Lambda dual

Alberto Angurel

28th December 2025

Contents

0.1 Galois cohomology

Definition 0.1.1. An element $n \in \mathcal{N}(\mathcal{P})$ is said to be a *core vertex* if either $H^1_{\mathcal{F}(n)}(\mathbb{Q}, T) = 0$ or $H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*) = 0$.

Proposition 0.1.2. ([MR04, corollary 4.1.9]) For every $n \in \mathcal{N}(\mathcal{P})$, there is some core vertex $m \in \mathcal{N}(\mathcal{P})$ such that $n|m$.

Proposition 0.1.3. ([MR04, proposition 3.6.1]) Let $c_1, c_2 \in H^1(\mathbb{Q}, T) \setminus \{0\}$ and let $c_3, c_4 \in H^1(\mathbb{Q}, T^*) \setminus \{0\}$. For every $k \in \mathbb{N}$, there exists an infinite set of primes $S \subset \mathcal{P}_k$ such that

$$\mathrm{loc}_\ell(c_i) \neq 0 \quad \forall \ell \in S, \ \forall i = 1, 2, 3, 4$$

The main consequence of this proposition is that it can be used to find primes whose finite localisation maps are surjective.

Corollary 0.1.4. Let $(T, \mathcal{F}, \mathcal{P})$ be a Selmer triple satisfying **??**-**??** and let $j \in \mathcal{N}$ be such that $\mathfrak{m}^{j-1} H^1_{\mathcal{F}}(\mathbb{Q}, T) \neq 0$. Then there are infinitely many primes $\ell \in \mathcal{P}$ such that

$$\mathrm{loc}_\ell(H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^j)) = H^1_f(\mathbb{Q}_\ell, T/\mathfrak{m}^j)$$

Assume further than $\mathfrak{m}^{j-1} H^1_{\mathcal{F}}(\mathbb{Q}, T^*) \neq 0$. Then there are infinitely many primes $\ell \in \mathcal{P}$ such that both localisation maps

$$\mathrm{loc}^{\mathrm{f}}_\ell(H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^j)) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j), \quad \mathrm{loc}^{\mathrm{f}}_\ell(H^1_{\mathcal{F}}(\mathbb{Q}, T^*[\mathfrak{m}^j])) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^j])$$

are surjective.

Proof. By lemmas **??** and **??**, we can find some elements $d_1 \in H^1_{\mathcal{F}}(\mathbb{Q}, T/m^j)$ and $d_3 \in H^1_{\mathcal{F}}(\mathbb{Q}, T^*[\mathfrak{m}])$ such that $\mathfrak{m}^{j-1} d_1 \neq 0$ and $\mathfrak{m}^{j-1} d_3 \neq 0$. Consider $c_1 = \pi^{j-1} d_1$ and $c_3 = \pi^{j-1} d_3$, where π is some generator of $\mathfrak{m}$. Since both c_1 and c_3 are nonzero, proposition 0.1.3 guarantees the existence of infinitely many primes $\ell \in \mathcal{P} \cap \mathcal{P}_j$ such that $\mathrm{loc}_\ell(c_1)$ and $\mathrm{loc}_\ell(c_3)$ are non-zero. Moreover, since c_1 and c_3 belong to the Selmer groups, their localisation belong to the finite cohomology groups, so $\mathrm{loc}^{\mathrm{f}}_\ell(c_1) \neq 0$ and $\mathrm{loc}^{\mathrm{f}}_\ell(c_3) \neq 0$. By corollary **??**, $H^1_f(\mathbb{Q}_\ell, T/\mathfrak{m}^j)$ and $H^1_f(\mathbb{Q}_\ell, T^*[\mathfrak{m}^j])$ are free of rank one over $R/\mathfrak{m}^j$. Therefore, the only way the localizations of c_1 and c_3 do not vanish is when $\mathrm{loc}^f_\ell(d_1)$ generates $H^1_f(\mathbb{Q}_\ell, T/\mathfrak{m}^j)$ and $\mathrm{loc}^f_\ell(d_3)$ generates $H^1_f(\mathbb{Q}_\ell, T^*[\mathfrak{m}^j])$. □

This result alongside the following lemma plays a central role in the proof of theorem **??** below.

Lemma 0.1.5. ([MR04, lemma 4.1.7(ii)]) Let $\ell \in \mathcal{P}_k$ be a prime not dividing $n \in \mathcal{N}_k$. If the localisation map

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

is surjective, then

$$H^1_{\mathcal{F}^*(n\ell)}(\mathbb{Q}, T^*[\mathfrak{m}^k]) = H^1_{\mathcal{F}^*_\ell(n)}(\mathbb{Q}, T^*[\mathfrak{m}^k])$$

Chapter 1

Kolyvagin systems

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 $G_F = \mathrm{Gal}(\overline{K}/F)$.

Notation 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 $GL_{rank(T)}(R)$ 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.

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

Definition 1.1.7. 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 1.1.8. 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 confussion, 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 1.1.9. (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

$$H^1_{\mathrm{f}}(K_\ell, T) := H^1(K_\ell^{\mathrm{ur}}, T) = \ker\Big(H^1(K_\ell, T) \to H^1(\mathcal{I}_\ell, T)\Big)$$

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 1.1.10. Let ℓ be a finite place of K as in Definition 1.1.9. The *singular cohomology* at ℓ is the quotients

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

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

Proposition 1.1.11. ([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 1.1.12. 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 1.1.13. 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 1.1.14. ([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 1.1.15. ([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 1.1.16. 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 1.1.17. (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 1.1.17.

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 1.1.17, 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 of R, the inclusion $T^*[I] \hookrightarrow T^*$ induces an isomorphism

$$H^1(K, T^*[I]) \cong H^1(K, T^*)[I]$$

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. review with assumptions on R.

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 1.1.17, 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

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

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. do □

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 approppriate 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. do □

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 study the propagated Selmer group to the quotient $T/\mathfrak{m}^{e_1}$ and its dual $T^*[m^{e_1}]$.

Applying Proposition 1.2.21 for some nonzero $c_1 \in \mathfrak{m}^{e_1-1}H^1_{\mathcal{F}}(\mathbb{Q},T/\mathfrak{m}^{e_1})$ and some nonzero $c_1^* \in \mathfrak{m}^{e_1-1}H^1_{\mathcal{F}^*}(K,T[\mathfrak{m}^{e_1}]^*)$, we can find infinitely many primes $\ell \in \mathcal{P}$ such that the localisation maps technicality Kolyvagin primes with quotients

$$\mathrm{loc}_\ell : H^1_{\mathcal{F}}(\mathbb{Q},T/\mathfrak{m}^{e_1}) \to H^1_{\mathrm{f}}(\mathbb{Q}_\ell,T/\mathfrak{m}^{e_1}), \quad \mathrm{loc}_\ell^* : H^1_{\mathcal{F}^*}(\mathbb{Q},T^*[\mathfrak{m}^{e_1}]) \to H^1_{\mathrm{f}}(\mathbb{Q},T^*[\mathfrak{m}^{e_1}])$$

are surjective. Since $\ell \in \mathcal{P}$, both $H^1_{\mathrm{f}}(\mathbb{Q}_\ell,T/\mathfrak{m}^{e_1})$ and $H^1_{\mathrm{f}}(\mathbb{Q}_\ell,T^*[e_1])$ are free $R/\mathfrak{m}^{e_1}$-modules of rank one by Proposition 1.1.11. technicality with quotients

By Proposition 1.2.10 and Lemma 1.2.22,

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

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

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

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. □

When $\chi(\mathcal{F}) = 0$, 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 $\mathbb{Z}_p[[G_{\mathbb{Q}}]] \to \mathrm{End}(T)$.

Lemma 1.2.27. Let $\mathcal{F}$ be a cartesian Selmer structure satisfying Assumptions 1.1.5 and 1.2.26. Assume that

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

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

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

fix references

Proof. By corollary 0.1.4, we can find an auxiliary prime $b \in \mathcal{N}_k$ such that the localisation maps

$$\mathrm{loc}_b^{\mathrm{f}} : \ H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^{e_1}) \to H^1_{\mathrm{f}}(\mathbb{Q}_b, T/\mathfrak{m}^{e_1}), \quad \mathrm{loc}_b^{\mathrm{f}} : \ H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^{e_1}]) \to H^1_{\mathrm{f}}(\mathbb{Q}_b, T^*[\mathfrak{m}^{e_1}])$$

are surjective. By corollary **??**, $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ is isomorphic to $R/\mathfrak{m}^{e_1}$ and

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

Since $\chi(\mathcal{F}^b) = 1$ by proposition **??**, we have that

$$H^1_{\mathcal{F}^b}(\mathbb{Q}, T/\mathfrak{m}^k) \approx R/\mathfrak{m}^k \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s} \tag{1.2}$$

By proposition 1.7.5, we can find a prime ℓ satisfying the following:

- The kernel of the localisations loc_ℓ and loc_b defined on $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])$ are the same. By fixing generators x_b and x_ℓ of $H^1_{\mathrm{f}}(\mathbb{Q}_b, T^*[\mathfrak{m}^k])$ and $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$, respectively, we are defining an isomorphism

  $$H^1_{\mathrm{f}}(\mathbb{Q}_b, T^*[\mathfrak{m}^k]) \cong R/\mathfrak{m}^k \cong H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$$

  Under this isomorphism, we can understand $\mathrm{loc}_b^{\mathrm{f}}, \mathrm{loc}_\ell^{\mathrm{f}} \in \mathrm{Hom}(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]), R/\mathfrak{m}^k)$. In this setting, the above condition implies that there exists a unit $u \in (R/\mathfrak{m}^k)^\times$ such that $\mathrm{loc}_\ell = u\mathrm{loc}_b$.

- The kernel of the finite localisation map

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

  coincides with $H^1_{\mathcal{F}_b}(\mathbb{Q}, T/\mathfrak{m}^k)$. It implies that

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

Since $\chi(\mathcal{F}^{\ell b}) = 2$ by proposition **??**, there is an isomorphism

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

By proposition 1.2.5, we can consider the following exact sequence

$$H^1_{\mathcal{F}^{\ell b}}(\mathbb{Q}, T/\mathfrak{m}^k) \longrightarrow H^1_{\mathrm{s}}(\mathbb{Q}_b, T/\mathfrak{m}^k) \oplus H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k) \longrightarrow H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])$$

Let $\widehat{x_b} \in H^1_s(\mathbb{Q}_b, T/\mathfrak{m}^k)$ and $\widehat{x_\ell} \in H^1_s(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ be the dual elements of x_b and x_ℓ under the pairing given in proposition 1.1.17. The element $(\widehat{x_b}, -u\widehat{x_\ell}) \in H^1_{\mathrm{s}}(\mathbb{Q}_b, T/\mathfrak{m}^k) \oplus H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ belongs to the kernel of the second map, so there is an element $z \in H^1_{\mathcal{F}^{\ell b}}(\mathbb{Q}, T/\mathfrak{m}^k)$ such that $\mathrm{loc}^s_b(z) = \widehat{x_b}$ and $\mathrm{loc}^s_\ell(z) = -u\widehat{x_\ell}$. The relaxed Selmer groups splits as follows.

$$H^1_{\mathcal{F}^{\ell b}}(\mathbb{Q}, T/\mathfrak{m}^k) = (R/\mathfrak{m}^k)z \oplus H^1_{\mathcal{F}^b}(\mathbb{Q}, T/\mathfrak{m}^k) = (R/\mathfrak{m}^k)z \oplus H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k)$$

We want to show now that

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

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

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

then $\pi^{k-e_1}x \in H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^k) \subset H^1_{\mathcal{F}^b}(\mathbb{Q}, T/\mathfrak{m}^k)$ so $\alpha \in \mathfrak{m}^{e_1}/\mathfrak{m}^k$. Then $\pi^{k-1}\beta \neq 0$. Since $\mathrm{loc}^{\mathrm{f}}_\ell(H^1_{\mathcal{F}^b}(\mathbb{Q}, T/\mathfrak{m}^k))$ is equal to $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$, the isomorphism in (1.2) implies that $\mathrm{loc}^{\mathrm{f}}_\ell(\beta)$ generates $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$.

As $\mathrm{loc}^{\mathrm{f}}_\ell(x) - \mathrm{loc}^{\mathrm{f}}_\ell(\beta) = \alpha \mathrm{loc}^{\mathrm{f}}_\ell(z) \in \mathfrak{m}^{e_1} H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$, then $\mathrm{loc}^{\mathrm{f}}_\ell(x)$ is also a generator and thus $\mathrm{loc}^{\mathrm{f}}_\ell$ is surjective when considered as a map from $H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k)$. Then the structure theorem over principal ideal domains implies

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

□

1.3 Fitting ideals

The Selmer groups defined in the previous section are the objects we want to study. We aim to give a description of the structure of this groups. In order to be precise, we introduce the concept of Fitting ideals.

Definition 1.3.1. 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 $\mathrm{Fitt}^R_i(M)$ is the ideal in R generated by the minors of size $(m - i)$ of A.

Remark 1.3.2. The i^{th} Fitting ideal coincides with the image of the following map, induced by the matrix A.

$$\mathrm{Fitt}_i^R(M) = \mathrm{Im}\left(\bigwedge^{m-i} R^n \to \bigwedge^{m-i} R^m\right)$$

It can be shown that Fitting ideals are well defined.

Proposition 1.3.3. ([Eis95, Corollary 20.4]) The Fitting ideals $\mathrm{Fitt}_i^R(M)$ 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 1.3.4. Let R be a discrete valuation ring 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

$$A = \left(\begin{array}{c:ccc} \mathbf{0}_{r\times r} & & \mathbf{0}_{s\times r} & \\ \hdashline & \pi^{\alpha_1} & & \\ \mathbf{0}_{r\times s} & & \ddots & \\ & & & \pi^{\alpha_s} \end{array}\right)$$

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 $i \geq 0$, $\alpha_i = \mathrm{Fitt}_{r+i+1}(M)\mathrm{Fitt}_{r+i}(M)^{-1}$.

$\square$

1.4 Classical Kolyvagin systems

Fix the canonical homomorphism for the local cohomology / generator of $\mathcal{G}_\ell$

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 1.4.1. Assume that R is a principal, artinian, local ring with maximal ideal $\mathfrak{m}$ generated by some π and finite residue field k of characteristic p. In addition, assume $\mathcal{F}$ is a cartesian Selmer structure such that $\chi(\mathcal{F}) = 1$.

Definition 1.4.2. A *Kolyvagin system* for a Selmer structure $\mathcal{F}$

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

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

$$\mathrm{loc}_\ell(\kappa_{n\ell}) = \phi_\ell^{\mathrm{fs}} \circ \mathrm{loc}_\ell(\kappa_n) \tag{1.3}$$

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

Remark 1.4.3. 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 1.4.4. Let M be an R-module and let $a \in M$. Consider the canonical map into the bidual module

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

The *index* of a is defined as

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

Remark 1.4.5. 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 1.4.6. 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 1.4.7. 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 1.4.8. ([MR04, Theorem 4.3.3]) Under Assumption 1.4.1, $\mathrm{KS}(\mathcal{F})$ is a free, cyclic R-module.

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

Definition 1.4.9. 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 1.4.10. ([MR04, Theorem 4.5.9]) 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 $\mathcal{F}$ be a cartesian Selmer structure on T satisfying that $\chi(\mathcal{F}) = 1$. If $\kappa \in \mathrm{KS}(\mathcal{F})$ is a primitive Kolyvagin system, then

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

The proof of Theorem 1.4.10 is divided in the following two lemmas:

Lemma 1.4.11. Under Assumption 1.4.1, 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 1.4.12. Under Assumption 1.4.1, then

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

1.5 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 1.5.1. ([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 1.5.2. 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 $\overline{T} := T \otimes k$

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

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 GG, the quantity

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

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

Remark 1.5.3. 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 $\chi(\mathcal{F}^\ell) = 1$.

prove quotient at l is free of rank one

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 1.5.4. 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 1.5.5. 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 $\kappa \in \mathrm{KS}(\mathcal{G})$. We can define

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

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

Theorem 1.5.6. 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, and let $\mathcal{F} \leq \mathcal{G}$ be a 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

$$\Theta_i^{(0)}(\kappa,\mathcal{F}) \subset \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(K,T)\big) \tag{1.4}$$

Moreover, if one of the following conditions is satisfied

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

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

(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

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

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

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

Similarly to the core rank case, the proof is divided in the following two lemmas:

Lemma 1.5.7. 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 1.5.8. If $\mathcal{F}$ is a cartesian

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

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

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

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

Lemma 1.5.9. There exists some vertex $n_r \in \mathcal{N}_r$ such that

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

Note that Lemma 1.5.9 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

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

We can extend this construction to higher values of i.

Lemma 1.5.10. 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 1.5.6 for their respective indices.

Corollary 1.5.11. For the indices $k \geq 0$ such that there exists an element $n_r \in \mathcal{N}_r$ as in Lemma 1.5.10, there is an equality

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

Final comments

1.5.1 Proof of Lemma 1.5.7

The proof of Lemma 1.5.7 involves comparing the indices of κ_n and δ_n, so we can then apply Lemma 1.4.11.

Lemma 1.5.12. 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

$$H^1_{\mathcal{G}(n)}(K, T) \approx R \oplus H^1_{\mathcal{G}^*(n)}(K, T^*) \tag{1.5}$$

Let (x_n, y_n) be the components of κ_n under this identification. By Lemma 1.4.11, $\mathrm{ind}(\kappa_n) = \mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*}(K, T^*)\big)$, then $y_n = 0$ and x_n is a generator of $\mathrm{ind}(\kappa_n)$. The decomposition in (1.5) induces a map in R^+ defined by

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

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

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

local coh. free of rk 1 □

Proof of Lemma 1.5.7. 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 1.4.11 and the last one from Lemma 1.5.12. □

1.5.2 Proof of Lemma 1.5.8

In order to prove Lemma 1.5.8, we need to show, for any $n \in \mathcal{N}_i$, the inclusion

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

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 1.3.4 (not fully exact, revise) implies that

$$\mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*_n}(K,T)\big) \subset \mathrm{Fitt}_{\nu(n)}^R\big(H^1_{\mathcal{F}^*}(K,T)\big)$$

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

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

Combining both inclusions, we can conclude the proof of Lemma 1.5.8.

1.5.3 Proof of Lemma 1.5.9

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

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

1.5.4 Proof of Lemma 1.5.10

Note that the element $n_r \in \mathcal{N}_r$ was already constructed in Lemma 1.5.9. 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 1.5.10.

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

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

1.6 Non-self dual Galois representations of rank 0

1.7 Old stuff

Lemma 1.7.1. ([Kim25, lemma 5.3]) If κ is a primitive Kolyvagin system, there is some $n \in \mathcal{N}$ such that $\delta_n \in R^*$.

Proof. By proposition 1.1.17, for every $n \in \mathcal{N}$ there is an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]) \longrightarrow H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]) \longrightarrow C_n^\vee \longrightarrow 0 \tag{1.6}$$

By proposition 0.1.2, there is some $n_0 \in \mathcal{N}$ such that

$$H^1_{\mathcal{F}^*(n_0)}(\mathbb{Q}, T^*) = 0$$

By lemma **??**,

$$H^1_{\mathcal{F}^*(n_0)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_{n_0}}]) = H^1_{\mathcal{F}^*(n_0)}(\mathbb{Q}, T^*)[\mathfrak{m}^{k_{n_0}}] = 0$$

Therefore, (1.6) implies that $C_{n_0} = 0$. Moreover, by lemma **??** and theorem **??**, $\mathrm{ord}(\delta_{n_0}) = \mathrm{ord}(\kappa_{n_0}) = 0$.

□

Remark 1.7.2. Assume either

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

Then $\mathrm{rank}_R(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee)$ 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 1.7.3. Assume R is a discrete valuation ring and write $\Theta_i(\kappa) = \mathfrak{m}^{n_i}$. Then

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

Proof. Write $\mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee\right)=\mathfrak{m}^{m_i}$, 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}:

$$m_i \leq \frac{m_{i+1}+m_{i-1}}{2} \tag{1.7}$$

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 (1.7) and we obtain

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

□

Proof of theorem **??**. If R is artinian, choose $k=\mathrm{length}(R)$. If R is a discrete valuation ring, we can choose some $k\in\mathbb{N}$ such that $\mathcal{P}_k\subset\mathcal{P}$ and

$$k \geq \mathrm{length}(H^1_{\mathcal{F}}(\mathbb{Q},T^*)^\vee_{\mathrm{tors}}) \tag{1.8}$$

It is enough to study the Fitting ideals of $H^1_{\mathcal{F}^*}(\mathbb{Q},T^*[\mathfrak{m}^k]^\vee)$. Indeed, let $\alpha_i\in\mathbb{Z}_{\geq 0}$ be such that $\mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee\right)=\mathfrak{m}^{\alpha_i}$. By lemma **??**,

$$\mathrm{Fitt}_i^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*[\mathfrak{m}^k])\right)=\mathrm{Fitt}_i^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee[\mathfrak{m}^j]\right)=\mathfrak{m}^{\min\{k,\alpha_i\}}$$

Since k has been chosen satisfying (1.8), then $\min\{k,\alpha_i\}=0$ if and only if $\alpha_i=0$.

For every $n\in\mathcal{N}$, consider the exact sequence

$$0\longrightarrow H^1_{\mathcal{F}_n}(\mathbb{Q},T/\mathfrak{m}^{k_n})\longrightarrow H^1_{\mathcal{F}}(\mathbb{Q},T/\mathfrak{m}^{k_n})\longrightarrow \textstyle\bigoplus_{\ell|n} H^1_{\mathrm{f}}(\mathbb{Q}_\ell,T/\mathfrak{m}^{k_n})$$

Note the last term is a free $R/\mathfrak{m}^{k_n}$-module of rank $\nu(n)$ by corollary **??**. Since $\chi(\mathcal{F})=0$, we have that

$$\min\{k_n,\alpha_i\}\leq \mathrm{length}\left(H^1_{\mathcal{F}_n}(\mathbb{Q},T/\mathfrak{m}^{k_n})\right)\leq \mathrm{length}\left(H^1_{\mathcal{F}(n)}(\mathbb{Q},T/\mathfrak{m}^{k_n})\right)$$

since $H^1_{\mathcal{F}_n}(\mathbb{Q}, T/\mathfrak{m}^{k_n}) \subset H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})$. By lemma **??**, for every $n \in \mathcal{N}$ such that $\nu(n) = i$, we then have that

$$\mathrm{ord}(\delta_n) \geq \alpha_i \Rightarrow \delta_n \in \mathfrak{m}^{\alpha_i}$$

Therefore,

$$\Theta_i(\kappa) \subset \mathrm{Fitt}_i^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])^\vee\right)$$

To prove the equality in (1.4) for some $i \in \mathbb{Z}_{\geq 0}$, we need to find some $n \in \mathcal{N}_k$ such that $\nu(n) = i$ and $\mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T)) = \alpha_i$.

If $\mathrm{Fitt}_i^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])^\vee\right) = 0$, then $\alpha_i = k$ and the result is clear. So let i be the rank of $H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^k) \cong H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])$ as an $R/\mathfrak{m}^k$-module.

Using an inductive application of corollary 0.1.4, we can choose primes $\ell_1, \ldots, \ell_i$ such that the maps

$$H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^k) \to \bigoplus_{k=1}^{i} H^1_{\mathrm{f}}(\mathbb{Q}_{\ell_i}, T/\mathfrak{m}^k), \quad H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]) \to \bigoplus_{k=1}^{i} H^1_{\mathrm{f}}(\mathbb{Q}_{\ell_i}, T^*[\mathfrak{m}^k])$$

are surjective. By lemma 0.1.5, for $n_r := \ell_1 \cdots \ell_i$ we have that $H^1_{\mathcal{F}^*(n_r)}(\mathbb{Q}, T^*[\mathfrak{m}^k]) = H^1_{\mathcal{F}^*_{n_r}}(\mathbb{Q}, T^*[\mathfrak{m}^k])$. Thus

$$\mathrm{ord}(\delta_{n_r}) = \mathrm{length}\left(H^1_{\mathcal{F}^*(n_r)}(\mathbb{Q}, T^*[\mathfrak{m}^k])\right) = \mathrm{length}\left(H^1_{\mathcal{F}^*_{n_r}}(\mathbb{Q}, T^*[\mathfrak{m}^k])\right) = \alpha_i$$

where the last equality comes from the structure theorem of finitely generated $R/\mathfrak{m}^k$-modules. Therefore, the equality holds for $i = r$.

For every $i > r$, construct $n_i \in \mathcal{N}$ and $h_i \in \mathbb{N}$ inductively as follows. Note that n_r was already constructed and let h_r be the exponent of $H^1_{\mathcal{F}^*(n_r)}(\mathbb{Q}, T^*[\mathfrak{m}^k])$

Assume that $n_i \in \mathcal{N}$ was already constructed satisfying that $\nu(n_i) = i$.xx

Write the structure of the Selmer group as

$$H^1_{\mathcal{F}(n_i)}(\mathbb{Q}, T/\mathfrak{m}^k) \approx H^1_{\mathcal{F}^*(n_i)}(\mathbb{Q}, T^*[\mathfrak{m}^k]) \approx R/\mathfrak{m}^{h_i} \times R/\mathfrak{m}^{e_{i+2}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for some integers $e_{i+2}, \ldots, e_s$. By lemma **??**, there are infinitely many primes $\ell_{i+1} \in \mathcal{P}_k$ satisfying that

$$H^1_{\mathcal{F}^*(n\ell_{i+1})}(\mathbb{Q}, T^*[\mathfrak{m}^k]) \approx R/\mathfrak{m}^{h_{i+1}} \times R/\mathfrak{m}^{e_{i+3}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

for $e_{i+2} \leq h_{i+1} \leq k$. We can choose the prime ℓ_{i+1} minimising h_{i+1} and define $n_{i+1} := n_i \ell_{i+1}$.

By lemma **??**

$$\delta_{n_i} R = \mathfrak{m}^{h_i} \prod_{j=i+2}^{s} \mathfrak{m}^{e_j} \subset \prod_{j=i+1}^{s} \mathfrak{m}^{e_j} = \mathrm{Fitt}_{i+1}^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])\right)$$

When $h_i = e_{i+i}$,

$$\Theta_{i+1}(\kappa) = \mathrm{Fitt}_{i+1}^{R/\mathfrak{m}^k}\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])\right)$$

When $h_i > e_{i+1} \geq e_{i+2}$ or $h_i \geq e_{i+1} > e_{i+2}$, lemma **??** implies the existence ℓ_{i+1} such that $h_{i+1} = e_{i+2}$.

If assumption (ii) holds true, then $\Theta_i(\kappa) \subsetneq \mathrm{Fitt}_i^R(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]))$ and $h_i > e_{i+1}$, so $h_{i+1} = e_{i+2}$.

Same result can be obtained assuming hypothesis (iii). In this case, $e_i > e_2$ and we obtain that

$$\Theta_{i+1}(\kappa) = \mathrm{Fitt}_{i+1}^R(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k])) \qquad \square$$

1.7.1 Non-self-dual case

In the case when T is not residually self-dual, we can improve the previous result to get the equality in (1.4) for every $i \in \mathbb{Z}_{\geq 0}$. More precisely, assume the following extra assumptions.

- (N1) $\mathrm{Hom}_{\mathbb{F}_p[G_\mathbb{Q}]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$.
- (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, the following improvement of theorem **??** is true. Sakamoto proves the equality (1.9) 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.

Theorem 1.7.4. Let $(T, \mathcal{F}, \mathcal{P})$ be a Selmer triple satisfying **??**-**??** and (N1)-(N2). Then for every $i \in \mathbb{Z}_{\geq 0}$, the following equality is satisfied:

$$\Theta_i(\kappa) = \mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) \tag{1.9}$$

The reason assuming (N1)-(N2) is that we can apply the following result.

Proposition 1.7.5. ([MR04, proposition 3.6.2]) Assume that T satisfies **??**-**??** and (N1)-(N2). Let $C \subset H^1(\mathbb{Q}, T)$ and $D \subset H^1(\mathbb{Q}, T^*)$ be finite submodules and choose some homomorphisms

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

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

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

The proof of theorem 1.7.4 is based on the following lemma.

Proof of theorem 1.7.4. Assume that

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

By theorem **??**,

$$\Theta_i(\kappa) \subset \mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right)$$

By lemma **??**, for every $i \in \mathbb{Z}_{\geq 0}$ we just need to find some $n \in \mathcal{N}$ such that $\nu(n) = i$ and $\mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) = \mathfrak{m}^{\lambda(n)}$, where $\lambda(n) = \mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]))$. For every $i \in \{0, \ldots, s\}$, we will construct some $n_i \in \mathcal{N}_k$ such that $\nu(n_i) = i$ and

$$H^1_{\mathcal{F}^*(n_i)}(\mathbb{Q}, T^*)^\vee \cong R/\mathfrak{m}^{e_{i+1}} \times \cdots \times R/\mathfrak{m}^{e_s}$$

The process for constructing the n_i was described in the proof of theorem **??** and, under assumptions (N1) and (N2), lemma 1.2.27 guarantees that $h_i = e_{i+1}$ for all i, so the Selmer group for $\mathcal{F}^*(n_i)$ has the desired structure.

□

Chapter 2

Patched Cohomology

2.1 Ultrafilters

2.1.1 Definition

Definition 2.1.1. 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 2.1.2. 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). $\square$

Last proposition can be reinterpreted in the following form:

Corollary 2.1.3. ([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 2.1.4. 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 2.1.5. 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 2.1.2, 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 2.1.10 below. They are those ultrafilters containing the Fréchet filter consisting of sets with finite complement.

Definition 2.1.6. The *Fréchet filter* is the collection of subsets of the natural number defined as

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

2.1.2 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 2.1.7. 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 2.1.8. The boolean ring structure in 2.1.7 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 2.1.9. 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 2.1.10. 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 2.1.9, $\mathcal{U}$ 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 $1 + S = \emptyset + S = S^c$. □

2.1.3 Ultraproducts

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

Definition 2.1.11. 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 2.1.12. (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 2.1.13. 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

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

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 2.1.14. 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 $\Psi(\varphi_n) \neq \Psi(\psi_n)$. $\square$

Notation 2.1.15. 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 2.1.16. 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 2.1.17. ([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 $\overline{\varepsilon}$. $\square$

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 2.1.18. 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 2.1.3 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 2.1.19. 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 2.1.17 and Lemma 2.1.18, 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. □

2.1.4 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 2.1.20. 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 2.1.21. 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 2.1.3 to define the Frobenius element associated to an ultraprime $\mathfrak{u}$ in the absolute Galois group G_K.

Proposition 2.1.22. 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 2.1.3 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 2.1.23. 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 2.1.24. In order to guarantee that Definition 2.1.23 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 $\mathrm{Frob}_{\ell_n} |_{L'} = \sigma$, for some $\sigma \in \mathrm{Gal}(L'/K)$ for $\mathcal{U}$-many n. For all those n, $\mathrm{Frob}_{\ell_n} |_L = \sigma |_L$, so $\sigma |_L$ coincides with Frob_{ℓ_n} for $\mathcal{U}$-many n.

Remark 2.1.25. Definition 2.1.23 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 2.1.26. 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 2.1.27. 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 2.1.28. 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 2.1.29. Let T be a G_K-module. We define an action of $G_{\mathfrak{u}}$ on T via the quotient $G_{\mathfrak{u}} \twoheadrightarrow \langle \mathrm{Frob}_{\mathfrak{u}} \rangle$.

2.2 Patched cohomology

2.2.1 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 2.2.1. 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

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

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

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

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

Proposition 2.2.2. 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 2.2.3. 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 □

2.2.2 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 2.2.4. 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 2.1.27.

Proposition 2.2.5. 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 2.1.18.

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 2.2.6. 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 2.2.7. (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 2.2.8. (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 2.2.9. 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 2.2.10. 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 2.2.11. 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 2.2.12. 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 2.2.13. 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 2.2.14. (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 2.1.13

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

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 2.1.14, 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.

limits □

finite cohomology annihilators

2.2.3 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 2.2.15. Let $\mathfrak{u}_1 = \left(\ell_k^{(1)}\right)_{k\in\mathbb{N}}, \ldots, \mathfrak{u}_s = \left(\ell_k^{(s)}\right)_{k\in\mathbb{N}}$ 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 2.2.16. ([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

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

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 2.2.17. 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 2.2.18. ([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 2.2.19. 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 2.2.20. ([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 2.2.19.

Definition 2.2.21. 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 2.2.22. ([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

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

2.2.4 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 2.2.23. 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 2.2.24. 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 2.2.25. By Proposition 2.2.22, 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 2.2.26. 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 2.2.27. ([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,

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

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 2.2.28. ([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 2.2.29. 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 2.2.6 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 2.1.17 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 2.1.17 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

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

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

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

$\square$

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

Definition 2.2.30. 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 2.2.14

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

Lemma 2.2.31. 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 2.2.30, 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 2.2.14. 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 2.1.14. By Proposition 1.1.17 and 2.1.17, 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 2.2.32. (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 2.2.29, 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 2.1.17, 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 2.2.31 and Proposition 2.1.17, 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 2.1.17.

profinite or ind-finite □

2.2.5 Patched Selmer modules

In this section, we endow the group T with an R-module structure, for some discrete valuation ring R.

Notation 2.2.33. 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 2.2.34. 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 2.2.35. (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 2.2.36. By [MR04, Lemma 3.7.1], if a Selmer structure on T is cartesian as in Definition 2.2.35, 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.

Proposition 2.2.37. 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 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

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

By the definition of Selmer group, there is an injection

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

Since the Selmer structure is cartesian, the product is torsion-free, so the domain is torsion free as well. By the snake's lemma, it implies that the top vertical map in the following diagram is injective.

$$\begin{tikzcd}
\mathbf{H}^1_{\mathcal{F}}(K,T)/\mathfrak{m}^k \arrow[r] \arrow[d, tail] & \mathbf{H}^1_{\mathcal{F}}(K,T/\mathfrak{m}^k) \arrow[d, tail] \\
\mathbf{H}^1(K,T)/\mathfrak{m}^k \arrow[r, tail] & \mathbf{H}^1(K,T/\mathfrak{m}^k)
\end{tikzcd}$$

Hence the top horizontal map is also injective. Snake's lemma shows that

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

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.

Proposition 2.2.38. 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

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

Proof. write □

assumptions on H^0

Proposition 2.2.39. Let $\mathcal{F}$ be a cartesian Selmer structure on T of core rank $\chi(\mathcal{F})$. Then

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

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 2.2.38, then

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

By Proposition 2.2.37, 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 $a + \chi(\mathcal{F})$. □

2.3 Ultra Kolyvagin systems

Definition 2.3.1. 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 3

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 2 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].

3.1 Preliminaries on exterior powers

The goal of this section is to introduce the necessary background to construct systems in the exterior biduals of the Selmer groups. The all have in common that they are constructed from different versions of maps of the following kind.

Proposition 3.1.1. 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 3.1.1.

Lemma 3.1.2. 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 $j \in \{1, \dots, s\}$ 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. $\square$

Lemma 3.1.3. 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] $\square$

Proof of proposition 3.1.1. Let I be the image of the map $N \to M$ inside Λ^s. By lemma 3.1.2, $\mathrm{Ext}^1(I, \Lambda)$ 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 3.1.3 implies that their duals are equal, so the above map can be rewritten as

$$\bigcap^{r+s} M^* \to \bigcap^r N^*$$

$\square$

Proposition 3.1.4. 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 3.1.1. 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 3.1.1. 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. $\square$

3.2 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 3.1.1, 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 3.2.1. 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 3.2.2. 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 $\square$

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

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

3.2.1 Weak core vertices

Definition 3.2.3 might seem abstract, but the Stark systems can be controlled by their values at some particular $n \in \mathcal{N}$.

Definition 3.2.4. 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 $\mathbf{H}^1_{\mathcal{F}}(\mathbb{Q}, \mathbf{T})$ is a free Λ-module of rank $r + \nu(n)$.

Proposition 3.2.5. 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

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

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 $r + \nu(n)$. □

Weak core vertices control the Stark systems.

Theorem 3.2.6. Let $n \in \mathcal{N}$ be a core vertex. Then the projection map

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

is an isomorphism.

Proof. 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 3.2.7. 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 3.2.8. Under assumption 3.2.7, 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 3.2.9. Let $\varepsilon = (\varepsilon)_{n\in\mathcal{N}}$ be a generator of $\mathbf{SS}(\mathcal{F})$. For every $m \in \mathcal{N}$, the image of $\varepsilon_m \in \operatorname{Hom}\left(\bigwedge^{r+\nu(m)} \mathbf{H}^1_{\mathcal{F}^m}(K,\mathbf{T})^+, \Lambda\right)$ contains the 0^{th} Fitting ideal of $\mathbf{H}^1_{\mathcal{F}^*_m}(\mathbb{Q},\mathbf{T}^*)$ with finite index.

Proof. By assumption 3.2.7 and proposition 3.2.5, there exists a core vertex n such that $m \mid n$, which leads to the following exact sequence

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

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 3.2.6 implies that ε_n generates $\bigcap^{r+\nu(n)}$. Since $\varepsilon_m = \phi_{n,m}(\varepsilon_n)$, then proposition 3.1.4 implies that the image of ε_n contains $\mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}_m}(\mathbb{Q},\mathbf{T}^*))$ with finite index. $\square$

Chapter 4

Cartesian systems

4.1 The graph of cartesian Selmer structures

Definition 4.1.1. We consider the graph CART 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 4.1.2. 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 2.2.32, there is an exact sequence

$$H^1_{\mathcal{F}}(K, T) \rightarrowtail H^1_{\mathcal{G}}(K, T) \longrightarrow \mathcal{L}_{\mathcal{G}/\mathcal{F}} \longrightarrow H^1_{\mathcal{G}^*}(K, T^*)^\vee \twoheadrightarrow H^1_{\mathcal{F}^*}(K, T^*)^\vee$$

By Proposition 2.2.39, we see that the rank of $\mathcal{L}_{\mathcal{G}/\mathcal{F}}$ is $\chi(\mathcal{G}) - \chi(\mathcal{F})$. □

Proposition 4.1.3. Let $\mathcal{F} \leq \mathcal{G}$ be cartesian Selmer structures. There is a canonical homomorphism

$$\bigcap^{\chi(\mathcal{G})} \mathbf{H}^1_{\mathcal{G}}(K, T) \otimes \det(\mathcal{L}_{\mathcal{G}/\mathcal{F}}) \to \bigcap^{\chi(\mathcal{F})} \mathbf{H}^1_{\mathcal{G}}(K, T)$$

Proof. use general properties of biduals □

Bibliography

[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]`.

[Eis95] David Eisenbud. *Commutative Algebra*. Springer New York, NY, 1995.

[Kim25] Chan-Ho Kim. *The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves*. 2025. arXiv: `2203.12159 [math.NT]`.

[MR04] Barry Mazur and Karl Rubin. 'Kolyvagin systems'. In: *Mem. Amer. Math. Soc.* 168.799 (2004), pp. viii+96.

[NSW00] Jürgen Neukirch, Alexander Schmidt and Key Wingberg. *Cohomology of number fields*. Grundlehren der mathematischen Wissenschaften. Springer-Berlin, Heidelberg, 2000, pp. xv–826.

[Sak18] Ryotaro Sakamoto. 'Stark systems over Gorenstein local rings'. In: *Algebra and Number Theory* 12.10 (2018), pp. 2295–2326.

[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`.