finite cyclic group whose order is exactly divisible by p^k for some $k \in \mathbb{N}$. If x is a generator of the p-primary part H, then for every $a \in H$ we will define $\log_x(a)$ to be the unique element in $y \in \mathbb{Z}/p^k$ such that $a^{-1}x^y$ has order prime to p.

Remark 6.0.35. Given two generators x_1 and x_2 of the p-primary part of H, the logarithms $\log_{x_1}(a)$ and $\log_{x_2}(a)$ have the same p-adic valuation.

Proposition 6.0.36. ([Sak22, lemma 3.11]) Let R be a ring, let $n = \ell_1 \cdots \ell_s \in \mathcal{N}_k$ and let

$$\theta = \sum_{\sigma \in \mathcal{G}_n} a_\sigma \sigma \in R[\mathcal{G}_n]$$

be an element such that $D_n\theta$ is Galois invariant modulo p^k. Then

$$D_n\theta \equiv \sum_{\sigma \in \mathcal{G}_n} a_\sigma \prod_{\ell | n} \log_{\tau_\ell}(\sigma) N_n \mod p^k R[\mathcal{G}_n]$$

where $N_n = \sum_{\sigma \in \mathcal{G}_n} \sigma$ is the norm element and τ_ℓ is the generator of $\mathcal{G}_\ell$ used to define the Kolyvagin derivative.

Proof. Denoting $T_i = \tau_{\ell_i} - 1$ for every i, we can write

$$D_n\theta = \sum_{i_1=1}^{\beta_{\ell_1}} \cdots \sum_{i_s=1}^{\beta_{\ell_s}} a_{\tau_{\ell_1}^{i_1} \cdots \tau_{\ell_s}^{i_s}} D_n (1+T_{\ell_1})^{i_1} \cdots (1+T_{\ell_s})^{i_s}$$

where $\beta_{\ell_i} := \#\mathcal{G}_{\ell_i}$. Modulo p^k, equation (**??**) implies that $D_n T_{\ell_i} = -N_{\ell_i}$ and $D_n T_{\ell_i}^2 = 0$. Thus

$$D_n\theta \equiv a_{\tau_{\ell_1}^{i_1} \cdots \tau_{\ell_s}^{i_s}} (1 - i_1 N_{\ell_1}) \cdots (1 - i_s N_{\ell_s}) \mod p^k$$

Since $D_n\theta$ is Galois invariant, the only non-vanishing summand in the right hand side is the multiple of $N_{\ell_1} \cdots N_{\ell_s}$. Since $i_i = \log_{\tau_{\ell_i}}(\sigma)$, we have

$$D_n\theta \equiv (-1)^{\nu(n)} \sum_{\sigma \in \mathcal{G}_n} a_\sigma \prod_{\ell | n} \log_{\tau_\ell}(\sigma) \mod p^k$$

□

Proposition 6.0.36 motivates definition 6.0.9 of the (twisted) Kurihara numbers.

Remark 6.0.37. The definition of $\delta_{n,\chi}$ depends on the choices of the generators $\eta_\ell \in (\mathbb{Z}/\ell)^\times$ for every $\ell \mid n$. However, by remark 6.0.35, the p-adic valuation of $\delta_{n,\chi}$ is well defined independently of the choices made in the construction of $\delta_{n,\chi}$.

From propositions 6.0.33 and 6.0.36, we obtain the following.

Corollary 6.0.38. For every primitive character χ of $\mathrm{Gal}(K/\mathbb{Q})$ and every $n \in \mathcal{N}_k$,

$$D_n e_\chi(\Theta_{cn}) \equiv \frac{\varphi(n)}{n}(1 - p^{-1}a_p\overline{\chi}(p) + p^{-1}\mathbf{1}_N(p)\overline{\chi}(p)^2)\delta_{n,\overline{\chi}} e_{\chi\times\mathbf{1}_n}$$

modulo $\frac{p^{k+k'_{\overline{\chi}}}}{\varphi(c)}\mathbb{Z}_p[\chi][G_{\mathbb{Q}(\mu_c)/\mathbb{Q}} \times \mathcal{G}_n]$.

Proof. Since $D_n\chi(\theta_{cn}) \equiv \delta_{n,\overline{\chi}} N_n = \delta_{n,\overline{\chi}}\varphi(n)e_{\mathbf{1}_n} \mod p^k\mathbb{Z}_p[\mathcal{G}_n]$ by proposition 6.0.36, the congruence holds modulo $p^{k+k'_{\overline{\chi}}}\varphi(c)^{-1}$ after multiplying both sides by the Euler product $\left(1 - p^{-1}a_p\overline{\chi}(p) + \mathbf{1}_N(p)p^{-1}\overline{\chi}(p)^2\right)$ and by the idempotent element. Thus, the corollary follows from proposition 6.0.33. □

We can adapt corollary 6.0.38 to describe the χ-part of $\Theta_{K(n)}$ in terms of the Kurihara numbers.

Corollary 6.0.39. For every primitive character χ of $\mathrm{Gal}(K/\mathbb{Q})$, we have that

$$D_n e_\chi(\Theta_{K(n)}) = \frac{\varphi(n)}{n}(1 - p^{-1}a_p\overline{\chi}(p) + p^{-1}\mathbf{1}_N(p)\overline{\chi}(p)^2)\delta_{n,\overline{\chi}} e_{\chi\times\mathbf{1}_n}$$

modulo $p^{k+k'_{\overline{\chi}}}\mathbb{Z}_p[\chi][G \times \mathcal{G}_n]$.

Proof. It follows from corollary 6.0.38, projecting the congruence to $\mathbb{Z}_p[\chi][G \times G_n]$.

Since both sides of that equation are invariant under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_c)/K)$, whose order is $\varphi(c)/d$, we can remove the denominator $\varphi(c)$ from the ideal of the congruence. □

By equation (6.15), we obtain the following corollary.

Corollary 6.0.40. For every primitive character χ of $\mathrm{Gal}(K/\mathbb{Q})$ and every $n \in \mathcal{N}_k$, modulo $p^{k+k'_\chi}\mathbb{Z}_p[G \times \mathcal{G}_n](\xi_{K(n)})$, we have that

$$D_n(w_{\mathbb{Q}(n),\chi}) \equiv \frac{(-1)^{\nu(n)}\chi(n)}{n}(1 - p^{-1}a_p\chi(p) + p^{-1}\mathbf{1}_N(p)\chi(p)^2)\delta_{n,\chi}\varphi(c)e_{\overline{\chi}}(\zeta_c)$$

Proof. By the transitivity of the trace,

$$\mathrm{Tr}_{K(n)/K}(\xi_{K(n)}) = \mathrm{Tr}_{\mathbb{Q}(\mu_{nc})/K}\left(\sum_{n\widetilde{c}|d|nc}\zeta_d\right) = (-1)^{\nu(n)}\ \mathrm{Tr}_{\mathbb{Q}(\mu_c)/K}\left(\sum_{\widetilde{c}|d|c}\zeta_d^{(n^{-1})}\right)$$

Denote

$$\widetilde{\xi}_K = \mathrm{Tr}_{\mathbb{Q}(\mu_c)/K}\left(\sum_{\widetilde{c}|d|c}\zeta_d^{(n^{-1})}\right)$$

Since χ has conductor c, by corollary 6.0.24

$$e_{\chi\times\mathbf{1}_n}(\xi_{K(n)}) = \frac{(-1)^{\nu(n)}}{\varphi(n)}e_\chi(\widetilde{\xi}_K) = \frac{(-1)^{\nu(n)}\overline{\chi}(n)}{\varphi(n)}[\mathbb{Q}(\mu_c) : K]e_\chi(\zeta_c)$$

Since $[\mathbb{Q}(\mu_c) : K] = \frac{\varphi(c)}{d}$, by equation (6.15) and corollary 6.0.39, we obtain that

$$D_n(w_{\mathbb{Q}(n),\chi}) \equiv \frac{(-1)^{\nu(n)}\chi(n)}{n}(1 - p^{-1}a_p\chi(p) + p^{-1}\chi(p)^2)\delta_{n,\chi}\varphi(c)e_{\overline{\chi}}(\zeta_c) \qquad \square$$

6.0.5 Image of Bloch-Kato dual exponential map

In §6.0.2, we have introduced the dual exponential map

$$\exp^*_{\omega_E} : \ H^1_{/\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, V) \xrightarrow{\sim} K_\mathfrak{p}$$

where $K_\mathfrak{p}$ is the completion of K at a prime $\mathfrak{p}$ above p. However, the group we are interested in is $H^1_{/\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, T)$. Hence we want to know the image of the composition map

$$H^1_{/\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, T) \to H^1_{/\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, V) \to K_\mathfrak{p}$$

By the identifications we have made so far, some $z \in H^1_{/\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, T)$ is identified under local Tate duality to the map

$$E(K_\mathfrak{p}) \otimes \mathbb{Q}_p \to \mathbb{Q}_p, \ x \mapsto \mathrm{Tr}_{K_\mathfrak{p}/\mathbb{Q}_p}(\exp^*_{\omega_E}(z)\log_{\omega_E}(x))$$

Hence an element $y \in K_\mathfrak{p}$ belongs to $\exp^*_{\omega_E}(H^1_{\mathcal{F}_{\mathrm{BK}}}(K_\mathfrak{p}, T))$ if and only if

$$\mathrm{Tr}_{K_\mathfrak{p}/\mathbb{Q}_p}(y\log_{\omega_E}(x)) \in \mathbb{Z}_p \ \forall x \in E(K_\mathfrak{p}) \tag{6.20}$$

where the logarithm is the extension of the one defined in the formal group of the elliptic curve.

Denote by $\mathcal{O}_\mathfrak{p}$ and $\mathfrak{m}_\mathfrak{p}$ to the ring of integers of $K_\mathfrak{p}$ and its maximal ideal, respectively. Denote by $E_1(K_\mathfrak{p})$ the kernel of the reduction map and $E_0(K_\mathfrak{p})$ the points whose reduction is a non-singular point. Since $K_\mathfrak{p}/\mathbb{Q}_p$ is unramified by (K1), the logarithm induces an isomorphism

$$\log_{\omega_E} : E_1(K_\mathfrak{p}) \xrightarrow{\sim} \mathfrak{m}_\mathfrak{p}$$

To describe the image $\log_{\omega_E}(E(K_\mathfrak{p}))$, we look at the χ-part of this map for the different characters χ of $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$. By (K3), $E(K_\mathfrak{p})_\chi$ is free of rank one over $\mathcal{O}[\chi]$. Since p does not divide the Tamagawa number $c_\mathfrak{p}$ by (K4), then the quotient $E(K_\mathfrak{p})/E_0(K_\mathfrak{p})$ has order prime to p. Therefore

$$\log_{\omega_E}(E(K_\mathfrak{p})) = \log_{\omega_E}(E_0(K_\mathfrak{p}))$$

Consider the exact sequence

$$0 \longrightarrow E_1(K_\mathfrak{p}) \longrightarrow E_0(K_\mathfrak{p}) \longrightarrow \widetilde{E}_0(\kappa_\mathfrak{p}) \longrightarrow 0$$

where $\widetilde{E}_0(\kappa_\mathfrak{p})$ denote the groups of non-singular points of the reduced curve modulo $\mathfrak{p}$. Since $[K_\mathfrak{p} : \mathbb{Q}_p]$ is prime to p by (K2), the sequence remains exact after taking χ-parts. Since $E(K_\mathfrak{p})[p] = 0$ by (K3), we have that

$$\log_{\omega_E}(E_0(K_p)_\chi) = \frac{1}{p^{\mathrm{length}(\widetilde{E}_0(\kappa_\mathfrak{p})[p^\infty]_\chi)}}\log_{\omega_E}(E_1(K_p)_\chi)$$

Since $K_\mathfrak{p}/\mathbb{Q}_p$ is unramified by (K1), then $\log_{\omega_E}(E_1(K_\mathfrak{p})_\chi) = (\mathfrak{m}_\mathfrak{p})_\chi = p(\mathcal{O}_\mathfrak{p})_\chi$ and

$$\log_{\omega_E}(E(K_\mathfrak{p})_\chi) = \frac{p}{p^{\text{length}(\widetilde{E}_0(\kappa_\mathfrak{p})[p^\infty]_\chi)}}\mathcal{O}_\chi \tag{6.21}$$

The trace map satisfies, for every $x \in K_\mathfrak{p}$, the identity $\text{Tr}(x) = \text{Tr}(e_1 x)$, where $e_1 \in \mathbb{Z}_p[\text{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)]$ is the idempotent element associated to the trivial character, i.e., $e_1 = \frac{1}{[K_\mathfrak{p}:\mathbb{Q}_p]}\sum_{\sigma\in\text{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)}\sigma$. By (K2), $[K_\mathfrak{p} : \mathbb{Q}_p]$ is prime to p. Thus $\text{Tr}(x) \in \mathbb{Z}_p$ if and only if $e_1 x \in \mathbb{Z}_p$.

Moreover, note that given $x_1, x_2 \in K_\mathfrak{p}$ such that $\sigma(x_1) = \chi_1(\sigma)x_1$ and $\sigma(x_2) = \chi_2(\sigma)x_2$ for every $\sigma \in \text{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ and some characters χ_1 and χ_2, then $\sigma(x_1x_2) = (\chi_1\chi_2)(\sigma)(x_1x_2)$.

Combining equations (6.20) and (6.21), we obtain

$$\exp^*(H^1_{/\mathcal{F}_{\text{BK}}}(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi))) = p^{\text{length}(\widetilde{E}_0(\kappa_\mathfrak{p})[p^\infty]_{\overline{\chi}})-1}\mathcal{O}_{\overline{\chi}} \tag{6.22}$$

We will now relate the length of $\widetilde{E}_0(\kappa_\mathfrak{p})_\chi$ to the p-adic valuation of the Euler factor at p evaluated at $s = 1$.

Proposition 6.0.41. The length of $e_\chi\left(\widetilde{E}_0(\kappa_p)[p^\infty]\right)$ as an $\mathcal{O}_d$-module is one unit larger than the valuation of the twsited Euler factor $1 - \frac{a_p}{p}\chi(p) + \mathbf{1}_N(p)\frac{1}{p}\chi(p)^2$ at p evaluated at $s = 1$.

Proof. Recall the definition of $k'_\chi = v_p\left(1 - \frac{a_p}{p}\chi(p) + \mathbf{1}_N(\ell)\frac{1}{p}\chi(p)^2\right)$ in definition 6.0.9. We will consider different cases depending of the type of reduction of E at p.

Assume first that E has good ordinary reduction at p and let $\alpha \in \mathbb{Z}_p^\times$ be the unit root of the Euler polynomial $X^2 - a_pX + p$. Then the arithmetic Frobenius acts on the reduced p-primary torsion $\widetilde{E}[p^\infty]$ by multiplication by α and thus acts on $\widetilde{E}[p^\infty]\otimes O(\overline{\chi})$ multiplying by $\alpha\overline{\chi}(p)$. $\widetilde{E}(\kappa_\mathfrak{p})_\chi$ is the kernel of the action of $\text{Frob}_p - 1$ on $\widetilde{E}[p^\infty]\otimes O(\overline{\chi})$, so its length is the p-adic valuation of $(\alpha\overline{\chi}(p) - 1)$.

Thus we just need to compute the p-adic valuation of $\alpha\overline{\chi}(p) - 1$. The twisted Euler polynomial factors as

$$\chi(p)^2X^2 - a_p\chi(p)X + p = \chi(p)^2(\overline{\chi}(p)\alpha - X)(\overline{\chi}(p)\beta - X)$$

where $\beta \in p\mathbb{Z}_p$ is the other root. Since $\overline{\chi}(p)\beta - 1$ is a unit, evaluating at $X = 1$ we get

$$(\chi(p)^2 - \chi(p)a_p + p) \sim (\overline{\chi}(p)\alpha - 1)$$

where $\sim$ denotes equality up to multiplication by a p-adic unit.

It E has good supersingular reduction at p, then clearly $\widetilde{E}(\kappa_\mathfrak{p})[p^\infty] = \{O\}$. In the supersingular case, then $p \nmid N$ and $p \mid a_p$, so the k'_χ has p-adic valuation -1 when evaluated at $X = 1$. Since $E(\kappa_\mathfrak{p})_\chi = \{0\}$, then the proposition holds true in this case.

If E has multiplicative reduction, then $\widetilde{E}_0(\kappa_\mathfrak{p}) \cong \kappa_\mathfrak{p}^\times$ has order prime to p, so the p-adic valuation of the right hand side is -1. In this case, $a_p = \pm 1$ depending on the reduction being split or not and $\mathbf{1}_N(\ell) = 0$, so k'_χ has p-adic valuation -1 as well.

If E has additive reduction, then

$$\widetilde{E}_0(\kappa_{\mathfrak{p}})_\chi \cong (\kappa_{\mathfrak{p}})_\chi = \#(\mathcal{O}_{\mathfrak{p}}/p\mathcal{O}_p)_\chi$$

has length one, so the equality is also satisfied in this case. □

By (K3), $H^2(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi)) = H^0(\mathbb{Q}_p, E[p^\infty]\otimes\mathcal{O}_d(\overline{\chi})) = 0$, so there is an isomorphism

$$H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi))/p^k \cong H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T/p^kT\otimes\mathcal{O}_d(\chi))$$

The dual exponential map induces thus an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T/p^kT\otimes\mathcal{O}_d(\chi)) \cong \frac{\exp^*_{\omega_E}(H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi)))}{p^k\exp^*_{\omega_E}(H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T\otimes\mathcal{O}_d(\chi)))} = \frac{p^{k'_{\overline{\chi}}}(\mathcal{O}_p)_{\overline{\chi}}}{p^{k+k'_{\overline{\chi}}}(\mathcal{O}_p)_{\overline{\chi}}} \quad (6.23)$$

where $\mathcal{O}_p := \bigoplus_{\mathfrak{p}|p}\mathcal{O}_{\mathfrak{p}} \subset K\otimes\mathbb{Q}_p$.

6.0.6 Kato's Kolyvagin system

In §6.0.4, we have computed the value of the dual exponential map

$$\exp^*_{\omega_E,\overline{\chi}}(D_n z_{\mathbb{Q}(n),\chi}) \equiv \frac{(-1)^{\nu(n)}\chi(n)}{n}(1-p^{-1}a_p\chi(p)+p^{-1}\chi(p)^2)\delta_{n,\chi}\varphi(c)e_{\overline{\chi}}(\zeta_c)$$

modulo $p^{k+k'_\chi}\mathbb{Z}_p[\mathcal{G}_n](\xi_{K(n)})$. Since $p^{k+k'_\chi}\mathbb{Z}_p[\mathcal{G}_n](\xi_{K(n)})\cap K$ is contained in $p^{k+k'_\psi}\mathcal{O}_p$, the congruence also holds modulo the latter.

The goal of this section is to relate this value with Kato's Kolyvagin system. After that, we will check that the p-divisibility of Kato's Kolyvagin system and the Kurihara numbers coincide.

As defined in (**??**), $\kappa_{n,\chi}$ is the preimage of $D_n z_{\mathbb{Q}(n),\chi}$ under the restriction map

$$\mathrm{res}_{\mathbb{Q}(n)/\mathbb{Q}}:\ H^1(\mathbb{Q}, T/p^k\otimes\mathcal{O}_d(\chi)) \to H^1(\mathbb{Q}(n), T/p^k\otimes\mathcal{O}_d(\chi))^{\mathcal{G}_n}$$

If we understand $\mathrm{loc}^{\mathrm{s}}_p(\kappa_{n,\chi})$ and $\mathrm{loc}^{\mathrm{s}}_v(D_n\omega_{\mathbb{Q}(n),\chi})$ as maps in the duals of $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T^*\otimes\mathcal{O}_d(\overline{\chi}))$ and $H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T^*\otimes\mathcal{O}_d(\overline{\chi}))$, we obtain by [NSW00, proposition 1.5.3(iv)] that

$$\mathrm{loc}^{\mathrm{s}}_v(D_n w_{n,\chi}) = \mathrm{loc}^{\mathrm{s}}_p(\kappa_{n,\chi})\circ\mathrm{cor}_{\mathbb{Q}(n)/\mathbb{Q}}$$

Similarly to the argument in proposition 6.0.26, we can study the behaviour of the dual exponential map under restriction maps.

Proposition 6.0.42. Let $c \in H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, V\otimes\mathcal{O}_d(\chi))$ and denote its restriction by $d = \mathrm{res}_{\mathbb{Q}(n)/\mathbb{Q}}(c) \in H^1_{/\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}(n), V\otimes\mathcal{O}_d(\chi))$. Then

$$\exp^*_{\omega_E,\overline{\chi}}(c) = \exp^*_{\omega_E,\overline{\chi}}(d) \in (\mathbb{Q}(n)\otimes\mathbb{Q}_p\otimes\mathcal{O}_d(\chi))^{\mathcal{G}_n}$$

Proof. Localising at primes above p, we get that

$$\mathrm{loc}^{\mathrm{s}}_p(d) = \left(\bigoplus_{v|p}\mathrm{res}_{\mathbb{Q}(n)_v/\mathbb{Q}_p}\right)\left(\mathrm{loc}^{\mathrm{s}}_p(c)\right)$$

By [NSW00, proposition 1.5.3 (iv)], if $\mathrm{loc}_p^{\mathrm{s}}(c)^\vee$ and $\mathrm{loc}_p^{\mathrm{s}}(d)^\vee$ are considered as maps in duals of the Bloch-Kato cohomology groups, then

$$\mathrm{loc}_p^{\mathrm{s}}(d)^\vee = \mathrm{loc}_p^{\mathrm{s}}(c)^\vee \circ \left(\bigoplus_{v|p} \mathrm{cor}_{\mathbb{Q}(n)_v/\mathbb{Q}_p} \right)$$

By [NSW00, proposition 1.5.2], $\exp^*_{\omega_E,\overline{\chi}}(d) = \exp^*_{\omega_E,\overline{\chi}}(c) \circ N_{\mathbb{Q}(n)/\mathbb{Q}}$

By the identification in (6.7),

$$\exp^*_{\omega_E,\overline{\chi}}(c) = \exp^*_{\omega_E,\overline{\chi}}(d) \qquad \square$$

Under the isomorphism in (6.23), the weak Kato's Kolyvagin system is

$$\widetilde{\kappa}_{n,\chi} = \frac{(-1)^{\nu(n)}\chi(n)}{n}(1 - p^{-1}a_p\chi(p) + p^{-1}\chi(p)^2)\delta_{n,\chi}\varphi(c)e_{\overline{\chi}}(\zeta_c)$$

In order to obtain Kato's Kolyvagin system κ_χ from $\widetilde{\kappa}_\chi$, we need to apply the construction from theorem **??**. However, in this case, $\kappa_\chi = \widetilde{\kappa}_\chi$. In fact, by the definition of Kolyvagin primes, $a_\ell = 2 \mod p^k$ for every $\ell \mid n$. Therefore, for every ℓ, we have that

$$P_\ell = X^2 - a_\ell X + \ell \equiv (X-1)^2 \mod p^k$$

Therefore, for every $\ell \mid n$, $\rho_\ell(P_\ell(\mathrm{Frob}_{\pi(\ell)}^{-1})) = 0$. Hence, in the formula of theorem **??**, the only term that does not vanish is the one associated to the trivial permutation, so $\widetilde{\kappa}_{n,\chi} = \kappa_{n,\chi}$.

Since p is unramified in $K/\mathbb{Q}$ by (K1), then $\varphi(c)e_{\overline{\chi}}(\zeta_c)$ generates the module $(\mathcal{O}_p)_{\overline{\chi}}$, and taking into account the description of the image of the dual exponential map in (6.23), we get that

$$\mathrm{ord}(\mathrm{loc}_s^p(\kappa_{n,\chi})) = \mathrm{ord}(\delta_{n,\chi}) \tag{6.24}$$

6.0.7 Primitivity of Kato's Euler system and proof of theorem 6.0.18

In this section we will prove theorem 6.0.18. From the χ-twisted Kato's Euler system constructed in §6.0.3, one can apply the Kolyvagin derivative process as in theorem **??** to obtain a Kolyvagin system $\kappa_\chi^\infty \in \mathrm{KS}(T \otimes \Lambda \otimes \mathcal{O}_d(\chi), \mathcal{F}_\Lambda, \mathcal{P})$.

By (K3) and (K4), the assumptions in proposition **??** are satisfied, so $\mathrm{KS}(T \otimes \Lambda \otimes \mathcal{O}_d(\chi), \mathcal{F}_\Lambda, \mathcal{P})$ is free of rank one over Λ and, by theorem **??**, κ_χ^∞ is primitive if and only if the Iwasawa main conjecture 6.0.2 holds true.

Kolyvagin derivative process can be applied to obtain the Kolyvagin system $\kappa_\chi \in \mathrm{KS}(T \otimes \mathcal{O}_d(\chi), \mathcal{F}^{\mathrm{can}}, \mathcal{P})$ which was studied in §6.0.6. By proposition **??**, it will be the image of κ_χ^∞ under the canonical map

$$\mathrm{KS}(T \otimes \mathcal{O}_d(\chi) \otimes \Lambda, \mathcal{F}_\Lambda, \mathcal{P}) \to \mathrm{KS}(T \otimes \mathcal{O}_d(\chi), \mathcal{F}^{\mathrm{can}}, \mathcal{P}) \tag{6.25}$$

By corollary **??**, κ_χ is primitive if and only if κ_χ^∞ is primitive. By lemma **??** and equation (6.24), this is equivalent to $\partial^{(\infty)}(\delta_\chi) = 0$, which is M. Kurihara's conjecture 6.0.17.

Hence the Iwasawa main conjecture and the Kurihara conjecture are equivalent for the twist $T \otimes \mathcal{O}_d(\chi)$, so theorem 6.0.18 holds.

Nevertheless, a non-primitive Kolyvagin system is useful for determining the structure of the Selmer group as long as it is non-zero. If we assume hypothesis (K5), then $\kappa_\chi^\infty \notin (X\Lambda)\,\mathrm{KS}(T \otimes \Lambda \otimes \mathcal{O}_d(\chi), \mathcal{F}_\Lambda, \mathcal{P})$ by corollary **??**. But this is the kernel of the map in (6.25), so this condition means that κ_χ is nonzero, fact that will be necessary to apply theorems **??** and **??** in the next section.

6.0.8 Functional equation and proof of theorem 6.0.13

The second part of theorem 6.0.13 is a direct consequence of theorem **??**. By equation (6.24), the ideals $\Theta_i(\widetilde{\delta}_\chi)$ in theorem 6.0.13 coincides with the ideals $\Theta_i(\kappa_\chi)$ in theorem **??**. By remark 6.0.15, we can assume χ is primitive.

Theorem **??** describe the structure of the Selmer group in a different way depending on whether the character χ is a quadratic character or not.

Assume first that $\chi \neq \overline{\chi}$. In this case, theorem **??** implies that the ideals $\Theta_i(\widetilde{\delta}_\chi)$

$$\Theta_i(\widetilde{\delta}_\chi) = \mathrm{Fitt}_i^{\mathcal{O}_d}(H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi)))$$

Since $\mathcal{O}_d$ is a principal ideal domain, the structure theorem of finitely generated modules implies that

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi)) \approx \mathcal{O}_d^r \oplus \bigoplus_{i=1}^{s-r} \frac{\mathcal{O}_d}{(p)^{\partial^{(r+i)}(\widetilde{\delta}) - \partial^{(r+i-1)}(\widetilde{\delta})}}$$

where we are using the notation of theorem 6.0.13. Therefore, the proof of the second part is complete.

Now consider the case when $\chi = \overline{\chi}$, the module $T \otimes \mathcal{O}_d(\chi)$ is self-dual and theorem **??** does not apply. We have to use **??** instead, which leads to a weaker control on the Fitting ideals of the Selmer group. However, Kurihara numbers satisfy a functional equation (inherited from the Mazur-Tate elements) and this fact leads to the determination of the structure of the Selmer group.

Recall that N is the conductor of the elliptic curve. The Mazur-Tate element satisfy the following functional equation

Proposition 6.0.43. ([MT87, §1.6]) Let $\iota : \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})] \to \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$ be the map induced from the inversion in $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. Then

$$\iota(\theta_n) = \varepsilon\sigma_{-N}\theta_n$$

where $\varepsilon \in \{\pm 1\}$ is the root number of the elliptic curve and $\sigma_N \in \mathrm{Gal}(\mathbb{Q}(\mu_n/\mathbb{Q}))$ is the Galois automorphism that sends ζ_n to ζ_n^N.

Corollary 6.0.44. If ψ is a character of G, then

$$\iota\left(\overline{\psi}(\theta_{K(n)})\right) = \varepsilon\chi(-N)\psi(\theta_{K(n)}) \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$$

Assume $\ell \in \mathcal{P}_k$. Then the construction of the Kolyvagin derivative implies for every $\theta \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$ that

$$D_\ell \iota(\theta) \equiv -D_\ell(\theta) \mod p^k$$

Therefore, for every $n \in \mathcal{N}_k$,

$$D_n\overline{\psi}(\theta_{K(n)}) = (-1)^{\nu(n)}\varepsilon\psi(N)D_n\psi(\theta_{K(n)})$$

Since $\chi = \overline{\chi}$, we have that

$$\delta_{n,\chi}(1 - (-1)^{\nu(n)}\varepsilon\chi(-N)) = 0$$

Since $\chi(-N) = \pm 1$, we have two possible cases.

Corollary 6.0.45. Depending on the root number ε of the elliptic curve and the value $\chi(-N)$, we have that

- If $\varepsilon\chi(-N) = 1$, then $\delta_{n,\chi} = 0$ when n has an odd number of prime divisors.
- If $\varepsilon\chi(-N) = -1$, then $\delta_{n,\chi} = 0$ when n has an even number of prime divisors.

Call $r = \mathrm{rank}_{\mathcal{O}_d} H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T \otimes \mathcal{O}_d(\chi))$. The first condition of theorem **??** is satisfied in this case, so

$$\Theta_r(\widetilde{\delta}_\chi) = \mathrm{Fitt}_r^{\mathcal{O}_d} H^1_{\mathcal{F}_{\mathrm{BK}}}(Q, T \otimes \mathcal{O}_d(\chi))$$

For any index $i \geq r$ having different parity that r, $\Theta_{i,\chi} = 0$ by corollary 6.0.45 and the corresponding Fitting ideal is non-zero. Hence the second condition of theorem **??** holds for $i+1$, so

$$\Theta_{i+1}(\widetilde{\delta}_\chi) = \mathrm{Fitt}_{i+1}^{\mathcal{O}_d} H^1_{\mathcal{F}_{\mathrm{BK}}}(Q, T \otimes \mathcal{O}_d(\chi))$$

By the structure theorem of finitely generated modules over principal ideal domains, we obtain

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}, T(\chi)) \approx \mathcal{O}_d^r \oplus \bigoplus_{i=1}^{\frac{s-r}{2}} \frac{\mathcal{O}_d}{(p)^{\partial^{(r+2i)}(\widetilde{\delta}) - \partial^{(r+2i-2)}(\widetilde{\delta})}}$$

so theorem 6.0.13 has been proven.

6.0.9 Examples

We end this article by showing some examples of computations o the Selmer group of elliptic curves. All the computations are done using Sagemath [The]. For all the elliptic curves E and abelian extensions $K/\mathbb{Q}$ appearing in these examples, we will assume that $Ш(E/K)$ is finite.

Example 6.0.46. Consider the elliptic curve 196 794cd1 in Cremona's database and the prime $p = 5$. Over the abelian extension $K = \mathbb{Q}(\mu_7)$, we can determine the full group structure of the Selmer group. We proceed by studying the twisted Kurihara number for every Dirichlet character of conductor dividing 7.

When χ is the trivial character, we compute $\delta_{1,\chi} = 0$, so $\mathrm{rank}(E(\mathbb{Q})) \geq 1$. To obtain further information about the structure of the Selmer group, we need to compute $\Theta_{1,\chi}$.

The smallest Kolyvagin prime $\ell = 93\,251$ satisfies that $\mathrm{ord}_5(\delta_{\ell,\chi}) = 2$. It guarantees that $\mathrm{rank}(E(\mathbb{Q})) = 1$ and $\#Ш(E/\mathbb{Q})[5^\infty] \mid 25$. If we compute $\mathrm{ord}_5(\delta_{\ell,\chi})$ for the smallest Kolyvagin primes, we will obtain the value 2 for approximately the 80% of the computations and a higher value in the remaining cases. That would lead us to guess that $\Theta_2 = 25\mathbb{Z}_5$, which is equivalent to $\#Ш(E/\mathbb{Q})[5^\infty] = 25$. However, we cannot prove it with only a finite amount of computations.

But we can use a different method to compute the order of the Tate-Shafarevich group using the Iwasawa main conjecture, which can be numerically verified it using theorem 6.0.18. The smallest Kolyvagin primes for $k = 1$ are 11, 31 and 131. Their product $n = 44\,671$ satisfies that $\delta_{n,\chi} \in \mathbb{Z}_5^\times$, so the Iwasawa main conjecture holds true in this elliptic curve.

Using Sagemath, we can check that the 5-adic L-function can be written as

$$\mathrm{char}(X_\infty) = \mathcal{L}_5(E,T) = (5^2 + O(5^3))T + O(T^2)$$

Under our assumptions, Mazur's control theorem works perfectly, so we can conclude that $\mathrm{Sel}(\mathbb{Q}, T_5E) \approx \mathbb{Z}_5 \times \mathbb{Z}_5/(5) \times \mathbb{Z}_5/(5)$. Therefore,

$$Ш(E/\mathbb{Q})[5^\infty] = Ш(E/K)[5^\infty]^{\mathrm{Gal}(K/\mathbb{Q})} \approx \mathbb{Z}_5/(5) \times \mathbb{Z}_5/(5)$$

If χ is the quadratic character of conductor 7, then $\delta_{1,\chi} = 0$, so $\mathrm{rank}(E(K)_\chi) \geq 1$. In order to determine the full structure of the twisted Selmer group, we need to compute $\Theta_{1,\chi}$. Since 11 is a Kolyvagin prime and $\mathrm{ord}_5(\delta_{11,\chi}) = 0$, we deduce that $\Theta_1 = \mathbb{Z}_5$. Hence $\mathrm{rank}(E(K)_\chi) = 1$ and $Ш(E/K)[5^\infty]_\chi = \{0\}$.

For all other characters of conductor 7, we compute $\mathrm{ord}_5(\delta_{1,\chi}) = 1$, which implies that $Ш(E/K)_\chi \approx \mathcal{O}_6/(5)$.

All the information above is enough to compute the structure of the Selmer group $\mathrm{Sel}(K, T_5E) \otimes \mathcal{O}_6$ as an $\mathcal{O}_6[\mathrm{Gal}(K/\mathbb{Q})]$-module. By proposition 6.0.6, the Fitting ideal are then given by the expressions

$$\begin{aligned}
\mathrm{Fitt}^0_{\mathbb{Z}_5}(\mathrm{Sel}(K, T_5E)) &= \frac{5}{3}(2\sigma_1 - \sigma_2 - \sigma_4) \\
\mathrm{Fitt}^1_{\mathbb{Z}_5}(\mathrm{Sel}(K, T_5E)) &= 5\sigma_1 + 4(\sigma_2 + \sigma_3 + \sigma_4 + \sigma_5 + \sigma_6) \\
\mathrm{Fitt}^2_{\mathbb{Z}_5}(\mathrm{Sel}(K, T_5E)) &= \frac{5}{3}\sigma_1 + \frac{2}{3}(\sigma_2 + \sigma_3 + \sigma_4 + \sigma_5 + \sigma_6)
\end{aligned}$$

By proposition 6.0.6, there is an isomorphism of $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-modules

$$\mathrm{Sel}(K, T_5E) = \frac{\mathbb{Z}_p[G]}{(5(2\sigma_1 - \sigma_2 - \sigma_4))} \times \left(\frac{\mathbb{Z}_p[G]}{(5\sigma_1 + 2(\sigma_2 + \sigma_3 + \sigma_4 + \sigma_5 + \sigma_6))}\right)^2$$

Example 6.0.47. Let E be the elliptic curve 35a1 in Cremona's database and let $p = 7$. For a Dirichlet character χ of conductor 51 and order 8 such that $\chi(35) = -1$ and $\chi(37)$ is a primitive 8^{th} root of unity ζ_8 satisfying that $\zeta_8^2 + 3\zeta_8 + 1 \in 7\mathbb{Z}_7$.

We can compute $\mathrm{ord}_7(\delta_{1,\chi}) = 2$, so we know that $\mathrm{rank}(E(\mathbb{Q}(\mu_{51})))_\chi = 0$ and

$$\#Ш(E/\mathbb{Q}(\mu_{51}))[7^\infty]_\chi = \big(\#(\mathcal{O}_{16}/(7))\big)^2$$

Note that χ is not self-dual, so there are no non-degenerate pairings defined on the twisted Selmer group that determine its structure. In this case, the computation of $\Theta_{1,\chi}$ is what determines whether the Tate-Shafarevich group is isomorphic to $\mathcal{O}_{16}/(7^2)$ or $\mathcal{O}_{16}/(7) \times \mathcal{O}_{16}/(7)$.

The smallest Kolyvagin prime is $\ell = 2\,801$ and satisfies that $\delta_{\ell,\chi} \in \mathcal{O}_8^\times$. Hence $\Theta_{1,\chi} = \mathcal{O}_8$ and

$$\#Ш(E/\mathbb{Q}(\mu_{51}))[7^\infty]_\chi \approx \mathcal{O}_{16}/(7^2)$$

Example 6.0.48. Consider the elliptic curve 11a1 in Cremona's database, the abelian extension $K = \mathbb{Q}(\mu_{61})$ and the prime $p = 101$.

Let χ be the character of conductor 61 and order 20 such that $\chi(2)$ is the unique primitive 20^{th} root of unity in $60 + 101\mathbb{Z}_{101}$. Then

$$\mathrm{ord}_{101}(\delta_{1,\chi}) = \mathrm{ord}_{101}(\delta_{1,\overline{\chi}}) = 1$$

Theorem 6.0.13 then implies that

$$\mathrm{Sel}(\mathbb{Q}, T_pE \otimes \mathbb{Z}_{101}(\chi)) \approx \mathrm{Sel}(\mathbb{Q}, T_pE \otimes \mathbb{Z}_{101}(\overline{\chi})) \approx \mathbb{Z}_{101}/(101)$$

For the quadratic character χ' of conductor 61, we obtain that $\delta_{1,\chi'} = 0$, so theorem 6.0.13 implies that $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Sel}(\mathbb{Q}, T_pE\otimes)) \geq 1$. To determine the full structure of this Selmer group, we need to compute $\Theta_{1,\chi'}$. The smallest Kolyvagin prime is $\ell' = 64\,237$ and satisfies that $\mathrm{ord}_{101}(\delta_{\ell',\chi}) = 0$. Hence, $\Theta_{i,\chi} = \mathbb{Z}_p$, so

$$\mathrm{Sel}(\mathbb{Q}, T_pE \otimes \mathbb{Z}_{101}) \approx \mathbb{Z}_{101}$$

Finally, consider a character χ'' of conductor 61 and order 6. It satisfies that $\chi(2)$ is a 6^{th}-root of unity. Then $\delta_{1,\chi''} = \delta_{1,\overline{\chi''}} = 0$. The smallest Kolyvagin prime for these characters is $\ell'' = 2\,528\,233$, satisfying that

$$\mathrm{ord}_{101}(\delta_{\ell'',\chi''}) = \mathrm{ord}_{101}(\delta_{\ell'',\overline{\chi''}}) = 0$$

Hence,

$$\mathrm{Sel}\big(\mathbb{Q}, T_pE \otimes \mathcal{O}_6(\chi'')\big) \approx \mathrm{Sel}\big(\mathbb{Q}, T_pE \otimes \mathcal{O}_6(\overline{\chi''})\big) \approx \mathcal{O}_6$$

Overall, assuming the finiteness of the Tate-Shafarevich group, we know that $\mathrm{rank}(E(K)) = 3$. Furthermore, we know how the rank grows along the subextensions of $K/\mathbb{Q}$. Indeed, if K_2 and K_3 are the subextensions of degrees 2 and 3, respectively, we know that $\mathrm{rank}(E(K_2)) = 1$ and $\mathrm{rank}(E(K_3)) = 2$.

Similarly, if L is a subextension of $K/\mathbb{Q}$, then $Ш(E/L)$ would have order 101^2 if $[L : \mathbb{Q}] \in 20\mathbb{Z}$ and would be trivial otherwise.

Example 6.0.49. We can use this method to find Tate-Shafarevich groups divisible by large primes. Consider the elliptic curve 27a1 in the Cremona tables and the prime $p = 472\,558\,791\,937$. Let χ be the Dirichlet character of conductor 89 satisfying that $\chi(3)$ is the unique primitive 88^{th} root of unity in $382\,613\,086\,515 + p\mathbb{Z}_p$. Then

$$\mathrm{ord}_p(\delta_{1,\chi}) = 1$$

Therefore, we can conclude that

$$\mathrm{Sel}(\mathbb{Q}, T_pE \otimes \mathbb{Z}_p(\chi)) \approx \mathbb{Z}_p/(p)$$

Appendix A

Algebraic Preliminaries

A.1 Fitting ideals

Definition A.1.1. Let M be a finitely presented R-module. Choose a resolution

$$R^n \xrightarrow{A} R^m \longrightarrow M \longrightarrow 0$$

where the map $R^n \to R^m$ is represented by the matrix A. For every $i \geq 0$, we define the i^{th} Fitting ideal $\text{Fitt}_i^R(M)$ is the ideal in R generated by the minors of size $(m-i)$ of A.

Remark A.1.2. The i^{th} Fitting ideal coincides with the image of the following map, induced by the matrix A.

$$\text{Fitt}_i^R(M) = \text{Im}\left(\bigwedge^{m-i} R^n \to \bigwedge^{m-i} R^m\right)$$

It can be shown that Fitting ideals are well defined.

Proposition A.1.3. ([Eis95, Corollary 20.4]) The Fitting ideals $\text{Fitt}_i^R(M)$ are independent of the chosen resolution.

When the coefficient ring R is simple enough, the sequence of Fitting ideals can recover M up to pseudo-isomorphism.

Proposition A.1.4. Let R be a either a discrete valuation ring or a quotient of it, and let M be a finitely generated R-module. Then the Fitting ideals determine M up to isomorphism.

Proof. Let $\mathfrak{m}$ be the maximal ideal of R. The structure theorem of finitely generated modules over principal ideal domains implies that there are integers r, s and $\alpha_1 \geq \ldots \geq \alpha_s$ such that

$$M \approx R^r \times R/\mathfrak{m}^{\alpha_1} \times \cdots \times R/\mathfrak{m}^{\alpha_s}$$

Then M admits a resolution

$$R^{r+s} \xrightarrow{A} R^{r+s} \longrightarrow M \longrightarrow 0$$

where the matrix A is given by

$$A = \left(\begin{array}{c:ccc} \mathbf{0}_{r\times r} & \multicolumn{3}{c}{\mathbf{0}_{s\times r}} \\ \hdashline & \pi^{\alpha_1} & & \\ \mathbf{0}_{r\times s} & & \ddots & \\ & & & \pi^{\alpha_s} \end{array}\right)$$

where π is a generator of $\mathfrak{m}$. We can then compute,

- $i \in \{0, \ldots, r-1\} \Rightarrow \mathrm{Fitt}_i(M) = (0)$
- $j \in \{0, \ldots, s-1\} \Rightarrow \mathrm{Fitt}_{r+j} = \prod_{k=j+1}^{s} \mathfrak{m}^{i_k} = \mathfrak{m}^{\sum_{k=j+1}^{s} i_k}$
- $i \geq r+s \Rightarrow \mathrm{Fitt}_i(M) = (1)$.

The Fitting ideals determine M up to isomorphism, since

- r is the minimum i such that $\mathrm{Fitt}_i(M) \neq 0$.
- For $i \geq 0$, $\alpha_i = \mathrm{Fitt}_{r+i+1}(M)\mathrm{Fitt}_{r+i}(M)^{-1}$.

□

A.2 Preliminaries on exterior powers

The goal of this section is to introduce the necessary theory of exterior biduals.

Definition A.2.1. Let R be a ring, let M be an R-module and let $r \in M$. The r^{th} *exterior power*

$$\bigwedge^{r} M$$

is defined as the quotient of the tensor product $M^{\otimes r}$ by the submodule generated by the elements of the form

$$m_1 \otimes \cdots \otimes m_i \otimes \cdots \otimes m_j \otimes \cdots \otimes m_r + m_1 \otimes \cdots \otimes m_j \otimes \cdots \otimes m_i \otimes \cdots \otimes m_r$$

Definition A.2.2. If F is a free R-module of rank s, the determinant of F is defined as

$$\det(F) = \bigwedge^{s} F$$

We now state two basic properties of the determinant.

Proposition A.2.3. Let $A \subset B$ be free R-modules such that B/A is also free. Then there is a canonical isomorphism

$$\det(A) \otimes \det(B/A) \cong \det(B)$$

Proposition A.2.4. Let A be a free R-module. There is a canonical isomorphism

$$\det(A) \otimes \det(A^+) \cong R$$

Definition A.2.5. Let R be a ring, let M be an R-module and let $r \in M$. The r^{th} *exterior bidual* is defined as

$$\bigcap^r M = \left(\bigwedge^r M^+\right)^+$$

The properties of exterior biduals will be deduced assuming certain properties of the ring R.

A.2.1 Exterior powers over self-injective rings

The goal of this section is to introduce the necessary theory of exterior biduals over self injective ring.

properties of self-injective rings

Proposition A.2.6. Let R be a self-injective ring. The dual functor $M \mapsto M^+$ is exact.

Proposition A.2.7. If we have an exact sequence of R-modules over a self-injective ring R

$$0 \longrightarrow M \xrightarrow{\mu} N \xrightarrow{\varepsilon} R^s$$

for some natural number s. If $r \geq s$ is another natural number, there is a canonical map

$$\phi_{N,M} : \bigcap^r N \to \bigcap^{r-s} M$$

Proof. By Proposition A.2.6, there is another exact sequence

$$R^s \xrightarrow{\varepsilon^+} N^+ \xrightarrow{\mu^+} M+ \longrightarrow 0$$

For every $m \in M^+$, choose a lift $n \in N^+$. With this choices, there is a lifting map of sets

$$\widetilde{\mu^+} : \ M^+ \to N^+$$

Denote by $\{e_1, \ldots, e_s\}$ the canonical basis of R_s. Then define the map

$$\phi^*_{N,M} : \bigwedge^{r-s} M^+ \to \bigwedge^r N^+ : \ m_1 \wedge \cdots \wedge m_{r-s} \mapsto \widetilde{\mu^+}(m_1) \wedge \cdots \wedge \widetilde{\mu^+}(m_{r-s}) \wedge \varepsilon^+(e_1) \wedge \cdots \wedge \varepsilon^+(e_s)$$

One can chech that this definition is independend of the lifting choices made and an R-homomorphism.

The dual of this map induces a map

$$\phi_{N,M} : \bigcap^r N \to \bigcap^{r-s} M$$

□

When the last term of the previous exact sequence is free, but not R^s, the map $\phi_{N,M}$ is no longer canonical unless we tensor with the determinant of the dual module.

Proposition A.2.8. If we have an exact sequence of R-modules over a self-injective ring R

$$0 \longrightarrow M \xrightarrow{\mu} N \xrightarrow{\varepsilon} F$$

where F is a free R-module of rank s. If $r \geq s$ is a natural number, there is a canonical map

$$\phi_{N,M} : \bigcap^{r} N \otimes \det(F^+) \to \bigcap^{r-s} M$$

Proof. As in Proposition A.2.7, we can construct a lifting map of sets

$$\widetilde{\mu^+} : \bigwedge^{r-s} M^+ \to \bigwedge^{r-s} N^+$$

We can use it to construct a well-defined R-homomorphism

$$\phi^*_{N,M} : \bigwedge^{r-s} M^+ \otimes \det(F^+) \to \bigwedge^{r-s} N^+,\ m \otimes f \mapsto \widetilde{\mu^+}(m) \otimes \varepsilon^+(f)$$

The dual map can be expressed as

$$\phi_{N,M} : \bigcap^{r-s} N \otimes \det(F^+) \to \bigcap^{r} M$$

□

A.2.2 Exterior biduals over discrete valuation rings

When R is a discrete valuation ring, we can prove an analogue of Propositions A.2.8 and A.2.8.

Proposition A.2.9. If we have an exact sequence of R-modules over a discrete valuation ring R

$$0 \longrightarrow M \xrightarrow{\mu} N \xrightarrow{\varepsilon} R^s$$

for some natural number s. If $r \geq s$ is another natural number, there is a canonical map

$$\phi_{N,M} : \bigcap^{r} N \to \bigcap^{r-s} M$$

Proof. The image of ε is a submodule of R^s so, in particular, it is torsion-free. Therefore, it is a free R-module, so $\mathrm{Ext}(\mathrm{Im}(\varepsilon), R) = 0$. Hence there is an exact sequence

$$R^s \longrightarrow N^+ \longrightarrow M^+ \longrightarrow 0$$

We can use this exact sequence to construct the map $\phi_{N,M}$ as in Proposition A.2.7. □

Similarly, we can adapt the previous result to the case when the last term is a free R-module, non-canonically isomorphic to R^s.

Proposition A.2.10. If we have an exact sequence of R-modules over a discrete valuation ring R

$$0 \longrightarrow M \xrightarrow{\mu} N \xrightarrow{\varepsilon} F$$

where F is a free R-module of rank s. If $r \geq s$ is a natural number, there is a canonical map

$$\phi_{N,M} : \bigcap^{r} M \otimes \det(F^+) \to \bigcap^{r-s} N$$

A.2.3 Exterior biduals over the Iwasawa algebra

Proposition A.2.11. Consider the exact sequence of Λ-modules

$$0 \longrightarrow N \longrightarrow M \longrightarrow \Lambda^s$$

Then there is a canonical map

$$\Phi : \bigcap^{r+s} M \to \bigcap^{r} N$$

Since Λ is not a self-injective ring, we need to prove some basic facts about the extension groups of Λ-modules before addressing the proof of Proposition **??**.

Lemma A.2.12. Let M be a submodule of Λ^s. Then $\mathrm{Ext}^1(M, \Lambda)$ is finite.

Proof. For every Λ-module M, recall that $M^+ := \mathrm{Hom}(M, \Lambda)$. There is a canonical map

$$\Phi : \ M \to M^{++}, \ m \mapsto (\varphi \in M^+ \mapsto \varphi(a))$$

Let $T_1(M) = \ker \Phi$. Since M is contained in Λ^s, we claim that $T_1(M) = 0$. Indeed, fix an inclusion $\iota : \ M \hookrightarrow \Lambda^s$ and denote by $\pi^i : \ \Lambda^s \to \Lambda$ the projection at the i^{th} coordinate. Let $m \in M \setminus \{0\}$. Then there is some $j \in \{1, \ldots, s\}$ such that the j^{th} coordinate of $\iota(m)$ is non-zero. Then

$$\Phi(m)(\pi^j \circ \iota) = \pi_j(\iota(m)) \neq 0$$

Thus $m \notin T_1(M)$ and the proof of the claim is complete.

By [NSW00, Corollary 5.5.9], $\mathrm{Ext}^1(M, \Lambda)$ is finite. □

Lemma A.2.13. Let $N \subset M$ be Λ modules such that N has finite index in M. Then $N^* = M^*$.

Proof. There is an exact sequence

$$(M/N)^* \longrightarrow M^* \longrightarrow N^* \longrightarrow \mathrm{Ext}^1(M/N, \Lambda)$$

Since M/N is finite, then both $(M/N)^*$ and $\mathrm{Ext}^1(M/N, \Lambda)$ vanish. Indeed, $(M/N)^* = 0$ since Λ does not contain elements of finite order and $\mathrm{Ext}^1(M/N, \Lambda) = 0$ by [NSW00, Corollary 5.5.4] □

Proof of proposition **??**. Let I be the image of the map $N \to M$ inside Λ^s. By lemma A.2.12, $\mathrm{Ext}^1(I,\Lambda)$ is finite. There is an exact sequence

$$\Lambda^s \longrightarrow M^* \longrightarrow N^* \longrightarrow \mathrm{Ext}^1(I,\Lambda)$$

Call J to the image of M^* inside N^*, which has finite index in N^* because of the finiteness of $\mathrm{Ext}^1(I,\Lambda)$. The exact sequence

$$\Lambda^s \longrightarrow M^* \longrightarrow J \longrightarrow 0$$

induces a canonical map

$$\bigwedge^r J \to \bigwedge^{r+s} M^*$$

The dual of this map is

$$\bigcap^{r+s} M^* \to \mathrm{Hom}\left(\bigwedge^r J, \Lambda\right)$$

Since $\bigwedge^r J$ has finite index in $\bigwedge^r N^*$, lemma A.2.13 implies that their duals are equal, so the above map can be rewritten as

$$\bigcap^{r+s} M^* \to \bigcap^r N^*$$

□

Proposition A.2.14. Consider the exact sequence of Λ-modules

$$0 \longrightarrow N \longrightarrow \Lambda^{r+s} \longrightarrow \Lambda^s \longrightarrow M \longrightarrow 0$$

Let φ be a generator of $\bigcap^{r+s} \Lambda^{r+s}$ and let

$$\Phi : \bigcap^{r+s} \Lambda^{r+s} \to \bigcap^r N$$

be the map constructed in proposition **??**. Then the image of $\Phi(\varphi) \in \mathrm{Hom}\left(\bigwedge^r N^*, \Lambda\right)$ contains the 0^{th} Fitting ideal of M.

Proof. Let Ψ be the composition of the following maps

$$\bigwedge^r (\Lambda^{r+s})^* \longrightarrow \bigwedge^r N^* \longrightarrow \bigwedge^{s+t} (\Lambda^{r+s})^* \xrightarrow{\varphi} \Lambda$$

where the first map is induced by the homomorphism $(\Lambda^{r+s})^* \to N^*$ and has finite cokernel, the second map is the one constructed in the proof of **??**. Since $\Phi(\varphi)$ is the composition of the last two maps, its image contains the image of Ψ with finite index. The proof concludes by noticing the image of Ψ coindides with the 0^{th} Fitting ideal of M. □

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Reading, Massachusetts: Addison-Wesley, 1969. ISBN: 978-0-201-00361-0.

[BK90] Spencer Bloch and Kazuya Kato. 'L-functions and Tamagawa numbers of motives'. In: *The Grothendieck Festschrift, Vol. I*. Vol. 86. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BSS18] David Burns, Ryotaro Sakamoto and Takamichi Sano. *On the theory of higher rank Euler, Kolyvagin and Stark systems, II*. 2018. arXiv: 1805.08448 [math.NT].

[DD09] Tim Dokschitser and Vladimir Dokschitser. 'Self-duality of Selmer groups'. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 146.2 (Mar. 2009), pp. 257–267.

[Edi91] Bas Edixhoven. 'On the Manin constants of modular elliptic curves'. In: *Arithmetic algebraic geometry (Texel, 1989)*. Vol. 89. Progr. Math. Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[Eis95] David Eisenbud. *Commutative Algebra*. Springer New York, NY, 1995.

[FW22] Olivier Fouquet and Xin Wan. *The Iwasawa Main Conjecture for universal families of modular motives*. 2022. arXiv: 2107.13726 [math.NT].

[Kat04] Kazuya Kato. 'p-adic Hodge theory and values of zeta functions of modular forms'. In: 295. Cohomologies p-adiques et applications arithmétiques. III. 2004, pp. ix, 117–290.

[Kat21] Takenori Kataoka. 'Equivariant Iwasawa theory for elliptic curves'. In: *Math. Z.* 298.3-4 (2021), pp. 1653–1725.

[Kim25] Chan-Ho Kim. *The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves*. 2025. arXiv: 2203.12159 [math.NT].

[KKS20] Chan-Ho Kim, Myoungil Kim and Hae-Sang Sun. 'On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms'. In: *Selecta Math. (N.S.)* 26.2 (2020), Paper No. 31, 47.

[Kur14a] Masato Kurihara. 'Refined Iwasawa theory for p-adic representations and the structure of Selmer groups'. In: *Münster J. Math.* 7.1 (2014), pp. 149–223.

[Kur14b] Masato Kurihara. 'The structure of Selmer groups of elliptic curves and modular symbols'. In: *Iwasawa theory 2012*. Vol. 7. Contrib. Math. Comput. Sci. Springer, Heidelberg, 2014, pp. 317–356.

[Man72] Ju. I. Manin. 'Parabolic points and zeta functions of modular curves'. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 36 (1972), pp. 19–66.

[Maz78] B. Mazur. 'Rational isogenies of prime degree (with an appendix by D. Goldfeld)'. In: *Invent. Math.* 44.2 (1978), pp. 129–162.

[MR04] Barry Mazur and Karl Rubin. 'Kolyvagin systems'. In: *Mem. Amer. Math. Soc.* 168.799 (2004), pp. viii+96.

[MT87] B. Mazur and J. Tate. 'Refined conjectures of the "Birch and Swinnerton-Dyer type"'. In: *Duke Mathematical Journal* 54.2 (1987), pp. 711–750.

[MTT86] B. Mazur, J. Tate and J. Teitelbaum. 'On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer'. In: *Invent. Math.* 84.1 (1986), pp. 1–48.

[NSW00] Jürgen Neukirch, Alexander Schmidt and Key Wingberg. *Cohomology of number fields*. Grundlehren der mathematischen Wissenschaften. Springer-Berlin, Heidelberg, 2000, pp. xv–826.

[Ota18] Kazuto Ota. 'Kato's Euler system and the Mazur-Tate refined conjecture of BSD type'. In: *Amer. J. Math.* 140.2 (2018), pp. 495–542.

[Rub00] Karl Rubin. *Euler systems*. Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, pp. xii+227.

[Sak18] Ryotaro Sakamoto. 'Stark systems over Gorenstein local rings'. In: *Algebra and Number Theory* 12.10 (2018), pp. 2295–2326.

[Sak22] Ryotaro Sakamoto. 'p-Selmer group and modular symbols'. In: *Doc. Math.* 27 (2022), pp. 1891–1922.

[Ste89] Glenn Stevens. 'Stickelberger elements and modular parametrizations of elliptic curves'. In: *Invent. Math.* 98.1 (1989), pp. 75–106.

[SU14] Christopher Skinner and Eric Urban. 'The Iwasawa main conjectures for GL_2'. In: *Invent. Math.* 195.1 (2014), pp. 1–277.

[Swe22] Naomi Sweeting. *Kolyvagin's Conjecture and patched Euler systems in anticyclotomic Iwasawa theory*. 2022. arXiv: `2012.11771 [math.NT]`. URL: `https://arxiv.org/abs/2012.11771`.

[The] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*. `https://www.sagemath.org`.

[WW22] Hanneke Wiersema and Christian Wuthrich. 'Integrality of twisted L-values of elliptic curves'. In: *Doc. Math.* 27 (2022), pp. 2041–2066.